

UC Berkeley

UC Berkeley Electronic Theses and Dissertations

Title

Infinitely Many Supersingular Primes for Some Abelian Varieties

Permalink

<https://escholarship.org/uc/item/1281h5mk>

ISBN

9798189271229

Author

Chen, Fangu

Publication Date

2026-05-01

Peer reviewed|Thesis/dissertation

Infinitely Many Supersingular Primes for Some Abelian Varieties

by

Fangu Chen

A dissertation submitted in partial satisfaction of the

requirements for the degree of

Doctor of Philosophy

in

Mathematics

in the

Graduate Division

of the

University of California, Berkeley

Committee in charge:

Professor Yunqing Tang, Chair

Professor Sug Woo Shin

Professor Martin Olsson

Spring 2026

Infinitely Many Supersingular Primes for Some Abelian Varieties

Copyright 2026
by
Fangu Chen

Abstract

Infinitely Many Supersingular Primes for Some Abelian Varieties

by

Fangu Chen

Doctor of Philosophy in Mathematics

University of California, Berkeley

Professor Yunqing Tang, Chair

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 the work of Madapusi [Mad16], and on the analysis of real points of a Shimura curve, based on the work of Shimura [Shi75].

Baba and Granath ([BG08b]) generalize Elkies' theorem to abelian surfaces with quaternionic multiplication of discriminant 6, whose field of moduli is $\mathbb{Q}$ and which is a Jacobian in characteristic 2 and 3. We extend the field of moduli to any number field with a real embedding, and weaken the local conditions at 2 and 3. The proof relies on the intersection theory of Heegner divisors on Shimura curves.

Contents

Contents	i
1 Introduction	1
1.1 Background	1
1.2 The main results	1
1.3 Related works and heuristics	3
1.4 The strategy of the proof	4
2 Preliminaries	8
2.1 Intersection number	8
2.2 Quaternionic Shimura curves	9
3 Some Kuga-Satake abelian varieties	11
3.1 The Shimura curves	11
3.2 Integral model and special endomorphisms	15
3.3 CM points	18
3.4 Non-Archimedean place	24
3.5 Archimedean place	35
3.6 Proof of main theorem	41
3.7 Examples	48
4 Some QM abelian surfaces	50
4.1 The Shimura modular curves	50
4.2 CM points	51
4.3 Integral model and intersection number at bad primes	54
4.4 Proof of main theorem	56
Bibliography	60

Acknowledgments

I would like to express my sincere gratitude to my advisor, Yunqing Tang, for introducing this problem to me and for the many enlightening discussions that shaped this work. Her constant encouragement and support have been invaluable throughout my graduate studies. I feel truly fortunate to have learned from her, both in mathematics and beyond.

I thank Frank Calegari for helpful comments and the 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, and John Voight and Tonghai Yang for comments on a previous draft of this work.

I would also like to thank all the members of the Department of Mathematics at Berkeley for creating a supportive and stimulating academic environment. I am grateful to my friends Robin Huang and Phoebe Huang, who have introduced me to many new experiences and made these years both enjoyable and memorable.

Finally, I owe a debt of gratitude to my family, especially my mother, for her unconditional support. Their presence has been a constant source of strength throughout my life.

Chapter 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 ([Del+82, 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], [BG08b], [Li+25]). 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 results

Some Mumford's abelian fourfolds and Kuga-Satake abelian varieties

The main result of this work 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 1.2.1. *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 $\mathbb{P}_F^1$. 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 $\rho_i : F \hookrightarrow \mathbb{R}$, and ρ_i , $i = 1, \dots, n$, varies over the n different embeddings $F \hookrightarrow \mathbb{R}$;
4. $F(\sqrt{-\epsilon_1}, \dots, \sqrt{-\epsilon_n})$ has class number 1.

Let A be an abelian variety parametrized by the Hodge type Shimura datum (G, X) (see Section 3.1). 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.

Remark 1.2.2. Condition (4) in Theorem 1.2.1 is unnecessary; see Remark 3.5.5. However, removing this condition does not yield further examples covered by the theorem.

Remark 1.2.3. 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 1.2.4. *Let F be a totally real cubic number field with $\text{disc}(F) \in \{49, 81, 169, 321, 361, 473, 785, 993\}$ 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.*

See [Bou+25] for explicit equations for the Mumford-type Shimura curves when $\text{disc}(F)$ is 49 and 81. More examples satisfying all the assumptions of Theorem 1.2.1 can be found in Example 3.7.3.

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

²The 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.

Some abelian surfaces with quaternionic multiplication

We extend the result of [BG08b] to number fields with at least one real embedding, and weaken the local conditions at the bad reduction primes 2 and 3.

A special case of our main theorem is as follows.

Theorem 1.2.5. *Let C be a genus 2 curve with Jacobian that has multiplication by the maximal quaternion order with discriminant 6, and has field of moduli a number field L with at least one real embedding. Assume C has potentially smooth stable reduction at primes above 2 and 3. Then its Jacobian has superspecial reduction at infinitely many primes.*

More generally, the coarse moduli variety of principally polarized abelian surfaces with potential multiplication by the maximal quaternion order of discriminant 6 is isomorphic to $\mathbb{P}^1$, and an arithmetic j -function (see (4.1.0.1) in section 4.2) is defined in [BG08a]. In terms of this coordinate, the assumption at primes $\mathfrak{p}$ above 2 and 3 in Theorem 1.2.5 corresponds to the case $v_{\mathfrak{p}}(j(C)) = 0$ by [BG08b, Proposition 2], and our main theorem can be stated as follows.

Theorem 1.2.6. *Let C be a genus 2 curve with Jacobian that has multiplication by the maximal quaternion order with discriminant 6, and has field of moduli a number field L with at least one real embedding. Write $j_0 := j(C) \in L$ and $\mathrm{Nm}_{L/\mathbb{Q}}(j_0) = \frac{n}{d}$ with $n, d \in \mathbb{Z}$, $(n, d, 6) = 1$, $d > 0$. Assume at least one of the following conditions:*

1. $v_{\mathfrak{p}}(j_0) \leq 0$ for $\mathfrak{p}$ above 2, 3, and $[L : \mathbb{Q}] + v_3(d \mathrm{Nm}_{L/\mathbb{Q}}(27j_0 + 16))$ is odd or j_0 has at least one real conjugate in $(-\frac{16}{27}, 0)$;
2. $v_{\mathfrak{p}}(j_0) \geq 0$ for $\mathfrak{p}$ above 2, $v_{\mathfrak{p}}(j_0) \leq 0$ for $\mathfrak{p}$ above 3, and j_0 has at least one real conjugate in $(0, \infty)$;
3. $[L : \mathbb{Q}]$ is even, $v_{\mathfrak{p}}(j_0) \geq 0$ for $\mathfrak{p}$ above 2, 3, j_0 has at least one real conjugate in $(-\infty, -\frac{16}{27}) \cup (0, \infty)$.

Then the Jacobian of C has superspecial reduction at infinitely many primes.

1.3 Related works and heuristics

Elkies' result has been generalized to elliptic curves defined over more general number fields ([Jao03]), some families of abelian surfaces with quaternionic multiplication (see [BG08b] for the case of discriminant 6, and [Sad04] for the case of discriminant 21, 33), and some abelian fourfolds with an action of μ_5 ([Li+25]). 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 $A \bmod \mathfrak{p}$ lies in the Hecke orbit of a codimension

d subvariety $V \subset S_{\mathbb{F}_p}$ is roughly $(N\mathfrak{p})^{-d/2}$. Since

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

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; Sha+22; 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

Our proof builds on the idea of Elkies. 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 $\mathbb{Q}$ -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.

Kuga-Satake abelian varieties

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

³If 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 $\mathcal{O}_F[\sqrt{-\lambda}] \subseteq R \subseteq \mathcal{O}_{F(\sqrt{-\lambda})}$.

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 $\mathfrak{p}$.

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], [Li+25]), we follow the approach of Madapusi [Mad16] 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 [BG08b], 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.

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 $Z_\alpha := \{z \in \mathcal{H} : \alpha(\bar{z}) = z\}$, 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 [BG08b] 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 $\mathcal{F} := F(\sqrt{-\epsilon_1}, \dots, \sqrt{-\epsilon_n})$ 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 $\text{nrd}(v) = \lambda$, 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 the results at the non-archimedean place λ and the real places to obtain a desired supersingular prime using quadratic reciprocity theorem 1.4.1.

Theorem 1.4.1 ([Hec81, Theorem 167]). *Fix a number field K with r_1 real embeddings $\rho_1, \dots, \rho_{r_1} : K \hookrightarrow \mathbb{R}$. 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*

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

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

QM abelian surfaces

An abelian surface with action of a maximal order in a rational quaternion algebra B has either ordinary or superspecial reduction modulo primes not dividing the discriminant of B ([Cla03, p.70] and [Rib89, p.23]). It therefore suffices to construct primes of supersingular reduction, for which we follow Elkies' general strategy. Given a genus 2 curve C , we find supersingular reduction of its Jacobian from its intersection with some Heegner cycle $\mathcal{P}_D$ of discriminant D . The intersection at a prime p is captured by $v_p(P_D(j_0)) > 0$, where $P_D(x)$ is the integral minimal polynomial of the j -invariants of the points in $\mathcal{P}_D$, and when this occurs, supersingular reduction at p is detected by $\left(\frac{D}{p}\right) \neq 1$.

As in [BG08b], we need to consider certain elliptic point in addition to the Heegner cycle in order to pair the roots of $P_D(x)$ modulo primes dividing D . We use [Jao03] to generalize [BG08b] through a more detailed, case-by-case study, where in each case the discriminant D is chosen in a form adapted to the conditions. In characteristic 2 and 3, [BG08b] shows that the reduction of any Heegner cycle lies in the superspecial locus $\{j = 0, \infty\}$, and the intersection formula of Heegner divisors in [KR08] provides the new input that determines the specific superspecial point for each chosen Heegner cycle. The local conditions on j_0 at primes above 2 and 3 ensure that it avoids intersection with the chosen Heegner cycles at these primes. This is a showcase of relaxing the assumption on B in Theorem 1.2.1. For more

on the choice of local conditions and Heegner cycles, and for potential further weakenings of these conditions, see Remark 4.4.1.

Chapter 2

Preliminaries

2.1 Intersection number

Definition 2.1.1. Let R be a Dedekind domain and $\mathcal{X} \rightarrow \operatorname{Spec} R$ 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 2.1.2. 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 $\mathcal{X} \rightarrow \operatorname{Spec} R$, 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 $\mathcal{A} \rightarrow \mathcal{X}$, then the complete local ring $\widehat{\mathcal{O}}_{\mathcal{X}, z_0}$ is the universal deformation ring for z_0 and

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

2. if $\mathcal{X} = \mathbb{P}_R^1$ 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 2.1.3. *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 $\mathcal{Y} \rightarrow \operatorname{Spec} R$ 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 $(R[[T]])^{G_{y_0}} = R[[\operatorname{Nm}_{\overline{G}_{y_0}}(T)]]$, where $\overline{G}_{y_0}$ is the image of G_{y_0} in $\operatorname{Aut}_R(R[[T]])$ and $\operatorname{Nm}_{\overline{G}_{y_0}}(T) = \prod_{\gamma \in \overline{G}_{y_0}} \gamma(T)$.*
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 $\underline{y}, \underline{y}' : \widehat{\mathcal{O}}_{\mathcal{Y}, y_0} \rightarrow R$, respectively. Let $\underline{x}, \underline{x}'$ be the images of $\underline{y}, \underline{y}'$, respectively, then*

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

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

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

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]

□

2.2 Quaternionic Shimura curves

Let F be 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. Let B be a quaternion algebra over F split at exactly one real place $\rho : F \hookrightarrow \mathbb{R}$, and $\mathcal{O} = \mathcal{O}_B$ be a maximal order of B .¹

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

$$|B_{>0}^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times| = |F_{>0}^\times \backslash \widehat{F}^\times / \operatorname{nrd}(\widehat{\mathcal{O}}^\times)| = h_+(F) = 1, \quad (2.2.0.1)$$

and then

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

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

where

$$\begin{aligned}\tilde{\Gamma} &= \{\alpha \in \mathcal{O}^\times : \text{nrd}(\alpha) \in \mathcal{O}_F^\times \text{ is totally positive}\}, \\ \tilde{\Gamma}^1 &= \mathcal{O}^1 = \{\alpha \in \mathcal{O}^\times : \text{nrd}(\alpha) = 1\}.\end{aligned}$$

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

Let $\tilde{\Gamma}^* = \{\alpha \in N_{B^\times}(\mathcal{O}) : \text{nrd}(\alpha) \text{ is totally positive}\}$. Since F has narrow class number 1,

$$\tilde{\Gamma}^* / F^\times \tilde{\Gamma} = N_{B^\times}(\mathcal{O}) / F^\times \mathcal{O}^\times \simeq \prod_{\text{prime ideal } \mathfrak{p} \mid \text{disc}(B)} (\mathbb{Z}/2\mathbb{Z})$$

is the Artin-Lehner group of $\mathcal{O}$, and there is a finite map

$$\tilde{\Gamma} \backslash \mathcal{H} \rightarrow \tilde{\Gamma}^* \backslash \mathcal{H}$$

of degree $2^{\#\text{finite primes ramified in } B}$.

In Chapter 3, we will consider the case when $[F : \mathbb{Q}] > 1$ and B is unramified at all finite primes. In Chapter 4, we will consider the case when $F = \mathbb{Q}$ and B is ramified at some finite primes.

Chapter 3

Some Kuga-Satake abelian varieties

In this chapter, assume the following unless specified otherwise.

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 . 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 . Its normalizer $N_{B^\times}(\mathcal{O}) = F^\times \mathcal{O}^\times$.

In §3.1, we introduce the Shimura curves considered in this work. In §3.2, we review the theory of integral canonical model for Shimura varieties of Hodge type, focusing on the GSpin case. In §3.3, we construct the CM cycles and study their basic properties. In §3.4, we investigate the reduction of the CM cycles modulo a finite prime, and pair the liftings in the neighborhood of each closed point. In §3.5, we analyze the distribution of the CM points in the real locus of the Shimura curve. In §3.6, we combine the results in previous sections to prove Theorem 1.2.1. In §3.7, we compute explicit examples in which all the technical assumptions of Theorem 1.2.1 are satisfied.

3.1 The Shimura curves

The GSpin Shimura varieties

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 $F \subseteq \text{End}_{Hdg}(V)$.

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 $\text{GSpin}(V, Q)$ over $\mathbb{Q}$ is defined by

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

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 $\bigoplus_{d=0}^\infty V^{\otimes d}$, and the spinor norm $\nu : \text{GSpin}(V, Q) \rightarrow \mathbb{G}_m$ 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 $\psi_\delta : C(V) \times C(V) \rightarrow \mathbb{Q}$, $(x, y) \mapsto \text{Trd}(x\delta y^*)$. The action of $\text{GSpin}(V, Q)$ on $C(V)$ by left multiplication induces an embedding $\text{GSpin}(V, Q) \hookrightarrow \text{GSp}(C(V), \psi_\delta)$, under which the similitude character on $\text{GSp}(C(V), \psi_\delta)$ restricts to the spinor norm ν on $\text{GSpin}(V, Q)$ ([Mad16, 1.6, 1.7]).

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

$$1 \rightarrow \mathbb{G}_m \rightarrow \text{GSpin}(V, Q) \rightarrow \text{SO}(V, Q) \rightarrow 1. \quad (3.1.0.1)$$

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

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

for any $\mathbb{Q}$ -algebra R , so that the image of G under (3.1.0.1) is G_0 . Since $(\alpha, \beta) \mapsto \text{Tr}_{F/\mathbb{Q}}(\alpha\beta)$ is a perfect pairing on the $\mathbb{Q}$ -vector space F , we have $G_0(\mathbb{Q}) = \text{SO}(V, Q_F)(F) = B^\times/F^\times$.

The embedding

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

realizes (G, X) as a Shimura datum of Hodge type. When F is cubic, we have $\text{Cor}_{F/\mathbb{Q}}(B) \simeq M_8(\mathbb{Q})$ since B is split at all finite places, and this Kuga-Satake construction from K3 type Hodge structures with real multiplication is consistent with Mumford's original construction ([Gee08, 6.4]).

The morphism of Shimura data

We can use the corestriction of algebras to describe the morphism $\tilde{G} = \text{Res}_{F/\mathbb{Q}} \text{GL}_{1,B} \rightarrow G$ ([Mum69, §4], [Gee08, 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

$$C(V) \otimes_{\mathbb{Q}} \tilde{F} = C_{\tilde{F}}(V \otimes_{\mathbb{Q}} \tilde{F}) = \widehat{\bigotimes}_{\sigma: F \hookrightarrow \tilde{F}} C_{\tilde{F}}(V \otimes_{F, \sigma} \tilde{F}) = \widehat{\bigotimes}_{\sigma: F \hookrightarrow \tilde{F}} (C_F(V) \otimes_{F, \sigma} \tilde{F}), \quad (3.1.0.2)$$

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 $\bigotimes_{\sigma: F \hookrightarrow \tilde{F}} (C_F^+(V) \otimes_{F, \sigma} \tilde{F})$ lies in the even part of $\widehat{\bigotimes}_{\sigma: F \hookrightarrow \tilde{F}} (C_F(V) \otimes_{F, \sigma} \tilde{F})$. The Galois group $\text{Gal}(\tilde{F}/\mathbb{Q})$ 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 $g \in \text{Gal}(\tilde{F}/\mathbb{Q})$, we have $g: V \otimes_{F, \sigma} \tilde{F} \rightarrow V \otimes_{F, g\sigma} \tilde{F}$ defined by $r \otimes a \mapsto r \otimes g(a)$. Similarly, $\text{Gal}(\tilde{F}/\mathbb{Q})$ acts on $C(V) \otimes_{\mathbb{Q}} \tilde{F}$ via the second factor of the tensor product. Over $\tilde{F}$, we have

$$(C_F^+(V) \otimes_{\mathbb{Q}} \tilde{F})^{\times} = \prod_{\sigma: F \hookrightarrow \tilde{F}} (C_F^+(V) \otimes_{F, \sigma} \tilde{F})^{\times}$$

and a group homomorphism

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

where the norm map is defined by

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

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 $(C_F^+(V) \otimes_{\mathbb{Q}} \tilde{F})^{\times} \rightarrow G(\tilde{F})$. Taking $\text{Gal}(\tilde{F}/\mathbb{Q})$ -invariants gives a group homomorphism $C_F^+(V)^{\times} \rightarrow G(\mathbb{Q})$. Under the identification $C_F^+(V) \xrightarrow{\sim} B$, we obtain the corresponding morphism of algebraic groups $\tilde{G} \rightarrow G$ over $\mathbb{Q}$, whose kernel is the algebraic torus T_F^1 over $\mathbb{Q}$ defined by $T_F^1(\mathbb{Q}) = \{x \in F^{\times} : \text{Nm}_{F/\mathbb{Q}} x = 1\}$. The morphism $\tilde{G} \rightarrow G$ induces $\tilde{G}^{\text{der}} \rightarrow G^{\text{der}}$

and the following diagram

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \\
 & & T_F^1 & \xrightarrow{x \mapsto x^2} & T_F^1 & & \\
 & & \downarrow & & \downarrow & & \\
 1 & \longrightarrow & \tilde{G}^{\text{der}} & \longrightarrow & \tilde{G} & \xrightarrow{\text{nrd}} & \text{Res}_{F/\mathbb{Q}} \mathbb{G}_m \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \text{Nm}_{F/\mathbb{Q}} \\
 1 & \longrightarrow & G^{\text{der}} & \longrightarrow & G & \xrightarrow{\nu} & \mathbb{G}_m \longrightarrow 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & 1 & & 1 & &
 \end{array}$$

