©2016 The Mathematical Society of Japan
J. Math. Soc. Japan
Vol. 68, No. 2 (2016) pp. 609–635
doi: 10.2969/jmsj/06820609

The kernel of Ribet's isogeny for genus three Shimura curves

By Josep González and Santiago Molina

(Received Nov. 20, 2013)
(Revised June 4, 2014)

Abstract. There are exactly nine reduced discriminants D of indefinite quaternion algebras over $\mathbb{Q}$ for which the Shimura curve X_D attached to D has genus 3. We present equations for these nine curves and, moreover, for each D we determine a subgroup $c(D)$ of cuspidal divisors of degree zero of $\mathrm{Jac}(X_0(D))^{\mathrm{new}}$ such that the abelian variety $\mathrm{Jac}(X_0(D))^{\mathrm{new}}/c(D)$ is the jacobian of the curve X_D.

1. Introduction.

Let D be the reduced discriminant of an indefinite quaternion algebra over $\mathbb{Q}$. Let us denote by $X_D/\mathbb{Q}$ the Shimura curve attached to D. In [**16**], K. Ribet established the existence of an isogeny defined over $\mathbb{Q}$ between $\mathrm{Jac}(X_0(D))^{\mathrm{new}}$ and $\mathrm{Jac}(X_D)$ by proving that both abelian varieties have the same L-series, but it is not known an explicit description of such an isogeny. A. P. Ogg studied the problem of determining the kernel of an isogeny of minimal degree and conjectured that it may be a subgroup of the group of cuspidal divisors of degree zero of the curve $X_0(D)$. Moreover, for some particular cases that D is the product of two primes, he predicted which subgroup should be this kernel (cf. [**15**]).

When the genus g of X_D is 1, there are exactly five discriminants $D = 14, 15, 21, 33$ and 34. In all these cases, two elliptic curves defined over $\mathbb{Q}$ of conductor D are isomorphic over $\mathbb{Q}$ if and only if both have the same type of reduction at every prime dividing D . Therefore, the elliptic curve $\mathrm{Jac}(X_D)$ can be determined among the isomorphism classes of elliptic curves over $\mathbb{Q}$ of conductor D in Cremona's tables by using the theory of Čerednik–Drinfeld. For the subgroup $c(D)$ of cuspidal divisors of degree zero displayed in the next table

D	14	15	21	33	34
$c(D)$	$\langle 3(0) - 3(\infty)\rangle$	$\{0\}$	$\langle 2(0) - 2(\infty)\rangle$	$\{0\}$	$\langle (0) - (\infty)\rangle$
$\lvert c(D)\rvert$	2	1	2	1	3

one has that $\mathrm{Jac}(X_0(D))^{\mathrm{new}}/c(D) \simeq \mathrm{Jac}(X_D)$. This result can be obtained by checking that $\mathrm{Jac}(X_0(D))^{\mathrm{new}}/c(D)$ and $\mathrm{Jac}(X_D)$ have the same type of reduction at every prime dividing D or checking that the lattice of $\mathrm{Jac}(X_0(D))^{\mathrm{new}}/c(D)$ corresponds to the elliptic

2010 *Mathematics Subject Classification.* Primary 11G18, 14G35.
Key Words and Phrases. Shimura curves, genus three hyperelliptic curves.
All authors are supported in part by DGICYT Grant MTM2012-34611. The second author is also supported by the German Research Council (DFG), via CRC 701.

curve $\mathrm{Jac}(X_D)$.

For $g = 2$, there are exactly three curves X_D and a kernel $c(D)$ for these three cases is presented in Theorem 3.1 of [**5**]:

D	26	38	58
$c(D)$	$\langle 3(0) - 3(\infty)\rangle$	$\langle 3(0) - 3(\infty)\rangle$	$\langle (0) - (\infty)\rangle$
$\lvert c(D)\rvert$	7	5	5

In this case, once an equation for X_D is determined, the proof is based on the fact that X_D is bielliptic and the lattices of $\mathrm{Jac}(X_0(D))^{\mathrm{new}}$ and $\mathrm{Jac}(X_D)$ can be handled through their elliptic quotients.

The aim of this paper is double. The first goal is determining equations for all curves X_D of genus three; although these nine curves have a hyperelliptic involution defined over $\mathbb{Q}$, uniquely seven of them are hyperelliptic over $\mathbb{Q}$. The second goal is checking the existence of a subgroup of $\mathrm{Jac}(X_0(D))^{\mathrm{new}}(\mathbb{Q})$ formed by cuspidal divisors of $X_0(D)$ to be the kernel of an isogeny between $\mathrm{Jac}(X_0(D))^{\mathrm{new}}$ and $\mathrm{Jac}(X_D)$ for each of these values of D.

In [**12**], it is given a method to compute equations for Atkin–Lehner quotients of Shimura curves attached to an odd discriminant D which are hyperelliptic over $\mathbb{Q}$ and some equations are computed. This method has a computational limitation since it exploits the MAGMA instruction *IndexFormEquation* that only applies for general number fields of degree at most four. For this reason, we show in Section 3 how to obtain equations for all Shimura curves of genus three from certain particular equations of their Atkin–Lehner quotients, where the number fields involved are of degree smaller or equal than four. In the beginning of Section 4 we determine equations of the Atkin–Lehner quotients when D is even, which is more laborious than the odd case; next, in Theorem 4.5 we present a list of all genus three equations, together with the projections onto their Atkin–Lehner quotients presented in Proposition 4.4. Finally, for each of the the nine curves of genus 3, we present in Theorem 5.1 of Section 5 a subgroup of cuspidal divisors of degree zero of $X_0(D)$ which provides in $\mathrm{Jac}(X_0(D))^{\mathrm{new}}(\mathbb{Q})$ the kernel of a Ribet's isogeny.

2. Genus three Shimura curves and their Atkin–Lehner quotients.

We recall that a curve X defined over a field K of genus $g > 1$ is said to be hyperlliptic over K if there exists an involution w defined over K such that the quotient curve X/w has genus zero and K-rational points. If the characteristic of K is greater than 2, then this definition amounts to saying that X admits an affine equation of the form $y^2 = P(x)$ for some polynomial $P(x) \in K[x]$.

Let $X_D/\mathbb{Q}$ be the Shimura curve and, for a divisor $m|D$, let us denote by ω_m the corresponding Atkin–Lehner involution of X_D.

Proposition 2.1. *The curve X_D has genus 3 exactly for the following values of D:*

$$2\cdot 31, 2\cdot 41, 2\cdot 47, 3\cdot 13, 3\cdot 17, 3\cdot 19, 3\cdot 23, 5\cdot 7, 5\cdot 11.$$

In all these cases, X_D is hyperelliptic over $\overline{\mathbb{Q}}$ and the hyperelliptic involution w is the Atkin–Lehner involution ω_D except for the values $D = 57$ and 82, for which w is ω_{19} and ω_{41} respectively. Moreover, X_D is hyperelliptic over $\mathbb{Q}$ if and only if $w = \omega_D$.

Proof. Let g be the genus of X_D. From the genus formula for X_D, we can deduce that, if the number of primes dividing D is greater than 2, then $g > 3$. Moreover, if $g = 3$ and D is the product of two primes, we obtain that $\varphi(D) \leq 52$, where φ is the Euler function. Checking the genus for these possible values of D, we obtain the first part of the statement. The other claims can be found in Theorem 7 of [**14**]. □

From now on, D is one of these nine values of the above proposition. By [**8**], we know that the group of the automorphisms of the Shimura curve X_D is the group of the Atkin–Lehner involutions $\{\omega_m : m|D\}$ and, thus, we have that $\mathrm{Aut}(X_D) = \mathrm{Aut}_{\mathbb{Q}}(X_D) \simeq (\mathbb{Z}/2\mathbb{Z})^2$. We denote by w the hyperelliptic involution of X_D and by u the unique Atkin–Lehner involution such that the quotient curve $X^{(u)} := X_D/\langle u\rangle$ has genus one. It follows that $\mathrm{Aut}(X_D) = \{1, u, w, v\}$, where $v = u \cdot w$, and the quotient curves $X^{(w)} := X_D/\langle w\rangle$ and $X^{(v)} := X_D/\langle v\rangle$ have genus 0 and 2 respectively. The Atkin-lehner involutions $\omega_m = u$, $\omega_m = v$ and $\omega_m = w$ are displayed in the following table:

D	$2\cdot 31$	$2\cdot 41$	$2\cdot 47$	$3\cdot 13$	$3\cdot 17$	$3\cdot 19$	$3\cdot 23$	$5\cdot 7$	$5\cdot 11$
u	ω_2	ω_{82}	ω_2	ω_{13}	ω_3	ω_{57}	ω_3	ω_7	ω_5
v	ω_{31}	ω_2	ω_{47}	ω_3	ω_{17}	ω_3	ω_{23}	ω_5	ω_{11}
w	ω_{62}	ω_{41}	ω_{94}	ω_{39}	ω_{51}	ω_{19}	ω_{69}	ω_{35}	ω_{55}

Given a nontrivial involution $\iota \in \mathrm{Aut}(X_D)$, let us denote by $\pi_\iota : X_D \to X^{(\iota)}$ the natural projection and $\mathcal{F}_\iota$ denotes the set of fixed points under ι. Hence, $\mathcal{F}_v = \emptyset$, $|\mathcal{F}_u| = 4$ and $|\mathcal{F}_w| = 8$. For $\iota \neq v$, the number field generated by the coordinates of the projection $\pi_\iota(P)$ of a point $P \in \mathcal{F}_\iota$ can be found in [**6**]. For instance, if $U \in \mathcal{F}_u$ we have

Table 1.

D	$\mathbb{Q}(U)$	$\mathbb{Q}(\pi_v(U)) = \mathbb{Q}(\pi_w(U))$
$2\cdot 31$	$\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}$
$2\cdot 41$	$\mathbb{Q}(\sqrt{-3 \pm 4\sqrt{-2}}\,)$	$\mathbb{Q}(\sqrt{-2})$
$2\cdot 47$	$\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}$
$3\cdot 13$	$\mathbb{Q}(\sqrt{-13}, \sqrt{13}\,)$	$\mathbb{Q}(\sqrt{-1})$
$3\cdot 17$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}$
$3\cdot 19$	$\mathbb{Q}(\sqrt{3}, \sqrt{-3}\,)$	$\mathbb{Q}(\sqrt{-3})$
$3\cdot 23$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}$
$5\cdot 7$	$\mathbb{Q}(\sqrt{-7})$	$\mathbb{Q}$
$5\cdot 11$	$\mathbb{Q}(\sqrt{-5}, \sqrt{5})$	$\mathbb{Q}(\sqrt{-1})$

where for $D = 62, 94$, i.e. $u = \omega_2$, there are two fixed points whose coordinates generate $\mathbb{Q}(\sqrt{-1})$, while the coordinates of the other two fixed points generate $\mathbb{Q}(\sqrt{-2})$.

The involution w induces involutions on the curves $X^{(v)}$ and $X^{(u)}$ that will be also denoted by w. For the genus two curve $X^{(v)}$, w is the hyperelliptic involution and, thus, the curve $X^{(v)}$ admits a hyperelliptic model over $\mathbb{Q}$.

For the curve $X^{(u)}$, since w is defined over $\mathbb{Q}$, it has an equation of the form $y^2 = F(x)$ with $F(x) \in \mathbb{Q}[x]$ of degree 3 or 4 and for which the involution w acts sending (x, y) to $(x, -y)$. Any equation for $X^{(u)}$ of the form $y^2 = G(x)$ with $G(x) \in \mathbb{Q}[x]$ of degree 3 or 4 for which the action of w is given by $(x, y) \mapsto (x, -y)$ is equivalent over $\mathbb{Q}$ to $y^2 = F(x)$, namely, there exist

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in GL(2, \mathbb{Q}) \quad \text{and} \quad \lambda \in \mathbb{Q}^*$$

such that

$$G(x) = \lambda^2 F\left(\frac{\alpha\, x + \beta}{\gamma\, x + \delta}\right)(\gamma\, x + \delta)^4.$$

3. Equations for X_D from its Atkin–Lehner quotients.

In [**12**], the second author gives a method to compute equations for Atkin–Lehner quotients of Shimura curves attached to an odd discriminant D which are hyperelliptic over $\mathbb{Q}$. For the particular case that X_D has genus 3, he provides in Table 2 of [**12**] equations for X_D when $D = 39, 55$ and for $X^{(v)}$ when $D = 35, 51, 57, 69$. In this section we show how one can obtain an equation for X_D, even if X_D is not hyperelliptic over $\mathbb{Q}$, from certain particular equations for $X^{(u)}$ and $X^{(v)}$.

