EQUATIONS OF HYPERELLIPTIC SHIMURA CURVES

SANTIAGO MOLINA

Abstract. We describe an algorithm that computes explicit models of hyperelliptic Shimura curves attached to an indefinite quaternion algebra over $\mathbb{Q}$ and Atkin-Lehner quotients of them. It exploits Cerednik-Drinfeld's nonarchimedean uniformisation of Shimura curves, a formula of Gross and Zagier for the endomorphism ring of Heegner points over Artinian rings and the connection between Ribet's bimodules and the specialization of Heegner points, as introduced in [21]. As an application, we provide a list of equations of Shimura curves and quotients of them obtained by our algorithm that had been conjectured by Kurihara.

1. Introduction

Let D be the reduced discriminant of an indefinite quaternion algebra B over $\mathbb{Q}$ and let $N \geq 1$ be a positive integer, prime to D. Let $X_0^D(N)/\mathbb{Q}$ denote the Shimura curve over $\mathbb{Q}$ attached to an Eichler order of level N in B.

As it is well-known, in the classical modular case automorphic forms of $X_0(N) := X_0^1(N)$ admit Fourier expansions around the cusp of infinity. This allows to compute explicit generators of the field of functions of such curves. Also, explicit methods are known to determine bases of the space of their regular differentials, which are used to compute equations for them and their quotients by Atkin-Lehner involutions.

In the general case, $D > 1$, the question of writing down explicit equations of curves $X_0^D(N)$ over $\mathbb{Q}$ remains quite unapproachable. The absence of cusps has been an obstacle for explicit approaches to Shimura curves. Methods to handle functions and regular differential forms on these curves are less accessible and we refer the reader to [1] for progress in this regard. Ihara [12] was probably one of the first to express an interest on this problem, and already found an equation for the genus 0 curve $X_0^6(1)$, while challenged to find others. Since then, several authors have contributed to this question (Kurihara [16], Jordan [14], Elkies [7], Clark and Voight [33] for genus 0 or/and 1, Gonzalez and Rotger [9], [8] for genus 1 and 2).

Elkies computes equations for the list of Shimura curves that he deals with using their hyperbolic (rather than the non-Archimedean uniformizations at primes dividing the discriminant) uniformizations. His method has the advantage that allows the identification of Heegner points in the equation, but is limited to very small discriminants D and levels N.

The methods of Gonzalez and Rotger are heavily based on Cerednik-Drinfeld's theory for the special fiber at $p \mid D$ and the arithmetic properties of Heegner points. It allows to work with larger D and N but is again subjected to sever restrictions: the genus must be at most 2 and, in the hyperelliptic case, the curve must be bielliptic. In addition, this method does not allow to locate Heegner points in the given model of the curve. The present paper is in the line of [8] and one of the aims is removing such strong restrictions.

More precisely, the aim of this note is to introduce an algorithm to compute equations for hyperelliptic Shimura curves with good reduction at 2. For the sake of simplicity we restrict ourselves to the case $N = 1$ and write $X_0^D = X_0^D(1)$, although we believe that the procedure can be easily generalized to the case of arbitrary square-free N. Polynomials defining equations of hyperelliptic curves are closely related to their set of *Weierstrass points*. The set of Weierstrass points $\mathrm{WP}(X_0^D)$ of a hyperelliptic Shimura curve X_0^D turns out to be a disjoint union of Heegner points:

$$\mathrm{WP}(X_0^D) = \bigsqcup_i \mathrm{CM}(R_i),$$

for suitable orders R_i in imaginary quadratic fields. As a consequence, X_0^D admits an equation of the form

$$y^2 = \prod_i p_i(x), \tag{1.1}$$

where $p_i(x)$ is a polynomial attached to each set of Heegner points $\mathrm{CM}(R_i)$.

Let $\mathcal{X}_0^D$ denote Morita's integral model of X_0^D. Over $\mathbb{Z}[1/2]$, $\mathcal{X}_0^D$ will also be defined by an equation of the form (1.1). As we shall explain in detail, the specialization of Weierstrass points at the special fiber of $\mathcal{X}_0^D$ at a prime p can be exploited in order to compute the p-adic valuation of the discriminants $\mathrm{disc}(p_i)$ and resultants $\mathrm{Res}(p_1, p_j)$ of the above polynomials. We will make use of the theory of specialization of Heegner points introduced in [21] in order to obtain such information.

Moreover, by means of the classical theory of complex multiplication we can also compute the splitting fields of each p_i. Exploiting the theory developed by Gross-Zagier in [10] we can further compute the leading coefficients of each p_i, once we have fixed a pair of Heegner points at infinity.

As a combination of all this data, we are able to compute an explicit model (1.1) for X_0^D. The only algorithmic limitation of this method relies on the fact that it exploits certain instructions which are currently implemented (e.g. in *MAGMA*) only for small degree field extensions. As long as the genus increases, the degrees of the fields involved in the computation become so large that make it impossible to proceed with the algorithm.

In §2 we recall basic facts about semi-stable hyperelliptic curves and the specialization of their Weierstrass points. In §3 we introduce Shimura curves with special emphasis to the finite list of them which are hyperelliptic. In §4 we describe the singular specialization of Heegner points and in §5 we give an explicit recipe to compute it in terms of Ribet bimodules. In §6 we exploit the moduli interpretation of Shimura curves in order to compute the supersingular specialization of a suitable set of Heegner points. This is a crucial step in the computation of the leading coefficients of the polynomials involved, once we have fixed a pair of such Heegner points at infinity. In §7 we present our algorithm and we devote §8 and §9 to exhibit two examples of its implementation.

Finally, in §10 we explain how to adapt the algorithm to quotients of Shimura curves by Atkin-Lehner involutions. The degrees of the fields involved in the computation in this case are smaller and, consequently, we are able to compute more examples. In §10.4 we present a list of equations of Shimura curves and Atkin-Lehner quotients obtained by means of the algorithms introduced in the previous sections. These equations were unknown until now and were conjectured by Kurihara in [17].

Acknowledgements. The author would like to thank Bas Edixhoven, Qing Liu, Ariel Martin Pacetti and specially Josep González and Víctor Rotger for their comments and discussions throughout the development of this paper. The author also thanks Xevi Guitart for carefully reading a draft of the paper and providing many helpful comments. Finally, the author gratefully acknowledges the generous help received from the *Centre de Recerca Matemàtica* of Bellaterra (Barcelona) during these last months.

2. Semi-stable hyperelliptic curves

Let X be a smooth, geometrically connected, projective curve of genus $g > 1$ defined over a field k. It is said that X is a *hyperelliptic curve* over k if there exists a finite separable morphism $X \to \mathbb{P}^1_k$ of degree 2. Whenever there is no risk of confusion about the field k we shall only say that X is hyperelliptic. This is equivalent to the existence of an involution ω defined over k such that the quotient curve X/ω has genus 0 and k-rational points. When this is the case, this involution is unique and is called *the hyperelliptic involution.* Moreover, it is well known that there exist functions $x, y \in k(X)$ satisfying a relation of the type

(2.2)

$$y^2 + Q(x)y + P(x) = 0, \quad P, Q \in k[x], \quad 2g + 1 \leq \max\{\deg P, 2\deg Q\} \leq 2g + 2,$$

and such that the function field of X is $k(X) = k(x, y)$. The hyperelliptic involution ω is then given by $(x, y) \to (x, Q(x) - y)$ and, for the particular case that $\mathrm{char}(k) \neq 2$, we can take $Q(x) = 0$. The set of $\overline{k}$-rational points of X consists of the set of affine points defined by (2.2) together with a k-rational point at infinity if $\deg(Q(x)^2 - 4P(x)) = 2g + 1$, or a pair of points at infinity if

$\deg(Q(x)^2-4P(x))=2g+2$. In the later case, both points are either k-rational or Galois conjugate over a quadratic extension of k.

We shall denote by $\mathrm{WP}(X)$ the set of Weierstrass points of X. It coincides with the set of fixed points of ω. Hence, $\mathrm{WP}(X)$ contains the point at infinity in case $\deg(Q^2(x)-4P(x))=2g+1$, and all points of the form $(\gamma, Q(\gamma)/2)$ or $(\gamma, \sqrt{P(\gamma)})$, depending whether $\mathrm{char}(k)\neq 2$ or not, where γ is a root of $R(x)=Q^2(x)-4P(x)$.

If $k=\mathbb{Q}$, a *Weierstrass model* for X is a model $\mathcal{W}$ over $\mathbb{Z}$, i.e. a normal fibered surface over $\mathrm{Spec}(\mathbb{Z})$ with generic fiber X, such that ω can be extended to an involution on $\mathcal{W}$, which we still denote by ω, and the quotient $\mathcal{W}/\langle\omega\rangle$ is smooth over $\mathbb{Z}$. We shall also denote by $\mathrm{WP}(\mathcal{W})$ the set of fixed points of ω on $\mathcal{W}$. By [20, Remark 3.5], every smooth model of $\mathbb{P}^1_{\mathbb{Q}}$ is isomorphic to $\mathbb{P}^1_{\mathbb{Z}}$. Hence, any Weierstrass model $\mathcal{W}$ satisfies $\mathcal{W}/\langle\omega\rangle=\mathbb{P}^1_{\mathbb{Z}}$ and, by [18, Lemme 1], $\mathcal{W}$ is the projective closure of the affine curve defined by:

(2.3)
$$y^2+Q(x)y+P(x)=0,\quad P,Q\in\mathbb{Z}[x],\quad 2g+1\leq\max\{\deg P, 2\deg Q\}\leq 2g+2.$$

Given such a hyperelliptic equation, we define the *discriminant of the Weierstrass model* as follows:

$$\Delta(\mathcal{W})=\left\{\begin{array}{ll} 2^{-4(g+1)}\mathrm{disc}(R(x)) & \text{if } \deg R(x)=2g+2\,,\\ 2^{-4(g+1)}c^2\mathrm{disc}(R(x)) & \text{if } \deg R(x)=2g+1\,,\end{array}\right. \tag{2.4}$$

where $R(x)=Q(x)^2-4P(x)$ and c is its leading coefficient. The special fiber $\mathcal{W}_p$ of $\mathcal{W}$ at p is smooth over $\mathbb{F}_p$ if and only if $p\nmid\Delta(\mathcal{W})$ (c.f. [18]).

Assume now that k is algebraically closed, let C be an algebraic curve over k, and let $x\in C(k)$. We say that x is an ordinary double point if

$$\widehat{O_{C,x}}\simeq k[[u,v]]/(uv)\simeq k[[u,v]]/(u^2-v^2), \tag{2.5}$$

where $\widehat{O_{C,x}}$ is the completion of the local ring $O_{C,x}$. A curve C over k is said to be *semi-stable* if it is reduced and all its singular points are ordinary double points.

Let S be an affine Dedekind scheme of dimension 1, with fraction field K. Let C be a normal, connected, projective curve over K. A *model of C over S* is a normal fibered surface $\mathcal{C}\rightarrow S$ together with an isomorphism of its generic fiber $f:\mathcal{C}_\eta\rightarrow C$. We say that the model $\mathcal{C}\rightarrow S$ is *semi-stable* if for each $s\in S$ the geometric fiber $\mathcal{C}_s\times_{k(s)}\overline{k(s)}$ is semi-stable over $\overline{k(s)}$, where $k(s)$ stands for the residue field of S at s.

Proposition 2.1. [19, Corollary 10.3.22] *Let $\mathcal{C}\rightarrow S$ be a semi-stable model of a curve C. Let $s\in S$, and let $x\in\mathcal{C}_s$ be a singular point of $\mathcal{C}_s$. Then there exists a Dedekind scheme S', étale over S, such that any point $x'\in\mathcal{C}':=\mathcal{C}\times_S S'$ above x lying on $\mathcal{C}'_{s'}$ is an ordinary double point in $\mathcal{C}'_{s'}\rightarrow\mathrm{Spec}(k(s'))$. Moreover,*

$$\widehat{O_{\mathcal{C}',x'}}\cong\widehat{O_{S',s'}}[[u,v]]/(uv-c)\quad c\in\mathfrak{m}_{s'}O_{S',s},$$

where $\widehat{O_{C',x'}}$ and $\widehat{O_{S',s'}}$ are the completions of $O_{C',x'}$ and $O_{S',s'}$ respectively.

If C is smooth, then $c \neq 0$. Let e_x be the normalized valuation of c in $O_{S',s'}$, then e_x does not depend on the scheme S' chosen.

Definition 2.2. The value e_x described in the above proposition is called *the thickness of the singularity $x \in \mathcal{C}_s$*.

Theorem 2.3. *Let $\mathcal{W} \to \mathrm{Spec}(\mathbb{Z})$ be a Weierstrass semi-stable model, and let p be an odd prime of bad reduction. Let $\tilde{P} \in \mathcal{W}_p(\overline{\mathbb{F}}_p)$ be a singular point lying in an affine open defined by an equation $y^2 + Q(x)y + P(x) = 0$. Then, there exist exactly two Weierstrass points $P_1, P_2 \in \mathrm{WP}(X)$ that specialize to $\tilde{P}$. Moreover, the thickness of $\tilde{P}$ is $e_{\tilde{P}} = 2\nu(\gamma_1 - \gamma_2)$, where ν is the normalized valuation at p and γ_i are the roots of $R(x) = Q(x)^2 - 4P(x)$ corresponding to P_1 and P_2.*

To prove this result we need the following technical lemma.

Lemma 2.4. *Let A be a ring such that $n \in A^*$. Then $s = (1+t)^n - 1 \in A[t]$ satisfies $A[[t]] = A[[s]]$ and, moreover, there exists $f(s) \in sA[[s]]$ such that $1+s = (1+f(s))^n$.*

Proof. This is exercise 1.3.9 of [19]. The proof is left to the reader. □

Proof of Theorem 2.3. First we shall prove that there are exactly two Weierstrass points $P_1, P_2 \in \mathrm{WP}(X)$ specializing to $\tilde{P}$. Write $\overline{\mathcal{W}}_p = \mathcal{W} \times \mathrm{Spec}(\overline{\mathbb{F}}_p)$ for the geometric fiber of $\mathcal{W}$ at p. Since $p \neq 2$, an affine open $\mathcal{U}$ of $\overline{\mathcal{W}}_p$ shall be of the form $\mathcal{U} = \mathrm{Spec}(\overline{\mathbb{F}}_p[x,y]/(y^2 - \tilde{R}(x)))$, where $\tilde{R}(x)$ is the reduction of $R(x)$ modulo p. Hence it is clear that singularities of $\mathcal{U}$ correspond to multiple roots of $\tilde{R}(x)$. Without loss of generality, assume $x = 0$ is the multiple root of $\tilde{R}(x)$ corresponding to $\tilde{P}$. We get $\tilde{R}(x) = x^m \tilde{h}(x)$, where $\tilde{h}(x) = \tilde{h}(0)(1 + x\tilde{r}(x))$ and $\tilde{h}(0) \neq 0$. The local ring $O_{\overline{\mathcal{W}}_p, \tilde{P}}$ at $\tilde{P}$ is given by:

$$O_{\overline{\mathcal{W}}_p, \tilde{P}} = (\overline{\mathbb{F}}_p[x,y]/(y^2 - x^m \tilde{h}(x)))_{(x,y)},$$

and it follows that

$$\widehat{O_{\overline{\mathcal{W}}_p, \tilde{P}}} = \overline{\mathbb{F}}_p[[x,y]]/(\frac{y^2}{\tilde{h}(x)} - x^m).$$

By Lemma 2.4, taking $A = \overline{\mathbb{F}}_p[[y]]$, $t = x\,\tilde{r}(x)$ and $n = 2$, we obtain that $\tilde{h}(x)$ is a square in $(\overline{\mathbb{F}}_p[[x,y]])^*$. Hence $\widehat{O_{\overline{\mathcal{W}}_p, \tilde{P}}} = A_m$, where

$$A_m := \overline{\mathbb{F}}_p[[x,y]]/(y^2 - x^m), \ \ m \geq 2.$$

Since $\mathcal{W}$ is semi-stable, $\overline{\mathcal{W}}_p/\overline{\mathbb{F}}_p$ must be semi-stable. Therefore $\tilde{P}$ is an ordinary double point and $\widehat{O_{\overline{\mathcal{W}}_p, \tilde{P}}} \simeq \overline{\mathbb{F}}_p[[x,y]]/(y^2 - x^2) = A_2$. From $A_2 \simeq A_m$, it follows that $m = 2$. As a consequence, $\tilde{P}$ is attached to a root $\tilde{\gamma}$ of $\tilde{R}(x)$ with multiplicity 2 and we conclude that there exist exactly two $P_1, P_2 \in \mathrm{WP}(X)$ that specialize to P (attached to the roots γ_1 and γ_2 of $R(x)$ that reduce to $\tilde{\gamma}$).

Next, we proceed to compute the thickness $e_{\tilde{P}}$ of $\tilde{P}$: the equation $Y^2 = R(x) = Q(x)^2 - 4P(x)$ defines $\mathcal{W}$ in a neighborhood of $(p) \in \operatorname{Spec}(\mathbb{Z})$. After extending to a finite extension $k' \supseteq \mathbb{F}_p$ if necessary, we can suppose that any singular point $\tilde{P}' \in \mathcal{W}_p \times \operatorname{Spec}(k')$ lying over $\tilde{P}$ is k'-rational. Without loss of generality, assume that $\tilde{P}'$ is defined by $x = 0, Y = 0$. That is,

$$\tilde{R}(x) = x^2\tilde{h}(x), \quad \tilde{h}(0) \neq 0.$$

We can choose an étale scheme S' over $\operatorname{Spec}(\mathbb{Z})$ and a point $\pi \in S'$ above (p) such that $k' = \mathbb{F}_p(\pi')$. Notice that, if we write $\mathcal{W}' = \mathcal{W} \times_S S'$, the point $\tilde{P}'$ lies in $(\mathcal{W}')_{\pi'}$ and its local ring is $\mathcal{O}_{\mathcal{W}',(\pi',\tilde{P}')} = (\mathcal{O}_{S',\pi'}[x,Y]/(Y^2 - R(x)))_{(x,Y)}$.

