Infinitude of Superspecial Primes for QM Abelian Surfaces of Discriminant 10

Edward Beckon, Rayan Gummiid, Yuhao Liu, Junseo Park, Milena Safaryan, Luke Trunnell, Janeen Wang

July 30, 2026

Abstract

A classical theorem of Elkies states that every elliptic curve over a number field with a real embedding has infinitely many supersingular primes. Baba and Granath (2008) and Chen (2025) extended this to abelian surfaces with quaternionic multiplication (QM) by the quaternion algebra of discriminant 6 satisfying certain conditions, producing infinitely many superspecial primes in these cases. In this paper, we discuss the strategy underlying these results and present our progress adapting it to QM abelian surfaces of discriminant 10. We compute the superspecial locus at 5, control reductions of Heegner cycles at the ramified primes, classify unpaired roots mod ℓ, and prove a first case of superspecial infinitude conditional on the position of real roots.

1 Introduction

1.1 Main Result

Let $E/\mathbb{Q}$ be an elliptic curve. A prime p of good reduction is called *supersingular* for E if the reduction E_p is a supersingular elliptic curve, that is, if $\mathrm{End}(E_p \otimes \overline{\mathbb{F}}_p)$ is an order in a quaternion algebra rather than in an imaginary quadratic field. A theorem of [Elk87] states that every elliptic curve over $\mathbb{Q}$ has infinitely many supersingular primes.

This paper concerns the two-dimensional analogue of Elkies' theorem. The natural generalization of a supersingular elliptic curve is a *superspecial* abelian surface: one isomorphic over $\overline{\mathbb{F}}_p$ to a product of two supersingular elliptic curves. The natural class of surfaces to consider are those with quaternionic multiplication (QM), in other words, abelian surfaces $\mathcal{A}$ such that a maximal order Λ of an indefinite rational quaternion algebra B_Δ of discriminant Δ embeds into $\mathrm{End}(\mathcal{A})$; for such surfaces the reduction at any good prime $p \nmid \Delta$ is either ordinary or superspecial, so superspecial primes play precisely the role that supersingular primes play in dimension one. Baba and Granath [BG08b] proved

the first infinitude result in this setting, for $\Delta = 6$, and Chen [Che25] recently extended their theorem to number fields with a real embedding while weakening the local hypotheses at the ramified primes.

We study the case $\Delta = 10$ as past work in [BG08a] provides a coordinate map $j : E_{10} \to \mathbb{P}^1_{\mathbb{Q}}$. Our main result is Theorem 1.1 below, proved in §7 conditionally on two conjectures about the real roots of $P_{-\ell}(x)$, stated as Conjectures 8.1 and 8.3 in §8. The real-root hypotheses are expected to follow from the distribution argument similar to Elkies and Jao, and §6 develops the framework for verifying them; removing them is the principal remaining obstacle to an unconditional theorem.

The precise statement of our main result, restated and proved in §8, is as follows.

Theorem 1.1. *Let C be a genus-2 curve whose Jacobian has QM by a maximal order in B_{10}, and whose field of moduli is a number field L with at least one real embedding. Write $j_0 \coloneqq j(C) \in L$, let $d > 0$ be minimal such that $\mathrm{Nm}_{L/\mathbb{Q}}(j_0) = n/d$ with $(n, d, 10) = 1$, and set $Q \coloneqq |\mathrm{Nm}_{L/\mathbb{Q}}(8j_0 - 27)|$. Suppose that:*

(i) $v_{\mathfrak{p}}(j_0) \leq 0$ for every prime $\mathfrak{p}$ of L above 2;

(ii) $v_{\mathfrak{p}}(j_0) = 0$ for every prime $\mathfrak{p}$ of L above 5;

(iii) $[L : \mathbb{Q}] + v_2(dQ) + v_5(dQ)$ is odd;

(iv) every real conjugate of j_0 lies in $(-\infty, 0)$.

Assuming Conjectures 8.1 and 8.3 in §8, $\mathrm{Jac}(C)$ has superspecial reduction at infinitely many primes.

Example 1.2. *Here, we show that the conditions of Theorem 1.1 are satisfied by infinitely many $j_0 \in \mathbb{Q}$. For example, every negative odd integer $j_0 \equiv -3 \pmod{10}$. For such j_0, we can see that*

1. *$v_2(j_0) = 0$, since j_0 is odd;*
2. *$v_5(j_0) = 0$, since $j_0 \equiv 2 \pmod 5$;*
3. *$[L : \mathbb{Q}] + v_2(dQ) + v_5(dQ) = 1 + 0 + 0 = 1$ is odd;*
4. *the only real conjugate of j_0 is itself and it is negative.*

As such, $j_0 \equiv -3 \mod 10$ satisfies the conditions of Theorem 1.1.

1.2 History and related work

Before presenting the arguments of Elkies and Chen in detail, we first motivate their approaches by reviewing earlier results.

In 1941, Deuring showed that the number of isomorphism classes of supersingular elliptic curves over the algebraic closure $\overline{\mathbb{F}}_p$ is asymptotic to $\frac{p}{12}$.

More specifically, Deuring showed that the number of isomorphism classes is

$$\begin{aligned}
&\lfloor \frac{p}{12} \rfloor \text{ if } p \equiv 1 \mod 12 \\
&\lfloor \frac{p}{12} \rfloor + 1 \text{ if } p \equiv 5 \mod 12 \\
&\lfloor \frac{p}{12} \rfloor + 1 \text{ if } p \equiv 7 \mod 12 \\
&\lfloor \frac{p}{12} \rfloor + 2 \text{ if } p \equiv 11 \mod 12
\end{aligned}$$

In 1961, Shimura and Taniyama proved that for any elliptic curve over a number field with CM, the supersingular primes have density $\frac{1}{2}$.

In 1968, Serre proved that for any elliptic curve over a number field without CM, the supersingular primes have density 0.

In 1987, Elkies proved that for any elliptic curve over a number field K such that $[K : \mathbb{Q}]$ is odd, there are infinitely many supersingular primes. Later that year, Elkies extended this result to elliptic curves over number fields with a real embedding.

Elkies' result was extended by Baba–Granath and by Chen to curves C of genus 2. Baba–Granath proved that, if C has field of moduli $\mathbb{Q}$ and has potentially smooth stable reduction at 2 and 3, and if the Jacobian $\mathrm{Jac}(C)$ has multiplication by the maximal quaternion order of discriminant 6, then $\mathrm{Jac}(C)$ has superspecial reduction at infinitely many primes. Chen extended Baba–Granath's result to genus-2 curves whose field of moduli is a number field with a real embedding.

1.3 Organization of Paper

In §2, we cover the relevant background on elliptic curves, abelian surfaces, Jacobians, supersingularity, endomorphism algebras, Shimura curves, and other concepts necessary to understand this work and related results by [Elk87], [BG08a], [BG08b], and [Che25]. In §3, we give an exposition on the Elkies' proof strategy and how it has been extended to prove higher-dimensional analogues of the infinitude of supersingular primes for certain families of abelian surfaces. In §4, we outline our proof for the case of discriminant 10. In §5 we use intersection theory to analyze the reduction of $P_D(x)$ mod 2 and 5. In §6, we analyze the reduction of $P_D(x)$ mod ℓ by looking at the possible unpaired roots and the leading coefficient. In §8, we analyze the distribution of the real roots of $P_D(x)$, and outline the difficulties faced in applying Jao's approach to the discriminant 10 case. In §9, we prove our main result.

1.4 Notation

- By E, we mean an elliptic curve.
- By $\mathcal{A}$, we mean an abelian surface.
- By B_Δ, we mean the indefinite rational quaternion algebra of discriminant Δ.
- By Λ_Δ, we mean a maximal order of B_Δ.
- By $\mathcal{O}_D$, we mean a maximal order of an imaginary quadratic field of discriminant D.
- By $\mathbb{H}$, we mean the upper half plane of $\mathbb{C}$

2 Background

2.1 Quaternion Algebras

Here, quaternion algebras are important for two key reasons. First, in the theory of elliptic curves, we say that E is *supersingular* if we can find a maximal order Λ in a quaternion algebra and produce an embedding

$$\Lambda \hookrightarrow \mathrm{End}(E).$$

Second, when working with an abelian surface, we work with ones that have quaternionic multiplication before reducing modulo p. We present relevant definitions from [Voi21].