We recall that, if a curve Y defined over a field K of genus g is hyperelliptic over $\overline{K}$, then for a point $P \in Y(\overline{K})$ there exists a basis $\{\lambda_i\}_{1 \le i \le g}$ of $H^0(Y, \Omega^1)$ such that for all i:

$$\operatorname{ord}_P \lambda_i = \begin{cases} 2\,i - 2 & \text{if } P \text{ is a Weierstrass point,} \\ i - 1 & \text{otherwise.} \end{cases}$$

For such a basis, the functions $x = \lambda_{g-1}/\lambda_g$, $y = dx/\lambda_g$ generate the function field of Y and provide a hyperelliptic model for Y, that is $y^2 = F(x)$ for some polynomial $F(x) \in \overline{K}[x]$ without double roots, of degree $2\,g + 1$ or $2\,g$ according to whether P is a Weierstrass point or not. If the hyperelliptic involution w is defined over K and P projects to a K-rational point of $Y/\langle w \rangle$, then we can take $\lambda_i \in H^0(Y, \Omega^1_{Y/K})$ for all i and, thus, $F(x) \in K[x]$ (see for instance Lemma 2.5 of [**1**]).

In our particular setting, we point out the following facts:

(a) The curve X_D has a hyperelliptic model over $\mathbb{Q}$ if and only if $X^{(w)}(\mathbb{Q}) \simeq \mathbb{P}^1(\mathbb{Q})$, i.e. $D \neq 57, 82$. Since $X_D(\mathbb{R}) = \emptyset$ (cf. [**18**]), a point Q lies in $\pi_w^{-1}(X^{(w)}(\mathbb{Q}))$ if and only if there is an integer $e < 0$ such that $Q \in X_D(\mathbb{Q}(\sqrt{e}\,))$ with $w(Q) = Q^\sigma$, where σ is

the nontrivial automorphism in $\mathrm{Gal}(\mathbb{Q}(\sqrt{e})/\mathbb{Q})$. In this case, X_D admits an affine equation of the form:

$$y^2 = e\,F(x), \quad F(x) \in \mathbb{Q}[x], \tag{1}$$

where F is monic without double roots, $x \in \mathbb{Q}(X_D)$ and $\operatorname{div} x + (Q) + (w(Q)) \geq 0$. The curve X_D does not have any real point and, thus, does not have any rational Weierstrass point. Therefore, $\deg F = 8$.

(b) From the equality

$$H^0(X_D, \Omega^1_{X_D/\mathbb{Q}}) = \pi_u^*\big(H^0(X^{(u)}, \Omega^1_{X^{(u)}/\mathbb{Q}})\big) \oplus \pi_v^*\big(H^0(X^{(v)}, \Omega^1_{X^{(v)}/\mathbb{Q}})\big),$$

we can take a basis $\{\nu_1, \nu_2, \nu_3\}$ of $H^0(X_D, \Omega^1_{X_D/\mathbb{Q}})$ such that ν_1 lies in $\pi_u^*(H^0(X^{(u)}, \Omega^1_{X^{(u)}/\mathbb{Q}}))$ and ν_2, ν_3 are in $\pi_v^*(H^0(X^{(v)}, \Omega^1_{X^{(v)}/\mathbb{Q}}))$. Since the hyperelliptic involution w acts on $H^0(X_D, \Omega^1_{X_D/\mathbb{Q}})$ as the multiplication by -1 and $w = u \cdot v$, the action of u, v on this basis is the following:

	ν_1	ν_2	ν_3
u	ν_1	$-\nu_2$	$-\nu_3$
v	$-\nu_1$	ν_2	ν_3

It is clear that $\operatorname{div} \nu_1 = \sum_{U \in \mathcal{F}_u} (U)$.

(c) The set of Weierstrass points of $X_D^{(v)}$ consists of the four points of the set $\pi_v(\mathcal{F}_w)$ and the two points of $\pi_v(\mathcal{F}_u)$.

Now, we split our nine cases in three types and we present for each of them a particular class of equations. The first two types correspond to the case X_D hyperelliptic over $\mathbb{Q}$.

3.1. Type 1: $D \in \{35, 51, 62, 69, 94\}$.

PROPOSITION 3.1. *Assume $D \in \{35, 51, 62, 69, 94\}$. Then, the curve $X^{(v)}$ admits an equation of the form*

$$Y^2 = e\,X(X^4 + a\,X^3 + b\,X^2 + c\,X + d)$$

for some $a, b, c, d, e \in \mathbb{Q}$, where $\pi_v(\mathcal{F}_u)$ is the set of Weierstrass points corresponding to $X = 0, \infty$ and $\mathbb{Q}(\sqrt{e})$ is the field of definition of a point $U \in \mathcal{F}_u$. For any such an equation,

(i) *if $D \in \{35, 51, 69\}$, then*

$$y^2 = e(x^8 + a\,x^6 + b\,x^4 + c\,x^2 + d)$$

is an equation for X_D and $y^2 = e\,(X^4 + a\,X^3 + b\,X^2 + c\,X + d)$ is an equation for $X^{(u)}$ for which $w(X, y) = (X, -y)$.

(ii) *if* $D \in \{62, 94\}$ *and, additionally,* $y^2 = e\,(X^4 + a\,X^3 + b\,X^2 + c\,X + d)$ *is an equation for* $X^{(u)}$ *with* $w(X, y) = (X, -y)$*, then*

$$y^2 = e(x^8 + a\,x^6 + b\,x^4 + c\,x^2 + d)$$

is an equation for X_D*.*

Proof. Every $Q \in \mathcal{F}_u$ is defined over an imaginary quadratic field (cf. Table 1) and $w(Q)$ is the Galois conjugate of Q. We fix one of such $Q \in \mathcal{F}_u$. Since the Weierstrass point $\pi_u(Q)$ of $X^{(v)}$ is rational, we can choose $\nu_2 \in \pi_v^*\big(H^0(X^{(v)}, \Omega^1_{X^{(v)}/\mathbb{Q}})\big)$ such that

$$\operatorname{div} \nu_2 = 2(Q) + 2(w(Q)).$$

Set $x = \nu_1/\nu_2$ and $y = dx/\nu_2$. By scaling y by a suitable rational if necessary, x and y satisfies a relationship as in (1), where $\mathbb{Q}(\sqrt{e})$ is the field of definition of Q. The involutions u and v act by sending (x, y) to $(-x, y)$ and $(-x, -y)$ respectively. Therefore, there is a polynomial $G(x) = x^4 + a\,x^3 + b\,x^2 + c\,x + d \in \mathbb{Q}[x]$ such that

$$\begin{aligned} X_D &: y^2 = e\,G(x^2), \\ X^{(u)} &: y^2 = e\,G(X), \\ X^{(v)} &: Y^2 = e\,X\,G(X), \end{aligned}$$

where $X = x^2$ and $Y = y\,x$.

It is clear that w acts on $X^{(u)}$ by sending (X, y) to $(X, -y)$. Since $\operatorname{div} x = (Q') + (w(Q')) - (Q) - (w(Q))$ for $Q' \in \mathcal{F}_u \backslash \{Q, w(Q)\}$, we have that $\mathcal{F}_u$ coincides with the set of points in X_D with coordinates $x = 0, \infty$. Thus, the expressions $X = 0$ and $X = \infty$ yield the set $\pi_v(\mathcal{F}_u)$ on the curve $X_D^{(v)}$. Since $\mathbb{Q}(\sqrt{ed})$ is the field of definition of Q', one has $d \in \mathbb{Q}^2$, for $D \neq 62, 94$, and $2d \in \mathbb{Q}^2$, otherwise.

Let $T^2 = e\,Z\,F(Z)$ be any equation of $X^{(v)}$ with $F(Z) \in \mathbb{Q}[Z]$ monic of degree 4 and such that $\pi_v(\mathcal{F}_u)$ is the set of points in $X^{(v)}$ corresponding to $Z = 0, \infty$. Since the group $\operatorname{Aut}(X^{(v)})$ is commutative (cf. Proposition 1.5 of [**8**]), the set of fixed points of u in $X^{(v)}$ is stable under the action of all automorphisms of the curve. Hence, any isomorphism between $T^2 = e\,Z\,F(Z)$ and $Y^2 = e\,X\,G(X)$ must send the points $Z = 0$ and $Z = \infty$ to the points $X = 0$ and $X = \infty$. Therefore, it must be of the form $(X, Y) = (\alpha\,Z, \lambda\,T)$ or $(X, Y) = (\alpha/Z, \lambda\,T/Z^3)$ for some $\alpha, \lambda \in \mathbb{Q}^*$. Observe that if $d \in \mathbb{Q}^2$, by changing in the equation $y^2 = e\,G(x^2)$ the variables (x, y) by $(1/x, \sqrt{d}\,y/x^4)$ if necessary, we can assume that the isomorphism sends $Z = 0$ to $X = 0$ and, thus, $(X, Y) = (\alpha\,Z, \lambda\,T)$.

If $(X, Y) = (\alpha\,Z, \lambda\,T)$, it is easy to check that $\alpha^5 = \lambda^2$ and, thus, $(\alpha, \lambda) = (\beta^2, \beta^5)$ for some $\beta \in \mathbb{Q}^*$. The changes of variables $(x, y) = (\beta\,z, \beta^4 t)$ and $(X, y) = (\beta^2\,Z, \beta^4 t)$ provide isomorphisms between the genus three curves $y^2 = e\,G(x^2)$ and $t^2 = e\,F(z^2)$ and the genus one curves $y^2 = e\,G(X)$ and $t^2 = e\,F(Z)$ respectively.

If $(X, Y) = (\alpha/Z, \lambda\,T/Z^3)$, then $d\,\alpha = \lambda^2$. If, moreover, the equation

$$t^2 = \frac{e}{d} G\left(\frac{\alpha}{Z}\right) Z^4$$

is equivalent to the equation $y^2 = e\,G(X)$, then d must be a rational square and, thus, the result follows. □

REMARK 3.1. According to Table 1, the values e, up to rational square factors, for each of the three cases of the above proposition are:

D	$3 \cdot 17$	$3 \cdot 23$	$5 \cdot 7$
e	-3	-3	-7

and for $D = 62, 94$ we will choose $e = -1$.

3.2. Type 2: $D \in \{39, 55\}$.

PROPOSITION 3.2. *Assume $D \in \{39, 55\}$. Let $e < 0$ be an integer for which there is a point Q defined over $\mathbb{Q}(\sqrt{e})$ such that $\pi_w(Q) \in X^{(w)}(\mathbb{Q})$. Then, $X^{(v)}$ admits an equation of the form*

$$Y^2 = e(X^4 + a\,X^3 + b\,X^2 + c\,X + d)(X^2 + 4)$$

for some $a, b, c, d \in \mathbb{Q}$, where $\pi_v(\mathcal{F}_u)$ is the set of Weierstrass points corresponding to the roots of $X^2 + 4$ and

$$V^2 = e(X^4 + a\,X^3 + b\,X^2 + c\,X + d)$$

is an equation for $X^{(u)}$ with $w(X, V) = (X, -V)$. For any such an equation for $X^{(v)}$, the curve X_D is defined by the equation

$$y^2 = e(x^8 + a\,x^7 + B\,x^6 + C\,x^5 + E\,x^4 - C\,x^3 + B\,x^2 - a\,x + 1),$$

where $B = b - 4$, $C = c - 3\,a$, $E = d - 2\,b + 6$.

PROOF. In this case, for any choice of Q in $\pi_w^{-1}(X^{(w)}(\mathbb{Q}))$ we have $Q \notin \mathcal{F}_u$. Since u is defined over $\mathbb{Q}$, also $u(Q) \in X_D(\mathbb{Q}(\sqrt{e}))$ and $v(Q) = u(w(Q)) = u(Q)^\sigma$.

We can choose $\lambda_1, \lambda_2 \in H^0(X_D, \Omega^1_{X_D/\mathbb{Q}})$ such that:

$$\operatorname{div}\lambda_1 = (Q) + (w(Q)) + (v(Q)) + (u(Q)), \quad \operatorname{div}\lambda_2 = 2(Q) + 2(w(Q)).$$

Set $x = \lambda_1/\lambda_2$ and $y = dx/\lambda_2 = x\,dx/\lambda_1$. Then, we have a relationship as in (1) by escaling y by a suitable rational if necessary. Due to the fact that

$$\operatorname{div} u^*(x) = \operatorname{div} u^*(\lambda_1) - \operatorname{div} u^*(\lambda_2) = \operatorname{div}\lambda_2 - \operatorname{div}\lambda_1 = -\operatorname{div} x,$$

it is clear that $u^*(x) = \varepsilon/x$ for some $\varepsilon \in \mathbb{Q}^*$. The divisor of λ_1 is invariant under u and $\lambda_1 \notin \langle \nu_1 \rangle$ since $\operatorname{div}\nu_1 = \sum_{U \in \mathcal{F}_u}(U)$. Therefore, λ_1 must satisfy $u^*(\lambda_1) = -\lambda_1$.

