Primes of Superspecial Reduction for QM Abelian Surfaces

Srinath Baba, Håkan Granath*

Abstract

We show that any abelian surface with multiplication by the quaternion $\mathbb{Q}$-algebra of discriminant 6, with field of moduli $\mathbb{Q}$ and which is a Jacobian in characteristic 2 and 3, has infinitely many primes of superspecial reduction. This is done by examining CM points in characteristic 0 and p and the values of a certain j-function on the associated moduli space at these points.

Key words: abelian surface, quaternionic multiplication, superspecial reduction
2000 Mathematics Subject Classification: 11G18, 14G35, 11G25

An abelian variety A over an algebraically closed field of characteristic $p > 0$ is supersingular if it is isogenous to a product of supersingular elliptic curves. If A is isomorphic to such a product, then A is said to be superspecial. Elkies showed in [4] that if $A/\mathbb{Q}$ is an elliptic curve, then it has infinitely many supersingular primes. His proof uses properties of the classical j-invariant of elliptic curves and the reduction theory of elliptic curves with complex multiplication to characteristic p. Similar techniques have since been used by M.L. Brown to prove the infinitude of supersingular primes for certain Drinfeld modules, and more recently by D. Jao to points on $X_0(N)$.

In the case of A being an abelian surface, Sadykov has shown in [14] that certain abelian surfaces with quaternionic multiplication by the quaternion algebras of discriminant 22 and 33 have infinitely many supersingular primes. In this paper, we establish the corresponding result for the Shimura curve of discriminant 6. Using properties of the j-invariant constructed in [2], we apply the idea of proof of Elkies to show the following.

Theorem 1. *Let C be a genus 2 curve whose Jacobian has multiplication by the maximal quaternion order with discriminant 6, has field of moduli equal to $\mathbb{Q}$ and has potentially smooth stable reduction at 2 and 3. Then its Jacobian has superspecial reduction at infinitely many primes.*

---

*The second named author was supported by a Marie Curie Intra-European Fellowship under the Sixth Framework Programme of the European Commission (MEIF-CT-2004-501793).

1 Preliminaries

For any square free integer $\Delta > 0$, let B_Δ denote the quaternion algebra over $\mathbb{Q}$ ramified at the places dividing Δ. When Δ has a positive and even number of prime divisors, then B_Δ is an indefinite skew field. We fix such a Δ. Let $x \mapsto x^*$ be the canonical involution on B_Δ, and let Λ_Δ be a maximal order in B_Δ. Fix an element $\mu \in \Lambda_\Delta$ with $\mu^2 = -\Delta$. It determines a positive anti-involution $a \mapsto a'$ on B_Δ by $a' = \mu^{-1}a^*\mu$, i.e., the quadratic form $a \mapsto \mathrm{tr}(a'a)$ is positive definite. We call the pair (Λ_Δ, μ) a principally polarized maximal order in B_Δ. Given (Λ_Δ, μ), let V_Δ denote the Shimura curve which is the moduli space of triples $[A, \rho, \iota]$ where A is an abelian surface, ρ is the Rosati involution corresponding to a principal polarization on A, and $\iota : \Lambda_\Delta \to \mathrm{End}(A)$ is an embedding such that the Rosati involution defined by ρ on $\iota(\Lambda_\Delta)$ is $'$. Shimura showed in [15] that V_Δ is defined over $\mathbb{Q}$. For any positive integer $d \mid \Delta$, the Atkin-Lehner involution w_d on V_Δ is defined by $w_d([A, \rho, \iota]) = [A, \gamma_d^*\rho, \gamma_d^{-1}\iota\gamma_d]$, where γ_d is an element of norm d in B_Δ. Let $W = W_\Delta$ denote the Atkin-Lehner group acting on V_Δ.

