[1]

THE SHIMURA COVERING OF A SHIMURA CURVE: AUTOMORPHISMS AND ÉTALE SUBCOVERINGS

CARLOS DE VERA-PIQUERO

Abstract. Let X_D be the Shimura curve associated with an indefinite rational quaternion algebra of discriminant D, and let p be a prime dividing D. In their investigations on the arithmetic of X_D, Jordan and Skorobogatov introduced a covering $X_{D,p}$ of X_D whose maximal étale quotient is referred to as the Shimura covering of X_D at p. The goal of this note is to describe the group of modular automorphisms of the curve $X_{D,p}$ and its quotients. As an application, we construct cyclic étale Galois coverings of Atkin-Lehner quotients of X_D.

Introduction

Modular curves and Shimura curves have great arithmetic significance, for they are moduli spaces of (fake) elliptic curves and, at the same time, thanks to the work of Eichler, Shimura and Wiles, give rise to modular parameterizations of all elliptic curves over $\mathbb{Q}$. The study of diophantine properties of these curves is therefore of fundamental importance in number theory.

In his celebrated article [Maz77], Mazur proved that for integers $N \geq 13$ the only rational points on the modular curve $X_1(N)$ are cusps. This result yields in turn the classification of rational torsion subgroups of elliptic curves over $\mathbb{Q}$.

The research line started by Mazur in [Maz77] was intensively and successfully explored by many others. The general philosophy is that rational points on modular and Shimura curves should correspond only to cusps or (fake) elliptic curves with complex multiplication, except for a few exceptional cases.

One useful strategy to investigate the set of rational points on Shimura curves is to apply descent (see [Sko01]) to suitable étale coverings of them. The question of the existence of rational points is then transferred to these coverings and their twists, and one hopes this problem to have a simpler resolution (applications of this principle can be found in [RdVP], [dVP]). Therefore, the knowledge of étale coverings of Shimura curves is a necessary requirement to use the machinery of descent in order to tackle the existence or nonexistence of rational points on them.

The main goal of this note is to determine the group of modular automorphisms of a cyclic Galois covering of a Shimura curve introduced by Jordan in [Jor81] and, as an application, to construct cyclic étale Galois coverings of its Atkin-Lehner quotients.

[1]The author is supported by AGAUR grant 2009 SGR 1220, DGICYT grant MTM2009-13060-C02-02 and Catalunya's Government and ESF FI-DGR grant.

2010 *Mathematics Subject Classification.* 11G18, 14G35.

Key words and phrases. Shimura curves, modular automorphisms, Atkin-Lehner quotients, étale coverings.

1. Statement of the main results

Let B_D be an indefinite rational quaternion algebra of reduced discriminant $D > 1$, and fix a maximal order $\mathcal{O}_D \subseteq B_D$. We denote by $\mathrm{n} : B_D \to \mathbb{Q}$ the reduced norm on B_D. After fixing an identification $\psi : B_D \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{R})$, the group of units $B_D^\times \subseteq \mathrm{GL}_2(\mathbb{R})$ acts by linear fractional transformations on $\mathfrak{H}^\pm = \mathbb{C} - \mathbb{R}$.

Let $\mathbb{A}_{\mathbb{Q}}$ be the ring of $\mathbb{Q}$-adèles, and $\mathbb{A}_f := \mathbb{A}_{\mathbb{Q},f}$ the ring of finite $\mathbb{Q}$-adèles. Let $\hat{\mathbb{Z}} := \prod_\ell \mathbb{Z}_\ell$ be the profinite completion of the ring of integers, and write $\hat{\mathcal{O}}_D := \mathcal{O}_D \otimes_{\mathbb{Z}} \hat{\mathbb{Z}}$. For a compact open subgroup $K \subseteq \hat{\mathcal{O}}_D^\times$, consider the topological space of double cosets

$$X_K := B_D^\times \setminus (\mathfrak{H}^\pm \times (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / K),$$

where $B_D^\times$ acts simultaneously on the left on both $\mathfrak{H}^\pm$ and $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$, and K acts on the right on $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$: that is, for $z \in \mathfrak{H}^\pm$, $\beta = (\beta_\ell)_\ell \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$, $b \in B_D^\times$ and $k = (k_\ell)_\ell \in K$,

$$b \cdot (z, \beta) \cdot k = (bz, b\beta k) = (bz, (b\beta_\ell k_\ell)_\ell).$$

After the work of Shimura and Deligne (see, e.g., [Shi63], [Shi67], [Del71], [Mil04]), X_K admits a canonical model which is an algebraic curve over $\mathbb{Q}$. We will still denote this Shimura curve by X_K, which need not be geometrically connected: in general, $X_K \times_{\mathbb{Q}} \mathbb{C}$ is the disjoint union of $|\hat{\mathbb{Z}}^\times / \mathrm{n}(K)|$ compact connected complex curves.

When we take $K = \hat{\mathcal{O}}_D^\times$, the curve $X_D := X_{\hat{\mathcal{O}}_D}/\mathbb{Q}$ is the usual Shimura curve associated with the indefinite rational quaternion algebra B_D, which is the coarse moduli scheme over $\mathbb{Q}$ classifying pairs (A, ι) where A is an abelian surface and $\iota : \mathcal{O}_D \hookrightarrow \mathrm{End}(A)$ is a monomorphism of rings (see [Shi63], [Shi67]). Such pairs are called *fake elliptic curves* by some authors, or simply abelian surfaces with quaternionic multiplication by $\mathcal{O}_D$. The curve X_D is projective and smooth, and it depends neither on the choice of $\mathcal{O}_D$ nor of ψ, which are unique up to conjugation. In this case, $X_D/\mathbb{Q}$ is geometrically connected.

When we let K vary, the algebraic curves X_K form an inverse system indexed by the compact open subgroups K of $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$, as there is a natural projection $X_{K'} \to X_K$ whenever $K' \subseteq K$.

The system $\{X_K\}_K$ is endowed with certain natural automorphisms. Namely, multiplication on the right by any element $\beta \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ induces an isomorphism of algebraic curves

$$\rho_K(\beta) : X_K \longrightarrow X_{\beta^{-1}K\beta}, \quad [z, \alpha] \mapsto [z, \alpha\beta]$$

which is defined over $\mathbb{Q}$ ([Mil04, Theorem 13.6]). If q is an arbitrary prime and $\alpha_q \in B_{D,q}^\times := (B_D \otimes_{\mathbb{Q}} \mathbb{Q}_q)^\times$, we will make a slight abuse of notation writing $\rho_K(\alpha_q)$ for the automorphism $\rho_K(\beta)$, where $\beta = (\beta_\ell)_\ell \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ is defined by $\beta_q = \alpha_q$ and $\beta_\ell = 1$ at all primes $\ell \neq q$. More generally, for a finite collection of elements $\alpha_{\ell_i} \in B_{D,\ell_i}^\times$, $i = 1, \dots, t$, we shall write $\rho_K(\alpha_{\ell_1}, \dots, \alpha_{\ell_t})$ for $\rho_K(\beta)$, where $\beta = (\beta_\ell)_\ell \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ is defined by $\beta_{\ell_i} = \alpha_{\ell_i}$ at the primes ℓ_i, and $\beta_\ell = 1$ otherwise.

Let

$$N(K) := \mathrm{Norm}_{(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times}(K) \subseteq (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$$

be the normalizer of K in $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$. For every $\beta \in N(K)$, $\rho_K(\beta)$ is actually an automorphism of X_K. Observe also that $\rho_K(qk)$ is the identity automorphism on X_K

for all $q \in \mathbb{Q}^\times$, $k \in K$. Indeed, for any pair $\beta, \beta' \in N(K)$, $\rho_K(\beta) = \rho_K(\beta')$ if and only if $\beta' = q\beta k$ for some $q \in \mathbb{Q}^\times$ and $k \in K$. This leads us to consider the group

$$\mathrm{Aut}^{\mathrm{mod}}(X_K) := N(K)/\mathbb{Q}^\times K. \tag{1}$$

Definition 1.1. *An automorphism of X_K is* modular *if it is of the form $\rho_K(\beta)$ for some $\beta \in N(K)$. We call* $\mathrm{Aut}^{\mathrm{mod}}(X_K)$ the group of modular automorphisms of X_K, *which is naturally a subgroup of* $\mathrm{Aut}_{\mathbb{Q}}(X_K)$.

For the Shimura curve X_D, we recover the Atkin-Lehner group of $\mathcal{O}_D$,

$$\mathrm{Aut}^{\mathrm{mod}}(X_D) = W_D \simeq (\mathbb{Z}/2\mathbb{Z})^{2r} \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_D),$$

where $2r$ is the number of prime factors of D (see [Vig80, Chapter III, Exercises 5.4, 5.5]). The automorphisms ω_m in W_D act as rational involutions on X_D, the so-called Atkin-Lehner involutions, and they are indexed by the positive divisors m of D.

The aim of the present note is to determine the group of modular automorphisms of the Shimura curve defined by a certain compact open subgroup of $\hat{\mathcal{O}}_D^\times$ attached to an odd prime p dividing D, and to use this information to construct étale Galois coverings of Atkin-Lehner quotients of X_D.

