FAILURE OF THE HASSE PRINCIPLE FOR ATKIN–LEHNER QUOTIENTS OF SHIMURA CURVES OVER $\mathbb{Q}$

VICTOR ROTGER, ALEXEI SKOROBOGATOV AND ANDREI YAFAEV

Abstract. We show how to construct counter-examples to the Hasse principle over the field of rational numbers on Atkin–Lehner quotients of Shimura curves and on twisted forms of Shimura curves by Atkin–Lehner involutions. A particular example is the quotient of the Shimura curve $X_{23\cdot 107}$ attached to the indefinite rational quaternion algebra of discriminant $23\cdot 107$ by the Atkin–Lehner involution ω_{107}. The quadratic twist of $X_{23\cdot 107}$ by $\mathbb{Q}(\sqrt{-23})$ with respect to this involution is also a counter-example to the Hasse principle over $\mathbb{Q}$.

Introduction

A systematic approach to the Hasse principle for smooth and projective curves of genus greater than one does not seem to be known. It is an open question whether or not the Manin obstruction to the Hasse principle suffices to explain all possible counter-examples to it. We refer the reader to [22], p. 127–128, for a survey of a small number of available results and examples.

Shimura curves provide a lot of possibilities to experiment with the Hasse principle due to a range of well established tools like the Eichler–Selberg trace formula, modular interpretation, the Cherednik–Drinfeld p-adic uniformization. These enabled Jordan and Livné [8] to find the necessary and sufficient conditions for the existence of points over local fields on these curves. Previously Shimura [20] proved that Shimura curves have no real points. In [7] Jordan studied the points on Shimura curves over number fields, extending some of the ideas of the celebrated paper of Mazur [10]. In particular, he found a Shimura curve which is a counter-example to the Hasse principle over an imaginary quadratic field. This counter-example can be accounted for by the Manin obstruction [21], subject to the verification that the conjectured explicit equations of this curve found by A. Kurihara are correct. (Note that equations of Shimura curves are in general hard to find, which is why they are seldom used to study rational points.) Recently two of the present authors used descent for a certain natural unramified Galois covering of Shimura curves with level structure to produce a large family of counter-examples to the Hasse principle [24], again over imaginary quadratic fields. Independently, Clark in his thesis showed

1991 *Mathematics Subject Classification.* 11G18, 14G35.

Key words and phrases. Shimura curves, rational points, Hasse principle, descent.

that when the level and the reduced discriminant are large such curves violate the Hasse principle for infinitely many imaginary quadratic fields ([4], Thm. 121).

To construct similar examples over the field of rational numbers one can no longer use Shimura curves in the strict sense for they have no real points. In this note we construct a counter-example to the Hasse principle over $\mathbb{Q}$ on the quotient of a Shimura curve by an Atkin–Lehner involution without fixed points. In Section 2 we study local points on such quotients in the case of good reduction following the approach of Jordan and Livné, and then in Section 3 we summarize the work of Ogg in the case of bad reduction. This leads to a criterion for the existence of adelic points on Atkin–Lehner quotients (Theorem 3.1, see also Corollary 3.3). In Section 4 some of these results are also obtained by another method based on the determination of the fields of definition of CM-points by Jordan ([6], Ch. 3). In Section 5 we apply descent to the double covering given by the original Shimura curve. For this we need to analyse local points on the twisted coverings which are quadratic twists of the Shimura curve with respect to the Atkin–Lehner involution. We consider an explicit example where only one quadratic twist turns out to be everywhere locally soluble. However, a global result of Jordan [7] implies that it has no $\mathbb{Q}$-points, so this twisted Shimura curve is itself a counter-example to the Hasse principle over $\mathbb{Q}$. This fact does not allow us to conclude that our counter-example is accounted for by the Manin obstruction, though we see no particular reason why it should not be so. In Proposition 4.3 we use CM-points to construct a rational divisor of degree one on our curve.

1. **Preliminaries**

Let B_D be a quaternion algebra over $\mathbb{Q}$ of reduced discriminant $D \neq 1$, and let $\mathcal{O}_D$ be a maximal order in B_D. Let $n : B_D \to \mathbb{Q}$ be the reduced norm. The quaternion algebra B_D is indefinite if $B_D \otimes \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R})$, or, equivalently, if $D = p_1 \dots p_{2s}$ for distinct prime numbers p_i; B_D is definite if $B_D \otimes \mathbb{R}$ is the Hamilton quaternion algebra $(\frac{-1,-1}{\mathbb{R}})$, that is, if $D = p_1 \dots p_{2s+1}$.

When B_D is indefinite we can view $\Gamma = \{\gamma \in \mathcal{O}_D | n(\gamma) = 1\}$ as an arithmetic subgroup of $\mathrm{SL}_2(\mathbb{R})$ through the identification of $B_D \otimes \mathbb{R}$ with $M_2(\mathbb{R})$, and consider the Riemann surface $\Gamma\backslash\mathcal{H}$, where $\mathcal{H}$ is the upper-half plane. Shimura showed [19] that $\Gamma\backslash\mathcal{H}$ is the set of complex points of a projective curve X_D over $\mathbb{Q}$ parameterizing abelian surfaces with quaternionic multiplication by $\mathcal{O}_D$. The genus of X_D is given by the Eichler mass formula ([1], Ch. II, [23], p. 120).

Let $B_D^+ = \{\beta \in B_D | n(\beta) > 0\}$, and let $N(\Gamma)$ be the normalizer of Γ in B_D^+. The quotient of $N(\Gamma)$ by $\mathbb{Q}^* \cdot \Gamma$ is called the Atkin–Lehner group W. For any positive integer m dividing D there is an element $\omega_m \in \mathcal{O}_D$ of reduced norm m. Then $\{\omega_m\}$ is a set of representatives of W. We have $[\omega_m \cdot \omega'_m] = [\omega_{mm'/(m,m')^2}]$, hence $W \cong (\mathbb{Z}/2\mathbb{Z})^{2s}$. The elements of the Atkin–Lehner group act as involutions on the

Shimura curve X_D, and there is a natural inclusion $W \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D)$ (see, e.g., [15]). The number of fixed points of ω_m was found by Ogg ([13], (4) p. 286).

For any integer $m > 1$ dividing D we write $X_D^{(m)} = X_D/\omega_m$ for the quotient of the Shimura curve X_D by the Atkin–Lehner involution ω_m. These curves can be given modular interpretation through their embedding into the Hilbert–Blumenthal surfaces or the Igusa threefold $\mathcal{A}_2$ (cf. [16], [17]). They are also interesting in connection with the modularity conjectures for abelian surfaces with quaternionic multiplication (cf. [3]).

For any order R in an imaginary quadratic field K let $h(R)$ denote its class number, $\mathrm{cond}(R)$ its conductor, $\omega(R)$ the number of roots of unity in R, and $s(K)$ the number of primes $p \mid D$ which are inert in K. For any positive integer n we define

$$\Sigma_n(D) = \sum_{t \in \mathbb{Z},\ t^2 < 4n} \sum_{R} \frac{2^{s(K)} h(R)}{\omega(R)},$$

where R ranges through the set of orders in imaginary quadratic fields K such that R contains the roots of $x^2 + tx + n$, $(\mathrm{cond}(R), D) = 1$, and no prime factor of D splits in K. Note that there may be no terms in this sum. We set $\Sigma_n(D) = 0$ if n is not a positive integer.