Let A be an abelian surface with QM by $\Lambda = \Lambda_\Delta$. Denote the commutator of the image of Λ in $\mathrm{End}(A)$ by $\mathrm{End}_{\mathrm{QM}}(A)$. In characteristic 0, $\mathrm{End}_{\mathrm{QM}}(A)$ is either $\mathbb{Z}$ or a complex quadratic order $\mathcal{O}_D$. In characteristic $p > 0$, every QM abelian surface is either ordinary or supersingular [3, Proposition 68]. In the ordinary case, $\mathrm{End}_{\mathrm{QM}}(A)$ is a complex order. In the supersingular case, $\mathrm{End}_{\mathrm{QM}}(A)$ is an order in the quaternion algebra $B_{p\Delta}$ (resp. $B_{\Delta/p}$) if $p \nmid \Delta$ (resp. $p \mid \Delta$). See [3], Corollary 69.

Let $\mathcal{O}_D$ be the complex quadratic order with discriminant D. We say that A has CM by $\mathcal{O}_D$ if there exists an optimal embedding of $\mathcal{O}_D$ into $\mathrm{End}_{\mathrm{QM}}(A)$. An abelian surface is clearly supersingular if it has CM by at least 2 quadratic orders, or equivalently if it has CM by an order $\mathcal{O}_D$ in a field in which p does not split.

Consider a QM abelian surface A over $\mathbb{C}$ with CM by $\mathcal{O}_D$. The corresponding lattice in $\mathbb{C}^2$ is a natural $\mathcal{O}_D$ module, hence it is of the form $\mathfrak{a}_1 l_1 + \mathfrak{a}_2 l_2$, where $\mathfrak{a}_i$ is an $\mathcal{O}_D$ ideal and $l_i \in \mathbb{C}^2$, for $i = 1, 2$. It follows that the A is the product of two CM elliptic curves (as a complex torus). In particular, the endomorphism ring of A over $\mathbb{C}$ contains two orthogonal idempotents. Consider now any QM abelian surface A in characteristic 0 with CM. It is, together with its endomorphism ring, defined over some number field k. Since, by the above, $\mathrm{End}(A)$ contains orthogonal idempotents, we observe that A/k is *isomorphic* to a product of CM elliptic curves (as unpolarized varieties).

Supersingular abelian surfaces with QM are described in detail in Ribet's paper [13]. If $p \mid \Delta$, then every abelian surface with QM by B_Δ is supersingular [13, Lemma 4.1], but not necessarily superspecial. On the other hand, if $p \nmid \Delta$, every QM abelian surface over $\bar{\mathbb{F}}_p$ is either ordinary or superspecial ([13, p. 23], and [3]).

Let now D be the fundamental discriminant of an imaginary quadratic field. Let $K = K_D = \mathbb{Q}(\sqrt{D})$, with maximal order $\mathcal{O} = \mathcal{O}_D$ and let $H = H_D$ denote the Hilbert class field and h the class number of K. Let W' denote the subgroup of W generated by elements w_p, where $p \mid \Delta$ is a rational prime inert in K. Similarly, let W'' denote the subgroup of W generated by elements w_p, where $p \mid \Delta$ is a prime ramified in K, so $W \cong W' \times W''$. We will use the following facts, all of which are proved in [9]. If $a \in V_\Delta$ is a point such that the corresponding abelian surface has CM by $\mathcal{O}$, then a is defined over the field H. There is a homomorphism $W'' \to \mathrm{Gal}(H/K)$, given by $w_d \mapsto \sigma_d$ where $\sigma_d = (\mathfrak{a}, H/K) \in \mathrm{Gal}(H/K)$ is defined by the class of an ideal $\mathfrak{a}$ of norm d in K, such that $w_d(a) = \sigma_d(a)$. The natural action of the group $W' \times \mathrm{Gal}(H/K)$ on the points on V_Δ with CM by $\mathcal{O}$ is effective and transitive. Hence the number of $\mathcal{O}$ CM points on V_Δ is $h\#(W')$. Let $H' = \{x \in H \mid x^\sigma = x \text{ for all } \sigma \in W''\}$, and let h' be the degree of the extension H'/K, i.e., $h' = h/\#(W'')$. Consider the set of points on the quotient curve V_Δ/W which are images of $\mathcal{O}$ CM on V_Δ. The number of elements in this set, counted with appropriate multiplicities, is h'.

