HAL open science

Computation of a cover of Shimura curves using a Hurwitz space

Emmanuel Hallouin

▶ To cite this version:

Emmanuel Hallouin. Computation of a cover of Shimura curves using a Hurwitz space. Journal of Algebra, 2009, 351 (2), pp.558-566. hal-00975438

HAL Id: hal-00975438
https://hal.science/hal-00975438v1

Submitted on 8 Apr 2014

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Computation of a cover of Shimura curves using a Hurwitz space

Emmanuel Hallouin*

November 16, 2013

Summary — Using a Hurwitz space computation, we determine the canonical model of the cover of Shimura curves $\mathcal{X}_0(2) \to \mathcal{X}(1)$ associated to the quaternion algebra over the cubic field of discriminant 13^2, which is ramified at exactly two real places and unramified at finite places. Then, we list the coordinates of some rational CM points on $\mathcal{X}(1)$.

Introduction

In his classic "Shimura curve computations" [Elk98], Elkies considers Shimura curves from a computational point of view. He explicitly determines covers between Shimura curves associated to the same quaternion algebra and also coordinates of some CM points of those curves. His approach relies mostly on the uniformization of these curves by a quotient of the hyperbolic plane. Several mathematicians have investigated this kind of computational challenge [Voi06, BT07, GR04]. Elkies himself published a second article on the area [Elk06], where he computes the canonical models of some Shimura curves associated with quaternion algebras whose center is one of the cubic cyclic totally real fields of discriminant $49 = 7^2$ or $81 = 9^2$ and ramified at no finite place and exactly two of the three real places of the center. He ends his article by describing the cover of Shimura curves $\mathcal{X}_0(2) \to \mathcal{X}(1)$ (see §1 for definitions) for the cubic field K of discriminant 13^2. More precisely, he shows that the curve $\mathcal{X}(1)$ has genus zero and that the cover $\mathcal{X}_0(2) \to \mathcal{X}(1)$ is a degree 9 cover with a certain ramification behavior. But he does not compute equations for the canonical model of this cover. In this work, we compute such a model explicitly.

We also illustrate the utility of the computation of Hurwitz spaces. A great tool to compute an explicit model of a cover of $\mathbb{P}^1_{\mathbb{C}}$ with given ramification data is to consider the whole family of covers having this ramification data. This kind of family is parameterized by a moduli space called a Hurwitz space. Hurwitz spaces date back to Hurwitz himself [Hur91] and they show up in the classical study of moduli of curves. More recently, they have been studied in

*Institut de Mathématiques de Toulouse (Laboratoire Émile Picard), University of Toulouse II, France.

the context of inverse Galois theory by many authors including Fried, Völklein, Malle, Matzat, Debes [FV91, Völ96, MM99, DF94]. At the same time, they have been considered from a computational point of view [MM99, Cou99]. As we will see, they can also be very useful when looking for explicit models of interesting curves, such as Shimura curves.

The connection between Hurwitz spaces and the Shimura cover computed here is that the latter belongs to a family of degree 9 covers of $\mathbb{P}^1_{\mathbb{C}}$ with Galois group $PSL_2(\mathbb{F}_8)$. A precise definition of this family is given at the beginning of §2. This family is parameterized by one Hurwitz space. This Hurwitz space and the associated universal family can be computed, using deformation methods, as in our previous work [Hal05]. Then the computation of the Shimura curve is reduced to finding the corresponding parameter in the Hurwitz space. This parameter is characterized by the existence of extra automorphisms.

The paper is organized as follows. In §1, we study the cover $\mathcal{X}_0(2) \to \mathcal{X}(1)$ in detail, focusing on the fields of definition of the cover and of the elliptic points. We use Shimura and Deligne's theory of canonical models. In §2, we show that the existence of an extra automorphism of $\mathcal{X}_0(2)$, the Atkin-Lehner involution of $\mathcal{X}_0(2)$, results in the existence of relations between branch points of the cover $\mathcal{X}_0(2) \to \mathcal{X}(1)$. We show that these relations characterize a non-trivial closed subset of the moduli space. Since this Hurwitz space has dimension 1, only a finite number of values of the parameter can appear; in fact there is exactly one such value, the one corresponding to the Shimura cover we are looking for. Once we explicitly know the map $\mathcal{X}_0(2) \to \mathcal{X}(1)$ and the Atkin-Lehner involution, it is an easy task to deduce the coordinates of some CM points on $\mathcal{X}(1)$. In §3, we obtain, this way, some rational CM points on $\mathcal{X}(1)$.

Acknowledgments: The author would like to thank Jean-Marc Couveignes for helping him to give a more geometric flavor to this paper, Anne Hernandez for having very kindly corrected his English and the anonymous referee for having extremely carefully read the first submitted version of this work.

1 The cover of Shimura curves

In this section we will introduce several Shimura curves and give some of their properties; we refer to Shimura's initial article [Shi67] for this section. The book by Alsina and Bayer [AB04] is also a very concrete reference, even if it only deals with Shimura curves associated to quaternion algebras over $\mathbb{Q}$. We will need some classical results about the arithmetic of quaternion algebras; besides Vignéras' classic [Vig80] on this subject, we recommend the book by Maclachlan and Reid [MR03].

Let K be the unique cyclic cubic field of discriminant 13^2 which can be obtained by adjoining to $\mathbb{Q}$ a root θ_0 of $x^3 + x^2 - 4x + 1 \in \mathbb{Q}[x]$. It has narrow class number one and thus class number one. We denote by $\sigma_1, \sigma_2, \sigma_3$, $1 \leq i \leq 3$, the three real embeddings of K into $\mathbb{R}$.