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

The integral structures

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 a quaternion $\mathcal{O}_F$ order $\mathcal{O}'$ we have $\mathcal{O}' = \mathcal{O}_F + \text{discrd}(\mathcal{O}')(\mathcal{O}'^\#)^0(\mathcal{O}'^\#)^0 = C_{\mathcal{O}_F}^+((\mathcal{O}'^\#)^0, N \text{nrd})$, where $\text{discrd}(\mathcal{O}') = (N)$ and

$$(\mathcal{O}'^\#)^0 = \{\alpha \in B : \text{trd}(\alpha \mathcal{O}') \subseteq \mathcal{O}_F, \text{trd}(\alpha) = 0\}.$$

Here $\text{discrd}(\mathcal{O}) = \text{disc}(B) = (1)$ and $\mathcal{O}^\# = \mathcal{O}$ since $\mathcal{O}$ is maximal and B is split at all finite places. Define

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

The image of $\tilde{K} = \widehat{\mathcal{O}}^\times = \prod \mathcal{O}_v^\times$ under $\tilde{G} \rightarrow G \rightarrow G_0$ 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 $\{g \in K_0 : g \text{ acts trivially on } L_{\widehat{\mathbb{Z}}}^\vee / L_{\widehat{\mathbb{Z}}}\}$ ([Mad16, 2.6]). The dual lattice $L^\vee = \mathfrak{D}_{F/\mathbb{Q}}^{-1} L \subset V$, where $\mathfrak{D}_{F/\mathbb{Q}} \subset \mathcal{O}_F$ is the different of $F/\mathbb{Q}$. There are well-defined maps

$$\tilde{G}(\mathbb{Q}) \backslash \mathcal{H}^\pm \times \tilde{G}(\mathbb{A}_f) / \tilde{K} \rightarrow G_0(\mathbb{Q}) \backslash X \times G_0(\mathbb{A}_f) / K_0 \quad (3.1.0.3)$$

and

$$G(\mathbb{Q}) \backslash X \times G(\mathbb{A}_f) / K \rightarrow G_0(\mathbb{Q}) \backslash X \times G_0(\mathbb{A}_f) / K_0. \quad (3.1.0.4)$$

Note that $1 \rightarrow \text{Res}_{F/\mathbb{Q}} \mathbb{G}_m \rightarrow \tilde{G} \rightarrow G_0 \rightarrow 1$ and

$$H^1(\mathbb{Q}_l, \text{Res}_{F/\mathbb{Q}} \mathbb{G}_m) \simeq H^1(\mathbb{Q}_l, \prod_{v|l} \text{Res}_{F_v/\mathbb{Q}_l} \mathbb{G}_m) \simeq \prod_{v|l} H^1(\mathbb{Q}_l, \text{Res}_{F_v/\mathbb{Q}_l} \mathbb{G}_m) \simeq \prod_{v|l} H^1(F_v, \mathbb{G}_m)$$

is trivial by Hilbert's 90. Therefore, the map (3.1.0.3) is surjective, and in particular, $G_0(\mathbb{Q}) \backslash X \times G_0(\mathbb{A}_f)/K_0$ is connected. Let $\Gamma_0 := G_0(\mathbb{Q})_+ \cap K_0 \subset F^\times \mathcal{O}^\times / F^\times$, then (3.1.0.3) is an isomorphism

$$\tilde{\Gamma} \backslash \mathcal{H} \xrightarrow{\sim} \Gamma_0 \backslash X^+, \quad (3.1.0.5)$$

where $\tilde{\Gamma} = \{\alpha \in \mathcal{O}^\times : \text{nrd}(\alpha) \in \mathcal{O}_F^\times \text{ is totally positive}\}$. 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 (3.1.0.4) gives a finite map

$$\Gamma_g \backslash X^+ \rightarrow \Gamma_0 \backslash X^+. \quad (3.1.0.6)$$

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 (3.1.0.4), then the corresponding abelian varieties $\mathcal{A}_{x_1}, \mathcal{A}_{x_2}$ are isogenous.

Genus 0 Shimura curves

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

3.2 Integral model and special endomorphisms

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 $L_{(p)} \xrightarrow{\sim} L_{(p)}^\vee$, and $\text{GSpin}(V, Q)$ extends to a reductive group scheme $\text{GSpin}(L_{(p)}, Q)$ over $\mathbb{Z}_{(p)}$. Via left multiplication, the group $C^+(L_{(p)}) \subset \text{GL}(H_{(p)})$ is the subgroup of automorphisms that preserves the grading and centralizes the right $C(L_{(p)})$ -action on $H_{(p)}$. The pairing

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

on $\text{End}(H_{(p)})$ restricts to $[\cdot, \cdot]_Q$ on $L_{(p)}$ since $[v, v] = \frac{1}{2^{3[F:\mathbb{Q}]-1}} \text{Tr}(Q(v)|_{H_{(p)}}) = 2Q(v)$ for all $v \in L_{(p)}$. Let $\pi : \text{End}(H_{(p)}) \rightarrow \text{End}(H_{(p)})$ be the orthogonal projection onto $L_{(p)}$. Then $\text{GSpin}(L_{(p)}, Q) \subset C^+(L_{(p)})$ is the stabilizer of the idempotent operator π ([Mad16, 1.4]). For $\epsilon_1, \dots, \epsilon_m \in \mathcal{O}_F$ such that $\mathcal{O}_F = \mathbb{Z}[\epsilon_1, \dots, \epsilon_m]$, consider the endomorphism $\pi_{\epsilon_i} : \text{End}(H_{(p)}) \rightarrow \text{End}(H_{(p)})$ given by $\pi_{\epsilon_i}(\varphi) = \epsilon_i(\pi(\varphi))$. Let $G_{\mathbb{Z}_{(p)}} \subset \text{GSpin}(L_{(p)}, Q)$ be the stabilizer of all π_{ϵ_i} . Let $\{s_\alpha\} \subset H_{(p)}^\otimes$ denote a finite collection of tensors defining $G \subset \text{GL}(H_{(p)})$ with $\pi, \pi_{\epsilon_i} \in \{s_\alpha\}$.

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 $\text{Sh}_{K_p K^p} = \text{Sh}_{K_p K^p}(G, X)$ the Shimura curve attached to G and $\mathcal{S}_{K_p K^p}$ its integral

canonical model. The integral model $\mathcal{S}_{K_p K^p}$ is constructed in [Kis10] as the normalization of $\mathcal{S}_{K_p K^p}^-(G, X)$, the closure of $\text{Sh}_{K_p K^p}$ in the natural integral model of the Siegel modular variety. The normalization step can be removed by [Xu22]. Let $\mathcal{A} \rightarrow \mathcal{S}_{K_p K^p}$ denote the universal abelian scheme, which exists assuming that K^p sufficiently small. Let $s_{\alpha, ?}$ denote the cohomological realizations of s_α , where $? = B, \text{dR}, \ell, p, \text{cris}$.

Let $k = \mathbb{F}_q \subset \overline{\mathbb{F}}_p$ and $W = W(k)$ be its ring of Witt vectors. Suppose $x \in \mathcal{S}_{K_p K^p}(k)$ is a closed point. Write $\widehat{U}_x$ for the completion of $\mathcal{S}_{K_p K^p}$ at x . Suppose $\tilde{x} \in \mathcal{S}_{K_p K^p}(E)$ 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

$$H_{\text{dR}}^1(\mathcal{A}_{\tilde{x}}/E) \otimes_{E, \iota} \mathbb{C} \xrightarrow{\sim} H_B^1(\mathcal{A}_{\iota(\tilde{x})}(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C} \quad (3.2.0.1)$$

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

$$H_B^1(\mathcal{A}_{\iota(\tilde{x})}(\mathbb{C}), \mathbb{Z}_{(p)}) \otimes_{\mathbb{Z}_{(p)}} \mathbb{Z}_p \xrightarrow{\sim} H_{\text{ét}}^1(\mathcal{A}_{\tilde{x}_E}, \mathbb{Z}_p) \quad (3.2.0.2)$$

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

$$H_{\text{ét}}^1(\mathcal{A}_{\tilde{x}_E}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} B_{\text{cris}} \xrightarrow{\sim} H_{\text{cris}}^1(\mathcal{A}_x/W) \otimes_W B_{\text{cris}}, \quad (3.2.0.3)$$

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

$$H_{\text{ét}}^1(\mathcal{A}_{\tilde{x}_E}, \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} W \rightarrow H_{\text{cris}}^1(\mathcal{A}_x/W) \quad (3.2.0.4)$$

taking $s_{\alpha, p, \tilde{x}}$ to $s_{\alpha, \text{cris}, x}$ ([Kis10, 1.4.3]). From (3.2.0.2) and (3.2.0.4), there exists a W -linear isomorphism $H_{(p)} \otimes_{\mathbb{Z}_{(p)}} W \rightarrow H_{\text{cris}}^1(\mathcal{A}_x/W)$ taking s_α to $s_{\alpha, \text{cris}, x}$, and the tensors $s_{\alpha, \text{cris}, x}$ define a reductive subgroup $G_W \subset GL(H_{\text{cris}}^1(\mathcal{A}_x/W))$, which is isomorphic to $G_{\mathbb{Z}_{(p)}} \times_{\text{Spec } \mathbb{Z}_{(p)}} \text{Spec } W$. Let $\mathbf{L}_{\text{cris}, x}$ be the image of $\pi_{\text{cris}, x}$ on $\text{End}(H_{\text{cris}}^1(\mathcal{A}_x/W))$, then since all π_{ϵ_i} and the quadratic form on $L_{(p)}$ are absolute Hodge cycles, there is an $\mathcal{O}_F$ -linear isometry

$$L_{(p)} \otimes_{\mathbb{Z}_{(p)}} W \rightarrow \mathbf{L}_{\text{cris}, x}, \quad (3.2.0.5)$$

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

$$\mathbf{L}_{\text{cris}, x} \simeq L_{(p)} \otimes_{\mathbb{Z}_{(p)}} W = \bigoplus_{\sigma' : F \hookrightarrow W[p^{-1}]} L \otimes_{\mathcal{O}_F, \sigma'} W, \quad (3.2.0.6)$$

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 $\text{Spf } R_{G_W}$, where R_{G_W} is the complete local ring at the identity section of the opposite unipotent defined by a cocharacter $\mathbb{G}_m \rightarrow G_W$

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

$$H_{\text{dR}}^1(\mathcal{A}_{\tilde{x}'}/E') \xrightarrow{\sim} H_{\text{cris}}^1(\mathcal{A}_x/W) \otimes_W E'$$

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

We follow [Mad16, 5.1-5.13] to define the space of special endomorphisms $L(\mathcal{A}_x)$ of a point $x \rightarrow \mathcal{S}_{K_p K^p}$.

Special endomorphism at a $\mathbb{C}$ -point

Let $x \rightarrow \text{Sh}_{K_p K^p}$ be a geometric point with $k(x) \subseteq \mathbb{C}$ and ℓ be a rational prime. The comparison isomorphism

$$H_B^1(\mathcal{A}_x(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell} \xrightarrow{\sim} H_{\text{ét}}^1(\mathcal{A}_x, \mathbb{Q}_{\ell}) \quad (3.2.0.7)$$

takes $s_{\alpha, B, x} \otimes 1$ to $s_{\alpha, \ell, x}$. Let $\mathbf{V}_{\ell, x}$ be the image of $\pi_{\ell, x}$, then (3.2.0.7) induces an F -linear isometry

$$V \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell} \xrightarrow{\sim} \mathbf{V}_{\ell, x}. \quad (3.2.0.8)$$

Let $\mathbf{L}_{\ell, x} = \mathbf{V}_{\ell, x} \cap \text{End}(T_{\ell}(\mathcal{A}_x))$, 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

$$H_B^1(\mathcal{A}_x(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell} \xrightarrow{\sim} H_{\text{ét}}^1(\mathcal{A}_x, \mathbb{Z}_{\ell}) \quad (3.2.0.9)$$

and $L = V \cap \text{End}(C(L))$, under (3.2.0.8) we have

$$L \otimes_{\mathbb{Z}} \mathbb{Z}_{\ell} \simeq \mathbf{L}_{\ell, x}. \quad (3.2.0.10)$$

Definition 3.2.1 ([Mad16, 5.4, 5.5]). An endomorphism $f \in \text{End}(\mathcal{A}_x)$ is special if it satisfies any of the equivalent conditions:

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

Special endomorphism at a $\overline{\mathbb{F}}_p$ -point

Let $x \in \mathcal{S}_{K_p K^p}(\overline{\mathbb{F}}_p)$ and $\ell \neq p$.

Definition 3.2.2. An endomorphism $f \in \text{End}(\mathcal{A}_x)$ is special if its crystalline realization lies in $\mathbf{L}_{\text{cris}, x}$.

The definition of $\mathbf{V}_{\ell, x}$ and $\mathbf{L}_{\ell, x}$ carries over since $T_{\ell}(\mathcal{A}_{\tilde{x}}) \xrightarrow{\sim} T_{\ell}(\mathcal{A}_x)$ for any lift $\mathcal{A}_{\tilde{x}}$ of $\mathcal{A}_x$. By [Mad16, 5.13], if $f \in \text{End}(\mathcal{A}_x)$ is special, then its ℓ -adic realization is an element of $\mathbf{L}_{\ell, x}$.

3.3 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 3.3 using subtori of $\tilde{G}$. Each CM cycle on $\tilde{G}(\mathbb{Q}) \backslash \mathcal{H}^\pm \times \tilde{G}(\mathbb{A}_f) / \tilde{K} = \tilde{\Gamma} \backslash \mathcal{H} \simeq \Gamma_0 \backslash X^+$ corresponds to an $\mathcal{O}_F$ -order in a CM extension of F by Lemma 3.3.1, and it is defined over F by Lemma 3.3.2. Its size equals the class number of the corresponding $\mathcal{O}_F$ -order, as shown in Lemma 3.3.5 and computed in Lemma 3.3.6. The specific $\mathcal{O}_F$ -orders we will consider are described in 3.3.7. Finally, using the Shimura-Taniyama formula, we obtain in 3.3.10 a sufficient condition for the primes at which the abelian varieties on the CM cycle have supersingular reduction.

CM cycles

Let $L = F(\sqrt{-\lambda})$ be a CM extension of F and $\phi : L \hookrightarrow B$ be an embedding.¹ 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 $\tilde{T} = \text{Res}_{L/\mathbb{Q}} \mathbb{G}_m$ and $\tilde{h} : \text{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m \rightarrow \tilde{G}_{\mathbb{R}}$ be the cocharacter defined by

$$\mathbb{C}^\times \rightarrow \prod_{\sigma: F \hookrightarrow \mathbb{R}} \mathbb{C}^\times = \prod_{\sigma: F \hookrightarrow \mathbb{R}} (L \otimes_{F, \sigma} \mathbb{R})^\times = L \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\phi} B \otimes_{\mathbb{Q}} \mathbb{R}, \quad (3.3.0.1)$$

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

$$\tilde{T}(\mathbb{Q}) \backslash \{\tilde{h}\} \times \tilde{T}(\mathbb{A}_f) / K_{\tilde{T}} \hookrightarrow \tilde{G}(\mathbb{Q}) \backslash \mathcal{H}^\pm \times \tilde{G}(\mathbb{A}_f) / \tilde{K}, \quad (3.3.0.2)$$

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

This CM cycle can be described via optimal embeddings $\phi^{-1}(\mathcal{O}) \hookrightarrow \mathcal{O}$ by Lemma 3.3.1, which is a special case of the trace formula [Voi21, 30.4.7]. Let

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

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 embeddings $\phi^{-1}(\mathcal{O}) \hookrightarrow \mathcal{O}$. Given $e_1 \in \hat{\mathcal{E}}$, if $[\tilde{h}, e_1] = [\tilde{h}, e_2]$ in $\tilde{G}(\mathbb{Q}) \backslash \mathcal{H}^\pm \times \tilde{G}(\mathbb{A}_f) / \tilde{K}$

¹Such 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 .

with $e_2 \in \tilde{G}(\mathbb{A}_f)$, then there exist $a \in \tilde{G}(\mathbb{Q})$ and $k \in \tilde{K} = \hat{\mathcal{O}}^\times$ such that $e_2 = ae_1k \in \hat{\mathcal{E}}$. Thus, $e \mapsto [\tilde{h}, e]$ defines a bijection from $\phi(L)^\times \backslash \hat{\mathcal{E}}/\hat{\mathcal{O}}^\times$ to a set of CM points in $\tilde{G}(\mathbb{Q}) \backslash \mathcal{H}^\pm \times \tilde{G}(\mathbb{A}_f)/\tilde{K}$. Note that $\tilde{T}(\mathbb{A}_f) \hookrightarrow \hat{\mathcal{E}}$.

Lemma 3.3.1. 1. When $\hat{B}^\times = B^\times \hat{\mathcal{O}}^\times$, the set of CM points $\{[\tilde{h}, e] : e \in \hat{\mathcal{E}}\}$ 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 $\{[\tilde{h}, e] : e \in \hat{\mathcal{E}}\}$ is the image of the CM cycle $\tilde{T}(\mathbb{Q}) \backslash \{\tilde{h}\} \times \tilde{T}(\mathbb{A}_f)/K_{\tilde{T}}$, which has cardinality $h(\phi^{-1}(\mathcal{O}))$.

