Canad. J. Math. Vol. **66** (5), 2014 pp. 1167–1200
http://dx.doi.org/10.4153/CJM-2013-020-3
© Canadian Mathematical Society 2013

Galois Representations Over Fields of Moduli and Rational Points on Shimura Curves

Victor Rotger and Carlos de Vera-Piquero

Abstract. The purpose of this note is to introduce a method for proving the non-existence of rational points on a coarse moduli space X of abelian varieties over a given number field K in cases where the moduli problem is not fine and points in $X(K)$ may not be represented by an abelian variety (with additional structure) admitting a model over the field K. This is typically the case when the abelian varieties that are being classified have even dimension. The main idea, inspired by the work of Ellenberg and Skinner on the modularity of $\mathbb{Q}$-curves, is that one may still attach a Galois representation of $\mathrm{Gal}(\overline{K}/K)$ with values in the quotient group $\mathrm{GL}(T_\ell(A))/\mathrm{Aut}(A)$ to a point $P = [A] \in X(K)$ represented by an abelian variety $A/\overline{K}$, provided $\mathrm{Aut}(A)$ lies in the centre of $\mathrm{GL}(T_\ell(A))$. We exemplify our method in the cases where X is a Shimura curve over an imaginary quadratic field or an Atkin–Lehner quotient over $\mathbb{Q}$.

1 Introduction

Let B_D be an indefinite rational quaternion algebra of discriminant $D > 1$ and fix a maximal order $\mathcal{O}_D$ in B_D, which is unique up to conjugation. Let $X_D/\mathbb{Q}$ denote the Shimura curve arising as the coarse moduli scheme classifying isomorphism classes of abelian surfaces $(A, \iota\colon \mathcal{O}_D \hookrightarrow \mathrm{End}(A))$ with multiplication by $\mathcal{O}_D$ (see [Shi63, Shi67]).

The main theme of this note is the study of the set of points on X_D and on their Atkin–Lehner quotients, rational over a given number field. A theorem of Shimura states that X_D has no real points (*cf.* [Shi75]), so a fortiori $X_D(\mathbb{Q}) = \varnothing$, and the simplest number fields to look at are the imaginary quadratic extensions of $\mathbb{Q}$.

If k is a field of characteristic zero, a k-rational point P on X_D corresponds to the isomorphism class of a pair $(A, \iota)/\overline{k}$ that is isomorphic to all its $\mathrm{Gal}(\overline{k}/k)$-conjugates. However, the pair $(A, \iota)/\overline{k}$ does not necessarily admit a model rational over k, because the moduli problem associated with X_D is not fine. B. Jordan [Jor86, Theorem 1.1] studied this issue and proved that (A, ι) admits a model over k if and only if k splits B_D.

Assuming this condition for an imaginary quadratic field $K/\mathbb{Q}$, in [Jor86], Jordan gave sufficient conditions for the emptiness of $X_D(K)$ or, in other words, for the non-

Received by the editors February 26, 2013; revised March 15, 2013.
Published electronically July 4, 2013.
During the preparation of this work, the authors received financial support from MTM2009-13060-C02-01. The second author was also financially supported by the *Comissionat per a Universitats i Recerca del DIUE de la Generalitat de Catalunya* and the *European Social Fund*.
AMS subject classification: **11G18**, 14G35, 14G05.
Keywords: Shimura curves, rational points, Galois representations, Hasse principle, Brauer–Manin obstruction.

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

existence of abelian surfaces with multiplication by $\mathcal{O}_D$ defined over K (*cf.* [Jor86, Theorem 6.3]).

There is no reason to expect the hypothesis that K splits B to be correlated with the failure of X_D to admit points over K, and in fact standard conjectures predict that $X_D(K)$ should be empty when both D and disc(K) are large enough.

The first main result of this paper provides sufficient conditions for $X_D(K)$ to be empty without assuming that hypothesis. The method of proof pushes the original one of Jordan, as strengthened by Skorobogatov in [Sko05], in order to prove that the non-existence of points in $X_D(K)$ is accounted for by the Brauer–Manin obstruction. The novelty in our setting is that a pair $(A,\iota)/\overline{K}$ represented by a point $P \in X_D(K)$ may not admit a model over K, and we overcome this by attaching to P (and to any choice of prime p) a Galois representation

$$\varrho_P\colon\ \mathrm{Gal}\,(\overline{K}/K)\longrightarrow(B_D\otimes\mathbb{Q}_p)^\times/\pm1, \tag{1.1}$$

following an idea pioneered by Ellenberg and Skinner [ES01] in the context of elliptic $\mathbb{Q}$-curves.

In order to precisely state our result, let us fix some notations, already present in [Jor86, Sko05]. For a given rational prime q, let us define $P_1(q)$ to be the set of prime factors of the non-zero integers in the set

$$\bigcup_{s,a}\{a^2-sq^2, a^4-4a^2q^2+q^4\},$$

where the union is over $s = 0,1,2,3,4$ and the integers a such that $|a| \le 2q$. For $q \ne 2$, define also $\mathcal{B}_1(q)$ to be the set of indefinite rational quaternion algebras that are not split by $\mathbb{Q}(\sqrt{-q})$. Similarly, define $\mathcal{B}_1(2)$ as the set of indefinite rational quaternion algebras that are not split by either $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-1})$.

We say that a point $P \in X_D(\overline{\mathbb{Q}})$ has CM (by an imaginary quadratic field K) if the abelian surfaces in the isomorphism class corresponding to P have complex multiplication (by K).

Write $X_D(\mathbb{A}_K)^{\mathrm{Br}}$ for the subset of the set $X_D(\mathbb{A}_K)$ of adelic points on $X_D \times K$ cut out by the Brauer–Manin conditions; $X_D(\mathbb{A}_K)^{\mathrm{Br}}$ always contains the set of global points $X_D(K)$, and when $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \varnothing$ one says that the emptiness of $X_D(K)$ is explained by the Brauer–Manin obstruction.

Theorem 1.1 *Let K be an imaginary quadratic field in which a prime q is ramified. If $B_D \in \mathcal{B}_1(q)$ is such that D is divisible by a prime $p \notin P_1(q)$, $p \ge 5$, and p is not split in K, then $X_D(K)$ consists only of CM-points.*

If in addition $K \ne \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \varnothing$.

Similar techniques to those used in the proof of Theorem 1.1 should still be useful to tackle the questions addressed in this paper over larger number fields, although the authors made no attempt of generalization in this direction.

In [Jor86, pp. 93–94], Jordan calls a pair (B_D, K) *exceptional* if K fails to split B_D and $X_D(K_v) \ne \varnothing$ for every place v of K; he adopted this terminology as these are precisely the pairs for which the results of [Jor86, Sko05] do not apply. In Table 1

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

$D = 2 \cdot p$	$K = \mathbb{Q}(\sqrt{d})$
$2 \cdot 19$	$\mathbb{Q}(\sqrt{-39}), \mathbb{Q}(\sqrt{-87}), \mathbb{Q}(\sqrt{-111}), \mathbb{Q}(\sqrt{-159})$
$2 \cdot 29$	$\mathbb{Q}(\sqrt{-15}), \mathbb{Q}(\sqrt{-55}), \mathbb{Q}(\sqrt{-95}), \mathbb{Q}(\sqrt{-119})$
$2 \cdot 31$	$\mathbb{Q}(\sqrt{-39}), \mathbb{Q}(\sqrt{-87}), \mathbb{Q}(\sqrt{-111}), \mathbb{Q}(\sqrt{-159}), \mathbb{Q}(\sqrt{-183})$
$2 \cdot 37$	$\mathbb{Q}(\sqrt{-15}), \mathbb{Q}(\sqrt{-39}), \mathbb{Q}(\sqrt{-87}), \mathbb{Q}(\sqrt{-111}), \mathbb{Q}(\sqrt{-183})$
$2 \cdot 43$	$\mathbb{Q}(\sqrt{-15}), \mathbb{Q}(\sqrt{-87}), \mathbb{Q}(\sqrt{-95}), \mathbb{Q}(\sqrt{-111}), \mathbb{Q}(\sqrt{-183})$
$2 \cdot 47$	$\mathbb{Q}(\sqrt{-55}), \mathbb{Q}(\sqrt{-95})$
$2 \cdot 53$	$\mathbb{Q}(\sqrt{-39}), \mathbb{Q}(\sqrt{-55})$
$2 \cdot 59$	$\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-119})$
$2 \cdot 61$	$\mathbb{Q}(\sqrt{-55}), \mathbb{Q}(\sqrt{-87}), \mathbb{Q}(\sqrt{-111}), \mathbb{Q}(\sqrt{-159}), \mathbb{Q}(\sqrt{-183})$

Table 1: Exceptional pairs (B_D, K) with $X_D(\mathbb{A}_K)^{\mathrm{Br}} = \varnothing$.

we list some examples of exceptional pairs (B_D, K) to which Theorem 1.1 applies to show that $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \varnothing$.

We now introduce our second main result. The Shimura curve X_D is supplied with a natural group of rational involutions, namely the Atkin–Lehner group $W_D \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$ of $\mathcal{O}_D$, whose elements are the so-called Atkin–Lehner involutions (see [Rot04, §3]). Although $X_D(\mathbb{Q}) = \varnothing$, one may ask whether the quotient of X_D by an Atkin–Lehner involution ω_m, which we denote by $X_D^{(m)}$, has rational points or not.

In [RSY05], Skorobogatov, Yafaev and the first author established a criterion for the existence of local points on $X_D^{(m)}$ at every place of $\mathbb{Q}$, using previous work of Ogg. This allowed them to exhibit that $X_{23\cdot 107}^{(107)}$ is a counterexample to the Hasse principle over $\mathbb{Q}$. In [Cla03], Clark studied the quotient of the Shimura curve X_D by the full Atkin–Lehner involution ω_D and showed that $X_D^{(D)}$ has points rational over every completion of $\mathbb{Q}$.

On the other hand, Parent and Yafaev [PY07] have given a method for studying global rational points on certain Atkin–Lehner quotients of Shimura curves. They study the case where $D = pm$ is the product of two odd primes with $p \equiv 1 \bmod 4$ and $m \equiv 3 \bmod 4$, which corresponds to the "non-ramifié" case in the terminology of Ogg (see [Ogg85]). In [PY07], explicit conditions for rational points on these quotients to be "trivial" (arising from CM points) are given, and they also find an infinite family of such quotients satisfying them. This work has recently been taken a step further by Gillibert in [Gil10], where Parent–Yafaev conditions are made explicit.

In this paper we tackle this question by exploiting the moduli interpretation of $X_D^{(m)}$ as the classifying space of abelian surfaces with real multiplication by $\mathbb{Q}(\sqrt{m})$ whose endomorphism algebras contain the maximal order $\mathcal{O}_D$ (*cf.* Proposition 2.20 for more details) and the Galois representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with values in $\mathrm{GL}_2(\mathbb{Q}(\sqrt{m}) \otimes \mathbb{Q}_p)/\{\pm 1\}$ that we can attach to these abelian surfaces, in the same fashion as in (1.1).

As a result, we are able to prove the following statement. For a given rational prime

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

q we define $P_2(q)$ to be the set of prime factors of the non-zero integers in the set

$$\bigcup_{s,a}\{a^2 - sq, a^4 - 4a^2q + q^2\},$$

where the union now is over $s = 0, 1, 2, 3, 4$ and the integers a such that $|a| \leq 2\sqrt{q}$. If $\mathcal{Q}$ denotes the set of indefinite rational quaternion algebras, define

$$\mathcal{B}_2(q) := \left\{ B \in \mathcal{Q} \;\middle|\; \begin{array}{l} B \in \mathcal{B}_1(q) \text{ and } q \text{ is not inert in any imaginary} \\ \text{quadratic field } K \text{ such that } \underline{\mathrm{disc}}(K) \mid \mathrm{disc}(B) \end{array} \right\} \subset \mathcal{Q},$$

where $\underline{\mathrm{disc}}(K)$ is the (square-free) product of the primes ramifying in K.

Theorem 1.2 *Let B_D be an indefinite quaternion algebra of odd discriminant $D = pm$, with $p \geq 7$ a prime such that $p \equiv 3 \mod 4$. If there is a prime q such that $B_D \in \mathcal{B}_2(q)$ and $p \notin P_2(q)$, then $X_D^{(m)}(\mathbb{Q}) = \emptyset$.*

Using the criterion given in [RSY05, Theorem 3.1] we can check whether a pair (p, m) satisfying the hypotheses of Theorem 1.2 gives rise to a curve $X_D^{(m)}$ that has points everywhere locally and thus violates the Hasse principle over $\mathbb{Q}$; Table 2 lists some of such pairs (p, m).

Pairs (p, m) such that $X_{pm}^{(m)}$ violates the Hasse principle over $\mathbb{Q}$.
(23, 17), (31, 17), (31, 29), (31, 37), (31, 53), (31, 61), (47, 13),
(47, 41), (59, 13), (71, 13), (71, 17), (79, 17), (83, 5), (83, 13),
(103, 5), (107, 5), (107, 17), (127, 5), (151, 13), (167, 5), (223, 5),
(227, 5), (263, 5), (283, 5), (307, 5), (347, 5), (367, 5), (383, 5)

Table 2

As opposed to the approach taken in [PY07] and [Gil10], observe that if we consider discriminants of the form $D = pm$ with p, m different odd primes, the conditions on the above theorem place us in Ogg's "ramifié" case (see [Ogg85]). Therefore, our results are complementary to those in [PY07, Gil10].

In addition to the ideas mentioned above, our proof of Theorem 1.2 also borrows the descent techniques from [Sko05] together with some ideas from [Rot08].

This paper is organized as follows. Section 2 is devoted to constructing the Galois representations that were alluded to above. We present the main ideas in a somewhat general framework, giving special attention to the case of Shimura curves and their Atkin–Lehner quotients. In Section 3 we use these representations in combination with the machinery of descent applied to the étale Shimura covering $Z_{D,p}$ of X_D that is associated with a prime factor p of D to prove Theorem 1.1. Section 4 follows similar lines to prove Theorem 1.2.

Finally, the last section is a short appendix in which we show how the techniques of [Rot08] alone can also be used to find counterexamples to the Hasse principle among

Atkin–Lehner quotients of Shimura curves. Notice that Theorem A.1 applies to Ogg's "ramifié" case. The proof is comparatively simpler, because there all rational points can be represented by an abelian surface that admits a model over $\mathbb{Q}$, and therefore one can work directly with the usual Galois representations, but we find it is worth stating, as it strengthens the results of [RSY05] and is directly related to Coleman's conjecture described in [BFGR06].

1.1 Notation

Given a field k of characteristic zero, let $\overline{k}$ denote a fixed algebraic closure of k and $G_k = \operatorname{Gal}(\overline{k}/k)$ be the absolute Galois group of k. By a field extension of k we will always mean a subfield of $\overline{k}$ containing k. Given an abelian variety A defined over k, write $\operatorname{End}(A)$ for the $\mathbb{Z}$-algebra of endomorphisms of A and $\operatorname{End}^0(A) = \mathbb{Q}\otimes_{\mathbb{Z}}\operatorname{End}(A)$. If L/k is a field extension, we will often write $\operatorname{End}_L(A)$ for $\operatorname{End}(A \times L)$.

2 Galois Representations Over the Field of Moduli

The aim of this section is to adapt to our setting an idea of Ellenberg and Skinner that arose while proving the modularity of $\mathbb{Q}$-curves (see [ES01]).

Given a number field K, a $\mathbb{Q}$-curve over K is an elliptic curve E/K such that there exists a K-isogeny $\mu_\sigma\colon {}^\sigma E \to E$ for every $\sigma \in G_{\mathbb{Q}}$. Using these isogenies, Ellenberg and Skinner showed that for any prime p the usual Galois representation

$$\phi_{E,p}\colon G_K \to \operatorname{Aut}\big(T_p(E)\big) \simeq \mathrm{GL}_2(\mathbb{Z}_p)$$

can be extended to a representation $\rho_{E,p}\colon G_{\mathbb{Q}} \to \overline{\mathbb{Q}}_p^\times\, \mathrm{GL}_2(\mathbb{Q}_p)$ such that $\mathbb{P}\rho_{E,p|G_K} = \mathbb{P}\phi_{E,p}$. To do this, they considered the cohomology class $[c_E] \in \mathrm{H}^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^\times)$ of the 2-cocycle on $G_{\mathbb{Q}}$ with values on the trivial $G_{\mathbb{Q}}$-module $\overline{\mathbb{Q}}^\times$ given by

$$c_E(\sigma,\tau) = \mu_\sigma \cdot {}^\sigma\mu_\tau \cdot \mu_{\sigma\tau}^{-1} \in \big(\operatorname{Hom}(E,E)\otimes\mathbb{Q}\big)^\times = \mathbb{Q}^\times.$$

According to a theorem of Tate, $[c_E]$ is trivial, and hence there exists a continuous map $\alpha\colon G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^\times$ such that $c_E(\sigma,\tau) = \alpha(\sigma)\alpha(\tau)\alpha(\sigma\tau)^{-1}$. The rule

$$\rho_{E,p}(\sigma)(1\otimes x) = \alpha(\sigma)^{-1} \otimes \mu_\sigma({}^\sigma x)$$

then gives rise to an action of $G_{\mathbb{Q}}$ on $\overline{\mathbb{Q}}_p^\times \otimes T_p(E)$ that extends the one of G_K given by $\phi_{E,p}$. Note that if E is already defined over $\mathbb{Q}$, we can choose $\mu_\sigma = \mathrm{id}$ for all $\sigma \in G_{\mathbb{Q}}$ and $\alpha = 1$, so that this action is nothing but the usual one.

The role of this representation regarding modularity relies on the fact that a $\mathbb{Q}$-curve E/K is modular if and only if there exists a normalized eigenform f and a prime p such that $\rho_{E,p} \simeq \rho_{f,p}$.