Definition 2.1 (Quaternion Algebra)**.** *An algebra B over a field K is a quaternion algebra if there exists $\alpha, \beta \in B$ such that $\{1, \alpha, \beta, \alpha\beta\}$ is a K-basis of B and*

$$\alpha^2 = a, \beta^2 = b, \alpha\beta = -\beta\alpha$$

for some invertible $a, b \in K^*$

The most familiar example is the Hamiltonian quaternions. This algebra describes three-dimensional rotations.

Example 2.2 (Hamiltonian Quaternion Algebra)**.** *Our field of definition is $\mathbb{R}$. Set $a = b = -1$ so the $\mathbb{R}$-basis is $\{1,i,j,k\}$ where,*

$$\alpha^2 = \beta^2 = (\alpha\beta)^2 = -1$$

An important property of the Hamiltonian quaternion algebra is that it is a division algebra, so nonzero elements have inverses. We now introduce a key technical detail.

Definition 2.3 (Ramified and Split)**.** *Let $\mathfrak{v}$ be a place of K. We say B ramifies at $\mathfrak{v}$ if $B_{\mathfrak{v}} = B \otimes_K K_v$ is a division ring. Here, K_v denotes the completion of K with respect to the place $\mathfrak{v}$. Otherwise, B is split at $\mathfrak{v}$ and $B_{\mathfrak{v}} = B \otimes_K K_v \cong M_2(K_{\mathfrak{v}})$. See [Voi21].*

We can observe that the Hamiltonian quaternion algebra is ramified at 2 and infinity. In fact, any quaternion algebra defined over a global field must be ramified at a finite even number of places. Next, we offer a different way to categorize quaternion algebras based on their splitting behavior at infinity.

Definition 2.4 (Definite vs. Indefinite)**.** *A quaternion algebra B is called definite if it ramifies or becomes a division algebra at every infinite place, and B is called indefinite if it splits at least one infinite place.*

We are concerned with the places at which quaternion algebras ramify. To track this, we define the discriminant.

Definition 2.5 (Discriminant)**.** *The discriminant of quaternion algebra B is the product of all finite places at which B ramifies.*

From now on we will only use quaternion algebras ramified at two finite primes. The two such algebras with which we will work are B_6 and B_{10}, ramified at {2,3} and {2,5}, respectively. Our work concerning B_{10} is based on existing work on B_6. These two quaternion algebras are convenient because they ramify at the smallest primes. In general, we do not expect infinitely many supersingular primes for abelian surfaces with QM by a quaternion algebra ramified at arbitrarily large primes.

The quaternion algebra B_{10} is generated over $\mathbb{Q}$ by two elements α, β such that

$$\alpha^2 = -2, \beta^2 = 5, \alpha\beta = -\beta\alpha.$$

Similarly, B_6 is generated over $\mathbb{Q}$ by two elements α, β such that

$$\alpha^2 = -2, \beta^2 = 3, \alpha\beta = -\beta\alpha$$

Next, we explain how an element of a quaternion algebra acts on the $\mathbb{H}$ This is necessary for discussing moduli spaces of QM abelian surfaces. Any indefinite quaternion algebra can be embedded into the matrix algebra $\mathrm{M}_2(\mathbb{R})$. This embedding allows each element to be represented as a unique matrix that acts naturally on $\mathbb{H}$.

2.2 Endomorphism Rings

Before discussing, endomorphism rings, we define orders.

Definition 2.6 (Order)**.** *An order in a quaternion algebra is a subring $\Lambda \subset B$ that is a finitely generated $\mathcal{O}_K$-module, where $\mathcal{O}_K$ is the ring of algebraic integers of K. An order is called maximal if it is not contained in any other order.*

Orders are relevant to us because, as they embed into the endomorphism rings of QM abelian surfaces.

Endomorphism rings are central in the study of elliptic curves and abelian surfaces. A larger endomorphism ring signifies that the curve/surface has more symmetries. The most straightforward example we see is the endomorphism ring of an ordinary elliptic curve.

Example 2.7. *An ordinary elliptic curve over a field with characteristic 0 has endomorphism ring* $\mathrm{End}(E) = \mathbb{Z}$.

Most elliptic curves' endomorphism rings are $\mathbb{Z}$; however, some curves have more structure-preserving maps to itself, and we refer to these larger symmetries as Complex Multiplication.

Definition 2.8 (CM Elliptic Curve)**.** *An elliptic curve E is said to have CM by an order $\mathcal{O}_D$ of an imaginary quadratic field $\mathbb{Q}(\sqrt{-D})$ if such $\mathcal{O}_D$ is isomorphic to the endomorphism ring* $\mathrm{End}(E)$.

Example 2.9. *The elliptic curve $E/\mathbb{Q}$ given by $y^2 = x^3 + x$ has CM by $\mathbb{Z}[i]$. We can see this because the map*

$$i : (x, y) \to (x, iy)$$

is an endomorphism of E. We call this map "multiplication by i." Another way to see this is in terms of complex tori. In particular, the elliptic curve in this example has the structure of the complex torus $\mathbb{C}/(\mathbb{Z} \oplus i\mathbb{Z})$. It can be observed that this structure has CM by $\mathbb{Z}[i]$; in other words, multiplication by i: $i : z \mapsto iz$ maps the lattice onto to itself.

It is a well known fact that when reducing the curve from characteristic 0 to some finite characteristic, the endomorphism ring does not become smaller. There exists a natural embedding the endomorphism ring before to after. Interestingly, in rare cases, $End(E)$ becomes larger and loses the abelian group structure. We call this supersingular reduction.

Definition 2.10 (Supersingular Elliptic Curve)**.** *Let $E/\mathbb{F}_p$ be an elliptic curve defined over a field with characteristic p. We say E is supersingular if we can find an embedding of a maximal order Λ in a quaternion algebra into the endomorphism ring of E such that* $\mathrm{Im}(\Lambda) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$.

We move on to endomorphism rings of abelian surfaces. Given an abelian surface $\mathcal{A}$ over a field with characteristic 0, we see that the ordinary case is given by $\mathrm{End}(\mathcal{A}) = \mathbb{Z}$. In order to prove the infinitude superspecial primes, this is not good enough as a starting point. Thus, we assume that our abelian surface already has quaternion multiplication.

Definition 2.11 (QM Abelian surface)**.** *An abelian surface $\mathcal{A}$ is said to have QM by B_Δ, where Δ is the discriminant of B_Δ, if there exists an embedding of a maximal order $\Lambda_\Delta \subset B_\Delta$ into the endomorphism ring of $\mathcal{A}$*

$$\Lambda_\Delta \hookrightarrow \mathrm{End}(\mathcal{A}).$$

Since QM is our starting point, we are interested in what happens when an abelian surface has an endormorphism ring that becomes even larger.

Definition 2.12 (Superspecial Abelian Surface)**.** *An abelian surface $\mathcal{A}$ is called superspecial if it is isomorphic to the product of two supersingular elliptic curves. In characteristic p, QM abelian surfaces are either ordinary or superspecial, hence supersingular implies superspecial.*

To detect this phenomenon in the case of QM abelian surfaces, we have to investigate further the endomorphism ring of $\mathcal{A}$ and add the theory of complex multiplication.

Lemma 2.13. *[BG08b] Let $\mathcal{A}$ be a QM abelian surface and $\mathrm{End}_{QM}(\mathcal{A})$ be the centralizer of the image of Λ_Δ in $\mathrm{End}(\mathcal{A})$. $\mathcal{A}$ has CM by $\mathcal{O}_D$ if $\mathcal{O}_D$ embeds optimally in $\mathrm{End}_{QM}(\mathcal{A})$. Furthermore, if π is a prime whose residual characteristic does not split in $\mathbb{Q}(\sqrt{-D})$, then the reduction of $\mathcal{A}$ at π is superspecial.*

To make checking this condition easier, we offer a necessary condition for an order of an imaginary quadratic field to embed into the centralizer of the endomorphism ring.

