SUPERSPECIAL PRIMES FOR QM ABELIAN SURFACES OVER REAL NUMBER FIELDS

FANGU CHEN
fangu@berkeley.edu

Abstract. Baba and Granath generalize Elkies' theorem on infinitude of supersingular primes for elliptic curves 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.

1. Introduction

1.1. **Background.** Elkies proved in [Elk87] that an elliptic curve defined over a number field of odd degree has infinitely many primes of supersingular reduction, and extended the result in [Elk89] to elliptic curves over any number field with at least one real embedding. This has been generalized to various families of abelian varieties such as abelian surfaces with multiplication by the quaternion algebra of discriminant 6, with field of moduli $\mathbb{Q}$ and which is a Jacobian in characteristic 2 and 3 in [BG08b]. For a detailed discussion of related works, see [Che].

1.2. **The main result.** 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. We expect that similar methods can be applied to the settings in [Jao03, Sad04, LMPT, Che].

A special case of our main theorem is as follows.

Theorem 1.1. *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 (2.3.1) in section 2.3) is defined in [BG08a]. In terms of this coordinate, the assumption at primes $\mathfrak{p}$ above 2 and 3 in Theorem 1.1 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. *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) $v_{\mathfrak{p}}(j_0) \le 0$ 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) $v_{\mathfrak{p}}(j_0) \ge 0$ for $\mathfrak{p}$ above 2, $v_{\mathfrak{p}}(j_0) \le 0$ for $\mathfrak{p}$ above 3, and j_0 has at least one real conjugate in $(0, \infty)$;

(3) $[L : \mathbb{Q}]$ is even, $v_{\mathfrak{p}}(j_0) \ge 0$ 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.

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. For more on the choice of local conditions and Heegner cycles, and for potential further weakenings of these conditions, see Remark 4.1.

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

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

2. Preliminaries

In this section, we recall the setup in [BG08b].

2.1. **The Shimura modular curves.** Let V_Δ be the Shimura curve over $\mathbb{Q}$ associated to Λ. It is the coarse moduli space of isomorphism classes of $[A, \iota]$, where A is a principally polarized abelian surface, and $\iota : \Lambda \hookrightarrow \mathrm{End}(A)$ is an embedding such that the Rosati involution defined by the polarization on $\iota(\Lambda_\Delta)$ is $'$.[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

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

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

$$E_\tau : \Lambda_\tau \times \Lambda_\tau \to \mathbb{Z},$$
$$\left(\iota_\infty(x)\begin{pmatrix}\tau\\1\end{pmatrix}, \iota_\infty(y)\begin{pmatrix}\tau\\1\end{pmatrix}\right) \mapsto \frac{1}{\Delta}\,\mathrm{trd}(\mu x \bar{y})$$

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

There is the natural forgetful map $V_\Delta \to \mathcal{A}_2$ 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^0_Δ 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 $V_6 \to \mathcal{A}_2$ has degree 4 and factors as $V_6 \to V_6/W_6 \simeq E_6 \hookrightarrow \mathcal{A}_2$, where the Atkin-Lehner group $W_6 = N_{B^\times}(\Lambda)/\mathbb{Q}^\times\Lambda^\times = \{1, w_2, w_3, w_6\} \simeq \prod_{p|6}\mathbb{Z}/2\mathbb{Z}$, and w_d is represented by some $\chi_d \in \mathcal{O} \cap N_{B^\times}(\Lambda)$ with $\mathrm{trd}(\chi_d) = 0$, $\mathrm{nrd}(\chi_d) = d$. Moreover, there is a unique $N_{B^\times}(\Lambda)$-conjugacy class of embedding $\mathbb{Z}[\sqrt{-6}] \hookrightarrow \Lambda$, 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 Λ.

[1] The 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.

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

$$\begin{array}{ccc} & & V_6 \\ & & \downarrow{\scriptstyle W_6} \\ E_6^0 & \hookrightarrow & E_6 \\ \downarrow & & \downarrow \\ \mathcal{M}_2 & \hookrightarrow & \mathcal{A}_2 \end{array}$$

2.2. **CM points.** Let K be an imaginary quadratic field and suppose $K \hookrightarrow B$ embeds. Let $\mathcal{O}_D = K \cap \Lambda$ 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 $\mathrm{End}_{\mathrm{QM}}(\mathcal{A}_\tau) \simeq \mathcal{O}_D$.