2.1 Galois Representations Attached to Abelian Varieties

We turn now to a scenario that is more germane to the goals of this paper. Let k be a field of characteristic zero and A be a polarized abelian variety of dimension g defined

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

over a field L/k. Unless needed, we will not make explicit the choice of polarization on A. For any prime p, there is a Galois representation

$$\varrho_A = \varrho_{A,p} \colon G_L \longrightarrow \operatorname{Aut}(V_p(A)) \simeq \operatorname{GSp}_{2g}(\mathbb{Q}_p)$$

arising from the action of G_L on the p-adic Tate module $V_p(A) = T_p(A) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ of A, equipped with the alternate pairing induced by the Weil pairing and the choice of polarization. We will drop p from the notation whenever it is clear from the context.

Let R be a finite $\mathbb{Z}$-algebra and assume that A is equipped with a monomorphism of $\mathbb{Z}$-algebras $i \colon R \hookrightarrow \operatorname{End}(A)$.

Definition 2.1 Let

$$C_R(A) := \{\varphi \in \operatorname{End}^0(A) : \varphi \circ i(r) = i(r) \circ \varphi \text{ for all } r \in R\}$$

denote the $\mathbb{Q}$-subalgebra of endomorphisms of A that commute with the action of R.

Similarly, define the $\mathbb{Z}_p$-algebra $C_R(T_p(A))$ to be the commutator of $R \otimes_{\mathbb{Z}} \mathbb{Z}_p$ in $\operatorname{End}(T_p(A))$; that is,

$$C_R(T_p(A)) := \{\varphi \in \operatorname{End}(T_p(A)) : \varphi \circ i(r) = i(r) \circ \varphi \text{ for all } r \in R\}.$$

Observe that $C_R(A) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is a $\mathbb{Q}_p$-subalgebra of $C_R(T_p(A)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$.

Definition 2.2 Let

$$G_p := C_R(T_p(A))^\times \quad \text{and} \quad \overline{G_p} := \Big(C_R\big(T_p(A)\big) / pC_R\big(T_p(A)\big) \Big)^\times$$

denote the group of units of $C_R(T_p(A))$ and $C_R(T_p(A))/pC_R(T_p(A))$, respectively.

Since the action of G_L on the Tate module $T_p(A)$ commutes with the action of R induced by the embedding i, there is a Galois representation

$$\varrho_{(A,i)} = \varrho_{(A,i),p} \colon G_L \longrightarrow G_p$$

attached to the pair (A, i).

The reduction of $\varrho_{(A,i)}$ modulo p corresponds to the Galois representation given by the action of G_L on the p-torsion subgroup $A[p] = T_p(A)/pT_p(A)$ of A, which we denote by

$$\overline{\varrho}_{(A,i)} = \overline{\varrho}_{(A,i),p} \colon G_L \longrightarrow \overline{G_p}.$$

2.2 Galois Representations Attached to Points on Shimura Varieties

Let k be a field of characteristic 0 and R a finite $\mathbb{Z}$-algebra such that $\mathbb{Q} \otimes R$ is a semisimple algebra. Let X be the moduli space parametrizing isomorphism classes of pairs (A, i), where A is a polarized abelian variety and $i \colon R \hookrightarrow \operatorname{End}(A)$ is a monomorphism of $\mathbb{Z}$-algebras. We omit here the technicalities concerning the compatibility between

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

the polarization and i; we shall treat this with care only in the cases under study in this paper.

The theory of Shimura varieties of PEL type (*cf. e.g.*, [Mil04, §8 and 14]) affords a canonical model of X over $\mathbb{Q}$, that we still denote X by a slight abuse of notation, so that a point $P \in X(\bar{k})$ corresponds to the $\bar{k}$-isomorphism class

$$P = [(A,i)] = \{(A',i')/\bar{k} : \text{ there exists an isomorphism of pairs } (A',i') \simeq (A,i)\}$$

of a polarized abelian variety $(A,i)/\bar{k}$ with multiplication by R.

We say that the pair $(A,i)/\bar{k}$ admits a model rational over a field L/k if there exists a pair (A',i') defined over L for which there is an isomorphism $(A' \times \bar{k}, i' \times \bar{k}) \simeq (A,i)$. When this is the case, we say that L is a *field of definition* for (A,i). Besides, the *field of moduli* $k_P = k_{(A,i)}$ of (A,i) is the minimal field extension k_P/k such that for each $s \in G_{k_P}$ there is an isomorphism of pairs $f_s \colon {}^s(A,i) \to (A,i)$. Clearly, the field of moduli of (A,i) is unique and is contained in every field of definition of (A,i). Then for any field extension L/k the set $X(L)$ of L-rational points of X is

$$X(L) = \{P \in X(\bar{k}) : k_P \subseteq L\}.$$

In particular, note that if (A,i) admits a model rational over L, then $P = [(A,i)]$ belongs to $X(L)$. However, the converse is not true in general.

Fix a point $P = [(A,i)]$ on X and assume without loss of generality that $k_P = k$ (if $k_P \supsetneq k$, replace k by k_P). For the rest of this section, we shall make the following hypothesis.

Hypothesis 2.3 *$C_R(A)$ is a field whose only roots of unity are ± 1.*

Lemma 2.4 *Let $\operatorname{Aut}(A,i)$ denote the group of automorphisms of the polarized abelian variety (A,i) with multiplication by R. If Hypothesis 2.3 holds, then $\operatorname{Aut}(A,i) = \{\pm 1\}$.*

Proof From the definitions, $C_R(A) = \operatorname{End}^0(A,i)$, so that $\operatorname{Aut}(A,i)$ is contained in the multiplicative group $C_R(A)^\times$ of the invertible elements in $C_R(A)$. Since the automorphism group of a polarized abelian variety is finite (see [Mil86, Proposition 17.5]), it follows that $\operatorname{Aut}(A,i)$ consists of roots of unity in $C_R(A)$. By our assumption, $\operatorname{Aut}(A,i) = \{\pm 1\}$. ■

From the definition of field of moduli, attached to the point P, we can construct a two-cocycle $c_P \colon G_k \times G_k \to \{\pm 1\}$ as follows: choose a collection of isomorphisms $\mathbf{f} = \{f_s : {}^s(A,i) \to (A,i)\}_{s \in G_k}$ and set

$$c_P(s,t) = f_s \cdot {}^s f_t \cdot f_{st}^{-1} \in \operatorname{Aut}(A,i) = \{\pm 1\}, \quad \text{for any } s,t \in G_k.$$

Lemma 2.5 *The class $[c_P] \in \mathrm{H}^2(G_k, \{\pm 1\})$ does not depend on the choice of $\mathbf{f}$.*

Proof Suppose $\mathbf{f} = \{f_s : {}^s(A,i) \to (A,i)\}_{s \in G_k}$ and $\mathbf{f}' = \{f'_s \colon {}^s(A,i) \to (A,i)\}_{s \in G_k}$ are two distinct collections of isomorphisms, and let c_P and c'_P be the corresponding cocycles defined as above. Then, for each $s \in G_k$, $\lambda_s := f'_s \cdot f_s^{-1}$ is an automorphism of (A,i), hence $\lambda_s = \pm 1$, and we can write $f'_s = \lambda_s \cdot f_s$. Therefore,

$$c'_P(s,t) = (\lambda_s \cdot f_s) \cdot {}^s(\lambda_t \cdot f_t) \cdot (\lambda_{st} \cdot f_{st})^{-1} = \lambda_s \cdot \lambda_t \cdot \lambda_{st}^{-1} c_P(s,t),$$

so that c_P and c'_P define the same cohomology class in $\mathrm{H}^2(G_k, \{\pm 1\})$. ■

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

The following lemma is consequence of a well-known result due to Weil (see [Wei56, Theorem 3]).

Lemma 2.6 *A field L/k is a field of definition for (A, i) if and only if the restriction $c_{P,L}$ of c_P to G_L becomes trivial in $\mathrm{H}^2(G_L, \{\pm 1\})$.*

Let $\mathcal{Q}_k$ denote the set of isomorphism classes of quaternion algebras over the field k.

Definition 2.7 Let $B_P \in \mathcal{Q}_k$ be the quaternion algebra over k (up to isomorphism) corresponding to $[c_P] \in \mathrm{H}^2(G_k, \{\pm 1\})$ via the isomorphism $\mathrm{H}^2(G_k, \{\pm 1\}) \simeq \mathcal{Q}_k$ provided by class field theory.

Examples 2.8 If $g = 1$ and $R = \mathbb{Z}$, then $X \simeq \mathbb{A}^1/\mathbb{Q}$ is the j-line classifying elliptic curves. This moduli space is not fine, but it is nevertheless true that for any point $j \in X(k)$ there exists an elliptic curve E_j defined over k representing the isomorphism class given by j. If $j \neq 0, 1728$, then $\mathrm{Aut}(E_j) = \{\pm 1\}$ and $B_j = \mathrm{M}_2(k)$.

If $g = 2$, $R = \mathbb{Z}$ and the polarizations are assumed to be principal, X is commonly referred to as the Igusa threefold. The generic point $P \in X(k)$ corresponds to the isomorphism class of a principally polarized abelian surface $A/\overline{k}$ such that $\mathrm{End}(A) = \mathbb{Z}$. In this case Hypothesis 2.3 is fulfilled, and an algorithm for computing the quaternion algebra B_P is due to Mestre [Me90].

In general it is a difficult problem to compute the class of the cocycle c_P and the quaternion algebra B_P. See Theorems 2.13 and 2.21 for yet other instances.

In terms of B_P, Lemma 2.6 asserts that a field L is a field of definition for (A, i) if and only if $B_P \otimes_k L \simeq \mathrm{M}_2(L)$. When this holds, we say that L *splits* B_P. As an immediate consequence of that we obtain the following corollary.

Corollary 2.9 *There exist infinitely many quadratic extensions L/k that are a field of definition of (A, i), namely, those which split B_P.*

We are finally in a position to construct representations of G_k attached to the point $P \in X(k)$. First, we choose a collection $\mathbf{f} = \{f_s \colon {}^s(A, i)) \to (A, i)\}_{s \in G_k}$ as before and define

$$\varrho_P = \varrho_{P,p} \colon G_k \longrightarrow G_p/\{\pm 1\}$$

by the rule

$$x \in T_p(A) \longmapsto \varrho_P(s)(x) := f_s({}^s x), \quad s \in G_k. \tag{2.1}$$

By passing to the quotient we similarly define

$$\overline{\varrho}_P = \overline{\varrho}_{P,p} \colon G_k \longrightarrow \overline{G_p}/\{\pm 1\}.$$

We do not keep track of the choice of $\mathbf{f}$ in the above representations because of the following result:

Lemma 2.10 *ϱ_P and $\overline{\varrho}_P$ are group homomorphisms that do not depend on the choice of* $\mathbf{f}$.

Proof First observe that for $s, t \in G_k$ and $x \in T_p(A)$ we have

$$\varrho_P(st)(x) = f_{st}({}^{st}x) = c_P(s,t)^{-1}\Big(f_s\big({}^s f_t({}^s({}^t x))\big)\Big) = c_P(s,t)^{-1}\Big(\varrho_P(s)\big(\varrho_P(t)(x)\big)\Big),$$

so that $\varrho_P(st) = \varrho_P(s) \cdot \varrho_P(t)$, since $c_P(s,t) = \pm 1$. Hence, $\varrho_P \colon G_k \to G_p/\{\pm 1\}$ is a group homomorphism.

Now let $\mathbf{f} = \{f_s \colon {}^s(A,i) \to (A,i)\}_{s\in G_k}$ and $\mathbf{f}' = \{f_s' \colon {}^s(A,i) \to (A,i)\}_{s\in G_k}$ be two distinct collections of isomorphisms. As before, define the map $\lambda \colon G_k \to \operatorname{Aut}(A,i) = \{\pm 1\}$ by $s \mapsto \lambda_s := f_s' \cdot f_s^{-1}$. Then

$$\begin{aligned} \varrho_{P,\mathbf{f}'}(s) \colon x &\longmapsto f_s'({}^s x), \\ \lambda_s \cdot \varrho_{P,\mathbf{f}}(s) \colon x &\longmapsto f_s' \cdot f_s^{-1} \cdot f_s({}^s x) = f_s'({}^s x). \end{aligned}$$

This shows that $\varrho_{P,\mathbf{f}'} = \varrho_{P,\mathbf{f}}$, since λ takes values in $\{\pm 1\}$. In fact, for any collection $\mathbf{f}$ as above and any map $\lambda \colon G_k \to \{\pm 1\}$, $f_s' := \lambda_s \cdot f_s$ defines a second collection $\mathbf{f}'$ of isomorphisms satisfying the above relation. The statement for $\overline{\varrho}_P$ follows similarly. ■

Remark 2.11 In view of Lemma 2.10, if (A,i) is defined over L/k, we can choose $f_s = \mathrm{id}$ for all $s \in G_L \subseteq G_k$. Then the restrictions of ϱ_P and $\overline{\varrho}_P$ to G_L clearly coincide with the reduction modulo ± 1 of $\varrho_{(A,i)}$ and $\overline{\varrho}_{(A,i)}$, respectively.

Remark 2.12 While Hypothesis 2.3 is fulfilled in the two scenarios we treat in detail, it could probably be relaxed by asking that $\operatorname{Aut}(A,i)$ be contained in the centre of $C_R(T_p(A))$, and working with Galois representations with values in $G_p/\operatorname{Aut}(A,i)$ and $\overline{G_p}/\operatorname{Aut}(A,i)$.

We devote the next two sections to performing a detailed analysis of the Galois representations that arise by the above construction when we deal with a Shimura curve over an imaginary quadratic field and, respectively, an Atkin–Lehner quotient of these curves over $\mathbb{Q}$.

2.3 The Case of Shimura Curves

Let B_D be an indefinite rational quaternion algebra of discriminant $D > 1$, fix a maximal order $\mathcal{O}_D \subseteq B_D$ and a positive anti-involution $\rho \colon B_D \to B_D, b \mapsto b^\rho$. By the Noether–Skolem Theorem, there exists $\mu \in B_D^\times$ such that $b^\rho = \mu^{-1}\overline{b}\mu$ for all $b \in B_D$. Further, one can check (see [Rot03]) that the positiveness of ρ implies that $\operatorname{tr}(\mu) = 0$ and $\operatorname{n}(\mu) > 0$. Since the element μ is determined up to multiplication by elements of $\mathbb{Q}^\times$, we can assume that μ^2 is a negative square-free integer, and we will sometimes write $\rho = \rho_\mu$.

An *abelian surface with multiplication by* $(B_D, \mathcal{O}_D, \rho)$ is a triplet $(A, \iota, \mathcal{L})$, where A is an abelian surface, $\iota \colon \mathcal{O}_D \hookrightarrow \operatorname{End}(A)$ is a monomorphism of rings, and $\mathcal{L}$ is a weak polarization on A such that the Rosati involution $*$ induced by $\mathcal{L}$ satisfies $\iota(b)^* = \iota(b^\rho)$ for all $b \in B_D$. By a result of Milne, the weak polarization is completely determined by the data $(B_D, \mathcal{O}_D, \rho)$. More precisely, if A is an abelian surface

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

endowed with a monomorphism of rings $\iota\colon \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$, then there is a unique weak polarization $\mathcal{L}$ on A such that $(A, \iota, \mathcal{L})$ is an abelian surface with multiplication by $(B_D, \mathcal{O}_D, \rho)$ (see [Mil79]), which is uniquely determined by the choice of μ. For this reason, we shall often drop the polarization from the triplet and work with pairs (A, ι).

If $(B_D, \mathcal{O}_D, \rho)$ is clear or not relevant in the context, we may just refer to (A, ι) as an abelian surface with QM by B_D, or simply a QM-abelian surface.

Let $\mathcal{O}_D^1$ denote the group of units of $\mathcal{O}_D$ of norm 1. By fixing an isomorphism $B_D \otimes \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$, the group $\mathcal{O}_D^1$ embeds in the group $\mathrm{SL}_2(\mathbb{R})$ of conformal transformations of the upper-half plane $\mathfrak{H}$.

The quotient $V_D := \mathcal{O}_D^1 \backslash \mathfrak{H}$ is a compact Riemann surface, and the work of Shimura [Shi67] shows that there exists a smooth projective algebraic curve X_D over $\mathbb{Q}$ such that $X_D(\mathbb{C})^{\mathrm{an}} \simeq V_D$. This curve is constructed as the coarse moduli space of abelian surfaces with QM by B_D, and is commonly known as *the Shimura curve associated with B_D*. The isomorphism class of this curve does not depend on the choices made above.

Let k be a field of characteristic zero and $P \in X_D(k)$ be a k-rational point on X_D. By the moduli interpretation of X_D, P corresponds to a pair $(A, \iota)/\bar{k}$ whose field of moduli is k. This amounts to saying that there exists a collection

$$\mathbf{f} = \left\{ f_s\colon {}^s(A, \iota) \to (A, \iota) \right\}_{s \in G_k}$$

of isomorphisms of pairs, indexed by the elements of the absolute Galois group of k.

Hypothesis 2.3 holds for (A, ι), unless A has complex multiplication by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. Indeed, if A has no complex multiplication, so that $\iota\colon \mathcal{O}_D \overset{\simeq}{\to} \mathrm{End}(A)$ is an isomorphism, then the commutator of $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Q} \simeq B_D$ in $\mathrm{End}^0(A) \simeq B_D$ is $\mathbb{Q}$, hence Hypothesis 2.3 is clearly satisfied. Otherwise, suppose that A has complex multiplication by an order in an imaginary quadratic field $M/\mathbb{Q}$. Then $B_D \hookrightarrow \mathrm{End}^0(A) \simeq \mathrm{M}_2(M)$, and the commutator of $\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Q} \simeq B_D$ in $\mathrm{End}^0(A)$ is M. Whenever $M \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, Hypothesis 2.3 is still satisfied, so the claim follows.

The obstruction for the abelian surfaces parametrized by X_D to admit a model rational over their field of moduli was studied by Jordan in [Jor86], where he proved the following theorem (see [Jor86, Theorem 1.1]).

Theorem 2.13 (Jordan) *Let $P \in X_D(k)$ be a k-point on X_D and assume it has complex multiplication neither by $\mathbb{Q}(\sqrt{-1})$ nor by $\mathbb{Q}(\sqrt{-3})$. Then $B_P = B_D \otimes k$.*

In other words, for a given field extension L/k, there exists a QM-abelian surface (A, ι) over L such that $P = [(A, \iota) \times \bar{k}]$ if and only if L splits B_D.