Lemma 1.1 (Eichler's criterion)**.** *Let R be an order in a quadratic field K, and let B_D be a division quaternion algebra over $\mathbb{Q}$ of reduced discriminant D. A maximal order $\mathcal{O} \subset B_D$ and an embedding $\iota : R \hookrightarrow \mathcal{O}$ such that $\iota(R) = \iota(K) \cap \mathcal{O}$ exist if and only if $(\mathrm{cond}(R), D) = 1$, no prime factor of D splits in K, and K is imaginary if B_D is definite.*

Proof. See [23], Ch. III, Thm. 5.11, 5.15 and 5.16, [13], §1. □

An embedding $\iota : R \hookrightarrow \mathcal{O}$ such that $\iota(R) = \iota(K) \cap \mathcal{O}$ is usually called *optimal*. Note that it follows from Eichler's criterion that if a quadratic order R of K optimally embeds into $\mathcal{O}$, then the ring of integers R_K of K also has an optimal embedding into K.

If B_D is indefinite there is only one class of maximal orders in B_D up to conjugation. Hence a quadratic order R admits an optimal embedding into either none or all maximal orders of B_D. However, this is no longer true when B_D is definite: there may be several conjugacy classes of maximal orders, and R may admit an optimal embedding into some but not all of them.

Lemma 1.2. *Let $D = p_1 \dots p_{2s}$, $s \geq 1$, and $n \in \mathbb{Z}$, $n \geq 1$. Then $\Sigma_n(D)$ is non-zero if and only if there exists an imaginary quadratic field K which splits B_D and contains an integral element of norm n.*

Proof. A quadratic field K splits B_D if and only if K can be embedded into B_D, and also if and only if every prime factor q of D is inert or ramified in K. If there

exists a splitting imaginary quadratic field K with an integral element of norm n, then the ring of integers R_K of K contributes to the expression for $\Sigma_n(D)$; hence the sum is non-zero. Conversely, if $\Sigma_n(D) \neq 0$ and R is an order in an imaginary quadratic field K that contributes to $\Sigma_n(D)$, then K satisfies the conditions of the lemma. □

2. **Local points: good reduction**

Let $m > 1$ be an integer dividing D, and let $p \nmid D$ be a prime. Morita ([12], Thm. 1) proved that the curves X_D and $X_D^{(m)}$ have good reduction at p. Let $\tilde{X}_D$ (resp. $\tilde{X}_D^{(m)}$) denote the reduction of Morita's integral model of X_D (resp. of $X_D^{(m)}$) at p. The natural surjective morphism $f : X_D \to X_D^{(m)}$ extends to a morphism of Morita's models ([12], Thm. 2), moreover, the morphism of the closed fibres $f : \tilde{X}_D \to \tilde{X}_D^{(m)}$ is separable ([12], Thm. 3 (*iii*)).

In this section we determine the zeta function of $\tilde{X}_D^{(m)}$, and explicitly compute the number of $\mathbb{F}_{p^r}$-points on this curve. We also consider twisted forms of X_D with respect to the action of ω_m.

Proposition 2.1. *Let p be a prime not dividing D, and $m > 1$ an integer dividing D. The number of $\mathbb{F}_{p^r}$-points on the $\mathbb{F}_p$-curve $\tilde{X}_D^{(m)}$ equals*

$$\left|\tilde{X}_D^{(m)}(\mathbb{F}_{p^r})\right| = \frac{\Sigma_{p^r}(D) + \Sigma_{mp^r}(D)}{2} - p\frac{\Sigma_{p^{r-2}}(D) + \Sigma_{mp^{r-2}}(D)}{2} + \delta(r)\frac{p-1}{24}\prod_{q|D}(q-1),$$

where $\delta(r) = 0$ if r is odd, $\delta(r) = 1$ if r is even, and q ranges over the prime factors of D.

Proof. We refer to Sect. 5.3 of [11] for the definition of Hecke operators T_n, $n \geq 1$, in the case of unit groups of quaternion algebras. Note that for $m|D$ we have $T_m = \omega_m$. The Hecke operators act on the vector space $H^0(X_D, \Omega^1)$ of regular complex differentials of X_D. The $+1$-eigenspace of T_m can be identified with $H^0(X_D^{(m)}, \Omega^1)$. Let us write $T_n^{(m)}$ for the restriction of T_n to this eigenspace. In what follows the trace $\mathrm{tr}(T_n)$ is taken over the vector space $H^0(X_D, \Omega^1)$, and the trace $\mathrm{tr}(T_n^{(m)})$ is taken over the $+1$-eigenspace of T_m.

As in [8] the Eichler–Shimura relations determine the Zeta-function of $\tilde{X}_D^{(m)}/\mathbb{F}_p$:

$$Z(\tilde{X}_D^{(m)}/\mathbb{F}_p, t) = \frac{\det(1 - T_p^{(m)}t + pt^2)}{(1-t)(1-pt)}.$$

From this it follows by an argument of Ihara (cf. [8], Prop. 2.1) that for any $r \geq 1$ we have

$$\left|\tilde{X}_D^{(m)}(\mathbb{F}_{p^r})\right| = 1 + p^r - \mathrm{tr}(T_{p^r}^{(m)}) + p\mathrm{tr}(T_{p^{r-2}}^{(m)}),$$

where we set $T^{(m)}_{p^{-1}} = 0$. Since $T_n \cdot T_{n'} = T_{n'} \cdot T_n = T_{n'n}$ when $(n, n') = 1$, and T_m is an involution, we have $\mathrm{tr}(T^{(m)}_n) = (\mathrm{tr}(T_n) + \mathrm{tr}(T_{mn}))/2$ for any $(n, m) = 1$.

The trace $\mathrm{tr}(T_n)$ is computed by the Eichler–Selberg trace formula (see [11], Thm. 6.8.4 and Remark 6.8.1; see [24], Prop. 1.4 for a minor correction):

$$\mathrm{tr}(T_n) = \prod_{p^r || n,\ p \nmid D} (1 + p + ... + p^r) - \Sigma_n(D) + ss,$$

where $ss = 0$ if n is not a perfect square, while $ss = \prod_{q|D}(q-1)/12$ otherwise. The application of this formula finishes the proof. □

Corollary 2.2. *For any $p \nmid D$ we have $X^{(m)}_D(\mathbb{Q}_p) \neq \emptyset$ if and only if $\Sigma_p(D) \neq 0$ or $\Sigma_{mp}(D) \neq 0$.*

Proof. This follows from the previous proposition and Hensel's lemma. □

For any field k the non-zero elements of $H^1(k, \mathbb{Z}/2)$ bijectively correspond to quadratic extensions of k. To a k-variety X with an action of $\mathbb{Z}/2$ one associates twisted forms ${}^\sigma X$ defined, up to isomorphism, by the classes $\sigma \in H^1(k, \mathbb{Z}/2)$. The action of the Atkin–Lehner involution ω_m on X_D allows us to consider the twisted forms of X_D over $\mathbb{Q}$. The elements of $H^1(\mathbb{Q}, \mathbb{Z}/2)$ bijectively correspond to the quadratic fields $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Q}^*/\mathbb{Q}^{*2}$. With this correspondence in mind we write ${}^d X_D$ for the twisted form ${}^\sigma X_D$. Each of the twisted curves is equipped with a morphism to $X^{(m)}_D$, which is a $\overline{\mathbb{Q}}/\mathbb{Q}$-form of the double covering $f : X_D \to X^{(m)}_D$. Every point $P \in X^{(m)}_D(\mathbb{Q})$ in which f is unramified lifts to exactly one twisted form, namely to ${}^d X_D$ such that $\mathbb{Q}(f^{-1}(P)) = \mathbb{Q}(\sqrt{d})$.

