Mathematical Research Letters **12**, 10001–100NN (2005)

SHIMURA COVERINGS OF SHIMURA CURVES AND THE MANIN OBSTRUCTION

Alexei Skorobogatov

Abstract. We prove that the counterexamples to the Hasse principle on Shimura curves over imaginary quadratic fields found by B. Jordan are accounted for by the Manin obstruction.

Introduction

Let B be an indefinite quaternion algebra over $\mathbb{Q}$ of reduced discriminant D. All maximal orders in B are conjugate; so let us fix one maximal order $\mathcal{O} \subset B$. Let $\mathcal{O}^+ \subset \mathcal{O}^*$ be the group of elements of reduced norm 1. On identifying $B \otimes \mathbb{R}$ with $\mathrm{M}_2(\mathbb{R})$ we can think of $\mathcal{O}^+$ as an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{R})$. The compact Riemann surface $\mathcal{O}^+ \backslash \mathcal{H}$, where $\mathcal{H}$ is the upper-half plane, is the set of complex points of an algebraic curve X over $\mathbb{Q}$, a Shimura curve [10]. The curve X is the coarse moduli scheme over $\mathbb{Q}$ which classifies the isomorphism classes of pairs (A, i), where A is an abelian surface and i is an embedding of $\mathcal{O}$ into $\mathrm{End}(A)$. By an abuse of language such a pair is called an abelian surface with quaternionic multiplication, or a QM-abelian surface.

It appears that Jordan's work on global points on Shimura curves [3] did not receive the attention it justly deserved. His approach is based on the modular interpretation and is inspired by the strategy of the celebrated work of Mazur [6]. Jordan proves that certain Shimura curves have no points defined over certain imaginary quadratic fields k; yet in some cases such Shimura curves have points in all completions of k. Until now it was not clear whether or not these counterexamples to the Hasse principle can be accounted for by the Manin obstruction. One particular counterexample on a curve of genus 3 has been treated in [11], but this explanation was conditional on a conjectured equation of the curve. We review Jordan's approach interpreting it in terms of descent. The main idea is to consider the 'Shimura covering' of X attached to a prime factor p of D. It is the maximal étale subcovering $Z \to X$ of the covering of X parameterizing triples (A, i, P), where P is a generator of the $\mathcal{O}$-module $A[I_p]$ for the unique two-sided ideal $I_p \subset \mathcal{O}$ of reduced norm p. The morphism $Z \to X$ is a torsor under a constant group scheme. A small modification of Jordan's approach allows us to interpret his results on the non-existence of global points on X in terms of the descent performed on a closely related torsor. (When we had nothing to add to Jordan's arguments we preferred to only sketch them by referring to [3] for details.) This leads us to an explanation of all counterexamples to the Hasse principle stemming from his work [3] in terms of the Manin obstruction. Our main results are Theorems 2.4 and 3.1; a more explicit particular case of the latter result is Corollary 3.2.

For the sake of completeness let us mention that counterexamples to the Hasse principle on Shimura curves and their Atkin–Lehner quotients have been recently constructed in [2], [13], [7]. All those obtained by the method of [13] are automatically accounted for by the Manin obstruction. In the end of this note we deduce from a recent result of M. Stoll [14] that the explicit counterexamples to the Hasse principle over $\mathbb{Q}$ constructed in [7] can also be explained by the Manin obstruction. This approach relies on well known but deep facts about modular forms.

1. A cyclic étale covering of X attached to a prime factor of D

We write $\mathbb{A}_{\mathbb{Q}}$ for the ring of $\mathbb{Q}$-adèles, and $\mathbb{A}_{\mathbb{Q},\mathtt{f}}$ for the ring of finite $\mathbb{Q}$-adèles, i.e., adèles without archimedean components. Let $\mathcal{H}^{\pm} = \mathbb{C} \setminus \mathbb{R}$. Let $n : B \to \mathbb{Q}$ be the reduced norm. We write $\hat{\mathcal{O}}$ for $\mathcal{O} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$.

Let $K \subset \hat{\mathcal{O}}^*$ be a compact open subgroup. Consider the topological space of double cosets

$$X_K = B^* \backslash \mathcal{H}^{\pm} \times (B \otimes_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q},\mathtt{f}})^* / K,$$

where B^* acts on the left simultaneously on both factors, and K acts on the right on the second factor. By Shimura and Deligne X_K is a disjoint union of $|\hat{\mathbb{Z}}^*/n(K)|$ compact connected complex curves, and it has a canonical model which is an irreducible algebraic curve over $\mathbb{Q}$. If $K = \hat{\mathcal{O}}^*$, then X_K is the Shimura curve X described in the introduction. This curve defined over $\mathbb{Q}$ is geometrically connected.