Observe that B_P does not depend on the choice of the point P nor of the field k.

Towards the proof of Theorem 1.1, we now focus on local points on the Shimura curve X_D over imaginary quadratic fields. Fix at the outset a quadratic extension $K'/\mathbb{Q}$ splitting B_D, and let $K/\mathbb{Q}$ be an imaginary quadratic field. Let v and v' be places of K and K', respectively, above the same rational prime ℓ, and let us denote by w the unique extension of the ℓ-adic valuation on $\mathbb{Q}_\ell$ to the composite field $L_w := K_v \cdot K'_{v'}$. Since $K'_{v'}$ splits B_D, so does L_w. Let $P_v \in X_D(K_v)$ be a K_v-rational point.

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

By [Jor86, Theorem 1.1], we can choose a pair (A_v, ι_v) defined over L_w such that $P_v = [(A_v, \iota_v)]$.

As before, for each prime p dividing D there is a Galois representation

$$\varrho_{(A_v,\iota_v)} = \varrho_{(A_v,\iota_v),p}\colon G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v)) \simeq (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times \subseteq (B_D \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times,$$

arising from the action of G_{L_w} on the p-adic Tate module $V_p(A_v) = T_p(A_v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ of A_v, where the isomorphism $\mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v)) \simeq (\mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_p)^\times$ follows from [Oht64]. In the notation introduced above, we have $\mathrm{Aut}_{\mathcal{O}_D}(T_p(A_v)) = C_{\mathcal{O}_D}(T_p(A_v))^\times$.

The reduction modulo p of this representation takes the form

$$\overline{\varrho}_{(A_v,\iota_v)} = \overline{\varrho}_{(A_v,\iota_v),p}\colon G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(A_v[p]) \simeq (\mathcal{O}_D/p\mathcal{O}_D)^\times \subseteq \mathrm{GL}_2(\mathbb{F}_{p^2}).$$

Along with these two representations, Jordan attached to the pair (A_v, ι_v) a finite order character as follows. Let $I(p)$ denote the unique two-sided $\mathcal{O}_D$-ideal of reduced norm p ([Vig80, p. 86]) and define

$$C_p = A_v[I(p)] \simeq \mathcal{O}_D/I(p) \subseteq A_v[p],$$

which we shall regard as an $\mathcal{O}_D$-module. Jordan called C_p the *canonical torsion subgroup* of (A_v, ι_v) at the prime p.

By uniqueness, C_p is rational over L_w and is isomorphic as abstract module to $\mathbb{F}_{p^2}$. It follows that $\mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^\times$ and the action of G_{L_w} on C_p gives rise to the *canonical isogeny character at* p:

$$\alpha_{(A_v,\iota_v)} = \alpha_{(A_v,\iota_v),p}\colon G_{L_w} \longrightarrow \mathrm{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}_{p^2}^\times.$$

We shall sometimes regard $\alpha_{(A_v,\iota_v)}$ as a character on $G_{L_w}^{\mathrm{ab}} = \mathrm{Gal}\,(L_w^{\mathrm{ab}}/L_w)$, where L_w^{ab} is the abelian closure of L_w in $\overline{L}_w$.

Proposition 2.14 *With notations as before, we have the following.*

(i) *There is a $\mathbb{F}_{p^2}$-basis of $A_v[p]$ with respect to which*

$$\overline{\varrho}_{(A_v,\iota_v)} = \begin{pmatrix} (\alpha_{(A_v,\iota_v)})^p & 0 \\ * & \alpha_{(A_v,\iota_v)} \end{pmatrix}.$$

For any $\sigma \in G_{L_w}$, the characteristic polynomial of $\varrho_{(A_v,\iota_v)}(\sigma) \in \mathrm{Aut}_{\mathbb{F}_p}(A_v[p])$ is

$$\Big[\big(T - \alpha_{(A_v,\iota_v)}(\sigma)\big)\big(T - \alpha_{(A_v,\iota_v)}(\sigma)^p\big)\Big]^2.$$

(ii) *If $p \neq \ell$, $\varrho^{12}_{(A_v,\iota_v)}$ and $\alpha^{12}_{(A_v,\iota_v)}$ are unramified.*

Proof Statement (i) is [Jor81, Proposition 4.3.10], and (ii) follows from [Jor86, §3]. ■

Also, as in [Jor86, Proposition 4.6], we have the following lemma.

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

Lemma 2.15 *Let $\overline{\chi}_p\colon G_{K_v} \to \operatorname{Aut}(\mu_p) \simeq \mathbb{F}_p^\times$ be the reduction of the p-cyclotomic character. Then $N_{\mathbb{F}_{p^2}/\mathbb{F}_p} \circ \alpha_{(A_v,\iota_v)} = \overline{\chi}_{p|G_{L_w}}$.*

Assume that A_v has complex multiplication by neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-3})$, and let $P_v \in X_D(K_v)$ denote the point on X_D parametrizing the pair (A_v, ι_v). As explained in §2.2, attached to P_v there are Galois representations

$$\varrho_{P_v} = \varrho_{P_v,p}\colon G_{K_v} \longrightarrow \operatorname{Aut}_{\mathcal{O}_D}(T_p(A_v))/\{\pm 1\} \subseteq \mathrm{GL}_4(\mathbb{Z}_p)/\{\pm 1\},$$
$$\overline{\varrho}_{P_v} = \overline{\varrho}_{P_v,p}\colon G_{K_v} \longrightarrow \operatorname{Aut}_{\mathcal{O}_D}(A_v[p])/\{\pm 1\} \subseteq \mathrm{GL}_2(\mathbb{F}_{p^2})/\{\pm 1\}$$

and a character

$$\alpha_{P_v} = \alpha_{P_v,p}\colon G_{K_v} \longrightarrow \operatorname{Aut}_{\mathcal{O}_D}(C_p)/\{\pm 1\} \simeq \mathbb{F}_{p^2}^\times/\{\pm 1\}.$$

By Remark 2.11, the restrictions of these representations to $G_{L_w} \subseteq G_{K_v}$ coincide with the reduction modulo ±1 of $\varrho_{(A_v,\iota_v)}$, $\overline{\varrho}_{(A_v,\iota_v)}$ and $\alpha_{(A_v,\iota_v)}$, respectively.

We conclude this section by collecting a few basic properties of the characters α_{P_v} that will be crucial in the proof of Theorem 1.1 in Section 3. To begin with, note that from Proposition 2.14 we deduce the following corollary.

Corollary 2.16 *For $p \neq \ell$, $\alpha_{P_v,p}^{12}$ is unramified.*

Let us write

$$\widetilde{\varrho}_{P_v}\colon G_{K_v} \to \operatorname{Aut}_{\mathcal{O}_D}(T_p(A_v)) \quad \text{and} \quad \widetilde{\alpha}_{P_v}\colon G_{K_v} \to \mathbb{F}_{p^2}^\times$$

for the lifts of ϱ_{P_v} and α_{P_v}, respectively, associated with a choice of $\mathbf{f}$ as defined in (2.1). These lifts are not homomorphisms in general, but it is easy to check that for any $\sigma \in G_{K_v}$ we have $\widetilde{\varrho}_{P_v}(\sigma^2) = \pm\widetilde{\varrho}_{P_v}(\sigma)^2$ and $\widetilde{\alpha}_{P_v}(\sigma^2) = \pm\widetilde{\alpha}_{P_v}(\sigma)^2$.

While α_{P_v} factors through the maximal abelian quotient $G_{K_v}^{\mathrm{ab}}$ of G_{K_v}, the same is not true for the lift $\widetilde{\alpha}_{P_v}$; it does not necessarily descend to a map on $G_{K_v}^{\mathrm{ab}}$. However, it will suffice for our purposes to make the (obvious) observation that for every $\sigma \in G_{K_v}$, the value $\widetilde{\alpha}_{P_v}(\sigma)^2 \in \mathbb{F}_{p^2}^\times$ depends only on the class of σ in $G_{K_v}^{\mathrm{ab}}$.

Using the fact that $\widetilde{\alpha}_{P_v|G_{L_w}}$ coincides with $\alpha_{(A_v,\iota_v)}$, Lemma 2.15 implies that

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}\big(\widetilde{\alpha}_{P_v|G_{L_w}}(\sigma)\big) = \chi_{p|G_{L_w}}(\sigma), \quad \text{for all } \sigma \in G_{L_w}.$$

Since L_w has at most degree 2 over K_v, we can write

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}\big(\widetilde{\alpha}_{P_v|G_{L_w}}(\sigma^2)\big) = \chi_{p|G_{L_w}}(\sigma^2) = \chi_p(\sigma)^2, \quad \text{for all } \sigma \in G_{K_v}.$$

And, using that $\widetilde{\alpha}_{P_v|G_{L_w}}(\sigma^2) = \pm\widetilde{\alpha}_{P_v}(\sigma)^2$ for all $\sigma \in G_{K_v}$, we get that

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}\big(\widetilde{\alpha}_{P_v}(\sigma)^2\big) = \chi_p(\sigma)^2, \quad \text{for all } \sigma \in G_{K_v}. \tag{2.2}$$

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

2.4 The Case of Atkin–Lehner Quotients of Shimura Curves

Keeping the same notations as in the previous section, put

$$B_{D,+}^{\times} = \{b \in B_D : \mathrm{n}(b) > 0\}$$

and define the *Atkin–Lehner group* of X_D to be

$$W_D = \mathrm{N}_{B_{D,+}^{\times}}(\mathcal{O}_D^1)/\mathbb{Q}^{\times}\mathcal{O}_D^1,$$

the normalizer of $\mathcal{O}_D^1$ in $B_{D,+}^{\times}$, up to homotheties and units in $\mathcal{O}_D^1$.

As is shown *e.g.*, in [Jor81, p. 10], there is an isomorphism $W_D \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$ of abstract groups, where $2r$ is the number of prime factors of D. A complete set of representatives for W_D is given by any set of elements $\{\mathrm{w}_m\}_{m|D}$, where $\mathrm{w}_m \in \mathcal{O}_D$ has reduced norm m and m ranges over the positive divisors of D .

The action of an involution $\omega_m = [\mathrm{w}_m] \in W_D$ can be modularly interpreted as follows. If $P = [(A, \iota, \mathcal{L})]$ denotes the isomorphism class of an abelian surface with QM by B_D, regarded as a closed point of X_D, then

$$\omega_m(P) = \big[(A, \iota_{\omega_m}, \mathcal{L}_{\omega_m})\big],$$

where $\iota_{\omega_m}(\beta) = \iota(\mathrm{w}_m^{-1}\beta\mathrm{w}_m)$ for $\beta \in \mathcal{O}_D$ and $\mathcal{L}_{\omega_m} = \frac{\iota(\mathrm{w}_m)^*(\mathcal{L})}{m}$.

It follows from this description that the Atkin–Lehner group W_D acts on X_D as a subgroup of algebraic involuting automorphisms over $\mathbb{Q}$.

For an integer $m > 1$ dividing D, let $X_D^{(m)}$ denote the quotient curve $X_D/\langle\omega_m\rangle$ and write $\pi_m \colon X_D \to X_D^{(m)}$ for the natural projection. This quotient also admits a natural moduli interpretation, which we now describe.

Definition 2.17 We say that $\mathcal{O}_D$ admits a *twist of degree* $\delta \geq 1$ if there exists $m \in \mathbb{Z}$, $m \mid D$, such that

$$B_D = \mathbb{Q} + \mathbb{Q}\mu + \mathbb{Q}\chi + \mathbb{Q}\mu\chi = \Big(\frac{-D\delta, m}{\mathbb{Q}}\Big),$$

with $\mu, \chi \in \mathcal{O}_D$, $\mu^2 = -D\delta$, $\chi^2 = m$ and $\mu\chi = -\chi\mu$. In this case we say that the twist is of norm m. If $\delta = 1$, we say that $\mathcal{O}_D$ admits a *principal twist*. Fixed an element $\mu \in \mathcal{O}_D$, $\mu^2 + D\delta = 0$, we say that the pair $(\mathcal{O}_D, \mu)$ admits a twist of norm $m \mid D$ if there exists $\chi \in \mathcal{O}_D$ satisfying the above conditions.

Note that $\mathcal{O}_D$ does not necessarily admit twists of a fixed degree $\delta \geq 1$. However, we have the following lemma.

Lemma 2.18 *Assume that $D = pm$ is odd, with p a prime such that $(\frac{m}{p}) = -1$. There exists an integer $\delta \geq 1$ such that $\mathcal{O}_D$ admits a twist of degree δ and norm m.*

Proof An easy computation of Hilbert symbols shows (using Čebotarev's Theorem) that there exist infinitely many primes δ such that $B_D \simeq \big(\frac{-D\delta, m}{\mathbb{Q}}\big)$. Hence, we can choose $\mu, \chi \in B_D$ 3 such that $\mu^2 + D\delta = 0$, $\chi^2 = m$ and $\mu\chi = -\chi\mu$. Furthermore,

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

since $\mathbb{Z}[\mu, \chi]$ is an integral order in B_D and any maximal order is conjugated to $\mathcal{O}_D$, the elements μ and χ can be taken to lie in $\mathcal{O}_D$. ■

Theorem 1.2, which will be proved in Section 4, gives sufficient conditions for $X_D^{(m)}(\mathbb{Q})$ to be empty. Since we can only apply our methods when D is odd and $m \neq D$, by [RSY05, Theorem 3.1] it is harmless to assume that $D = pm$ for some odd prime p with $(\frac{m}{p}) = -1$, as otherwise $X_D^{(m)}(\mathbb{A}_{\mathbb{Q}}) = \varnothing$. In view of this, we will make the following assumption for the rest of this section.

Assumption 2.19 D is odd, and $D = pm$ for some prime p with $(\frac{m}{p}) = -1$.

By virtue of the previous lemma, choose elements $\mu, \chi \in \mathcal{O}_D$ with $\mu^2 + D\delta = 0$, $\chi^2 = m$, and $\mu\chi = -\chi\mu$, for some integer $\delta \geq 1$. Without loss of generality, we can assume that X_D is the Shimura curve attached to the datum $(B_D, \mathcal{O}_D, \rho_\mu)$.

Since $\mathrm{n}(\chi) = -m$ and the set of elements of norm $\pm m$ in $\mathcal{O}_D$ is a homogeneous space under the action of $\mathcal{O}_D^\times$, we have $\chi = \mathrm{w}_m\alpha$ for some $\alpha \in \mathcal{O}_D^\times$ of reduced norm -1.

Let R_m be the ring of integers of the quadratic field $E = \mathbb{Q}(\sqrt{m})$, and denote by $\mathcal{H}_m$ the Hilbert modular surface classifying isomorphism classes of triplets $(A, i, \mathcal{L})$, where

- A is an abelian surface,
- $i\colon R_m \hookrightarrow \mathrm{End}(A)$ is a ring monomorphism, and
- $\mathcal{L}$ is a weak polarization on A.

The element χ determines an embedding $R_m \hookrightarrow \mathcal{O}_D$ of R_m into $\mathcal{O}_D$. This embedding in turn induces a forgetful map $\pi_{R_m}\colon X_D \to \mathcal{H}_m$, given in terms of moduli by the transformation $(A, \iota, \mathcal{L}) \mapsto (A, \iota_{|R_m}, \mathcal{L})$. The next statement is easily obtained by following the same arguments as in the proof of [Rot04, Theorem 4.4].

Proposition 2.20 *The map π_{R_m} is a quasifinite map that factors over $\mathbb{Q}$ into the natural projection $\pi_m\colon X_D \to X_D^{(m)}$ of X_D onto its quotient $X_D^{(m)}$ and a birational morphism $b_{R_m}\colon X_D^{(m)} \dashrightarrow \pi_{R_m}(X_D) \subseteq \mathcal{H}_m$ into the image of X_D by π_{R_m} in $\mathcal{H}_m$. Moreover, $b_{R_m}^{-1}$ is defined on the whole $\pi_{R_m}(X_D)$ except for a finite set of CM points.*

As a consequence, the Atkin–Lehner quotient $X_D^{(m)}$ is a solution to the coarse moduli problem of classifying isomorphism classes of abelian surfaces $(A, i, \mathcal{L})$ with real multiplication by E and admitting multiplication by $(B_D, \mathcal{O}_D, \rho_\mu)$. As before, there is no need to mention the weak polarization $\mathcal{L}$, and we shall rather work with pairs $(A, i\colon R_m \hookrightarrow \mathrm{End}(A))$.

If k is a field of characteristic zero, a point Q in $X_D^{(m)}$ is k-rational if and only if Q corresponds under the moduli interpretation to the isomorphism class of a pair $(A, i)/\bar{k}$ where:

- A is an abelian surface such that the ring $\mathrm{End}(A)$ contains $\mathcal{O}_D$;
- $i\colon R_m \hookrightarrow \mathrm{End}(A)$;
- there exists a collection of isomorphisms $\mathbf{f} = \{f_s\colon {}^s(A, i) \to (A, i)\}_{s \in G_k}$, that is,

for each $s \in G_k$ there is an isomorphism $f_s \colon {}^sA \to A$ such that the diagram

$$(2.3)\qquad \begin{tikzcd} {}^sA \arrow[r, "f_s"] \arrow[d, "{}^s i(\alpha)"'] & A \arrow[d, "i(\alpha)"] \\ {}^sA \arrow[r, "f_s"] & A \end{tikzcd}$$

commutes for every $\alpha \in R_m$.

Theorem 2.21 (Bruin–Flynn–González–Rotger) *Let $Q = [(A, i)] \in X_D^{(m)}(k)$ be a non-CM point and K/k be the (at most quadratic) extension of k generated by the coordinates of $\pi_m^{-1}(Q)$. Write $K = k(\sqrt{\delta})$ for some $\delta \in k^\times$. Then*

$$B_Q = (B_D \otimes_{\mathbb{Q}} k) \otimes \left(\frac{\delta, m}{k}\right),$$

that is to say, (A, i) admits a model rational over K/k if and only if $B_D \otimes_{\mathbb{Q}} K \simeq (\frac{\delta, m}{K})$.

The main ingredient in the proof of Theorem 1.2 is the study of the Galois representations attached to rational points on $X_D^{(m)}$ over a local field. Let us describe these representations in some detail here.