The quaternion algebra. Let B be the quaternion algebra over K which is ramified at σ_2 and σ_3 and nowhere else; the algebra B is unique up to K-

algebra isomorphism. The unramified place σ_1 gives rise to an embedding $i_\infty : B \hookrightarrow M_2(\mathbb{R})$ which restricts to σ_1 on K. Let $\mathcal{O}$ be a maximal order in B; the ring $\mathcal{O}$ is unique up to conjugation in B since K has narrow class number one [MR03, Theorem 6.7.6]. We denote by $\mathcal{O}^1$ the group of invertible elements of $\mathcal{O}$ of reduced norm 1. Then the group $\Gamma(1) = i_\infty(\mathcal{O}^1)/\{\pm 1\}$ is an arithmetic Fuchsian group [Vig80, Chapter IV, §1, Example 5], and in particular a discrete subgroup of $PSL_2(\mathbb{R})$.

The Shimura curves. Let $\mathcal{H}$ be the upper half-plane. The group $PSL_2(\mathbb{R})$ acts on $\mathcal{H}$ via $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).\tau = \frac{a\tau+b}{c\tau+d}$. The quotient $\Gamma(1)\backslash\mathcal{H}$ can be given the structure of a compact Riemann surface. Let us denote by $\mathcal{X}(1)_\mathbb{C}$ the associated complex algebraic curve.

Let $\mathbb{Q}_8$ denote the unique unramified degree 3 extension of the 2-adic field $\mathbb{Q}_2$. The prime 2 is inert in K and unramified in B, so we have an embedding $i_2 : B \hookrightarrow M_2(\mathbb{Q}_8)$ in such a way that $i_2(\mathcal{O}) = M_2(\mathbb{Z}_8)$. Let $\mathcal{O}_2$ be the suborder defined by:

$$\mathcal{O}_2 = \{\omega \in \mathcal{O} : i_2(\omega) \text{ is upper triangular modulo } 2\}.$$

It is an Eichler order of level 2 [MR03, Definition 6.6.6]. We denote by $\mathcal{O}_2^1$ the group of units of reduced norm 1 and then consider the subgroups $\Gamma(2) \subset \Gamma_0(2)$ of $\Gamma(1)$ defined as follows:

$$\begin{aligned} \Gamma_0(2) &= i_\infty\left(\mathcal{O}_2^1\right)/\{\pm 1\} \\ \Gamma(2) &= i_\infty\left(\left\{\omega \in \mathcal{O}_2^1 : i_2(\omega) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod 2\right\}\right)/\{\pm 1\}. \end{aligned}$$

These are also discrete subgroups of $PSL_2(\mathbb{R})$. The quotients of $\mathcal{H}$ by these subgroups can also be given the structure of a compact Riemann surface; we respectively denote by $\mathcal{X}_0(2)_\mathbb{C}$ and $\mathcal{X}(2)_\mathbb{C}$ the corresponding complex algebraic curves. We have the tower:

$$\begin{tikzcd} \mathcal{X}(2)_\mathbb{C} \arrow[r, "56"] \arrow[rr, bend left, "PSL_2(\mathbb{F}_8)"] & \mathcal{X}_0(2)_\mathbb{C} \arrow[r, "9"] & \mathcal{X}(1)_\mathbb{C} \end{tikzcd}$$

The cover $\mathcal{X}(2)_\mathbb{C} \to \mathcal{X}(1)_\mathbb{C}$ is the Galois closure of the cover $\mathcal{X}_0(2)_\mathbb{C} \to \mathcal{X}(1)_\mathbb{C}$.

The field $K(\sqrt{-2})$ embeds in B and there exists $\omega_2 \in \mathcal{O}$ such that $\omega_2^2 + 2 = 0$. This element normalizes the Eichler order $\mathcal{O}_2$ and its image $i_\infty(\omega_2) \in PSL_2(\mathbb{R})$ normalizes the group $\Gamma_0(2)$. It induces an a morphism $w_2 : \mathcal{X}_0(2)_\mathbb{C} \to \mathcal{X}_0(2)_\mathbb{C}$ which is an involution since $\omega_2^2 \in \mathbb{R}$. It is called the Atkin-Lehner involution on $\mathcal{X}_0(2)_\mathbb{C}$.

The cover $\mathcal{X}_0(2)_\mathbb{C} \to \mathcal{X}(1)_\mathbb{C}$. Thanks to Shimizu's area formula, Elkies [Elk06, p. 314-315] proves that $\mathcal{X}(1)_\mathbb{C}$ has four elliptic points: P_0 of order 3 and P_1, P_2, P_3 of order 2. Moreover the curve $\mathcal{X}(1)_\mathbb{C}$ has genus zero. The map $\mathcal{X}_0(2)_\mathbb{C} \to \mathcal{X}(1)_\mathbb{C}$ is a cover of degree $9 = \#\mathbb{F}_8 + 1$, with Galois group $PSL_2(\mathbb{F}_8)$ (acting

on the nine points of $\mathbb{P}^1_{\mathbb{F}_8}$) and is ramified at the elliptic points P_0, P_1, P_2, P_3. Since elements of order 3 and 2 in $PSL_2(\mathbb{F}_8)$ have cycle shapes 3^3 and 2^41 respectively, the ramification data of this cover must be $(3^3, 2^41, 2^41, 2^41)$. We denote by Q_1, Q_2, Q_3 the three unramified points on $\mathcal{X}_0(2)_{\mathbb{C}}$ above P_1, P_2, P_3 respectively.

