ALGEBRA AND NUMBER THEORY 14:10 (2020)
https://doi.org/10.2140/ant.2020.14.2713

An intriguing hyperelliptic Shimura curve quotient of genus 16

Lassina Dembélé

Let F be the maximal totally real subfield of $\mathbb{Q}(\zeta_{32})$, the cyclotomic field of 32-nd roots of unity. Let D be the quaternion algebra over F ramified exactly at the unique prime above 2 and 7 of the real places of F. Let $\mathcal{O}$ be a maximal order in D, and $X_0^D(1)$ the Shimura curve attached to $\mathcal{O}$. Let $C = X_0^D(1)/\langle w_D\rangle$, where w_D is the unique Atkin–Lehner involution on $X_0^D(1)$. We show that the curve C has several striking features. First, it is a hyperelliptic curve of genus 16, whose hyperelliptic involution is exceptional. Second, there are 34 Weierstrass points on C, and exactly half of these points are CM points; they are defined over the Hilbert class field of the unique CM extension E/F of class number 17 contained in $\mathbb{Q}(\zeta_{64})$, the cyclotomic field of 64-th roots of unity. Third, the normal closure of the field of 2-torsion of the Jacobian of C is the Harbater field N, the unique Galois number field $N/\mathbb{Q}$ unramified outside 2 and ∞, with Galois group $\mathrm{Gal}(N/\mathbb{Q}) \simeq F_{17} = \mathbb{Z}/17\mathbb{Z} \rtimes (\mathbb{Z}/17\mathbb{Z})^\times$. In fact, the Jacobian $\mathrm{Jac}(X_0^D(1))$ has the remarkable property that each of its simple factors has a 2-torsion field whose normal closure is the field N. Finally, and perhaps the most striking fact about C, is that it is also hyperelliptic over $\mathbb{Q}$.

1. Introduction

Let F be the maximal totally real subfield of $\mathbb{Q}(\zeta_{32})$, the cyclotomic field of 32-nd roots of unity. Recall that 2 is totally ramified in F, and let $\mathfrak{p}$ be the unique prime above it. Let D be the quaternion algebra defined over F ramified exactly at $\mathfrak{p}$ and 7 of the real places of F. Let $\mathcal{O}$ be a maximal order in D, and $X_0^D(1)$ the Shimura curve attached to $\mathcal{O}$. Let $C = X_0^D(1)/\langle w_D\rangle$, where w_D is the unique Atkin–Lehner involution on $X_0^D(1)$. Let $\mathrm{Jac}(X_0^D(1))$ and $\mathrm{Jac}(C)$ be the Jacobians of $X_0^D(1)$ and $\mathrm{Jac}(C)$, respectively. In this note, we show that C has several striking properties. First, we prove the following theorem (Theorem 5.13).

Theorem A. *The curve C is a hyperelliptic curve of genus* 16 *defined over* $\mathbb{Q}$.

We first show that C is hyperelliptic over F (Theorem 5.9), then we apply a descent argument from [Sijsling and Voight 2016] to show that both the curve and the hyperelliptic involution are defined over $\mathbb{Q}$. For the first part, we simply count the number of Weierstrass points on C. This count yields that C has 34 Weierstrass points, the maximum number for a hyperelliptic curve of genus 16 by the Weierstrass gap

The author was supported by EPSRC Grants EP/J002658/1 and EP/L025302/1, a Visiting grant from the Max-Planck Institute for Mathematics, and a Simons Collaboration Grant (550029).
MSC2010: primary 11F41; secondary 11F80.
Keywords: abelian varieties, Hilbert modular forms, Shimura curves.

theorem. Half of those Weierstrass points are CM points defined over the Hilbert class field of the unique CM extension E/F of class number 17 contained in $\mathbb{Q}(\zeta_{64})$, the cyclotomic field of 64-th roots of unity.

To show that C is in fact defined over $\mathbb{Q}$, we determine the automorphism group $\mathrm{Aut}(C)$ of C as a curve over F. We do this by exploiting the Čerednik–Drinfel'd 2-adic uniformisation of $X_0^D(1)$ and the fact that the automorphism group of a stable curve injects into an *admissible* subgroup of the automorphism group of its dual graph (see [Deligne and Mumford 1969] and Section 4F for the definition of admissibility). A careful study of the dual graph of the stable model of C over the completion of F at $\mathfrak{p}$ then yields that $\mathrm{Aut}(C) = \mathbb{Z}/2\mathbb{Z}$. As a result, we get that the *only* nontrivial automorphism of C is the hyperelliptic involution, which in this case must be exceptional since the curve C is obtained as the quotient of $X_0^D(1)$ by the unique Atkin–Lehner involution w_D.

Our second result concerns the field of 2-torsion of $\mathrm{Jac}(C)$. It is known that 17 is the smallest odd integer which can occur as the degree of a number field $K/\mathbb{Q}$ for which 2 is the only finite prime which ramifies. That there is no such integer less than 17 follows from [Jones 2010]. On the other hand, Harbater [1994] proved that there is a unique Galois number field $N/\mathbb{Q}$ unramified outside 2 and ∞, with Galois group $\mathrm{Gal}(N/\mathbb{Q}) \simeq F_{17} = \mathbb{Z}/17\mathbb{Z} \rtimes (\mathbb{Z}/17\mathbb{Z})^\times$. So, the fixed field of the Sylow 2-subgroup of F_{17} is a number field of degree 17 in which 2 is the only ramified finite prime. Noam Elkies provided a degree 17 polynomial whose splitting field is N. The computation which led to that polynomial stemmed from a discussion on `mathoverflow.net` [Rouse and Elkies 2014] initiated by Jeremy Rouse. In the context of that discussion, it is natural to ask whether there is a curve defined over $\mathbb{Q}$, with good reduction away from 2, whose field of 2-torsion is the Harbater field N. The following theorem provides an affirmative answer to that question (Theorem 6.1).

Theorem B. *The field of* 2*-torsion of* $\mathrm{Jac}(C)$ *is the Harbater field* N*.*

The fact that the Harbater field can be realised as the field of 2-torsion of a *hyperelliptic* curve of rather large genus, with good reduction outside 2, seems rather remarkable to us. For that reason, we think that it would be very interesting to find a defining equation for C over $\mathbb{Q}$. This is a question of independent interest that we hope to consider in the future.

In fact, we prove a slightly stronger result than Theorem B. Namely, up to isogeny, the Jacobian $\mathrm{Jac}(X_0^D(1))$ decomposes as the product of four abelian varieties of dimension 4 and one of dimension 24. We give two different proofs of the following (Theorem 6.4).

Theorem C. *Let* A *be a simple factor of* $\mathrm{Jac}(X_0^D(1))$*. Then the normal closure of the field of* 2*-torsion of* A *is the Harbater field* N*.*

The second proof of Theorem C uses congruences. Namely, let $S_2^D(1)$ be the space of automorphic forms of level (1) and weight 2 over the quaternion algebra D, and $\mathbb{T}$ be the Hecke algebra acting on $S_2^D(1)$. We show that there are two congruence classes modulo 2 among the newforms in $S_2^D(1)$, whose associated mod 2 residual Galois representations have the same image D_{17}. These two congruence classes are permuted by $\mathrm{Gal}(F/\mathbb{Q})$. As a result, we get that the normal closure of the field of 2-torsion of every simple factor of $\mathrm{Jac}(X_0^D(1))$ is the Harbater field N. Interestingly, the existence of these two *distinct*

congruence classes modulo 2 turns out to have the following amusing consequence: the connectedness of Spec($\mathbb{T}$), which is obtained by an argument à la Mazur [1977, Proposition 10.6], *cannot* arise from a single congruence modulo 2. In other words, the existence of the Harbater field as the normal closure of the field of 2-torsion of $\mathrm{Jac}(X_0^D(1))$ is an obstruction to the connectedness of Spec($\mathbb{T}$) being achieved via a unique congruence modulo 2. This is due to the tautological reason that the semidirect product $F_{17} = D_{17} \rtimes \mathbb{Z}/8\mathbb{Z}$ is *nonsplit*. In fact, we show that the connectedness of Spec($\mathbb{T}$) is given by two different congruences modulo 3 and 5.

Our initial interest in the curve $X_0^D(1)$ stems from a conjecture of Benedict H. Gross which states that, for any prime p, there is a nonsolvable number field $K/\mathbb{Q}$ ramified at p (and possibly at ∞) only. In [Dembélé 2009], we proved that conjecture for $p = 2$ by using Hilbert modular forms of level (1) and weight 2 over F. Theorem C implies that none of the simple factors of $\mathrm{Jac}(X_0^D(1))$ has a 2-torsion field that can be used to provide an affirmative answer to the Gross conjecture for number fields given that N is solvable. Amusingly, it turns out that the simple factors of $\mathrm{Jac}(X_0^D(1))$ are more interesting in relation to other conjectures of Gross [2016] which concern modularity of abelian varieties not of GL_2-type. Indeed, functorially, these simple factors are related to abelian varieties defined over $\mathbb{Q}$ with *small* or even trivial endomorphism rings, but which acquire extra endomorphisms over F, as we explain later (see also [Cunningham and Dembélé 2017]).

The outline of the paper is as follows. In Section 2, we recall the necessary background on Weierstrass points and hyperellipticity. In Section 3, we recall the necessary background on arithmetic groups in quaternion algebras, and compliment this by discussing optimal embeddings into maximal arithmetic Fuchsian groups. In Section 4, we review the theory of Shimura curves, especially their p-adic uniformisation. Finally, in Sections 5 and 6, we discuss our example, its Jacobian and the connection of their 2-torsion fields with the Harbater field.

2. Background on Weierstrass points

Throughout this section, X is a smooth projective curve of genus $g \geq 2$ defined over a field k of characteristic 0, with algebraic closure $\bar{k}$.

2A. ***Definition and properties.*** Let P be a point on X. We say that P is a *Weierstrass point* if there exists a differential form $\omega \in H^0(X, \Omega_X^1)$ such that $\mathrm{ord}_P(\omega) \geq g$. We let $\mathscr{W}$ be the set of all Weierstrass points on $X(\bar{k})$. Alternatively, one can describe $\mathscr{W}$ as follows. Let D be a divisor on X, and $\mathscr{L}(D)$ the Riemann–Roch space associated to D, i.e.,

$$\mathscr{L}(D) := \{f \in k(X)^\times : \mathrm{div}(f) + D \geq 0\} \cup \{0\}.$$

By the Riemann–Roch theorem, $\mathscr{L}(D)$ is finite dimensional, and we let $\ell(D)$ be its dimension.

Proposition 2.1. *Let P be a point on X. Then, $P \in \mathscr{W}$ if and only if $\ell(gP) \geq 2$.*

Proof. This is a consequence of the Riemann–Roch theorem [Hindry and Silverman 2000, §A.4]. □

The *gap sequence* associated to a Weierstrass point P is the set

$$G(P) := \{n \in \mathbb{Z}_{\geq 0} : \ell(nP) = \ell((n-1)P)\}.$$

The *weight* of the Weierstrass point P is defined by

$$w(P) := \left(\sum_{n \in G(P)} n\right) - \frac{g(g+1)}{2}.$$

Theorem 2.2. *Let P be a point on X. Then P is a Weierstrass point if and only if $w(P) \geq 1$, and $\sum w(P)P$ belongs to the complete linear system*

$$\left|\frac{g(g+1)}{2} K_X\right|,$$

where K_X is a canonical divisor on X. In particular, we have that

$$\sum_{P \in \mathscr{W}} w(P) = g(g^2 - 1).$$

Proof. See [Farkas and Kra 1980, §III.5] or [Hindry and Silverman 2000, Exercise A.4.14]. □

2B. *Hyperellipticity.* We recall that X is a *hyperelliptic* curve if there is a degree 2 map $\phi : X \to \mathbb{P}^1$ defined over $\bar{k}$. In that case, ϕ is unique (up to automorphisms of $\mathbb{P}^1$). The map ϕ induces a degree 2 extension $\bar{k}(X)/\bar{k}(\mathbb{P}^1)$, which is Galois since $\mathrm{char}(k) = 0$. So, this gives rise to a map $\iota : X \to X$ called the *hyperelliptic involution*. We say X is hyperelliptic over k if ϕ is defined over k. The following is a well-known classical result.

Proposition 2.3. *Let X be a curve of genus $g \geq 2$ defined over a field k of characteristic 0, and $\mathscr{W}$ the set of Weierstrass points of $X(\bar{k})$. Then, we have*

$$2g + 2 \leq \#\mathscr{W} \leq g^3 - g.$$

Furthermore, X is hyperelliptic if and only if $\#\mathscr{W} = 2g + 2$. In that case, the branch points are the Weierstrass points.

Proof. See [Farkas and Kra 1980, §III.5] or [Hindry and Silverman 2000, Exercise A.4.14]. □

2C. *Galois action.* Let $\mathscr{W}$ be the set of all Weierstrass points over $X(\bar{k})$, then $\mathscr{W}$ is preserved by the action of $\mathrm{Gal}(\bar{k}/k)$. In particular, when X is a hyperelliptic curve, this action factors through the symmetric group S_{2g+2}.

3. Arithmetic Fuchsian groups

From now on, F is a totally real number field of degree g. We denote the real embeddings of F by $v_1, \ldots, v_g$. We let $\mathcal{O}_F$ be the ring of integers of F, and $\mathcal{O}_F^{\times +}$ the group of totally positive units in $\mathcal{O}_F$. We let D be a quaternion algebra defined over F, and fix a maximal order $\mathcal{O}$ in D. Let v be a place of F,

and F_v the completion of F at v. We recall that D is said to be ramified at v if $D_v = D \otimes F_v$ is a division quaternion algebra. We let S_∞ (resp. S_f) be the set of archimedean places (resp. finite places) where D is ramified; and set $S = S_\infty \cup S_f$. We let $r = \#S_f$.

3A. ***Fuchsian groups.*** From now on, we assume that D is ramified at all but one archimedean places; namely, that $S_\infty = \{v_2, \dots, v_g\}$. This means that, we have $D \otimes \mathbb{R} \simeq \mathrm{M}_2(\mathbb{R}) \times \mathbb{H}^{g-1}$, where $\mathbb{H}$ is the Hamilton quaternion algebra over $\mathbb{R}$. We let $j_1 : D \otimes_{v_1} \mathbb{R} \to \mathrm{M}_2(\mathbb{R})$ be the projection onto the factor corresponding to v_1. We will also denote the map induced on the unit groups by $j_1 : (D \otimes_{v_1} \mathbb{R})^\times \to \mathrm{GL}_2(\mathbb{R})$. For the definition of the reduced norm $\mathrm{Nrd} : D \to F$ below, we refer to [Vignéras 1980, Chapitre I, §1] or [Voight 2018, §3.3]. We let

$$\mathcal{O}^1 := \{x \in \mathcal{O} : \mathrm{Nrd}(x) = 1\}; \quad \mathcal{O}^\times := \{x \in \mathcal{O} : \mathrm{Nrd}(x) \in \mathcal{O}_F^\times\}; \quad \mathcal{O}_+^\times := \{x \in \mathcal{O} : \mathrm{Nrd}(x) \in \mathcal{O}_F^{\times +}\}.$$

We recall that the *normaliser* of $\mathcal{O}$ inside D is defined by

$$N_D(\mathcal{O}) := \{x \in D^\times : x\mathcal{O} = \mathcal{O}x\}.$$

We set

$$N_D(\mathcal{O})_+ := \{x \in N_D(\mathcal{O}) : \mathrm{Nrd}(x) \in F_+^\times\}.$$

We let Γ^1 (resp. Γ, $\Gamma_\mathcal{O}$) be the image of $\mathcal{O}^1$ (resp. $\mathcal{O}_+^\times$, $N_D(\mathcal{O})_+$) in $\mathrm{PGL}_2^+(\mathbb{R}) := \mathrm{GL}_2^+(\mathbb{R})/\mathbb{R}^\times$ via j_1, where

$$\mathrm{GL}_2^+(\mathbb{R}) := \{\gamma \in \mathrm{GL}_2(\mathbb{R}) : \det(\gamma) > 0\}.$$

We will also use the same notation to identify these groups with their respective images in $D^\times/F^\times$. We recall that Γ^1 is an *arithmetic Fuchsian group*, i.e., a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$. The *commensurability class* of Γ^1, consists of all the subgroups $\Gamma' \subset \mathrm{PGL}_2^+(\mathbb{R})$ that are commensurable with Γ^1, i.e., such that $\Gamma' \cap \Gamma^1$ has finite index in both Γ' and Γ^1. Any Fuchsian group that is commensurable to an arithmetic Fuchsian group is itself arithmetic. So, the commensurability class of Γ^1 is independent of the embedding j_1. We define it simply as the commensurability class of $\mathcal{O}^1$ in $D^\times/F^\times$, and denote it by $\mathscr{C}(D)$. In $\mathscr{C}(D)$, one is particularly interested in those groups Γ' with minimal covolume. Borel [1981] showed that, up to conjugacy, there are finite many such groups, and gave their covolume purely in terms of the number theoretic data used in defining them. These groups are called *maximal arithmetic Fuchsian groups*, and are the main objects of interest to us in this section.