Let ℓ be a prime, $Q_\ell \in X_D^{(m)}(\mathbb{Q}_\ell)$ be a $\mathbb{Q}_\ell$-point on $X_D^{(m)}$, and $(A_\ell, i_\ell)/L$ be a pair as above, defined over some finite extension $L/\mathbb{Q}_\ell$, such that $Q_\ell = [(A_\ell, i_\ell)]$. The action of G_L on $T_p(A_\ell)$ gives rise to a Galois representation

$$\varrho_{(A_\ell, i), p} \colon G_L \longrightarrow \operatorname{Aut}_{R_m}\bigl(T_p(A_\ell)\bigr) \subseteq \operatorname{Aut}\bigl(T_p(A_\ell)\bigr) \simeq \operatorname{GSp}_4(\mathbb{Z}_p).$$

Recall our running assumption that the prime p be inert in E, let $\mathfrak{p} = pR_m$ denote the unique prime of E above p and $R_{m,\mathfrak{p}} = R_m \otimes \mathbb{Z}_p$ the completion of R_m along $\mathfrak{p}$.

The Galois group G_L acts on $T_p(A_\ell)$ by $R_{m,\mathfrak{p}}$-linear transformations, giving rise to a Galois representation

$$\varrho_{(A_\ell, i_\ell), \mathfrak{p}} \colon G_L \longrightarrow \operatorname{Aut}_{R_m}\bigl(T_p(A_\ell)\bigr) \simeq \operatorname{GL}_2(R_{m,\mathfrak{p}}),$$

which may be regarded as a subrepresentation of $\varrho_{(A_\ell, i_\ell), p}$. Likewise, the reduction of $\varrho_{(A_\ell, i_\ell), \mathfrak{p}}$ modulo $\mathfrak{p}$ yields a residual Galois representation

$$\overline{\varrho}_{(A_\ell, i_\ell), \mathfrak{p}} \colon G_L \longrightarrow \operatorname{Aut}_{R_m}(A_\ell[\mathfrak{p}]) \simeq \operatorname{GL}_2(\mathbb{F}_{p^2}).$$

Finally, consider again the canonical torsion subgroup $C_p = A_\ell[I(p)]$ of A_ℓ at p, now regarded as a subgroup of $A_\ell[\mathfrak{p}]$. The local quaternion algebra $B_{D,p} := B_D \otimes_{\mathbb{Q}} \mathbb{Q}_p$ can be written as $B_{D,p} = E_{\mathfrak{p}} + E_{\mathfrak{p}}\pi$, where $\pi^2 = p$ and $\pi\beta = {}^\tau\beta\pi$ for any $\beta \in E_{\mathfrak{p}}$, with τ the non-trivial element in $\operatorname{Gal}(E_{\mathfrak{p}}/\mathbb{Q}_p)$. Moreover, the local maximal order of $B_{D,p}$ is $\mathcal{O}_{D,p} = R_{m,\mathfrak{p}} + R_{m,\mathfrak{p}}\pi$ (*cf.* [Vig80, p. 33]) and $I(p)_p := I(p) \otimes_{\mathbb{Z}} \mathbb{Z}_p = \mathfrak{p}R_{m,\mathfrak{p}} + R_{m,\mathfrak{p}}\pi$.

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

Since $T_p(A_\ell)$ is a principal $\mathcal{O}_{D,p}$-module, we have

$$A_\ell[\mathfrak{p}] = T_p(A_\ell)/\mathfrak{p}T_p(A_\ell) \simeq \mathcal{O}_{D,p}/\mathfrak{p}\mathcal{O}_{D,p},$$
$$C_p = \mathcal{O}_{D,p}/I(p)_p \simeq R_{m,\mathfrak{p}}/\mathfrak{p}R_{m,\mathfrak{p}} \simeq \mathbb{F}_{p^2}.$$

Since $I(p)$ is the unique two-sided $\mathcal{O}_D$-ideal of reduced norm p, the action of G_L leaves $I(p)$ invariant. Moreover, G_L acts R_m-linearly on C_p, giving rise to a character

$$\alpha_{(A_\ell,i_\ell),\mathfrak{p}}\colon G_L \longrightarrow \mathrm{Aut}_{R_m}(C_p) \simeq \mathbb{F}_{p^2}^\times.$$

Let $P_\ell \in X_D(\overline{\mathbb{Q}}_\ell)$ be a preimage of Q_ℓ under π_m. Its field of moduli $\mathbb{Q}_\ell(P_\ell)$ is an extension of $\mathbb{Q}_\ell$ of degree at most 2, and it can be represented by the pair $(A_\ell,\iota_\ell)/\overline{\mathbb{Q}}_\ell$, where $\iota_\ell\colon \mathcal{O}_D \hookrightarrow \mathrm{End}(A_\ell)$ is a monomorphism such that $\iota_{\ell|R_m} = i_\ell$. Moreover, we have the following lemma.

Lemma 2.22 *The pair (A_ℓ,ι_ℓ) admits a model rational over any quadratic extension K_ℓ of $\mathbb{Q}_\ell$ containing $\mathbb{Q}_\ell(P_\ell)$.*

Proof Appealing to [Jor86, Theorem 1.1], it suffices to show that any quadratic extension K_ℓ of $\mathbb{Q}_\ell$ containing $\mathbb{Q}_\ell(P_\ell)$ splits the quaternion algebra B_D.

If $\ell \nmid D$, this is immediate as $B_D \otimes_{\mathbb{Q}} \mathbb{Q}_\ell \simeq \mathrm{M}_2(\mathbb{Q}_\ell)$. Assume therefore that $\ell \mid D$. Since we are assuming D is odd, the results in [JL85] (see also [Jor86, Theorem 0]) show that $X_D(\mathbb{Q}_\ell) = \varnothing$, so that $[\mathbb{Q}_\ell(P_\ell)\colon\mathbb{Q}_\ell] = 2$ and we only need to prove that $K_\ell = \mathbb{Q}_\ell(P_\ell)$ splits B_D. Indeed, by choosing any element $e \in \mathbb{Z}_\ell^\times \setminus \mathbb{Z}_\ell^{\times 2}$, up to isomorphism the only quadratic extensions of $\mathbb{Q}_\ell$ are $\mathbb{Q}_\ell(\sqrt{e})$, $\mathbb{Q}_\ell(\sqrt{\ell})$, and $\mathbb{Q}_\ell(\sqrt{e\ell})$. And all of them are subfields of $B_{D,\ell}$, since

$$B_{D,\ell} \simeq \mathbb{Q}_\ell(\sqrt{e}) + \mathbb{Q}_\ell(\sqrt{e})\pi,$$

where $\pi^2 = \ell$ and $\pi\beta = {}^\tau\beta\pi$ for all $\beta \in \mathbb{Q}_\ell(\sqrt{e})$, with $\tau \in \mathrm{Gal}\,(\mathbb{Q}_\ell(\sqrt{e})/\mathbb{Q}_\ell)$ the nontrivial automorphism (see [Vig80, Théorème II.1.3]). Thus in any case K_ℓ splits B_D. ■

Therefore, we can choose a quadratic extension K_ℓ of $\mathbb{Q}_\ell$ together with pairs (A_ℓ,ι_ℓ) and $(A, i_\ell = \iota_{\ell|R_m})$ defined over K_ℓ representing P_ℓ and Q_ℓ, respectively. With these choices, the following is an immediate consequence of Proposition 2.14 and Lemma 2.15.

Proposition 2.23 *With notations as before:*

(i) *There is a $\mathbb{F}_{p^2}$-basis of $A_\ell[\mathfrak{p}]$ with respect to which*

$$\overline{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}} = \begin{pmatrix} (\alpha_{(A_\ell,i_\ell),\mathfrak{p}})^p & 0 \\ * & \alpha_{(A_\ell,i_\ell),\mathfrak{p}} \end{pmatrix}.$$

(ii) *If $p \neq \ell$, then $\varrho^{12}_{(A_\ell,i_\ell),\mathfrak{p}}$ is unramified. In particular, $\alpha^{12}_{(A_\ell,i_\ell),\mathfrak{p}}$ is unramified.*

(iii) *If $\overline{\chi}_p\colon G_{\mathbb{Q}_\ell} \to \mathrm{Aut}(\mu_p) \simeq \mathbb{F}_p^\times$ denotes the reduction of the p-cyclotomic character, then $\mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p} \circ \alpha_{(A_\ell,i_\ell),\mathfrak{p}} = \overline{\chi}_{p|G_{K_\ell}}$. Hence, $\det(\overline{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}}) = \overline{\chi}_{p|G_{K_\ell}}$.*

As in the previous section, we can now apply the machinery introduced in Section 2.2 to attach Galois representations to the points in $X_D^{(m)}(\mathbb{Q}_\ell)$, even if they cannot be represented by an abelian surface defined over $\mathbb{Q}_\ell$.

Lemma 2.24 *Assume that A_ℓ has no complex multiplication by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. Then the pair (A_ℓ, i_ℓ) satisfies Hypothesis 2.3.*

Proof Suppose first that A_ℓ has no complex multiplication. In this case, the commutator of $R_m \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}(\sqrt{m}) = E$ in $\operatorname{End}^0(A_\ell) \simeq B_D$ is E itself, because it is a maximal subfield of B_D. Since E is a real quadratic field, its only units are ± 1.

Assume now that A_ℓ has complex multiplication by an order in an imaginary quadratic field $M/\mathbb{Q}$. We have $B_D \hookrightarrow \operatorname{End}^0(A_\ell) \simeq \mathrm{M}_2(M)$, and the commutator of $R_m \otimes_{\mathbb{Z}} \mathbb{Q} = E$ in $\operatorname{End}^0(A_v)$ is ME. It is easy to check that the only roots of unity in ME are ± 1, unless $M = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. ■

From now on, assume that A_ℓ has no complex multiplication by $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. In light of Lemma 2.24, we can attach to the point $Q_\ell = [(A_\ell, i_\ell)] \in X_D^{(m)}(\mathbb{Q}_\ell)$ Galois representations

$$\begin{aligned}
\varrho_{Q_\ell,\mathfrak{p}} \colon G_{\mathbb{Q}_\ell} &\longrightarrow \operatorname{Aut}_{R_m}\big(T_p(A_\ell)\big)/\{\pm 1\} \simeq \mathrm{GL}_2(R_{m,\mathfrak{p}})/\{\pm 1\},\\
\overline{\varrho}_{Q_\ell,\mathfrak{p}} \colon G_{\mathbb{Q}_\ell} &\longrightarrow \operatorname{Aut}_{R_m}(A_\ell[\mathfrak{p}])/\{\pm 1\} \simeq \mathrm{GL}_2(\mathbb{F}_{p^2})/\{\pm 1\},\\
\alpha_{Q_\ell,\mathfrak{p}} \colon G_{\mathbb{Q}_\ell} &\longrightarrow \operatorname{Aut}_{R_m}(C_p)/\{\pm 1\} \simeq \mathbb{F}_{p^2}^\times/\{\pm 1\},
\end{aligned}$$

extending $\varrho_{(A_\ell,i_\ell),\mathfrak{p}}$, $\overline{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}}$ and $\alpha_{(A_\ell,i_\ell),\mathfrak{p}}$, respectively.

As before, we write $\widetilde{\varrho}_{Q_\ell,\mathfrak{p}} \colon G_{\mathbb{Q}_\ell} \to \operatorname{Aut}_{R_m}(T_p(A_\ell))$ and $\widetilde{\alpha}_{Q_\ell,\mathfrak{p}} \colon G_{\mathbb{Q}_\ell} \to \mathbb{F}_{p^2}^\times$ for the lifts of $\varrho_{Q_\ell,\mathfrak{p}}$ and $\alpha_{Q_\ell,\mathfrak{p}}$ associated with a choice of $\mathbf{f}$ by (2.1). Again, these lifts are not homomorphisms in general, but their restrictions to G_{K_ℓ} coincide with $\varrho_{(A_\ell,i_\ell),\mathfrak{p}}$ and $\alpha_{(A_\ell,i_\ell),\mathfrak{p}}$, respectively, and for any $\sigma \in G_{\mathbb{Q}_\ell}$ it is easy to see that $\widetilde{\varrho}_{Q_\ell}(\sigma^2) = \pm\widetilde{\varrho}_{Q_\ell}(\sigma)^2$ and $\widetilde{\alpha}_{Q_\ell}(\sigma^2) = \pm\widetilde{\alpha}_{Q_\ell}(\sigma)^2$.

While both $\alpha_{(A_\ell,i_\ell),\mathfrak{p}}$ and $\alpha_{Q_\ell,\mathfrak{p}}$ descend to characters on $G_{K_\ell}^{\mathrm{ab}}$ and $G_{\mathbb{Q}_\ell}^{\mathrm{ab}}$, respectively, the map $\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}$ does not necessarily factor through $G_{K_\ell}^{\mathrm{ab}}$, though $\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}^2$ does.

From Proposition 2.23 we deduce the following corollary.

Corollary 2.25 *With the above notations:*

(i) *If $\ell \neq p$, $\alpha_{Q_\ell,\mathfrak{p}}^{12}$ is unramified. More precisely, we have $\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(I_\ell)^{24} = \{1\}$.*
(ii) $\det(\overline{\varrho}_{Q_\ell,\mathfrak{p}}(\sigma)) = \pm\overline{\chi}_p(\sigma)$ *for every $\sigma \in G_{\mathbb{Q}_\ell}$.*

To conclude with the basic properties of these representations, we now give an explicit description of $\overline{\varrho}_{Q_\ell,\mathfrak{p}}$ in terms of the character $\alpha_{Q_\ell,\mathfrak{p}}$.

To do so, choose a family of isomorphisms $\mathbf{f} = \{f_\sigma \colon {}^\sigma(A_\ell, i_\ell) \to (A_\ell, i_\ell)\}_{\sigma \in G_{\mathbb{Q}_\ell}}$ satisfying (2.3); this is possible because the field of moduli of (A_ℓ, i_ℓ) is $\mathbb{Q}_\ell$. For each $\sigma \in G_{\mathbb{Q}_\ell}$, the automorphism $B_D \to B_D$, $\beta \mapsto f_\sigma {}^\sigma\beta f_\sigma^{-1}$, is inner by the Noether–Skolem Theorem, hence there exists an element $\omega_\sigma \in \mathcal{O}_D$ such that $f_\sigma {}^\sigma\beta f_\sigma^{-1} = \omega_\sigma \beta \omega_\sigma^{-1}$ for all $\beta \in B_D$. Moreover, by the commutativity of (2.3), $\beta = \omega_\sigma \beta \omega_\sigma^{-1}$ for every $\beta \in E$, so that ω_σ belongs to the commutator of E in B_D, which is E itself because it is a maximal subfield of B_D. This shows that, for every $\sigma \in G_{\mathbb{Q}_\ell}$, ω_σ lies in $R_m = \mathcal{O}_D \cap E$, and

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

in this way we obtain a character

$$\psi\colon G_{\mathbb{Q}_\ell} \longrightarrow E^\times/\mathbb{Q}^\times, \quad \sigma \longmapsto \omega_\sigma.$$

Actually, write $\operatorname{Gal}(K_\ell/\mathbb{Q}_\ell) = \{1, \sigma_0\}$ and fix an isomorphism of pairs

$$f_0\colon ({}^{\sigma_0}A_\ell, {}^{\sigma_0}i_\ell) \longrightarrow (A_\ell, i_\ell).$$

We can extend f_0 to a collection of isomorphisms $\mathbf{f} = \{f_\sigma\}_{\sigma\in G_{\mathbb{Q}_\ell}}$ by setting $f_\sigma = \mathrm{id}$ if $\sigma \in G_{K_\ell}$ and $f_\sigma = f_0$ otherwise, and note that $\mathbf{f}$ satisfies (2.3). Accordingly, set $\omega_\sigma = 1$ if $\sigma \in G_{K_\ell}$ and $\omega_\sigma = \omega_0$ otherwise. Then the character ψ factors through the quotient $\operatorname{Gal}(K_\ell/\mathbb{Q}_\ell)$, thus we will regard

$$\psi\colon G_{\mathbb{Q}_\ell} \longrightarrow \{\pm 1\}$$

as a character with values in $\{\pm1\}$ that is trivial on $G_{K_\ell} \subseteq G_{\mathbb{Q}_\ell}$.