We now attach a subgroup K to a prime factor p of the discriminant D of B. There is a unique two-sided prime ideal $I_p \subset \mathcal{O}$ of reduced norm p (see [15], p. 86). More concretely, I_p is the set of elements of $\mathcal{O}$ with reduced norm divisible by p; we have $I_p^2 = p\mathcal{O}$. The field $\mathcal{O}/I_p$ is isomorphic to $\mathbb{F}_{p^2}$. Define K_p as the set of elements of $\hat{\mathcal{O}}^*$ which are congruent to 1 modulo I_p, and let X_p be the Shimura curve over $\mathbb{Q}$ which is the canonical model of X_{K_p}. The natural finite flat morphism $X_p \to X$ is a Galois covering whose Galois group is isomorphic to $\mathbb{F}_{p^2}^{*2} = \mathbb{F}_{p^2}^*/\{\pm 1\}$ if $p \neq 2$, and to $\mathbb{F}_4^* \simeq \mathbb{Z}/3$ for $p = 2$. The curve X is in fact the quotient of X_p by the action of the 'constant' group scheme $\mathbb{Z}/\frac{p^2-1}{2}$ if $p \neq 2$ (resp. $\mathbb{Z}/3$ if $p = 2$).

If $p \neq 2$ the curve X_p defined over $\mathbb{Q}$ is not geometrically connected. The complex curve $X_p \times_{\mathbb{Q}} \mathbb{C}$ is a disjoint union of $p-1 = |\mathbb{Z}_p^*/1+p\mathbb{Z}_p|$ irreducible curves which are conjugate over $\mathbb{Q}(\mu_p)$. Each irreducible component is isomorphic to the Riemann surface $\Gamma_p \backslash \mathcal{H}$, where $\Gamma_p = \mathcal{O}^+ \cap K_p$. Note that Γ_p is normal in $\mathcal{O}^+$ with quotient $\mathbb{Z}/(p+1)$. The only non-trivial element of $\mathcal{O}^+$ that acts trivially on $\mathcal{H}$ is -1, and $-1 \notin \Gamma_p$ if p is odd. Hence each irreducible component of $X_p \times_{\mathbb{Q}} \mathbb{C}$ is a cyclic Galois covering of $X \times_{\mathbb{Q}} \mathbb{C}$ of degree $(p+1)/2$. If $p = 2$ we have $-1 \in K_2$, so that the degree of the covering $X_2 \to X$ is 3.

Following [4], p. 108, for a quadratic field k we set $\left(\frac{B}{k}\right)$ equal to 1 if k splits B, and 0 otherwise. Define

$$\varepsilon(p) = \begin{cases} \left(1 + 2\left(\frac{B}{\mathbb{Q}(\sqrt{-3})}\right)\right)\left(1 + \left(\frac{B}{\mathbb{Q}(\sqrt{-1})}\right)\right) & \text{for} \quad p > 3; \\ 1 + \left(\frac{B}{\mathbb{Q}(\sqrt{-1})}\right) & \text{for} \quad p = 3; \\ 1 + 2\left(\frac{B}{\mathbb{Q}(\sqrt{-3})}\right) & \text{for} \quad p = 2. \end{cases}$$

For $p \neq 2$ we note that $\varepsilon(p)$ divides $(p^2-1)/2$.

Lemma 1.1 (Jordan)**.** *Let $p \neq 2$. Define Z as the quotient of X_p by the group subscheme $\mathbb{Z}/\varepsilon(p) \subset \mathbb{Z}/\frac{p^2-1}{2}$. Then the natural morphism $Z \to X$ is étale.*

Proof. Let $e = \mathrm{hcf}(\varepsilon(p), (p+1)/2)$. Since all the irreducible components of X_p are conjugate it is enough to choose one of them, say X', and prove that the quotient of X' by $\mathbb{Z}/e$ is an unramified covering of X. This is an immediate consequence of the fact that the image of the set of elliptic elements of $\mathcal{O}^+/\{\pm 1\}$ in $\mathcal{O}^+/\{\pm 1\} \cdot \Gamma_p \simeq \mathbb{Z}/\frac{p+1}{2}$ is the subgroup $\mathbb{Z}/e$ ([4], Prop. 5.1.3). QED

The analogous statement for $p = 2$ is that the covering $X_2 \to X$ is unramified if and only if $\varepsilon(2) = 1$, that is, if and only if $\mathbb{Q}(\sqrt{-3})$ does not split B.

In the rest of the paper we assume that $p \geq 5$; then 6 divides $(p^2-1)/2$. Define Y as the quotient of X_p by $\mathbb{Z}/6$.

