# RATIONAL POINTS ON TWISTS OF $X_0(63)$

NILS BRUIN, JULIO FERNÁNDEZ, JOSEP GONZÁLEZ, AND JOAN-C. LARIO

ABSTRACT. Let $\varrho : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$ be a Galois representation with cyclotomic determinant, and let $N > 1$ be an integer that is square mod $p$. There exist two twisted modular curves $X^+(N,p)_\varrho$ and $X^+(N,p)'_\varrho$ defined over $\mathbb{Q}$ whose rational points classify the quadratic $\mathbb{Q}$-curves of degree $N$ realizing $\varrho$. The paper focuses on the only genus-three instance: the case $N = 7$, $p = 3$. From an explicit description of the automorphism group of the modular curve $X_0(63)$, it follows that the twisted curves are isomorphic over $\mathbb{Q}$ in this case. We also obtain a plane quartic equation for the twists and then produce the desired $\mathbb{Q}$-curves, provided that the set of rational points on this quartic can be determined. The existence of elliptic quotients and of an unramified double cover $X(7,3)_\varrho$ having a genus-two quotient permits a variety of combinations of covers and Prym-Chabauty methods to determine these rational points. We include two examples where these methods apply.

## 1. INTRODUCTION

Let $p$ be an odd prime and $\varrho : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$ be a representation of the absolute Galois group of $\mathbb{Q}$. One says that a $\mathbb{Q}$-curve $E$ *realizes* $\varrho$ if this representation is isomorphic to the odd projective representation of $\mathrm{G}_{\mathbb{Q}}$ arising from the $p$-torsion subgroup of $E$, as explained in [ES01], [FLR02] or [Fer04].

The moduli problem classifying the $\mathbb{Q}$-curves that realize $\varrho$ splits into two different cases, cyclotomic and non-cyclotomic, according to the determinant of $\varrho$. For a given integer $N > 1$ prime to $p$, let us consider the non-CM $\mathbb{Q}$-curves realizing $\varrho$ which are defined over a quadratic field and have a cyclic isogeny of degree $N$ to its Galois conjugate. In this case, the cyclotomic condition amounts to asking that $N$ be a square mod $p$. Moreover, such $\mathbb{Q}$-curves are given by the rational points on either a twist of a certain modular curve $X(N,p)$ in the non-cyclotomic case, or on two twists of a degree-two quotient $X^+(N,p)$ in the cyclotomic case (cf. [Fer04]).

The octahedral cases $X(5,3)$ and $X^+(7,3)$ cover all genus-three instances for the moduli problem under consideration. Slightly different arguments to those employed in [FGL] for the non-cyclotomic case $X(5,3)$ enable us here to deal with the cyclotomic case $X^+(7,3)$, and yet this second case presents new important features. Indeed, $X^+(7,3)$ has an unramified double cover isomorphic to the modular curve $X_0(63)$. The structure of the automorphism group of this curve was suggested by Kenku and Momose in [KM88] and then established by Elkies in [Elk90]. Here we give an explicit description for this automorphism group; as an application, we show

*Date*: February 7, 2006.

*Key words and phrases.* Galois representations, elliptic curves, genus-three curves, Prym varieties, Chabauty methods, quadratic $\mathbb{Q}$-curves.

The first author is partially supported by an NSERC grant. The second and fourth authors are partially supported by DGICYT Grant BFM2003-06768-C02-01. The third author is partially supported by DGICYT Grant BFM2003-06768-C02-02.

that the two twisted curves admit the same model $X^+(7,3)_\varrho$ over $\mathbb{Q}$. With the aim of finding the rational points on this curve, we construct a genus-one quotient $E_\varrho$ defined over a cubic field. Furthermore, the existence of an unramified double cover $X(7,3)_\varrho$ allows us to translate our problem into finding the rational points on a finite number of explicit twists $X(7,3)_{\varrho,\,m}$. This configuration is dealt with in general in [Bru04]. However, in this particular setting, it turns out that $X(7,3)_{\varrho,\,m}$ actually covers a genus-two curve $\widetilde{C}_{\varrho,\,m}$. We can then use for our purposes a wide variety of methods to determine the rational points on curves of genus two.

The plan of the paper is as follows. Section 2 summarizes the construction of the modular curves $X(N,p)$, $X^+(N,p)$ and their twists by $\varrho$ in the cyclotomic case. In Section 3 we obtain a rational model for $X_0(63)$ as an unramified double cover of $X_0(63)/\langle w_7\rangle$, and provide a description for the automorphism groups of these curves. In Section 4 we make explicit $X^+(7,3)$ as a cover of the modular curve $X^+(7) = X_0(7)/\langle w_7\rangle$, which is needed later on to exhibit the quadratic $\mathbb{Q}$-curves of degree 7 realizing a given surjective representation $\varrho : \mathrm{G}_\mathbb{Q} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3)$. The study of the twisted curve $X^+(7,3)_\varrho$ is accomplished in Section 5. We develop a method to retrieve, from a degree-four polynomial in $\mathbb{Z}[X]$ having the same splitting field as $\varrho$, a plane quartic model for $X^+(7,3)_\varrho$ along with a rational model for its double cover $X(7,3)_\varrho$. We also determine morphisms $X^+(7,3)_\varrho \longrightarrow E_\varrho$ and $X(7,3)_\varrho \longrightarrow \widetilde{C}_\varrho$, where $E_\varrho$ and $\widetilde{C}_\varrho$ are curves of genus one and two, respectively. This allows us to use a combination of covers and Chabauty methods to determine all rational points on $X^+(7,3)_\varrho$ and, therefore, all $\mathbb{Q}$-curves of degree 7 realizing $\varrho$. In Section 6 we present two complete examples where these methods do apply.

## 2. Twisting the modular curves $X(N,p)$ and $X^+(N,p)$

Let $N > 1$ be an integer prime to $p$. We denote by $X(N,p)$ the fiber product over $X(1)$ of the modular curves $X_0(N)$ and $X(p)$. We take for $X_0(N)$ its canonical model over $\mathbb{Q}$. As for $X(p)$, we fix the rational model attached to a matrix $V$ in $\mathrm{PGL}_2(\mathbb{F}_p) \setminus \mathrm{PSL}_2(\mathbb{F}_p)$ of order 2, as a particular case of a general procedure that can be found in Section II.3 of [Lig77] or Section 2 of [Maz77]. Its $\mathbb{Q}$-isomorphism class does not depend on the choice of such a matrix. Let also $X^+(N)$ be the quotient of $X_0(N)$ by the Atkin-Lehner involution $w_N$. We recall that the non-cuspidal non-CM rational points on $X^+(N)$ parametrize the isomorphism classes of *quadratic $\mathbb{Q}$-curves of degree $N$*. By this term we mean, for simplicity, the $\mathrm{G}_\mathbb{Q}$-stable pairs of non-CM elliptic curves related by a cyclic isogeny of degree $N$.

From now on, we assume $N$ to be a square mod $p$. The automorphism group of the cover $X(N,p) \longrightarrow X^+(N)$ is then seen to be canonically isomorphic to $\mathrm{PSL}_2(\mathbb{F}_p) \times \mathbb{Z}/2\,\mathbb{Z}$. Put $w$ for the involution of $X(N,p)$ corresponding to the non-trivial element in the center of this group, and denote by $X^+(N,p)$ the quotient curve. The automorphism group, call it $\mathcal{G}(N,p)$, of the cover

$$X^+(N,p) \longrightarrow X^+(N)$$

is thus canonically isomorphic to $\mathrm{PSL}_2(\mathbb{F}_p)$. Through the identification of the automorphisms of this group with the elements in $\mathrm{PGL}_2(\mathbb{F}_p)$, the Galois action on $\mathcal{G}(N,p)$ is given by the morphism

$$\varepsilon : \mathrm{G}_\mathbb{Q} \longrightarrow \mathbb{F}_p^*/\,\mathbb{F}_p^{*2} \simeq \langle V\rangle$$

obtained from the mod $p$ cyclotomic character $\mathrm{G}_\mathbb{Q} \longrightarrow \mathbb{F}_p^*$.