We let $B(a,b)$, where $a, b \in \mathbb{Q}$ and $ab \neq 0$, denote the quaternion algebra $\mathbb{Q}[\mu,\nu]$, where $\mu^2 = a$, $\nu^2 = b$ and $\mu\nu + \nu\mu = 0$. Let τ denote the action of complex conjugation on V_Δ. Jordan [9] used Shimura reciprocity to calculate the action of τ on CM points in the following sense. If a is an $\mathcal{O}$ CM point, then so is $\tau(a)$, and hence $\tau(a) = w\sigma a$ for a unique pair $(w,\sigma) \in W' \times \mathrm{Gal}(H/K)$. If a is replaced with some other $\mathcal{O}$ CM point a', then (w,σ) is replaced with $(w, \sigma\beta^2)$ for some $\beta \in G = \mathrm{Gal}(H/K)$. Hence, complex conjugation defines a well defined class $[\tau] := (w,\sigma) \in W' \times G/G^2$. Theorem 3.1.3 in [9] states that $[\tau] = (w_d, (\mathfrak{a}, H/K))$ for an ideal $\mathfrak{a}$ of $\mathcal{O}$ and $d \mid \Delta$ if and only if $B_\Delta \cong B(D, d\,\mathrm{nr}(\mathfrak{a}))$.

2 The moduli space E_6

In the case $\Delta = 6$, the group of Atkin-Lehner involutions on the curve V_6 is $W = \{1, w_2, w_3, w_6\}$, and we define $E_6 = V_6/W$. E_6 is the moduli space of principally polarized abelian surfaces with potential quaternionic multiplication by Λ_6. The curve E_6 contains an open subvariety E_6^0 which is the moduli space of genus 2 curves whose Jacobians lie on E_6.

A point in the moduli space $\mathcal{A}_2$ of genus 2 curves is determined by its Igusa invariants $[J_2, J_4, J_6, J_{10}]$, which should be considered as a point in the weighted projective space $\mathbb{P}(2,4,6,10)$, see [8]. In [2] we showed that there is an isomorphism $j = j_6 : E_6^0 \to \mathbb{A}^1 \setminus \{0\}$ given by

$$j = \frac{12^{10} J_{10}^2}{(J_2^2 - 24J_4)^5}, \tag{1}$$

and that this map extends to an isomorphism of E_6 with $\mathbb{P}^1_{\mathbb{Q}}$ as varieties defined over $\mathbb{Q}$. The inverse of the map j is given as follows: For any j, the corresponding genus 2 curve C, which is defined over some field k, has Igusa invariants

$$\begin{aligned} J_2 &= 12(j+1)s, & J_4 &= 6(j^2+j+1)s^2, \\ J_6 &= 4(j^3-2j^2+1)s^3 & J_{10} &= j^3 s^5 \end{aligned} \tag{2}$$

for some $s \in k$.

As varieties over $\mathbb{Q}$, it is well known [12] that the curve V_6 can be identified with the conic $\{x^2 + 3y^2 + z^2 = 0\} \subset \mathbb{P}^2_{\mathbb{Q}}$. This identification was made explicit in [2]. Composing the quotient map $V_6 \to E_6$ with j, we get a map $V_6 \to \mathbb{P}^1_{\mathbb{Q}}$ which, in terms of these coordinates, is given by

$$j = \frac{16y^2}{9x^2}. \tag{3}$$

In particular, the j-value of any $\mathcal{O}_D$ CM point on E_6 is always a square in H.

The following result strengthens Proposition 32 in [2].

Proposition 2. *Let C/k be a genus 2 curve corresponding to a point on E_6^0, and $\mathfrak{p}$ a prime in k. Then C has potentially smooth stable reduction at $\mathfrak{p}$ if and only if $v_{\mathfrak{p}}(j(C)) = 0$. In the case $v_{\mathfrak{p}}(j(C)) \neq 0$, the stable reduction of C at $\mathfrak{p}$ is a union of two smooth elliptic curves meeting transversally in one point. Furthermore, the elliptic j-invariants of these two components are* 1728 *if $v_{\mathfrak{p}}(j(C)) < 0$ and* 0 *otherwise.*

Proof. This is a direct application of Théorème 1 in [11] using the expressions of the Igusa invariants given by (2). □

In other words, the primes occurring in j are exactly the places where the genus 2 curve does not have potentially smooth stable reduction.