Corollary 1.2. *Y is an X-torsor under the constant group scheme $\mathbb{F}_{p^2}^{*12} \simeq \mathbb{Z}/\frac{p^2-1}{12}$.*

Proof. $\varepsilon(p)$ divides 6 if $p \geq 5$, thus the covering $Y \to X$ is a quotient of an étale covering $Z \to X$. QED

Let k be a field of characteristic 0. We choose one of two possible field isomorphisms of $\mathcal{O}/I_p$ with $\mathbb{F}_{p^2}$. By specialization a torsor $Y \to X$ under the constant group scheme $\mathbb{F}_{p^2}^{*12}$ associates to a point $Q \in X(k)$ a continuous character by which the Galois group acts on the fibre of $Y \to X$ at Q. We denote it by $\phi_Q \in \mathrm{Hom}(\mathrm{Gal}(\overline{k}/k), \mathbb{F}_{p^2}^{*12})$.

2. Modular interpretation and local characters

A natural modular interpretation of X was discussed in the introduction. A similar interpretation exists for X_p. Let (A, i) be an abelian surface with multiplication by $\mathcal{O}$, and let $C_p = A[I_p]$ be the kernel of the action of $I_p \subset \mathcal{O}$. Then C_p is an $\mathcal{O}$-submodule of $A[p]$ canonically isomorphic to $\mathcal{O}/I_p \simeq \mathbb{F}_{p^2}$. The $\mathbb{Q}$-curve X_p is the coarse moduli scheme over $\mathbb{Q}$ classifying triples (A, i, P), where (A, i) is an abelian surface with multiplication by $\mathcal{O}$, and P is a generator of the $\mathcal{O}$-module C_p (see [4], p. 110, see also [1], III, 1.1).

Note that a QM-abelian surface (A, i) is not necessarily defined over the residue field $\mathbb{Q}(P)$ of the corresponding point P on X, called the field of moduli of (A, i). In Thm. 1.1 of [3] Jordan proves that (A, i) is defined over a field k containing $\mathbb{Q}(P)$ if and only if k splits B.

Let (A, i) be a QM-abelian surface defined over a field k of characteristic 0. There is only one non-trivial $\mathcal{O}$-submodule in $A[p]$, that is, C_p, hence it is defined over k. Our choice of a field isomorphism of $C_p = \mathcal{O}/I_p$ with $\mathbb{F}_{p^2}$ defines a character

$$\rho_A : \mathrm{Gal}(\overline{k}/k) \to \mathbb{F}_{p^2}^*$$

coming from the Galois action on C_p. Changing the isomorphism has the effect of replacing ρ_A by ρ_A^p, and the similar effect on ϕ_Q.

Lemma 2.1. *Let k be a field of characteristic 0 which splits B, and let $Q \in X(k)$. If (A, i) is a QM-abelian surface defined over k represented by Q, then $\rho_A^{12} = \phi_Q$.*

Proof. This is a consequence of the modular interpretation of the morphism $X_p \to X$ and the fact that Y is the quotient of X_p by $\mathbb{Z}/6$. QED

Proposition 2.2 (Jordan)**.** *Let k be a number field which splits B. Let v be a prime of k which does not divide p. Then for any $Q_v \in X(k_v)$ the character ϕ_{Q_v} is unramified.*

Perhaps a most natural way to prove this proposition would be to show that the étale morphism of $\mathbb{Q}$-curves $Y \to X$ extends to an étale morphism of proper regular $\mathbb{Z}[1/p]$-schemes $\mathcal{Y} \to \mathcal{X}$. In other words, the torsor $Y \to X$ under the constant group scheme $\mathbb{F}_{p^2}^{*12}$ extends to a torsor over $\mathrm{Spec}(\mathbb{Z}[1/p])$. This would imply that if v does not divide p, then for any $Q_v \in X(k_v)$ the character ϕ_{Q_v} is unramified. (This argument does not require the assumption that k splits B.) Jordan's proof, which we now sketch, is indirect but it establishes some other useful facts as by-products.

Proof of Proposition 2.2. (cf. [3], Sections 3 and 4) Any point $Q_v \in X(k_v)$ represents a QM-abelian surface (A, i) defined over k_v. To this surface one canonically associates a character ρ_A as above (well defined up to replacing ρ_A by ρ_A^p). By Lemma 2.1 it suffices to show that ρ_A^{12} is unramified away from p. For this we need to show that if $I(v)$ is the inertia subgroup of the maximal abelian extension k_v^{ab}/k_v, then $\rho_A(I(v))^{12} = 1$.

Let ℓ be a prime invertible in $\mathbb{F}_v$. It is known that A has potentially good reduction. By the Néron–Ogg–Shafarevich theorem this implies that the kernel N of the action of $I(v)$ on the Tate module $T_\ell(A)$ is a subgroup of $I(v)$ of finite index (and N does not depend on ℓ). Set $\Phi(A/k_v) = I(v)/N$. Choose a Frobenius element $\sigma \in \mathrm{Gal}(\overline{k_v}/k_v)$. Let $\hat{\mathbb{Z}} \subset \mathrm{Gal}(\overline{k_v}/k_v)$ be the

