AUTOMORPHISMS AND REDUCTION OF HEEGNER POINTS ON SHIMURA CURVES AT CEREDNIK-DRINFELD PRIMES

SANTIAGO MOLINA AND VICTOR ROTGER

1. Introduction

Given an indefinite division quaternion algebra B over $\mathbb{Q}$ of reduced discriminant $D > 1$ and a maximal order $\mathcal{O}$ in B, Shimura [16] constructed a canonical model $X_D/\mathbb{Q}$ of a curve over $\mathbb{Q}$ which is the coarse moduli space of abelian surfaces with multiplication by $\mathcal{O}$ and whose underlying Riemann surface $X_D(\mathbb{C})^{\mathrm{an}}$ is the (compact) quotient of the upper half-plane by the Fuchsian group Γ_D of units in $\mathcal{O}$ of positive norm, which is a subgroup of $\mathrm{SL}_2(\mathbb{R})$ once we choose an embedding of B into $\mathrm{M}_2(\mathbb{R})$.

This curve, commonly referred to as the Shimura curve of discriminant D (and full level structure), is equipped with a natural group of modular involutions called the Atkin-Lehner group. On $X_D(\mathbb{C})^{\mathrm{an}}$ it is defined as the normalizer

$$W_D = \frac{\mathrm{Norm}_{B^\times}(\Gamma_D)}{\mathbb{Q}^\times \cdot \Gamma_D}$$

of Γ_D, and one shows –by exhibiting the way these automorphisms act on the moduli problem– that in fact W_D is naturally a subgroup of the group $\mathrm{Aut}(X_D)$ of automorphisms of $X_D/\mathbb{Q}$.

There is one Atkin-Lehner involution ω_m for each positive divisor m of D and as an abstract group $W_D = \{\omega_m;\ m \mid D\} \subset \mathrm{Aut}(X_D)$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ where r is the number of prime divisors of D.

The main theme of this note is exploring the following conjecture.

Conjecture 1.1. *Assume the genus g_D of X_D is at least 2. Then*

$$\mathrm{Aut}(X_D) = W_D.$$

One motivation for conjecturing that relies on the fact that the analogous statement for the classical modular curve $X_0(N)$ of level $N \geq 1$ holds true except for $N = 37$ and 63 (cf. [4], [7],[14]), in which cases there exist non-modular automorphisms. The appearance of these exceptional automorphisms is explained by the particular geometry of the curves; in the first case, for example, $X_0(37)$ has genus 2 and therefore there is a hyperelliptic involution u acting on it, while the single non-trivial modular involution ω_{37} has only 2 fixed points, which prevents it from being hyperelliptic. See [4] for a detailed analysis of the geometry of $X_0(63)$ and of its automorphism group.

Such phenomena in low genera does not arise among Shimura curves X_D (but see the discussion around (4.12) in §4). Besides, in support of Conjecture 1.1 there is the following result, due to Kontogeorgis and the second author:

Theorem 1.2. [8, Corollary 1.8, Proposition 3.5] *Assume $g_D \geq 2$. Then*

(1) $\mathrm{Aut}(X_D) = \mathrm{Aut}(X_D \times \mathrm{Spec}(\bar{\mathbb{Q}}))$,
(2) $\mathrm{Aut}(X_D) = (\mathbb{Z}/2\mathbb{Z})^s$ *with* $r \leq s \leq r+1$, *and*

(3) $s = r$ *if* $D \leq 1500$ *, except possibly for* $D = 493, 583, 667, 697, 943$.

The main tools in the proof of these statements is the analysis of the action of $\mathrm{Aut}(X_D)$ on

(a) The special fiber of Čerednik-Drinfeld's integral model of X_D at a prime $p \mid D$ of bad reduction of the curve, *or*
(b) Sets of Heegner points (or CM-points) on $X_D(\bar{\mathbb{Q}})$.

These actions were studied separately, and the interrelation between the two has not been explored. The aim of this short note is to show how the interplay of the action of $\mathrm{Aut}(X_D)$ on (a) and (b) can be exploited to prove some instances of Conjecture 1.1 in cases where the techniques of [8] turned out to be insufficient. We shall illustrate it by performing the explicit calculations in the particular case of the Shimura curve of discriminant $D = 667$.

Acknowledgements. We thank the anonymous referee for his/her many suggestions, which helped us to improve considerably the readability of this note. During the preparation of this work, the authors received financial support from MTM2009-13060-C02-01.