We can also twist the $\mathbb{F}_p$-curve $\tilde{X}_D$. The non-zero element $\sigma \in H^1(\mathbb{F}_p, \mathbb{Z}/2) \simeq \mathbb{Z}/2$ corresponds to $\mathbb{F}_{p^2}/\mathbb{F}_p$, and the non-trivial twist of $\tilde{X}_D$ is unique up to isomorphism.

Proposition 2.3. *Let p be a prime not dividing D, and $m > 1$ an integer dividing D. The number of $\mathbb{F}_{p^r}$-points on the $\mathbb{F}_p$-curve ${}^\sigma \tilde{X}_D$, where σ is the non-zero element of $H^1(\mathbb{F}_p, \mathbb{Z}/2)$, equals*

$$\left|{}^\sigma \tilde{X}_D(\mathbb{F}_{p^r})\right| = \left|\tilde{X}_D(\mathbb{F}_{p^r})\right| = \Sigma_{p^r}(D) - p\Sigma_{p^{r-2}}(D) + \frac{p-1}{12}\prod_{q|D}(q-1),$$

if r is even (here q ranges over the prime factors of D), and

$$\left|{}^\sigma \tilde{X}_D(\mathbb{F}_{p^r})\right| = \Sigma_{mp^r}(D) - \Sigma_{mp^{r-2}}(D),$$

if r is odd.

Proof. If r is even, the curves $\tilde{X}_D$ and ${}^\sigma \tilde{X}_D$ are isomorphic over $\mathbb{F}_{p^r}$. The second equality in our first formula is a particular case of Prop. 2.3 of [8]. Now assume that r is odd. Every point $P \in \tilde{X}^{(m)}_D(\mathbb{F}_{p^r})$ in which the separable double covering

$f : \tilde{X}_D \to \tilde{X}_D^{(m)}$ is unramified lifts to exactly one of the curves $\tilde{X}_D$ or ${}^\sigma\tilde{X}_D$. The $\mathbb{F}_{p^r}$-points where f is ramified lift to both of these curves. Hence we have the equality

$$2\big|\tilde{X}_D^{(m)}(\mathbb{F}_{p^r})\big| = \big|\tilde{X}_D(\mathbb{F}_{p^r})\big| + \big|{}^\sigma\tilde{X}_D(\mathbb{F}_{p^r})\big|.$$

Our second formula now follows from Proposition 2.1. □

Corollary 2.4. *Let d be a square free integer, and let p be a prime not dividing dD. If $(\frac{d}{p}) = 1$, then ${}^dX_D(\mathbb{Q}_p) = X_D(\mathbb{Q}_p) \neq \emptyset$ if and only if $\Sigma_p(D) \neq 0$. If $(\frac{d}{p}) = -1$, then ${}^dX_D(\mathbb{Q}_p) \neq \emptyset$ if and only if $\Sigma_{mp}(D) \neq 0$.*

Proof. The reduction of ${}^dX_D$ at p is isomorphic to $\tilde{X}_D$ or to ${}^\sigma\tilde{X}_D$ depending on whether d is a square at p or not. Now the statement follows from the previous proposition, Prop. 2.3 of [8] and Hensel's lemma. □

Corollary 2.5. *Let m and ℓ be odd primes such that $\ell \equiv 3 \bmod 4$ and $(\frac{-m}{\ell}) = 1$. Then ${}^{-\ell}X_{\ell m}(\mathbb{Q}_p) \neq \emptyset$ if $p \neq m$ is such that $(\frac{-\ell}{p}) = -1$.*

Proof. By Corollary 2.4 it is enough to prove that $\Sigma_{mp}(\ell m) \neq 0$. A non-zero contribution to the double sum in the definition of $\Sigma_{mp}(\ell m)$ comes from the term given by $t = 0$ and the maximal order in $\mathbb{Q}(\sqrt{-mp})$ (cf. Lemma 1.2). Indeed, $B_{\ell m}$ is split by $\mathbb{Q}(\sqrt{-mp})$ since in this field m is ramified and ℓ is inert: by quadratic reciprocity $(\frac{-m}{\ell}) = 1$ and $(\frac{-\ell}{p}) = -1$ imply $(\frac{-mp}{\ell}) = -1$. □

3. **Local points: bad reduction**

We now review the results of Ogg [13], [14] on $\mathbb{Q}_p$-points on $X_D^{(m)}$ for the primes $p \mid D$ of bad reduction (see also [2]). The combination of these results with the results of the previous section sums up in a criterion for the existence of adelic points on $X_D^{(m)}$. We write $\mathbb{A}_\mathbb{Q}$ for the ring of adèles of $\mathbb{Q}$.

Theorem 3.1. *Let $D = p_1 \dots p_{2s}$, $s \geq 1$, be the product of an even number of distinct primes, and let $m > 1$ be an integer dividing D. Let g be the genus of $X_D^{(m)}$. Then $X_D^{(m)}(\mathbb{A}_\mathbb{Q}) \neq \emptyset$ if and only if one of the following conditions holds:*

- *(i)* $m = D$
- *(ii)* $m = D/\ell$ *for a prime* $\ell \neq 2$ *such that*
  - $(\frac{m}{\ell}) = -1$;
  - (a) $(\frac{-m}{\ell}) = 1$, $(\frac{-\ell}{p}) \neq 1$ *for all primes* $p \mid m$, *or* (b) $\ell \equiv 1 \bmod 4$, $p \not\equiv 1 \bmod 4$ *for all primes* $p \mid m$;
  - *when* $s \geq 2$ *we have* $(\frac{-m/p}{\ell}) = -1$ *for all odd primes* $p \mid m$, *and if* $2|D$ *we also have either* $(\frac{-m/2}{\ell}) = -1$, *or* $q \equiv 3 \bmod 4$ *for all primes* $q \mid D/2$;
  - *for every prime* $p \nmid D$, $p < 4g^2$, *we have* $\Sigma_p(D) \neq 0$ *or* $\Sigma_{pD/\ell}(D) \neq 0$.
- *(iii)* $m = D/2$ *such that*
  - $m \not\equiv 1 \bmod 8$;

- $p \equiv 3 \bmod 4$ *for all* $p \mid m$, *or* $p \equiv 5$ *or* $7 \bmod 8$ *for all* $p \mid m$;
- *if* $s \geq 2$, *then for every prime* $p \mid m$ *we have* $m/p \not\equiv -1 \bmod 8$;
- *for every prime* $p \nmid D$, $p < 4g^2$, *we have* $\Sigma_p(D) \neq 0$ *or* $\Sigma_{pD/2}(D) \neq 0$.