Proof. 1. Clearly $\mathcal{E} \subset \hat{\mathcal{E}}$ and there is a natural map $\phi(L)^\times \backslash \mathcal{E}/\mathcal{O}^\times \rightarrow \phi(L)^\times \backslash \hat{\mathcal{E}}/\hat{\mathcal{O}}^\times$. This is injective since $B \cap \hat{\mathcal{O}}^\times = \mathcal{O}^\times$. For any $\hat{\beta} \in \hat{B}^\times$, since $\hat{B}^\times = B^\times \hat{\mathcal{O}}^\times$, there is $\beta \in B^\times$ such that $\hat{\beta} \hat{\mathcal{O}}^\times = \beta \hat{\mathcal{O}}^\times$. Note that the class $\beta \mathcal{O}^\times$ is well-defined, and $\hat{\beta} \in \hat{\mathcal{E}}$ if and only if $\beta \in \mathcal{E}$. Therefore, for $[\tilde{h}, \hat{\beta}]$ where $\hat{\beta} \in \hat{\mathcal{E}}$, pick $\beta \in \mathcal{E}$ such that $\hat{\beta} \mathcal{O}^\times = \beta \mathcal{O}^\times$, then $[\tilde{h}, \hat{\beta}] = [\tilde{h}, \beta] = [\beta^{-1} \cdot \tilde{h}, 1]$, 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 $\phi(L)^\times \backslash \hat{\mathcal{E}}/\hat{\mathcal{O}}^\times \rightarrow \widehat{\phi(L)}^\times \backslash \hat{\mathcal{E}}/\hat{\mathcal{O}}^\times$ whose fiber over the identity element is $\phi(L)^\times \backslash \widehat{\phi(L)}^\times / (\widehat{\phi(L)}^\times \cap \hat{\mathcal{O}}^\times) \simeq \text{Pic}(\phi^{-1}(\mathcal{O}))$. There is a bijection

$$\widehat{\phi(L)}^\times \backslash \hat{\mathcal{E}}/\hat{\mathcal{O}}^\times \xrightarrow{\sim} \{\hat{\mathcal{O}}^\times\text{-conjugacy classes of optimal } \widehat{\phi^{-1}(\mathcal{O})} \hookrightarrow \hat{\mathcal{O}}\}.$$

In the case B is split at all finite primes of F , since

$$\#\{GL_2(\mathcal{O}_{F_v})\text{-conjugacy classes of optimal } S \hookrightarrow M_2(\mathcal{O}_{F_v})\} = 1$$

for any $\mathcal{O}_{F_v}$ -order S by [Voi21, 30.5.3], we have $\#\widehat{\phi(L)}^\times \backslash \hat{\mathcal{E}}/\hat{\mathcal{O}}^\times = \prod_v 1 = 1$. □

Lemma 3.3.2. When B is split at all finite primes of F , complex conjugation defines an involution on the CM cycle $\tilde{T}(\mathbb{Q}) \backslash \{\tilde{h}\} \times \tilde{T}(\mathbb{A}_f)/K_{\tilde{T}}$. 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 $t \in \tilde{T}(\mathbb{A}_f)$, its complex conjugate is $[\iota \tilde{h}, t]$ ([MS81]), where $\iota \tilde{h}$ is induced by $\bar{\phi} : L \hookrightarrow B$, $\bar{\phi}(z) = \phi(\bar{z})$. By the Skolem-Noether theorem, there exists $\beta \in B^\times$ such that $\bar{\phi}(\alpha) = \beta^{-1} \phi(\alpha) \beta$, 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 $\beta^{-1} \phi(L) \beta = \bar{\phi}(L) = \phi(L)$ and $\beta^{-1} \phi(\phi^{-1}(\mathcal{O})) \beta = \phi(\phi^{-1}(\mathcal{O})) = \phi(\phi^{-1}(\mathcal{O})) = \phi(L) \cap \mathcal{O}$, we have $\beta \in \mathcal{E}$, then $\bar{t} \beta \in \hat{\mathcal{E}}$, and the result follows from the second part of Lemma 3.3.1. □

Lemma 3.3.3. 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 $\tilde{T}(\mathbb{Q}) \backslash \{\tilde{h}\} \times \tilde{T}(\mathbb{A}_f)/K_{\tilde{T}}$ defined by ϕ .

Proof. Existence of a real point follows from Lemma 3.3.2. Note that $\widehat{B}^\times = B^\times \widehat{\mathcal{O}}^\times$ by (2.2.0.1). Then by Lemma 3.3.1, 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 $t \in \tilde{T}(\mathbb{A}_f)$ 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 $\beta \in \tilde{T}(\mathbb{Q})\tilde{K}$, and then $[\tilde{h}, \bar{t}\beta] = [\tilde{h}, \bar{t}]$.

By Lemma 3.3.5, there is an isomorphism of groups $i : \tilde{T}(\mathbb{Q}) \backslash \tilde{T}(\mathbb{A}_f) / K_{\tilde{T}} \xrightarrow{\sim} \text{Pic}(\phi^{-1}(\mathcal{O}))$ 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 $\tilde{T}(\mathbb{Q}) \backslash \tilde{T}(\mathbb{A}_f) / K_{\tilde{T}} \simeq \text{Pic}(\phi^{-1}(\mathcal{O})) \rightarrow \text{Pic}(\mathcal{O}_F) = \text{Cl}(F)$. 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 $I\bar{I} = \text{Nm}_{L/F}(I)\phi^{-1}(\mathcal{O})$ a principal ideal in $\phi^{-1}(\mathcal{O})$. Then the real CM points in this CM cycle correspond to the 2-torsion points in $\text{Pic}(\phi^{-1}(\mathcal{O}))$. Under the assumption that $h(\phi^{-1}(\mathcal{O}))$ is odd, there is a unique 2-torsion point in $\text{Pic}(\phi^{-1}(\mathcal{O}))$; thus there is a unique real CM point in this cycle. $\square$

Lemma 3.3.4. *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 $\text{Gal}(L/F)$.*

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 $\text{disc}_{L/F}(R) = f^2 \text{disc}_{L/F}(\mathcal{O}_L)$. 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 $R = \mathcal{O}_F + f\mathcal{O}_K$. $\square$

Lemma 3.3.5. *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 $\mathbb{A}_{L, f}^\times / (L^\times \prod_{\mathfrak{p}} R_{\mathfrak{p}}^\times) \simeq \text{Pic}(R)$.*

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 $\mathbb{I}_{\mathfrak{f}, R} := \{(\alpha_{\mathfrak{q}}) \in \mathbb{A}_{L, f}^\times : (\alpha_{\mathfrak{q}})_{\mathfrak{q}|\mathfrak{p}} \in R_{\mathfrak{p}}^\times \text{ for all } \mathfrak{p}|\mathfrak{f}\} \text{ and } L_{\mathfrak{f}, R} := \{x \in L^\times : x \in R_{\mathfrak{p}}^\times \text{ for all } \mathfrak{p}|\mathfrak{f}\} = L^\times \cap \mathbb{I}_{\mathfrak{f}, R}$. 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 $\mathbb{I}_{\mathfrak{f}, R} / ((L^\times \prod_{\mathfrak{p}} R_{\mathfrak{p}}^\times) \cap \mathbb{I}_{\mathfrak{f}, R}) \xrightarrow{\sim} \mathbb{A}_{L, f}^\times / (L^\times \prod_{\mathfrak{p}} R_{\mathfrak{p}}^\times)$, 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 $J(R, \mathfrak{f}) \xrightarrow{\sim} J(\mathcal{O}_L, \mathfrak{f})$ ([Neu99, I.12.6, I.12.10]). The natural map $\mathbb{I}_{\mathfrak{f}, R} \rightarrow J(\mathcal{O}_L, \mathfrak{f})$

has kernel $\prod_{\mathfrak{p}} R_{\mathfrak{p}}^{\times}$ and defines an isomorphism

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

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

$$J(\mathcal{O}_L, \mathfrak{f})/\{x\mathcal{O}_L : x \in L_{\mathfrak{f}}\} \rightarrow \text{Pic}(R), \quad (3.3.0.3)$$

whose composition with $\text{Pic}(R) \rightarrow \text{Pic}(\mathcal{O}_L) \simeq J(\mathcal{O}_L, \mathfrak{f})/\{x\mathcal{O}_L \in J(\mathcal{O}_L, \mathfrak{f}) : x \in L\}$ is surjective. Then surjectivity of (3.3.0.3) follows from the exact sequence $(\mathcal{O}_L/\mathfrak{f}\mathcal{O}_L)^{\times}/(R/\mathfrak{f}\mathcal{O}_L)^{\times} \rightarrow \text{Pic}(R) \rightarrow \text{Pic}(\mathcal{O}_L) \rightarrow 1$ ([Neu99, I.12.9, I.12.11]) and surjectivity of $\{x \in L^{\times} : x\mathcal{O}_L \in J(\mathcal{O}_L, \mathfrak{f})\} \rightarrow (\mathcal{O}_L/\mathfrak{f}\mathcal{O}_L)^{\times}$. $\square$

Lemma 3.3.6. *Let F be a totally real number field with odd narrow class number, and $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ 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. $\square$

3.3.7. 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 corresponding 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 3.3.6, both orders have odd class numbers, and therefore, each corresponding CM cycle has a unique real point.

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 $C_F^+(V) \xrightarrow{\sim} B$, under which $C_F^+(V_v) \xrightarrow{\sim} \phi(L)$. Thus, we have $\text{Res}_{F/\mathbb{Q}} \text{GSpin}(V_v, F) \hookrightarrow \text{Res}_{F/\mathbb{Q}} \text{GSpin}(V, F)$ 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 $\mathbb{C} \rightarrow C_F^+(V_v) \otimes_{F,\rho} \mathbb{R}$ 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 $\text{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m \rightarrow (\text{Res}_{F/\mathbb{Q}} \text{GSpin}(V, F))_{\mathbb{R}}$. Under the isomorphism $C_F^+(V) \otimes_{F,\rho} \mathbb{R} \simeq B \otimes_{F,\rho} \mathbb{R}$, we have

$$\{e_1e_2, e_2e_1\} = \left\{ \frac{1}{\sqrt{\lambda}}v, -\frac{1}{\sqrt{\lambda}}v \right\}. \quad (3.3.0.4)$$

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

Definition field

Let $\tilde{\mu} = \mu_{\tilde{h}} : \mathbb{G}_{m,\mathbb{C}} \rightarrow \tilde{T}_{\mathbb{C}}$ be the cocharacter defined by $\tilde{\mu}(z) = \tilde{h}_{\mathbb{C}}(z, 1)$. Let T be the image of $\tilde{T}$ in G and μ (resp. h) be the composition $\mathbb{G}_{m,\mathbb{C}} \xrightarrow{\tilde{\mu}} \tilde{T}_{\mathbb{C}} \rightarrow T_{\mathbb{C}}$ (resp. $\text{Res}_{\mathbb{C}/\mathbb{R}} \mathbb{G}_m \xrightarrow{\tilde{h}} \tilde{T}_{\mathbb{R}} \rightarrow T_{\mathbb{R}}$). 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 $K' \subset \tilde{T}(\mathbb{A}_f)$ be a compact open subgroup such that K'_p is maximal and K'^p is small enough such that $\text{Sh}_{K'}(T, \{h\}) := T(\mathbb{Q}) \backslash \{h\} \times T(\mathbb{A}_f)/K'$ is a fine moduli space for abelian varieties with Hodge cycles and sufficiently high level structure away from p . By definition of canonical model, $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/L)$ acts on $\text{Sh}_{K'}(T, \{h\})$ by

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

and the homomorphism $r(T, \mu) : \text{Res}_{L/\mathbb{Q}} \mathbb{G}_m = \tilde{T} \rightarrow T$ is the natural surjection under $T \simeq \tilde{T}/T_F^1$. Then there exists an abelian extension L'/L , unramified at the primes above p , such that $\text{Gal}(\overline{\mathbb{Q}}/L')$ fixes $\text{Sh}_{K'}(T, \{h\})$. 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 $\text{Sh}_{K'}(T, \{h\})$, the abelian varieties are defined over L' . Moreover, since $\text{Gal}(\overline{\mathbb{Q}}/L')$ fixes μ , it fixes the special endomorphism.

Supersingular reduction

Lemma 3.3.8. *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 $E \subseteq \text{End}^0(A/K)$ (so that $E^* \subseteq K$). 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^* . 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 $\sigma \in \text{Hom}(E, \overline{\mathbb{Q}})$, where

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

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 $N_{\Phi} : E^{*\times} \rightarrow E^{\times}$ described by $N_{\Phi}(a) = \prod_{\psi \in \Phi^*} \psi(a)$. Let $\tilde{\sigma} \in \text{Aut}(\tilde{E})$ 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, $N_{\Phi}(\alpha) \cdot cN_{\Phi}(\alpha) = \text{Nm}_{E^*/\mathbb{Q}}(\alpha)$ and $v(\text{Nm}_{E^*/\mathbb{Q}}(\alpha)) = v(\text{Nm}_{E^*/\mathbb{Q}} \mathfrak{q}'^N) = v(p^{f(\mathfrak{q}'/p)N})$. Thus, the Newton slopes are all $\frac{1}{2}$. $\square$

Corollary 3.3.9. *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 $E \subseteq \text{End}^0(A/K)$. 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 $E_i \subseteq \text{End}^0(A_i/K)$. 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. $\square$

3.3.10. For a CM abelian variety A constructed from $L = F(\sqrt{-\lambda}) \hookrightarrow B$, since the Hodge cocharacter factors through $\text{Res}_{L/\mathbb{Q}} \mathbb{G}_m$, elements of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ 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 $\mathfrak{P}$.

3.4 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 3.4.6 and Proposition 3.4.8, which together show that CM liftings of a closed point $x \in \mathcal{S}_{K_0}(k)$ occur in pairs when we consider liftings to cycles corresponding to all orders containing $\mathcal{O}_F[\sqrt{-\lambda}]$. Proposition 3.4.6 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 parametrized by a GSpin Shimura variety as the deformation space of isotropic lines in [Mad16, 5.16], which we adapt to our setting in Lemma 3.4.2 by considering the F -linear structure on $\mathbf{L}_{\text{cris},x}$ defined by $\pi_{\varepsilon_i, \text{cris}, x}$. In addition, we define an F -linear structure on the space of special quasi-endomorphisms $V(\mathcal{A}_x)$ in section 3.4. When $\mathcal{A}_x$ is supersingular, the structure of $V(\mathcal{A}_x)$ as a quadratic space over F is described in Lemma 3.4.3 and Lemma 3.4.4.

Extra work is required when x admits an even order automorphism, analogous to the case $j = 1728$ in [Elk87; Elk89]. In this situation, Lemma 3.4.5 and Lemma 3.4.10 give a pairing of the special endomorphisms, which in turn yields a pairing of liftings in Proposition 3.4.8. Moreover, Proposition 3.4.8 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 $\rho = \iota \circ \rho'$.

Lifting of abelian varieties

Let $x \in \mathcal{S}_{K_p K^p}(k)$ be a closed point and $\widehat{U}_x$ be the completion of $\mathcal{S}_{K_p K^p}$ at x . We follow [Mad16, 5.15, 5.16] to relate the infinitesimal deformations of x to the liftings of certain isotropic lines in the quadratic spaces associated to $\mathbf{L}_{\text{cris},x}$, and then apply the Grothendieck existence theorem to lift a compatible system of such deformations to a certain finite extension of W .

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

$$\left\{ \begin{array}{c} \text{Isomorphism classes of} \\ \text{abelian schemes over } \mathcal{O}_2 \text{ lifting } \mathcal{A}_{x_1} \end{array} \right\} \xrightarrow{\sim} \left\{ \begin{array}{c} \text{Direct summands } \text{Fil}^1 \mathbf{H}_{\mathcal{O}_2} \subset \mathbf{H}_{\mathcal{O}_2} \\ \text{lifting } \text{Fil}^1 \mathbf{H}_{\mathcal{O}_1} \end{array} \right\} \quad (3.4.0.1)$$

by Serre-Tate theory ([Kat81, 1.2.1]) and Grothendieck-Messing theory ([Mes72, V. 1.6]).²

²Serre-Tate theory and Grothendieck-Messing theory apply to surjections $\mathcal{O} \rightarrow \overline{\mathcal{O}}$ such that p is nilpotent

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

Theorem 3.4.1 (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 $\mathrm{Hom}_R(X, Y) \rightarrow \varprojlim \mathrm{Hom}_{R_n}(X_n, Y_n)$ is bijective.*

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

Lemma 3.4.2. *Suppose p is an odd prime unramified in F . Let $k = \mathbb{F}_q \subset \overline{\mathbb{F}}_p$ and $x \in \mathcal{S}_{K_p K^p}(k)$. Suppose E is a finite extension of $W[p^{-1}]$ of ramification index $e \leq p-1$ with uniformizer ϖ . Let*

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

Then there is a natural bijection

$$\{\tilde{x} \in \mathcal{S}_{K_p K^p}(E) \text{ lifting } x\} \xrightarrow{\sim} \{\mathrm{Fil}^1(\mathbf{L}_{\mathrm{cris},x} \otimes_W E) \in \mathrm{Iso} \text{ lifting } \mathrm{Fil}^1 \mathbf{L}_{\mathrm{dR},x}\}. \quad (3.4.0.2)$$

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

$$\left\{ \begin{array}{l} \tilde{x} \in \mathcal{S}_{K_p K^p}(E) \text{ lifting } x, \\ \tilde{v} \in L(\mathcal{A}_{\tilde{x}}) \text{ lifting } v \end{array} \right\}^3 \xrightarrow{\sim} \left\{ \begin{array}{l} \mathrm{Fil}^1(\mathbf{L}_{\mathrm{cris},x} \otimes_W E) \in \mathrm{Iso} \text{ lifting } \mathrm{Fil}^1 \mathbf{L}_{\mathrm{dR},x} \\ \text{and orthogonal to } v \end{array} \right\}. \quad (3.4.0.3)$$

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

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

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

$$\mathrm{Fil}^1(H_{\mathrm{cris}}^1(\mathcal{A}_x/W) \otimes_W E) = \ker(\mathrm{Fil}^1(\mathbf{L}_{\mathrm{cris},x} \otimes_W E)) = \mathrm{im}(\mathrm{Fil}^1(\mathbf{L}_{\mathrm{cris},x} \otimes_W E)). \quad (3.4.0.4)$$

in $\mathcal{O}$ 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 uniformizing 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.

³If $\tilde{v}$ 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 $\mathrm{Fil}^1(\mathbf{L}_{\mathrm{cris},x} \otimes_W E)$ lifts $\mathrm{Fil}^1 \mathbf{L}_{\mathrm{dR},x}$ as $\mathrm{Fil}^1(H_{\mathrm{cris}}^1(\mathcal{A}_x/W) \otimes_W E)$ lifts $\mathrm{Fil}^1 H_{\mathrm{dR}}^1(\mathcal{A}_x/k)$. By construction, the filtration on $H_{\mathrm{dR}}^1(\mathcal{A}_{\tilde{x}}/E) \otimes_{E,\iota} \mathbb{C} \simeq H_B^1(\mathcal{A}_{\iota(\tilde{x})}(\mathbb{C}), \mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{C}$ 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 $\pi_{\epsilon_i, B, \iota(\tilde{x})} \otimes 1$ 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 (3.2.0.1) takes $\pi_{\epsilon_i, \mathrm{dR}, \tilde{x}} \otimes 1$ to $\pi_{\epsilon_i, B, \iota(\tilde{x})} \otimes 1$, we have $\pi_{\epsilon_i, \mathrm{dR}, \tilde{x}}(w) \otimes_{E, \iota} 1 = w \otimes_{E, \iota} \rho(\epsilon_i)$, i.e., $\pi_{\epsilon_i, \mathrm{dR}, \tilde{x}}(w) = \rho'(\epsilon_i)w$.

To show the map (3.4.0.2) is a bijection, we work successively with the thickenings $\mathcal{O}_E/(\varpi^n) \rightarrow \mathcal{O}_E/(\varpi^{n-1})$ following the proof of [Mad16, 5.16] and then apply Grothendieck existence theorem. Let Iso_n denote the set of isotropic lines in $\mathbf{L}_{\mathrm{cris},x} \otimes_W (\mathcal{O}_E/(\varpi^n))$ on which each $\pi_{\epsilon_i, \mathrm{cris}, x} \otimes 1$ 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 $\mathrm{Fil}^1 \mathbf{L}_{\mathrm{dR},x}$, and consider

$$\left\{ x_n \in \widehat{U}_x(\mathcal{O}_E/(\varpi^n)) \text{ lifting } x_{n-1} \right\} \rightarrow \{ l_n \in \mathrm{Iso}_n \text{ lifting } l_{n-1} \}. \quad (3.4.0.5)$$

Injectivity of (3.4.0.5) follows from (3.4.0.1) and the correspondence

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

Then we can prove (3.4.0.5) 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 (3.4.0.5) is a 1-dimensional vector space over $\mathcal{O}_E/(\varpi)$. On the other hand, since $\mathbf{L}_{\mathrm{cris},x}$ 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 (3.4.0.5) is $\{ \langle w_n + \varpi^{n-1}u \rangle \subset \mathbf{L}_{\mathrm{cris},x} \otimes_W (\mathcal{O}_E/(\varpi^n)) : \varpi^{n-1}u \perp w_n, (\pi_{\epsilon_i, \mathrm{cris}, x} \otimes 1)(u) = \rho'(\epsilon_i)u \} \simeq \{ u \in \mathbf{L}_{\mathrm{cris},x} \otimes_W (\mathcal{O}_E/(\varpi)) : u \in l_1^\perp, (\pi_{\epsilon_i, \mathrm{cris}, x} \otimes 1)(u) = \rho'(\epsilon_i)u \} / l_1$, which is a 1-dimensional $\mathcal{O}_E/(\varpi)$ -vector space. Hence (3.4.0.5) is a bijection. Applying Theorem 3.4.1 to a compatible system of polarized abelian varieties associated to $\{l_n\}$, the map (3.4.0.2) is a bijection.