Lemma 2.14. *Let $\mathcal{O}_D$ embed in B_Δ. Then, for all $p \mid \Delta$, p does not split in $\mathcal{O}_D$. This implies that if p splits in $\mathcal{O}_D$, then it is impossible for $\mathcal{O}_D$ to embed in B_Δ*

Proof. Taken from [ALMW20]. □

2.3 Moduli spaces

Related works like [Che25] and [BG08a] treat abelian surfaces as points in a moduli space. Hence, it is necessary to review the functorial meanings and constructions of the relevant moduli spaces. The moduli spaces we will consider are E_Δ and V_Δ. For more details, see [BG08a]

Example 2.15 (Coarse moduli space V_Δ)**.** *Let B_Δ be an indefinite quaternion algebra over $\mathbb{Q}$, and Λ be a maximal order in B_Δ. Consider the functor sending a scheme S to the set of principally polarized abelian surfaces (A, ι) over S with an embedding $\Lambda \overset{\eta}{\hookrightarrow} \mathrm{End}\, A$. This functor admits a coarse moduli space called V_Δ.*

To introduce the main moduli space E_Δ that we will use in this paper, we need to explain the Atkin-Lehner group and its action on V_Δ. For simplicity, we only take $\Delta = 10$ for the indefinite quaternion algebra B_{10}. For more details, see [BG08b, Section 1].

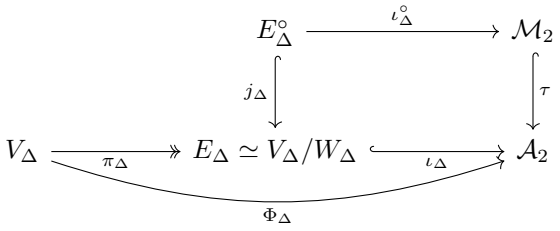
Example 2.16 (Coarse moduli spaces E_Δ and E_Δ^0)**.** *As discussed in works such as [BG08a][BG08b], [Kur79], and [Che25], we consider the Atkin-Lehner group*

$W_\Delta : \mathrm{N}_{B_\Delta^\times}(\Lambda)/\mathbb{Q}^\times\Lambda^\times$, *which acts on* V_Δ. *Hence we get a scheme* $W_\Delta\backslash V_\Delta$, *which is again a coarse moduli space. In fact,* E_Δ *parametrizes principally polarized abelian surfaces with potential quaternion embedding; in other words, it represents the following functor:*

$$\begin{aligned} h_{E_\Delta} : (\mathsf{Sch}/S)^{\mathrm{op}} &\longrightarrow \mathsf{Set}, \\ T &\longmapsto \mathrm{Hom}_S(T, E_\Delta). \end{aligned}$$

In addition, $E_\Delta^0 \subset E_\Delta$ *is the coarse moduli space that parametrizes principally polarized abelian surfaces with potential quaternion embedding such that they are Jacobian curves of the smooth genus* 2.

Remark 2.17. *All the examples of arithmetic moduli spaces explained above have factoring relation that is the following diagram:*



2.4 Intersection theory

In the works of Elkies, Baba, Granath, and Chen, we are often concerned with the arithmetic properties of a polynomial like

$$P_D(x) = b\big(x - j(a_1)\big)\cdots\big(x - j(a_n)\big),$$

where $a_1, \ldots, a_n$ are the distinct curves/surfaces with CM by an order of discriminant D. We demonstrate a way to address this question geometrically through the language of intersection theory.

In Figure 1, the horizontal axis $\operatorname{Spec}\mathbb{Z}$ represents each prime, along with zero; we interpret this as a one-dimensional geometric object. (In general, we can work with $\operatorname{Spec}\mathcal{O}_K$ for any number field K, but we stick to the rational case for simplicity.) The vertical axis E_Δ represents the moduli space of "principally polarized" abelian surfaces with QM by discriminant Δ, i.e. our one-dimensional space of j-invariants of surfaces in characteristic 0. Moving right represents surfaces in characteristic $p > 0$. This two-dimensional ambient space $\mathcal{E}$ is called an *integral model* of the Shimura curve V_Δ.
The integral model that we will be working with arises from extending our moduli space corresponding to discriminant 10, E_{10}. This surface, $\mathcal{E}$, is where we will be doing intersection theory. Figure 1 can offer some heuristic intuition for what this surface looks like.

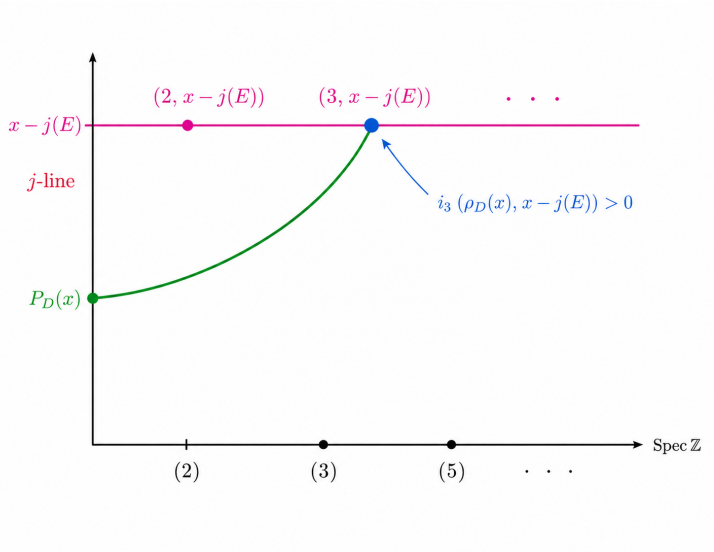


Figure 1: A visualization of the intersection of the closure of $x - j(E)$ and the divisor defined by $P_D(x)$.

A priori, there exist curves on $\mathcal{E}$ called *Heegner divisors*. Specifically, the Heegner divisor $\mathcal{P}_D$ is defined as the collection of points that have CM by an order of discriminant D. (We sometimes write $\mathcal{P}_{D,\mathcal{E}}$ with respect to the integral model.) The geometry of how Heegner divisors intersect each other at small primes is very helpful in determining how P_D reduces modulo those primes, as seen in the proof of Lemma 5.3.

As an example, fix a discriminant D and a prime p. Consider elliptic curves over $\mathbb{Q}$, where our integral model is $\mathbb{Z}[x]$. Arithmetically, to determine whether a given elliptic curve has CM by $\mathcal{O}_D$ in characteristic p, we check if its j-invariant is a root of the modular polynomial $P_D(x)$ modulo p. To understand how intersection theory applies to this situation, we must define the local intersection number. The local intersection number at a prime ideal $\mathfrak{q} \subset \mathbb{Z}[x]$ is given by

$$i_{\mathfrak{q}}(f, g) = \text{length}_{\mathbb{Z}[x]_{\mathfrak{q}}} \left(\frac{\mathbb{Z}[x]_{\mathfrak{q}}}{(f, g)} \right),$$

where $f, g \in \mathbb{Z}[x]$ are the defining polynomials. Now take

$$\mathfrak{q} = (p, x - j(E)), \qquad f = x - j(E), \qquad g = P_D(x).$$

Then,

$$\frac{\mathbb{Z}[x]_{\mathfrak{q}}}{(x - j(E), P_D(x))} \cong \left(\frac{\mathbb{Z}}{(P_D(j(E)))} \right)_{(p)}.$$

Therefore,

$$i_{\mathfrak{q}}(x - j(E), P_D(x)) = \text{length}_{\mathbb{Z}_{(p)}} \left(\frac{\mathbb{Z}_{(p)}}{(P_D(j(E)))} \right).$$

This length is exactly the p-adic valuation:

$$i_{\mathfrak{q}}(x - j(E), P_D(x)) = v_p\big(P_D(j(E))\big).$$

In particular,

$$i_{\mathfrak{q}}(x - j(E), P_D(x)) > 0 \iff p \mid P_D(j(E)).$$

Thus, the local intersection number detects precisely whether

$$P_D(j(E)) \equiv 0 \pmod{p},$$

matching the condition that the reduction E modulo p has CM by $\mathcal{O}_D$.

3 Exposition of Elkies '89, Baba and Granath '08, and Chen '25

3.1 Elkies '89

Given an elliptic curve E over number field L with real embedding, Elkies proves E has infinitely many supersingular primes by providing an algorithm to construct a new supersingular prime outside of S, where S is a finite set of primes in L. Denoting by E_π the reduction of E modulo a prime π in a number field, and p for the residual characteristic of π, the strategy is to find $\pi \notin S$ so that E_π has CM by $\mathcal{O}_D$, with p not split in $\mathbb{Q}(\sqrt{D})$. To do this, Elkies chooses a CM cycle $\mathcal{O}_D$ so that the residual characteristic of every prime in S splits in $\mathbb{Q}(\sqrt{D})$. Thus, if the prime j_E intersects this CM cycle above a prime not split in $\mathbb{Q}(\sqrt{D})$, it is a new supersingular prime.