Lemma 2.26 *There exists a $\mathbb{F}_{p^2}$-basis of $A_\ell[\mathfrak{p}]$ with respect to which*

$$\begin{aligned} \overline{\varrho}_{Q_\ell,\mathfrak{p}}\colon\ G_{\mathbb{Q}_\ell} &\longrightarrow \mathrm{GL}_2(\mathbb{F}_{p^2})/\{\pm1\} \\ \sigma &\longmapsto \begin{pmatrix} \psi(\sigma)\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma)^p & 0 \\ * & \widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma)\end{pmatrix} \mod \pm 1. \end{aligned}$$

Proof Write $\mathcal{O}_{D,p} = R_{m,\mathfrak{p}} + R_{m,\mathfrak{p}}\cdot\pi$, and let $x \in A_\ell[\mathfrak{p}]$ be such that

$$A_\ell[\mathfrak{p}] = \mathcal{O}_{D,p}/\mathfrak{p}\mathcal{O}_{D,p}\cdot x = R_{m,\mathfrak{p}}/\mathfrak{p}R_{m,\mathfrak{p}}\cdot x + R_{m,\mathfrak{p}}/\mathfrak{p}R_{m,\mathfrak{p}}\cdot\pi(x).$$

We shall compute $\overline{\varrho}_{Q_\ell,\mathfrak{p}}$ with respect to the $\mathbb{F}_{p^2}$-basis $\{x, \pi(x)\}$ of $A_\ell[\mathfrak{p}]$. Fix an element $\sigma \in G_{\mathbb{Q}_\ell}$ and write

$$\widetilde{\varrho}_{Q_\ell,\mathfrak{p}}(\sigma)(x) = f_\sigma({}^\sigma x) = u_\sigma\cdot x + v_\sigma\cdot\pi(x)$$

for some $u_\sigma, v_\sigma \in R_{m,\mathfrak{p}}$, which are uniquely determined modulo $\mathfrak{p}$. In order to compute $\widetilde{\varrho}_{Q_\ell,\mathfrak{p}}(\sigma)(\pi(x))$, first note that

$$f_\sigma{}^\sigma\pi f_\sigma^{-1} = \omega_\sigma\pi\omega_\sigma^{-1} = \pi\,{}^\tau\omega_\sigma\omega_\sigma^{-1} = \psi(\sigma)\pi,$$

where $\tau \in \operatorname{Gal}(E_\mathfrak{p}/\mathbb{Q}_p)$ denotes the non-trivial automorphism. This shows that

$$f_\sigma\big({}^\sigma(\pi(x))\big) = \psi(\sigma)\pi\big(f_\sigma({}^\sigma x)\big) = \psi(\sigma)\pi\big(u_\sigma\cdot x + v_\sigma\cdot\pi(x)\big) = \psi(\sigma){}^\tau u_\sigma\cdot\pi(x).$$

Switching u_σ and $\psi(\sigma){}^\tau u_\sigma$ for ease of notation and reducing modulo ±1 and then modulo $\mathfrak{p}$, we finally obtain that

$$\overline{\varrho}_{Q_\ell,\mathfrak{p}}(\sigma) = \begin{pmatrix}\psi(\sigma)u_\sigma^p & 0 \\ v_\sigma & u_\sigma\end{pmatrix} \mod \pm 1.$$

We deduce that $\alpha_{Q_\ell,\mathfrak{p}}(\sigma) = u_\sigma \mod \pm 1$, so the lemma follows. ■

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

Notice that the proof of the lemma recovers Proposition 2.23(i), since the restriction of $\widetilde{\varrho}_{Q_\ell,\mathfrak{p}}$ and $\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}$ to G_{K_ℓ} coincides with $\varrho_{(A_\ell,i_\ell),\mathfrak{p}}$ and $\alpha_{(A_\ell,i_\ell),\mathfrak{p}}$, respectively. We can thus rewrite Proposition 2.23(i) by saying that, in a suitable $\mathbb{F}_{p^2}$-basis of $A_\ell[\mathfrak{p}]$,

$$\begin{aligned} \overline{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}}\colon\ G_{K_\ell} &\longrightarrow \mathrm{GL}_2(\mathbb{F}_{p^2}) \\ \sigma &\longmapsto \begin{pmatrix} \widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma)^p & 0 \\ * & \widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma) \end{pmatrix}. \end{aligned}$$

Now let $\sigma_\ell \in G_{\mathbb{Q}_\ell}$ be a Frobenius element at ℓ, *i.e.*, one whose reduction coincides with the Frobenius automorphism $\mathrm{Fr}_\ell \in \mathrm{Gal}\,(\overline{\mathbb{F}}_\ell/\mathbb{F}_\ell)$.

Corollary 2.27 *If $\ell \neq p$ and $\sigma_\ell \in G_{K_\ell}$, then the characteristic polynomial $\Phi_\ell(T) \in R_m[T]$ of $\varrho_{(A_\ell,i_\ell),\mathfrak{p}}(\sigma_\ell)$ satisfies the congruence*

$$\Phi_\ell(T) \equiv T^2 - \left(\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell) + \ell\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)^{-1}\right) T + \ell \quad \bmod \mathfrak{p}.$$

Proof If $\sigma_\ell \in G_{K_\ell}$, then by the above observation, $\Phi_\ell(T)$ satisfies the congruence

$$\Phi_\ell(T) \equiv T^2 - \left(\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell) + \widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)^p\right) T + N_{\mathbb{F}_{p^2}/\mathbb{F}_p}\left(\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)\right) \quad \bmod \mathfrak{p}.$$

Also, from Proposition 2.23(iii), $\det(\overline{\varrho}_{(A_\ell,i_\ell),\mathfrak{p}}(\sigma_\ell)) = \ell$, so we can write

$$\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)^p\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell) = \ell \in \mathbb{F}_{p^2}^\times,$$

and therefore the statement follows noting that

$$\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell) + \widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)^p \equiv \widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell) + \ell\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma_\ell)^{-1} \quad \bmod \mathfrak{p}. \qquad \blacksquare$$

Remark 2.28 We have already seen that, for a prime $\ell \neq p$, the character $\alpha^{12}_{Q_\ell,\mathfrak{p}}$ is unramified. We now make an observation for the case $\ell = p$. First, recall that the local Artin reciprocity map gives us an isomorphism $w_p\colon \mathbb{Z}_p^\times \overset{\simeq}{\to} I_p^{\mathrm{ab}} \subseteq G^{\mathrm{ab}}_{\mathbb{Q}_p}$. Also, the character $\alpha_{Q_p,\mathfrak{p}}$ factors through $\alpha_{Q_p,\mathfrak{p}}\colon G^{\mathrm{ab}}_{\mathbb{Q}_p} \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$. Therefore, we can consider the composition

$$\alpha_{Q_p,\mathfrak{p}} \circ w_p\colon \mathbb{Z}_p^\times \underset{\simeq}{\xrightarrow{w_p}} I_p^{\mathrm{ab}} \subseteq G^{\mathrm{ab}}_{\mathbb{Q}_p} \xrightarrow{\alpha_{Q_p,\mathfrak{p}}} \mathbb{F}_{p^2}^\times/\{\pm 1\},$$

which is a continuous homomorphism. The image of $\mathbb{Z}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$ under $\alpha_{Q_p,\mathfrak{p}} \circ w_p$ is then a cyclic subgroup of $\mathbb{F}_{p^2}^\times/\{\pm 1\}$, but since $\alpha_{Q_p,\mathfrak{p}} \circ w_p$ must be trivial on the pro-p-part, $\alpha_{Q_p,\mathfrak{p}} \circ w_p(\mathbb{Z}_p^\times)$ is indeed a cyclic subgroup of $\mathbb{F}_p^\times/\{\pm 1\} \simeq \mathbb{Z}/\frac{p-1}{2}\mathbb{Z}$ that we identify with the unique subgroup of index 2 of $\mathbb{Z}/(p-1)\mathbb{Z}$. Therefore, for any $x \in \mathbb{Z}_p^\times$,

$$\alpha_{Q_p,\mathfrak{p}}(w_p(x))^2 = \alpha_{Q_p,\mathfrak{p}}(w_p(x^2)) \in \mathbb{F}_p^\times/\{\pm 1\}.$$

If we take any representative $\tau \in I_p$ of $w_p(x) \in I_p^{\mathrm{ab}}$, this implies that $\alpha_{Q_p,\mathfrak{p}}(\tau^2) \in \mathbb{F}_p^\times/\{\pm 1\}$. As a consequence, $\widetilde{\alpha}_{Q_p,\mathfrak{p}}(\tau^2) \in \mathbb{F}_p^\times$ for any $\tau \in I_p \subseteq G_{\mathbb{Q}_p}$.

3 Proof of Theorem 1.1

Let $(A,\iota)/\bar{k}$ be an abelian surface with multiplication by $\mathcal{O}_D$. Fix an odd prime factor p of D, and recall that $C_p = A[I(p)]$, the canonical torsion subgroup of A at p, is a cyclic $\mathcal{O}_D$-module isomorphic to $\mathcal{O}_D/I(p) \simeq \mathbb{F}_{p^2}$.

We can consider the moduli problem of classifying isomorphism classes of triplets (A,ι,x_p), where (A,ι) is an abelian surface with multiplication by $\mathcal{O}_D$ and x_p is a generator of its canonical torsion subgroup C_p, as an $\mathcal{O}_D$-module. Here, by an isomorphism $(A,\iota,x_p)\overset{\simeq}{\to}(A',\iota',x'_p)$ we mean an isomorphism of pairs $(A,\iota)\to(A',\iota')$ sending x_p to x'_p. The solution $X_{D,p}/\mathbb{Q}$ to this moduli problem leads to a cyclic Galois covering $X_{D,p}\to X_D$, with automorphism group $\operatorname{Aut}(X_{D,p}/X_D)$ isomorphic to $\mathbb{F}_{p^2}^{\times}/\{\pm1\}\simeq\mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$. The curve $X_{D,p}/\mathbb{Q}$ is not geometrically connected. If ζ_p denotes a primitive p-th root of unity, then $X_{D,p}\times_{\mathbb{Q}}\mathbb{Q}(\zeta_p)$ is the disjoint union of $p-1$ geometrically irreducible curves which are conjugate by the action of $\operatorname{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ (see [Sko05, dVP] for details).

Jordan constructed explicitly the maximal étale subcovering $Z_{D,p}\to X_D$ of the covering $X_{D,p}\to X_D$, commonly referred to as the *Shimura covering*. Its order (for $p\neq 2$) is $(p^2-1)/2e$ for $e=1,2,3$ or 6, depending on the arithmetic of B_D (see [Jor81, p. 108]). In particular, the quotient of $X_{D,p}$ by $\mathbb{Z}/6\mathbb{Z}$ leads to a subcovering $f_p\colon Y_{D,p}\to X_D$ of the Shimura covering $Z_{D,p}/X_D$, hence it is étale, and

$$\operatorname{Aut}(Y_{D,p}/X_D)\simeq\mathbb{F}_{p^2}^{\times 12}\simeq\mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}.$$

This way, $Y_{D,p}$ is an X_D-torsor under the constant group scheme $\mathbb{F}_{p^2}^{\times 12}\simeq\mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$ (see [Sko05, Corollary 1.2]). Therefore, by specialization of $Y_{D,p}$ there is attached to each point $P\in X_D(k)$ a continuous character $\phi_P\colon G_k\to\mathbb{F}_{p^2}^{12}$ by which the Galois group G_k acts on the fibre of $f_p\colon Y_{D,p}\to X_D$ at P.

Assume for example that $K/\mathbb{Q}$ is an imaginary quadratic field, let v be a place of K over a prime ℓ and let (A_v,ι_v) be a pair corresponding to a K_v-point $P_v\in X_D(K_v)$. Assuming that K splits B_D, K_v also splits B_D, so that (A_v,ι_v) admits a model rational over K_v by [Jor86, Theorem 1.1]. Then, by the modular interpretation of the Galois covering $X_{D,p}\to X_D$, the canonical isogeny character $\alpha_{(A_v,\iota_v)}\colon G_{K_v}\to\operatorname{Aut}_{\mathcal{O}_D}(C_p)\simeq\mathbb{F}_{p^2}^{\times}$ at p satisfies $\phi_{P_v}=\alpha_{(A_v,\iota_v)}^{12}$ (see [Sko05, Lemma 2.1]). Exploiting this relation and performing descent to the torsor $f_p\colon Y_{D,p}\to X_D$, Skorobogatov proved in [Sko05, Theorem 3.1] the following result, which strengthens [Jor86, Theorem 6.3]. Here, $P'_1(q)$ is a finite set of primes depending on q, defined in a similar way to $P_1(q)$ (see [Sko05] for details).

Theorem 3.1 (Skorobogatov) *Let K be an imaginary quadratic field in which a prime q is ramified, and let B_D be a quaternion algebra in $\mathcal{B}_1(q)$ whose discriminant is divisible by a prime $p\notin P'_1(q)$, $p\geq 5$, and which is split by K. Then $X_D(\mathbb{A}_K)^{\mathrm{Br}}=\varnothing$.*

Now assume that K does not necessarily splits B_D, and construct an extension L_w/K_v as in the previous section, over which the pair (A_v,ι_v) corresponding to P_v admits a rational model. We can assume that (A_v,ι_v) is defined over L_w. Then, again because of the modular interpretation of $X_{D,p} \to X_D$ we have that $\phi_{P_v|G_{L_w}} = \alpha^{12}_{(A_v,\iota_v)}$, where now $\alpha_{(A_v,\iota_v)}\colon G_{L_w} \to \operatorname{Aut}_{\mathcal{O}_D}(C_p) \simeq \mathbb{F}^{\times}_{p^2}$.

In order to avoid the restriction to G_{L_w}, we can use the character $\alpha_{P_v}\colon G_{K_v} \to \mathbb{F}^{\times}_{p^2}/\{\pm 1\}$ attached to the point P_v.

Lemma 3.2 *For any $\sigma \in G_{K_v}$, $\widetilde{\alpha}_{P_v}(\sigma)^{24} = \phi_{P_v}(\sigma)^2$. In terms of α_{P_v}, we have*

$$\alpha_{P_v}(\sigma)^{12} = \phi_{P_v}(\sigma) \mod \pm 1, \quad \forall \sigma \in G_{K_v}.$$

Proof Since $\widetilde{\alpha}_{P_v}$ restricted to G_{L_w}, coincides with $\alpha_{(A_v,\iota_v)}$, we can write $(\widetilde{\alpha}_{P_v|G_{L_w}})^{12} = \phi_{P_v|G_{L_w}}$. Therefore, if $\sigma \in G_{K_v}$, then

$$\widetilde{\alpha}_{P_v}(\sigma)^{24} = \big(\pm\widetilde{\alpha}_{P_v}(\sigma^2)\big)^{12} = \big(\widetilde{\alpha}_{P_v|G_{L_w}}(\sigma^2)\big)^{12} = \phi_{P_v|G_{L_w}}(\sigma^2) = \phi_{P_v}(\sigma)^2,$$

so the lemma follows. ■

Together with Corollary 2.16, we obtain the following corollary.

Corollary 3.3 *For $p \neq \ell$, $\phi^2_{P_v}$ is unramified.*

We are now in position to prove Theorem 1.1, which will follow immediately from Theorem 3.4 and Corollary 3.5. The finite set of primes $P_1(q)$ and the set of indefinite algebras $\mathcal{B}_1(q)$ associated with a prime q were defined in the introduction.

Theorem 3.4 *Let K be an imaginary quadratic field in which a prime q is ramified. If $B_D \in \mathcal{B}_1(q)$ is such that D is divisible by a prime $p \notin P_1(q)$, $p \geq 5$, and p is not split in K, then $X_D(K)$ consists only of CM-points.*

Proof Let $p \notin P_1(q)$, $p \geq 5$, be a prime factor of D such that p is not split in K, and let $\mathfrak{p}$ be the unique prime of K above p. Let also $K'/\mathbb{Q}$ be a quadratic extension splitting the algebra B_D and such that q is not inert in K'. If $D = p_1 \cdots p_{2r}$, the existence of such a K' reduces to the existence of a discriminant d such that $\big(\frac{d}{p_i}\big) \neq 1$, $i = 1, \dots, 2r$ and $\big(\frac{d}{q}\big) \neq -1$. By Čebotarev's Theorem, there are infinitely many such d.

Assume that $P \in X_D(K)$ is a K-rational point that has no complex multiplication by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. By the modular interpretation of X_D, we can choose an abelian surface $(A,\iota)/\overline{K}$ with multiplication by $\mathcal{O}_D$ whose field of moduli is K. By means of the diagonal embedding $X_D(K) \hookrightarrow X_D(\mathbb{A}_K)$, the point P defines a sequence of local points $\{P_v\}_v \in X_D(\mathbb{A}_K)$. For each one of these points, say $P_v \in X_D(K_v)$, we can choose the same abelian surface (A,ι) representing it, now regarded as an abelian surface over $\overline{K}_v$. However, let v' be a place of K' above the same rational prime ℓ lying below v and, with the same notations as before, consider the composite field $L_w := K_v \cdot K'_{v'}$. Then, since $K'_{v'}$ splits B_D, we can choose a model (A_v,ι_v) of $(A,\iota)/\overline{K}_v$ rational over L_w. In particular, $P_v = [(A_v,\iota_v)]$. Note that (A_v,ι_v) has no complex multiplication by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$.

The global character $\phi\colon G_K \to \mathbb{F}^{\times 12}_{p^2}$ obtained by specialization of the torsor f_p at P restricts to each one of the local characters ϕ_{P_v} attached to each point P_v on G_{K_v}. By

Corollary 3.3 we have that ϕ^2 is unramified away from $\mathfrak{p}$. Moreover, the restriction of ϕ_{P_v} to G_{L_w} coincides with the Galois representation $\alpha^{12}_{(A_v,\iota_v)}$.

On the other hand, let $\mathfrak{q}$ be the unique prime of K above q, and let $\sigma_{\mathfrak{q}} \in G_{K_{\mathfrak{q}}}$ be a Frobenius element at $\mathfrak{q}$, *i.e.*, an element inducing the Frobenius automorphism $\mathrm{Fr}_q \in \mathrm{Gal}\,(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ under reduction. We claim that $\widetilde{\alpha}_{P_{\mathfrak{q}}}(\sigma_{\mathfrak{q}}^2)^{24} = q^{24}$.

By global class field theory, we have an exact sequence

$$\prod_v U_v \longrightarrow G_K^{\mathrm{ab}} \longrightarrow \mathrm{Cl}(K) \longrightarrow 0,$$

where U_v is the group of units of the ring of integers of K_v and $U_v \to G_K^{\mathrm{ab}}$ is defined by the local Artin map w_v. The idèle in $\prod_v U_v$ all of whose components equal $1/q$ except for the component at $\mathfrak{q}$, which equals π^2/q with π a uniformizer at $\mathfrak{q}$, maps to $\mathrm{Frob}_{\mathfrak{q}}^2$, the square of a Frobenius element $\mathrm{Frob}_{\mathfrak{q}} \in G_K^{\mathrm{ab}}$ at $\mathfrak{q}$. Then $\sigma_{\mathfrak{q}}^2 \cdot \mathrm{Frob}_{\mathfrak{q}}^{-2} \in I_{K_{\mathfrak{q}}}$ and $\phi^2(\sigma_{\mathfrak{q}}^2) = \phi^2(\mathrm{Frob}_{\mathfrak{q}}^2)$, since ϕ^2 is unramified away from $\mathfrak{p}$. But now observe that

$$\phi^2(\sigma_{\mathfrak{q}}^2) = \phi^2_{P_{\mathfrak{q}}}(\sigma_{\mathfrak{q}}^2) = \widetilde{\alpha}_{P_{\mathfrak{q}}}(\sigma_{\mathfrak{q}}^2)^{24},$$
$$\phi^2(\mathrm{Frob}_{\mathfrak{q}}^2) = \phi^2_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(q^{-1})) = \widetilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(q^{-1}))^{24},$$

so that our claim is reduced to proving that $\widetilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(q^{-1}))^{24} = q^{24}$. There are two cases:

(a) p is inert in K. In this case, the group of units $U_{\mathfrak{p}}$ is an extension of $\mathbb{F}_{p^2}^{\times}$ by a pro-p-group. The homomorphism $\alpha_{P_{\mathfrak{p}}} \circ w_{\mathfrak{p}} \colon U_{\mathfrak{p}} \to I_{\mathfrak{p}}^{\mathrm{ab}} \to \mathbb{F}_{p^2}^{\times}/\{\pm 1\}$ must be trivial on the pro-p-part, so that $\alpha_{P_{\mathfrak{p}}} \circ w_{\mathfrak{p}}$ factors through a homomorphism $\mu\colon \mathbb{F}_{p^2}^{\times} \to \mathbb{F}_{p^2}^{\times}/\{\pm 1\}$. If $a \in \mathbb{F}_{p^2}^{\times}$ is a generator of the cyclic group $\mathbb{F}_{p^2}^{\times}$, then the class $[a]$ of a in $\mathbb{F}_{p^2}^{\times}/\{\pm 1\}$ is a generator of $\mathbb{F}_{p^2}^{\times}/\{\pm 1\}$ as well, so that the homomorphism μ is determined by an integer c (uniquely determined modulo $(p^2-1)/2$) such that $\mu(a) = [a]^{-c}$.