Suppose that we are now given a surjective Galois representation

$$\varrho : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$$

with cyclotomic determinant. For the moduli classification of quadratic $\mathbb{Q}$-curves of degree $N$ realizing $\varrho$, we produce two twists of $X^+(N,p)$ from certain elements in the cohomology set $H^1(\mathrm{G}_{\mathbb{Q}}, \mathcal{G}(N,p))$. Specifically, we consider the 1-cocycles $\xi = \varrho\,\varepsilon$ and $\xi' = V\,\xi\,V$, where we use the identification of $\mathrm{PSL}_2(\mathbb{F}_p)$ with $\mathcal{G}(N,p)$. For the two twists of $X(N,p)$ attached to $\xi$ and $\xi'$, respectively, we fix rational models $X^+(N,p)_\varrho$ and $X^+(N,p)'_\varrho$ along with isomorphisms

$$\Psi : X^+(N,p)_\varrho \longrightarrow X^+(N,p)$$
$$\Psi' : X^+(N,p)'_\varrho \longrightarrow X^+(N,p)$$

satisfying $\Psi = \xi_\sigma\, {}^\sigma\Psi$ and $\Psi' = \xi'_\sigma\, {}^\sigma\Psi'$ for every $\sigma$ in $\mathrm{G}_{\mathbb{Q}}$. We note that the $\mathbb{Q}$-isomorphism class of each of these twists only depend on the splitting field of $\varrho$.

**Theorem 2.1.** [Fer04] *There exists a quadratic $\mathbb{Q}$-curve of degree $N$ realizing $\varrho$ if and only if the set of non-cuspidal non-CM rational points on the curves $X^+(N,p)_\varrho$ and $X^+(N,p)'_\varrho$ is not empty. In this case, the compositions*

$$X^+(N,p)_\varrho \xrightarrow{\Psi} X^+(N,p) \longrightarrow X^+(N)$$
$$X^+(N,p)'_\varrho \xrightarrow{\Psi'} X^+(N,p) \longrightarrow X^+(N)$$

*define a one-to-one correspondence between this set of rational points and the set of isomorphism classes of quadratic $\mathbb{Q}$-curves of degree $N$ realizing $\varrho$.*

Through the embedding $\mathcal{G}(N,p) \hookrightarrow \mathrm{Aut}\,(X(N,p))$, the 1-cocycle $\xi$ defining the twist $X^+(N,p)_\varrho$ extends to a 1-cocycle of $\mathrm{G}_{\mathbb{Q}}$ with values in $\mathrm{Aut}\,(X(N,p))$. Denote by $X(N,p)_\varrho$ the corresponding twist of $X(N,p)$. We have a commutative diagram

$$\begin{array}{ccc} X(N,p)_\varrho & \xrightarrow{\Psi} & X(N,p) \\ \downarrow & & \downarrow \\ X^+(N,p)_\varrho & \xrightarrow{\Psi} & X^+(N,p) \end{array}$$

where the vertical arrows are $\mathbb{Q}$-rational double covers; the left one corresponds to the quotient by the involution $\Psi^{-1} w\, \Psi$, which is defined over $\mathbb{Q}$.

For a nonzero integer $m$, let $X(N,p)_{\varrho,\,m}$ denote the quadratic twist of $X(N,p)_\varrho$ defined by the 1-cocycle

$$\chi_m : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{Gal}\left(\mathbb{Q}(\sqrt{m}\,)/\mathbb{Q}\right) \simeq \langle \Psi^{-1} w\, \Psi \rangle.$$

We have then a $\mathbb{Q}$-rational double cover

$$X(N,p)_{\varrho,\,m} \xrightarrow{\varphi_m} X(N,p)_\varrho \longrightarrow X^+(N,p)_\varrho\,,$$

where the isomorphism $\varphi_m$ is defined over $\mathbb{Q}(\sqrt{m}\,)$ and is sent by the Galois conjugation of this quadratic field to $\Psi^{-1} w\, \Psi\, \varphi_m$.

Attached to the 1-cocycle $\xi'$, one has analogous twists $X(N,p)'_\varrho$ and $X(N,p)'_{\varrho,\,m}$. Theorem 2.1 can then be refined in the following way.

**Theorem 2.2.** [Fer04] *The isomorphism classes of quadratic $\mathbb{Q}$-curves of degree $N$ realizing $\varrho$ and with field of moduli $\mathbb{Q}(\sqrt{m}\,)$ are in bijection with the non-cuspidal non-CM rational points on the curves $X^+(N,p)_\varrho$ and $X^+(N,p)'_\varrho$ lifting to rational points on $X(N,p)_{\varrho,\,m}$ and $X(N,p)'_{\varrho,\,m}$, respectively.*

**Proposition 2.1.** *The genus of $X^+(N,p)$ is at least three. The genus is three only for $N=7$ and $p=3$.*

*Proof.* The involution $w$ restricts to the Atkin-Lehner involution $w_N$ on $X_0(pN)$, thus inducing a cover $X^+(N,p) \longrightarrow X_0(pN)/\langle w_N\rangle$, whose degree is $p\,(p-1)/2$. This map ramifies with index $p$ above $\lceil \nu_\infty/2\rceil$ cusps, where $\nu_\infty$ is the number of cusps of $X_0(N)$. So the Hurwitz formula yields

$$2\,(g^+-1) \;\geq\; p\,(p-1)(g-1) \,+\, \left\lceil \frac{\nu_\infty}{2} \right\rceil \frac{(p-1)^2}{2}\,,$$

where $g^+$ and $g$ stand for the genera of $X^+(N,p)$ and $X_0(pN)/\langle w_N\rangle$, respectively. If $g^+$ is at most three, it follows that either $g=0$ or $p=3$ and $g=1$. Now, the only pairs $(N,p)$, with $N$ prime to $p$ and square mod $p$, satisfying one of these two conditions are $(4,3)$, $(4,5)$ and $(7,3)$. Indeed, it suffices to check among the modular curves $X_0(pN)$ which have genus $\leq 1$ or are hyperelliptic [Ogg74] or bielliptic [Bar99]. The curves $X^+(4,3)$ and $X^+(4,5)$ have genera zero and four, respectively (see Proposition 5.7 in [Fer04]). As for $X^+(7,3)$, the genus can be obtained from the Hurwitz formula applied to the degree-twelve Galois cover $X^+(7,3) \longrightarrow X^+(7)$, whose ramification points are those lying above the cusp, the elliptic point with $j$-invariant 0 and the two points of $X_0(7)$ fixed by $w_7$. □

From now on, we assume $p=3$. The function field of $X(N,3)$ over $\mathbb{Q}$ can be taken to be the field of modular functions for $\Gamma_0(N)\cap\Gamma(3)$ with rational Fourier coefficients, so that the automorphism of the complex upper-half plane given by $\tau\mapsto\tau/3$ induces an isomorphism

$$\Phi : X(N,3) \longrightarrow X_0(9N)$$

defined over $\mathbb{Q}$. Moreover, the above involution $w$ corresponds through $\Phi$ to the Atkin-Lehner involution $w_N$ of $X_0(9N)$, so that we have an induced isomorphism

$$\Phi : X^+(N,3) \longrightarrow X_0(9N)/\langle w_N\rangle.$$

The following result highlights the special behaviour of the automorphism group of this curve for $N=7$, thus complementing Proposition 2.1. Note that there is an isomorphism between $\mathrm{PGL}_2(\mathbb{F}_3)$ and the symmetric group $\mathcal{S}_4$ unique up to conjugation; in particular, the cover group $\mathcal{G}(N,3)$ is isomorphic to the alternating group $\mathcal{A}_4$.

**Proposition 2.2.** *For a prime $N\equiv 1 \pmod 3$ different from 7,*

$$\mathrm{Aut}\,(X(N,3)) \,=\, \mathcal{G}(N,3)\,\times\,\langle w\rangle \,\simeq\, \mathcal{A}_4\,\times\,\mathbb{Z}/2\,\mathbb{Z},$$

*whereas* $\mathrm{Aut}\,(X(7,3)) \,\simeq\, \mathcal{S}_4\times\langle w\rangle$.