For such a prime $p \mid D$, let $I_p \subseteq \mathcal{O}_{D,p} := \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_p$ be the unique two-sided $\mathcal{O}_{D,p}$-ideal of reduced norm $p\mathbb{Z}_p$, and define $K_p \subseteq \hat{\mathcal{O}}_D^\times$ to be the subgroup of elements in $\hat{\mathcal{O}}_D^\times$ that locally at p are congruent to 1 modulo I_p. Write $X_{D,p}$ for the canonical model over $\mathbb{Q}$ of the curve X_{K_p} defined as above. This Shimura curve has appeared a few times in the literature, with applications to the study of rational points on X_D over number fields (see, e.g., [Jor81], [Sko05]). As we show in [RdVP], a better understanding of it is useful to study the scarcity of rational points on Atkin-Lehner quotients of Shimura curves.

The curve $X_{D,p} \times_{\mathbb{Q}} \mathbb{Q}(\mu_p)$ is the disjoint union of $p-1$ irreducible curves which are conjugate by the action of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ (see [Sko05] and Section 2 below), and the natural finite flat morphism $X_{D,p} \to X_D$ induced by the inclusion $K_p \subseteq \hat{\mathcal{O}}_D^\times$ is a Galois covering whose automorphism group $\Delta := \mathrm{Aut}(X_{D,p}/X_D)$ is isomorphic to the cyclic group $\mathbb{F}_{p^2}^\times/\{\pm 1\} \simeq \mathbb{Z}/\frac{p^2-1}{2}\mathbb{Z}$.

We show in Section 4 that the Atkin-Lehner involutions $\omega_m \in W_D$ on X_D can be lifted to involutions $\hat{\omega}_m$ on the curve $X_{D,p}$, and they generate an abelian subgroup $W_{D,p} \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$ of $\mathrm{Aut}(X_{D,p})$. Write $W_{D/p,p} \simeq (\mathbb{Z}/2\mathbb{Z})^{2r-1}$ for the subgroup of $W_{D,p}$ generated by the involutions $\hat{\omega}_m$ associated with positive divisors m of D/p.

Both Δ and $W_{D,p}$ are in fact subgroups of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$, and we prove in Section 5 that one actually has $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p}) = \Delta W_{D,p}$. More precisely, the first main result of this note can be summarized as follows:

Theorem 1.2. (i) *The Atkin-Lehner involutions $\omega_m \in W_D$ on X_D lift to involutions $\hat{\omega}_m$ on the curve $X_{D,p}$. The group $W_{D,p}$ generated by them is naturally a subgroup of* $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$, *and* $W_{D,p} \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}$.

(ii) *The group* $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ *is isomorphic to*

$$(\Delta \rtimes \langle \hat{\omega}_p \rangle) \times W_{D/p,p} \simeq \left(\mathbb{F}_{p^2}^\times/\{\pm 1\} \rtimes \mathbb{Z}/2\mathbb{Z}\right) \times (\mathbb{Z}/2\mathbb{Z})^{2r-1},$$

where $\hat{\omega}_p \cdot \delta \cdot \hat{\omega}_p = \delta^p$ for any $\delta \in \Delta$.

We leave open the question of studying whether the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ of modular automorphisms of $X_{D,p}$ is the full group $\mathrm{Aut}(X_{D,p})$ or not.

In his PhD thesis [Jor81, Chapter 5], Jordan showed that the maximal étale quotient of the covering $f : X_{D,p} \to X_D$ has degree $(p^2-1)/2e_p$, where $e_p = e_p(D)$ is a positive integer dividing 6 which depends on the arithmetic of B_D (see (10) below for its definition). In Section 6 we apply Theorem 1.2 to investigate sufficient conditions for the natural map $f^{(m)} : X_{D,p}^{(m)} \to X_D^{(m)}$ induced by f to factor through a cyclic étale Galois covering of the Atkin-Lehner quotient $X_D^{(m)}$, where we write $X_{D,p}^{(m)} := X_{D,p}/\langle\hat{\omega}_m\rangle$ and $X_D^{(m)} := X_D/\langle\omega_m\rangle$ for the quotients of $X_{D,p}$ and X_D by the action of $\hat{\omega}_m$ and ω_m, respectively. In this direction, the second main result of this article is the following (cf. Theorem 6.2):

Theorem 1.3. *Let s be a positive integer dividing $(p^2-1)/2n$, where*

$$n := \begin{cases} e_p & \text{if } p \nmid m, \\ \mathrm{lcm}(e_p, (p+1)/2) & \text{if } p \mid m. \end{cases}$$

The map $f^{(m)} : X_{D,p}^{(m)} \to X_D^{(m)}$ factors through a cyclic étale Galois covering of degree s of $X_D^{(m)}$ if either of the following conditions holds:

(i) *ω_m is fixed point free,*
(ii) *$p \nmid m$, $(\frac{m}{p}) = 1$ and s divides $p-1$,*
(iii) *$p \mid m$ and $(\frac{m/p}{p}) = -1$, or*
(iv) *s divides $(p^2-1)/4n$.*

When the Atkin-Lehner involution ω_m is fixed point free, descent techniques were applied to the natural $X_D^{(m)}$-torsor $X_D \to X_D^{(m)}$ under the constant group scheme $\mathbb{Z}/2\mathbb{Z}$ in [RSY05] to prove the emptiness of $X_D^{(m)}(\mathbb{Q})$ in many cases. We hope the étale coverings from the above theorem will be useful in the study of rational points on $X_D^{(m)}$ also in the case where ω_m has fixed points (details will appear in [dVP]).

2. The Shimura curve $X_{D,p}$

Fix for the rest of this note an indefinite rational quaternion algebra B_D of reduced discriminant D and a maximal order $\mathcal{O}_D \subseteq B_D$ as in the Introduction. Write $D = p_1 \cdots p_{2r}$, where the p_i are pairwise distinct primes and $r \geq 1$. For every prime p_i dividing D, the local maximal order $\mathcal{O}_{D,p_i} := \mathcal{O}_D \otimes_{\mathbb{Z}} \mathbb{Z}_{p_i}$ will be regarded as a matrix ring after the choice of an isomorphism

$$\psi_{p_i} : \mathcal{O}_{D,p_i} \xrightarrow{\simeq} \left\{ \begin{pmatrix} x & y \\ p_i\, {}^\sigma y & {}^\sigma x \end{pmatrix} : x, y \in \mathbb{Z}_{p_i^2} \right\} \subseteq \mathrm{M}_2(\mathbb{Z}_{p_i^2}),$$

where $\mathbb{Z}_{p_i^2}$ is the ring of integers of the unique unramified quadratic extension $\mathbb{Q}_{p_i^2}$ of $\mathbb{Q}_{p_i}$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}_{p_i^2}/\mathbb{Q}_{p_i})$ is the nontrivial automorphism (see [Jor81, p. 4]).

Fix also an odd prime p dividing D, and let $X_{D,p}/\mathbb{Q}$ be the canonical model of the Shimura curve X_{K_p} associated to the compact subgroup $K_p \subseteq \hat{\mathcal{O}}_D^\times$, which is defined locally as

$$K_p = \prod_\ell K_{p,\ell}, \quad \text{where} \quad K_{p,\ell} := \begin{cases} \mathcal{O}_{D,\ell}^\times & \text{if } \ell \neq p, \\ 1 + I_p & \text{if } \ell = p. \end{cases} \tag{2}$$

Using the isomorphism ψ_p, we shall make the identification

$$I_p = \left\{ \begin{pmatrix} px & y \\ p\,{}^\sigma y & p\,{}^\sigma x \end{pmatrix} : x, y \in \mathbb{Z}_{p^2} \right\} \subseteq \mathcal{O}_{D,p}.$$

This section is devoted to studying the geometry of the Shimura curve $X_{D,p}$, and we start this task by describing the connected components of the complex curve $X_{D,p} \times_\mathbb{Q} \mathbb{C}$. First, if we write $B_{D,+}^\times := \{b \in B_D^\times : \mathrm{n}(b) > 0\}$, by means of the natural homeomorphism

$$B_D^\times \setminus \mathfrak{H}^\pm \times (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times \to B_{D,+}^\times \setminus \mathfrak{H} \times (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times$$

we see that

$$X_{D,p} \times_\mathbb{Q} \mathbb{C} \simeq B_{D,+}^\times \setminus (\mathfrak{H} \times (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times / K_p).$$

Then, the set $\mathcal{C} := \pi_0(X_{D,p} \times_\mathbb{Q} \mathbb{C})$ of connected components of $X_{D,p} \times_\mathbb{Q} \mathbb{C}$ is encoded (see [Mil04, Lemmas 5.12, 5.13]) by the finite set

$$B_{D,+}^\times \setminus (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times / K_p \simeq \mathbb{Q}^{>0} \setminus \mathbb{A}_f^\times / \mathrm{n}(K_p) \simeq \hat{\mathbb{Z}}^\times / \mathrm{n}(K_p) \simeq \mathbb{Z}_p^\times / \mathrm{n}(1 + I_p), \tag{3}$$

where the first isomorphism is induced by the reduced norm, taking into account that $\mathrm{n}(B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times = \mathbb{A}_f^\times$ and $\mathrm{n}(B_{D,+}^\times) = \mathbb{Q}^{>0}$ because B_D is indefinite (see [Vig80, Théorème III.4.1]). In fact, the set $\mathcal{C}$ is in bijection with the fibres of the natural map

$$B_{D,+}^\times \setminus (\mathfrak{H} \times (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times / K_p) \to B_{D,+}^\times \setminus (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times / K_p, \quad [z, b] \mapsto [b],$$

and there is a homeomorphism

$$X_{D,p} \times_\mathbb{Q} \mathbb{C} \simeq \bigsqcup_{c \in \mathcal{C}} \Gamma_c \setminus \mathfrak{H},$$

where we identify $\mathcal{C}$ with a set of representatives of $B_{D,+}^\times \setminus (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times / K_p$ and for every $c \in \mathcal{C}$ we write $\Gamma_c := B_{D,+}^\times \cap c K_p c^{-1}$. It is easy to check that $\mathrm{n}(1 + I_p) = 1 + p\mathbb{Z}_p$, thus (3) establishes a bijection between the set $\mathcal{C}$ and $\mathbb{F}_p^\times$.