CM points. Let L be a CM extension of K and $\mathcal{O}_L$ its ring of integers. It is possible to embed the field L into the quaternion algebra B [MR03, Theorem 7.3.3], via $i : L \hookrightarrow B$, in such a way that $i^{-1}(i(L) \cap \mathcal{O}) = \mathcal{O}_L$ (it is said that the embedding i is optimal). Then all the elements of $i_\infty \circ i(L)$ share the same fixed point $\tau \in \mathcal{H}$. The image of τ in the quotient $\Gamma(1) \setminus \mathcal{H}$ is called a CM point by L on $\mathcal{X}(1)_{\mathbb{C}}$. Two embeddings i and i' give rise to the same CM point on $\mathcal{X}(1)_{\mathbb{C}}$ if and only if there exists $\omega \in \mathcal{O}^1$ such that $i' = \omega i \omega^{-1}$ or $i' = \omega \bar{i} \omega^{-1}$, where $\bar{i}$ denotes the embedding i composed with the canonical involution of B. This links the counting of CM points by L on $\mathcal{X}(1)_{\mathbb{C}}$ and the counting of the embeddings of $\mathcal{O}_L$ in $\mathcal{O}$ up to an invertible element as in Vignéras [Vig80, Chapter III, §5-C]. In our case, the final result is that there are as many CM points associated to L as the class number of $\mathcal{O}_L$ (for a very concrete introduction to CM points, see Alsina and Bayer [AB04, Chapter 6]).

Shimura-Deligne canonical model. Shimura [Shi67] proved that so-called Shimura curves admit a canonical model defined over the narrow class field of K, namely K itself here. A few years later, Deligne [Del71, Mil90] gave his own construction of these canonical models in a more functorial setting.

Concerning the curve $\mathcal{X}(1)_{\mathbb{C}}$, the *Main Theorem I* [Shi67, §3.2] implies that there exists an algebraic curve $\mathcal{X}(1)$ and a holomorphic map $j : \mathcal{H} \to \mathcal{X}(1)$ satisfying the following conditions.

- The curve $\mathcal{X}(1)$ is defined over the narrow class field of K, namely K itself.
- The map j yields an analytic isomorphism from $\Gamma(1) \setminus \mathcal{H}$ to $\mathcal{X}(1)(\mathbb{C})$.
- Let L be a CM-extension of K with class number h_L. Then there are exactly h_L points with CM by L on $\mathcal{X}(1)$. If $\tau_1, \ldots, \tau_{h_L} \in \mathcal{H}$ are the fixed points of the corresponding embeddings of L into B then the values $j(\tau_i)$, for $1 \leq i \leq h_L$, form a complete Galois orbit over K and for each i, the Hilbert class field of L is generated by $j(\tau_i)$ over L.

It is also a consequence of the *Main Theorem* that the curve $\mathcal{X}(2)_{\mathbb{C}}$ admits a canonical model: there exists an algebraic curve $\mathcal{X}(2)$ and a holomorphic map $j_2 : \mathcal{H} \to \mathcal{X}(2)$ such that:

- the curve $\mathcal{X}(2)$ is defined over the ray class field of K with modulus $2\sigma_1\sigma_2\sigma_3$ which, in that case, is K itself;
- the cover $\mathcal{X}(2) \to \mathcal{X}(1)$ is also defined over K;
- the map j_2 yields an analytic isomorphism from $\Gamma(2) \setminus \mathcal{H}$ to $\mathcal{X}(2)(\mathbb{C})$.

Being a subcover of the Galois cover $\mathcal{X}(2) \to \mathcal{X}(1)$ whose automorphisms are defined over K, the curve $\mathcal{X}_0(2)_{\mathbb{C}}$ admits also a canonical model defined over K. It will be denoted by $\mathcal{X}_0(2)$. As in the classical context of modular curves, the modular polynomial relating the functions j and $j \circ w_2$ gives a birational realization of $\mathcal{X}_0(2)$ in $\mathbb{P}^1_{\mathbb{C}} \times \mathbb{P}^1_{\mathbb{C}}$; this polynomial has coefficients in K. Finally, the involution w_2 is an automorphism of $\mathcal{X}_0(2)$ which is also defined over K.

Galois descent to $\mathbb{Q}$. Elkies [Elk98, p. 38] and Voight [Voi06, §6] show how to descend Shimura curves to $\mathbb{Q}$ in certain cases. Here we need a different argument.

The elliptic point P_0 of order 3 has CM by $K(\sqrt{-3})$ which has class number 1. It follows from Shimura's result, that the point P_0 is thus defined over K.

Similarly, the elliptic points P_1, P_2, P_3 of order 2 have CM by $K(\sqrt{-1})$ which has class number equal to 3. Thus these points must form a complete Galois orbit over K. The field $K(P_1)$ is a cyclic degree 3 extension of K and $K(P_i) = K(P_1)$ for $i = 2, 3$.

Proposition 1 *The curve $\mathcal{X}(1)$ is defined over $\mathbb{Q}$, in such a way that:*

1. *the unique elliptic point P_0 of order 3 is rational over $\mathbb{Q}$;*
2. *the three elliptic points P_1, P_2, P_3 of order 2 form a complete Galois orbit over $\mathbb{Q}$.*

The curve $\mathcal{X}_0(2)$ is defined over $\mathbb{Q}$, in such a way that:

1. *the Atkin-Lehner involution w_2 is an automorphism of $\mathcal{X}_0(2)$ defined over $\mathbb{Q}$;*
2. *the three elliptic points Q_1, Q_2, Q_3 order 2 form a complete Galois orbit over $\mathbb{Q}$ and are pointwise fixed by w_2.*

Proof — We begin with the descent for the curve $\mathcal{X}(1)$. We will in fact prove that the marked curve $\mathcal{X}(1) \setminus \{P_0\} \cup \{P_1, P_2, P_3\}$[1] descends to $\mathbb{Q}$.