We use the presentation $B_6 = B(3, -1) = \mathbb{Q}[\mu, \nu]$, and choose the maximal order Λ_6 given by $\Lambda_6 = \mathbb{Z}[\mu, \nu, (1 + \mu + \nu + \mu\nu)/2]$. We now want to describe the real locus of E_6. Consider the elements $\gamma_{-4} = \nu$, $\gamma'_{-4} = -2\nu + \mu\nu$, $\gamma_{-3} = (1 + \mu - 3\nu + \mu\nu)/2$ and $\gamma_{-24} = 3\nu - \mu\nu$ of Λ_6. From the description of the upper half plane uniformization given in [1], one can choose a fundamental domain bounded by the hyperbolic triangle with vertices at the fixed points of γ_{-4}, γ_{-3} and γ'_{-4} respectively. The real line for the function $j = j_6$ is given by the following: The (open) hyperbolic line segment from the fixed point of γ_{-3} to the fixed point of γ_{-24} maps under j to the interval $(-\infty, -16/27)$. Similarly the line segments determined by γ_{-24} and γ_{-4} yields the interval $(-16/27, 0)$, and γ_{-4} and γ_{-3} corresponds to the interval $(0, \infty)$.

Let D be the fundamental discriminant of a complex quadratic order $\mathcal{O}_D$ embedding into B_6, i.e., $D \not\equiv 1 \pmod 8$ and $D \not\equiv 1 \pmod 3$. Let $E_6(D)$ denote the set of points with CM by $\mathcal{O}_D$. The elements of $E_6(D)$ are denoted

$$a_1, a_2, \ldots, a_{h'} \in E_6(D).$$

Define the polynomial

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

for $D \neq -3$, and let $Q_{-3}(x) = 1$. Since $\mathrm{Gal}(H/K)$ acts on the roots of $Q_D(x)$, it is clear that $Q_D(x) \in K[x]$. Since also complex conjugation preserves the set of points with CM by $\mathcal{O}_D$, we can conclude that $Q_D(x) \in \mathbb{Q}[x]$. Define $P_D(x)$ to be the integral minimal polynomial of the j-invariants of the points in $E_6(D)$, so

$$P_D(x) = b_{h'} Q_D(x),$$

where $b_{h'} > 0$ is the smallest integer such that $b_{h'} Q_D(x)$ is integral. We write

$$P_D(x) = b_{h'} x^{h'} + \cdots + b_1 x + b_0.$$

Recall that for any $w_d \in W''$ the corresponding Galois element σ_d acts as w_d on the $\mathcal{O}$ CM points of V_6, and hence by definition σ_d acts trivially on the roots of $P_D(x)$. It is therefore clear that H' is a splitting field of the polynomial $P_D(x)$. We now prove some general arithmetic properties of the coefficients of the polynomials $P_D(x)$.

Lemma 3. *$P_D(x) \equiv x^n \pmod 2$ for some n, and $P_D(x) \equiv \pm x^m \pmod 3$ for some m.*

Proof. Let $p = 2$ or 3 and $\mathfrak{p}$ a prime ideal in $\mathcal{O}_H$ above p. Since, in characteristic 0, all $\mathcal{O}_D$ CM surfaces are products of elliptic curves, their reductions modulo $\mathfrak{p}$ are superspecial. It is a known fact, that in characteristic 2 and 3 there are no genus 2 curves whose Jacobians are superspecial [5, Proposition 7.5]. Hence, by Proposition 2, $v_{\mathfrak{p}}(j_i) \neq 0$ for every root j_i of $P_D(x)$. It follows that $P_D(x)$ reduces to a single monomial modulo $\mathfrak{p}$. $\square$

It follows from Proposition 2 and Lemma 3, that any genus 2 curve in characteristic 0 with potentially smooth stable reduction at 2 or 3 has a simple Jacobian.