Let $\widehat{\mathcal{O}_{S',\pi'}}$ be the completion of $\mathcal{O}_{S',\pi'}$ and denote by ν its normalized valuation. Let us consider $R(x)$ over $\widehat{\mathcal{O}_{S',\pi'}}$. Since its reduction is $\tilde{R}(x) = x^2\tilde{h}(x)$ with $\tilde{h}(0) \neq 0$, we apply the Classical Hensel's Lemma (cf.[24]) to x^2 and $\tilde{h}(x)$ and we obtain that $R(x) = (x^2+ax+b)\cdot h(x)$, where $\nu(h(0)) = 0$, $\nu(a) > 0$ and $\nu(b) > 0$. Extending S' to a bigger étale $\operatorname{Spec}(\mathbb{Z})$-scheme if necessary, we can suppose that $h(0)$ has a square root in $\widehat{\mathcal{O}_{S',\pi'}}$. Since $h(x) = h(0)(1 + x\cdot r(x)) \in \widehat{\mathcal{O}_{S',\pi'}}[[x]]^*$, by Lemma 2.4, there exists $s(x) \in \widehat{\mathcal{O}_{S',\pi'}}[[x]]^*$ such that $s(x)^2 = h(x)$. Therefore

$$\begin{aligned}\widehat{\mathcal{O}_{\mathcal{W}',(\pi',\tilde{P}')}} &= \widehat{\mathcal{O}_{S',\pi'}}[[x,Y]]/(Y^2 - (x^2+ax+b)\cdot h(x)) \\ &= \widehat{\mathcal{O}_{S',\pi'}}[[x,Y]]/(\left(\frac{Y}{s(x)}\right)^2 - \left(x+\frac{a}{2}\right)^2 - \Delta),\end{aligned}$$

where $\Delta = a^2 - 4\cdot b$. Writing $u = Y/s(x) + x + a/2$ and $v = Y/s(x) - x - a/2$, we obtain that $\widehat{\mathcal{O}_{S',\pi'}}[[x,Y]] = \widehat{\mathcal{O}_{S',\pi'}}[[u,v]]$ and

$$\widehat{\mathcal{O}_{\mathcal{W}',(\pi',\tilde{P}')}} = \widehat{\mathcal{O}_{S',\pi'}}[[u,v]]/(u\cdot v - \Delta).$$

Hence, we deduce that $e_{\tilde{P}} = \nu(\Delta)$.

Since the roots of the polynomial $x^2 + ax + b$ are precisely the two unique roots $\gamma_1, \gamma_2 \in \overline{\mathbb{Q}}$ that reduce to $\tilde{\gamma}$, and Δ is the discriminant of the polynomial $x^2 + ax + b$, it follows that $\Delta = (\gamma_1 - \gamma_2)^2$ and $e_{\tilde{P}} = 2\nu(\gamma_1 - \gamma_2)$. □

3. Hyperelliptic Shimura curves

Let B be an indefinite division quaternion algebra over $\mathbb{Q}$ and let $\mathcal{O}$ be a maximal order in B. By an abelian surface with quaternionic multiplication (QM) by $\mathcal{O}$ over a field K we mean a pair (A, i) where:

i) A/K is an abelian surface.

ii) $i : \mathcal{O} \hookrightarrow \operatorname{End}(A)$ is an embedding.

For such a pair we denote by $\operatorname{End}(A, i)$ the ring of endomorphisms which commute with i, i.e., $\operatorname{End}(A, i) = \{\phi \in \operatorname{End}(A) : \phi i(\alpha) = i(\alpha)\phi \text{ for all } \alpha \in \mathcal{O}\}$. Two abelian surfaces (A, i) and (A', i') with QM by $\mathcal{O}$ are isomorphic if there is an isomorphism $\phi : A \to A'$ such that $\phi \circ i(\alpha) = i'(\alpha) \circ \phi$ for all $\alpha \in \mathcal{O}$. Throughout, we shall denote by $[A, i]$ the isomorphism class of (A, i).

Let us denote by $X_0^D/\mathbb{Q}$ Shimura's canonical model of the Shimura curve associated to $\mathcal{O}$. As Riemann surfaces, $X_0^D(\mathbb{C}) = \Gamma_0^D\backslash\mathcal{H}$, where $\mathcal{H}$ is the Poincaré upper half plane and Γ_0^D is the image of $\mathcal{O}$ through the embedding $B \hookrightarrow B \otimes \mathbb{R} \simeq M(2, \mathbb{R})$. As is well known, X_0^D represents, as a coarse moduli space, the moduli problem of classifying abelian surfaces with quaternionic multiplication by $\mathcal{O}$. Hence an isomorphism class $P = [A, i]$ shall be often regarded as a point on X_0^D.

It follows from the work of Morita, Cerednik and Drinfeld that X_0^D admits a proper integral model $\mathcal{X}$ over $\mathbb{Z}$, smooth over $\mathbb{Z}[\frac{1}{D}]$, which suitably extends the moduli interpretation to arbitrary base schemes (cf.[22],[3]). Moreover, $\mathcal{X}$ is semi-stable at every prime p dividing D, and singular points of $\mathcal{X}_p$ are in correspondence with certain algebraic objects (see correspondence (4.7)), from which we will recover their thicknesses (see Lemma 4.1).

Let K be an imaginary quadratic field and let R be an order in K. A point $P = [A, i] \in X_0^D(\mathbb{C})$ is a Heegner (or CM) point by R if $\mathrm{End}(A, i) \simeq R$. Throughout, we shall fix the isomorphism $R \simeq \mathrm{End}(A, i)$ to be the canonical one described in [13, Definition 1.3.1]. We denote by $\mathrm{CM}(R)$ the set of Heegner points by R. By main Theorem I of [28], the extension $K(P)$ of K generated by the coordinates any $P \in \mathrm{CM}(R) \subset X_0^D$ is the ring class field of R, H_R. Moreover, $[K(P) : \mathbb{Q}(P)]$ is 1 or 2 and the number field $\mathbb{Q}(P)$ can be determined, up to Galois conjugation (see Theorem 5.12 of [9]).

For every divisor $m|D$ let us denote by ω_m the corresponding Atkin-Lehner involution on X_0^D, which is defined over $\mathbb{Q}$. The property $\omega_m \cdot \omega_n = \omega_{m\cdot n/(m,n)^2}$ implies that the set $W(D) = \{\omega_d : d|D\}$ is a subgroup of automorphisms of X_0^D isomorphic to $(\mathbb{Z}/2\mathbb{Z})^{\#\{p|D\}}$. The action of these involutions on Heegner points can be found in Lemmas 5.9 and 5.10 of [9] and, as the following result shows, their set of fixed points is also a set of Heegner points.

Proposition 3.1. [23, §1] *Let $m \mid D$, $m > 0$. The set $\mathfrak{F}_{\omega_m}$ of fixed points of the Atkin-Lehner involution ω_m acting on X_0^D is*

$$\mathfrak{F}_{\omega_m} = \begin{cases} \mathrm{CM}(\mathbb{Z}[\sqrt{-1}]) \sqcup \mathrm{CM}(\mathbb{Z}[\sqrt{-2}]) & \text{if m} = 2 \\ \mathrm{CM}(\mathbb{Z}[\sqrt{-m}]) \sqcup \mathrm{CM}(\mathbb{Z}[\frac{1+\sqrt{-m}}{2}]) & \text{if m} \equiv 3 \mod 4 \\ \mathrm{CM}(\mathbb{Z}[\sqrt{-m}]) & \text{otherwise.} \end{cases}$$

Ogg determined in [23] the 24 values of D for which X_0^D is hyperelliptic over $\overline{\mathbb{Q}}$ and proved that only for 21 values of them the corresponding curves X_0^D are hyperelliptic over $\mathbb{Q}$. The aim of this paper is to give a procedure to compute equations for all these cases. Since those of genus 2 were computed by J. González and V. Rotger in [8], we assume that $X_0^D/\mathbb{Q}$ is hyperelliptic over $\mathbb{Q}$ of genus $g > 2$.

We present the values of D and the corresponding genera for the remaining 18 cases:

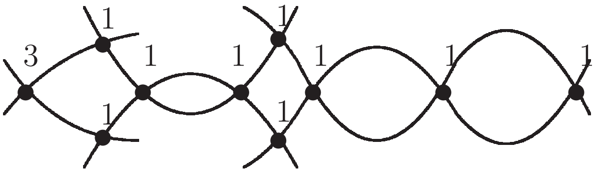
g	D
3	$2\cdot 31, 2\cdot 47, 3\cdot 13, 3\cdot 17, 3\cdot 23, 5\cdot 7, 5\cdot 11$
4	$2\cdot 37, 2\cdot 43$
5	$3\cdot 29$
6	$2\cdot 67$
7	$2\cdot 73, 3\cdot 37, 5\cdot 19$
9	$2\cdot 97, 2\cdot 103, 3\cdot 53, 7\cdot 17$

Table 1

The hyperelliptic involution ω of X_0^D in all these cases turns out to be the Atkin-Lehner involution ω_D. Since the action of ω_D has an interpretation in terms of the moduli problem, it can be extended to an involution on the integral model $\mathcal{X}$. Moreover, we have an explicit description of the fibers $\mathcal{X}_p$ and the action of $\omega = \omega_D$ on them. Hence we can easily check whether the quotient $\mathcal{X}/\langle\omega\rangle$ is smooth over $\mathbb{Z}$. If $\mathcal{X}/\langle\omega\rangle$ is not smooth over $\mathbb{Z}$, then $\mathcal{X}$ is not a Weierstrass model for X_0^D. Sometimes it is possible to blow-down certain exceptional irreducible components in order to obtain a model $\mathcal{W}$ such that $\mathcal{W}/\langle\omega\rangle$ is smooth over $\mathbb{Z}$ and, thus, defined by an equation of the form (2.3):

$$\begin{aligned}\mathcal{W} : y^2 + Q(x)y + P(x) = 0, \quad P, Q \in \mathbb{Z}[x],\\ 2g+1 \leq \max\{2\deg(Q), \deg(P)\} \leq 2g+2.\end{aligned}$$

Remark 3.2. But this is not always possible. For example, the special fiber of Morita's integral model of X_0^{87} at $p = 29$ has the following form:



Clearly, by blowing-down exceptional divisors it is not possible to obtain a fiber $\mathcal{W}_p$ such that $\mathcal{W}_p/\langle\omega\rangle$ is smooth over $\mathbb{F}_p$.

In order to obtain explicit equations, we will focus our attention in two directions:

1. Determination of the thicknesses of Weierstrass points at every prime $p|D$. Since the hyperelliptic involution is the Atkin-Lehner involution ω_D, we have that $\mathrm{WP}(\mathcal{W}) = \bigsqcup_i \mathrm{CM}(R_i)$, where $\{R_i\}$ is the set of the orders in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ containing the order $\mathbb{Z}(\sqrt{-D})$. By Theorem 2.3, thicknesses of singular specializations of $\mathrm{WP}(\mathcal{W})$ are related with roots of the polynomial $R(x) = P(x)^2 - 4Q(x)$. In §4 we shall discuss singular specialization of Heegner points and we shall give an explicit recipe to obtain such thicknesses.

2. Determination of the leading coefficient of $R(x) = P(x)^2 - 4Q(x)$*.*

Given the Weierstrass model $\mathcal{W}$ of X_0^D, let $\mathcal{U}$ be the affine open defined by the equation $y^2 + P(x)y + Q(x) = 0$. The set of *points at infinity* of $\mathcal{U}$ is the set of geometric points of the generic fiber of $\mathcal{W} \setminus \mathcal{U}$. Since Shimura curves do not have real points (cf. [29, Proposition 4.4]), this set corresponds to a pair of conjugate points living in a quadratic extension of $\mathbb{Q}$ such that the hyperelliptic involution acts on them via the unique non-trivial Galois conjugation. In particular, this implies that $\deg(P^2 - 4Q) = 2g+2$. In order to fix a hyperelliptic equation of $\mathcal{W}$, we must choose a pair of points defined over an imaginary quadratic field such that the hyperelliptic involution acts suitably on them.

It turns out that for every value D in Table 1, there exists a maximal order R_∞ in an imaginary quadratic field K_∞ with number class $h_{R_\infty} = 1$, i.e. $K_\infty = H_{R_\infty}$, discriminant coprime to D and such that $\mathrm{CM}(R_\infty) \neq \emptyset$. By [9, Lemma 5.10], complex conjugation acts on every $P_\infty \in \mathrm{CM}(R_\infty)$ as the hyperelliptic involution ω_D. We fix $P_\infty \in \mathrm{CM}(R_\infty)$ and we choose the set $\{P_\infty, \omega_D(P_\infty)\}$ to be our set of points at infinity. This choice shall fix a hyperelliptic equation $y^2 + P(x)y + Q(x) = 0$ of $\mathcal{W}$, up to transformations of the form $(x, y) \mapsto (x + a, y + h(x))$, $a \in \mathbb{Z}$, $h(x) \in \mathbb{Z}[x]$, $\deg(h(x)) \leq g + 1$.

Our goal is to determine the leading coefficient a_R of the polynomial $R(x) = P(x)^2 - 4Q(x)$. As a first approach, recall that the field of definition of P_∞ is $K_\infty = \mathbb{Q}(\sqrt{a_R})$. Moreover, a prime p divides a_R if and only if P_∞ and $\omega_D(P_\infty)$ specialize to the same $\mathbb{F}_p$-rational Weierstrass point. Hence, the determination of the specialization of these specific Heegner points will give a valuable information about the leading coefficient $a_R \in \mathbb{Z}$.

Since any $p \mid D$ is inert in R_∞, P_∞ has good reduction at p. Any Weierstrass point has singular specialization at any prime dividing D, hence $(a_R, D) = 1$. In order to determine the remaining p-adic valuations of a_R, we introduce the following definition:

Definition 3.3. Let R be a local valuation ring with uniformizer π. *The intersection index* of two ideals I_1 and I_2 of an algebra A over R is the length of the algebra $A/(I_1 + I_2)$.

Let P_1 and P_2 be the points in $\mathrm{Spec}(A)$ defined by I_1 and I_2. By [27, Lemma 3.13], the intersection index of I_1 and I_2 measures the maximal power n of π in which their inverse image $\tilde{P}_1$ and $\tilde{P}_2$ coincide in $\mathrm{Spec}(A \otimes_R (R/\pi^n R))$.

Recall that P_∞ lies in the affine open defined by the relation $z^2 + Q_1(v)z + P_1(v) = 0$, where $Q_1(v) = v^{g+1}Q(1/v)$ and $P_1(v) = v^{2g+2}P(1/v)$. Moreover, the ideals defining P_∞ and $\omega_D(P_\infty)$ are

$$I_{P_\infty} = \langle v, z + \frac{Q_1(0)+\sqrt{a_R}}{2}\rangle, \quad I_{\omega_D(P_\infty)} = \langle v, z + \frac{Q_1(0)-\sqrt{a_R}}{2}\rangle.$$

Set $K_p = K_\infty \otimes_{\mathbb{Q}} \mathbb{Q}_p$, let K_p^{unr} be the maximal unramified extension of K_p and let R_p^{unr} be its integer ring with uniformizer π. Write $\mathcal{W}_p^{\mathrm{unr}}$ for the extension of scalars $\mathcal{W} \times \mathrm{Spec}(R_p^{\mathrm{unr}})$ and denote also by P_∞ and $\omega_D(P_\infty)$ their inverse image in $\mathcal{W}_p^{\mathrm{unr}}$. Write $(P_\infty, \omega_D(P_\infty))_p$ for the intersection index between P_∞ and $\omega_D(P_\infty)$ in $\mathcal{W}_p^{\mathrm{unr}}$. Then, it is easy to check that $(P_\infty, \omega_D(P_\infty))_p$ is precisely $\nu_p(a_R)$, if p ramifies or splits in K_∞, and $\nu_p(a_R)/2$, if p is inert in K_∞.

Assume that $p \nmid D$. Since $\mathcal{X}/\mathbb{Z}$ is the coarse moduli space associated to the algebraic stack that classifies abelian surfaces with QM by $\mathcal{O}$ over any arbitrary base scheme (cf. [3]) and $\mathcal{W}_p^{\mathrm{unr}} = \mathcal{X}_p^{\mathrm{unr}}$, this intersection index can be interpreted in terms of the algebraic objects classified by $P_\infty = [A_\infty, i_\infty]$ and $\omega_D(P_\infty) = [A'_\infty, i'_\infty]$. Namely,

(3.6)
$$(P_\infty, \omega_D(P_\infty))_p := \max\{n \geq 1 : \ (A_\infty, i_\infty) \simeq (A'_\infty, i'_\infty) \text{ over } \mathrm{R_p^{unr}/\pi^n R_p^{unr}}\}.$$

In section §6 we describe the specialization of those Heegner points $P \in \mathrm{CM}(R)$ with class number $h_R = 1$ and we provide a description of $(P, \omega_D(P))_p$ in purely algebraic and computable terms.

4. Specialization of Heegner points

For any two square-free positive integers d and n let $\mathrm{Pic}(d,n)$ stand for the set of isomorphism classes of oriented Eichler orders of level n in a quaternion algebra of discriminant d (see [21, §2.1] for the definition of oriented Eichler order).

Let $\mathcal{X}/\mathbb{Z}$ be Morita's integral model of X_0^D as above. Let $p \mid D$ be a prime of bad reduction of $\mathcal{X}$. Thanks to the work of Cerednik and Drinfeld (cf. [4],[5]), we know that the special fiber $\mathcal{X}_p$ at p is semi-stable. Moreover, its sets of singular points $(\mathcal{X}_p)_{\mathrm{sing}}$ and irreducible components $(\mathcal{X}_p)_c$ are in one-to-one correspondence with the sets $\mathrm{Pic}(\frac{D}{p}, p)$ and two copies of $\mathrm{Pic}(\frac{D}{p}, 1)$, respectively. We shall denote by

$$\varepsilon_s : (\mathcal{X}_p)_{\mathrm{sing}} \overset{1:1}{\longleftrightarrow} \mathrm{Pic}(D/p, p) \tag{4.7}$$

and

$$\varepsilon_c : (\mathcal{X}_p)_c \overset{1:1}{\longleftrightarrow} \mathrm{Pic}(D/p, 1) \sqcup \mathrm{Pic}(D/p, 1) \tag{4.8}$$

the corresponding bijections.

For any $\tilde{P} = [\tilde{A}, \tilde{i}] \in (\mathcal{X}_p)_{\mathrm{sing}}$, the endomorphism ring $\mathrm{End}(\tilde{A}, \tilde{i})$ is an Eichler order of level p in a definite quaternion algebra of discriminant D/p, equipped with natural orientations [26, Proposition 2.1], hence its isomorphism class can be regarded as an element of $\mathrm{Pic}(\frac{D}{p}, p)$. Moreover, one can see in [21, §5] that $\varepsilon_s(\tilde{P}) = \mathrm{End}(\tilde{A}, \tilde{i})$.

Lemma 4.1. [6, §3] *The thickness $e_{\tilde{P}}$ of any $\tilde{P} \in (\mathcal{X}_p)_{\rm sing}$ is given by $e_{\tilde{P}} = \epsilon(\varepsilon_s(\tilde{P}))$, where $\epsilon : \mathrm{Pic}(D/p,p) \to \mathbb{Z}$ stands for the natural map*

$$\epsilon(\mathcal{O}_i) = \#(\mathcal{O}_i^*/\langle \pm 1\rangle), \quad \textit{for all } \mathcal{O}_i \in \mathrm{Pic}(D/p,p). \tag{4.9}$$

We proceed to introduce the concept of optimal embedding. It shall be useful for future computations since Heegner points are in correspondence with certain optimal embeddings. Throughout, for any $\mathbb{Z}$-algebra $\mathcal{D}$, write $\mathcal{D}^0 = \mathcal{D} \otimes_{\mathbb{Z}} \mathbb{Q}$.