Proof. Let p be a prime factor of D/m. It follows from Eichler's criterion and parts $i)$ and $ii)$ of Ogg's theorem in [14], p. 206, that $X_D^{(m)}(\mathbb{Q}_p) \neq \emptyset$ if and only if one of the following conditions holds:

(a) $p = 2$ and either $\ell \equiv 3 \bmod 4$ for all primes $\ell \mid D/2$, or $m = D/2$ and $\ell \equiv 5$ or $7 \bmod 8$ for all primes $\ell \mid D/2$.
(b) $p > 2, m = D/p$ or $m = D/2p$, $(\frac{-m}{p}) = 1, (\frac{-p}{\ell}) \neq 1$ for all primes $\ell \mid D/p$.
(c) $p \equiv 1 \bmod 4$, $m = D/p$ or $m = D/2p$, $\ell \not\equiv 1 \bmod 4$ for all primes $\ell \mid D/p$, and $(\frac{-D/2}{2}) \neq 1$ if $m = D/2p$.

Assume first that there exist two different primes $p, q \mid D$, $p, q \nmid m$ (so that D is the product of at least four different primes) such that $X_D^{(m)}(\mathbb{Q}_p) \neq \emptyset$ and $X_D^{(m)}(\mathbb{Q}_q) \neq \emptyset$. It is clear from (a), (b) and (c) that one of these primes is 2, say $q = 2$, and $D = 2pm$. Moreover, we must have $p \equiv 3 \bmod 4$, $\ell \equiv 3 \bmod 4$ for all primes $\ell \mid m$, $(\frac{-m}{p}) = 1$ and $(\frac{-p}{\ell}) = -1$ for all primes $\ell \mid m$. Since m is the product of an even number of odd primes, we deduce a contradiction with the quadratic reciprocity law. Therefore, m must be as in (i), (ii) or (iii).

Let $m = D$. Ogg's criterion ([13], §3, Prop. 1) for the existence of real points on the Atkin–Lehner quotients of Shimura curves implies that $X_D^{(D)}(\mathbb{R}) \neq \emptyset$. Indeed, by Eichler's criterion, the ring of integers of $\mathbb{Q}(\sqrt{D})$ embeds into any maximal order of B_D, since no prime $p \mid D$ splits in $\mathbb{Q}(\sqrt{D})$.

According to $iv)$ of Ogg's theorem in [14], p. 206, we have $X_D^{(D)}(\mathbb{Q}_p) \neq \emptyset$ for any prime $p \mid D$, because the ring of integers of $\mathbb{Q}(\sqrt{-D/p})$ embeds into some maximal order of the definite quaternion algebra $B_{D/p}$ of discriminant D/p. Indeed, this is guaranteed by Eichler's criterion since no ramified prime $\ell \mid D/p$ of $B_{D/p}$ splits in $\mathbb{Q}(\sqrt{-D/p})$.

We have $X_D^{(D)}(\mathbb{Q}_p) \neq \emptyset$ for all $p \nmid D$, because one may apply Lemma 1.2 and Corollary 2.2 to the splitting quadratic field $\mathbb{Q}(\sqrt{-pD})$. We conclude that $X_D^{(D)}$ has points everywhere locally.

Now let $m = D/\ell$ for some prime ℓ. By Ogg's criterion [13], $X_D^{(m)}(\mathbb{R}) \neq \emptyset$ if and only if the ring of integers of $\mathbb{Q}(\sqrt{m})$ embeds into the maximal orders of B_D; and this holds if and only if $(\frac{m}{\ell}) \neq 1$. Let $p \nmid D$ be a prime of good reduction of $X_D^{(m)}$. It follows from Weil's bound that $\tilde{X}_D^{(m)}(\mathbb{F}_p) \neq \emptyset$ when $p > 4g^2$. By Hensel's lemma this implies that $X_D^{(m)}(\mathbb{Q}_p) \neq \emptyset$. Now the last condition in (ii) and (iii) follows from Corollary 2.2.

It remains to study the necessary and sufficient conditions for the existence of local points at the primes of bad reduction of $X_D^{(m)}$.

Consider the prime ℓ. If ℓ is odd, then by $i)$ and $ii)$ of Ogg's theorem in [14], p. 206, $X_D^{(D/\ell)}(\mathbb{Q}_\ell) \neq \emptyset$ if and only if $D = 2\ell$ with $\ell \equiv 1 \bmod 4$, or (a) $(\frac{-m}{\ell}) = 1$ and $(\frac{-\ell}{p}) \neq 1$ for all primes $p \mid D/\ell$, or (b) $\ell \equiv 1 \bmod 4$ and $p \not\equiv 1 \bmod 4$ for all primes $p \mid D/\ell$. Since the first of these conditions is included in (b), this accounts for the second item in (ii).

For $\ell = 2$ the statements $i)$ and $ii)$ of the same theorem assert that $X_D^{(D/2)}(\mathbb{Q}_2) \neq \emptyset$ if and only if $\sqrt{-1}$ or $\sqrt{-2} \in \mathcal{O}_D$. These conditions are equivalent to the conditions that $p \equiv 3 \bmod 4$ for all primes $p \mid D/2$, and $(\frac{-2}{p}) = -1$ for all primes $p \mid D/2$, respectively. This is the second item in (iii).

We now consider the primes $p \mid m$. Suppose first that m is prime. According to $i)$ and $iii)$ of Ogg's theorem, $X_{m\ell}^{(m)}(\mathbb{Q}_m) \neq \emptyset$ if and only if $m = 2$, $\ell \equiv 3 \bmod 4$, or $\ell = 2, m \equiv 1 \bmod 4$, or some maximal order in B_ℓ contains $\sqrt{-m}$ or a unit $u \neq \pm 1$. Note that under the hypothesis $(\frac{m}{\ell}) \neq 1$ which we already assumed, these conditions do not restrict m and ℓ any further. Indeed, if $\ell \equiv 3 \bmod 4$, then $\sqrt{-1}$ embeds into a maximal order of B_ℓ; if $\ell \equiv 1 \bmod 4$, then $(\frac{-m}{\ell}) = (\frac{m}{\ell}) = -1$ and thus some maximal order of B_ℓ contains $\sqrt{-m}$; if $\ell = 2$, then the group of units of any maximal order in B_2 has order 24.

Suppose now that $m = D/\ell$ is not prime, so that $s \geq 2$. Let $p \mid m$. Then $i)$ and $iv)$ of Ogg's theorem assert that $X_D^{(D/\ell)}(\mathbb{Q}_p) \neq \emptyset$ if and only if either ℓ is odd, $p = 2$ and $\sqrt{-1} \in \mathcal{O}_D$ (that is, $q \equiv 3 \bmod 4$ for all primes $q \mid D/2$), or $\sqrt{-D/p\ell}$ lies in some maximal order of $B_{D/p}$ (that is, $(\frac{-m/p}{\ell}) \neq 1$). This accounts for the third item in (ii) and (iii) of our statements. □

The existence of points on $X_D^{(D)}$ over all completions of $\mathbb{Q}$ has already been established by Clark in [4]. Unfortunately, the natural projection $f : X_D \to X_D^{(D)}$ is always ramified, and so the method of descent cannot be applied to it.