Intersection at π with residual characteristic p is equivalent to

$$v_p(\text{Nm}_{L/\mathbb{Q}}(P_D(j_E))) > 0$$

Thus, it suffices to show that for some p dividing the numerator of $\text{Nm}_{L/\mathbb{Q}}(P_D(j_E))$, p is a quadratic non-residue in $\mathbb{Q}(\sqrt{D})$. Elkies uses Jacobi symbols to detect a non-split prime by controlling sign contributions from unpaired roots, the denominator of $P_D(x)$, and the sign of $\text{Nm}_{L/\mathbb{Q}}(P_D(j_E))$.

To control the unpaired roots of $P_D(x)$ in mod ℓ, Elkies proves the if E_π does not have CM by $\mathcal{O}_{-4}$, the number of non-isomorphic curves is even. This comes from the observation that normalized lifts of E_π come in conjugate pairs, with an isomorphism between the two lifts corresponding to E_π having CM by $\mathcal{O}_{-4}$. Equivalently, E_π has j-invariant 1724.

$$P_D(x) \equiv (x - 1728)^k S(x)^2 \pmod{\pi},\ S(x) \in \mathbb{Z}[x]$$

The degree of $P_D(x)$ is the class number h of $\mathbb{Q}(\sqrt{D})$, hence by choosing discriminants with even class number, Elkies eliminates the possibility of unpaired roots.

Through the choice of D, the real roots of $P_D(x)$ be placed relative to real conjugates of j_E so that the sign of $\mathrm{Nm}_{L/\mathbb{Q}}(P_D(j_E))$ is negative. Thus letting $N = \mathrm{Num}(\mathrm{Nm}_{L/\mathbb{Q}}(P_D(j_E)))$, we have $\left(\frac{N}{D}\right) = -1$, hence $P_D(j_E)$ has positive π-adic valuation for some non-split prime π. [Elk89]

3.2 Baba and Granath '08

To prove the existence of infinitely many superspecial primes, Baba and Granath follow a similar strategy to Elkies of intersecting CM cycles with $\mathcal{A}$ above primes that do not split in $\mathbb{Q}(\sqrt{D})$. The proof is more complex at each step.

First, there are multiple unpaired roots, hence more work is required to determine their parity. As in Elkies, lifts of abelian surface $\mathcal{A}$ in mod ℓ to characteristic 0 come in conjugate pairs, with isomorphic lifts corresponding to $\mathcal{A}$ having CM by $\mathcal{O}_{-4}$. In addition, further unpaired roots arise from the identification of conjugate lifts by Atkin-Lehner involutions during the descent from V_6 to E_6. [Jao03] provides a strategy for eliminating some unpaired roots. In particular, in the case of one unknown root, the parity of $P_D(x)$ can be used to determine whether the parity of the root.

Second, the CM cycles chosen must be compatible with the existing QM structure. 2 and 3 cannot split in $\mathbb{Q}(\sqrt{D})$, hence their sign contribution must be accounted for during computation with Jacobi symbols. To do this, Baba and Granath impose the local condition that $v_2(j_0) = v_3(j_0) = 0$ and use the fact that there are no superspecial curves in characteristic 2 and 3 to prove that $P_D(x) \equiv x^n \bmod 2$, $P_D(x) \equiv ax^m \bmod 3$.

Third, $P_D(x)$ is no longer being monic, hence the leading coefficient $b_{h'}$ also contributes to the sign of Jacobi symbols. Baba and Granath prove that the only odd prime powers in the leading coefficent are primes unramified in $\mathbb{Q}(\sqrt{D})$, which allows them to determine $b_{h'}$.

To control the sign of $P_D(j_0)$, we need to determine two properties: the number of real roots and their location on the real line. Baba and Granath prove that the real root for $P_{-4l}(x)$, where $l \equiv 13 \pmod{24}$, is unique. To determine its location, Baba and Granath analyze how j maps the fundamental region to the real line. The preimage of the real line under the modular function $j = j_6$ consists of three open hyperbolic segments. By taking linear combinations of the quaternion algebra elements that correspond to the vertices of the hyperbolic

segments, with positive integer coefficients, we can span the entire collection of principally polarized abelian surfaces with CM by $\mathcal{O}_D$ that have a real root in a specified interval.

3.3 Chen '25

Chen strengthens Baba and Granath's result by weakening the local conditions at 2, 3, and generalizing to abelian surfaces with field of moduli a number field L, where L has a real embedding. This changes the argument in two ways.

First, to weaken the condition $v_2(j_0) = v_3(j_0) = 0$, Chen uses the intersection formula from [KR06] to calculate the exact degree of $P_D(x)$ mod 2 and 3. For example, using the fact that $\mathcal{P}_{-4}$ goes to infinity, she determines that for some D, $\mathcal{P}_{-4}$ and $\mathcal{P}_D$ have zero intersection above 2, hence $\mathcal{P}_{-D} = x^{h'} \bmod 2$.

Second, controlling the sign becomes an issue involving the real conjugates of j_0 and the distribution of real roots of $P_D(x)$. Using Hecke's equidistribution result, Chen controls the sign by changing the position of a real root of $P_D(x)$ relative to real conjugates of j_0 in order to get the contradiction in signs for her proof.

4 Our Argument

In our proof, we follow the strategy of [Che25]. The reduction of $P_D(X)$ at 2 follows easily; however, we find an obstacle at the reduction at 5. Unlike the case with discriminant 6, there exists a superspecial curve in characteristic 5, which allows the superspecial reduction of a Heegner cycle in characteristic 5. Then, using intersection formulas, we prove that our chosen D avoids reduction to the superspecial curve in $\mathbb{F}_5$.

Example 4.1 (Unique Superspecial Curve in Characteristic 5)**.** *The unique genus-2 curve with superspecial Jacobian is*

$$y^2 = x^5 - x \mod 5$$

Following the strategy used in [Jao03], we determine the unpaired roots of $P_D(X) \mod \ell$. To do this, Jao notes two possible ways unpaired roots can arise. Starting with a point in shimura curve V lying over a root of $P_D(X) \mod \ell$, he applies the Shimura analogue to Deuring lift. Here if the conjugate pairs of lifts are isomorphic we get our first unpaired roots. Taking the quotient from V_Δ to E_Δ we get further unpaired roots if our lifted points stack. In other words, if they are identified by an Atkin-Lehner involution. Due to the Shimura curve coordinate function no longer being a perfect square, it requires some additional work to prove the same result regarding odd prime powers in $b_{h'}$.
Finally, the main obstacle in the discriminant 10 case is determining the real

roots of $P_D(x)$. In the existing work with discriminant 6, the Shimura curve comes from a quotient of a triangle group, and Jao was able to find real roots by searching the boundary of the hyperbolic triangle that is the fundamental domain of this quotient. In the discriminant 10 case, we have to quotient by a quadrilateral group. This results in a hyperbolic quadrilateral fundamental domain instead of a hyperbolic triangle. Attempting to apply Jao's method to this situation created some difficulty. Specifically we applied his method to our quadrilateral and found contradictions indicating inconclusive results about which intervals contain real roots under which congruence conditions. We make partial progress in finding the real roots, and under Conjecture 8.1, which matches by numerical evidence from CM cycles computed by Elkies in [Elk00], we prove the infinitude of supersingular primes for certain abelian surfaces.

5 Reduction of $P_D(x)$ mod 2, 5

The first thing we must check is that our special fibers on our integral model above 2 and 5 behave nicely. We know that all fibers above primes p not diving the discriminant will be isomorphic to $\mathbb{P}^1_{\mathbb{F}_p}$. For primes dividing the discriminant, in our case 2 and 5, this must be verified. The reason we need this lemma is to be able to apply the intersection formula from [KR06] to our surface $\mathcal{E}$.

Lemma 5.1.

$$\mathcal{E}_p \cong \mathbb{P}^1_{\mathbb{F}_p} \quad \textit{for any prime } p$$

Proof. Following Chen's argument in [Che25, Lemma 3.1], we use results from [Kur79] and [Kur79].