Lemma 4. *Let p be a rational prime. The following hold: (a) If p occurs with odd multiplicity in b_0 or $b_{h'}$, then p is ramified in K. (b) Assume $p > 3$. If $p \mid b_0$, then $\left(\frac{-1}{p}\right) = -1$, and if $p \mid b_{h'}$, then $\left(\frac{-3}{p}\right) = -1$.*

Proof. Let $x_i = j(a_i)$ for $i = 1, \ldots, h'$. We have $\prod x_i = \pm b_0/b_{h'}$. Since, by (3), x_1 is a square in H, and the field extension H/H' is unramified, we get $x_1 \mathcal{O}_{H'} = \mathfrak{b}^2$ for some fractional ideal $\mathfrak{b}$ in H'. Write $\mathfrak{b} = \mathfrak{b}_0/\mathfrak{b}_{h'}$, with $\mathfrak{b}_0$ and $\mathfrak{b}_{h'}$ relatively prime integral ideals in $\mathcal{O}_{H'}$. We have $b_0 = \pm \operatorname{nr}_{H'/K}(\mathfrak{b}_0^2)$, so $b_0^2 = \operatorname{nr}_{H'/\mathbb{Q}}(\mathfrak{b}_0^2)$. Hence $\mathfrak{a}_0 = \operatorname{nr}_{H'/K}(\mathfrak{b}_0)$ is an ideal in $\mathcal{O}_K$ such that

$$b_0 = \pm \operatorname{nr}_{K/\mathbb{Q}}(\mathfrak{a}_0). \tag{4}$$

Similarly,

$$b_{h'} = \operatorname{nr}_{K/\mathbb{Q}}(\mathfrak{a}_{h'}) \tag{5}$$

for some ideal $\mathfrak{a}_{h'} \subseteq \mathcal{O}_K$.

To prove (a), assume that p divides b_0 (resp. $b_{h'}$). Then some $\mathcal{O}_D$ CM abelian surface must be supersingular at some prime $\mathfrak{p}$ above p, so p must be ramified or inert in K. But if p is inert, then it must occur with even multiplicity, by (4) (resp. (5)).

(b) Assume p divides the constant term b_0. Then there exists a $\mathcal{O}_D$ CM surface A and a prime $\mathfrak{p}$ above p such that the reduction $\bar{A}$ of A at $\mathfrak{p}$ is isomorphic to the $\mathcal{O}_{-4}$ CM abelian surface in characteristic p, i.e., $\bar{A} \cong E_0 \times E_0$, where E_0 is the elliptic curve with modular j-invariant 0. But $\bar{A}$ has also $\mathcal{O}_D$ CM, so E_0 must be supersingular at p, and hence $\left(\frac{-1}{p}\right) = -1$. The case of p dividing the leading coefficient $b_{h'}$ is analogous. $\square$

3 The construction of supersingular primes

To prove Theorem 1, we will use the basic strategy of Elkies in [4]. In particular, we will give an algorithm which, given any finite set of superspecial primes, produces a new one. To achieve this, we will consider the family of CM points having discriminants of the particular type $D = -4l$, where l is a prime such that $l \equiv 13 \pmod{24}$. For these discriminants D, we need more detailed information about the polynomials $P_D(x)$, in particular about its real roots and about the reductions of $P_D(x)$ modulo various integers.

From now on, we only consider D of the form $D = -4l$ as above. For the convenience of the reader, we give the first few polynomials $P_D(x)$:

$$\begin{aligned}
P_{-4\cdot 13}(x) &= 5^6 x + 2^6 3^4 \\
P_{-4\cdot 37}(x) &= 5^6 17^6 x + 2^6 3^4 7^4 11^4 \\
P_{-4\cdot 61}(x) &= 17^6 29^6 x^3 + 94525046763039936 x^2 \\
&\quad + 786711750553350144 x + 2^{18} 3^{12} 19^4 \\
P_{-4\cdot 109}(x) &= 17^6 41^6 53^6 x^3 + 10968775518096466071945031872 x^2 \\
&\quad + 18314519349761523526089682944 x + 2^{18} 3^{12} 7^{12} 31^4.
\end{aligned}$$