The following corollaries are immediate consequences of the theorem.

Corollary 3.2. *If $X_D^{(m)}(\mathbb{A}_\mathbb{Q}) \neq \emptyset$, then $m = D$ or D/ℓ for a prime $\ell \mid D$.*

Corollary 3.3. *(i) Let ℓ and m be odd primes such that $\ell \equiv 3 \bmod 4$, and $(\frac{m}{\ell}) = -1$. Assume that either $\Sigma_p(D) \neq 0$ or $\Sigma_{mp}(D) \neq 0$ for all $p \nmid D$, $p < 4g^2$. Then $X_{m\ell}^{(m)}(\mathbb{A}_\mathbb{Q}) \neq \emptyset$.*

(ii) Let $m \not\equiv 1 \bmod 8$ be an odd prime. Assume that for all primes $p \nmid D$, $p < 4g^2$, either $\Sigma_p(D) \neq 0$ or $\Sigma_{mp}(D) \neq 0$. Then $X_{2m}^{(m)}(\mathbb{A}_\mathbb{Q}) \neq \emptyset$.

In the case of bad reduction we do not know a general criterion for the existence of local points on twisted Shimura curves, but we have the following partial result.

Proposition 3.4. *Let m be a prime dividing D, and let c be a square free integer such that $(\frac{c}{m}) = -1$. Then ${}^cX_D(\mathbb{Q}_m) = \emptyset$ if and only if there exist primes p and q dividing D/m such that $p \equiv 1 \bmod 4$ and $q \equiv 1 \bmod 3$.*

Proof. We follow [9], Sect. 4, and [8], Sect. 4. Let B' be the definite quaternion algebra over $\mathbb{Q}$ ramified only at the primes dividing D/m and ∞, $\mathcal{O}$ a maximal order in B', $\mathbb{Z}^{(m)}$ the set of rational numbers whose denominators are powers of m, $\mathcal{O}^{(m)} = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}^{(m)}$. Consider the subgroup of units in $\mathcal{O}^{(m)}$ whose reduced norms have even valuation at m. Define Γ_+ as the quotient of this group by $\mathbb{Z}^{(m)*}$. Let Δ be the Bruhat–Tits tree of $SL_2(\mathbb{Q}_m)$; the set of vertices of Δ is $PGL_2(\mathbb{Q}_m)/PGL_2(\mathbb{Z}_m)$. Drinfeld's theorem stated as Thm. 4.3 of [8] describes a model of X_D projective over $\mathrm{Spec}(\mathbb{Z}_m)$. The closed fibre of this model is a union of rational curves with normal crossings. The intersections of the components are described by a 'graph with lengths'. The vertices of the graph are the irreducible components; an oriented edge is a branch of a component passing through a double point. The length $l(y)$ of the edge y equals e if after tensoring with the maximal unramified extension of $\mathbb{Z}_m$ and completion the local ring of the double point is isomorphic to the local ring of the point of $\mathrm{Spec}(\mathbb{Z}_m[x,y]/(xy - m^e))$ given by the ideal (x, y, m). In particular, the model is regular if and only if the length of every edge is 1. The set of vertices of the graph is $\Gamma_+\backslash\Delta$, and their number is twice the class number $h(B')$. The action of Frobenius on $\Gamma_+\backslash\Delta$ is given by an involution of the model over $\mathrm{Spec}(\mathbb{Z}_m)$ which extends the Atkin–Lehner involution ω_m on the generic fibre X_D, and is denoted also by ω_m. Thus the model of X_D over $\mathbb{Z}_m$ is a 'twisted Mumford curve'. Since c is a unit at m, we can twist the model of X_D by $\mathbb{Q}(\sqrt{c})$ with respect to the action of ω_m and obtain a model of ${}^cX_D$; the two models are isomorphic over the unramified quadratic extension of $\mathbb{Z}_m$. The closed fibre of the model of ${}^cX_D$ is described by the same graph with a different action of Frobenius: since c is not a square modulo m, in the case of ${}^cX_D$ the action of Frobenius on the graph is trivial. Thus the model of ${}^cX_D$ over $\mathrm{Spec}(\mathbb{Z}_m)$ so obtained is an (untwisted) Mumford curve; all of its components are rational curves defined over $\mathbb{F}_m$ and all the intersection points are $\mathbb{F}_m$-points. For $v \in \Gamma_+\backslash\Delta$ let $f(v)$ be the cardinality of the stabilizer in Γ_+ of a vertex of Δ which maps to v. For any edge y originating in v we have $l(y)|f(v)$. By a formula on top of p. 292 of [9] (stated there for Γ_0, but true also for Γ_+ as follows from the explanations on p. 296) for every vertex v of $\Gamma_+\backslash\Delta$ the sum of $f(v)/l(y)$ over all edges y originating in v equals $m + 1$. There are three possibilities:

A) If $f(v) = 1$ for every vertex v, then $l(y) = 1$ for every edge y, so that the Mumford curve is regular, and each component has exactly $m + 1$ double points. Hence, there are no smooth $\mathbb{F}_m$-points in the closed fibre. By the valuative criterion of properness a $\mathbb{Q}_m$-point of ${}^cX_D$ extends to a section of the model over $\mathrm{Spec}(\mathbb{Z}_m)$. On a regular model the intersection of a section with the closed fibre is smooth. Therefore in this case ${}^cX_D(\mathbb{Q}_m) = \emptyset$.

B) If $f(v) > 1$ for a vertex v, but $l(y) = 1$ for all edges y originating in v, then the component corresponding to v has less than $m + 1$ double points. Hence, this component contains an $\mathbb{F}_m$-point which is smooth in the closed fibre. By Hensel's lemma this point lifts to a $\mathbb{Q}_m$-point on ${}^cX_D$.

C) Finally, if $f(v) > 1$ for a vertex v, and there is an edge y such that $l(y) > 1$, then the closed fibre has a double point which is singular on the model. Blowing this point up we obtain a new component which is a rational curve over $\mathbb{F}_m$ meeting at most two other components. Hence it contains an $\mathbb{F}_m$-point which is smooth in the closed fibre. By Hensel's lemma such a point lifts to a $\mathbb{Q}_m$-point on ${}^cX_D$.

We conclude that ${}^cX_D(\mathbb{Q}_m) = \emptyset$ if and only if there are no vertices $v \in \Gamma_+ \backslash \Delta$ such that $f(v) > 1$. According to [9], p. 291, this happens if and only if there exist primes p and q dividing D/m such that $p \equiv 1 \bmod 4$ and $q \equiv 1 \bmod 3$. □

In the rest of this paper we study rational points over global fields on $X_{m\ell}^{(m)}$ and on twisted forms of $X_{m\ell}$, where ℓ and m are as in Corollary 3.3 (i). The following fact is of crucial importance for our method.