2. Specialization of Heegner points

Fix an embedding $B \hookrightarrow \mathrm{M}_2(\mathbb{R})$. The set of complex points of $X = X_D$ is given by

$$X(\mathbb{C}) = B^\times \backslash ((\widehat{B}^\times / \widehat{\mathcal{O}}^\times) \times \mathcal{H}^\pm), \tag{2.1}$$

where $\widehat{\mathcal{O}} = \lim_{\leftarrow n \geq 1} \mathcal{O}/n\mathcal{O}$ denotes the profinite completion of $\mathcal{O}$, $\widehat{B} = \widehat{\mathcal{O}} \otimes \mathbb{Q}$ and $B^\times$ acts on $\mathcal{H}^\pm = \mathbb{C} \setminus \mathbb{R}$ by linear fractional transformations.

Let K be an imaginary quadratic field that splits in B and fix an embedding $\varphi : K \hookrightarrow B$. We denote by $X_{\mathrm{CM}(K)}$ the set of Heegner points in X with CM by K. As a set of points in $X(\mathbb{C})$, it can be explicitly described once a choice of one of the two fixed points $\tau \in \mathcal{H}^\pm$ of $\varphi(K^\times) \subset B^\times$ has been made –and for definiteness we may choose it to be the one on the upper half-plane–, as then

$$X_{\mathrm{CM}(K)} = B^\times \backslash (\widehat{B}^\times / \widehat{\mathcal{O}}^\times \times B^\times \tau) \simeq (K^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}^\times) \times \{\tau\} \tag{2.2}$$

as a subset of (2.1). The bijection in (2.2) holds because $\{b \in B^\times,\ b\tau = \tau\} = K^\times$.

In order to describe the specialization of such points at a prime of bad reduction of the curve we must specify first a model of X over $\mathrm{Spec}(\mathbb{Z})$. Thanks to the work of Morita [13], there exists a proper integral model $\mathcal{X}/\mathrm{Spec}(\mathbb{Z})$ that suitably extends the moduli interpretation of X to arbitrary schemes and is smooth over $\mathrm{Spec}(\mathbb{Z}[\frac{1}{D}])$.

Fix a prime p dividing the discriminant D of B and write $\mathcal{X}_p = \mathcal{X} \times \mathrm{Spec}(\mathbb{F}_p)$ for the special fiber of $\mathcal{X}$ at p. Let B' denote the definite quaternion algebra over $\mathbb{Q}$ of discriminant $D' = D/p$ and $\mathcal{O}'$ (resp. $\mathcal{O}'_p$) be any maximal order (resp. Eichler order of level p) in B'.

By the theory of Čerednik-Drinfeld (cf. [2], [3]), the special fiber $\mathcal{X}_p$ is semi-stable, that is to say, all singular points are double ordinary points. Hence, given $Q \in \mathcal{X}_p^{\mathrm{sing}}$, there exists a finite unramified extension $L/\mathbb{Q}_p$, such that, if we let $\mathcal{O}_L$ denote the ring of integers of L with maximal ideal $\mathfrak{P}$ and uniformizer π, then the $\mathfrak{P}$-adic completion of the local ring $\mathcal{O}_{\mathcal{X} \times \mathrm{Spec}(\mathcal{O}_L), Q}$ is

$$\widehat{\mathcal{O}}_{\mathcal{X} \times \mathrm{Spec}(R), Q} \simeq \mathcal{O}_L[[u, v]]/(uv - \pi^\ell),$$

for some $\ell = \ell(Q) \geq 1$. The integer $\ell(Q)$ is an invariant of the singularity Q, independent of the chosen extension $L/\mathbb{Q}_p$ [9, Corollary 10.3.22], called the *thickness* of Q.

In addition, the theory of Čerednik-Drinfeld asserts that all irreducible components of $\mathcal{X}_p$ are isomorphic to $\mathbb{P}^1$ over $\mathbb{F}_{p^2}$; the set $C(\mathcal{X}_p)$ of components of $\mathcal{X}_p$ is in bijection with the disjoint union of two copies of

$$\mathrm{Pic}(\mathcal{O}') = B'^{\times}\backslash(\widehat{B}')^{\times}/(\widehat{\mathcal{O}}')^{\times}, \tag{2.3}$$

and the set $\mathcal{X}_p^{\mathrm{sing}}$ of singular points of $\mathcal{X}_p$ is in bijection with the double coset

$$\mathrm{Pic}(\mathcal{O}'_p) = B'^{\times}\backslash(\widehat{B}')^{\times}/(\widehat{\mathcal{O}}'_p)^{\times}, \tag{2.4}$$

which is in turn in bijection with the set of oriented Eichler orders in B' of level p up to conjugation by elements in $B'^{\times}$. Denote these bijections by

$$\lambda_p : C(\mathcal{X}_p) \xrightarrow{\simeq} \mathrm{Pic}(\mathcal{O}') \sqcup \mathrm{Pic}(\mathcal{O}') \quad \text{and} \quad \lambda_p : \mathcal{X}_p^{\mathrm{sing}} \xrightarrow{\simeq} \mathrm{Pic}(\mathcal{O}'_p). \tag{2.5}$$

From this description, the thickness of a singular point of $\mathcal{X}_p$ can be read off as

$$\ell(Q) = \#\lambda_p(Q)^{\times}/2, \tag{2.6}$$

that is to say, half the number of units in any of the Eichler orders of level p corresponding to Q by (2.5). (Note that all the orders in the conjugation class $\lambda_p(Q)$ have isomorphic unit group.)