Hence, $u^*(y) = y\,\varepsilon^2/x^4$ and u sends (x,y) to $(\varepsilon/x, y\,\varepsilon^2/x^4)$. Note that $\varepsilon \notin \mathbb{Q}^2$, otherwise $\pi_w(\mathcal{F}_u) \subset X^{(w)}(\mathbb{Q})$. By scaling x by a suitable rational, we can assume that ε is square-free. Since $\mathbb{Q}(\sqrt{\varepsilon}) \subseteq \mathbb{Q}(\pi_v(U))$ for all $U \in \mathcal{F}_u$, it follows that $\varepsilon = -1$ (see Table 1). Hence,

$$\begin{aligned} X_D &: y^2 = e(x^8 + A\,x^7 + B\,x^6 + C\,x^5 + E\,x^4 - C\,x^3 + B\,x^2 - A\,x + 1), \\ X^{(u)} &: V^2 = e(X^4 + A\,X^3 + (B+4)X^2 + (C+3\,A)X + E + 2\,b + 2), \\ X^{(v)} &: Y^2 = e(X^4 + AX^3 + (B+4)X^2 + (C+3A)X + E + 2B + 2)(X^2+4), \end{aligned} \tag{2}$$

for some $A, B, C, E \in \mathbb{Q}$ and where

$$X = x - 1/x, \quad V = y/x^2 \quad \text{and} \quad Y = V(x + 1/x) = y(x^2+1)/x^3.$$

Writing $a = A$, $b = B + 4$, $c = C + 3\,A$ and $d = E + 2\,B + 2$, we recover the notation as in the statement. Since the points of $\mathcal{F}_u$ correspond to the points whose x-coordinates satisfy $x^2 = -1$, it follows that their projections to $X^{(v)}$ satisfy $X^2 = -4$. Moreover, w acts on $X^{(u)}$ by sending (X, V) to $(X, -V)$.

Set $g(x) := e(x^8 + A\,x^7 + B\,x^6 + C\,x^5 + E\,x^4 - C\,x^3 + B\,x^2 - A\,x + 1)$ and $G(X) := X^4 + a\,X^3 + b\,X^2 + c\,X + d$. Let $T^2 = e\,(Z^2+4)F(Z)$ be any equation of $X^{(v)}$ with $F(Z) \in \mathbb{Q}[Z]$ monic of degree 4 and such that $\pi_v(\mathcal{F}_u)$ is the set of points corresponding to $Z^2 = -4$ and $S^2 = e\,F(Z)$ is an equation of $X^{(u)}$ equivalent to $V^2 = e\,G(X)$. Changing (x,y) by $(-x,y)$ in the equation given in (2) for X_D if necessary, we can assume that an isomorphism defined over $\mathbb{Q}$ between $T^2 = e\,(Z^2+4)F(Z)$ and $Y^2 = e(X^2+4)G(X)$ sends $Z = 2\,i$ and $Z = -2\,i$ to $X = 2\,i$ and $X = -2\,i$ respectively. Therefore, this isomorphism must be of the form

$$(X,Y) = \left(-\frac{4}{Z}, \lambda\,\frac{T}{Z^3}\right) \quad \text{or} \quad (X,Y) = \left(\frac{Z - 4\gamma}{\gamma\,Z + 1}, \lambda\,\frac{T}{(\gamma Z + 1)^3}\right)$$

for some $\gamma, \lambda \in \mathbb{Q}$.

If $(X,Y) = (-4/Z, \lambda\,T/Z^3)$, we consider the equation $t^2 = f(z)$ obtained from the equation $y^2 = g(x)$ by means of the change of variables

$$(x,y) = ((z-1)/(z+1), \lambda\,2\,t/(z+1)^4).$$

It is easy to prove that

$$\left(\frac{t}{z^4}\right)^2 = f\left(-\frac{1}{z}\right),\ Z = z - \frac{1}{z},\ S = \frac{t}{z^2},\ T = t\frac{z^2+1}{z^3}. \tag{3}$$

Hence, $t^2 = f(z)$ is the equation of the genus three curve obtained from the equation $T^2 = e(Z^2+4)F(Z)$ after applying the rule given in the statement.

For the isomorphism $(X,Y) = ((Z - 4\gamma)/(\gamma\,Z + 1), \lambda\,T/(\gamma Z + 1)^3)$, we get that $\gamma(1 + 4\,\gamma^2)(a + \gamma + b\,\gamma + c\,\gamma^2 + d\,\gamma^3) = \lambda^2$. Moreover, since the equation

$$S^2 = e\,F(Z) = \frac{e}{\gamma(a+\gamma+b\,\gamma+c\,\gamma^2+d\,\gamma^3)} G\left(\frac{Z-4\gamma}{\gamma\,Z+1}\right)(\gamma\,Z+1)^4,$$

is equivalent to $V^2 = e\,G(X)$, the expression $\gamma(a+\gamma+b\,\gamma+c\,\gamma^2+d\,\gamma^3)$ must be a rational square and, thus, also $1+4\,\gamma^2 \in \mathbb{Q}^2$. Let ν be any root of the polynomial $\gamma\,x^2+x-\gamma$, which is a rational number different from ± 1. The change of variables

$$(x,y) = \left(\frac{z-\nu}{\nu\,z+1}, -\lambda\frac{\nu^2+1}{(\nu^2-1)^3}\,\frac{t}{(\nu\,z+1)^4}\right)$$

provides an equation $t^2 = f(z)$ for X_D satisfying all conditions in (3). Hence, the statement is proved. □

REMARK 3.2. By the theory of Heegner points, we can choose e of the previous proposition to be -7 for $D = 39$ and -3 for $D = 55$, up to rational square factors.

3.3. Type 3: $D = 57, 82$.

PROPOSITION 3.3. *Assume $D = 57, 82$. Let $e < 0$ be a square-free integer for which there exists a point $P \in X_D(\mathbb{Q}(\sqrt{e}))$ such that $\pi_u(P) \in X^{(u)}(\mathbb{Q})$ and let α be either 3 or 2 depending on whether D is equal to 57 or 82. Then, $X^{(v)}$ admits an equation of the form*

$$Y^2 = e(x^2+\alpha)F(x),$$

where $F(x) \in \mathbb{Q}[x]$ is a monic polynomial of degree 4, $\pi_v(\mathcal{F}_u)$ is the set of Weierstrass points corresponding to $x = \pm\sqrt{-\alpha}$ and $y^2 = F(x)$ is an equation for $X^{(u)}$ with $w(x,y) = (x,-y)$. For such an equation,

$$y^2 = F(x), \quad t^2 = e(x^2+\alpha)$$

is an equation for X_D.

PROOF. Since for $D = 57, 82$ we have that $|\ X^{(u)}(\mathbb{Q})\ | = \infty$, we can choose two points P, Q in $\pi_u^{-1}(X^{(u)}(\mathbb{Q}))$ such that the sets $\{P, u(P), v(P), w(P)\}$ and $\{Q, u(Q), v(Q), w(Q)\}$ are disjoint. It is clear that both sets are stable by Galois conjugations and each of them has all its points defined in the same imaginary quadratic field.

With the same argument used for λ_1 in the above proposition, we choose ν_2, ν_3 in $\pi_v^*(H^0(X^{(v)}, \Omega^1_{X^{(v)}/\mathbb{Q}}))$ such that

$$\operatorname{div}\nu_2 = (Q) + (u(Q)) + (w(Q)) + (v(Q)), \quad \operatorname{div}\nu_3 = (P) + (u(P)) + (w(P)) + (v(P)).$$

Set $x = \nu_2/\nu_3$ and $y = dx/\nu_1$. The functions x and y^2, viewed as functions on $X_D/\langle u, v\rangle$, have a unique pole of multiplicity 1 and 4 respectively at the projection of P. Therefore,

$$\mathbb{Q}(X^{(u)}/\langle w\rangle) = \mathbb{Q}(X^{(v)}/\langle w\rangle) = \mathbb{Q}(x), \quad \mathbb{Q}(X^{(u)}) = \mathbb{Q}(x,y) \quad \text{and} \quad y^2 = F(x),$$

where $F(x) \in \mathbb{Q}[x]$ has degree 4 and w acts by sending (x,y) to $(x,-y)$. Observe that the leading coefficient of F and $F(0)$ are rational squares since the projections of P and Q into $X^{(u)}$ are rational.

Set $t = \nu_1/\nu_3 \in \mathbb{Q}(X_D)$. Of course, $u^*(t) = v^*(t) = -t$ and $w^*(t) = t$. In particular $t \notin \mathbb{Q}(X^{(v)})$ and $t^2 \in \mathbb{Q}(X_D/\langle u, v\rangle)$. Since t^2, viewed as a function on $X_D/\langle u,v\rangle$, has a unique pole of multiplicity 2 at the projection of P, t^2 is a polynomial of degree 2 in x with rational coefficients. The function t^2, now viewed as a function on $X^{(v)}$, has its zeros at the points of $\pi_v(\mathcal{F}_u)$, defined over $\mathbb{Q}(\sqrt{-\alpha})$ (see Table 1), and has its poles at the points of $\pi_v(\{P, u(P)\}$, defined over $\mathbb{Q}(\sqrt{e})$. Therefore, after changing the variables t by $a\,t$ and x by $b\,x + c$ for a suitable $a, b, c \in \mathbb{Q}$, we get $t^2 = e(x^2 + \alpha)$. Now, by scaling y by a suitable rational, F can be chosen to be monic. Taking $Y = t\,y$, we obtain the following equation for X_D:

$$\begin{aligned} X_D &: y^2 = F(x) \quad \text{and} \quad t^2 = e\,(x^2 + \alpha), \\ X^{(u)} &: y^2 = F(x), \\ X^{(v)} &: Y^2 = e(x^2 + \alpha)F(x). \end{aligned} \tag{4}$$

Set $F(x) = x^4 + a\,x^3 + b\,x^2 + c\,x + d$. Let $T^2 = d(z^2 + \alpha)G(z)$ be any equation for $X^{(v)}/\mathbb{Q}$ such that $\pi_v(\mathcal{F}_u)$ corresponds to the set of points with $x = \pm\sqrt{-\alpha}$ and $t^2 = G(z)$ is an equation equivalent to $y^2 = F(x)$. We can assume that the isomorphism between both equations for $X^{(v)}$ sends $z = \sqrt{-\alpha}$ and $z = -\sqrt{-\alpha}$ to $x = \sqrt{-\alpha}$ and $x = -\sqrt{-\alpha}$ respectively. So, the isomorphism must be of the form

$$(x, Y) = \left(-\frac{\alpha}{z}, \lambda\frac{T}{z^3}\right) \text{ or } (x,Y) = \left(\frac{z - \alpha\,\gamma}{\gamma\,z + 1}, \lambda\frac{T}{(\gamma\,z+1)^3}\right).$$

If $(x,Y) = (-\alpha/z, \lambda\,T/z^3)$, the condition that the equation

$$t^2 = G(z) = \frac{\alpha}{\lambda^2}F\left(-\frac{\alpha}{z}\right)z^4$$

is equivalent to $y^2 = F(x)$ leads to the contradiction that α should be a rational square.

If $(x,Y) = ((z - \alpha\,\gamma)/(\gamma\,z+1), \lambda\,T/(\gamma\,z+1)^3)$, then

$$(1 + \alpha\,\gamma^2)(1 + b\,\gamma^2 + c\,\gamma^3 + d\,\gamma^4) = \lambda^2.$$

Moreover, since

$$t^2 = G(z) = \frac{1}{1 + b\,\gamma^2 + c\,\gamma^3 + d\,\gamma^4}F\left(-\frac{\alpha}{z}\right)z^4$$

is equivalent to $y^2 = F(x)$, we have that $1 + b\,\gamma^2 + c\,\gamma^3 + d\,\gamma^4$ is a rational square and,

thus, $1+\alpha\,\gamma^2=\beta^2$ for some $\beta\in\mathbb{Q}$. Hence, the change of variables

$$(x,Y,t)=\left(\frac{z-\alpha\,\gamma}{\gamma\,z+1},\lambda\frac{T}{(\gamma\,z+1)^3},\beta\,W\right)$$

provides an isomorphism between the equation for X_D given in (4) and the equation $T^2=G(z)$ and $W^2=e(z^2+\alpha)$. □

REMARK 3.3. By the theory of Heegner points, we can choose $e=-1$ and $e=-3$ for $D=59$ and $D=82$ respectively.