Recall that the cubic field K is a Galois extension of $\mathbb{Q}$. For each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, let B^σ be the unique quaternion algebra ramified at $\sigma_2 \circ \sigma$ and $\sigma_3 \circ \sigma$ and nowhere else. The algebras B and B^σ are σ-isomorphic, meaning that there exists a $\mathbb{Q}$-isomorphism $\phi_\sigma : B \to B^\sigma$ which restricts to σ on K. The order $\mathcal{O}^\sigma = \phi_\sigma(\mathcal{O})$ is a maximal order of B^σ and the image by $i_\infty \circ \phi_\sigma^{-1}$ of the units of reduced norm 1 in $\mathcal{O}^\sigma$ is again a Fuchsian group $\Gamma(1)_\sigma \subset PSL_2(\mathbb{R})$. The corresponding Shimura curve is denoted by $\mathcal{X}^{B^\sigma}(1)_{\mathbb{C}}$, so that $\mathcal{X}(1)_{\mathbb{C}} = \mathcal{X}^B(1)_{\mathbb{C}}$. In fact, as explained in Milne [Mil90, Theorem 5.5], one has an isomorphism (of algebraic curves over K) between the canonical models $\mathcal{X}^{B^\sigma}(1)_K \simeq \mathcal{X}(1)_K^\sigma$.

By the functoriality of the Deligne's construction of canonical model [Del71, §6], the $\mathbb{Q}$-algebra isomorphism $B \to B^\sigma$ induces a K-isomorphism of canonical models $\mathcal{X}^B(1) \to \mathcal{X}^{B^\sigma}(1)$. Thanks to our previous identification, we deduce

[1] By this notation, we mean that the points P_1, P_2, P_3 are unordered. Thus an automorphism of this (affine) curve is the restriction of an automorphism of $\mathcal{X}(1)$ which fixes P_0 and permutes P_1, P_2, P_3.

that for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, there exists an isomorphism $\varphi_\sigma : \mathcal{X}(1) \to \mathcal{X}(1)^\sigma$ of algebraic curves over K. Moreover it is easy to verify that these isomorphisms map an elliptic point of a given order to an elliptic point of the same order. So φ_σ is an isomorphism between the curve $\mathcal{X}(1)$ and its conjugate $\mathcal{X}(1)^\sigma$ which sends P_0 to P_0^σ and $\{P_1, P_2, P_3\}$ to $\{P_1^\sigma, P_2^\sigma, P_3^\sigma\}$.

We want to show that the morphisms φ_σ yield effective Galois descent data to $\mathbb{Q}$ in the spirit of Weil [Wei56]. We need to verify that the cocycle conditions are satisfied by the isomorphisms φ_σ. As noted by Milne [Mil08, §16, Theorem 16.32], it suffices to prove that the curve $\mathcal{X}(1)$ does not have any non-trivial automorphism which fixes P_0 and permutes $\{P_1, P_2, P_3\}$. Such an automorphism would be of order 2 or 3. The cross ratio[2] $\lambda = (P_0, P_1; P_2, P_3)$ would then be equal to one of the following three cross-ratios:

$$(\infty, 0; 1, -1) = -1 \quad \text{or} \quad (\infty, 1; \zeta_3, \zeta_3^2) = 1 + \zeta_3 \quad \text{or} \quad (\infty, 1; \zeta_3, -2\zeta_3^2) = -\zeta_3,$$

where $\zeta_3 = e^{\frac{2i\pi}{3}}$. On the other hand, since P_0 is rational over K and since the points P_1, P_2, P_3 form a complete Galois orbit, we have $\lambda \in K(P_1)$. Let $\tau \in \mathrm{Gal}(K(P_1)/K)$ be such that $\tau(P_1) = P_2$, $\tau(P_2) = P_3$ and $\tau(P_3) = P_1$. If λ were in K then

$$\lambda = \tau(\lambda) = (P_0, P_3; P_1, P_2) = \frac{\lambda - 1}{\lambda}.$$

Hence $\lambda^2 - \lambda + 1 = 0$ which leads to a contradiction (recall that $[K(P_1) : K] = 3$). Therefore $K(\lambda) = K(P_1)$. Finally, let us denote by $H_{K(\sqrt{-1})}$ the Hilbert class field of $K(\sqrt{-1})$. Since $H_{K(\sqrt{-1})} = K(\sqrt{-1}) \cdot K(P_1)$, the cross ratio λ must satisfy:

$$H_{K(\sqrt{-1})} = K(\lambda, \sqrt{-1}).$$

Neither $(\infty, 0; 1, -1)$, nor $(\infty, 1; \zeta_3, \zeta_3^2)$, nor $(\infty, 1; \zeta_3, -2\zeta_3^2)$ satisfies this, thus the curve $\mathcal{X}(1)$ does not have any non-trivial automorphism fixing P_0 and permuting P_1, P_2, P_3. As we said, in this case, the Weil descent criterion is automatically satisfied.