*Proof.* Let us first note that, under the hypotheses in the statement, the modular curve $X_0(9N)$ has genus greater than one. Its automorphism group has no other elements outside the normalizer $B(9N)$ of $\Gamma_0(9N)$ in $\mathrm{PSL}_2(\mathbb{R})$ unless $N=7$ (cf. [KM88], where two possibilities were given for this case). Moreover, the group $B(9N)$ is generated by the Atkin-Lehner involutions $w_9$, $w_N$ and the automorphism $S$ whose action on the complex upper-half plane is given by $\tau\mapsto\tau+1/3$. Since $N\equiv 1 \pmod 3$, an easy checking shows that $w_9$ and $S$ generate a subgroup isomorphic to $\mathcal{A}_4$ and commute with $w_N$. As for $X_0(63)$, the actual structure of its automorphism group was settled in [Elk90] (cf. Section 3 below). □

## 3. The modular curve $X_0(63)$ and its quotient by $w_7$

In this section we give a rational model for the genus-three curve $X_0(63)/\langle w_7\rangle$ and for its genus-five double cover $X_0(63)$. We also study the automorphism group of both curves. For future use, let us fix a basis $\{\omega_1,\dots,\omega_5\}$ for the vector space of regular differentials $\Omega^1(X_0(63))$ in the following way. Take

$$\omega_i \,=\, f_i(q)\,\frac{dq}{q}\,,$$

where $f_1$ is the normalized newform of level 21, $f_2(q) = f_1(q^3)$ and $f_3, f_4, f_5$ are the normalized newforms of level 63 :

$$f_1 = q-q^2+q^3-q^4-2\,q^5-q^6-q^7+3\,q^8+q^9-2\,q^{10}+4\,q^{11}-q^{12}-2\,q^{13}+q^{14}-2\,q^{15}-q^{16}+6\,q^{17}+\cdots$$

$$f_2 = q^3 - q^6 + q^9 - q^{12} - 2\,q^{15} - q^{18} - q^{21} + 3\,q^{24} + q^{27} - 2\,q^{30} + 4\,q^{33} - q^{36} + \cdots$$

$$f_3 = q + q^2 - q^4 + 2\,q^5 - q^7 - 3\,q^8 + 2\,q^{10} - 4\,q^{11} - 2\,q^{13} - q^{14} - q^{16} + 6\,q^{17} + \cdots$$

$$f_4 = q+\sqrt{3}\,q^2+q^4-2\,\sqrt{3}\,q^5+q^7-\sqrt{3}\,q^8-6\,q^{10}+2\sqrt{3}\,q^{11}+2\,q^{13}+\sqrt{3}\,q^{14}-5\,q^{16}+2\,\sqrt{3}\,q^{17}+\cdots$$

$$f_5 = q-\sqrt{3}\,q^2+q^4+2\,\sqrt{3}\,q^5+q^7+\sqrt{3}\,q^8-6\,q^{10}-2\sqrt{3}\,q^{11}+2\,q^{13}-\sqrt{3}\,q^{14}-5\,q^{16}-2\,\sqrt{3}\,q^{17}+\cdots$$

Note that $\omega_1, \omega_2, \omega_3$ are defined over $\mathbb{Q}$, while $\omega_4, \omega_5$ are Galois conjugates defined over $\mathbb{Q}(\sqrt{3}\,)$.

3.1. **A rational plane quartic model for $X_0(63)/\langle w_7\rangle$.** We start by observing that the pullback of $\Omega^1_{\mathbb{Q}}(X_0(63)/\langle w_7\rangle)$ by the projection $X_0(63) \longrightarrow X_0(63)/\langle w_7\rangle$ is the vector subspace of $\Omega^1_{\mathbb{Q}}(X_0(63))$ invariant by $w_7$, so that it is generated by the differential forms $\omega_1, \omega_2, \omega_3$. In particular, the Jacobian of $X_0(63)/\langle w_7\rangle$ is $\mathbb{Q}$-isogenous to $E_{21}^2 \times E_{63}$, where $E_{21}$ and $E_{63}$ are elliptic curves over $\mathbb{Q}$ of conductors 21 and 63, respectively.

**Proposition 3.1.** *The genus-three curve $X_0(63)/\langle w_7\rangle$ is nonhyperelliptic and admits an affine quartic model over $\mathbb{Q}$ given by*

$$x^4 - 8\,x^3\,y + 46\,x^2\,y^2 - 72\,x\,y^3 + 81\,y^4 - 2\,x^2 - 8\,x\,y - 18\,y^2 + 1 = 0, \tag{1}$$

*where $x = \omega_1/\omega_3$ and $y = \omega_2/\omega_3$. In particular, $\mathbb{Q}\,(X_0(63)/\langle w_7\rangle) \,=\, \mathbb{Q}(x, y)$.*

*Proof.* Let $X_{/\mathbb{C}}$ be a curve of genus at least two and $\phi : X_0(M) \longrightarrow X$ be a nonconstant morphism unramified at the cusp $\infty$. With the same arguments as in Proposition 6.5 of [BGGP05], it can be proved that $X$ is hyperelliptic if and only if part (3) of that proposition is satisfied for the vector subspace $S_2(A)$ of $S_2(\Gamma_0(M))$ such that $S_2(A)\,dq/q$ is the pullback of $\Omega^1(X)$ by $\phi$. In our case, the cover $X_0(63) \longrightarrow X_0(63)/\langle w_7\rangle$ is unramified and part (3) fails for $\langle f_1, f_2, f_3\rangle$, so the first assertion follows.

In view of this, the image of $X_0(63)/\langle w_7\rangle$ under the canonical embedding is the zero locus of a homogeneous polynomial $P$ in $\mathbb{Q}[X, Y, Z]$ of degree four. Such a polynomial is unique up to non-zero rational multiples and satisfies $P(\omega_1, \omega_2, \omega_3) = 0$. It can be explicitly determined using the first seventeen Fourier coefficients of each $\omega_i$ (cf. Section 2 of [BGGP05]). This yields the equation in the statement. □

3.2. **A rational model for the cover $X_0(63) \longrightarrow X_0(63)/\langle w_7\rangle$.** In order to make explicit the unramified cover $X_0(63) \longrightarrow X_0(63)/\langle w_7\rangle$, let us take for $\Omega^1_{\mathbb{Q}}(X_0(63))$ the basis $\{\omega_1, \omega_2, \omega_3, \nu_4, \nu_5\}$, where

$$\nu_4 = (\omega_4 + \omega_5)/2 \qquad \text{and} \qquad \nu_5 = (\omega_4 - \omega_5)/(2\sqrt{3}).$$

The involution $w_7$ scales $\nu_4$ and $\nu_5$ by $-1$, so that $\nu_4^2, \nu_4\,\nu_5, \nu_5^2$ belong to the tensor product of the vector space $\Omega^1_{\mathbb{Q}}(X_0(63)/\langle w_7\rangle)$ by itself. Using Fourier expansions, we obtain

$$\nu_4^2 = Q_1(\omega_1, \omega_2, \omega_3)\,, \quad \nu_4\,\nu_5 = Q_2(\omega_1, \omega_2, \omega_3)\,, \quad \nu_5^2 = Q_3(\omega_1, \omega_2, \omega_3)\,,$$

where

$$\begin{aligned} Q_1(X,Y,Z) &= \phantom{-}(X^2 + 9\,Y^2 - 10\,XY + 2\,XZ + 6\,YZ + Z^2)/4\,,\\ Q_2(X,Y,Z) &= -(X^2 + 9\,Y^2 - 2\,XY - Z^2)/4\,,\\ Q_3(X,Y,Z) &= -(X^2 + 9\,Y^2 - 10\,XY - 2\,XZ - 6\,YZ + Z^2)/12\,. \end{aligned}$$

Note that the relation

$$Q_1(x,y,1)\,Q_3(x,y,1) - Q_2(x,y,1)^2 = 0$$

is exactly equation (1).