Remark 2.1. By Eichler, the number of $\Lambda^\times$-conjugacy classes of optimal embeddings $\mathcal{O}_D \hookrightarrow \Lambda$ 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 $\mathcal{O}_D \hookrightarrow \Lambda$ 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'
$-4l$, $l \equiv 13 \bmod 24$	$\equiv 2 \pmod 4$	odd
$-l$, $l \equiv 19 \bmod 24$	odd	odd
$-3l$, $l \equiv 1 \bmod 24$	$\equiv 0 \pmod 4$	even

2.3. **The coordinate functions.** It is shown in [BG08a, 3.6] that there is an isomorphism $j = j_6 : E_6^0 \to \mathbb{P}^1 \backslash \{0, \infty\}$ given by

$$j = \frac{12^{10} J_{10}^2}{(J_2^2 - 24J_4)^5}. \tag{2.3.1}$$

Denote the elements of $E_6(D)$ to be $a_1, \ldots, a_{h'}$, 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 $t : E_6 \to \mathbb{P}^1$, 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	$\mathbb{Z}\left[\sqrt{-1}\right]$	0	1
2	$\mathbb{Z}\left[\sqrt{-6}\right]$	$-\frac{16}{27}$	0

Lemma 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
$-4l$, $l \equiv 13 \bmod 24$		$*$	
$-l$, $l \equiv 19 \bmod 24$			$*$
$-3l$, $l \equiv 1 \bmod 24$	$*$		$*$

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 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 $\sigma_i : \mathbb{A}_{F_i}^\times \to \mathbb{R}/(\ln \varepsilon_i)\mathbb{Z}$ given by

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

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

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 $\sigma = (\sigma_1 \circ \mathrm{Nm}_{F/F_1}, \sigma_3 \circ \mathrm{Nm}_{F/F_3}) : \mathbb{A}_F^\times \to \mathbb{R}/(\ln \varepsilon_1)\mathbb{Z} \times \mathbb{R}/(\ln \varepsilon_3)\mathbb{Z}$, 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 $\tau : \{\text{primes of } F\} \to \mathbb{A}_F^\times$ 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 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 $P_D(x) \bmod l$ 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 $P_D(x)$ modulo l is as follows: (see* [Jao03, 3.4.2] *for a complete list)*

D	*divisor*
$-4l$, $l \equiv 13 \bmod 24$	$(-16/27)$
$-l$, $l \equiv 19 \bmod 24$	$(-16/27)$
$-3l$, $l \equiv 1 \bmod 24$	$\emptyset$

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 $\mathcal{E}_{\mathbb{F}_p} \simeq \mathbb{P}^1_{\mathbb{F}_p}$. 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 3.1. *For $p = 2, 3$, the special fiber $\mathcal{E}_{\mathbb{F}_p} \simeq \mathbb{P}^1_{\mathbb{F}_p}$.*

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 $\mathfrak{O} \otimes \mathbb{Z}_q \simeq \Lambda \otimes \mathbb{Z}_q$ for any prime $q \neq p$. Let

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

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 $E_6 \simeq \mathbb{P}^1_{\mathbb{Q}}$, which has genus 0 and a rational point, it follows that $\mathcal{E}_{\mathbb{F}_2} \simeq \mathbb{P}^1_{\mathbb{F}_2}$ and $\mathcal{E}_{\mathbb{F}_3} \simeq \mathbb{P}^1_{\mathbb{F}_3}$. □

3.1. **Intersection number.**

Definition 3.2. Let R be a Dedekind domain and $\mathcal{X} \to \operatorname{Spec} R$ 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 3.3. Let R be a discrete valuation ring with field of fraction K, maximal ideal $\mathfrak{p}$ and residue field k. Let $x, y \in \mathcal{X}(K)$ be distinct, then x, y extend uniquely to $\underline{x}, \underline{y} \in \mathcal{X}(R)$ by properness of $\mathcal{X} \to \operatorname{Spec} R$, 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 $\mathcal{A} \to \mathcal{X}$, then the complete local ring $\widehat{\mathcal{O}}_{\mathcal{X},z_0}$ is the universal deformation ring for z_0 and