As it is costumary, Čerednik-Drinfeld's description of $\mathcal{X}_p$ can be conveniently packaged in a single *weighted graph*, the so-called dual graph $\mathcal{G}_p$ of $\mathcal{X}_p$. The set $\mathcal{V}_p$ of vertices of $\mathcal{G}_p$ is defined to be $C(\mathcal{X}_p)$ and we link two vertices u, v with as many edges as singular points lying in the intersection of the two components C_u and C_v corresponding to u and v. We write $\mathcal{E}_p$ for the total set of edges in $\mathcal{G}_p$.

We decorate this graph by assigning a *length* to each vertex and edge; namely, given a vertex v or an edge e one sets $\ell(v) = \#\lambda(C_u)^{\times}/2$ and $\ell(e) = \ell(Q_e) = \#\lambda(Q_e)^{\times}/2$, respectively.

Let us introduce the double cosets

$$\mathrm{CM}(K) = \widehat{\mathcal{O}}^{\times}\backslash\widehat{B}^{\times}/K^{\times} \quad \text{and} \quad \mathrm{CM}_p(K) = \widehat{\mathcal{O}'_p}^{\times}\backslash\widehat{B'}^{\times}/K^{\times}.$$

Both can be expressed as the disjoint union

$$\mathrm{CM}(K) = \bigsqcup_{c\geq 1} \mathrm{CM}(K,c) \quad \text{and} \quad \mathrm{CM}_p(K) = \bigsqcup_{c\geq 1} \mathrm{CM}_p(K,c),$$

where we define

$$\mathrm{CM}(K,c) = \{[g] \in \mathrm{CM}(K) \text{ such that } K \cap g\widehat{\mathcal{O}}g^{-1} \text{ is an order of conductor } c \text{ in } K\}, \tag{2.7}$$

and similarly for $\mathrm{CM}_p(K,c)$.

In the sequel we shall regard $\mathrm{CM}(K,c)$ as a subset of $X_{\mathrm{CM}(K)} \subset X(\mathbb{C})$ by means of the isomorphism $\mathrm{CM}(K) \simeq X_{\mathrm{CM}(K)}$ induced by the embedding φ as in (2.2).

The following theorem due to Shimura characterizes the field of definition of a Heegner point $P \in X_{\mathrm{CM}(K)}$.

Theorem 2.1. [16] *Let R_c be the unique order of K of conductor c. Then the field of definition $K(Q)$ of a* CM *point $Q \in \mathrm{CM}(K,c)$ of conductor c is H_c^K the ring class field of R_c.*

Finally, the following result characterizes the specialization of a Heegner point in $X_{\mathrm{CM}(K)}$ at the singular fibre of $\mathcal{X}$ at p. In order to state it, note that there is a natural projection map:

$$\pi_p : \mathrm{CM}_p(K) = \widehat{\mathcal{O}'_p}^{\times}\backslash\widehat{B'}^{\times}/K^{\times} \longrightarrow \widehat{\mathcal{O}'_p}^{\times}\backslash\widehat{B'}^{\times}/B'^{\times} = \mathrm{Pic}(\mathcal{O}'_p).$$

Theorem 2.2. [12, Theorem 1.1] *If p ramifies in K then all points in $X_{\mathrm{CM}(K)}$ specialize to a singular point in $\mathcal{X}_p$. Moreover, for any given $c \geq 1$ relatively prime to D there exists a bijection*

$$\theta_p : \mathrm{CM}(K, c) \xrightarrow{\simeq} \mathrm{CM}_p(K, c)$$

such that $\pi_p(\theta_p(P)) = \lambda_p(\tilde{P}) \in \mathrm{Pic}(\mathcal{O}'_p)$, where $\tilde{P} \in \mathcal{X}_p^{\mathrm{sing}}$ is the specialization of $P \in X_{\mathrm{CM}(K)}$.

Remark 2.3. It is easy to check that the set $\mathrm{CM}_p(K, c)$ is in correspondence with the set of optimal embeddings of R_c into any order in $\mathrm{Pic}(\mathcal{O}'_p)$. Moreover, the map π_p sends an optimal embedding to the isomorphism class of its target in $\mathrm{Pic}(\mathcal{O}'_p)$.

3. The main result

We finally show how the above material can be exploited to prove particular instances of Conjecture 1.1. In order to state our main result let us first introduce some notations.