(i). For good primes $p \neq 2, 5$, the integral model has good reductions, and $\mathcal{E}_p \cong \mathbb{P}^1_{\mathbb{F}_p}$ since $\mathcal{E}_0 \cong E_{10} \cong \mathbb{P}^1_{\mathbb{Q}}$.

(ii). Consider the bad primes 2 and 5. By [BC], a consequence of Čerednik-Drinfeld's theorem implies that the formal completion of the integral model $\mathcal{E}$ along the special fiber at p is isomorphic to a finite union of Galois twists over unramified extensions. Then the special fiber can be regarded by a graph by [Kur79], and we can follow Kurihara on the computations.

Let $B^{(p)}$ be the definite quaternion algebra ramified at $10/p$ and ∞ with discriminant $10/p$ for bad primes $p = 2$ or 5. Let $\mathfrak{O} \subset B^{(p)}$ be a maximal order of $B^{(p)}$ such that $\mathfrak{O} \otimes \mathbb{Z}_p \cong \Lambda \otimes \mathbb{Z}_p$. Let

$$\Gamma_0 = \mathfrak{O}[p^{-1}]^\times / \mathbb{Z}[p^{-1}]^\times$$
$$\Gamma^* = \{\gamma \in B^{(p),\times} : \gamma\mathfrak{O}[p^{-1}] = \mathfrak{O}[p^{-1}]\gamma\}$$

regarded as discrete subgroups of $\mathrm{PGL}_2(\mathbb{Q}_p)$, and $\mathcal{T}$ be the Bruhat-Tits tree. Then [Kur79, § 3] defined graphs with lengths $\Gamma_0\backslash\mathcal{T}$ and $\Gamma^*\backslash\mathcal{T}$ defined by the quotients of the Bruhat-Tits tree. The number of vertices

of $\Gamma_0\backslash\mathcal{T}$ equals the class number $h(B^{(p)})$. By Eichler's formula, see [Kur79, Equation 4-1],

$$h = \frac{1}{12}\prod_{\ell|d}(\ell-1) + \frac{1}{4}\prod_{\ell|d}\left(1-\left(\frac{-4}{\ell}\right)\right) + \frac{1}{3}\prod_{\ell|d}\left(1-\left(\frac{-3}{\ell}\right)\right)$$

where $d = \mathrm{disc}(B^{(p)}) = 10/p$. Then

$$h(B^{(5)}) = \frac{1}{12} + \frac{1}{4} + \frac{2}{3} = 1$$

and

$$h(B^{(2)}) = \frac{4}{12} + 0 + \frac{2}{3} = 1.$$

The dual graph of the geometric special fiber $\mathcal{E}_{\overline{\mathbb{F}}_p}$ is obtained by removing self-inverse edges from the graph $\Gamma^*\backslash\mathcal{T}$. But $\Gamma^*\backslash\mathcal{T}$ is a quotient graph of $\Gamma_0\backslash\mathcal{T}$, and $h(B^{(2)}) = h(B^{(5)}) = 1$, so both $\mathcal{E}_{\overline{\mathbb{F}}_2}$ and $\mathcal{E}_{\overline{\mathbb{F}}_5}$ consist of a single irreducible component. Since the genric fiber $E_{10} \cong \mathbb{P}^1_{\mathbb{Q}}$ is a smooth curve with a $\mathbb{Q}$-valued point and has genus 0, it follows that $\mathcal{E}_p \cong \mathbb{P}_{\mathbb{F}_p}$ for bad primes 2 and 5.

□

Now that we have established that our special fibers are well behaved, we move on to checking the possible roots of $P_D(X)$ mod 2 and 5. This comes down to checking what possible superspecial curves exist in these characteristics.

Lemma 5.2. *Let D be a fundamental discriminant, $K_D := \mathbb{Q}(\sqrt{D}) \hookrightarrow B_{10}$. Then, any $x \in E_{10}(\overline{\mathbb{Q}})$ reduces to only $j = 0$, $1/4$, or ∞ mod 5.*

Proof. We first claim that the superspecial locus at 5 is $j = 0, 1/4$, or ∞. First, consider the boundary points $E_{10}\backslash E^0_{10}$. By Table 2 of [BG08a], they correspond to $\{j = 0\}$ and $\{j = \infty\}$. By the same table, they are CM-points with discriminants -3 and -8, respectively. By [KR06, Proposition 2.1], since they are both CM points with fundamental discriminants, geometrically $A \cong E_1 \times E_2$, A is either $j = 0$ or $j = \infty$, and E_1 and E_2 are elliptic curves such that $\mathrm{End}(E_1) \cong \mathrm{End}(E_2) \cong \mathcal{O}_D$. Recall that 5 does not split in $K_D = \mathbb{Q}(\sqrt{D})$ since $\mathcal{O}_D \hookrightarrow \Lambda \subset B_{10}$. Now by Deuring's criterion, both E_1 and E_2 are supersingular at 5, hence both $j = 0$ and $j = \infty$ have superspecial supports at 5.

It remains to check the interior E^0_{10}. By [IKO86, Theorem 3.3], there is only one smooth genus-2 curve up to isomorphism whose Jacobian is superspecial at 5. By [IKO86, Lemma 1.1], it is easy to verify that the curve C_{-20} mentioned in [BG08a, Proposition 4.3] is isomorphic to this curve.

Next we will show that any CM point $x \in E_{10}(D)$ reduces superspecially at 5, which completes the proof.

We invoke again [KR06, Proposition 2.1]. Since D is fundamental, and x has CM by $\mathcal{O}_D$, Proposition 2.1 gives

$$E \cong E_1 \times E_2, \quad \mathrm{End}(E_1) \cong \mathrm{End}(E_2) \cong \mathcal{O}_D$$

Now by Deuring's criterion, E is superspecial. Hence x can only reduce to $j = 0, 1/4$, or ∞. □

The following two results use the intersection theory of Heegner divisors on Shimura curves. See Sec. 2.7 for exposition.

Lemma 5.3. *Suppose D is a fundamental discriminant and p a prime.*

- *When $2 \nmid D$, the Heegner divisors $\mathcal{P}_{-8,\mathcal{E}}$ and $\mathcal{P}_{D,\mathcal{E}}$ have zero local intersection at p if $-8D$ is not a square modulo $40p$.*
- *When $2 \nmid D$ and $5 \nmid D$, the Heegner divisors $\mathcal{P}_{-20,\mathcal{E}}$ and $\mathcal{P}_{D,\mathcal{E}}$ have zero local intersection at p if $-20D$ is not a square modulo $40p$.*

Proof. This follows from [KR06, Theorem 3.2]. □

Lemma 5.4. *For $D = -\ell$, where $\ell > 5$ is a prime congruent to 3 or 27 mod 40, we have $P_D(x) \equiv x^{h'} \mod 2$ and $P_D(x) \equiv kx^m \mod 5$ for some $m \geq 0, k \in \{1, 2, 3, 4\}$.*

Proof. Since $2 \nmid D$ and $-8D \equiv 24, 56 \mod 80$ is not a square modulo 80, the Heegner divisors $\mathcal{P}_{-8,\mathcal{E}}$ and $\mathcal{P}_{D,\mathcal{E}}$ have zero local intersection at 2 by Lemma 5.3. Since $j(-8)$ goes to ∞, we must therefore have $j(D) \equiv 0 \mod 2$, giving us $P_D(x) \equiv x^{h'} \mod 2$.

Since $2, 5 \nmid D$ and $-20D \equiv 60, 140 \mod 200$ is not a square modulo 200, the Heegner divisors $\mathcal{P}_{-20,\mathcal{E}}$ and $\mathcal{P}_{D,\mathcal{E}}$ have zero local intersection at 5 by Lemma 5.3. Since $j(-20) \equiv 1/4 \mod 5$, we must therefore have $j(D) \equiv 0, \infty \mod 5$, giving us $P_D(x) \equiv kx^m \mod 5$ for some $m \geq 0, k \in \{1, 2, 3, 4\}$. □

6 Degree of $P_D(x)$

To determine the degree of $P_D(x)$, we follow Chen's strategy. We have

$$h' = \frac{h(\mathcal{O}_D)}{N},$$

where h' is the degree of $P_D(x)$, $h(\mathcal{O}_D)$ is the class number of the order $\mathcal{O}_D$, and N is the order of the subgroup generated by the primes $p \mid 10$ that ramify in $\mathbb{Q}(\sqrt{D})$. In our case,

$$D = -\ell, \qquad \ell \equiv 3 \text{ or } 27 \pmod{40}.$$

Hence 2 and 5 do not ramify in $\mathbb{Q}(\sqrt{D})$. Therefore, $N = 1$. Moreover, since ℓ is prime and $\ell \equiv 3 \pmod 4$, genus theory implies that $h(\mathcal{O}_D)$ is odd [CH88]. It follows that

$$\deg P_D(x) = h' = h(\mathcal{O}_D)$$

is odd.