Definition 4.2. Let $\mathcal{O}_{d,n}$ be an oriented Eichler order in $\mathrm{Pic}(d,n)$ and let R be an order in an imaginary quadratic field K. An *optimal embedding* with respect to R is a ring monomorphism $\varphi : K \hookrightarrow \mathcal{O}_{d,n}^0$ such that $\varphi(K) \cap \mathcal{O}_{d,n} = \varphi(R)$. For any oriented Eichler order $\mathcal{O}_{d,n}$, let $\mathrm{CM}_{\mathcal{O}_{d,n}}(R)$ denote the set of optimal embeddings $\varphi : R \hookrightarrow \mathcal{O}_{d,n}$, up to conjugation by $\mathcal{O}_{d,n}^*$. Let $\mathrm{CM}_{d,n}(R) = \sqcup_{\mathcal{O}_{d,n} \in \mathrm{Pic}(d,n)} \mathrm{CM}_{\mathcal{O}_{d,n}}(R)$, where $\mathcal{O}_{d,n} \in \mathrm{Pic}(d,n)$ runs over a set of representatives of oriented Eichler orders.

It is well known (see [21, §2.2]) that there is a one-to-one correspondence between the set $\mathrm{CM}(R)$ and the set of optimal embeddings $\mathrm{CM}_{D,1}(R)$. We denote this correspondence by:

$$\begin{array}{rcl} \varphi : \mathrm{CM}(R) & \longrightarrow & \mathrm{CM}_{D,1}(R) \\ P & \longmapsto & \varphi(P). \end{array} \tag{4.10}$$

Let $\mathrm{Pic}(R)$ be the Picard group of R, i.e. the group of isomorphism classes of projective R-modules of rank 1. Let $\Phi_R : \mathrm{Pic}(R) \to \mathrm{Gal}(H_R/K)$ be the group isomorphism given by Artin's reciprocity map. Recall that all $P \in \mathrm{CM}(R)$ are defined over H_R.

As is well known (cf. [32, §5]), there is a faithful action of $\mathrm{Pic}(R)$ on $\mathrm{CM}_{d,n}(R)$. For any $[J] \in \mathrm{Pic}(R)$ and $\psi \in \mathrm{CM}_{d,n}(R)$, denote such action by $[J] * \psi$. The following theorem, known as the *Shimura reciprocity law*, describes the Galois action of $\mathrm{Gal}(H_R/K)$ in terms of the action of $\mathrm{Pic}(R)$ on $\mathrm{CM}_{D,1}(R)$, via the correspondence of (4.10):

Theorem 4.3. [28, Main Theorem I] *Let $P \in \mathrm{CM}(R) \subset X_0^D(H_R)$. Then, if $[J] \in \mathrm{Pic}(R)$,*

$$[J]^{-1} * \varphi(P) = \varphi(P^{\Phi_R([J])}).$$

Fix an algebraic closure $\mathbb{F}$ of $\mathbb{F}_p$. We proceed to describe the specialization map

$$\Pi : X_0^D(\overline{\mathbb{Q}}) \to \mathcal{X}_p(\mathbb{F}), \tag{4.11}$$

focusing on the specialization of Heegner points. Let $P = [A, i] \in X_0^D(\bar{\mathbb{Q}})$. Pick a field of definition H of (A, i). Fix a prime $\mathfrak{P}$ of H above p and let $\tilde{A}$ be the specialization of A at $\mathfrak{P}$. By [25, Theorem 3], A has potential good reduction. Hence after extending H if necessary, we obtain that $\tilde{A}$ is smooth over $\mathbb{F}$. The pair $(\tilde{A},\tilde{i})$, where the embedding $\tilde{i}$ stands for the composition $\mathcal{O}\overset{i}{\hookrightarrow}\mathrm{End}(A)\hookrightarrow\mathrm{End}(\tilde{A})$, defines an abelian surface with quaternionic multiplication by $\mathcal{O}$. Moreover, $\Pi(P)=[\tilde{A},\tilde{i}]\in\mathcal{X}_p(\mathbb{F})$ is the specialization of P.

Let $P=[A,i]\in\mathrm{CM}(R)$ be a Heegner point. By [21, Lemma 4.1], when P specializes to a singular point the natural map $\phi_P:\mathrm{End}(A,i)\to\mathrm{End}(\tilde{A},\tilde{i})$ turns out to be an optimal embedding in $\mathrm{CM}_{D/p,p}(R)$. If instead P has non-singular specialization, modifying the embedding $\mathrm{End}(A,i)\hookrightarrow\mathrm{End}(\tilde{A},\tilde{i})$ as in [21, §5] one obtains an optimal embedding $\phi_P^c\in\mathrm{CM}_{D/p,1}(R)$. In both cases, the isomorphism class of their target, that lies in $\mathrm{Pic}(D/p,p)$ and $\mathrm{Pic}(D/p,1)$ respectively, characterizes the singular point or the irreducible component where P lies.

The following result describes the specialization of the point P in terms of the behavior of p in $K=R\otimes\mathbb{Q}$, and relates the action of $\mathrm{Pic}(R)\simeq\mathrm{Gal}(H_R/K)$ on P with the corresponding ones on ϕ_P and ϕ_P^c.

Theorem 4.4. *Let $P=[A,i]\in\mathrm{CM}(R)$. Then $\Pi(P)=[\tilde{A},\tilde{i}]\in(\mathcal{X}_p)_{\mathrm{sing}}$ if and only if p ramifies in K. In this case, the assignation $P\mapsto\phi_P$ defines a bijective map*

$$\phi_s:\mathrm{CM}(R)\longrightarrow\mathrm{CM}_{\frac{D}{p},p}(R)\tag{4.12}$$

satisfying $\phi_s(P^{\Phi_R([J])})=[J]*\phi_s(P)$ for all $[J]\in\mathrm{Pic}(R)$. Moreover, if $\Pi(P)\notin(\mathcal{X}_p)_{\mathrm{sing}}$, the assignation $P\mapsto\phi_P^c$ defines a bijective map

$$\phi_c:\mathrm{CM}(R)\longrightarrow\mathrm{CM}_{\frac{D}{p},1}(R)\sqcup\mathrm{CM}_{\frac{D}{p},1}(R)\tag{4.13}$$

satisfying $\phi_c(P^{\Phi_R([J])})=[J]*\phi_c(P)$ for all $[J]\in\mathrm{Pic}(R)$

Proof. Combine [21, Theorem 5.3], [21, Theorem 5.4] and [21, Theorem 5.8] with Theorem 4.3. □

Remark 4.5. Let $\pi\colon\mathrm{CM}_{D/p,p}(R)\to\mathrm{Pic}(D/p,p)$ and $\pi'\colon$ $\mathrm{CM}_{D/p,1}(R)\sqcup\mathrm{CM}_{D/p,1}(R)\to\mathrm{Pic}(D/p,1)\sqcup\mathrm{Pic}(D/p,1)$ be the natural forgetful projections that map a conjugacy class of optimal embeddings $\varphi\colon R\hookrightarrow\mathcal{O}_i$ to the isomorphism class of its target $\mathcal{O}_i$. Notice that, if the specialization $\Pi(P)$ lies in $(\mathcal{X}_p)_{\mathrm{sing}}$, such specialization is characterized by $\varepsilon_s(\Pi(P))=\pi(\phi_s(P))$. On the other hand, if $\Pi(P)\notin(\mathcal{X}_p)_{\mathrm{sing}}$, then $\varepsilon_c(\Pi(P))=\pi'(\phi_c(P))$.

If we are able to compute the map ϕ_s explicitly, by Lemma 4.1 we shall obtain the thickness of the singular specialization of any Heegner point $P\in\mathrm{CM}(R)$ through the rule:

$$e_{\Pi(P)}=\epsilon(\pi(\phi_s(P))).\tag{4.14}$$

Once we know the specialization and the thickness of a singular Heegner point in $\mathcal{X}$, we can easily determine its specialization and its thickness in $\mathcal{W}$. Indeed, if $pr : \mathcal{X} \to \mathcal{W}$ is the blown-down map, then the thickness of a singular point $\tilde{P} \in \mathcal{W}$ is:

$$e_{\tilde{P}} = \sum_{\tilde{Q} \in \mathcal{X}_p,\, pr(\tilde{Q}) = \tilde{P}} e_{\tilde{Q}} + \#\{\mathcal{C} \text{ connected component, } pr(\mathcal{C}) = \tilde{P}\} - 1 \tag{4.15}$$

5. Computable description of the CM map ϕ_s

In order to give a computable description of the map ϕ_s we shall introduce the concept of $(\mathcal{O}, \mathcal{S})$-bimodule. We will see that the specialization of any point $P \in \mathrm{CM}(R)$ is characterized by a certain bimodule and the optimal embedding $\phi_s(P)$ can be described in purely algebraic terms.

Let p be a prime and let $\mathcal{S} \in \mathrm{Pic}(p, 1)$. An $(\mathcal{O}, \mathcal{S})$-bimodule $\mathcal{M}$ is a free module of rank 4 over $\mathbb{Z}$ endowed with structures of left $\mathcal{O}$-module and right $\mathcal{S}$-module. The $(\mathcal{O}, \mathcal{S})$-bimodules were introduced by Ribet in [26] and they provide a useful tool for the analysis of certain supersingular points on the fiber $\mathcal{X}_p$, as we now describe.

Let $\tilde{P} = [\tilde{A}, \tilde{i}] \in \mathcal{X}_p(\mathbb{F})$ such that $\tilde{A}$ is isomorphic to the product of two supersingular elliptic curves. By [30, Theorem 3.5], $\tilde{A} \simeq \tilde{E}^2$ for any fixed supersingular elliptic curve $\tilde{E}$ over $\mathbb{F}$. Let $\mathcal{S}$ be the endomorphism ring of $\tilde{E}$. Then $\mathcal{S}$ is a maximal order in a definite quaternion algebra of discriminant p. By [26, p. 37], $\mathcal{S}$ comes equipped with a natural orientation at p and therefore can be regarded as an element of $\mathrm{Pic}(p, 1)$. Hence, giving such an abelian surface $(\tilde{A}, \tilde{\imath})$ with QM by $\mathcal{O}$ is equivalent to providing an optimal embedding

$$\tilde{\imath} : \mathcal{O} \hookrightarrow M(2, \mathcal{S}) \simeq \mathrm{End}(\tilde{A}).$$

Moreover, such a map provides a left $\mathcal{O}$-module structure on the right $\mathcal{S}$-module $\mathcal{M}_{\tilde{P}} = \mathcal{S} \times \mathcal{S}$. Since $\mathcal{S} \times \mathcal{S}$ is free of rank 4 over $\mathbb{Z}$, $\mathcal{M}_{\tilde{P}}$ defines an $(\mathcal{O}, \mathcal{S})$-bimodule.

Given $\tilde{P} = [\tilde{A}, \tilde{i}] \in \mathcal{X}_p(\mathbb{F})$ as above, one can compute the endomorphism ring $\mathrm{End}(\tilde{A}, \tilde{\imath})$ in terms of the bimodule $\mathcal{M}_{\tilde{P}}$. Let $\mathrm{End}_{\mathcal{O}}^{\mathcal{S}}(\mathcal{M}_{\tilde{P}})$ be the set of $(\mathcal{O}, \mathcal{S})$-module endomorphism of $\mathcal{M}_{\tilde{P}}$, i.e., $\mathbb{Z}$-endomorphisms which are equivariant for the left action of $\mathcal{O}$ and the right action of $\mathcal{S}$. Then it is easy to check that $\mathrm{End}(\tilde{A}, \tilde{\imath}) = \mathrm{End}_{\mathcal{O}}^{\mathcal{S}}(\mathcal{M}_{\tilde{P}})$ (cf.[21, p.7]).

Let $P = [A, i] \in \mathrm{CM}(R)$ be a Heegner point and assume that $p \mid D$. It follows from [26, §4] that if $\Pi(P) = [\tilde{A}, \tilde{i}] \in (\mathcal{X}_p)_{\mathrm{sing}}$, the abelian surface $\tilde{A}$ is isomorphic to a product of supersingular elliptic curves. It thus makes sense to consider its attached bimodule $\mathcal{M}_{\Pi(P)}$. Next theorem allows us to describe the maps ϕ_s in terms of the $(\mathcal{O}, \mathcal{S})$-bimodule $\mathcal{M}_{\Pi(P)}$.

Theorem 5.1. [21, Theorem 4.2] *Let $P = [A, i] \in \mathrm{CM}(R)$ be a Heegner point and let $(\varphi(P) : R \hookrightarrow \mathcal{O}) \in \mathrm{CM}_{D,1}(R)$ be its corresponding optimal embedding. Assume that $p \mid D$ and $\Pi(P) \in (\mathcal{X}_p)_{\mathrm{sing}}$. Then,*

(a) *There exists an optimal embedding $\psi_p : R \hookrightarrow \mathcal{S}$ such that*

$$\mathcal{M}_{\Pi(P)} = \mathcal{O} \otimes_R \mathcal{S}, \tag{5.16}$$

where $\mathcal{S}$ is regarded as left R-module via ψ_p and $\mathcal{O}$ as right R-module via $\varphi(P)$.

(b) *The optimal embedding $\phi_s(P)$ is given by the rule*

$$\begin{array}{rcl} R & \hookrightarrow & \mathrm{End}^{\mathcal{S}}_{\mathcal{O}}(\mathcal{O}\otimes_R\mathcal{S}) \\ \delta & \longmapsto & \alpha\otimes s\mapsto\alpha\delta\otimes s, \end{array} \tag{5.17}$$

up to conjugation by $\mathrm{End}^{\mathcal{S}}_{\mathcal{O}}(\mathcal{O}\otimes_R\mathcal{S})^{\times}$.

Remark 5.2. The embedding $\psi_p : R \hookrightarrow \mathcal{S}$ depends on the immersion $\rho : H_R \hookrightarrow \overline{\mathbb{Q}}_p$ chosen for the specialization. Given another optimal embedding $\psi_p' \in \mathrm{CM}_{p,1}(R)$, there exists a different immersion $\rho' : H_R \hookrightarrow \overline{\mathbb{Q}}_p$ such that, specializing via ρ', Theorem 5.1 applies with ψ_p' instead of ψ_p. Indeed, as one can see in [21, §4], the embedding ψ_p corresponds to the inclusion $\mathrm{End}(E) \hookrightarrow \mathrm{End}(\tilde{E})$, where E is the CM elliptic curve $\mathbb{C}/R$ and $\tilde{E}$ is its specialization via ρ. Both, the set of immersions $H_R \hookrightarrow \overline{\mathbb{Q}}_p$ and $\mathrm{CM}_{p,1}(R)$ are $\mathrm{Pic}(R)$-torsors and the action of $\sigma \in \mathrm{Gal}(H_R/K) \simeq \mathrm{Pic}(R)$ turns ψ_p into the embedding $\mathrm{End}(E^\sigma) \hookrightarrow \mathrm{End}(\tilde{E}^\sigma)$, where $\tilde{E}^\sigma$ is specialized by means of ρ. It is clear that such an optimal embedding coincides with the one obtained specializing E via $\rho' = \rho\circ\sigma$.

Since the above theorem describes the map ϕ_s in terms of purely algebraic objects, we shall be able to compute the image $\phi_s(P)$ starting from the corresponding embedding $\varphi(P) \in \mathrm{CM}_{D,1}(R)$ of (4.10). Next, we shall present an explicit description of $\phi_s(P)$ obtained from an explicit description of $\varphi(P)$.

Definition 5.3. Given a quaternion algebra B, an imaginary quadratic field K and an embedding $\psi : K \hookrightarrow B$, *the quaternionic complement of* $\psi(K)$ is the set

$$\psi(K)_- = \{\alpha\in B\colon\ \alpha\psi(x) = \psi(x^\sigma)\alpha,\ \text{ for all } x\in K\},$$

where σ is the single non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$. By [32, §1], $\psi(K)_-$ is a K-vector space of dimension 1. We sometimes refer the element of a basis as a *quaternionic complement of* ψ. It is an element $j\in B$ such that $j\psi(x) = \psi(x^\sigma)j,$ for all $x\in K$ and $j^2\in\mathbb{Q}$.

Let $(\psi : R \hookrightarrow \mathcal{O}_{d,n}) \in \mathrm{CM}_{d,n}(R)$ be an optimal embedding. The free right R-module structure of $\mathcal{O}_{d,n}$ given by ψ provides a decomposition $\mathcal{O}_{d,n} \simeq R\oplus eI$, where I is a locally free R-module and $e\in\mathcal{O}^0_{d,n}$. This decomposition determines completely ψ. On the other hand, $\mathcal{O}^0_{d,n}$ is characterized by the presentation $\mathcal{O}^0_{d,n} \simeq K\oplus jK$, where $\mathcal{O}^0_{d,n}$ is also regarded as a right K-vector space via ψ and jK is the quaternionic complement of $K \overset{\psi}{\hookrightarrow} \mathcal{O}^0_{d,n}$. Recall that j is determined by $j^2\in\mathbb{Q}$ and the fact that $j\psi(x) = \psi(x^\sigma)j,$ for all $x\in K$.

In conclusion, in order to compute $(\phi_s(P) : R\hookrightarrow\Lambda)\in\mathrm{CM}_{D/p,Np}(R)$ explicitly, we only have to present the corresponding decompositions of Λ and Λ^0 via $\phi_s(P)$.