Theorem 3.1 [Borel 1981]. *Every maximal arithmetic Fuchsian group in $\mathscr{C}(D)$ is of the form $\Gamma_\mathcal{O}$, where $\mathcal{O}$ is a maximal order in D. In that case, the covolume of $\Gamma_\mathcal{O}$ is given by*

$$\mathrm{Vol}(\Gamma_\mathcal{O}\backslash\mathfrak{H}) = \frac{8\pi D_F^{3/2}\zeta_F(2)}{(4\pi^2)^g[H : F^{\times 2}]} \prod_{\mathfrak{q} \in S_f} (\mathrm{N}\,\mathfrak{q} - 1),$$

where $H = \{\mathrm{Nrd}(x) : x \in N_D(\mathcal{O})_+\}$. In particular, it depends only on F and S_f.

Proof. See [Borel 1981, §8.4]. □

3B. ***The Atkin–Lehner group.*** We define the *Atkin–Lehner group*

$$W := N_D(\mathcal{O})/F^\times \mathcal{O}^\times.$$

By the Skolem–Noether theorem [Vignéras 1980, Chapitre II, Théorème 2.1], W can be identified with the group of automorphisms of $\mathcal{O}$. It is generated by the classes $[u] \in W$ such that (u) is a principal two-sided ideal whose norm is supported at the prime ideals in S_f. By the Hasse–Schilling–Maass theorem [Vignéras 1980, Chapitre III, Théorème 5.7], W is a *finite* elementary abelian 2-group. So, there is a positive integer r such that

$$W \simeq (\mathbb{Z}/2\mathbb{Z})^r.$$

We define the *positive Atkin–Lehner groups*

$$W_+ := N_D(\mathcal{O})_+/F^\times \mathcal{O}_+^\times, \quad W^1 := N_D(\mathcal{O})/F^\times \mathcal{O}^1.$$

There is a split exact sequence

$$1 \to \mathcal{O}_F^{\times +}/(\mathcal{O}_F^\times)^2 \to W^1 \to W_+ \to 1,$$

which gives an isomorphism

$$W^1 \simeq \mathcal{O}_F^{\times +}/(\mathcal{O}_F^\times)^2 \times W_+ \simeq (\mathbb{Z}/2\mathbb{Z})^s,$$

where $s \leq (n-1)+r$. The rank s of W^1 can be determined from the Dirichlet unit theorem and the fact that the image of W_+ inside W is generated by those principal two-sided ideals whose norms are totally positive and supported at S_f.

3C. ***Optimal embeddings.*** Let E/F be a CM extension, i.e., a totally imaginary quadratic extension. By [Vignéras 1980, Chapitre III, Théorème 3.8], E embeds into D if and only if, every finite place $v \in S_f$ is ramified or inert in E. The following theorem will be very useful for us.

Theorem 3.2. *Let E/F be a* CM *extension, and $\sigma : E \hookrightarrow D$ an embedding. Let $\alpha \in E \setminus F$, and* $\mathrm{disc}(\alpha) = \mathrm{Tr}_{E/F}(\alpha)^2 - 4\,\mathrm{N}_{E/F}(\alpha)$. *Then, up to conjugation, $\sigma(\alpha) \in N_D(\mathcal{O})_+$ if and only if* $\mathrm{disc}(\alpha)/\mathrm{N}_{E/F}(\alpha) \in \mathcal{O}_F$, *and $\mathrm{N}_{E/F}(\alpha) \in F_+^\times$ is supported at S_f modulo squares.*

Proof. This follows from [Chinburg and Friedman 1999, Lemma 4.3] (see also [Maclachlan 2006, Theorem 3.1]). □

Let E/F be a CM extension, and $\mathfrak{O}$ an $\mathcal{O}_F$-order in E. An *optimal embedding* of $\mathfrak{O}$ in $\mathcal{O}$ is a homomorphism $\iota : E \hookrightarrow D$ such that $\iota(\mathfrak{O}) = \iota(E) \cap \mathcal{O}$. We denote the set of optimal embeddings of $\mathfrak{O}$ into $\mathcal{O}$ by $\mathrm{Emb}(\mathfrak{O}, \mathcal{O})$. We fix an embedding $E \hookrightarrow D$. Then, by the Skolem–Noether theorem, every embedding of E into D is of the form $(x \mapsto \alpha x \alpha^{-1})$ for some $\alpha \in D^\times$. So, we can identify $\mathrm{Emb}(\mathfrak{O}, \mathcal{O})$ with the coset space $E^\times \backslash \mathscr{E}(\mathfrak{O}, \mathcal{O})$ where

$$\mathscr{E}(\mathfrak{O}, \mathcal{O}) := \left\{\alpha \in D^\times : \alpha E \alpha^{-1} \cap \mathcal{O} = \mathfrak{O}\right\} = \left\{\alpha \in D^\times : E \cap \alpha^{-1}\mathcal{O}\alpha = \alpha^{-1}\mathfrak{O}\alpha\right\}.$$

Conjugation induces a right action of $N_D(\mathcal{O})/F^\times$ on $\mathrm{Emb}(\mathfrak{O}, \mathcal{O})$. For any subgroup $\Gamma^1 \subset \Gamma \subset N_D(\mathcal{O})/F^\times$, we let $\mathrm{Emb}(\mathfrak{O}, \mathcal{O}; \Gamma)$ be the set of Γ-conjugacy classes of optimal embeddings. Similarly, if $\mathcal{O}^1 \subset G \subset N_D(\mathcal{O})$, we let $\mathrm{Emb}(\mathfrak{O}, \mathcal{O}; G) := \mathrm{Emb}(\mathfrak{O}, \mathcal{O}; \overline{G})$, where $\overline{G}$ is the image of G in $N_D(\mathcal{O})/F^\times$. The set $\mathrm{Emb}(\mathfrak{O}, \mathcal{O}; \Gamma)$ is *finite* since Γ has finite index in $N_D(\mathcal{O})/F^\times$. The cardinality $m(\mathfrak{O}, \mathcal{O}; \Gamma)$ of this set is called the embedding number of $\mathfrak{O}$ into $\mathcal{O}$, with respect to Γ; or simply the embedding number of $\mathfrak{O}$ into $\mathcal{O}$ when $\Gamma = \mathcal{O}^\times$. There are formulae for $m(\mathfrak{O}, \mathcal{O}; \mathcal{O}^\times)$, see for example [Vignéras 1980, Chapitre II, §3 and Chapitre III, §5; Voight 2018, §30]. The following lemma can be used to get $m(\mathfrak{O}, \mathcal{O}; G)$ for any subgroup $\mathcal{O}^1 \subset G \subset \mathcal{O}^\times$.

Lemma 3.3. *Let $\mathcal{O}^1 \subset G \subset \mathcal{O}^\times$ be a subgroup. Then we have*

$$m(\mathfrak{O}, \mathcal{O}; G) = m(\mathfrak{O}, \mathcal{O}; \mathcal{O}^\times)[\mathrm{Nrd}(\mathcal{O}^\times) : \mathrm{Nrd}(G)\,\mathrm{N}_{E/F}(\mathfrak{O}^\times)].$$

Proof. See [Voight 2018, Lemma 30.3.14]. (We note that the statement in [Vignéras 1980, Chapitre III, Corollaire 5.13] is only correct with the inclusion $G \subset N_D(\mathcal{O})$ replaced by $G \subset \mathcal{O}^\times$.) □

Here we are interested in the case when $\mathcal{O}_+^\times \subset G \subset N_D(\mathcal{O})_+$. In particular, we want $\mathrm{Emb}(\mathfrak{O}, \mathcal{O}; N_D(\mathcal{O})_+)$ when $\mathcal{O}$ is a maximal order in D.

Lemma 3.4. *Let $\mathcal{O}_+^\times \subset G \subset N_D(\mathcal{O})_+$ be a subgroup. Then we have*

$$m(\mathfrak{O}, \mathcal{O}; \mathcal{O}_+^\times) = m(\mathfrak{O}, \mathcal{O}; G)\big[\mathrm{Nrd}(G) : \mathrm{Nrd}(G) \cap \mathrm{N}_{E/F}(E^\times)\mathcal{O}_F^{\times +}\big].$$

Proof. There is a natural surjection

$$E^\times \backslash \mathscr{E}(\mathfrak{O}, \mathcal{O})/\mathcal{O}_+^\times \to E^\times \backslash \mathscr{E}(\mathfrak{O}, \mathcal{O})/G.$$

To prove the lemma, we need to understand the fibres of this map. For $\alpha \in \mathscr{E}(\mathfrak{O}, \mathcal{O})$, the fibre of $E^\times \alpha G$ is

$$T := E^\times \backslash E^\times \alpha G/\mathcal{O}_+^\times \simeq (\alpha E^\times \alpha^{-1} \cap G)\backslash G/\mathcal{O}_+^\times.$$

It is enough to show that the cardinality of T is independent of α. To see this, we recall that the reduced norm $\mathrm{Nrd} : D_+^\times \to F_+^\times$ induces a map

$$\phi : (\alpha E^\times \alpha^{-1} \cap G)\backslash G/\mathcal{O}_+^\times \to \mathrm{Nrd}(G)/\,\mathrm{Nrd}(G) \cap \mathrm{N}_{E/F}(E^\times)\mathcal{O}_F^{\times +},$$

which is a bijection since $\ker(\phi) = \mathcal{O}^1 \subset \mathcal{O}_+^\times \subset G \subset N_D(\mathcal{O})_+$.

Alternatively, we can see that $\mathcal{O}_+^\times$ is a normal subgroup of G. So, we can identify $(\alpha E^\times \alpha^{-1} \cap G)\backslash G/\mathcal{O}_+^\times$ with a subgroup of W_+. This means that $\#T$ divides $\#W_+$, and is always a power of 2. □

Let $\widehat{\mathcal{O}} := \mathcal{O} \otimes \widehat{\mathbb{Z}} = \prod_{v<\infty} \mathcal{O}_v$ and $\widehat{D} := D \otimes \widehat{\mathbb{Q}}$, where $\widehat{\mathbb{Z}}$ and $\widehat{\mathbb{Q}}$ are the finite adèles of $\mathbb{Z}$ and $\mathbb{Q}$, respectively. For every finite place v, let $\mathcal{O}_v^\times \subset G_v \subset N_{D_v}(\mathcal{O}_v)$ be a subgroup, and $\widehat{G} := \prod_{v<\infty} G_v$. We would like to understand the global embedding numbers of the group $\widehat{G}$, or $G := \widehat{G} \cap D_+^\times$. Since D satisfies the Eichler condition, we have $D_+^\times \backslash \widehat{D}^\times / \widehat{\mathcal{O}}^\times \simeq \mathrm{Cl}_F^+$, where Cl_F^+ is the narrow class group of F.

Let $h = \#\mathrm{Cl}_F^+$ be the narrow class number of F, and

$$\widehat{D}^\times = \coprod_{i=1}^{h} D_+^\times g_i \widehat{\mathcal{O}}^\times,$$

where $g_i \in \widehat{D}^\times$, $i = 1, \dots, h$, and $g_1 = 1$. Then, for each i, $\mathcal{O}_i := g_i \widehat{\mathcal{O}} g_i^{-1} \cap D$ is a maximal order, and $N_D(\mathcal{O}_i) = g_i N_{\widehat{D}}(\widehat{\mathcal{O}}) g_i^{-1} \cap D$. Letting $G_i := g_i \widehat{G} g_i^{-1} \cap D_+^\times$, we have $(\mathcal{O}_i)_+^\times \subset G_i \subset N_D(\mathcal{O}_i)_+$.

For $\widehat{G} = \widehat{\mathcal{O}}^\times$, there are formulae for global optimal embeddings numbers (see [Vignéras 1980, Chapitre III, §5; Voight 2018, §30]). For $\widehat{\mathcal{O}}^\times \subset \widehat{G} \subset N_{\widehat{D}}(\widehat{\mathcal{O}})$, we have the following theorem.

Theorem 3.5. *Keeping the above notations, let $G := G_1$ and $h_{\mathfrak{O}}$ be the class number of $\mathfrak{O}$. Then we have*

$$\sum_{i=1}^{h} m(\mathfrak{O}, \mathcal{O}_i; G_i) = \frac{2h_{\mathfrak{O}}}{[H : H \cap \mathrm{N}_{E/F}(E^\times)\mathcal{O}_F^{\times +}]} \prod_{v<\infty} m(\mathfrak{O}_v, \mathcal{O}_v; \mathcal{O}_v^\times),$$

where $H := \mathrm{Nrd}(G)$, and $m(\mathfrak{O}_v, \mathcal{O}_v; \mathcal{O}_v^\times)$ is the local embedding number at the place v. (Here v runs over all finite places.)

Proof. By applying Lemma 3.3 with $G = \mathcal{O}_+^\times$, we have

$$\begin{aligned} m(\mathfrak{O}, \mathcal{O}; \mathcal{O}_+^\times) &= m(\mathfrak{O}, \mathcal{O}; \mathcal{O}^\times)[\mathrm{Nrd}(\mathcal{O}^\times) : \mathrm{Nrd}(\mathcal{O}_+^\times)\,\mathrm{N}_{E/F}(\mathfrak{O}^\times)] \\ &= m(\mathfrak{O}, \mathcal{O}; \mathcal{O}^\times)[\mathrm{Nrd}(\mathcal{O}^\times) : \mathcal{O}_F^{\times +}] = 2m(\mathfrak{O}, \mathcal{O}, \mathcal{O}^\times). \end{aligned}$$

The latter equality follows from the fact that D is ramified at all but one archimedean place, the norm theorem [Vignéras 1980, Chapitre III, Théorème 4.1] and the Dirichlet unit theorem.