For any positive integer m set $K_m = \mathbb{Q}(\sqrt{-m})$ and define the set

$$\mathcal{M}(m) = \begin{cases} \{(1,1),(2,1)\} & \text{if } m = 2 \\ \{(m,1),(m,2)\} & \text{if } m \equiv 3 \pmod 4 \\ \{(m,1)\} & \text{otherwise.} \end{cases}$$

Let $D = p_1 \cdot \ldots \cdot p_r$ be the square-free product of an even number of primes and $p \mid D$ be one of its prime factors. For any set of points $S \subseteq X_D(\bar{\mathbb{Q}})$ we shall write $\tilde{S} \subset \mathcal{X}_p(\overline{\mathbb{F}}_p)$ for its image under the reduction map and $\bar{S}$ for its image in the graph $\mathcal{G}_p$ under the map

$$\mathcal{X}_p(\overline{\mathbb{F}}_p) \longrightarrow \mathcal{V}_p \sqcup \mathcal{E}_p$$

which to a point $Q \in \mathcal{X}_p(\overline{\mathbb{F}}_p)$ assigns the vertex or edge over which Q lies.

As a piece of notation, for a fundamental discriminant d write $h(d)$ for the class number of the quadratic order of that discriminant.

Theorem 3.1. *Assume the genus of the Shimura curve X_D is at least 2. Let $m \mid D$ be a positive divisor of D; if $m \equiv 3 \pmod 4$, assume that $h(-4m) > h(-m)$. Let (n, c) be a pair in $\mathcal{M}(m)$ and $p \mid D$ be a prime.*

Assume there exists a subset $S \subseteq \mathrm{CM}(K_n, c)$ such that

(i) $\mathrm{ord}_2(\sharp S) \leq r - 1$,
(ii) $\overline{S} \cap \overline{\mathrm{CM}(K_n, c) \setminus S} = \emptyset$, *and*
(iii) *any automorphism of the weighted graph $\mathcal{G}_p$ leaves $\bar{S}$ invariant.*

Then $\mathrm{Aut}(X_D) \simeq W_D$.

Remark 3.2. As the reader can check from the proof, if $m \equiv 3 \pmod 4$ but $h(-4m) = h(-m)$, Theorem 3.1 still holds true if in the statement we replace the sentence "there exists a subset $S \subseteq \mathrm{CM}(n, c)$" by "there exists a subset $S \subseteq \mathrm{CM}(m, 1) \cup \mathrm{CM}(m, 2)$".

We devote the remainder of this section to proving Theorem 3.1. Write $\mathfrak{F}_m$ for the set of fixed points of the Atkin-Lehner involution ω_m on $X(\bar{\mathbb{Q}})$. By [15, §1] we have

$$\mathfrak{F}_m = \bigcup_{(n,c) \in \mathcal{M}(m)} \mathrm{CM}(K_n, c). \tag{3.8}$$

Since $\mathrm{Aut}(X)$ is abelian by Theorem 1.2,

$$\omega_D(\phi(P)) = \phi(\omega_D(P)) = \phi(P)$$

for all $\phi \in \mathrm{Aut}(X)$ and $P \in \mathfrak{F}_D$. Hence $\phi(\mathfrak{F}_D) = \mathfrak{F}_D$.

Let us show that in fact we have:

Lemma 3.3. *$\phi(\mathrm{CM}(K_n, c)) = \mathrm{CM}(K_n, c)$ for any $(n, c) \in \mathcal{M}(m)$.*

Proof. Note first that this is obvious if m is neither equal to 2 nor congruent to 3 (mod 4), as then $\mathfrak{F}_D = \mathrm{CM}(K_m, 1)$.

If $m = 2$, note that $\mathfrak{F}_2 = \mathrm{CM}(\mathbb{Q}(\sqrt{-1}), 1) \sqcup \mathrm{CM}(\mathbb{Q}(\sqrt{-2}), 1)$. Since the class number of both quadratic fields is 1, Theorem 2.1 implies that $\mathrm{CM}(\mathbb{Q}(\sqrt{-1}), 1)$ is contained in $X(\mathbb{Q}(\sqrt{-1}))$ and $\mathrm{CM}(\mathbb{Q}(\sqrt{-2}), 1)$ is contained in $X(\mathbb{Q}(\sqrt{-2}))$. The claim follows because $\mathrm{Aut}(X) = \mathrm{Aut}(X \times \mathrm{Spec}\,\bar{\mathbb{Q}})$ by Theorem 1.2.