In order to describe the connected components of $X_{D,p} \times_\mathbb{Q} \mathbb{C}$, under the natural inclusion $\mathcal{O}_D^1 \hookrightarrow \mathcal{O}_{D,p}^\times$ we shall regard the intersection $\Gamma_{D,p} := \mathcal{O}_D^1 \cap (1 + I_p)$ as a subgroup of the group $\mathcal{O}_D^1$ of units of norm 1 in $\mathcal{O}_D$, which acts by linear fractional transformations on $\mathfrak{H}$. Then:

Lemma 2.1. *Every connected component of $X_{D,p} \times_\mathbb{Q} \mathbb{C}$ is isomorphic to the compact Riemann surface*

$$V_{D,p} := \Gamma_{D,p} \setminus \mathfrak{H}.$$

Proof. As before, let us identify $\mathcal{C}$ with a set of representatives of the finite double coset $B_{D,+}^\times \setminus (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times / K_p$, and let $c \in \mathcal{C}$, $c = (c_\ell)_\ell \in (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times$. We can assume that $c_\ell = 1$ for all the primes $\ell \neq p$, thus $c = (1, \dots, 1, c_p, 1, \dots)$ for some $c_p \in B_{D,p}^\times$.

Since p divides D, the maximal order $\mathcal{O}_{D,p} \subseteq B_{D,p}$ in the local quaternion division algebra $B_{D,p}$ is unique, and consists of *all* the integral elements in $B_{D,p}$ (see [Vig80, Lemme II.1.5]). In particular, $c_p \mathcal{O}_{D,p} c_p^{-1} = \mathcal{O}_{D,p}$. Besides, since the reduced norm is invariant under conjugation and I_p is the unique two-sided $\mathcal{O}_{D,p}$-ideal of norm p, we deduce that $c_pI_pc_p^{-1} = I_p$, hence also $c_p(1+I_p)c_p^{-1} = 1+I_p$. As a consequence, $cK_pc^{-1} = K_p$, so that all the connected components of $X_{D,p}$ are isomorphic to

$$(B_{D,+}^{\times} \cap K_p) \setminus \mathfrak{H},$$

and the statement follows by observing that $B_{D,+}^{\times} \cap K_p = \mathcal{O}_D^1 \cap (1+I_p)$. □

That is, the complex curve $X_{D,p} \times_{\mathbb{Q}} \mathbb{C}$ is the disjoint union of $p-1$ compact connected curves, and each of them is isomorphic to the Riemann surface $V_{D,p} = \Gamma_{D,p} \setminus \mathfrak{H}$. Even though the curve $X_{D,p}$ is defined over $\mathbb{Q}$, its geometric connected components are only defined over $\mathbb{Q}(\mu_p)$. Indeed, the choice of $X_{D,p}$ as a model of X_{K_p} over $\mathbb{Q}$ defines an action of $\mathrm{Aut}(\mathbb{C})$ on $X_{K_p}(\mathbb{C})$, which is compatible with the action of $\mathrm{Aut}(\mathbb{C})$ on the set

$$\mathcal{C} \overset{\sim}{\to} B_{D,+}^{\times} \setminus (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^{\times}/K_p \simeq \mathbb{Q}^{>0} \setminus \mathbb{A}_f^{\times}/\mathrm{n}(K_p) \simeq \hat{\mathbb{Z}}^{\times}/\mathrm{n}(K_p)$$

through its quotient $\mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^{\times}$ under the map

$$\begin{array}{rcl} X_{D,p} \times_{\mathbb{Q}} \mathbb{C} \simeq B_{D,+}^{\times} \setminus (\mathfrak{H} \times (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^{\times}/K_p) & \longrightarrow & \mathbb{Q}^{>0} \setminus \mathbb{A}_f^{\times}/\mathrm{n}(K_p) \simeq \hat{\mathbb{Z}}^{\times}/\mathrm{n}(K_p) \\ [z,b] & \longmapsto & [\mathrm{n}(b)]. \end{array}$$

If we identify a connected component $c \in \mathcal{C}$ with an element in $B_{D,+}^{\times} \setminus (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^{\times}/K_p$, then the open subgroup $U_c \subseteq \hat{\mathbb{Z}}^{\times}$ fixing $[\mathrm{n}(c)] \in \hat{\mathbb{Z}}^{\times}/\mathrm{n}(K_p)$ is

$$U_c = \prod_{\ell \neq p} \mathbb{Z}_\ell^{\times} \times (1+p\mathbb{Z}_p),$$

thus the number field contained in $\mathbb{Q}^{ab}$ fixed by the action of U_c on $\mathbb{Q}^{ab}$ is the p-th cyclotomic field $\mathbb{Q}(\mu_p)$. From this we deduce that every geometric connected component of $X_{D,p}$ is defined over $\mathbb{Q}(\mu_p)$.

Summing up, the curve $X_{D,p} \times_{\mathbb{Q}} \mathbb{Q}(\mu_p)$ is the disjoint union of $p-1$ geometrically connected curves defined over $\mathbb{Q}(\mu_p)$. These connected components are conjugated by the action of $\mathrm{Gal}\,(\mathbb{Q}(\mu_p)/\mathbb{Q})$, and all of them become isomorphic to the Riemann surface $V_{D,p}$ as complex curves.

2.1. **Action of modular automorphisms on the set $\mathcal{C}$.** Let $\rho_{K_p}(\alpha) \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ be the modular automorphism of $X_{D,p}$ defined by some $\alpha = (\alpha_\ell)_\ell \in N(K_p)$. Let $[z,(\beta_\ell)_\ell] \in X_{D,p} \times_{\mathbb{Q}} \mathbb{C}$ be a point on the Riemann surface underlying $X_{D,p}$ and assume without loss of generality that $z \in \mathfrak{H}$. Let also $c \in \mathcal{C}$ be the connected component of $X_{D,p} \times_{\mathbb{Q}} \mathbb{C}$ in which this point lies, where again we identify $\mathcal{C}$ with a set of representatives of the double coset

$$B_{D,+}^{\times} \setminus (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^{\times}/K_p \simeq \mathbb{Q}^{>0} \setminus \mathbb{A}_f^{\times}/\mathrm{n}(K_p) \simeq \mathbb{Z}_p^{\times}/(1+p\mathbb{Z}_p) \simeq \mathbb{F}_p^{\times}.$$

Then the connected component in which the point $\rho_{K_p}(\alpha)([z,(\beta_\ell)_\ell]) = [z,(\beta_\ell\alpha_\ell)_\ell]$ lies is given by the class of $\mathrm{n}((\beta_\ell\alpha_\ell)_\ell)$ in $\mathbb{Q}^{>0} \setminus \mathbb{A}_f^{\times}/\mathrm{n}(K_p) \simeq \mathbb{F}_p^{\times}$. Since the double coset

$$B_{D,+}^{\times} \setminus (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^{\times}/\hat{\mathcal{O}}_D^{\times}$$

is trivial, there are elements $b \in B_{D,+}^{\times}, (\gamma_\ell)_\ell \in \hat{\mathcal{O}}_D^{\times}$ such that $(\beta_\ell\alpha_\ell)_\ell = b(\beta_\ell)_\ell(\gamma_\ell)_\ell$. Hence, taking classes in $B_{D,+}^{\times} \setminus (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^{\times}/K_p$ we see that

$$[(\beta_\ell\alpha_\ell)_\ell] = [b(\beta_\ell\gamma_\ell)_\ell] = [(\beta_\ell)_\ell(1,\dots,1,\gamma_p,1,\dots)],$$

and using the reduced norm we deduce that $\rho_{K_p}(\alpha)([z,(\beta_\ell)_\ell])$ lies in the connected component given by $c[\mathrm{n}(\gamma_p)] \in \mathbb{F}_p^\times$. In other words, $\rho_{K_p}(\alpha)$ acts on $\mathcal{C} \simeq \mathbb{F}_p^\times$ as multiplication by $[\mathrm{n}(\gamma_p)]$.