Now we return to the situation $\mathcal{O}_+^\times \subset G \subset N_D(\mathcal{O})_+$. Combining the above identity with Lemma 3.4, we have

$$2m(\mathfrak{O}, \mathcal{O}; \mathcal{O}^\times) = m(\mathfrak{O}, \mathcal{O}; G)[\mathrm{Nrd}(G) : \mathrm{Nrd}(G) \cap \mathrm{N}_{E/F}(E^\times)\mathcal{O}_F^{\times +}].$$

A similar identity holds for the other maximal orders. In other words, for each maximal order $\mathcal{O}_i$, we have

$$2m(\mathfrak{O}, \mathcal{O}_i; \mathcal{O}_i^\times) = m(\mathfrak{O}, \mathcal{O}; G_i)[\mathrm{Nrd}(G_i) : \mathrm{Nrd}(G_i) \cap \mathrm{N}_{E/F}(E^\times)\mathcal{O}_F^{\times +}].$$

However, the group $\mathrm{Nrd}(G_i)$ is independent of i again by the norm theorem. Hence setting $H := \mathrm{Nrd}(G)$, we get

$$2m(\mathfrak{O}, \mathcal{O}_i; \mathcal{O}_i^\times) = m(\mathfrak{O}, \mathcal{O}_i; G_i)[H : H \cap \mathrm{N}_{E/F}(E^\times)\mathcal{O}_F^{\times +}].$$

So, we have

$$\sum_{i=1}^{h} m(\mathfrak{O}, \mathcal{O}_i; G_i) = \frac{2}{[H : H \cap \mathrm{N}_{E/F}(E^\times)\mathcal{O}_F^{\times +}]} \sum_{i=1}^{h} m(\mathfrak{O}, \mathcal{O}_i; \mathcal{O}_i^\times).$$

We then apply [Vignéras 1980, Chapitre III, Théorème 5.11] or [Voight 2018, Theorem 30.7.3] to conclude the proof. □

3D. ***Torsion in maximal arithmetic groups.*** From now on, we will assume that the field F has narrow class number one. However, the results discussed here can be easily adapted to any field by following [Voight 2018, §31 and §39] given that our maximal orders do *not* satisfy the selectivity condition in [Chinburg and Friedman 1999].

Since F has narrow class number one, under the assumptions of Theorem 3.5, we have

$$m(\mathfrak{O}, \mathcal{O}; G) = \frac{2h_{\mathfrak{O}}}{[H : H \cap \mathrm{N}_{E/F}(E^\times)\mathcal{O}_F^{\times+}]} \prod_{v<\infty} m(\mathfrak{O}_v, \mathcal{O}_v; \mathcal{O}_v^\times).$$

Theorem 3.6. *Let $q \geq 2$ be an integer, and e_q the number of elliptic points of order q in G. Suppose that $e_q > 0$. For $q \geq 3$, let $E = F(\zeta_q)$, where ζ_q is a primitive q-th root of unity, and let $\mathscr{S}_q$ be the set of $\mathcal{O}_F$-orders defined by*

$$\mathscr{S}_q := \big\{\mathcal{O}_F[\zeta_q] \subset \mathfrak{O} \subset \mathcal{O}_E : \#\mathfrak{O}^\times_{\mathrm{tors}} = q\big\}.$$

For $q = 2$, let $\mathscr{N}_q$ be a set of representatives for the norms of elements in G in $\mathrm{Nrd}(W_+)$, *and let $\mathscr{S}_q$ be the set of $\mathcal{O}_F$-orders defined by*

$$\mathscr{S}_q := \bigcup_{\substack{n \in \mathscr{N}_q \\ E = F(\sqrt{-n})}} \big\{\mathcal{O}_F[\sqrt{-n}] \subset \mathfrak{O} \subset \mathcal{O}_E\big\}.$$

Then the number of elliptic points of order q in G is given by

$$e_q := \frac{1}{2} \sum_{\mathfrak{O} \in \mathscr{S}_q} m(\mathfrak{O}, \mathcal{O}; G).$$

Proof. The proof is essentially an adaptation of the discussion of [Voight 2018, §39.4] (see also [Vignéras 1980, Chapitre IV, Section 2]); the only difference arises from the elliptic points that are fixed by the Atkin–Lehner group W_+. However, the number of 2-torsion elliptic elements can be computed by combining Theorem 3.2 and Section 3B. □

Remark 3.7. There seems to be very little discussion on the number of elliptic elements (or optimal embeddings) in maximal arithmetic Fuchsian groups. The only literature we could find on this topic is from Michon [1981] and Vignéras [1980, Chapitre IV, §3] for $F = \mathbb{Q}$, and Maclachlan [2006; 2009] for $[F : \mathbb{Q}] > 1$. In the latter case, however, the presentation is very different than ours. Our results are stated in a way as to draw the most parallel with optimal embeddings in Fuchsian groups, which correspond to Shimura curves, given that there is an abundance of literature in this case; see, for example, [Voight 2018, §30].

3E. ***Genus formula.*** Let Γ be a Fuchsian group of signature $(g; e_1, \ldots, e_r)$, then the quotient $\Gamma\backslash\mathfrak{H}$ is a compact Riemann surface, whose volume is given by

$$\mathrm{Vol}(\Gamma\backslash\mathfrak{H}) = 2\pi\left(2g - 2 + \sum_{i=1}^{r}\left(1 - \frac{1}{e_i}\right)\right).$$

When $\Gamma = \Gamma_{\mathcal{O}}$ is maximal in some commensurability class $\mathscr{C}(D)$, the volume depends only on F and S_f according to Theorem 3.1. In fact, it follows from [Maclachlan 2009, Corollary 5.7] that all maximal

arithmetic Fuchsian groups in the commensurability class $\mathscr{C}(D)$ have the same signature, and we can compute their genus by combining the volume formula in Theorem 3.1 with the results of Section 3D (at least when F has narrow class number one).

4. Shimura curves

We keep the notations of Section 3. Here, we summarise the necessary backgrounds on canonical models and $\mathfrak{p}$-adic uniformisation of Shimura curves. Our main references are [Boutot and Carayol 1991; Boutot and Zink 1995; Carayol 1986; Nekovář 2012; Sijsling 2013]. We view F as a subfield of $\mathbb{C}$ via the embedding $v_1 : F \hookrightarrow \mathbb{C}$.

4A. ***Complex uniformisation.*** Let $U = \prod_{\mathfrak{q}} U_{\mathfrak{q}} \subset \widehat{\mathcal{O}}^\times$ be a compact open subgroup, such that $U_{\mathfrak{p}}$ is maximal. We consider the quotient

$$X_U(\mathbb{C}) := D^\times \backslash X \times \widehat{D}^\times / U,$$

where $X := \mathbb{P}^1(\mathbb{C}) - \mathbb{P}^1(\mathbb{R}) = \mathfrak{H}^+ \sqcup \mathfrak{H}^-$, and $\mathfrak{H}^-$ and $\mathfrak{H}^+$ are the lower and upper Poincaré half-planes. Since D is a division algebra, $X_U(\mathbb{C})$ is a Riemann surface.

There is a right action of $\widehat{D}^\times$ on $X \times \widehat{D}^\times$ by conjugation. For each $g \in \widehat{D}^\times$, this induces an isomorphism of complex curves

$$X_U(\mathbb{C}) \xrightarrow{\sim} X_{g^{-1}Ug}(\mathbb{C}).$$

By the strong approximation theorem, we have the following bijections

$$D_+^\times \backslash \widehat{D}^\times / U \simeq D^\times \backslash \{\pm 1\} \times \widehat{D}^\times / U \simeq F_+^\times \backslash \widehat{F}^\times / \operatorname{Nrd}(U).$$

By class field theory, there is a unique abelian extension F_U of F such that the Artin map induces an isomorphism

$$\operatorname{Art}_F : \operatorname{Gal}(F_U/F) \simeq F_+^\times \backslash \widehat{F}^\times / \operatorname{Nrd}(U).$$

So the set $F_+^\times \backslash \widehat{F}^\times / \operatorname{Nrd}(U)$ is a Galois set. Thus there is a finite étale scheme $\mathscr{T}_U$ defined over F such that

$$\mathscr{T}_U(F_U) = \mathscr{T}_U(\bar{F}) = \mathscr{T}_U(\mathbb{C}) = F_+^\times \backslash \widehat{F}^\times / \operatorname{Nrd}(U).$$

Shimura [1970] showed that $X_U(\mathbb{C})$ admits a canonical model defined over F (see also [Deligne 1971]). Namely, we have the following result.

Theorem 4.1. *There is a curve X_U defined over F, called a* ***canonical model****, which satisfies the following properties*:

(i) *The set of complex points of X_U is $X_U(\mathbb{C})$, i.e.,*

$$(X_U \otimes_{F, v_1} \mathbb{C})(\mathbb{C}) = X_U(\mathbb{C}).$$

(ii) *For a compact open $U' \subset U$, the morphism $X_{U'}(\mathbb{C}) \to X_U(\mathbb{C})$ is induced by an F-morphism $X_{U'} \to X_U$.*

(iii) *For each $g \in \widehat{D}^\times$, the morphism $X_U(\mathbb{C}) \to X_{g^{-1}Ug}(\mathbb{C})$ is induced from a F-morphism $X_U \to X_{g^{-1}Ug}$.*

(iv) *The morphism $X_U(\mathbb{C}) \to \mathscr{T}_U(\mathbb{C})$, has connected fibres, and is induced by a morphism of F-schemes $X_U \to \mathscr{T}_U$. In particular, the group of connected component $\pi_0(X_U)$ is a finite étale group scheme over F such that $\pi_0(X_U)(\mathbb{C}) = \pi_0(X_U(\mathbb{C})) = \mathscr{T}_U(\mathbb{C})$, where $\pi_0(X_U(\mathbb{C}))$ is the group of connected components of $X_U(\mathbb{C})$.*

Proof. This is essentially a summary of the properties of canonical models of Shimura curves listed in [Carayol 1986, §1.1 and §1.2]. □

Theorem 4.1(iv) is known as the Shimura reciprocity law. It implies that X_U is an irreducible scheme, which is not geometrically irreducible in general. However, when $\mathrm{Nrd}(U) = \widehat{\mathcal{O}}_F^\times$, then X_U is geometrically irreducible since we assume that F has narrow class number one.

We define the *adelic Atkin–Lehner group* by $\widehat{W} := N_{\widehat{D}}(U)/\widehat{F}^\times U$. By making use of the weak approximation theorem, one can show that

$$\widehat{W} \simeq \prod_{\mathfrak{q} \in S_f \cup S_0} \mathbb{Z}/2\mathbb{Z},$$

where S_0 is the set of primes where $U_\mathfrak{q}$ is nonmaximal.

Corollary 4.2. *The group $\widehat{W}$ acts on $X_U(\mathbb{C})$. This action is induced from an action of $\widehat{W}$ on X_U defined over F. In particular, if $W' \subseteq \widehat{W}$ is a subgroup, then the quotient X_U/W' is defined over F.*

Proof. Every element $g \in \widehat{W}$ defines an automorphism of $X_U(\mathbb{C})$. By Theorem 4.1 (iii), this automorphism descends to F. □

When there is an integral ideal $\mathfrak{N}$ coprime with the discriminant $\mathrm{disc}(D)$ of $\mathcal{O}$, and an Eichler order $\mathcal{O}_0(\mathfrak{N}) \subset \mathcal{O}$ of level $\mathfrak{N}$ such that $U = \widehat{\mathcal{O}_0(\mathfrak{N})}^\times$, we will denote the Shimura curve X_U by $X_0^D(\mathfrak{N})$, or simply write $X_0^D(1)$ when $\mathfrak{N} = (1)$.

4B. ***Bruhat-Tits tree.*** Let $\mathcal{T}_\mathfrak{p}$ be the Bruhat-Tits tree attached to $\mathrm{GL}_2(F_\mathfrak{p})$. Its set of vertices $\mathcal{V}(\mathcal{T}_\mathfrak{p})$ consists of maximal $\mathcal{O}_{F_\mathfrak{p}}$-orders in $\mathrm{M}_2(F_\mathfrak{p})$, two vertices being adjacent if their intersection is an Eichler order of level $\mathfrak{p}$. Let $\vec{\mathcal{E}}(\mathcal{T}_\mathfrak{p})$ denote the set of ordered edges of $\mathcal{T}_\mathfrak{p}$, i.e., the set of ordered pairs (s, t) of adjacent vertices of $\mathcal{T}_\mathfrak{p}$. If $e = (s, t)$, the vertex s is called the *source* of e and the vertex t is called its *target*; they are denoted by $s(e)$ and $t(e)$ respectively.

The Atkin–Lehner involution $\iota : \vec{\mathcal{E}}(\mathcal{T}_\mathfrak{p}) \to \vec{\mathcal{E}}(\mathcal{T}_\mathfrak{p})$ sends the edge $e = (s, t)$ to the opposite edge $\bar{e}$. We let $\mathcal{E}(\mathcal{T}_\mathfrak{p}) = \vec{\mathcal{E}}(\mathcal{T}_\mathfrak{p})/\langle\iota\rangle$ be the set of nonoriented edges.

The tree $\mathcal{T}_\mathfrak{p}$ is endowed with a natural left action of $\mathrm{PGL}_2(F_\mathfrak{p})$ by isometries corresponding to conjugation of maximal orders by elements of $\mathrm{GL}_2(F_\mathfrak{p})$. This action is transitive on both $\mathcal{V}(\mathcal{T}_\mathfrak{p})$ and $\vec{\mathcal{E}}(\mathcal{T}_\mathfrak{p})$.

4C. ***$\mathfrak{p}$-adic uniformisation.*** Let $\overline{F_\mathfrak{p}}$ be an algebraic closure of $F_\mathfrak{p}$, and $\mathbb{C}_\mathfrak{p} := \widehat{\overline{F_\mathfrak{p}}}$ be a fixed completion of $\overline{F_\mathfrak{p}}$. Let $\widehat{\mathscr{H}_\mathfrak{p}}$ be $\mathfrak{p}$-adic upper half plane. This is the formal scheme over $\mathrm{Spf}(\mathcal{O}_{F_\mathfrak{p}})$ defined in [Boutot and Carayol 1991, §1.3] by

$$\widehat{\mathscr{H}_\mathfrak{p}} := \mathbb{P}^1(\mathbb{C}_\mathfrak{p}) - \mathbb{P}^1(F_\mathfrak{p}).$$

The scheme $\widehat{\mathscr{H}}_{\mathfrak{p}}$ admits a natural action by the group $\mathrm{GL}_2(F_{\mathfrak{p}})$, which factors through the adjoint group $\mathrm{PGL}_2(F_{\mathfrak{p}})$. We let

$$\widehat{\mathscr{H}}_{\mathfrak{p}}^{\mathrm{ur}} = \widehat{\mathscr{H}}_{\mathfrak{p}} \times_{\mathrm{Spf}(\mathcal{O}_{F_{\mathfrak{p}}})} \mathrm{Spf}(\mathcal{O}_{F_{\mathfrak{p}}}^{\mathrm{ur}}).$$

Let B be the totally definite quaternion algebra defined over F whose set of ramified *finite* places is $S_f \setminus \{\mathfrak{p}\}$ so that $B_{\mathfrak{p}} \simeq \mathrm{M}_2(F_{\mathfrak{p}})$. (Note that this means that the set of ramified archimedean places of B is $S_\infty \cup \{v_1\}$.) We write $\widehat{B} = B_{\mathfrak{p}} \times B^{\mathfrak{p}}$ and $\widehat{D} = D_{\mathfrak{p}} \times D^{\mathfrak{p}}$, and we fix an isomorphism $\varphi : D^{\mathfrak{p}} \xrightarrow{\sim} B^{\mathfrak{p}}$. We let $K = K_{\mathfrak{p}} \times K^{\mathfrak{p}}$ be a compact open subgroup of $\widehat{B}^\times$ such that $K_{\mathfrak{p}} \simeq \mathrm{GL}_2(\mathcal{O}_{F_{\mathfrak{p}}})$ and $\varphi(U^{\mathfrak{p}}) = K^{\mathfrak{p}}$. We also let

$$K_{\mathfrak{p}}^0 := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K_{\mathfrak{p}} : c \equiv 0 \bmod \mathfrak{p} \right\},$$

and $K_0(\mathfrak{p}) = K_{\mathfrak{p}}^0 \times K^{\mathfrak{p}}$.