closure of the infinite cyclic group generated by σ, and let K/k_v be the extension cut out by the subgroup $N\hat{\mathbb{Z}}$. This is a totally ramified extension with the Galois group $\mathrm{Gal}(K/k_v) = \Phi(A/k_v)$. By the Néron–Ogg–Shafarevich theorem the abelian surface A_K has good reduction. Let $\tilde{A}$ be the special fibre. We have canonical isomorphisms $T_\ell(A) = T_\ell(A_K) = T_\ell(\tilde{A})$. By the universal property of the Néron models the action of $\Phi(A/k_v)$ on $A_K = A \times_k K$ via K extends uniquely to an action on the Néron model of A_K. Since $\mathrm{Gal}(K/k_v)$ acts trivially on the residue field, the action of this group on $\tilde{A}$ is by $\mathbb{F}_v$-automorphisms of $\tilde{A}$ (which commute with the action of $\mathcal{O}$). Thus the representation of $\Phi(A/k_v)$ in $T_\ell(A)$ factors through an injective homomorphism $\Phi(A/k_v) \hookrightarrow \mathrm{Aut}_{\mathcal{O}}(\tilde{A}/\mathbb{F}_v)$ (this argument goes back to Serre and Tate, see [9], Thm. 2). The analysis of the automorphism groups over finite fields in Section 2 of [3] then shows that an abelian quotient of $\Phi(A/k_v)$ is a cyclic group of order 1, 2, 3, 4, or 6. We assumed that $p \geq 5$, and in this case these are the only possible sizes of $\Phi(A/k_v)$.

Now assume that p is invertible in $\mathbb{F}_v$. To complete the proof choose $\ell = p$. Since N acts trivially on $T_p(A)$ it acts trivially on $C_p \subset T_p(A)/p$, hence $\rho_A(I(v)) = \rho_A(\Phi(A/k_v))$. Thus $\rho_A^{12}(I(v)) = 1$. QED

Proposition 2.3 (Jordan)**.** *Let k be an imaginary quadratic field which splits B, and such that a prime $p > 7$, $p \not\equiv 1 \bmod 4$, is inert in k. Denote by $\mathfrak{p}$ the unique prime of k over p. Then for any $Q_\mathfrak{p} \in X(k_\mathfrak{p})$ the restriction of the character $\phi_{Q_\mathfrak{p}}$ to the inertia subgroup of the Galois group of the maximal abelian extension of $k_\mathfrak{p}$ is surjective onto $\mathbb{F}_{p^2}^{*12}$.*

Proof. As in the beginning of the previous proof any point $Q_\mathfrak{p} \in X(k_\mathfrak{p})$ represents a QM-abelian surface (A, i) defined over $k_\mathfrak{p}$. To this surface one associates a character ρ_A. By Lemma 2.1 we can write ρ_A^{12} for $\phi_{Q_\mathfrak{p}}$.

Let $U_\mathfrak{p}$ be the group of units of the ring of integers of $k_\mathfrak{p}$, and let $\omega_\mathfrak{p} : U_\mathfrak{p} \to I(\mathfrak{p})$ be the Artin map. For $u \in U_\mathfrak{p}$ we write $\tilde{u} \in \mathbb{F}_{p^2}^*$ for the reduction of u modulo $\mathfrak{p}$. Since $U_\mathfrak{p}$ is an extension of $\mathbb{F}_{p^2}^*$ by a pro-p-group, and the homomorphism $\rho_A \circ \omega_\mathfrak{p} : U_\mathfrak{p} \to \mathbb{F}_{p^2}^*$ is trivial on the pro-p-part, we have that ρ_A factors through a homomorphism $\mathbb{F}_{p^2}^* \to \mathbb{F}_{p^2}^*$. Hence we can write $\rho_A(\omega_\mathfrak{p}(u)) = (\tilde{u})^{-c}$ for an integer c which is uniquely defined modulo $p^2 - 1$.

The Galois group $\mathrm{Gal}(\overline{k}/k)$ acts on $A[p]/C_p$ via the conjugate character ρ_A^p, thus $\rho_A^{p+1} = \mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\rho_A)$ is the cyclotomic character χ_p. We have $\chi_p(u) = \mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\tilde{u})^{-1}$ (cf. [8], XIV, 7, remark 1). Hence $c \equiv 1 \bmod p - 1$.

Consider C_p as a group subscheme of the abelian surface with good reduction A_K, where K is a totally ramified extension of $k_\mathfrak{p}$ of degree $n(A) = |\Phi(A/k_\mathfrak{p})|$ constructed in the proof of Proposition 2.2 (for $p > 3$ the number $n(A)$ can be 1, 2, 3, 4, or 6). Then $C_p \subset A_K$ extends to a finite flat group scheme over the ring of integers $\mathcal{O}_K$. Raynaud's theorem implies that $n(A)c \equiv d_0 + d_1 p \bmod p^2 - 1$, where $0 \leq d_i \leq n(A)$, $i = 1, 2$. We are free to change the isomorphism $C_p \simeq \mathbb{F}_{p^2}$; this replaces c by pc. Elementary computations then show that for $p > n(A)$ we have, possibly after replacing c by pc, either $12c \equiv 12 \bmod p^2 - 1$, or $12c \equiv 12 + 4(p-1) \bmod p^2 - 1$. In both cases c is coprime to $(p^2 - 1)/12$. Therefore, $\rho_A^{12}(I(\mathfrak{p})) = \mathbb{F}_{p^2}^{*12}$. QED

The next result is an adaptation of Theorem 6.1 of [3].