7 Reduction of $P_D(x)$ mod ℓ

We want $P_D(X) \bmod \ell$ to be a square so that we can control the Jacobi symbol. Unfortunately, this is too much to ask and we will inevitably end up with unpaired roots. To find our unpaired roots, we adapt the strategy from [Jao03] detailed in Section 3.2 from discriminant 6 to discriminant 10. The main difference is that no unpaired roots can arise from the conjugate pair of lifts from characteristic ℓ to characteristic zero.

Lemma 7.1. *For $x_0 \in V_{10}$ mod ℓ lying above a root of $P_D(X)$ mod ℓ, lifts of x_0 to $x, x' \in V_{10}$ in characteristic zero cannot be isomorphic.*

Proof. From [Jao03] we see that if there is an isomorphism between the abelian surfaces x, x', then both have CM by $\mathcal{O}_{-4}$. However, this is impossible because 5 splits in $\mathbb{Q}(\sqrt{D})$ 2.14. □

Thus, from Jao we only have unpaired roots that arise if $x, x' \in V_{10}$ are identified by an Atkin-Lehner involution, implying the roots reduce to the same point in E_{10}. Since points fixed by an Atkin-Lehner involution must be identified by another, our unpaired roots must be those fixed points.

Lemma 7.2 (Fixed points of Atkin-Lehner involutions in V_{10})**.** *Each Atkin-Lehner involution ω_n fixes exactly two points on V_{10}. Specifically, ω_2 fixes the two -8 CM points, ω_5 fixes the two -20 CM points, and ω_{10} fixes the two -40 CM points.*

Proof. Taken from [GPS+25] □

Corollary 7.3 (Unpaired roots of $P_D(x) \bmod \ell$)**.** *The possible unpaired roots are exactly the three CM points corresponding to discriminants $-8, -20, -40$.*

Proof. This follows from the fact that unpaired roots are fixed by Atkin-Lehner, and we have identified such points. □

Lemma 7.4. *If we have a root of $P_D(x)$ mod ℓ corresponding to CM by $O_{D'}$, where $D' \in \{-8, -20, -40\}$, then $2, 5, \ell$ do not split in $\mathbb{Q}(\sqrt{D'})$.*

Proof. Any root of $P_D(x) \bmod \ell$ will have O_D and $O_{D'}$, thus it corresponds to a supersingular surface. For $\ell \neq 2, 5$, this is a superspecial surface.

Let $\mathcal{A}$ be this surface mod ℓ. Recall this means $O_{D'}$ embeds in $\mathrm{End}_{QM}(A)$. Since this is a superspecial surface in characteristic ℓ, End_{QM} is a maximal order in the quaternion algebra $B_{10\ell}$. Thus, we conclude 2, 5, ℓ do not split. □

This gives us a method of ruling out unpaired roots. In particular, we use this to compute the following.

Lemma 7.5. *For prime $\ell \equiv 3, 27$ mod 40, the only unpaired root of $P_{-\ell}(x)$ mod ℓ is $j_{-40} = 27/8$, corresponding to CM by O_{-40}.*

Proof. For $D' \in \{-8, -20, -40\}$, we have
$\left(\frac{-8}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{2}{\ell}\right) = (-1)(-1) = +1$
$\left(\frac{-20}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{5}{\ell}\right) = (-1)(-1) = +1$
$\left(\frac{-40}{\ell}\right) = \left(\frac{-1}{\ell}\right)\left(\frac{2}{\ell}\right)\left(\frac{5}{\ell}\right) = (-1)(-1)(-1) = -1$
Hence the only unpaired root corresponds to CM by O_{-40}. □

Lemma 7.6. *Let $b_{h'}$ be the leading coefficient of $P_D(x)$. If p occurs with odd multiplicity in $b_{h'}$, then p is ramified in $K = \mathbb{Q}(\sqrt{D})$.*

Proof. We follow the argument of [BG08b, Lemma 4]. Let H be the Hilbert class field of K.

From [Kur79], the Shimura curve V_{10} can be identified with the algebraic curve $x^2 + y^2 + 2 = 0$, which in homogeneous coordinates is isomorphic to $\{x^2 + 2y^2 + z^2 = 0\} \subset \mathbb{P}^2(\mathbb{Q})$. As in [BG08a], we have the isomorphism $j_m : V_{10}(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ given by

$$j_m(z) = \frac{g(z)^3}{a_2(z)^2}$$

for modular forms g, a_2 satisfying

$$a_2^2 + 2a_5^2 + a_{10}^2 = 0$$

and

$$4g^3 + 27a_5^2 + a_{10}^2 = 0.$$

In particular, $j = j_m$, as proved in [BG08a], and in terms of homogeneous coordinates this implies

$$j = \frac{x^2 - 25y^2}{4x^2}.$$

Let $\alpha = x^2 - 25y^2$ and $\beta = 2x$ so that $j = \alpha/\beta^2$. Using homogeneous coordinates, force x, y to be integral.

We want to show that $j\mathcal{O}_H = (\alpha)/(\beta)^2$ remains a square in the denominator when in reduced form. Let $\mathfrak{p}$ be a prime of $\mathcal{O}_H$. If we can show $v_\mathfrak{p}(\alpha)$ even or $v_\mathfrak{p}(\alpha) \geq v_\mathfrak{p}(\beta^2)$, then we will be done because $\mathfrak{p}$ always cancels in pairs.

Case 1: $v_\mathfrak{p}(x^2) \neq v_\mathfrak{p}(-25y^2)$. In this case, it is a property of the $\mathfrak{p}$-adic valuation that

$$v_\mathfrak{p}(\alpha) = v_\mathfrak{p}(x^2 - 25y^2) = \min\{v_\mathfrak{p}(x^2), v_\mathfrak{p}(-25y^2)\} = \min\{2v_\mathfrak{p}(x), v_\mathfrak{p}(-25y^2)\},$$

where

$$v_{\mathfrak{p}}(-25y^2) = v_{\mathfrak{p}}(-1) + 2v_{\mathfrak{p}}(5y) = \text{even}$$

since the $\mathfrak{p}$-adic valuation of a unit is zero. Thus, $v_{\mathfrak{p}}(\alpha)$ even.

Case 2: $v_{\mathfrak{p}}(x^2) = v_{\mathfrak{p}}(-25y^2)$. By the same simplifications, this means $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(5) + v_{\mathfrak{p}}(y)$.

Case 2a: $v_{\mathfrak{p}}(2) = 0$. Observe that

$$v_{\mathfrak{p}}(x \pm 5y) \geq \min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(5) + v_{\mathfrak{p}}(y)\} = v_{\mathfrak{p}}(x),$$

implying $v_{\mathfrak{p}}(\alpha) \geq 2v_{\mathfrak{p}}(x)$. But

$$v_{\mathfrak{p}}(\beta^2) = 2v_{\mathfrak{p}}(2) + 2v_{\mathfrak{p}}(x) = 2v_{\mathfrak{p}}(x),$$

so $v_{\mathfrak{p}}(\alpha) \geq v_{\mathfrak{p}}(\beta^2)$.

Case 2b: $v_{\mathfrak{p}}(2) > 0$. Recall that j has CM by $\mathcal{O}_D$. Then, the Heegner divisors $\mathcal{P}_{-8}$ and $\mathcal{P}_D$ have zero local intersection at 2 for suitable D. Since $j(-8)$ corresponds to ∞, we have $v_{\mathfrak{p}}(j) \geq 0$ for each prime $\mathfrak{p}$ lying above 2. Therefore, $v_{\mathfrak{p}}(\alpha) \geq v_{\mathfrak{p}}(\beta^2)$, as desired.