Since $U_{\mathfrak{p}}$ is the maximal compact open subgroup of $D_{\mathfrak{p}}^\times$, the norm map induces an isomorphism $D_{\mathfrak{p}}^\times / U_{\mathfrak{p}} \xrightarrow{\sim} F_{\mathfrak{p}}^\times / \mathcal{O}_{F_{\mathfrak{p}}}^\times$ (see [Vignéras 1980, Chapitre II, Lemme 1.5]). The group $B_{\mathfrak{p}}^\times$ acts on $F_{\mathfrak{p}}^\times / \mathcal{O}_{F_{\mathfrak{p}}}^\times$ through its reduced norm map $\mathrm{Nrd} : B_{\mathfrak{p}}^\times \to F_{\mathfrak{p}}^\times$. We obtain a corresponding action of $B_{\mathfrak{p}}^\times$ on $D_{\mathfrak{p}}^\times / U_{\mathfrak{p}}$. This, together with the isomorphism φ, gives an action of $\widehat{B}^\times$ on $\widehat{D}^\times / U$.

Theorem 4.3 (Čerednik–Drinfel'd). *There exist a model $\mathscr{M}$ of X_U over $\mathcal{O}_{F_{\mathfrak{p}}}$, and an isomorphism of formal schemes*

$$\widehat{\mathscr{M}}^{\mathrm{ur}} = \widehat{\mathscr{M}} \times_{\mathrm{Spf}(\mathcal{O}_{F_{\mathfrak{p}}})} \mathrm{Spf}(\mathcal{O}_{F_{\mathfrak{p}}}^{\mathrm{ur}}) \simeq B^\times \backslash \widehat{\mathscr{H}}_{\mathfrak{p}}^{\mathrm{ur}} \times \widehat{D}^\times / U,$$

where $\widehat{\mathscr{M}}$ is the completion of $\mathscr{M}$ along its special fibre.

Proof. See [Boutot and Zink 1995, Theorem 3.1]. □

4D. ***The dual graph.*** The *dual graph* associated to $B^\times \backslash \widehat{\mathscr{H}}_{\mathfrak{p}}^{\mathrm{ur}} \times \widehat{D}^\times / U$ is the weighted graph

$$\mathcal{G} := B^\times \backslash \mathcal{T}_{\mathfrak{p}} \times \widehat{D}^\times / U.$$

The vertices of $\mathcal{V}(\mathcal{G})$ and oriented edges $\vec{\mathcal{E}}(\mathcal{G})$ of $\mathcal{G}$ are given respectively by

$$\mathcal{V}(\mathcal{G}) := B^\times \backslash \mathcal{V}(\mathcal{T}_{\mathfrak{p}}) \times \widehat{D}^\times / U \quad \text{and} \quad \vec{\mathcal{E}}(\mathcal{G}) := B^\times \backslash \vec{\mathcal{E}}(\mathcal{T}_{\mathfrak{p}}) \times \widehat{D}^\times / U.$$

We define the weight of a vertex $v \in \mathcal{V}(\mathcal{G})$ to be $\#\mathrm{Stab}_{B^\times / F^\times}(v)$, and the weight of an edge $e \in \vec{\mathcal{E}}(\mathcal{G})$ to be $\#\mathrm{Stab}_{B^\times / F^\times}(e)$. For a vertex v, we let $\mathrm{Star}(v)$ denote the set of all edges containing v.

Proposition 4.4. *The maps*

$$\begin{aligned} \vartheta_1 : (B_{\mathfrak{p}}^\times / F_{\mathfrak{p}}^\times K_{\mathfrak{p}}) \times (D_{\mathfrak{p}}^\times / U_{\mathfrak{p}}) \times (D^{\mathfrak{p}\times} / U^{\mathfrak{p}}) &\to (B_{\mathfrak{p}}^\times / K_{\mathfrak{p}}) \times \mathbb{Z} \times (B^{\mathfrak{p}\times} / K^{\mathfrak{p}}) \\ (x_{\mathfrak{p}}, y_{\mathfrak{p}}, y^{\mathfrak{p}}) &\mapsto (x_{\mathfrak{p}}, \mathrm{ord}_{\mathfrak{p}}(\mathrm{Nrd}(y_{\mathfrak{p}})), \varphi(y^{\mathfrak{p}})), \\ \vartheta_2 : (B_{\mathfrak{p}}^\times / F_{\mathfrak{p}}^\times K_{\mathfrak{p}}^0) \times (D_{\mathfrak{p}}^\times / U_{\mathfrak{p}}) \times (D^{\mathfrak{p}\times} / U^{\mathfrak{p}}) &\to (B_{\mathfrak{p}}^\times / K_{\mathfrak{p}}^0) \times \mathbb{Z} \times (B^{\mathfrak{p}\times} / K^{\mathfrak{p}}) \\ (x_{\mathfrak{p}}, y_{\mathfrak{p}}, y^{\mathfrak{p}}) &\mapsto (x_{\mathfrak{p}}, \mathrm{ord}_{\mathfrak{p}}(\mathrm{Nrd}(y_{\mathfrak{p}})), \varphi(y^{\mathfrak{p}})) \end{aligned}$$

induce an isomorphism of bipartite graphs

$$\mathcal{V}(\mathcal{G}) = B^\times\backslash\mathcal{V}(\mathcal{T}_\mathfrak{p}) \times \widehat{D}^\times/U \xrightarrow{\sim} (B^\times\backslash\widehat{B}^\times/K) \times \mathbb{Z}/2\mathbb{Z},$$
$$\vec{\mathcal{E}}(\mathcal{G}) = B^\times\backslash\vec{\mathcal{E}}(\mathcal{T}_\mathfrak{p}) \times \widehat{D}^\times/U \xrightarrow{\sim} (B^\times\backslash\widehat{B}^\times/K_0(\mathfrak{p})) \times \mathbb{Z}/2\mathbb{Z}$$

as follows: *we write* $\mathcal{V}(\mathcal{G}) = \mathcal{V} \sqcup \mathcal{V}' \simeq B^\times\backslash\widehat{B}^\times/K \sqcup B^\times\backslash\widehat{B}^\times/K$, *and we let the adjacency matrix in the basis* $\mathcal{V} \cup \mathcal{V}'$ *be given by the matrix*

$$\begin{bmatrix} 0 & T_\mathfrak{p} \\ T_\mathfrak{p} & 0 \end{bmatrix},$$

where $T_\mathfrak{p}$ *is the Hecke operator at* $\mathfrak{p}$ *acting on the Brandt module* $M := \mathbb{Z}[B^\times\backslash\widehat{B}^\times/K]$. *In that identification, the action of the Atkin–Lehner involution* $w_\mathfrak{p}$ *on* $\mathcal{V}(\mathcal{G})$ *is given by the matrix*

$$\begin{bmatrix} 0 & \mathbf{1}_M \\ \mathbf{1}_M & 0 \end{bmatrix}.$$

Proof. See [Sijsling 2013, Propositions 3.1.8 and 3.1.9], [Nekovář 2012, §1.5] or [Kurihara 1979, §4]. □

Remark 4.5. In the isomorphism of Proposition 4.4, the set of nonoriented edges is given by

$$\mathcal{E}(\mathcal{G}) = B^\times\backslash\mathcal{E}(\mathcal{T}_\mathfrak{p}) \times \widehat{D}^\times/U \simeq B^\times\backslash\widehat{B}^\times/K_0(\mathfrak{p}).$$

The following result is an essential ingredient in the description of the special fibre of the Čerednik–Drinfel'd model described in Theorem 4.3. As we will see later, it is also useful in understanding the automorphism group of the curve X_U.

Theorem 4.6. *Let* $\mathscr{M}$ *be the scheme in Theorem 4.3. Then, we have the following*:

(i) $\mathscr{M} \otimes_{\mathcal{O}_{F_\mathfrak{p}}} \mathcal{O}_{F_{\mathfrak{p}^2}}$ *is a normal, proper, flat and semistable scheme over* $\mathcal{O}_{F_{\mathfrak{p}^2}}$.

(ii) *The special fibre of* $\mathscr{M} \otimes_{\mathcal{O}_{F_\mathfrak{p}}} \mathcal{O}_{F_{\mathfrak{p}^2}}$ *is reduced. Its components are rational curves, and all its singular points are ordinary double points.*

(iii) *The weighted dual graph associated to* $\mathscr{M} \otimes_{\mathcal{O}_{F_\mathfrak{p}}} \mathcal{O}_{F_{\mathfrak{p}^2}}$ *is the graph* $\mathcal{G}$ *described in Proposition 4.4.*

(iv) *Let* $\mathcal{H}$ *be a connected component of* $\mathcal{G}$, *and* $\mathscr{M}_\mathcal{H}$ *the corresponding irreducible component of* $\mathscr{M}$. *Then the arithmetic genus of* $\mathscr{M}_\mathcal{H}$ *is given by the Betti number* $1 + \#\mathcal{E}(\mathcal{H}) - \#\mathcal{V}(\mathcal{H})$.

Proof. See [Nekovář 2012, Proposition 1.5.5] or [Kurihara 1979, Proposition 3.2]. □

4E. ***Special fibre of*** $\mathscr{M} \otimes_{\mathcal{O}_{F_\mathfrak{p}}} \mathcal{O}_{F_{\mathfrak{p}^2}}$**.** The curve $\mathscr{M}$ is an *admissible* curve over $\mathcal{O}_{F_\mathfrak{p}}$ in the following sense:

(i) $\mathscr{M} \otimes_{\mathcal{O}_{F_\mathfrak{p}}} \mathcal{O}_{F_{\mathfrak{p}^2}}$ is a normal, proper, flat and semistable scheme over $\mathcal{O}_{F_{\mathfrak{p}^2}}$. Each irreducible component has a smooth generic fibre.

(ii) The completion of the local ring of $\mathscr{M} \otimes_{\mathcal{O}_{F_\mathfrak{p}}} \mathcal{O}_{F_{\mathfrak{p}^2}}$ at each of its singular points x is isomorphic, as an $\mathcal{O}_{F_\mathfrak{p}}$-algebra, to $\mathcal{O}_{F_\mathfrak{p}}[[X, Y]]/(XY - \varpi_\mathfrak{p}^w)$, where $\varpi_\mathfrak{p}$ is a uniformising element at $\mathfrak{p}$, and $w = w(x) \in \{1, 2, 3, \ldots\}$.

(iii) The special fibre $\mathscr{M} \otimes_{\mathcal{O}_{F_\mathfrak{p}}} k(\mathfrak{p})$ is reduced; the normalisation of each of its irreducible components is isomorphic to $\mathbb{P}^1(k(\mathfrak{p}))$; its only singular points are ordinary double points, where $k(\mathfrak{p})$ is the residue field of $\mathcal{O}_{F_{\mathfrak{p}^2}}$.

The dual graph encodes the following combinatoric data of the special fibre.

(iv) Each vertex $v \in \mathcal{V}(\mathcal{G})$ corresponds to an irreducible component C_v of the special fibre $\mathscr{M} \otimes_{\mathcal{O}_{F_\mathfrak{p}}} k(\mathfrak{p})$.

(v) Each edge $e = \{v, v'\} \in \mathcal{E}(\mathcal{G})$ corresponds to a singular point in $x_e \in C_v \cap C_{v'}$. The completion of local ring at x_e is of the form $\mathcal{O}_{F_\mathfrak{p}}[[X, Y]]/(XY - \varpi_\mathfrak{p}^w)$, where $w = w(e)$ is the weight of the edge e.

The above description can be found in [Nekovář 2012; Kurihara 1979].

4F. ***Automorphism groups.*** An *automorphism of weighted graph* $\mathcal{G}$ is an automorphism of graphs which preserves the weights of the edges. We will denote the group of such automorphisms by $\mathrm{Aut}(\mathcal{G})$. We note that there is a natural inclusion $\mathrm{Aut}(\mathcal{G}) \subset \mathrm{Aut}^s(\mathcal{G})$, where $\mathrm{Aut}^s(\mathcal{G})$ is the automorphism group of the underlying simple graph to $\mathcal{G}$.

For the next statement, we recall the notion of admissibility from [Kontogeorgis and Rotger 2008]. We say that an element $\omega \in \mathrm{Aut}(\mathcal{G})$ is *admissible* if there is no vertex $v \in \mathcal{V}(\mathcal{G})$ fixed by ω such that $\mathrm{Star}(v)$ has at least 3 edges also fixed by ω. We say that a subgroup $H \subset \mathrm{Aut}(\mathcal{G})$ is *admissible* if every nontrivial element $\omega \in H$ is admissible.

Proposition 4.7. *Let $W' \subset \widehat{W}$ be a subgroup. Then, we have the following*:

(1) *The dual graph of $(\mathscr{M}/W') \otimes_{\mathcal{O}_{F_\mathfrak{p}}} \mathcal{O}_{F_{\mathfrak{p}^2}}$ is the graph $\mathcal{G}' = (\mathcal{G}/W')^*$, where * means we remove all loops from the quotient graph $\mathcal{G}/W'$.*

(2) *Assume that the genus of X_U/W' is at least 2, and let $\mathcal{G}_{st}$ be the dual graph of the stable model $(\mathscr{M}/W')_{st}$ of $\mathscr{M}/W'$. Then there is a natural injection $\varrho : \mathrm{Aut}(X_U/W') \hookrightarrow \mathrm{Aut}(\mathcal{G}_{st})$ whose image $\mathrm{im}(\varrho)$ lies in an admissible subgroup.*

Proof. Part (1) follows from general properties of Mumford curves. From [Deligne and Mumford 1969, Lemmas 1.12 and 1.16], and universal properties of stable models, there is an injection $\varrho : \mathrm{Aut}(X_U/W') \hookrightarrow \mathrm{Aut}(\mathcal{G}_{st})$. To prove Part (2), we only need to show that every nontrivial element in the image of ϱ is admissible. To this end, let $\omega \in \mathrm{Aut}(X_U/W')$ be such that $\varrho(\omega)$ fixes a vertex v, and at least 3 edges in $\mathrm{Star}(v)$. Then, since every automorphism of the projective line, which fixes at least 3 points is the identity, the restriction $\omega|_{C_v}$ is the identity, where C_v is the irreducible component associated to v. This would imply that, as an automorphism of the Riemann surface $(X_U/W')(\mathbb{C})$, ω fixes more than $2g(X_U/W') + 2$ points, where $g(X_U/W')$ is the genus of X_U/W'. Hence ω must be the identity. Therefore, if ω is nontrivial, then $\varrho(\omega)$ must be admissible. □

5. The hyperelliptic Shimura quotient curve

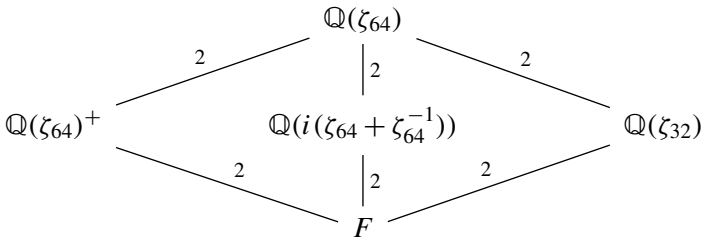
5A. ***The quaternion algebra.*** Let $F = \mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_{32} + \zeta_{32}^{-1})$ be the maximal totally real subfield of the cyclotomic field of the 32-nd roots of unity. This field is defined by the polynomial $x^8 - 8x^6 + 20x^4 - 16x^2 + 2$.

Let σ be a generator of $\mathrm{Gal}(F/\mathbb{Q})$. Let $\mathcal{O}_F$ be the ring of integers of F. Let $v_1, \ldots, v_8$ be the real places of F. We consider the quaternion algebra D/F ramified at $v_2, \ldots, v_8$ and the unique prime $\mathfrak{p}$ above 2. More concretely, we have $D = \left(\frac{u,-1}{F}\right)$, where $u = -\alpha^2 + \alpha$ has signature $(+, -, \ldots, -)$. Let $\mathcal{O}$ be the maximal order in D given by

$$\mathcal{O} := \mathcal{O}_F\left[1, i, \frac{(\alpha^7+\alpha^6+\alpha^4+1)+\alpha^7 i + j}{2}, \frac{(\alpha^7+\alpha^6+\alpha^4+1)i + k}{2}\right].$$

We also let B/F be the totally definite quaternion algebra ramified exactly at all the real places $v_1, \ldots, v_8$, and fix a maximal order $\mathcal{O}_B$ in B. Both these orders were computed using the quaternion algebras package in `Magma` [1997] implemented by Voight [2005].