Theorem 5.4. *Let $P \in \mathrm{CM}(R)$ be a Heegner point and assume that $p \mid D$ and $\Pi(P) \in (\mathcal{X}_p)_{\mathrm{sing}}$. Let $(\psi_p : R \hookrightarrow \mathcal{S}) \in \mathrm{CM}_{p,1}(R)$ be the fixed optimal embedding of Theorem 5.1. Write $\mathcal{S}^0 = H$ and let $H = K \oplus j_2 K$, $\mathcal{S} \simeq R \oplus e_2 I_2$, $j_2^2 = m_2$, $e_2 = e_{2,1} + j_2 e_{2,2}$, be the presentations of H and $\mathcal{S}$ induced by ψ_p. Analogously, let $B = K \oplus j_1 K$ and $\mathcal{O} \simeq R \oplus e_1 I_1$, $j_1^2 = m_1$, $e_1 = e_{1,1} + j_1 e_{1,2}$, be the presentations of B and $\mathcal{O}$ induced by $\varphi(P)$. Then, the optimal embedding $\phi_s(P) : R \hookrightarrow \Lambda$ is characterized by:*

$$\Lambda^0 = K \oplus j_3 K \quad \textit{and} \quad \Lambda = R \oplus e_3 I_3\,,$$

where j_3 is a quaternionic complement of $\phi_s(P)$ such that $j_3^2 = m_1 \cdot m_2$, $e_3 = e_{2,1} \cdot e_{1,1}^\sigma - j_3 e_{2,2} \cdot e_{1,2}^\sigma$ and

$$I_3 = \begin{cases} I_2 I_1^\sigma & \textit{if } e_{1,1} = 0, e_{2,1} = 0,\\ I_2 I_1^\sigma \cap \frac{1}{e_{1,1}^\sigma} I_2 & \textit{if } e_{1,1} \neq 0, e_{2,1} = 0,\\ (I_2 \cap \frac{1}{e_{2,1}} R) I_1^\sigma & \textit{if } e_{1,1} = 0, e_{2,1} \neq 0,\\ (I_2 \cap \frac{1}{e_{2,1}} R) I_1^\sigma \cap \frac{1}{e_{1,1}^\sigma} I_2 & \textit{if } e_{1,1} \neq 0, e_{2,1} \neq 0. \end{cases}$$

Proof. Attached to the right K-module structure of B via $\varphi(P)$ we have two distinct basis, namely $\langle 1, j_1\rangle$ and $\langle 1, e_1\rangle$. We denote by $M_{e_1} = \begin{pmatrix} 1 & e_{1,1} \\ 0 & e_{1,2} \end{pmatrix}$ the matrix attached to the change of basis.

It follows that an element $z = x + j_1 y \in K \oplus j_1 K = B$ acts on $K \oplus j_1 K$ via the matrix

$$M_z = \begin{pmatrix} x & m_1 y^\sigma \\ y & x^\sigma \end{pmatrix} \in M_2(K).$$

Since $B \otimes_K H = (K \oplus j_1 K) \otimes_K H = H \oplus j_1 H$, any element $z = x + j_1 y \in B$ acts on $B \otimes_K H$ through the same matrix M_z. Hence

$$\Lambda^0 = \mathrm{End}_B^H(B \otimes_K H) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(H) \;/\; M_z \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} M_z \right\}.$$

This implies that $a = d$, $m_1 c = b$, $a \in \{x \in H\colon\ xy = yx, \ \text{ for all } y \in K\} = K$ and $b \in \{x \in H\colon\ xy = y^\sigma x, \ \text{ for all } y \in K\} = j_2 K$. Thus

$$\Lambda^0 = K \oplus \begin{pmatrix} 0 & m_1 j_2 \\ j_2 & 0 \end{pmatrix} K = K \oplus j_3 K, \quad j_3 = \begin{pmatrix} 0 & m_1 j_2 \\ j_2 & 0 \end{pmatrix} \tag{5.18}$$

where j_3 satisfies $x j_3 = j_3 x^\sigma$ for all $x \in K$ and $j_3^2 = m_1 m_2 \in \mathbb{Q}$. Hence j_3 is a quaternionic complement of $\phi_s(P) : K \hookrightarrow \Lambda^0$.

The R-module decomposition $\mathcal{O} = R \oplus e_1 I_1$ yields the $\mathcal{S}$-module structure of $\mathcal{O} \otimes_R \mathcal{S}$ as $\mathcal{S} \times (I_1 \otimes_R \mathcal{S})$ with basis $\langle 1, e_1\rangle$. We turn it into our original basis $\langle 1, j_1\rangle$ by means of M_{e_1}. Then,

$$\Lambda = \{(a + j_3 b) \in \Lambda \otimes_{\mathbb{Z}} \mathbb{Q} \;/\; M_{e_1}^{-1}(a + j_3 b) M_{e_1} (\mathcal{S} \times (I_1 \otimes_R \mathcal{S})) \subseteq \mathcal{S} \times (I_1 \otimes_R \mathcal{S})\}.$$

We obtain that $M_{e_1}^{-1}(a+j_3b)M_{e_1}=a+M_{e_1}^{-1}j_3M_{e_1}b$ where:

$$M_{e_1}^{-1}j_3M_{e_1}=\begin{pmatrix}-j_2&0\\0&j_2\end{pmatrix}\frac{1}{e_{1,2}^{\sigma}}\begin{pmatrix}e_{1,1}^{\sigma}&\mathrm{N}(e_1)\\1&e_{1,1}\end{pmatrix}.$$

Hence the R-module Λ consists of elements $a+j_3b\in\Lambda^0$ with $a,b\in K$ such that, for all $x\in\mathcal{S}$ and all $y\in(I_1\otimes_R\mathcal{S})$,

$$\begin{pmatrix}ax\\ay\end{pmatrix}+\begin{pmatrix}-j_2&0\\0&j_2\end{pmatrix}\frac{1}{e_{1,2}^{\sigma}}\begin{pmatrix}e_{1,1}^{\sigma}&\mathrm{N}(e_1)\\1&e_{1,1}\end{pmatrix}\begin{pmatrix}bx\\by\end{pmatrix}\in\mathcal{S}\times(I_1\otimes_R\mathcal{S}).$$

We deduce that

(5.19)
$$\begin{cases}ax-j_2\dfrac{e_{1,1}^{\sigma}bx+\mathrm{N}(e_1)by}{e_{1,2}^{\sigma}} & =ax+\dfrac{e_{2,1}(e_{1,1}^{\sigma}bx+\mathrm{N}(e_1)by)}{e_{1,2}^{\sigma}\cdot e_{2,2}}-e_2\dfrac{e_{1,1}^{\sigma}bx+\mathrm{N}(e_1)by}{e_{1,2}^{\sigma}\cdot e_{2,2}}\in\mathcal{S}\\ ay+j_2\dfrac{bx+e_{1,1}by}{e_{1,2}^{\sigma}} & =ay-\dfrac{e_{2,1}(bx+e_{1,1}by)}{e_{1,2}^{\sigma}\cdot e_{2,2}}+e_2\dfrac{bx+e_{1,1}by}{e_{1,2}^{\sigma}\cdot e_{2,2}}\in I_1\otimes_R\mathcal{S}.\end{cases}$$

Set $e_3=e_{2,1}\cdot e_{1,1}^{\sigma}-j_3e_{2,2}\cdot e_{1,2}^{\sigma}$. For all $a,b\in K$, we have that $a+j_3b=a'+e_3b'$, where $a'=a+\frac{e_{2,1}e_{1,1}^{\sigma}}{e_{2,2}\cdot e_{12}^{\sigma}}b$ and $b'=-\frac{b}{e_{2,2}\cdot e_{1,2}^{\sigma}}$.

Thus the expressions of (5.19) become (with this new basis $\langle 1,e_3\rangle$):

$$(a'x-e_{2,1}\mathrm{N}(e_1)b'y)+e_2(e_{1,1}^{\sigma}b'x+\mathrm{N}(e_1)b'y)\in\mathcal{S}\tag{5.20}$$

$$(a'y+e_{2,1}\mathrm{Tr}(e_{1,1})b'y+e_{2,1}b'x)-e_2(b'x+e_{1,1}b'y)\in I_1\otimes_R\mathcal{S}.\tag{5.21}$$

In particular, assuming $y=0$ we obtain from (5.20) that $(a'+e_2e_{1,1}^{\sigma}b')x\in\mathcal{S}=R\oplus e_2I_2$. This implies that $a'\in R$ and $e_{1,1}^{\sigma}b'\in I_2$. It follows from (5.21) that $(e_{2,1}-e_2)b'x\in(I_1\otimes_R\mathcal{S})$, that is $b'^{\sigma}j_2e_{2,2}=(e_{2,1}-e_2)b'\in(I_1\otimes_R\mathcal{S})$. Hence $b'\in I_1^{\sigma}I_2'$ where

$$I_2'=\begin{cases}I_2\cap\frac{1}{e_{2,1}}R & \text{if } e_{2,1}\neq 0\\ I_2 & \text{if } e_{2,1}=0.\end{cases}$$

Assuming that $x=0$, it follows from (5.20) that $-(e_{2,1}-e_2)\mathrm{N}(e_1)b'y\in\mathcal{S}$, which is deduced from $(e_{2,1}-e_2)b'\in(I_1\otimes_R\mathcal{S})$ above and the fact that, since $e_1I_1\in\mathcal{O}$, $\mathrm{N}(e_1)I_1I_1^{\sigma}\subseteq R$. Moreover, by (5.21) we have that $(a'+e_{2,1}\mathrm{Tr}(e_{1,1})b'-e_2e_{1,1}b')y\in I_1\otimes_R\mathcal{S}$, which is again deduced from $(e_{2,1}-e_2)b'\in I_1\otimes_R\mathcal{S}$ and $(a'+e_2e_{1,1}^{\sigma}b')x\in\mathcal{S}$, since

$$(a'+e_{2,1}\mathrm{Tr}(e_{1,1})b'-e_2e_{1,1}b')y=y(a'+e_2e_{1,1}^{\sigma}b')+(e_{2,1}-e_2)\mathrm{Tr}(e_{1,1}y)b'\in I_1\otimes_R\mathcal{S}.$$

for all $y\in I_1$ and $\mathrm{Tr}(e_{1,1}y)=\mathrm{Tr}(e_1y)\in\mathrm{Tr}(e_1I_1)\subseteq\mathbb{Z}\subset R$.

In conclusion, $a'+e_3b'\in\Lambda$ if and only if $a'\in R$ and $b'\in I_3$, where

$$I_3=\begin{cases}I_2'I_1^{\sigma}\cap\frac{1}{e_{1,1}^{\sigma}}I_2 & \text{if } e_{1,1}\neq 0\\ I_2'I_1^{\sigma} & \text{if } e_{1,1}=0.\end{cases}\tag{5.22}$$

Thus $\Lambda \simeq R \oplus e_3 I_3$, where $e_3 = e_{2,1} \cdot e_{1,1} - j_3 e_{2,2} \cdot e_{1,2}$, and j_3 is a quaternionic complement of $\phi_s(P)$, such that $j_3^2 = m_1 m_2$. □

6. Specialization of Heegner points with class number 1

Let p be a prime not dividing D. Notice that the special fiber $\mathcal{X}_p$ at p is a smooth curve over $\mathbb{F}_p$. We say that a point $P = [\tilde{A}, \tilde{i}] \in \mathcal{X}_p(\overline{\mathbb{F}}_p)$ is *supersingular* if $\tilde{A}$ is isogenous to a product of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Write $(\mathcal{X}_p)_{ss}$ for the set of supersingular points of $\mathcal{X}_p$.

It is well known that the set $(\mathcal{X}_p)_{ss}$ is in one-to-one correspondence with $\mathrm{Pic}(Dp, 1)$ (cf. [26, §3]). We denote the corresponding bijection by:

$$\varepsilon_{ss} : (\mathcal{X}_p)_{ss} \xleftrightarrow{1:1} \mathrm{Pic}(Dp, 1). \tag{6.23}$$

In analogy with the previous situation, for any $\tilde{P} = [\tilde{A}, \tilde{i}] \in (\mathcal{X}_p)_{ss}$ the endomorphism ring $\mathrm{End}(\tilde{A}, \tilde{i})$ is a maximal order in a quaternion algebra of discriminant Dp endowed with a natural orientation (cf. [26, Proposition 2.1]). Moreover, the map ε_{ss} is given by $\varepsilon_{ss}(\tilde{P}) = \mathrm{End}(\tilde{A}, \tilde{i}) \in \mathrm{Pic}(Dp, 1)$.

Let K be an imaginary quadratic field and let R be an order in K of conductor c. Let $P = [A, i] \in \mathrm{CM}(R)$ be a Heegner point. Recall the description of the specialization map $\Pi : X_0^D(\overline{\mathbb{Q}}) \rightarrow \mathcal{X}_p(\mathbb{F})$ of (4.11). By [21, §2.2], A is isomorphic to the product of two isogenous elliptic curves with CM by R, say $A \simeq E_1 \times E_2$. Therefore, since a CM elliptic curve specializes to a supersingular elliptic curve if and only if p does not split in K, we deduce that $\Pi(P) = [\tilde{A}, \tilde{i}] \in (\mathcal{X}_p)_{ss}$ if and only if p does not split in K.

We proceed to describe the specialization of those Heegner points that lie in $\mathcal{X}_p \setminus (\mathcal{X}_p)_{ss}$.

Proposition 6.1. *Let $P = [A, i] \in \mathrm{CM}(R)$ be a Heegner point and assume that $\Pi(P) = [\tilde{A}, \tilde{i}] \notin (\mathcal{X}_p)_{ss}$ (i.e. p splits in K). Then the natural map ϕ_P : $\mathrm{End}^0(A, i) \hookrightarrow \mathrm{End}^0(\widetilde{A}, \widetilde{i})$ is an isomorphism.*

Proof. We have $A \cong E_1 \times E_2$, where E_1 are E_2 are isogenous elliptic curves with CM by R. Write $\widetilde{E}_1$ and $\widetilde{E}_2$ for their specialization modulo p. Since $[\tilde{A}, \tilde{i}] \notin (\mathcal{X}_p)_{ss}$, each curve $\widetilde{E}_i$ is an ordinary elliptic curve over $\overline{\mathbb{F}}_p$ such that $K = \mathrm{End}^0(E_i) = \mathrm{End}^0(\tilde{E}_i)$. This implies that $\mathrm{End}^0(\widetilde{A}) = M_2(K) = \mathrm{End}^0(A)$ and consequently $\phi_P(\mathrm{End}^0(A, i)) = \mathrm{End}^0(\widetilde{A}, \widetilde{i})$. □

In order to describe supersingular specialization, recall that, in case $P = [A, i] \in \mathrm{CM}(R)$ and p does not split in K, the endomorphism ring $\mathrm{End}(\tilde{A}, \tilde{i})$ acquires structure of oriented Eichler order in $\mathrm{Pic}(Dp, 1)$. If in addition we assume that c is prime-to-p, by [21, Remark 4.2] the natural monomorphism ϕ_P : $\mathrm{End}(A, i) \rightarrow \mathrm{End}(\tilde{A}, \tilde{i})$ can be regarded as an optimal embedding in $\mathrm{CM}_{Dp,1}(R)$. One can see in [21, §2.1] that the set $\mathrm{CM}_{Dp,1}(R)$ is equipped with an action of the group $W(D)$ of Atkin-Lehner involutions. The following theorem relates the action of $W(D)$ on $P \in \mathrm{CM}(R)$ with the one on $\phi_P \in \mathrm{CM}_{Dp,1}(R)$.

Theorem 6.2. [21, Theorem 6.1] *Let $P = [A, i] \in \mathrm{CM}(R)$. Assume that p does not split in K and $p \nmid c$. Then, the map $P \mapsto (\mathrm{End}(A, i) \hookrightarrow \mathrm{End}(\tilde{A}, \tilde{i}))$ defines an injective map*

$$\phi_{ss} : \mathrm{CM}(R) \longrightarrow \mathrm{CM}_{Dp,1}(R), \tag{6.24}$$

satisfying $\phi_{ss}(\omega_n(P)) = \omega_n(\phi_{ss}(P))$, for all $\omega_n \in W(D)$.

Remark 6.3. Recall the natural forgetful projection $\pi : \mathrm{CM}_{Dp,1}(R) \rightarrow \mathrm{Pic}(Dp, 1)$ defined in Remark 4.5. Then, as in the previous setting, the specialization $\Pi(P) \in (\mathcal{X}_p)_{ss}$ is determined by:

$$\varepsilon_{ss}(\Pi(P)) = \pi(\phi_{ss}(P)).$$

Assume from now on that R has class number $h_R = 1$. For any $P = [A, i] \in \mathrm{CM}(R)$, we proceed to compute the intersection index $(P, \omega_m(P))_p$ of (3.6) for any $m \mid D$ in case of supersingular specialization.

Write $K_p = K \otimes_{\mathbb{Q}} \mathbb{Q}_p$, let K_p^{unr} be the maximal unramified extension of K_p and let R_p^{unr} be its integer ring with uniformizer π. Write $W_n = R_p^{\mathrm{unr}}/\pi^n R_p^{\mathrm{unr}}$. If $\omega_m(P) = [A', i'] \in \mathrm{CM}(R)$, we deduced in §3 that $(\omega_m(P), P)_p = \max\{n : (A, i) \simeq (A', i') \text{ over } W_n\}$. The following theorem computes $(\omega_m(P), P)_p$ explicitly.

Theorem 6.4. *Let $P = [A, i] \in \mathrm{CM}(R)$ be a Heegner point and let $p \nmid D$ be a prime that does not split in K and does not divide the conductor of R. Let $\Lambda = \mathrm{End}(\tilde{A}, \tilde{i}) \in \mathrm{Pic}(Dp, 1)$ and write $\Lambda^0 = \Lambda^0_+ + \Lambda^0_-$, where $\Lambda^0_+ = \phi_{ss}(P)(K)$ and Λ^0_- is its quaternionic complement. Let $\Lambda \simeq R \oplus eR$ be the decomposition of Λ provided by its free right R-module structure via $\phi_{ss}(P)$. For any $\lambda \in \Lambda^0$, write $\lambda = \lambda_+ + \lambda_-$, where $\lambda_+ \in \Lambda^0_+$ and $\lambda_- \in \Lambda^0_-$. Finally, for any $\lambda \in \Lambda$, write $\lambda = \lambda^+ + e\lambda^-$, where $\lambda^+, \lambda^- \in R$. Then, the integer $(\omega_m(P), P)_p$ is given by:*

$$(\omega_m(P), P)_p = \max\left\{ \frac{\mathrm{ord}_p(\mathrm{N}(\lambda^-))}{1 - \left(\frac{d}{p}\right)} + 1 \ : \ \lambda \in \Lambda, \ \mathrm{N}(\lambda) = m \right\} \tag{6.25}$$

where d is the discriminant of K and $\left(\frac{d}{p}\right)$ is the usual Legendre symbol. Moreover, if $\lambda \in \Lambda$ is such that $\mathrm{N}(\lambda) = m$, the following equality holds:

$$-dc^2 m = -dc^2 \mathrm{N}(\lambda_+) + \mathrm{N}(\lambda^-) D \cdot p. \tag{6.26}$$

Proof. Since $h_R = 1$, there is a single isomorphism class of elliptic curves E with CM by R, and E has supersingular specialization modulo p. Due to the fact that E has potentially good reduction, after extending K_p^{unr} if necessary, we can choose a smooth model $\mathcal{E}$ of E over R_p^{unr}.