Theorem 2.4. *Let B be a rational indefinite quaternion algebra ramified at a prime $p \geq 11$, $p \equiv 3 \bmod 4$, and X be the Shimura curve defined by B. Assume that B is split by an imaginary quadratic field k in which p is inert, and denote by $\mathfrak{p}$ the unique prime of k over p. Assume also that there is no surjective homomorphism from the ray class group of k of conductor $\mathfrak{p}$ to the product of the class group Cl_k and $\mathbb{Z}/\frac{p^2-1}{12}$. Then $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$.*

Proof. We can assume that $X(\mathbb{A}_k) \neq \emptyset$ as otherwise there is nothing to prove. We want to prove that no family of local characters ϕ_{Q_v} such that $Q_v \in X(k_v)$ comes from a character of $\mathrm{Gal}(\overline{k}/k)$. This means that no twist of the covering Y of X has points everywhere locally. Then the theorem will follow from the main theorem of the descent theory of Colliot-Thélène and Sansuc applied to the torsor $Y \to X$ (see [12], Thm. 6.1.2).

Assume for contradiction that the family of local characters ϕ_{Q_v} for some $Q_v \in X(k_v)$ comes from a character ϕ of $\mathrm{Gal}(\overline{k}/k)$. Proposition 2.2 implies that ϕ is unramified away from $\mathfrak{p}$. The inertia subgroup of the Galois group of the maximal abelian extension of $k_\mathfrak{p}$ is an extension of $(\mathcal{O}_k/\mathfrak{p})^*$ by a pro-p-group. Any homomorphism to the group of order $(p^2-1)/12$ is trivial on the pro-p-part, hence ϕ factors through the generalized class group $\mathrm{Cl}_k^\mathfrak{p}$ of conductor $\mathfrak{p}$, which is the Galois group of the ray class field of k of conductor $\mathfrak{p}$. The natural map $\mathrm{Cl}_k^\mathfrak{p} \to \mathrm{Cl}_k$ fits into the exact sequence

$$1 \to (\mathcal{O}_k/\mathfrak{p})^*/\mathcal{O}_k^* \to \mathrm{Cl}_k^\mathfrak{p} \to \mathrm{Cl}_k \to 1.$$

By Proposition 2.3 the restriction of ϕ to $(\mathcal{O}_k/\mathfrak{p})^*/\mathcal{O}_k^*$ is surjective, a contradiction. QED

3. Congruence conditions

Let q be a prime number. Let $P(q)$ be the set of prime factors of the non-zero integers in the sets $\{a, a \pm q, a \pm 2q, a^2 - 3q^2\}$, where $|a| \leq 2q$. If $q \neq 2$ we let $\mathcal{B}(q)$ be the set of rational indefinite quaternion algebras such that $\mathbb{Q}(\sqrt{-q})$ does not split B. Let $\mathcal{B}(2)$ be the set of rational indefinite quaternion algebras such that neither $\mathbb{Q}(\sqrt{-1})$ nor $\mathbb{Q}(\sqrt{-2})$ splits B. Define $\mathcal{C}(q) \subset \mathcal{B}(q)$ as the set of algebras in $\mathcal{B}(q)$ with reduced discriminant divisible by a prime $p \notin P(q)$. It is clear that the set $\mathcal{B}(q) \setminus \mathcal{C}(q)$ is finite.

The following result is an adaptation of Theorem 6.3 of [3].

Theorem 3.1. *Let k be an imaginary quadratic field in which q is ramified, B a quaternion algebra in $\mathcal{C}(q)$ which is split by k, and X the Shimura curve defined by B. Then $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$.*

Proof. Let $p \notin P(q)$ be a prime factor of the reduced discriminant D of B. Since $p|D$ and k splits B, the prime p is either inert or ramified in k. Let $\mathfrak{p}$ be the unique prime of k over p.

We assume that $X(\mathbb{A}_k) \neq \emptyset$ as otherwise there is nothing to prove. A point $Q_v \in X(k_v)$ defines a character $\phi_{Q_v} : \mathrm{Gal}(\overline{k_v}/k_v) \to \mathbb{F}_{p^2}^{*12}$. Our goal is to prove that there does not exist a family of points $Q_v \in X(k_v)$ for all non-archimedean completions k_v of k, such that the characters ϕ_{Q_v} come from a character $\phi : \mathrm{Gal}(\overline{k}/k) \to \mathbb{F}_{p^2}^{*12}$. Then we can conclude as in the previous theorem by appealing to Thm. 6.1.2 of [12].