5B. ***The CM field and its embedding.*** We recall the following diagram:



The subfield $K := \mathbb{Q}(\beta) = \mathbb{Q}(i(\zeta_{64} + \zeta_{64}^{-1}))$ is the unique CM extension of F with class number 17. For later, we observe that $\beta^2 = -2 - \alpha$, where $\mathfrak{p} = (2 + \alpha)$. Since $\mathfrak{p}$ is the unique prime of F that ramifies in both K and D, we see that K is a splitting field of D by [Vignéras 1980, Chapitre III, Théorème 3.8]. It is possible to compute an explicit embedding $K \hookrightarrow D$ using the quaternion algebras package in `Magma` (see [Voight 2005]), but we will not need such a map here.

5C. ***The spaces of forms.*** Let $S_2(\mathfrak{p})^{\mathrm{new}}$ be the new subspace of Hilbert cusp forms of level $\mathfrak{p}$ and weight 2. This is a 40-dimensional space. Let $S_2^D(1)$ be the space of automorphic forms of level (1) and weight 2 on D, and let $S_2^B(\mathfrak{p})^{\mathrm{new}}$ be the new subspace of automorphic forms of level $\mathfrak{p}$ and weight 2 on B. By the Jacquet–Langlands correspondence, we have isomorphisms of Hecke modules

$$S_2(\mathfrak{p})^{\mathrm{new}} \simeq S_2^D(1) \simeq S_2^B(\mathfrak{p})^{\mathrm{new}}.$$

The space $S_2(\mathfrak{p})^{\mathrm{new}}$ decomposes into 5 Hecke constituents of dimensions 4, 4, 4, 4 and 24 respectively. (We note that all the computations have been performed using the Hilbert modular forms package in `Magma`, the algorithms are described in [Dembélé and Donnelly 2008; Dembélé and Voight 2013; Greenberg and Voight 2011].) There are choices of newforms f, f', g, g' and h in those constituents such that we have:

(i) The forms f and f' have the same coefficient field $L_f = L_{f'}$, which is the real quartic field $\mathbb{Q}(\zeta_{15})^+$ given by $x^4 + x^3 - 4x^2 - 4x + 1$. They satisfy the relations ${}^{\sigma}f = f'$ and ${}^{\sigma^2}f = f^{\tau}$, where τ is a generator of $\mathrm{Gal}(L_f/\mathbb{Q})$.

(ii) The forms g and g' have the same coefficient field $L_g = L_{g'}$, which is the real quartic subfield of $\mathbb{Q}(\zeta_{95})^+$ given by $x^4 + 19x^3 - 59x^2 + 19x + 1$. They satisfy the relations ${}^{\sigma}g = g'$ and ${}^{\sigma^2}g = g^{\tau}$, where τ is a generator of $\mathrm{Gal}(L_g/\mathbb{Q})$.

(iii) The coefficient field of the form h is a field L_h of degree 24, which is cyclic over the field $K_h = \mathbb{Q}(c)$ defined by $c^3 + c^2 - 229c + 167 = 0$. More precisely, it is the ray class field of conductor $\mathfrak{c} = \left(\frac{1}{2}(c^2 - 16c + 25)\right)$. The form h satisfies the relation ${}^{\sigma}h = h^{\tau}$, where τ is a generator of $\mathrm{Gal}(L_h/K_h)$.

(We summarise that data in Table 1, and the relations among the forms.) Let w and w_D be the Atkin–Lehner involutions acting on $S_2(\mathfrak{p})^{\mathrm{new}}$ and $S_2^D(1)$, respectively. The Atkin–Lehner involution w acts as follows:

$$wf = -f, \quad wf' = -f', \quad wg = -g, \quad wg' = -g', \quad wh = h.$$

We recall that $w_D = -w$.

5D. ***The Shimura curve and its quotient.*** Let $X_0^D(1)$ be the Shimura curve attached to $\mathcal{O}$. Let w_D be the Atkin–Lehner involution at $\mathfrak{p}$, and $C := X_0^D(1)/\langle w_D \rangle$. We can canonically identify $S_2^D(1)$ with the space of 1-differential forms on $X_0^D(1)$. From the discussion in Section 5C, it follows that $X_0^D(1)$ is a curve of genus 40; and that C is a curve of genus 16.

Theorem 5.1. *The curves $X_0^D(1)$ and C have the respective signatures* $(40; 3^{18}, 16^1)$ *and* $(16; 2^{17}, 3^9, 32^1)$.

Proof. The complex points of the curve $X_0^D(1)$ are determined by the quotient $\Gamma^1 \backslash \mathfrak{H}$, where Γ^1 is the image of $\mathcal{O}^1$ inside $\mathrm{PSL}_2(\mathbb{R})$. So it is a Shimura curve. So, we can compute the signature of $X_0^D(1)$ using the Shimura curves package in `Magma`, which was implemented by Voight [2009]. This gives that $X_0^D(1)$ has signature $(40; 3^{18}, 16^1)$.

The curve $C = X_0^D(1)/\langle w_D \rangle$ is given by the maximal arithmetic Fuchsian group $\Gamma_{\mathcal{O}}$. It is not a Shimura curve. Although Voight has implemented algorithms for computing with maximal arithmetic Fuchsian groups, they are not publicly available yet. So, we compute the signature of C by using the results of Section 3.

Let $q > 2$ be an integer. Then, by Theorem 3.2, $\Gamma_{\mathcal{O}}$ contains an elliptic element of order q if and only if the following three conditions are satisfied:

(i) $2\cos(2\pi/q) \in F$;

(ii) No prime $\mathfrak{q} \in S_f$ splits in $E = F(\zeta_q)$;

(iii) The ideal generated by $2 + 2\cos(2\pi/q)$ is supported at S_f modulo squares.

It is enough to test all integers q between 3 and 64. The only $q \geq 3$ which satisfy these three conditions are 3, 4, 6, 8, 16 and 32.

For $q = 4$, 8, 16 or 32, we have $E = F(\zeta_q) = \mathbb{Q}(\zeta_{32})$. In that case, the only $\mathcal{O}_F$-order which contains $\mathcal{O}_F[\zeta_{32}]$ and optimally embeds into D is the maximal order $\mathcal{O}_E$. By Theorem 3.6, we get that $e_{32} = 1$.

Newform	Coefficient field L_f	Fixed field $K_f = L_f^{\Delta}$	$\mathrm{Gal}(L_f/K_f)$
$f,\ f'$	$\mathbb{Q}(\zeta_{15})^+$	$\mathbb{Q}$	$\mathbb{Z}/4\mathbb{Z}$
$g,\ g'$	Quartic subfield of $\mathbb{Q}(\zeta_{95})^+$	$\mathbb{Q}$	$\mathbb{Z}/4\mathbb{Z}$
h	Ray class field of modulus $\mathfrak{c} = \left(\frac{1}{2}(c^2 - 16c + 25)\right)$	$\mathbb{Q}(c) := \mathbb{Q}[x]/(r(x))$, $r = x^3 + x^2 - 229x + 167$	$\mathbb{Z}/8\mathbb{Z}$
Relations	${}^{\sigma}f = f'$ and ${}^{\sigma^2}f = f^{\tau}$	${}^{\sigma}g = g'$ and ${}^{\sigma^2}g = g^{\tau}$	${}^{\sigma}h = h^{\tau}$

Table 1. Newforms of level $\mathfrak{p}$ and weight 2 on $F = \mathbb{Q}(\zeta_{32})^+$

For $q = 3$, we have $E = F\left(\frac{1}{2}(1+\sqrt{-3})\right)$. In that case, the only $\mathcal{O}_F$-order which contains $\mathcal{O}_F\left[\frac{1}{2}(1+\sqrt{-3})\right]$ and optimally embeds into D is also the maximal order $\mathfrak{O} := \mathcal{O}_E$. We have $h_{\mathfrak{O}} = 9$. Now since the prime $\mathfrak{p}$ is inert in the relative extension E/F, we have $[H : H \cap \mathrm{N}_{E/F}(E^{\times})\mathcal{O}_F^{\times +}] = 2$. So, by Theorem 3.6, we get that $e_3 = 9$.

Finally, for $q = 2$, we have $W^1 = W_+ = \mathbb{Z}/2\mathbb{Z}$ since F has narrow class number one and there is a unique prime in S_f; namely, the prime $\mathfrak{p}$ above 2. So the unique CM extension E/F which satisfies the condition of Theorem 3.2 is the extension K discussed in Section 5B. Recall that the ideal $\mathfrak{p}$ is generated by the totally positive element $n = 2 + \alpha$. The only $\mathcal{O}_F$-order which contains $\mathcal{O}_F[\sqrt{-n}]$ and optimally embeds into D is also the maximal order $\mathfrak{O} := \mathcal{O}_K$. We have $h_{\mathfrak{O}} = 17$. Now since the prime $\mathfrak{p}$ is ramified in the relative extension K/F, we have $[H : H \cap \mathrm{N}_{E/F}(E^{\times})\mathcal{O}_F^{\times +}] = 1$. So, by Theorem 3.6, we get that $e_2 = 17$.

So we conclude that there are 3 classes of elliptic elements in $\Gamma_{\mathcal{O}}$ of orders 2, 3 and 32, with respective multiplicities 17, 9 and 1.

By the volume formula in Theorem 3.1 and the genus formula in Section 3E, the genus g of the curve C must satisfy the equality

$$\frac{\mathrm{Vol}(\Gamma_{\mathcal{O}} \backslash \mathfrak{H})}{2\pi} = \frac{1455}{32} = 2(g-1) + 17\left(1 - \frac{1}{2}\right) + 9\left(1 - \frac{1}{3}\right) + \left(1 - \frac{1}{32}\right).$$

Solving this, we get that $g = 16$. Hence the curve C has signature $(16; 2^{17}, 3^9, 32^1)$. □

Lemma 5.2. *The curve $X_0^D(1)$ and the Atkin–Lehner involution w_D are both defined over $\mathbb{Q}$. In particular, the curve C descends to $\mathbb{Q}$.*

Proof. Since $\sigma(\mathfrak{p}) = \mathfrak{p}$ and the ray class group of modulus $\mathfrak{p}v_2 \cdots v_8$ is trivial, the curve $X_0^D(1)$ is defined over F by [Doi and Naganuma 1967, Corollary], and the field of moduli is $\mathbb{Q}$. The field $\mathbb{Q}(\zeta_{32})$ is a splitting field for D whose class number is one. So, there is a unique CM point attached to the extension $\mathbb{Q}(\zeta_{32})/F$, and it is defined over F. Therefore, by [Sijsling and Voight 2016, Corollary 1.9], the curve $X_0^D(1)$ descends to $\mathbb{Q}$.

Alternatively, by using the moduli interpretation in [Carayol 1986], or the more recent work [Tian and Xiao 2016], one can show that both $X_0^D(1)$ and w_D are defined over $\mathbb{Q}$. □

5E. ***The dual graph of the quotient curve.*** The dual graph $\mathcal{G}'$ of the curve $\mathscr{M}/\langle w_{\mathfrak{p}}\rangle$ is displayed in Figure 1. It was computed by using Propositions 4.4 and 4.7. The computations combine both `Magma` [1997] and `Sage` [2019].

Lemma 5.3. *The automorphism group of* $\mathcal{G}'$ *is* $\mathrm{Aut}(\mathcal{G}') \simeq \mathbb{Z}/4\mathbb{Z} \ltimes (\mathbb{Z}/2\mathbb{Z})^4$.

Proof. We compute the dual graph $\mathcal{G}'$ of the quotient $\mathscr{M}/\langle w_{\mathfrak{p}}\rangle$ using Propositions 4.4 and 4.7. Let B be the definite quaternion algebra defined in Section 5A. Then, by Propositions 4.4 and 4.7, the dual graphs $\mathcal{G}$ and $\mathcal{G}'$ are determined by the Brandt module $M_B := \mathbb{Z}[B^\times \backslash \widehat{B}^\times / \widehat{\mathcal{O}}_B^\times]$. In this case, the class number of the maximal order $\mathcal{O}_B$ is 58, and a basis of this module is given by equivalence classes of $\mathcal{O}_B$-right ideals. We let $v_1, v_2, \ldots, v_{58}$ be such a basis, which we order so that the weights of the elements are in decreasing order. We get the following sequence of weights: 32, 24, 16, 8^2, 4^3, 3^4, 2^6 and 1^{40}, where the exponent indicates the number of times each weight is repeated. Similarly, we compute the set of edges, and we obtain the following sequence for their weights: 32, 16^2, 8^6, 4^6, 2^{12} and 1^{128}. By combining this with the Hecke operator $T_{\mathfrak{p}}$, we obtain the graph $\mathcal{G}'$ in Figure 1.

We compute the automorphism group $\mathrm{Aut}^s(\mathcal{G}')$ of the underlying simple graph using `Magma`, and check that every element in $\mathrm{Aut}^s(\mathcal{G}')$ preserves the weights of the edges, i.e., that $\mathrm{Aut}(\mathcal{G}') = \mathrm{Aut}^s(\mathcal{G}')$.

To determine the group structure of $\mathrm{Aut}(\mathcal{G}')$, we first check that there is a unique normal subgroup of $\mathrm{Aut}(\mathcal{G}')$ which is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. Finally, we show that there is a unique cyclic subgroup of order 4 whose intersection with $(\mathbb{Z}/2\mathbb{Z})^4$ is the neutral element. □

Remark 5.4. As a byproduct of the computation of $\mathcal{G}'$, we check that

$$1 + \#\mathcal{E}(\mathcal{G}') - \#\mathcal{V}(\mathcal{G}') = 1 + 73 - 58 = 16,$$

which is the genus of $\mathscr{M}/\langle w_{\mathfrak{p}}\rangle$, or equivalently C.

Let $(\mathscr{M}/\langle w_{\mathfrak{p}}\rangle)_{st}$ be the stable model of $\mathscr{M}/\langle w_{\mathfrak{p}}\rangle$, and $\mathcal{G}_{st}$ its dual graph. By definition, $(\mathscr{M}/\langle w_{\mathfrak{p}}\rangle)_{st}$ is stable if for all $v \in \mathcal{V}(\mathcal{G}_{st})$, we have $\#\,\mathrm{Star}(v) \geq 3$. So, we obtain $(\mathscr{M}/\langle w_{\mathfrak{p}}\rangle)_{st}$ by blowing down all components C_v associated to a vertex v such that $\#\,\mathrm{Star}(v) < 3$. On graphs, this corresponds to doing the following:

(a) For all $v \in \mathcal{V}(\mathcal{G}')$, with $\#\,\mathrm{Star}(v) = 1$, remove v and all edges in $\mathrm{Star}(v)$.

(b) For each $v \in \mathcal{V}(\mathcal{G}')$, with $\#\,\mathrm{Star}(v) = 2$, contract the chain $v' \overset{e'}{-} v \overset{e''}{-} v''$ to $v' \overset{e}{-} v''$ with $w(e) = w(e') + w(e'')$.

By applying this process to the curve $\mathscr{M}/\langle w_{\mathfrak{p}}\rangle$, and then relabelling the resulting graph, we obtain the stable model whose dual graph $\mathcal{G}_{st}$ is given by Figure 2. The graph $\mathcal{G}_{st}$ has 30 vertices and 45 edges so that

$$1 + \#\mathcal{E}(\mathcal{G}_{st}) - \#\mathcal{V}(\mathcal{G}_{st}) = 1 + 45 - 30 = 16.$$

Lemma 5.5. *Let* $(\mathscr{M}/\langle w_{\mathfrak{p}}\rangle)_{st}$ *be the stable model of* $\mathscr{M}/\langle w_{\mathfrak{p}}\rangle$, *and* $\mathcal{G}_{st}$ *its dual graph. Then,* $\mathcal{G}_{st}$ *is a connected graph such that* $\mathrm{Aut}(\mathcal{G}_{st}) = \mathrm{Aut}(\mathcal{G}')$.