4. Equations for Atkin–Lehner quotients and X_D.

4.1. Genus one quotients.

Here, we focus our attention on the curve $X^{(u)}$. The Jacobian of the curve $X^{(u)}$ has conductor D because it is a quotient of the new part of the Jacobian of $X_0(D)$ defined over $\mathbb{Q}$ and its $\mathbb{Q}$-isomorphism class can be determined by using the Cěrednik–Drinfeld description of the fibers of X_D at primes $p\mid D$ (cf. [**17**] and the footnote in page 938 of [**6**]). Next, we show the set $X^{(u)}(\mathbb{Q})$, given as group when $X^{(u)}$ is elliptic over $\mathbb{Q}$, and Cremona's label of the elliptic curve $\mathrm{Jac}(X^{(u)})$:

D	$2\cdot 31$	$2\cdot 41$	$2\cdot 47$	$3\cdot 13$	$3\cdot 17$	$3\cdot 19$	$3\cdot 23$	$5\cdot 7$	$5\cdot 11$
$X^{(u)}(\mathbb{Q})$	$\emptyset$	$\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$	$\emptyset$	$\emptyset$	$\{0\}$	$\mathbb{Z}$	$\emptyset$	$\mathbb{Z}/3\mathbb{Z}$	$\emptyset$
$\mathrm{Jac}(X^{(u)})$	$A3$	$A1$	$A2$	$A1$	$A2$	$A1$	$A2$	$A1$	$A1$

PROPOSITION 4.1. *The following table shows equations for $X^{(u)}/\mathbb{Q}$ of the form $Z^2=F(X)$, for which the involution w acts sending (X,Z) to $(X,-Z)$:*

Table 2.

D	$X^{(u)}$
35	$Z^2=-(7\,X+1)(X^3+197\,X^2+51\,X+7)$
39	$Z^2=-(7\,X^2+23\,X+19)(X^2+X+1)$
51	$Z^2=-(X+3)(243\,X^3+235\,X^2-31\,X+1)$
55	$Z^2=-(3\,X^2-4\,X+16)(X^2+4\,X+48)$
57	$Z^2=(X+4)(X^3+20\,X^2+48\,X+32)$
62	$Z^2=-(64\,X^4+99\,X^3+90\,X^2+43\,X+8)$
69	$Z^2=-(3X^4+28\,X^3+74\,X^2-1268\,X+2187)$
82	$Z^2=16X^4-32\,X^3+1032\,X^2+1576\,X+1549$
94	$Z^2=-(8\,X^4-69\,X^3+234\,X^2-381\,X+256)$

In particular, any equation for $X^{(u)}$ of the form $Z^2=G(X)$ with $\deg G(X)=3$ or 4 for which the action of w is given by $(X,Z)\mapsto(X,-Z)$ is equivalent over $\mathbb{Q}$ to the equation given in Table 2.

Proof. When $X^{(u)}(\mathbb{Q}) = \emptyset$, i.e. for $D \neq 35, 51, 57$ and 82, see Theorem 4.2 of [**6**]. For $D = 51, 57$ and 82, we proceed as in [**6**]. We take a subset $\{P_1, \dots, P_n\} \subset \mathrm{Jac}(X^{(u)})(\mathbb{Q})$ of representative elements of the group $\mathrm{Jac}(X^{(u)})(\mathbb{Q})/2\,\mathrm{Jac}(X^{(u)})(\mathbb{Q})$ and for each P_i we attach an equation $y^2 = F_i(x)$ as in Subsection 2.1 of [**6**]. The equation in the statement corresponds to the unique equivalence class such that the number field generated by the roots of $F_i(x)$ agrees with the number field generated by the coordinates of the points in $\pi_u(\mathcal{F}_w)$. Since for $D = 35$ this procedure gives two equivalence classes satisfying the previous condition, we use another argument in this case. Indeed, from [**12**] we know that

$$y^2 = -x(9\,x + 4)(4\,x + 1)(172\,x^3 + 176\,x^2 + 60\,x + 7)$$

is an equation for $X^{(v)}$ and, moreover, it can be checked that the x-coordinates of the Weierstrass points coming from $\mathcal{F}_u$ are 0 and $-4/9$. Since the change

$$x = \frac{4X}{-9X + 1}, \quad y = \frac{4Y}{(-9X + 1)^3}$$

provides an isomorphism with the curve $Y^2 = -X(7X + 1)(X^3 + 197X^2 + 51X + 7)$ sending $x = 0, -4/9$ to $X = 0, \infty$, the equation in Table 2 is obtained by applying part (1) of Proposition 3.1. □

4.2. Genus two quotients.

Now, we deal with the curve $X^{(v)}$. Equations for $D = 35, 51, 57, 69$ can be found in [**12**]. Moreover, the procedure used in this paper allows us to determine which Weierstrass points come from fixed points of u. For $D = 39, 55$ we can determine equations for $X^{(v)}$ either following the same procedure used for the before mentioned cases or finding the explicit action of the automorphism v in the equations presented for X_D in [**12**] and determining equations por the corresponding quotients. We omit details of these computations. Equations for all these cases, namely for D odd, are presented in Table 4 of Proposition 4.4.

For D even, i.e. $D = 62, 82, 94$, it is harder to find equations for $X^{(v)}$ than for the odd case. We do not have a description of the thicknesses of the singular points in terms of the valuation of the difference of the roots of the polynomials involved in a suitable model of the form $Y^2 = R(X)$ at $p = 2$ (see Theorem 2.3 of [**12**]). This is basically due to the fact that a model of the form $Y^2 = R(X)$ is not a good model at $p = 2$.

Let $\mathcal{W}$ be a model for $X^{(v)}$ over $\mathbb{Z}$ of the form:

$$\mathcal{W} : Y^2 + Q(X)Y = P(X), \quad P(X), Q(X) \in \mathbb{Z}[X]. \tag{5}$$

For such a model, its *discriminant* is defined as follows:

$$\Delta(\mathcal{W}) = \begin{cases} 2^{-12}\mathrm{Disc}(4P(X) + Q(X)^2) & \text{if } \deg(4P(X) + Q(X)^2) = 6, \\ 2^{-12}c^2\mathrm{Disc}(4P(X) + Q(X)^2) & \text{if } \deg(4P(X) + Q(X)^2) = 5, \end{cases}$$

where c is the leading coefficient of $4P(X)+Q(X)^2$. Let $\mathcal{W}_0$ be the model with minimal discriminant. The following result due to Q. Liu [**10**, Théorèmes 1, 2 and Proposition 1] describes the valuation of the discriminant $\Delta(\mathcal{W}_0)$ in terms of the canonical model of $X^{(v)}$, its minimal regular model and the exponent of the conductor attached to the Galois representation on the Tate module of its Jacobian. Since the Jacobian of $X^{(v)}$ is isogenous over $\mathbb{Q}$ to an abelian subvariety of $\mathrm{Jac}(X_0(D))^{\mathrm{new}}$, we know by H. Carayol (cf. [**2**]) that its conductor is D raised to its dimension. Thus the result provides the valuations of the discriminant $\Delta(\mathcal{W}_0)$.

THEOREM 4.2. *Let C be a smooth projective geometrically connected curve of genus 2 defined over a finite extension K of $\mathbb{Q}_p$, with integer ring $\mathcal{O}_K$. Let $\mathfrak{C}_{\mathrm{can}}/\mathcal{O}_K$ and $\mathfrak{C}_{\mathrm{min}}/\mathcal{O}_K$ be its canonical and minimal regular models, respectively. Let us denote by σ the extension of the hyperelliptic involution of C to $\mathfrak{C}_{\mathrm{can}}$. Let n be the number of irreducible components of the special fiber of $\mathfrak{C}_{\mathrm{min}}$ and let d be the number of connected components of the special fiber of the minimal desingularization of $\mathfrak{C}_{\mathrm{can}}/\sigma$. Then, the exponent of the conductor f of C/K can be expressed as*:

$$f(C/K) = v(\Delta(\mathcal{W}_0)) - 11 \cdot \frac{d-1}{2} - n + 1,$$

where v is the normalized valuation of K.

Since the conductor of the Jacobian of $X^{(p)}$ is D raised to its dimension, we have $f(X^{(v)}/\mathbb{Q}_p) = 2$ at every prime $p \mid D$. Moreover, the Cěrednik–Drinfeld special fiber of X_D at $p \mid D$ can be computed using MAGMA, together with the action of u, v and w on its irreducible components and singular points (see [**8**]). Hence, we are able to compute the special fiber of a semistable model for $X^{(v)}$ and the action of the hyperelliptic involution w on it. Contracting exceptional divisors and next blowing-down and blowing-up singularities, we obtain the special fibers of $\mathfrak{X}^{(v)}_{\mathrm{can}}$ and $\mathfrak{X}^{(v)}_{\mathrm{min}}$, the canonical and minimal regular models of $X^{(v)}$ respectively, together with the action of the hyperelliptic involution on both of them. Thus, we determine n, d and, thus, $v_p(\Delta(\mathcal{W}_0))$ at every prime $p \mid D$. Using this procedure we obtain the following result

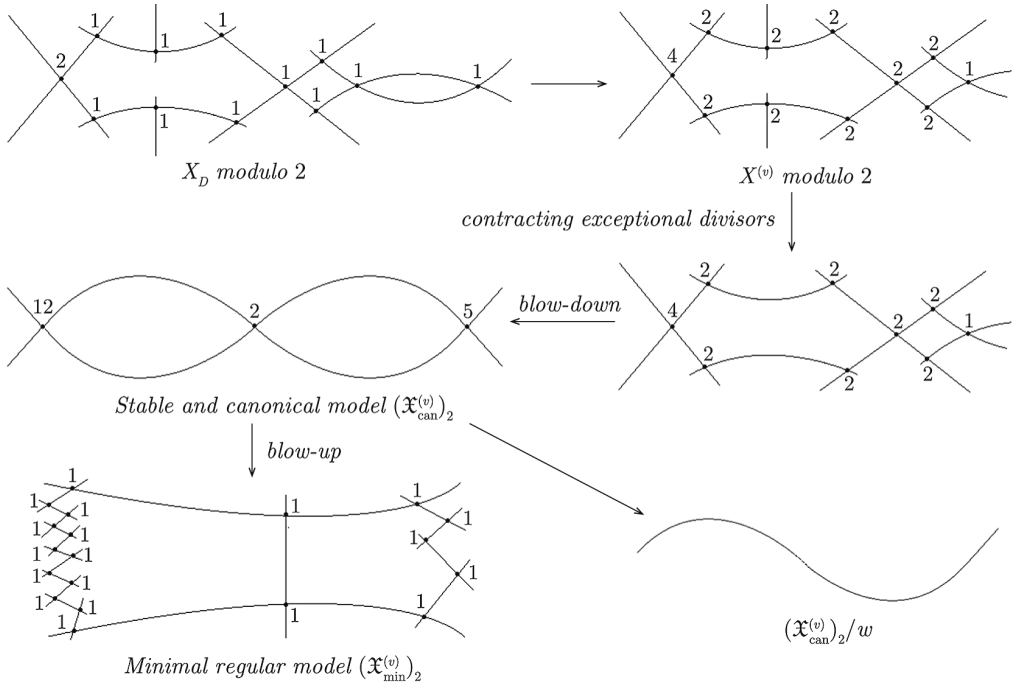
PROPOSITION 4.3. *The absolute values of the discriminants $\Delta(\mathcal{W}_0)$ of the minimal hyperelliptic models $\mathcal{W}_0/\mathbb{Z}$ of $X^{(v)}$ are given by the following table*:

D	$2 \cdot 31$	$2 \cdot 41$	$2 \cdot 47$
$\lvert\Delta(\mathcal{W}_0)\rvert$	$2^{15} \cdot 31^4$	$2^{15} \cdot 41^7$	$2^{19} \cdot 47^2$

PROOF. We compute the valuation of $\Delta(\mathcal{W}_0)$ at every prime of bad reduction using the above theorem and the procedure, described in the previous paragraph, to compute the special fibers of $\mathfrak{X}^{(v)}_{\mathrm{can}}$ and $\mathfrak{X}^{(v)}_{\mathrm{min}}$ together with the action of the hyperelliptic involution on both of them. We show this procedure for the three even values of D and $p = 2$.