3. The cyclic Galois covering $X_{D,p} \to X_D$

Once we have described the geometry of the curve $X_{D,p}$, we study the natural covering of Shimura curves $X_{D,p} \to X_D$ induced by the inclusion $K_p \subseteq \hat{\mathcal{O}}_D^\times$. Since K_p is a normal subgroup of $\hat{\mathcal{O}}_D^\times$, we can regard the Shimura curve $X_{\hat{\mathcal{O}}_D^\times}$ as the quotient of X_{K_p} by the action of $\hat{\mathcal{O}}_D^\times$. This means that every automorphism of the covering

$$X_{K_p} = X_{D,p} \times_{\mathbb{Q}} \mathbb{C} \longrightarrow X_{\hat{\mathcal{O}}_D^\times} = X_D \times_{\mathbb{Q}} \mathbb{C}$$

is of the form $\rho_{K_p}(\alpha)$ for some $\alpha \in \hat{\mathcal{O}}_D^\times$. Moreover, after the choice of canonical models $X_{D,p}$ and X_D over $\mathbb{Q}$ for the curves X_{K_p} and $X_{\hat{\mathcal{O}}_D^\times}$, respectively, all these (modular) automorphisms are defined over $\mathbb{Q}$. Hence,

$$\mathrm{Aut}(X_{D,p}/X_D) := \mathrm{Aut}_{\mathbb{Q}}(X_{D,p}/X_D) = \mathrm{Aut}(X_{D,p} \times_{\mathbb{Q}} \mathbb{C}/X_D \times_{\mathbb{Q}} \mathbb{C})$$

and there is a surjective homomorphism

$$\hat{\mathcal{O}}_D^\times \longrightarrow \mathrm{Aut}(X_{D,p}/X_D), \quad \alpha \longmapsto \rho_{K_p}(\alpha),$$

whose kernel clearly contains the normal subgroup $K_p \subseteq \hat{\mathcal{O}}_D^\times$. Thus we have in fact a surjective homomorphism

$$\begin{aligned} \hat{\mathcal{O}}_D^\times/K_p \simeq \mathcal{O}_{D,p}^\times/(1+I_p) &\longrightarrow \mathrm{Aut}(X_{D,p}/X_D) \\ \alpha_p(1+I_p) &\longmapsto \rho_{K_p}(\alpha_p) = \rho_{K_p}(1,\dots,1,\alpha_p,1,\dots). \end{aligned}$$

Since we have assumed p to be odd, $-1 \notin 1+I_p$ and the kernel of this last homomorphism is $\{\pm 1\}$, so that

$$\mathrm{Aut}(X_{D,p}/X_D) \simeq (\mathcal{O}_{D,p}^\times/(1+I_p))/\{\pm 1\}. \tag{4}$$

Definition 3.1. *We denote by Δ the group of covering automorphisms* $\mathrm{Aut}(X_{D,p}/X_D)$*, regarded as a subgroup of* $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$*. The elements of Δ will be called* diamond automorphisms*.*

As explained in [Sko05], the covering $X_{D,p} \to X_D$ is Galois and cyclic of degree $(p^2-1)/2$, so $\Delta \simeq \mathbb{F}_{p^2}^\times/\{\pm 1\}$, but for our purposes we shall study here the group Δ in more detail. Similarly as in [Jor81, Chapter 5], let us define the *Nebentypus character of $\mathcal{O}_D$ at p* as the homomorphism $\varepsilon_p : \mathcal{O}_{D,p}^\times \to \mathbb{F}_{p^2}^\times$ given by the rule

$$\varepsilon_p(\gamma) = x \bmod p\mathbb{Z}_{p^2} \in \mathbb{F}_{p^2}^\times \quad \text{if} \quad \psi_p(\gamma) = \begin{pmatrix} x & y \\ p\,{}^\sigma y & {}^\sigma x \end{pmatrix} \text{ with } x, y \in \mathbb{Z}_{p^2}.$$

The homomorphism ε_p is clearly surjective, and its kernel is $1 + I_p$. Therefore:

Lemma 3.2. *The quotient $\mathcal{O}_{D,p}^\times/(1+I_p)$ is isomorphic to $\mathbb{F}_{p^2}^\times$.*

Actually, every equivalence class in $\mathcal{O}_{D,p}^\times/(1+I_p)$ is represented (via ψ_p) by a matrix

$$\begin{pmatrix} x & 0 \\ 0 & {}^\sigma x \end{pmatrix} \in \mathcal{O}_{D,p}^\times \tag{5}$$

for some $x \in \mathbb{Z}_{p^2}^\times$, uniquely determined modulo $p\mathbb{Z}_{p^2}$. Combining this lemma with (4), we obtain as we announced that

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

In particular, all the intermediate coverings of $X_{D,p} \to X_D$, which are in bijection with the subgroups of Δ, are cyclic Galois coverings. For a subgroup $\Theta \subseteq \Delta$, the corresponding curve Y_Θ arises as the quotient of $X_{D,p}$ by the action of Θ by covering automorphisms and $\deg(Y_\Theta \to X_D) = [\Delta : \Theta]$.

Following the recipe in Section 2.1, the diamond automorphism $\delta = \rho_{K_p}(\alpha_p) \in \Delta$ defined by some $\alpha_p \in \mathcal{O}_{D,p}^\times$ acts on the set $\mathcal{C} \simeq \mathbb{F}_p^\times$ of geometric connected components of $X_{D,p}$ as multiplication by $[\mathrm{n}(\alpha_p)] \in \mathbb{F}_p^\times$. If the class of α_p in $\mathcal{O}_{D,p}^\times/(1+I_p)$ is represented by a matrix as in (5), then this is the same as saying that δ acts on $\mathcal{C}$ as multiplication by $N_{\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times}(\bar{x}) \in \mathbb{F}_p^\times$, where $\bar{x}$ is the reduction of x modulo $p\mathbb{Z}_{p^2}$. The next lemma follows directly from this observation:

Lemma 3.3. *The diamond automorphisms in $\Delta \simeq \mathbb{F}_{p^2}^\times/\{\pm 1\}$ acting trivially on the set $\mathcal{C}$ are exactly those in the unique subgroup of index $p-1$ in Δ, which is identified with $\mathbb{F}_{p^2}^1/\{\pm 1\}$, where*

$$\mathbb{F}_{p^2}^1 := \ker(N_{\mathbb{F}_{p^2}/\mathbb{F}_p} : \mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times) = \{\bar{x} \in \mathbb{F}_{p^2}^\times : \bar{x}^{p+1} = 1\} \subseteq \mathbb{F}_{p^2}^\times.$$

In particular, two diamond automorphisms $\delta, \delta' \in \Delta$ induce the same action on the set $\mathcal{C}$ if and only if $\delta^{-1}\delta' \in \mathbb{F}_{p^2}^1/\{\pm 1\}$.

Besides, each geometric connected component of $X_{D,p}$ defines a covering of complex Riemann surfaces

$$V_{D,p} = \Gamma_{D,p} \setminus \mathfrak{H} \longrightarrow X_D \times_{\mathbb{Q}} \mathbb{C} \simeq \mathcal{O}_D^1 \setminus \mathfrak{H},$$

whose automorphism group can be determined as follows. First of all, by the very definition of $\Gamma_{D,p}$, the natural inclusion of $\mathcal{O}_D^1$ in $\mathcal{O}_{D,p}^\times$ identifies the quotient $\mathcal{O}_D^1/\Gamma_{D,p}$ as a subgroup of $\mathcal{O}_{D,p}^\times/(1+I_p)$. Secondly, the restriction of the Nebentypus character of $\mathcal{O}_D$ at p to $\mathcal{O}_D^1$ has kernel $\Gamma_{D,p} = \mathcal{O}_D^1 \cap (1+I_p)$, but it is no longer surjective[1] onto $\mathbb{F}_{p^2}^\times$:

Lemma 3.4. *The image of $\mathcal{O}_D^1$ under the Nebentypus character ε_p is $\mathbb{F}_{p^2}^1 \subseteq \mathbb{F}_{p^2}^\times$, the unique subgroup of order $p+1$ of $\mathbb{F}_{p^2}^\times$. In particular,*

$$\mathcal{O}_D^1/\Gamma_{D,p} = \mathcal{O}_D^1/(\mathcal{O}_D^1 \cap (1+I_p)) \simeq \mathbb{F}_{p^2}^1.$$

Proof. If $\gamma \in \mathcal{O}_D^1$, a straightforward computation using the definition of both ψ_p and ε_p shows that $\varepsilon_p(\gamma)$ lies in $\mathbb{F}_{p^2}^1$. Conversely, if $\bar{x} \in \mathbb{F}_{p^2}^1 \subseteq \mathbb{F}_{p^2}^\times$ one can choose a representative

[1] It seems to be implicitly stated in [Jor81, p. 109] that the restriction of ε_p to $\mathcal{O}_D^1$ is still surjective, which in view of Lemma 3.4 is not true.

$x \in \mathbb{Z}_{p^2}^\times$ of $\bar{x}$ such that $x^\sigma x = 1 + pa$ for some $a \in \mathbb{Z}_p^\times$. Therefore we can write $1 = x^\sigma x - py^\sigma y$ for some $y \in \mathbb{Z}_{p^2}$, hence

$$\gamma_p = \begin{pmatrix} x & y \\ p\,{}^\sigma y & {}^\sigma x \end{pmatrix} \in \mathcal{O}_{D,p}^\times$$

has reduced norm 1 and satisfies $\varepsilon_p(\gamma_p) = \bar{x}$. Applying [Miy89, Theorem 5.2.10], there exists $\gamma \in \mathcal{O}_D^1$ such that $\gamma - \gamma_p \in p\mathbb{Z}_{p^2}$, thus $\varepsilon_p(\gamma) = \bar{x}$. □

Finally, the only nontrivial element of $\mathcal{O}_D^1$ acting as the identity on $\mathfrak{H}$ is -1, but $-1 \notin \Gamma_{D,p}$. Therefore,

$$\mathrm{Aut}(V_{D,p}/X_D \times_{\mathbb{Q}} \mathbb{C}) \simeq (\mathcal{O}_D^1/\Gamma_{D,p})/\{\pm 1\} \simeq \mathbb{F}_{p^2}^1/\{\pm 1\},$$

thus $V_{D,p} \to \mathcal{O}_D^1 \setminus \mathfrak{H} \simeq X_D \times_{\mathbb{Q}} \mathbb{C}$ is a cyclic covering of order $(p+1)/2$.