Proof. This follows from a direct calculation. □

Lemma 5.6. *Every admissible subgroup of* $\mathrm{Aut}(\mathcal{G}_{st})$ *of exponent* 2 *has order* 2.

Proof. First, we note that, since the degree of the Hecke operator $T_{\mathfrak{p}}$ is 3, and $(\mathscr{M}/\langle w_{\mathfrak{p}}\rangle)_{st}$ is stable, $\#\,\mathrm{Star}(v) = 3$ for each $v \in \mathcal{V}(\mathcal{G}_{st})$.

In the notations of Figure 2, we label the vertices $1, 2, \ldots, 30$. There are 19 permutations of order 2 in $\mathrm{Aut}(\mathcal{G}_{st}) \subset S_{30}$. Of those 19 permutations, there are exactly 4 with the same support of length 28. Each of the remaining 17 has a support whose length belongs to $\{2, 4, 6, 8\}$. The permutations of length 28 fix the vertices $v = 1$ and $v' = 2$. So, they must be admissible since a nonadmissible element must fix at least 4 different vertices. For each of remaining 17 permutations, one easily sees that the complement of its support contains a vertex v and its $\mathrm{Star}(v)$, meaning that it cannot be admissible.

To conclude the proof of the lemma, we let σ_i, $i = 1, 2, 3, 4$ be the 4 admissible permutations obtained above, and we check that $\sigma_i\sigma_j$ is not admissible for $i \neq j$. □

Lemma 5.7. *There is an injection* $\mathrm{Aut}(C) \hookrightarrow H$ *into an admissible subgroup of* $\mathrm{Aut}(\mathcal{G}_{st})$ *of exponent* 2. *In particular* $\mathrm{Aut}(C)$ *has order at most* 2.

Proof. In Section 5G, we will show that the endomorphism ring of each of the simple factor of $\mathrm{Jac}(C)$ is a totally real field. (This follows from the decomposition (2).) Using this, we see that $\mathrm{Aut}(C) \subset (\mathbb{Z}/2\mathbb{Z})^4$. So, by Proposition 4.7, $\mathrm{Aut}(C)$ injects into an admissible subgroup H of $\mathrm{Aut}(\mathcal{G}_{st})$ of exponent 2. By Lemma 5.6, H has order at most 2. □

Remark 5.8. The graph $\mathcal{G}'$ of the integral model $\mathscr{M}/\langle w_{\mathfrak{p}}\rangle$ (see Figure 1) is an example of a graph whose automorphism group does *not* have an element that is admissible. Indeed, it is easy to see that every element of $\mathrm{Aut}(\mathcal{G}')$ must fix the vertex v_4 and the 3 edges of weight 8 contained in $\mathrm{Star}(v_4)$. However, the vertex v_4 and $\mathrm{Star}(v_4)$ are removed when we blow down $\mathscr{M}/\langle w_{\mathfrak{p}}\rangle$ to obtain the stable model $(\mathscr{M}/\langle w_{\mathfrak{p}}\rangle)_{st}$ (see Figure 2). This example shows that [Kontogeorgis and Rotger 2008, Proposition 3.4] is incorrect as stated and needs to be modified slightly.

5F. ***Hyperellipticity of the curve C.*** We are now ready to prove one of our main results.

Theorem 5.9. *The curve C is hyperelliptic over F.*

Proof. Let $\gamma \in \Gamma_{\mathcal{O}}$ be an elliptic element of order 2, and P a fixed point by γ. Then P is a CM point by construction, and γ acts on the local ring $\mathcal{O}_{C,P}$ as an involution. More specifically, letting t be a uniformiser at P, we see that γ acts on t as

$$t \pmod{t^2} \mapsto -t \pmod{t^2}.$$

This forces any global differential form in $H^0(C, \Omega^1_C)$, which vanishes at P, to vanish to *even* order. We claim that this implies that P is a Weierstrass point. To prove this, we use Riemann–Roch.

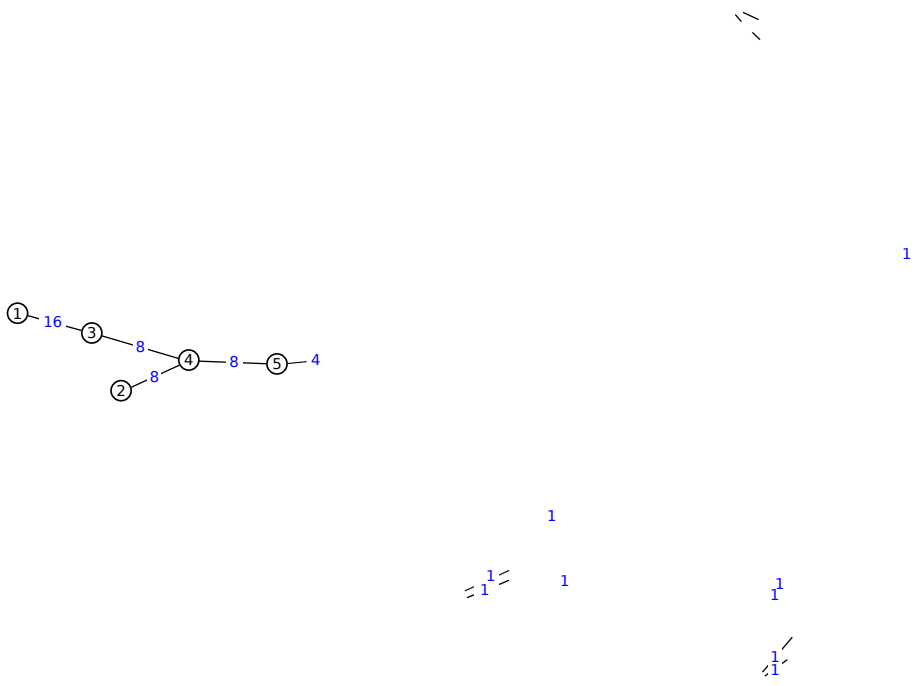


Figure 1. The dual graph $\mathcal{G}'$ of the quotient curve $\mathscr{M}/\langle w_{\mathfrak{p}}\rangle$.

Let K_C the canonical divisor. Then, we have $\ell(K_C - 2P) = \ell(K_C - P)$, i.e., every differential that vanishes at P vanishes to order 2. By Riemann–Roch, we have

$$\ell(K_C - 2P) - \ell(2P) = \deg(K_C - 2P) - g + 1 = (2g-4) - g + 1 = g - 3;$$

and

$$\ell(K_C - P) - \ell(P) = \deg(K_C - P) - g + 1 = (2g-3) - g + 1 = g - 2.$$

So, if $\ell(K_C - 2P) = \ell(K_C - P)$, then $\ell(2P) - \ell(P) = 1$. Now, since $\mathscr{L}(P)$ is the space of constant functions, we see that $\mathscr{L}(2P)$ must be nontrivial, and thus P is a (hyperelliptic) Weierstrass point.

From the above argument, it follows that C has 17 hyperelliptic Weierstrass points that are all CM. By Shimura reciprocity law, these CM points are all defined over the Hilbert class field H_K of K, where K is the CM-field defined in Section 5B. Let M be the normal closure of H_K over F. Then $[M : F] = 34$ and $\mathrm{Gal}(M/F) \simeq D_{17}$; and the action of $\mathrm{Gal}(\bar{F}/F)$ on the set of Weierstrass points $\mathscr{W}$ must factor through it (see Section 2C). Therefore, we must have $\#\mathscr{W} = 34$. In other words, C has 34 hyperelliptic Weierstrass points. Since C has genus 16, it must therefore be hyperelliptic by Proposition 2.3. □

Remark 5.10. It follows from the proof of Theorem 5.9 that half of the Weierstrass points on C are CM, while the remaining half are non CM. This means that the hyperelliptic involution must necessarily be exceptional. However, this should be expected since $C = X_0^D(1)/\langle w_D \rangle$, where w_D is the *unique* Atkin–Lehner involution acting on $X_0^D(1)$.

Theorem 5.11. *The automorphism group of the curve C is* $\mathrm{Aut}(C) = \mathbb{Z}/2\mathbb{Z}$.

Proof. By Theorem 5.9, the group $\mathrm{Aut}(C)$ is nontrivial since it contains the hyperelliptic involution. By Lemma 5.7, it injects into an admissible subgroup H of $\mathrm{Aut}(\mathcal{G}_{st})$ of order 2. □

Remark 5.12. By Theorem 5.11, $\mathrm{Aut}(C) = \mathbb{Z}/2\mathbb{Z}$, so that $\mathrm{Aut}(X_0^D(1)) = (\mathbb{Z}/2\mathbb{Z})^s$, with $1 \le s \le 2$. We note that $s = 2$ if and only if the hyperelliptic involution on C comes from an exceptional automorphism on $X_0^D(1)$. We also note that it is conjectured that there are only finitely many Shimura curves X defined over $\mathbb{Q}$ such that $\mathrm{Aut}(X)$ contains an exceptional automorphism (see [Kontogeorgis and Rotger 2008]). This conjecture would imply that there are very few Shimura curve quotients defined over $\mathbb{Q}$ which have automorphisms arising from exceptional automorphisms. However, analogues of this conjecture have barely been explored over totally real fields.

Theorem 5.13. *The curve C is hyperelliptic over* $\mathbb{Q}$.

Proof. Since C descends to $\mathbb{Q}$, it is enough to show that the hyperelliptic involution $\iota : C \to C$ also descends to $\mathbb{Q}$. By Theorem 5.11, $\mathrm{Aut}(C)/\langle \iota \rangle$ is trivial. Furthermore, the field $\mathbb{Q}(\zeta_{32})$ is a splitting field for D whose class number is one. So the CM point attached to the extension $\mathbb{Q}(\zeta_{32})/F$ is defined over F. So C descends to $\mathbb{Q}$ as a hyperelliptic curve by [Sijsling and Voight 2016, Proposition 4.8]. □

Remark 5.14. One should be able to compute an equation for C by using [Voight and Willis 2014]. However, currently, the strategy for doing so is not fully implemented. It should also be possible to use a generalisation of the p-adic approach discussed in [Franc and Masdeu 2014], which was inspired by [Kurihara 1979; 1994]. Given that the determination of equations for Shimura curves defined over totally real fields is one question that is of independent interest in its own right, we hope to return to this in the future.

Remark 5.15. We note that Michon [1981] (and also unpublished work of Ogg) provided a complete list of all hyperelliptic Shimura curves with square-free level defined over $\mathbb{Q}$. Shimura curves defined over $\mathbb{Q}$ which admit hyperelliptic quotients have also been investigated quite a bit; see, for example, [Molina 2012; González and Molina 2016; Guo and Yang 2017]. In contrast, there has been very little work on these types of questions for Shimura curves defined over totally real fields F larger than $\mathbb{Q}$. This makes Theorem 5.9 of the more striking. Indeed, not only does it give one of the few examples of Shimura curves with a hyperelliptic quotient over a totally real field, but also one whose genus is larger than most known examples over $\mathbb{Q}$.

5G. *The Jacobian varieties* $\mathbf{Jac}(X_0^D(1))$ *and* $\mathbf{Jac}(C)$. In this section, we explain the connection between the simple factors of $\mathrm{Jac}(X_0^D(1))$ and the conjectures in [Gross 2016]. There is more in [Cunningham and Dembélé 2017], where this connection is established via lifts of Hilbert modular forms.

Figure 2. The dual graph $\mathcal{G}_{st}$ of the stable model for the quotient $\mathscr{M}/\langle w_{\mathfrak{p}}\rangle$.

From the discussion in Sections 5C and 5D, we have the decomposition for $\mathrm{Jac}(X_0^D(1))$ over F (up to isogeny):

$$\mathrm{Jac}(X_0^D(1)) \sim A_f \times A_{f'} \times A_g \times A_{g'} \times A_h. \tag{1}$$

From (1), and the fact that $w_D = -w$, we see that

$$\mathrm{Jac}(C) \sim A_f \times A_{f'} \times A_g \times A_{g'}. \tag{2}$$

The fourfolds A_f and $A_{f'}$ (resp. A_g and $A_{g'}$) are Galois conjugate. We will see later that one of consequences of the compatibility between the base change action and Hecke orbits is that the decompositions (1) and (2) descend to subfields of F.

Theorem 5.16. *The abelian variety A_h descends to a* 24*-dimensional variety B_h defined over $\mathbb{Q}$, with good reduction outside* 2*, such that* $\mathrm{End}_{\mathbb{Q}}(B_h) \otimes \mathbb{Q} = K_h$ *and*

$$L(B_h, s) = \prod_{\Pi' \in [\Pi_h]} L(\Pi', s),$$

where π_h is the automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ *attached to h, Π_h it lifts to* $\mathrm{GSpin}_{17}(\mathbb{A}_{\mathbb{Q}})$*, and $[\Pi_h]$ the Hecke orbit of Π_h.*

Proof. By Table 1, there exists a generator $\tau \in \mathrm{Gal}(L_h/K_h)$ such that ${}^{\sigma}h = h^{\tau}$. So, by [Cunningham and Dembélé 2017, Theorem 5.4], π_h lifts to an automorphic representation Π_h on a split form of $\mathrm{GSpin}_{17}(\mathbb{A}_{\mathbb{Q}})$, with field of rationality the cubic field K_h. The Hecke orbit $[\Pi_h]$ of Π_h has 3 elements, and by functoriality

$$L(B_h, s) = \prod_{\Pi' \in [\Pi_h]} L(\Pi', s).$$

It follows that $\mathrm{End}_{\mathbb{Q}}(B_h) \otimes \mathbb{Q} = K_h$. Since the level of the form h is the unique prime $\mathfrak{p}$ above 2, B_h has good reduction outside 2. □

Now, we turn to the quotient $C := X_0^D(1)/\langle w_D \rangle$.

Theorem 5.17. *The abelian varieties A_f and $A_{f'}$ (resp. A_g and $A_{g'}$) descend to pairwise conjugate fourfolds B_f and $B_{f'}$ (resp. B_g and $B_{g'}$) over $\mathbb{Q}(\sqrt{2})$, with trivial endomorphism rings, such that*

$$L(B_f, s) = L(\Pi_f, s) \quad \text{and} \quad L(B_{f'}, s) = L(\Pi_{f'}, s),$$
$$L(B_g, s) = L(\Pi_g, s) \quad \text{and} \quad L(B_{g'}, s) = L(\Pi_{g'}, s),$$

where $\pi_f, \pi_{f'}, \pi_g$ and $\pi_{g'}$ are the automorphic representations of $\mathrm{GL}_2(\mathbb{A}_F)$ *attached to f, f', g and g', respectively; and Π_f, $\Pi_{f'}$, Π_g and $\Pi_{g'}$ their respective lifts to* $\mathrm{GSpin}_9/\mathbb{Q}(\sqrt{2})$*. They have good reduction outside* $(\sqrt{2})$.

Proof. The identities in Table 1, combined with [Cunningham and Dembélé 2017, Theorem 5.4], implies that $\pi_f, \pi_{f'}, \pi_g$ and $\pi_{g'}$ indeed lift to automorphic representations $\Pi_f, \Pi_{f'}, \Pi_g$ and $\Pi_{g'}$ on $\mathrm{GSpin}_9/\mathbb{Q}(\sqrt{2})$ with field of rationality $\mathbb{Q}$. Consequently, the fourfolds A_f, $A_{f'}$, A_g and $A_{g'}$ descend to pairwise conjugate fourfolds B_f and $B_{f'}$ (resp. B_g and $B_{g'}$) such that

$$\mathrm{End}_{\mathbb{Q}(\sqrt{2})}(B_f) = \mathrm{End}_{\mathbb{Q}(\sqrt{2})}(B_{f'}) = \mathrm{End}_{\mathbb{Q}(\sqrt{2})}(B_g) = \mathrm{End}_{\mathbb{Q}(\sqrt{2})}(B_{g'}) = \mathbb{Z}.$$

The equalities of L-series follow by functoriality. For the same reason as above, the fourfolds have good reduction outside $(\sqrt{2})$. □

Remark 5.18. The decomposition (1) is only true *a priori* over F. However, Theorem 5.16 and Theorem 5.17 imply that it descends to $\mathbb{Q}(\sqrt{2})$. In fact, the products $A_f \times A_{f'}$ (resp. $A_g \times A_{g'}$) further descend to $\mathbb{Q}$. And so, the decomposition (1) will descend to $\mathbb{Q}$ if we group them accordingly.