Proposition 3.5. *Let ℓ and m be odd primes such that $\ell \equiv 3 \bmod 4$ and $(\frac{m}{\ell}) = -1$. Then the double covering $f : X_{\ell m} \to X_{\ell m}^{(m)}$ is unramified.*

Proof. The formula for the number of fixed points of an Atkin–Lehner involution on X_D ([13], (4)) implies that ω_m is fixed point free if and only if $(\frac{-m}{p}) = 1$ for a prime $p \mid D$. □

4. **CM-points**

The theory of complex multiplication on abelian varieties provides a natural procedure to construct points on Shimura curves defined over certain class fields (cf. [19], [6], Ch. 3). Let R be an order in an imaginary quadratic field K which splits B_D. Then K can be embedded into B_D. Let $\mathrm{CM}(R) \subset X_D(\mathbb{C})$ be the image of the set of points $z \in \mathcal{H}$ such that the intersection of stabilizer of z in B_D^+ with $\mathcal{O}_D$ is $R \setminus \{0\}$. The points of $\mathrm{CM}(R)$ bijectively correspond to optimal embeddings $R \hookrightarrow \mathcal{O}_D$ modulo conjugation by elements of Γ. This leads to the formula $|\mathrm{CM}(R)| = 2^{s(K)}h(R)$, where $s(K)$ is the number of prime factors of D which are inert in K (see [23], [6], Prop. 1.3.2, or [4]). Note that the set $\mathrm{CM}(R)$ is preserved by Atkin–Lehner involutions.

Proposition 4.1. *Let ℓ and m be odd primes such that $\ell \equiv 3 \bmod 4$, and $(\frac{m}{\ell}) = -1$. There exist an imaginary quadratic field K and a point $P \in \mathrm{CM}(\mathcal{O}_K) \subset X_{\ell m}(\mathbb{C})$ such that $f(P) \in X_{\ell m}^{(m)}(\mathbb{Q})$ if and only if the class number of $\mathbb{Q}(\sqrt{-\ell})$ is 1 or the class number of $\mathbb{Q}(\sqrt{-\ell m})$ is 2.*

Proof. Shimura proved that for any $P \in \mathrm{CM}(\mathcal{O}_K)$ the field $K(P)$ is the Hilbert class field H_K. Assume that $s(K) \geq 1$. Then we also have $\mathbb{Q}(P) = H_K$ ([6], Thm. 3.1.5). In order for $f(P)$ to be a $\mathbb{Q}$-point we must have $[\mathbb{Q}(P) : \mathbb{Q}] = 2$. Thus $\mathbb{Q}(P) = H_K = K$, so that the class number of K is 1. We have $K = \mathbb{Q}(\sqrt{-d})$ where d is ℓ or m. The field $\mathbb{Q}(\sqrt{-m})$ does not split $B_{\ell m}$, but $\mathbb{Q}(\sqrt{-\ell})$ does. We conclude that if $s(K) \geq 1$, then $\mathbb{Q}(\sqrt{-\ell})$ must have class number 1. Conversely, if this is the

case, the non-trivial action of ω_m on the 2-element set $\mathrm{CM}(\mathcal{O}_{\mathbb{Q}(\sqrt{-\ell})})$ (cf. Proposition 3.5) gives rise to a $\mathbb{Q}$-point on $X_{\ell m}^{(m)}$. Now assume that $s(K) = 0$, that is, ℓ and m are ramified in K, so that $K = \mathbb{Q}(\sqrt{-d})$ for a positive square free integer d divisible by ℓ and m. In this case Thm. 3.1.5 of [6] says that $[H_K : \mathbb{Q}(P)] = 2$. Since $\mathbb{Q}(P)$ must be a quadratic extension of $\mathbb{Q}$, the class number of K is 2. If d is divisible by a prime distinct from ℓ and m, then the class number of K is divisible by 4, since the primes over ℓ and m generate a subgroup $(\mathbb{Z}/2)^2 \subset \mathrm{Cl}_K$. Hence we conclude that if $s(K) = 0$ the class number of $K = \mathbb{Q}(\sqrt{-\ell m})$ is 2. Conversely, if this is so, the non-trivial action of ω_m on the 2-element set $\mathrm{CM}(\mathcal{O}_{\mathbb{Q}(\sqrt{-\ell m})})$ gives rise to a $\mathbb{Q}$-point on $X_{\ell m}^{(m)}$. □

Thus in the case when the class numbers of $\mathbb{Q}(\sqrt{-\ell})$ and $\mathbb{Q}(\sqrt{-\ell m})$ are greater than 1 and 2, respectively, the curves $X_{\ell m}^{(m)}$ are natural candidates for counter-examples to the Hasse principle over $\mathbb{Q}$. In the next section we consider an explicit example of this kind.

The following statement will be used in the next section. Note that for $\mathbb{R}$ and the primes of bad reduction it also gives another proof of Corollary 3.3 (i) in a particular case.

Proposition 4.2. *Let ℓ and m be odd primes such that $\ell \equiv 3 \bmod 4$, and $(\frac{m}{\ell}) = -1$. If the class number of $\mathbb{Q}(\sqrt{-\ell})$ is odd, then the twisted Shimura curve ${}^{-\ell}X_{\ell m}$ and the Atkin–Lehner quotient $X_{\ell m}^{(m)}$ have points in $\mathbb{Q}_\ell$, $\mathbb{Q}_m$ and $\mathbb{R}$.*

Proof. Write $K = \mathbb{Q}(\sqrt{-\ell})$, and let h be the class number of K. The involution ω_m acts on the $2h$-element set $\mathrm{CM}(\mathcal{O}_K) \subset X_{\ell m}(\mathbb{C})$ without fixed points. For any $P \in \mathrm{CM}(\mathcal{O}_K)$ we have $\mathbb{Q}(P) = H_K$ by Thm. 3.1.5 of [6], thus the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts transitively on $\mathrm{CM}(\mathcal{O}_K)$, and hence also on $f(\mathrm{CM}(\mathcal{O}_K)) \subset X_{\ell m}^{(m)}(\mathbb{C})$. This implies that $[\mathbb{Q}(f(P)) : \mathbb{Q}] = h$. Since h is odd we have $H_K = K \otimes_{\mathbb{Q}} \mathbb{Q}(f(P))$, and therefore $\mathbb{Q}(P) = K(f(P))$. Hence the inverse image of $f(P)$ in ${}^{-\ell}X_{\ell m}$ is the union of two $\mathbb{Q}(f(P))$-points.

Suppose that a prime p is inert or ramified in K, and that the unique ideal $\mathfrak{P}$ of $\mathcal{O}_K$ over p is principal. By global class field theory $\mathfrak{P}$ completely splits in H_K, so that $H_K \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq (K_{\mathfrak{P}})^h$. Hence the direct factors of $\mathbb{Q}(f(P)) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ are subfields of $K_{\mathfrak{P}}$, and since h is odd at least one of them is isomorphic to $\mathbb{Q}_p$. It follows that ${}^{-\ell}X_{\ell m}(\mathbb{Q}_p)$ is not empty. This argument can be applied to $p = \ell$, $\mathfrak{P} = (\sqrt{-\ell})$ and to $p = m$, $\mathfrak{P} = (m)$. With $\mathbb{Q}_p$ and $K_{\mathfrak{P}}$ replaced by $\mathbb{R}$ and $\mathbb{C}$, respectively, the same argument shows that ${}^{-\ell}X_{\ell m}(\mathbb{R}) \neq \emptyset$. □

When a smooth and projective curve X is a counter-example to the Hasse principle and X does not have a rational divisor class of degree 1, this counter-example can

be explained by the Manin obstruction (conditionally on the finiteness of the Tate–Shafarevich group of the Jacobian of X, see [22], Cor. 6.2.5). In this connection we note the following fact.