Denote by $\mathcal{S}^n = \mathrm{End}_{W_n}(\mathcal{E})$. In particular, $\mathcal{S}^1 = \mathcal{S} = \mathrm{End}(\tilde{E})$ shall be regarded as an element of $\mathrm{Pic}(p,1)$. The monomorphism of algebras $\phi : K \simeq \mathrm{End}^0(E) \hookrightarrow \mathrm{End}^0(\tilde{E})$ yields a decomposition

$$\mathcal{S}^0 = \mathcal{S}^0_+ \oplus \mathcal{S}^0_-,$$

where $\mathcal{S}^0_+ = \phi(K)$ and $\mathcal{S}^0_-$ is its quaternionic complement. Then by the work of Gross-Zagier [10, Proposition 3.7.3],

$$\mathcal{S}^n = \mathrm{End}_{W_n}(\mathcal{E}) = \{\alpha \in \mathcal{S} \ : \ d \cdot \mathrm{N}(\alpha_-) \equiv 0 \mod p \cdot \mathrm{N}(\mathfrak{P})^{n-1}\},$$

where $\mathfrak{P} \subset R$ is the prime ideal lying above p.

By [21, §2.2], the abelian surface A is isomorphic to E^2. Hence, in order to specialize (A,i) over W_n as in the above setting, we must consider a smooth model $\mathcal{A}$ of A over R_p^{unr} and reduce modulo π^n. Write

$$\Lambda^n := \mathrm{End}_{W_n}(A,i) = \{\lambda \in \mathrm{End}_{W_n}(\mathcal{A}) \ : \ i(\alpha)\lambda = \lambda i(\alpha) \ \forall \alpha \in \mathcal{O}\}.$$

We claim that:

$$\Lambda^n = \{\alpha \in \Lambda \ : \ d \cdot \mathrm{N}(\alpha_-) \equiv 0 \mod p \cdot \mathrm{N}(\mathfrak{P})^{n-1}\}.$$

Indeed, since $A \simeq E^2$, we have $\mathrm{End}_{W_n}(\mathcal{A}) \simeq M_2(\mathcal{S}^n)$. Moreover, due to the fact that $\mathcal{O} \simeq R \times R$ as a right R-module via $\varphi(P)$, the $(\mathcal{O}, \mathcal{S}^n)$-bimodule $\mathcal{M}_P^n = \mathcal{O} \otimes_R \mathcal{S}^n$ is isomorphic to $\mathcal{S}^n \times \mathcal{S}^n$ as a right $\mathcal{S}^n$-order. By a similar argument as in [21, Theorem 4.2], we obtain that $\Lambda^n = \mathrm{End}_{\mathcal{O}}^{\mathcal{S}^n}(\mathcal{M}_P^n)$.

For any prime $q \neq p$ $\mathcal{S}_q = \mathcal{S}_q^n$. Hence we deduce that $\Lambda_q^n = \Lambda_q^1 = \Lambda_q$. On the other hand, Λ_p^n corresponds to matrices in $M_2(\mathcal{S}_p^n)$ that commute with $\mathcal{O}_p = M_2(\mathbb{Z}_p)$, thus $\Lambda_p^n \simeq \mathcal{S}_p^n$. Applying the description of $\mathcal{S}^n$ above, the desired claim follows.

Let us consider $\omega_m(P) = [A', i'] \in \mathrm{CM}(R)$. By [11, Corollary 2], the abelian surfaces with QM (A,i) and (A',i') are isogenous. By this we mean that there exists an isogeny $\lambda : A \rightarrow A'$ making, for all $\alpha \in \mathcal{O}$, the following diagram commutative:

$$\begin{tikzcd} A \arrow[r, "\lambda"] \arrow[d, "i(\alpha)"'] & A' \arrow[d, "i'(\alpha)"] \\ A \arrow[r, "\lambda"] & A' \end{tikzcd}$$

Write $I_m^n = \mathrm{Hom}_{W_n}((A,i),(A',i'))$ for the set of isogenies between $(A,i)/W_n$ and $(A',i')/W_n$. Then it is easy to check that $I_m^n = \mathrm{Hom}_{\mathcal{O}}^{\mathcal{S}_n}(\mathcal{M}_P^n, \mathcal{M}_{\omega_m(P)}^n)$ and, consequently, I_m^n is a right Λ^n-module. Clearly, $(A,i) \simeq (A',i')$ over W_n if and only if I_m^n is principal.

By [21, Remark 4.10], $I_m^1 = \mathrm{Hom}_{\mathbb{F}}((A,i),(A',i'))$ is the single (two-sided) ideal of Λ of norm m. Hence, if (A,i) and (A',i') were isomorphic over $\mathbb{F}$, I_m^1 would be principal, i.e. it would be generated by an element $\lambda \in \Lambda$ of norm m.

Since $p \nmid D$, under the embedding $\Lambda^n \hookrightarrow \Lambda$, the ideal I_m^n is the only ideal in Λ^n lying above I_m^1. This means that I_m^n is principal if and only if there exists an element $\lambda \in \Lambda_n$ that generates I_m^1, or equivalently, $\lambda \in \Lambda$, $\mathrm{N}(\lambda) = m$ and $d\mathrm{N}(\lambda_-) \equiv 0 \mod p \cdot \mathrm{N}(\mathfrak{P})^{n-1}$. Computing the norm $\mathrm{N}(\mathfrak{P})$ in both cases $p \mid d$ and $p \nmid d$ we conclude that :

$$(6.27)\quad (\omega_m(P), P)_p = \begin{cases} \max\{\mathrm{ord}_p(d \cdot \mathrm{N}(\lambda_-)) \ : \ \lambda \in \Lambda,\ \mathrm{N}(\lambda) = m\} & p \mid d \\ \max\{\frac{1}{2}(\mathrm{ord}_p(\mathrm{N}(\lambda_-)) + 1) \ : \ \lambda \in \Lambda,\ \mathrm{N}(\lambda) = m\} & p \nmid d \end{cases}$$

Finally, the decomposition $\Lambda \simeq R \oplus eR$, where $e = e_+ + e_-$, allows us to compute the reduced discriminant of Λ in terms of R and e. Indeed we obtain that $\mathrm{disc}(\Lambda) = e_-^2 c^2 d$. Since $\Lambda \in \mathrm{Pic}(Dp, 1)$ we deduce $Dp = e_-^2 c^2 d$ (Notice that $d < 0$ and $e_-^2 < 0$ since $\Lambda^0 = \left(\frac{d, e_-^2}{\mathbb{Q}}\right)$ is definite).

For any $\lambda \in \Lambda$, we have that $\lambda_+ = \lambda^+ + \lambda^- \cdot e_+$ and $\lambda_- = e_- \cdot \lambda^-$. If in addition $\mathrm{N}(\lambda) = m$, then $\mathrm{N}(\lambda) = \mathrm{N}(\lambda_+) + \mathrm{N}(\lambda_-) = m$, where $\mathrm{N}(\lambda_-) = -e_-^2 \cdot \mathrm{N}(\lambda^-) = -\frac{\mathrm{N}(\lambda^-) Dp}{c^2 d}$. Thus,

$$-dc^2 m = -dc^2 \mathrm{N}(\lambda_+) + \mathrm{N}(\lambda^-) Dp.$$

Since by hypothesis $\mathrm{ord}_p(c) = 0$, we have that

$$\mathrm{ord}_p(d \cdot \mathrm{N}(\lambda_-)) = \mathrm{ord}_p(dc^2 \cdot \mathrm{N}(\lambda_-)) = \mathrm{ord}_p(-pD \cdot \mathrm{N}(\lambda^-)) = \mathrm{ord}_p(\mathrm{N}(\lambda^-)) + 1.$$

Finally, one obtains the desired formula from (6.27). □

Remark 6.5. Notice that the integers $-dc^2 m$, $-dc^2 \mathrm{N}(\lambda_+)$ and $\mathrm{N}(\lambda_-) Dp$ are all positive. Hence, given D, m and d, equation (6.26) gives a finite number of possible p and $\mathrm{N}(\lambda_-)$. Moreover, the valuation of such $\mathrm{N}(\lambda_-)$ at p provides the intersection index $(\omega_m(P), P)_p$.

7. Algorithm to compute equations

Let $X = X_0^D/\mathbb{Q}$ be an hyperelliptic Shimura curve of genus $g \geq 3$ and let $\mathcal{X}/\mathbb{Z}$ be Morita's integral model of X. Assume that we can obtain a Weierstrass model $\mathcal{W}$ of X by blowing down certain exceptional divisors of some special fibers of $\mathcal{X}$. We proceed to describe an algorithm to compute an hyperelliptic equation for $\mathcal{W}$ over $\mathbb{Z}[1/2]$:

$$\mathcal{W} : y^2 = R(x), \quad R(x) \in \mathbb{Z}[x], \quad \deg(R) = 2g + 2.$$

Step 1: Reduction of the set of Weierstrass points at bad primes. Let $\mathrm{CM}(R_i)$ be a set of Heegner points in $\mathrm{WP}(X)$. By [32, Theorem 5.11 and Theorem 3.1], $\mathrm{CM}_{D,1}(R_i)$ is a $\mathrm{Pic}(R_i)$-orbit. Thus by Theorem 4.3, the set $\mathrm{CM}(R_i)$ is a Galois orbit. The decomposition $\mathrm{WP}(\mathcal{W}) = \bigsqcup_j \mathrm{CM}(R_j)$ gives rise to a factorization $R(x) = \prod_j p_{R_j}(x)$, where each $p_{R_i} \in \mathbb{Z}[x]$ is irreducible, $\deg(p_{R_i}) = \#\mathrm{Pic}(R_i)$ and roots of p_{R_i} correspond to Weierstrass points $\mathrm{CM}(R_i)$. Moreover, the splitting field of each p_{R_i} coincides with the field of definition of any $P \in \mathrm{CM}(R_i)$.

Fix $P \in \mathrm{CM}(R_i)$ and let $p \mid D$ be a prime. Since $R_i^0 = \mathbb{Q}(\sqrt{-D})$, Theorem 4.4 asserts that its specialization $\Pi(P)$ lies in the singular locus $(\mathcal{X}_p)_{\mathrm{sing}}$. By Remark

4.5, we are able to compute $\Pi(P)$ through the map ϕ_s of Theorem 4.4. Indeed, upon the correspondence ε_s of (4.7):

$$\varepsilon_s(\Pi(P)) = \pi(\phi_s(P)) \in \mathrm{Pic}(D/p, p).$$

Finally, in order to compute ϕ_s we exploit the theory of bimodules and the algebraic description of ϕ_s. In fact, Theorem 5.4 gives $\phi_s(P)$ explicitly.

Once we have obtained $\varepsilon_s(\Pi(P))$ for a fixed $P \in \mathrm{CM}(R_i)$, we proceed to obtain the specialization of all $Q \in \mathrm{CM}(R_i)$ using the fact that $\mathrm{CM}(R_i)$ is a Galois orbit. By Theorem 4.4,

$$\varepsilon_s(\Pi(P^{\Phi_{R_i}([J])})) = \pi(\phi_s(P^{\Phi_{R_i}([J])})) = \pi([J] * \phi_s(P)). \tag{7.28}$$

Moreover, since we have an explicit description of $\phi_s(P)$ and the $\mathrm{Pic}(R)$-action on $\phi_s(P)$ is easily computable with *MAGMA* [2], we obtain the specialization of all points in $\mathrm{CM}(R_i)$.

Notice that this recipe provides $\varepsilon_s(\Pi(Q)) \in \mathrm{Pic}(D/p, Np)$ for all $Q \in \bigsqcup \mathrm{CM}(R_i)$ which, by Lemma 4.1, describes its specialization and its thickness in $\mathcal{X}_p$. In order to obtain its thickness in $\mathcal{W}_p$ we apply formula (4.15).

Step 2: Choice of the points at infinity. As pointed out in §3, we may choose an order R_∞ with class number $h_{R_\infty} = 1$ in an imaginary quadratic field K_∞ of discriminant prime-to-D, such that $\mathrm{CM}(R_\infty) \neq \emptyset$. Notice that we can always assume that R_∞ is maximal. Fix $P_\infty = [A_\infty, i_\infty] \in \mathrm{CM}(R_\infty)$ and assume that $\{P_\infty, \omega_D(P_\infty)\}$ are the points at infinity. This fixes an affine open set of $\mathcal{W}$ defined, over $\mathbb{Z}[1/2]$, by the equation $y^2 = R(x) = \prod p_{R_i}(x)$, where $\deg(R(x)) = 2g + 2$ and the factorization $R(x) = \prod p_{R_i}(x)$ is attached to the decomposition $\mathrm{WP}(\mathcal{W}) = \bigsqcup_i \mathrm{CM}(R_i)$. Let a_R and a_{R_i} be the leading coefficients of $R(x)$ and $p_{R_i}(x)$ respectively, $a_R = \prod_i a_{R_i}$. Since $\mathbb{Q}(\sqrt{a_R}) = K_\infty$, we control the sign of a_R (which is negative since K_∞ is imaginary) and its absolute value modulo squares.

In order to determine a_R, recall that $(a_R, D) = 1$ and primes dividing a_R correspond to places where both points at infinity specialize to the same $\mathbb{F}_p$-rational Weierstrass point. Thus, $\Pi(P_\infty) = \Pi(\omega_D(P_\infty)) = \Pi(P) = [\tilde{A}, \tilde{i}]$ for some $P = [A, i] \in \mathrm{WP}(\mathcal{W})$. Suppose that $\Pi(P_\infty) = \Pi(P) \notin (\mathcal{X}_p)_{ss}$. Then, by Proposition 6.1, $K \simeq \mathrm{End}^0(A, i) \simeq \mathrm{End}^0(\tilde{A}, \tilde{i}) \simeq \mathrm{End}^0(A_\infty, i_\infty) \simeq K_\infty$, which is impossible since discriminant of K_∞ is prime-to-D. Hence, for all primes $p \mid a_R$, $\Pi(P_\infty) = \Pi(\omega_D(P_\infty)) \in (\mathcal{X}_p)_{ss}$; equivalently, p does not split in both K and K_∞.

Assume that $p \mid a_R$. By relation (3.6), the valuation of a_R at p is given by

$$\nu_p(a_R) = \left(1 - \left(\frac{d}{p}\right)\right)(P_\infty, \omega_D(P_\infty))_p.$$

Since $\Pi(P_\infty) \in (\mathcal{X}_p)_{ss}$, we deduce from Theorem 6.4 that:

$$\nu_p(a_R) = \max\left\{\mathrm{ord}_p(\mathrm{N}(\lambda^-)) + 1 - \left(\frac{d}{p}\right) \;:\; \lambda \in \varepsilon(\Pi(P_\infty)),\ \mathrm{N}(\gamma) = D\right\}$$

where d is the discriminant of K_∞. Moreover, for any $\lambda \in \Lambda$ such that $\mathrm{N}(\lambda) = D$, the following relation holds:

$$-dD = -d\mathrm{N}(\lambda_+) + \mathrm{N}(\lambda^-)Dp.$$

This gives a finite number of possible p and $\mathrm{N}(\lambda^-)$ for given D and $d = \mathrm{disc}(K_\infty)$. Consequently, we have a finite number of possible $\nu_p(a_R)$.

Once we have the set of possible p dividing a_R, in order to determine which a_{R_i} is divisible by p recall the maps ϕ_{ss} of (6.24) attached to supersingular specialization. By Remark 6.3, $p \neq 2$ divides a_{R_i} if and only if $\varepsilon(\Pi(P_\infty)) = \pi(\phi_{ss}(P_\infty)) \in \pi(\phi_{ss}(\mathrm{CM}(R_i)))$. Equivalently, R_i is embedded in $\varepsilon(\Pi(P_\infty)) \in \mathrm{Pic}(Dp, 1)$ optimally. There exists no pair of orders $R_i \neq R_j$ embedding optimally in the same $\Lambda \in \mathrm{Pic}(Dp, 1)$ since ϕ_{ss} is injective and two Weierstrass points can not have the same specialization whenever p is a prime of good reduction.

We are able to compute $\varepsilon(\Pi(P_\infty)) = R_\infty \oplus eR_\infty$, and consequently we shall check whether R_i is embedded optimally in it.

In case $p = 2$, we control the valuation $\nu_2(a_R)$ but we do not control the 2-valuation of each a_{R_i} if $\nu_2(a_R) \neq 0$. In any case we have an upper bound; $\nu_2(a_{R_i}) \leq \nu_2(a_R)$.

Step 3: Discriminants, Resultants and Fields of definition. For any $P \in \mathrm{WP}(\mathcal{W})$, write γ_P for the root of $R(x)$ attached to P. Since we control the specialization of every point in $\mathrm{WP}(\mathcal{W})$ and we know how to compute its thickness, Theorem 2.3 yields the valuations $\nu_p(\gamma_P - \gamma_{P'})$ for every $P, P' \in \mathrm{WP}(\mathcal{W})$ and every $p \neq 2$. This provides the discriminants $\mathrm{disc}(p_{R_i})$ and the resultants $\mathrm{Res}(p_{R_i}, p_{R_j})$ up to a power-of-2 factor, namely

$$\nu_p(\mathrm{disc}(p_{R_i})) = \sum_{P,P' \in \mathrm{CM}(R_i)} 2\cdot\nu_p(\gamma_P - \gamma_{P'}), \quad \nu_p(\mathrm{Res}(p_{R_i}, p_{R_j})) = \sum_{\substack{P \in \mathrm{CM}(R_i) \\ Q \in \mathrm{CM}(R_j)}} \nu_p(\gamma_P - \gamma_Q). \tag{7.29}$$

If in addition we assume good reduction at 2, by (2.4) we have that

$$4(g+1) = \nu_2(\mathrm{disc}(R)) = \sum_i \nu_2(\mathrm{disc}(p_{R_i})) + \sum_{i,j} \nu_2(\mathrm{Res}(p_{R_j}, p_{R_j})^2). \tag{7.30}$$

In general we obtain a finite number of possible powers of 2 dividing $\mathrm{disc}(p_{R_i})$ and $\mathrm{Res}(p_{R_i}, p_{R_j})$.

By Theorem 4.3, points in $\mathrm{CM}(R_i)$ are defined over a subfield of the ring class field H_{R_i} of R_i. We compute such field using the following theorem:

Theorem 7.1. [9, Theorem 5.12] *Let $Q \in \mathrm{CM}(R) \subset X_0^D(H_R)$ for some order R in the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$. Fix an embedding $H_R \subset \mathbb{C}$ and denote by c the complex conjugation. Then $[H_R : \mathbb{Q}(Q)] = 2$ and $\mathbb{Q}(Q) \subset H_R$ is the subfield fixed by $\sigma = c \cdot \Phi_R([\mathfrak{a}]) \in \mathrm{Gal}(H_R/\mathbb{Q})$ for some ideal $\mathfrak{a}$ such that $B \simeq \left(\frac{-D, \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})}{\mathbb{Q}}\right)$.*

Remark 7.2. One can see in [9, §5] that the class $[\mathfrak{a}] \in \mathrm{Pic}(R)$ does depend on Q. Assume that $[\mathfrak{a}] = [\mathfrak{c}]^2[\mathfrak{b}]$. Then, the Heegner point $P = \Phi_R([\mathfrak{c}])(Q) \in \mathrm{CM}(R)$ is fixed by $c \cdot \Phi_R([\mathfrak{b}])$, indeed

$$c\cdot\Phi_R([\mathfrak{b}])(P) = c\cdot\Phi_R([\mathfrak{b}][\mathfrak{c}])(Q) = c\cdot\Phi_R([\mathfrak{c}]^{-1}[\mathfrak{a}])(Q) = \Phi_R([\mathfrak{c}])\cdot c\cdot\Phi_R([\mathfrak{a}])(Q) = P$$

Thus, for any $\mathfrak{b}$ verifying that $[\mathfrak{a}]\cdot[\mathfrak{b}]^{-1} \in \mathrm{Pic}(R)^2$, there exists some $P \in \mathrm{CM}(R)$ such that $\mathbb{Q}(P)$ is the fixed field by $c \cdot \Phi_R([\mathfrak{b}])$.