Case 4.1. For $D = 94$ and $p = 2$, we compute the special fiber of X_D using Cěrednik–

Drinfeld theory. We describe graphically the quotients, contractions of exceptional divisors, blown-ups and blow-downs we have apply to obtain the special fibers of $\mathfrak{X}_{\mathrm{can}}^{(v)}$ and $\mathfrak{X}_{\mathrm{min}}^{(v)}$:



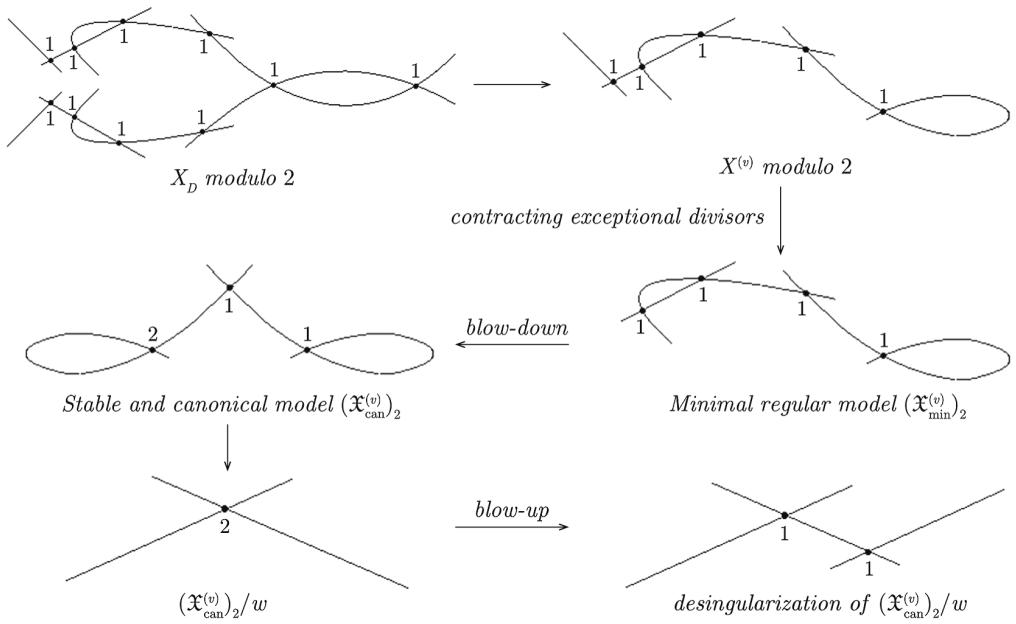
We obtain that the number of irreducible components of the special fiber of the minimal regular model is $n = 18$ and, moreover, the number of connected components of the special fiber of the minimal desingularization of $\mathfrak{X}_{\mathrm{can}}^{(v)}/w$ is $d = 1$. Thus, we get $v_2(\Delta(\mathcal{W}_0)) = 19$.

Case 4.2. The case $D = 62$ and $p = 2$ is similar to the previous case. We obtain that the number of irreducible components of the special fiber of the minimal regular model is $n = 14$. Moreover, the number of connected components of the special fiber of the minimal desingularization of $\mathfrak{X}_{\mathrm{can}}^{(v)}/w$ is also $d = 1$. Thus, we get $v_2(\Delta(\mathcal{W}_0)) = 15$.

Case 4.3. For $D = 82$ and $p = 2$, we have the following special fibers:
We obtain that the number of irreducible components of the special fiber of the minimal regular model is $n = 3$ and, moreover, the number of connected components of the special fiber of the minimal desingularization of $\mathfrak{X}_{\mathrm{can}}^{(v)}/w$ is $d = 3$. Thus, we get $v_2(\Delta(\mathcal{W}_0)) = 15$.

The computation of the valuations $v_p(\Delta(\mathcal{W}_0))$ provides $\Delta(\mathcal{W}_0)$ up to sign, namely, the absolute value $|\Delta(\mathcal{W}_0)|$. □

From $\mathcal{W}_0$, we obtain a model $\mathcal{W}_0'$ of the form $Y^2 = R(X) = 4P(X) + Q^2(X)$. Note that $\Delta(\mathcal{W}_0)$ provides the discriminant of $R(X)$. The roots of $R(X)$ are the X-coordinates of the Weierstrass points of $X^{(v)}$, i.e. $\pi_v(\mathcal{F}_w) \cup \pi_v(\mathcal{F}_u)$. In Table 1, it is given the field



of definition L_u of the coordinates of any $U \in \pi_v(\mathcal{F}_u)$. Again by using [**6**], the fields of definition L_w of the coordinates of any $W \in \pi_v(\mathcal{F}_w)$ are:

Table 3.

D	$L_w = \mathbb{Q}(W)$
$2 \cdot 31$	$\mathbb{Q}[X]/(X^4 + X^3 + 4X^2 - 2X + 4)$
$2 \cdot 41$	$\mathbb{Q}[X]/(X^4 + 2X^3 - X^2 - 2X + 2)$
$2 \cdot 47$	$\mathbb{Q}[X]/(X^4 + 5X^2 + 18)$

Note that L_u and L_w are the fields involved in the factorization of $R(X) = \prod_i p_i(X)$. The above analysis of the special fibers provides

$$\mathrm{Disc}(R) = \prod_i \mathrm{Disc}(p_i) \prod_{i,j} \mathrm{Res}(p_i, p_j)^2.$$

By using specialization of Heegner points we can determine the valuations of $\mathrm{Disc}(p_i)$ and $\mathrm{Res}(p_i, p_j)$ at every odd prime (see Section 4 of [**12**]). Since we know the 2-valuation of $\mathrm{Disc}(R)$, we have a finite number of possible 2-valuations for $\mathrm{Disc}(p_i)$. Moreover, its sign is determined by the field of definition of p_i. A suitable choice of the points at infinity (they are going to be also Heegner points) provides the leading coefficients of the p_i.

Once we know the leading coefficient c_i, we proceed to determine the corresponding monic polynomial $q_i(X) = c_i^{\deg p_i - 1} p_i(X/c_i) \in \mathbb{Z}[X]$, whose discriminant is $\mathrm{Disc}\, q_i = c_i^{(\deg p_i - 1)(\deg p_i - 2)} \mathrm{Disc}\, p_i$. By [**7**], there are only finitely many monic polynomials with integer coefficients, up to translation by integers, with the same discriminant and field

of definition as q_i. Let L_i is the field of definition of p_i and let $\mathcal{O}_{L_i}$ be its integer ring, let $\alpha_i \in \mathcal{O}_{L_i}$ be a root of q_i. Since the discriminant of q_i provide the index of the order $\mathbb{Z}[\alpha_i]$ in $\mathcal{O}_i$, by means of the instruction *IndexFormEquation* of *MAGMA*, we determine a finite number of candidates for α_i and p_i up to translation by integers. For any of these choices for all i, we determine $R(x)$ by using that $\mathrm{Res}(p_i, p_j)$ is known. Next, we will use properties of Shimura curves to discard fake equations in case that our procedure produces more than one candidate.

4.2.1. Computing equations.

The cases $D = 62$ and 94 are similar and correspond to type 1 introduced in Section 3. In both cases the pair of Weierstrass points coming from the fixed points of u are rational. We choose one of these rational Weierstrass points to be the point of infinity. Therefore the model $\mathcal{W}_0'$ is given by

$$\mathcal{W}_0' : \ Y^2 = R(X) = \pm p_1(X) \cdot p_2(X),$$

where p_1 is the polynomial of degree 1 corresponding to the other rational point and p_2 is the irreducible polynomial corresponding the Galois orbit $\pi_v(\mathcal{F}_w)$ with field of definition L_w. Recall that $\Delta(\mathcal{W}_0) = 2^{-12}c^2 \,\mathrm{Disc}(R)$ is given, where c is the leading coefficient of R. For the case $D = 62$, we have $\Delta(\mathcal{W}_0) = 2^{15}31^4$ while for $D = 94$, $\Delta(\mathcal{W}_0) = 2^{19}47^2$. By the results on the reduction of Heegner points (cf. [**13**], [**12**]), we can compute the valuation of $\mathrm{Disc}(p_2)$ at every odd prime. Set $v_2(\mathrm{Disc}(p_2)) = t$, we computed

$$\mathrm{Disc}(p_2) = \begin{cases} 2^t 31^4, & \text{if } D = 62, \\ 2^t 47^2, & \text{if } D = 94. \end{cases}$$

Since $\mathrm{Disc}(R) = \mathrm{Disc}(p_2)\,\mathrm{Res}(p_1, p_2)^2$, we obtain that c and $\mathrm{Res}(p_1, p_2)$ are powers of 2. Therefore,

$$\begin{cases} p_1(X) = 2^\alpha X + b, \\ p_2(X) = 2^\gamma X^4 + dX^3 + eX^3 + fX^2 + g, \end{cases}$$

$$\mathrm{Disc}(p_2)\,\mathrm{Res}(p_1, p_2)^2 = 2^{12}c^{-2}\Delta(\mathcal{W}_0) = \begin{cases} 2^{27}2^{-2\alpha-2\gamma}31^4 & \text{if } D = 62, \\ 2^{31}2^{-2\alpha-2\gamma}47^2 & \text{if } D = 94, \end{cases} \tag{6}$$

$$\alpha + \gamma \leq \frac{12 + v_2(\Delta(\mathcal{W}_0))}{2}; \quad \alpha + \gamma \leq \begin{cases} 13 & \text{if } D = 62, \\ 15 & \text{if } D = 94. \end{cases} \tag{7}$$

First we compute the polynomial p_2. Notice that

$$t \leq 12 + v_2(\Delta(\mathcal{W}_0)) - 2\alpha - 2\gamma = \begin{cases} 27 - 2\alpha - 2\gamma & \text{if } D = 62, \\ 31 - 2\alpha - 2\gamma & \text{if } D = 94. \end{cases} \tag{8}$$

Instead of determining the polynomial $p_2(X)$, we determine the corresponding monic

polynomial with integer coefficients

$$q_2(X) = 2^{3\gamma}p_2(X/2^\gamma) = X^4 + dX^3 + 2^\gamma eX^3 + 2^{2\gamma}fX^2 + 2^{3\gamma}g$$

with $\mathrm{Disc}(q_2) = 2^{6\gamma}\,\mathrm{Disc}(p_2)$. We do not know explicitly $\upsilon_2(\mathrm{Disc}(q_2))$, but we can bound it thanks to (7) and (8):

$$\upsilon_2(\mathrm{Disc}(q_2)) = t + 6\gamma \le 12 + \upsilon_2(\Delta(\mathcal{W}_0)) + 4\gamma \le 36 + 3\upsilon_2(\Delta(\mathcal{W}_0)).$$

Since q_2 is monic and defines the field L_w given in Table 2, we have $\mathrm{Disc}(q_2) = N^2\,\mathrm{Disc}(L_w)$, where $N \in \mathbb{Z}$ is the index. It is known that there are finitely many possible q_2 for a given N and L_w, up to translation by integers. In our case, $N = 2^m$ and, moreover, m is bounded since $\upsilon_2(\mathrm{Disc}(q_2)) \le 36 + 3\upsilon_2(\Delta(\mathcal{W}_0))$.

By means of the instruction *IndexFormEquation* of *MAGMA*, we compute all the possible values of m which provide candidates for q_2. We obtain

D	m
62	$3, 9, 12, 15, 18, 21, 24$
94	$3, 6, 9, 12, 15, 18, 21, 24, 27$

Notice that $2m + \upsilon_2(\mathrm{Disc}(L)) = \upsilon_2(\mathrm{Disc}(q_2)) = t + 6\gamma$ and, thus,

$$\gamma \le \frac{2m + \upsilon_2(\mathrm{Disc}(L))}{6}.$$

This inequality provides a finite number of possibilities for the leading coefficient 2^γ for a fixed q_2. Among all possibilities for the pairs (q_2, γ), we select those for which there is an integer s in a set of representatives modulo 2^γ such that $p_2(x) = 2^{-3\gamma}q_2(2^\gamma x + s)$ has integer coefficients and, moreover, $\upsilon_2(\mathrm{Disc}(p_2)) \le 12 + \upsilon_2(\Delta(\mathcal{W}_0)) - 2\gamma$. Finally, we obtain 17 possibilities for p_2 if $D = 62$ and 68 if $D = 94$.

Recall that

$$\mathrm{Res}(p_1, p_2)^2 = 2^{8\alpha}p_2(-b/2^\alpha)^2 = 2^{12}2^{-2\alpha-2\gamma}\,\mathrm{Disc}(p_2)^{-1}\Delta(\mathcal{W}_0).$$

Thus, $\alpha \le (12 - 2\gamma - \upsilon_2(\mathrm{Disc}(p_2)) + \upsilon_2(\Delta(\mathcal{W}_0)))/2 := r$. Now, for a given p_2 and a in the range $[0, \dots, r]$, we select the pairs (p_2, α) such that the equation $p_2(x) = \pm 2^{r-5\alpha}$ admits the rational solution $-b/2^\alpha$. For each of such pairs, we have two possible equations for $X^{(v)}$: $Y^2 = \pm(2^\alpha X + b)p_2(X)$.

In the case $D = 62$, we obtain 6 possible solutions up to $\mathbb{Q}$-isomorphisms:

$$Y^2 = (X+6)(X^4 + 6X^3 + 27X^2 + 116X + 236), \qquad (C_1^+)$$

$$Y^2 = -(X+6)(X^4 + 6X^3 + 27X^2 + 116X + 236), \qquad (C_1^-)$$

$$Y^2 = (X+3)(4X^4 + 12X^3 + 27X^2 + 58X + 59), \qquad (C_2^+)$$

$$Y^2 = -(X+3)(4X^4+12X^3+27X^2+58X+59), \qquad (C_2^-)$$

$$Y^2 = X(64X^4+99X^3+90X^2+43X+8), \qquad (C_3^+)$$

$$Y^2 = -X(64X^4+99X^3+90X^2+43X+8). \qquad (C_3^-)$$

By using the instruction *genus2reduction* of *SAGE*, we determine the type of reduction modulo $p=2$ of these curves. We obtain that (C_1^+), (C_1^-), (C_2^+) and (C_2^-) have stable reduction of type V, while (C_3^+) and (C_3^-) have stable reduction of type IV with the Liu notation (cf. [**11**]). Since $X^{(v)}$ have stable reduction of type IV at $p=2$, our candidates are now (C_3^+) and (C_3^-).