Suppose finally that $m \equiv 3 \pmod 4$, in which case we have $\mathfrak{F}_m = \mathrm{CM}(K_m, 1) \sqcup \mathrm{CM}(K_m, 2)$. By Theorem 2.1, points in $\mathrm{CM}(K_m, 1)$ (resp. in $\mathrm{CM}(K_m, 2)$) generate the ring class field $H_1^{K_m}$ (resp. $H_2^{K_m}$) over K. These two class fields are different (in general we have $H_1^{K_m} \subseteq H_2^{K_m}$ and the assumption $h(-4m) > h(-m)$ amounts to saying that the inclusion is proper). Again because $\mathrm{Aut}(X) = \mathrm{Aut}(X \times \mathrm{Spec}\,\bar{\mathbb{Q}})$, it follows that any automorphism of X must leave each of the sets $\mathrm{CM}(K_m, 1)$ and $\mathrm{CM}(K_m, 2)$ invariant. □

In order to conclude the proof of Theorem 3.1, let $S \subseteq \mathrm{CM}(K_n, c)$ be a set as in the statement of Theorem 3.1. Lemma 3.3 combined with condition (ii) imply that $\mathrm{Aut}(X)$ leaves S invariant.

We invoke at this point the following result, proved by Ogg in [14].

Lemma 3.4. *Let C be an irreducible curve defined over a field L of characteristic 0 and $P \in C(L)$ a regular point on it. Any finite subgroup G of $\mathrm{Aut}(C/L)$ which leaves the point P fixed can be embedded as a subgroup of the group $\mu(L)$ of roots of unity in L.*

Fix a point $P \in S$. As a corollary of this lemma and Theorem 1.2 (2), we deduce that the subgroup $G_P \subset \mathrm{Aut}(X \times \mathrm{Spec}\,\bar{\mathbb{Q}})$ of automorphisms which fix P has at most two elements. Together with Theorem 1.2 we obtain that $\mathrm{Aut}(X)/G_P \simeq (\mathbb{Z}/2\mathbb{Z})^{s'}$ for some $s' \geq s - 1$. Summing up, we have a set S endowed with a *free action* of a group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{s'}$. The orbits of this action all have cardinal $2^{s'}$ and it follows from (i) that $r - 1 \geq s'$.

Combining the above two inequalities with Theorem 1.2 we deduce that $s = r$ and this shows that $\mathrm{Aut}(X) = W_D$, as wished.

4. Applicability

The obvious questions arise as to whether it is possible in practice to check the hypothesis of Theorem 3.1 and how often should we expect them to hold.

The answer to the first question is that there is an algorithm which allows to check the hypothesis of Theorem 3.1 and can be implemented in practice in the computer algebra system MAGMA [1]. We do not sketch the details here, as these treated at length in [8], [12] and [11]; we will rather content with illustrating the method with a few successful examples.

Unfortunately we do not have a satisfactory answer for the second question beyond the following remarks and heuristics, which fail short to settle the problem.

Fix an imaginary quadratic field K, let $\mathrm{disc}(K)$ denote its discriminant and $d_2(K)$ be the number of prime factors of $\mathrm{disc}(K)$. Genus theory yields the lower bound

$$d_2(K) - 1 \leq \mathrm{ord}_2\, h(K) \tag{4.9}$$

for the 2-adic valuation of the class number of K. Write

$$\delta_2(K) = \mathrm{ord}_2\, h(K) - d_2(K) + 1 \geq 0$$

for the extent to which (4.9) fails to be an equality.

It is enlightening to compare our Theorem 3.1 to [8, Theorem 1.6 (ii)], which in the current terminology has the following immediate corollary:

Theorem 4.1. *Assume $m \not\equiv 1 \pmod 4$. If $m \equiv 3 \pmod 4$, assume further that $h(-4m) > h(-m)$. If $\delta_2(K) = 0$, that is to say, if (4.9) is an equality, then $\mathrm{Aut}(X_D) = W_D$.*

Theorem 3.1 is thus a new contribution to Conjecture 1.1 when either $\delta_2(K) > 0$, or $m \equiv 1 \pmod 4$, or $m \equiv 3 \pmod 4$ and $h(-4m) = h(-m)$.

Together with K, fix now a prime $p \mid \mathrm{disc}(K)$. A deep result of P. Michel [10] implies, together with the results of [12], that as D runs over the set of discriminants of indefinite quaternion algebras ramified at p, for any $c \geq 1$ the elements of $\overline{\mathrm{CM}(K,c)}$ are equidistributed in the set $\mathcal{E}_p(X_D)$ of edges of the special fiber of X_D at p. See [11, Corollary 2.1] for more details.

Hence, given an integer $m > 1$ and a pair $(n,c) \in \mathcal{M}(m)$, the points in $\overline{\mathrm{CM}(K_n,c)}$ are equidistributed in $\mathcal{E}_p(X_D)$ for large values of D with $m \mid D$. We expect this may force the set $\mathrm{CM}(K_n,c)$ to be the disjoint union of sets S which are natural candidates for sets satisfying the hypothesis of Theorem 3.1.