Let M_{R_i} be the isomorphism class of the field $\mathbb{Q}(P)$, for any $P \in \mathrm{CM}(R_i)$. Then M_{R_i} is characterized by the class $\{\mathfrak{a}\} \in \mathrm{Pic}(R)/\mathrm{Pic}(R)^2$. It is clear that any ideal $\mathfrak{b}$ in $\{\mathfrak{a}\}$ satisfies the isomorphism $B \simeq \left(\frac{-D,\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{b})}{\mathbb{Q}}\right)$. In general, the converse is not true, but if $[H_R : H]$ is odd, where H is the Hilbert class field of K, then $\{\mathfrak{a}\} \in \mathrm{Pic}(R)/\mathrm{Pic}(R)^2$ is uniquely determined by such isomorphism (see [9, Remark 5.11]). In our particular setting, the conductor of R is 2 and, thus, $[H_R : H]$ is either 1 or 3.

This results yields the field M_{R_i} attached to $\mathrm{CM}(R_i)$. Recall that this field coincides with the splitting field of $p_{R_i}(x)$.

Step 4: Computing equations. Since we have computed the leading coefficients of each p_{R_i}, we are able to convert them into monic polynomials. Given $p_{R_i}(x) \in \mathbb{Z}[x]$ of discriminant d, leading coefficient a_{R_i} and degree n, the polynomial $q_{R_i}(x) = a_{R_i}^{n-1}(p_{R_i}(x/a_{R_i}))$ turns out to be monic with integer coefficients and discriminant $a_{R_i}^{2n-2}d$. It defines the same field as $p_{R_i}(x)$.

Let δ_{R_i} be any root of q_{R_i}. Since $q_{R_i} \in \mathbb{Z}[x]$ is monic, the root δ_{R_i} belongs to $\mathcal{O}_{M_{R_i}}$, the ring of integers of M_{R_i}. Moreover, $\mathrm{disc}(q_{R_i})$ provides the $\mathbb{Z}$-index $[\mathcal{O}_{M_{R_i}} : \mathbb{Z}[\delta_{R_i}]]$. Through the instruction *IndexFormEquation* of *MAGMA* [2] we obtain all possible δ_{R_i} of given index, up to sign and translations by integers. Thus, we are able compute all possible polynomials q_{R_i} (and consequently p_{R_i}) up to transformations of the form $p(x) \to p(\pm x + r)$ with $r \in \mathbb{Z}$. The polynomials p_{R_i} can be determined with no ambiguity by means of the resultants $R_{i,j} = \mathrm{Res}(p_{R_i}, p_{R_j})$. Namely, given $p_{R_i}(x + r_i)$ and $p_{R_j}(x + r_j)$, the equation $R_{i,j} = \mathrm{Res}(p_{R_i}(x + r_i), p_{R_j}(x + r_j))$ provides the difference $r_i - r_j$. This way we obtain the product $p_{R_i} \cdot p_{R_j}$ up to translations by an integer. Notice that, given the equation $y^2 = R(x)$, the polynomial $R(x)$ is also defined up to translations by an integer.

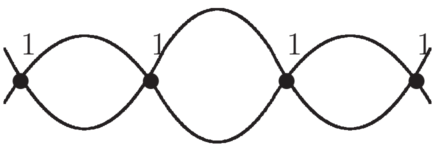
8. Siksek-Skorogatov Shimura curve $D = 3 \cdot 13$

In this section we shall compute an explicit equation for the hyperelliptic Shimura curve of discriminant $D = 39$ exploiting the algorithm explained above. This curve was used in [31] by Siksek and Skorogatov in order to find a counterexample to the Hasse principle explained by the Manin obstruction. Since their results depend on the conjectural equation of the curve given by Kurihara

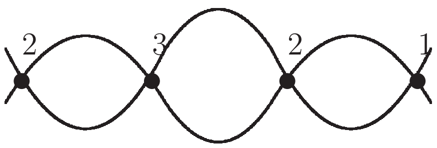
[17], the verification of such conjectural equation shows that the results of [31] are unconditionally true.

Step 1: Reduction of the set of Weierstrass points at bad primes. Let X denote the hyperelliptic Shimura curve $X_0^{39}/\mathbb{Q}$. By Proposition 3.1, $\mathrm{WP}(X) = \mathrm{CM}(R)\bigsqcup \mathrm{CM}(R_0)$, where $R_0 = \mathbb{Z}[\frac{1+\sqrt{-39}}{2}]$ and $R = \mathbb{Z}[\sqrt{-39}]$. Let $K = \mathbb{Q}(\sqrt{-39})$. Notice that both R and R_0 have class number 4, so their ring class fields have degree 4 over K.

We can compute the geometric special fiber of $\mathcal{X}$ at 3 and 13 by means of Cerednik-Drinfeld's theory (cf. [15, §3] for a step-by-step guide on the computation of these special fibers using *MAGMA* [2]). Notice that, in this case, $\mathcal{X} = \mathcal{W}$ since $\mathcal{X}/\langle\omega_D\rangle$ is smooth over $\mathbb{Z}$. In the drawings below, the integer on each singular point stands for its thickness:



Special fiber at p=3



Special fiber at p=13

Let $\mathcal{O}$ be a maximal order in the quaternion algebra B of discriminant 39. Choose arbitrary points $P \in \mathrm{CM}(R)$ and $P_0 \in \mathrm{CM}(R_0)$. As it is more convenient for computations to work with optimal embeddings instead of Heegner points, let $\varphi(P) \in \mathrm{CM}_{39,1}(R)$ and $\varphi(P_0) \in \mathrm{CM}_{39,1}(R_0)$ be the optimal embeddings attached to P and P_0, respectively, via (4.10). In particular, $\varphi(P)$ and $\varphi(P_0)$ yield the following decompositions computed with *MAGMA* [2]:

$$\begin{cases} B = K \oplus i_1 K \\ \mathcal{O} = R \oplus e_1 I_1 \end{cases} \text{where} \begin{cases} i_1 \text{ is a quaternionic complement of } \varphi(P), \quad i_1^2 = 447 \\ e_1 = i_1 + (7\cdot\sqrt{-39}+18) \\ I_1 = \langle \frac{1}{2}, \frac{\sqrt{-39}}{894} + \frac{63}{298}\rangle_R \end{cases}$$

and

$$\begin{cases} B = K \oplus i_1' K \\ \mathcal{O} = R_0 \oplus e_1' I_1' \end{cases} \text{where} \begin{cases} i_1' \text{ is a quaternionic complement of } \varphi(P_0), \quad i_1'^2 = 6 \\ e_1' = i_1' \\ I_1' = \langle 1, \frac{\sqrt{-39}-9}{12}\rangle_{R_0} \end{cases}$$

Reduction modulo 3. In order to compute the specialization modulo $p = 3$ of P and P_0, we shall compute the optimal embeddings $\psi_R \in \mathrm{CM}_{13,3}(R)$ and $\psi_{R_0} \in \mathrm{CM}_{13,3}(R_0)$ of Theorem 5.1. Their targets are maximal orders $\mathcal{S}_3$ and $\mathcal{S}_3'$ of the quaternion algebra H_3 of discriminant 3. Again both embeddings define the following decompositions:

$$\begin{cases} H_3 = K \oplus i_2 K \\ \mathcal{S}_3 = R \oplus e_2 I_2 \end{cases} \text{where} \begin{cases} i_2 \text{ is a quaternionic complement, of } \psi_R, \quad i_2^2 = -43 \\ e_2 = i_2 - 387 \\ I_2 = \langle \frac{1}{2}, \frac{\sqrt{-39}}{1118} - \frac{10}{43} \rangle_R \end{cases}$$

and

$$\begin{cases} H_3 = K \oplus i_2' K \\ \mathcal{S}_3' = R_0 \oplus e_2' I_2' \end{cases} \text{where} \begin{cases} i_2' \text{ is a quaternionic complement of } \psi_{R_0}, \quad i_2'^2 = -12 \\ e_2' = i_2' - 12 \\ I_2' = \langle 1, \frac{\sqrt{-39}-1}{156 \cdot 2} - \frac{29}{78} \rangle_{R_0} \end{cases}$$

Hence, by Theorem 5.4 the optimal embedding $\phi_s(P) : R \hookrightarrow \mathrm{End}_{\mathcal{O}}^{\mathcal{S}_3}(\mathcal{O} \otimes_R \mathcal{S}_3) = \Lambda_3$ of (4.12) is given by the decomposition:

$$\begin{cases} \Lambda_3 \otimes \mathbb{Q} = K \oplus i_3 K \\ \Lambda_3 = R \oplus e_3 I_3 \end{cases} \text{where} \begin{cases} i_3 \text{ is a quaternionic complement of } \phi_s(P), \\ \qquad\qquad\qquad\qquad\qquad i_3^2 = -43 \cdot 447 \\ e_3 = -387 \cdot (18 - 7 \cdot \sqrt{-39}) - i_3 \\ I_3 = (I_2 \cap \frac{-1}{387} R) \overline{I_1} \cap \frac{1}{18 - 7 \cdot \sqrt{-39}} I_2 \end{cases}$$

Similarly $\phi_s(P_0) : R_0 \hookrightarrow \mathrm{End}_{\mathcal{O}}^{\mathcal{S}_3'}(\mathcal{O} \otimes_{R_0} \mathcal{S}_3') = \Lambda_3'$ is given by:

$$\begin{cases} \Lambda_3' \otimes \mathbb{Q} = K \oplus i_3' K \\ \Lambda_3' = R_0 \oplus e_3' I_3' \end{cases} \text{where} \begin{cases} i_3' \text{ is a quaternionic complement of } \phi_s(P_0), \\ \qquad\qquad\qquad\qquad\qquad i_3'^2 = -12 \cdot 6 \\ e_3' = -i_3' \\ I_3' = (I_2' \cap \frac{-1}{12} R_0) \overline{I_1'}. \end{cases}$$

Once we have a characterization of the embeddings $\phi_s(P)$ and $\phi_s(P_0)$, we proceed to describe the specialization of all Heegner points in $\mathrm{CM}(R)$ and $\mathrm{CM}(R_0)$. Recall that, in both cases, the sets $\mathrm{CM}(R)$ and $\mathrm{CM}(R_0)$ are $\mathrm{Pic}(R)$ and $\mathrm{Pic}(R_0)$-orbits respectively. Moreover, $\mathrm{Pic}(R) \simeq \mathrm{Pic}(R_0) \simeq \mathbb{Z}/4\mathbb{Z}$.

Case $\mathrm{CM}(R)$: We pick a representative J of a generator $[J] \in \mathrm{Pic}(R)$. We construct the left-Λ_3-ideals $\Lambda_3\phi_s(P)(J)$, $\Lambda_3\phi_s(P)(J^2)$, $\Lambda_3\phi_s(P)(J^3)$ and we compute their right orders $\pi([J^i] * \phi_s(P))$. We obtain that their number of units are:

$$\#(\Lambda_3^*)/2 = \#(\pi([J]*\phi_s(P))^*)/2 = \#(\pi([J^2]*\phi_s(P))^*)/2 = \#(\pi([J^3]*\phi_s(P))^*)/2 = 1.$$

Thus, by (4.9), such integers are the thickness of each singular specializations.

Besides, we checked that $\Lambda_3\phi_s(P)(J)$ and $\Lambda_3\phi_s(P)(J^2)(\Lambda_3\phi_s(P)(J^3))^{-1}$ are principal, whereas $\Lambda_3\phi_s(P)(J^2)$, $\Lambda_3\phi_s(P)(J^3)$, $\Lambda_3\phi_s(P)(J)(\Lambda_3\phi_s(P)(J^2))^{-1}$, $\Lambda_3\phi_s(P)(J)(\Lambda_3\phi_s(P)(J^3))^{-1}$ are not. Since for any pair of left Λ_3-ideals I_1 and I_2 their right orders are isomorphic as oriented Eichler orders if and only if $I_1 \cdot I_2^{-1}$ is principal, it follows from (7.28) that

$$\Pi(P) = \varepsilon^{-1}(\pi(\phi_s(P))) = \varepsilon^{-1}(\pi([J] * \phi_s(P))) = \Pi(P^{\Phi_R([J])})$$

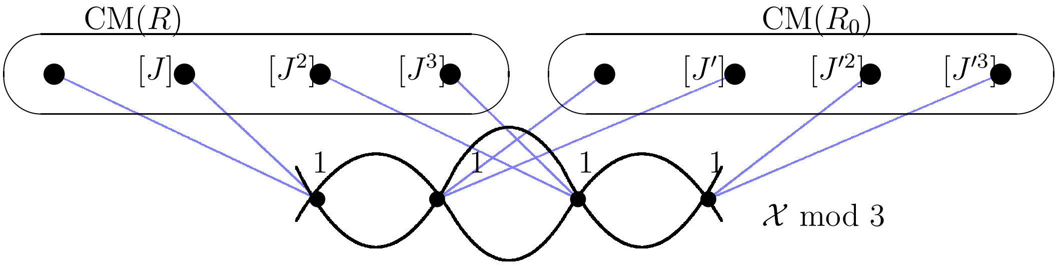
$$\Pi(P^{\Phi_R([J^2])}) = \varepsilon^{-1}(\pi([J^2] * \phi_s(P))) = \varepsilon^{-1}(\pi([J^3] * \phi_s(P))) = \Pi(P^{\Phi_R([J^3])}).$$

Case CM(R_0): Let J' be a representative of a generator of Pic(R_0). Similarly as above, we construct the corresponding left-Λ_3'-ideals and we obtain:

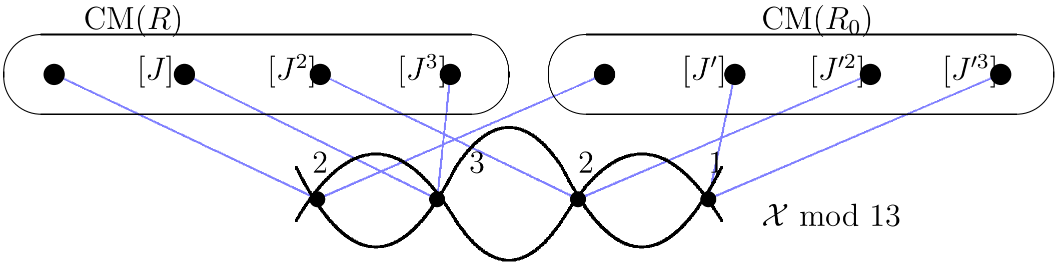
$$\begin{aligned}\#(\Lambda_3'^{*})/2 &= \#(\pi([J']*\phi_s(P_0))^*)/2\\ &= \#(\pi([J'^2]*\phi_s(P_0))^*)/2 = \#(\pi([J'^3]*\phi_s(P_0))^*)/2 = 1.\end{aligned}$$

Moreover, we checked that $\Lambda_3'\phi_s(P_0)(J')$ and $\Lambda_3'\phi_s(P_0)(J'^2)(\Lambda_3'\phi_s(P_0)(J'^3))^{-1}$ are principal, whereas the remaining ones are not. Thus $\Pi(P_0) = \Pi(P_0^{\Phi_{R_0}([J'])})$ and $\Pi(P_0^{\Phi_{R_0}([J'^2])}) = \Pi(P_0^{\Phi_{R_0}([J'^3])})$.

In conclusion we obtain the following diagram, describing the specialization of the Weierstrass points modulo $p = 3$.



Reduction modulo 13. With the same computations as in the previous setting, we obtain that the reduction of CM(R) and CM(R_0) modulo $p = 13$ is given by the following diagram:



Step 2: Choice of the points at infinity. Let $K_\infty = \mathbb{Q}(\sqrt{-7})$ and let R_∞ be its maximal order. As it is well known, $\#\mathrm{Pic}(R_\infty) = 1$. Hence, by §7, for any $P_\infty \in \mathrm{CM}(R_\infty)$ we can choose P_∞ and $\omega_{39}(P_\infty)$ to be our points at infinity. This choice of the points at infinity gives rise to an equation

$$y^2 = R(x), \quad \deg(R(x)) = 2g + 2 = 8,$$

defining the Weierstrass model $\mathcal{W}$. Let $R(x) = p_R(x)\cdot p_{R_0}(x)$ be the factorization attached to the decomposition $\mathrm{WP}(\mathcal{W}) = \mathrm{CM}(R)\sqcup \mathrm{CM}(R_0)$. Let a_R and a_{R_0} be the leading coefficients of p_R and p_{R_0} respectively.

Since $\mathbb{Q}(\sqrt{a_R \cdot a_{R_0}}) = K_\infty = \mathbb{Q}(\sqrt{-7})$, we deduce that $a_R \cdot a_{R_0} = -7 \cdot N^2$ for some $N \in \mathbb{Z}$. Given a prime p dividing $a_R \cdot a_{R_0}$, by (6.26) we know that:

$$7 \cdot 39 = m + \mathrm{N}(\lambda^-)39 \cdot p, \text{ where } m = 7\mathrm{N}(\lambda_+) \in \mathbb{Z}^+.$$

From this we obtain that $39 \mid m = 7\mathrm{N}(\lambda_+) \in \mathrm{N}(K_\infty)$. Since 3 and 13 are inert in K_∞, the fact that $39 \mid m \in \mathrm{N}(K_\infty)$ implies that $39^2 \mid m$. Then, dividing the above identity by 39, one obtains $7 = 39 \cdot m' + \mathrm{N}(\lambda^-)p$, where $m' \in \mathbb{Z}^+$. Thus $m = m' = 0$, $p = 7$ and $\mathrm{N}(\lambda^-) = 1$. Finally, by (6.25) one concludes that the leading coefficient of the hyperelliptic equation must be $a_R \cdot a_{R_0} = -7$.