Since $\mathrm{Jac}(X_{62})$ is isogenous over $\mathbb{Q}$ to $\mathrm{Jac}(X_0(62))^{\mathrm{new}}$ and this abelian variety is isogenous over $\mathbb{Q}$ to the product of an elliptic curve and a simple abelian surface, there is a normalized newform $f = q + \sum_{n>1} a_n q^n \in S_2(\Gamma_0(62))$ such that the abelian surface A_f attached to f by Shimura is isogenous over $\mathbb{Q}$ to $\mathrm{Jac}(X^{(v)})$. One has that $\mathbb{Q}(\{a_n\}) = \mathbb{Q}(\sqrt{3})$ and, moreover, $a_3 = 1+\sqrt{3}$. Applying the Eichler-Shimura congruence, we know that the trace of the Frobenius automorphism Frob_3 acting on the ℓ-adic ($\ell \neq 3$) Tate module of the reduction of $\mathrm{Jac}(X^{(u)})$ mod 3 is equal to a_3 plus its Galois conjugate, i.e. 2. An easy computation allows us to discard the equation C_3^+ and we obtain that $X^{(v)}$ has the following equation

$$X^{(v)}:\ Y^2 = -X(64X^4+99X^3+90X^2+43X+8).$$

In the case $D=94$, we only obtain two possibilities up to $\mathbb{Q}$-isomorphisms:

$$Y^2 = (X+3)(8X^4+27X^3+45X^2+24X+4), \qquad (C_1^+)$$

$$Y^2 = -(X+3)(8X^4+27X^3+45X^2+24X+4). \qquad (C_1^-)$$

Now, the corresponding normalized newform f of level 94 attached to $\mathrm{Jac}(X^{(v)})$ is $f = q - q^2 + \cdots + (-2-2\sqrt{2})q^7 + \cdots$ and, thus, the trace of Frob_7 is -4. We conclude that $X^{(v)}$ has the following equation

$$X^{(v)}:\ Y^2 = -(X+3)(8X^4+27X^3+45X^2+24X+4).$$

The case $D=82$ corresponds to type 3 and, thus, is slightly different to the above cases. In this case, $X^{(v)}$ does not have any rational Weierstrass point. Let $\{P_\infty, \bar{P}_\infty\}$ be the image, under π_v, of the set of Heegner points with CM by $\mathbb{Z}[(1+\sqrt{-11})/2]$. Since such order has class number 1, by [**6**] we know that P_∞ and $\bar{P}_\infty$ lie in $X^{(v)}(\mathbb{Q}(\sqrt{-11}))$ and the hyperelliptic involution acts on these points as the complex conjugation mapping P_∞ to $\bar{P}_\infty$. We choose $P_\infty, \bar{P}_\infty$ to be our infinity points in the hyperelliptic model.

Let c be the leading coefficient of the equation $Y^2 = R(X)$ of $\mathcal{W}_0'$, once we have chosen the infinity points to be P_∞ and $\bar{P}_\infty$. It is clear that $c = -11N^2$ for some $N \in \mathbb{Z}$. In Section 6 of [**12**], it is computed the valuation of c at every $p \nmid D$ in terms of the moduli interpretation of $X_D/\mathbb{Q}$ and its Morita's integral model $\mathcal{X}_D/\mathbb{Z}[1/D]$ as spaces that classify abelian surfaces with quaternionic multiplication. Since $\mathcal{W}_0'$ has good reduction outside

D, it is isomorphic to $\mathcal{X}_D$ locally at $p \nmid D$. This provides an interpretation of the valuation of c at every $p \nmid D$ in terms of the CM abelian surfaces attached to P_∞ and $\bar{P}_\infty$. Applying formulas of Theorem 6.4 in [**12**], we obtain that $v_p(c) = 0$ for all $p \nmid 11 \cdot D$ and $v_{11}(c) = 1$.

To analyze the case $p \mid D$, we return to the integer model $\mathcal{W}_0$: $Y^2 + Q(X)Y = P(X)$, where $R(X) = Q(X)^2 + 4P(X)$. Note that P_∞ lives in the affine open defined by $v^2 + Q_1(u)v = P_1(u)$, where $Q_1(u) = u^3 Q(1/u)$ and $P_1(u) = u^6 P(1/u)$. More precisely, P_∞ and $\bar{P}_\infty$ corresponds to the points $(u, v) = (0, \pm\sqrt{c})$. Thus, if $p \mid c$ then both infinity points specialize to a single Weierstrass point. Using the results of [**13**], we determine that all Weierstrass points have singular specialization at every $p \mid D$. Thus, if $p \mid D$ and $p \mid c$ then P_∞ specializes to a singular point in $\mathcal{W}_0$.

Any model $\mathcal{W}_0$ as in (5) satisfies that $\mathcal{W}_0/\omega$ is smooth. Moreover one can see that, locally at p, such a model $\mathcal{W}_0$ with minimal discriminant can be obtained by normalizing in $X^{(v)}$ any of the irreducible components of $(\mathfrak{X}^{(v)}_{\mathrm{can}}/\omega)_p$. Thus if we show that P_∞ lies in a non-singular point of any of the irreducible components of $(\mathfrak{X}^{(v)}_{\mathrm{can}})_p$, we will conclude that there exists a model $\mathcal{W}_0$ such that P_∞ has good reduction in it.

By Theorem 1.1 of [**13**], we know that the elements of the set $\pi_v^{-1}(P_\infty \cup \bar{P}_\infty)$ have non-singular specialization in the Cěrednik–Drinfeld special fiber and we have a description of the irreducible components were these points lie. Using this computation we check that, even contracting exceptional divisors and blowing-down singularities (see Case 4.3), P_∞ and $\bar{P}_\infty$ have non-singular specialization in $(\mathfrak{X}^{(v)}_{\mathrm{can}})_p$ where $p \mid D$. Thus, if we choose a suitable model $\mathcal{W}_0$, the infinity point P_∞ has good reduction at $p \mid D$, which implies that $c = -11$.

Recall that, since the set of Weierstrass points consists of the pair of Galois orbits $\pi_v(\mathcal{F}_w)$ and $\pi_v(\mathcal{F}_u)$, an equation for $\mathcal{W}_0'$ is of the form $Y^2 = R(X) = p_u(X)p_w(X)$, where p_u determines L_u and p_w determines L_w. By means of the results of [**13**] and [**12**] on the supersingular specialization of Heegner points, we can determine which Weierstrass points reduce to the specialization of P_∞ at $p = 11$. We obtain that the only Weierstrass point that reduces to the specialization of P_∞ is in $\pi_v(\mathcal{F}_u)$. This fact implies that the leading coefficients of p_u and p_w are -11 and 1 respectively. Thus, $p_w(X) = X^4 + cX^3 + dX^2 + eX + f$, $p_u(X) = -11X^2 + aX + b$ and, moreover, $\mathrm{Disc}(R) = \mathrm{Disc}(p_u)\,\mathrm{Disc}(p_w)\,\mathrm{Res}(p_u, p_w)^2 = 41^7 \cdot 2^{27}$. As in the previous cases, we computed that $\mathrm{Disc}(p_w) = 41 \cdot 2^{t_w}$, where $t_w \leq 24$ because $\mathrm{Disc}(L_u) = 2^3$. Since p_w determines L_w, we computed by means of the instruction *IndexFormEquation* that the only possibilities for t_w are $4, 6, 10$ and 12, and we have 8 possible monic polynomials p_w, up to translation. By a similar computation we obtain 6 possibilities for p_u with $\mathrm{Disc}(p_u) = 2^{t_u}$. On the other hand, we know that

$$\mathrm{Res}(p_w(X + \alpha), p_u(X)) = \pm 41^3 \cdot 2^{(27 - t_w - t_u)/2}$$

for some $\alpha \in \mathbb{Z}$. Selecting all pairs (p_u, p_w) for which the above equality admits an integer solution α, we obtain 4 possibilities and, hence, 4 equations for the curve $X^{(v)}$, that turn to be isomorphic. Thus, we obtain the following equation for $X^{(v)}$:

$$X^{(v)} : Y^2 = -(11X^2 - 40X + 48)(X^4 - 6X^3 + 13X^2 - 8X + 4).$$

Observe that for the equations presented for X_D when $D = 62, 82$ and 94, the Weierstrass points coming from fixed points of the involution u are those whose X-coordinates are rational or ∞ for $D = 62$ and 94, or lie in $\mathbb{Q}(\sqrt{-2})$ for $D = 82$.

Proposition 4.4. *Equations for the genus two curves $X^{(v)}$ together with the coordinates of the two points of $\pi_v(\mathcal{F}_u)$ are given in the following table*:

Table 4.

D	$X^{(v)}$	$\pi_v(\mathcal{F}_u)$
35	$Y^2 = -X(7X+1)(X^3+197X^2+51X+7)$	$X = 0, \infty$
51	$Y^2 = -X(X+3)(243X^3+235X^2-31X+1)$	$X = 0, \infty$
62	$Y^2 = -X(64X^4+99X^3+90X^2+43X+8)$	$X = 0, \infty$
69	$Y^2 = -X(3X^4+28X^3+74X^2-1268X+2187)$	$X = 0, \infty$
94	$Y^2 = -X(8X^4-69X^3+234X^2-381X+256)$	$X = 0, \infty$
39	$Y^2 = -(7X^2+23X+19)(X^2+X+1)(X^2+4)$	$X = \pm 2\sqrt{-1}$
55	$Y^2 = -(3X^2-4X+16)(X^2+4X+48)(X^2+4)$	$X = \pm 2\sqrt{-1}$
57	$Y^2 = -(X^2+3)(X+4)(X^3+20X^2+48X+32)$	$X = \pm\sqrt{-3}$
82	$Y^2 = -3(X^2+2)(16X^4-32X^3+1032X^2+1576X+1549)$	$X = \pm\sqrt{-2}$

where, moreover, $Z^2 = F(X)/X$, $Z^2 = F(X)/(X^2+4)$, $Z^2 = -F(X)/(X^2+3)$ and $Z^2 = -(1/3)F(X)/(X^2+2)$ is an equation for $X^{(u)}$ equivalent to the equation given in Table 2 for $D \in \{35, 51, 62, 69, 94\}$, $D \in \{39, 55\}$, $D = 57$ and $D = 82$ respectively.

4.3. Genus three Shimura curves.

As a consequence of Propositions 3.1, 3.2 and 3.3, the equations in Proposition 4.4 determine equations for X_D.

Theorem 4.5. *The following table shows equations for the genus three Shimura curves*:

Table 5.

D	X_D
35	$y^2 = -(7x^2+1)(x^6+197x^4+51x^2+7)$
51	$y^2 = -(x^2+3)(243x^6+235x^4-31x^2+1)$
62	$y^2 = -(64x^8+99x^6+90x^4+43x^2+8)$
69	$y^2 = -(3x^8+28x^6+74x^4-1268x^2+2187)$
94	$y^2 = -(8x^8-69x^6+234x^4-381x^2+256)$
39	$y^2 = -(x^4+x^3-x^2-x+1)(7x^4+23x^3+5x^2-23x+7)$
55	$y^2 = -(x^4-x^3+x^2+x+1)(3x^4+x^3-5x^2-x+3)$
57	$y^2 = (x+4)(x^3+20x^2+48x+32)$, $t^2 = -(x^2+3)$
82	$y^2 = 16x^4-32x^3+1032x^2+1576x-1549$, $t^2 = -3(x^2+2)$

REMARK 4.1. In Table 1 of [**9**], Kurihara conjectured equations for all Shimura curves X_D with $D \leq 65$ and genus > 1. The six equations in Table 5 with $D \leq 62$ are according to the presented in [**9**].

5. The kernel of Ribet's isogeny.

We recall that an abelian variety B is said to be an optimal quotient of an abelian variety A over a field K if there is a surjective morphism $\pi : A \to B$ defined over K with connected kernel. In such a case, if K is a subfield of $\mathbb{C}$, B is determined by the K-vector space $\pi^*(\Omega^1_{B/K})$ and a complex torus for B is obtained by fixing a basis $\omega_1, \ldots, \omega_n$ of $\pi^*(\Omega^1_{B/K})$ and taking the lattice $\{(\int_\gamma \omega_1, \ldots, \int_\gamma \omega_n) : \gamma \in H_1(A, \mathbb{Z})\}$. Note that the property of being optimal quotient over K has the transitive property.

