[1]

LOCAL POINTS ON SHIMURA COVERINGS OF SHIMURA CURVES AT BAD REDUCTION PRIMES

CARLOS DE VERA-PIQUERO

ABSTRACT. Let X_D be the Shimura curve associated with an indefinite rational quaternion algebra of reduced discriminant $D > 1$. For each prime $\ell \mid D$, there is a natural cyclic Galois covering of Shimura curves $X_{D,\ell} \to X_D$ constructed by adding certain level structure at ℓ. The main goal of this note is to study the existence of local points at primes $p \neq \ell$ of bad reduction on the intermediate curves of these coverings and their Atkin-Lehner quotients.

CONTENTS

INTRODUCTION

Let $X_D/\mathbb{Q}$ be the Shimura curve associated with a maximal order $\mathcal{O}_D$ in an indefinite rational quaternion algebra B_D of reduced discriminant $D > 1$. The existence of points on X_D rational over local fields was studied by Jordan and Livné in [JL85]. At primes $p \mid D$ (the primes of bad reduction for X_D), their results rely mainly on the p-adic uniformisation theory of Cherednik and Drinfeld (see [Dri76, BC91]), together with the combinatorial description of the special fibre of admissible curves over $\mathbb{Z}_p$ obtained by Mumford uniformisation through their dual graphs, following previous work of Kurihara [Kur79]. Similarly, Ogg [Ogg85] analysed the existence of local points on the Atkin-Lehner quotients of X_D at primes of bad reduction.

In contrast, a systematic approach to the problem of the existence of global points on Shimura curves or their Atkin-Lehner quotients is not known so far, and in spite of this, they are expected to provide non-trivial candidates to test cohomological obstructions to the Hasse principle. One strategy to tackle this problem is to apply descent to étale coverings of these curves. Then the question is transferred to these coverings and their twists, where one hopes to find a simpler resolution. In this direction, this note addresses the study of local points at primes of bad reduction on the intermediate curves of a cyclic Galois covering of Shimura curves $X_{D,\ell} \to X_D$ associated to a prime $\ell \mid D$, which was first introduced by Jordan [Jor81] in his investigations of the arithmetic of X_D. As described in [dVP13], the curves $X_{D,\ell}$ give rise to étale Galois coverings of the classical Shimura curves X_D and their Atkin-Lehner quotients, and hence play an important role in the understanding of the diophantine arithmetic of the latter curves (cf. for example [Sko05],[Jor81, Ch. 5],[RdVP]).

Curves $X_{D,\ell}$ admit a moduli interpretation in terms of abelian surfaces with quaternionic multiplication and a suitable level structure at ℓ, and they are of arithmetic interest also in other scenarios. For instance, the Jacobian variety $J_{D,\ell}$ of $X_{D,\ell}$ provides a compatible system of Galois representations whose local conductor at ℓ is ℓ^2. Further, the theory of Jacquet-Langlands on automorphic representations of twists of GL_2 shows that automorphic forms on the classical modular curve $X_0(\ell D)$ may be lifted to $X_{D,\ell}$. This affords a modular parametrisation

$$\pi_{D,\ell} : J_{D,\ell} \longrightarrow E$$

[1]During the elaboration of this work, the author was supported in part by the Catalan Research Council under grant 2009SGR1220, by the Spanish Council under project MTM2012-34611 and by a FPU grant from the Ministerio de Educación de España.

2010 *Mathematics Subject Classification.* 11G18, 11G20, 14G05, 14G35.
Key words and phrases. Shimura curves, Atkin-Lehner quotients, local points, coverings.

of any elliptic curve $E/\mathbb{Q}$ of conductor ℓD, which becomes particularly interesting for applications to the theory of Heegner points and the conjecture of Birch and Swinnerton-Dyer when the local root number of E at ℓ is -1 (cf. [LRdVP]).

In the next section we describe in some detail the results of this article. The main goal is to study the local diophantine properties of the intermediate curves of the coverings $X_{D,\ell} \to X_D$, and to characterise the existence of local points on them at primes p of bad reduction. The reader may notice that we leave aside the case $p = \ell$, and we do so not because that case lacks interest, but rather because the methods required to approach that setting are strikingly different from the ones employed here. We hope to cover this case elsewhere.

1. Statement of the main results

Let $\mathbb{A}_\mathbb{Q}$ and $\mathbb{A}_f := \mathbb{A}_{\mathbb{Q},f}$ denote the ring of $\mathbb{Q}$-adèles and finite $\mathbb{Q}$-adèles, respectively. Write $\hat{\mathbb{Z}} := \prod_v \mathbb{Z}_v$ for the profinite completion of the ring of integers, and $\widehat{\mathcal{O}}_D := \mathcal{O}_D \otimes_\mathbb{Z} \hat{\mathbb{Z}}$. Besides, fix once and for all an isomorphism $\Psi : B_D \otimes_\mathbb{Q} \mathbb{R} \xrightarrow{\simeq} \mathrm{M}_2(\mathbb{R})$, under which the group of units of norm 1 in $B_D^\times$ acts as conformal transformations on the complex upper half plane $\mathcal{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Similarly, the group of units $B_D^\times$ acts naturally by linear fractional transformations on $\mathcal{H}^\pm := \mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R}) = \mathbb{C} - \mathbb{R}$.

For any compact open subgroup $U \subseteq \widehat{\mathcal{O}}_D^\times$, consider the topological space of double cosets

$$X_U := B_D^\times \setminus (\mathcal{H}^\pm \times (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times / U),$$

where $B_D^\times$ acts simultaneously on the left on both $\mathcal{H}^\pm$ and $(B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times$, and U acts on the right on $(B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times$: that is, for $z \in \mathcal{H}^\pm$, $\beta = (\beta_v)_v \in (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times$, $b \in B_D^\times$ and $u = (u_\ell)_v \in U$,

$$b \cdot (z, \beta) \cdot u = (bz, b\beta u) = (bz, (b\beta_\ell u_v)_v).$$

After the work of Shimura and Deligne (see, for example, [Shi63, Shi67, Del71, Mil04]), X_U admits a canonical model which is an algebraic curve over $\mathbb{Q}$. We still denote this Shimura curve by X_U, which need not be geometrically connected. Indeed, the connected components of $X_U \times_\mathbb{Q} \mathbb{C}$ are indexed by the double coset space (see [Mil04, Lemmas 5.12, 5.13])

$$\mathcal{C}_\infty(U) := B_{D,+}^\times \setminus (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times / U. \tag{1}$$

Write $\mathrm{n} : B_D \to \mathbb{Q}$ for the reduced norm on B_D and, by slight abuse of notation, denote also by n the reduced norm induced on the local quaternion algebras $B_{D,v} := B_D \otimes_\mathbb{Q} \mathbb{Q}_v$, where v is place of $\mathbb{Q}$, and on the adelisation $B_D \otimes_\mathbb{Q} \mathbb{A}_f$. Since B_D is indefinite, the reduced norm induces an isomorphism

$$\mathcal{C}_\infty(U) = B_{D,+}^\times \setminus (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times / U \xrightarrow{\simeq} \mathbb{Q}^{>0} \setminus \mathbb{A}_f^\times / \mathrm{n}(U) \simeq \hat{\mathbb{Z}}^\times / \mathrm{n}(U), \tag{2}$$

which allows us to identify $\mathcal{C}_\infty(U)$ with the finite set $\hat{\mathbb{Z}}^\times / \mathrm{n}(U)$.

For $\beta \in (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times$, the stabiliser of the corresponding double coset with respect to the action of $B_{D,+}^\times$ on the left is easily seen to be $\Gamma_\beta := B_{D,+}^\times \cap \beta U \beta^{-1}$. By using the isomorphism Ψ, the groups Γ_β should be regarded as cocompact subgroups of $\mathrm{GL}_2(\mathbb{R})$, and the quotients $\Gamma_\beta \setminus \mathcal{H}$ are connected compact Riemann surfaces (we can even consider the image of Γ_β in $\mathrm{PGL}_2(\mathbb{R})$). Letting β vary over a set of representatives in $\mathcal{C}_\infty(U)$, one has

$$X_U \times_\mathbb{Q} \mathbb{C} \simeq \bigsqcup_{[\beta]} \Gamma_\beta \setminus \mathcal{H}.$$

When taking $U = \widehat{\mathcal{O}}_D^\times$, the curve $X_D := X_{\widehat{\mathcal{O}}_D^\times}/\mathbb{Q}$ is the usual Shimura curve associated with the indefinite rational quaternion algebra B_D, which is the coarse moduli scheme over $\mathbb{Q}$ classifying abelian surfaces with quaternionic multiplication (QM) by $\mathcal{O}_D$, also called *fake elliptic curves*. That is to say, 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]). 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, and $X_D(\mathbb{C})$ is identified with the compact Riemann surface $\Psi(\mathcal{O}_D^1) \setminus \mathcal{H}$, where $\mathcal{O}_D^1$ is the group of units in $\mathcal{O}_D$ of reduced norm 1.

In general, as U varies, the algebraic curves X_U form a projective system indexed by the compact open subgroups U of $(B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times$, as there is a natural projection $X_{U'} \to X_U$ whenever $U' \subseteq U$. This projective system is endowed with a natural action of $(B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times$: if $b \in (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times$, right multiplication by b induces an isomorphism of algebraic curves

$$\rho_U(b) : X_U \longrightarrow X_{b^{-1}Ub}. \tag{3}$$

Notice that if $b \in \mathrm{Norm}_{(B_D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times}(U)$, then the isomorphism $\rho_U(b)$ is actually an automorphism of X_U. This leads to the definition of the so-called *group of modular automorphisms* of the Shimura curve X_U, namely the group $\mathrm{Aut}^{\mathrm{mod}}(X_U) := \mathrm{Norm}_{(B_D\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times}(U)/\mathbb{Q}^\times U$.

Let us fix for the rest of this note a prime $\ell > 3$ dividing D. Associated with ℓ, we define a compact open subgroup $\mathcal{U}_D \subseteq \widehat{\mathcal{O}}_D^\times$ in the following way. For all primes $q \neq \ell$, set $\mathcal{U}_{D,q} := \mathcal{O}_{D,q}^\times$, whereas for the prime ℓ set $\mathcal{U}_{D,\ell} := 1 + I_\ell \subseteq \mathcal{O}_{D,\ell}^\times$, where $I_\ell \subseteq \mathcal{O}_{D,\ell}$ is the unique maximal ideal of $\mathcal{O}_{D,\ell}$, consisting of the non-invertible elements (that is, I_ℓ is the unique two-sided $\mathcal{O}_{D,\ell}$-ideal of reduced norm $\ell\mathbb{Z}_\ell$). We emphasise that $\mathcal{U}_D$ is maximal outside ℓ, thus we are only adding a certain *level structure* at ℓ.

We denote the canonical model over $\mathbb{Q}$ of the Shimura curve associated to $\mathcal{U}_D$ by $X_{D,\ell}$. As X_D, this curve has also a moduli interpretation. Namely, it is the coarse moduli scheme over $\mathbb{Q}$ for triplets (A, ι, x_ℓ), where (A, ι) is an abelian surface with QM by $\mathcal{O}_D$ and x_ℓ is a generator of the canonical torsion subgroup of (A, ι) at the prime ℓ, regarded as an $\mathcal{O}_D$-module (see [Jor81, p. 110], [Sko05, Section 2]). However, the curve $X_{D,\ell}$ is not geometrically connected. Indeed, $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}(\mu_\ell)$ decomposes as a disjoint union of $\ell-1$ isomorphic geometrically connected components, defined over $\mathbb{Q}(\mu_\ell)$ and conjugated by the action of $\mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$, where $\mathbb{Q}(\mu_\ell)$ denotes the ℓ-th cyclotomic field (cf. [dVP13] or Section 2 below).

The inclusion $\mathcal{U}_D \subseteq \widehat{\mathcal{O}}_D^\times$ induces a natural finite flat morphism $X_{D,\ell} \to X_D$ defined over $\mathbb{Q}$, which is a cyclic Galois covering with Galois group isomorphic to (cf. [dVP13] and Section 2 below)

$$\widehat{\mathcal{O}}_D^\times/\{\pm 1\}\mathcal{U}_D \simeq \mathcal{O}_{D,\ell}^\times/\{\pm 1\}(1 + I_\ell) \simeq \mathbb{F}_{\ell^2}^\times/\{\pm 1\}.$$

In particular, for every positive divisor d of $(\ell^2 - 1)/2$, there is a unique intermediate cyclic Galois covering $Y_d \to X_D$ of degree d. Namely, the curve Y_d is the Shimura curve corresponding to the unique intermediate compact open subgroup $\mathcal{U}_D \subseteq U_d \subseteq \widehat{\mathcal{O}}_D^\times$ of index d in $\widehat{\mathcal{O}}_D^\times$, or, equivalently, to the unique subgroup $H_d \subseteq \mathbb{F}_{\ell^2}^\times$ of index d.

In [dVP13], we studied the geometry of these coverings and the group of modular automorphisms of the Shimura curves Y_d, which are described as a semidirect product of the group of covering automorphisms of $Y_d \to X_D$ with the group of lifted Atkin-Lehner involutions from X_D to Y_d (*ibid.*). In particular, if ω_m denotes the Atkin-Lehner involution on X_D attached to a positive divisor m of D and $\hat{\omega}_m$ is the corresponding lifted involution on Y_d, then we have an induced covering

$$Y_d^{(m)} := Y_d/\langle\hat{\omega}_m\rangle \longrightarrow X_D^{(m)} := X_D/\langle\omega_m\rangle.$$

The purpose of this note is to study the existence of local points at primes p dividing D/ℓ on the curves Y_d and their Atkin-Lehner quotients. Curves Y_d have bad reduction at these primes, and we therefore require the theory of Cherednik and Drinfeld on the p-adic uniformisation of Shimura curves to describe the formal completion along the closed fibre of the $\mathbb{Z}_p$-integral models of the curves $Y_d \times_{\mathbb{Q}} \mathbb{Q}_p$ as quotients of Drinfeld's p-adic upper half plane in the category of formal schemes. After a brief review of the geometry and the arithmetic of the covering $X_{D,\ell} \to X_D$ and its intermediate curves in Section 2, we devote Section 3 to present this theory, following mainly [BC91] and with special emphasis on the algebraisation of these formal schemes.

In order to state the main results of this paper, to be proved in Sections 4 and 5, fix a positive divisor d of $(\ell^2 - 1)/2$ and consider the corresponding curve $Y_d/\mathbb{Q}$ as before. Write $t_d := (\ell^2 - 1)/d$ for the order of H_d. Even in the cases where Y_d is not geometrically connected, so that its geometric connected components are defined over a non-trivial cyclic extension of $\mathbb{Q}$ (cf. Section 2.2 below), it may be the case that the geometric connected components of $Y_d \times_{\mathbb{Q}} \mathbb{Q}_p$ are defined over $\mathbb{Q}_p$. When this happens, we say that Y_d *decomposes completely over* $\mathbb{Q}_p$. If this does not occur, one can prove the non-existence of rational points over $\mathbb{Q}_p$ (and in fact, over infinitely many extensions $K/\mathbb{Q}_p$) on Y_d by elementary Galois-theoretic arguments. We refer the reader to Section 4.1 for the details. In contrast, when Y_d decomposes completely over $\mathbb{Q}_p$, we need to invoke Cherednik-Drinfeld theory to describe a $\mathbb{Z}_p$-integral model $\mathcal{Y}_d$ of $Y_d \times_{\mathbb{Q}} \mathbb{Q}_p$ as a finite disjoint union of quadratic twists of Mumford curves. Namely, if $c_\infty(d)$ is the number of geometric connected components of Y_d, there is a discrete cocompact subgroup $\Gamma_d \subseteq \mathrm{GL}_2(\mathbb{Q}_p)$ (obtained from the definite quaternion algebra whose local invariants at p and ∞ are the opposite from those of B_D) such that

$$\mathcal{Y}_d \simeq \coprod_{i=1}^{c_\infty(d)} \mathcal{Y}_{\Gamma_d}, \tag{4}$$

where $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is a quadratic twist of the Mumford curve[1] $\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p$ associated with an index two subgroup $\Gamma_{d,+}$ of Γ_d.

In particular, $\mathcal{Y}_{\Gamma_d}$ is an admissible curve over $\mathbb{Z}_p$ in the sense of [JL85, Definition 3.1], and the existence of $\mathbb{Q}_p$-rational points on $\mathcal{Y}_{\Gamma_d}$ (hence on Y_d) can be tackled via Hensel's lemma by studying the combinatorics of its dual graph. In Section 4 we prove the following statement (cf. Proposition 4.18 and Corollary 4.20):

Theorem 1.1. *Assume Y_d decomposes completely over $\mathbb{Q}_p$. Let $K/\mathbb{Q}_p$ be a finite extension, and write $f_K := f(K/\mathbb{Q}_p)$, $e_K := e(K/\mathbb{Q}_p)$. Then:*

- a) *If f_K is even, then $Y_d(K) \neq \emptyset$.*
- b) *If f_K is odd and e_K is even, then $Y_d(K) \neq \emptyset$ if and only if any of the following conditions holds:*
  - i) *$\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$ and $4 \mid t_d$,*
  - ii) *$p = 2$, $4 \mid t_d$, $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and H_d contains a root of $x^2 + 2x + 2 = 0$, or*
  - iii) *$p = 3$, $6 \mid t_d$, $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and H_d contains a root of $x^2 + 3x + 3 = 0$.*
- c) *If both f_K and e_K are odd, then $Y_d(K) \neq \emptyset$ if and only if $p = 2$, every prime dividing $D/2$ is congruent to 3 mod 4 (in particular, $\ell \equiv 3 \mod 4$), $4 \mid t_d$ and either $\mathbb{Q}(\sqrt{-2})$ splits $B_{D/p}$ or H_d contains a root of $x^2 + 2x + 2$.*

Combining this result with the work of Jordan and Livné in [JL85], we can find examples where $X_D(K) \neq \emptyset$ but $Y_d(K) = \emptyset$ (cf. Corollaries 4.21 and 4.22 below).

After proving the previous theorem, in Section 5 we focus on the existence of $\mathbb{Q}_p$-rational points on the Atkin-Lehner quotients of the curves Y_d. Suppose that $Y_d(\mathbb{Q}_p)$ is empty (as otherwise $\mathbb{Q}_p$-rational points obviously exist in every Atkin-Lehner quotient of Y_d), and choose a positive divisor m of D. Similarly as above, if Y_d does not decompose completely over $\mathbb{Q}_p$ or $\hat{\omega}_m$ does not act trivially on the set of geometric connected components of Y_d, then one can easily predict the emptiness of $Y_d^{(m)}(\mathbb{Q}_p)$ in most of the cases. Thus we may assume that Y_d decomposes completely over $\mathbb{Q}_p$, and further that $\hat{\omega}_m$ acts as an involution on each geometric connected component of Y_d. Notice that this is clearly the case if Y_d is already geometrically connected.

In this setting, a $\mathbb{Z}_p$-integral model of $Y_d^{(m)}$ is given from (4) as the union of $c_\infty(d)$ copies of the quotient of $\mathcal{Y}_{\Gamma_d}$ by the action induced by $\hat{\omega}_m$. In this way, the existence of $\mathbb{Q}_p$-rational points on $Y_d^{(m)}$ can be characterised by studying the action of $\hat{\omega}_m$ on the dual graphs of the $\mathbb{Z}_p$-admissible curve $\mathcal{Y}_{\Gamma_d}$.

When $m = p$, the quotient of $\mathcal{Y}_{\Gamma_d}$ by $\hat{\omega}_p$ is isomorphic to the (untwisted) Mumford curve $\mathcal{M}_{\Gamma_d}/\mathbb{Z}_p$ associated with Γ_d, and by studying the dual graph of this curve we deduce the criterion for the existence of $\mathbb{Q}_p$-rational points on $Y_d^{(p)}$ (cf. Section 5.2):

Theorem 1.2. *Assume Y_d decomposes completely over $\mathbb{Q}_p$. Then the set $Y_d^{(p)}(\mathbb{Q}_p)$ is not empty if and only if any of the following conditions holds:*

- i) *$\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and $4 \mid t_d$,*
- ii) *$\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and $6 \mid t_d$,*
- iii) *$\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$ and $4 \mid t_d$,*

In contrast, when $m \neq p$ the criterion for the existence of $\mathbb{Q}_p$-rational points on the curve $Y_d^{(m)}$ is deduced in Sections 5.3 and 5.4 by studying the action of the lifted Atkin-Lehner involutions induced on the dual graph of $\mathcal{Y}_{\Gamma_d}$. The next result summarises Theorems 5.24 and 5.28:

Theorem 1.3. *Assume Y_d decomposes completely over $\mathbb{Q}_p$ and $Y_d(\mathbb{Q}_p) = \emptyset$. Let $m > 1$ be a positive divisor of D/p and assume $\hat{\omega}_m$ acts trivially on the set of geometric connected components of Y_d. Then:*

1) *$Y_d^{(m)}(\mathbb{Q}_p)$ is not empty if and only if any of the following conditions holds:*
   - i) *$B_{D/p} \simeq (-m, -p)_{\mathbb{Q}}$, and either*
     - a) *$4 \mid t_d$, or*
     - b) *$p = 3$, $\ell \mid m$, $6 \mid t_d$ and H_d contains a root of $x^2 + 3x + 3 = 0$.*
   - ii) *$B_{D/p} \simeq (-mp, -1)_{\mathbb{Q}}$ and $4 \mid t_d$.*
2) *$Y_d^{(pm)}(\mathbb{Q}_p)$ is not empty if and only if any of the following conditions holds:*
   - i) *$\mathbb{Q}(\sqrt{-m})$ splits $B_{D/p}$, and either*
     - a) *$\ell \mid m$ or $4 \mid t_d$, or*

[1]Strictly speaking, if the image of $\Gamma_{d,+}$ in $\mathrm{PGL}_2(\mathbb{Q}_p)$ is not a Schottky subgroup, then $\mathcal{M}_{\Gamma_{d,+}}$ is not a Mumford curve, but rather a quotient of a Mumford curve by a finite group. Some authors use the term *Mumford quotient* instead.

b) $m = 3$, $6 \mid t_d$ *and* $s_3 H_d$ *contains a root of* $x^2 + 3x + 3 = 0$, *where* $s_3 \in \mathbb{F}_{\ell^2}^\times$ *is a square root of* $3 \mod \ell$.

ii) $m = 2$, $4 \mid t_d$, $\mathbb{Q}(\sqrt{-1})$ *splits* $B_{D/p}$ *and* $s_2 H_d$ *contains a root of* $x^2 + 2x + 2 = 0$, *where* $s_2 \in \mathbb{F}_{\ell^2}^\times$ *is a square root of* $2 \mod \ell$.

We have not tackled in this note the existence of $\mathbb{Q}_p$-rational points on the intermediate curves Y_d of the covering $X_{D,\ell} \to X_D$ and their Atkin-Lehner quotients when $p = \ell$. The main difference with the case $p \neq \ell$ is that one needs to apply Cherednik-Drinfeld theory for Shimura curves with level structure at p (that is to say, the subgroups $U \subseteq \widehat{\mathcal{O}}_D^\times$ to be considered are not maximal at p anymore), which requires to replace Drinfeld's p-adic upper half plane by certain étale Galois coverings of it (cf. [BC91, III.5.7], [Dri76], or also [Te90]). We content here to mention that using the work of Teitelbaum in [Te90] it can be shown that the curves Y_d fail to have $\mathbb{Q}_\ell$-rational points very frequently. More details will appear in [dVP].

2. Shimura coverings of X_D

As in the Introduction, we fix once and for all a prime $\ell > 3$ dividing D and consider the cyclic Galois covering of Shimura curves $X_{D,\ell} \to X_D$. The group of covering automorphisms of $X_{D,\ell} \to X_D$ is isomorphic to the quotient $\widehat{\mathcal{O}}_D^\times/\{\pm 1\}\mathcal{U}_D$, which in turn is isomorphic to $\mathcal{O}_{D,\ell}^\times/\{\pm 1\}(1 + I_\ell)$ because $\mathcal{U}_D$ is locally maximal outside ℓ. As in [Jor81, p. 4], one can regard $\mathcal{O}_{D,\ell}$ as a matrix subring of $\mathrm{M}_2(\mathbb{Z}_{\ell^2})$,

$$\mathcal{O}_{D,\ell} = \left\{ \begin{pmatrix} x & y \\ \ell\bar{x} & \bar{y} \end{pmatrix} : x, y \in \mathbb{Z}_{\ell^2} \right\} \subseteq \mathrm{M}_2(\mathbb{Z}_{\ell^2}),$$

where $x \mapsto \bar{x}$ denotes the non-trivial automorphism in $\mathrm{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p)$, hence we may fix an isomorphism

$$\varphi : \mathcal{O}_{D,\ell}^\times/(1 + I_\ell) \xrightarrow{\simeq} \mathbb{F}_{\ell^2}^\times \tag{5}$$

by setting

$$\varphi(\gamma) := x \mod \ell\mathbb{Z}_{\ell^2} \in \mathbb{F}_{\ell^2}^\times \quad \text{if} \quad \gamma = \begin{pmatrix} x & y \\ \ell\bar{x} & \bar{y} \end{pmatrix}.$$

Therefore, φ provides an automorphism between the groups $\Delta := \mathrm{Aut}(X_{D,\ell}/X_D)$ and $\mathbb{F}_{\ell^2}^\times/\{\pm 1\}$. Furthermore, notice that if $\gamma \in \mathcal{O}_{D,\ell}^\times$ and $\varphi(\gamma(1 + I_\ell)) = x \in \mathbb{F}_{\ell^2}^\times$, then

$$\mathrm{n}(\gamma) \mod \ell\mathbb{Z}_\ell = N_{\mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times}(x). \tag{6}$$

Besides, the group of modular automorphisms $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is recovered from $\mathrm{Aut}^{\mathrm{mod}}(X_D) \simeq W_D$ and Δ. Indeed, the Atkin-Lehner involutions $\omega_m \in W_D$ can be lifted to involutions $\hat{\omega}_m$ on $X_{D,\ell}$, and they fit again into a group $W_{D,\ell} \simeq C_2^{2r}$. The group $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ is then a semidirect (and not direct) product of the groups Δ and $W_{D,\ell}$ (see [dVP13, Theorem 1.2] for further details).

2.1. **Intermediate curves: geometry.** The intermediate curves appearing in the covering $X_{D,\ell} \to X_D$ arise as the Shimura curves X_U associated with the intermediate subgroups $\mathcal{U}_D \subseteq U \subseteq \widehat{\mathcal{O}}_D^\times$. Since $\mathcal{U}_D$ is maximal outside ℓ, the curves X_U actually arise when varying U_ℓ through the subgroups of $\mathcal{O}_{D,\ell}^\times$ containing $1 + I_\ell$. If one of these subgroups does not contain -1, then the subgroup $\{\pm 1\}U_\ell$ gives rise to the same Shimura curve, thus we can restrict ourselves to those subgroups U_ℓ of $\mathcal{O}_{D,\ell}^\times$ containing $\{\pm 1\}(1 + I_\ell)$. In turn, these subgroups are in one to one correspondence with the (cyclic) subgroups Θ_U of Δ: the curve X_U defined by U_ℓ is the quotient of $X_{D,\ell}$ by the action of the subgroup of automorphisms $\Theta_U \subseteq \Delta$, the degree of $X_U \to X_D$ is equal to the index $[\Delta : \Theta_U]$, and the group of covering automorphisms of $X_U \to X_D$ is isomorphic to $\Delta_U := \Delta/\Theta_U$.