Then if we denote by $\widetilde{u} \in \mathbb{F}_{p^2}^{\times}$ the reduction modulo $\mathfrak{p}$ of $u \in U_{\mathfrak{p}}$, we have

$$\alpha_{P_{\mathfrak{p}}}\big(w_{\mathfrak{p}}(u)\big) = \mu(\widetilde{u}) = [\widetilde{u}]^{-c}.$$

In particular, $\widetilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u)) = \pm\widetilde{u}^{-c}$.

On the other hand, from [Ser72, Prop. 3, 8] we have $\chi_p(w_{\mathfrak{p}}(u)) = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\widetilde{u})^{-1}$ for every $u \in U_{\mathfrak{p}}$. Thus, applying (2.2),

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}\big(\widetilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u))^2\big) = \chi_p(w_{\mathfrak{p}}(u))^2 = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\widetilde{u})^{-2} = \widetilde{u}^{-2(p+1)} \in \mathbb{F}_p^{\times},$$

and we also have

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}\big(\widetilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(u))^2\big) = N_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\widetilde{u}^{-2c}) = \widetilde{u}^{-2c(p+1)} \in \mathbb{F}_p^{\times}.$$

From this we get that $2c \equiv 2 \bmod p-1$. Therefore, $\widetilde{\alpha}_{P_{\mathfrak{p}}}(w_{\mathfrak{p}}(q^{-1}))^{24} = q^{24}$ as claimed.

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

(b) p is ramified in K. In this case, $U_\mathfrak{p}$ is an extension of $\mathbb{F}_p^\times$ by a pro-p-group. Hence, the homomorphism $\alpha_{P_\mathfrak{p}} \circ w_\mathfrak{p}\colon U_\mathfrak{p} \to I_\mathfrak{p}^{\mathrm{ab}} \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$ factors now through a homomorphism $\mu\colon \mathbb{F}_p^\times \to \mathbb{F}_{p^2}^\times/\{\pm 1\}$. Then, $\alpha_{P_\mathfrak{p}}(w_\mathfrak{p}(U_\mathfrak{p}))$ must be contained in the unique cyclic subgroup of order $p-1$ of $\mathbb{F}_{p^2}^\times/\{\pm 1\}$. In particular, for every $u \in U_\mathfrak{p}$, $\alpha_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2$ lies in $\mathbb{F}_p^\times/\{\pm 1\} \subseteq \mathbb{F}_{p^2}^\times/\{\pm 1\}$, which is the unique subgroup of order $(p-1)/2$ of $\mathbb{F}_{p^2}^\times/\{\pm 1\}$.

So, if we again denote by $\widetilde{u} \in \mathbb{F}_p^\times$ the reduction of u modulo $\mathfrak{p}$, there exists an integer c, uniquely determined modulo $(p-1)/2$ such that $\alpha_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2 = [\widetilde{u}]^{-c}$, where $[\widetilde{u}]$ denotes the class of $\widetilde{u}$ in $\mathbb{F}_p^\times/\{\pm 1\}$. In particular, $\widetilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2 = \pm\widetilde{u}^{-c}$.

Now, [Ser72, Prop. 3, 8] implies $\chi_p(w_\mathfrak{p}(u)) = N_{\mathbb{F}_p/\mathbb{F}_p}(\widetilde{u})^{-2} = \widetilde{u}^{-2}$, so that applying (2.2) we get

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}\big(\widetilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2\big) = \chi_p\big(w_\mathfrak{p}(u)\big)^2 = \widetilde{u}^{-4}.$$

On the other hand,

$$N_{\mathbb{F}_{p^2}/\mathbb{F}_p}\big(\widetilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2\big) = \big(\pm\widetilde{u}^{-c}\big)^2 = \widetilde{u}^{-2c},$$

since $\widetilde{\alpha}_{P_\mathfrak{p}}(w_\mathfrak{p}(u))^2 \in \mathbb{F}_p^\times$. Hence, $2c \equiv 4 \bmod p-1$. We deduce that

$$\widetilde{\alpha}_{P_\mathfrak{p}}\big(w_\mathfrak{p}(q^{-1})\big)^{24} = q^{24} \in \mathbb{F}_p^\times,$$

and the claim also follows in this case.

Now, since q is not inert in K', if $\mathfrak{q}'$ is a prime of K' above q, the residue field of $K'_{\mathfrak{q}'}$ is $\mathbb{F}_q$. As a consequence, the residue field of $L_\mathfrak{Q} = K_\mathfrak{q} \cdot K'_{\mathfrak{q}'}$ is also $\mathbb{F}_q$.

Then, since $A_\mathfrak{q}/L_\mathfrak{Q}$ has potential good reduction, following the construction of Serre and Tate [ST68, p. 498] we get an abelian surface $\widetilde{A}_\mathfrak{q}$ defined over $\mathbb{F}_q$ such that the quaternion algebra $B_D \subseteq \mathrm{End}^0_{L_\mathfrak{q}}(A_\mathfrak{q})$ embeds in $\mathrm{End}^0_{\mathbb{F}_q}(\widetilde{A}_\mathfrak{q})$. Moreover, $\sigma_\mathfrak{q} \in G_{L_\mathfrak{Q}}$, and its action on the Tate modules $T_p(A_\mathfrak{q})$ and $T_p(\widetilde{A}_\mathfrak{q})$ is the same.

As in [Jor86, §5], the trace of $\overline{\varrho}_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n)$ is the reduction modulo p of an integer $a_{\mathfrak{q},n}$, $|a_{\mathfrak{q},n}| \leq 2q^{n/2}$, such that

$$a_{\mathfrak{q},n} \bmod p = \mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}\big(\alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n)\big) = \alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n) + q^n\alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^n)^{-1}.$$

In particular, if $a_\mathfrak{q} := a_{\mathfrak{q},2}$, then

$$a_\mathfrak{q} \bmod p = \alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^2) + q^2\alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})}(\sigma_\mathfrak{q}^2)^{-1}.$$

Since $\alpha_{(A_\mathfrak{q},\iota_\mathfrak{q})} = \widetilde{\alpha}_{P_\mathfrak{q}|G_{L_\mathfrak{Q}}}$ and $\sigma_\mathfrak{q} \in G_{L_\mathfrak{Q}}$, using the claim proved above we can write

$$a_\mathfrak{q} \bmod p = \widetilde{\alpha}_{P_\mathfrak{q}}(\sigma_\mathfrak{q}^2) + q^2\widetilde{\alpha}_{P_\mathfrak{q}}(\sigma_\mathfrak{q}^2)^{-1} = q(\zeta + \zeta^{-1}),$$

where $\zeta = \frac{\widetilde{\alpha}_{P_\mathfrak{p}}(\sigma_\mathfrak{q}^2)}{q}$ is a 24-th root of unity. Computing the possible values of $q(\zeta+\zeta^{-1})$ we get that either $a_\mathfrak{q} \mod p = 0$ or p divides

$$a_\mathfrak{q} \pm q,\ a_\mathfrak{q}^2 - 2q^2,\ a_\mathfrak{q}^2 - 3q^2,\ a_\mathfrak{q} \pm 2q, \text{ or } a_\mathfrak{q}^4 - 4a_\mathfrak{q}^2q^2 + q^4.$$

Since $|a_{\mathfrak{q}}| \leq 2q$, the hypothesis $p \notin P_1(q)$ implies that actually

$$a_{\mathfrak{q}} = 0, \pm q, \pm\sqrt{2}q, \pm\sqrt{3}q, \pm 2q, \text{ or } \pm q\sqrt{2 \pm \sqrt{3}}.$$

But, since $a_{\mathfrak{q}}$ is an integer, the only possibilities are $a_{\mathfrak{q}} = 0, \pm q$, or $\pm 2q$. Now, if we let ξ be a 48-th root of unity such that $\xi^2 = \zeta$, the trace of the characteristic polynomial of $\overline{\varrho}_{(A_{\mathfrak{q}},\iota_{\mathfrak{q}})}(\sigma_{\mathfrak{q}})$ is the reduction modulo p of an integer $b_{\mathfrak{q}} := a_{\mathfrak{q},1}$ of absolute value at most $2\sqrt{q}$ with $b_{\mathfrak{q}} \bmod p = \sqrt{q}(\xi + \xi^{-1})$. Applying the Honda–Tate theory (see [Jor86, Theorem 2.1]) for both cases, we get the following list of possibilities:

- $a_{\mathfrak{q}} = 0, q = 2$: then $\mathbb{Q}(\sqrt{-1})$ splits B_D;
- $a_{\mathfrak{q}} = q = 3$: then $\mathbb{Q}(\sqrt{-3})$ splits B_D;
- $a_{\mathfrak{q}} = -2q$: then $\mathbb{Q}(\sqrt{-q})$ splits B_D.

In any case, we obtain a contradiction with the assumption that $B_D \in \mathcal{B}_1(q)$, hence the statement follows. ■

Directly from the above proof, we see that for a pair (B_D, K) satisfying the hypotheses of Theorem 3.4, $X_D(K)$ contains only points with CM by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$. Thus, in order to give sufficient conditions for the emptiness of $X_D(K)$, it remains to study the sets $X_D(K) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-1}))$ and $X_D(K) \cap \mathrm{CM}(\mathbb{Q}(\sqrt{-3}))$. Here, for an imaginary quadratic field L, $\mathrm{CM}(L)$ denotes the union of the sets $\mathrm{CM}(R) \subseteq X_D(\overline{\mathbb{Q}})$, where R ranges through the quadratic orders in L.

In all cases where we can prove that $X_D(K) = \varnothing$, it is almost immediate from the proof of Theorem 3.4 that this is accounted for by the Brauer–Manin obstruction.

Corollary 3.5 *Assume that the pair (B_D, K) satisfies the hypotheses of Theorem 1.1.*

(i) *If $K \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \varnothing$.*

(ii) *If $K = \mathbb{Q}(\sqrt{-1})$ and there exists a prime $\ell \equiv 1 \bmod 4$ dividing D, then $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \varnothing$.*

(iii) *If $K = \mathbb{Q}(\sqrt{-3})$ and there exists a prime $\ell \equiv 1 \bmod 3$ dividing D, then $X_D(K) = X_D(\mathbb{A}_K)^{\mathrm{Br}} = \varnothing$.*

Proof The existence of CM points on Shimura curves and their fields of definition are well characterized and described. Using the results from [GR06, §5], for example, it immediately follows that $X_D(K)$ is empty under the hypotheses of the statement.

Now, assume that $X_D(\mathbb{A}_K) \neq \varnothing$, as otherwise there is nothing to prove. Assume there exists a sequence of local points $P_v \in X_D(K_v)$, one for each nonarchimedean place v of K, and let $\phi_{P_v}\colon G_{K_v} \to \mathbb{F}_{p^2}^{\times 12}$ denote the local character given by specialization of the torsor f_p at P_v. Assume that all these local characters are the restriction of a global character $\phi\colon G_K \to \mathbb{F}_{p^2}^{\times 12}$. For each point P_v, we can choose a pair $(A_v, \iota_v)/\overline{K}_v$ with field of moduli K_v representing it, and then the proof of Theorem 3.4 applies verbatim to yield a contradiction, showing that such a sequence of local points cannot exist. Therefore, the descent subset $X_D(\mathbb{A}_K)^{f_p}$ associated with the torsor f_p is empty, and applying the main theorem of descent theory of Colliot-Thélène and Sansuc (see [Sko01, Theorem 6.1.2]), the statement follows. ■

Since the hypotheses of Corollary 3.5 are explicit and computable, we can produce pairs (B_D, K) such that K is deficient for X_D, that is, such that $X_D(K) = \varnothing$. Using the

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

work of Jordan and Livné in [JL85], we can even give explicit sufficient conditions for X_D to be a counterexample to the Hasse principle over K. Let us recall first some notations from [JL85].

For an order R in an imaginary quadratic field L, let us set

$$S(R) = \frac{h(R)}{[R^\times : \mathbb{Z}^\times]} \prod_{\substack{q \mid D \\ q \text{ prime}}} \left(1 - \left\{\frac{R}{q}\right\}\right),$$

where $h(R)$ is the class number of R, and for a rational prime q,

$$\left\{\frac{R}{q}\right\} = \begin{cases} 1 & \text{if } q \mid \operatorname{cond}(R), \\ \left(\frac{L}{q}\right) & \text{otherwise.} \end{cases}$$

Note that $S(R) \neq 0$ if and only if the conductor of R is prime to D and L splits B_D. Then define

$$\Sigma_\ell(D) = \frac{1}{2} \sum_{\substack{s \in \mathbb{Z} \\ s^2 < 4\ell}} \sum_R S(R), \tag{3.1}$$

where R runs through the set of orders in imaginary quadratic fields L such that R contains the roots of $x^2 + sx + \ell$.

Corollary 3.6 *Let $g = g(X_D)$ be the genus of X_D. Under the hypotheses of Corollary 3.5, assume also that the following conditions hold:*

(i) $\Sigma_\ell(D) \neq 0$ *for every prime* $\ell < 4g^2$, $\ell \nmid D$, ℓ *not inert in* K*;*

(ii) *for every prime* $\ell \mid D$ *ramifying in* K*, either* $\mathbb{Q}(\sqrt{-\ell})$ *splits* B_D *or* $\ell = 2$ *and* $\mathbb{Q}(\sqrt{-1})$ *splits* B_D*;*

(iii) *for every prime* $\ell \mid D$ *splitting in* K*, either* $D = 2\ell$ *with* $\ell \equiv 1 \mod 4$*, or* $\ell = 2$ *and* $D = 2q_1 \cdots q_{2r-1}$ *with primes* $q_i \equiv 3 \mod 4$ *not splitting in* K*.*

Then X_D is a counterexample to the Hasse principle over K.

Proof The statement follows directly from the work in [JL85], together with the fact that $X_D(\mathbb{Q}_\ell) \neq \varnothing$ for every prime $\ell > 4g^2$, by Weil's bound. ■

Table 1 in the introduction collects some counterexamples to the Hasse principle arising from the above corollary that are given by exceptional pairs (B_D, K), that is, for which $K = \mathbb{Q}(\sqrt{d})$ fails to split B_D.

4 Proof of Theorem 1.2

We now turn our attention to the Atkin–Lehner quotients $X_D^{(m)}$, for which we need to construct a suitable étale covering in order to apply similar techniques to those used by Skorobogatov.

As in Section 2.4, we place ourselves under Assumption 2.19, so that $D = pm$ is odd and $\left(\frac{m}{p}\right) = -1$. Towards the proof of Theorem 1.2, we assume moreover

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

that $p \equiv 3 \mod 4$. By Ogg's formula for the number of fixed points of ω_m, this implies that ω_m is fixed point free, hence the natural quotient map $\pi_m \colon X_D \to X_D^{(m)}$ is unramified. Applying descent to this double cover of $X_D^{(m)}$, some sufficient conditions for the emptiness of $X_D^{(m)}(\mathbb{Q})$ were found in [RSY05].

Here we shall construct an étale covering of $X_D^{(m)}$ from the covering $Y_{D,p} \to X_D$ defined in the previous section. The basic idea behind our construction is that ω_m can be lifted to an involution $\widehat{\omega}_m$ on $X_{D,p}$, which induces in turn an involution lifting ω_m on each intermediate covering of $X_{D,p} \to X_D$. A detailed study of the group of modular automorphisms of the curve $X_{D,p}$ provides a criterion to construct cyclic étale Galois coverings of Atkin–Lehner quotients of X_D from the intermediate coverings of $X_{D,p} \to X_D$ (see [dVP]), but for the purposes of this paper we can proceed in a simpler way as follows.

By virtue of Lemma 2.18, we can choose a twist χ_m of norm m as a representative of ω_m in $\mathrm{N}_{B^\times_{D,+}}(\mathcal{O}_D^1)$. Then $\chi_m^2 = m$ and $\mathrm{w}_m = \chi_m \alpha$ for some $\alpha \in \mathcal{O}_D^\times$ of reduced norm -1. The Atkin–Lehner involution $\omega_m \colon X_D \to X_D$ does not depend on this choice, and notice that now the monomorphism ι_{ω_m} is described by $\iota_{\omega_m}(\beta) = \iota(\chi_m^{-1}\beta\chi_m)$ for all $\beta \in \mathcal{O}_D$. Having fixed this choice, we define an automorphism $\widehat{\omega}_m \colon X_{D,p} \to X_{D,p}$ using the moduli interpretation of $X_{D,p}$ by the rule

$$P = \big[(A, \iota, x_p)\big] \longmapsto \widehat{\omega}_m(P) = \big[(A, \iota_{\omega_m}, x_p)\big]\,. \tag{4.1}$$

Since χ_m normalizes $\mathcal{O}_D$, observe that x_p is still a generator of the canonical torsion subgroup $C_p \subseteq A[p]$ when we regard it as an $\mathcal{O}_D$-module via ι_{ω_m}, hence $\widehat{\omega}_m$ is well defined. Moreover, the condition $\chi_m^2 = m$ implies that $\widehat{\omega}_m$ certainly is an involution lifting ω_m to $X_{D,p}$. In fact, it follows from standard moduli considerations that $\widehat{\omega}_m$ is a rational involution of the curve $X_{D,p}/\mathbb{Q}$.