In the modular case, the assignation $h(q) \mapsto h(q)\, dq/q$, where $q = e^{2\pi iz}$, yields a bijection between the $\mathbb{C}$-vector spaces $S_2(\Gamma_0(N))$ and $\Omega^1_{X_0(N)/\mathbb{C}}$ and, moreover, $\Omega^1_{X_0(N)/\mathbb{Q}}$ corresponds to the $\mathbb{Q}$-vector space of cuspidal newforms in $S_2(\Gamma_0(N))$ with rational q-expansion, i.e. $S_2(\Gamma_0(N)) \cap \mathbb{Q}[[q]]$. The abelian variety $\mathrm{Jac}(X_0(N))^{\mathrm{new}}$ denotes the optimal quotient of $\mathrm{Jac}(X_0(N))$ over $\mathbb{Q}$ corresponding to the $\mathbb{Q}$-vector space $S_2(\Gamma_0(N))^{\mathrm{new}} \cap \mathbb{Q}[[q]]$ and for a normalized newform f of level N, A_f shall denote the optimal quotient of $\mathrm{Jac}(X_0(N))^{\mathrm{new}}$ over $\mathbb{Q}$ determined by the $\mathbb{Q}$-vector space of cuspidal newforms with rational q-expansion in the $\mathbb{C}$-vector space generated by all Galois conjugates of f .

Assume that the Shimura curve X_D has genus three and set $A_3 := \mathrm{Jac}(X_0(D))^{\mathrm{new}}$. Since $\mathrm{Jac}(X_D)$ is isogenous over $\mathbb{Q}$ to A_3, there are exactly three normalized newforms f_1, f_2 and f_3 in $S_2(\Gamma_0(D))^{\mathrm{new}}$. Let f_1 be such that $A_1 := A_{f_1}$ is isogenous over $\mathbb{Q}$ to $\mathrm{Jac}(X^{(u)})$. Let A_2 be the optimal quotient of A_3 such that it is isogenous over $\mathbb{Q}$ to $\mathrm{Jac}(X^{(v)})$. For $D \neq 57$, $A_2 = A_{f_2}$ and f_3 is the Galois conjugate of f_2. For $D = 57$, A_2 is isogenous over $\mathbb{Q}$ to the product $A_{f_2} \times A_{f_3}$, where A_{f_2} and A_{f_3} are non-isogenous elliptic curves over $\mathbb{Q}$ of conductor 57.

Due to the fact that D is the product of two primes p_1 and p_2, $X_0(D)$ has exactly 4 cusps: 0, $1/p_1$, $1/p_2$ and ∞. Since D is square-free, all of them are rational points and the following cuspidal divisors

$$D_\infty = (0) - (\infty), \quad D_{p_1} = (0) - (1/p_1), \quad D_{p_2} = (0) - (1/p_2)$$

are torsion points in $\mathrm{Jac}(X_0(D))(\mathbb{Q})$ because a multiple of each of them is the divisor of a function in $\mathbb{Q}(X_0(D))$ obtained as product of integer powers of η-functions (for instance, see [**3**]). Hence, they generate a finite subgroup $\mathcal{G}$ of $\mathrm{Jac}(X_0(D))(\mathbb{Q})$ and each element of $\mathcal{G}$ provides a rational torsion point in any quotient of $\mathrm{Jac}(X_0(D))$ defined over $\mathbb{Q}$ that will be denoted using the same notation. Let $\mathcal{G}_3$, $\mathcal{G}_2$ and $\mathcal{G}_1$ be the groups generated by all these divisors in A_3, A_2 and A_1 respectively. We can view $\mathcal{G}_i$ as a finite subgroup of $H_1(A_i, \mathbb{Z}) \otimes \mathbb{Q}/H_1(A_i, \mathbb{Z})$. By fixing a basis of regulars differentials of A_i, we can determine the groups $\mathcal{G}_3$, $\mathcal{G}_2$ and $\mathcal{G}_1$. In Table 6 of the Appendix, we present a description of all of them.

In our strategy to determine a subgroup $c(D)$ of $\mathcal{G}_3$ such that $\mathrm{Jac}(X_0(D))^{\mathrm{new}}/c(D)$ is $\mathrm{Jac}(X_D)$, an important ingredient is finding a subgroup $\mathcal{G}'$ of $\mathcal{G}_2$ such that $A_2/\mathcal{G}'$ is

the jacobian of a genus two curve defined over $\mathbb{Q}$. To do that, we will need to have a polarization on A_2 defined over $\mathbb{Q}$ to apply the procedure used in [**4**]. In order to get such a polarization, we will proceed as follows. We will determine the abelian subvariety A_2' of $\mathrm{Jac}(X_0(D))$ isogenous over $\mathbb{Q}$ to A_2 and stable under Hecke operators. Hence, $\pi(A_2') = A_2$, where $\pi : \mathrm{Jac}(X_0(N)) \to A_2$ is the natural projection. The action of the Riemann form corresponding to the canonical polarization on $\mathrm{Jac}(X_0(D))$ restricted to $H_1(A_2', \mathbb{Z})$ provides a polarization on A_2' defined over $\mathbb{Q}$. Determining $\pi_*^{-1}(H_1(A_2, \mathbb{Z}))$ as a subgroup of $H_1(A_2', \mathbb{Z}) \otimes \mathbb{Q}$, we will obtain a polarization on A_2 defined over $\mathbb{Q}$.

Theorem 5.1. *With the above notation, there is a subgroup $c(D)$ of $\mathcal{G}_3$ which is the kernel of an isogeny $\Phi : \mathrm{Jac}(X_0(D))^{\mathrm{new}} \longrightarrow \mathrm{Jac}(X_D)$ defined over $\mathbb{Q}$. The following table shows $c(D)$ for each of these values D:*

D	$2 \cdot 31$	$2 \cdot 41$	$2 \cdot 47$	$3 \cdot 13$	$3 \cdot 17$	$3 \cdot 19$	$3 \cdot 23$	$5 \cdot 7$	$5 \cdot 11$
$c(D)$	$\langle 3D_\infty \rangle$	$\langle D_\infty \rangle$	$\langle D_\infty \rangle$	$\langle 4D_\infty \rangle$	$\langle 4D_\infty \rangle$	$\mathcal{G}_3$	$\mathcal{G}_3$	$\langle 12D_\infty \rangle$	$\{0\}$
$\lvert c(D) \rvert$	8	7	4	7	3	20	8	2	1

Proof. Let $\{h_1, h_2, h_3\}$ be a basis of $S_2(\Gamma_0(D))^{\mathrm{new}}$ with rational q-expansion such that $h_1 = f_1$ and $\{h_2, h_3\}$ is a basis of the vector space generated by f_2 and f_3. Let $\Omega_{c(D)}$ be a period matrix for $\mathrm{Jac}(X_0(D))^{\mathrm{new}}/c(D)$ corresponding to this basis and a basis of the $\mathbb{Z}$-module $H_1(A_3, \mathbb{Z}) + \mathbb{Z}\, c(D) \subseteq H_1(A_3, \mathbb{Z}) \otimes \mathbb{Q}$, where $c(D)$ is as in the statement. For a fixed basis of $\Omega^1_{X_D/\mathbb{Q}}$, let us denote by Ω_{sh} a period matrix for $\mathrm{Jac}(X_D)$ with respect this basis. The statement amounts to prove that there are two matrices $C \in GL_3(\mathbb{Q})$ and $M \in GL_6(\mathbb{Z})$ satisfying

$$\Omega_{c(D)} \cdot M = C \cdot \Omega_{sh}. \tag{9}$$

For X_D, we take the equation $y^2 = f(x)$ given in Table 5 of Theorem 4.5. Let $Z^2 = F(X)$ and $Y^2 = H(X)$ be the corresponding equations presented for $X^{(u)}$ and $X^{(v)}$ respectively in Table 4 of Proposition 4.4. For any subgroup $\mathcal{G}_3'$ of $\mathcal{G}_3$, let us denote by $\mathcal{G}_2'$ and $\mathcal{G}_1'$ its projections in $\mathcal{G}_2$ and $\mathcal{G}_1$ respectively.

Since the proof will be done computationally, we have to take care with mistakes coming from numerical approximations. For this reason, our procedure is based on the two following facts. On the one hand, we shall determine a quotient of A_2 by a subgroup of $\mathcal{G}_2$ which is the jacobian of a genus two curve $\mathcal{C}$ defined over $\mathbb{Q}$. This fact allows us to find the explicit isogeny between $\mathrm{Jac}(\mathcal{C})$ and $\mathrm{Jac}(X^{(v)})$. On the other hand, to compute Ω_{sh} we shall choose the following basis of $\Omega^1_{X_D/\mathbb{Q}}$:

$$\{\omega_1, \omega_2, \omega_3\} = \{\pi_u^*(dX/Z), \pi_v^*(dX/Y), \pi_v^*(X\, dX/Y)\}.$$

In thus way, the matrix C as in (9) should be of the following form

$$C = \begin{pmatrix} * & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix} \in GL_3(\mathbb{Q}).$$

We sketch the proof by splitting the procedure used in the following steeps:

(i) Compute period matrices Ω_3, Ω_2 and Ω_1 for A_3, A_2 and A_1 with respect the bases $\{h_1(q)d/q, h_2(q)dq/q, h_3(q)dq/q\}$, $\{h_2(q)dq/q, h_3(q)dq/q\}$ and $h_1(q)dq/q$ respectively.

(ii) For every $i \leq 3$, determine the coordinates of D_∞, D_{p_1} and D_{p_2} with respect the bases of the homologies $H_1(A_i, \mathbb{Z})$ used for computing the period matrices Ω_i, $1 \leq i \leq 3$.

(iii) Find a subgroup $\mathcal{G}'$ of $\mathcal{G}_2$ such that $A' = A_2/\mathcal{G}'$ has an irreducible principal polarization over $\mathbb{Q}$. Take a basis for $\mathcal{G}' + H_1(A_2, \mathbb{Z})$ and let Ω'_2 be a period matrix with respect this basis and the same basis of regular differentials used to compute the matrix Ω_2. Following the procedure used in 4.6 of [**4**], compute a genus two curve $\mathcal{C} : y^2 = r(x)$ such that $\mathrm{Jac}(\mathcal{C}) = A'$ (if possible, take $\mathcal{G}'$ such that $\mathcal{C}$ is isomorphic over $\mathbb{Q}$ to $X^{(v)}$). Observe that using this procedure, the matrix Ω'_2 is a matrix period for $\mathrm{Jac}(\mathcal{C})$ with respect the basis $\{dx/y, x\,dx/y\}$. For instance,

D	$\mathcal{G}'$	$\mathcal{C}$
$2 \cdot 31$	$\{0\}$	$y^2 = (2+x)(10 - x + 24\,x^2 - 21\,x^3 + 8\,x^4)$
$2 \cdot 41$	$\langle D_\infty \rangle$	$y^2 = -3(2+x^2)(1549 + 1576\,x + 1032\,x^2 - 32\,x^3 + 16\,x^4)$
$2 \cdot 47$	$\{0\}$	$y^2 = -x(-1+3\,x)(8 - 27\,x + 45\,x^2 - 24\,x^3 + 4\,x^4)$
$3 \cdot 13$	$\{0\}$	$y^2 = (1+2\,x)(3+2\,x)(3+5\,x+x^2)(1+3\,x+3\,x^2)$
$3 \cdot 17$	$\langle 2D_\infty \rangle$	$y^2 = (1+2\,x)(5+7\,x)(7+10\,x)(51 + 255\,x + 421\,x^2 + 229\,x^3)$
$3 \cdot 19$	$\langle 5D_\infty, D_{19} \rangle$	$y^2 = 2(-4+x)(-1+x)(4+5\,x)(-2 - 2\,x + x^3)$
$3 \cdot 23$	$\langle D_3 \rangle$	$y^2 = -(1+4\,x+x^2)(1+14\,x+43\,x^2+6\,x^3+9\,x^4)$
$5 \cdot 7$	$\langle 2D_\infty \rangle$	$y^2 = -(1+2\,x)(3+2\,x)(1+3\,x)(5+25\,x+43\,x^2+19\,x^3)$
$5 \cdot 11$	$\{0\}$	$y^2 = -x(-1+3\,x)(8 - 27\,x + 45\,x^2 - 24\,x^3 + 4\,x^4)$

(iv) Compute a period matrix Ω_{sh2} for $X^{(v)}$ with respect the basis $dX/Y, X\,dX/Y$ and determine a matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$ for which there exists a matrix $M_2 \in M_4(\mathbb{Z})$ such that

$$\Omega'_2 \cdot M_2 = A \cdot \Omega_{sh2}.$$

In order to do that, we can use the instruction *IsIsogenousPeriodMatrices* of the program *MAGMA* to determine these matrices. When $\mathcal{C}$ is isomorphic to X_v, the explicit isomorphism between both curves provides the matrices A and M_2.