Using the identification $\Delta \simeq \mathbb{F}_{\ell^2}^\times/\{\pm 1\}$, we see the above subgroups U_ℓ in correspondence with the cyclic subgroups H of $\mathbb{F}_{\ell^2}^\times$ containing $\{\pm 1\}$. Then, the degree of $X_U \to X_D$ equals the index of H in $\mathbb{F}_{\ell^2}^\times$. For simplicity, let us fix the following notation. For every positive divisor d of $(\ell^2 - 1)/2$, we put:

$Y_d/\mathbb{Q}$: the unique intermediate curve with $\deg(Y_d \to X_D) = d$;
H_d : the unique (cyclic) subgroup of $\mathbb{F}_{\ell^2}^\times$ with $[\mathbb{F}_{\ell^2}^\times : H_d] = d$;
$t_d := |H_d| = (\ell^2 - 1)/d$;
U_d : the compact open subgroup $U_d \subseteq \widehat{\mathcal{O}}_D^\times$ defining Y_d, with $-1 \in U_{d,\ell}$;
$\mathcal{C}_\infty(d) := \mathcal{C}_\infty(U_d)$, the set of geometric connected components of Y_d;
$c_\infty(d) := |\mathcal{C}_\infty(d)|$.

From (1) and (2), the integer $c_\infty(d)$ equals the cardinality of $\hat{\mathbb{Z}}^\times/\mathrm{n}(U_d)$. After (5) and (6),

$$c_\infty(d) = [\mathbb{F}_\ell^\times : N(H_d)] = (\ell-1)/|N(H_d)|, \tag{7}$$

where $N = N_{\mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times} : \mathbb{F}_{\ell^2}^\times \to \mathbb{F}_\ell^\times$ is the norm map. The kernel of N is $\mathbb{F}_{\ell^2}^1 := \{x \in \mathbb{F}_{\ell^2}^\times : x^{\ell+1} = 1\}$, the unique subgroup of order $\ell+1$ in $\mathbb{F}_{\ell^2}^\times$, hence

$$|N(H_d)| = |H_d/(H_d \cap \mathbb{F}_{\ell^2}^1)| = t_d/\gcd(t_d, \ell+1). \tag{8}$$

Therefore, the number $c_\infty(d)$ of geometric connected components of Y_d can be easily computed solely in terms of d and ℓ. Indeed:

Lemma 2.1. *With the above notations,*

$$c_\infty(d) = \gcd(\ell-1, d). \tag{9}$$

In particular:

a) $c_\infty(d) = 1$ *if and only if* d *is an odd divisor of* $\ell+1$*;*
b) $c_\infty(d) = 2$ *if and only if* d *is an even divisor of* $2(\ell+1)$ *and either* $\ell \equiv 3 \pmod 4$ *or* $4 \nmid d$*;*
c) $c_\infty(d)$ *is even if and only if* d *is even, or equivalently, if and only if* $N(H_d) \subseteq \mathbb{F}_\ell^{\times 2}$*.*

Proof. The equality (9) follows by direct computation from (7) and (8). And then the three remaining assertions are immediate, except probably the second part of (c). But notice that (7) tells us that $c_\infty(d)$ is even if and only if $N(H_d)$ is contained in the unique subgroup of $\mathbb{F}_\ell^\times$ of index 2, which is precisely the subgroup $\mathbb{F}_\ell^{\times 2}$ of quadratic residues modulo ℓ. □

Considering the action of the lifted Atkin-Lehner involutions $\hat{\omega}_m$ on $X_{D,\ell}$, as well as the induced involutions on the curves Y_d, we have commutative diagrams

$$\begin{array}{ccccc} X_{D,\ell} & \longrightarrow & Y_d & \longrightarrow & X_D \\ \downarrow & & \downarrow & & \downarrow \\ X_{D,\ell}^{(m)} & \longrightarrow & Y_d^{(m)} & \longrightarrow & X_D^{(m)}, \end{array}$$

where the superscript (m) means quotient by $\hat{\omega}_m$ (or ω_m, in the case of X_D), and the vertical arrows are the natural quotient maps.

Identifying the set of geometric connected components of $X_{D,\ell}$ with $\mathbb{F}_\ell^\times$, we know (see [dVP13]) that the action of $\hat{\omega}_m$ on it is by multiplication by

$$\varepsilon(m) := \begin{cases} \left(\frac{m}{\ell}\right) & \text{if } \ell \nmid m, \\ -\left(\frac{m/\ell}{\ell}\right) & \text{if } \ell \mid m. \end{cases} \tag{10}$$

If we consider an intermediate curve Y_d, the action of the induced involution $\hat{\omega}_m$ on its set of geometric connected components is by multiplication by $\varepsilon_d(m) := \varepsilon(m) \mod N(H_d)$ on $\mathbb{F}_\ell^\times/N(H_d)$. Thus $\varepsilon_d(m)$ is non-trivial if and only if $\varepsilon(m) = -1$ and $-1 \notin N(H_d)$. Regarding the last condition:

Lemma 2.2. *With the above notations,* $-1 \in N(H_d)$ *if and only if* $\mathrm{ord}_2(d) < \mathrm{ord}_2(\ell-1)$*.*

Proof. Since $-1 \in \mathbb{F}_\ell^\times$ is the unique element of order 2 and $\mathbb{F}_\ell^\times$ is cyclic, we have that $-1 \in N(H_d)$ if and only if $|N(H_d)|$ is even. On the other hand, combining (7) and (9) we have that

$$|N(H_d)| = \frac{\ell-1}{\gcd(\ell-1, d)},$$

hence it is clear that $|N(H_d)|$ is even if and only if $\mathrm{ord}_2(d) < \mathrm{ord}_2(\ell-1)$, thus the statement follows. □

After this lemma, we can easily determine whether a lifted Atkin-Lehner involution $\hat{\omega}_m$ acts trivially on the set of geometric connected components of an intermediate curve Y_d or not. In particular, we can compute the number of geometric connected components of $Y_d^{(m)}$, which is either $c_\infty(d)$ or $c_\infty(d)/2$, respectively. For example, by combining Lemmas 2.1 and 2.2:

Lemma 2.3. *The curve* $Y_d^{(m)}$ *is geometrically connected if and only if either*

i) d *is an odd divisor of* $\ell+1$*, or*
ii) d *is an even divisor of* $2(\ell+1)$*,* $\varepsilon(m) = -1$ *and* $\ell \equiv 3 \pmod 4$*.*

2.2. **Intermediate curves: arithmetic.** Although the Shimura curve $X_{D,\ell}$ is defined over $\mathbb{Q}$, its geometric connected components are only defined over the ℓ-th cyclotomic extension $\mathbb{Q}(\mu_\ell)$. Indeed, the choice of a model over $\mathbb{Q}$ for $X_{D,\ell}$ induces an action of $\mathrm{Aut}(\mathbb{C})$ on $X_{D,\ell}(\mathbb{C})$, which is compatible with the action of $\mathrm{Aut}(\mathbb{C})$ through its quotient $\mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q}) \simeq \hat{\mathbb{Z}}^\times$ on the set

$$\mathcal{C}_\infty(\mathcal{U}_D) \simeq \hat{\mathbb{Z}}^\times/\mathrm{n}(\mathcal{U}_D) \simeq \mathbb{F}_\ell^\times$$

under the map

$$X_{D,\ell}(\mathbb{C}) = B_{D,+}^\times \setminus (\mathcal{H} \times (B_D \otimes_\mathbb{Q} \mathbb{A}_f)^\times/\mathcal{U}_D) \longrightarrow \mathcal{C}_\infty(\mathcal{U}_D) \simeq \hat{\mathbb{Z}}^\times/\mathrm{n}(\mathcal{U}_D)$$

given by $[z,b] \mapsto [\mathrm{n}(b)]$. The open subgroup $U_c \subseteq \hat{\mathbb{Z}}^\times \simeq \mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q})$ fixing the class $[\mathrm{n}(c)]$ corresponding to a component $c \in \mathcal{C}_\infty(\mathcal{U}_D)$ is

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

thus the number field contained in $\mathbb{Q}^{ab}$ fixed by the action of U_c is $\mathbb{Q}(\mu_\ell)$, the ℓ-th cyclotomic field. It follows that the $\ell - 1$ geometric connected components of $X_{D,\ell} \times \bar{\mathbb{Q}}$ are defined over $\mathbb{Q}(\mu_\ell)$, and conjugated by the action of $\mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q})$. Hence we can write

$$X_{D,\ell} \times_\mathbb{Q} \mathbb{Q}(\mu_\ell) \simeq \bigsqcup_{\sigma \in \mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q})} {}^\sigma(X_{D,\ell}^0), \tag{11}$$

where $X_{D,\ell}^0/\mathbb{Q}(\mu_\ell)$ is a geometrically connected curve, and the isomorphism is over $\mathbb{Q}(\mu_\ell)$.

Analogously, the field of definition of the geometric connected components of an intermediate curve Y_d is determined in the same way. Replacing $X_{D,\ell}$ by Y_d and $\mathcal{C}_\infty(\mathcal{U}_D)$ by $\mathcal{C}_\infty(d)$, the open subgroup $U_{c'} \subseteq \hat{\mathbb{Z}}^\times \simeq \mathrm{Gal}\,(\mathbb{Q}^{ab}/\mathbb{Q})$ fixing the class $[\mathrm{n}(c')] \in \hat{\mathbb{Z}}^\times/\mathrm{n}(U_d)$ of a component $c' \in \mathcal{C}_\infty(d)$ is now

$$U_{c'} = \prod_{q \neq \ell} \mathbb{Z}_q^\times \times \mathrm{n}(U_{d,\ell}).$$

Using again the relationship between the reduced norm n on subgroups of $\mathcal{O}_{D,\ell}^\times$ containing $\{\pm 1\}(1 + I_\ell)$ and the norm map N on subgroups of $\mathbb{F}_{\ell^2}^\times$ given by (6), we see that the subfield of $\mathbb{Q}^{ab}$ fixed by the action of $U_{c'}$ is the subextension $\mathbb{Q} \subseteq K_d \subseteq \mathbb{Q}(\mu_\ell)$ corresponding, by Galois theory, to the unique subgroup G_d of $\mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q}) \simeq \mathbb{F}_\ell^\times$ of index $c_\infty(d)$. In particular, $\mathrm{Gal}\,(K_d/\mathbb{Q}) \simeq \mathrm{Gal}\,(\mathbb{Q}(\mu_\ell)/\mathbb{Q})/G_d$ is cyclic of order $c_\infty(d)$, thus $[K_d : \mathbb{Q}] = c_\infty(d)$. Similarly as before, we obtain that the $c_\infty(d)$ geometric connected components of Y_d are now defined over K_d, and $\mathrm{Gal}\,(K_d/\mathbb{Q})$ acts freely and transitively on $\mathcal{C}_\infty(d)$. Thus we have a decomposition

$$Y_d \times_\mathbb{Q} K_d \simeq \bigsqcup_{\sigma \in \mathrm{Gal}\,(K_d/\mathbb{Q})} {}^\sigma(Y_d^0) \tag{12}$$

over K_d, where now Y_d^0 is a geometrically connected curve defined over K_d.

Now fix a prime p dividing D, $p \neq \ell$. We consider the curve $X_D \times_\mathbb{Q} \mathbb{Q}_p$ over $\mathbb{Q}_p$ obtained from X_D through extension of scalars from $\mathbb{Q}$ to $\mathbb{Q}_p$, and also the curve $X_{D,\ell} \times_\mathbb{Q} \mathbb{Q}_p$ obtained in the same way from $X_{D,\ell}$. Let us describe how the curve $X_{D,\ell} \times_\mathbb{Q} \mathbb{Q}_p$ and its quotients decompose as a union of geometrically connected curves over unramified extensions of $\mathbb{Q}_p$; this description motivates the p-adic uniformisation of the curves $X_{D,\ell}$ and Y_d that we will work out later.

The curve $X_{D,\ell} \times_\mathbb{Q} \mathbb{Q}_p$ still has $\ell - 1$ geometric connected components, and they are defined over $\mathbb{Q}_p(\mu_\ell)$. Since $p \neq \ell$, the ℓ-th cyclotomic extension $\mathbb{Q}_p(\mu_\ell)$ of $\mathbb{Q}_p$ is unramified, and the ℓ-th cyclotomic character $\chi_\ell : \mathrm{Gal}\,(\mathbb{Q}_p(\mu_\ell)/\mathbb{Q}_p) \to \mathbb{F}_\ell^\times$ maps the Frobenius automorphism to the inverse class of $p \mod \ell$. It follows that $[\mathbb{Q}_p(\mu_\ell) : \mathbb{Q}_p]$ equals the order of $p \mod \ell$ in $\mathbb{F}_\ell^\times$.

For each integer $f \geq 1$, let us denote by $\mathbb{Q}_{p^f}$ the unique unramified extension of $\mathbb{Q}_p$ of degree f. Recall that $\mathbb{Q}_{p^f}$ is the cyclotomic extension $\mathbb{Q}_p(\mu_{p^f-1})$ obtained by adjoining to $\mathbb{Q}_p$ the $(p^f - 1)$-th roots of unity. Hence, if we set f to be the order of $p \mod \ell$ in $\mathbb{F}_\ell^\times$, then $\mathbb{Q}_p(\mu_\ell) = \mathbb{Q}_{p^f}$ is the unique unramified extension of degree f of $\mathbb{Q}_p$. Since f divides $\ell - 1$, let us write $\ell - 1 = fc$, where c is a positive integer.

The geometric interpretation is the following. After extending scalars from $\mathbb{Q}$ to $\mathbb{Q}_p$, the geometric connected components of $X_{D,\ell} \times_\mathbb{Q} \mathbb{Q}_p$ are defined over $\mathbb{Q}_{p^f}$. If $c > 1$, then the Galois action of $\mathrm{Gal}\,(\mathbb{Q}_{p^f}/\mathbb{Q}_p) \simeq \mathbb{Z}/f\mathbb{Z}$ is not transitive in the set of geometric connected components of $X_{D,\ell} \times_\mathbb{Q} \mathbb{Q}_p$, but it defines $c = (\ell - 1)/f$ Galois orbits instead, each of them having f components. Each of the geometric components of $X_{D,\ell} \times_\mathbb{Q} \mathbb{Q}_p$ is then isomorphic to

$$X_{D,\ell}^0 \times_{\mathbb{Q}(\mu_\ell)} \mathbb{Q}_p(\mu_\ell) = X_{D,\ell}^0 \times_{\mathbb{Q}(\mu_\ell)} \mathbb{Q}_{p^f},$$

where $X^0_{D,\ell}/\mathbb{Q}(\mu_\ell)$ is as above, hence the p-adic counterpart of (11) can be written as

$$X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}_{p^f} \;\simeq\; \bigsqcup_{i=1}^{c} \bigsqcup_{\sigma\in \mathrm{Gal}\,(\mathbb{Q}_{p^f}/\mathbb{Q}_p)} {}^{\sigma}(X^0_{D,\ell} \times_{\mathbb{Q}(\mu_\ell)} \mathbb{Q}_{p^f}).$$

Now we look at the intermediate curve $Y_d \times_{\mathbb{Q}} \mathbb{Q}_p$ in the covering $X_{D,\ell} \times_{\mathbb{Q}} \mathbb{Q}_p \to X_D \times_{\mathbb{Q}} \mathbb{Q}_p$. The field of definition $K_d\mathbb{Q}_p$ of the geometric connected components of this curve is a subfield of $\mathbb{Q}_p(\mu_\ell) = \mathbb{Q}_{p^f}$, thus it is an unramified extension of $\mathbb{Q}_p$ contained in $\mathbb{Q}_{p^f}$. Therefore, we can write $K_d\mathbb{Q}_p = \mathbb{Q}_{p^{f_d}}$ for some positive integer f_d dividing f. In order to determine the integer f_d, observe that the ℓ-th cyclotomic character induces, by passage to the quotient, a character $\mathrm{Gal}\,(\mathbb{Q}_{p^{f_d}}/\mathbb{Q}_p) \to \mathbb{F}_\ell^\times/N(H_d)$. Similarly as before, the integer $f_d = [\mathbb{Q}_{p^{f_d}} : \mathbb{Q}_p]$ is the order of $p \mod \ell$ in $\mathbb{F}_\ell^\times/N(H_d)$. In particular, f_d divides $c_\infty(d)$. Equivalently, f_d is the smallest positive integer such that $p^{f_d} \mod \ell \in N(H_d)$. Writing $c_\infty(d) = c_p(d)f_d$, we eventually find the p-adic counterpart of (12):

$$Y_d \times_{\mathbb{Q}} \mathbb{Q}_{p^{f_d}} \;\simeq\; \bigsqcup_{i=1}^{c_p(d)} \bigsqcup_{\sigma\in \mathrm{Gal}\,(\mathbb{Q}_{p^{f_d}}/\mathbb{Q}_p)} {}^{\sigma}(Y^0_d \times_{K_d} \mathbb{Q}_{p^{f_d}}).$$

3. Cherednik-Drinfeld theory

In this section we review the Theorem of Cherednik and Drinfeld on the p-adic uniformisation of Shimura curves at primes p of bad reduction, assuming that there is no level structure at p. Especially in Section 3.1, we have followed the exposition in [BC91]. By extending the moduli problems for Shimura curves X_U to moduli problems in the category of $\mathbb{Z}$-schemes, curves X_U admit a proper, flat, integral (but not smooth) model over $\mathbb{Z}$. We denote by $\mathcal{X}_U/\mathbb{Z}_p$ the base change from $\mathbb{Z}$ to $\mathbb{Z}_p$ of these $\mathbb{Z}$-schemes, so that $\mathcal{X}_U$ is a $\mathbb{Z}_p$-integral model of the Shimura curve X_U. In particular, we write $\mathcal{X}_D$, $\mathcal{X}_{D,p}$ and $\mathcal{Y}_d$ for the $\mathbb{Z}_p$-integral models thus obtained for the curves X_D, $X_{D,p}$ and Y_d, respectively.

3.1. **Statement of the Theorem of Cherednik and Drinfeld.** Let p be a prime dividing D, and assume we are given a compact open subgroup $U \subseteq \widehat{\mathcal{O}}_D^\times$ of the form $U_p^0U^p$, where $U_p^0 = \mathcal{O}_{D,p}^\times$ and $U^p \subseteq \prod_{q\neq p}\mathcal{O}_{D,q}^\times$ (i.e. U is maximal at p). Let also $B_{D/p}$ be the definite rational quaternion algebra of reduced discriminant D/p. One can think of $B_{D/p}$ as obtained from B_D by interchanging the local invariants at the primes p and ∞. We fix an isomorphism

$$(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times \xrightarrow{\;\simeq\;} (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times, \tag{13}$$

obtained from an anti-isomorphism $B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p \longrightarrow B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p$ composed by the inversion. Having fixed this isomorphism, by a slight abuse of notation the image of an element $b^p = (b_v^p)_{v\neq p} \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ will be written as $(b^p)^{-1} = ((b_v^p)^{-1})_{v\neq p} \in (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$. In particular, $U^p \subseteq (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ can also be regarded as a subgroup of $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$, so that we can compare the actions of U^p by multiplication on $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ and $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$: right multiplication by $u \in U^p$ on $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ corresponds with left multiplication by u^{-1} on $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$. We also fix an isomorphism $B_{D/p,p}^\times = (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{Q}_p)^\times \simeq \mathrm{GL}_2(\mathbb{Q}_p)$ by identifying the local quaternion algebra $B_{D/p,p}$ with $\mathrm{M}_2(\mathbb{Q}_p)$. Then $\mathrm{GL}_2(\mathbb{Q}_p)$ acts naturally on the left on the collection of double cosets

$$Z_U := U^p \setminus (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times / B_{D/p}^\times.$$

This action has only finitely many orbits, thus the set

$$\mathcal{C}_p(U) := \mathrm{GL}_2(\mathbb{Q}_p) \setminus Z_U = U^p \setminus (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times / B_{D/p}^\times$$

is finite. The integer $c_p(U) := |\mathcal{C}_p(U)|$ is closely related to the number $c_\infty(U) := |\mathcal{C}_\infty(U)|$ of geometric connected components of the Shimura curve X_U. Indeed, the reduced norm induces now an isomorphism

$$\mathrm{GL}_2(\mathbb{Q}_p) \setminus Z_U = U^p \setminus (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times / B_{D/p}^\times \xrightarrow{\;\simeq\;} \mathrm{n}(U^p) \setminus (\mathbb{A}_f^p)^\times / \mathbb{Q}^{>0},$$

and using $(\mathbb{A}_f^p)^\times = \mathbb{Q}^{>0}(\hat{\mathbb{Z}}^p)^\times$ and $\mathbb{Q}^{>0} \cap (\hat{\mathbb{Z}}^p)^\times = \langle p\rangle = \{p^a : a \in \mathbb{Z}\}$ we identify the right hand side with

$$\mathrm{n}(U^p) \setminus (\hat{\mathbb{Z}}^p)^\times / \langle p\rangle.$$

But now observe that the maximality condition at p implies $\mathrm{n}(U_p) = \mathbb{Z}_p^\times$, so that we have

$$\mathrm{n}(U^p) \setminus (\hat{\mathbb{Z}}^p)^\times \simeq \mathrm{n}(U) \setminus \hat{\mathbb{Z}}^\times \simeq \mathcal{C}_\infty(U).$$

Regarding $\langle p\rangle$ as a subgroup of $(\hat{\mathbb{Z}}^p)^\times$, we therefore identify $\mathcal{C}_p(U)$ with the quotient of $\mathcal{C}_\infty(U)$ modulo $\langle p\rangle/(\mathrm{n}(U^p)\cap\langle p\rangle)$. The latter is a finite cyclic group, and its order is the smallest positive integer $f_p(U)$ such that $p^{f_p(U)}\in \mathrm{n}(U^p)\cap\mathbb{Q}^{>0}$. In particular, we have a natural projection map $\mathcal{C}_\infty(U)\to\mathcal{C}_p(U)$ and

$$c_\infty(U)=c_p(U)f_p(U). \tag{14}$$

Geometrically, the $c_\infty(U)$ connected components of $X_U\times_{\mathbb{Q}}\bar{\mathbb{Q}}_p$ are classified into $c_p(U)$ distinct classes, each of them having $f_p(U)$ connected components. Two geometric connected components $c,c'\in\mathcal{C}_\infty(U)$ *belong to the same* p*-class* if c and c' have the same image in $\mathcal{C}_p(U)$.

Finally, we remark that for U^p *small enough*, the collections of double cosets Z_U form a projective system, as U^p varies, on which $(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times$ acts naturally by multiplication on the left: if $b\in(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times$, multiplication on the left by b induces an isomorphism (compare this with (3))

$$\lambda_U(b):Z_U\longrightarrow Z_{bUb^{-1}}.$$

Theorem 3.1 (Cherednik-Drinfeld)**.** *For every U^p small enough, and with $U=U_p^0U^p$ as before, one has an isomorphism of formal $\mathbb{Z}_p$-schemes*

$$\widehat{\mathcal{X}}_U\simeq \mathrm{GL}_2(\mathbb{Q}_p)\setminus[\widehat{\mathcal{H}}_p\widehat{\otimes}\widehat{\mathbb{Z}}_p^{\mathrm{ur}}\times Z_U], \tag{15}$$

where $\widehat{\mathcal{X}}_U$ is the formal completion of $\mathcal{X}_U$ along its closed fiber. This isomorphism is compatible with the natural projections as U^p varies, and also with the action of $(B_D\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times\simeq(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times$ on both sides. It also lifts to an isomorphism between the special formal $\mathcal{O}_{D,p}$-modules associated with the two formal schemes.

We refer the reader to [BC91, Dri76] for a proof of this theorem.

Remark 3.2. The group $\mathrm{GL}_2(\mathbb{Q}_p)$ acts on $\widehat{\mathcal{H}}_p\widehat{\otimes}\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ through the natural action on $\widehat{\mathcal{H}}_p$ and through $g\mapsto\widetilde{\mathrm{Fr}}_p^{-\mathrm{val}_p(\det g)}$ on $\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$, where $\widetilde{\mathrm{Fr}}_p:\mathbb{Z}_p^{\mathrm{ur}}\to\mathbb{Z}_p^{\mathrm{ur}}$ is the lift of the Frobenius automorphism $\mathrm{Fr}_p:\bar{\mathbb{F}}_p\to\bar{\mathbb{F}}_p$ to a $\mathbb{Z}_p$-automorphism. This action is defined over $\mathbb{Z}_p$. Similarly, the right action of an element $b_p\in B_{D,p}^\times$ on $\widehat{\mathcal{X}}_U$ induced by the isomorphism

$$\rho_U(1,\dots,1,b_p,1,\dots):X_U\longrightarrow X_U$$

is translated under (15) to the right hand side to the action on $\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ through $b_p\mapsto\widetilde{\mathrm{Fr}}_p^{-\mathrm{val}_p(\mathrm{n}(b_p))}$.

Remark 3.3. The compatibility of the isomorphism (15) with the right action of $(B_D\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times$ on the left hand side and the left action of $(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times$ on the right hand side requires to compare these two actions by using the anti-isomorphism in (13). We elaborate more on this in paragraph 3.3 below.

Remark 3.4. The special formal $\mathcal{O}_{D,p}$-module associated with $\widehat{\mathcal{X}}_U$ is the formal completion of the universal abelian variety given by the moduli problem associated with U, whereas the special formal $\mathcal{O}_{D,p}$-module associated to the right hand side of the isomorphism in the theorem arises from the moduli description of $\widehat{\mathcal{H}}_p\widehat{\otimes}\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$.

3.2. **Algebraisation: decomposing $\mathcal{X}_U$ as a union of Mumford curves.** Even though (15) is an isomorphism of formal $\mathbb{Z}_p$-schemes, the left hand side is the completion of an algebraic $\mathbb{Z}_p$-scheme along its closed fibre, hence it is obviously algebraisable. As a consequence, the right hand side of (15) is algebraisable as well, and a closer analysis will allow us to obtain an algebraisation. For every subgroup $G\subseteq\mathrm{GL}_2(\mathbb{Q}_p)$, we write $ZG:=G\cap\mathbb{Q}_p^\times$ and denote by $G':=G/ZG$ the image of G in $\mathrm{PGL}_2(\mathbb{Q}_p)$.

First of all, choose representatives $b_i\in(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f)^\times$ for the distinct p-classes in $\mathcal{C}_p(U)$ such that $b_{i,p}=1$, $i=1,\dots,c_p(U)$. For each i, the stabilisers

$$\Gamma_i:=\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Q}_p)}(b_i)=\{g_p\in\mathrm{GL}_2(\mathbb{Q}_p):g_p\cdot b_i\in U^pb_iB_{D/p}^\times\}=B_{D/p}^\times\cap b_i^{-1}U^pb_i$$

are discrete and cocompact subgroups of $\mathrm{GL}_2(\mathbb{Q}_p)$, and it is easy to check that they are conjugated one to each other. Further, they contain some power of $p\in\mathbb{Q}_p^\times\subseteq\mathrm{GL}_2(\mathbb{Q}_p)$. We assume throughout that the groups Γ_i are closed under the canonical involution $b\mapsto\bar{b}$ induced from $B_{D/p}$. It is enough to assume this for one of the Γ_i's, for example for $\Gamma:=\Gamma_1=B_{D/p}^\times\cap U^p$, and this amounts to assuming $\bar{U}^p=U^p$.