As in the previous section, Q_v represents a QM-abelian surface (A_v, i_v) defined over k_v, to which is attached a character ρ_{A_v} such that $\phi_{Q_v} = \rho_{A_v}^{12}$.

Suppose on the contrary that a global character ϕ exists. Then the restriction of ϕ to $\mathrm{Gal}(\overline{k_v}/k_v)$ is $\phi_{Q_v} = \rho_{A_v}^{12}$ which is unramified for $v \neq \mathfrak{p}$ by Proposition 2.2.

Let $\mathfrak{q}$ be the unique prime of k above q, and let $\mathrm{Frob}_\mathfrak{q} \in \mathrm{Gal}(\overline{k}/k)^{\mathrm{ab}}$ be a Frobenius at $\mathfrak{q}$. By global class field theory we have an exact sequence

$$\prod_v U_v \to \mathrm{Gal}(\overline{k}/k)^{\mathrm{ab}} \to \mathrm{Cl}_k \to 0,$$

where v ranges over all primes of k, U_v is the group of units of the ring of integers of k_v, and $U_v \to \mathrm{Gal}(\overline{k}/k)^{\mathrm{ab}}$ is defined by the Artin map ω_v. Since $\mathfrak{q}^2 = (q)$ the order of the image of $\mathrm{Frob}_\mathfrak{q}$ in the class group divides 2, hence $\mathrm{Frob}_\mathfrak{q}^2$ comes from an element of $\prod_v U_v$. This element can be made explicit. Note that $\mathrm{Frob}_\mathfrak{q}$ comes from the idèle all of whose components equal 1 except the component at $\mathfrak{q}$ which equals π, a uniformizer at $\mathfrak{q}$. Then $\mathrm{Frob}_\mathfrak{q}^2$ comes from the idèle all of whose

components equal $1/q$ except the component at q which equals π^2/q. This last idèle is in $\prod_v U_v$, and so it is a lifting of $\mathrm{Frob}_{\mathfrak{q}}^2$ to $\prod_v U_v$. Since ϕ is unramified away from $\mathfrak{p}$ we have $\phi(\omega_v(U_v)) = 1$. It follows that $\phi(\mathrm{Frob}_{\mathfrak{q}}^2) = \phi(\omega_{\mathfrak{p}}(q^{-1})) = \rho_{A_{\mathfrak{p}}}^{12}(\omega_{\mathfrak{p}}(q^{-1}))$. (There is an alternative argument based on the global reciprocity for the norm residue symbol (ϕ, q).)

Let us first deal with the case when p is inert in k. We think of q as an element of $U_{\mathfrak{p}}$ and follow the proof of Proposition 2.3. We have $\rho_{A_{\mathfrak{p}}}(\omega_{\mathfrak{p}}(q)) \equiv q^{-c} \bmod p$, where c is 1 modulo $p-1$, hence $\rho_{A_{\mathfrak{p}}}(\omega_{\mathfrak{p}}(q^{-1})) \equiv q \bmod p$. If p is ramified in k, then the arguments in the proof of Proposition 2.3 should be slightly modified. Now $U_{\mathfrak{p}}$ is an extension of $\mathbb{F}_p^*$ by a pro-p-group, the homomorphism $\rho_{A_{\mathfrak{p}}} \circ \omega_{\mathfrak{p}}$ factors through the natural injection $\mathbb{F}_p^* \to \mathbb{F}_{p^2}^*$, and we again have $\rho_{A_{\mathfrak{p}}}(\omega_{\mathfrak{p}}(q)) \equiv q^{-c} \bmod p$. However in this case we only have $2c \equiv 2 \bmod p-1$ ([3], Prop. 4.8). This implies $\rho_{A_{\mathfrak{p}}}(\omega_{\mathfrak{p}}(q^{-1})) \equiv \pm q \bmod p$. In both cases we obtain $\phi(\mathrm{Frob}_{\mathfrak{q}}^2) = \rho_{A_{\mathfrak{p}}}^{12}(\omega_{\mathfrak{p}}(q^{-1})) \equiv q^{12} \bmod p$.

Restricting ϕ to $\mathrm{Gal}(\overline{k_{\mathfrak{q}}}/k_{\mathfrak{q}})$ we get $\rho_{A_{\mathfrak{q}}}^{12}(\mathrm{Frob}_{\mathfrak{q}}^2) \equiv q^{12} \bmod p$. Therefore in $\mathbb{F}_{p^2}$ we have the equality $\rho_{A_{\mathfrak{q}}}(\mathrm{Frob}_{\mathfrak{q}}^2) = \varepsilon q$, where $\varepsilon \in \mathbb{F}_{p^2}$, $\varepsilon^{12} = 1$.