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

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

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

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

$$\langle \mathcal{P}_{-3,\mathcal{E}}, \mathcal{P}_{D,\mathcal{E}} \rangle_{\mathcal{E}} = \frac{2}{4} \cdot \frac{2 \cdot 3}{2\eta(m)} \langle \mathcal{P}_{-3,\mathcal{X}}, \mathcal{P}_{D,\mathcal{X}} \rangle_{\mathcal{X}}, \tag{3.1.1}$$

$$\langle \mathcal{P}_{-4,\mathcal{E}}, \mathcal{P}_{D,\mathcal{E}} \rangle_{\mathcal{E}} = \frac{2}{4} \cdot \frac{2 \cdot 2}{2\eta(m)} \langle \mathcal{P}_{-4,\mathcal{X}}, \mathcal{P}_{D,\mathcal{X}} \rangle_{\mathcal{X}}. \tag{3.1.2}$$

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

Lemma 3.4. *Let D be a fundamental discriminant.*

(1) When $3 \nmid D$, the local intersection of $\mathcal{P}_{-3,\mathcal{E}}$ and $\mathcal{P}_{D,\mathcal{E}}$ at p is 0 if $-3D$ is not a square modulo $24p$.
(2) When $2 \nmid D$, the local intersection of $\mathcal{P}_{-4,\mathcal{E}}$ and $\mathcal{P}_{D,\mathcal{E}}$ 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 (3.1.1),(3.1.2). □

Lemma 3.5. *Let $l \geq 5$ be a prime. For discriminants D of the form in the table, the following reductions hold:*

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

Proof. For $D = -4l$ where $l \equiv 13 \bmod 24$ or $D = -l$ where $l \equiv 19 \bmod 24$, since $-3D$ is not a square modulo 72, the local intersection of $\mathcal{P}_{-3,\mathcal{E}}$ and $\mathcal{P}_{D,\mathcal{E}}$ 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 $l \equiv 1 \bmod 24$, since $12l$ is not a square modulo 72, the local intersection of $\mathcal{P}_{-4,\mathcal{E}}$ and $\mathcal{P}_{-3l,\mathcal{E}}$ 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 $l \equiv 19 \bmod 24$ or $D = -3l$ where $l \equiv 1 \bmod 24$, since $-4D$ is not a square modulo 48, the local intersection of $\mathcal{P}_{-4,\mathcal{E}}$ and $\mathcal{P}_{D,\mathcal{E}}$ 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 $P_{-4l} \bmod 2$ where $l \equiv 13 \bmod 24$ is proved in [BG08b, Lemma 6]. □

4. Proof of main theorem

Let S be a finite set of primes containing primes above $2, 3$ and all primes occuring in j_0 and $27j_0+16$. Write $P = |\operatorname{Nm}_{L/\mathbb{Q}}(P_D(j_0))|, Q = |\operatorname{Nm}_{L/\mathbb{Q}}(27j_0+16)|, s = \operatorname{sgn}(\operatorname{Nm}_{L/\mathbb{Q}}(P_D(j_0))), s' = \operatorname{sgn}(\operatorname{Nm}_{L/\mathbb{Q}}(27j_0+16))$, 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 $p \notin \operatorname{Nm}_{L/\mathbb{Q}}(S)$ 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 $q \in \operatorname{Nm}_{L/\mathbb{Q}}(S) \backslash \{2, 3\}$,
- $P_{-4l}(x)$ 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 3.5,

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

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 $T \subset \mathrm{Hom}(L, \overline{\mathbb{Q}})$ and any prime dividing d lies in $\mathrm{Nm}_{L/\mathbb{Q}}(S)$, then $N, dQ \in \mathbb{N}$ and $(N, 6) = 1$, $(dQ, 2) = 1$. Suppose $l \nmid N$, then

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

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 $p \notin \mathrm{Nm}_{L/\mathbb{Q}}(S)$ and $v_p(\mathrm{Nm}_{L/\mathbb{Q}}(P_D(j_0))) = v_p(N) > 0$. If $l|N$, then since $l \notin \mathrm{Nm}_{L/\mathbb{Q}}(S)$ by construction, we can choose $p = l$.