In this case $W' = \{1, w_3\}$, so the number of $\mathcal{O}_{-4l}$ CM points on E_6 is $h' = h(\mathbb{Q}(\sqrt{-l}))/2$. This number is odd [6, Theorem 41]. Let σ_2 denote the element of $G = \mathrm{Gal}(H/K)$ which induces w_2 on the points on V_6 with CM by $\mathcal{O}_K$. The roots of $P_{-4l}(x)$ lie in H' which is the quadratic subextension of H fixed by σ_2. The subgroup G^2 of G, which consists of the elements of G of odd order, cuts out the unique quadratic unramified extension L of K. It is easy to see that $L = K(\sqrt{-1})$, and since $G = W'G^2$ we have $H = H'L$, so

$$H = H'(\sqrt{-1}). \tag{6}$$

Since $P_D(x)$ has odd degree, it has at least one real root. Assume that $j(a_1)$ is real. Let $\hat{a}_1$ be a point on V_6 above a_1. To apply the results in section 1 describing the action of complex conjugation τ in this case, we note that $B_6 \cong B(-4l, 3)$. We conclude that $\tau(\hat{a}_1) = w_3(\hat{a}_1)$. The group G^2 acts effectively and transitively on $E_6(D)$, so any $a \in E_6(D)$ can be written as $a = \sigma(a_1)$ for some $\sigma \in G^2$. Hence $\tau(a) = \sigma^{-2} a$, and it follows that a_1 is the only real point.

Lemma 5. *The polynomial $P_{-4l}(x)$ has exactly one real root $j(a_1)$, and it satisfies $-16/27 < j(a_1) < 0$. Furthermore, let m and n be positive integers* *with $(m, 6n) = 1$, and $\epsilon > 0$ a real number. Then there exists a prime l such that $l \equiv 13 \pmod{24}$, $l \equiv n \pmod{m}$ and $-16/27 < j(a_1) < -16/27 + \epsilon$.*

Proof. In order to locate the real zero $j(a_1)$ of $P_{-4l}(x)$, we are led by our description of the real locus of E_6 to compute the quadratic forms

$$\begin{aligned} \mathrm{nr}(b\gamma_{-3} + c\gamma_{-24}) &= 3(b^2 + 4bc + 2c^2), \\ \mathrm{nr}(b\gamma_{-24} + c\gamma_{-4}) &= 6b^2 + 6bc + c^2, \\ \mathrm{nr}(b\gamma_{-4} + c\gamma_{-3}) &= b^2 + 6bc + 3c^2, \end{aligned}$$

where $b, c > 0$ are integers. It is clear that only the second form represents primes l with $l \equiv 13 \pmod{24}$, hence $-16/27 < j(a_1) < 0$.

For the second part, it is therefore enough to show that for any $\delta > 0$ there exists integers $b, c > 0$ and a prime l such that $l = 6b^2 + 6bc + c^2$, $l \equiv 13 \pmod{24}$, $l \equiv n \pmod{m}$ and $c/b < \delta$. This is a direct application of Hecke's classical results on the distribution of primes represented by forms. See [7], in particular formula (52). ◻

Lemma 6. *The following reductions hold:*

(a) $P_{-4l}(x) \equiv x^{h'} \pmod{4}$.

(b) $P_{-4l}(x) \equiv (27x + 16)S(x)^2 \pmod{l}$, for some $S(x) \in \mathbb{Z}[x]$,

Proof. (a) Take any prime $\mathfrak{p}$ above 2 in H. We need to show that $v_{\mathfrak{p}}(j(a_i)) > v_{\mathfrak{p}}(4) = 4$ for every i. Now $j(a_i) = 16y^2/(9x^2)$ where

$$x^2 + 3y^2 + z^2 = 0 \tag{7}$$

and $x, y, z \in H_{\mathfrak{p}}$. Identify the local field $H_{\mathfrak{p}}$ with $\mathbb{Q}_2[\sqrt{-l}]$. We can assume that $x, y, z \in \mathbb{Z}_2[\sqrt{-l}]$ and that they are are coprime, i.e., not all divisible by $\pi = \sqrt{-l} - 1$. Assume $x^2 \in (4\pi) = (\pi^5)$. Then π^3 divides x, and we get a contradiction by considering (7) modulo π^6. Hence x^2 is at most divisible by 4 and we are done.