Consider now the functions $r = \nu_4/\omega_3$ and $s = \nu_5/\omega_3$ on $X_0(63)$. Since they are not fixed by $w_7$, one has

$$\mathbb{Q}(X_0(63)) \;=\; \mathbb{Q}(x,y,r) \;=\; \mathbb{Q}(x,y,s),$$

and we can think of the above equalities as a rational model for the double cover $X_0(63) \longrightarrow X_0(63)/\langle w_7\rangle$, namely

$$r^2 = Q_1(x,y,1)\,, \qquad r\,s = Q_2(x,y,1)\,, \qquad s^2 = Q_3(x,y,1)\,. \tag{2}$$

3.3. **The automorphism groups of $X_0(63)$ and $X_0(63)/\langle w_7\rangle$.** As noted in the previous section, the automorphism group of $X_0(63)$ is isomorphic to $\mathcal{S}_4 \times \mathbb{Z}/2\,\mathbb{Z}$. This was conjectured in [KM88], and then settled in [Elk90] by proving the existence of an involution which is not in the normalizer $B(63)$. An explicit description for this *extra* involution is obtained in this section.

We begin by recalling that the automorphism subgroup $B(63)$ is generated by the Atkin-Lehner involutions $w_7, w_9$ and the order-three automorphism $S$ in the proof of Proposition 2.2. The action of these generators on the regular differentials of $X_0(63)$ is displayed in the following table:

| | $w_7$ | $w_9$ | $S$ |
|---|---|---|---|
| $\omega_1$ | $\omega_1$ | $-3\,\omega_2$ | $-1/2\,\omega_1 + 3/2\,\omega_2 + \sqrt{-3}/2\,\omega_3$ |
| $\omega_2$ | $\omega_2$ | $-1/3\,\omega_1$ | $\omega_2$ |
| $\omega_3$ | $\omega_3$ | $-\omega_3$ | $\sqrt{-3}/2\,\omega_1 - \sqrt{-3}/2\,\omega_2 - 1/2\,\omega_3$ |
| $\omega_4$ | $-\omega_4$ | $\omega_4$ | $-1/2\,\omega_4 + \sqrt{-3}/2\,\omega_5$ |
| $\omega_5$ | $-\omega_5$ | $\omega_5$ | $\sqrt{-3}/2\,\omega_4 - 1/2\,\omega_5$ |

In particular, $w_7$ commutes with $w_9$ and $S$, and one gets the relation $(w_9\,S)^3 = 1$. So $B(63)$ is indeed isomorphic to $\mathcal{A}_4 \times \mathbb{Z}/2\,\mathbb{Z}$.

Let us now turn to the quotient $X_0(63)/\langle w_7\rangle$. The automorphisms induced on this curve by $w_9$ and $S$ can be denoted in the same way:

$$\mathcal{A}_4 \simeq \langle S, w_9\rangle \hookrightarrow \mathrm{Aut}\,(X_0(63)/\langle w_7\rangle)\,.$$

Now, equation (1) yields an involution $W$ on $X_0(63)/\langle w_7\rangle$ which acts sending an affine point $(x, y)$ to $(-x, -y)$ and which does not come from $B(63)$. From the Hurwitz formula, it follows that the quotient of the curve by $\langle W\rangle$ has genus one, so the matrix of the action of $W$ on $\Omega^1_{\mathbb{Q}}(X_0(63)/\langle w_7\rangle)$ with respect to the basis $\{\omega_1, \omega_2, \omega_3\}$ is

$$\begin{pmatrix} -1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

One can then check that $W$ commutes with $w_7$ while $W\,S\,W = S^{\,2}$. This explicitly yields $\mathcal{S}_4$ as a subgroup of $X_0(63)/\langle w_7\rangle$, which can be theoretically deduced from [Elk90] together with the observation that $\langle w_7\rangle$ is the center of $\mathrm{Aut}\,(X_0(63))$:

$$\mathcal{S}_4 \simeq \mathrm{Aut}(X_0(63))/\langle w_7\rangle \hookrightarrow \mathrm{Aut}(X_0(63)/\langle w_7\rangle).$$

To conclude that this embedding is actually surjective, we note that the isomorphism given by

$$(X, Y) = \left(\frac{-2\sqrt{-3}/3\,x + 2\sqrt{-3}\,y}{-\sqrt{-3}/3\,x - \sqrt{-3}\,y + 1}\,,\,\frac{\sqrt{-3}/3\,x + \sqrt{-3}\,y + 1}{-\sqrt{-3}/3\,x - \sqrt{-3}\,y + 1}\right)$$

transforms (1) into the simpler equation

$$X^4 + Y^4 + 1 + \frac{2}{7}\,(X^2 + Y^2 + X^2\,Y^2) = 0\,.$$

From the classification in [Dol], the automorphism group of this plane quartic is isomorphic to $\mathcal{S}_4$. So we have

$$\mathrm{Aut}\,(X_0(63)/\langle w_7\rangle) \;=\; \langle W, S, w_9\rangle \;\simeq\; \mathcal{S}_4.$$

**Remark 3.1.** The determinant of every automorphism of $X_0(63)/\langle w_7\rangle$ acting on the regular differentials is trivial. This implies that the quotient of this curve by any subgroup of automorphisms has at most genus one. In particular, the quotient by an involution has always genus one.

Lastly, the automorphism $W$ lifts to two involutions on $X_0(63)$ which differ by multiplication by $w_7$. From equations (2) and the action of $W$ on $X_0(63)/\langle w_7\rangle$, it follows that these liftings send the regular differentials $\nu_4$ and $\nu_5$ to $\pm\sqrt{-3}\,\nu_5$ and $\mp\sqrt{-3}/3\,\nu_4$, respectively. In particular, both involutions are defined over the quadratic field $\mathbb{Q}(\sqrt{-3}\,)$, whereas $W$ is defined over $\mathbb{Q}$. Notice also that they send $\omega_4$ and $\omega_5$ to $\mp\sqrt{-1}\,\omega_5$ and $\pm\sqrt{-1}\,\omega_4$, respectively. The choice of one of these two liftings fixes an identification

$$\mathrm{Aut}\,(X_0(63)) \;=\; \mathrm{Aut}\,(X_0(63)/\langle w_7\rangle) \times \langle w_7\rangle.$$

## 4. The modular curve $X^+(7,3)$ as a cover of $X^+(7)$

Let us now resume Section 2 in the particular case $N = 7, p = 3$. Our goal is to describe explicitly the modular cover $X^+(7,3) \longrightarrow X^+(7)$. This is needed in the next sections to recover the $\mathbb{Q}$-curves of degree 7 realizing a given octahedral Galois representation $\varrho$ once the rational points on the twisted curves $X^+(7,3)_\varrho$ and $X^+(7,3)'_\varrho$ have been found.

Recall that we have a commutative diagram

$$\begin{array}{ccc} X(7,3) & \xrightarrow{\Phi} & X_0(63) \\ \downarrow & & \downarrow \\ X^+(7,3) & \xrightarrow{\Phi} & X_0(63)/\langle w_7\rangle \end{array}$$

where the horizontal arrows are isomorphisms induced by the automorphism $\tau \mapsto \tau/3$ of the complex upper-half plane.

From now on, we use the following notation: for a function $F \in \mathbb{Q}(X_0(63))$, a regular differential $\omega \in \Omega^1(X_0(63))$ or an automorphism $A \in \mathrm{Aut}(X_0(63))$, we put $\overline{F} = \Phi^*(F)$, $\overline{\omega} = \Phi^*(\omega)$, $\overline{A} = \Phi\, A\, \Phi^{-1}$ for the corresponding function, differential or automorphism of $X(7,3)$. Through the isomorphism $\Phi$, equations (1) and (2) in the previous section yield rational models for $X^+(7,3)$ and $X(7,3)$, respectively, and we have

$$\mathbb{Q}(X^+(7,3)) = \mathbb{Q}(\overline{x},\overline{y}), \qquad \mathbb{Q}(X(7,3)) = \mathbb{Q}(\overline{x},\overline{y},\overline{r}) = \mathbb{Q}(\overline{x},\overline{y},\overline{s})$$

$$\Omega^1_{\mathbb{Q}}(X^+(7,3)) = \langle \overline{\omega}_1, \overline{\omega}_2, \overline{\omega}_3\rangle_{\mathbb{Q}}, \qquad \Omega^1_{\mathbb{Q}}(X(7,3)) = \langle \overline{\omega}_1, \overline{\omega}_2, \overline{\omega}_3, \overline{\nu}_4, \overline{\nu}_5\rangle_{\mathbb{Q}}.$$