Remark 3.5. There is a unique intermediate curve $X_{D,p}^0/\mathbb{Q}$ in the cyclic covering $X_{D,p} \to X_D$ for which $X_{D,p}^0 \to X_D$ is cyclic of degree $(p+1)/2$, namely the quotient of $X_{D,p}$ by the unique subgroup of Δ of order $p-1$. However, we warn the reader that $X_{D,p}^0$ is not in general a model over $\mathbb{Q}$ for $V_{D,p}$, as it may not be geometrically connected. Actually, similarly as we did for determining the geometric connected components of $X_{D,p}$, one can check that $X_{D,p}^0$ is geometrically connected if and only if $p \equiv 1 \mod 4$.

4. Atkin-Lehner involutions and their lifts to $X_{D,p}$

Now we turn our attention to another family of modular automorphisms of the Shimura curve $X_{D,p}$. For every positive divisor m of D, we shall define an involution $\hat{\omega}_m$ on $X_{D,p}$ lifting the usual Atkin-Lehner involution ω_m on X_D.

Let q be a prime dividing D. The usual Atkin-Lehner involution ω_q on X_D attached to q is defined adèlically as the modular automorphism $\rho_{\hat{\mathcal{O}}_D^\times}(\mathrm{w}_q)$, where

$$\mathrm{w}_q = \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix} \in \mathcal{O}_{D,q} \cap B_{D,q}^\times.$$

This way, $\omega_q \in \mathrm{Aut}^{\mathrm{mod}}(X_D) = W_D$ is clearly an involution because $\mathrm{w}_q^2 = q \in \mathcal{O}_{D,q}$ and $(1, \dots, 1, q, 1, 1, \dots) \in \mathbb{Q}^\times \hat{\mathcal{O}}_D^\times$. Besides, the action of ω_q on the Shimura curve X_D can be interpreted in moduli-theoretic terms (see, e.g., [Jor81]).

The first attempt in order to lift the involution ω_q to $X_{D,p}$ is to consider the modular automorphism $\rho_{K_p}(\mathrm{w}_q) \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$. Clearly, this automorphism lifts the involution ω_q to $X_{D,p}$, but now

$$\rho_{K_p}(\mathrm{w}_q)^2 = \rho_{K_p}(\mathrm{w}_q^2) = \rho_{K_p}(1, \dots, 1, q, 1, \dots), \tag{6}$$

where the q is in the q-th position, and this automorphism is not necessarily the identity on $X_{D,p}$:

Lemma 4.1. *For each prime $q \neq p$ dividing D, we have*

$$\rho_{K_p}(\mathrm{w}_q)^2 = \delta_q \in \Delta = \mathrm{Aut}(X_{D,p}/X_D),$$

where $\delta_q = \rho_{K_p}(1, \dots, 1, q^{-1}, 1, \dots)$, $q^{-1} \in \mathcal{O}_{D,p}^\times$. Besides, the automorphism $\rho_{K_p}(\mathrm{w}_p)$ is an involution.

Proof. For the distinguished prime p, it follows immediately from (6) that $\rho_{K_p}(\mathrm{w}_p^2)$ acts as the identity automorphism on $X_{D,p}$, since $p \in \mathcal{O}_{D,\ell}^\times$ for all $\ell \neq p$ and

$$\rho_{K_p}(1/p)\rho_{K_p}(\mathrm{w}_p^2)\rho_{K_p}(p, \dots, p, 1, p \dots) = \rho_{K_p}(1, 1, \dots).$$

And for each prime $q \mid D/p$, let $k = (q, \dots, q, 1, q, \dots, q, 1, q, \dots) \in K_p$, where the 1's are in the q-th and p-th positions. Then, using (6) again, we see that

$$\rho_{K_p}(\mathrm{w}_q)^2 = \rho_{K_p}(1/q)\rho_{K_p}(\mathrm{w}_q^2)\rho_{K_p}(k) = \rho_{K_p}(1, \dots, 1, q^{-1}, 1, \dots) = \delta_q$$

as claimed. □

As a consequence, for primes $q \neq p$ we see that the automorphism $\rho_{K_p}(\mathrm{w}_q)$ lifting ω_q is an involution on $X_{D,p}$ if and only if $\delta_q = \mathrm{id}$, which is equivalent to saying that $q \equiv \pm 1 \mod p$. However, we can still lift the Atkin-Lehner involutions ω_q to involutions on $X_{D,p}$ as follows.

Continue assuming that $q \neq p$, and choose an element $s_q \in \mathbb{Z}_{p^2}^\times$ such that its reduction $\bar{s}_q \in \mathbb{F}_{p^2}^\times$ modulo $p\mathbb{Z}_{p^2}$ satisfies $\bar{s}_q^2 = q \in \mathbb{F}_p^\times \subseteq \mathbb{F}_{p^2}^\times$. Then consider the element

$$u_q := \begin{pmatrix} s_q & 0 \\ 0 & {}^\sigma s_q \end{pmatrix} \in \mathcal{O}_{D,p}^\times,$$

which satisfies $u_q^2 \in q(1 + I_p) \subseteq \mathcal{O}_{D,p}^\times$, hence $\rho_{K_p}(u_q)^2 = \delta_q^{-1}$.

Remark 4.2. The diamond automorphism $\rho_{K_p}(u_q) \in \Delta$ is well defined. It is clear by construction that $\rho_{K_p}(u_q)$ does not depend on the choice of s_q modulo $p\mathbb{Z}_{p^2}$. In addition, since $\rho_{K_p}(1, \dots, 1, -1, 1, \dots)$ (with the -1 in the p-th position) is the identity automorphism on $X_{D,p}$, $\rho_{K_p}(u_q)$ does not depend on replacing s_q by $-s_q$ either.

Definition 4.3. *Let q be a prime dividing D. We define the modular automorphism $\hat{\omega}_q \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ by*

$$\hat{\omega}_q := \begin{cases} \rho_{K_p}(\mathrm{w}_p) & \text{if } q = p, \\ \rho_{K_p}(\mathrm{w}_q, u_q) = \rho_{K_p}(\mathrm{w}_q)\rho_{K_p}(u_q) & \text{if } q \neq p. \end{cases}$$

Corollary 4.4. *For every prime q dividing D, the automorphism $\hat{\omega}_q \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ is an involution lifting the Atkin-Lehner involution ω_q on X_D to the curve $X_{D,p}$.*

Finally, we observe that the involutions $\hat{\omega}_q$ commute pairwise as q ranges over the prime divisors of D. We state this fact in the following lemma, whose proof is left to the reader:

Lemma 4.5. *For primes q, q' dividing D, $\hat{\omega}_q\hat{\omega}_{q'} = \hat{\omega}_{q'}\hat{\omega}_q$.*

As a consequence, we can attach an involution $\hat{\omega}_m \in \mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ lifting ω_m to each positive divisor m of D just by defining $\hat{\omega}_m$ as the product of the involutions $\hat{\omega}_q$ as q ranges over the prime divisors of m. We call $\hat{\omega}_m$ the *Atkin-Lehner involution on $X_{D,p}$ associated with m* and write

$$W_{D,p} := \{\hat{\omega}_m : m \mid D, m > 0\} = \langle \hat{\omega}_q : q \mid D, q \text{ prime} \rangle \subseteq \mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$$

for the abelian group consisting of these involutions, which is generated by the involutions $\hat{\omega}_q$ with $q \mid D$ prime. It is naturally a subgroup of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ and, by Lemma 4.5, there is a natural isomorphism

$$W_{D,p} \simeq (\mathbb{Z}/2\mathbb{Z})^{2r}.$$

Moreover, for any pair of positive divisors m, m' of D, we have $\hat{\omega}_m \hat{\omega}_{m'} = \hat{\omega}_{mm'/gcd(m,m')^2}$.

As we did for the diamond automorphisms, the discussion in Section 2.1 allows us to determine easily the action of a lifted Atkin-Lehner involution on the set $\mathcal{C} \simeq \mathbb{F}_p^\times$ of geometric connected components of $X_{D,p} \times_{\mathbb{Q}} \mathbb{C}$:

Lemma 4.6. *If m is a positive divisor of D and we regard the Kronecker symbol $\left(\frac{\cdot}{p}\right)$ as taking values in $\mathbb{F}_p$, then $\hat{\omega}_m \in W_{D,p}$ acts on $\mathcal{C}$ as multiplication by*

$$\begin{cases} \left(\frac{m}{p}\right) & \text{if } p \nmid m, \\ -\left(\frac{m/p}{p}\right) & \text{if } p \mid m. \end{cases}$$

Proof. It is enough to prove the statement for $\hat{\omega}_q$ with $q \mid D$ prime. When $q \neq p$, one applies the recipe in Section 2.1 to the automorphisms $\rho_{K_p}(\mathrm{w}_q)$ and $\rho_{K_p}(u_q)$, whereas for the prime p one only needs to deal with $\rho_{K_p}(\mathrm{w}_p)$. The details are routinary and we leave them to the reader. □

So far, we have introduced two *natural* abelian subgroups of the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ of modular automorphisms of $X_{D,p}$. Namely, the group $\Delta = \mathrm{Aut}(X_{D,p}/X_D)$ of diamond automorphisms and the group $W_{D,p}$ of Atkin-Lehner involutions. The above description of $W_{D,p}$ establishes part (i) of Theorem 1.2, and in the next section we will conclude the proof of part (ii). Before that, we show how an Atkin-Lehner involution interacts with a diamond automorphism:

Proposition 4.7. *Let $\delta \in \Delta$ be a diamond automorphism, and let $m \mid D$, $m > 0$. Then, in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$, it holds*

$$\delta\hat{\omega}_m = \begin{cases} \hat{\omega}_m \delta & \text{if } p \nmid m, \\ \hat{\omega}_m \delta^p & \text{if } p \mid m. \end{cases}$$

Proof. Since Atkin-Lehner involutions on $X_{D,p}$ commute pairwise, it suffices to prove the statement for $m = q$ prime. Moreover, we can also assume that $\delta = \rho_{K_p}(\alpha_p)$, where

$$\alpha_p = \begin{pmatrix} x & 0 \\ 0 & {}^\sigma x \end{pmatrix} \in \mathcal{O}_{D,p}^\times \text{ for some } x \in \mathbb{Z}_{p^2}^\times.$$

If $q \neq p$, the automorphism $\delta = \rho_{K_p}(\alpha_p)$ commutes with both $\rho_{K_p}(u_q)$ and $\rho_{K_p}(\mathrm{w}_q)$, thus clearly $\delta\hat{\omega}_q = \rho_{K_p}(\alpha_p)\rho_{K_p}(\mathrm{w}_q)\rho_{K_p}(u_q) = \rho_{K_p}(\mathrm{w}_q)\rho_{K_p}(u_q)\rho_{K_p}(\alpha_p) = \hat{\omega}_q\delta$. And for the prime p, the congruence ${}^\sigma x \equiv x^p \bmod p\mathbb{Z}_{p^2}$ implies that $\rho_{K_p}({}^\sigma\alpha_p) = \rho_{K_p}(\alpha_p^p) = \rho_{K_p}(\alpha_p)^p$, hence the statement follows from the identity $\alpha_p \mathrm{w}_p = \mathrm{w}_p\, {}^\sigma\alpha_p$. □

5. The group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ of modular automorphisms

At this point, we know that both $\Delta = \mathrm{Aut}(X_{D,p}/X_D)$ and $W_{D,p}$ are subgroups of the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ of modular automorphisms of $X_{D,p}$. Moreover, notice that

$\Delta \cap W_{D,p} = \{1\}$. Otherwise, some nontrivial Atkin-Lehner involution $\hat{\omega}_m$ on $X_{D,p}$ would be an automorphism of the covering $X_{D,p} \to X_D$, and this would force the corresponding Atkin-Lehner involution ω_m on X_D to be trivial, that is to say, $m = 1$, which is a contradiction. In addition, if we set $G := \langle \Delta, W_{D,p} \rangle \subseteq \mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$, Proposition 4.7 implies that Δ is normal in G, which is therefore a semidirect product of its subgroups Δ and $W_{D,p}$. In particular, $|G| = (p^2-1)2^{2r-1}$.

The goal of this section is to prove part (ii) of Theorem 1.2. Recall from (1) that the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ is defined as the quotient $N(K_p)/\mathbb{Q}^\times K_p$, where $N(K_p)$ is the normalizer of K_p in $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$. Writing $K_p = \prod_\ell K_{p,\ell}$ as in (2), observe that

$$N(K_p) = (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times \cap \prod_\ell N_\ell(K_{p,\ell}),$$

where $N_\ell(K_{p,\ell}) := \mathrm{Norm}_{B_{D,\ell}^\times}(K_{p,\ell})$. For primes $\ell \nmid D$, the local quaternion algebra $B_{D,\ell}$ is isomorphic to $\mathrm{M}_2(\mathbb{Q}_\ell)$ and all its maximal orders are conjugate to $\mathrm{M}_2(\mathbb{Z}_\ell)$, hence the normalizer of $\mathcal{O}_{D,\ell}^\times$ in $B_{D,\ell}^\times$ is $\mathbb{Q}_\ell^\times \mathcal{O}_{D,\ell}^\times$. In contrast, for primes $\ell \mid D$ this normalizer is the full group of units $B_{D,\ell}^\times$, because $\mathcal{O}_{D,\ell}$ is the unique maximal order in the local quaternion algebra $B_{D,\ell}$. At the prime p, since I_p is the unique two-sided $\mathcal{O}_{D,p}$-ideal of reduced norm p we also have $N_p(1+I_p) = B_{D,p}^\times$. Summing up,

$$N(K_p) = \{(b_\ell)_\ell \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times : b_\ell \in \mathbb{Q}_\ell^\times \mathcal{O}_{D,\ell}^\times \text{ for all } \ell \nmid D\}. \tag{7}$$

Now consider the surjective homomorphism

$$\varphi : N(K_p) \longrightarrow \prod_{\ell \mid D} N_\ell(K_{p,\ell})/\mathbb{Q}_\ell^\times K_{p,\ell}, \quad (b_\ell)_\ell \longmapsto ([b_\ell])_{\ell \mid D},$$

which induces an exact sequence

$$1 \longrightarrow N_\varphi := \ker(\varphi) \longrightarrow N(K_p) \xrightarrow{\ \varphi\ } \prod_{\ell \mid D} N_\ell(K_{p,\ell})/\mathbb{Q}_\ell^\times K_{p,\ell} \longrightarrow 1.$$

From (7) and the definition of φ, observe that $N_\varphi = \mathbb{A}_f^\times K_p$, hence $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ fits in the following short exact sequence:

$$1 \longrightarrow \mathbb{A}_f^\times K_p/\mathbb{Q}^\times K_p \longrightarrow \mathrm{Aut}^{\mathrm{mod}}(X_{D,p}) \longrightarrow \prod_{\ell \mid D} N_\ell(K_{p,\ell})/\mathbb{Q}_\ell^\times K_{p,\ell} \longrightarrow 1. \tag{8}$$

Lemma 5.1. *The quotient $\mathbb{A}_f^\times K_p/\mathbb{Q}^\times K_p$ is isomorphic to $\mathbb{F}_p^\times/\{\pm 1\}$.*

Proof. There is a natural isomorphism $\mathbb{A}_f^\times K_p/\mathbb{Q}^\times K_p \simeq \mathbb{A}_f^\times/(\mathbb{A}_f^\times \cap \mathbb{Q}^\times K_p)$, and it is an easy exercise to check that $\mathbb{A}_f^\times \cap \mathbb{Q}^\times K_p = \mathbb{Q}^\times S$, where $S = (1+p\mathbb{Z}_p)\prod_{\ell \neq p} \mathbb{Z}_\ell^\times$. Therefore, one obtains

$$\mathbb{A}_f^\times K_p/\mathbb{Q}^\times K_p \simeq \mathbb{A}_f^\times/\mathbb{Q}^\times S \simeq \hat{\mathbb{Z}}^\times/S\{\pm 1\} \simeq (\mathbb{Z}_p^\times/(1+p\mathbb{Z}_p))/\{\pm 1\} \simeq \mathbb{F}_p^\times/\{\pm 1\}.$$

□

Lemma 5.2. *The group $\prod_{\ell \mid D} N_\ell(K_{p,\ell})/\mathbb{Q}_\ell^\times K_{p,\ell}$ is isomorphic to the direct product of $(\mathbb{Z}/2\mathbb{Z})^{2r-1}$ and an extension of $\mathbb{Z}/2\mathbb{Z}$ by $\mathbb{Z}/(p+1)\mathbb{Z}$.*

Proof. For the primes $\ell \mid D/p$ (there are $2r-1$ of them), the quotient $N_\ell(K_{p,\ell})/\mathbb{Q}_\ell^\times K_{p,\ell} = B_{D,\ell}^\times/\mathbb{Q}_\ell^\times \mathcal{O}_{D,\ell}^\times$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ (see [Vig80, Chapter III, Exercises 5.4, 5.5]). In contrast, at the prime p the quotient $B_{D,p}^\times/\mathbb{Q}_p^\times(1+I_p)$ fits in the short exact sequence

$$1 \longrightarrow \mathbb{Q}_p^\times \mathcal{O}_{D,p}^\times/\mathbb{Q}_p^\times(1+I_p) \longrightarrow B_{D,p}^\times/\mathbb{Q}_p^\times(1+I_p) \longrightarrow B_{D,p}^\times/\mathbb{Q}_p^\times \mathcal{O}_{D,p}^\times \longrightarrow 1.$$

As before, $B_{D,p}^\times/\mathbb{Q}_p^\times \mathcal{O}_{D,p}^\times \simeq \mathbb{Z}/2\mathbb{Z}$, whereas the quotient $\mathbb{Q}_p^\times \mathcal{O}_{D,p}^\times/\mathbb{Q}_p^\times(1+I_p)$ is cyclic of order $p+1$ (the kernel of the surjective homomorphism $\mathcal{O}_{D,p}^\times \to \mathbb{F}_{p^2}^\times \to \mathbb{F}_p^\times$ obtained by composing the Nebentypus character with the natural quotient map is $\mathbb{Z}_p^\times(1+I_p)$), hence the statement follows. □

As a direct consequence of Lemmas 5.1 and 5.2, together with (8):

Proposition 5.3. *The group* $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ *is generated by its subgroups* Δ *and* $W_{D,p}$*, i.e.* $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p}) = \Delta W_{D,p} = G$.