In the proof of Proposition 2.2 we constructed a QM-abelian surface $\tilde{A}_{\mathfrak{q}}$ over $\mathbb{F}_q$ such that the action of $\mathrm{Frob}_{\mathfrak{q}}$ on the Tate modules $T_p(A_{\mathfrak{q}})$ and $T_p(\tilde{A}_{\mathfrak{q}})$ is the same. The characteristic polynomial of $\mathrm{Frob}_{\mathfrak{q}}^2$ reduced modulo p is the square of $(t - \rho_{A_{\mathfrak{q}}}(\mathrm{Frob}_{\mathfrak{q}}^2))(t - \rho_{A_{\mathfrak{q}}}^p(\mathrm{Frob}_{\mathfrak{q}}^2))$, and so $\mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(\rho_{A_{\mathfrak{q}}}(\mathrm{Frob}_{\mathfrak{q}}^2)) = (\varepsilon+\varepsilon^{-1})q$ is the reduction modulo p of an integer a of absolute value at most $2q$. Since $\varepsilon^{12} = 1$ we have the following possibilities: $a \equiv 0, \pm q, \pm 2q \bmod p$ or $a^2 \equiv 3q^2 \bmod p$. Assume first that q divides a. From the Honda–Tate theory and the fact that $\rho_{A_{\mathfrak{q}}}(\mathrm{Frob}_{\mathfrak{q}}) + q\rho_{A_{\mathfrak{q}}}^{-1}(\mathrm{Frob}_{\mathfrak{q}})$ is an integer one deduces the following list of possibilities (see [3], Thm. 2.1):

$a = 0$, then $q = 2$ and $\mathbb{Q}(\sqrt{-1})$ splits B;
$a = 3$, then $q = 3$ and $\mathbb{Q}(\sqrt{-3})$ splits B;
$a = -2q$, then $\mathbb{Q}(\sqrt{-q})$ splits B.

Each of these conditions contradicts the assumption that the algebra B is in $\mathcal{C}(q)$. Now if q and a are coprime, then p divides one of the non-zero integers a, $a \pm q$, $a \pm 2q$, $a^2 - 3q^2$, where $|a| \le 2q$. This contradiction finishes the proof. QED

It is worth spelling out the theorem in the case $q = 2$. One easily computes $P(2) = \{2, 3, 5, 7, 11\}$, which leads to the following

Corollary 3.2. *Let $k = \mathbb{Q}(\sqrt{d})$, where $d < 0$ is congruent to 2 or 3 modulo 4. Let B be a rational indefinite quaternion algebra split by k, whose discriminant is divisible by a prime greater than 11, a prime congruent to 1 modulo 4 and a prime congruent to 1 or 3 modulo 8 (these primes do not have to be distinct). Then $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$, where X is the Shimura curve defined by B.*

4. Examples

1. In Example 6.4 of [3] Jordan considers the case $D = 39$ and $k = \mathbb{Q}(\sqrt{-13})$. The corresponding Shimura curve X has points everywhere locally over k, as can be checked using [5]. For this particular Shimura curve the property $X(\mathbb{A}_k)^{\mathrm{Br}} = \emptyset$ was explicitly checked in [11] using a conjectural equation of X found by A. Kurihara. Corollary 3.2 does this unconditionally.

2. A numerical example of Theorem 2.4 over the field $\mathbb{Q}(\sqrt{-23})$ can be found in [7]. It is the Shimura curve X attached to the quaternion algebra of discriminant $23 \cdot 107$. The genus of X is 193. Computations based on Theorem 2.5 of [5] show that $X(\mathbb{Q}_\ell) \ne \emptyset$ unless $\ell = 23$ or $\ell = 107$, but Theorems 5.1 and 5.4 of the same paper imply that X has points in the completions of $\mathbb{Q}(\sqrt{-23})$ at the primes over 107 and 23. Thus X has points in all completions of $\mathbb{Q}(\sqrt{-23})$. An application of

Theorem 2.4 with $p = 107$ shows that X is a counterexample to the Hasse principle over $\mathbb{Q}(\sqrt{-23})$ accounted for by the Manin obstruction. Indeed,

$$\mathrm{Cl}^{(107)}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/17172 \simeq \mathbb{Z}/4 \times \mathbb{Z}/81 \times \mathbb{Z}/53,$$

whereas $\mathrm{Cl}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/3$, so that

$$\mathbb{Z}/\big(\frac{107^2-1}{12}\big) \times \mathrm{Cl}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/2 \times \mathbb{Z}/9 \times \mathbb{Z}/53 \times \mathbb{Z}/3,$$

and the conditions of Theorem 2.4 are satisfied.