Then the natural projection map

$$\mathrm{pr}:\mathrm{GL}_2(\mathbb{Q}_p)\setminus[\widehat{\mathcal{H}}_p\widehat{\otimes}\widehat{\mathbb{Z}}_p^{\mathrm{ur}}\times Z_U]\longrightarrow\mathcal{C}_p(U)=\{[b_1],\dots,[b_{c_p(U)}]\} \tag{16}$$

induces a decomposition into p-classes

$$\mathrm{GL}_2(\mathbb{Q}_p) \setminus [\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}} \times Z_U] = \bigsqcup_{i=1}^{c_p(U)} \mathrm{pr}^{-1}([b_i]) \simeq \bigsqcup_{i=1}^{c_p(U)} \Gamma_i \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}), \tag{17}$$

and using that the Γ_i are conjugated one to each other we conclude that each p-class is isomorphic to

$$\Gamma \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}). \tag{18}$$

Now define $k = k(\Gamma) \geq 1$ to be the positive integer such that $\mathrm{val}_p(Z\Gamma) = k\mathbb{Z}$. Equivalently, since every element in $Z\Gamma = \Gamma \cap \mathbb{Q}^\times$ is of the form p^r for some integer r, k is the smallest positive integer such that $p^k \in \Gamma$. Similarly, define $f = f(\Gamma)$ as the positive integer such that $\mathrm{val}_p(\mathrm{n}(\Gamma)) = f\mathbb{Z}$. In other words, f is the smallest positive integer such that there is an element $\gamma \in \Gamma$ with $\mathrm{val}_p(\mathrm{n}(\gamma)) = f$.

Lemma 3.5. *With notations as before,* $\mathrm{n}(\Gamma) = \mathrm{n}(U^p) \cap \mathbb{Q}^{>0}$. *In particular,* $f(\Gamma) = f_p(U)$ *(cf. (14)).*

Proof. The inclusion $\mathrm{n}(\Gamma) \subseteq \mathrm{n}(U^p) \cap \mathbb{Q}^{>0}$ is clear, because $B_{D/p}^\times$ is definite. So let $t \in \mathrm{n}(U^p) \cap \mathbb{Q}^{>0}$, regarded in $\mathbb{A}_f^p$, and choose $u \in U^p$ with $\mathrm{n}(u) = t$. Since $\mathrm{n}(B_{D/p}^\times) = \mathbb{Q}^{>0}$, we can choose $b \in B_{D/p}^\times$ with $\mathrm{n}(b) = t$. Therefore, $bu^{-1} \in (B_{D/p} \otimes \mathbb{A}_f^p)^\times$ has reduced norm 1. By the Eichler-Kneser strong approximation theorem (see [Vig80, Ch. III, Théorème 4.3]), there are elements $b_1 \in B_{D/p}^\times$, $u_1 \in U^p$, both of norm 1, such that $bu^{-1} = b_1 u_1$. Therefore, $b_1^{-1} b = u_1 u$ holds in $U^p \cap B_{D/p}^\times = \Gamma$ and both sides of the equality have norm t. This shows the inclusion $\mathrm{n}(\Gamma) \supseteq \mathrm{n}(U^p) \cap \mathbb{Q}^{>0}$, thus the first part of the lemma follows. The second part is now a direct consequence of the definitions of $f(\Gamma)$ and $f_p(U)$. □

Since Γ is closed under conjugation, we have $\mathrm{n}(\Gamma) \subseteq \Gamma \cap \mathbb{Q}^\times = Z\Gamma$, hence $\mathrm{val}_p(\mathrm{n}(\Gamma)) \subseteq \mathrm{val}_p(Z\Gamma)$. As a consequence $f\mathbb{Z} \subseteq k\mathbb{Z}$, so that k divides f. Further, from $Z\Gamma \subseteq \Gamma$ we deduce $2k\mathbb{Z} = \mathrm{val}_p(\det(Z\Gamma)) \subseteq \mathrm{val}_p(\mathrm{n}(\Gamma)) = f\mathbb{Z}$, hence f divides $2k$ and we must have either $f = k$ or $f = 2k$. Write

$$\Gamma_+ := \{\gamma \in \Gamma : \mathrm{val}_p(\mathrm{n}(\gamma)) \in 2k\mathbb{Z}\}, \qquad W := \Gamma/\Gamma_+.$$

If $f = 2k$, then $\Gamma_+ = \Gamma$ and W is trivial, whereas if $f = k$, then Γ_+ has index 2 in Γ_+ and W is cyclic of order two, with its non-trivial element represented by any $w \in \Gamma$ such that $\mathrm{val}_p(\mathrm{n}(w)) = f = k$.

Proposition 3.6. *Let* $\widehat{\mathcal{X}}_\Gamma$ *be the formal* $\mathbb{Z}_p$*-scheme corresponding to the formal quotient* (18)*, and let* $\mathcal{M}_{\Gamma_+}/\mathbb{Z}_p$ *be the Mumford curve associated with* Γ_+*, whose formal completion along the closed fibre is the formal quotient* $\Gamma_+ \setminus \widehat{\mathcal{H}}_p$*. Then* $\widehat{\mathcal{X}}_\Gamma$ *is the formal completion along the closed fibre of a projective scheme* $\mathcal{X}_\Gamma/\mathbb{Z}_p$ *such that:*

a) *if* $f = 2k$*, then*

$$\mathcal{X}_\Gamma \times \mathbb{Z}_{p^f} \simeq \bigsqcup_{i=1}^{f} \mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f},$$

the f *copies of* $\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f}$ *being conjugated by the action of* $\mathrm{Gal}\,(\mathbb{Q}_{p^f}/\mathbb{Q}_p)$*;*

b) *if* $f = k$*, then*

$$\mathcal{X}_\Gamma \times \mathbb{Z}_{p^f} \simeq \bigsqcup_{i=1}^{f} (\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f})^\xi,$$

where now the superscript ξ *means that* $\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f}$ *is twisted by the* 1*-cocycle*

$$\xi : \mathrm{Gal}\,(\mathbb{Q}_{p^{2f}}/\mathbb{Q}_{p^f}) \longrightarrow \mathrm{Aut}(\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{2f}}/\mathbb{Z}_{p^{2f}}), \quad \widetilde{\mathrm{Fr}}_p^f \mapsto w \times \mathrm{id},$$

the f *copies of this curve being conjugated by the action of* $\mathrm{Gal}\,(\mathbb{Q}_{p^f}/\mathbb{Q}_p)$.

Proof. By construction, $\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}$ is the extension of scalars of the formal $\mathbb{Z}_p$-scheme $\widehat{\mathcal{H}}_p$ to $\widehat{\mathbb{Z}}_p^{\mathrm{ur}}$, thus we can endow it with its natural Weil descent datum α. Since p^k is the smallest power of p in $Z\Gamma$, and $Z\Gamma$ acts trivially on $\widehat{\mathcal{H}}_p$,

$$\Gamma \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}) \simeq \Gamma' \setminus (Z\Gamma \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}})) \simeq \Gamma' \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \mathbb{Z}_{p^{2k}}) \simeq \Gamma \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \mathbb{Z}_{p^{2k}}).$$

In other words, α^{2k} is effective, and as a consequence of étale descent, α is effective as well. Therefore, we may regard (18) as an algebraisable formal scheme over $\mathbb{Z}_p$, thus it is the formal completion of a projective scheme $\mathcal{X}_\Gamma/\mathbb{Z}_p$ along its special fibre.

From the above observation, using that Γ_+ acts trivially on $\mathbb{Z}_{p^{2k}}$ we have therefore an isomorphism

$$\widehat{\mathcal{X}}_\Gamma \widehat{\otimes} \mathbb{Z}_{p^{2k}} \simeq [W \setminus ((\Gamma_+ \setminus \widehat{\mathcal{H}}_p) \widehat{\otimes} \mathbb{Z}_{p^{2k}})] \widehat{\otimes} \mathbb{Z}_{p^{2k}}.$$

Now the formal quotient $\Gamma_+ \setminus \widehat{\mathcal{H}}_p$ is algebraisable (see [Mum72, Kur79]) by a geometrically connected projective scheme $\mathcal{M}_{\Gamma_+}$ of relative dimension one over $\mathbb{Z}_p$, (a finite quotient of) a Mumford curve. By a slight abuse of notation, we call $\mathcal{M}_{\Gamma_+}$ the Mumford curve associated with Γ_+. If $f = 2k$, then W is trivial, thus the base change to $\mathbb{Z}_{p^{2k}}$ of the $\mathbb{Z}_p$-scheme $\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{2k}}$ is isomorphic to $f = 2k$ copies of $\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{2k}}$ (now as a $\mathbb{Z}_{p^{2k}}$-scheme) conjugated by Galois, hence item a) follows.

In contrast, when $f = k$ we find that the formal $\mathbb{Z}_p$-scheme

$$W \setminus ((\Gamma_+ \setminus \widehat{\mathcal{H}}_p)\widehat{\otimes}\mathbb{Z}_{p^{2f}}),$$

hence $\widehat{\mathcal{X}}_\Gamma$, is algebraisable by the quadratic twist $(\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f})^\xi$ as in the statement, *regarded as a scheme over* $\mathbb{Z}_p$. Then $\mathcal{X}_\Gamma \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f}$ decomposes as f copies of $(\mathcal{M}_{\Gamma_+} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^f})^\xi$ (now regarded as a $\mathbb{Z}_{p^f}$-scheme), again conjugated by Galois. This completes the proof in case b). □

Remark 3.7. Proposition 3.6, together with (17), gives an arithmetic meaning to the the notion of *p-classes*. Namely, the curve $X_U \times_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathcal{X}_U \times_{\mathbb{Z}_p} \mathbb{Q}_p$ decomposes *over* $\mathbb{Q}_p$ as a union of $c_p(U)$ copies of the (not geometrically connected, in general) curve $\mathcal{X}_\Gamma \times_{\mathbb{Z}_p} \mathbb{Q}_p$. Each of these copies corresponds to a p-class in the set $\mathcal{C}_p(U)$, and the f geometric connected components in each p-class, conjugated by the action of $\mathrm{Gal}(\mathbb{Q}_{p^f}/\mathbb{Q}_p)$, arise only after base change to $\mathbb{Q}_{p^f}$.

3.3. ***p*-modular automorphisms.** Recall that the group $\mathrm{Aut}^{\mathrm{mod}}(X_U)$ of modular automorphisms of the Shimura curve $X_U/\mathbb{Q}$ is defined as

$$\mathrm{Aut}^{\mathrm{mod}}(X_U) := \mathrm{Norm}_{(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times}(U)/\mathbb{Q}^\times U \subseteq \mathrm{Aut}_{\mathbb{Q}}(X_U).$$

We now describe a group of automorphisms of $\mathcal{X}_U$ closely related to $\mathrm{Aut}^{\mathrm{mod}}(X_U)$ that can be defined in a similar way from the p-adic counterpart of X_U. Indeed, we have seen above that for U small enough there is a left action of $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ on the projective system Z_U: every element $b \in (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ induces an isomorphism $\lambda_U(b) : Z_U \to Z_{bUb^{-1}}$. It follows that the elements in $\mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)$ induce automorphisms of Z_U, hence automorphisms of $\widehat{\mathcal{X}}_U$. Actually, one has $\lambda_U(b) \in \mathrm{Aut}_{\mathbb{Z}_p}(\mathcal{X}_U)$ for every $b \in \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)$. On the other hand, if $b \in (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$, then $\lambda_U(b)$ is the identity on $\mathcal{X}_U$ if and only if $b \in U^p$. In view of this, we define

$$\mathrm{Aut}^{p\text{-mod}}(\mathcal{X}_U) := \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)/U^p \subseteq \mathrm{Aut}_{\mathbb{Z}_p}(\mathcal{X}_U)$$

and call $\mathrm{Aut}^{p\text{-mod}}(\mathcal{X}_U)$ the group of *p-modular automorphisms* of $\mathcal{X}_U$.

In order to exhibit the close relation between $\mathrm{Aut}^{p\text{-mod}}(\mathcal{X}_U)$ and $\mathrm{Aut}^{\mathrm{mod}}(X_U)$, write $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times \simeq (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times \times B_{D,p}^\times$, so that $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ is identified as a subgroup of $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ via the natural monomorphism $x \mapsto (x, 1)$ into the first factor. Then, by using the anti-isomorphism in (13), we can also regard $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ as a subgroup of $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$.

Now let $(b_v)_{v\neq p} \in \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)$. Then its image $((b_v^{-1})_{v\neq p}, 1)$ in $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ clearly normalises U, and furthermore, $((b_v^{-1})_{v\neq p}, 1) \in \mathbb{Q}^\times U$ if and only if $(b_v)_{v\neq p} \in U^p$ (where here U^p is regarded as a subgroup in $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$). Hence, the group $\mathrm{Aut}^{p\text{-mod}}(\mathcal{X}_U)$ of p-modular automorphisms of $\mathcal{X}_U$ is naturally a subgroup of $\mathrm{Aut}^{\mathrm{mod}}(X_U)$. As Remark 3.3 points out, the modular automorphisms of X_U of the form $\rho_U(((b_v^p)_{v\neq p}, 1))$ correspond with the p-modular automorphisms of $\mathcal{X}_U$ of the form $\lambda_U((b_v^p)^{-1}_{v\neq p})$.

As above, let $\Gamma := B_{D/p}^\times \cap U^p$ be regarded as a subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$, so that

$$\widehat{\mathcal{X}}_\Gamma \simeq \Gamma \setminus (\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}}).$$

Then define

$$\Gamma^* := \mathrm{Norm}_{B_{D/p}^\times}(U^p),$$

which can also be regarded as a subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$. The natural inclusion of $B_{D/p}^\times$ in $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times$ induces an inclusion $\Gamma^* \hookrightarrow \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)$. Furthermore:

Lemma 3.8. *The quotient* Γ^*/Γ *is a subgroup of* $\mathrm{Aut}^{p\text{-}mod}(\mathcal{X}_U)$*, and every p-modular automorphism in* Γ^*/Γ *acts trivially on the set* $\mathcal{C}_p(U)$.

Proof. From the definitions, if $\gamma \in \Gamma^*$, then $\gamma \in \Gamma$ if and only if $\gamma \in U^p$. Therefore, the natural inclusion $\Gamma^* \hookrightarrow \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)$ induces by passing to the quotient a monomorphism of groups

$$\Gamma^*/\Gamma \hookrightarrow \mathrm{Norm}_{(B_{D/p}\otimes_{\mathbb{Q}}\mathbb{A}_f^p)^\times}(U^p)/U^p = \mathrm{Aut}^{p\text{-mod}}(\mathcal{X}_U).$$

As for the second part of the statement, every element in Γ^* normalises Γ, hence its action on $\mathcal{X}_U$ as a p-modular automorphism preserves the fibres of (16). □

4. Local points on the curves Y_d

We keep the notations from the previous sections. Let $X_{D,\ell} \to X_D$ be the Shimura covering of X_D at a prime divisor $\ell > 3$ of D, d be a positive divisor of $(\ell^2-1)/2$ and $Y_d/\mathbb{Q}$ be the unique intermediate curve of degree d over X_D. Let also $p \neq \ell$ be a prime divisor of D. The goal of this section is to study the existence of K-rational points on Y_d for finite extensions K of $\mathbb{Q}_p$. The main tool for this purpose is Cherednik-Drinfeld theory described in Section 3.

4.1. **p-adic uniformisation of the curves Y_d.** Let $\mathcal{X}_D/\mathbb{Z}_p$ (resp. $\mathcal{Y}_d/\mathbb{Z}_p$) be the $\mathbb{Z}_p$-integral model for X_D (resp. Y_d) as in Section 3. In particular, $\mathcal{X}_D$ (resp. $\mathcal{Y}_d$) is a projective, but not smooth, curve over $\mathbb{Z}_p$ with generic fibre $X_D \times_{\mathbb{Q}} \mathbb{Q}_p$ (resp. $Y_d \times_{\mathbb{Q}} \mathbb{Q}_p$). Since U_d is maximal at p (because $p \neq \ell$), we can apply the Theorem of Cherednik and Drinfeld presented in the previous section to the curve Y_d.

We write

$$\Gamma_D := \widehat{\mathcal{O}}_{D/p}^{(p)\times} \cap B_{D/p}^\times = (\mathcal{O}_{D/p} \otimes_{\mathbb{Z}} \mathbb{Z}[1/p])^\times = \mathcal{O}_{D/p}^{(p)\times} \quad \text{and} \quad \Gamma_d := U_d^{(p)} \cap B_{D/p}^\times,$$

regarded as subgroups of $\mathrm{GL}_2(\mathbb{Q}_p)$ after fixing a monomorphism $B_{D/p} \hookrightarrow B_{D/p} \otimes_{\mathbb{Q}} \mathbb{Q}_p$ and an isomorphism $B_{D/p} \otimes_{\mathbb{Q}} \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p)$. Notice that Γ_d is naturally a subgroup of Γ_D. Indeed, writing

$$\nu : \Gamma_D \hookrightarrow \mathcal{O}_{D/p,\ell}^\times \tag{19}$$

for the natural inclusion of Γ_D into $\mathcal{O}_{D/p,\ell}^\times$, we clearly have $\Gamma_d = \nu^{-1}(U_{d,\ell})$. By a slight abuse of notation, we will often just write $\Gamma_d = \Gamma_D \cap U_{d,\ell}$. Furthermore, fixing an anti-isomorphism $\mathcal{O}_{D,\ell}^\times \to \mathcal{O}_{D/p,\ell}^\times$ compatible with (13), the isomorphism in (5) gives rise to an analogous isomorphism

$$\psi : (1+I_\ell) \setminus \mathcal{O}_{D/p,\ell}^\times \xrightarrow{\simeq} \mathbb{F}_{\ell^2}^\times, \tag{20}$$

where here we still denote by I_ℓ the unique maximal ideal of $\mathcal{O}_{D/p,\ell}$, consisting of the non-invertible elements. If $\gamma \in \mathcal{O}_{D/p,\ell}^\times$ and we set $x = \psi((1+I_\ell)\gamma) \in \mathbb{F}_{\ell^2}^\times$, then

$$\mathrm{n}(\gamma) \mod \ell\mathbb{Z}_\ell = N_{\mathbb{F}_{\ell^2}^\times/\mathbb{F}_\ell^\times}(x). \tag{21}$$

Lemma 4.1. *Γ_d is a normal subgroup of Γ_D, and $[\Gamma_D : \Gamma_d]c_p(d) = d$.*

Proof. First of all, observe that since $1+I_\ell$ is normal in $\mathcal{O}_{D/p,\ell}^\times$ and $(1+I_\ell)\setminus \mathcal{O}_{D/p,\ell}^\times \simeq \mathbb{F}_{\ell^2}^\times$ is abelian, $U_{d,\ell}$ is also normal in $\mathcal{O}_{D/p,\ell}^\times$. Now we prove that Γ_d is normal in Γ_D, which by means of the natural inclusion ν from (19) is equivalent to proving that

$$\nu(g^{-1}\gamma g) \in \nu(\Gamma_d) = \nu(\Gamma_D) \cap U_{d,\ell} \quad \text{for all } g \in \Gamma_D, \gamma \in \Gamma_d.$$

Since clearly $\nu(g^{-1}\gamma g) \in \nu(\Gamma_D)$, this holds if and only if $\nu(g^{-1}\gamma g) = \nu(g^{-1})\nu(\gamma)\nu(g) \in U_{d,\ell}$. And this is true because $U_{d,\ell}$ is normal in $\mathcal{O}_{D/p,\ell}^\times$, $\nu(g) \in \mathcal{O}_{D/p,\ell}^\times$ and $\nu(\gamma) \in U_{d,\ell}$.

Besides, it is clear that $\nu(\Gamma_d) \subseteq U_{d,\ell}$, thus composing ν with the natural quotient homomorphism $\mathcal{O}_{D/p,\ell}^\times \to U_{d,\ell} \setminus \mathcal{O}_{D/p,\ell}^\times$ we obtain a monomorphism

$$\Gamma_D/\Gamma_d \hookrightarrow U_{d,\ell} \setminus \mathcal{O}_{D/p,\ell}^\times.$$

Furthermore, the quotient of $U_{d,\ell}\setminus\mathcal{O}_{D/p,\ell}^\times$ by Γ_D/Γ_d can be identified with $\mathcal{C}_p(d)$, thus $[\Gamma_D : \Gamma_d]c_p(d) = d$ as claimed. Indeed, since

$$\widehat{\mathcal{O}}_{D/p}^{(p)\times} \setminus (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times / B_{D/p}^\times$$

is trivial, it follows that every class in

$$\mathcal{C}_p(d) = U_d^{(p)} \setminus (B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times / B_{D/p}^\times$$

is represented by $(1,\dots,1,a_\ell,1,\dots)$ for some $a_\ell \in \mathcal{O}_{D/p,\ell}^\times$ modulo $U_{d,\ell}$. Even more, Γ_D acts transitively on these classes, and the stabiliser of an arbitrary class is $\Gamma_d \subseteq \Gamma_D$. □

While the integers $k(\Gamma_D)$ and $f(\Gamma_D)$ (defined before Lemma 3.5) are both equal to 1, this might not be the case for the integers $k_d := k(\Gamma_d)$ and $f_d := f(\Gamma_d)$, but they are easily determined:

Lemma 4.2. *k_d is the smallest positive integer such that $p^{k_d} \mod \ell$ belongs to $H_d \subseteq \mathbb{F}_{\ell^2}^\times$, and f_d is the smallest positive integer such that $p^{f_d} \mod \ell$ belongs to $N(H_d) \subseteq \mathbb{F}_\ell^\times$.*

Proof. The integer k_d is the smallest positive integer such that $p^{k_d} \in \Gamma_d$. Since clearly $p \in B_{D/p}^\times$, k_d is actually the smallest positive integer such that $p^{k_d} \in U_d^p$. Further, as $p \in \mathcal{O}_{D/p,q}^\times$ for all primes $q \neq p$, we deduce that $p^{k_d} \in \Gamma_d$ if and only if $p^{k_d} \in U_{d,\ell}$. But using the isomorphism ψ from (20), this is equivalent to $p^{k_d} \mod \ell \in H_d$. As for the integer f_d, by Lemma 3.5 we know that f_d is the smallest positive integer such that $p^{f_d} \in \mathrm{n}(U_d^p)$. Since U_d is maximal outside ℓ, this condition is equivalent to saying that $p^{f_d} \in \mathrm{n}(U_{d,\ell})$. By (21), this happens if and only if $p^{f_d} \in N(H_d)$. □

Remark 4.3. Plainly, the integers k_d and f_d are explicitly computable from ℓ, p and d. Indeed, let f be the order of $p \mod \ell$ in $\mathbb{F}_\ell^\times$. Equivalently, f is the order of the cyclic group $\langle p \mod \ell\rangle$ in $\mathbb{F}_\ell^\times \subseteq \mathbb{F}_{\ell^2}^\times$. Then k_d is the order of the image of $\langle p \mod \ell\rangle$ in $\mathbb{F}_{\ell^2}^\times/H_d$, thus

$$k_d = \frac{f}{\gcd(f, t_d)}, \quad \text{where } t_d := |H_d|.$$

Similarly, f_d is the order of the image of $\langle p \mod \ell\rangle$ in $\mathbb{F}_\ell^\times/N(H_d)$, hence using (8) and (9) we have

$$f_d = \frac{f}{\gcd(f, |N(H_d)|)}, \quad \text{where } |N(H_d)| = \frac{t_d}{\gcd(t_d, \ell+1)} = \frac{\ell-1}{\gcd(\ell-1, d)}.$$

Notice that the notation for the integer $f_d = f(\Gamma_d)$ is coherent with the notation used in Section 2.2. Indeed, once the integers k_d and f_d are determined, with $c_\infty(d) = c_p(d) f_d$, Proposition 3.6 (see also Remark 3.7) provides the p-adic uniformisation of the curve Y_d and makes more precise our digression in Section 2.2. Namely, one has a decomposition (over $\mathbb{Z}_p$)

$$\mathcal{Y}_d \simeq \bigsqcup_{i=1}^{c_p(d)} \mathcal{Y}_{\Gamma_d} \tag{22}$$

of $\mathcal{Y}_d$ as a union of its p-classes, all of them isomorphic to a curve $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$: two geometric connected components of $\mathcal{Y}_d$ belong to the same p-class if and only if both are geometric connected components of the same copy of $\mathcal{Y}_{\Gamma_d}$. Furthermore,

$$\mathcal{Y}_{\Gamma_d} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}} \simeq \bigsqcup_{\sigma \in \mathrm{Gal}\,(\mathbb{Q}_{p^{f_d}}/\mathbb{Q}_p)} {}^{\sigma}(\mathcal{Y}_{\Gamma_d}^0), \tag{23}$$

where $\mathcal{Y}_{\Gamma_d}^0/\mathbb{Z}_{p^{f_d}}$ is geometrically connected. Moreover, $\mathcal{Y}_{\Gamma_d}^0$ is isomorphic to either

a) the base change $\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}}$ of the Mumford curve $\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p$ to $\mathbb{Z}_{p^{f_d}}$, if $f_d = 2k_d$, or
b) the quadratic Frobenius twist $(\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}})^\xi$, if $f_d = k_d$, where ξ is induced by the 1-cocycle

$$\mathrm{Gal}\,(\mathbb{Q}_{p^{2f_d}}/\mathbb{Q}_{p^{f_d}}) \longrightarrow \mathrm{Aut}(\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{2f_d}}/\mathbb{Z}_{p^{2f_d}}), \quad \widetilde{\mathrm{Fr}}_p^{f_d} \mapsto w_p \times \mathrm{id},$$

where $w_p \in \Gamma_d$ represents the non-trivial class in $W = \Gamma_d/\Gamma_{d,+}$ (i.e., $w_p \in \Gamma_d$ is any element with $\mathrm{val}_p(\mathrm{n}(w_p)) = f_d$).

As a direct consequence, we find:

Proposition 4.4. *Assume $f_d > 1$, and let $K/\mathbb{Q}_p$ be a finite extension. If $\mathbb{Q}_{p^{f_d}} \not\subseteq K$, then the set $Y_d(K)$ is empty. In particular, $Y_d(\mathbb{Q}_p) = \emptyset$. In contrast, when $\mathbb{Q}_{p^{f_d}}$ is a subfield of K:*

a) *if $f_d = k_d$, then $Y_d(K) \neq \emptyset$ if and only if $(\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}})^\xi(K) \neq \emptyset$.*
b) *if $f_d = 2k_d$, then $Y_d(K) \neq \emptyset$ if and only if $(\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}})(K) \neq \emptyset$.*

Therefore, when $f_d > 1$ we can prove the non-existence of K-rational points on Y_d for *infinitely many* finite extensions $K/\mathbb{Q}_p$ (namely, for all $K/\mathbb{Q}_p$ not containing $\mathbb{Q}_{p^{f_d}}$ as a subfield), although the set $X_D(K)$ may be non-empty. By combining Proposition 4.4 with [JL85], we can give explicit sufficient conditions for $Y_d(K) = \emptyset$ and $X_D(K) \neq \emptyset$ to hold simultaneously. Because of its simplicity, let us point out the following particular case:

Corollary 4.5. *Assume $f_d > 1$, and let $K/\mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$ whose residual degree $f(K/\mathbb{Q}_p)$ is even and such that $\mathbb{Q}_{p^{f_d}} \not\subseteq K$. Then $Y_d(K) = \emptyset$ and $X_D(K) \neq \emptyset$.*

Proof. The assertion $Y_d(K) = \emptyset$ follows from the previous proposition, whereas the non-emptiness of $X_D(K)$ follows from [JL85, Theorem 5.1]. □

Focusing on the study of $\mathbb{Q}_p$-rational points, again using the work of Jordan and Livné we find the following:

Corollary 4.6. *Assume $\ell \equiv 3 \pmod 4$ and $D = 2\ell q_1 \cdots q_{2r}$ for pairwise distinct primes $q_i \equiv 3 \pmod 4$, $1 \leq i \leq 2r$, $r \geq 0$. Let d be a positive divisor of $(\ell^2-1)/2$. If the order of 2 in $\mathbb{F}_\ell^\times$ does not divide $N_d := (\ell-1)/\gcd(\ell-1,d)$, then $Y_d(\mathbb{Q}_2) = \emptyset$, although $X_D(\mathbb{Q}_2) \neq \emptyset$.*

Proof. By [JL85, Theorem 5.6], the set $X_D(\mathbb{Q}_2)$ is non-empty because every prime divisor of $D/2$ is congruent to 3 modulo 4. Hence, if we set $f := \mathrm{ord}_{\mathbb{F}_\ell^\times}(2)$, then we must show that $Y_d(\mathbb{Q}_2)$ is empty if f does not divide N_d.