Let us consider the curve $\mathcal{X}_0(2)$. Again we use the functoriality of the Deligne construction of canonical models but the Shimura data consists now in the algebra B, the maximal order $\mathcal{O}$ and the Eichler order $\mathcal{O}_2$. For each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, since the inert prime 2 of K is $\mathrm{Gal}(K/\mathbb{Q})$-invariant, the suborder $\phi_\sigma(\mathcal{O}_2)$ is again the Eichler order of level 2 of $\mathcal{O}^\sigma$. Then the isomorphism of canonical models $\varphi_\sigma : \mathcal{X}(1) \to \mathcal{X}(1)^\sigma$ lifts to an isomorphism of canonical models $\mathcal{X}_0(2) \to \mathcal{X}_0(2)^\sigma$. On the other hand, since $PSL_2(\mathbb{F}_8)$ is equal to its centralizer in the group of permutations of the points of $\mathbb{P}^1_{\mathbb{F}_8}$, the cover $\mathcal{X}_0(2) \to \mathcal{X}(1)$ and its conjugates do not have any non-trivial automorphisms. Therefore the previous isomorphisms between $\mathcal{X}_0(2)$ and its conjugate give an effective descent data to $\mathbb{Q}$.

[2] Recall that the cross ratio between four distinct points $P_0, P_1, P_2, P_3 \in \mathbb{P}^1$ is defined by $(P_0, P_1; P_2, P_3) = \frac{(x_0y_2 - x_2y_0)(x_1y_3 - x_3y_1)}{(x_1y_2 - x_2y_1)(x_0y_3 - x_3y_0)}$, where $P_i = (x_i : y_i)$. If $Q_0, Q_1, Q_2, Q_3 \in \mathbb{P}^1$ are four other points, then there exists $h \in \mathrm{Aut}(\mathbb{P}^1)$ such that $h(P_i) = Q_i$ if and only if $(P_0, P_1; P_2, P_3) = (Q_0, Q_1; Q_2, Q_3)$.

We know that the Atkin-Lehner involution w_2 of $\mathcal{X}_0(2)$ comes from a trace zero element $\omega_2 \in B$ of reduced norm 2. The element $\phi_\sigma(\omega_2)$ is clearly a trace zero element in $\mathcal{O}^\sigma$ of reduced norm 2 which normalizes the Eichler order $\mathcal{O}_2^\sigma$. Thus the construction of the Atkin-Lehner involution is Galois-invariant and the automorphism $w_2 : \mathcal{X}_0(2) \to \mathcal{X}_0(2)$ must be defined over $\mathbb{Q}$. Moreover, since w_2 permutes elliptic points of given order, it permutes the Q_i's. So w_2 must fix one of them. By Galois conjugation, it fixes all of them. $\square$

2 The Shimura curve and the Hurwitz space

In our previous work [Hal05], we computed an algebraic model of the universal family of degree 9 covers of $\mathbb{P}^1_{\mathbb{C}}$ with Galois group $PSL_2(\mathbb{F}_8)$, with ramification type $(3^3, 2^41, 2^41, 2^41)$ and such that the first branch point is rational while the three others are conjugate to each other. The final result (Proposition 9, loc. cit.) consists in an open set $\mathcal{U}$ of $\mathbb{P}^1_{\mathbb{Q}}$ together with a fibered surface $\varepsilon : \mathcal{E} \to \mathcal{U}$ in genus one curves defined by the following equation[3]:

$$\begin{aligned} E(f,g,h) = &\left(T^3 + \tfrac{531}{223}T^2 + \tfrac{189}{223}T + \tfrac{81}{223}\right) f^3 - \left(T + \tfrac{3}{5}\right) f^2 g \\ &- \left(T^2 + \tfrac{18}{37}T + \tfrac{9}{37}\right) f^2 h + \frac{7 \cdot 223 \left(T + \frac{9}{7}\right)}{2^2 3 \cdot 5 \cdot 37 (T+3)} fgh \\ &+ \frac{163 \cdot 223 \left(T^2 + \frac{84}{163}T + \frac{81}{163}\right)}{3 \cdot 5^2 37^2 (T+3)} fh^2 \\ &+ \frac{223^2}{2 \cdot 3^3 5^3 7^2 (T+3)(T^2 + \frac{6}{49}T + \frac{9}{49})} g^3 \\ &- \frac{2 \cdot 223}{3^2 5^3 37^2 (T+3)} gh^2 - \frac{2^3 7 \cdot 223^2 \left(T^2 - \frac{48}{7}T + 97\right)}{3^3 5^3 37^3 (T+3)^2} h^3. \end{aligned}$$

We denote by $\mathcal{E}_\eta$ the generic fiber. The open set $\mathcal{U}$ is the so-called (absolute) Hurwitz space parameterizing our family and the variable T is one of its coordinates[4]. This model is minimal in the sense that every fiber is a smooth genus 1 curve, i.e. the morphism $\mathcal{E} \to \mathcal{U}$ is smooth. This can be proved by computing Δ, the analogue for cubic plane curves, of the usual discriminant for cubic Weierstrass equations, as in Poonen [Poo01, §3]. Here one has:

$$\Delta = \frac{3^{12} 223^{12}}{2^3 5^{24} 7^8 37^{12}} \frac{(T-1)^{13}}{(T+3)^{12} (T^2 + \frac{6}{49}T + \frac{9}{49})^4},$$

and the support of Δ does not intersect $\mathcal{U}$.

[3] Actually, this equation is not exactly the one given in the cited proposition. During the present work, we realize that the equation we gave in our previous article was not minimal. By an easy linear change of variables, we obtain the new equation which is minimal as we will see.