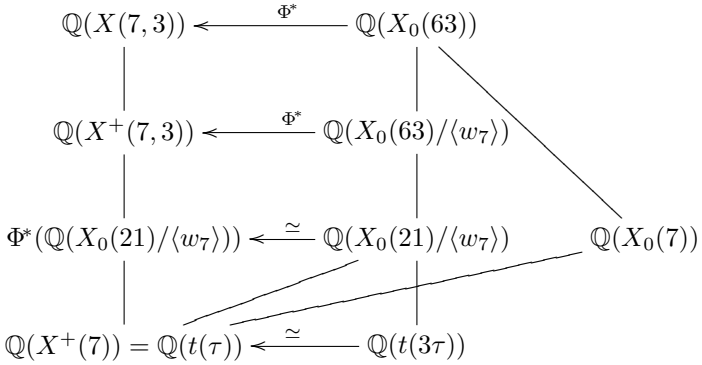
Analogously,

$$\mathcal{S}_4 \simeq \langle \overline{W}, \overline{S}, \overline{w}_9\rangle = \mathrm{Aut}\left(X^+(7,3)\right) \hookrightarrow \mathrm{Aut}\left(X(7,3)\right),$$

and the involution $w$ defining $X^+(7,3)$ as a quotient of $X(7,3)$ is precisely $\overline{w}_7$.

**Remark 4.1.** The automorphism group of $X^+(N)$ is trivial when the genus of this curve is at least three and $N$ is prime (cf. [BH03]). Thus, for any such a level $N$, the curve $X^+(N,3)$ has no involutions $\overline{W}$ with $\langle \overline{W}, \overline{S}, \overline{w}_9\rangle \simeq \mathcal{S}_4$. This reinforces the exceptionality of the case $N = 7$ exhibited in Proposition 2.2.

Consider the following diagram of function fields, where the horizontal arrows are isomorphisms induced by $\Phi$ while the vertical ones are inclusions:




We now dissect the left column of the diagram by proceeding in several steps.

**The function field of $X^+(7)$.** For this function field, we take the following generator over $\mathbb{Q}$:

$$t(\tau) \;=\; \left(\frac{\eta(\tau)}{\eta(7\tau)}\right)^4 + \;7^2\left(\frac{\eta(7\tau)}{\eta(\tau)}\right)^4 \;=\; \frac{1}{q} \;-4+51\,q-204\,q^2+\cdots$$

where $\eta$ denotes the Dedekind function on the complex upper-half plane. Let us also recall, for future use, that $\mathbb{Q}(X_0(7))$ is generated over $\mathbb{Q}(X^+(7))$ by the elliptic modular function $j$. The relation between the functions $j$ and $t$ can be computed using the procedure described in [GL98]:

$$j^2-(13+t)(-96+5t+t^2)(-1371-1710t-170t^2+10t^3+t^4)j+(13+t)^2(3529+250t+t^2)^3=0.$$

A non-CM rational value of $t$ gives rise to a quadratic $\mathbb{Q}$-curve of degree 7 with $j$-invariant such that $\mathbb{Q}(j)=\mathbb{Q}\big(\sqrt{t^2-196}\,\big)$.

**The function field of $X_0(21)/\langle w_7\rangle$.** Using Proposition 3 of [Gon91], we obtain a rational function $u_0$ on $X_0(21)$ with divisor $2(1/3)-2(\infty)$ and normalized Fourier expansion, namely

$$u_0=\frac{\eta(3\tau)^3\,\eta(7\tau)}{\eta(\tau)\,\eta(21\tau)^3} \;=\; \frac{1}{q^2}+\frac{1}{q}+2+2\,q^2+\cdots$$

Moreover, the involution $w_7$ sends $u_0$ to $7/u_0$. Then, the functions

$$u \;=\; u_0 \,+\, \frac{7}{u_0} \;=\; \frac{1}{q^2}+\frac{1}{q}+2+9\,q^2-6\,q^3+\cdots$$

$$v \;=\; \frac{du}{2\,\omega_1} \;=\; \frac{1}{q^3}+\frac{3}{2\,q^2}+\frac{1}{2\,q}-6\,q+\cdots$$

generate $\mathbb{Q}(X_0(21)/\langle w_7\rangle)$ over $\mathbb{Q}$ and satisfy the equation

$$v^2 \;=\; u^3-23/4\,u^2-28\,u+161\,. \tag{3}$$

This is the elliptic curve of conductor 21 with label A3 in Cremona's notation, while the label of $X_0(21)$ is A1.

**The extension of function fields $\mathbb{Q}(X^+(7,3))\,/\,\Phi^*(\mathbb{Q}(X_0(21)/\langle w_7\rangle))$.** This extension corresponds through $\Phi$ to $\mathbb{Q}(x,y)/\,\mathbb{Q}(u,v)$. So all we need is to express $u$ and $v$ as rational functions in $x$ and $y$. We first observe that the degree-three rational cover $X_0(63)\longrightarrow X_0(63)/\langle w_9\,S\,w_9\rangle$ is actually the forgetful map $X_0(63)\longrightarrow X_0(21)$, since the pullback of the regular differentials is $\langle\omega_1\rangle$. Thus, the functions on $X_0(21)/\langle w_7\rangle$ are exactly those on $X_0(63)/\langle w_7\rangle$ which are invariant by the automorphism $w_9\,S\,w_9$. The functions

$$U=\frac{(-3+x-9\,y)(3+x-9\,y)}{x^2} \qquad\text{and}\qquad V=\frac{(-3+x-9\,y)^3}{x^3} \tag{4}$$

satisfy this. Since $[\mathbb{Q}(x,y):\mathbb{Q}(U,V)]=3$, these functions generate the function field of $X_0(21)/\langle w_7\rangle$ over $\mathbb{Q}$, that is, $\mathbb{Q}(u,v)$. Using the $q$-expansions of $x$, $y$, $u$ and $v$, we obtain the equalities

$$u=4\,\frac{-144-348\,U+26\,U^2+42\,V+17\,U\,V+2\,V^2}{(24+2\,U+V)^2}\,,$$

$$v=9\,\frac{432(48+16U-5U^2)-V(2880-2208U+40U^2-132V+22\,UV+V^2)}{(24+2\,U+V)^3}\,,$$

which combined with (4) give the desired expressions.

**The function field $\Phi^*(\mathbb{Q}(X_0(21)/\langle w_7\rangle))$ as an extension of $\mathbb{Q}(X^+(7))$.** What remains to be done is to express $t$ as a rational function in $\overline{u}$ and $\overline{v}$. As $t(\tau) = \overline{t(3\tau)}$, this is equivalent to giving $t(3\tau)$ as a rational function in $u$ and $v$. The function $t(3\tau)$, viewed on $X_0(21)/\langle w_7\rangle$, has exactly a pole of order 3 at each cusp. Since the function

$$R(\tau) \;=\; \frac{\eta(\tau)^3\,\eta(7\tau)^3}{\eta(3\tau)^3\,\eta(21\tau)^3} \;=\; \frac{1}{q^2} - \frac{3}{q} - 8\,q + \cdots$$

has divisor $2(0) + 2(1/7) - 2(1/3) - 2(\infty)$ on $X_0(21)$ and is sent to $-R$ by $w_7$ (cf. [Gon91]), its square lies in $\mathbb{Q}(X_0(21)/\langle w_7\rangle)$. More precisely, we get

$$R^2 = u^2 - 8v + 16u - 120\,.$$

Analogously, the function $R^2(\tau)\,t(3\tau)$ has a unique pole (of order 7) at the cusp $\infty$ of $X_0(21)/\langle w_7\rangle$, so it must also be a polynomial in $u$ and $v$. Using again the $q$-expansions of $u$ and $v$, we finally obtain

$$t \;=\; \frac{-1624 + 742\,\overline{u} + 25\,\overline{u}^2 - 19\,\overline{u}^3 - 168\,\overline{v} + 58\,\overline{u}\;\overline{v} + 2\,\overline{u}^2\,\overline{v}}{2\,(\overline{u}^2 - 8\,\overline{v} + 16\,\overline{u} - 120)}\,. \tag{5}$$

To finish this section, we note that the Prym variety associated with the cover $X(7,3) \longrightarrow X^+(7,3)$ is isomorphic over $\mathbb{Q}$ to the modular Abelian variety $A_{f_4}$ attached to the newform $f_4$ by Shimura [Shi71] as a subvariety of the Jacobian $J_0(63)$ of $X_0(63)$. This Abelian surface is the Jacobian of the curve (cf. [Bru04])

$$\widehat{C} : \hat{y}^2 = -\frac{1}{27}\,\hat{x}^6 - 2\,\hat{x}^3 + 1\,. \tag{6}$$

Note that this genus-two curve is the one given for the Abelian surface $S_{63,B}$ in the tables of [GJGG02], where it was computed by analytical means.