5H. ***The connectedness of*** **Spec($\mathbb{T}$).** Let $\mathbb{T}$ be the $\mathbb{Z}$-subalgebra of $\mathrm{End}_{\mathbb{C}}(S_2^D(1))$ acting on $S_2^D(1)$. We recall that $S_2^D(1)$ is isomorphic to $S_2(\mathfrak{p})^{\mathrm{new}}$ as a Hecke module.

Proposition 5.19. Spec($\mathbb{T}$) *is connected.*

Proof. The curve $X_0^D(1)$ is a Shimura curve of prime level, and each Hecke constituent appears with multiplicity one. So, the proof in [Mazur 1977, Proposition 10.6] applies readily. □

The following two propositions determine the congruences which realise the connectedness of Spec($\mathbb{T}$).

Proposition 5.20. *The forms f, f', g and g' are congruent modulo* 5.

Proof. The prime 5 is totally ramified in $L_f = L_{f'}$. Let $\mathfrak{P}_5$ be the unique prime above it, and $\rho_{f,5}, \rho_{f',5} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathcal{O}_{L_f,\mathfrak{P}_5})$ the $\mathfrak{P}_5$-adic representations attached to f and f', respectively. By reduction modulo $\mathfrak{P}_5$, we get two representations $\bar{\rho}_{f,5}, \bar{\rho}_{f',5} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathbb{F}_5)$. From Table 1, we have and ${}^{\sigma}f = f'$, ${}^{\sigma^2}f = f^{\tau}$. Also, since $\mathfrak{P}_5$ is totally ramified in L_f, we have $\tau(\mathfrak{P}_5) = \mathfrak{P}_5$. It follows that $\bar{\rho}_{f,5} = \bar{\rho}_{f',5}$ is a base change from $\mathbb{Q}(\sqrt{2})$. The prime 5 is also totally ramified in $L_g = L_{g'}$. With obvious notations, the same argument as above shows that $\bar{\rho}_{g,5} = \bar{\rho}_{g',5}$ is also a base change from $\mathbb{Q}(\sqrt{2})$.

By using the multiplicity one argument in [Billerey et al. 2018, §6], we show that $\bar{\rho}_{f,5} \simeq \bar{\rho}_{g,5}$. This implies that f, f', g and g' are congruent modulo 5. □

Proposition 5.21. *The forms f, f' and h are congruent modulo* 3.

Proof. There is a unique prime $\mathfrak{P}_3$ above 3 in $L_f = L_{f'}$; it has inertia degree 2 and ramification degree 2. Let $\rho_{f,3}, \rho_{f',3} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathcal{O}_{L_f,\mathfrak{P}_3})$ the $\mathfrak{P}_3$-adic representations attached to f and f', respectively. By reduction modulo $\mathfrak{P}_3$, we get two representations $\bar{\rho}_{f,3}, \bar{\rho}_{f',3} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathbb{F}_9)$. From Table 1, we have and ${}^{\sigma}f = f'$, ${}^{\sigma^2}f = f^{\tau}$. Also, since $\mathfrak{P}_3$ is the unique prime above 3 in L_f, we have $\tau(\mathfrak{P}_3) = \mathfrak{P}_3$. It follows that $\bar{\rho}_{f,3} = \bar{\rho}_{f',3}$ is a base change from $\mathbb{Q}(\zeta_{16})^+$.

In the cubic subfield K_h of L_h, the prime 3 factors as $(3) = \mathfrak{p}_3\mathfrak{p}_3'$, where $\mathfrak{p}_3$ has inertia degree 1, and $\mathfrak{p}_3'$ inertia degree 2. The prime $\mathfrak{p}_3'$ is totally ramified in L_h. We let $\mathfrak{P}_3'$ be the unique prime above it, and $\rho_{h,3} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathcal{O}_{L_h,\mathfrak{P}_3'})$ the $\mathfrak{P}_3'$-adic representation attached to h. By reduction modulo $\mathfrak{P}_3'$, we get a representation $\bar{\rho}_{h,3} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathbb{F}_9)$. From Table 1, we have and ${}^{\sigma}h = h^{\tau}$. Also, since $\mathfrak{P}_3'$ is the unique prime above $\mathfrak{p}_3'$ in L_h, we have $\tau(\mathfrak{P}_3') = \mathfrak{P}_3'$. It follows that $\bar{\rho}_{h,3}$ is also a base change from $\mathbb{Q}(\zeta_{16})^+$.

By using the multiplicity one argument in [Billerey et al. 2018, §6], we show that $\bar{\rho}_{f,3} \simeq \bar{\rho}_{h,3}$. This implies that f, f' and h are congruent modulo 3. □

6. The 2-torsion field of Jac($X_0^D(1)$) and the Harbater field

The main result of this section establishes that every simple factor of $\mathrm{Jac}(X_0^D(1))$ has a 2-torsion field whose normal closure is the Harbater field. We start with the following theorem.

Theorem 6.1. *Let N the field of* 2*-torsion of* Jac(C) *over* $\mathbb{Q}$*. Then N is the Harbater field.*

Proof. Keeping the notation in the proof of Theorem 5.9, N is the normal closure of M. It follows from this, and direct calculations, that $\mathrm{Gal}(N/\mathbb{Q}) \simeq F_{17}$. By construction, N is unramified outside 2 and ∞.

However, by [Harbater 1994, Theorem 2.25], there is a unique Galois number field unramified outside 2 and ∞, with Galois group F_{17}. So N must be the Harbater field. □

Remark 6.2. The field N is the splitting field of the polynomial

$$H := x^{17}-2x^{16}+8x^{13}+16x^{12}-16x^{11}+64x^9-32x^8-80x^7+32x^6+40x^5+80x^4+16x^3-128x^2-2x+68.$$

This polynomial was computed by Noam Elkies following a `mathoverflow.net` discussion [Rouse and Elkies 2014] initiated by Jeremy Rouse. We thank David P. Roberts for bringing this discussion to our attention.

6A. ***The mod 2 Hecke eigensystems.*** Let $\mathbb{T}_f$, $\mathbb{T}_{f'}$ $\mathbb{T}_g$, $\mathbb{T}_{g'}$ and $\mathbb{T}_h$ be the $\mathbb{Z}$-subalgebras acting on the Hecke constituents of f, f', g, g' and h respectively. From the discussion in Section 5C, we have

$$\begin{aligned}\mathbb{T}\otimes\mathbb{Q} &= (\mathbb{T}_f\otimes\mathbb{Q})\times(\mathbb{T}_{f'}\otimes\mathbb{Q})\times(\mathbb{T}_g\otimes\mathbb{Q})\times(\mathbb{T}_{g'}\otimes\mathbb{Q})\times(\mathbb{T}_h\otimes\mathbb{Q})\\ &= L_f\times L_{f'}\times L_g\times L_{g'}\times L_h.\end{aligned}$$

By direct calculations, we get the following:

- $[\mathcal{O}_{L_f} : \mathbb{T}_f] = [\mathcal{O}_{L_{f'}} : \mathbb{T}_{f'}]$ divides 3,
- $[\mathcal{O}_{L_g} : \mathbb{T}_g] = [\mathcal{O}_{L_{g'}} : \mathbb{T}_{g'}] = 1$,
- $[\mathcal{O}_{L_h} : \mathbb{T}_h]$ divides $3\cdot 5^6$.

Therefore $\mathbb{T}\otimes\mathbb{Z}_2$ decomposes into $\mathbb{Z}_2$-algebras as

$$\mathbb{T}\otimes\mathbb{Z}_2 = (\mathbb{T}_f\otimes\mathbb{Z}_2)\times(\mathbb{T}_{f'}\otimes\mathbb{Z}_2)\times(\mathbb{T}_g\otimes\mathbb{Z}_2)\times(\mathbb{T}_{g'}\otimes\mathbb{Z}_2)\times(\mathbb{T}_h\otimes\mathbb{Z}_2).$$

The prime 2 is inert in $L_f = L_{f'}$, and $L_g = L_{g'}$, so the first four factors are local $\mathbb{Z}_2$-algebras. Let $\mathfrak{m}_f$, $\mathfrak{m}_{f'}$, $\mathfrak{m}_g$ and $\mathfrak{m}_{g'}$ be the corresponding maximal ideals. Then, by the identities in Table 1, we have $\sigma(\mathfrak{m}_f) = \mathfrak{m}_{f'}$ and $\sigma^2(\mathfrak{m}_f) = \tau_f(\mathfrak{m}_f)$ for some $\tau_f \in \mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2)$; and $\sigma(\mathfrak{m}_g) = \mathfrak{m}_{g'}$ and $\sigma^2(\mathfrak{m}_g) = \tau_g(\mathfrak{m}_g)$ for some $\tau_g \in \mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2)$. We let $\theta_f, \theta_{f'}, \theta_g, \theta_{g'} : \mathbb{T}\otimes\mathbb{Z}_2 \to \mathbb{F}_{16}$ be the corresponding mod 2 Hecke eigensystems.

Next, we recall that L_h is the ray class field of conductor $\mathfrak{c} = \left(\frac{1}{2}(c^2 - 16c + 25)\right)$ over the field $K_h = \mathbb{Q}(c)$, with $c^3 + c^2 - 229c + 167 = 0$. The prime 2 is totally ramified in K_h. Letting $\mathfrak{p}_2$ be the unique prime above it, we get that $\mathfrak{p}_2 = \mathfrak{P}\mathfrak{P}'$, where $\mathfrak{P}$ and $\mathfrak{P}'$ are inert primes, and $\tau(\mathfrak{P}) = \mathfrak{P}'$. Therefore, there are two maximal ideals $\mathfrak{m}_h$ and $\mathfrak{m}'_h$ in $\mathbb{T}_h\otimes\mathbb{Z}_2$ such that $\sigma(\mathfrak{m}_h) = \mathfrak{m}'_h$ and $\sigma^2(\mathfrak{m}_h) = \tau_h(\mathfrak{m}_h)$. We let $\theta_h, \theta'_h : \mathbb{T}\otimes\mathbb{Z}_2 \to \mathbb{F}_{16}$ be the resulting two mod 2 Hecke eigensystems.

Proposition 6.3. *The forms f, f', g, g' and h give rise to two mod 2 Hecke eigensystems θ and θ' that $\theta' = \theta\circ\sigma$ and $\theta\circ\sigma^2 = \bar{\tau}\circ\theta$, where $\mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2) = \langle\bar{\tau}\rangle$. Up to relabelling, we have $\theta = \theta_f = \theta_g = \theta_h$, and $\theta' = \theta_{f'} = \theta_{g'} = \theta'_h$.*

Proof. We will apply the multiplicity one argument in [Billerey et al. 2018, §6] to deduce that, up to relabelling, $\theta_f = \theta_g = \theta_h$, and $\theta_{f'} = \theta_{g'} = \theta'_h$. Let M be the underlying $\mathbb{F}_2$-module to $\mathbb{T}\otimes\mathbb{F}_2$. Then, the pair $(\theta_f, \theta_{f'})$ comes from two simple Hecke constituents of dimension 4 over $\mathbb{F}_2$ that are conjugate by the

action of $\mathrm{Gal}(F/\mathbb{Q})$. These Hecke constituents belong to the socle S of M, i.e., the largest semisimple $\mathbb{T}\otimes\mathbb{F}_2$-submodule of M. Likewise for the pairs $(\theta_g,\theta_{g'})$ and (θ_h,θ_h'). Let $\mathbb{T}'$ be the $\mathbb{Z}$-subalgebra of $\mathbb{T}$ generated by the Hecke operators $T_{\mathfrak{p}}$, with $\mathrm{N}\,\mathfrak{p}\le 1000$. We view M as a $\mathbb{T}'\otimes\mathbb{F}_2$-module, and let S' be its socle. By direct calculations in `Magma`, we show that S' has two irreducible constituents, and each constituent has dimension 4 and multiplicity one. Furthermore, each of those constituents decomposes into 4 one-dimensional Hecke constituents over $\mathbb{T}'\otimes\mathbb{F}_{16}$. This means that S' must necessarily be the socle of M viewed as a $\mathbb{T}\otimes\mathbb{F}_2$-module, and that its $\mathbb{T}'\otimes\mathbb{F}_{16}$-decomposition is also the $\mathbb{T}\otimes\mathbb{F}_{16}$-decomposition of S. By comparing these one-dimensional $\mathbb{F}_{16}$-valued Hecke eigensystems with the reduction modulo 2 of the Hecke eigenvalues of the newforms in $S_2^D(1)$, we see that $\theta_f=\theta_g=\theta_h$, and $\theta_{f'}=\theta_{g'}=\theta_h'$, up to relabelling. The identities $\theta'=\theta\circ\sigma$ and $\theta\circ\sigma^2=\bar{\tau}\circ\theta$ follow from the relations between the forms. □

6B. *The fields of* 2*-torsion of the simple factors of* $\mathbf{Jac}(X_0^D(1))$.

Theorem 6.4. *Let A be a simple factor of* $\mathrm{Jac}(X_0^D(1))$, *and $M=F(A[2])$ the field of* 2*-torsion of A. Then, the normal closure of M is the Harbater field N.*

We will give two proofs of this result, starting with the simplest one.

First proof of Theorem 6.4. In light of Proposition 6.3, it is enough to prove this for the simple factors of $\mathrm{Jac}(C)$. To this end, recall that

$$\mathrm{Jac}(C)\sim A_f\times A_{f'}\times A_g\times A_{g'}.$$

By Theorem 6.1, we know that the field of 2-torsion of $\mathrm{Jac}(C)$ is the Harbater field. So it is enough to show that the compositum of the fields of 2-torsion of its simple factors is also the Harbater field. But, again by Proposition 6.3, A_f and A_g have the same field of 2-torsion. It is the field M_θ cut out by the Galois representation attached to the Hecke eigensystem θ. Similarly, $A_{f'}$ and $A_{g'}$ have the same field of 2-torsion, the field $M_{\theta'}$ cut out by the Galois representation attached to θ'. Since θ and θ' are interchanged by $\mathrm{Gal}(F/\mathbb{Q})$, we must have $M_{\theta'}=M_\theta^\sigma$. Therefore M_θ and $M_{\theta'}$ have the same normal closure $N_\theta=N_{\theta'}$. By replacing the isogeny $\phi_f:\mathrm{Jac}(C)\to A_f$ if necessary, we can assume that M_θ, and hence N_θ, is a subfield of N. From the Frobenius data attached to θ, we see that the order of $\mathrm{Gal}(N_\theta/\mathbb{Q})$ is divisible by 17, hence $[N:N_\theta]\mid 16$. Since $\mathrm{Gal}(N/\mathbb{Q})\simeq F_{17}$ has no nontrivial normal subgroup whose order divides 16, we conclude that $N_\theta=N$. □

For the second proof, we need the following result.