For (3.4.0.3), by Theorem 3.4.1, given a lift $\tilde{x} \in \mathcal{S}_{K_p K^p}(E)$ 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 $v_{\mathrm{cris},n} \in \mathbf{L}_{\mathcal{O}_E/(\varpi^n)}$ preserves the Hodge filtration $\mathrm{Fil}^1 \mathbf{H}_{\mathcal{O}_E/(\varpi^n)}$ if and only if $v_{\mathrm{cris},n} \in \mathrm{Fil}^0 \mathbf{L}_{\mathcal{O}_E/(\varpi^n)}$ if and only if $v_{\mathrm{cris},n}$ is orthogonal to $\mathrm{Fil}^1 \mathbf{L}_{\mathcal{O}_E/(\varpi^n)}$. $\square$

Structure of the space of special endomorphisms

Let $x \in \mathcal{S}_{K_p K^p}(k)$ be a closed point and $v \in L(\mathcal{A}_x)$ be a special endomorphism. By Lemma 3.4.2 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 π_{ϵ_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 $\pi_{\epsilon_i}(\tilde{v})$ agrees with $\pi_{\epsilon_i, \mathrm{cris}, x}(v_{\mathrm{cris}})$ in $\mathbf{L}_{\mathrm{cris},x}$. Applying this process to a basis for $L(\mathcal{A}_x)$ shows

that it is stable under the $\mathcal{O}_F$ -action on $\mathbf{L}_{\text{cris},x}$, thereby endowing $L(\mathcal{A}_x)$ with an $\mathcal{O}_F$ -linear structure compatible with that on $\mathbf{L}_{\text{cris},x}$ and $\mathbf{L}_{\ell,x}$ 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 $\text{Tr}_{F/\mathbb{Q}}$ is perfect, and for $u, w \in L(\mathcal{A}_x)$, $[\epsilon_i u, w]_{Q'} = [\pi_{\epsilon_i, \text{cris}, x} u_{\text{cris}}, w_{\text{cris}}]_{\text{cris}} = [u_{\text{cris}}, \pi_{\epsilon_i, \text{cris}, x} w_{\text{cris}}]_{\text{cris}} = [u, \epsilon_i w]_{Q'}$, there is a quadratic form Q'_F on $V(\mathcal{A}_x)$ over F determined by $\text{Tr}_{F/\mathbb{Q}}(f[u, w]_{Q'_F}) = [fu, w]_{Q'}$ for all $f \in F$. In particular, $Q' = \text{Tr}_{F/\mathbb{Q}} \circ Q'_F$. The orthogonal direct sum decompositions

$$\begin{aligned} (V(\mathcal{A}_x) \otimes_{\mathbb{Q}} W[p^{-1}], Q') &= \bigoplus_{\sigma': F \hookrightarrow W[p^{-1}]} (V(\mathcal{A}_x) \otimes_{F, \sigma'} W[p^{-1}], \sigma' \circ Q'_F), \\ \mathbf{L}_{\text{cris},x}[p^{-1}] \simeq (V \otimes_{\mathbb{Q}} W[p^{-1}], Q) &= \bigoplus_{\sigma': F \hookrightarrow W[p^{-1}]} (V \otimes_{F, \sigma'} W[p^{-1}], \sigma' \circ Q_F) \end{aligned}$$

and the F -linear isometric embedding

$$V(\mathcal{A}_x) \otimes_{\mathbb{Q}} W[p^{-1}] \hookrightarrow \mathbf{L}_{\text{cris},x}[p^{-1}] \quad (3.4.0.6)$$

induce an isometric embedding

$$(V(\mathcal{A}_x) \otimes_{F, \sigma'} W[p^{-1}], \sigma' \circ Q'_F) \hookrightarrow (V \otimes_{F, \sigma'} W[p^{-1}], \sigma' \circ Q_F) \quad (3.4.0.7)$$

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

$$\begin{aligned} (V(\mathcal{A}_x) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}, Q') &= \bigoplus_{v|\ell} (V(\mathcal{A}_x) \otimes_F F_v, \text{Tr}_{F_v/\mathbb{Q}_{\ell}} \circ Q'_F), \\ \mathbf{V}_{\ell,x} \simeq (V \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell}, Q) &= \bigoplus_{v|\ell} (V \otimes_F F_v, \text{Tr}_{F_v/\mathbb{Q}_{\ell}} \circ Q_F) \end{aligned}$$

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

$$V(\mathcal{A}_x) \otimes_{\mathbb{Q}} \mathbb{Q}_{\ell} \hookrightarrow \mathbf{V}_{\ell,x} \quad (3.4.0.8)$$

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

$$(V(\mathcal{A}_x) \otimes_F F_v, Q'_F) \hookrightarrow (V \otimes_F F_v, Q_F) \quad (3.4.0.9)$$

of quadratic spaces over F_v for each $v|\ell$. The next lemma shows that (3.4.0.6) – (3.4.0.9) are isomorphisms when $\mathcal{A}_x$ is supersingular.

Lemma 3.4.3. *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 [Mad16, 5.12]. The Tate-conjecture ([Mad15, 6.4]) implies that under the natural isometric embedding $V(\mathcal{A}_x)_{\mathbb{Q}_p} = L(\mathcal{A}_x) \otimes_{\mathbb{Z}} \mathbb{Q}_p \hookrightarrow \mathbf{L}_{\text{cris},x} \otimes_W W(\bar{k})[p^{-1}]$, the subspace $V(\mathcal{A}_x)_{\mathbb{Q}_p}$ consists of Frobenius invariant vectors in the isocrystal $\mathbf{L}_{\text{cris},x} \otimes_W W(\bar{k})[p^{-1}]$, 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 $V(\mathcal{A}_x) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \hookrightarrow \mathbf{V}_{\ell,x} \simeq V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ is an isomorphism for the dimension reason.

Since $Q' = \text{Tr}_{F/\mathbb{Q}} \circ Q'_F$, 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 $V(\mathcal{A}_x) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \xrightarrow{\simeq} \mathbf{V}_{\ell,x} \simeq V \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ 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 $v \nmid \ell$. $\square$

Lemma 3.4.4. *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. Moreover, 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 $x_1, \dots, x_n$ ($n = 3[F : \mathbb{Q}]$) of $L \otimes_{\mathbb{Z}} \mathbb{Z}_p \simeq \oplus_{\sigma': \mathcal{O}_F \rightarrow \mathbb{Z}_p} L \otimes_{\mathcal{O}_F, \sigma'} \mathbb{Z}_p$ 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

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

Under the fixed isomorphism $\iota : \overline{W[p^{-1}]} \rightarrow \mathbb{C}$, 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 $G^{\text{der}} \simeq \text{Res}_{F/\mathbb{Q}} \text{SL}_{1,B}$, which is simply connected, and the embedding $G \hookrightarrow \text{GSpin}(V, Q)$ induces

$$G/G^{\text{der}} \simeq \text{GSpin}(V, Q) / \text{GSpin}(V, Q)^{\text{der}} \simeq \mathbb{G}_m,$$

if we set $b = x_3(p^{-1}x_1 + x_2) \in G(\mathbb{Q}_p) \subset \text{GSpin}(V, Q)(\mathbb{Q}_p)$, then the isocrystal $\mathbf{L}_{\text{cris},x} \otimes_W K$ 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 $M^\perp = \bigoplus_{\sigma' \neq \rho'} V \otimes_{F,\sigma'} \mathbb{Q}_p$. 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 . $\square$

By definition, we have

$$L(\mathcal{A}_x) = \{v \in V(\mathcal{A}_x) : v_{\text{cris}} \in \mathbf{L}_{\text{cris},x}, v_\ell \in \mathbf{L}_{\ell,x} \text{ for all } \ell \neq p\}. \quad (3.4.0.10)$$

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

Lemma 3.4.5. *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 $\alpha \in \text{SO}(V(\mathcal{A}_x), Q'_F)$ such that $\alpha(\mathbf{L}_{\text{cris},x}) = \mathbf{L}_{\text{cris},x}$ under the identification $L(\mathcal{A}_x) \otimes_{\mathbb{Z}} W \simeq \mathbf{L}_{\text{cris},x}$ and $\alpha(\mathbf{L}_{\ell,x}) = \mathbf{L}_{\ell,x}$ under the identification $L(\mathcal{A}_x) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \simeq \mathbf{L}_{\ell,x}$ 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 3.4.3 and Lemma 3.4.4, 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

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

Since $\text{SO}(B'^0, \text{nrd}|_{B'^0}) = B'^\times / F^\times$ 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 (3.4.0.7) 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 $g_{\sigma'} \circ \alpha \circ g_{\sigma'}^{-1}(x) = u_{\sigma'} x u_{\sigma'}^{-1}$ for all $x \in V \otimes_{F, \sigma'} W[p^{-1}]$. Since the automorphism preserves $\mathbf{L}_{\text{cris}, x} \simeq L \otimes_{\mathbb{Z}} W = \bigoplus_{\sigma': F \hookrightarrow W[p^{-1}]} L \otimes_{\mathcal{O}_F, \sigma'} W$, 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, $\sigma'(Q'_F(u')) = \text{nrd}(u_{\sigma'}) \in W[p^{-1}]^\times$ has even valuation, and $u_{\sigma'} \in L \otimes_{\mathcal{O}_F, \sigma'} W$ if and only $\text{nrd}(u_{\sigma'})$ 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 (3.4.0.9) 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 $\mathbf{L}_{\ell, x} \simeq L \otimes_{\mathbb{Z}} \mathbb{Z}_\ell = \bigoplus_{v|\ell} L \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v}$, we have

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

In particular, $Q'_F(u') = \text{nrd}(u_v) \in F_v^\times$ has even valuation, and $u_v \in L \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v}$ if and only if $\text{nrd}(u_v)$ 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 $\sum_{\sigma': F \hookrightarrow W[p^{-1}]} c_1 c_2 u_{\sigma'} \in \mathbf{L}_{\text{cris}, x}$ and $\sum_{v|\ell} c_1 c_2 u_v \in \mathbf{L}_{\ell, x}$ for all $\ell \neq p$. $\square$

Pairing at points without even order automorphisms

Let T be an $\mathcal{S}_{K_p K^p}$ -scheme, then $x \in \mathcal{S}_{K_p K^p}(T)$ gives a triple $(\mathcal{A}_x, \lambda_x, \bar{\eta}_x)$, where $(\mathcal{A}_x, \lambda_x : \mathcal{A}_x \rightarrow \mathcal{A}_x^\vee)$ is a polarized abelian scheme over T up to isomorphism and the level structure $\eta \in \Gamma(T, \text{Isom}_G(H_{\widehat{\mathbb{Z}}^p}, \varprojlim_{p \nmid n} \mathcal{A}_x[n])/K^p)$. An integral model $\mathcal{S}_{K_0}$ of $\Gamma_0 \backslash X^+$ is constructed from $\mathcal{S}_{K_p K^p}$ by action of a finite group. Two points $x_1, x_2 \in \mathcal{S}_{K_p K^p}(\mathbb{C})$, corresponding to $(\mathcal{A}_{x_1}, \lambda_1, \bar{\eta}_1), (\mathcal{A}_{x_2}, \lambda_2, \bar{\eta}_2)$, are identified in $\mathcal{S}_{K_0}$ if there is a prime-to- p quasi-isogeny $\mathcal{A}_{x_1} \rightarrow \mathcal{A}_{x_2}$ that preserves polarization up to $\mathbb{Z}_{(p)}^\times$, sends s_{α, B, x_1} to s_{α, B, x_2} and takes $\mathbf{L}_{\ell, x_1}$ to $\mathbf{L}_{\ell, x_2}$ for all $\ell \neq p$.

Proposition 3.4.6. *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 (3.3.0.2). For $x \in \mathcal{S}_{K_0}(k)$ without even order automorphisms,⁴ points in the CM cycle lifting x are paired, i.e., there is a map*

$$\{\text{lifts of } x \text{ in (3.3.0.2)}\} \longrightarrow \{\langle v \rangle : v \in L(\mathcal{A}_x), Q'_F(v) = \lambda\} / \text{Aut}(x)$$

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 3.3, 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 $\mathcal{A}_{\tilde{x}}$ is supersingular by 3.3.10. 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 $L(\mathcal{A}_x) \hookrightarrow \mathbf{L}_{\text{cris},x}$, then $\text{Fil}^1 \mathbf{L}_{\text{dR},x} \in v_{\text{cris}}^\perp$ over k . By (3.2.0.6), we have an orthogonal direct sum decomposition $v_{\text{cris}} = \sum_{\sigma' : F \hookrightarrow W[p-1]} v_{\text{cris},\sigma'}$ and $Q_{\text{cris},x}(v_{\text{cris},\sigma'}) = \sigma'(Q_F(\tilde{v})) = \sigma'(\lambda)$, where $Q_{\text{cris},x}$ denotes the quadratic form on $\mathbf{L}_{\text{cris},x}$. 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 3.4.2. 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 $\mathbf{L}_{\text{dR},x}$ that are orthogonal to $(v_{\text{cris},\rho'} \otimes 1)$ in the subspace of $\mathbf{L}_{\text{cris},x} \otimes_W \mathcal{O}_E$ where each $\pi_{\epsilon_i, \text{cris},x}$ acts as $\rho'(\epsilon_i) \otimes 1$, by the linear algebra computation Lemma 3.4.7.

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-isogeny $f : \mathcal{A}_{\tilde{x}_1} \rightarrow \mathcal{A}_{\tilde{x}_2}$ that sends $s_{\alpha,?,\tilde{x}_1}$ to $s_{\alpha,?,\tilde{x}_2}$, where $? = \ell, p, \text{dR}$, and takes $\mathbf{L}_{\ell,\tilde{x}_1}$ to $\mathbf{L}_{\ell,\tilde{x}_2}$ and $\mathbf{L}_{p,\tilde{x}_1}$ to $\mathbf{L}_{p,\tilde{x}_2}$. In particular, $f(v_1) = f \circ v_1 \circ f^{-1} \in V(\mathcal{A}_{\tilde{x}_2}) \cap (\prod_{\ell \text{ prime}} \mathbf{L}_{\ell,\tilde{x}_2}) = L(\mathcal{A}_{\tilde{x}_2})$. Then f induces a quasi-isogeny of $\mathcal{A}_x$ such that $f : H_{\text{cris}}^1(\mathcal{A}_x/W) \otimes_W E \rightarrow H_{\text{cris}}^1(\mathcal{A}_{\tilde{x}_2}/W) \otimes_W E$ preserves all $s_{\alpha,\text{cris},x}$, and $f(\text{Fil}^1 H_{\text{dR}}^1(\mathcal{A}_{\tilde{x}_1}/E)) = \text{Fil}^1 H_{\text{dR}}^1(\mathcal{A}_{\tilde{x}_2}/E)$, which gives a $\mathcal{O}_F$ -linear isometry of $\mathbf{L}_{\text{cris},x} \otimes_W \mathcal{O}_E$ taking $\text{Fil}^1 \mathbf{L}_{\text{dR},\tilde{x}_1}$ to $\text{Fil}^1 \mathbf{L}_{\text{dR},\tilde{x}_2}$. The isotropic line $\text{Fil}^1 \mathbf{L}_{\text{dR},\tilde{x}_2} \in (v_{\text{cris}} \otimes 1)^\perp \cap f(v_{\text{cris}} \otimes 1)^\perp$ and it lies in the 3-dimensional ρ' -eigenspace of $\mathbf{L}_{\text{cris},x}$. There is an isometry from $L(\mathcal{A}_x) \otimes_{\mathcal{O}_F,\rho'} W$ to the ρ' -eigenspace of $\mathbf{L}_{\text{cris},x}$, where $v \otimes 1$ (resp. $f(v) \otimes 1$) maps to $v_{\text{cris},\rho'}$ (resp. $f(v)_{\text{cris},\rho'}$). 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 $f(\text{Fil}^1 \mathbf{L}_{\text{dR},\tilde{x}_2}) \in f(v_{\text{cris},\rho'} \otimes 1)^\perp = (v_{\text{cris},\rho'} \otimes 1)^\perp$ implies $f(F^1 \mathbf{L}_{\text{dR},\tilde{x}_2}) = F^1 \mathbf{L}_{\text{dR},\tilde{x}_1}$. Therefore, f fixes the line spanned by $v_{\text{cris},\rho'} \otimes 1$ and switches the two isotropic lines $\text{Fil}^1 \mathbf{L}_{\text{dR},\tilde{x}_1}, \text{Fil}^1 \mathbf{L}_{\text{dR},\tilde{x}_2}$. 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-isogeny $f : \mathcal{A}_{\tilde{x}_1} \rightarrow \mathcal{A}_{\tilde{x}_1}'$ that sends $s_{\alpha,?,\tilde{x}_1}$ to $s_{\alpha,?,\tilde{x}_1}'$, where $? = \ell, p, \text{dR}$, and takes $\mathbf{L}_{\ell,\tilde{x}_1}$ to $\mathbf{L}_{\ell,\tilde{x}_1}'$ and $\mathbf{L}_{p,\tilde{x}_1}$ to $\mathbf{L}_{p,\tilde{x}_1}'$. 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 $\text{Fil} \mathbf{L}_{\text{dR},\tilde{x}_2}$ to $\text{Fil} \mathbf{L}_{\text{dR},\tilde{x}_2}'$, which implies that $\mathcal{A}_{\tilde{x}_2}$ and $\mathcal{A}_{\tilde{x}_2}'$ give the same point in $\Gamma_0 \backslash X^+$. $\square$

⁴The automorphisms are defined over $\bar{k}$.

Lemma 3.4.7. *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 , 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 $a_1 x^2 + a_2 y^2 + a_3 z^2 = 0$ and $a_1 c_1 x + a_2 c_2 y + a_3 c_3 z = 0$ 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 $(-a_1 a_2 a_3 c_1 c_2 \pm a_3 c_3 \sqrt{-a_1 a_2 a_3 t})e_1 + a_1 a_3 (t - a_2 c_2^2)e_2 + (\mp a_1 c_1 \sqrt{-a_1 a_2 a_3 t} - a_1 a_2 a_3 c_2 c_3)e_3$ defined over $E := W[p^{-1}](\sqrt{-a_1 a_2 a_3 t})$ where $-a_1 a_2 a_3 t$ is a uniformizer of W . Note that $a_1 a_3 (t - a_2 c_2^2) \in W^\times$, and modulo the maximal ideal of $\mathcal{O}_E$, both lines reduce to $\langle c_1 e_1 + c_2 e_2 + c_3 e_3 \rangle = \langle v \rangle$. $\square$

Pairing at points with an even order automorphism

Proposition 3.4.8. *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 $x \in \mathcal{S}_{K_0}(k)$ with an even order automorphism, there is a bijection*

$$\left\{ \begin{array}{l} \text{lifts of } x \text{ admitting} \\ \text{a special endomorphism } \sqrt{-\lambda} \end{array} \right\} \xrightarrow{\simeq} \{ \langle v \rangle : v \in L(\mathcal{A}_x), Q'_F(v) = \lambda \} / \text{Aut}(x), \quad (3.4.0.11)$$

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 3.4.8 uses Lemma 3.4.10 and the linear algebra computation Lemma 3.4.11. The proof of Lemma 3.4.10 uses the linear algebra computation Lemma 3.4.9.