Moreover, we can compute $\pi(\phi_{ss}(\varphi(P_\infty))) \in \mathrm{Pic}(39 \cdot 7, 1)$ of Remark 6.3. Namely,

$$\pi(\phi_{ss}(\varphi(P_\infty))) = R_\infty \oplus jR_\infty,$$

where jR_∞ is the quaternionic complement of R_∞ with $j^2 = -39$. Since it can be checked that $R_0 = \mathbb{Z}[\frac{1+\sqrt{-39}}{2}]$ can not be embedded in Λ, we conclude that $R = \mathbb{Z}[\sqrt{-39}]$ is embedded optimally in it. Therefore, $a_{R_0} = 1$ and $a_R = -7$.

Step 3: Discriminants, Resultants and Fields of definition. By Theorem 7.1, points in $\mathrm{CM}(R)$ and $\mathrm{CM}(R_0)$ are defined over a subfield of index 2 of the Hilbert class field H_K of K. By Remark 7.2, to find such subextension we must find an ideal $\mathfrak{a}$ of R such that $B \simeq \left(\frac{-39, \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})}{\mathbb{Q}}\right)$. As one checks, any $\mathfrak{a}$ such that $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) = 5$ does. Notice that 5 splits in K, hence writing $5 = \mathfrak{P} \cdot \mathfrak{P}'$ we have $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{P}') = 5$.

We used MAGMA [2] to compute that the Hilbert class field of K is defined by the polynomial $q(x) = x^4 + 4x^2 - 48$ over K. If α is any root of $q(x)$, then $H_K = \mathbb{Q}(\alpha, \sqrt{-39})$.

The automorphisms $\Phi_R(\mathfrak{P})$ and complex conjugation c act on H_K by the rules:

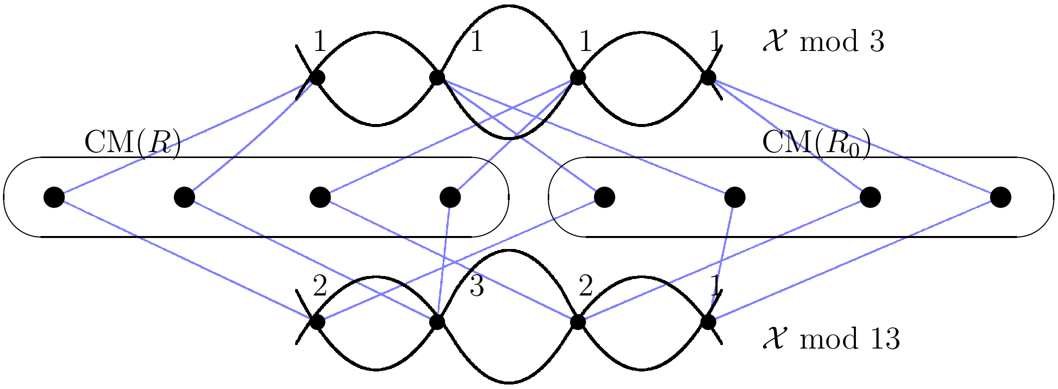
$$\Phi_R(\mathfrak{P}) : \begin{cases} \sqrt{-39} & \rightarrow & \sqrt{-39} \\ \alpha & \rightarrow & -\frac{\sqrt{-39}\alpha^3}{156} - \frac{7\sqrt{-39}\alpha}{39} \end{cases} \qquad c : \begin{cases} \sqrt{-39} & \rightarrow & -\sqrt{-39} \\ \alpha & \rightarrow & -\alpha \end{cases}$$

Thus $\sigma = c \cdot \Phi_R(\mathfrak{P})$ acts as:

$$\sigma : \begin{cases} \sqrt{-39} & \rightarrow & -\sqrt{-39} \\ \alpha & \rightarrow & -\frac{\sqrt{-39}\alpha^3}{156} - \frac{7\sqrt{-39}\alpha}{39} \end{cases}$$

We obtain that M_R, the fixed field by σ, is defined by the polynomial $x^4 + 8x^2 - 24x + 16$ over $\mathbb{Q}$. Since $\mathrm{disc}(M_R) = 3^2 \cdot 13$, we have that $\mathrm{disc}(p_R), \mathrm{disc}(p_{R_0}) = N^2 \cdot 3^2 \cdot 13$, for certain $N \in \mathbb{Z}$.

Recall the following diagram summarizing the specialization of the Weierstrass points:



By Theorem 2.3 and (7.29), we have that $|\mathrm{disc}(p_R)| = 2^{2k}\cdot 3^2\cdot 13^3$, $|\mathrm{disc}(p_{R_0})| = 2^{2k'}\cdot 3^2\cdot 13$ and $\mathrm{Res}(p_R, p_{R_0})^2 = 2^{2k''}\cdot 13^4$. Moreover, since X_0^{39} has good reduction at 2, (7.30) shows that $2k + 2k' + 2k'' = 16$.

Step 4: Computing equations. Since the leading coefficient of p_R is $a_R = -7$, we deduce that $q_R(x) = 7^3 p_R(x/7)$ is a monic polynomial of discriminant $7^6\mathrm{disc}(p_R) = 2^{2k}\cdot 3^2\cdot 13^3\cdot 7^6$.

The instruction *IndexFormEquation* of *MAGMA* [2] provides the possible candidates for p_{R_0}, q_R and p_R (denoted $\tilde{p}_{R_0}$, $\tilde{q}_R$ and $\tilde{p}_R$ respectively), up to transformations of the form $p(x) \to p(\pm x + r)$ with $r \in \mathbb{Z}$. We obtain that

$$\tilde{p}_R(x) = \left\{\begin{array}{cc} -7x^4 - 51x^3 - 116x^2 - 84x - 19 & \mathrm{disc}(\tilde{p}_R) = 3^2\cdot 13^3 \\ \left.\begin{array}{c} -7x^4 - 74x^3 - 200x^2 - 22x - 1 \\ -7x^4 + 38x^3 + 16x^2 - 182x - 169 \end{array}\right\} & \mathrm{disc}(\tilde{p}_R) = 2^{12}\cdot 3^2\cdot 13^3 \end{array}\right.$$

and there are 16 more candidates $\tilde{p}_{R_0}(x)$ for $p_{R_0}(x)$, with discriminants $3\cdot 13$, $2^4{\cdot}3{\cdot}13$, $2^{12}{\cdot}3{\cdot}13$ and $2^{16}{\cdot}3{\cdot}13$. If we compute the resultant $\mathrm{Res}(\tilde{p}_R(\mp x+\alpha), \tilde{p}_{R_0}(x))$ and look for solutions $\alpha \in \mathbb{Z}$ such that $\mathrm{Res}(\tilde{p}_R(\mp x + \alpha), \tilde{p}_{R_0}(x))^2 = 2^{2k''}\cdot 13^4$, we obtain a single solution:

$$p_{R_0}(x) = x^4 + 9x^3 + 29x^2 + 39x + 19, \quad p_R(x) = -7x^4 - 79x^3 - 311x^2 - 497x - 277.$$

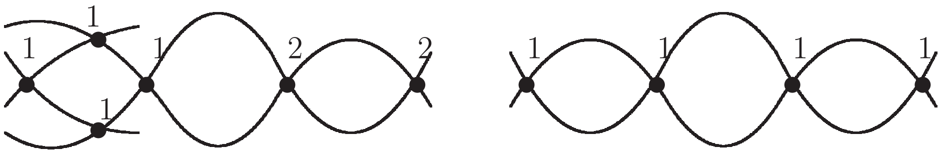
In conclusion the equation we are looking for is

$$\boxed{y^2 = -(7x^4 + 79x^3 + 311x^2 + 497x + 277)\cdot(x^4 + 9x^3 + 29x^2 + 39x + 19).}$$

Notice that this curve coincides with the one conjectured by Kurihara in [17].

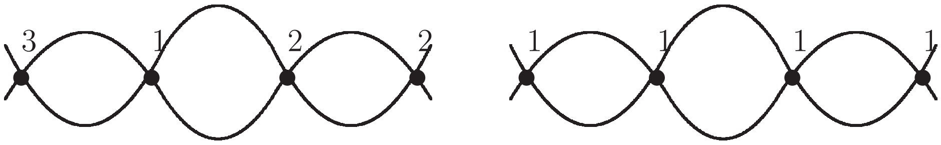
9. Case $D = 5\cdot 11$

Let X be the hyperelliptic Shimura curve $X_0^{55}/\mathbb{Q}$. In this case the set of Weierstrass points is $\mathrm{WP}(X) = \mathrm{CM}(\mathbb{Z}[\sqrt{-55}]) \bigsqcup \mathrm{CM}(\mathbb{Z}[\frac{1+\sqrt{-55}}{2}])$ and both $\mathbb{Z}[\frac{1+\sqrt{-55}}{2}]$ and $\mathbb{Z}[\sqrt{-55}]$ have class number 4. As is the above situation, we can compute the geometric special fiber of $\mathcal{X}$ at 5 and 11 using [15, §3]. In this case, the integral model $\mathcal{X}$ does not correspond to a Weierstrass model since $\mathcal{X}/\langle\omega_D\rangle$ is not smooth over $\mathbb{Z}$.



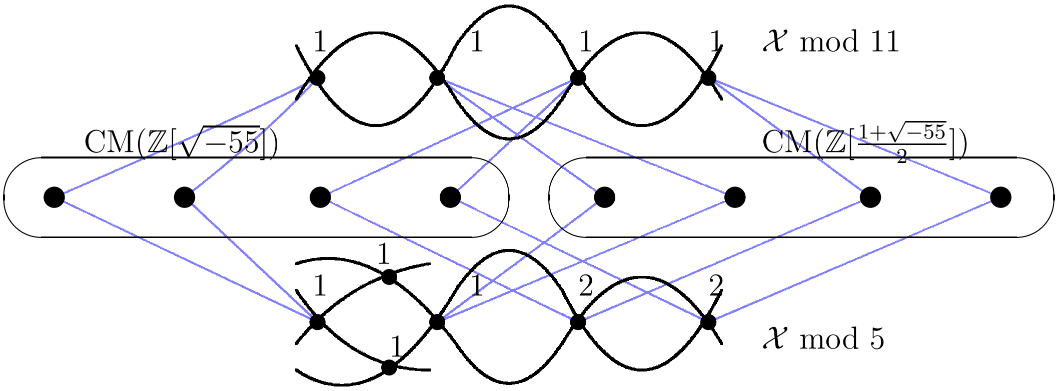
Special fiber of $\mathcal{X}$ at p=5 Special fiber of $\mathcal{X}$ at p=11

In order to transform $\mathcal{X}$ into a Weierstrass model $\mathcal{W}$ we shall need to blow down the exceptional divisors and apply relation (4.15) to obtain new thicknesses.



Special fiber of $\mathcal{W}$ at p=5 Special fiber of $\mathcal{W}$ at p=11

Applying our algorithm, we obtain that the specialization of the Heegner points $\mathrm{CM}(\mathbb{Z}[\sqrt{-55}])$ and $\mathrm{CM}(\mathbb{Z}[\frac{1+\sqrt{-55}}{2}])$ in $\mathcal{X}$ is given by the following diagram:


1
1
1
1
$\mathcal{X}$ mod 11
$\mathrm{CM}(\mathbb{Z}[\sqrt{-55}])$
$\mathrm{CM}(\mathbb{Z}[\frac{1+\sqrt{-55}}{2}])$
1
1
1
1
2
2
1
$\mathcal{X}$ mod 5

Hence, blowing-down $\mathcal{X}$ as above, we obtain the thickness of the specialization of each Weierstrass point $P \in \mathrm{WP}(\mathcal{W})$. Applying the rest of the algorithm just as in §8, we obtain that the model $\mathcal{W}$ over $\mathbb{Z}[1/2]$ is given by the equation:

$$\boxed{y^2 = (-3x^4 + 32x^3 - 130x^2 + 237x - 163) \cdot (x^4 - 8x^3 + 34x^2 - 83x + 81).}$$

This curve also coincides with the one conjectured by Kurihara (cf. [17]) in this case.

10. Atkin-Lehner quotients

In §7 we gave an algorithm which in principle works for any hyperelliptic Shimura curve of odd discriminant admitting a Weierstrass model $\mathcal{W}$ obtained by blowing-down exceptional divisors of $\mathcal{X}$. However, this algorithm exploits the instruction *IndexFormEquation*, which is implemented in *MAGMA* only for small degree field extensions. As long as the genus increases, the degrees of the fields involved in the computation become so large that make impossible to proceed with the algorithm.

In this section we shall explain how to adapt the algorithm of §7 to compute equations of hyperelliptic quotients of Shimura curves by Atkin-Lehner involutions. We expect that the degrees of the fields involved in this case will be smaller and, consequently, we shall be able to compute more examples.

10.1. **Quotient of the special fiber.** As above, denote by $\mathcal{X}/\mathbb{Z}$ Morita's integral model of $X = X_0^D$. Write $Y = X/\langle\omega_m\rangle$ and $\mathcal{Y} = \mathcal{X}/\langle\omega_m\rangle$. Due to Cerednik-Drinfeld's uniformization, we have an explicit description of the fiber $\mathcal{X}_p$ at $p \mid D$ and the action of the Atkin-Lehner involutions on its set of irreducible components and singular points. This allows us to compute the irreducible components of the fiber $\mathcal{Y}_p$. In order to obtain the thicknesses of its singular points $(\mathcal{Y}_p)_{\rm sing}$, recall that the completed local ring of any singular point x of $\mathcal{X}_p$ is of the form:

$$\widehat{O_{\mathcal{X}',x'}} \simeq \widehat{O_{S',\mathfrak{p}}}[[u,v]]/(uv-c) \quad c \in \mathfrak{m}_{\mathfrak{p}}.$$

Here, u and v vanish respectively on each of the irreducible components that meet in x.

Let $\pi : \mathcal{X} \rightarrow \mathcal{Y}$ be the quotient map. If ω_m fixes x there are two possibilities: ω_m fixes u and v or ω_m exchanges them. If ω_m fixes u and v, the completed local ring of the image $\pi(x)$ is given by

$$\widehat{O_{\mathcal{Y}',\pi(x')}} \simeq \widehat{O_{S',\mathfrak{p}}}[[x,y]]/(xy-c^2),$$

where the induced pull-back $\pi^* : \widehat{O_{\mathcal{Y}',\pi(x')}} \rightarrow \widehat{O_{\mathcal{X}',x'}}$ is given by $x \mapsto u^2,\ y \mapsto v^2$. Thus the thickness of the singular point $\pi(x)$ is twice the thickness of x. If $\omega_m u = v$, the completed local ring of the image $\pi(x)$ is given by

$$\widehat{O_{\mathcal{Y}',\pi(x')}} \simeq \widehat{O_{S',\mathfrak{p}}}[[z]]/(z-c),$$

where the induced pull-back $\pi^* : \widehat{O_{\mathcal{Y}',\pi(x')}} \rightarrow \widehat{O_{\mathcal{X}',x'}}$ is given by $z \mapsto uv$. Thus $\pi(x)$ becomes a non-singular point of $\mathcal{Y}_p$. Finally, if $\omega_m(x) = x' \neq x$ the map π is not ramified at x. Hence it provides an isomorphism of local rings $O_{\mathcal{X},x} \simeq O_{\mathcal{Y},\pi(x)}$. This implies that the thickness of $\pi(x)$ coincides with that of x. Notice that, since we control the singular specialization of Heegner points in $\mathcal{X}_p$, we also control that of their image in $\mathcal{Y}_p$.

10.2. **Weierstrass points, leading coefficients and fields of definition.** We shall assume that there exists a quadratic order $R_\infty \subset K_\infty$ of discriminant prime-to-D and class number $h_{R_\infty} = 1$ such that $\emptyset \neq \mathrm{CM}(R_\infty) \subset X(K_\infty)$. Assume also that Y is hyperelliptic and that the hyperelliptic involution ω of Y is the image of ω_n for some $n \mid D$. Notice that all hyperelliptic Shimura curves in Table 1 verify these assumptions. Clearly $n \neq m$ since ω_m is trivial in Y. Finally, assume that blowing-down suitably exceptional divisors of $\mathcal{Y}$ we can obtain a Weierstrass model $\mathcal{W}_Y$ of Y.

As above, the set of Weierstrass points $\mathrm{WP}(Y)$ coincides with the set of fixed points of ω. Let $\pi(P) \in \mathrm{WP}(Y)$. Then $\pi(P) = \omega(\pi(P)) = \pi(\omega_n(P))$, thus $\omega_n(P) = P$ or $\omega_n(P) = \omega_m(P)$. It follows that the set $\mathrm{WP}(Y)$ is the image of the union of the set of fixed points of ω_n and of $\omega_m \circ \omega_n = \omega_{n\cdot m/\gcd(m,n)^2}$. By Theorem 3.1, this set coincides with a set of Heegner points $\bigsqcup_i \mathrm{CM}(R_i)$, where $R_i^0 = \mathbb{Q}(\sqrt{-n})$ or $\mathbb{Q}(\sqrt{-n\cdot m})$.

Recall that if $P \in \mathrm{CM}(R_i)$ is fixed by ω_D, then $\mathbb{Q}(P)$ can be computed by means of Theorem 7.1. Besides, if P is fixed by ω_n, $n \neq D$, then the field of definition of P is just H_{R_i} by [9, Theorem 5.12]. The following proposition describes the field of definition of each $\pi(P) \in \mathrm{WP}(Y)$:

Proposition 10.1. *Let $n \neq m$ be divisors of D. Let $P \in \mathrm{CM}(R)$ be a Heegner point fixed by ω_n. Write $Y = X/\langle\omega_m\rangle$ and set $\pi : X \to Y$ for the quotient map. Fix an embedding $H_R \subset \mathbb{C}$ and let c denote complex conjugation.*

1. *If $m \mid n$ then $\mathbb{Q}(\pi(P))$ is the subfield of $\mathbb{Q}(P)$ fixed by $\Phi_R(\mathfrak{m})$, where $\mathfrak{m}$ is the unique ideal of R of norm m.*
2. *If $\omega_m(P) = \omega_D(P)$ (i.e. either $m = D$ or $n = D/m$) then $\mathbb{Q}(\pi(P))$ is the subfield of $\mathbb{Q}(P)$ fixed by $c \cdot \Phi_{R_i}([\mathfrak{a}]$, where $\mathfrak{a}$ is an ideal of R (depending on P) satisfying*

$$B \simeq \left(\frac{-n, \frac{D}{n}\cdot \mathrm{N}_{R^0/\mathbb{Q}}(\mathfrak{a})}{\mathbb{Q}}\right). \tag{10.31}$$

3. *If $\omega_m(P) \neq \omega_D(P)$ and $m \nmid n$ then $\mathbb{Q}(\pi(P)) = \mathbb{Q}(P)$.*

Proof. This follows immediately from the fact that if $m \mid n$ then $\omega_m(P) = P^{\Phi_R(\mathfrak{m})}$ (cf. [9, Lemma 5.9]), if $\omega_m(P) = \omega_D(P)$ then $\omega_m(P) = P^{c\cdot\Phi_{R_i}([\mathfrak{a}])}$ (cf. [9, Lemma 5.10]), and if neither $m \mid n$ nor $\omega_m(P) = \omega_D(P)$ then ω_m acts transitively on the $\mathrm{Gal}(H_R/\mathbb{Q})$-orbit of P. □

Just as in Remark 7.2, the ideal $\mathfrak{a}$ depends on P but its class $\{\mathfrak{a}\} \in \mathrm{Pic}(R_i)/\mathrm{Pic}(R_i)^2$ only depends on R and determines the isomorphism class of $\mathbb{Q}(\pi(P))$ for every $P \in \mathrm{CM}(R)$. Furthermore, in our particular setting where $[H : H_R]$ is odd, the class $\{\mathfrak{a}\}$ is uniquely determined by (10.31).