Proposition 4.3. *Let ℓ and m be primes such that $\ell \equiv m \equiv 3 \bmod 4$, and $(\frac{m}{\ell}) = -1$. If the class number of $\mathbb{Q}(\sqrt{-\ell})$ is odd, then each of the curves ${}^{-\ell}X_{\ell m}$ and $X_{\ell m}^{(m)}$ has a divisor of degree 1 defined over $\mathbb{Q}$.*

Proof. It is enough to construct such a divisor on ${}^{-\ell}X_{\ell m}$. The first part of the proof of Proposition 4.2 shows that ${}^{-\ell}X_{\ell m}$ has a point defined over an odd degree extension of $\mathbb{Q}$. Next, ℓ and m are inert in $\mathbb{Q}(\sqrt{-1})$, so this field of class number 1 splits $B_{\ell m}$. The set $\mathrm{CM}(\mathcal{O}_{\mathbb{Q}(\sqrt{-1})}) \subset X_{\ell m}$ has four elements and is stable under ω_m. It defines a divisor of degree 4 on any twist of $X_{\ell m}$ by ω_m. □

5. **Descent and twisted forms of Shimura curves**

The method of descent is used in the proof of the following result.

Theorem 5.1. *Let ℓ and m be odd primes such that $\ell \equiv 3 \bmod 4$ and $(\frac{m}{\ell}) = -1$.*

(i) If $m \equiv 3 \bmod 4$ and $X_{\ell m}(\mathbb{Q}(\sqrt{-\ell})) = \emptyset$, then $X_{\ell m}^{(m)}(\mathbb{Q}) = \emptyset$.

(ii) If $m \equiv 1 \bmod 4$ and $X_{\ell m}(\mathbb{Q}(\sqrt{-\ell})) = X_{\ell m}(\mathbb{Q}(\sqrt{-\ell m})) = \emptyset$, then $X_{\ell m}^{(m)}(\mathbb{Q}) = \emptyset$.

Proof. The set $X_{\ell m}^{(m)}(\mathbb{Q})$ is the union of the images of ${}^{d}X_{\ell m}(\mathbb{Q})$ for all $d \in \mathbb{Q}^*$. Thus $X_{\ell m}^{(m)}(\mathbb{Q}) = \emptyset$ if and only if ${}^{d}X_{\ell m}(\mathbb{Q}) = \emptyset$ for all $d \in \mathbb{Q}^*$.

Corollary 3.5 implies that the natural morphism $f : X_{\ell m} \to X_{\ell m}^{(m)}$ is a torsor under $\mathbb{Z}/2$. By Morita's results ([12], Thm. 1 and 2) f extends to a morphism of smooth and projective curves over $\mathrm{Spec}(\mathbb{Z}[1/\ell m])$. Moreover, when ℓ and m are odd, the restriction of this morphism to the closed fibre at $\mathrm{Spec}(\mathbb{F}_2)$ is separable ([12], Thm. 3 (*iii*)). Hence the morphism of the Morita models is a torsor under the étale $\mathbb{Z}[1/\ell m]$-group scheme $\mathbb{Z}/2$. A well known result (see, e.g., [24], Lemma 1.1) now implies that if $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field such that a prime $p \neq \ell, m$ is ramified in K, then ${}^{d}X_{\ell m}(\mathbb{Q}_p) = \emptyset$. Therefore we only need to consider the fields $\mathbb{Q}(\sqrt{d})$ which are unramified away from m and ℓ.

Our next observation is that the twists ${}^{d}X_{\ell m}$, $d > 0$, have no $\mathbb{R}$-points and hence no $\mathbb{Q}$-points. Indeed, if $d > 0$, then ${}^{d}X_{\ell m} \times_{\mathbb{Q}} \mathbb{R} \simeq X_{\ell m} \times_{\mathbb{Q}} \mathbb{R}$. However, a theorem of Shimura [20] says that $X_{\ell m}(\mathbb{R}) = \emptyset$.

Among the quadratic fields $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-\ell})$, $\mathbb{Q}(\sqrt{-m})$, $\mathbb{Q}(\sqrt{-\ell m})$ the first one is excluded since it is ramified at 2. We also exclude $\mathbb{Q}(\sqrt{-m})$ using the fact that $(\frac{-m}{\ell}) = (\frac{-1}{\ell})(\frac{m}{\ell}) = 1$, so that $-m$ is a square in $\mathbb{Q}_\ell$. This implies that ${}^{-m}X_{\ell m} \times_{\mathbb{Q}} \mathbb{Q}_\ell \simeq X_{\ell m} \times_{\mathbb{Q}} \mathbb{Q}_\ell$, but $X_{\ell m}(\mathbb{Q}_\ell) = \emptyset$ by Thm. 5.6 of Jordan–Livné [8]. This finishes the proof in the case $m \equiv 1 \bmod 4$.

Let us now assume that $m \equiv 3 \bmod 4$. Then $\mathbb{Q}(\sqrt{-\ell m})$ is ramified at 2, hence ${}^{-\ell m}X_{\ell m}(\mathbb{Q}) = \emptyset$. To complete the proof note that ${}^{-\ell}X_{\ell m}(\mathbb{Q}) = \emptyset$ if $X_{\ell m}(\mathbb{Q}(\sqrt{-\ell})) = \emptyset$, because $X_{\ell m} \times_{\mathbb{Q}} \mathbb{Q}(\sqrt{-\ell}) \simeq {}^{-\ell}X_{\ell m} \times_{\mathbb{Q}} \mathbb{Q}(\sqrt{-\ell})$. □

For certain discriminants D and imaginary quadratic fields K global results of Jordan [7] show that $X_D(K) = \emptyset$. These apply even in some cases when X_D has points over all completions of K.

Corollary 5.2. *Let ℓ and m be primes congruent to 3 modulo 4, $m > 7$, such that $(\frac{m}{\ell}) = -1$. Let $K = \mathbb{Q}(\sqrt{-\ell})$. Write Cl_K and $\mathrm{Cl}_K^{(m)}$ for the class group of K and the ray class group of K of conductor m, respectively. If there does not exist a surjective homomorphism*

$$\mathrm{Cl}_K^{(m)} \twoheadrightarrow \mathbb{Z}/(\frac{m^2-1}{12}) \times \mathrm{Cl}_K,$$

then $X_{\ell m}^{(m)}(\mathbb{Q}) = \emptyset$.

Proof. In our assumptions Thm. 6.1 of [7] implies $X_{\ell m}(K) = \emptyset$. The statement now follows from Theorem 5.1 (i). □

Recall that if $2 \nmid m$ there is an exact sequence of abelian groups

$$0 \to (\mathcal{O}_K/m)^*/\mathcal{O}_K^* \to \mathrm{Cl}_K^{(m)} \to \mathrm{Cl}_K \to 0.$$

In our case when m is inert in K we have $(\mathcal{O}_K/m)^*/\mathcal{O}_K^* \simeq \mathbb{Z}/\frac{m^2-1}{2}$ for $\ell > 3$. Hence, it is quite possible that there exists a surjective homomorphism $\mathrm{Cl}_K^{(m)} \twoheadrightarrow \mathbb{Z}/\frac{m^2-1}{12} \times \mathrm{Cl}_K$, and this is indeed the case in many examples. We do not know how often this happens.