Lemma 3.4.9. *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).⁵ Suppose $Q : L \rightarrow \mathcal{O}_F$ is a quadratic module over $\mathcal{O}_F$ such that the extension $Q : L \otimes_{\mathcal{O}_F} F \rightarrow F$ 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 $\alpha \in \text{SO}(L, Q)$, 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 $\alpha(e_1) \in \text{Span}(e_1)$. $\square$

Lemma 3.4.10. *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 $x \in \mathcal{S}_{K_0}(k)$. 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 3.4.5. 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 $\alpha \in \text{SO}(L(\mathcal{A}_x), Q'_F)$ such that $\alpha(e_2) = \pm e_3$.*

Proof. Note that $e_2 \perp e_1$ by Lemma 3.4.9. 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 $(B'^0, \text{nr}_d|_{B'^0}) \simeq (V(\mathcal{A}_x), Q'_F)$. Under this identification, let $e_3 = e_1 e_2$ 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

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

⁵Given a totally positive number $\lambda \in F$ such that $\text{Nm}_{F/\mathbb{Q}}(\lambda)$ 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 $\mathcal{O}_F^\times \rightarrow \mathbb{R}^r$, $x \mapsto (-\log |\rho_i(x)|)_{\rho_i : F \hookrightarrow \mathbb{R}}$ 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 $\gamma_1 = (\gamma_{1,1}, \dots, \gamma_{1,r-1}, -\sum_{i=1}^{r-1} \gamma_{1,i}, \dots, \gamma_{r-1} = (\gamma_{r-1,1}, \dots, \gamma_{r-1,r-1}, -\sum_{i=1}^{r-1} \gamma_{r-1,i})$ for the rank $(r-1)$ lattice $2\Gamma \subset H$. Write $a_i = \log(\rho_i(\lambda)) - \log(4)$ for each $i = 1, \dots, r$ and $a = \sum_{i=1}^r a_i = \log \text{Nm}_{F/\mathbb{Q}}(\lambda) - r \log(4)$. Consider $\sum_{i=1}^{r-1} c_i \gamma_i = (a_1 - \frac{a}{2(r-1)}, \dots, a_{r-1} - \frac{a}{2(r-1)}, a_r - \frac{a}{2}) \in H$ with $c_1, \dots, c_{r-1} \in \mathbb{R}$, and $\gamma = \sum_{i=1}^{r-1} [c_i] \gamma_i$ where each $[c_i] \in \mathbb{Z}$ with $||c_i] - c_i| \leq \frac{1}{2}$. If $a > (r-1) \max_{1 \leq j \leq r-1} \sum_{i=1}^{r-1} |\gamma_{i,j}|$, then the cube $C = \{(x_{\rho_i}) : \sum_{i=1}^r x_{\rho_i} = 0, a_j - \frac{a}{r-1} < x_{\rho_j} < a_j \text{ for each } j = 1, \dots, r-1\} \subset H$ contains $\gamma \in 2\Gamma$.

be the isometry (3.4.0.7) over $W[p^{-1}]$, and for $v \nmid p$, let

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

be the isometry (3.4.0.9) 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, $\sum_{\sigma'} g_{\sigma'}(e_3 \otimes 1) \in \mathbf{L}_{\text{cris}, x}$. 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 isomorphism, 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 $\alpha \in \text{SO}(L(\mathcal{A}_x))$, then $\alpha(e_1) = \pm e_1$ by Lemma 3.4.9. 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 $g_v : B'_v \rightarrow B_v$, the automorphism $g_v \circ \alpha \circ g_v^{-1} : B_v \rightarrow B_v$ 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 $v(\text{nrd}(1 + e_1)) = v(\text{nrd}(1 - e_1)) = v(2)$ 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 3.4.5, there is $u \in L(\mathcal{A}_x)$ with $Q'_F(u) = 1$ and $\alpha(u) = u$. By Lemma 3.4.9, we have $u \perp e_2$ and $u \perp e_3$, which implies $u \in \text{Span}(e_1)$ and $\alpha(u) = -u$, leading to contradiction. $\square$

Lemma 3.4.11. *Let K be a local field with valuation ring $\mathcal{O}$, maximal ideal $\mathfrak{p}$, residue field k , and a uniformizer ϖ . Suppose $Q : L \rightarrow \mathcal{O}$ is a rank 3 quadratic module over $\mathcal{O}$ such that the reduction $L \otimes_{\mathcal{O}} k \rightarrow k$ 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 $e_3 = c_1 e_1 + c_2 e_2 + \varpi v$ 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 $c_1 \equiv 0 \pmod{\mathfrak{p}}$. $\square$

Proof of Proposition 3.4.8. 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 3.3.10. Let $e_1 \in L(\mathcal{A}_x)$ such that $Q'_F(e_1) = 1$ by Lemma 3.4.5. 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 3.4.10.

By Lemma 3.4.11, 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 [Mad16, 5.16] or the proof of Lemma 3.4.2, 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 3.4.6, there exists a quasi-isogeny $\mathcal{A}_{\tilde{x}_2} \rightarrow \mathcal{A}_{\tilde{x}_3}$ inducing an automorphism $\alpha \in \text{SO}(L(\mathcal{A}_x), Q'_F)$ with $\alpha(e_2) = \pm(e_3)$, which contradicts Lemma 3.4.10.

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) corresponding to l_1 or l'_1 . $\square$

3.5 Archimedean place

In this section, we prove Proposition 3.5.6 and its slightly more general form, Proposition 3.5.7, 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 3.5, 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 3.5, we study the CM points on this geodesic, and in section 3.5, we use equidistribution of primes to show the density of the CM points on it.

Real points on the Shimura curve

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

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

for any $\alpha \in F^\times \mathcal{O}^\times$ with $\rho(\text{nrd}(\alpha)) < 0$. 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 $\text{trd}(\alpha) = 0$ and $\text{nrd}(\alpha) = -\alpha^2 = \epsilon$, as any two maximal orders in B are conjugate to each other. Let

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

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

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

Since every totally poistive unit in $\mathcal{O}_F^\times$ is a square, by [Shi75, 7.4], the real points of $\tilde{\Gamma} \backslash \mathcal{H}$ 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 $\tilde{\Gamma}$. This set is in bijection with the set of $\tilde{\Gamma}$ -conjugacy classes of embeddings $\mathcal{O}_F[\sqrt{-\epsilon}] \hookrightarrow \mathcal{O}$, where $\mathcal{O}_F[\sqrt{-\epsilon}]$ is an order in $F(\sqrt{-\epsilon})$.

One geodesic case

Assume $[F : \mathbb{Q}] > 1$, $\mathcal{O}_F[\sqrt{-\epsilon}]$ is the maximal order of $F(\sqrt{-\epsilon})$ ⁶ and $F(\sqrt{-\epsilon})$ has class number $h(F(\sqrt{-\epsilon})) = 1$, then the real points of $\tilde{\Gamma} \backslash \mathcal{H}$ is $\varphi(Z_\alpha)$ for any $\alpha \in U(\epsilon)$ by Lemma 3.5.1.

Lemma 3.5.1. *For any quadratic $\mathcal{O}_F$ -order $S \subset F[\sqrt{-\epsilon}]$, the number of $\tilde{\Gamma}$ -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 $m(S, \mathcal{O}; \tilde{\Gamma}) = m(S, \mathcal{O}; \mathcal{O}^\times) [\text{nrd}(\mathcal{O}^\times) : \text{nrd}(\tilde{\Gamma}) \text{nrd}(S^\times)]$ by [Voi21, 30.3.14], where $[\text{nrd}(\mathcal{O}^\times) : \text{nrd}(\tilde{\Gamma}) \text{nrd}(S^\times)] = 1$ since $\rho(\text{Nm}_{F(\sqrt{-\epsilon})/F}(S)) \cap \mathbb{R}_{<0} \neq \emptyset$. Since F has narrow class number 1, the maximal order $\mathcal{O}$ of B has class number 1 and then $m(S, \mathcal{O}; \mathcal{O}^\times) = h(S) m(\hat{S}, \hat{\mathcal{O}}; \hat{\mathcal{O}}^\times)$ by [Voi21, 30.4.17]. Finally, as B is split at all finite places, we have $m(\hat{S}, \hat{\mathcal{O}}; \hat{\mathcal{O}}^\times) = \prod_{v \text{ finite}} m(S_v, \mathcal{O}_v; \mathcal{O}_v^\times) = 1$. $\square$

⁶Since 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 $F(\sqrt{-\epsilon})$.

We assume F has only one prime $\mathfrak{p}_2$ above 2, then the quaternion algebra $B \simeq \left(\frac{-\epsilon, -1}{F}\right)$ ⁷ 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 3.5.2. *The quaternion algebra $\left(\frac{-\epsilon, -1}{F}\right)$ has a maximal order of the form*

$$\mathcal{O} = \mathcal{O}_F[\mu, \frac{a + b\mu + \nu}{2}] = \mathcal{O}_F + \mathcal{O}_F\mu + \mathcal{O}_F\frac{a + b\mu + \nu}{2} + \mathcal{O}_F\frac{-\epsilon b + a\mu + \mu\nu}{2} \quad (3.5.0.1)$$

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 $\text{disc}(\mathcal{O}) = (\frac{1}{4})^2 \text{disc}(\mathcal{O}_F[\mu, \nu]) = (\frac{1}{4})^2 (-4\epsilon)^2 = \epsilon^2$ is a unit in F . $\square$

We may assume $\mathcal{O}$ is the maximal order as defined by (3.5.0.1) and $\alpha = \mu \in U(\epsilon)$. Then the geodesic

$$Z_\alpha = \{iy : y > 0\} \quad (3.5.0.2)$$

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

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

By assumption, the Shimura curve $\tilde{\Gamma} \backslash \mathcal{H}$ 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 $\ker(\mathcal{O}_F[\sqrt{-\epsilon}]^\times \xrightarrow{\text{Nm}} \mathcal{O}_F^\times)$ with $\rho(u) > 1$.⁸ Then $\pm u^2 = \pm \frac{u}{u'}$ generates $\{\frac{a'}{a} : a \in \mathcal{O}_F[\sqrt{-\epsilon}]^\times\}$,⁹ and $[i, i\rho(u^2)]$ is a fundamental domain for $\varphi(Z_\alpha)$.

⁷This is the quaternion algebra unramified at all odd primes and exactly one of the real places ρ of F .

⁸The rank of $\ker(\mathcal{O}_F[\sqrt{-\epsilon}]^\times \xrightarrow{\text{Nm}} \mathcal{O}_F^\times)$ is $\text{rank}(\mathcal{O}_F[\sqrt{-\epsilon}]^\times) - \text{rank}(\mathcal{O}_F^\times) = (2 + ([F : \mathbb{Q}] - 1) - 1) - ([F : \mathbb{Q}] - 1) = 1$. Thus, $\ker(\mathcal{O}_F[\sqrt{-\epsilon}]^\times \xrightarrow{\text{Nm}} \mathcal{O}_F^\times) = \{\pm u^m : m \in \mathbb{Z}\}$.

⁹The 2-rank of $H^1(\text{Gal}(F(\sqrt{-\epsilon})/F), \mathcal{O}_F[\sqrt{-\epsilon}]^\times)$ 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 $H^1(\text{Gal}(F(\sqrt{-\epsilon})/F), \mathcal{O}_F[\sqrt{-\epsilon}]^\times)$.

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 $\lambda = bb' \in \text{Nm}_{F(\sqrt{-\epsilon})/F}(F(\sqrt{-\epsilon})^\times)$. 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 3.5.3. *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 $\lambda = \text{Nm}_{F(\sqrt{-\epsilon})/F}(x)$; 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 $\ker(\mathcal{O}_{F(\sqrt{-\epsilon})}^\times \xrightarrow{\text{Nm}} \mathcal{O}_F^\times)$.*

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

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

which implies (λ) splits in $F(\sqrt{-\epsilon})$. Let $x \in \mathcal{O}_{F(\sqrt{-\epsilon})}$ 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 $z \in (\mathcal{O}_F^\times)^2 \subset \text{Nm}_{F(\sqrt{-\epsilon})/F}(\mathcal{O}_{F(\sqrt{-\epsilon})}^\times)$; 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 $\mathcal{O}_{F(\sqrt{-\epsilon})}$. $\square$

By Lemma 3.5.3, 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 3.3.7 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.

Equidistribution

Given a CM cycle on the Shimura curve defined by $\tilde{T} \subset \tilde{G}$ and $\tau \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, by [Del+82, V], the conjugate of the CM cycle on the conjugate Shimura curve is defined by $\tilde{T} = {}^{\tau, \mu} \tilde{T} \subset {}^{\tau, \mu} \tilde{G}$, where μ is the Hodge cocharacter and ${}^{\tau, \mu} \tilde{G}$ is a twist of $\tilde{G}$. Explicitly, as in [MS10, 1.4], ${}^{\tau, \mu} \tilde{G}$ arises from a quaternion algebra ${}^\tau B$ such that $\text{inv}_v({}^\tau B) = \text{inv}_{\tau \circ v}(B)$ for all infinite places

v of F and $\text{inv}_v({}^\tau B) = \text{inv}_v(B)$ for all finite places v of F . Moreover, the isomorphism $\tilde{G}(\mathbb{A}_f) \simeq {}^{\tau,\mu}\tilde{G}(\mathbb{A}_f)$ induced by $B_v \simeq {}^\tau B_v$ maps $\tilde{K} = \prod \mathcal{O}_v^\times$ to ${}^{\tau,\mu}\tilde{K} = \prod \mathcal{O}'_v{}^\times$, 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 $i = 1, \dots, n$.¹⁰ 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 natural 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 $\lambda = \text{Nm}_{F_i/F}(b_i)$, where $\rho_{i,1}$ is a real place of F_i above ρ_i and $\lambda \in F$ totally positive.

Let $\mathcal{F} = F_1 \cdots F_n$ be the compositum. Assume $\mathcal{F}$ has class number $h(\mathcal{F}) = 1$. The image of $\text{Nm}_{\mathcal{F}/F} = \text{Nm}_{F_i/F} \circ \text{Nm}_{\mathcal{F}/F_i} : \mathcal{F}^\times \rightarrow F^\times$ is totally positive. Suppose λ is a totally positive prime of F such that $-\lambda$ is a square modulo 4. Then by Lemma 3.5.3, (λ) splits in each F_i , and thus splits completely in the compositum $\tilde{F}$.

Lemma 3.5.4. *Let P be the set of prime ideals of $\mathcal{F}$. Assume $\mathcal{F}$ has class number $h(\mathcal{F}) = 1$. Then the set*

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

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 $\ker(\mathcal{O}_{F(\sqrt{-\epsilon_i})}^\times \rightarrow \mathcal{O}_F^\times)$ with $\rho_{i,1}(u_i) > 1$.

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

$$\prod_{w|\rho_i} \mathbb{C}^\times = \prod_{v|\rho_i} \prod_{w|v} \mathbb{C}^\times \xrightarrow{(\text{Nm}_{\mathcal{F}/F_i}, \text{Nm}_{\mathcal{F}/F_i})} \prod_{v|\rho_i} \mathbb{R}_{>0} \xrightarrow{(x,y) \mapsto \sqrt{\frac{x}{y}}} \mathbb{R}_{>0} \xrightarrow{\log} \mathbb{R}, \quad (3.5.0.3)$$

where v denotes infinite places of F_i , w denotes infinite places of $\mathcal{F}$, and $\text{Nm}_{\mathcal{F}/F_i}$ is the local norm. For $\alpha \in \mathcal{F}^\times \hookrightarrow \prod_{w|\rho_i} \mathbb{C}^\times$, we have $N_i(\alpha) = \frac{1}{2} \log \frac{\rho_{i,1}(\text{Nm}_{\mathcal{F}/F_i}(\alpha))}{\rho_{i,1}(\text{Nm}_{\mathcal{F}/F_i}(\alpha'))}$. Note that (3.5.0.3) induces a surjection $\{(z_w)_{w|\rho_i} : \prod_{w|\rho_i} \|z_w\| = 1\} / \mathcal{O}_{\mathcal{F}}^\times \twoheadrightarrow \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$. Then

¹⁰If $F/\mathbb{Q}$ is Galois, this is true if and only if one of the ϵ_i satisfies the assumption.

$\prod_{i=1}^n N_i : \prod_{w|\infty} \mathbb{C}^\times = \prod_{i=1}^n \prod_{w|\rho_i} \mathbb{C}^\times \rightarrow \prod_{i=1}^n \mathbb{R}$ induces a Hecke character $\chi : \mathbb{A}_{\mathcal{F}}^\times \rightarrow \prod_{i=1}^n \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$ 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]. $\square$

Remark 3.5.5. Since $h(F_i) = 1$ by assumption, we have isomorphisms

$$\left(\prod_{v|\rho_i} \mathbb{R} \prod_{v|\infty, v \nmid \rho_i} \mathbb{C}^\times \right) / \mathcal{O}_{F_i}^\times \xrightarrow{\sim} \mathbb{A}_{F_i}^\times / (F_i^\times \left(\prod_{\mathfrak{p}|\infty} \mathcal{O}_{(F_i)_{\mathfrak{p}}}^\times \right))$$

for $i = 1, \dots, n$, then we can define the Hecke character

$$\chi = (\chi_1, \dots, \chi_n) : \mathbb{A}_{\mathcal{F}}^\times \rightarrow \prod_{i=1}^n \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$$

by

$$\chi_i : \mathbb{A}_{\mathcal{F}}^\times \xrightarrow{\text{Nm}_{\mathcal{F}/F_i}} \mathbb{A}_{F_i}^\times \twoheadrightarrow \left(\prod_{v|\rho_i} \mathbb{R} \prod_{v|\infty, v \nmid \rho_i} \mathbb{C}^\times \right) / \mathcal{O}_{F_i}^\times \xrightarrow{((x,y), (z_j)_{j \neq i}) \mapsto \frac{1}{2} \log \left| \frac{x}{y} \right|} \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$$

without assuming $h(\mathcal{F}) = 1$.

Recall that $iy \mapsto \log y$ gives an isomorphism $\varphi_i(Z_{\alpha_i}) \rightarrow \mathbb{R}/(2 \log \rho_{i,1}(u_i))\mathbb{Z}$, 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 3.5.6. *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 $t_{i,0}$ 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 $\pi_{\mathfrak{m}} : \mathbb{A}_F^\times \rightarrow C_{\mathfrak{m}}$ 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 $\chi_0 = \pi_{\mathfrak{m}} \circ \text{Nm}_{\mathcal{F}/F}$, then $\chi_0(\mathbb{A}_{\mathcal{F}}^1) \cap V_{\mathfrak{m}} \neq \emptyset$ since (λ) splits in $\mathcal{F}$.