[4] Exactly 18 points have been removed from $\mathbb{P}^1_{\mathbb{Q}}$ to obtain $\mathcal{U}$. These points correspond to the degenerate covers of the family. The zeros of the denominators of the coefficients of the equation are among these values.

A function $\varphi \in \mathbb{Q}(\mathcal{U})(\mathcal{E})$ is also given. This function is such that the map $\mathcal{E}_\eta \xrightarrow{\varphi} \mathbb{P}^1_{\mathbb{Q}(T)}$ is a degree 9 cover, with (geometric) Galois group $PSL_2(\mathbb{F}_8)$, and with four branch points: the point of type 3^3 is at $\varphi = \infty$, the three points of type 2^41 have the φ-coordinates equal to the three roots of $x^3 + H(T)(x+1)$, where $H \in \mathbb{Q}(\mathcal{U})$ is explicit.

We denote by $\mathcal{Q}_{1,\eta}, \mathcal{Q}_{2,\eta}, \mathcal{Q}_{3,\eta}$ the zeros of the function f on the generic fiber. These are the three unramified points of φ on $\mathcal{E}_\eta$ over the three branch points of type 2^41. Each $\mathcal{Q}_{i,\eta}$ extends to a horizontal divisor on $\mathcal{E}$ which will play a role in the proof bellow.

The specializations of this family at rational points of $\mathcal{U}$ yield $PSL_2(\mathbb{F}_8)$ covers of $\mathbb{P}^1_{\mathbb{Q}}$ defined over $\mathbb{Q}$, with four branch points and expected ramification data.

We now determine the rational specialization of $\varepsilon : \mathcal{E} \to \mathcal{U}$ corresponding to the cover $\mathcal{X}_0(2) \to \mathcal{X}(1)$.

Proposition 2 *The cover $\mathcal{X}_0(2) \to \mathcal{X}(1)$ corresponds to the specialization at the value $T = -1$ of our family.*

Proof — First, the cover $\mathcal{X}_0(2) \to \mathcal{X}(1)$ is truly a member of our family. Indeed the ramification data and the Galois group correspond and we know that the unique elliptic point of order three on $\mathcal{X}(1)$ is rational and that the three other points of order 2 are conjugate to each other.

Let $\mathcal{E}_t$ be the specialization we are looking for[5]. Since points Q_1, Q_2, Q_3 are known to be the unramified points over the branch points of the cover $\mathcal{X}_0(2) \to \mathcal{X}(1)$ of type 2^41, these points must necessarily be the specializations $\mathcal{Q}_{i,t}$ of $\mathcal{Q}_i$, $1 \leq i \leq 3$. On $\mathcal{E}_t$, we also know that there exists the involution w_2 defined over $\mathbb{Q}$ which fixes these specializations. Extending the scalars to $\mathbb{Q}(\mathcal{Q}_{1,t})$, the genus 1 curve $\mathcal{E}_t$ becomes an elliptic curve whose origin can be chosen to be equal to $\mathcal{Q}_{1,t}$. Since w_2 fixes $\mathcal{Q}_{1,t}$, it must be negation and the 2-torsion is generated by $\mathcal{Q}_{2,t}, \mathcal{Q}_{3,t}$. Thus in the group of points of the elliptic curve $(\mathcal{E}_t, \mathcal{Q}_{1,t})$, we are looking for, there must be the equalities $2\mathcal{Q}_{1,t} = 2\mathcal{Q}_{2,t} = 2\mathcal{Q}_{3,t}$.

In order to solve these equations in t, we need a section of $\varepsilon : \mathcal{E} \to \mathcal{U}$. We introduce the base change given by the horizontal divisor $\mathcal{Q}_1$. Let $\mathcal{U}' \to \mathcal{U}$ the cover defined by the equation $E(0, g, 1) = 0$ (recall that $\mathcal{Q}_1$ is a zero of the function f on the generic fiber $\mathcal{E}_\eta$). We verify that this cover is unramified (the genus of $\mathbb{Q}(\mathcal{U}')$ equals 2). Therefore the base change $\varepsilon' : \mathcal{E} \otimes_{\mathcal{U}} \mathcal{U}' \to \mathcal{U}'$ is still smooth. This time, there is a section, namely the horizontal divisor $\mathcal{Q}_1$, so the fibration becomes an elliptic surface. On this surface, let us consider the divisor $\mathcal{D} = 2\mathcal{Q}_1 + 2\mathcal{Q}_2 + 2\mathcal{Q}_3$ (where doubles are calculated with $\mathcal{Q}_1$ as the origin). The restriction of the morphism ε' to $\mathcal{D}$ gives rise to a degree 3 cover $\mathcal{D} \to \mathcal{U}'$. This cover has a single point above the value t we are looking for. Using a Weierstrass model of the elliptic surface, it is an easy computational task to deduce the actual value of t. Details of the computations are unfortunately too large to figure in this paper. The result is that only $T = -1$ holds. $\square$

[5] We know that $\mathcal{E}_t$ is defined over $\mathbb{Q}$ so the value t is an element of $\mathcal{U}(\mathbb{Q})$. Unfortunately, knowing that a point on a curve is defined over $\mathbb{Q}$ does not help to find it.