We ignore how to prove this claim, but to motivate this expectation let us place ourselves under the hypothesis that $m \not\equiv 1 \pmod 4$, $h(-4m) > h(-m)$ if $m \equiv 3 \pmod 4$, and $\delta_2(K) > 0$ (a similar circle of ideas is available with slight variations in the remaining scenarios where Theorem 4.1 does not apply).

Let

$$W_D^m = \langle w_\ell : \ell \mid D, (\frac{K_m}{\ell}) = -1 \rangle \subset W_D, \quad \text{and} \quad W_{D,m} = \langle w_\ell : \ell \mid D, (\frac{K_m}{\ell}) = 0 \rangle$$

denote the subgroups of W_D consisting of those Atkin-Lehner involutions supported at primes which remain inert (resp. ramify) in K_m. Since there are no primes $\ell \mid D$ which split in K_m, we have $W_D = W_D^m \cdot W_{D,m}$ and $W_D^m \cap W_{D,m} = \{1\}$.

By [6, Prop. 5.6], the group $W_D^m \times \mathrm{Cl}(K_m)$ acts freely and transitively on the set $\mathrm{CM}(K_m,1)$ and the orbit decomposition under $\mathrm{Cl}(K_m)$ gives rise to the splitting

$$\mathrm{CM}(K_m,1) = \bigsqcup T_i \tag{4.10}$$

of $\mathrm{CM}(K_m,1)$ as a disjoint union of sets T_i, $i = 1, ..., 2^{\#\{\ell \mid D, (\frac{K_m}{\ell}) = -1\}}$. Each T_i has cardinal $h(-m)$ and is acted on by $W_{D,m}$ (cf. [6, Lemma 5.9]). This action is not free, as $\omega_m \in W_{D,m}$ fixes each of the points of T_i; but the quotient group $W_{D,m}/\langle \omega_m \rangle$ does act *freely* on T_i. This action is compatible with genus theory in that there exists a bijection of sets

$$\alpha : \mathrm{Cl}(K_m) \xrightarrow{\sim} T_i \tag{4.11}$$

such that, for each ideal class $\mathfrak{a} \in \mathrm{Cl}(K_m)$, the subset $\mathrm{gen}(\mathfrak{a}) \subseteq \mathrm{Cl}(K_m)$ of ideal classes which belong to the same genus of $\mathfrak{a}$ satisfies

$$\alpha(\mathrm{gen}(\mathfrak{a})) = \frac{W_{D,m}}{\langle \omega_m \rangle} \cdot \alpha(\mathfrak{a}) \subseteq T_i.$$

Fix one of the indexes i, set $T = T_i$, choose a point P in T and define $S = \frac{W_D}{\langle \omega_m \rangle} \cdot P \subset \mathrm{CM}(K_m, 1)$.

We believe Theorem 3.1 gives its best fruits when the set S is chosen to be one of these sets introduced. To explain why, note first that the cardinal of S is 2^{r-1} and hence satisfies condition (i) of Theorem 3.1.

Regarding (ii), the number of edges in the dual graph $\mathcal{G}_p$ is roughly $|\mathcal{E}_p| \sim \frac{p+1}{12} \prod_{\ell | D'} (\ell - 1)$ (cf. [17, Ch. V, §2]) and therefore comparatively larger than

$$\#\,\mathrm{CM}(K_m, 1) = 2^{\#\{\ell | D, (\frac{K_m}{\ell}) = -1\}} h(-m) \ll 2^{\#\{\ell | D, (\frac{K_m}{\ell}) = -1\}} m^{\frac{1}{2} + \varepsilon}$$

as $D \gg 0$. In view of this, the equidistribution result alluded to above implies that the reduction map $\mathrm{CM}(K_m, 1) \longrightarrow \mathcal{E}_p(X_D)$ is injective and therefore condition (ii) of Theorem 3.1 also holds for large multiples D of m, that is to say, $\bar{S}$ does not overlap with $\overline{\mathrm{CM}(K_m, 1) \setminus S}$.

As for (iii) is concerned, by construction

$$\bar{S} = \frac{W_D}{\langle \omega_m \rangle} \cdot \bar{P}.$$

and hence the set S is invariant under the action of W_D. Nevertheless, a priori there is no reason why S should be invariant under the whole automorphism group $\mathrm{Aut}(\mathcal{G}_p)$. This can be rephrased more explicitly as follows: the above construction gives rise to exactly $\bar{h}(-m) = \frac{h(-m)}{2^{\#\{\ell | D, (\frac{K_m}{\ell}) = 0\} - 1}}$ different sets S; denote the list of such sets by $\mathcal{S} = \{S_j\}_{j=1,\ldots,\bar{h}(-m)}$. Note that $2^{\delta_2(K)}$ divides $\bar{h}(-m)$) exactly; since $\delta_2(K) > 0$, the door is open to the existence of an exceptional involution $u \in \mathrm{Aut}(\mathcal{G}_p) \setminus W_D$ inducing a non-trivial involution on the set $\mathcal{S}$. Condition (iii) holds if and only if there exists no such involution.