There also exists a genus-two curve $\widetilde{C}$ over $\mathbb{Q}$ which is dominated by $X(7,3)$ and whose Jacobian is isogenous to $A_{f_4}$ over $\mathbb{Q}$. Specifically,

$$\widetilde{C} : \tilde{y}^2 = \tilde{x}^6 - 26\,\tilde{x}^3 - 27\,, \tag{7}$$

where $\tilde{x} = \overline{\nu}_4/\overline{\nu}_5 = \overline{r}/\overline{s}$ and $\tilde{y} = d\tilde{x}/\overline{\nu}_5$. The nonconstant morphism $X(7,3) \longrightarrow \widetilde{C}$ sending $(\overline{x},\overline{y},\overline{r},\overline{s})$ to $(\tilde{x},\tilde{y})$ has degree four, so it is unramified, and is defined over $\mathbb{Q}$. The curve $\widetilde{C}$ is labeled $C_{63}$ in Table 1 of [GJG03]. It turns out that the above curve $\widehat{C}$ is not isomorphic to $\widetilde{C}$, so it is not dominated by $X(7,3)$.

## 5. The twisted curves $X^+(7,3)_\varrho$ and $X(7,3)_{\varrho,m}$

Let us now twist the modular curve $X^+(7,3)$ following the general recipe given in Section 2. We start from a fixed representation $\varrho : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3)$ with cyclotomic determinant, and denote by $L$ its splitting field. We take $\varrho$ to be surjective, so that it is determined by $L$ up to conjugation in $\mathrm{PGL}_2(\mathbb{F}_3)$. Since this group is isomorphic to the symmetric group $\mathcal{S}_4$, we can actually take as input data a degree-four polynomial $f \in \mathbb{Z}[X]$ with splitting field $L$. Note that the condition on the determinant amounts to saying that $L$ contains $\sqrt{-3}$ or, equivalently, that the discriminant of $f$ is $-3$ up to a rational square.

We identify $\mathrm{Gal}(L/\mathbb{Q})$ with $\mathcal{S}_4$ by fixing an order of the roots of $f$. For convenience, we take as generators for this Galois group the following permutations:

$$\sigma_1 = (1,2,3), \qquad \sigma_2 = (1,2)(3,4), \qquad \sigma_3 = (1,2).$$

Note that $\mathbb{Q}(\sqrt{-3}\,)$ is the fixed field by $\langle\sigma_1,\sigma_2\rangle$. Then, the (conjugacy class of the) representation $\varrho$ translates into the isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Aut}\,(X^+(7,3))$ sending $\sigma_1,\sigma_2,\sigma_3$ to $\overline{S}^{\,2},\overline{w}_9,\overline{W}$, respectively. This isomorphism identifies the conjugacy class in $\mathrm{PGL}_2(\mathbb{F}_3)$ of the matrix $V$ fixed in Section 2 with the conjugacy class in $\mathrm{Aut}\,(X^+(7,3))$ of the automorphism $\overline{W}$. Thus, the 1-cocycle attached to $\varrho$ can be given as follows:

$$\xi_{\sigma_1} = \overline{S}^{\,-1}, \qquad \xi_{\sigma_2} = \overline{w}_9\,, \qquad \xi_{\sigma_3} = 1.$$

5.1. **The isomorphism between $X^+(7,3)_\varrho$ and $X^+(7,3)'_\varrho$.** The 1-cocycles $\xi$ and $\xi'$ are related by the formula $\xi' = \overline{W}\,\xi\,\overline{W}$, hence cohomologous. It follows that the composition

$$X^+(7,3)'_\varrho \xrightarrow{\Psi'} X^+(7,3) \xrightarrow{\overline{W}} X^+(7,3) \xrightarrow{\Psi^{-1}} X^+(7,3)_\varrho$$

is defined over $\mathbb{Q}$, where $\Psi$ and $\Psi'$ are the isomorphisms in Theorem 2.1. The set of isomorphism classes of quadratic $\mathbb{Q}$-curves of degree 7 realizing $\varrho$ are in bijection with the union of the disjoint sets $\Psi\left(X^+(7,3)_\varrho(\mathbb{Q})\right)$ and $\Psi'\left(X^+(7,3)'_\varrho(\mathbb{Q})\right)$. Since one set is the image of the other by $\overline{W}$, to get all such $\mathbb{Q}$-curves it suffices to determine just one of the two sets and then use the next result.

**Proposition 5.1.** *The automorphism $\overline{W}$ induces a nontrivial involution on $X^+(7)$ given by*

$$t \;\mapsto\; (-196 - 13\,t)/(13 + t).$$

*Proof.* The automorphism group of the cover $X^+(7,3) \longrightarrow X^+(7)$ is $\langle\overline{S},\overline{w}_9\rangle$. Since $\overline{W}$ normalizes this group, it induces a nontrivial automorphism on $X^+(7)$, whose action on $t$ comes from the expression of this Hauptmodul as an element in $\mathbb{Q}(X^+(7,3))$, given in Section 4, together with the action of $\overline{W}$ on this function field, given in Section 3. □

It follows a corollary which is reobtained in Subsection 5.6 below.

**Corollary 5.1.** *Fix a nonzero integer $m$. Among the isomorphism classes of quadratic $\mathbb{Q}$-curves of degree 7 realizing $\varrho$, those with field of moduli $\mathbb{Q}(\sqrt{m}\,)$ are the same in number as those with field of moduli $\mathbb{Q}(\sqrt{-3m}\,)$.*

*Proof.* A non-cuspidal value $t \in \mathbb{Q}$ provides a quadratic $\mathbb{Q}$-curve of degree 7 with $j$-invariant in $\mathbb{Q}\big(\sqrt{t^2-196}\,\big)$. Then, the value $(-196-13\,t)/(13+t)$ obtained from Proposition 5.1 provides a $\mathbb{Q}$-curve with $j$-invariant in $\mathbb{Q}\Big(\sqrt{-3\,(t^2-196)}\,\Big)$. □

5.2. **A plane quartic model for $X^+(7,3)_\varrho$.** In this subsection we provide a method to produce a plane quartic rational model for $X^+(7,3)_\varrho$. The background strategy is as in [FGL]: such a model can be obtained from a basis of the 3-dimensional $\mathbb{Q}$-vector space $\Omega^1_{\mathbb{Q}}(X^+(7,3)_\varrho)$.

Consider on $\Omega^1_{\overline{\mathbb{Q}}}(X^+(7,3)) = \Omega^1_{\mathbb{Q}}(X^+(7,3)) \otimes \overline{\mathbb{Q}}$ the Galois action twisted by the 1-cocycle $\xi$. It is defined by

$$(\omega\otimes\gamma)^\sigma_\xi := \left({}^\sigma\omega\;\xi_\sigma^{-1}\right)\otimes\sigma(\gamma)$$

for $\omega \in \Omega^1_{\mathbb{Q}}(X^+(7,3))$, $\gamma \in \overline{\mathbb{Q}}$ and $\sigma \in \mathrm{G}_{\mathbb{Q}}$. This action factors through $\mathrm{Gal}(L/\mathbb{Q})$, and the regular differentials on $X^+(7,3)_\varrho$ defined over $\mathbb{Q}$ can be identified with the

fixed elements in $\Omega^1_L(X^+(7,3))$, that is,

$$\Omega^1_{\mathbb{Q}}\big(X^+(7,3)_\varrho\big) \;=\; \big(\Omega^1_{\mathbb{Q}}\big(X^+(7,3)\big)\otimes L\big)^{\mathrm{Gal}(L/\mathbb{Q})}_{\xi}\,.$$

We fix a basis $\{\overline{\omega}_i\otimes\theta_j\}_{i,j}$ for $\Omega^1_{\mathbb{Q}}(X^+(7,3))\otimes L$, where $\omega_1,\omega_2,\omega_3$ are the forms in $\Omega^1_{\mathbb{Q}}(X_0(63)/\langle w_7\rangle)$ introduced in Section 3, $\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3$ are the corresponding forms in $\Omega^1_{\mathbb{Q}}(X^+(7,3))$, and $\{\theta_1,\dots,\theta_{24}\}$ is an integral basis of $L$.