(b) By definition, $P_{-4l}(x) = b_{h'} \prod (x - j(a_i))$. By the above, we know that all the $j(a_i)$ lie in H', and that $P_{-4l}(x)$ has exactly one real root $j(a_1)$. Since h' is odd, there is a degree 1 prime ideal $\mathfrak{p}'$ of residue characteristic l in H' which is fixed by complex conjugation. Thus $\tau(a_i) \equiv a_i \pmod{\mathfrak{p}'}$ for all i.

Let $\hat{a}_1$ be a point on V_6 that lies above a_1. As before $\tau(\hat{a}_1) = w_3(\hat{a}_1)$, so $\sigma_2(\tau(\hat{a}_1)) = w_6(\hat{a}_1)$. By (6) and the fact that the primes above $\mathfrak{p}'$ have have prime residue fields, it follows that they are switched by complex conjugation τ. Hence there is a prime $\mathfrak{p}$ in H above $\mathfrak{p}'$ which is fixed by $\sigma_2\tau$ (in fact, both primes above $\mathfrak{p}'$ are), so $\sigma_2(\tau(\hat{a}_1)) \equiv \hat{a}_1 \pmod{\mathfrak{p}}$. Thus, $\hat{a}_1$ reduces mod $\mathfrak{p}$ to a fixed point of w_6, so $j(a_1) \cong -16/27 \pmod{\mathfrak{p}}$.

Thus $P_{-4l}(x) \equiv b_{h'}(x + 16/27)S(x)^2 \pmod{\mathfrak{p}}$. Since $\mathfrak{p}$ is a degree 1 prime, we obtain (b) up to a constant factor. We will be done if we can show that the highest coefficient $b_{h'}$ of $P_{-4l}(x)$ is a square modulo l. But by part (a) of Lemma 4 the only possible odd prime powers in $b_{h'}$ are 2 and l. By part (b) of Lemma 4 we have $l \nmid b_{h'}$, and that $2 \nmid b_{h'}$ follows from part (a) of this lemma. ◻

Lemma 7. *Let $j_0 \in \mathbb{Q}$ be such that $v_2(j_0) = v_3(j_0) = 0$. Suppose that $\left(\frac{-4l}{q}\right) = 1$ for all primes q such that $v_q(j_0)$ or $v_q(27j_0+16)$ is non-zero, and that $(27j_0+16)P_{-4l}(j_0) > 0$. If $l \nmid P_{-4l}(j_0)$, then*

$$\left(\frac{-4l}{|P_{-4l}(j_0)|}\right) = -1.$$

Proof. Let $P = |P_{-4l}(j_0)|$, $Q = |(27j_0+16)|$, and $s = \operatorname{sign}(P_{-4l}(j_0))$. Assume that $l \nmid P$. Note, by Lemma 3, that $v_2(P) = v_3(P) = 0$. By the condition on the primes occurring in Q, we get $\left(\frac{Q}{l}\right) = \left(\frac{-1}{Q}\right)$. By the reduction of $P_{-4l}(x)$ in Lemma 6 we have $\left(\frac{P}{l}\right) = \left(\frac{Q}{l}\right)$. Hence

$$\begin{aligned}\left(\frac{-4l}{P}\right) = \left(\frac{-1}{P}\right)\left(\frac{l}{P}\right) = \left(\frac{-1}{P}\right)\left(\frac{P}{l}\right) = \left(\frac{-1}{P}\right)\left(\frac{Q}{l}\right) = \\ = \left(\frac{-1}{P}\right)\left(\frac{-1}{Q}\right) = \left(\frac{-1}{sj_0^{h'}}\right)\left(\frac{-1}{s3j_0}\right) = -1.\end{aligned}$$