Let us denote by $X_{D,p}^{(m)} := X_{D,p}/\langle\widehat{\omega}_m\rangle$ the quotient of $X_{D,p}$ by the action of the involution $\widehat{\omega}_m$. By construction, we have a commutative diagram

$$\begin{tikzcd}
X_{D,p} \arrow[r] \arrow[d] & X_D \arrow[d] \\
X_{D,p}^{(m)} \arrow[r] & X_D^{(m)},
\end{tikzcd}$$

where the horizontal arrows are covering maps. It is clear from (4.1) that $\widehat{\omega}_m$ commutes with every automorphism $\alpha \in \mathrm{Aut}(X_{D,p}/X_D)$. As a consequence, $X_{D,p}^{(m)} \to X_D^{(m)}$ is a cyclic Galois covering with automorphism group

$$\mathrm{Aut}(X_{D,p}^{(m)}/X_D^{(m)}) \simeq \mathrm{Aut}(X_{D,p}/X_D) \simeq \mathbb{F}_{p^2}/\{\pm 1\}.$$

From the fact that the involution $\widehat{\omega}_m$ commutes with every automorphism of $X_{D,p} \to X_D$ we also deduce that $\widehat{\omega}_m$ induces an involution lifting ω_m on each intermediate covering of $X_{D,p} \to X_D$. By a slight abuse of notation, we will still denote

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

these involutions by $\widehat{\omega}_m$. In particular, if $Z_{D,p} \to X_D$ is the maximal étale subcovering of $X_{D,p} \to X_D$ and we write $Z_{D,p}^{(m)} := Z_{D,p}/\langle\widehat{\omega}_m\rangle$, then the induced covering $Z_{D,p}^{(m)} \to X_D^{(m)}$ is étale because under our assumptions ω_m is fixed point free. Thus we have a commutative diagram

$$\begin{tikzcd}
Z_{D,p} \arrow[r, "\text{ét}"] \arrow[d] & X_D \arrow[d] \\
Z_{D,p}^{(m)} \arrow[r, "\text{ét}"] & X_D^{(m)},
\end{tikzcd}$$

and the same is true if we replace $Z_{D,p}$ by $Y_{D,p}$ and $Z_{D,p}^{(m)}$ by $Y_{D,p}^{(m)} := Y_{D,p}/\langle\widehat{\omega}_m\rangle$. Notice that $\mathrm{Aut}(Y_{D,p}^{(m)}/X_D^{(m)}) \simeq \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$. In particular, we have the following lemma.

Lemma 4.1 *$h_p\colon Y_{D,p}^{(m)} \to X_D^{(m)}$ is an $X_D^{(m)}$-torsor under the constant group scheme $\mathbb{F}_{p^2}^{\times 12} \simeq \mathbb{Z}/\frac{p^2-1}{12}\mathbb{Z}$.*

Then, if k is a field of characteristic zero and $Q \in X_D^{(m)}(k)$, by specialization of the torsor h_p at the point Q we get a continuous character $\varphi_Q\colon G_k \to \mathbb{F}_{p^2}^{\times 12}$ by which the Galois group acts on the fibre of $h_p\colon Y_{D,p}^{(m)} \to X_D^{(m)}$ at Q. For example, the specialization of h_p at a point $Q_\ell \in X_D^{(m)}(\mathbb{Q}_\ell)$ gives rise to a (local) Galois character $\varphi_{Q_\ell}\colon G_{\mathbb{Q}_\ell} \to \mathbb{F}_{p^2}^{\times 12}$.

Using the moduli interpretation of $X_D^{(m)}$ (*cf.* Proposition 2.20), if (A_ℓ, i_ℓ) is a pair parametrized by the point $Q_\ell \in X_D^{(m)}(\mathbb{Q}_\ell)$, then the local character φ_{Q_ℓ} is closely related to the Galois representation $\alpha_{Q_\ell,\mathfrak{p}}\colon G_{\mathbb{Q}_\ell} \to \mathbb{F}_{p^2}^{\times}/\{\pm 1\}$ attached to the point Q_ℓ in the previous section. The proof of the next lemma is analogous to that of Lemma 3.2.

Lemma 4.2 *For any $\sigma \in G_{\mathbb{Q}_\ell}$, $\widetilde{\alpha}_{Q_\ell,\mathfrak{p}}(\sigma)^{24} = \varphi_{Q_\ell}(\sigma)^2$. In terms of $\alpha_{Q_\ell,\mathfrak{p}}$, we have*

$$\alpha_{Q_\ell,\mathfrak{p}}(\sigma)^{12} = \varphi_{Q_\ell}(\sigma) \mod \pm 1, \quad \forall \sigma \in G_{\mathbb{Q}_\ell}.$$

Combining this with Corollary 2.25(i), the next corollary follows immediately.

Corollary 4.3 *For $\ell \neq p$, the local character $\varphi_{Q_\ell}^2$ is unramified.*

At this point, we have only considered abelian surfaces parametrized by local points on $X_D^{(m)}$. However, we need to discuss some global considerations before proving Theorem 1.2. In the following lemmas, we assume again that D is odd. Let also $Q \in X_D^{(m)}(\mathbb{Q})$, and let $K/\mathbb{Q}$ be an imaginary quadratic extension over which its preimages by π_m lie. That is, $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_D(K)$.

Understanding the field K is of great importance, and this fact appears reflected in the definition of the set $\mathcal{B}_2(q)$ introduced before the statement of Theorem 1.2.

Lemma 4.4 *The involution ω_m is fixed point free if and only if the imaginary quadratic field $\mathbb{Q}(\sqrt{-m})$ does not embed in B_D.*

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

Proof It follows immediately from the criterion of Hasse and the formula for the number of fixed points of an Atkin–Lehner involution due to Ogg ([Ogg83]). ∎

Now we use descent to prove the following lemma.

Lemma 4.5 *If $\mathbb{Q}(\sqrt{-m})$ does not embed in B_D, then K is unramified away from D.*

Proof By the above lemma, $\pi_m\colon X_D \to X_D^{(m)}$ is unramified, so it is an $X_D^{(m)}$-torsor under the constant group scheme $\mathbb{Z}/2\mathbb{Z}$. By the work of Morita on integral models of X_D (see [Mor81]), π_m extends to a smooth morphism of smooth and projective schemes over $\operatorname{Spec}(\mathbb{Z}[1/D])$, and yields a torsor under $\mathbb{Z}/2\mathbb{Z}$, now regarded as a constant $\operatorname{Spec}(\mathbb{Z}[1/D])$-group scheme.

As is well known, the $\mathbb{Q}$-rational points of $X_D^{(m)}$ can be recovered from the $\mathbb{Q}$-rational points on the twisted torsors of $\pi_m\colon X_D \to X_D^{(m)}$. More precisely,

$$X_D^{(m)}(\mathbb{Q}) = \bigcup_{\tau \in H^1(\mathbb{Q},\{\pm 1\})} {}^{\tau}X_D{}^{(m)}(\mathbb{Q}),$$

where ${}^{\tau}X_D{}^{(m)}(\mathbb{Q})$ is an abbreviation for ${}^{\tau}\pi_m({}^{\tau}X_D(\mathbb{Q}))$. Here the cohomology classes $\tau \in H^1(\mathbb{Q},\{\pm 1\})$ must be regarded as Galois quadratic characters $\tau\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \{\pm 1\}$, hence they are in correspondence with quadratic extensions. Since X_D has no real points, we can restrict ourselves to the imaginary quadratic ones. Moreover, by [SY04, Lemma 1.1] or [Sko05, p. 106], if $L/\mathbb{Q}$ is a quadratic extension ramified at a prime not dividing D, then ${}^{\tau_L}X_D(\mathbb{Q}) = \varnothing$, where τ_L is the Galois quadratic character corresponding to L. In other words, only the quadratic characters unramified away from D contribute in the above decomposition of $X_D^{(m)}(\mathbb{Q})$.

In particular, since $P \in X_D(K)$ and $\pi_m(P) = Q \in X_D^{(m)}(\mathbb{Q})$, the class $\zeta(Q) \in \mathrm{H}^1(\mathbb{Q},\{\pm 1\})$ of the $\mathbb{Q}$-torsor given by the fibre $X_{D,Q} \to Q$ is the quadratic character τ_K corresponding to the quadratic extension $K/\mathbb{Q}$. Hence, the point Q comes from a $\mathbb{Q}$-rational point on the twisted curve ${}^{\tau_K}X_D$. By the above discussion, K must be unramified away from D. ∎

Indeed, Lemma 4.5 proves the case $F = \mathbb{Q}$ of [Rot08, Proposition 1.3], which states how K depends on the pair $(\mathcal{O}, R_m)$. We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2 First of all, notice that if $(\frac{m}{p}) = 1$, then $X_D^{(m)}(\mathbb{A}_{\mathbb{Q}}) = \varnothing$ by [RSY05, Theorem 3.1] and there is nothing to prove. Thus, we can assume $(\frac{m}{p}) = -1$, placing ourselves under Assumption 2.19 as before.

Suppose there exists a point $Q \in X_D^{(m)}(\mathbb{Q})$ that has complex multiplication by neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-3})$. By the modular interpretation of $X_D^{(m)}$, we can choose an abelian surface (A, i) with real multiplication by the ring of integers R_m of $E = \mathbb{Q}(\sqrt{m})$ whose field of moduli is $\mathbb{Q}$, and such that $\mathcal{O}_D \hookrightarrow \operatorname{End}_{\overline{\mathbb{Q}}}(A)$, corresponding to the point Q. The preimages of Q under π_m^{-1} are rational over a quadratic extension $K/\mathbb{Q}$, that is, $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_D(K)$. After Shimura, K must be imaginary. By means of the diagonal embedding $X_D^{(m)}(\mathbb{Q}) \hookrightarrow X_D^{(m)}(\mathbb{A}_{\mathbb{Q}})$, the point Q defines a sequence of local points $\{Q_\ell\}_\ell \in X_D^{(m)}(\mathbb{A}_{\mathbb{Q}})$. For each one of these points, say $Q_\ell \in X_D^{(m)}(\mathbb{Q}_\ell)$, we can choose the same abelian surface (A, i) representing it. For

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

the sake of clarity, however, we denote it by (A_ℓ, i_ℓ). Note that (A_ℓ, i_ℓ) has complex multiplication by neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-3})$.

The global character $\varphi\colon G_{\mathbb{Q}} \to \mathbb{F}_{p^2}^{\times 12}$ obtained by specialization of the torsor h_p at Q restricts to each one of the local characters φ_{Q_ℓ} attached to each point Q_ℓ on $G_{\mathbb{Q}_\ell}$. Therefore, by Corollary 4.3 we have that φ^2 is unramified away from p.

Consider the abelian surface (A_q, i_q) representing the point $Q_q \in X_D^{(m)}(\mathbb{Q}_q)$, and the representation $\alpha_{Q_q,\mathfrak{p}}\colon G_{\mathbb{Q}_q} \to \mathbb{F}_{p^2}^{\times}/\{\pm 1\}$, as well as the map $\widetilde{\alpha}_{Q_q,\mathfrak{p}}\colon G_{\mathbb{Q}_q} \to \mathbb{F}_{p^2}^{\times}$. The local character $\varphi_{Q_q}\colon G_{\mathbb{Q}_q} \to \mathbb{F}_{p^2}^{\times 12}$ attached to Q_q by specialization of f_p satisfies $\varphi_{Q_q}^2 = \widetilde{\alpha}_{Q_q,\mathfrak{p}}^{24}$ and $\varphi_q \mod \pm 1 = \alpha_{Q_q,\mathfrak{p}}^{12}$ (see Lemma 4.2).

Choose a Frobenius element $\sigma_q \in G_{\mathbb{Q}_q}$, *i.e.*, an element inducing $\mathrm{Fr}_q \in \mathrm{Gal}\,(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ under reduction. We first claim that $\widetilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q)^{24} = q^{12} \in \mathbb{F}_p^{\times}$.

For each prime ℓ, consider the local Artin reciprocity map

$$w_\ell\colon \mathbb{Z}_\ell^{\times} \xrightarrow{\simeq} I_\ell^{\mathrm{ab}},$$

and let

$$w\colon \prod_\ell \mathbb{Z}_\ell^{\times} \overset{\prod w_\ell}{\twoheadrightarrow} G_{\mathbb{Q}}^{\mathrm{ab}}$$

be the global Artin map. Observe that the image under w of the idèle

$$\beta = \Bigl(\frac{1}{q}, \dots, \frac{1}{q}, 1, \frac{1}{q}, \dots\Bigr) \in \prod_\ell \mathbb{Z}_\ell^{\times},$$

where the 1 is in the q-th position, is a Frobenius element $\mathrm{Frob}_q \in G_{\mathbb{Q}}^{\mathrm{ab}}$ at q. Therefore, $\sigma_q \circ \mathrm{Frob}_q^{-1} \in I_q$, and since φ restricted to $\mathrm{Gal}\,(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$ coincides with φ_{Q_q}, whose square is unramified, we have $\varphi(\sigma_q)^2 = \varphi(\mathrm{Frob}_q)^2$.

In order to show our claim, first note that we have

$$\varphi(\sigma_q)^2 = \varphi_{Q_q}(\sigma_q)^2 = \widetilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q)^{24},$$

because $\varphi_{|G_{\mathbb{Q}_q}} = \varphi_{Q_q}$. Besides, since φ^2 is unramified away from p,

$$\varphi(\mathrm{Frob}_q)^2 = \varphi(w(\beta))^2 = \varphi_{Q_p}(w_p(q^{-1}))^2 = \varphi_{Q_p}(\tau_{q^{-1}})^2 = \widetilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_{q^{-1}})^{24},$$

where we choose any representative $\tau_{q^{-1}} \in I_p$ of $w_p(q^{-1}) \in I_p^{\mathrm{ab}}$. Then we must show that $\widetilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_{q^{-1}})^{24} = q^{12}$. More generally, let us denote by $\tau_x \in I_p$ any representative of $w_p(x) \in I_p^{\mathrm{ab}}$, for $x \in \mathbb{Z}_p^{\times}$, and denote also by $\widetilde{x} \in \mathbb{F}_p^{\times}$ the reduction modulo p of x. By [Ser72, Prop. 3, 8], if $\overline{\chi}_p\colon G_{\mathbb{Q}_p} \to \mathbb{F}_p^{\times}$ is the reduction modulo p of the p-cyclotomic character, then we have $\overline{\chi}_p(\tau_x) = \widetilde{x}^{-1}$ for all $x \in \mathbb{Z}_p^{\times}$. Then (*cf.* Corollary 2.25, Lemma 2.26)

$$\begin{aligned}\widetilde{x}^{-2} &= \overline{\chi}_p(\tau_x^2) = \pm\det\bigl(\overline{\varrho}_{Q_p,\mathfrak{p}}(\tau_x^2)\bigr) = \pm\psi(\tau_x^2)N_{\mathbb{F}_{p^2}/\mathbb{F}_p}\bigl(\widetilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_x^2)\bigr)\\ &= \pm\widetilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_x^2)^2 = \pm\widetilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_x)^4,\end{aligned}$$

where we have used that $\widetilde{\alpha}_{Q_p,\mathfrak{p}}(\tau^2) \in \mathbb{F}_p^\times$ for every $\tau \in I_p$ (see Remark 2.28). In particular, for $x = q^{-1}$ we get

$$\widetilde{\alpha}_{Q_p,\mathfrak{p}}(\tau_{q^{-1}})^{24} = q^{12} \in \mathbb{F}_p^\times, \tag{4.2}$$

as we claimed.

Now, since $(\frac{m}{p}) = -1$ and $p \equiv 3 \mod 4$, we have $(\frac{-m}{p}) = 1$, so that $\mathbb{Q}(\sqrt{-m})$ does not embed in B_D. By Lemma 4.5, K is unramified away from D. Also, since $B_D \in \mathcal{B}_2(q)$ the prime q is not inert in K. If we let $\mathfrak{q}$ be a prime of K above q, then we can regard the point P as a point in $X_D(K_\mathfrak{q})$, where $K_\mathfrak{q}$ is the completion of K at $\mathfrak{q}$, so that according to Lemma 2.22 we can choose (A_q, ι_q) and (A_q, i_q) to be defined over $K_q := K_\mathfrak{q}$. Moreover, note that the residue field of $K_q/\mathbb{Q}_q$ is isomorphic to $\mathbb{F}_q$.

On the other hand, since A_q/K_q has potential good reduction, following the construction of Serre and Tate at the end of [ST68, p. 498], we can choose a finite totally ramified extension L_q/K_q such that the closed fibre of the Néron model of $A_q \times_{K_q} L_q$ over the ring of integers of L_q is an abelian surface $\widetilde{A}_q$ over $\mathbb{F}_q$. Moreover, the action of the Frobenius element σ_q on the Tate modules $T_p(A_q)$ and $T_p(\widetilde{A}_q)$ is the same.