We pass now to illustrate our method in a couple of explicit examples.

Proposition 4.2. $\mathrm{Aut}(X_{667}) = W_{667}$.

Proof. Set $D = 667 = 23 \cdot 29$, $m = n = D$ and $c = 1$. We have $h(-4D) = 12$ and $h(-D) = 4$ (in particular $\delta_2(\mathbb{Q}(\sqrt{-D})) = 1$, so Theorem 4.1 does not apply). Take $p = 29$, which ramifies in K_D. By Theorem 2.2, the set $\mathrm{CM}(K_D, 1) \subset X_{\mathrm{CM}(K_D)}$ is in bijection with $\mathrm{CM}_p(K_D, 1)$, which in turn classifies optimal embeddings of the maximal order of K_D into any of the Eichler orders parametrized by $\mathrm{Pic}(\mathcal{O}'_p)$ as discussed in (2.4).

Following [12] and [11], we computed a full system of optimal embeddings representing the classes in $\mathrm{CM}_p(K_D, 1)$. The cardinal of this set is 4 and we may label its elements as

$$\mathrm{CM}_p(K_D, 1) = \{\varphi_1, \varphi_2, \varphi_3, \varphi_4\}.$$

We also computed the image of each of the elements $[\varphi_i]$ under the map π_p, obtaining that there exist three different conjugacy classes $\mathcal{O}_1$, $\mathcal{O}_2$ and $\mathcal{O}_3$ of orders in $\mathrm{Pic}(\mathcal{O}'_p)$ such that

$$\pi_p(\varphi_1) = \mathcal{O}_1, \quad \pi_p(\varphi_2) = \pi_p(\varphi_4) = \mathcal{O}_2, \quad \pi_p(\varphi_3) = \mathcal{O}_3,$$

Moreover, we have

$$\#\mathcal{O}_1^\times/2 = \#\mathcal{O}_3^\times/2 = 2, \quad \#\mathcal{O}_2^\times/2 = 1.$$

By Theorem 2.2, this implies that the points in $\mathrm{CM}(K_D, 1) = \{P_1, P_2, P_3, P_4\}$ specialize as follows: we have $\tilde{P}_2 = \tilde{P}_4$, $\tilde{P}_1 \neq \tilde{P}_3 \neq \tilde{P}_2$ and $\ell(\tilde{P}_1) = \ell(\tilde{P}_3) = 2$, $\ell(\tilde{P}_2) = \ell(\tilde{P}_4) = 1$.

In conclusion, the set $S = \{P_1, P_2\}$ satisfies conditions (i), (ii) and (iii) of Theorem 3.1, and therefore $\mathrm{Aut}(X_{667}) = W_{667}$. □

The ideas underlying the proof of Theorem 3.1 are quite flexible, and can be adapted easily to slightly different settings. Let us exemplify it by considering the automorphism group of an *Atkin-Lehner quotient* of a Shimura curve.

Given a divisor $n > 1$ of $D = p_1 ... p_r$, let $X_D^{(n)} = X_D/\langle \omega_n \rangle$ denote the quotient of X_D by the Atkin-Lehner involution ω_n. Since W_D is abelian, the quotient group $W_D^{(n)} = W_D/\langle \omega_n \rangle$ acts in a natural way on $X_D^{(n)}$. But in general it is not true that $\mathrm{Aut}(X_D^{(n)}) = W_D^{(n)}$, even if it holds that $\mathrm{Aut}(X_D) = W_D$. Obvious examples of this phenomenon arise when the genus of $X_D^{(n)}$ is 0 or 1.

If $g(X_D^{(n)}) \geq 2$, one can still prove that $\mathrm{Aut}(X_D^{(n)}) = \mathrm{Aut}(X_D^{(n)} \times \mathrm{Spec}(\bar{\mathbb{Q}}))$ and that $\mathrm{Aut}(X_D^{(n)}) \simeq (\mathbb{Z}/2\mathbb{Z})^t$ for some $t \geq r - 1$ (cf. [8, Prop. 1.5]). But even when the genus of $X_D^{(n)}$ is greater than 1 we find interesting examples for which $\mathrm{Aut}(X_D^{(n)}) \simeq (\mathbb{Z}/2\mathbb{Z})^t$ with $t > r - 1$. Namely, this occurs for the pairs

$$\begin{aligned}(D, n) \in \{&(91, 91), (123, 123), (141, 141), (142, 2), (142, 142),\\ &(155, 155), (158, 158), (254, 254), (326, 326), (446, 446)\},\end{aligned} \tag{4.12}$$

for which $g(X_D^{(n)}) = 2$, $r = 2$ and it is proved in [5, Prop. 4.2] that $\mathrm{Aut}(X_D^{(n)}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. One of the exceptional automorphisms appearing in these ten cases is the hyperelliptic involution, while the single non-trivial involution in $W_D^{(n)}$ has only 2 fixed points.