Numerical example. Let $\ell = 23$ and $m = 107$. The Eichler mass formula [1], Ch. II, [23], p. 120, tells us that the genus of $X_{\ell m}$ equals 193; it follows that the genus of $X_{\ell m}^{(m)}$ is 97.

The curve $X_{23\cdot 107}^{(107)}$ is a counter-example to the Hasse principle over $\mathbb{Q}$. A computation based on Thm. 2.5 of [8] shows that $X_{23\cdot 107}$ has $\mathbb{Q}_p$-points for all primes p other than 23 and 107. Proposition 4.2 implies that $X_{23\cdot 107}^{(107)}$ has points in $\mathbb{Q}_{23}$, $\mathbb{Q}_{107}$ and $\mathbb{R}$. One computes

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

whereas $\mathrm{Cl}_{\mathbb{Q}(\sqrt{-23})} \simeq \mathbb{Z}/3$. Thus there is no surjective homomorphism from $\mathrm{Cl}_{\mathbb{Q}(\sqrt{-23})}^{(107)}$ onto

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

Therefore $X_{23\cdot 107}^{(107)}(\mathbb{Q}) = \emptyset$ by Corollary 5.2. Hence $X_{23\cdot 107}^{(107)}$ is indeed a counter-example to the Hasse principle over $\mathbb{Q}$. An application of Proposition 4.3 shows that this curve has a divisor of degree 1 defined over $\mathbb{Q}$.

The twisted Shimura curve ${}^{-23}X_{23\cdot 107}$ *is a counter-example to the Hasse principle over* $\mathbb{Q}$. This curve has points in $\mathbb{Q}_{23}$, $\mathbb{Q}_{107}$ and $\mathbb{R}$ by Proposition 4.2. If p is such that $(\frac{-\ell}{p}) = 1$ then it has points in $\mathbb{Q}_p$ by Corollary 2.5. Over all other p-adic fields and also over $\mathbb{Q}(\sqrt{-\ell})$ this curve is isomorphic to $X_{23\cdot 107}$, thus it is soluble everywhere locally but not globally. This curve also has a divisor of degree 1 defined over $\mathbb{Q}$ by Proposition 4.3.

Note also that *the Shimura curve* $X_{23\cdot 107}$ *is a counter-example to the Hasse principle over* $\mathbb{Q}(\sqrt{-\ell})$. It is possible to explain this counter-example by the Manin obstruction, as will be shown in another place.

Remark. We did not find an Atkin-Lehner quotient of a Shimura curve that is a counter-example to the Hasse principle over $\mathbb{Q}$ for which the non-existence of $\mathbb{Q}$-points on all the twisted coverings could be established by purely local means, e.g. by appealing to the results of [8]. By the descent theory such a counter-example will be automatically accounted for by the Manin obstruction, see [22], Thm. 6.1.2.

We thank the organizers of the workshop "Rational and integral points on algebraic varieties" (American Institute of Mathematics, Palo Alto, 2002) where the work on this paper has been started for stimulating environment. Our computations were performed with `pari`. We are grateful to the referees for their suggestions.

References

[1] M. Alsina and P. Bayer, *Quaternion orders, quadratic forms, and Shimura curves*, CRM Monograph series, **22** (2004).
[2] S. Baba, Shimura curve quotients with odd Jacobian, *J. Number Theory* **87** (2001), 96–108.
[3] N. Bruin, E. V. Flynn, J. González, and V. Rotger, On finiteness conjectures for quaternion endomorphism algebras of abelian surfaces, submitted.
[4] P.L. Clark, *Local and global points on moduli spaces of abelian surfaces with potential quaternionic multiplication*, PhD thesis, Harvard, 2003.
[5] L.V. Dieulefait and V. Rotger, The arithmetic of QM-abelian surfaces through their Galois representations, *J. Algebra* **281** (2004), 124–143.
[6] B.W. Jordan, *On the Diophantine arithmetic of Shimura curves*, PhD thesis, Harvard, 1981.
[7] B.W. Jordan, Points on Shimura curves rational over number fields, *J. reine angew. Math.* **371** (1986), 92–114.
[8] B.W. Jordan and R. Livné, Local diophantine properties of Shimura curves, *Math. Ann.* **270** (1985), 235–248.
[9] A. Kurihara, On some examples of equations defining Shimura curves and the Mumford uniformization, *J. Fac. Sci. Univ. Tokyo* Sec. IA **25** (1979), 277–300.
[10] B. Mazur, Rational isogenies of prime degree, *Inv. Math.* **44** (1978), 129–162.
[11] T. Miyake, *Modular forms*, Springer-Verlag, 1989.
[12] Y. Morita, Reduction modulo $\mathfrak{P}$ of Shimura curves, *Hokkaido Math. J.* **10** (1981), 209–238.
[13] A.P. Ogg, Real points on Shimura curves, *Arithmetic and geometry*, Progr. Math. **35**, Birkhäuser, 1983, 277–307.
[14] A.P. Ogg, Mauvaise réduction des courbes de Shimura, *Séminaire de théorie des nombres*, Progr. Math. **59**, Birkhäuser, 1985, 199–217.

[15] V. Rotger, On the group of automorphisms of Shimura curves and applications, *Comp. Math.* **132** (2002), 229–241.
[16] V. Rotger, Modular Shimura varieties and forgetful maps, *Trans. Amer. Math. Soc.* **356** (2004), 1535–1550.
[17] V. Rotger, Shimura curves embedded in Igusa's threefold, *Modular curves and abelian varieties*, Progr. Math. **224**, Birkhäuser, 2003, 263–273.
[18] G. Shimura, On analytic families of polarized abelian varieties and automorphic functions, *Ann. Math.* **78** (1963), 149–192.
[19] G. Shimura, Construction of class fields and zeta functions of algebraic curves, *Ann. Math.* **85** (1967), 58–15.
[20] G. Shimura, On the real points of an arithmetic quotient of a bounded symmetric domain, *Math. Ann.* **215** (1975), 135–164.
[21] S. Siksek and A.N. Skorobogatov, On a Shimura curve that is a counterexample to the Hasse principle, *Bull. London Math. Soc.* **35** (2003), 409–414.
[22] A.N. Skorobogatov, *Torsors and rational points*, Cambridge University Press, 2001.
[23] M.F. Vignéras, *Arithmétique des algèbres de quaternions*, Lect. Notes Math. **800**, 1980.
[24] A. Yafaev and A.N. Skorobogatov, Descent on certain Shimura curves, *Israel J. Math.* **140** (2004), 319–332.

Escola Universitària Politècnica de Vilanova i la Geltrú, Av. Víctor Balaguer s/n, E-08800 Vilanova i la Geltrú, Spain.
E-mail address: vrotger@mat.upc.es

Department of Mathematics, Imperial College London, South Kensington Campus, London SW7 2AZ England.
E-mail address: a.skorobogatov@imperial.ac.uk

Department of Mathematics, University College London, Gower Street, London WC1E 6BT England.
E-mail address: yafaev@math.ucl.ac.uk