From (7) and (9), the integer N_d is precisely the order of $N(H_d)$ in $\mathbb{F}_\ell^\times$, where $H_d \subseteq \mathbb{F}_{\ell^2}^\times$ is the unique subgroup of index d in $\mathbb{F}_{\ell^2}^\times$. From Remark 4.3, it is immediate that if f does not divide N_d then $f_d > 1$ (and conversely), hence the claim follows by applying Proposition 4.4. □

As an example, for each prime $\ell \equiv 3 \pmod 4$ with $7 \leq \ell \leq 23$, the positive divisors d of $(\ell^2-1)/2$ satisfying the conditions of the previous corollary are listed in Table 4.1. Therefore, for every pair (ℓ, d) in Table 4.1 we have $Y_d(\mathbb{Q}_2) = \emptyset$ and $X_D(\mathbb{Q}_2) \neq \emptyset$ for every D as in the statement of the corollary.

ℓ	$n = (\ell^2-1)/2$	positive divisors d of n with $f_d > 1$
7	24	3, 6, 12, 24
11	60	2, 4, 5, 6, 10, 12, 15, 20, 30, 60
19	180	2, 3, 4, 6, 9, 10, 12, 15, 18, 20, 30, 36, 45, 60, 90, 180
23	264	11, 22, 33, 44, 66, 88, 132, 264

TABLE 1. Some examples of pairs (ℓ, d) for which $Y_d(\mathbb{Q}_2) = \emptyset$ but $X_D(\mathbb{Q}_2) \neq \emptyset$.

Henceforth, we focus on the case $f_d = 1$ (in particular, $k_d = 1$ as well). According to the p-adic uniformisation of the curves Y_d described above, studying the existence of K-rational points on Y_d for finite extensions K of $\mathbb{Q}_p$ amounts to studying the existence of K-rational points on the twisted Mumford curve $\mathcal{M}^\xi_{\Gamma_{d,+}}$. As we show below, this can be done very much in the same way as it is done in [JL85] for the Shimura curve X_D. The rest of this section is thus devoted to prove Theorem 1.1.

Under the assumption $f_d = 1$, from (22) and (23) we have an isomorphism of $\mathbb{Z}_p$-schemes

$$\mathcal{Y}_d \simeq \bigsqcup_{i=1}^{c_p(d)} \mathcal{Y}_{\Gamma_d},$$

where the curve $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is isomorphic to $\mathcal{M}^\xi_{\Gamma_{d,+}}/\mathbb{Z}_p$, the quadratic twist of the Mumford curve $\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p$ by the 1-cocycle

$$\xi : \mathrm{Gal}(\mathbb{Q}_{p^2}/\mathbb{Q}_p) \longrightarrow \mathrm{Aut}(\mathcal{M}_{\Gamma_{d,+}} \times \mathbb{Z}_{p^2}/\mathbb{Z}_{p^2}), \quad \mathrm{Fr}_p \longmapsto w_p \times \mathrm{id}.$$

In particular, $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is an *admissible curve* in the sense of [JL85, Definition 3.1], and its special fibre is therefore described by a graph with lengths (its *dual graph*). If $K/\mathbb{Q}_p$ is a finite extension, with ring of integers $\mathcal{O}_K$ and residue field $\mathbb{F}_K$, by virtue of Hensel's Lemma there exists a K-rational point on Y_d if and only if the special fibre of a regular model of $\mathcal{Y}_{\Gamma_d} \times_{\mathbb{Z}_p} \mathcal{O}_K$ contains a smooth $\mathbb{F}_K$-rational point. The latter problem can be tackled by studying the combinatorics of the dual graph of $\mathcal{Y}_{\Gamma_d}$.

Let us recall briefly some basic facts about admissible curves over $\mathbb{Z}_p$, following [JL85, Section 3]. If $\mathcal{X}/\mathbb{Z}_p$ is an admissible curve over $\mathbb{Z}_p$, then its dual graph with lengths will be denoted by $\mathcal{G}(\mathcal{X}/\mathbb{Z}_p)$, and $F(\mathcal{X}/\mathbb{Z}_p)$ will stand for the automorphism of $\mathcal{G}(\mathcal{X}/\mathbb{Z}_p)$ induced by the Frobenius automorphism $\mathcal{X}_0 \times_{\mathbb{F}_p} \bar{\mathbb{F}}_p \to \mathcal{X}_0 \times_{\mathbb{F}_p} \bar{\mathbb{F}}_p$, where $\mathcal{X}_0 := \mathcal{X} \times_{\mathbb{Z}_p} \mathbb{F}_p$ is the special fibre of $\mathcal{X}$. The curve $\mathcal{X}_{\mathcal{O}_K} := \mathcal{X} \times_{\mathbb{Z}_p} \mathcal{O}_K$ is again admissible, and if we set $f_K := f(K/\mathbb{Q}_p)$ and $e_K := e(K/\mathbb{Q}_p)$, then

$$(\mathcal{G}(\mathcal{X}_{\mathcal{O}_K}/\mathcal{O}_K), F(\mathcal{X}_{\mathcal{O}_K}/\mathcal{O}_K)) \simeq (\mathcal{G}(\mathcal{X}/\mathbb{Z}_p)^{e_K}, F(\mathcal{X}/\mathbb{Z}_p)^{f_K}),$$

where for a finite graph $\mathcal{G}$ and an integer $e \geq 1$, $\mathcal{G}^e$ is the graph obtained by considering the same underlying graph as $\mathcal{G}$ but whose length function $\ell_{\mathcal{G}^e} : \mathrm{Ed}(\mathcal{G}^e) \to \mathrm{Ed}(\mathcal{G}^e)$ is defined by setting $\ell_{\mathcal{G}^e}(y) = e\ell_{\mathcal{G}}(y)$ for every $y \in \mathrm{Ed}(\mathcal{G}^e) = \mathrm{Ed}(\mathcal{G})$. Further, if $\widetilde{\mathcal{X}}_{\mathcal{O}_K}$ denotes a regular model of $\mathcal{X}_{\mathcal{O}_K}$, obtained by resolution of singularities, then

$$(\mathcal{G}(\widetilde{\mathcal{X}}_{\mathcal{O}_K}/\mathcal{O}_K), F(\widetilde{\mathcal{X}}_{\mathcal{O}_K}/\mathcal{O}_K)) \simeq (\widetilde{\mathcal{G}}(\mathcal{X}_{\mathcal{O}_K}/\mathcal{O}_K), \widetilde{F}(\mathcal{X}_{\mathcal{O}_K}/\mathcal{O}_K)),$$

where now for a finite graph $\mathcal{G}$, the graph $\widetilde{\mathcal{G}}$ is obtained from $\mathcal{G}$ by replacing every edge y of non-trivial length in $\mathcal{G}$ such that $\bar{y} \neq y$ by a chain of $\ell_{\mathcal{G}}(y)$ edges, and for an automorphism F of $\mathcal{G}$, we write $\widetilde{F}$ for the automorphism induced by F on $\widetilde{\mathcal{G}}$. Finally, twists of admissible curves are again admissible curves, and the effect of twisting an admissible curve on its dual graph is described in [JL85, Proposition 3.7].

The goal of Section 4.2 below is to determine and describe the dual graph $\mathcal{G}(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p)$ of the admissible curve $\mathcal{Y}_{\Gamma_d}$. Then in Section 4.3 we conclude with a proof of Theorem 1.1 by translating the existence of a smooth $\mathbb{F}_K$-rational point on the special fibre of a regular model of $\mathcal{Y}_{\Gamma_d} \times_{\mathbb{Z}_p} \mathcal{O}_K$ into a combinatorial condition on $\mathcal{G}(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p)$.

4.2. **Combinatorics of the dual graphs.** As above, we fix a positive divisor d of $(\ell^2-1)/2$ and the corresponding intermediate curve Y_d of the Shimura covering $X_{D,\ell} \to X_D$. Let U_d be the intermediate subgroup $\mathcal{U}_D \subseteq U_d \subseteq \widehat{\mathcal{O}}^\times$ defining the Shimura curve Y_d (with the convention that $-1 \in U_d$). When describing the p-adic uniformisation of Y_d, recall that we regard $\Gamma_d = U_d^{(p)} \cap B_{D/p}^\times$ as a subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$ through a fixed embedding $B_{D/p} \hookrightarrow B_{D/p,p} \simeq \mathrm{M}_2(\mathbb{Q}_p)$. We also defined the index two subgroup

$$\Gamma_{d,+} = \{\gamma \in \Gamma_d : \mathrm{val}_p(\mathrm{n}(\gamma)) \in 2\mathbb{Z}\} \subseteq \Gamma_d,$$

so that the non-trivial class in $W_d := \Gamma_d/\Gamma_{d,+}$ is represented by an element $w_p \in \Gamma_d$ with $\mathrm{val}_p(\mathrm{n}(w_p)) = 1$. If $\mathcal{T}_p$ denotes the Bruhat-Tits tree associated with $\mathrm{GL}_2(\mathbb{Q}_p)$, then the quotients

$$\mathcal{G}_d := \Gamma_d \setminus \mathcal{T}_p, \quad \mathcal{G}_{d,+} := \Gamma_{d,+} \setminus \mathcal{T}_p$$

are naturally finite graphs with lengths. Since the action of $Z(\mathrm{GL}_2(\mathbb{Q}_p)) = \mathbb{Q}_p^\times$ is trivial on $\mathcal{T}_p$, we can replace the groups Γ_d and $\Gamma_{d,+}$ by their images Γ'_d and $\Gamma'_{d,+}$ in $\mathrm{PGL}_2(\mathbb{Q}_p)$, respectively.

Observe that taking $d = 1$ we have $Y_1 = X_D$. In this case, $\Gamma_1 = \widehat{\mathcal{O}}_D^{(p)\times} =: \Gamma_D$ and the finite graphs with lengths $\mathcal{G}_D := \mathcal{G}_1$, $\mathcal{G}_{D,+} := \mathcal{G}_{1,+}$ are described in detail in [Kur79]. Let us write $\ell_D := \ell_1$ for the length function on $\mathcal{G}_D$ and $\mathcal{G}_{D,+}$. Since we will describe the finite graph with lengths $\mathcal{G}_d$ from $\mathcal{G}_D$, and then we will obtain a description of $\mathcal{G}_{d,+}$ from $\mathcal{G}_d$ in an analogous way as $\mathcal{G}_{D,+}$ is described from $\mathcal{G}_D$, let us start by recalling briefly the description of $\mathcal{G}_D$ (see *ibid.* for further details).

The set of vertices of $\mathcal{T}_p$ is by definition

$$\mathrm{Ver}(\mathcal{T}_p) = \mathrm{PGL}_2(\mathbb{Q}_p)/\mathrm{PGL}_2(\mathbb{Z}_p) \simeq B_{D/p,p}^\times/\mathbb{Q}_p^\times \mathcal{O}_{D/p,p}^\times,$$

and it is in bijection with the set of maximal orders $\mathcal{O}$ in $B_{D/p}$ which are locally equal to $\mathcal{O}_{D/p}$ at every prime $q \neq p$. If $\tilde{v} \in \mathrm{Ver}(\mathcal{T}_p)$ is represented by $g \in B_{D/p,p}^\times \simeq \mathrm{GL}_2(\mathbb{Q}_p)$, then the maximal order $\mathcal{O}_{\tilde{v}}$ corresponding to $\tilde{v}$ is the unique maximal order such that $\mathcal{O}_{\tilde{v},q} = \mathcal{O}_{D/p,q} = \mathcal{O}_{D/p} \otimes_{\mathbb{Z}} \mathbb{Z}_q$ for every finite prime q and $\mathcal{O}_{\tilde{v},p} = g\mathcal{O}_{D/p,p}g^{-1}$. The set of vertices $\mathrm{Ver}(\mathcal{G}_D)$ is then $\Gamma_D \setminus \mathrm{Ver}(\mathcal{T}_p)$, where Γ_D acts naturally on $\mathrm{Ver}(\mathcal{T}_p)$ by conjugation using the above description in terms of maximal orders.

The cardinality of $\mathrm{Ver}(\mathcal{G}_D)$ is $h := h(B_{D/p})$, the class number of $B_{D/p}$; write $\mathrm{Ver}(\mathcal{G}_D) = \{v_1, \dots, v_h\}$, and choose maximal orders $\mathcal{O}_i := \mathcal{O}_{\tilde{v}_i}$ corresponding to vertices $\tilde{v}_i$ in $\mathcal{T}_p$ above v_i, for each $i = 1, \dots, h$. The length $\ell_D(v_i)$ of v_i is defined to be the cardinality of $\mathrm{Stab}_{\Gamma'_D}(\tilde{v}_i) = \mathcal{O}_i^\times/\mathbb{Z}^\times$. Unless $D/p = 2$ or 3, it follows that $\ell_D(v_i) = 1$, 2, or 3. Further, deciding the number h_j of vertices in $\mathcal{G}_D$ of length j, for $j = 1, 2, 3$, amounts to computing the number of optimal embeddings of $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[(1+\sqrt{-3})/2]$ into the orders $\mathcal{O}_1, \cdots, \mathcal{O}_h$. By using Eichler's embedding theorems, it turns out (see [Kur79, p. 291]) that

$$h_2 = \frac{1}{2}\prod_{q|D/p}\left(1 - \left(\frac{-4}{q}\right)\right), \quad h_3 = \frac{1}{2}\prod_{q|D/p}\left(1 - \left(\frac{-3}{q}\right)\right), \quad h_1 = h - h_2 - h_3. \tag{24}$$

Similarly as for vertices, the length $\ell_D(y)$ of an edge $y \in \mathrm{Ed}(\mathcal{G}_D)$ is by definition the cardinality of $\mathrm{Stab}_{\Gamma'_D}(\tilde{y})$, where now $\tilde{y}$ is any edge in $\mathcal{T}_p$ above y. If $v = o(y)$ is the origin of the edge y and we choose lifts $\tilde{y}$ and $\tilde{v} = o(\tilde{y})$ in $\mathcal{T}_p$ of y and v, respectively, then $\mathrm{Stab}_{\Gamma'_D}(\tilde{y})$ is clearly a subgroup of $\mathrm{Stab}_{\Gamma'_D}(\tilde{v})$, thus $\ell_D(y)$ divides $\ell_D(v)$. Further, fixed $v \in \mathrm{Ver}(\mathcal{G}_D)$, the number of edges emanating from v having a given length is easily computed following the table in [Kur79, Proposition 4.2].

In order to describe the graph $\mathcal{G}_d$ from $\mathcal{G}_D$, recall from Lemma 4.1 that Γ_d is naturally a normal subgroup of Γ_D. Furthermore, under our assumption that $f_d = k_d = 1$, we have $p \in U_{d,\ell}$, so that $\Gamma_d = \Gamma_D \cap U_{d,\ell}$ contains $\Gamma_D \cap Z(\mathrm{GL}_2(\mathbb{Q}_p)) = \mathbb{Z}[1/p]^\times$, hence $\Gamma_d \cap Z(\mathrm{GL}_2(\mathbb{Q}_p)) = \mathbb{Z}[1/p]^\times$ as well. As a consequence, since both $\mathbb{Z}[1/p]^\times$ and Γ_d are normal in Γ_D we have

$$\Gamma'_D/\Gamma'_d = (\Gamma_D/\mathbb{Z}[1/p]^\times)/(\Gamma_d/\mathbb{Z}[1/p]^\times) \simeq \Gamma_D/\Gamma_d.$$

This implies that $d_{\mathcal{G}} := [\Gamma_D : \Gamma_d]$ is the degree of the natural projection map $\pi_d : \mathcal{G}_d \to \mathcal{G}_D$ (which is also the degree of $\pi_{d,+} : \mathcal{G}_{d,+} \to \mathcal{G}_{D,+}$). By Lemma 4.1, $d_{\mathcal{G}} c_p(d) = d$.

However, let us remark that the natural maps π_d and $\pi_{d,+}$ might not preserve in general the lengths of vertices and edges. Indeed, let $\tilde{x}$ be either a vertex or an edge in $\mathcal{T}_p$ as before, and let x (resp. x_+) be its image in $\mathcal{G}_d$ (resp. $\mathcal{G}_{d,+}$). Then the length of x (resp. of x_+) is defined to be

$$\ell_d(x) := |\mathrm{Stab}_{\Gamma'_d}(\tilde{x})| \qquad (\text{resp. } \ell_{d,+}(x_+) := |\mathrm{Stab}_{\Gamma'_{d,+}}(\tilde{x})|).$$

It is easily seen that this definition does not depend on the representative $\tilde{x}$ in $\mathcal{T}_p$. Focusing first on the description of $\mathcal{G}_d$, we start by observing that the lengths $\ell_d(x) = |\operatorname{Stab}_{\Gamma'_d}(\tilde{x})|$ and $\ell_D(\pi_d(x)) = |\operatorname{Stab}_{\Gamma'_D}(\tilde{x})|$ are related by

$$\ell_D(\pi_d(x)) = |\operatorname{Stab}_{\Gamma'_D/\Gamma'_d}(\tilde{x})|\ell_d(x) = \frac{|\operatorname{Stab}_{\Gamma'_D}(\tilde{x})|}{|\operatorname{Stab}_{\Gamma'_D}(\tilde{x}) \cap \Gamma'_d|}\ell_d(x).$$

Under our assumption $\ell > 3$, $\ell_D(\pi_d(x)) = |\operatorname{Stab}_{\Gamma'_D}(\tilde{x})|$ is either 1, 2, or 3, hence

$$\ell_d(x) = \begin{cases} \ell_D(\pi_d(x)) & \text{if } \operatorname{Stab}_{\Gamma'_D}(\tilde{x}) \subseteq \Gamma'_d, \\ 1 & \text{if } \operatorname{Stab}_{\Gamma'_D}(\tilde{x}) \cap \Gamma'_d = \{1\}. \end{cases} \tag{25}$$

Lemma 4.7. *Let $\tilde{v}$ be a vertex in $\mathcal{T}_p$, and write v for its image in $\mathcal{G}_d$.*

a) *If $\ell_D(\pi_d(v)) = 1$, then $\ell_d(v) = 1$.*
b) *If $\ell_D(\pi_d(v)) = 2$, then $\ell_d(v) = 2$ if and only if $4 \mid t_d$. Otherwise, $\ell_d(v) = 1$.*
c) *If $\ell_D(\pi_d(v)) = 3$, then $\ell_d(v) = 3$ if and only if $6 \mid t_d$. Otherwise, $\ell_d(v) = 1$.*

Proof. The statement in a) is clear, since $\ell_D(\pi_d(v))$ is divisible by $\ell_d(v)$. By (25), in order to prove b) and c) we shall determine when $\operatorname{Stab}_{\Gamma'_D}(\tilde{v}) \subseteq \Gamma'_d$. Equivalently, we shall determine when $\operatorname{Stab}_{\Gamma_D}(\tilde{v}) \subseteq \Gamma_d$. If $\mathcal{O}_{\tilde{v}}$ denotes the maximal order corresponding to $\tilde{v}$, by using the monomorphism ν from (19) this inclusion holds if and only if $\nu(\mathcal{O}_{\tilde{v}}^\times)$ is a subgroup of $U_{d,\ell}$. Now the isomorphism $\psi : (1+I_\ell) \setminus \mathcal{O}_{D/p,\ell}^\times \to \mathbb{F}_{\ell^2}^\times$ induces an isomorphism $U_{d,\ell} \setminus \mathcal{O}_{D/p,\ell}^\times \simeq \mathbb{F}_{\ell^2}^\times / H_d$, so that $\nu(\mathcal{O}_{\tilde{v}}^\times)$ is a subgroup of $U_{d,\ell}$ if and only if

$$\psi((1 + I_\ell)\nu(\mathcal{O}_{\tilde{v}}^\times))$$

is a subgroup of H_d.

Assume that $\ell_D(\pi_d(v)) = 2$, so that $\operatorname{Stab}_{\Gamma_D}(\tilde{v}) = \mathcal{O}_{\tilde{v}}^\times = \{\pm 1, \pm i\}$, where $i \in \mathcal{O}_{\tilde{v}}^\times$ satisfies $i^2 + 1 = 0$. By the above discussion we have $\ell_d(v) = 2$ if and only if $\psi((1 + I_\ell)\nu(i)) \in H_d$. First of all, observe that $\nu(i) \notin 1 + I_\ell$, because $\mathrm{n}(\nu(i) - 1) = 2 \notin \ell\mathbb{Z}$. And also notice that $\nu(i)^2 = -1 \notin 1 + I_\ell$, again because ℓ is odd. In other words, the image of $\nu(i)$ in $(1 + I_\ell) \setminus \mathcal{O}_{D/p,\ell}^\times$ has order 4, hence also $\psi((1 + I_\ell)\nu(i))$ has order 4. Being $\mathbb{F}_{\ell^2}^\times$ cyclic, it follows that $\psi((1 + I_\ell)\nu(i)) \in H_d$ if and only if 4 divides t_d, the order of H_d. This proves b).

If $\ell_D(\pi_d(v)) = 3$, then $\operatorname{Stab}_{\Gamma_D}(\tilde{v}) = \mathcal{O}_{\tilde{v}}^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$, where $\omega \in \mathcal{O}_{\tilde{v}}^\times$ satisfies $\omega^2 + \omega + 1 = 0$, and we can proceed similarly as before. Since $\ell > 3$ and $\mathrm{n}(\nu(\omega) - 1) = \mathrm{n}(\nu(\omega^2) - 1) = 3$, we see that neither $\nu(\omega)$ nor $\nu(\omega^2)$ belong to $1 + I_\ell \subseteq \mathcal{O}_{D/p,\ell}^\times$. Moreover, $\omega^3 = -1$, so that we also have $\nu(\omega^3) \notin 1 + I_\ell$. Therefore, the image of $\nu(\omega)$ in $(1 + I_\ell) \setminus \mathcal{O}_{D/p,\ell}^\times$ must still have order 6, thus also the order of $\psi((1 + I_\ell)\nu(\omega))$ in $\mathbb{F}_{\ell^2}^\times$ is 6. Again, H_d is the unique (cyclic) subgroup of order t_d in $\mathbb{F}_{\ell^2}^\times$, thus we conclude that $\psi((1 + I_\ell)\nu(\omega)) \in H_d$ if and only if 6 divides t_d. This proves c). ☐

From this lemma, we can determine how many vertices of given length are in $\mathcal{G}_d$. Indeed, let v_0 be a vertex in $\mathcal{G}_D$, and let $\pi_d^{-1}(v_0) \subseteq \operatorname{Ver}(\mathcal{G}_d)$ be the set of vertices of $\mathcal{G}_d$ above v_0. If $\ell_D(v_0) = 1$, then it is clear that $\pi_d^{-1}(v_0)$ consists of $d_{\mathcal{G}}$ vertices of length 1. Besides, if $\ell_D(v_0) = 2$ (resp. 3), then $\pi_d^{-1}(v_0)$ consists of $d_{\mathcal{G}}$ vertices of length 2 (resp. 3) if $4 \mid t_d$ (resp. $6 \mid t_d$), and $d_{\mathcal{G}}/2$ (resp. $d_{\mathcal{G}}/3$) vertices of length 1 otherwise. If for positive integers r, s, we set

$$\phi_r(s) = \begin{cases} 1 & \text{if } r \mid s, \\ 0 & \text{if } r \nmid s, \end{cases} \quad \phi'_r(s) = 1 - \phi_r(s) = \begin{cases} 0 & \text{if } r \mid s, \\ 1 & \text{if } r \nmid s, \end{cases}$$

then we can summarise the above computations as follows:

Corollary 4.8. *Let h_i denote the number of vertices in $\mathcal{G}_D$ of length i, $i = 1, 2, 3$, as in (24). If $h_{d,i}$ denotes the number of vertices in $\mathcal{G}_d$ of length i, $i = 1, 2, 3$, then*

$$h_{d,2} = \phi_4(t_d)d_{\mathcal{G}}h_2, \quad h_{d,3} = \phi_6(t_d)d_{\mathcal{G}}h_3, \quad h_{d,1} = d_{\mathcal{G}}(h_1 + \frac{\phi'_4(t_d)h_2}{2} + \frac{\phi'_6(t_d)h_3}{3}),$$

and therefore the total number of vertices in $\mathcal{G}_d$ is computed as $h_d = h_{d,1} + h_{d,2} + h_{d,3}$.

Corollary 4.9. *With the above notations:*

a) *There is a vertex of length 2 in $\mathcal{G}_d$ if and only if $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and $4 \mid t_d$.*
b) *There is a vertex of length 3 in $\mathcal{G}_d$ if and only if $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and $6 \mid t_d$.*

We can also compute the lengths of the edges in $\mathcal{G}_d$. Fix a vertex v in $\mathcal{G}_d$, and let $\tilde{v}$ be a vertex of $\mathcal{T}_p$ above v. Then let $\mathrm{Star}(v)$ be the set of edges y of $\mathcal{G}_d$ with $o(y) = v$ and, similarly, let also $\mathrm{Star}(\tilde{v})$ be the set of edges $\tilde{y}$ of $\mathcal{T}_p$ with $o(\tilde{y}) = \tilde{v}$. Recall that $|\mathrm{Star}(\tilde{v})| = p+1$. There is a natural map $\mathrm{Star}(\tilde{v}) \to \mathrm{Star}(v)$, and $\ell_d(y)$ divides $\ell_d(v)$ for every $y \in \mathrm{Star}(v)$. Furthermore,

$$p + 1 = \sum_{y\in\mathrm{Star}(v)} \frac{\ell_d(v)}{\ell_d(y)}.$$

From this relation, it is clear that $\ell_d(y) = 1$ for every $y \in \mathrm{Star}(v)$ if $\ell_d(v) = 1$. Besides, if $\ell_d(v) = 2$ or 3, then the above equality can be rewritten as

$$p + 1 = \ell_d(v)|\{y \in \mathrm{Star}(v) : \ell_d(y) = 1\}| + |\{y \in \mathrm{Star}(v) : \ell_d(y) = \ell_d(v)\}|,$$

so that it is enough to determine how many edges of length $\ell_d(v)$ are in $\mathrm{Star}(v)$ to describe $\mathrm{Star}(v)$ completely. But this is the same local problem as in [Kur79, p. 292], thus we deduce the following:

Proposition 4.10. *Given a vertex v in $\mathcal{G}_d$, its length $\ell_d(v) \in \{1, 2, 3\}$ can be computed by Lemma 4.7 and, according to the value of $\ell_d(v)$, the integers*

$$s_k(v) := |\{y \in \mathrm{Star}(v) : \ell_d(y) = k\}|, \quad k = 1, 2, 3,$$

can be obtained from the following table, where $(\frac{-4}{\cdot})$ and $(\frac{-3}{\cdot})$ denote the Kronecker symbol:

	$s_1(v)$	$s_2(v)$	$s_3(v)$
$\ell_d(v) = 1$	$p + 1$	0	0
$\ell_d(v) = 2$	$\frac{1}{2}(p - (\frac{-4}{p}))$	$1 + (\frac{-4}{p})$	0
$\ell_d(v) = 3$	$\frac{1}{3}(p - (\frac{-3}{p}))$	0	$1 + (\frac{-3}{p})$

We notice that the above table is the same as in [Kur79, Proposition 4.2], with the rows corresponding to $D/p = 2$ and 3 removed, as we have assumed $\ell > 3$. This proposition, together with Lemma 4.7 and Corollary 4.8 gives a precise description of the combinatorics of $\mathcal{G}_d$.