Finally, we describe the structure of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ as an abstract group. By Propositions 4.7 and 5.3, Δ is normal in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p}) = \Delta W_{D,p}$ with quotient isomorphic to $W_{D,p}$, thus the inclusion of $W_{D,p}$ in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ makes the short exact sequence

$$1 \longrightarrow \Delta \longrightarrow \mathrm{Aut}^{\mathrm{mod}}(X_{D,p}) \longrightarrow W_{D,p} \longrightarrow 1 \tag{9}$$

split. Therefore, $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ is recovered as the semidirect product $\Delta \rtimes_\theta W_{D,p}$ of its subgroups Δ and $W_{D,p}$, where the action $\theta : W_{D,p} \to \mathrm{Aut}(\Delta)$ is given by

$$\theta(\hat{\omega}_m)(\delta) = \hat{\omega}_m^{-1}\delta\hat{\omega}_m = \hat{\omega}_m\delta\hat{\omega}_m = \begin{cases} \delta & \text{if } p \nmid m, \\ \delta^p & \text{if } p \mid m. \end{cases}$$

Now observe that the involutions in the subgroup $W_{D/p,p} := \langle \hat{\omega}_q : q \text{ prime}, q \mid \frac{D}{p} \rangle$ of $W_{D,p}$ of index two commute with the diamond automorphisms, hence the action θ is trivial on $W_{D/p,p}$. Since clearly $W_{D,p} = \langle \hat{\omega}_p \rangle \times W_{D/p,p}$, we get a natural isomorphism

$$\mathrm{Aut}^{\mathrm{mod}}(X_{D,p}) = \Delta \rtimes_\theta W_{D,p} \simeq (\Delta \rtimes_\eta \langle \hat{\omega}_p \rangle) \times W_{D/p,p},$$

where now $\eta : \langle \hat{\omega}_p \rangle \to \mathrm{Aut}(\Delta)$ is determined by the rule $\eta(\hat{\omega}_p)(\delta) = \hat{\omega}_p\delta\hat{\omega}_p = \delta^p$, and this concludes the proof of Theorem 1.2.

Remark 5.4. Identifying $W_{D,p} \simeq W_D$ in the natural way, the short exact sequence (9) becomes

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \Delta & \longrightarrow & \mathrm{Aut}^{\mathrm{mod}}(X_{D,p}) & \longrightarrow & W_D & \longrightarrow & 1, \\ & & \delta & \longmapsto & \delta & & & & \\ & & & & \delta\hat{\omega}_m & \longmapsto & \omega_m & & \end{array}$$

which shows that the modular automorphisms of $X_{D,p}$ lifting an Atkin-Lehner involution ω_m on X_D are precisely those in the coset $\Delta\hat{\omega}_m = \hat{\omega}_m\Delta$.

Remark 5.5. Let $\hat{\omega}_q \in W_{D,p}$ be the Atkin-Lehner involution on $X_{D,p}$ associated with a prime $q \mid D$. After the previous remark, it is natural to ask whether there are other involutions in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ lifting ω_q or not. Indeed, the choice of $\hat{\omega}_q$ is not unique.

By Remark 5.4, every modular automorphism lifting ω_q can be written as $\delta\hat{\omega}_q$ for some $\delta \in \Delta$. If $q \neq p$, $\hat{\omega}_q$ commutes with every diamond automorphism, hence $\delta\hat{\omega}_q$ is an involution if and only if $\delta^2 = 1$. Therefore, there are exactly two involutions in

$\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ lifting ω_q, namely $\hat{\omega}_q$ and $\tau\hat{\omega}_q$, where τ is the unique diamond involution in Δ. In contrast, the involution $\hat{\omega}_p$ associated to p does not commute with the diamond automorphisms, and from the identity $(\delta\hat{\omega}_p)^2 = \delta\hat{\omega}_p\delta\hat{\omega}_p = \delta^{p+1}$ we see that $\delta\hat{\omega}_p$ is an involution if and only if δ lies in the unique subgroup of Δ of order $p+1$, thus there are exactly $p+1$ involutions in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ lifting ω_p.

We emphasize that the structure of the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ as stated in Theorem 1.2 does not depend on which involutions in $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ lifting the usual Atkin-Lehner involutions on X_D we choose.

6. Cyclic étale Galois coverings of $X_D^{(m)}$

Let m be a positive divisor of D, and ω_m be the corresponding Atkin-Lehner involution on X_D. We write $X_D^{(m)} := X_D/\langle\omega_m\rangle$ for the quotient of X_D by the action of ω_m, and $\pi_m : X_D \to X_D^{(m)}$ for the natural projection map.

The cyclic Galois covering $f : X_{D,p} \to X_D$ can be used to prove the nonexistence of rational points on the Shimura curve X_D over imaginary quadratic fields under certain congruence conditions (see [Jor86], [Sko05], [RdVP]). Combined with the work of Jordan and Livné [JL85], such results often lead to counterexamples to the Hasse principle accounted for by the Brauer-Manin obstruction.

After the study of the group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$ of modular automorphisms of $X_{D,p}$, now we want to obtain cyclic Galois coverings of $X_D^{(m)}$ from the intermediate coverings of $f : X_{D,p} \to X_D$. Even more, we will construct cyclic étale Galois coverings of $X_D^{(m)}$ that can be used to study the set of rational points $X_D^{(m)}(\mathbb{Q})$ by applying descent techniques.

Let $\hat{\omega}_m$ be the Atkin-Lehner involution on $X_{D,p}$ lifting ω_m, and consider the natural projection map $\hat{\pi}_m : X_{D,p} \to X_{D,p}^{(m)} := X_{D,p}/\langle\hat{\omega}_m\rangle$ onto the quotient. Then we have a commutative diagram

$$\begin{array}{ccc} X_{D,p} & \xrightarrow{f} & X_D \\ \downarrow{\scriptstyle \hat{\pi}_m} & & \downarrow{\scriptstyle \pi_m} \\ X_{D,p}^{(m)} & \xrightarrow{f^{(m)}} & X_D^{(m)}. \end{array}$$

For every positive divisor s of $(p^2-1)/2$, we write $\Theta(s) \subseteq \Delta$ for the unique (cyclic) subgroup of Δ of index s, and $f_s : X_{D,p}(s) \to X_D$ for the intermediate covering of $f : X_{D,p} \to X_D$ arising as the quotient of $X_{D,p}$ by $\Theta(s)$, so that $\deg(f_s) = s$.

By virtue of Proposition 4.7, the action of the Atkin-Lehner involution $\hat{\omega}_m$ on $X_{D,p}$ commutes with the action of each subgroup $\Theta(s)$ of Δ. That is, $\hat{\omega}_m$ induces an involution on every intermediate curve $X_{D,p}(s)$ lifting ω_m, which we will still denote by $\hat{\omega}_m$. We write $X_{D,p}^{(m)}(s)$ for the quotient of $X_{D,p}(s)$ by its action and $f_s^{(m)} : X_{D,p}^{(m)}(s) \to X_D^{(m)}$ for the natural induced map.

6.1. **The Galois property.** The covering $X_{D,p} \to X_D^{(m)}$ obtained by composing f with π_m is Galois of degree p^2-1, and its automorphism group $\mathrm{Aut}(X_{D,p}/X_D^{(m)})$ is the group

$$\Delta^{(m)} := \Delta\langle\hat{\omega}_m\rangle \subseteq \mathrm{Aut}^{\mathrm{mod}}(X_{D,p})$$

generated by Δ and $\langle\hat{\omega}_m\rangle$. Therefore, the cyclic Galois coverings of $X_D^{(m)}$ induced by intermediate coverings of $f : X_{D,p} \to X_D$ and not factoring through X_D are in one to one correspondence with the normal subgroups of $\Delta^{(m)}$ containing $\hat{\omega}_m$. After Theorem 1.2, the subgroups of $\Delta^{(m)}$ containing $\hat{\omega}_m$ are precisely those of the form $\Theta(s)\langle\hat{\omega}_m\rangle$, as s ranges through the positive divisors of $(p^2-1)/2$.

Corollary 6.1. *Let s be a positive divisor of $(p^2-1)/2$, and $f_s : X_{D,p}(s) \to X_D$ be the above defined covering. Then:*

(i) *If p does not divide m, $f_s^{(m)} : X_{D,p}^{(m)}(s) \to X_D^{(m)}$ is a cyclic Galois covering of degree s. In particular, $X_{D,p}^{(m)} \to X_D^{(m)}$ is cyclic and Galois with automorphism group isomorphic to Δ.*

(ii) *If p divides m, $f_s^{(m)} : X_{D,p}^{(m)}(s) \to X_D^{(m)}$ is a cyclic Galois covering if and only if s divides $p-1$. In particular, $X_{D,p}^{(m)}(p-1) \to X_D^{(m)}$ is cyclic and Galois with automorphism group isomorphic to $\Delta/(\mathbb{F}_{p^2}^1/\{\pm1\}) \simeq \mathbb{F}_p^\times$.*

Proof. If $p \nmid m$, $\Delta^{(m)} \simeq \Delta \times \langle\hat{\omega}_m\rangle$ is abelian, hence (i) is clear. As for (ii), if $p \mid m$ one checks that $\Theta(s)\langle\hat{\omega}_m\rangle$ is normal in $\Delta^{(m)}$ if and only if $\delta^{p-1} \in \Theta(s)$ for all $\delta \in \Delta$. □

6.2. **The étale property.** Jordan showed in [Jor81, Chapter 5] that the maximal étale quotient of $f : X_{D,p} \to X_D$ (the so-called *Shimura covering of X_D at p*) is the covering $f_{\frac{p^2-1}{2e_p}} : X_{D,p}((p^2-1)/2e_p) \to X_D$, where $e_p := e_p(D)$ is a positive divisor of $(p^2-1)/2$ depending on the arithmetic of B_D. Under our assumption of p being odd, this integer is given by the recipe (see [Jor81, p. 108])

$$e_p := \begin{cases} \left(1 + 2\left(\frac{B_D}{\mathbb{Q}(\sqrt{-3})}\right)\right)\left(1 + \left(\frac{B_D}{\mathbb{Q}(\sqrt{-1})}\right)\right) & \text{if } p > 3, \\ 1 + \left(\frac{B_D}{\mathbb{Q}(\sqrt{-1})}\right) & \text{if } p = 3, \end{cases} \tag{10}$$

where for a quadratic field F, we set $(\frac{B_D}{F}) = 1$ if F splits B_D and 0 otherwise. In particular, for a positive divisor s of $(p^2-1)/2$, the covering $f_s : X_{D,p}(s) \to X_D$ is étale[2] if and only if s divides $(p^2-1)/2e_p$. Notice that e_p divides 6.