Define a Hecke character $\chi = (\chi_0, \chi_\infty) : \mathbb{A}_{\mathcal{F}}^\times \rightarrow C_{\mathfrak{m}} \times (\prod_{i=1}^n \mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z})$, where χ_∞ is defined in the proof of Lemma 3.5.4 by (3.5.0.3). Note that $\chi_0(\prod_{w|\infty} \mathbb{C}^\times) = 1$, 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 $\text{Nm}_{\mathcal{F}/F}(\alpha)$ is totally positive since (3.5.0.3) always gives positive terms in the middle. Let $\mathfrak{q} = \text{Nm}_{\mathcal{F}/F}((\alpha))$, where we may assume (α) lies above a totally split rational prime, as such primes have density one in $\mathcal{F}$. $\square$

Proposition 3.5.7. *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 $t_i, s_{i,1}, \dots, s_{i,d_i}$ be points on the circle $\varphi(Z_{\alpha_i}) \simeq \mathbb{R}/(2 \log \rho_{i,1}(u_i))\mathbb{Z}$ 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 3.5.6, 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 $V_i := (\bigcap_{j \in J_i} V_{i,j}) \setminus (\bigcup_{j \notin J_i} V_{i,j}) \neq \emptyset$ is a non empty open subspace of the compact space $\mathbb{R}/(\log \rho_{i,1}(u_i))\mathbb{Z}$. $\square$

3.6 Proof of main theorem

In this section, we prove Theorem 1.2.1. We begin by defining the polynomials associated to the CM cycles constructed in §3. In section 3.6 we use the input from §4 to study the polynomials modulo λ after clearing denominators, and in section 3.6 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 3.6 we combine all of the ingredients and apply quadratic reciprocity to complete the proof.

Suppose the Shimura curve $\Gamma \backslash \mathcal{H} \simeq \Gamma_0 \backslash X^+$ has genus 0. Its canonical model is defined over the reflex field $\rho(F) \subset \mathbb{C}$. Assume the canonical model is isomorphic to $\mathbb{P}_F^1$. 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 $\mathbb{P}_{\mathcal{O}_F}^1$. Choose a coordinate j compatible with the model over $\mathcal{O}_F$.

Fix an embedding $\bar{F} \hookrightarrow \mathbb{C}$, and let $\tau_1, \dots, \tau_{[F:\mathbb{Q}]} \in \text{Gal}(\bar{F}/\mathbb{Q})$ 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 $\sigma_1, \dots, \sigma_{[F':F]} \in \text{Gal}(\bar{F}/F)$ such that $\text{Hom}_F(F', \bar{F}) = \{\sigma_1|_{F'}, \dots, \sigma_{[F':F]}|_{F'}\}$. 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' contains all the primes ramified in F' and all the primes p such that $v_{\mathfrak{p}}(j_0) \neq 0$ or $v_{\mathfrak{p}}(j_\infty) \neq 0$ for some prime $\mathfrak{p}$ of F' 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 .

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, $\text{Gal}(\bar{F}/F)$ 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

$$\begin{aligned} b_{\lambda} \prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\alpha_k) < 0}}^{h_1} (x - \alpha_k) &\equiv \tilde{b}_{\lambda} \not\equiv 0 \pmod{\mathfrak{l}}, & \tilde{b}_{\lambda} &:= b_{\lambda} \prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\alpha_k) < 0}}^{h_1} (-\alpha_k), \\ b_{4\lambda} \prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\beta_k) < 0}}^{h_2} (x - \beta_k) &\equiv \tilde{b}_{4\lambda} \not\equiv 0 \pmod{\mathfrak{l}}, & \tilde{b}_{4\lambda} &:= b_{4\lambda} \prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\beta_k) < 0}}^{h_2} (-\beta_k). \end{aligned}$$

By Proposition 3.4.6 and the first part of Proposition 3.4.8, roots of $P_{\lambda}(x)P_{4\lambda}(x)$ are paired modulo $\mathfrak{l}$. Then Lemma 3.6.1 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 3.6.1. *Modulo $\mathfrak{l}$, we have*

$$\mathrm{Nm}_{F'/F}(d_0^{h_1+h_2}b_{\lambda}P_{\lambda}(j_0)b_{4\lambda}P_{4\lambda}(j_0)) \equiv (\tilde{b}_{\lambda}\tilde{b}_{4\lambda})^{[F':F]} \cdot \text{square}, \quad (3.6.0.1)$$

$$\mathrm{Nm}_{F'/F}(d_{\infty}^{h_1+h_2}b_{\lambda}P_{\lambda}(j_{\infty})b_{4\lambda}P_{4\lambda}(j_{\infty})) \equiv (\tilde{b}_{\lambda}\tilde{b}_{4\lambda})^{[F':F]} \cdot \text{square}. \quad (3.6.0.2)$$

Proof. We prove (3.6.0.2), and (3.6.0.1) 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

$$\begin{aligned} & \text{Nm}_{F'/F}(d_\infty^{h_1} b_\lambda P_\lambda(j_\infty)) \\ &= \left(b_\lambda^{[F':F]} \prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\alpha_k) < 0}}^{h_1} \prod_i (d_\infty(\sigma_i(j_\infty) - \alpha_k)) \right) \left(\prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\alpha_k) \geq 0}}^{h_1} \prod_i (d_\infty(\sigma_i(j_\infty) - \alpha_k)) \right) \in \mathcal{O}_{H_{\mathfrak{l}}}, \\ & \text{Nm}_{F'/F}(d_\infty^{h_2} b_{4\lambda} P_{4\lambda}(j_\infty)) \\ &= \left(b_{4\lambda}^{[F':F]} \prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\beta_k) < 0}}^{h_2} \prod_i (d_\infty(\sigma_i(j_\infty) - \beta_k)) \right) \left(\prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\beta_k) \geq 0}}^{h_2} \prod_i (d_\infty(\sigma_i(j_\infty) - \beta_k)) \right) \in \mathcal{O}_{H_{\mathfrak{l}}}. \end{aligned}$$

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

$$\begin{aligned} b_\lambda^{[F':F]} \prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\alpha_k) < 0}}^{h_1} \prod_i (d_\infty(\sigma_i(j_\infty) - \alpha_k)) &\equiv \tilde{b}_\lambda^{[F':F]} \not\equiv 0 \pmod{\mathfrak{l}}, \\ b_{4\lambda}^{[F':F]} \prod_{\substack{k=1 \\ v_{\mathfrak{l}}(\beta_k) < 0}}^{h_2} \prod_i (d_\infty(\sigma_i(j_\infty) - \beta_k)) &\equiv \tilde{b}_{4\lambda}^{[F':F]} \not\equiv 0 \pmod{\mathfrak{l}}. \end{aligned}$$

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 3.4.6; 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 3.4.8.¹¹ Therefore, for any $\bar{j} \in \mathcal{O}_{H_{\mathfrak{l}}}/\mathfrak{l}\mathcal{O}_{H_{\mathfrak{l}}}$,

$$\left(\prod_{\substack{k=1 \\ \overline{\alpha_k} = \bar{j}}}^{h_1} \prod_i (d_\infty(\sigma_i(j_\infty) - \alpha_k)) \right) \left(\prod_{\substack{k=1 \\ \overline{\beta_k} = \bar{j}}}^{h_2} \prod_i (d_\infty(\sigma_i(j_\infty) - \beta_k)) \right) \quad (3.6.0.3)$$

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 $\mathcal{O}_{H_{\mathfrak{l}}}/\mathfrak{l}\mathcal{O}_{H_{\mathfrak{l}}}$. $\square$

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

¹¹Here we need the assumption 2 inert in F .

$\text{Nm}_{F'/F}(d_0^{h_1+h_2} b_\lambda P_\lambda(j_0) b_{4\lambda} P_{4\lambda}(j_0))$ modulo λ , we need to divide appropriate power of λ from $\text{Nm}_{F'/F}(d_\infty^{h_1+h_2} b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty))$ to get a nonzero square, so we use Proposition 3.4.8 to prove Lemma 3.6.2.

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

$$\# \text{Aut}(\sigma_i(j_\infty)_{\overline{\mathbb{F}_{\mathfrak{l}'}}}) = \# \text{Aut}(\sigma_i(j_\infty)) = 2.$$

Lemma 3.6.2. *Each $\#A_i$ is even, and we have*

$$\lambda^{-\sum_{i=1}^{[F':F]} \#A_i} \text{Nm}_{F'/F}(d_\infty^{h_1+h_2} b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty)) \equiv (\tilde{b}_\lambda \tilde{b}_{4\lambda})^{[F':F]} \cdot \text{nonzero square} \quad (3.6.0.4)$$

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 , (3.6.0.3) is a nonzero square in $\mathcal{O}_{H_{\mathfrak{l}}}/\mathfrak{l}\mathcal{O}_{H_{\mathfrak{l}}}$ as in the proof of Lemma 3.6.1. From the pairing in the neighborhood of $\sigma_i(j_\infty)_{\overline{\mathbb{F}_{\mathfrak{l}'}}}$ as described in Proposition 3.4.8, elements in A_i are paired and for each pair $\{\gamma_1, \gamma_2\}$, by Lemma 2.1.3, we have

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

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

$$\begin{aligned} v_{\mathfrak{l}} \left(\prod_{m=1}^{[F':F]} (d_\infty(\sigma_m(j_\infty) - \gamma_1)) \right) &= v_{\mathfrak{l}} \left(\prod_{m=1}^{[F':F]} (d_\infty(\sigma_m(j_\infty) - \gamma_2)) \right) = 2[F' : F(j_\infty)], \\ \lambda^{-[F':F(j_\infty)]} \left(\prod_{m=1}^{[F':F]} (d_\infty(\sigma_m(j_\infty) - \gamma_1)) - \prod_{m=1}^{[F':F]} (d_\infty(\sigma_m(j_\infty) - \gamma_2)) \right) &\in \lambda \mathcal{O}_{H_{\mathfrak{l}}}. \end{aligned}$$

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. $\square$

As explained in Section 3.5, for each $\tau_i \in \text{Gal}(\overline{F}/\mathbb{Q})$, we have $\tau_i(\alpha_1), \dots, \tau_i(\alpha_{h_1})$ (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 $\mathbb{P}_{\tau_i(F)}^1$. The conjugate CM cycle is defined over $\tau_i(F) \subset \mathbb{R}$, then the set $\{\tau_i(\alpha_1), \dots, \tau_i(\alpha_{h_1})\}$ (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 3.3.3).

Lemma 3.6.3. *For each $\tau_i \in \text{Gal}(\overline{F}/\mathbb{Q})$, the sign of*

$$\tau_i(\text{Nm}_{F'/F}(P_\lambda(j_0)P_{4\lambda}(j_0)P_\lambda(j_\infty)P_{4\lambda}(j_\infty)))$$

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

$$\begin{aligned} \prod_{\substack{l=1 \\ \tau_i(\alpha_l) \neq \alpha_i^*}}^{h_1} (\tau_i\sigma(j_\infty) - \tau_i(\alpha_l)) &> 0, & \prod_{\substack{l=1 \\ \tau_i(\beta_l) \neq \beta_i^*}}^{h_2} (\tau_i\sigma(j_\infty) - \tau_i(\beta_l)) &> 0, \\ \prod_{\substack{l=1 \\ \tau_i(\alpha_l) \neq \alpha_i^*}}^{h_1} (\tau_i\sigma(j_0) - \tau_i(\alpha_l)) &> 0, & \prod_{\substack{l=1 \\ \tau_i(\beta_l) \neq \beta_i^*}}^{h_2} (\tau_i\sigma(j_0) - \tau_i(\beta_l)) &> 0, \end{aligned}$$

then

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

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

$k' \in \sigma_1, \dots, \sigma_{[F':F]} \in \text{Gal}(\overline{F}/F)$, where $k' = k$ if and only if $\tau_i(\sigma_k(F')) \subset \mathbb{R}$, then

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

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 $\sigma_{\infty,i}|_F = \rho_i$. $\square$

By Proposition 3.5.7, 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

$$\left(\frac{q}{-\lambda} \right) = \left(\frac{-\lambda}{q} \right) = 1 \text{ for any totally positive odd prime } q \in \mathcal{O}_F \text{ with } (q) \in S \quad (3.6.0.5)$$

by Theorem 1.4.1. The second condition implies that $\text{Nm}_{F'/F}(P_\lambda(j_0)P_{4\lambda}(j_0)P_\lambda(j_\infty)P_{4\lambda}(j_\infty))$ is totally negative. Let

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

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

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

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 1.4.1, 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 (3.6.0.5), so that $\mathfrak{p}$ is a good reduction prime and $\mathfrak{p}$ is unramified in F' .

If $v_{\mathfrak{p}}(\text{Nm}_{F'/F}(b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty))) > 0$, then $v_{\mathfrak{p}}(\text{Nm}_{F'/F}(b_\lambda P_\lambda(j_\infty) b_{4\lambda} P_{4\lambda}(j_\infty)))$ is even by Lemma 2.1.3.¹² Therefore, j_0 is a root of $b_\lambda P_\lambda(x) b_{4\lambda} P_{4\lambda}(x)$ modulo some prime above $\mathfrak{p}$.

3.7 Examples

In this section, we provide sufficient conditions for verifying some of the assumptions in Theorem 1.2.1. In particular, all the assumptions in Theorem 1.2.1 hold for the cases in Theorem 1.2.4, and hence we prove Theorem 1.2.4.

Lemma 3.7.1. *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 $C \simeq \mathbb{P}_k^1$. In particular, if there are divisors D_1 and D_2 such that $\deg D_1$ and $\deg D_2$ are relatively prime, then $C \simeq \mathbb{P}_k^1$.*

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 $C \simeq \mathbb{P}_k^1$ ([Liu02, 7.3.24]). $\square$

By Lemma 3.3.1 and Lemma 3.3.2, 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 $\mathbb{P}_F^1$.

Lemma 3.7.2. *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 $\prod_{F(\sqrt{u}) \subseteq M} h(F(\sqrt{u}))$.*

¹²This treatment follows the idea of [Li+25, §9.5].

Proof. Let $r = [F : \mathbb{Q}]$ and $u_1, \dots, u_{r-1}$ be fundamental units of F , then the field $M = F(\sqrt{-1}, \sqrt{u_1}, \dots, \sqrt{u_{r-1}})$ 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 $u \in \mathcal{O}_F^\times \setminus \mathcal{O}_F^{\times 2}$. 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. $\square$

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 $F\left(\sqrt{(-\epsilon_1)^{\delta_1} \dots (-\epsilon_n)^{\delta_n}}\right)$ 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 3.7.3. The following examples from [Voi09, §4] satisfy all the assumptions.

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

We used Magma [BCP97] to perform the computations.

Chapter 4

Some QM abelian surfaces

In this chapter, assume the following unless specified otherwise.

Let $B = B_\Delta$ be an indefinite quaternion algebra over $\mathbb{Q}$ of discriminant Δ , $\mathcal{O} = \mathcal{O}_B$ be a maximal order of B , and $\mathcal{O}^1 = \mathcal{O}_B^1$ be the group of units in $\mathcal{O}$ of norm 1. Fix an element $\mu \in \mathcal{O}_B$ such that $\mu^2 = -\Delta$,¹ then the involution $\alpha \mapsto \alpha' = \mu^{-1}\bar{\alpha}\mu$ is a positive anti-involution on B .

4.1 The Shimura modular curves

Let V_Δ be the Shimura curve over $\mathbb{Q}$ associated to $\mathcal{O}$. It is the coarse moduli space of isomorphism classes of $[A, \iota]$, where A is a principally polarized abelian surface, and $\iota : \mathcal{O} \hookrightarrow \text{End}(A)$ is an embedding such that the Rosati involution defined by the polarization on $\iota(\mathcal{O})$ is ' $\cdot$ '.² Fix an isomorphism $\iota_\infty : B_\mathbb{R} \xrightarrow{\sim} M_2(\mathbb{R})$. For any point τ on the upper half plane $\mathcal{H}$, consider the complex torus $A_\tau = \mathbb{C}^2/\Lambda_\tau$, where

$$\Lambda_\tau = \iota_\infty(\mathcal{O}) \begin{pmatrix} \tau \\ 1 \end{pmatrix}$$

is a lattice in $\mathbb{C}^2$, the map ι_∞ induces a natural embedding $\iota_\tau : \mathcal{O} \hookrightarrow \text{End}(A_\tau)$ as $\mathcal{O}$ is closed under multiplication. After possibly replacing μ by $-\mu$ once and for all, the Riemann form

$$E_\tau : \Lambda_\tau \times \Lambda_\tau \rightarrow \mathbb{Z},$$

$$\left(\iota_\infty(x) \begin{pmatrix} \tau \\ 1 \end{pmatrix}, \iota_\infty(y) \begin{pmatrix} \tau \\ 1 \end{pmatrix} \right) \mapsto \frac{1}{\Delta} \text{trd}(\mu x \bar{y})$$

defines the unique principal polarization on A_τ compatible with ι_τ . Let Γ^1 be the image in $\text{PSL}_2(\mathbb{R})$ of $\iota_\infty(\mathcal{O}^1)$, then the map $\Gamma^1 \tau \mapsto [A_\tau, \iota_\tau]$ gives a bijection $\Gamma^1 \backslash \mathcal{H} \rightarrow V_\Delta(\mathbb{C})$.

¹The element μ exists because the field $\mathbb{Q}(\sqrt{-\Delta})$ embeds in B by the local-global principle, and any two maximal orders in B are conjugate to each other by strong approximation.

²Given an abelian surface A and $\iota : \mathcal{O} \hookrightarrow \text{End}(A)$, there is a unique principal polarization on A such that the induced Rosati involution is compatible with μ .

There is the natural forgetful map $V_\Delta \rightarrow \mathcal{A}_2$ from V_Δ to the moduli threefold of principally polarized abelian surfaces under which $[A, \iota]$ maps to $[A, \mathcal{C}]$ where $\mathcal{C}$ is the unique principal polarization on A compatible with ι . Let E_Δ denote its image and E_Δ^0 denote the intersection of E_Δ with the image of the moduli space of genus 2 curves under the open Torelli map.

From now on, let $\Delta = 6$. By [Rot04], the forgetful map $V_6 \rightarrow \mathcal{A}_2$ has degree 4 and factors as $V_6 \rightarrow V_6/W_6 \simeq E_6 \hookrightarrow \mathcal{A}_2$, where the Atkin-Lehner group

$$W_6 = N_{B^\times}(\mathcal{O})/\mathbb{Q}^\times \mathcal{O}^\times = \{1, w_2, w_3, w_6\} \simeq \prod_{p|6} \mathbb{Z}/2\mathbb{Z},$$

and w_d is represented by some $\chi_d \in \mathcal{O} \cap N_{B^\times}(\mathcal{O})$ with $\text{trd}(\chi_d) = 0$, $\text{nrd}(\chi_d) = d$. Moreover, there is a unique $N_{B^\times}(\mathcal{O})$ -conjugacy class of embedding $\mathbb{Z}[\sqrt{-6}] \hookrightarrow \mathcal{O}$, then the image E_6 is independent of the choice of μ and E_6 is the moduli space of principally polarized abelian surfaces with potential QM by $\mathcal{O}$.

$$\begin{array}{ccc} & & V_6 \\ & & \downarrow w_6 \\ E_6^0 & \hookrightarrow & E_6 \\ \downarrow & & \downarrow \\ \mathcal{M}_2 & \hookrightarrow & \mathcal{A}_2 \end{array}$$

It is shown in [BG08a, 3.6] that there is an isomorphism $j = j_6 : E_6^0 \rightarrow \mathbb{P}^1 \setminus \{0, \infty\}$ given by

$$j = \frac{12^{10} J_{10}^2}{(J_2^2 - 24J_4)^5}. \quad (4.1.0.1)$$

4.2 CM points

Let K be an imaginary quadratic field and suppose $K \hookrightarrow B$ embeds. Let $\mathcal{O}_D = K \cap \mathcal{O}$ be an order of discriminant D , then the fixed point τ of $\iota_\infty(\mathcal{O}_D)$ in $\mathcal{H}$ is a CM point, its corresponding abelian variety A_τ has $\text{End}_{\text{QM}}(\mathcal{A}_\tau) \simeq \mathcal{O}_D$.