Corollary 4.11. *With the above notations:*

a) *There is an edge of length 2 in $\mathcal{G}_d$ if and only if $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$, $4 \mid t_d$ and $p \not\equiv 3 \pmod 4$.*
b) *There is an edge of length 3 in $\mathcal{G}_d$ if and only if $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$, $6 \mid t_d$ and $p \not\equiv 2 \pmod 3$.*

Now we describe the graph $\mathcal{G}_{d,+}$ by using the natural map $\mathcal{G}_{d,+} \to \mathcal{G}_d$, in the same way as it is done in [Kur79, Section 4] for $\mathcal{G}_{D,+}$ and $\mathcal{G}_D$. Namely, start by writing the set of vertices $\mathrm{Ver}(\mathcal{T}_p)$ of the Bruhat-Tits tree as $\mathrm{Ver}(\mathcal{T}_p) = V_1 \sqcup V_2$, in such a way that for every pair of vertices $\tilde{v}_i \in V_i$, $\tilde{v}_j \in V_j$, the distance between $\tilde{v}_i$ and $\tilde{v}_j$ is even if and only if $i = j$. Then, observe that $\Gamma_{d,+}V_i = V_i$ for $i = 1, 2$, whereas $\gamma V_1 = V_2$ and $\gamma V_2 = V_1$ for every $\gamma \in \Gamma_d - \Gamma_{d,+}$. Equivalently, this can be reformulated by saying that $\Gamma_{d,+}V_i = V_i$ for $i = 1, 2$ and $w_pV_1 = V_2$, $w_pV_2 = V_1$.

Therefore, every fibre of the natural maps

$$\mathrm{Ver}(\mathcal{G}_{d,+}) \to \mathrm{Ver}(\mathcal{G}_d) \quad \text{and} \quad \mathrm{Ed}(\mathcal{G}_{d,+}) \to \mathrm{Ed}(\mathcal{G}_d)$$

consists of two elements, and by construction we find the following:

Proposition 4.12. *There exists no edge $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$ such that $\bar{y} = y$. In particular,*

$$(\mathcal{G}(\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p), F(\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p)) \simeq (\mathcal{G}_{d,+}, \mathrm{id}),$$

that is, $\mathcal{G}_{d,+}$ is the dual graph of the Mumford curve $\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p$. Further, the dual graph of $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is the same graph with lengths $\mathcal{G}_{d,+}$, but with Frobenius action given by w_p. That is to say,

$$(\mathcal{G}(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p), F(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p)) \simeq (\mathcal{G}_{d,+}, w_p).$$

Proof. The non-existence of edges $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$ such that $y = \bar{y}$ follows directly from the above construction of $\mathcal{G}_{d,+}$. This implies that $(\mathcal{G}_{d,+})^* = \mathcal{G}_{d,+}$, and therefore the isomorphism of pairs

$$(\mathcal{G}(\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p), F(\mathcal{M}_{\Gamma_{d,+}}/\mathbb{Z}_p)) \simeq (\mathcal{G}_{d,+}, \mathrm{id}),$$

is consequence of [Kur79, Proposition 3.2]. Finally, by applying [JL85, Proposition 3.7] we obtain that

$$(\mathcal{G}(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p), F(\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p)) \simeq (\mathcal{G}_{d,+}, w_p).$$

□

Also, since w_p does not fix vertices or edges, it follows that the length of a vertex or an edge in $\mathcal{G}_{d,+}$ is the same as the length of its image in $\mathcal{G}_d$. In view of this, we will also write ℓ_d for the length function on $\mathcal{G}_{d,+}$. It will be clear from the context whether we use ℓ_d as the length function on $\mathcal{G}_{d,+}$ or on $\mathcal{G}_d$. In particular:

Lemma 4.13. *The number of vertices of length i in $\mathcal{G}_{d,+}$, for $i = 1, 2, 3$, is $2h_{d,i}$, where the integers $h_{d,i}$ are as in Corollary 4.8. Further, if $v \in \mathrm{Ver}(\mathcal{G}_{d,+})$ is such that $\ell_d(v) = k$, $k \in \{1, 2, 3\}$, then the number of edges in* $\mathrm{Star}(v)$ *of length k is $s_k(v)$, where $s_k(v)$ is as in Proposition 4.10.*

On the other hand, there may exist edges y in $\mathcal{G}_d$ such that $\bar{y} = y$. Observe that such an edge exists if and only if there is an edge y' in $\mathcal{G}_{d,+}$ with $w_p(y') = \overline{y'}$. Let us define a set of quadratic equations depending on p and d in the following way:

$$\mathcal{F}_{p,d} := \begin{cases} \{x^2+2=0, x^2+2x+2=0, x^2-2x+2=0\} & \text{if } p=2 \text{ and } 4 \mid t_d, \\ \{x^2+3=0, x^2+3x+3=0, x^2-3x+3=0\} & \text{if } p=3 \text{ and } 6 \mid t_d, \\ \{x^2+p=0\} & \text{otherwise.} \end{cases} \tag{26}$$

Lemma 4.14. *There exists an edge $y \in \mathrm{Ed}(\mathcal{G}_d)$ such that $\bar{y} = y$ if and only if Γ_d contains a root of some equation in $\mathcal{F}_{p,d}$.*

Proof. Assume there exists an edge $y \in \mathrm{Ed}(\mathcal{G}_d)$ such that $\bar{y} = y$. Write $v = o(y)$, and let $\tilde{v} \in \mathrm{Ver}(\mathcal{T}_p)$ be a vertex above v. Let also $\tilde{y} \in \mathrm{Star}(\tilde{v})$ be an edge above y. Then there exists $\gamma \in \Gamma_d$ such that $\gamma(\tilde{y}) = \bar{\tilde{y}}$. In particular, $\gamma^2 \in \mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Q}_p)}(\tilde{v}) = \mathbb{Q}_p^\times \mathcal{O}_{\tilde{v},p}^\times$, so that we can write $\gamma^2 = p^n u$, for some $n \in \mathbb{Z}$ and $u \in \mathcal{O}_{\tilde{v},p}^\times$. Further, observe that $\mathrm{val}_p(\mathrm{n}(\gamma))$ must be odd, because the distance between $\tilde{v}$ and $\gamma(\tilde{v})$ is odd, hence n is odd. If $n = 2b+1$, we can replace $p^{-b}\gamma$ by γ (because $p \in \Gamma_d$), thus we have $\gamma^2 = pu$, where $u \in \mathcal{O}_{\tilde{v}}^\times \cap U_{d,\ell}$ (locally at ℓ, $u \in U_{d,\ell}$ because both p and γ lie in Γ_d). Moreover, we have $\gamma \in \mathcal{O}_{\tilde{v}}$. Now, since u is a unit in $\mathcal{O}_{\tilde{v}}$, we have the following possibilities:

i) $u = \pm 1$,
ii) $u^2 + 1 = 0$, or
iii) $u^2 \pm u + 1 = 0$.

As in [Kur79, p.295], the cases $u = 1$ and $u^2+u+1 = 0$ cannot occur. Furthermore, since (locally at ℓ) u must lie in $U_{d,\ell}$, the case $u^2+1 = 0$ (resp. $u^2-u+1 = 0$) can only occur if $4 \mid t_d$ (resp. $6 \mid t_d$). Therefore, again proceeding as in *ibid.*, the above three cases are translated, respectively, into the following three options:

I) γ is a root of $x^2 + p = 0$,
II) $p = 2$, $4 \mid t_d$ and γ is a root of $x^2 \pm 2x + 2 = 0$, or
III) $p = 3$, $6 \mid t_d$ and γ is a root of $x^2 \pm 3x + 3 = 0$.

Thus γ is a root in Γ_d of some equation in $\mathcal{F}_{p,d}$.

Conversely, if $\gamma \in \Gamma_d$ is a root of some equation in $\mathcal{F}_{p,d}$, then either condition I), II) or III) holds. In particular, choosing a vertex $\tilde{v}$ of $\mathcal{T}_p$ such that $\gamma \in \mathcal{O}_{\tilde{v}}$, then clearly there is some edge $\tilde{y} \in \mathrm{Star}(\tilde{v})$ such that $\gamma(\tilde{y}) = \bar{\tilde{y}}$, hence the image y of $\tilde{y}$ in $\mathcal{G}_d$ satisfies $\bar{y} = y$. □

For $d = 1$, so that $Y_1 = X_D$, $\Gamma_1 = \mathcal{O}_{D/p}^{(p)\times}$ and $\mathcal{G}_1 = \mathcal{G}_D$, conditions $4 \mid t_d$ and $6 \mid t_d$ are obviously satisfied, since $t_d = (\ell^2-1)/2$. Thus the above lemma is just the computation in [Kur79, p. 295]. By examining the equations in $\mathcal{F}_p := \mathcal{F}_{p,1}$, there is an edge $y \in \mathrm{Ed}(\mathcal{G}_D)$ such that $\bar{y} = y$ if and only if one of the following conditions holds:

i) $p = 2$ and either $\mathbb{Q}(\sqrt{-2})$ or $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$,
ii) $p > 2$ and $\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$.

This is equivalent to saying that a quadratic order containing the roots of some equation in $\mathcal{F}_p$ embeds into some maximal order in $B_{D/p}$, and more precisely the number of edges $y \in \mathrm{Ed}(\mathcal{G}_D)$ such that $\bar{y} = y$ can be computed by counting the number of inequivalent optimal embeddings from such quadratic orders into the maximal orders $\mathcal{O}_1, \dots, \mathcal{O}_h$ (cf. *loc. cit.*).

Plainly, if Γ_d contains a root of some equation in $\mathcal{F}_{p,d}$, then $\Gamma_{d'}$ contains a root of some equation in $\mathcal{F}_{p,d'}$ for every $d' \mid d$. In terms of dual graphs, if $\mathcal{G}_d$ has an edge y satisfying $\bar{y} = y$, then its image y' in $\mathcal{G}_{d'}$ also verifies $\bar{y}' = y'$. In particular, if Γ_d contains a root of some equation in $\mathcal{F}_{p,d}$, then $\mathcal{O}_{D/p}^{(p)\times}$ contains a root of some equation in $\mathcal{F}_p = \mathcal{F}_{p,1}$.

In view of this, we shall study the existence of solutions in Γ_d of the quadratic equations in the set $\mathcal{F}_{p,d}$ assuming the existence of such solutions in $\mathcal{O}_{D/p}^{(p)\times}$. We carry out the details case by case in the next lemmas, where we make use of the natural morphism

$$\mathcal{O}_{D/p}^{(p)\times} \hookrightarrow \mathcal{O}_{D/p,\ell}^\times \longrightarrow (1+I_\ell) \setminus \mathcal{O}_{D/p,\ell}^\times \stackrel{\psi}{\longrightarrow} \mathbb{F}_{\ell^2}^\times$$

induced by ψ. If $\gamma \in \mathcal{O}_{D/p}^{(p)\times}$ is an arbitrary element, we write $\psi(\gamma)$ for its image in $\mathbb{F}_{\ell^2}^\times$ under the above composition. In particular, notice that $\gamma \in \Gamma_d$ if and only if $\psi(\gamma) \in H_d$.

Lemma 4.15. *Assume that $\mathcal{O}_{D/p}^{(p)\times}$ has a root of x^2+p. Then Γ_d has a root of x^2+p if and only if $4 \mid t_d$.*

Proof. Let $\tau, -\tau \in \mathbb{F}_{\ell^2}^\times$ be the two roots of x^2+p in $\mathbb{F}_{\ell^2}^\times$. If $\gamma \in \mathcal{O}_{D/p}^{(p)\times}$ is a root of x^2+p, then either $\psi(\gamma)=\tau$ or $\psi(\gamma)=-\tau$, and since $-1 \in H_d$, we deduce that $\gamma \in \Gamma_d$ if and only if $\tau \in H_d$. Observe that this condition does not depend on the choice of γ, hence assuming $\mathcal{O}_{D/p}^{(p)\times}$ has a root of x^2+p, we deduce that Γ_d has a root of x^2+p if and only if $\tau \in H_d$. Thus we shall prove that $-p$ is a square in H_d if and only if $4 \mid t_d$.

Indeed, under our running assumption $f_d = 1$, we have $p \mod \ell \in N(H_d)$, thus there exists an element $a \in H_d$ such that $a^{\ell+1} = p$ and being ℓ odd it follows that p is a square in H_d. We deduce that $-p$ is a square in H_d if and only if so is -1, and this is equivalent to saying that 4 divides $t_d = |H_d|$. □

Next we consider the quadratic polynomials $F_p^{\pm}(x) := x^2 \pm px + p$ when p is either 2 or 3.

Lemma 4.16. *Assume p is either 2 or 3, and suppose $\mathcal{O}_{D/p}^{(p)\times}$ has a root of either $F_p^+(x)$ or $F_p^-(x)$. Then Γ_d has a root of either $F_p^+(x)$ or $F_p^-(x)$ if and only if H_d has a root of $F_p^+(x)$ (or, equivalently, of $F_p^-(x)$).*

Proof. Fix a root $\sigma_+ \in \mathbb{F}_{\ell^2}^\times$ of $F_p^+(x)$. Then the roots of $F_p^+(x)$ (resp. $F_p^-(x)$) in $\mathbb{F}_{\ell^2}^\times$ are σ_+ and $\sigma'_+ := -\sigma_+ - p$ (resp. $\sigma_- := -\sigma_+$ and $\sigma'_- := \sigma_+ + p$). With these notations, it is straightforward to check that the existence of a root $\gamma \in \mathcal{O}_{D/p}^{(p)\times}$ of either $F_p^+(x)$ or $F_p^-(x)$ implies that there are elements γ_+, γ'_+, γ_-, $\gamma'_- \in \mathcal{O}_{D/p}^{(p)\times}$ such that $\psi(\gamma_+) = \sigma_+$, $\psi(\gamma'_+) = \sigma'_+$, $\psi(\gamma_-) = \sigma_-$ and $\psi(\gamma_+) = \sigma'_-$ (for instance, if γ is a root of $F_p^+(x)$, then one can set $\gamma_+ := \gamma$, $\gamma'_+ := -\gamma - p$, $\gamma_- := -\gamma$ and $\gamma'_- := \gamma + p$).

Similarly as in the previous lemma, the fact that at least one of the roots σ_+, σ'_+, σ_- and σ'_- lies in H_d does not depend on the choice of γ. Therefore, assuming that $\mathcal{O}_{D/p}^{(p)\times}$ has a root of either $F_p^+(x)$ or $F_p^-(x)$, then Γ_d has a root of either $F_p^+(x)$ or $F_p^-(x)$ if and only if at least one of the roots σ_+, σ'_+, σ_- and σ'_- belongs to H_d. Using that $-1 \in H_d$, since $\sigma_- = -\sigma_+$ and $\sigma'_- = -\sigma'_+$, this is in turn equivalent to saying that either σ_+ or σ'_+ lies in H_d, and hence the statement follows. □

Corollary 4.17. *Assume $f_d = 1$ as before. Then Γ_d contains a root of some equation in the set $\mathcal{F}_{p,d}$ if and only if any of the following conditions holds:*

i) *$\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$ and $4 \mid t_d$,*
ii) *$p = 2$, $4 \mid t_d$, $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and H_d contains a root of $x^2+2x+2=0$, or*
iii) *$p = 3$, $6 \mid t_d$, $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and H_d contains a root of $x^2+3x+3=0$.*

4.3. **Proof of Theorem 1.1.** Finally, we can use now the description of the graphs $\mathcal{G}_d$ and $\mathcal{G}_{d,+}$ from the previous section to prove Theorem 1.1. Indeed, the curve $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is admissible, and by Proposition 4.12 its dual graph is the finite graph with lengths $\mathcal{G}_{d,+}$ with Frobenius action given by w_p. Let $K/\mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$, and write $f_K := f(K/\mathbb{Q}_p)$, $e_K := e(K/\mathbb{Q}_p)$. Write also $\mathcal{O}_K$ and $\mathbb{F}_K \simeq \mathbb{F}_{p^{f_K}}$ for its ring of integers and residue field, respectively. In order to study the existence of K-rational points on Y_d, we may look at the base change $\mathcal{Y}_{\Gamma_d,\mathcal{O}_K} := \mathcal{Y}_{\Gamma_d} \times_{\mathbb{Z}_p} \mathcal{O}_K$. By Hensel's Lemma, the set $Y_d(K)$ is not empty if and only if the special fibre of a regular model of $\mathcal{Y}_{\Gamma_d,\mathcal{O}_K}$ has a smooth $\mathbb{F}_K$-rational point. We can obtain such a regular model by resolving singularities, and by [JL85, Propositions 3.4, 3.6] the result is still an admissible curve over $\mathcal{O}_K$, whose dual graph is the finite graph with lengths $\widetilde{\mathcal{G}}_{d,+}^{e_K}$, with Frobenius action given by $w_p^{f_K}$. The existence of a smooth $\mathbb{F}_K$-rational point on the special fibre is then read out from this graph.

With these observations, the next statement accounts for item a) in Theorem 1.1:

Proposition 4.18. *If f_K is even, then $Y_d(K) \neq \emptyset$.*

Proof. If f_K is even, then $w_p^{f_K}$ is the identity on $\mathcal{G}_{d,+}$, thus it is also the identity on $\widetilde{\mathcal{G}}_{d,+}^{e_K}$. In particular, every vertex v in $\widetilde{\mathcal{G}}_{d,+}^{e_K}$ is fixed by $w_p^{f_K}$, hence every component of the special fibre of $\widetilde{\mathcal{Y}}_{\Gamma_d,\mathcal{O}_K}$ is rational over $\mathbb{F}_K$. Since there are at most $p+1$ edges emanating from v, there are at most $p+1$ double points on the corresponding component. But since $f_K > 1$, this component has $p^{f_K}+1 > p+1$ points rational over $\mathbb{F}_K$, hence there is a smooth $\mathbb{F}_K$-rational point. By Hensel's Lemma, this completes the proof. □

In contrast, when f_K is odd the existence of a K-rational point is characterised in terms of the finite graph $\mathcal{G}_{d,+}$ as follows:

Proposition 4.19. *If f_K is odd, then $Y_d(K) \neq \emptyset$ if and only if there is an edge $y \in \mathcal{G}_{d,+}$ such that $e_K \ell_d(y)$ is even and $w_p(y) = \bar{y}$. Equivalently, if and only if there is an edge $y \in \mathrm{Ed}(\mathcal{G}_d)$ such that $e_K \ell_d(y)$ is even and $\bar{y} = y$.*

Proof. As explained above, by Hensel's Lemma we shall characterise the existence of a smooth $\mathbb{F}_K$-rational point on the special fibre $(\widetilde{\mathcal{Y}_{\Gamma_d,\mathcal{O}_K}})_0$, whose dual graph is $(\widetilde{\mathcal{G}}_{d,+}^{e_K}, w_p^{f_K})$.

If there is such a point, then $(\widetilde{\mathcal{Y}_{\Gamma_d,\mathcal{O}_K}})_0$ has a component rational over $\mathbb{F}_K$, that is, $\widetilde{\mathcal{G}}_{d,+}^{e_K}$ has a vertex fixed by $w_p^{f_K} = w_p$. But since w_p fixes no vertices on $\mathcal{G}_{d,+}$, this happens if and only if $\mathcal{G}_{d,+}^{e_K}$ has an edge y' of even length such that $w_p(y') = \bar{y}'$, which is the same as saying that $\mathcal{G}_{d,+}$ has an edge y such that $e_K\ell(y)$ is even and $w_p(y) = \bar{y}$.

Conversely, suppose $\mathcal{G}_{d,+}$ has en edge y with $e_K\ell(y)$ even and $w_p(y) = \bar{y}$. Then $\mathcal{G}_{d,+}^{e_K}$ has an edge y' of even length with $w_p(y') = \bar{y}'$. Again, we deduce that $\widetilde{\mathcal{G}}_{d,+}^{e_K}$ has a vertex fixed by w_p, which corresponds to an $\mathbb{F}_K$-rational component of $(\widetilde{\mathcal{Y}_{\Gamma_d,\mathcal{O}_K}})_0$ isomorphic to $\mathbb{P}^1_{\mathbb{F}_K}$ and having at most 2 double points. Since $2 < p^{f_K} + 1$, it follows that this component must have a smooth $\mathbb{F}_K$-rational point.

The second assertion in the statement follows immediately from the fact that the length of an edge in $\mathcal{G}_{d,+}$ and the length of its image in $\mathcal{G}_d$ is the same. □

By applying our description of the graphs $\mathcal{G}_{d,+}$ and $\mathcal{G}_d$, we end up with a proof of items b) and c) stated in Theorem 1.1.

Corollary 4.20. *Assume f_K is odd.*

a) *If e_K is even, then $Y_d(K) \neq \emptyset$ if and only if any of the following conditions holds:*
   i) *$\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$ and $4 \mid t_d$,*
   ii) *$p = 2$, $4 \mid t_d$, $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and H_d contains a root of $x^2 + 2x + 2 = 0$, or*
   iii) *$p = 3$, $6 \mid t_d$, $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$ and H_d contains a root of $x^2 + 3x + 3 = 0$.*

b) *If e_K is odd, then $Y_d(K) \neq \emptyset$ if and only if $p = 2$, every prime dividing $D/2$ is congruent to 3 mod 4 (in particular, $\ell \equiv 3 \mod 4$), $4 \mid t_d$ and either $\mathbb{Q}(\sqrt{-2})$ splits $B_{D/p}$ or H_d contains a root of $x^2 + 2x + 2$.*

Proof. When e_K is even, Proposition 4.19 says that $Y_d(K) \neq \emptyset$ if and only if there is an edge $y \in \mathcal{G}_d$ such that $w_p(y) = \bar{y}$. Then a) follows directly from Lemma 4.14 and Corollary 4.17.

As for b), suppose that e_K is odd. Then we know that $X_D(K)$ is empty unless $p = 2$ or $D = 2p$. Since $\ell > 3$, we can assume that $p = 2$, as otherwise $X_D(K)$ is empty and therefore $Y_d(K)$ is necessarily empty as well (we could also deduce this by using Proposition 4.19 and our study of $\mathcal{G}_{d,+}$).

If $Y_d(K)$ is not empty, Proposition 4.19 implies the existence of an edge $y \in \mathcal{G}_d$ such that $\ell_d(y) = 2$ and $\bar{y} = y$. By Corollary 4.11 and Lemma 4.14, this is equivalent to saying that $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$, $4 \mid t_d$ and Γ_d contains a root of some equation in $\mathcal{F}_{2,d}$. Using Lemmas 4.15 and 4.16, this is equivalent to saying that $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$, $4 \mid t_d$ and either $\mathbb{Q}(\sqrt{-2})$ splits $B_{D/p}$ or H_d contains a root of $x^2 + 2x + 2$. Here notice that the condition that $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ is equivalent to saying that every prime dividing D/p is congruent to 3 mod 4, thus we find b).

Conversely, suppose that $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$, $4 \mid t_d$ and either $\mathbb{Q}(\sqrt{-2})$ splits $B_{D/p}$ or H_d contains a root of $x^2 + 2x + 2$. Since $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and $4 \mid t_d$, we can choose $\gamma \in \Gamma_d$ satisfying $\gamma^2 + 1 = 0$, and there is a vertex $\tilde{v} \in \mathrm{Ver}(\mathcal{T}_p)$ such that $\gamma(\tilde{v}) = \tilde{v}$, so that $\mathrm{Stab}_{\Gamma'_{d,+}}(\tilde{v}) = \{[1], [\gamma]\}$. If v is the image of $\tilde{v}$ in $\mathcal{G}_d$ (or in $\mathcal{G}_{d,+}$), then $\ell_d(v) = 2$.

Now if $\mathbb{Q}(\sqrt{-2})$ splits $B_{D/p}$, there is an element $\gamma' \in \mathcal{O}_{D/2}^{(2)\times}$ such that $(\gamma')^2 + 2 = 0$. Since $4 \mid t_d$, Lemma 4.15 implies that actually $\gamma' \in \Gamma_d$. Having norm 2, γ' induces the same element as w_2 in $\Gamma_d/\Gamma_{d,+}$, hence the image y in $\mathcal{G}_d$ of the edge $\tilde{y} := \tilde{v} \to \gamma'(\tilde{v})$ satisfies $\ell_d(y) = 2$ and $\bar{y} = y$.

On the other hand, suppose H_d contains a root of the quadratic equation $x^2 + 2x + 2$. Since $\gamma - 1$ and $-\gamma - 1$ are roots in $\mathcal{O}_{D/2}^{(2)\times}$ of $x^2 + 2x + 2 = 0$, and they map to the two distinct roots of this quadratic equation in $\mathbb{F}_{\ell^2}^\times$, at least one of them lies in H_d by assumption, so either $\gamma - 1$ or $-\gamma - 1$ belongs to Γ_d. Let us write $\gamma' = \gamma - 1$ or $-\gamma - 1$ accordingly. Similarly as before, define $\tilde{v}' := \gamma'(\tilde{v})$ and let $\tilde{y} = \tilde{v} \to \tilde{v}' \in \mathrm{Ed}(\mathcal{T}_p)$. The element γ also fixes $\tilde{v}'$, and therefore the image y of $\tilde{y}$ in $\mathcal{G}_d$ satisfies $\ell_d(y) = 2$ and $\bar{y} = y$. This finishes the proof of b). □

Combining Theorem 1.1 with [JL85, Theorems 5.4, 5.6], we can give explicit conditions for the set $Y_d(K)$ to be empty even in cases where $X_D(K)$ is not.

Corollary 4.21. *Assuming $f_d = 1$, suppose that one of the following conditions is satisfied:*

a) *$p \neq 2, 3$, $\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$ and $4 \nmid t_d$;*

b) *$p = 2$, and either*
   i) *$\mathbb{Q}(\sqrt{-2})$ splits $B_{D/2}$ and $4 \nmid t_d$, or*
   ii) *$\mathbb{Q}(\sqrt{-1})$ splits $B_{D/2}$ and either $4 \nmid t_d$ or H_d does not contain any root of $x^2 + 2x + 2 = 0$.*

c) $p = 3$, $\mathbb{Q}(\sqrt{-3})$ *splits* $B_{D/3}$, $4 \nmid t_d$ *and either* $6 \nmid t_d$ *or* H_d *does not contain any root of* $x^2+3x+3 = 0$.

If $K/\mathbb{Q}_p$ *is any finite extension such that* $f(K/\mathbb{Q}_p)$ *is odd and* $e(K/\mathbb{Q}_p)$ *is even, then* $X_D(K) \neq \emptyset$ *and* $Y_d(K) = \emptyset$.

Corollary 4.22. *Assuming* $f_d = 1$, *suppose that* $p = 2$, *every prime dividing* $D/2$ *is congruent to* 3 *modulo* 4 *and either* $4 \nmid t_d$ *or* $\mathbb{Q}(\sqrt{-2})$ *does not split* $B_{D/2}$ *and* H_d *does not contain any root of* $x^2 + 2x + 2 = 0$. *If* $K/\mathbb{Q}_p$ *is any finite extension such that both* $f(K/\mathbb{Q}_p)$ *and* $e(K/\mathbb{Q}_p)$ *are even, then* $X_D(K) \neq \emptyset$ *and* $Y_d(K) = \emptyset$.

5. $\mathbb{Q}_p$-rational points on Atkin-Lehner quotients of Y_d

After studying local points on the curves Y_d, we now focus on the study of $\mathbb{Q}_p$-rational points on the quotients of these curves by the lifted Atkin-Lehner involutions $\hat{\omega}_m$ attached to positive divisors m of D. By analogy to the classical case, we call these curves *Atkin-Lehner quotients of* Y_d, and we denote by $Y_d^{(m)}$ the quotient of Y_d by the action of $\hat{\omega}_m$. In order to simplify the discussion, we assume throughout that $Y_d(\mathbb{Q}_p) = \emptyset$, as otherwise the sets $Y_d^{(m)}(\mathbb{Q}_p)$ are clearly non-empty for every positive divisor m of D as well. Equivalently, we thus assume that $\mathcal{Y}_{\Gamma_d}(\mathbb{Q}_p) = \emptyset$.