The action of the Galois generators $\sigma_1,\sigma_2,\sigma_3$ on this basis is given by three $72\times72$ matrices with rational entries. We call them $\mathcal{W}_1$, $\mathcal{W}_2$,$\mathcal{W}_3$, respectively. The computation of these matrices comes straightforward from the table in Subsection 3.3 and from the definition of the 1-cocycle $\xi$.

We must now look for three elements in $\Omega^1_{\mathbb{Q}}(X^+(7,3))\otimes L$ which are linearly independent over $\mathbb{Q}$ and invariant by the above Galois action. In other words, we compute a basis $\{X_\varrho\,,Y_\varrho\,,Z_\varrho\}$ for the 3-dimensional vector subspace of $\Omega^1_{\mathbb{Q}}(X^+(7,3))\otimes L$ corresponding to

$$\bigcap_{k=1}^{3}\ker\left(\mathcal{W}_k-\mathrm{Id}_{72}\right)\subseteq\mathbb{Q}^{72}\,.$$

Writing $X_\varrho\,,Y_\varrho\,,Z_\varrho$ as linear combinations of $\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3$, we get the $3\times3$ matrix $\Theta$ with entries in $L$ giving the basis change

$$(\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3)=(X_\varrho\,,Y_\varrho\,,Z_\varrho)\,\Theta\,.$$

Plugging $\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3$ in the homogenization of equation (1), replacing then $X_\varrho\,,Y_\varrho\,,Z_\varrho$ by projective variables $X,Y,Z$ and finally factoring out, one gets a plane quartic equation $F(X,Y,Z)=0$ for the twist $X^+(7,3)_\varrho$ over $\mathbb{Q}$. Then, the isomorphism $\Psi:X^+(7,3)_\varrho\longrightarrow X^+(7,3)$ in Theorem 2.1 is given by

$$(X\colon Y\colon Z)\;\longmapsto\;(X\colon Y\colon Z)\,\Theta\,.$$

**Remark 5.1.** Actually $\Psi$ is defined over the fixed field $L^{\langle\sigma_3\rangle}$, so the above matrix $\Theta$ has all its entries in this degree-twelve extension. Moreover, $\det\Theta\in\mathbb{Q}$. Indeed, one has

$$X_\varrho\wedge Y_\varrho\wedge Z_\varrho\;=\;\det\Theta^{-1}\;\overline{\omega}_1\wedge\overline{\omega}_2\wedge\overline{\omega}_3$$

in $\bigwedge^3\Omega^1(X^+(7,3))$. Then, for any $\sigma$ in $\mathrm{G}_{\mathbb{Q}}$,

$$(X_\varrho\wedge Y_\varrho\wedge Z_\varrho)^\sigma_\xi\;=\;\sigma(\det\Theta^{-1})\bigwedge_{i\,=\,1,2,3}(\overline{\omega}_i\,\xi_\sigma^{-1})\;=\;\sigma(\det\Theta^{-1})\,\det\xi_\sigma^{-1}\,(\overline{\omega}_1\wedge\overline{\omega}_2\wedge\overline{\omega}_3),$$

where $\xi_\sigma$ is seen as an automorphism in $\Omega^1(X^+(7,3))$. So the assertion follows from the facts that $X_\varrho\wedge Y_\varrho\wedge Z_\varrho$ is invariant under the twisted action of $\mathrm{G}_{\mathbb{Q}}$ and $\det\xi_\sigma=1$ for all $\sigma$ (see Remark 3.1).

5.3. **Genus-one quotients of $X^+(7,3)_\varrho$.** Recall that every quotient of $X^+(7,3)_\varrho$ by an involution has genus one (see Remark 3.1); we now make explicit two such quotients. In order to do that, we begin by introducing the cubic and quartic fields

$$L_3\;=\;L^{\langle\sigma_2,\,\sigma_3,\,\sigma_1^2\sigma_2\,\sigma_1\rangle},\qquad\qquad L_4\;=\;L^{\langle\,\sigma_3,\,\sigma_2\,\sigma_1\,\sigma_2\rangle}.$$

Note that $L_4$ is generated by a root of the polynomial $f$, whereas $L_3$ corresponds to its cubic resolvent. Since the discriminant of $L$ is $-3$ up to squares,

$$L_3\;=\;\mathbb{Q}(\alpha)$$

for some $\alpha$ satisfying $\alpha^3\in\mathbb{Q}$. Replacing $\alpha$ by $1/\alpha$, if necessary, we can further assume that $\sigma_1(\alpha)=\zeta\,\alpha$, where $\zeta=(-1+\sqrt{-3}\,)/2$.

Firstly, let us consider the involution $w_\varrho = \Psi^{-1}\,\overline{w}_9\,\Psi$ in $\mathrm{Aut}(X^+(7,3)_\varrho)$. A straightforward computation shows that $w_\varrho$ is defined over $L_3$. Let us denote by $E_\varrho$ the genus-one curve $X^+(7,3)_\varrho/\langle w_\varrho\rangle$. In Remark 5.2 below we shall give a procedure to get a model for the cover $X^+(7,3)_\varrho \longrightarrow E_\varrho$. Assume $E_\varrho$ is elliptic over $L_3$, otherwise $X^+(7,3)_\varrho(\mathbb{Q})$ is empty. The Weil restriction $\mathrm{Res}_{L_3/\mathbb{Q}}\,E_\varrho$ is $\mathbb{Q}$-isogenous to the Jacobian of $X^+(7,3)_\varrho$ and, in particular,

$$\mathrm{rank}_{\mathbb{Q}}\,\mathrm{Jac}\left(X^+(7,3)_\varrho\right) \;=\; \mathrm{rank}_{L_3}E_\varrho\,.$$

When this rank is at most two, we are able to apply an elliptic-Chabauty method to determine all rational points of $X^+(7,3)_\varrho$. Notice that $E_\varrho$ is isomorphic to the elliptic curve of conductor 21 with label A1 in Cremona's notation, that is, the modular curve $X_0(21)$.

A second genus-one quotient is constructed as follows. From the equality

$$\{\tau\in\mathrm{Gal}(L/\mathbb{Q}) : {}^{\tau}\Psi\,\Psi^{-1}\in\langle\,\overline{w}_9\,\overline{S}\,\overline{w}_9\,\rangle\} = \langle\,\sigma_3,\,\sigma_2\,\sigma_1\,\sigma_2\rangle$$

it follows that the composition

$$X^+(7,3)_\varrho \xrightarrow{\Psi} X^+(7,3) \longrightarrow X^+(7,3)/\langle\overline{w}_9\,\overline{S}\,\overline{w}_9\rangle \;\simeq\; X_0(21)/\langle w_7\rangle$$

is defined over $L_4$. Let us denote by $E_S$ the elliptic curve $X^+(7,3)/\langle\overline{w}_9\,\overline{S}\,\overline{w}_9\rangle$, for which a model over $\mathbb{Q}$ is given by equation (3). If $\mathrm{rank}_{\,L_4}E_S = 0$, then it is unnecessary to compute an equation for $X^+(7,3)_\varrho$. Indeed, in this case the values $t\in X^+(7)(\mathbb{Q})$ obtained from the torsion points in $E_S(L_4)$ using (5) provide a finite set of candidate $\mathbb{Q}$-curves $E$, and it suffices to check for each $E$ whether it realizes $\varrho$ or not. We also notice that

$$\mathrm{rank}_{\mathbb{Q}}\,\mathrm{Jac}\left(X^+(7,3)_\varrho\right) = \mathrm{rank}_{L_4}E_S\,,$$

since the Weil restriction $\mathrm{Res}_{L_4/\mathbb{Q}}\,E_S$ is isogenous to $E_S\times\mathrm{Jac}(X^+(7,3)_\varrho)$ over $\mathbb{Q}$ and $\mathrm{rank}_{\mathbb{Q}}E_S = 0$.