Besides, the quaternion algebra $B_D \subseteq \mathrm{End}^0_{K_q}(A_q)$ is embedded in $\mathrm{End}^0_{\mathbb{F}_q}(\widetilde{A}_q)$, since the residue field of $K_q/\mathbb{Q}_q$ is $\mathbb{F}_q$. Moreover, $\sigma_q \in \mathrm{Gal}\,(\overline{\mathbb{Q}}_q/K_q) \subseteq \mathrm{Gal}\,(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$, thus by Corollary 2.27 the characteristic polynomial of $\varrho_{(A_q,i_q),\mathfrak{p}}(\sigma_q)$ reduced modulo $\mathfrak{p}$ is congruent to

$$T^2 - \left(\widetilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q) + q\widetilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q)^{-1}\right) T + q \in \mathbb{F}_{p^2}[T].$$

This implies, by [Jor86, Theorem 2.1], that $\widetilde{\alpha}_{Q_{q,\mathfrak{p}}}(\sigma_q) + q\widetilde{\alpha}_{Q_{q,\mathfrak{p}}}(\sigma_q^{-1})$ is the reduction modulo p of an integer a_q of absolute value at most $2\sqrt{q}$. Then, using (4.2), we can write

$$a_q \equiv \sqrt{q}(\zeta + \zeta^{-1}) \mod \overline{\mathfrak{p}},$$

where $\zeta = (\widetilde{\alpha}_{Q_q,\mathfrak{p}}(\sigma_q))/\sqrt{q}$ is a 24-th root of 1, and $\overline{\mathfrak{p}}$ a prime of $\overline{\mathbb{Q}}$ over $\mathfrak{p}$. Computing the possible values of $\sqrt{q}(\zeta + \zeta^{-1})$ with ζ a 24-th root of 1 leads to

$$a_q \equiv 0, \pm\sqrt{q}, \pm\sqrt{2q}, \pm\sqrt{3q}, \pm 2\sqrt{q} \text{ or } \pm\sqrt{q}\cdot\sqrt{2 \pm \sqrt{3}} \mod \overline{\mathfrak{p}}.$$

In other words, $p | a_q^2 - sq$ for some $s = 0, 1, 2, 3, 4$ or $p | a_q^4 - 4a_q^2 q + q^2$. But since $|a_q| \leq 2\sqrt{q}$, from the definition of $P_2(q)$ the above congruence must be an equality. Moreover, since a_q is an integer the only possibilities are (i) $a_q = 0$, (ii) $q = 2$ and $a_2 = \pm 2$, or (iii) $q = 3$ and $a_q = \pm 3$.

According to the classification of abelian surfaces admitting quaternionic multiplication over finite fields following from the Honda-Tate theory (see [Jor86, Theorem 2.1]), we deduce that for these cases one has

$$\mathrm{End}^0_{\mathbb{F}_q}(\widetilde{A}_q) \simeq \mathrm{M}_2(\mathbb{Q}(\sqrt{-q})), \quad \mathrm{M}_2(\mathbb{Q}(\sqrt{-1})) \quad \text{or} \quad \mathrm{M}_2(\mathbb{Q}(\sqrt{-3})),$$

respectively. It follows that B_D is split by $\mathbb{Q}(\sqrt{-q})$, $\mathbb{Q}(\sqrt{-1})$, or $\mathbb{Q}(\sqrt{-3})$, respectively, which contradicts the assumption that $B_D \in \mathcal{B}_2(q)$. Then, all the points in $X_D^{(m)}(\mathbb{Q})$ must have CM by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$.

Finally, using again the results from [GR06, §5], one easily checks that (under our hypotheses) both $X_D^{(m)}(\mathbb{Q}) \cap \pi_m(\mathrm{CM}(\mathbb{Q}(\sqrt{-1})))$ and $X_D^{(m)}(\mathbb{Q}) \cap \pi_m(\mathrm{CM}(\mathbb{Q}(\sqrt{-3})))$ are empty. In other words, the points in $X_D^{(m)}(\overline{\mathbb{Q}})$ with CM by either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$ cannot be rational. As a consequence, $X_D^{(m)}(\mathbb{Q}) = \varnothing$. ■

Now it is natural to ask whether the examples of Atkin–Lehner quotients of Shimura curves without rational points arising from Theorem 1.2 include counterexamples to the Hasse principle or not. In [RSY05, Theorem 3.1], a criterion for the existence of adelic points on $X_D^{(m)}$ was given, which together with Theorem 1.2 can be used to produce counterexamples to the Hasse principle over $\mathbb{Q}$. In the particular case where D is the product of two primes, we obtain the following corollary, where for an integer $n > 0$ the quantity $\Sigma_n(D)$ is defined as in (3.1).

Corollary 4.6 *Assume that $D = pm$ satisfies the hypotheses of Theorem 1.2 with m a prime such that $\left(\frac{m}{p}\right) = -1$, and let g be the genus of $X_D^{(m)}$. If for every prime $\ell \neq p, m$ with $\ell < 4g^2$, $\Sigma_\ell(D) \neq 0$ or $\Sigma_{\ell m}(D) \neq 0$, then $X_D^{(m)}$ is a counterexample to the Hasse principle over $\mathbb{Q}$.*

Proof First of all, we have $X_{pm}^{(m)}(\mathbb{Q}) = \varnothing$ by Theorem 1.2. Secondly, by assumption we have $\left(\frac{m}{p}\right) = -1$ and $p \equiv 3 \mod 4$, so that using the Quadratic Reciprocity Law one obtains

$$\left(\frac{-m}{p}\right) = 1, \quad \left(\frac{-p}{m}\right) = -1.$$

Using [RSY05, Theorem 3.1], these conditions, together with the last hypothesis in the statement, imply that $X_{pm}^{(m)}(\mathbb{A}_\mathbb{Q}) \neq \varnothing$. ■

Some counterexamples to the Hasse principle over $\mathbb{Q}$ arising from Corollary 4.6 are shown in Table 2 in the introduction.

Remark 4.7 Assume $D = pm$ satisfies the hypotheses of Theorem 1.2, so that $X_D^{(m)}(\mathbb{Q}) = \varnothing$. We were unable to prove that this is accounted for by the Brauer–Manin obstruction, and we leave it as an open question for the reader. The reason why we managed to prove the analogous statement for Shimura curves over imaginary quadratic fields K and cannot do so here is revealed by Theorem 2.21, which shows that the obstruction B_Q for a point $Q \in X_D^{(m)}(\mathbb{Q})$ to be represented by an abelian surface admitting a model over $\mathbb{Q}$ *depends* on the point Q. This is in contrast with Theorem 2.13, which asserts that, for a point $P \in X_D(K)$, we have $B_P = B_D \otimes_\mathbb{Q} K$, independently of the choice of P and even of the field K.

This raises the following questions, which we find interesting in themselves. Let X be the moduli space of a family of abelian varieties, possibly equipped with additional structure (polarization, endomorphisms, marked torsion points, etc.), and assume X admits a canonical model over $\mathbb{Q}$. Let k be a field of characteristic 0 and assume Hypothesis 2.3 holds for all points $P \in X(k)$.

Questions Is the quaternion algebra $B_P \in \mathfrak{Q}_k$ independent of the choice of P? If not, is the set $\{B_P, P \in X(k)\} \subset \mathfrak{Q}_k$ comparatively more manageable than the set $X(k)$ itself? If yes, is there in fact a quaternion algebra $B \in \mathfrak{Q}_\mathbb{Q}$ such that $B_P = B \otimes k$ for all $P \in X(k)$, independently of the choice of k?

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

A Appendix: A Different Approach

In Theorem A.1 below we show how Lemma 4.5 together with [Rot08, Theorem 1.4] allows us to prove the non-existence of rational points on some Atkin–Lehner quotients of Shimura curves from a different approach to that of Theorem 1.2.

First, suppose that $Q \in X_D^{(m)}(\mathbb{Q})$, and let $K/\mathbb{Q}$ be an imaginary quadratic field such that $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_D(K)$. It follows from [Jor86, p. 93] that if D is odd, then $B_D \otimes K \simeq \mathrm{M}_2(K)$. In other words, by [Jor86, Theorem 1.1], we can choose a pair (A, ι) defined over K such that $P = [(A, \iota)]$.

On the other hand, for a given rational prime q, let us define $P_0(q) \subseteq P_2(q)$ to be the set of prime factors of the non-zero integers in the set

$$\bigcup_{s,a} \{a^2 - sq\},$$

where the union is over $s = 0, 1, 2, 3, 4$ and the integers a such that $|a| \leq 2\sqrt{q}$. For instance, we have $P_0(3) = \{2, 3, 5, 11\}$ and $P_0(5) = \{2, 3, 5, 7, 11, 19\}$.

Theorem A.1 *Let p and m be two primes with $p \equiv m \equiv 3 \bmod 4$, $(\frac{m}{p}) = -1$ and $p \neq 3, 7, 11, 19, 43, 67, 163$. If there exists an odd prime q such that $p \notin P_0(q)$, $(\frac{q}{p}) = 1$ and $(\frac{q}{m}) = -1$, then $X_{pm}^{(m)}(\mathbb{Q}) = \varnothing$.*

Proof Suppose there exists a non-CM point $Q \in X_{pm}^{(m)}(\mathbb{Q})$, and let K be the imaginary quadratic field such that $\pi_m^{-1}(Q) = \{P, \omega_m(P)\} \subseteq X_{pm}(K)$. By Lemma 4.5, K is unramified at the primes not dividing pm. Hence the only possibilities for K are $\mathbb{Q}(\sqrt{-p})$, $\mathbb{Q}(\sqrt{-m})$, and $\mathbb{Q}(\sqrt{-pm})$.

The last option is excluded because it is ramified at 2. But the case $\mathbb{Q}(\sqrt{-m})$ can also be excluded. Indeed, since $(\frac{-m}{p}) = (\frac{-1}{p})(\frac{m}{p}) = 1$ we get that $-m$ is a square in $\mathbb{Q}_p$. If ${}^{-m}X_{pm}$ denotes the twisted form ${}^{\tau}X_{pm}$ of X_{pm} by the cohomology class $\tau \in H^1(\mathbb{Q}, \mathbb{Z}/2\mathbb{Z})$ corresponding to the imaginary quadratic field $\mathbb{Q}(\sqrt{-m})$, this implies that ${}^{-m}X_{pm} \times \mathbb{Q}_p \simeq X_{pm} \times \mathbb{Q}_p$, but $X_{pm}(\mathbb{Q}_p) = \varnothing$ by [JL85]. Hence $K = \mathbb{Q}(\sqrt{-p})$.

But now observe that $B_{pm} \simeq (\frac{-p,m}{\mathbb{Q}})$. Therefore, by [BFGR06, Theorem 4.5], the point Q corresponds, in the terminology of [Rot08], to a *modular triplet* $(\mathcal{O}_{pm}, R_m, \mathbb{Q}(\sqrt{-p}))$. By applying [Rot08, Theorem 1.4], we deduce $(\frac{-q}{m}) = -1$, but our assumptions imply

$$\left(\frac{-q}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{q}{m}\right) = 1,$$

and thus we get a contradiction. This shows that the only points in $X_{pm}^{(m)}(\mathbb{Q})$ must be CM-points. But, from [BFGR06, Proposition 5.1], which follows from the work in [GR06, §5], one can easily check that under the hypotheses of the statement $X_D^{(m)}(\mathbb{Q})$ does not contain CM-points. ■

This result is significant progress with respect to [RSY05, Theorem 5.1] and [RSY05, Corollary 5.2]. Fixed a prime q, it says that $X_{pm}^{(m)}(\mathbb{Q}) = \varnothing$ whenever m and p are distinct primes such that $p \notin P_0(q)$, $p \neq 3, 7, 11, 19, 43, 67, 163$, $p \equiv m \equiv 3$

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press

mod 4, $(\frac{m}{p}) = -1$, $(\frac{q}{p}) = 1$ and $(\frac{q}{m}) = -1$. By Čebotarev Density Theorem, there exist infinitely many such m and p.

As in Corollary 4.6, we can use [RSY05, Theorem 3.1] to produce Atkin–Lehner quotients $X_{pm}^{(m)}$ violating the Hasse principle over $\mathbb{Q}$ arising from Theorem A.1. We collect some of them in the next table.

Some pairs (p, m) such that $X_{pm}^{(m)}(\mathbb{Q}) = \varnothing$ and $X_{pm}^{(m)}(\mathbb{A}_{\mathbb{Q}}) \neq \varnothing$
(23, 7), (23, 11), (23, 19), (23, 43), (31, 3), (31, 11), (31, 23), (31, 31),
(31, 43), (47, 11), (47, 19), (47, 23), (47, 31), (47, 43), (59, 11), (59, 23),
(59, 31), (59, 43), (59, 47), (71, 7), (71, 11), (71, 23), (71, 31), (71, 31),
(71, 47), (79, 3), (79, 7), (79, 43), (79, 47), (83, 19), (83, 43), (83, 47)

Table 3

Acknowledgment We are grateful to the anonymous referee for his/her helpful remarks and suggestions.

References

[BFGR06] N. Bruin, V. Flynn, J. Gonzàlez, and V. Rotger, *On finiteness conjectures for endomorphism algebras of abelian surfaces.* Math. Proc. Cambridge Philos. Soc. **141**(2006), no. 3, 383–408. http://dx.doi.org/10.1017/S0305004106009613

[Cla03] P. L. Clark, *Rational points on Atkin–Lehner quotients of Shimura curves.* Thesis (Ph.D.)–Harvard University, ProQuest LLC, Ann Arbor, MI, 2003.

[ES01] J. S. Ellenberg and C. Skinner, *On the modularity of* $\mathbb{Q}$*-curves.* Duke Math. J. **109**(2001), no. 1, 97–122. http://dx.doi.org/10.1215/S0012-7094-01-10914-9

[Gil10] F. Gillibert, *Points rationnels sur les quotients d'Atkin–Lehner de courbes de Shimura de discriminant pq.* arxiv:1012.3414v1, 2010.

[GR06] J. González and V. Rotger, *Non elliptic Shimura curves of genus one.* J. Math. Soc. Japan **58**(2006), no. 4, 927–948. http://dx.doi.org/10.2969/jmsj/1179759530

[Jor81] B. W. Jordan, *On the Diophantine arithmetic of Shimura curves.* Thesis (Ph.D.)–Harvard University, Proquest LLC, Ann Arbor, MI, 1981.

[Jor86] ———, *Points on Shimura curves rational over number fields.* J. Reine Angew. Math. **371**(1986), 92–114.

[JL85] B. W. Jordan and R. A. Livné, *Local Diophantine properties of Shimura curves.* Math. Ann. **270**(1985), no. 2, 235–248. http://dx.doi.org/10.1007/BF01456184

[Me90] J.-F. Mestre, *Construction de courbes de genre 2 à partir de leurs modules.* In: Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334.

[Mil79] J. S. Milne, *Points on Shimura varieties mod p.* In: Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, Proc. Sympos. Pure Math., 33, American Mathematical Society, Providence, RI, 1979, pp. 165–184.

[Mil86] ———, *Abelian varieties.* In: Arithmetic geometry (Storrs, Conn, 1984), Springer, New York, 1986, pp. 103–150.

[Mil04] ———, *Introduction to Shimura varieties.* http://www.jmilne.org/math/xnotes.

[Mor81] Y. Morita, *Reduction modulo* $\mathfrak{P}$ *of Shimura curves.* Hokkaido Math. J. **10**(1981), no. 2, 209–238.

[Ogg83] A. P. Ogg, *Real points on Shimura curves.* In: Arithmetic and geometry, Vol. 1, Progr. Math., 35, Birkäuser Boston, Boston, MA, 1983, pp. 277–307.

[Ogg85] ———, *Mauvaise réduction des courbes de Shimura.* Séminaire de théorie des nombres, Paris 1983–84, Progr. Math., 59, Birkhäuser Boston, MA, 1985, pp. 199–217.

[Oht64] M. Ohta, *On ℓ-adic representations of Galois groups obtained from certain two-dimensional abelian varieties.* J. Fac. Sci. Univ. Tokyo IA Math. **21**(1974), 299–308.

[PY07] P. Parent and A. Yafaev, *Proving the triviality of rational points on Atkin–Lehner quotients of Shimura curves.* Math. Ann. **339**(2007), no. 4, 915–935. http://dx.doi.org/10.1007/s00208-007-0136-9

[Rot03] V. Rotger, *Quaternions, polarizations and class numbers.* J. Reine Angew. Math. **561**(2003), 177–197.

[Rot04] ______, *Modular Shimura varieties and forgetful maps.* Trans. Amer. Math. Soc. **356**(2004), no. 4, 1535–1550. http://dx.doi.org/10.1090/S0002-9947-03-03408-1

[Rot08] ______, *Which quaternion algebras act on a modular abelian variety?* Math. Res. Lett. **15**(2008), no. 2, 251–263.

[RSY05] V. Rotger, A. Skorobogatov, and A. Yafaev, *Failure of the Hasse principle for Atkin–Lehner quotients of Shimura curves over* $\mathbb{Q}$. Moscow Math. J. **5**(2005), no. 2, 463–476, 495.

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. **15**(1972), no. 4, 259–331. http://dx.doi.org/10.1007/BF01405086

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties.* Ann. of Math. **88**(1968), 492–517. http://dx.doi.org/10.2307/1970722

[Shi63] G. Shimura, *On analytic families of polarized abelian varieties and automorphic functions.* Ann. of Math. **78**(1963), 149–192. http://dx.doi.org/10.2307/1970507

[Shi67] ______, *Construction of class fields and zeta functions of algebraic curves.* Ann. of Math. **85**(1967), 58–159. http://dx.doi.org/10.2307/1970526

[Shi75] ______, *On the real points of an arithmetic quotient of a bounded symmetric domain.* Math. Ann. **215**(1975), 135–164. http://dx.doi.org/10.1007/BF01432692

[Sko01] A. Skorobogatov, *Torsors and rational points.* Cambridge Tracts in Mathematics, 144, Cambridge University Press, Cambridge, 2001.

[Sko05] ______, *Shimura coverings of Shimura curves and the Manin obstruction.* Math. Res. Lett. **12**(2005), no. 5–6, 779–788.

[SY04] A. Skorobogatov and A. Yafaev, *Descent on certain Shimura curves.* Israel J. Math. **140**(2004), 319–332. http://dx.doi.org/10.1007/BF02786638

[dVP] C. de Vera-Piquero, *The Shimura covering of a Shimura curve: automorphisms and étale subcoverings.* J. Number Theory **133**(2013), no. 10, 3500–3516. http://dx.doi.org/10.1016/j.jnt.2013.04.018

[Vig80] M. F. Vignéras, *Arithmétique des algèbres de quaternions.* Lecture Notes in Mathematics, 800, Springer, Berlin, 1980.

[Wei56] A. Weil, *The field of definition of a variety.* Amer. J. Math. **78**(1956), 509–524. http://dx.doi.org/10.2307/2372670

Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, C. Jordi Girona 1-3, 08034 Barcelona, Spain
e-mail: victor.rotger@upc.edu carlos.de.vera@upc.edu

https://doi.org/10.4153/CJM-2013-020-3 Published online by Cambridge University Press