Again, we exploit the p-adic uniformisation of the curves Y_d worked out in Section 4.1. As it happens when studying the curves Y_d, there is a big difference between the cases $f_d = 1$ and $f_d > 1$. Moreover, in cases where Y_d is not geometrically connected we shall take into account whether $\varepsilon_d(m) = 1$ or not (i.e., whether $\hat{\omega}_m$ acts trivially on the set $\mathcal{C}_\infty(d)$ or not). After some considerations regarding these questions, we will soon restrict ourselves to the case $f_d = 1$ and $\varepsilon_d(m) = 1$. Our study of the existence of $\mathbb{Q}_p$-rational points on the curves $Y_d^{(m)}$ then borrows some of the ideas in Kurihara's and Ogg's work (cf. [Kur79], [Ogg85]).

5.1. **p-adic uniformisation of the curves $Y_d^{(m)}$ and first considerations.** We fix as usual a positive divisor d of $(\ell^2-1)/2$ and the corresponding intermediate curve Y_d of $X_{D,\ell} \to X_D$. Let also p be a prime dividing D/ℓ. Recall from Section 4.1 that Cherednik-Drinfeld theory applied to the curves Y_d provides us with isomorphisms

$$\mathcal{Y}_d \simeq \bigsqcup_{i=1}^{c_p(d)} \mathcal{Y}_{\Gamma_d}, \qquad \mathcal{Y}_{\Gamma_d} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^{f_d}} \simeq \bigsqcup_{j=0}^{f_d-1} \widetilde{\mathrm{Fr}}_p^j(\mathcal{Y}_{\Gamma_d}^0),$$

where $\mathcal{Y}_{\Gamma_d}$ is defined over $\mathbb{Z}_p$ and $\mathcal{Y}_{\Gamma_d}^0/\mathbb{Z}_{p^{f_d}}$ is isomorphic to either the base change of the Mumford curve $\mathcal{M}_{\Gamma_{d,+}}$ to $\mathbb{Z}_{p^{f_d}}$ or a quadratic twist of it (cf. (22) and (23)). From these isomorphisms we also recover the fact that the $c_\infty(d) = c_p(d)f_d$ geometric connected components of Y_d, indexed by the set $\mathcal{C}_\infty(d)$, are classified in $c_p(d)$ distinct p-classes, one for each element in $\mathcal{C}_p(d)$, corresponding to the $c_p(d)$ copies of the curve $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$. This corresponds with the natural quotient map

$$\mathcal{C}_\infty(d) \simeq \mathbb{F}_\ell^\times/N(H_d) \longrightarrow \mathcal{C}_p(d) \simeq \mathbb{F}_\ell^\times/N(H_d)\langle p\rangle.$$

Fix a positive divisor m of D. If $\hat{\omega}_m$ acts trivially on the set $\mathcal{C}_\infty(d)$ of geometric connected components of Y_d, (i.e., $\varepsilon_d(m) = 1$) then it obviously acts trivially as well on the set $\mathcal{C}_p(d)$ of p-classes. And when this is the case, we can predict easily the non-existence of $\mathbb{Q}_p$-rational points on $Y_d^{(m)}$ in many instances:

Proposition 5.1. *Assume that* $Y_d(\mathbb{Q}_p) = \emptyset$ *and* $\varepsilon_d(m) = 1$. *If* $f_d > 1$, *then* $Y_d^{(m)}(\mathbb{Q}_p) = \emptyset$.

Proof. Under the hypothesis $\varepsilon_d(m) = 1$, the involution $\hat{\omega}_m$ induces an involution on each geometric connected component of Y_d, which we still denote by $\hat{\omega}_m$. In particular, $\mathcal{Y}_d^{(m)}$ still decomposes over $\mathbb{Z}_p$ as $c_p(d)$ copies of a curve $\mathcal{Y}_{\Gamma_d}^{(m)}$ (namely, the quotient of $\mathcal{Y}_{\Gamma_d}$ by $\hat{\omega}_m$), and each of these curves has f_d geometric connected components, which are only defined over $\mathbb{Z}_{p^{f_d}}$ and conjugated by $\mathrm{Gal}(\mathbb{Q}_{p^{f_d}}/\mathbb{Q}_p)$. In particular, $\mathcal{Y}_{\Gamma_d}^{(m)}(\mathbb{Q}_p)$ is empty, hence so is the set $Y_d^{(m)}(\mathbb{Q}_p)$.

Alternatively, suppose there exists a point $P \in Y_d^{(m)}(\mathbb{Q}_p) = \emptyset$. Then there must be a point $Q \in Y_d(\bar{\mathbb{Q}}_p)$ such that $\{Q, \hat{\omega}_m(Q)\}$ is stable under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. But notice that both Q and $\hat{\omega}_m(Q)$ lie in the same geometric connected component of $\mathcal{Y}_d$. However, if $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ induces a non-trivial automorphism in $\mathrm{Gal}(\mathbb{Q}_{p^{f_d}}/\mathbb{Q}_p)$, then $\sigma(Q)$ lies in a different geometric connected component of $\mathcal{Y}_d$ as Q, hence $\sigma(Q) \notin \{Q, \hat{\omega}_m(Q)\}$, a contradiction. □

Besides, if $\varepsilon_d(m) \neq 1$ it is important to distinguish whether $\hat{\omega}_m$ acts on each p-class of geometric connected components or not. In this regard:

Lemma 5.2. *Assume $\varepsilon_d(m) \neq 1$. Then $\hat{\omega}_m$ acts trivially on the set $\mathcal{C}_p(d)$ of p-classes if and only if the integer f_d is even.*

Proof. Suppose $\varepsilon_d(m) \neq 1$, that is to say, $\varepsilon(m) = -1$ and $-1 \notin N(H_d)$. In particular, this implies that $|N(H_d)|$ is odd. By construction, the action of $\hat{\omega}_m$ on the set $\mathcal{C}_p(d) \simeq \mathbb{F}_\ell^\times / N(H_d)\langle p\rangle$ is trivial if and only if $-1 \in N(H_d)\langle p\rangle$. Being $\mathbb{F}_\ell^\times$ cyclic, this holds if and only if the order of $N(H_d)\langle p\rangle$ is even. And since $|N(H_d)|$ is odd, this is in turn equivalent to saying that the order of p in $\mathbb{F}_\ell^\times/N(H_d)$ is even. But this is exactly the same as having f_d even. □

Proposition 5.3. *Assume that $\varepsilon_d(m) \neq 1$ and $Y_d(\mathbb{Q}_p) = \emptyset$. If $f_d \neq 2$, then $Y_d^{(m)}(\mathbb{Q}_p) = \emptyset$.*

Proof. Suppose that $\varepsilon_d(m) \neq 1$ and $Y_d(\mathbb{Q}_p) = \emptyset$, and assume first that f_d is odd. By the previous lemma, $\hat{\omega}_m$ acts non-trivially on the set $\mathcal{C}_p(d)$ (in particular, $c_p(d)$ is even), and therefore $\mathcal{Y}_d^{(m)}/\mathbb{Z}_p$ is isomorphic (over $\mathbb{Z}_p$) to $c_p(d)/2$ copies of the curve $\mathcal{Y}_{\Gamma_d}$. Since $Y_d(\mathbb{Q}_p) = \emptyset$ by hypothesis, $\mathcal{Y}_{\Gamma_d}(\mathbb{Q}_p)$ is empty and the statement follows. Alternatively, suppose there is a $\mathbb{Q}_p$-rational point $P \in Y_d^{(m)}(\mathbb{Q}_p)$. Then there is a point $Q \in Y_d(\bar{\mathbb{Q}}_p)$ such that the set $\{Q, \hat{\omega}_m(Q)\}$ is stable under the action of $\mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$. But since $Y_d(\mathbb{Q}_p)$ is empty, there exists some $\sigma \in \mathrm{Gal}\,(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $\sigma(Q) = \hat{\omega}_m(Q)$. However, this is not possible, because $\sigma(Q)$ lies in the same p-class as Q, whereas $\hat{\omega}_m(Q)$ does not.

Now assume that f_d is even and $f_d \neq 2$. By the previous lemma, $\hat{\omega}_m$ acts trivially on the set of p-classes. Therefore, $\hat{\omega}_m$ induces an involution on each copy of $\mathcal{Y}_{\Gamma_d}$, which we still denote by $\hat{\omega}_m$. But since $\varepsilon_d(m) \neq 1$, $\hat{\omega}_m$ identifies the f_d geometric connected components of $\mathcal{Y}_{\Gamma_d}$ in pairs, and it follows that $\mathcal{Y}_{\Gamma_d}^{(m)} := \mathcal{Y}_{\Gamma_d}/\langle\hat{\omega}_m\rangle$ decomposes over $\mathbb{Z}_{p^{f_d/2}}$ as the disjoint union of $f_d/2$ geometrically connected curves, all of them defined over $\mathbb{Z}_{p^{f_d/2}}$ and conjugated by $\mathrm{Gal}\,(\mathbb{Q}_{p^{f_d/2}}/\mathbb{Q}_p)$. As a consequence the set $\mathcal{Y}_{\Gamma_d}^{(m)}(\mathbb{Q}_p)$ is empty because $f_d/2 > 1$, so $Y_d^{(m)}(\mathbb{Q}_p)$ is empty as well. □

Remark 5.4. Recall that both $\varepsilon_d(m)$ and f_d can be easily computed, by using (10) together with Lemma 2.2 and Remark 4.3, respectively. Therefore, by combining Theorem 1.1 with Propositions 5.1 and 5.3, we can provide many concrete instances where the set $Y_d^{(m)}(\mathbb{Q}_p)$ is empty.

Remark 5.5. When $\varepsilon_d(m) \neq 1$, Proposition 5.3 leaves open the question of determining whether $Y_d^{(m)}(\mathbb{Q}_p)$ is empty or not only in the case $f_d = 2$. This corresponds to the situation where $\mathcal{Y}_{\Gamma_d}$ decomposes over $\mathbb{Z}_{p^2}$ as the disjoint union of a geometrically connected curve $\mathcal{Y}_{\Gamma_d}^0/\mathbb{Z}_{p^2}$ and its Frobenius conjugate $\mathcal{Y}_{\Gamma_d}^1 := \widetilde{\mathrm{Fr}}_p(\mathcal{Y}_{\Gamma_d}^0)$, which are permuted also by the action of $\hat{\omega}_m$. The Atkin-Lehner quotient $\mathcal{Y}_{\Gamma_d}^{(m)}$ is therefore a model for $\mathcal{Y}_{\Gamma_d}^0$ over $\mathbb{Z}_p$. The twists of Mumford curves that one needs to deal with in order to study the existence of $\mathbb{Q}_p$-rational points on $\mathcal{Y}_{\Gamma_d}^{(m)}$ in this setting are not in the scope of this note, so we will not consider this particular case.

We thus assume for the rest of this note that $f_d = 1$ and $\varepsilon_d(m) = 1$. In particular, notice that $\mathcal{Y}_d/\mathbb{Z}_p$ decomposes completely over $\mathbb{Z}_p$ (that is to say, $c_\infty(d) = c_p(d)$). Hence we have an isomorphism of $\mathbb{Z}_p$-schemes

$$\mathcal{Y}_d^{(m)} \simeq \bigsqcup_{i=1}^{c_p(d)} \mathcal{Y}_{\Gamma_d}^{(m)}, \tag{27}$$

where $\mathcal{Y}_{\Gamma_d}^{(m)}$ stands for the quotient of $\mathcal{Y}_{\Gamma_d}$ by the action of the involution induced by $\hat{\omega}_m$ on $\mathcal{Y}_{\Gamma_d}$, which we still denote $\hat{\omega}_m$. Recall that $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$ is the quadratic twist $\mathcal{M}_{\Gamma_{d,+}}^{\xi}$ of the Mumford curve over $\mathbb{Z}_p$ associated with $\Gamma_{d,+}$ by the cohomology class corresponding to the 1-cocycle

$$\xi : \mathrm{Gal}\,(\mathbb{Q}_{p^2}/\mathbb{Q}_p) \longrightarrow \mathrm{Aut}(\mathcal{M}_{\Gamma_{d,+}} \times_{\mathbb{Z}_p} \mathbb{Z}_{p^2}/\mathbb{Z}_{p^2}), \quad \widetilde{\mathrm{Fr}}_p \longmapsto w_p \times \mathrm{id}.$$

As we did for the curve Y_d, next we study the existence of $\mathbb{Q}_p$-rational points on the curve $\mathcal{Y}_{\Gamma_d}^{(m)}$ (hence on $\mathcal{Y}_d^{(m)}$) by studying the existence of smooth $\mathbb{F}_p$-rational points on the special fibre of a regular model and applying Hensel's Lemma. And for this, we translate again the problem into a combinatoric issue on the dual graph $\mathcal{G}_{d,+}$ of the admissible curve $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$.

Remark 5.6. As pointed out in [dVP13, Remark 5.5], the Atkin-Lehner involutions on X_D can be lifted to $X_{D,\ell}$ in more than one way, although the structure of $\mathrm{Aut}^{\mathrm{mod}}(X_{D,\ell})$ as an abstract group does not depend on the choice of the involutions $\hat{\omega}_m$.

When considering intermediate curves Y_d and an Atkin-Lehner involution ω_m, it might still be the case that $\mathrm{Aut}^{\mathrm{mod}}(Y_d)$ contains more than one involution lifting ω_m. And in certain cases, the action of these lifted involutions on the set $\mathcal{C}_\infty(d)$ can be different (this will not be the case, of course, if Y_d is geometrically connected, for example). Nevertheless, we remark that when this occurs, the quotients of Y_d by different lifts of ω_m are different curves. Throughout this note, we always consider $\hat{\omega}_m$ to be the lifted Atkin-Lehner involution as in [dVP13, Definition 4.3].

5.2. **$\mathbb{Q}_p$-rational points on $Y_d^{(p)}$.** We start by studying the Atkin-Lehner quotient of Y_d by the involution $\hat{\omega}_p$, where we still assume $p \neq \ell$. First of all, we notice that the hypothesis $f_d = 1$ already implies that $\varepsilon_d(p) = 1$, thus we do not need to make this extra assumption:

Lemma 5.7. *Under the hypothesis $f_d = 1$, we always have $\varepsilon_d(p) = 1$. Furthermore, the action of $\hat{\omega}_p$ on the curve $\mathcal{Y}_{\Gamma_d}$ corresponds to the involution induced by w_p on $\mathcal{M}^\xi_{\Gamma_{d,+}}$.*

Proof. Our assumption $f_d = 1$ implies that $c_p(d) = c_\infty(d)$. If this integer is odd, then it must be $\varepsilon_d(p) = 1$. Assume on the contrary that $c_p(d) = c_\infty(d)$ is even. This means that $N(H_d)$ is a subgroup of $\mathbb{F}_\ell^{\times 2} \subseteq \mathbb{F}_\ell^\times$, the subgroup of $\mathbb{F}_\ell^\times$ consisting of the quadratic residues modulo ℓ. Since $f_d = 1$ is equivalent to $p \mod \ell$ being in $N(H_d)$, it follows that $(\frac{p}{\ell}) = 1$, hence $\varepsilon(p) = 1$, so that $\varepsilon_d(p) = 1$ as well. This proves the first assertion.

As for the second part, the action of the lifted involution $\hat{\omega}_p$ on $\widehat{\mathcal{Y}}_d$, the p-adic counterpart of $Y_d \times_{\mathbb{Q}} \bar{\mathbb{Q}}$, is induced (through (15)) by the modular automorphism

$$\rho_{U_d}(1, \dots, 1, \mathrm{w}_p, 1, \dots, 1, \alpha_p, 1, \dots) = \rho_{U_d}(\mathrm{w}_p)\rho_{U_d}(\alpha_p) : Y_d \longrightarrow Y_d,$$

with

$$\mathrm{w}_p = \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} \in \mathcal{O}_{D,p} \quad \text{and} \quad \alpha_p = \begin{pmatrix} s_p & 0 \\ 0 & \bar{s}_p \end{pmatrix} \in \mathcal{O}_{D,\ell}^\times,$$

where $s_p \in \mathbb{Z}_{\ell^2}^\times$ reduces to a square root of p modulo ℓ in $\mathbb{F}_{\ell^2}^\times$, and $a \mapsto \bar{a}$ denotes the non-trivial automorphism in $\mathrm{Gal}(\mathbb{Q}_{\ell^2}/\mathbb{Q}_\ell)$. By the assumption $f_d = 1$, the automorphism induced by $\rho_{U_d}(\mathrm{w}_p)$ acts on $\mathcal{Y}_{\Gamma_d}$ as the involution induced by w_p, via the isomorphism (15). Therefore, we need to show that $\rho_{U_d}(\alpha_p)$ induces the identity isomorphism, which is equivalent to showing that $\alpha_p \in U_{d,\ell}$. But since we are assuming $f_d = 1$, it turns out that $p \mod \ell = x^{\ell+1}$ for some $x \in H_d \subseteq \mathbb{F}_{\ell^2}^\times$. Since ℓ is odd, in particular $p \mod \ell$ is the square of an element in H_d. Hence, the reduction of s_p to $\mathbb{F}_{\ell^2}^\times$ lies in H_d, which implies that $\alpha_p \in U_{d,\ell}$ and the statement follows. □

As a consequence of this lemma, an integral model $\mathcal{Y}_d^{(p)}/\mathbb{Z}_p$ of the Atkin-Lehner quotient $Y_d^{(p)}$ is obtained by taking the quotient of each connected component by w_p, thus

$$\mathcal{Y}_d^{(p)} \simeq \bigsqcup_{i=1}^{c_p(d)} \mathcal{Y}_{\Gamma_d}^{(p)} \simeq \bigsqcup_{i=1}^{c_p(d)} \mathcal{M}_{\Gamma_d},$$

where in the last isomorphism we use that the quotient of the twisted Mumford curve $\mathcal{M}^\xi_{\Gamma_{d,+}}/\mathbb{Z}_p$ by the involution w_p is precisely the (untwisted) Mumford curve $\mathcal{M}_{\Gamma_d}/\mathbb{Z}_p$ associated with $\Gamma_d \subseteq \mathrm{GL}_2(\mathbb{Q}_p)$. In particular:

Corollary 5.8. *Assuming $f_d = 1$, $Y_d^{(p)}(\mathbb{Q}_p) \neq \emptyset$ if and only if $\mathcal{M}_{\Gamma_d}(\mathbb{Q}_p) \neq \emptyset$.*

Similarly as for $\mathcal{M}_{\Gamma_{d,+}}$, now the dual graph of $\mathcal{M}_{\Gamma_d}/\mathbb{Z}_p$ is the finite graph with lengths $\mathcal{G}_d^* := (\Gamma_d \backslash \mathcal{T}_p)^*$, with trivial Frobenius action, and where the $*$ means that one has to remove from $\mathcal{G}_d$ those edges y with $\bar{y} = y$ (see [Kur79, Proposition 3.2]). In contrast to the case of $\mathcal{G}_{d,+}$, now such edges may exist as we saw in Lemma 4.14. We thus have the following:

Lemma 5.9. *Assume $f_d = 1$. The set $Y_d^{(p)}(\mathbb{Q}_p)$ is not empty if and only if the graph $\mathcal{G}_d$ has a vertex of non-trivial length or an edge y with $\bar{y} = y$.*

Proof. "In general", every vertex in the finite graph $\mathcal{G}_d$ has $p+1$ edges in its star, and a smooth rational point on the special fibre of (a regular model of) $\mathcal{M}_{\Gamma_d}/\mathbb{Z}_p$ exists if and only if there is some vertex in $\widetilde{\mathcal{G}}_d^*$ with less than $p+1$ edges emanating from it. But this happens if and only if there is a vertex $v \in \mathrm{Ver}(\mathcal{G}_d)$ such that either v has non-trivial length or there is some edge y in $\mathcal{G}_d$ emanating from v such that $\bar{y} = y$ (such an edge is removed in $\mathcal{G}_d^*$, hence the vertex corresponding to v in $\widetilde{\mathcal{G}}_d^*$ has less than $p+1$ edges in its star). Then the statement follows by applying Hensel's Lemma. □

After our description of $\mathcal{G}_d$, we conclude with the following criterion for the existence of $\mathbb{Q}_p$-rational points on $Y_d^{(p)}$:

Theorem 5.10. *Assume $f_d = 1$. Then the set $Y_d^{(p)}(\mathbb{Q}_p)$ is not empty if and only if any of the following conditions holds:*

i) $\mathbb{Q}(\sqrt{-1})$ *splits* $B_{D/p}$ *and* $4 \mid t_d$,
ii) $\mathbb{Q}(\sqrt{-3})$ *splits* $B_{D/p}$ *and* $6 \mid t_d$,
iii) Γ_d *contains a root of some equation in* $\mathcal{F}_{p,d}$.

Proof. It follows immediately from the previous lemma together with Corollary 4.9 and Lemma 4.14. Indeed, condition i) (resp. ii)) is equivalent to $\mathcal{G}_d$ having an vertex of length 2 (resp. 3), whereas condition iii) is equivalent to $\mathcal{G}_d$ having an edge y such that $\bar{y} = y$. □

By virtue of Corollary 4.17, Theorem 1.2 is now a direct consequence of this theorem.

From [Ogg85], we know that $X_D^{(p)}(\mathbb{Q}_p)$ is not empty if and only if either $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$. This obviously holds when either of the conditions in the previous result is satisfied, since $Y_d^{(p)}(\mathbb{Q}_p) \neq \emptyset$ implies that $X_D^{(p)} \neq \emptyset$. Combining Theorem 1.2 with [Ogg85, p. 206], we point out the following:

Corollary 5.11. *Assume $f_d = 1$, and suppose that either $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$ or $\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$. Furthermore, in case that either $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-p})$ splits $B_{D/p}$, assume also $4 \nmid t_d$, whereas if $\mathbb{Q}(\sqrt{-3})$ splits $B_{D/p}$, assume $6 \nmid t_d$. Then $Y_d^{(p)}(\mathbb{Q}_p) = \emptyset$ and $X_D^{(p)}(\mathbb{Q}_p) \neq \emptyset$.*

Example 5.12. Take $\ell = 5$, and let p be a prime such that $(\frac{-p}{5}) = 1$. Set $D = \ell p = 5p$, and observe that the quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-p})$ do not split $B_5 = B_{D/p}$, whereas $\mathbb{Q}(\sqrt{-3})$ does. Further, let d be either 3 or 6 (so that $6 \nmid 12/d$) and assume that $f_d = 1$. Then the previous corollary applies and we conclude that $Y_d^{(p)}(\mathbb{Q}_p)$ is empty but $X_{5p}^{(p)}(\mathbb{Q}_p)$ is not.

We can illustrate this example by means of the corresponding dual graphs. The class number of B_5 is 1, so that $\mathcal{G}_D$ consists of only one vertex v of length 3. For simplicity, assume that $(\frac{-3}{p}) = -1$, so that $\mathrm{Star}(v)$ consists of $(p+1)/3$ edges y_i of length 1, all of them satisfying $\bar{y}_i \neq y_i$. Under the previous conditions, the graph $\mathcal{G}_d$ consists of $d_{\mathcal{G}}/3$ vertices of length 1 mapping to v. Further, each vertex $v' \in \mathrm{Ver}(\mathcal{G}_d)$ has $p+1$ edges y'_i of trivial length in its star, all of them satisfying again $\bar{y}'_i \neq y'_i$. This clearly implies that the special fibre of $\mathcal{Y}_{\Gamma_d}^{(p)}$ cannot have a smooth $\mathbb{F}_p$-rational point.

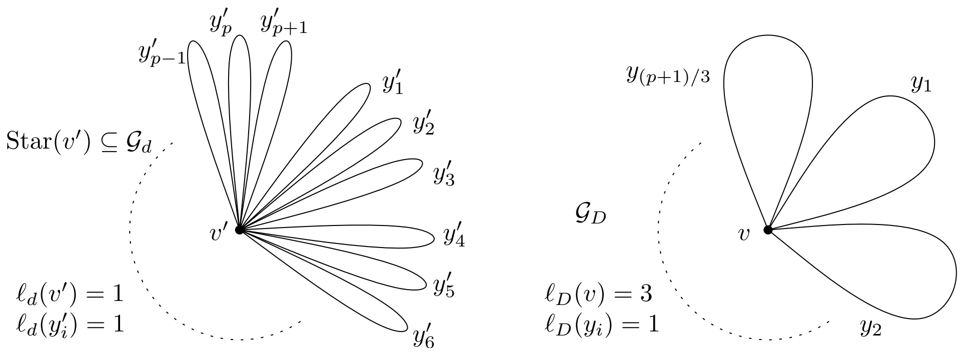

FIGURE 1. The graph $\mathcal{G}_D$ and the star of any vertex $v' \in \mathrm{Ver}(\mathcal{G}_d)$.

For example, take $p = 11$. Then notice $f = \mathrm{ord}_{\mathbb{F}_5^\times}(11) = 1$, so that $f_d = 1$ for all d. Furthermore, $(\frac{-11}{5}) = 1$ and $(\frac{-3}{11}) = -1$, hence the above conditions apply if we choose d to be either 3 or 6. In each case, Y_d has 1 or 2 geometric connected components, respectively.

5.3. **$\mathbb{Q}_p$-rational points on $Y_d^{(m)}$: the case $p \nmid m$.** Next we consider the quotient of Y_d by a lifted Atkin-Lehner involution $\hat{\omega}_m$ associated with a positive divisor m of D/p, $m > 1$. We still assume that $f_d = 1$ and $\varepsilon_d(m) = 1$, thus we have a decomposition of $\mathcal{Y}_d^{(m)}$ over $\mathbb{Z}_p$ as in (27) and the set $Y_d^{(m)}(\mathbb{Q}_p)$ is not empty if and only if so is the set $\mathcal{Y}_{\Gamma_d}^{(m)}(\mathbb{Q}_p)$. In order to study the set $\mathcal{Y}_{\Gamma_d}^{(m)}(\mathbb{Q}_p)$ by looking at the graph with lengths $\mathcal{G}_{d,+}$, first we describe the action of $\hat{\omega}_m$ on it.

Recall that the involution $\hat{\omega}_m$ acting on Y_d is defined as a modular automorphism, that is, $\hat{\omega}_m = \rho_{U_d}(b)$ for some $b \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f)^\times$ normalising U_d. Further, since we are assuming $p \nmid m$ we can choose b to be of the form $(b^p, 1) \in (B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^\times \times B_{D,p}^\times$. As in Section 3.3, this implies that the involution $\hat{\omega}_m$ corresponds, in the p-adic counterpart of Y_d, to the p-modular automorphism $\lambda_{U_d}((b_v^p)^{-1})$ acting on $\mathcal{Y}_d$. We start by describing this p-modular automorphism.

More precisely, assume first that $m = q$ is a prime dividing D/p. If $q \neq \ell$, then

$$\hat{\omega}_q = \rho_{U_d}(\dots, 1, \dots, \mathrm{w}_q, \dots, 1, \dots, \alpha_q, \dots, 1, \dots),$$

where

$$\mathrm{w}_q = \begin{pmatrix} 0 & 1 \\ q & 0 \end{pmatrix} \in \mathcal{O}_{D,q} \quad \text{and} \quad \alpha_q = \begin{pmatrix} s_q & 0 \\ 0 & \bar{s}_q \end{pmatrix} \in \mathcal{O}_{D,\ell}^{\times},$$

with $s_q \in \mathbb{Z}_{\ell^2}$ such that $s_q^2 \equiv q \mod \ell\mathbb{Z}_{\ell^2}$. In contrast, $\hat{\omega}_\ell = \rho_{U_d}(\mathrm{w}_\ell)$ (cf. [dVP13, Definition 4.3]).