Let $s \geq 1$ be a positive integer dividing $(p^2-1)/2$, and assume that $s \mid (p^2-1)/2e_p$, so that $f_s : X_{D,p}(s) \to X_D$ is a cyclic étale Galois covering of degree s. Assume moreover that the induced covering $f_s^{(m)} : X_{D,p}^{(m)}(s) \to X_D^{(m)}$ is Galois. By virtue of Corollary 6.1, this is equivalent to assuming that s divides $(p^2-1)/2n$, where

$$n := \begin{cases} e_p & \text{if } p \nmid m, \\ \operatorname{lcm}(e_p, (p+1)/2) & \text{if } p \mid m. \end{cases}$$

Observe that when p divides m the cyclic subgroup $\Theta((p^2-1)/2n)$ of Δ contains the subgroup $\Theta(p-1) \simeq \mathbb{F}_{p^2}^1/\{\pm1\}$, which by Lemma 3.3 consists of all the diamond automorphisms in Δ that act trivially on the set of connected components of $X_{D,p} \times_{\mathbb{Q}} \mathbb{C}$.

[2] In a more technical parlance, $f_s : X_{D,p}(s) \to X_D$ is an X_D-torsor under the constant group scheme $\mathbb{Z}/s\mathbb{Z}$.

Theorem 6.2. *Let s be a positive integer dividing $(p^2-1)/2n$. The cyclic Galois covering $f_s^{(m)} : X_{D,p}^{(m)}(s) \to X_D^{(m)}$ is étale if either of the following conditions holds:*

(i) *ω_m is fixed point free,*
(ii) *$p \nmid m$, $(\frac{m}{p}) = 1$ and s divides $p-1$,*
(iii) *$p \mid m$ and $(\frac{m/p}{p}) = -1$, or*
(iv) *s divides $(p^2-1)/4n$.*

Proof. Write $f' : X_{D,p} \to X_{D,p}((p^2-1)/2n)$. By the definition of n, the covering $f_s : X_{D,p}(s) \to X_D$ is étale, and the induced covering $f_s^{(m)} : X_{D,p}^{(m)}(s) \to X_D^{(m)}$ is Galois. When ω_m is fixed point free, the projection map $\pi_m : X_D \to X_D^{(m)}$ is étale, hence the commutative diagram

$$\begin{array}{ccc} X_{D,p}(s) & \xrightarrow{\text{ét}} & X_D \\ \downarrow & & \downarrow{\scriptstyle \text{ét}} \\ X_{D,p}^{(m)}(s) & \longrightarrow & X_D^{(m)} \end{array}$$

implies that $f_s^{(m)} : X_{D,p}^{(m)}(s) \to X_D^{(m)}$ is étale as well.

Now we show that $f_s^{(m)}$ is also étale if either (ii), (iii) or (iv) holds, and we can assume that ω_m has fixed points. So let $Q \in X_D(\bar{\mathbb{Q}})$ be a fixed point of ω_m, and let $P \in X_{D,p}(\bar{\mathbb{Q}})$ be any point such that $f(P) = Q$. Then,

$$f(\hat{\omega}_m(P)) = \omega_m(f(P)) = \omega_m(Q) = Q,$$

thus $\hat{\omega}_m$ acts on the fibre $f^{-1}(Q)$. Since $f : X_{D,p} \to X_D$ is Galois, there exists a diamond automorphism $\delta_Q \in \Delta$, which depends only on Q, such that

$$\hat{\omega}_m(P) = \delta_Q(P) \quad \text{for every} \quad P \in f^{-1}(Q). \tag{11}$$

In particular, $\delta_Q^2(P) = \hat{\omega}_m^2(P) = P$ for every $P \in f^{-1}(Q)$. It follows that $\delta_Q^2 \in \Theta((p^2-1)/2n) \subseteq \Theta(s)$, and hence it induces the trivial automorphism of the covering $f_s : X_{D,p}(s) \to X_D$. Otherwise, the relation $\delta_Q'^2(f'(P)) = f'(P)$ in $X_{D,p}((p^2-1)/2n)$, where δ_Q' is the class of δ_Q in $\Delta/\Theta((p^2-1)/2n)$, would prevent the action of $\Delta/\Theta((p^2-1)/2n)$ from being transitive on $f^{-1}_{\frac{p^2-1}{2n}}(Q)$, and this would contradict the fact that $f_{\frac{p^2-1}{2n}}$ is an étale Galois covering. If s divides $(p^2-1)/4n$, we have

$$\Theta((p^2-1)/2n) \subseteq \Theta((p^2-1)/4n) \subseteq \Theta(s),$$

thus it actually holds $\delta_Q \in \Theta(s)$. Repeating the argument for all the fixed points $Q \in X_D(\bar{\mathbb{Q}})$ of ω_m, we deduce that all the corresponding diamond automorphisms δ_Q satisfying (11) belong to $\Theta(s)$. Therefore, every fibre of $f_s : X_{D,p}(s) \to X_D$ above a point $Q \in X_D(\bar{\mathbb{Q}})$ with $\omega_m(Q) = Q$ consists of exactly $s = \deg(f_s)$ points $P_1, \dots, P_s$ which are all fixed by $\hat{\omega}_m$. In particular, the covering $f_s^{(m)} : X_{D,p}^{(m)}(s) \to X_D^{(m)}$ is étale when (iv) holds.

As for conditions (ii) and (iii), first observe that by the discussion in Section 2.1 the assumptions $(\frac{m}{p}) = 1$ and $(\frac{m/p}{p}) = -1$, respectively, are equivalent to saying that $\hat{\omega}_m$ acts trivially on the set of connected components $\pi_0(X_{D,p} \times_{\mathbb{Q}} \mathbb{C})$. Besides, the extra hypothesis $s \mid (p-1)$ in (ii) and the definition of n in (iii) imply that $\Theta(p-1) \subseteq \Theta(s)$ in both cases.

Hence, under condition (ii) or (iii), repeating the above argument the equality (11) implies that δ_Q acts trivially on the set of connected components of $X_{D,p} \times_{\mathbb{Q}} \mathbb{C}$, since a diamond automorphism cannot fix only one connected component of $X_{D,p} \times_{\mathbb{Q}} \mathbb{C}$. This means that $\delta_Q \in \Theta(p-1) \subseteq \Theta(s)$, thus $f_s^{(m)}$ is an étale covering. □

Acknowledgements

I am greatly indebted to Prof. Víctor Rotger for his guidance and his very valuable comments and suggestions throughout the elaboration of this work. I also wish to thank the Number Theory Group at the Warwick Mathematics Institute of the University of Warwick for their warm hospitality during the spring of 2012.

References

[Del71] P. Deligne, Travaux de Shimura, in *Séminaire Bourbaki, 23ème année (1970/1971), Exp. No. 389*, Lect. Notes in Math., vol. 244, Springer, 1971, 123-165.

[Jor81] B. W. Jordan, *On the Diophantine arithmetic of Shimura curves*, Harvard PhD. Thesis (1981).

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

[JL85] B. Jordan, J. Livné, Local diophantine properties of Shimura curves, *Math. Ann.* **270** (1985), 235-248.

[Maz77] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47** (1977), 33-186.

[Mil04] J. S. Milne, Introduction to Shimura varieties, course notes available online at http://www.jmilne.org/math/xnotes.

[Miy89] T. Miyake, *Modular Forms*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1989, Translated from the Japanese by Yoshitaka Maeda.

[RSY05] V. Rotger, A. Skorobogatov, A. Yafaev, Failure of the Hasse principle for Atkin-Lehner quotients of Shimura curves over $\mathbb{Q}$, *Moscow Math. J.* **5:2** (2005), 463-476.

[RdVP] V. Rotger, C. de Vera-Piquero, Galois representations over fields of moduli and rational points on Shimura curves, accepted for publication in Can. J. Math., DOI: 10.4153/CJM-2013-020-3.

[Shi63] G. Shimura, On analytic families of polarized abelian varieties and automorphic functions, *Ann. Math.* **78** (1963), 149-192.

[Shi67] G. Shimura, Construction of class fields and zeta functions of algebraic curves, *Ann. Math.* **85** (1967), 58-159.

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

[Sko05] A. Skorobogatov, Shimura coverings of Shimura curves and the Manin obstruction, *Math. Res. Lett.* **12** (2005), 779-788.

[dVP] C. de Vera-Piquero, Atkin-Lehner quotients of Shimura curves violating the Hasse principle, in progress.

[Vig80] M. F. Vignéras, *Arithmétique des algèbres de quaternions*, Lect. Notes in Math., vol. 800, Springer-Verlag, 1980.

Departament de Matemàtica Aplicada II, Universitat Politècnica de Catalunya, C. Jordi Girona 1-3, 08034 Barcelona, Spain

E-mail address: carlos.de.vera@upc.edu