Let x_1 be a root of P_D. From what we just proved, the fractional ideal $x_1\mathcal{O}_H$ is a square in the denominator in reduced form. Following [BG08b], we want this relation to hold true in the splitting field H' of P_D over K. For contradiction, suppose $x_1\mathcal{O}_{H'} = (\cdots)\mathfrak{p}^r$ for a prime $\mathfrak{p}$ and odd $r < 0$. Then, since H/H' is unramified, we would have $x_1\mathcal{O}_H = (\cdots)(\mathfrak{p}_1 \cdots \mathfrak{p}_n)^r$, contradicting that $x_1\mathcal{O}_H$ is a square in the denominator. Hence, we have $x_1\mathcal{O}_{H'} = (\cdots)/\mathfrak{b}^2$, where $\mathfrak{b}$ is an integral ideal of H' coprime to $(\cdots)$. The rest follows as [BG08b]
□

Lemma 7.7. *Let p divide $b_{h'}$. Then at least one root of $P_D(x)$ reduces to infinity mod p.*

Proof. Let $j_{a_1}, \ldots, j_{a_n}$ be the roots of $P_D(x)$. Since $v_p(b_{h'}) > 0$, for some $j_{a_i}, v_p(j_{a_i}) < 0$. Hence j_{a_i} reduces to infinity mod p. □

Lemma 7.8. *$P_D(x) \equiv 2(8x - 27)S(x)^2$ mod ℓ for prime $\ell \equiv 3, 27$ mod 40*

Proof. The only possible odd powers prime powers in $b_{h'}$ are primes which ramify 7.6. In particular, for our choice of D, the only prime which ramifies is ℓ. As computed in 7.7, ∞ is not a root of $P_D(x)$ mod ℓ. Hence $b_{h'}$ is a perfect square.

The only unpaired root of $P_D(x)$ is $\frac{27}{8}$. Using parity argument from degree of $P_D(x)$, we see $P_D(x) = 2(8x - 27)S(x)^2$ mod ℓ. □

8 Real Roots of $P_D(x)$

An important factor determining the conditions for superspecial reduction is the relative position between the real roots of the polynomial $P_D(x)$ and the real conjugates of the j-invariant. At first, we would like to know which points in the Shimura curve correspond to abelian surfaces with CM by the desired $\mathcal{O}_D$. This would enable us to construct $P_D(x)$ and analyze the real roots. According to Elkies, we need to search for x in Λ_{10} such that $(x-\bar{x})^2 = D$, where $\mathcal{O}$ is the maximal order of the quaternion algebra. Since the elements of the quaternion algebra can be represented as matrices, which have fractional linear transformation action on $\mathbb{H}$, we can analyze their fixed points, and it turns out that those fixed points precisely represent the abelian surfaces with CM by $\mathcal{O}_D$. Recall that the roots of $P_D(x)$ are determined by the coordinate function that we choose to parametrize the Shimura curve. Fortunately, Elkies has given some insights about the coordinate function corresponding to the discriminant 10 case. We provide a general overview of how the fundamental region is mapped to the real line, deriving the necessary conditions to achieve our main result.

8.1 Mapping to Real line

According to Elkies, deriving the mapping from the Shimura curve to the real line requires identifying the images of the elliptic fixed points under the coordinate map. The elliptic points are the fixed points of the elements in Γ_∞^*.

In accordance with Elkies, for the quaternion algebra of discriminant 10 we have exactly four elliptic elements with orders 3, 2, 2, 2. Recall that $\Gamma_\infty^* \backslash \mathcal{H}$ represents the fundamental region identifying the principally polarized abelian surfaces with QM. In order to understand the action of Γ_∞^* on the $\mathbb{H}$, it is more convenient to express elements in our quaternion algebra as matrices. Suppose B_{10} is generated over $\mathbb{Q}$ by elements b, e satisfying $b^2+2 = e^2-5 = be+eb = 0$, where

$$b := \begin{pmatrix} 0 & \sqrt{2} \\ -\sqrt{2} & 0 \end{pmatrix}, \quad e := \begin{pmatrix} \sqrt{5} & 0 \\ 0 & -\sqrt{5} \end{pmatrix}.$$

It turns out that with this identification, our elliptic elements are expressed as

$$s_3 = [2a-b-1], s_2 = [b], s_2' = [2b+5a-ab], s_2'' = [5a-ab]$$

with discriminants $-3, -8, -20, -40$, respectively. These elliptic elements correspond to fixed points in $\mathbb{H}$

$$z_{-3} = \frac{\sqrt{2}+i\sqrt{3}}{5(\sqrt{2}-1)}, z_{-8} = \frac{1+2i}{5}, z_{-20} = \frac{i}{\sqrt{5}(\sqrt{2}-1)}, z_{-40} = \frac{i}{\sqrt{5}}.$$

By the choice of coordinate function, we send z_{-3} to 0, z_{-8} to ∞, z_{-40} to $27/8$, and z_{-20} to $1/4$. Subsequently, each hyperbolic line segment connecting two elliptic points maps to a specific interval in the real line. For example, the hyperbolic line joining z_{-8} to z_{-3} maps to the interval $(-\infty, 0)$.

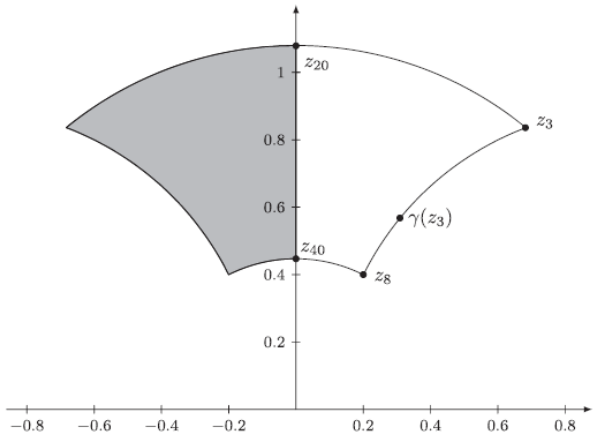


Figure 2: The fundamental domain for Γ^*_∞.

8.2 Necessary and Sufficient conditions for Real roots

As shown in the previous section, obtaining real roots within designated intervals requires the parameter point to lie along a particular hyperbolic segment. Combining this with the condition of having CM by $\mathcal{O}_D$, we get the following procedure.

- Search for x in Λ_Δ such that $(x - \bar{x})^2 = D$, where Λ_{10} is the maximal order of the quaternion algebra.
- Search for x in Λ_Δ such that x lies in a desired hyperbolic segment.
- Intersect them.

Following this strategy, we can indeed find the principally polarized abelian surfaces with CM by $\mathcal{O}_D$, and their j-invariants lie in a predetermined interval along the real line. Explicitly determining the necessary and sufficient conditions for x to lie within a given hyperbolic segment presents significant difficulties. However, based on numerical evidence, we formulate the following conjecture.

Conjecture 8.1. *The point x lies on the hyperbolic segment joining z_{-8} and z_{-3} and belongs to Λ_Δ if and only if*

$$x = as_3 + bs_2,$$

where a and b are positive integers.

With this conjecture in place, we can systematically apply our procedure. Executing this strategy yields the following result.

Lemma 8.2. *With Conjecture 8.1, the polynomial $P_D(x)$ has a real root in the interval $(-\infty, 0)$ if and only if*

$$|D| = 8a^2 + 16ab + 3b^2,$$

where a and b are positive integers.

Proof. Follows from our conjecture and results above. □

Although the quadratic form admits integer representations for prime l such that

$$\ell \equiv 3 \text{ or } 27 \pmod{40},$$

these representations are not necessarily positive. The proof of the following infinitude statement is still in progress. To carry out the preliminary calculations, we assume the following conjecture.

Conjecture 8.3. *Let S be any finite set of primes. Then there exists a prime*

$$\ell \equiv 3 \text{ or } 27 \pmod{40}$$

such that

$$\left(\frac{-\ell}{q}\right) = 1 \qquad \text{for every } q \in S \setminus \{2, 5\},$$

and such that the quadratic form appearing in Lemma 8.2 has no representation by positive integers. Note that by Dirichlet's theorem for primes in arithmetic progression, there exist infinitely many primes $\ell \equiv 3, 27$ mod 40 such that $(p/\ell) = 1$ for $p \in S \setminus \{2, 5\}$.

9 Proof of Main Theorem

We will now state our main result, under the assumption that Conjecture 8.1 and Conjecture 8.3 are true.