When m is not prime, $\hat{\omega}_m$ is obtained by composing the involutions $\hat{\omega}_q$ for all the primes q dividing m. Since all the involutions $\hat{\omega}_q$ commute one with each other, this is well-defined, and without loss of generality we can write the involution $\hat{\omega}_m$ acting on Y_d as

$$\hat{\omega}_m = \rho_{U_d}(\alpha_m) \cdot \prod_{\substack{q|m,\\ q\neq\ell}} \rho_{U_d}(\mathrm{w}_q),$$

where the elements w_q are as above (notice that $\mathrm{w}_q^2 = q$), and where $\alpha_m \in B_{D,\ell}^{\times}$ is given by

$$\alpha_m = \begin{cases} \prod_{q|m} \alpha_q & \text{if } \ell \nmid m, \\ \mathrm{w}_\ell \prod_{q|\frac{m}{\ell}} \alpha_q, & \text{if } \ell \mid m. \end{cases}$$

Notice that if $\ell \nmid m$, then $\mathrm{val}_\ell(\mathrm{n}(\alpha_m)) = 0$, whereas if $\ell \mid m$, then $\mathrm{val}_\ell(\mathrm{n}(\alpha_m)) = \mathrm{val}_\ell(\mathrm{n}(\mathrm{w}_\ell)) = 1$.

Since $p \nmid m$, the action of $\hat{\omega}_m$ on the p-adic counterpart of the adèlic description of Y_d, is then given by the p-modular automorphism

$$\lambda_{U_d}(\alpha_m^{-1}) \cdot \prod_{\substack{q|m,\\ q\neq\ell}} \lambda_{U_d}(\mathrm{w}_q^{-1}).$$

Here we write $\mathrm{w}_q^{-1} \in B_{D/p,q}^{\times}$ and $\alpha_m^{-1} \in B_{D/p,\ell}^{\times}$ for the images of w_q and α_m, respectively, according to our fixed anti-isomorphism between $(B_D \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^{\times}$ and $(B_{D/p} \otimes_{\mathbb{Q}} \mathbb{A}_f^p)^{\times}$. Thus the action of $\hat{\omega}_m$ on

$$\mathrm{GL}_2(\mathbb{Q}_p) \setminus [\widehat{\mathcal{H}}_p \widehat{\otimes} \widehat{\mathbb{Z}}_p^{\mathrm{ur}} \times Z_{U_d}]$$

is given by the rule

$$[x, z, [(a_v)]] \longmapsto [x, z, [(\dots, a_v, \dots, \mathrm{w}_q^{-1} a_q, \dots, \alpha_m^{-1} a_\ell, \dots)]]. \tag{28}$$

This gives therefore the action of $\hat{\omega}_m$ on $\mathcal{Y}_d$. In order to describe the action of $\hat{\omega}_m$ induced on each copy of $\mathcal{Y}_{\Gamma_d}$, we may identify $\mathcal{Y}_{\Gamma_d}$ with the p-class corresponding to the trivial element in $\mathcal{C}_p(d)$. Then, the action of $\hat{\omega}_m$ on $\mathcal{Y}_{\Gamma_d}$ is described just by restricting (28) to double cosets of the form

$$[x, z, [(1, 1, \dots, 1, \dots)]],$$

on which we have

$$[x, z, [(1, 1, \dots, 1, \dots)]] \longmapsto [x, z, [(1, 1, \dots, \mathrm{w}_q^{-1}, \dots, \alpha_m^{-1}, \dots, 1, \dots)]],$$

where α_m^{-1} is in the ℓ-th position. Since $\hat{\omega}_m$ acts trivially on the set $\mathcal{C}_p(d)$ of p-classes, there exist elements $g \in \mathrm{GL}_2(\mathbb{Q}_p)$, $b \in B_{D/p}^{\times}$ and $u = (u_v)_{v\neq p} \in U_d^p$ such that

$$[gu(1, 1, \dots, \mathrm{w}_q^{-1}, \dots, \alpha_m^{-1}, \dots, 1, \dots)b] = [(1, 1, \dots, 1, \dots)].$$

From this, we deduce the following:

i) $gb = 1$ (at the p-th place), so that $g = b^{-1} \in B_{D/p}^{\times}$ is in fact global;
ii) $u_v b = 1$ for all v such that $v \neq p, \ell$, $v \nmid m$, hence $g = b^{-1} \in U_{d,v} = \mathcal{O}_{D/p,v}^{\times}$ for all such places;
iii) $u_q \mathrm{w}_q^{-1} b = 1$ for all primes $q \mid m$, $q \neq \ell$, thus in particular $\mathrm{val}_q(\mathrm{n}(g)) = -\mathrm{val}_q(\mathrm{n}(b)) = -1$ for all these primes;
iv) $u_\ell \alpha_m^{-1} b = 1$, so that $\mathrm{val}_\ell(\mathrm{n}(g)) = -\mathrm{val}_\ell(\mathrm{n}(b)) = -\mathrm{val}_\ell(\mathrm{n}(\alpha_m))$, hence $\mathrm{val}_\ell(\mathrm{n}(g))$ is either -1 or 0, according to whether $\ell \mid m$ or not, respectively.

Hence, the lifted Atkin-Lehner involution $\hat{\omega}_m$ acts on $\mathcal{Y}_{\Gamma_d}$ via the action of $g \in B_{D/p}^{\times} \subseteq B_{D/p,p}^{\times} \simeq \mathrm{GL}_2(\mathbb{Q}_p)$ through $\mathcal{H}_p$, using that $\mathcal{Y}_{\Gamma_d}$ is the algebraisation of the Mumford quotient

$$W \setminus ((\Gamma_d \setminus \widehat{\mathcal{H}}_p) \widehat{\otimes} \widehat{\mathbb{Z}}_{p^2}).$$

Since $\mathbb{Q}^{\times} \hookrightarrow \mathbb{Q}_p^{\times} = Z(\mathrm{GL}_2(\mathbb{Q}_p))$ acts trivially on this quotient, we see that $\hat{\omega}_m$ acts on $\mathcal{Y}_{\Gamma_d}$ via the action of $w_m := mg$ through $\mathcal{H}_p$ as well. From i)-iv) above, we notice that $w_m \in \mathcal{O}_{D/p}^{(p)}$ normalises Γ_d (so that $w_m \in \Gamma_d^*$), $\mathrm{n}(w_m) = m$ and $w_m^2 \in m\Gamma_d \subseteq \mathbb{Q}^{\times}\Gamma_d$. Further, locally at ℓ we have $w_m \in m\alpha_m^{-1} U_{d,\ell}$. Regarding this local condition, observe the following:

Lemma 5.13. *Locally at ℓ, $w_m \in \alpha_m U_{d,\ell}$, thus in particular $w_m^2 = mu$ for some $u \in \mathcal{O}_{D/p}^{(p)\times} \cap U_{d,\ell}$.*

Proof. Since we know that $w_m \in m\alpha_m^{-1} U_{d,\ell}$, it is enough to prove that $m \in \alpha_m^2 U_{d,\ell}$. We distinguish the cases $\ell \nmid m$ and $\ell \mid m$. In the first case, we can write

$$\alpha_m = \begin{pmatrix} s & 0 \\ 0 & \bar{s} \end{pmatrix} \in \mathcal{O}_{D/p,\ell}, \quad s \in \mathbb{Z}_{\ell^2}, s^2 \equiv m \mod \ell\mathbb{Z}_{\ell^2}.$$

Therefore,

$$\alpha_m^2 = \begin{pmatrix} m+\ell c & 0 \\ 0 & m+\ell\bar{c} \end{pmatrix}$$

for some $c \in \mathbb{Z}_{\ell^2}$. Multiplying (on the right) by

$$u = \begin{pmatrix} 1+\ell x & 0 \\ 0 & 1+\ell\bar{x} \end{pmatrix} \in 1 + I_\ell, \quad x = -c(m+\ell c)^{-1} \in \mathbb{Z}_{\ell^2},$$

we find $\alpha_m^2 u = m$, and since $U_{d,\ell} \supseteq 1 + I_\ell$, the claim follows.

If $\ell \mid m$, then α_m is defined slightly different, namely

$$\alpha_m = \begin{pmatrix} 0 & 1 \\ \ell & 0 \end{pmatrix} \begin{pmatrix} s & 0 \\ 0 & \bar{s} \end{pmatrix} \in \mathcal{O}_{D/p,\ell}, \quad s \in \mathbb{Z}_{\ell^2}, s^2 \equiv \frac{m}{\ell} \mod \ell\mathbb{Z}_{\ell^2}.$$

Now, one checks that

$$\alpha_m^2 = \pm\ell \begin{pmatrix} \frac{m}{\ell}+\ell c & 0 \\ 0 & \frac{m}{\ell}+\ell\bar{c} \end{pmatrix}$$

for some $c \in \mathbb{Z}_{\ell^2}$. Proceeding as before, and noting that we always have $-1 \in U_{d,\ell}$ by our choice of the subgroup U_d, it holds again that $\alpha_m^2 u = m$ for some $u \in U_{d,\ell}$, and the claim also follows in this case.

Finally, the last assertion in the statement is now easily obtained by using that α_m normalises $U_{d,\ell}$, its square is $\pm m$ and $-1 \in U_{d,\ell}$. ☐

Altogether, we have proved the following:

Proposition 5.14. *The lifted Atkin-Lehner involution $\hat{\omega}_m$ acts on $\mathcal{Y}_{\Gamma_d}$ as the automorphism induced by the action of the element $w_m \in \mathcal{O}_{D/p}^{(p)} \cap \Gamma_d^*$ on $\mathcal{H}_p$ defined above. Further, w_m has reduced norm m, $w_m^2 \in m\Gamma_d$ and, locally at ℓ, $w_m \in \alpha_m U_{d,\ell}$ and $w_m^2 = mu$ for some $u \in \mathcal{O}_{D/p}^{(p)\times} \cap U_{d,\ell}$.*

Observe that the action of $w_m \in \Gamma_d^*$ on $\mathcal{Y}_{\Gamma_d}$ depends only on the image of w_m in $\Gamma_d^*/\mathbb{Q}^\times\Gamma_d$. It is important to remark, however, that we can choose w_m satisfying the properties stated in the above proposition. On the other hand, the above proposition also describes the action of $\hat{\omega}_m$ on the dual graph of the special fibre of $\mathcal{Y}_{\Gamma_d}$. Namely, it is naturally given by the action induced by w_m on $\mathcal{T}_p$.

Later we will make use of the following observation concerning the element w_m:

Lemma 5.15. *Let $\alpha \in \mathcal{O}_{D/p}^{(p)}$ be an element of reduced norm m normalising $\mathcal{O}_{D/p}^{(p)\times}$. Then $\alpha \in w_m\Gamma_d$ if and only if locally at ℓ it holds that $\alpha \in \alpha_m U_{d,\ell}$.*

Proof. Indeed, it is plain that the condition is local at ℓ, as U_d is maximal outside ℓ. And at the prime ℓ, using that $w_m \in \alpha_m U_{d,\ell}$ we deduce that $\alpha \in w_m U_{d,\ell}$ if and only if $\alpha \in \alpha_m U_{d,\ell}$. ☐

Once the action of $\hat{\omega}_m$ on $\mathcal{Y}_{\Gamma_d}$ (resp. on $\mathcal{G}_{d,+}$) is described through the action of $w_m \in \Gamma_d^*$ on $\mathcal{H}_p$ (resp. on $\mathcal{T}_p$), we are in position to study the existence of smooth $\mathbb{F}_p$-rational points on the special fibre of a regular model of $\mathcal{Y}_{\Gamma_d}^{(m)}$ by looking at the dual graph of $\mathcal{Y}_{\Gamma_d}/\mathbb{Z}_p$.

Let us consider the finite graph with lengths

$$\mathcal{G}_{d,+}^{(m)} := \langle w_m \rangle \setminus \mathcal{G}_{d,+} = \langle \Gamma_{d,+}, w_m \rangle \setminus \mathcal{T}_p.$$

Under our assumption that $p \nmid m$, this turns to be the dual graph of $\mathcal{Y}_{\Gamma_d}^{(m)}$:

Lemma 5.16. *There is no edge y in $\mathcal{G}_{d,+}^{(m)}$ such that $\bar{y} = y$. As a consequence, the finite graph $\mathcal{G}_{d,+}^{(m)}$ is the dual graph of $\mathcal{Y}_{\Gamma_d}^{(m)}$, with Frobenius action given by w_p.*

Proof. This follows by a similar argument to the one we used when studying the graph $\mathcal{G}_{d,+}$ from $\mathcal{G}_d$. Indeed, consider again the partition $\mathrm{Ver}(\mathcal{T}_p) = V_1 \sqcup V_2$ as before. Since $\mathcal{G}_{d,+}$ does not have edges y such that $\bar{y} = y$, such an edge exists in $\mathcal{G}_{d,+}^{(m)}$ if and only if there exists an edge y in $\mathcal{G}_{d,+}$ with $w_m(y) = \bar{y}$. But since $\mathrm{n}(w_m) = m$ and $p \nmid m$, it follows that $w_m(V_i) = V_i$ for $i = 1, 2$, thus there cannot be such an edge. ☐

Further, we emphasise the following:

Lemma 5.17. *There is no vertex in $\mathcal{G}_{d,+}^{(m)}$ fixed by w_p.*

Proof. Assume there is a vertex v in $\mathcal{G}_{d,+}^{(m)}$ such that $w_p(v) = v$. Since w_p fixes no vertex in $\mathcal{G}_{d,+}$, a preimage v' of v in $\mathcal{G}_{d,+}$ satisfies $w_p(v') = w_m(v')$. But therefore v' is fixed by $w_m^{-1}w_p$, and this is not possible because $w_m^{-1}w_p$ switches the sets of vertices V_1 and V_2. □

In other words, the special fibre of $\mathcal{Y}_{\Gamma_d}^{(m)}$ has no component rational over $\mathbb{F}_p$. If $\mathcal{Y}_{\Gamma_d}^{(m)}$ is already regular, which is equivalent to saying that every edge of $\mathcal{G}_{d,+}^{(m)}$ has length 1, then Hensel's Lemma implies that $\mathcal{Y}_{\Gamma_d}^{(m)}(\mathbb{Q}_p)$ is empty, hence so is $Y_d^{(m)}(\mathbb{Q}_p)$. In general:

Proposition 5.18. *Assume $f_d = 1$ and $\varepsilon_d(m) = 1$ as before. If $Y_d(\mathbb{Q}_p) = \emptyset$ and $p \nmid m$, then the set $Y_d^{(m)}(\mathbb{Q}_p)$ is not empty if and only if either*

i) *there exists an edge y in $\mathcal{G}_{d,+}$ of odd length such that $w_m(y) = y$ and $w_p(y) = \bar{y}$, or*
ii) *there exists an edge y in $\mathcal{G}_{d,+}$ of even length such that $w_pw_m(y) = \bar{y}$.*

Proof. By the above observations, the special fibre of a regular model of $\mathcal{Y}_{\Gamma_d}^{(m)}$ has a smooth $\mathbb{F}_p$-rational point if and only if the graph $\widetilde{\mathcal{G}}_{d,+}^{(m)}$ has a vertex fixed by w_p which is the origin of less than $p+1$ edges. But in view of the previous lemma, this happens if and only if such a vertex has appeared during the resolution of singularities, that is to say, if and only if there exists an edge y_m of even length in $\mathcal{G}_{d,+}^{(m)}$ such that $w_p(y_m) = \bar{y}_m$. By Hensel's Lemma, this is therefore equivalent to the set $\mathcal{Y}_{\Gamma_d}^{(m)}(\mathbb{Q}_p)$ being non-empty, and therefore to the non-emptiness of $Y_d^{(m)}(\mathbb{Q}_p)$ as well.

If the morphism $\mathcal{G}_{d,+} \to \mathcal{G}_{d,+}^{(m)}$ is ramified at y_m, the previous condition is equivalent to saying that there exists an edge y in $\mathcal{G}_{d,+}$ satisfying $w_m(y) = y$ and $w_p(y) = \bar{y}$. Observe that this edge is necessarily of odd length because we are assuming $Y_d(\mathbb{Q}_p)$ is empty, thus i) is satisfied.

In contrast, if the morphism $\mathcal{G}_{d,+} \to \mathcal{G}_{d,+}^{(m)}$ is not ramified at y_m, the above condition holds if and only if there is an edge y in $\mathcal{G}_{d,+}$ of even length such that either $w_p(y) = \bar{y}$ or $w_pw_m(y) = \bar{y}$. The first case is excluded because we are assuming that $Y_d(\mathbb{Q}_p)$ is empty, and therefore condition ii) holds. □

Now we translate the conditions of this proposition into explicit arithmetic conditions. For the first one, we need a couple of lemmas whose essence is the same as that of Lemmas 4.15 and 4.16.

Lemma 5.19. *Let $\alpha \in \mathcal{O}_{D/p}^{(p)}$ be a solution of $x^2 + m = 0$. If $\ell \mid m$, then $\alpha \in w_m\Gamma_d$, whereas if $\ell \nmid m$, then $\alpha \in w_m\Gamma_d$ if and only if $4 \mid t_d$.*

Proof. By Lemma 5.15, we know that $\alpha \in w_m\Gamma_d$ if and only if, locally at ℓ, it holds that $\alpha \in \alpha_m U_{d,\ell}$.

Assume first that $\ell \mid m$. Then $\alpha_m = \mathrm{w}_\ell\alpha'_m$, where $\alpha'_m \in \mathcal{O}_{D/p,\ell}^\times$ and $\tau' := \psi(\alpha'_m) \in \mathbb{F}_{\ell^2}^\times$ is a square root of m/ℓ in $\mathbb{F}_{\ell^2}^\times$. In this case, $\alpha \in \alpha_m U_{d,\ell}$ is equivalent to $\mathrm{w}_\ell^{-1}\alpha \in \alpha'_m U_{d,\ell}$, and by applying ψ this is in turn equivalent to $\psi(\mathrm{w}_\ell^{-1}\alpha) \in \tau' H_d$. But now observe that $\mathrm{w}_\ell^{-1}\alpha$ is a square root of m/ℓ in $\mathcal{O}_{D/p,\ell}^\times$, hence its image by ψ is either τ' or $-\tau'$. Since $-1 \in H_d$, we deduce that $\psi(\mathrm{w}_\ell^{-1}\alpha) \in \tau' H_d$, hence the assertion follows.

Now suppose that $\ell \nmid m$. In this case, $\alpha_m \in \mathcal{O}_{D/p,\ell}^\times$ and $\tau := \psi(\alpha_m) \in \mathbb{F}_{\ell^2}^\times$ is a square root of m in $\mathbb{F}_{\ell^2}^\times$. Besides, we also have $\alpha \in \mathcal{O}_{D/p,\ell}^\times$, but $\psi(\alpha) \in \mathbb{F}_{\ell^2}^\times$ is a square root of $-m$ in $\mathbb{F}_{\ell^2}^\times$ instead. Again, $\alpha \in \alpha_m U_{d,\ell}$ is now equivalent to $\psi(\alpha) \in \tau H_d$, hence we conclude that $\alpha \in \alpha_m U_{d,\ell}$ if and only if -1 is a square in H_d, which is equivalent to saying that $4 \mid t_d$. □

The next lemma deals with the existence of roots in $w_m\Gamma_d$ of the quadratic polynomials $F_m^\pm(x) := x^2 \pm mx + m$, when m is either 2 or 3.

Lemma 5.20. *Assume m is either 2 or 3, and suppose $\mathcal{O}_{D/p}^{(p)}$ has a root of either $F_m^+(x)$ or $F_m^-(x)$. Then $w_m\Gamma_d$ has a root of either $F_m^+(x)$ or $F_m^-(x)$ if and only if s_mH_d contains a root of $F_m^+(x)$ (or, equivalently, of $F_m^-(x)$), where $s_m \in \mathbb{F}_{\ell^2}^\times$ is a square-root of m.*

Proof. First notice that since $\ell > 3$ every root of either $F_m^+(x)$ or $F_m^-(x)$ in $\mathcal{O}_{D/p}^{(p)}$ can be regarded locally at ℓ as an element in $\mathcal{O}_{D/p,\ell}^\times$, thus it can be mapped by ψ to $\mathbb{F}_{\ell^2}^\times$. Then one proves, as in Lemma 4.16, that assuming the existence of a root in $\mathcal{O}_{D/p}^{(p)}$ of either $F_m^+(x)$ or $F_m^-(x)$ is actually equivalent to assuming that $\mathcal{O}_{D/p}^{(p)}$ contains roots of $F_m^+(x)$ and $F_m^-(x)$ mapping under ψ to each of the four roots in

$\mathbb{F}_{\ell^2}^\times$ of $F_m^+(x)F_m^-(x)$. Finally, using that $\psi(\alpha_m) \in \mathbb{F}_{\ell^2}^\times$ is a square root of m in $\mathbb{F}_{\ell^2}^\times$ and $-1 \in H_d$, so that $\psi(\alpha_m)H_d = s_m H_d$, one checks that one of such roots belongs to $w_m\Gamma_d$ if and only if its image under ψ lies in $s_m H_d$. □

We are now in position to translate condition i) in Proposition 5.18 by using the previous lemmas:

Lemma 5.21. *Assume $f_d = 1$, $\varepsilon_d(m) = 1$ and $p \nmid m$, and let $s_3 \in \mathbb{F}_{\ell^2}^\times$ be a square root of 3 in $\mathbb{F}_{\ell^2}^\times$. Then condition i) in Proposition 5.18 holds if and only if $B_{D/p} \simeq (-m, -p)_{\mathbb{Q}}$ and the following two conditions are satisfied:*

a) *either $4 \mid t_d$ or $p = 3$, $6 \mid t_d$ and H_d has a root of $x^2 + 3x + 3 = 0$;*
b) *either $\ell \mid m$, or $4 \mid t_d$, or $m = 3$, $6 \mid t_d$ and $s_3 H_d$ has a root of $x^2 + 3x + 3 = 0$.*

Proof. Assume the hypotheses, and suppose first that condition i) in Proposition 5.18 holds, so that there is an edge $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$ such that $\ell_d(y)$ is odd (hence 1 or 3), $w_m(y) = y$ and $w_p(y) = \bar{y}$. Let $\tilde{y} \in \mathrm{Ed}(\mathcal{T}_p)$ be any edge above y, and set $\tilde{v} := o(\tilde{y})$.

As in the proof of Lemma 4.14, on the one hand there is an element $\beta_o \in \Gamma_d \cap \mathcal{O}_{\tilde{v}}$ with $\beta_o(\tilde{y}) = \bar{\tilde{y}}$ such that $\beta_o^2 = p u_\beta$, where $u_\beta \in \Gamma_d \cap \mathcal{O}_{\tilde{v}}^\times$. Since $\ell_d(y)$ is odd, we find out moreover that either $u_\beta = -1$ or $u_\beta^2 - u_\beta + 1 = 0$. The second option implies, moreover, that $6 \mid t_d$. It follows that either $\beta_o^2 + p = 0$ or $p = 3$ and $\beta_o^2 \pm 3\beta_o + 3 = 0$, thus by Lemmas 4.15 and 4.16 condition a) holds. Further, we can assume in the following that $\beta_o^2 + 3\beta_o + 3 = 0$ (replace β_o by $-\beta_o$, if necessary). On the other hand, there is an element $\gamma \in \Gamma_d$ such that $\gamma w_m(\tilde{y}) = \tilde{y}$. Writing $\alpha_o := \gamma w_m$, we see that $\alpha_o \in \mathcal{O}_{\tilde{v}} \cap w_m\Gamma_d$ satisfies $\alpha_o(\tilde{v}) = \tilde{v}$, hence also $\alpha_o^2(\tilde{v}) = \tilde{v}$. Similarly as in the proof of Lemma 4.14, we have $\alpha_o^2 = m u_\alpha$ for some $u_\alpha \in \Gamma_d \cap \mathcal{O}_{\tilde{v}}^\times$, and again using that $\ell_d(y) = 1$ or 3, we have in fact that either $u_\alpha = -1$ or $u_\alpha^2 - u_\alpha + 1 = 0$. The first case implies that $\alpha_o^2 + m = 0$, whereas in the second case it follows that $m = 3$, $6 \mid t_d$ and $\alpha_o^2 \pm 3\alpha_o + 3 = 0$, hence condition b) holds as well by virtue of Lemmas 5.19 and 5.20. Again, we assume henceforth that $\alpha_o^2 + 3\alpha_o + 3 = 0$.

Now it remains to prove that $B_{D/p} \simeq (-m, -p)_{\mathbb{Q}}$. Suppose first that $u_\beta = u_\alpha = -1$, and take $\alpha := \alpha_o$, $\beta := \beta_o$. Then $\alpha^2 = -m$ and $\beta^2 = -p$, thus the claim will follow if we prove that $\alpha\beta = -\beta\alpha$. Indeed, let $\gamma := \alpha^{-1}\beta\alpha \in \Gamma_d$. Then $\gamma^2 = -p$, so that $\mathbb{Q}(\gamma) = \mathbb{Q}(\beta) \simeq \mathbb{Q}(\sqrt{-p})$, and it follows that either $\gamma = \beta$ or $\gamma = -\beta$. The first option is excluded, since $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are two distinct quadratic subfields of $B_{D/p}$, hence $\gamma = -\beta$ and consequently our claim is proved.

Suppose now that $u_\beta = -1$, but $u_\alpha^2 - u_\alpha + 1 = 0$, thus in particular $m = 3$. Set $\beta := \beta_o$ and $\alpha := 2\alpha_o + 3$; we have $\beta^2 = -p$ and $\alpha^2 = -m = -3$. Defining as before $\gamma := \alpha^{-1}\beta\alpha$, we see that $\mathbb{Q}(\gamma) = \mathbb{Q}(\beta) \simeq \mathbb{Q}(\sqrt{-p})$, and again it follows that $\alpha\beta = -\beta\alpha$, hence $B_{D/p} \simeq (-m, -p)_{\mathbb{Q}}$. By symmetry, the case where $u_\alpha = -1$ and $u_\beta^2 - u_\beta + 1 = 0$ (thus $p = 3$) is done in the same way. And finally, notice that $u_\alpha \neq -1$ and $u_\beta \neq -1$ cannot occur simultaneously, since this would imply $p = m = 3$.

Conversely, suppose that $B_{D/p} \simeq (-m, -p)_{\mathbb{Q}}$ and both a) and b) hold. We have to prove that there is an edge $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$ of odd length such that $w_m(y) = y$ and $w_p(y) = \bar{y}$. Indeed, let $\alpha, \beta \in B_{D/p}$ be such that $\alpha^2 = -m$, $\beta^2 = -p$ and $\alpha\beta = -\beta\alpha$, and choose a maximal order $\mathcal{O}_{\tilde{v}}$ containing α and β, for some vertex $\tilde{v} \in \mathrm{Ver}(\mathcal{T}_p)$. First we use condition a). By Corollary 4.17, Γ_d contains a root β_o of some equation in $\mathcal{F}_{p,d}$. Indeed, if $4 \mid t_d$, then it follows from Lemma 4.15 that $\beta \in \Gamma_d$: in this case, let us just write $\beta_o := \beta$. Otherwise, $p = 3$ and H_d contains a root of $x^2 + 3x + 3 = 0$. As in Lemma 4.16, the elements $(\beta - 3)/2, (-\beta - 3)/2 \in \mathcal{O}_{D/3}^{(3)\times}$ are roots of $x^2 + 3x + 3 = 0$, mapping to the two roots of $x^2 + 3x + 3 = 0$ in $\mathbb{F}_{\ell^2}^\times$. Since one of them is in H_d either $(\beta - 3)/2$ or $(-\beta - 3)/2$ lies in Γ_d: set $\beta_o := (\beta - 3)/2$ or $\beta_o := (-\beta - 3)/2$ accordingly. In any case, $\beta_o \in \Gamma_d$ is a root of an equation in $\mathcal{F}_{p,d}$. Thus if we set $\tilde{v}' := \beta_o(\tilde{v})$ and $\tilde{y}$ denotes the edge from $\tilde{v}$ to $\tilde{v}'$, then $\beta_o(\tilde{y}) = \bar{\tilde{y}}$ by Lemma 4.14 (actually, β_o acts like w_p on $\mathcal{G}_{d,+}$). As a consequence, if y denotes the image of $\tilde{y}$ in $\mathcal{G}_{d,+}$, then $w_p(y) = \bar{y}$. Since $Y_d(\mathbb{Q}_p)$ is empty by hypothesis, the length of y is necessarily odd.