Proposition 6.5. *Let θ and θ' be the Hecke eigensystems in Proposition 6.3, and let $\bar{\rho},\bar{\rho}':\mathrm{Gal}(\overline{\mathbb{Q}}/F)\to\mathrm{GL}_2(\mathbb{F}_{16})$ the mod* 2 *Galois representations attached to them. Then, there are characters $\chi,\chi':\mathrm{Gal}(\overline{\mathbb{Q}}/K)\to\mathbb{F}_{2^8}^\times$, with trivial conductor such that $\bar{\rho}=\mathrm{Ind}_K^F\,\chi$, and $\bar{\rho}'=\mathrm{Ind}_K^F\,\chi'$.*

Proof. We already computed the Hecke constituents of the space $S_2(1)$ in [Dembélé 2009]. The mod 2 Hecke eigensystems in that case have coefficient fields $\mathbb{F}_{2^s}$ where $s=1,2,8$. Therefore, since θ has coefficient field $\mathbb{F}_{16}$, it cannot arise from an eigenform of level 1. By the Serre conjecture for totally real fields (the totally ramified case) [Gee and Savitt 2011], it must appear on the quaternion algebra D' with

level (1) and nontrivial weight. The same is true for θ'. In fact, the analysis conducted in the proof of Proposition 6.3 also shows that they are the only eigensystems that can appear at that weight. (We note that there are only two Serre weights in this case.)

Let $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \overline{\mathbb{F}}_2^\times$ be a character with trivial conductor such that $\chi^s \neq \chi$, where $\mathrm{Gal}(K/F) = \langle s \rangle$. By class field theory, we can identity χ with its image under the Artin map. Since χ is unramified, it must factor as $\chi : K^\times \backslash \mathbb{A}_K^\times \twoheadrightarrow \mathrm{Cl}_K \to \overline{\mathbb{F}}_2^\times$. Furthermore, since $\mathrm{Cl}_K \simeq \mathbb{Z}/17\mathbb{Z}$, we must have $\chi : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{F}_{2^8}^\times$, and the representation $\bar{\rho}_\chi := \mathrm{Ind}_K^F \chi : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathbb{F}_{16})$ has coefficients in $\mathbb{F}_{16}$. So, $\bar{\rho}_\chi$ has level (1) and nontrivial weight by the argument above. Therefore, it must be isomorphic to a Galois conjugate of $\bar{\rho}$. Up to relabelling, we can assume that $\bar{\rho} \simeq \bar{\rho}_\chi$. Since θ and θ' are $\mathrm{Gal}(F/\mathbb{Q})$-conjugate, there is also a character $\chi' : K^\times \backslash \mathbb{A}_K^\times \to \mathbb{F}_{2^8}^\times$ such that $\bar{\rho}' \simeq \bar{\rho}_{\chi'}$.

Alternatively, we can show that θ appears on D' with the nontrivial weight without using the fact that it has coefficients in $\mathbb{F}_{16}$. Indeed, we have

$$\bar{\rho}_\chi|_{I_\mathfrak{p}} \simeq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

Let $K_\mathfrak{P}$ be the completion of K at $\mathfrak{P}$, the unique prime above $\mathfrak{p}$. Since $K = F[\beta]$, and $\beta^2 = -2 - \alpha$ is a generator of $\mathfrak{p}$, then we have $K_\mathfrak{p} = F_\mathfrak{p}[\sqrt{\varpi}]$, where ϖ is a uniformiser of $F_\mathfrak{p}$. Therefore, $\bar{\rho}_\chi|_{D_\mathfrak{p}}$ doesn't arise from a finite flat group scheme. Hence, $\bar{\rho}_\chi$ must have nontrivial weight. □

We are now ready for the second proof of Theorem 6.4.

Second proof of Theorem 6.4. Let $\bar{\rho}_\theta, \bar{\rho}_{\theta'} : \mathrm{Gal}(\overline{\mathbb{Q}}/F) \to \mathrm{GL}_2(\mathbb{F}_{16})$ be the mod 2 Galois representations attached to the eigensystems θ and θ'. By Proposition 6.5, $\bar{\rho}_\theta$ and $\bar{\rho}_{\theta'}$ are dihedral and we have that $\mathrm{im}(\bar{\rho}_\theta) = \mathrm{im}(\bar{\rho}_{\theta'}) = D_{17}$. Let M_θ, $M_{\theta'}$ be the fields cut out by $\bar{\rho}_\theta$ and $\bar{\rho}_{\theta'}$; and N_θ and $N_{\theta'}$ the normal closure of M_θ and $M_{\theta'}$, respectively. By Proposition 6.3, we have $M_{\theta'} = M_\theta^\sigma$, hence $N_\theta = N_{\theta'}$. Also, by construction M_θ and M_θ^σ are unramified extension of K. So, by uniqueness of the Hilbert class field, we must have $M_\theta = M_\theta^\sigma = M_\theta M_\theta^\sigma = H_K$, where $M_\theta M_\theta^\sigma$ is the compositum of M_θ and M_θ^σ; and H_K is the Hilbert class field of K. Since $\theta \circ \sigma^2 = \bar{\tau} \circ \theta$, we have

$$\mathrm{Gal}(N_\theta/\mathbb{Q}) = D_{17} \rtimes \mathbb{Z}/8\mathbb{Z} = F_{17}.$$

Again by [Harbater 1994, Theorem 2.25], we must have $N = N_\theta = N_{\theta'}$. □

Remark 6.6. From Theorem 6.4, we see that none of the fourfolds A_f, $A_{f'}$, A_g or $A_{g'}$ can be the Jacobian of a hyperelliptic curve since the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$ on the points of 2-torsion cannot factor through S_{10} (see Section 2C). However, as we explained earlier, A_f, $A_{f'}$, A_g and $A_{g'}$ descend, separately, into pairwise conjugate abelian varieties over $\mathbb{Q}(\sqrt{2})$. And the products $A_f \times A_{f'}$ and $A_g \times A_{g'}$ are 8-dimensional abelian varieties which further descend to $\mathbb{Q}$. So, we conclude with the following questions. Do there exist hyperelliptic curves C_f and C_g defined over F such that

$$\mathrm{Jac}(C_f) \sim A_f \times A_{f'} \quad \text{and} \quad \mathrm{Jac}(C_g) \sim A_g \times A_{g'}?$$

If so, do these two curves descend to $\mathbb{Q}$ as well? We were asked these two questions by Noam Elkies in an email. An affirmative answer to them would mean that the Harbater field is given by hyperelliptic curves of genus 8, which is much smaller. A priori, the hyperelliptic polynomials of these curves should have degree 18. However, the structure of the Galois group $\mathrm{Gal}(N/\mathbb{Q}) = F_{17}$ indicates that one of their roots would be rational and could be moved to ∞. This means that the hyperelliptic polynomials of the curves C_f and C_g would in fact have degree 17, the same as that of the Elkies polynomial displayed earlier.

Acknowledgements

I would like to thank Frank Calegari for several helpful email exchanges; Vladimir Dokchitser and Céline Maistret for some useful discussion; and Jeroen Sijsling for carefully reading an earlier draft of this work. I would also like to give a special thanks to John Voight as this note owes a lot to the lengthy discussions I had with him on this topic. I learned of the discussion about the Harbater field between Jeremy Rouse and Noam D. Elkies from David P. Roberts who pointed us to the `mathoverflow.net` post related to this. So, I would like to thank him for this. During the course of this project, I stayed at the following institutions: Dartmouth College, King's College London, the Max Planck Institute for Mathematics in Bonn, and the University of Barcelona; I would like to thank them for their generous hospitality. I also thank the referees for many helpful suggestions. Finally, as alluded to earlier, this note originated with a question of Benedict Gross. So I would like to thank him for this, and for his constant encouragement.

References

[Billerey et al. 2018] N. Billerey, I. Chen, L. Dembélé, L. Dieulefait, and N. Freitas, "Some extensions of the modular method and Fermat equations of signature $(13, 13, n)$", preprint, 2018. arXiv

[Borel 1981] A. Borel, "Commensurability classes and volumes of hyperbolic 3-manifolds", *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) **8**:1 (1981), 1–33. MR Zbl

[Boutot and Carayol 1991] J.-F. Boutot and H. Carayol, "Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfel'd", pp. 45–158 in *Courbes modulaires et courbes de Shimura* (Orsay, France, 1987/1988), Astérisque **196-197**, Soc. Math. France, Paris, 1991. MR Zbl

[Boutot and Zink 1995] J.-F. Boutot and T. Zink, "The p-adic uniformization of Shimura curves", preprint, 1995.

[Carayol 1986] H. Carayol, "Sur la mauvaise réduction des courbes de Shimura", *Compos. Math.* **59**:2 (1986), 151–230. MR Zbl

[Chinburg and Friedman 1999] T. Chinburg and E. Friedman, "An embedding theorem for quaternion algebras", *J. Lond. Math. Soc.* (2) **60**:1 (1999), 33–44. MR Zbl

[Cunningham and Dembélé 2017] C. Cunningham and L. Dembélé, "Lifts of Hilbert modular forms and application to modularity of abelian varieties", preprint, 2017. arXiv

[Deligne 1971] P. Deligne, "Travaux de Shimura", exposé 389, pp. 123–165 in *Séminaire Bourbaki,* 1970/1971, Lecture Notes in Math. **244**, Springer, 1971. MR Zbl

[Deligne and Mumford 1969] P. Deligne and D. Mumford, "The irreducibility of the space of curves of given genus", *Inst. Hautes Études Sci. Publ. Math.* **36** (1969), 75–109. MR Zbl

[Dembélé 2009] L. Dembélé, "A non-solvable Galois extension of $\mathbb{Q}$ ramified at 2 only", *C. R. Math. Acad. Sci. Paris* **347**:3-4 (2009), 111–116. MR Zbl

[Dembélé and Donnelly 2008] L. Dembélé and S. Donnelly, "Computing Hilbert modular forms over fields with nontrivial class group", pp. 371–386 in *Algorithmic number theory*, edited by A. J. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011**, Springer, 2008. MR Zbl

[Dembélé and Voight 2013] L. Dembélé and J. Voight, "Explicit methods for Hilbert modular forms", pp. 135–198 in *Elliptic curves, Hilbert modular forms and Galois deformations*, edited by H. Darmon et al., Birkhäuser, Basel, 2013. MR Zbl

[Doi and Naganuma 1967] K. Doi and H. Naganuma, "On the algebraic curves uniformized by arithmetical automorphic functions", *Ann. of Math.* (2) **86** (1967), 449–460. MR Zbl

[Farkas and Kra 1980] H. M. Farkas and I. Kra, *Riemann surfaces*, Grad. Texts in Math. **71**, Springer, 1980. MR Zbl

[Franc and Masdeu 2014] C. Franc and M. Masdeu, "Computing fundamental domains for the Bruhat–Tits tree for $\mathrm{GL}_2(\mathbb{Q}_p)$, p-adic automorphic forms, and the canonical embedding of Shimura curves", *LMS J. Comput. Math.* **17**:1 (2014), 1–23. MR Zbl

[Gee and Savitt 2011] T. Gee and D. Savitt, "Serre weights for mod p Hilbert modular forms: the totally ramified case", *J. Reine Angew. Math.* **660** (2011), 1–26. MR Zbl

[González and Molina 2016] J. González and S. Molina, "The kernel of Ribet's isogeny for genus three Shimura curves", *J. Math. Soc. Japan* **68**:2 (2016), 609–635. MR Zbl

[Greenberg and Voight 2011] M. Greenberg and J. Voight, "Computing systems of Hecke eigenvalues associated to Hilbert modular forms", *Math. Comp.* **80**:274 (2011), 1071–1092. MR Zbl

[Gross 2016] B. H. Gross, "On the Langlands correspondence for symplectic motives", *Izv. Ross. Akad. Nauk Ser. Mat.* **80**:4 (2016), 49–64. In Russian; translated in *Izv. Math.* **80**:4 (2016), 678–692. MR Zbl

[Guo and Yang 2017] J.-W. Guo and Y. Yang, "Equations of hyperelliptic Shimura curves", *Compos. Math.* **153**:1 (2017), 1–40. MR Zbl

[Harbater 1994] D. Harbater, "Galois groups with prescribed ramification", pp. 35–60 in *Arithmetic geometry* (Tempe, AZ, 1993), edited by N. Childress and J. W. Jones, Contemp. Math. **174**, Amer. Math. Soc., Providence, RI, 1994. MR Zbl

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Grad. Texts in Math. **201**, Springer, 2000. MR Zbl

[Jones 2010] J. W. Jones, "Number fields unramified away from 2", *J. Number Theory* **130**:6 (2010), 1282–1291. MR Zbl

[Kontogeorgis and Rotger 2008] A. Kontogeorgis and V. Rotger, "On the non-existence of exceptional automorphisms on Shimura curves", *Bull. Lond. Math. Soc.* **40**:3 (2008), 363–374. MR Zbl

[Kurihara 1979] A. Kurihara, "On some examples of equations defining Shimura curves and the Mumford uniformization", *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* **25**:3 (1979), 277–300. MR Zbl

[Kurihara 1994] A. Kurihara, "On p-adic Poincaré series and Shimura curves", *Int. J. Math.* **5**:5 (1994), 747–763. MR Zbl

[Maclachlan 2006] C. Maclachlan, "Torsion in arithmetic Fuchsian groups", *J. Lond. Math. Soc.* (2) **73**:1 (2006), 14–30. MR Zbl

[Maclachlan 2009] C. Maclachlan, "Existence and non-existence of torsion in maximal arithmetic Fuchsian groups", *Groups Complex. Cryptol.* **1**:2 (2009), 287–295. MR Zbl

[Magma 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I: The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Mazur 1977] B. Mazur, "Modular curves and the Eisenstein ideal", *Inst. Hautes Études Sci. Publ. Math.* **47** (1977), 33–186. MR Zbl

[Michon 1981] J.-F. Michon, "Courbes de Shimura hyperelliptiques", *Bull. Soc. Math. France* **109**:2 (1981), 217–225. MR Zbl

[Molina 2012] S. Molina, "Equations of hyperelliptic Shimura curves", *Proc. Lond. Math. Soc.* (3) **105**:5 (2012), 891–920. MR Zbl

[Nekovář 2012] J. Nekovář, "Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight two", *Canad. J. Math.* **64**:3 (2012), 588–668. MR Zbl

[Rouse and Elkies 2014] J. Rouse and N. Elkies, "Degree 17 number fields ramified only at 2", MathOverflow thread, 2014, available at https://mathoverflow.net/q/172148.

[Sage 2019] W. A. Stein et al., "Sage mathematics software", 2019, available at http://www.sagemath.org. Version 8.7.

[Shimura 1970] G. Shimura, "On canonical models of arithmetic quotients of bounded symmetric domains", *Ann. of Math.* (2) **91** (1970), 144–222. MR Zbl

[Sijsling 2013] J. Sijsling, "Canonical models of arithmetic (1; e)-curves", *Math. Z.* **273**:1-2 (2013), 173–210. MR Zbl

[Sijsling and Voight 2016] J. Sijsling and J. Voight, "On explicit descent of marked curves and maps", *Res. Number Theory* **2** (2016), art. id. 27. MR Zbl

[Tian and Xiao 2016] Y. Tian and L. Xiao, "On Goren–Oort stratification for quaternionic Shimura varieties", *Compos. Math.* **152**:10 (2016), 2134–2220. MR Zbl

[Vignéras 1980] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math. **800**, Springer, 1980. MR Zbl

[Voight 2005] J. M. Voight, *Quadratic forms and quaternion algebras: algorithms and arithmetic*, Ph.D. thesis, University of California, Berkeley, 2005, available at https://search.proquest.com/docview/305032530.

[Voight 2009] J. Voight, "Computing fundamental domains for Fuchsian groups", *J. Théor. Nombres Bordeaux* **21**:2 (2009), 469–491. MR Zbl

[Voight 2018] J. Voight, "Quaternion algebras", preprint, 2018, available at https://tinyurl.com/voightquat.

[Voight and Willis 2014] J. Voight and J. Willis, "Computing power series expansions of modular forms", pp. 331–361 in *Computations with modular forms* (Heidelberg, 2011), edited by G. Böckle and G. Wiese, Contrib. Math. Comput. Sci. **6**, Springer, 2014. MR Zbl

Communicated by Bjorn Poonen
Received 2019-07-24 Revised 2020-02-27 Accepted 2020-03-28

lassina.dembele@gmail.com *Department of Mathematics, University of Luxembourg, Luxembourg*