Since we know an algebraic model of the universal family $\varphi : \mathcal{E}_\eta \to \mathbb{P}^1_{\mathbb{Q}(T)}$, it is very easy to compute the specialization $\varphi_{-1} : \mathcal{E}_{-1} \to \mathbb{P}^1_{\mathbb{Q}}$. We deduce an explicit algebraic model of $\mathcal{X}_0(2) \to \mathcal{X}(1)$. The equation is simplified by taking the unitarization in f of $E_{T=-1}(\frac{1561}{1850}f, -\frac{70}{37}g, 1)$ in place of the specialization of E at $T = -1$ directly.

Corollary 3 *The curve $\mathcal{X}_0(2)$ has equation:*

$$f^3 - f^2g - f^2 - \tfrac{25}{84}fg + \tfrac{40}{147}f - \tfrac{625}{702}g^3 + \tfrac{50}{441}g - \tfrac{640}{9261} = 0$$

and the cover $\mathcal{X}_0(2) \to \mathcal{X}(1)$ is given by the function:

$$\varphi = -\tfrac{241129}{125}f^2g - \tfrac{36309}{125}f^2 + \tfrac{1715}{3}fg^2 + \tfrac{22099}{30}fg - \tfrac{637}{200}f - \tfrac{1715}{9}g^3 + \tfrac{1225}{36}g^2 - \tfrac{1708}{45}g - \tfrac{1301}{75}.$$

It is a degree 9 cover ramified at $\varphi = \infty$ and at the three roots of $x^3 - x^2 - 992x - 20736$.

Knowing this model, it is possible to check some easy facts.

• Since w_2 is defined over $\mathbb{Q}$, its set of fixed points, i.e. Q_1, Q_2, Q_3 and a fourth point R, is Galois invariant. But so is $\{Q_1, Q_2, Q_3\}$, hence R is $\mathbb{Q}$-rational. It has (f, g)-coordinates equal to $\left(\frac{16}{21}, 0\right)$. Thus $\mathcal{X}_0(2)$ is an elliptic curve which, as suggested by Watkins [Elk06, §4], is $\mathbb{Q}$-isomorphic to the elliptic curve $[1, -1, 1, -65773, -6478507]$.

• The involution w_2 of $\mathbb{Q}(f, g)$ is given by:

$$w_2(f) = \frac{733824f^2 - 733824fg - 454272f + 1715000g^3 - 218400g + 133120}{4501875g^3 + 733824g + 279552},$$
$$w_2(g) = \frac{-91728f^2g + 91728fg^2 + 56784fg + 62244g^2 - 3328g}{214375g^3 + 34944g + 13312}.$$

It fixes the Q_i's and the rational point $\left(\frac{16}{21}, 0\right)$.

• Besides the *absolute* Hurwitz space $\mathcal{U}$, we have also computed an explicit model of the *inner* Hurwitz space which parameterizes the $PSL_2(\mathbb{F}_8)$-Galois covers. The latter covers the first one by a degree three cyclic morphism. The field of definition of the points above $T = -1$ is known to be the field of moduli of the Galois closure of the cover $\mathcal{X}_0(2) \to \mathcal{X}(1)$, that is the cover $\mathcal{X}(2) \to \mathcal{X}(1)$. Here this field of definition is K itself, which was expected since the cover $\mathcal{X}(2) \to \mathcal{X}(1)$ is known to be defined over K (we recall that the field of moduli is included in all the fields of definition).

3 Rational CM points on $\mathcal{X}(1)$

We begin by considering the CM elliptic points of order 2, P_1, P_2, P_3 on $\mathcal{X}(1)$ corresponding to the field $K(\sqrt{-1})$. According to Shimura's result, the Hilbert class field of $K(\sqrt{-1})$ must satisfy:

$$H_{K(\sqrt{-1})} = K(\sqrt{-1}) \cdot K(P_1),$$

We check that the field of definition of the P_i's is the cubic field $\mathbb{Q}(\theta_1)$ with $\theta_1^3 - \theta_1^2 - 4\theta_1 + 12 = 0$ whose discriminant is equal to $2^2 13^2$; moreover we truly have $H_{K(\sqrt{-1})} = K(\sqrt{-1}, \theta_1)$.

Following Elkies [Elk98, §5.3], a rational CM point on $\mathcal{X}(1)$ must come from a CM a field L which is not only Galois over K but over $\mathbb{Q}$. Thus L must be equal to $K(\sqrt{-D})$ for some $D \in \mathbb{Z}_{>0}$ such that $\mathbb{Q}(\sqrt{-D})$ has class number one. An easy computation shows that only $D = 3, 7, 8$ can appear.

Proposition 4 *On $\mathcal{X}(1)$ there are CM points which are defined over $\mathbb{Q}$:*

1. *the point with $\varphi = \infty$ is a CM point corresponding to the field $K(\sqrt{-3})$,*
2. *the point with $\varphi = \frac{2^4 \cdot 3^3 \cdot 11}{5^3}$ is a CM point corresponding to the field $K(\sqrt{-7})$,*
3. *the point with $\varphi = -\frac{23549}{5^3}$ is a CM point corresponding to the field $K(\sqrt{-2})$.*

Proof — The point with $\varphi = \infty$ is known to correspond to the CM field $K(\sqrt{-3})$. In order to calculate some other rational CM points, we compute the "modular polynomial" $\Phi_2(X, Y)$ which is such that $\Phi_2(\varphi, \varphi \circ w_2) = 0$. It is a symmetric polynomial of bi-degree $(9, 9)$. The polynomial $\Phi_2(X, X)$ factorizes into:

$$\begin{aligned}\Phi_2(X,X) = &\left(X - \tfrac{4752}{125}\right)^2 \left(X + \tfrac{23549}{125}\right) \left(X^3 - X^2 - 992X - 20736\right) \cdot \\ &\left(X^3 + \tfrac{95568}{125}X^2 - \tfrac{1212672}{125}X - \tfrac{203493376}{125}\right)^2 \cdot \\ &\left(X^3 - \tfrac{16752}{125}X^2 - \tfrac{22910208}{15625}X + \tfrac{1126199296}{15625}\right)^2 .\end{aligned}$$

The two rational roots of this polynomial are necessarily rational CM points on $\mathcal{X}(1)$.