Secondly, we use now condition b). If $\ell \mid m$ or $4 \mid t_d$, then by Lemma 5.19 we have that $\alpha \in w_m\Gamma_d$. In this case, set $\alpha_o := \alpha$. Otherwise, if $m = 3$ and $s_3 H_d$ has a root of $x^2 + 3x + 3 = 0$, similarly as before one of the elements $(\alpha - 3)/2$, $(-\alpha - 3)/2 \in \mathcal{O}_{D/p}^{(p)}$ lies actually in $w_m\Gamma_d$: we write α_o for any of them satisfying this condition, and notice that α_o is a root of $x^2 + 3x + 3 = 0$. In any case, the element α_o induces the same action as w_m on the graph $\mathcal{G}_{d,+}$, because $p \nmid m$. Therefore, it remains to prove that $w_m(y) = y$, which amounts to proving that the edge $\alpha_o(\tilde{y}) \in \mathrm{Ed}(\mathcal{T}_p)$ lies above y. First of all, observe that locally at p we have $\alpha_o \in \mathcal{O}_{\tilde{v},p}^\times$, so that $\alpha_o(\tilde{v}) = \tilde{v}$. Thus it is enough to prove that $\alpha_o(\tilde{v}')$ is a vertex above the end vertex of y, i.e. above the same vertex as $\tilde{v}'$. For doing so, we translate the relation $\alpha\beta = -\beta\alpha$ into a relation between $\alpha_o\beta_o$ and $\beta_o\alpha_o$, depending on the expression of α_o and β_o in terms of α and β, respectively. The details can be done case by case:

1) Suppose that $\alpha_o = \alpha$ and $\beta_o = \beta$. Then we have clearly $\alpha_o\beta_o = -\beta_o\alpha_o$. As a consequence,
$$\alpha_o(\tilde{v}') = \alpha_o\beta_o(\tilde{v}) = -\beta_o\alpha_o(\tilde{v}) = \beta(\tilde{v}) = \tilde{v}',$$
and therefore $\alpha_o(\tilde{y}) = \tilde{y}$, which obviously implies our claim.
2) Now suppose that $m = 3$ and $\alpha_o := (\pm\alpha - 3)/2$. Then α_o satisfies the quadratic equation $\alpha_o^2 + 3\alpha + 3 = 0$. In particular, observe that $\mathrm{tr}(\alpha_o) = -3$ and $\mathrm{n}(\alpha_o) = 3$. Since $p \nmid m$, in this case we necessarily have $\beta_o = \beta$. Then from the relation $\alpha\beta = -\beta\alpha$ it follows that
$$\alpha_o\beta_o = \frac{1}{2}(\pm\alpha - 3)\beta = \frac{1}{2}(\pm\alpha\beta - 3\beta) = \frac{1}{2}(\mp\beta\alpha - 3\beta) = -\beta_o\alpha_o + 3\beta_o = -\beta_o(\alpha_o + 3).$$
But notice that $\mathrm{n}(\alpha_o + 3) = 3$, so that $\alpha_o + 3 \in \mathcal{O}_{\tilde{v},p}^\times$ fixes $\tilde{v}$. Therefore,
$$\alpha_o(\tilde{v}') = \alpha_o\beta_o(\tilde{v}) = -\beta_o(\alpha_o + 3)(\tilde{v}) = \beta_o(\tilde{v}) = \tilde{v}',$$
and again this implies that $\alpha_o(\tilde{y}) = \tilde{y}$ as we wanted.
3) When $p = 3$ and $\beta_o := (\pm\beta - 3)/2 \in \Gamma_d$, one can proceed in the same way as in 2), we leave the details to the reader.

□

Condition ii) in Proposition 5.18 is translated into a very explicit condition in Lemma 5.23 below. In its proof, we use the following lemma, which is proved in the same way as Lemma 5.19 by using that the assumption $f_d = 1$ implies that H_d contains the square roots in $\mathbb{F}_{\ell^2}^\times$ of p mod ℓ.

Lemma 5.22. *Let $\alpha \in \mathcal{O}_{D/p}^{(p)}$ be a solution of $x^2 + mp = 0$. If $\ell \mid m$, then $\alpha \in w_m\Gamma_d$, whereas if $\ell \nmid m$, then $\alpha \in w_m\Gamma_d$ if and only if $4 \mid t_d$.*

Lemma 5.23. *Assume $f_d = 1$, $\varepsilon_d(m) = 1$ and $p \nmid m$. Then condition ii) in Proposition 5.18 holds if and only if $4 \mid t_d$ and $B_{D/p} \simeq (-mp, -1)_{\mathbb{Q}}$.*

Proof. Assume the hypotheses, and suppose that condition ii) in Proposition 5.18 holds, so that there is an edge $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$ of length 2 such that $w_pw_m(y) = \bar{y}$. Choose an edge $\tilde{y} \in \mathrm{Ed}(\mathcal{T}_p)$ above y, and let $\tilde{v} := o(y)$. Since $\ell_d(y) = 2$, there is an element $\beta \in \Gamma_d \cap \mathcal{O}_{\tilde{v}}^\times$ such that $\beta^2 + 1 = 0$. This implies, in particular, that $4 \mid t_d$. On the other hand, since $w_pw_m(y) = \bar{y}$, there is an element $\gamma \in \Gamma_d$ such that $\gamma w_m(\tilde{y}) = \bar{\tilde{y}}$, thus $(\gamma w_m)^2(\tilde{y}) = \tilde{y}$. Write $\alpha := \gamma w_m$, and observe that $\alpha \in \mathcal{O}_{\tilde{v}} \cap w_m\Gamma_d$ normalises Γ_d. Besides, since w_m normalises Γ_d and $w_m^2 \in m\Gamma_d$, we have that $\alpha^2 = m\gamma'$ for some $\gamma' \in \Gamma_d$. Now, since $p \nmid m$ and $\mathrm{dist}(\alpha(\tilde{v}), \tilde{v}) = 1$, we deduce that $\mathrm{val}_p(\mathrm{n}(\gamma'))$ is odd, thus as in the proof of Lemma 4.14 we can assume it is 1. Then we can write $\alpha^2 = pmu$ for some $u \in \mathcal{O}_{\tilde{v}}^\times$, but observe that $\mathcal{O}_{\tilde{v}}^\times/\mathbb{Z}^\times = \{[1], [\beta]\}$. If it were $u = \pm\beta$, we would have $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$, and this is not possible. Therefore, $u = \pm 1$, and since $B_{D/p}$ is definite, the only option is $u = -1$ and this implies that $\alpha^2 = -pm$. Finally, observe that $\alpha^{-1}\beta\alpha$ fixes $\tilde{y}$, hence in particular $\alpha^{-1}\beta\alpha \in \mathcal{O}_{\tilde{v}}^\times$. Since $\beta \neq \pm 1$, it follows that $\alpha^{-1}\beta\alpha = \pm\beta$. But $\alpha^{-1}\beta\alpha = \beta$ is not possible, hence we have $\alpha\beta = -\beta\alpha$, and we conclude that $B_{D/p} \simeq (-1, -pm)_{\mathbb{Q}}$.

Conversely, assume that $4 \mid t_d$ and $B_{D/p} = (-mp, -1)_{\mathbb{Q}}$, and choose elements $\alpha, \beta \in B_{D/p}$ satisfying $\alpha^2 = -pm$, $\beta^2 = -1$ and $\alpha\beta = -\beta\alpha$. We can also choose a maximal order $\mathcal{O}_{\tilde{v}}$ containing α and β for some vertex $\tilde{v} \in \mathrm{Ver}(\mathcal{T}_p)$. Let $\tilde{v}' := \alpha(\tilde{v})$ (which is at distance 1 from $\tilde{v}$), $\tilde{y}$ be the edge from $\tilde{v}$ to $\tilde{v}'$ and v, y be their images in $\mathcal{G}_{d,+}$, respectively. Since $4 \mid t_d$, the element β actually lies in Γ_d (one can argue as in the proof of Lemma 4.7, for example), and we deduce that $\mathrm{Stab}_{\Gamma'_{d,+}}(\tilde{v}) = \{[1], [\beta]\}$, hence $\ell_d(v) = 2$. On the other hand, $\beta(\tilde{v}') = \beta\alpha(\tilde{v}) = -\alpha\beta(\tilde{v}) = \alpha(\tilde{v}) = \tilde{v}'$, thus β fixes $\tilde{y}$ as well, hence $\ell_d(y) = 2$. Finally, $\alpha(\tilde{y}) = \bar{\tilde{y}}$, and from Lemma 5.22 we have $\alpha \in w_m\Gamma_d$ because $4 \mid t_d$. This implies that $w_m(y') = \bar{y}'$, where y' is the image of y in $\mathcal{G}_d$, which means that either $w_m(y) = \bar{y}$ or $w_pw_m(y) = \bar{y}$. But since $p \nmid m$, the first option cannot occur, so that $w_pw_m(y) = \bar{y}$. Therefore, condition ii) in Proposition 5.18 is satisfied. □

As a direct consequence of Proposition 5.18 together with Lemmas 5.21 and 5.23, we conclude with the following criterion for the existence of $\mathbb{Q}_p$-rational points on $Y_d^{(m)}$, which accounts for part 1) of Theorem 1.3. Notice that condition i) is indeed equivalent to the conditions in Lemma 5.21, since $p = 3$ and $m = 3$ cannot hold simultaneously.

Theorem 5.24. *Assume $f_d = 1$, $\varepsilon_d(m) = 1$ and $p \nmid m$. If $Y_d(\mathbb{Q}_p) = \emptyset$, then the set $Y_d^{(m)}(\mathbb{Q}_p)$ is not empty if and only if one of the following conditions holds:*
i) *$B_{D/p} \simeq (-m, -p)_{\mathbb{Q}}$, and either*
  a) *$4 \mid t_d$, or*
  b) *$p = 3$, $\ell \mid m$, $6 \mid t_d$ and H_d contains a root of $x^2 + 3x + 3 = 0$.*
ii) *$B_{D/p} \simeq (-mp, -1)_{\mathbb{Q}}$ and $4 \mid t_d$.*

Corollary 5.25. *Assume $f_d = 1$, $\varepsilon_d(m) = 1$, $p \nmid m$ and $Y_d(\mathbb{Q}_p) = \emptyset$. If $4 \nmid t_d$ and $p \neq 3$, then $Y_d^{(m)}(\mathbb{Q}_p) = \emptyset$.*

5.4. **$\mathbb{Q}_p$-rational points on $Y_d^{(pm)}$.** Lastly, we discuss the existence of $\mathbb{Q}_p$-rational points on the quotients of Y_d by lifted Atkin-Lehner involutions of the form $\hat{\omega}_{pm}$, where $m \mid D/p$ and $m > 1$. As above, we assume $f_d = 1$ and $\varepsilon_d(pm) = 1$. By Lemma 5.7 observe that our assumption is equivalent to $f_d = 1$ and $\varepsilon_d(m) = 1$. Similarly as before, $\hat{\omega}_{pm}$ induces an action on each copy of $\mathcal{Y}_{\Gamma_d}$ in (22), and the set $Y_d^{(pm)}(\mathbb{Q}_p)$ is non-empty if and only if $\mathcal{Y}_{\Gamma_d}^{(pm)}(\mathbb{Q}_p)$ is non-empty.

Now, since $\hat{\omega}_{pm} = \hat{\omega}_p\hat{\omega}_m = \hat{\omega}_m\hat{\omega}_p$, its action on $\mathcal{Y}_{\Gamma_d}$ is induced by the action of w_pw_m (or w_mw_p) on $\widehat{\mathcal{H}}_p$. Besides, the action of $\hat{\omega}_{pm}$ on the graph $\mathcal{G}_{d,+} = \Gamma_{d,+} \setminus \mathcal{T}_p$ is naturally induced by the action of w_pw_m on $\mathcal{T}_p$, so we are lead to consider the finite graph with lengths

$$\mathcal{G}_{d,+}^{(pm)} := \langle \Gamma_{d,+}, w_pw_m \rangle \setminus \mathcal{T}_p.$$

In contrast to the case of $\mathcal{G}_{d,+}^{(m)}$ (with $p \nmid m$), where it holds that $\mathcal{G}_{d,+}^{(m)*} = \mathcal{G}_{d,+}^{(m)}$, now it might be the case that $\mathcal{G}_{d,+}^{(pm)*} \neq \mathcal{G}_{d,+}^{(pm)}$, because $\mathcal{G}_{d,+}^{(pm)}$ can have edges y with $\bar{y} = y$. Thus $\mathcal{G}_{d,+}^{(pm)}$ is not necessarily the dual graph of $\mathcal{Y}_{\Gamma_d}^{(pm)}$.

Lemma 5.26. *Let $m > 1$ be a divisor of D/p, and assume that $f_d = 1$, $Y_d(\mathbb{Q}_p) = \emptyset$ and $\varepsilon_d(m) = 1$. Then $Y_d^{(pm)}(\mathbb{Q}_p)$ is not empty if and only if there exists a vertex v in $\mathcal{G}_{d,+}$ such that $w_m(v) = v$.*

Proof. Suppose first that $Y_d^{(pm)}(\mathbb{Q}_p)$ is non-empty, hence so is $\mathcal{Y}_{\Gamma_d}^{(pm)}(\mathbb{Q}_p)$. Therefore, there is a vertex $x \in \mathrm{Ver}(\widetilde{\mathcal{G}}_{d,+}^{(pm)})$ such that $w_p(x) = x$. If x was already a vertex of $\mathcal{G}_{d,+}^{(pm)}$, then a preimage v of x in $\mathcal{G}_{d,+}$ would satisfy either $w_p(v) = v$ or $w_p(v) = w_pw_m(v)$. The first option is not possible because w_p fixes no vertex in $\mathcal{G}_{d,+}$, hence $w_p(v) = w_pw_m(v)$, and as a consequence $v = w_m(v)$.

Otherwise, the vertex x has appeared during the resolution of singularities. This implies that $\mathcal{G}_{d,+}^{(pm)}$ has an edge y of even length such that $w_p(y) = \bar{y}$. Now we claim that if y has two distinct preimages y_1 and $y_2 = w_pw_m(y_1)$ in $\mathcal{G}_{d,+}$, then we have the same situation for both y_1 and y_2. Indeed, the length of both y_1 and y_2 equals the length of y in $\mathcal{G}_{d,+}^{(pm)}$, as the natural projection is not ramified at y, and the identity $w_p(y) = \bar{y}$ implies that for $i = 1, 2$ we have either $w_p(y_i) = \bar{y}_i$ or $w_p(y_i) = \overline{w_pw_m(y_i)} = w_pw_m(\bar{y}_i)$. But since $p \nmid m$, the second option is not possible[2]. Then both y_1 and y_2 are edges of even length in $\mathcal{G}_{d,+}$ such that $w_p(y_1) = \bar{y}_1$ and $w_p(y_2) = \bar{y}_2$ as claimed. But this contradicts our assumption that $Y_d(\mathbb{Q}_p)$ is empty. Therefore we may assume that y has a unique preimage z in $\mathcal{G}_{d,+}$ (i.e., w_pw_m is ramified at y). But this means that $w_pw_m(z) = z$, which again is not possible because $p \nmid m$.

Conversely, assume there is a vertex $v \in \mathcal{G}_{d,+}$ such that $w_m(v) = v$. Then the image x of v in $\mathcal{G}_{d,+}^{(pm)}$ is fixed by w_p. Therefore, $\mathcal{Y}_{\Gamma_d}^{(pm)}(\mathbb{Q}_p)$, hence $Y_d^{(pm)}(\mathbb{Q}_p)$, is non-empty, except possibly if the vertex x is the origin of $p + 1$ edges y such that $w_p(y) = \bar{y}$. Let us work out this case.

Assume that x is in fact the origin of $p + 1$ edges y such that $w_p(y) = \bar{y}$. First we claim that if this is the case then the vertex v is the origin of $p + 1$ edges z such that $w_m(z) = z$. Indeed, write $v' := w_p(v)$, and notice that $v' = w_pw_m(v)$, so that v and v' are the two distinct preimages of x in $\mathcal{G}_{d,+}$. Observe that since x is the origin of $p + 1$ edges, then x has trivial length, and as a consequence every edge y emanating from x has trivial length as well. In particular, every edge $y \in \mathrm{Star}(x)$ has two distinct preimages of trivial length in $\mathcal{G}_{d,+}$, one in $\mathrm{Star}(v)$ and the other one in $\mathrm{Star}(v')$. Fix an edge $y \in \mathrm{Star}(x)$, and let z be the unique edge in $\mathrm{Star}(v)$ above y. Since we are assuming $w_p(y) = \bar{y}$, we deduce that either $w_p(z) = \bar{z}$ or $w_p(z) = \overline{w_pw_m(z)} = w_pw_m(\bar{z})$. The latter is not possible because $p \nmid m$, hence it is $w_p(z) = \bar{z}$. Besides, $w_m(z)$ maps to the same edge as $w_p(z) = \bar{z}$. Therefore, either $w_m(z) = \bar{z}$ or $w_m(z) = w_pw_mw_m(\bar{z}) = w_p(\bar{z}) = z$. Again, the first option is excluded because $p \nmid m$, so that $w_m(z) = z$. The same argument applies for every edge $y \in \mathrm{Star}(x)$, thus our claim is proved. Secondly, our claim implies in turn that w_m fixes every vertex of $\mathcal{G}_{d,+}$ at distance 1 of v. Being $\mathcal{G}_{d,+}$ connected, this implies that w_m acts trivially on $\mathcal{G}_{d,+}$. Therefore, if we write g_d (resp. $g_d^{(m)}$) for the genus of $\mathcal{Y}_{\Gamma_d}$ (resp. $\mathcal{Y}_{\Gamma_d}^{(m)}$), then it follows that $g_d = g_d^{(m)}$, and by applying the Riemann-Hurwitz formula, we deduce that $g_d \geq (g_d + 1)/2$, hence g_d is either 0 or 1. But this implies that there is some vertex in $\mathcal{G}_{d,+}$

[2]The graph $\mathcal{G}_{d,+}$ is bipartite: its set of vertices admits a decomposition as a disjoint union of two sets of vertices V_d^1, V_d^2, of the same cardinality, and there is no edge between vertices in the same set V_d^i. Further, $w_p(V_d^1) = V_d^2$ and $w_p(V_d^2) = V_d^1$, whereas $w_m(V_d^i) = V_d^i$ for $i = 1, 2$, because $p \nmid m$. Then for every edge $y \in \mathrm{Ed}(\mathcal{G}_{d,+})$, if $o(y) \in V_d^1$ then $o(w_p(y)) \in V_d^2$ and $o(w_pw_m(\bar{y})) \in V_d^1$, so that $w_p(y)$ and $w_pw_m(\bar{y})$ cannot be the same edge (and analogously if $o(y) \in V_d^2$).

which has less than $p+1$ edges emanating from it, and therefore its image in $\mathcal{G}_{d,+}^{(pm)}$ is a vertex fixed by w_p and with less than $p+1$ edges in its star, thus by Hensel's Lemma $\mathcal{Y}_{\Gamma_d}^{(pm)}(\mathbb{Q}_p)$ is not empty. Indeed, if every vertex of $\mathcal{G}_{d,+}$ were the origin of $p+1$ edges, then every vertex in $\mathcal{G}_{d,+}$ would have degree $p+1$, and we would have that

$$|\operatorname{Ver}(\mathcal{G}_{d,+})|(p+1) = 2|\operatorname{Ed}(\mathcal{G}_{d,+})|.$$

But on the other hand we know that the genus g_d of $\mathcal{Y}_{\Gamma_d}$ satisfies the relation $1-g_d = |\operatorname{Ver}(\mathcal{G}_{d,+})| - |\operatorname{Ed}(\mathcal{G}_{d,+})|$. And when g_d is either 0 or 1, this is not compatible with the above relation. □

Next we translate the existence of a vertex in $\mathcal{G}_{d,+}$ fixed by w_m into the existence of solutions in $w_m\Gamma_d$ of certain quadratic equations. We do this in the following lemma, where $\mathcal{F}_{m,d}$ denotes the set of quadratic equations defined in the same way as we defined $\mathcal{F}_{p,d}$ in (26) replacing p by m.

Lemma 5.27. *Let $m>1$ be a divisor of D/p, and assume that $f_d = 1$ and $\varepsilon_d(m) = 1$. Then there is a vertex $v \in \operatorname{Ver}(\mathcal{G}_{d,+})$ such that $w_m(v) = v$ if and only if there exists an element $\alpha \in w_m\Gamma_d$ satisfying some quadratic equation in $\mathcal{F}_{m,d}$.*

Proof. Suppose there is a vertex $v \in \operatorname{Ver}(\mathcal{G}_{d,+})$ fixed by w_m, and let $\tilde{v} \in \operatorname{Ver}(\mathcal{T}_p)$ be a vertex above v. Then there is an element $\gamma \in \Gamma_d$ such that $\gamma w_m(\tilde{v}) = \tilde{v}$. Writing $\alpha = \gamma w_m \in \Gamma_d w_m = w_m\Gamma_d$, we have $\alpha(\tilde{v}) = \tilde{v}$. In particular, $\alpha^2(\tilde{v}) = \tilde{v}$ as well, but notice that $\alpha^2 = \gamma w_m \gamma w_m = w_m^2\gamma' = mu$ for some elements $\gamma', u \in \Gamma_d$, where we have used that $w_m^2 \in m\Gamma_d$. But therefore u fixes $\tilde{v}$ as well, because m acts trivially on $\mathcal{T}_p$. Then $u \in \operatorname{Stab}_{\Gamma_d}(\tilde{v}) = \mathcal{O}_{\tilde{v}}^\times$, and it thus follows that either $u = \pm 1$, $u^2+1 = 0$ or $u^2 \pm u + 1 = 0$. As in the proof of Lemma 4.14, we deduce that one of the following holds:

i) $u=-1$ and $\alpha^2 + m = 0$,
ii) $u^2+1 = 0$, $m = 2$, $4 \mid t_d$ and $\alpha^2 \pm 2\alpha + 2 = 0$,
iii) $u^2 - u + 1 = 0$, $m = 3$, $6 \mid t_d$ and $\alpha^2 \pm 3\alpha + 3 = 0$.

And this implies that α is a root of some equation in $\mathcal{F}_{m,d}$.

Conversely, assume that there exists a root α of some equation in $\mathcal{F}_{m,d}$ such that $\alpha \in w_m\Gamma_d$. Since $w_m\Gamma_d \subseteq \mathcal{O}_{D/p}$, we can choose a maximal order $\mathcal{O}_{\tilde{v}}$ corresponding to some vertex $\tilde{v}$ of $\mathcal{T}_p$ such that $\alpha \in \mathcal{O}_{\tilde{v}}$. But now notice that $\operatorname{n}(\alpha) = m$, and since $p \nmid m$ this implies that α is invertible in $\mathcal{O}_{\tilde{v}}$, thus it fixes $\tilde{v}$. In particular, writing $\alpha = \gamma w_m$ for some $\gamma \in \Gamma_d$ (recall that $w_m\Gamma_d = \Gamma_d w_m$), it follows that $\gamma w_m(\tilde{v}) = \tilde{v}$. If v denotes the image of $\tilde{v}$ in $\mathcal{G}_{d,+}$, then v is fixed by w_m. □

Finally, we conclude with the following criterion for the existence of $\mathbb{Q}_p$-rational points on $Y_d^{(pm)}$, which corresponds to part 2) of Theorem 1.3. It is a direct consequence of the previous lemmas: indeed, one only has to translate the existence of solutions in $w_m\Gamma_d$ of equations in the set $\mathcal{F}_{m,d}$ into explicit conditions by using Lemmas 5.19 and 5.20:

Theorem 5.28. *Let $m>1$ be a divisor of D/p, and assume that $f_d = 1$, $Y_d(\mathbb{Q}_p) = \emptyset$ and $\varepsilon_d(m) = 1$. Then $Y_d^{(pm)}(\mathbb{Q}_p)$ is not empty if and only if any of the following conditions holds:*

i) *$\mathbb{Q}(\sqrt{-m})$ splits $B_{D/p}$, and either*
   a) *$\ell \mid m$ or $4 \mid t_d$, or*
   b) *$m = 3$, $6 \mid t_d$ and s_3H_d contains a root of $x^2+3x+3 = 0$, where $s_3 \in \mathbb{F}_{\ell^2}^\times$ is a square root of 3.*
ii) *$m = 2$, $4 \mid t_d$, $\mathbb{Q}(\sqrt{-1})$ splits $B_{D/p}$ and s_2H_d contains a root of $x^2+2x+2=0$, where s_2 is a square root of 2 in $\mathbb{F}_{\ell^2}^\times$.*

Acknowledgements. It is a pleasure to thank Prof. Víctor Rotger for his guidance and advice through the elaboration of this work, and also to Prof. Matteo Longo for helpful conversations during my pleasant stay at the Università degli Studi di Padova in the spring of 2013.

References

[BC91] J.-F. Boutot, H. Carayol, Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld, *Astérisque* **196-197** (1991), 45-158.

[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.

[Dri76] V. G. Drinfeld, Coverings of p-adic symmetric regions, *Functional Analysis and its Applications* **10**(2) (1976), 29-40.

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

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

[Kur79] A. Kurihara, On some examples of equations defining Shimura curves and the Mumford uniformization, *J. Fac. Sci. Univ. Tokyo, Sec. IA* **25** (1979), 277-301.

[LRdVP] M. Longo, V. Rotger, C. de Vera-Piquero, Étale coverings of Drinfeld's p-adic half-plane and the effective computation of Heegner points, in progress.

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

[Mum72] D. Mumford, An analytic construction of degenerating curves over complete local rings, *Compositio Math.* **24** (1972), 129-174.

[Ogg85] A. P. Ogg, Mauvaise réduction des courbes de Shimura, *Séminaire de théorie des nombres*, Progress in Math. **59**, Birkäuser, 1985, 199-217.

[RdVP] V. Rotger, C. de Vera-Piquero, Galois representations over fields of moduli and rational points on Shimura curves, *Canad. J. Math.* **66** (2014), 1167-1200.

[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. of Math.* **85** (1967), 58-159.

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

[Te90] J. Teitelbaum, Geometry of an étale covering of the p-adic upper half plane, *Ann. Inst. Fourier* **40** (1990), no. 1, 69-78.

[dVP13] C. de Vera-Piquero, The Shimura covering of a Shimura curve: automorphisms and étale subcoverings, J. Number Theory **133**(10) (2013), 3500-3516.

[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 Math. **800**, 1980.

Fakultät für Mathematik, Universität Duisburg-Essen, Essen, Germany
E-mail address: `carlos.de-vera-piquero@uni-due.de`
URL: `https://www.uni-due.de/~adf538d/`