(2) Choose a prime l satifying the conditions:

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

Let $D = -l$. By Lemma 3.5, Lemma 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 $T \subset \mathrm{Hom}(L, \overline{\mathbb{Q}})$ and any prime dividing d lies in $\mathrm{Nm}_{L/\mathbb{Q}}(S)\backslash\{2\}$, then $N, dQ \in \mathbb{N}$

and $(N,6)=1$. Suppose $l \nmid N$, then

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

Let j_t be the minimal real conjugate of j_0 in $(0,\infty)$ and n $(0 \le n < r)$ 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 $\mathrm{Nm}_{L/\mathbb{Q}}(P_{-l}(j_0))\,\mathrm{Nm}_{L/\mathbb{Q}}(27j_0+16) > 0$. 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 $\mathrm{Nm}_{L/\mathbb{Q}}(P_{-l}(j_0))\,\mathrm{Nm}_{L/\mathbb{Q}}(27j_0+16) < 0$. 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 $p \notin \mathrm{Nm}_{L/\mathbb{Q}}(S)$ and $v_p(\mathrm{Nm}_{L/\mathbb{Q}}(P_D(j_0))) = v_p(N) > 0$. If $l|N$, then since $l \notin \mathrm{Nm}_{L/\mathbb{Q}}(S)$ 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 $q \in \mathrm{Nm}_{L/\mathbb{Q}}(S)\backslash\{2,3\}$,
- the number of real conjugates of j_0 between the two real roots of $P_{-3l}(x)$ is odd, so that

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

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

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

Suppose $l \nmid P$, then

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

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 $p \notin \mathrm{Nm}_{L/\mathbb{Q}}(S)$ and $v_p(\mathrm{Nm}_{L/\mathbb{Q}}(P_D(j_0))) = v_p(N) > 0$. If $l|N$, then since $l \notin \mathrm{Nm}_{L/\mathbb{Q}}(S)$ by construction, we can choose $p = l$.

Remark 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 $\mathcal{P}_{D,\mathcal{E}}$ avoids intersection with one of $\mathcal{P}_{-3,\mathcal{E}}$ and $\mathcal{P}_{-4,\mathcal{E}}$ by Lemma 3.4. The local conditions on j_0 are determined so that it avoids intersection with the 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.

References

[BC91] J.-F. Boutot and H. Carayol, *Uniformisation p-adique des courbes de Shimura: les théorèmes de čerednik et de Drinfeld*, 1991, pp. 7, 45–158. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). MR1141456

[BG08a] Srinath Baba and Hå kan Granath, *Genus 2 curves with quaternionic multiplication*, Canad. J. Math. **60** (2008), no. 4, 734–757. MR2423455

[BG08b] ———, *Primes of superspecial reduction for QM abelian surfaces*, Bull. Lond. Math. Soc. **40** (2008), no. 2, 311–318. MR2414789

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

[Che] Fangu Chen, *Infinitely many supersingular primes for some mumford's abelian fourfolds.*

[Cla03] Pete L. Clark, *Rational points on atkin -lehner quotients of shimura curves*, Ph.D. Thesis, 2003 (English). Copyright - Database copyright ProQuest LLC; ProQuest does not claim copyright in the individual underlying works; Last updated - 2023-03-04.

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

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

[Elk98] ———, *Shimura curve computations*, Algorithmic number theory (Portland, OR, 1998), 1998, pp. 1–47. MR1726059

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

[KR08] Kevin Keating and David P. Roberts, *Intersection numbers of Heegner divisors on Shimura curves*, Pure Appl. Math. Q. **4** (2008), no. 4, 1165–1204. MR2441697

[Kur79] Akira Kurihara, *On some examples of equations defining Shimura curves and the Mumford uniformization*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **25** (1979), no. 3, 277–300. MR523989

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

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

[Mum72] David Mumford, *An analytic construction of degenerating curves over complete local rings*, Compositio Math. **24** (1972), 129–174. MR352105

[Rib89] Kenneth A. Ribet, *Bimodules and abelian surfaces*, Algebraic number theory, 1989, pp. 359–407. MR1097624

[Rot04] Victor Rotger, *Modular Shimura varieties and forgetful maps*, Trans. Amer. Math. Soc. **356** (2004), no. 4, 1535–1550. MR2034317

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