On $\mathcal{X}_0(2)$ there is a point Q, defined over $\mathbb{Q}(\sqrt{-7})$, such that $\varphi(Q) = \varphi(w_2(Q)) = \frac{4752}{125}$. This means that the point $\varphi = \frac{4752}{125}$ is a CM point corresponding to $K(\sqrt{-7})$.

There are eight points on $\mathcal{X}_0(2)$ above the φ-value $-\frac{23549}{125}$ which form a complete set of Galois conjugates over $\mathbb{Q}$ and of which the field of definition is a degree eight number field M. The compositum $K(\sqrt{-2}) \cdot M$ is the 2-ray class field of $K(\sqrt{-2})$. Thus, the point with φ-value $-\frac{23549}{125}$ is necessarily a CM point corresponding to the field $K(\sqrt{-2})$. □

References

[AB04] Montserrat Alsina and Pilar Bayer. *Quaternions Orders, Quadratic Forms, and Shimura Curves*, volume 22 of *CRM Monograph Series*. American Mathematical Society, 2004.

[BT07] P. Bayer and A. Travesa. Uniformizing functions for certain Shimura curves, in the case d=6. *Acta Arithmetica*, 126:315–339, 2007.

[Cou99] Jean-Marc Couveignes. Tools for the computation of families of coverings. In Helmut Völkein, David Harbater, Peter Müller, and J.G. Thompson, editors, *Aspects of Galois theory*, volume 256 of *London Mathematical Society Lecture Note Series*, pages 38–65. Cambridge, 1999. The following pages of this book were inadvertently numbered incorrectly: p. 21 should be p. 22, p. 22 should be p. 23 and p. 23 should be p. 21.

[Del71] Pierre Deligne. Travaux de Shimura (Exposé 389). In *Séminaire Bourbaki*, volume 13. http://www.numdam.org/, 1970-1971. in Collections/Seminars.

[DF94] Pierre Dèbes and Michael D. Fried. Nonrigid constructions in Galois theory. *Pacific Journal of Mathematics*, 163(1):81–122, 1994.

[Elk98] Noam D. Elkies. Shimura curve computation. In Joe P. Buhler, editor, *Proceedings of ANTS-III*, volume 1423 of *Lecture Notes in Computer Science*, pages 1–47. Springer, 1998.

[Elk06] Noam D. Elkies. Shimura curves for level-3 subgroups of the $(2, 3, 7)$ triangle group and some other examples. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 302–316. Springer, 2006.

[FV91] Michael D. Fried and Helmut Völklein. The inverse Galois problem and rational points on moduli spaces. *Mathematische Annalen*, 290:771–800, 1991.

[GR04] Josep González and Victor Rotger. Equations of Shimura curves of genus two. *Int Math Res Notices*, 2004:661–674, 2004.

[Hal05] Emmanuel Hallouin. Study and computation of a Hurwitz space and totally real $PSL_2(\mathbb{F}_8)$-extensions of $\mathbb{Q}$. *Journal of Algebra*, 292:259–281, 2005.

[Hur91] A. Hurwitz. Über riemann'sche flächen mit gegebenem verzweigunspunkten. *Math. Annalen*, 39:1–61, 1891.

[Mil90] James S. Milne. Canonical Models of (Mixed) Shimura Varieties and Automorphic Vector Bundles. In Laurent Clozel and James S. Milne, editors, *Automorphic Forms, Shimura varieties, and L-functions I*, volume 10 of *Perspectives in Mathematics*. Academic Press, 1990.

[Mil08] James S. Milne. *Algebraic Geometry*. available online: `www.jmilne.org/math/CourseNotes/AG510.pdf`, 2008.

[MM99] Gunter Malle and B. Heinrich Matzat. *Inverse Galois Theory*. Springer, 1999.

[MR03] Colin Maclachlan and Alan W. Reid. *The Arithmetic of Hyperbolic 3-Manifolds*, volume 219 of *Graduate Texts in Mathematics*. Springer, 2003.

[Poo01] Bjorn Poonen. An explicit algebraic family of genus-one curves violating the Hasse principle. *J. de Théorie des Nombres de Bordeaux*, 13(1):263–274, 2001.

[Shi67] Goro Shimura. Construction of class fields and zeta functions of algebraic curves. *Annals of Mathematics*, 85:58–159, 1967.

[Vig80] Marie-France Vignéras. *Arithmétique des Algèbres de Quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer-Verlag, 1980.

[Voi06] John Voight. Computing CM points on Shiumra curves arising from cocompact arithmetic triangle groups. In Florian Hess, Sebastian Pauli, and Michael Pohst, editors, *Proceedings of ANTS-VII*, volume 4076 of *Lecture Notes in Computer Science*, pages 406–420. Springer, 2006.

[Völ96] Helmut Völklein. *Groups as Galois Groups*, volume 53 of *Cambridge Studies in Advanced Mathematics*. Cambridge, 1996.

[Wei56] André Weil. The field of definition of a variety. *Amer. J. of Math.*, 78:509–524, 1956.