□

Proof of Theorem 1. Let $j_0 = j(C) \in \mathbb{Q}$. Since we assume potentially smooth stable reduction at 2 and 3, we have $v_2(j_0) = v_3(j_0) = 0$ by Proposition 2. Let S be a finite set of primes containing 2, 3 and all primes occurring in j_0 and $27j_0+16$. By Lemma 5, we can choose a prime l satisfying the conditions $l \equiv 13 \pmod{24}$, $\left(\frac{-4l}{q}\right) = 1$ for every prime $q \in S \setminus \{2,3\}$, and $(27j_0+16)P_{-4l}(j_0) > 0$. Assume first that $l \nmid P_{-4l}(j_0)$. Then, by Lemma 7, $\left(\frac{-4l}{|P_{-4l}(j_0)|}\right) = -1$. This means that there is a prime $p \mid P_{-4l}(j_0)$ with $\left(\frac{-4l}{p}\right) = -1$. Since $P_{-4l}(j_0)$ is a unit at 2 and 3, this prime p cannot be in S. So p must be a supersingular, and hence superspecial, prime for C outside of S. If $l \mid P_{-4l}(j_0)$, then similarly $p = l$ is a superspecial prime outside of S. □

Example. Consider the curve C with $j = -1$. This curve can not be defined over $\mathbb{Q}$. In fact, the Mestre obstruction for this is given by the algebra $B(-6j, -2(27j+16)) \cong B_{22}$ (cf. [2]), so it is defined for instance over $\mathbb{Q}(\sqrt{6})$. One model is given by

$$\begin{aligned}y^2 = 4(x^6 - 33x^5 - 462x^4 + 484x^3 - 10164x^2 - 15972x + 10648) \\ +3\sqrt{6}(x^6 + 198x^4 - 435x^2 - 10648).\end{aligned}$$

We get $P_{-4\cdot 13}(-1) = -53\cdot 197$, and in fact $\left(\frac{-4\cdot 13}{197}\right) = -1$, so 197 is a superspecial prime. Similarly the algorithm is applicable for the discriminant $D = -4l$ for $l = 61$ and 109, which yields the superspecial primes 281 and 673 respectively. In fact, a Hasse-Witt matrix computation on this example shows that the 6 first superspecial primes for this curve are 29, 83, 197, 281, 673 and 1009.

References

[1] M. Alsina, P. Bayer, *Quaternion orders, quadratic forms, and Shimura curves,* CRM Monograph Series 22, American Mathematical Society (2004)

[2] S. Baba, H. Granath, *Genus 2 curves with quaternionic multiplication,* Canadian Journal of Mathematics (to appear), available as preprint 18, 2005, at http://www.mpim-bonn.mpg.de/Research/MPIM+Preprint+Series/

[3] P. Clark, *Rational points on Atkin-Lehner quotients of Shimura curves,* Ph.D. Thesis, Harvard University (2003)

[4] N.D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$*,* Invent. Math. 89 (1987), 561–567

[5] T. Ekedahl, *On Supersingular Curves and Abelian Varieties,* Math. Scand. 60 (1987), 151–178

[6] A. Fröhlich, M. J. Taylor, *Algebraic number theory,* Cambridge University Press (1991)

[7] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen,* Math. Z. 6, no. 1–2 (1920), 11–51

[8] J.-I. Igusa, *Arithmetic Variety of Moduli for Genus Two,* Annals of Mathematics, vol. 72, no. 3 (1960), p. 612–649

[9] B.W. Jordan, *On the arithmetic of Shimura curves,* Ph.D. Thesis, Harvard University (1981)

[10] B.W. Jordan, *Points on Shimura curves rational over number fields,* J. Reine Angew. Math. 371 (1986), 92–114

[11] Q. Liu, *Courbes stable de genre 2 et leur schéma de modules,* Math. Ann. 295 (1993), 201–222

[12] A. 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

[13] K. Ribet, *Bimodules and Abelian Surfaces,* Adv. Stud. Pure Math. 17 (1989), 359–407

[14] M. Sadykov, *Two results in the arithmetic of Shimura curves,* Ph.D. Thesis, Columbia University (2004)

[15] G. Shimura, *On canonical models of arithmetic quotients of bounded symmetric domains,* Ann. of Math. 91 (1970), 144–222

Srinath Baba: Department of Mathematics and Statistics, Concordia University, 1455 de Maisonneuve Blvd. West, Montréal, Quebec, Canada H3G 1M8
E-mail address: sbaba@math.mcgill.ca

Håkan Granath: Max-Planck-Institut für Mathematik, Vivatsgasse 7, DE-53111 Bonn, Germany
E-mail address: granath@mpim-bonn.mpg.de