Theorem 9.1. *Let C be a genus-2 curve with Jacobian that has QM by B_{10} and has field of moduli a number field L with at least one real embedding.*

Write $j_0 \coloneqq j(C) \in L$ and $\mathrm{Nm}_{L/\mathbb{Q}}(j_0) = \dfrac{n}{d}$ with $(n, d, 10) = 1, d > 0$.
Suppose that $v_{\mathfrak{p}}(j_0) \leq 0$ for $\mathfrak{p}$ above 2, $v_{\mathfrak{p}}(j_0) = 0$ for $\mathfrak{p}$ above 5,
$[L : \mathbb{Q}] + v_2(d\mathrm{Nm}_{L/\mathbb{Q}}(8j_0 - 27)) + v_5(d\mathrm{Nm}_{L/\mathbb{Q}}(8j_0 - 27))$ is odd, and that all real conjugates of j_0 are in $(-\infty, 0)$. Then the Jacobian of C has superspecial reduction at infinitely many primes.

Proof. Let S be a finite set of primes containing primes above 2 and 5 and all primes occurring in j_0 and $8j_0 - 27$. We write $P = |\mathrm{Nm}_{L/\mathbb{Q}}(P_D(j_0))|$,
$Q = |\mathrm{Nm}_{L/\mathbb{Q}}(8j_0 - 27)|, s = \mathrm{sgn}(\mathrm{Nm}_{L/Q}(P_D(j_0))), s' = \mathrm{sgn}(\mathrm{Nm}_{L/Q}(8j_0 - 27))$
We will find a discriminant D and a rational prime $p \notin \mathrm{Nm}_{L/\mathbb{Q}}(S)$ such that $v_p(P_D(j_0)) > 0$ and $\left(\dfrac{D}{p}\right) \neq 1$; then, as in [BG08b], there is a prime $\mathfrak{p}$ above

p such that the Jacobian of C has supersingular, and therefore superspecial, reduction.
Choose a prime ℓ satisfying the following conditions:

- $\ell \equiv 3 \mod 40$ or $\ell \equiv 27 \mod 40$
- $\left(\frac{-\ell}{q}\right) = 1$ for every prime $q \in \mathrm{Nm}_{L/\mathbb{Q}}(S) \backslash \{2, 5\}$
- $P_{-\ell}(x)$ has no real roots in $(-\infty, 0)$

Let $D = -\ell$. By Lemma 5.4 and Lemma 7.8 we have

$$\begin{aligned} P_{-\ell}(x) &\equiv x^{h'} \mod 2 \\ P_{-\ell}(x) &\equiv kx^m \mod 5, k \in \{1, 2, 3, 4\} \\ P_{-\ell}(x) &\equiv 2(8x - 27)S(x)^2 \mod \ell, S(x) \in \mathbb{Z}[x] \end{aligned}$$

Since $v_{\mathfrak{p}}(j_0) \leq 0$ for all $\mathfrak{p}$ above 2 and $v_{\mathfrak{p}}(j_0) = 0$ for all $\mathfrak{p}$ above 5, we can choose d such that $d \prod_{\sigma \in T} \sigma(j_0)$ is integral for any $T \subset \mathrm{Hom}(L, \mathbb{Q})$ and any prime dividing d lies in $\mathrm{Nm}_{L/\mathbb{Q}}(S)$. Let $N = d^{h'} P$, where $h' = \deg P_D$; we have $N, dQ \in N$ and $(N, 10) = 1$.
Suppose $\ell \nmid N$. Then,

$$\begin{aligned} \left(\frac{-\ell}{N}\right) = \left(\frac{N}{\ell}\right) = \left(\frac{d^{h'}P}{\ell}\right) = \left(\frac{dP}{\ell}\right) = \left(\frac{ds\mathrm{Nm}_{L/\mathbb{Q}}(P_{-\ell}(j_0))}{\ell}\right) = \\ = \left(\frac{ds\mathrm{Nm}_{L/\mathbb{Q}}(2(8j_0 - 27))}{\ell}\right) = \left(\frac{ds2^{[L:\mathbb{Q}]}\mathrm{Nm}_{L/\mathbb{Q}}(8j_0 - 27)}{\ell}\right) = \\ = \left(\frac{ds2^{[L:\mathbb{Q}]}s'Q}{\ell}\right) = ss'\left(\frac{2^{[L:\mathbb{Q}]}dQ}{\ell}\right) = ss'(-1)^{[L:\mathbb{Q}]}\left(\frac{2}{\ell}\right)^{v_2(dQ)}\left(\frac{5}{\ell}\right)^{v_5(dQ)} = \\ = ss'(-1)^{[L:\mathbb{Q}]}(-1)^{v_2(dQ)}(-1)^{v_5(dQ)} = ss'(-1)^{[L:\mathbb{Q}]+v_2(dQ)+v_5(dQ)} = -ss' \end{aligned}$$

Since all real conjugates of j_0 are in $(-\infty, 0)$ and all real roots of $P_{-\ell}(x)$ line in $[0, \infty)$, we have $\mathrm{Nm}_{L/\mathbb{Q}}((8j_0 - 27)(P_{-\ell}(j_0))) > 0$ and thus $ss' = 1$. We see that

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

and thus there is a prime divisor p of N such that

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

The conditions on ℓ and the fact that $(N, 10) = 1$ imply that $p \notin \mathrm{Nm}_{L/\mathbb{Q}}(S)$ and $v_p(\mathrm{Nm}_{L/\mathbb{Q}}(P_D(j_0))) = v_p(N) > 0$.

If $\ell \mid N$, then since $\ell \notin \mathrm{Nm}_{L/\mathbb{Q}}(S)$ by construction, we can choose $p = \ell$. $\square$

10 Acknowledgments

This work was supported by National Science Foundation (DMS-2342225) and the Mathematical and Physical Sciences Foundation. We thank the Department of Mathematics at the University of California, Berkeley for hosting the Numbers, Symmetry, and Geometry RTG REU, and Professor Tony Feng for overseeing this program. We are especially grateful to Robin Huang and Hanson Hao for mentoring our project and introducing us to new interesting problems in math.

References

[ALMW20] Menny Aka, Manuel Luethi, Philippe Michel, and Andreas Wieser, *Simultaneous supersingular reductions of CM elliptic curves*, arXiv preprint arXiv:2005.01537 (2020).

[BC] Jean-François Boutot and Henri Carayol, *p-Adic Uniformization of Shimura Curves: The Theorems of Cerednik and Drinfeld*, English translation by Cameron Franc, Translation of "Uniformisation p-adique des courbes de Shimura : les théorèmes de Čerednik et de Drinfeld," Astérisque, no. 196–197 (1991), pp. 45–158.

[BG08a] Srinath Baba and Håkan Granath, *Genus 2 curves with quaternionic multiplication*, Canadian Journal of Mathematics **60** (2008), no. 4, 734–757.

[BG08b] ———, *Primes of superspecial reduction for qm abelian surfaces*, Bulletin of the London Mathematical Society, v.40, 311-318 (2008) **40** (2008).

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

[Che25] Fangu Chen, *Superspecial primes for qm abelian surfaces over real number fields*, 2025.

[Elk87] N.D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over q.*, Inventiones mathematicae **89** (1987), 561–568.

[Elk89] ———, *Supersingular primes for elliptic curves over real number fields*, Compositio Mathematica **72** (1989), 561–568.

[Elk00] Noam D. Elkies, *Shimura curve computations*, 2000.

[GPS+25] Tyler Genao, Tristan Phillips, Frederick Saia, Tim Santens, and John Yin, *Counting points on some genus zero shimura curves.*

[IKO86] Tomoyoshi Ibukiyama, Toshiyuki Katsura, and Frans Oort, *Supersingular curves of genus two and class numbers*, Compositio Mathematica **57** (1986), no. 2, 127–152. MR 827350

[Jao03] David Yen Jao, *Supersingular primes for rational points on modular curves*, ProQuest LLC, Ann Arbor, MI, 2003, Thesis (Ph.D.)–Harvard University. MR 2704678

[KR06] Kevin Keating and David P. Roberts, *Intersection numbers of heegner divisors on shimura curves*, 2006.

[Kur79] Akira Kurihara, *On some examples of equations defining shimura curves and the mumford uniformization*, Journal of the Faculty of Science, the University of Tokyo. Sect. 1 A, Mathematics **25** (1979), no. 3, 277–300.

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