Remark 4.2.1. By Eichler, the number of $\mathcal{O}^\times$ -conjugacy classes of optimal embeddings $\mathcal{O}_D \hookrightarrow \mathcal{O}$ is

$$s(\mathcal{O}_D) := h(\mathcal{O}_D) \prod_{p|\Delta} \left(1 - \left(\frac{\mathcal{O}_D}{p} \right) \right),$$

where

$$\left(\frac{\mathcal{O}_D}{p} \right) := \begin{cases} 1 & \text{if } p \text{ divides the conductor of } \mathcal{O}_D, \\ \left(\frac{K}{p} \right) & \text{otherwise.} \end{cases}$$

Note that $s(\mathcal{O}_D) \neq 0$ if and only if the conductor of $\mathcal{O}_D$ is relatively prime to Δ and K splits B . Therefore, in the case $2|\Delta$, there are no points with CM by an imaginary quadratic order of conductor 2.

From now on, let D be a fundamental discriminant such that $\mathcal{O}_D \hookrightarrow \mathcal{O}$ and $E_6(D)$ denote the set of points with CM by $\mathcal{O}_D$. The Hilbert class group of K acts on $E_6(D)$ and the complex conjugation preserves $E_6(D)$. Let W'' denote the subgroup of W generated by elements w_p , where $p|\Delta$ is a prime ramified in K , then the number of elements in $E_6(D)$, counted with appropriate multiplicities, is

$$h' = \frac{h(\mathcal{O}_D)}{\#W''}.$$

By genus theory and [CH88, 19.6], the parity of h' can be determined. Let l be a prime. The relevant cases considered in this work are summarized in the following table.

D	$h(\mathcal{O}_D)$	h'
$-4l, l \equiv 13 \pmod{24}$	$\equiv 2 \pmod{4}$	odd
$-l, l \equiv 19 \pmod{24}$	odd	odd
$-3l, l \equiv 1 \pmod{24}$	$\equiv 0 \pmod{4}$	even

Denote the elements of $E_6(D)$ to be $a_1, \dots, a_{h'}$, and define

$$P_D(x) = b_{h'} \prod_{i=1}^{h'} (x - j(a_i)),$$

where $b_{h'} > 0$ is the smallest integer such that $P_D(x) \in \mathbb{Z}[x]$.

Elkies ([Elk98]) computed a different rational coordinate function $t : E_6 \rightarrow \mathbb{P}^1$, which is used in [Jao03]. The relation between the two coordinate functions is $j = 16(t - 1)/27$. In particular, from the following correspondence of the coordinates of the elliptic points we can translate the results in [Jao03] to our setting.

Elliptic point of order	CM	j	t
6	$\mathbb{Z} \left[\frac{1+\sqrt{-3}}{2} \right]$	∞	∞
4	$\mathbb{Z} [\sqrt{-1}]$	0	1
2	$\mathbb{Z} [\sqrt{-6}]$	$-\frac{16}{27}$	0

Lemma 4.2.2 ([Jao03, 3.3.1]). *Let $l \geq 5$ be a prime. For discriminants D of the form in the table, the polynomial $P_D(x)$ has at most one real root in each of the intervals $I_1 = (-\infty, -\frac{16}{27})$, $I_2 = (-\frac{16}{27}, 0)$, and $I_3 = (0, \infty)$, with the roots being located as follows: (see [Jao03, 3.3.1] for a complete list, * denotes the presence of a real root in the interval)*

D	I_1	I_2	I_3
$-4l, l \equiv 13 \pmod{24}$		*	
$-l, l \equiv 19 \pmod{24}$			*
$-3l, l \equiv 1 \pmod{24}$	*		*

Furthermore, for any subinterval and sub-congruence class of any starred entry, there exist infinitely many primes l in that sub-congruence class for which $P_D(x)$ has a real root in the subinterval.

Remark 4.2.3. Let $F_1 = \mathbb{Q}(\sqrt{2})$, $F_2 = \mathbb{Q}(\sqrt{3})$, $F_3 = \mathbb{Q}(\sqrt{6})$, and ε_i be a fundamental unit of F_i , $i = 1, 2, 3$. The claim that any subinterval of an interval I_i , in which polynomials P_D with D of the specified form have real roots, supports infinitely many such D follows from an equidistribution result ([Lan94, XV, §5]) for primes in F_i , by constructing a Hecke character $\sigma_i : \mathbb{A}_{F_i}^\times \rightarrow \mathbb{R}/(\ln \varepsilon_i)\mathbb{Z}$ given by

$$\mathbb{A}_{F_i}^\times / (F_i^\times \prod_{\mathfrak{p} \nmid \infty} U_{\mathfrak{p}}) \simeq (\mathbb{R}^\times \times \mathbb{R}^\times) / U_{F_i} \rightarrow \mathbb{R}/(\ln \varepsilon_i)\mathbb{Z},$$

$$(a, b) \mapsto \frac{1}{2} \ln \frac{|a|}{|b|}.$$

If the polynomials P_D have real roots in both I_{i_1} and I_{i_2} , then the result generalizes to any open subset of $I_{i_1} \times I_{i_2}$ by equidistribution of primes in the compositum $F_{i_1}F_{i_2}$. For example, let $F = F_1F_3$ and define $\sigma = (\sigma_1 \circ \text{Nm}_{F/F_1}, \sigma_3 \circ \text{Nm}_{F/F_3}) : \mathbb{A}_F^\times \rightarrow \mathbb{R}/(\ln \varepsilon_1)\mathbb{Z} \times \mathbb{R}/(\ln \varepsilon_3)\mathbb{Z}$, then $\sigma(a, b, c, d) = (\frac{1}{2} \ln \frac{|ac|}{|bd|}, \frac{1}{2} \ln \frac{|ab|}{|cd|})$ for $(a, b, c, d) \in \mathbb{R}^\times \times \mathbb{R}^\times \times \mathbb{R}^\times \times \mathbb{R}^\times \hookrightarrow \mathbb{A}_F^\times$. In particular, $\sigma(a, \frac{1}{a}, 1, 1) = (\ln |a|, 0)$ and $\sigma(a, 1, \frac{1}{a}, 1) = (0, \ln |a|)$, so the restriction of σ to the subgroup of ideles of norm 1 is surjective. Let $\tau : \{\text{primes of } F\} \rightarrow \mathbb{A}_F^\times$ be the map taking a prime $\mathfrak{p}$ to an idele that is 1 at all places except a prime element of $F_{\mathfrak{p}}$ at $\mathfrak{p}$, and $\lambda = \sigma \circ \tau$, then the set of primes of F is λ -equidistributed in $\mathbb{R}/(\ln \varepsilon_1)\mathbb{Z} \times \mathbb{R}/(\ln \varepsilon_3)\mathbb{Z}$. Since a density 1 of primes of F lies above a totally split rational prime, the set

$$\left\{ \left(\frac{1}{2} \ln \left| \frac{\pi_1}{\pi'_1} \right|, \frac{1}{2} \ln \left| \frac{\pi_3}{\pi'_3} \right| \right) : l \text{ rational prime}, (l) = (\pi_1)(\pi'_1) \text{ in } F_1, (l) = (\pi_3)(\pi'_3) \text{ in } F_3 \right\}$$

is equidistributed in $\mathbb{R}/(\ln \varepsilon_1)\mathbb{Z} \times \mathbb{R}/(\ln \varepsilon_3)\mathbb{Z}$.

Lemma 4.2.4 ([Jao03, 3.4.1, 3.4.2]). *Let $l \geq 5$ be a prime. For discriminants D of the form in the table, each root of $P_D(x) \pmod{l}$ occurs with even multiplicity, except possibly for roots corresponding to points on E_6 which are congruent modulo l to one of the three elliptic points. The divisor of unpaired zeros of $P_D(x) \pmod{l}$ is as follows: (see [Jao03, 3.4.2] for a complete list)*

D	<i>divisor</i>
$-4l, l \equiv 13 \pmod{24}$	$(-16/27)$
$-l, l \equiv 19 \pmod{24}$	$(-16/27)$
$-3l, l \equiv 1 \pmod{24}$	$\emptyset$

4.3 Integral model and intersection number at bad primes

In this section, we compute $P_D(x)$ modulo 2 and 3 by computing intersection numbers of Heegner divisors on the integral model of E_6 .

Let $\mathcal{X} = \mathcal{X}_{1,6,m}$ be the moduli space for abelian surfaces with additional structure as in [KR08, §2]. An integral model $\mathcal{E}$ of E_6 (resp. $\mathcal{V}$ of V_6) is obtained by the quotient of $\mathcal{X}$ by a finite subgroup of order $4 \cdot 2\eta(m)$ (resp. $2\eta(m)$), where $\eta(m)$ is defined in [KR08, (3.4)].

Let p be a prime. For $p \neq 2, 3$, the curve E_6 has good reduction at p , and $\mathcal{E}_{\mathbb{F}_p} \simeq \mathbb{P}_{\mathbb{F}_p}^1$. Suppose $p|\Delta$. As a consequence of the theorem of Čerednik-Drinfeld (see for instance [BC91]), the formal completion of the integral model along its special fiber at p is isomorphic to a finite union of Galois twists (over unramified extensions) of quotients of Mumford curves ([Mum72]). Then the geometric special fiber $\mathcal{E}_{\overline{\mathbb{F}_p}}$ of $\mathcal{E}$ at p can be viewed as a graph, and we follow [Kur79] to compute its dual graph and thus determine $\mathcal{E}_{\mathbb{F}_p}$.

Lemma 4.3.1. *For $p = 2, 3$, the special fiber $\mathcal{E}_{\mathbb{F}_p} \simeq \mathbb{P}_{\mathbb{F}_p}^1$.*

Proof. Let $B_{\Delta/p}$ be the definite quaternion algebra of discriminant $\frac{\Delta}{p}$, and $\mathfrak{O}$ be a maximal order of $B_{\Delta/p}$, so that $\mathfrak{O} \otimes \mathbb{Z}_q \simeq \mathcal{O} \otimes \mathbb{Z}_q$ for any prime $q \neq p$. Let

$$\begin{aligned} \Gamma_0 &= \mathfrak{O}[p^{-1}]^\times / \mathbb{Z}[p^{-1}]^\times, \\ \Gamma^* &= \{\gamma \in B_{\Delta/p}^\times : \gamma \mathfrak{O}[p^{-1}] = \mathfrak{O}[p^{-1}] \gamma\} \end{aligned}$$

regarded as discrete subgroups of $\mathrm{PGL}_2(\mathbb{Q}_p)$, and I denote the Bruhat-Tits tree. We have graphs with lengths $\Gamma_0 \backslash I$ and $\Gamma^* \backslash I$ defined by the quotient of the Bruhat-Tits tree [Kur79, §3]. The number of vertices of $\Gamma_0 \backslash I$ equals the class number $h(B_{\Delta/p})$ of $B_{\Delta/p}$ [Kur79, p.291].

As explained in detail in [Kur79], the dual graph of the geometric special fiber $\mathcal{E}_{\overline{\mathbb{F}_p}}$ is obtained from $\Gamma^* \backslash I$ by removing self-inverse edges. The graph $\Gamma^* \backslash I$ is a quotient of $\Gamma_0 \backslash I$, and we have $h(B_2) = 1$ and $h(B_3) = 1$, so both $\mathcal{E}_{\overline{\mathbb{F}_2}}$ and $\mathcal{E}_{\overline{\mathbb{F}_3}}$ consist of a single irreducible component. Since the generic fiber $E_6 \simeq \mathbb{P}_{\mathbb{Q}}^1$, which has genus 0 and a rational point, it follows that $\mathcal{E}_{\mathbb{F}_2} \simeq \mathbb{P}_{\mathbb{F}_2}^1$ and $\mathcal{E}_{\mathbb{F}_3} \simeq \mathbb{P}_{\mathbb{F}_3}^1$. $\square$

Intersection number

Consider $\mathcal{X} \xrightarrow{2\eta(m)} \mathcal{V} \xrightarrow{4} \mathcal{E}$. We will use [KR08, (3.12)] to compute the arithmetic intersection number. Let D be a fundamental discriminant, and $\mathcal{P}_{D,\mathcal{X}}$ be the Heegner divisor of discriminant D on $\mathcal{X}$ as defined in [KR08, §2] and $\mathcal{P}_{D,\mathcal{E}} = \sum_{x \in E_6(D)} \underline{x}$ be the divisor on $\mathcal{E}$. On V_6 , the universal automorphism group is $\{\pm 1\}$, the elliptic points of order 3 have CM by $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ and the elliptic points of order 2 have CM by $\mathbb{Z}[-1]$. The Atkin-Lehner involutions w_2 has two fixed points (CM by $\mathbb{Z}[-1]$), w_3 has two fixed points (CM by $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$), w_6 has

two fixed points (CM by $\mathbb{Z}[\sqrt{-6}]$). For discriminants $D < -6$, we have

$$\langle \mathcal{P}_{-3,\varepsilon}, \mathcal{P}_{D,\varepsilon} \rangle_{\varepsilon} = \frac{2}{4} \cdot \frac{2 \cdot 3}{2\eta(m)} \langle \mathcal{P}_{-3,\chi}, \mathcal{P}_{D,\chi} \rangle_{\chi}, \quad (4.3.0.1)$$

$$\langle \mathcal{P}_{-4,\varepsilon}, \mathcal{P}_{D,\varepsilon} \rangle_{\varepsilon} = \frac{2}{4} \cdot \frac{2 \cdot 2}{2\eta(m)} \langle \mathcal{P}_{-4,\chi}, \mathcal{P}_{D,\chi} \rangle_{\chi}. \quad (4.3.0.2)$$

Recall [BG08b, Lemma 3] that $P_D(x) \equiv x^n \pmod{2}$ for some n and $P_D(x) \equiv \pm x^m \pmod{3}$ for some m . For discriminants D considered in this work, we obtain a strengthened version by computing the local intersection number of $\mathcal{P}_{-3,\chi}$ or $\mathcal{P}_{-4,\chi}$ with $\mathcal{P}_{D,\chi}$ at 2 and 3.

Lemma 4.3.2. *Let D be a fundamental discriminant.*

1. *When $3 \nmid D$, the local intersection of $\mathcal{P}_{-3,\varepsilon}$ and $\mathcal{P}_{D,\varepsilon}$ at p is 0 if $-3D$ is not a square modulo $24p$.*
2. *When $2 \nmid D$, the local intersection of $\mathcal{P}_{-4,\varepsilon}$ and $\mathcal{P}_{D,\varepsilon}$ at p is 0 if $-4D$ is not a square modulo $24p$.*

Proof. This follows immediately from the intersection formula in [KR08, Theorem 3.2] and (4.3.0.1), (4.3.0.2). $\square$

Lemma 4.3.3. *Let $l \geq 5$ be a prime. For discriminants D of the form in the table, the following reductions hold:*

D	$P_D \pmod{2}$	$P_D \pmod{3}$
$-4l, l \equiv 13 \pmod{24}$	$x^{h'}$	$\pm x^{h'}$
$-l, l \equiv 19 \pmod{24}$	1	$\pm x^{h'}$
$-3l, l \equiv 1 \pmod{24}$	1	± 1

Proof. For $D = -4l$ where $l \equiv 13 \pmod{24}$ or $D = -l$ where $l \equiv 19 \pmod{24}$, since $-3D$ is not a square modulo 72, the local intersection of $\mathcal{P}_{-3,\varepsilon}$ and $\mathcal{P}_{D,\varepsilon}$ at $p = 3$ is 0, then $v_3(j(a)) > 0$ for every root $j(a)$ of $P_D(x)$, so $P_D(x) \equiv \pm x^{h'} \pmod{3}$. For $l \equiv 1 \pmod{24}$, since $12l$ is not a square modulo 72, the local intersection of $\mathcal{P}_{-4,\varepsilon}$ and $\mathcal{P}_{-3l,\varepsilon}$ at $p = 3$ is 0, then $v_3(j(a)) < 0$ for every root $j(a)$ of $P_{-3l}(x)$, so $P_{-3l}(x) \equiv \pm 1 \pmod{3}$.

For $D = -l$ where $l \equiv 19 \pmod{24}$ or $D = -3l$ where $l \equiv 1 \pmod{24}$, since $-4D$ is not a square modulo 48, the local intersection of $\mathcal{P}_{-4,\varepsilon}$ and $\mathcal{P}_{D,\varepsilon}$ at $p = 2$ is 0, then $v_2(j(a)) < 0$ for every root $j(a)$ of $P_D(x)$, so $P_D(x) \equiv 1 \pmod{2}$. The case of $P_{-4l} \pmod{2}$ where $l \equiv 13 \pmod{24}$ is proved in [BG08b, Lemma 6]. $\square$

4.4 Proof of main theorem

Let S be a finite set of primes containing primes above 2, 3 and all primes occurring in j_0 and $27j_0 + 16$. Write $P = |\text{Nm}_{L/\mathbb{Q}}(P_D(j_0))|$, $Q = |\text{Nm}_{L/\mathbb{Q}}(27j_0 + 16)|$, $s = \text{sign}(\text{Nm}_{L/\mathbb{Q}}(P_D(j_0)))$, $s' = \text{sign}(\text{Nm}_{L/\mathbb{Q}}(27j_0 + 16))$, and $N = d^{h'}P$ where $h' = \deg P_D$. Let $j_1 < j_2 < \cdots < j_r$ be the real conjugates of j_0 .

In each case, we are going to find some discriminant D with a rational prime $p \notin \text{Nm}_{L/\mathbb{Q}}(S)$ such that $v_p(P_D(j_0)) > 0$ and $\left(\frac{D}{p}\right) \neq 1$, then as in [BG08b], there is a prime $\mathfrak{p} \notin S$ above p , such that the Jacobian of C has supersingular, and hence superspecial reduction.

1. Choose a prime l satisfying the conditions:

- $l \equiv 13 \pmod{24}$,
- $\left(\frac{-l}{q}\right) = 1$ for every prime $q \in \text{Nm}_{L/\mathbb{Q}}(S) \setminus \{2, 3\}$,
- $P_{-4l}(x)$ has a real root $j(a_i)$ in a subinterval of $(-\frac{16}{27}, 0)$ to be specified later.