We in fact suspect that $t = r - 1$ for all Atkin-Lehner quotients $X_D^{(n)}$, provided the genus is at least 2 and the pair (D, n) does not show up in the list (4.12). That this is the case can be proved in many instances by applying the results of [8] and the method introduced in this note. We sketch the details for the pair $(D, n) = (69, 23)$, the first example for which the ideas of [8] do not suffice to prove that $t = r - 1$, and one needs to invoke the tools explained above.

Proposition 4.3. $\mathrm{Aut}(X_{69}^{(23)}) = W_{69}^{(23)} \simeq \mathbb{Z}/2\mathbb{Z}$.

Proof. The involution ω_{23} leaves the set $\mathrm{CM}(K_{69}, 1)$ invariant, and the image of this set in $X_{69}^{(23)}$ under the natural projection $X_{69} \longrightarrow X_{69}^{(23)}$ consists of 4 different points. That is to say, we have

$$\mathrm{CM}(K_{69}, 1)/\langle \omega_{23} \rangle = \{P_1, P_2, P_3, P_4\}.$$

When we consider their specialization to the closed fiber at the prime 3, we find that $\tilde{P}_1 = \tilde{P}_2$, $\tilde{P}_1 \neq \tilde{P}_3 \neq \tilde{P}_4$, and $\ell(\tilde{P}_1) = 1$, $\ell(\tilde{P}_3) = 1$ and $\ell(\tilde{P}_4) = 3$.

Hence the whole automorphism group $\mathrm{Aut}(X_{69}^{(23)})$ must fix the point P_4 and Lemma 3.4 implies that $|\mathrm{Aut}(X_{69}^{(23)})| = 2$. This proves the statement. □

References

[1] Cannon J. Bosma, W. and C. Playoust. The magma algebra system. i. the user language. *J. Symbolic Comput.*, 24(3):235–265, 1997.

[2] I. V. Čerednik. Uniformization of algebraic curves by discrete arithmetic subgroups of $\mathrm{PGL}_2(k_w)$ with compact quotient spaces. *Mat. Sb. (N.S.)*, 100(142)(1):59–88, 165, 1976.

[3] V. G. Drinfeld. Coverings of p-adic symmetric domains. *Funkcional. Anal. i Priložen.*, 10(2):29–40, 1976.
[4] N. D. Elkies. The automorphism group of the modular curve $X_0(63)$. *Compositio Math.*, 74(2):203–208, 1990.
[5] J. González and V. Rotger. Equations of Shimura curves of genus two. *Int. Math. Res. Not.*, (14):661–674, 2004.
[6] J. González and V. Rotger. Non-elliptic Shimura curves of genus one. *J. Math. Soc. Japan*, 58(4):927–948, 2006.
[7] M. A. Kenku and F. Momose. Automorphism groups of the modular curves $X_0(N)$. *Compositio Math.*, 65(1):51–80, 1988.
[8] A. Kontogeorgis and V. Rotger. On the non-existence of exceptional automorphisms on Shimura curves. *Bull. London Math. Soc.*, (40):363–374, 2008.
[9] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the french by Reinie Erné, Oxford Science Publications.
[10] P. Michel. The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points. *Ann. of Math. (2)*, 160(1):185–236, 2004.
[11] S. Molina. Equations of hyperelliptic Shimura curves. *Submited for publication.*
[12] S. Molina. Ribet bimodules and specialization of Heegner points. *To appear in the Israel J. Math.*
[13] Y. Morita. Reduction modulo $\mathfrak{P}$ of Shimura curves. *Hokkaido Math. J.*, 10(2):209–238, 1981.
[14] A. P. Ogg. Über die Automorphismengruppe von $X_0(N)$. *Math. Ann.*, 228(3):279–292, 1977.
[15] A. P. Ogg. Real points on Shimura curves. In *Arithmetic and geometry I*, volume 35 of *Progr. Math.*, pages 277–307. Birkhäuser Boston, Boston, MA, 1983.
[16] G. Shimura. Construction of class fields and zeta functions of algebraic curves. *Ann. of Math. (2)*, 85:58–159, 1967.
[17] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

S. M.: Dep. Math., Universität Bielefeld, Germany
E-mail address: santimolin@gmail.com

V. R.: Dep. Mat. Apl. II, Universitat Politècnica de Catalunya, Barcelona, Spain
E-mail address: victor.rotger@upc.edu