As in the previous case, the model $\mathcal{Y}$ can be non-hyperelliptic (i.e. $\mathcal{Y}/\langle\omega\rangle$ may not be smooth over $\mathbb{Z}$). According to our previous assumptions, we can turn it into an hyperelliptic model $\mathcal{W}_Y/\mathbb{Z}$ by blowing-down suitably irreducible components.

By means of formula (4.15), we can recover the thicknesses of the singular points of the fiber $(\mathcal{W}_Y)_p$. Since we control the specialization of the Weierstrass points $\mathrm{WP}(Y)$ in $\mathcal{Y}_p$, we also control the specialization of the Weierstrass points in $\mathrm{WP}(\mathcal{W}_Y)$.

Notice that there may exist Weierstrass points $\pi(P) \in \mathrm{WP}(Y)$ specializing to non-singular points on $\mathcal{Y}_p$, but having singular specialization on $(\mathcal{W}_Y)_p$. This happens because their specialization on $\mathcal{Y}_p$ lie on irreducible components which were blown-down in order to obtain $\mathcal{W}_Y$. By means of (4.13), we control the irreducible component where the specialization P lies. Hence we control the singular specialization of $\pi(P)$ in the fiber $(\mathcal{W}_Y)_p$.

Choose $P_\infty \in \mathrm{CM}(R_\infty)$. Since $h_{R_\infty} = 1$, the set $\mathrm{CM}(R_\infty)$ is a $W(D)$-orbit. Moreover, $\pi(\omega_n(P_\infty)) = \omega(\pi(P_\infty)) \neq \pi(P_\infty)$ since $\omega_n(P_\infty) \neq \omega_m(P_\infty)$, and $\pi(P_\infty)$ is defined over a subfield of K_∞. This implies that we can set $\pi(P_\infty)$ and $\omega(\pi(P_\infty))$ to be our points at infinity.

Once we fix the points at infinity, the model $\mathcal{W}_Y$ is defined, over $\mathbb{Z}[1/2]$, by an equation of the form

$$y^2 = R(x) = \prod_i p_{R_i}(x),$$

where each of the polynomials $p_{R_i}(x)$ is attached to $\pi(\mathrm{CM}(R_i))$, and we control the field that each one defines.

We deduced in §3 that the valuation of the leading coefficient a_R at any prime p can be obtained from the intersection index between $\pi(P_\infty)$ and $\omega(\pi(P_\infty))$ at p. By the projection formula,

(10.32)

$$(\pi(P_\infty), \pi(\omega_n(P_\infty)))_p = (P_\infty, \pi^*\pi(\omega_n(P_\infty)))_p = (P_\infty, \omega_n(P_\infty))_p + (P_\infty, \omega_{n'}(P_\infty))_p,$$

where $n' = \frac{n \cdot m}{\gcd(m,n)^2}$. Hence, the valuation of the leading coefficient at any prime,

$$\nu_p(a_R) = \left(1 - \left(\frac{K_\infty}{p}\right)\right)(\pi(P_\infty), \pi(\omega_n(P_\infty)))_p,$$

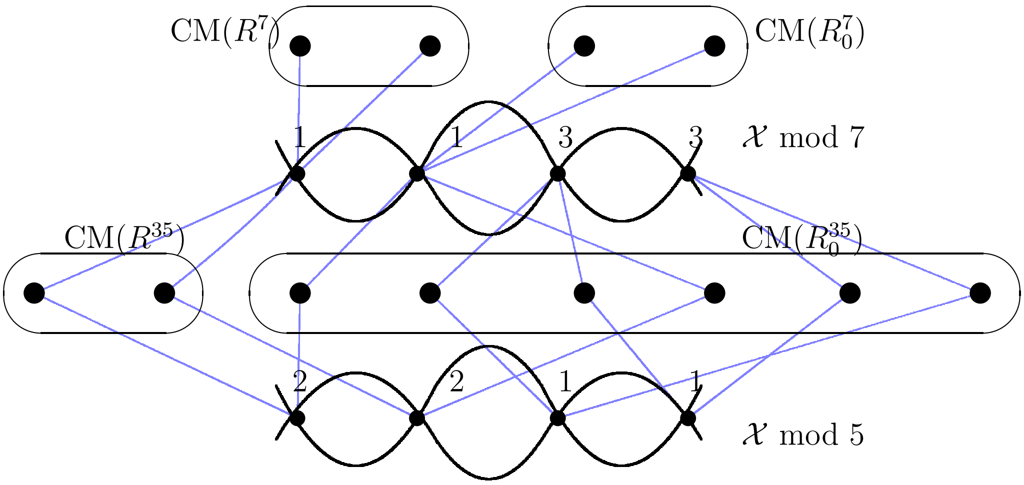
can be computed by means of (6.25). Since the leading coefficient a_{R_i} of each $p_{R_i}(x)$ also detects whether P_∞ specializes to the same supersingular point as an element of $\mathrm{CM}(R_i)$, we can compute each a_{R_i} just as in §7.

At this point, assuming that D is odd, we can proceed with the algorithm of §7 in order to obtain an equation for $\mathcal{W}_Y$. Indeed, we control the leading coefficient of each $p_{R_i}(x)$, their splitting field and the singular specialization of any $\pi(P) \in \mathrm{WP}(\mathcal{W}_Y)$.

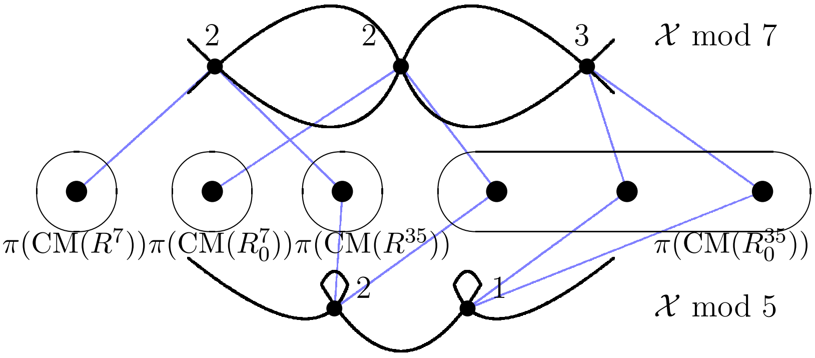
10.3. **Example.** Let $X = X_0^{35}/\mathbb{Q}$ be the Shimura curve of discriminant 35. In this section we shall compute the quotient curve $Y = X/\langle\omega_5\rangle$. Since X is itself hyperelliptic we deduce that Y is hyperelliptic. Moreover, we check that it satisfies the assumptions of the previous section.

Write $\pi : \mathcal{X} \rightarrow \mathcal{Y}$ for the quotient map as above. The set of Weierstrass points of Y is the image through π of the set of Heegner points $\mathfrak{S} = \mathrm{CM}(R^{35}) \sqcup \mathrm{CM}(R_0^{35}) \sqcup$

$\mathrm{CM}(R^7) \sqcup \mathrm{CM}(R_0^7)$, where $R^{35} = \mathbb{Z}[\frac{1+\sqrt{-35}}{2}]$, $R_0^{35} = \mathbb{Z}[\sqrt{-35}]$, $R^7 = \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ and $R_0^7 = \mathbb{Z}[\sqrt{-7}]$. We obtain that R^{35} has Picard number 2, R_0^{35} has Picard number 6, and both R^7 and R_0^7 have Picard number 1. Here, we present a diagram that describes the special fibers of $\mathcal{X}$ at $p = 5, 7$ and the specialization of $\mathfrak{S}$ computed using the techniques of §7.



By Cerednik-Drinfeld's description of the fiber $\mathcal{X}_5$, we know that ω_5 exchanges its irreducible components, moreover, it exchanges its singular points of thickness 1 and its singular points of thickness 2. Similarly, ω_5 fixes the irreducible components of $\mathcal{X}_7$, exchanges its singular points of thickness 3 and fixes its singular points of thickness 1. Applying the recipe detailed in §10.1, we obtained that the specialization of $\pi(\mathfrak{S})$ and the special fibers $\mathcal{Y}_5$ and $\mathcal{Y}_7$ are given by the following diagram:


2
2
3
$\mathcal{X}$ mod 7
$\pi(\mathrm{CM}(R^7))$
$\pi(\mathrm{CM}(R_0^7))$
$\pi(\mathrm{CM}(R^{35}))$
$\pi(\mathrm{CM}(R_0^{35}))$
2
1
$\mathcal{X}$ mod 5

Let R_∞ be the maximal order of $K_\infty = \mathbb{Q}(\sqrt{-43})$. Since $h_{R_\infty} = 1$ and $\mathrm{CM}(R_\infty) \neq \emptyset$, we choose $\{\pi(P_\infty), \pi(\omega_D(P_\infty))\} \subseteq \pi(\mathrm{CM}(R_\infty))$ to be our points at infinity. Then, by (10.32),

$$\nu_p(a_R) = \left(1 - \left(\frac{K_\infty}{p}\right)\right)((P_\infty, \omega_D(P_\infty))_p + (P_\infty, \omega_{D/m}(P_\infty))_p)$$

In order to compute $(P_\infty, \omega_D(P_\infty))_p$, we apply (6.26) and it follows that

$$43 \cdot 35 = n + \mathrm{N}(\lambda^-) \cdot 35 \cdot p, \qquad n = 43 \cdot \mathrm{N}(\lambda_+) \in \mathbb{Z}.$$

Since $35 \mid n$ and 7,5 are inert in K_∞, we deduce that $35^2 \cdot n' = n$. Thus,

$$43 = 35 \cdot n' + \mathrm{N}(\lambda^-) \cdot p, \qquad n' \in \mathbb{Z}.$$

Hence the solutions are $n' = 0$, $p = 43$, $\mathrm{N}(\lambda^-) = 1$ and $n' = 1$, $p = 2$, $\mathrm{N}(\lambda^-) = 4$. Applying formula (6.25), we deduce that $(P_\infty, \omega_D(P_\infty))_{43} = 1$ and $(P_\infty, \omega_D(P_\infty))_2 = 2$.

Similarly for $(P_\infty, \omega_{D/m}(P_\infty))_p$, we apply formula (6.26) obtaining:

$$43 \cdot 7 = n + \mathrm{N}(\lambda^-) \cdot 35 \cdot p, \qquad n = 43 \cdot \mathrm{N}(\lambda_+) \in \mathbb{Z}.$$

As above, $7 \mid n$ and it is inert in K_∞, hence $7^2 \cdot n' = n$ and it follows that

$$43 = 7 \cdot m' + 5 \cdot \mathrm{N}(\lambda^-) \cdot p, \qquad m' \in \mathbb{Z}.$$

This implies $m' \equiv 4 \pmod 5$ and, thus, $m' = 4$, $p = 3$, $\mathrm{N}(\lambda^-) = 1$. By means of (6.25) we have that $(P_\infty, \omega_D(P_\infty))_3 = 1$.

Therefore the unique primes that divide a_R are 43, 3 and 2 and their valuations are $\nu_{43}(a_R) = 1$, $\nu_3(a_R) = 2$ and $\nu_2(a_R) = 4$. Moreover, we can compute the specialization of P_∞ and $\omega(P_\infty)$ at $p = 3, 43$ and determine which Weierstrass point lie at the same supersingular point as them. We obtained that $\nu_{43}(a_{R_0^{35}}) = 1$ and $\nu_3(a_{R_0^7}) = 2$. We can not control the 2-valuation of any leading coefficient a_{R_i} but we know the valuation of the product $4 = \nu_2(a_R) = \sum_i \nu_2(a_{R_i})$ and this gives an upper bound for all of them.

Finally, applying the rest of the algorithm of §7, we obtained that Y is defined by the equation:

$$\boxed{y^2 = -x \cdot (9x + 4) \cdot (4x + 1) \cdot (172x^3 + 176x^2 + 60x + 7).}$$

10.4. **Results.** In this section we present a table with all the equations obtained using the algorithms explained in §7 and §10:

g	*curve*	$y^2 = p(x)$
3	X_0^{39}	$y^2 = -(7x^4+79x^3+311x^2+497x+277)\cdot(x^4+9x^3+29x^2+39x+19)$
3	X_0^{55}	$y^2 = -(3x^4-32x^3+130x^2-237x+163)\cdot(x^4-8x^3+34x^2-83x+81)$
2	$X_0^{35}/\langle\omega_5\rangle$	$y^2 = -x\cdot(9x+4)\cdot(4x+1)\cdot(172x^3+176x^2+60x+7)$
2	$X_0^{51}/\langle\omega_{17}\rangle$	$y^2 = -x\cdot(7x^3+52x^2+116x+68)\cdot(x-1)\cdot(x+3)$
2	$X_0^{57}/\langle\omega_3\rangle$	$y^2 = -(x-9)\cdot(x^3-19x^2+119x-249)\cdot(7x^2-104x+388)$
2	$X_0^{65}/\langle\omega_{13}\rangle$	$y^2 = -(x^2-3x+1)\cdot(7x^4-3x^3-32x^2+25x-5)$
2	$X_0^{65}/\langle\omega_5\rangle$	$y^2 = -(x^2+7x+9)\cdot(7x^4+81x^3+319x^2+508x+268)$
2	$X_0^{69}/\langle\omega_{23}\rangle$	$y^2 = -x\cdot(x+4)\cdot(4x^4-16x^3+11x^2+10x+3)$
2	$X_0^{85}/\langle\omega_5\rangle$	$y^2 = -(3x^2-41x+133)\cdot(x^4-23x^3+183x^2-556x+412)$
2	$X_0^{85}/\langle\omega_{85}\rangle$	$y^2 = (x^2-3x+1)\cdot(x^4+x^3-15x^2+20x-8)$

Table 2

References

[1] Pilar Bayer. Uniformization of certain Shimura curves. In *Differential Galois theory (Będlewo, 2001)*, volume 58 of *Banach Center Publ.*, pages 13–26. Polish Acad. Sci., Warsaw, 2002.

[2] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] J.-F. Boutot and H. Carayol. Uniformisation p-adique des courbes de Shimura: les théorèmes de Čerednik et de Drinfeld. *Astérisque*, (196-197):7, 45–158 (1992), 1991. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

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

[5] V. G. Drinfeld. Coverings of p-adic symmetric domains. *Funkcional. Anal. i Priložen.*, 10(2):29–40, 1976.

[6] B. Edixhoven. Appendix of: A rigid analytic Gross-Zagier formula and arithmetic applications. *Ann. of Math. (2)*, 146(1):111–147, 1997. Article by Maximo Bertolini and Henri Darmon.

[7] N. D. Elkies. Shimura curve computations. In *Algorithmic number theory (Portland, OR, 1998)*, volume 1423 of *Lecture Notes in Comput. Sci.*, pages 1–47. Springer, Berlin, 1998.

[8] J. González and V. Rotger. Equations of Shimura curves of genus two. *Int. Math. Res. Not.*, (14):661–674, 2004.

[9] J. González and V. Rotger. Non-elliptic Shimura curves of genus one. *J. Math. Soc. Japan*, 58(4):927–948, 2006.

[10] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[11] X. Guitart and S. Molina. Parametrization of abelian k-surfaces with quaternionic multiplication. *Comptes rendus - Mathematique*, (347):1325–1330, 2009.

[12] Y. Ihara. Congruence relations and Shimūra curves. In *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977),*

Part 2, Proc. Sympos. Pure Math., XXXIII, pages 291–311. Amer. Math. Soc., Providence, R.I., 1979.

[13] B. W. Jordan. On the diophantine arithmetic of Shimura curves. *Harvard University, Illinois*, 1981. Ph.D. thesis.

[14] B. W. Jordan and R. A. Livné. Local Diophantine properties of Shimura curves. *Math. Ann.*, 270(2):235–248, 1985.

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

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

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

[18] Q. Liu. Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète. *Trans. Amer. Math. Soc.*, 348(11):4577–4610, 1996.

[19] Q. Liu. *Algebraic geometry and arithmetic curves*, volume 6 of *Oxford Graduate Texts in Mathematics*. Oxford University Press, Oxford, 2002. Translated from the French by Reinie Erné, Oxford Science Publications.

[20] K. Lønsted and S. L. Kleiman. Basics on families of hyperelliptic curves. *Compositio Math.*, 38(1):83–111, 1979.

[21] S. Molina. Ribet bimodules and specialization of Heegner points. *submited*.

[22] Y. Morita. Reduction modulo $\mathfrak{P}$ of Shimura curves. *Hokkaido Math. J.*, 10(2):209–238, 1981.

[23] A. P. Ogg. Real points on Shimura curves. In *Arithmetic and geometry, Vol. I*, volume 35 of *Progr. Math.*, pages 277–307. Birkhäuser Boston, Boston, MA, 1983.

[24] P. Ribenboim. Equivalent forms of Hensel's lemma. *Exposition. Math.*, 3(1):3–24, 1985.

[25] K. A. Ribet. Endomorphism algebras of abelian varieties attached to newforms of weight 2. In *Seminar on Number Theory, Paris 1979–80*, volume 12 of *Progr. Math.*, pages 263–276. Birkhäuser Boston, Mass., 1981.

[26] K. A. Ribet. Bimodules and abelian surfaces. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 359–407. Academic Press, Boston, MA, 1989.

[27] M. Sadykov. Two results in the arithmetic of Shimura curves. *Columbia University, New York*, 2004. Ph.D. thesis.

[28] G. Shimura. Construction of class fields and zeta functions of algebraic curves. *Ann. of Math. (2)*, 85:58–159, 1967.

[29] G. Shimura. On the real points of an arithmetic quotient of a bounded symmetric domain. *Math. Ann.*, 215:135–164, 1975.

[30] T. Shioda. Supersingular $K3$ surfaces. In *Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, volume 732 of *Lecture Notes in Math.*, pages 564–591. Springer, Berlin, 1979.

[31] S. Siksek and A. Skorobogatov. On a Shimura curve that is a counterexample to the Hasse principle. *Bull. London Math. Soc.*, 35(3):409–414, 2003.

[32] M.-F. Vignéras. *Arithmétique des algèbres de quaternions*, volume 800 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980.

[33] J. Voight. Shimura curves of genus at most two. *Math. Comp.*, 78(266):1155–1172, 2009.

Santiago Molina
CRM