3. Let us now discuss counterexamples to the Hasse principle over $\mathbb{Q}$ constructed in [7]. These counterexamples use curves which are closely related to Shimura curves. Namely, consider the twist X' of the Shimura curve X from the previous example by the quadratic field $k = \mathbb{Q}(\sqrt{-23})$ with respect to the Atkin–Lehner involution ω_{107}. Thm. 7.2 and Prop. 5.7 of [14] imply that this counterexample is explained by the Manin obstruction. More precisely, the arguments in Section 5 of [14] show that this can be achieved using the descent attached to the restriction of the covering $R_{k/\mathbb{Q}}Y \to R_{k/\mathbb{Q}}X$ to X' with respect to the canonical morphism $X' \to R_{k/\mathbb{Q}}X' = R_{k/\mathbb{Q}}X$.

4. We explained the previous three counterexamples to the Hasse principle by the Manin obstruction by pointing to an abelian étale covering such that no twisted form of it has points everywhere locally. Let us consider a counterexample to the Hasse principle over $\mathbb{Q}$ for which we do not have a ready made descent argument. Let C be the quotient of X by ω_{107}. It is shown in [7] that X' is the only twisted form of the covering X of C which has points everywhere locally over $\mathbb{Q}$. Since $X'(\mathbb{Q}) = \emptyset$ we conclude that C is a counterexample to the Hasse principle over $\mathbb{Q}$.

Let us show how to explain this counterexample by the Manin obstruction. M. Stoll proved ([14], Cor. 6.10) that if a smooth and projective curve S has a non-constant morphism to an abelian variety A such that $A(\mathbb{Q})$ and the Tate–Shafarevich group of A are finite, then $S(\mathbb{Q})$ is in a natural bijection with the set of connected components of $S(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}}$. In particular, if $S(\mathbb{Q}) = \emptyset$, then $S(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$.

An appropriate combination of CM-points on C gives a divisor of degree 1 (see [7]). This divisor defines an embedding of C into its Jacobian J such that the image of C is not contained in a translate of a proper abelian subvariety of J. It is a deep but well known result that the Jacobian of X is isogenous to the new part of the Jacobian $J_0(D)$ of the modular curve $X_0(D)$ (this uses Jacquet–Langlands, Faltings, Ribet, ...). It follows that J is isogenous to the ω_{107}-anti-invariant part of $J_0(D)$ (since the Atkin–Lehner involutions acting on the modular and the Shimura sides differ by -1). From the results of Kolyvagin–Logachev (complemented by Gross–Zagier, Bump–Friedberg–Hoffstein and Murty–Murty) it follows that any quotient A of $J_0(D)$ of analytic rank 0 also has algebraic rank 0 and a finite Tate–Shararevich group. A glance at W. Stein's tables of modular forms (http://modular.fas.harvard.edu) shows that $J_0(D)$ has an ω_{107}-anti-invariant quotient of analytic rank 0 of dimension 54 (defined by a certain Hecke eigenform of level 2461 and weight 2). This finishes the proof of our claim.

It is clear that $C(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$ implies $X'(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}} = \emptyset$. This gives an alternative approach to the previous example.

The author thanks Kevin Buzzard, Victor Rotger, Andrei Yafaev for many helpful discussions, and Michael Stoll for sending his preprint [14].

References

[1] J-F. Boutot et H. Carayol, Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld. In: Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). *Astérisque* **196-197** (1992) 45–158.

[2] P.L. Clark, *Local and global points on moduli spaces of abelian surfaces with potential quaternionic multiplication*, PhD Thesis, Harvard, 2003.

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

[4] B.W. Jordan, *On the Diophantine arithmetic of Shimura curves*, PhD Thesis, Harvard, 1981.

[5] B.W. Jordan and R. Livné, Local diophantine properties of Shimura curves. *Math. Ann.* **270** (1985) 235–248.

[6] B. Mazur, Rational isogenies of prime degree. *Inv. Math.* **44** (1978) 129–162.

[7] 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), to appear.

[8] J-P. Serre, *Corps locaux*, Hermann, 1968.

[9] J-P. Serre and J. Tate, Good reduction of abelian varieties. *Ann. Math.* **88** (1968) 492–517.

[10] G. Shimura, Construction of class fields and zeta functions of algebraic curves. *Ann. Math.* **85** (1967) 58–159.

[11] S. Siksek and A. Skorobogatov, On a Shimura curve that is a counterexample to the Hasse principle. *Bull. London Math. Soc.* **35** (2003) 409–414.

[12] A. Skorobogatov, *Torsors and rational points*, Cambridge University Press, 2001.

[13] A. Skorobogatov and A. Yafaev, Descent on certain Shimura curves. *Israel J. Math.* **140** (2004) 319–332.

[14] M. Stoll, *Finite descent and rational points on curves*. Preprint, 2005.

[15] M-F. Vignéras, *Arithmétique des algèbres de quaternions*. Lecture Notes Math. **800**, 1980.

Department of Mathematics, Imperial College London, South Kensington Campus, London SW7 2AZ England.

E-mail address: a.skorobogatov@imperial.ac.uk