(v) Let $\mathcal{G}'_3$ be a subgroup of $\mathcal{G}_3$ such that $\mathcal{G}'_2 = \mathcal{G}'$. Let Ω'_1 be a period matrix of $A_1/\mathcal{G}'_1$ with respect the basis $h_1(q)dq/q$. Compute a period matrix Ω_{sh1} for $X^{(u)}$ with respect dX/Z and determine a rational m for which there exists a matrix $M_1 \in M_2(\mathbb{Z})$ such that

$$\Omega'_1 \cdot M_1 = m \cdot \Omega_{sh1}.$$

(vi) Compute a period matrix Ω_{sh} with respect to the basis $\omega_1 = \pi_u^*(dX/Z), \omega_2 = \pi_v^*(dX/Y), \omega_3 = \pi_v^*(X\,dX/Y)$ of $\Omega^1(X_D)$. Observe that for $D \neq 57, 82$, one has that

$$(\omega_1, \omega_2, \omega_3) = \begin{cases} (2xdx/y, 2dx/y, 2x^2dx/y) & \text{if } D \in \{35, 51, 62, 69, 94\}, \\ ((x^2+1)dx/y, xdx/y, (x^2-1)dx/y) & \text{if } D \in \{39, 55\}. \end{cases}$$

For $D = 57, 82$, we have that $H(X) = e(X^2+\alpha)F(X)$ and $Y = Z\,t$. Setting $u = t/(X + \sqrt{-\alpha})$, with the change

$$X = -\sqrt{-\alpha}\,\frac{u^2+e}{u^2-e}, \quad z = \frac{(u^2-e)^3\,Z\,t}{u},$$

we obtain the hyperelliptic model defined over $\mathbb{Q}(\sqrt{-\alpha})$ for $X^{(v)}$

$$z^2 = f(u) = \frac{(u^2-e)^6}{u^2} H\bigg(-\sqrt{-\alpha}\,\frac{u^2+e}{u^2-e}\bigg),$$

which allows us to compute a matrix period for this equation with respect the basis of regular differentials $\{du/z, u\,du/z, u^2\,du/z\}$. In this case

$$(\omega_1, \omega_2, \omega_3) = \bigg(8\,e^2\,\alpha\,\frac{u\,du}{z},\, 4\,e\sqrt{-\alpha}\bigg(\frac{u^2\,du}{z} - e\,\frac{du}{z}\bigg),\, 4\,e\,\alpha\bigg(\frac{u^2\,du}{z} + e\,\frac{du}{z}\bigg)\bigg).$$

(vii) Determine an integer λ for which there is a matrix $M' \in M_6(\mathbb{Z})$ such that

$$\Omega_{c(D)} \cdot M' = \lambda \cdot A' \cdot \Omega_{sh}, \quad \text{where } A' = \begin{pmatrix} m & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}.$$

(viii) By using the Hermite decomposition of the matrix M' and the action of $\mathrm{End}_{\mathbb{Q}}(A_3/c(D))$ on $\Omega_{c(D)}$, we can find an endomorphism $\phi \in \mathrm{End}_{\mathbb{Q}}(A_3/c(D))$ whose action on the basis $\{h_1, h_2, h_3\}$ is given by a matrix $B \in GL_2(\mathbb{Q})$ and for which

$$B \cdot \Omega_{c(D)} \cdot M = \Omega_{c(D)} \cdot M',$$

for some $M \in GL_6(\mathbb{Z})$. Finally, putting $C = \lambda \cdot B^{-1} \cdot A'$ we obtain that

$$\Omega_{c(D)} \cdot M = C \cdot \Omega_{sh}.$$

In Table 7 of the Appendix, we show the cusp forms h_2 and h_3 used in our computation, by giving the first terms of their q-expansions, and the matrix C obtained. The matrix M is omitted, since it depends on the chosen bases for the homologies of $\mathrm{Jac}(X_0(D))^{\mathrm{new}}/c(D)$ and $\mathrm{Jac}(X_D)$. □

6. Appendix.

Table 6.

D	$\mathcal{G}_3$	$\mathcal{G}_2$	$\mathcal{G}_1$
$2 \cdot 31$	$\mathbb{Z}/24\mathbb{Z}$ $24D_\infty = 8D_2 = 3D_{31} = 0$ $8D_\infty + D_{31} = 0$ $9D_\infty - D_2 = 0$	$\mathbb{Z}/6\mathbb{Z}$ $6D_\infty = 2D_2 = 3D_{31} = 0$ $2D_\infty + D_{31} = 0$ $3D_\infty + D_2 = 0$	$\mathbb{Z}/4\mathbb{Z}$ $4D_\infty = D_{31} = 0$ $D_\infty = D_2$
$2 \cdot 41$	$\mathbb{Z}/7\mathbb{Z}$ $7D_\infty = 7D_2 = D_{41} = 0$ $D_\infty = D_2$	$\mathbb{Z}/7\mathbb{Z}$ $7D_\infty = 7D_2 = D_{41} = 0$ $D_\infty = D_2$	$\{0\}$
$2 \cdot 47$	$\mathbb{Z}/4\mathbb{Z}$ $4D_\infty = 4D_2 = D_{47} = 0$ $D_\infty = D_2$	$\mathbb{Z}/2\mathbb{Z}$ $2D_\infty = 0$ $D_\infty = D_2$	$\mathbb{Z}/2\mathbb{Z}$ $2D_\infty = 0$ $D_\infty = D_2$
$3 \cdot 13$	$\mathbb{Z}/28\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $28D_\infty = 14D_3 = 4D_{13} = 0$ $12D_\infty + 2D_3 = 0$ $14D_\infty - 2D_{13} = 0$	$\mathbb{Z}/14\mathbb{Z}$ $14D_\infty = 7D_2 = 2D_{13} = 0$ $6D_\infty + D_3 = 0$ $7D_\infty - D_{13} = 0$	$\mathbb{Z}/2\mathbb{Z}$ $2D_\infty = 0$ $D_3 = 0$ $D_\infty = D_{13}$
$3 \cdot 17$	$\mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $12D_\infty = 6D_3 = 4D_{17} = 0$ $3D_\infty + 3D_3 + D_{17} = 0$ $4D_\infty + 2D_3 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $4D_\infty = 4D_{17} = 2D_3 = 0$ $D_\infty + D_3 - D_{17} = 0$ $2D_\infty + 2D_{17} = 0$	$\mathbb{Z}/3\mathbb{Z}$ $3D_\infty = 0$ $D_\infty = D_3$ $D_{17} = 0$
$3 \cdot 19$	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $10D_\infty = 10D_3 = 2D_{19} = 0$ $D_\infty - D_3 - D_{19} = 0$	$\mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $10D_\infty = 10D_3 = 2D_{19} = 0$ $D_\infty - D_3 - D_{19} = 0$	$\{0\}$
$3 \cdot 23$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $4D_\infty = 4D_3 = D_{23} = 0$ $2D_\infty + 2D_3 = 0$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $2D_\infty = 2D_3 = 0$	$\mathbb{Z}/2\mathbb{Z}$ $2D_\infty = 0$ $D_\infty = D_3$
$5 \cdot 7$	$\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $24D_\infty = 8D_5 = 6D_7 = 0$ $6D_\infty + 2D_5 = 0$ $16D_\infty + 2D_7 = 0$	$\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2Z$ $8D_\infty = 8D_5 = 2D_7 = 0$ $2D_\infty - 2D_5 = 0$ $D_\infty - D_5 + D_7 = 0$	$\mathbb{Z}/3\mathbb{Z}$ $3D_\infty = 0$ $D_\infty = D_7$ $D_5 = 0$
$5 \cdot 11$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ $4D_\infty = 4D_5 = 2D_{11} = 0$ $D_\infty - D_5 - D_{11} = 0$	$\mathbb{Z}/2Z$ $2D_\infty = D_{11} = 0$ $D_\infty = D_5$	$\mathbb{Z}/3\mathbb{Z}$ $2D_\infty = D_{11} = 0$ $D_\infty = D_5$

Table 7.

D	h_2	h_3	C
$2\cdot 31$	$q^3+\cdots$	$q-q^2+q^3+\cdots$	$\frac{1}{2}\begin{pmatrix}1&0&0\\0&-1&-1\\0&1&-1\end{pmatrix}$
$2\cdot 41$	$q+q^2+q^4+\cdots$	$q^3+\cdots$	$\frac{1}{36}\begin{pmatrix}-3&0&0\\0&6&8\\0&15&22\end{pmatrix}$
$2\cdot 47$	$q-q^2+q^4+\cdots$	$2q^3-q^5+\cdots$	$\frac{1}{4}\begin{pmatrix}1&0&0\\0&1&0\\0&3&-2\end{pmatrix}$
$3\cdot 13$	$q-q^2+q^3+\cdots$	$q^2-2q^4+\cdots$	$\begin{pmatrix}1&0&0\\0&-1&-1\\0&1&0\end{pmatrix}$
$3\cdot 17$	$q-q^3+\cdots$	$q^2-q^4+\cdots$	$\frac{1}{4}\begin{pmatrix}1&0&0\\0&-7&-10\\0&1&2\end{pmatrix}$
$3\cdot 19$	$q+q^2+q^3+\cdots$	$q-2q^2+q^3+\cdots$	$\frac{1}{6}\begin{pmatrix}3&0&0\\0&0&3\\0&4&-4\end{pmatrix}$
$3\cdot 23$	$q-q^3+\cdots$	$q^2-q^5+\cdots$	$\frac{1}{2}\begin{pmatrix}8&0&0\\0&13&-1\\0&5&-1\end{pmatrix}$
$5\cdot 7$	$q-q^3+\cdots$	$q^2-q^3+\cdots$	$\frac{1}{4}\begin{pmatrix}1&0&0\\0&-3&-2\\0&1&2\end{pmatrix}$
$5\cdot 11$	$q^2-2q^3+\cdots$	$q+2q^3+\cdots$	$\begin{pmatrix}1&0&0\\0&1&-2\\0&1&-3\end{pmatrix}$

References

[1] M. H. Baker, E. González-Jiménez, J. González and B. Poonen, Finiteness results for modular curves of genus at least 2, Amer. J. Math., **127** (2005), 1325–1387.

[2] H. Carayol, Sur les représentations l-adiques associées aux formes modulaires de Hilbert, Ann. Sci. École Norm. Sup. (4), **19** (1986), 409–468.

[3] J. Gonzàlez, Equations of hyperelliptic modular curves, Ann. Inst. Fourier (Grenoble), **41** (1991), 779–795.

[4] J. González, J. Guàrdia and V. Rotger, Abelian surfaces of GL_2-type as Jacobians of curves, Acta Arith., **116** (2005), 263–287.

[5] J. González and V. Rotger, Equations of Shimura curves of genus two, Int. Math. Res. Not., 2004, No. 14, 661–674.

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

[7] K. Győry, Sur les polynômes à coefficients entiers et de discriminant donné, III, Publ. Math. Debrecen, **23** (1976), 141–165.

[8] A. Kontogeorgis and V. Rotger, On the non-existence of exceptional automorphisms on Shimura

curves, Bull. Lond. Math. Soc., **40** (2008), 363–374.
[9] A. Kurihara, On p-adic Poincaré series and Shimura curves, Internat. J. Math., **5** (1994), 747–763.
[10] Q. Liu, Conducteur et discriminant minimal de courbes de genre 2, Compositio Math., **94** (1994), 51–79.
[11] Q. Liu, Algebraic geometry and arithmetic curves, **6**, Oxford Graduate Texts in Mathematics, Oxford University Press, Oxford, 2002. Translated from the french by Reinie Erné, Oxford Science Publications.
[12] S. Molina, Equations of hyperelliptic Shimura curves, Proc. Lond. Math. Soc. (3), **105** (2012), 891–920.
[13] S. Molina, Ribet bimodules and the specialization of Heegner points, Israel J. Math., **189** (2012), 1–38.
[14] A. P. Ogg, Real points on Shimura curves, In: Arithmetic and geometry, Vol. I, **35**, Progr. Math., Birkhäuser Boston, Boston, MA, 1983, 277–307.
[15] A. P. Ogg, Mauvaise réduction des courbes de Shimura, In: Séminaire de théorie des nombres, Paris 1983–84, **59**, Progr. Math., Birkhäuser Boston, Boston, MA, 1985, 199–217.
[16] K. Ribet, Sur les variétés abéliennes à multiplications réelles, C. R. Acad. Sci. Paris Sér. A-B, **291** (1980), A121–A123.
[17] V. Rotger, On the group of automorphisms of Shimura curves and applications, Compositio Math., **132** (2002), 229–241.
[18] G. Shimura, On the real points of an arithmetic quotient of a bounded symmetric domain, Math. Ann., **215** (1975), 135–164.

Josep González
Universitat Politècnica de Catalunya
Departament de Matemàtica Aplicada IV (EPSVG)
Av. Victor Balaguer s/n
08800 Vilanova i la Geltrú
Spain
E-mail: josepg@ma4.upc.edu

Santiago Molina
Centre de Recerca Matemàtica
Campus de Bellaterra
Edifici C 08193 Bellaterra (Barcelona)
Office 21 (C3b/024)
Spain
E-mail: smolina@crm.cat