Let $D = -4l$. By [BG08b, Lemma 6] and Lemma 4.3.3,

$$\begin{aligned} P_{-4l}(x) &\equiv x^{h'} \pmod{4}, \\ P_{-4l}(x) &\equiv \pm x^{h'} \pmod{3}, \\ P_{-4l}(x) &\equiv (27x + 16)S(x)^2 \pmod{l} \text{ for some } S(x) \in \mathbb{Z}[x]. \end{aligned}$$

Since $v_{\mathfrak{p}}(j_0) \leq 0$ for all $\mathfrak{p}$ above 2, 3, we can choose d such that $d \prod_{\sigma \in T} \sigma(j_0)$ is integral for any $T \subset \text{Hom}(L, \overline{\mathbb{Q}})$ and any prime dividing d lies in $\text{Nm}_{L/\mathbb{Q}}(S)$, then $N, dQ \in \mathbb{N}$ and $(N, 6) = 1$, $(dQ, 2) = 1$. Suppose $l \nmid N$, then

$$\begin{aligned} \left(\frac{-4l}{N}\right) &= \left(\frac{-1}{N}\right) \left(\frac{l}{N}\right) = \left(\frac{-1}{N}\right) \left(\frac{N}{l}\right) \\ &= \left(\frac{-1}{N}\right) \left(\frac{dQ}{l}\right) = \left(\frac{-1}{N}\right) \left(\frac{l}{dQ}\right) \\ &= \left(\frac{-1}{N}\right) \left(\frac{-1}{dQ}\right) \left(\frac{-l}{dQ}\right) \\ &= \left(\frac{-1}{s(d \text{Nm}_{L/\mathbb{Q}} j_0)^{h'}}\right) \left(\frac{-1}{s' 3^{[L:\mathbb{Q}]} d \text{Nm}_{L/\mathbb{Q}}(j_0)}\right) \left(\frac{-l}{3^{v_3(dQ)}}\right) \\ &= s s' (-1)^{[L:\mathbb{Q}] + v_3(dQ)}. \end{aligned}$$

If $[L : \mathbb{Q}] + v_3(dQ)$ is odd, let

$$j(a_1) \in \left(-\frac{16}{27}, -\frac{16}{27} + \min_{1 \leq i \leq r} \left|j_i + \frac{16}{27}\right|\right)$$

so that $(27j_i + 16)P_{-4l}(j_i) > 0$ for each $1 \leq i \leq r$. If $[L : \mathbb{Q}] + v_3(dQ)$ is even, by assumption let j_t be the minimal real conjugate of j_0 in $(-\frac{16}{27}, 0)$, and

$$j(a_1) \in (j_t, j_{t+1})$$

so that $(27j_i + 16)P_{-4l}(j_i) > 0$ for each $1 \leq i \leq r, i \neq t$ and $(27j_t + 16)P_{-4l}(j_t) < 0$. In either case we have

$$\left(\frac{-4l}{N}\right) = -1$$

and there is a prime divisor p of N such that

$$\left(\frac{-4l}{p}\right) = -1.$$

The conditions on l and $(N, 6) = 1$ imply that $p \notin \text{Nm}_{L/\mathbb{Q}}(S)$ and $v_p(\text{Nm}_{L/\mathbb{Q}}(P_D(j_0))) = v_p(N) > 0$. If $l|N$, then since $l \notin \text{Nm}_{L/\mathbb{Q}}(S)$ by construction, we can choose $p = l$.

2. Choose a prime l satisfying the conditions:

- $l \equiv 19 \pmod{24}$,
- $\left(\frac{q}{l}\right) = \left(\frac{-l}{q}\right) = 1$ for every prime $q \in \text{Nm}_{L/\mathbb{Q}}(S) \setminus \{2, 3\}$,
- $P_{-l}(x)$ has a real root $j(a_1)$ in a subinterval of $(0, \infty)$ to be specified later.

Let $D = -l$. By Lemma 4.3.3, Lemma 4.2.4, and [BG08b, Lemma 4],

$$\begin{aligned} P_{-l}(x) &\equiv 1 \pmod{2}, \\ P_{-l}(x) &\equiv \pm x^{h'} \pmod{3}, \\ P_{-l}(x) &\equiv 3(27x + 16)S(x)^2 \pmod{l} \text{ for some } S(x) \in \mathbb{Z}[x]. \end{aligned}$$

Since $v_{\mathfrak{p}}(j_0) \geq 0$ for $\mathfrak{p}$ above 2 and $v_{\mathfrak{p}}(j_0) \leq 0$ for $\mathfrak{p}$ above 3, we can choose d such that $d \prod_{\sigma \in T} \sigma(j_0)$ is integral for any $T \subset \text{Hom}(L, \overline{\mathbb{Q}})$ and any prime dividing d lies in $\text{Nm}_{L/\mathbb{Q}}(S) \setminus \{2\}$, then $N, dQ \in \mathbb{N}$ and $(N, 6) = 1$. Suppose $l \nmid N$, then

$$\begin{aligned} \left(\frac{-l}{N}\right) &= \left(\frac{N}{l}\right) \\ &= \left(\frac{s(d \text{Nm}_{L/\mathbb{Q}}(3(27j_0 + 16)))}{l}\right) \\ &= \left(\frac{ss'3^{[L:\mathbb{Q}]}dQ}{l}\right) \\ &= ss'(-1)^{[L:\mathbb{Q}] + v_3(dQ) + v_2(Q)} \end{aligned}$$

Let j_t be the minimal real conjugate of j_0 in $(0, \infty)$ and n ($0 \leq n < r$) be the number of real conjugates of j_0 in $(-\frac{16}{27}, 0)$. If $[L : \mathbb{Q}] + v_3(dQ) + v_2(Q)$ is odd, let

$$j(a_1) \in \begin{cases} (j_t, j_{t+1}) & n \text{ is odd,} \\ (0, j_t) & n \text{ is even,} \end{cases}$$

so that $\text{Nm}_{L/\mathbb{Q}}(P_{-l}(j_0)) \text{Nm}_{L/\mathbb{Q}}(27j_0 + 16) > 0$. If $[L : \mathbb{Q}] + v_3(dQ) + v_2(Q)$ is even, let

$$j(a_1) \in \begin{cases} (j_t, j_{t+1}) & n \text{ is even,} \\ (0, j_t) & n \text{ is odd,} \end{cases}$$

so that $\text{Nm}_{L/\mathbb{Q}}(P_{-l}(j_0)) \text{Nm}_{L/\mathbb{Q}}(27j_0 + 16) < 0$. In either case we have

$$\left(\frac{-l}{N}\right) = -1$$

and there is a prime divisor p of N such that

$$\left(\frac{-l}{p}\right) = -1.$$

The conditions on l and $(N, 6) = 1$ imply that $p \notin \text{Nm}_{L/\mathbb{Q}}(S)$ and $v_p(\text{Nm}_{L/\mathbb{Q}}(P_D(j_0))) = v_p(N) > 0$. If $l|N$, then since $l \notin \text{Nm}_{L/\mathbb{Q}}(S)$ by construction, we can choose $p = l$.

3. Choose a prime l satisfying the conditions:

- $l \equiv 1 \pmod{24}$,
- $\left(\frac{-3l}{q}\right) = 1$ for every prime $q \in \text{Nm}_{L/\mathbb{Q}}(S) \setminus \{2, 3\}$,
- the number of real conjugates of j_0 between the two real roots of $P_{-3l}(x)$ is odd, so that

$$\text{Nm}_{L/\mathbb{Q}}(P_{-3l}(j_0)) < 0.$$

Let $D = -3l$. By [BG08b, Lemma 4], the only possible odd prime power in $b_{h'}$ is 3 where 3 is a square modulo l . Then by Lemma 4.3.3 and Lemma 4.2.4,

$$\begin{aligned} P_{-3l}(x) &\equiv 1 \pmod{2}, \\ P_{-3l}(x) &\equiv \pm 1 \pmod{3}, \\ P_{-3l}(x) &\equiv S(x)^2 \pmod{l} \text{ for some } S(x) \in \mathbb{Z}[x]. \end{aligned}$$

Since $v_{\mathfrak{p}}(j_0) \geq 0$ for $\mathfrak{p}$ above 2, 3, we can choose d such that $d \prod_{\sigma \in T} \sigma(j_0)$ is integral for any $T \subset \text{Hom}(L, \overline{\mathbb{Q}})$ and any prime dividing d lies in $\text{Nm}_{L/\mathbb{Q}}(S) \setminus \{2, 3\}$, then $N \in \mathbb{N}$. Since $P_{-3l}(x)$ is constant modulo 6 and $[L : \mathbb{Q}]$ is even, we have

$$d^{h'} \text{Nm}_{L/\mathbb{Q}}(P_{-3l}(j_0)) \equiv 1 \pmod{6}.$$

Suppose $l \nmid P$, then

$$\left(\frac{-3l}{N}\right) = \left(\frac{N}{3l}\right) = \left(\frac{-1}{3l}\right) \left(\frac{d^{h'} \text{Nm}_{L/\mathbb{Q}}(P_{-3l}(j_0))}{3l}\right) = \left(\frac{-1}{3l}\right) = -1$$

since $P_{-3l}(x)$ is square modulo l . There is a prime divisor p of N such that

$$\left(\frac{-3l}{p}\right) = -1.$$

The conditions on l and $(N, 6) = 1$ imply that $p \notin \text{Nm}_{L/\mathbb{Q}}(S)$ and $v_p(\text{Nm}_{L/\mathbb{Q}}(P_D(j_0))) = v_p(N) > 0$. If $l \mid N$, then since $l \notin \text{Nm}_{L/\mathbb{Q}}(S)$ by construction, we can choose $p = l$.

Remark 4.4.1. One can try to further weaken the local conditions by considering Heegner cycles with different forms of discriminant D . For primes p dividing D , the unpaired roots of $P_D(x)$ modulo p can be predicted by checking whether a maximal order in a definite quaternion algebra ramified at $2, 3, p$ contains two anticommuting CM orders of some given discriminants, as computed in [Jao03, 3.4.2]. One can then impose conditions on the number of prime divisors of D and the congruence class modulo 24 of primes dividing D , so that $P_D(x)$ has no unpaired roots or $P_D(x)$ has a single unpaired root from the same elliptic point modulo each $p \nmid D$. In addition, one imposes a congruence condition on D so that $\mathcal{P}_{D,\varepsilon}$ avoids intersection with one of $\mathcal{P}_{-3,\varepsilon}$ and $\mathcal{P}_{-4,\varepsilon}$ by Lemma 4.3.2. The local conditions on j_0 are determined so that it avoids intersection with these $\mathcal{P}_D$ at $p = 2, 3$, and some real conjugate of j_0 and some real root of P_D lie in the subinterval corresponding to one geodesic. For D not of the form $-Np$ with $N = 1, 3, 4, 8, 12, 24$, it is possible that $P_D(x)$ has multiple real roots in each subinterval, but we still expect an equidistribution result.

Bibliography

- [BC91] J.-F. Boutot and H. Carayol. “Uniformisation p -adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld”. In: *Courbes modulaires et courbes de Shimura (Orsay, 1987/1988)*. 196–97. Société mathématique de France, 1991, pp. 45–158.
- [BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. “The Magma algebra system. I. The user language”. In: *J. Symbolic Comput.* 24.3–4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265.
- [BG08a] Srinath Baba and Håkan Granath. “Genus 2 curves with quaternionic multiplication”. In: *Canad. J. Math.* 60.4 (2008), pp. 734–757.
- [BG08b] Srinath Baba and Håkan Granath. “Primes of superspecial reduction for QM abelian surfaces”. In: *Bull. Lond. Math. Soc.* 40.2 (2008), pp. 311–318.
- [BO78] Pierre Berthelot and Arthur Ogus. *Notes on crystalline cohomology*. Princeton University Press, Princeton, NJ; University of Tokyo Press, Tokyo, 1978.
- [Bou+25] Thomas Bouchet et al. *Mumford-type Shimura curves contained in the Torelli locus*. 2025. arXiv: 2510.00093.
- [CH88] P. E. Conner and J. Hurrelbrink. *Class number parity*. Vol. 8. Series in Pure Mathematics. World Scientific Publishing Co., Singapore, 1988.
- [Cha18] François Charles. “Exceptional isogenies between reductions of pairs of elliptic curves”. In: *Duke Math. J.* 167.11 (2018), pp. 2039–2072.
- [Cla03] Pete L. Clark. “Rational points on Atkin -Lehner quotients of Shimura curves”. English. PhD thesis. Harvard University, 2003.
- [Con04] Brian Conrad. “Gross-Zagier revisited”. In: *Heegner points and Rankin L-series*. Vol. 49. Math. Sci. Res. Inst. Publ. With an appendix by W. R. Mann. Cambridge Univ. Press, Cambridge, 2004, pp. 67–163.
- [Del+82] Pierre Deligne et al. *Hodge cycles, motives, and Shimura varieties*. Vol. 900. Lecture Notes in Mathematics. Springer-Verlag, Berlin-New York, 1982.
- [Elk87] Noam D. Elkies. “The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$ ”. In: *Invent. Math.* 89.3 (1987), pp. 561–567.

- [Elk89] Noam D. Elkies. “Supersingular primes for elliptic curves over real number fields”. In: *Compositio Math.* 72.2 (1989), pp. 165–172.
- [Elk98] Noam D. Elkies. “Shimura curve computations”. In: *Algorithmic number theory (Portland, OR, 1998)*. Vol. 1423. Lecture Notes in Comput. Sci. Springer, Berlin, 1998, pp. 1–47.
- [Gal00] Federica Galluzzi. “Abelian fourfold of Mumford-type and Kuga-Satake varieties”. In: *Indag. Math. (N.S.)* 11.4 (2000), pp. 547–560.
- [Gee08] Bert van Geemen. “Real multiplication on $K3$ surfaces and Kuga-Satake varieties”. In: *Michigan Math. J.* 56.2 (2008), pp. 375–399.
- [Hec81] Erich Hecke. *Lectures on the theory of algebraic numbers*. Vol. 77. Graduate Texts in Mathematics. Translated from the German by George U. Brauer, Jay R. Goldman and R. Kotzen. Springer-Verlag, New York-Berlin, 1981.
- [HP17] Benjamin Howard and Georgios Pappas. “Rapoport-Zink spaces for spinor groups”. In: *Compos. Math.* 153.5 (2017), pp. 1050–1118.
- [Hui25] Chun-Yin Hui. *On distribution of supersingular primes of abelian varieties and $K3$ surfaces*. 2025. arXiv: 2504.08088.
- [Jao03] David Yen Jao. “Supersingular primes for rational points on modular curves”. English. PhD thesis. Harvard University, 2003.
- [Kat81] N. Katz. “Serre-Tate local moduli”. In: *Algebraic surfaces (Orsay, 1976–78)*. Vol. 868. Lecture Notes in Math. Springer, Berlin, 1981, pp. 138–202.
- [Kis10] Mark Kisin. “Integral models for Shimura varieties of abelian type”. In: *J. Amer. Math. Soc.* 23.4 (2010), pp. 967–1012.
- [KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*. Vol. 108. Annals of Mathematics Studies. Princeton University Press, Princeton, NJ, 1985.
- [KR08] Kevin Keating and David P. Roberts. “Intersection numbers of Heegner divisors on Shimura curves”. In: *Pure Appl. Math. Q.* 4.4 (2008), pp. 1165–1204.
- [Kur79] Akira Kurihara. “On some examples of equations defining Shimura curves and the Mumford uniformization”. In: *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 25.3 (1979), pp. 277–300.
- [Lan94] Serge Lang. *Algebraic number theory*. Second. Vol. 110. Graduate Texts in Mathematics. Springer-Verlag, New York, 1994.
- [Li+25] Wanlin Li et al. *Infinitely many primes of basic reduction for some abelian fourfolds*. 2025. arXiv: 2511.05322.
- [Liu02] Qing Liu. *Algebraic geometry and arithmetic curves*. Vol. 6. Oxford Graduate Texts in Mathematics. Translated from the French by Reinie Ern , Oxford Science Publications. Oxford University Press, Oxford, 2002.

- [Mad15] Keerthi Madapusi Pera. “The Tate conjecture for K3 surfaces in odd characteristic”. In: *Invent. Math.* 201.2 (2015), pp. 625–668.
- [Mad16] Keerthi Madapusi Pera. “Integral canonical models for spin Shimura varieties”. In: *Compos. Math.* 152.4 (2016), pp. 769–824.
- [Mes72] William Messing. *The crystals associated to Barsotti-Tate groups: with applications to abelian schemes*. Vol. Vol. 264. Lecture Notes in Mathematics. Springer-Verlag, Berlin-New York, 1972.
- [MS10] James S. Milne and Junecue Suh. “Nonhomeomorphic conjugates of connected Shimura varieties”. In: *Amer. J. Math.* 132.3 (2010), pp. 731–750.
- [MS81] J. S. Milne and Kuang-yen Shih. “The action of complex conjugation on a Shimura variety”. In: *Ann. of Math. (2)* 113.3 (1981), pp. 569–599.
- [Mum69] D. Mumford. “A note of Shimura’s paper “Discontinuous groups and abelian varieties””. In: *Math. Ann.* 181 (1969), pp. 345–351.
- [Mum72] David Mumford. “An analytic construction of degenerating curves over complete local rings”. In: *Compositio Math.* 24 (1972), pp. 129–174.
- [Neh33] Harald Nehr Korn. “Über absolute idealklassengruppen und einheiten in algebraischen zahlkörpern”. In: *Abh. Math. Sem. Univ. Hamburg* 9.1 (1933), pp. 318–334.
- [Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 1999.
- [Rib89] Kenneth A. Ribet. “Bimodules and abelian surfaces”. In: *Algebraic number theory*. Vol. 17. Adv. Stud. Pure Math. Academic Press, Boston, MA, 1989, pp. 359–407.
- [Rot04] Victor Rotger. “Modular Shimura varieties and forgetful maps”. In: *Trans. Amer. Math. Soc.* 356.4 (2004), pp. 1535–1550.
- [Sad04] Marat Sadykov. “Two results in the arithmetic of Shimura curves”. PhD thesis. Columbia University, 2004.
- [Ser81] Jean-Pierre Serre. “Quelques applications du théorème de densité de Chebotarev”. In: *Inst. Hautes Études Sci. Publ. Math.* 54 (1981), pp. 323–401.
- [Sha+22] Ananth N. Shankar et al. “Exceptional jumps of Picard ranks of reductions of K3 surfaces over number fields”. In: *Forum Math. Pi* 10 (2022), Paper No. e21, 49.
- [Shi75] Goro Shimura. “On the real points of an arithmetic quotient of a bounded symmetric domain”. In: *Math. Ann.* 215 (1975), pp. 135–164.
- [ST18] Ananth N. Shankar and Jacob Tsimerman. “Unlikely intersections in finite characteristic”. In: *Forum Math. Sigma* 6 (2018), Paper No. e13, 17.

- [ST20] Ananth N. Shankar and Yunqing Tang. “Exceptional splitting of reductions of abelian surfaces”. In: *Duke Math. J.* 169.3 (2020), pp. 397–434.
- [Tay25] Salim Tayou. “Picard rank jumps for K3 surfaces with bad reduction”. In: *Algebra Number Theory* 19.1 (2025), pp. 77–112.
- [Voi09] John Voight. “Shimura curves of genus at most two”. In: *Math. Comp.* 78.266 (2009), pp. 1155–1172.
- [Voi21] John Voight. *Quaternion algebras*. Vol. 288. Graduate Texts in Mathematics. Springer, Cham, 2021.
- [Xu22] Yujie Xu. “Normalization in the Integral Models of Shimura Varieties of Abelian Type”. PhD thesis. Harvard University, 2022.