5.4. **The unramified double cover $X(7,3)_\varrho \longrightarrow X^+(7,3)_\varrho$.** Recall that we have a commutative diagram

$$\begin{array}{ccc} X(7,3)_\varrho & \xrightarrow{\Psi} & X(7,3) \\ \downarrow & & \downarrow \\ X^+(7,3)_\varrho & \xrightarrow{\Psi} & X^+(7,3) \end{array}$$

where the vertical arrows are rational unramified double covers. We next show how to obtain equations for the left cover from the rational model

$$\overline{\nu}_4^{\,2} = Q_1(\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3)\,,\quad \overline{\nu}_4\,\overline{\nu}_5 = Q_2(\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3)\,,\quad \overline{\nu}_5^{\,2} = Q_3(\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3)$$

corresponding to the right cover (cf. Subsection 3.2). Recall also that

$$\Omega^1_{\mathbb{Q}}\big(X^+(7,3)_\varrho\big) \;=\; \Psi^*\left(\langle X_\varrho\,,Y_\varrho\,,Z_\varrho\rangle_{\mathbb{Q}}\right),$$

where $(\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3) = (X_\varrho\,,Y_\varrho\,,Z_\varrho)\,\Theta$.

**Proposition 5.2.** *Let $\alpha$ be as in Subsection* 5.3. *The regular differentials on $X(7,3)_\varrho$ corresponding through the isomorphism $\Psi$ to*

$$R_\varrho = (1/\alpha)\,\overline{\nu}_4 \qquad \textit{and} \qquad S_\varrho = \alpha\,\overline{\nu}_5$$

*are defined over* $\mathbb{Q}$. *In particular, a rational projective model for the double cover* $X(7,3)_\varrho \longrightarrow X^+(7,3)_\varrho$ *is given by the relations*

$$R_\varrho^2 = Q_{1,\varrho}(X_\varrho, Y_\varrho, Z_\varrho), \quad R_\varrho S_\varrho = Q_{2,\varrho}(X_\varrho, Y_\varrho, Z_\varrho), \quad S_\varrho^2 = Q_{3,\varrho}(X_\varrho, Y_\varrho, Z_\varrho),$$

*where*

$$\begin{aligned} Q_{1,\varrho}(X,Y,Z) &= 1/\alpha^2\, Q_1((X,Y,Z)\,\Theta), \\ Q_{2,\varrho}(X,Y,Z) &= Q_2((X,Y,Z)\,\Theta), \\ Q_{3,\varrho}(X,Y,Z) &= \alpha^2\, Q_3((X,Y,Z)\,\Theta). \end{aligned}$$

*Proof.* The statement follows from the definition of the 1-cocycle $\xi$ defining the twisted curve $X(7,3)_\varrho$ together with the observation that the involution $w_9$ acts trivially on $\nu_4$ and $\nu_5$ while $S^*\nu_4 = \zeta\,\nu_4$ and $S^*\nu_5 = \zeta^2\nu_5$. □

**Remark 5.2.** For an eigenvector $\overline{\omega} \in \Omega^1_{\mathbb{C}}(X^+(7,3))$ of $\overline{w}_9$ with eigenvalue $-1$, it can be checked that

$$\mathbb{C}\left(X^+(7,3)/\langle \overline{w}_9\rangle\right) = \mathbb{C}\left(Q_1(\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3)/Q_2(\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3),\, \overline{\omega}^2/Q_2(\overline{\omega}_1,\overline{\omega}_2,\overline{\omega}_3)\right)$$

if and only if $\overline{\omega}$ is not a multiple of $\overline{\omega}_1 + 3\,\overline{\omega}_2 \pm \sqrt{-3}\,\overline{\omega}_3$. Now, for the projective model for $X^+(7,3)_\varrho$ given by

$$Q_{1,\varrho}(X,Y,Z)\; Q_{3,\varrho}(X,Y,Z) - Q_{2,\varrho}(X,Y,Z)^2 = 0,$$

the involution $w_\varrho$ in Subsection 5.3 is defined over $L_3 = \mathbb{Q}(\alpha)$. Then, it follows that for any non-trivial element $\Psi^*(a\,X_\varrho + b\,Y_\varrho + c\,Z_\varrho)$ in the two-dimensional vector subspace of $\Omega^1_{L_3}(X^+(7,3)_\varrho)$ consisting of the eigenvectors of $w_\varrho$ with eigenvalue $-1$, the morphism $\phi_\varrho : X^+(7,3)_\varrho \longrightarrow \mathbb{P}^2$ given by

$$(X:Y:Z) \longmapsto (u:v:w) = \left(Q_{1,\varrho}(X,Y,Z) : Q_{2,\varrho}(X,Y,Z) : (a\,X + b\,Y + c\,Z)^2\right)$$

is defined over $L_3$ and its image is the genus-one curve $E_\varrho$.

5.5. **Genus-two curves attached to** $X(7,3)_\varrho$**.** Let us now twist by $\varrho$ the genus-two curves $\widehat{C}$ and $\widetilde{C}$ at the end of Section 4. Keep the notation in Proposition 5.2.

The Prym variety associated with the cover $X(7,3)_\varrho \longrightarrow X^+(7,3)_\varrho$ is the Jacobian of the genus-two curve

$$\widehat{C}_\varrho :\; \hat{y}_\varrho^2 = -\frac{1}{27}\, d^4 \hat{x}_\varrho^6 - 2\, d^2 \hat{x}_\varrho^3 + 1, \tag{8}$$

where $d = \alpha^3$. Indeed, since $d$ and $\det\Theta$ lie in $\mathbb{Q}$ (cf. Remark 5.1), an equation for such a curve is given by

$$\hat{y}_\varrho^2 = -\left(\frac{d}{\det\Theta}\right)^2 \det\left(Q_{1,\varrho} + 2\,\hat{x}_\varrho\, Q_{2,\varrho} + \hat{x}_\varrho^2\, Q_{3,\varrho}\right),$$

where we regard each $Q_{i,\varrho}$ as the symmetric $3\times 3$ matrix corresponding to the quadratic form that it represents. Since

$$Q_{1,\varrho} = \frac{1}{\alpha^2}\,\Theta\; Q_1\,\Theta^{\mathrm{t}}, \qquad Q_{2,\varrho} = \Theta\; Q_2\,\Theta^{\mathrm{t}}, \qquad Q_{3,\varrho} = \alpha^2\,\Theta\; Q_1\,\Theta^{\mathrm{t}},$$

the claim follows from the equality

$$\det(Q_{1,\varrho} + 2\,\hat{x}_\varrho\, Q_{2,\varrho} + \hat{x}_\varrho^2\, Q_{3,\varrho}) = \frac{\det\Theta^2}{\alpha^6}\det(Q_1 + 2\,\hat{x}_\varrho\,\alpha^2\, Q_2 + \hat{x}_\varrho^2\,\alpha^4\, Q_3)$$

together with equation (6) and the relation

$$\det(Q_1 + 2\,\hat{x}\, Q_2 + \hat{x}^2\, Q_3) = -\frac{1}{27}\,\hat{x}^6 - 2\,\hat{x}^3 + 1.$$

Whenever $\operatorname{rank}_{\mathbb{Q}} \operatorname{Jac} \widehat{C}_\varrho$ is at most one, one can use the Abel-Prym embedding $X^+(7,3)_\varrho \longrightarrow \operatorname{Jac} \widehat{C}_\varrho$ (or twice that, which turns out to be easier to compute), and apply Chabauty's method to bound the cardinality of $X^+(7,3)_\varrho(\mathbb{Q})$. This is described in general in [Bru04]. However, in our particular setting, the rational cover $X(7,3)_\varrho \longrightarrow \widetilde{C}_\varrho$ in the following proposition is more useful.

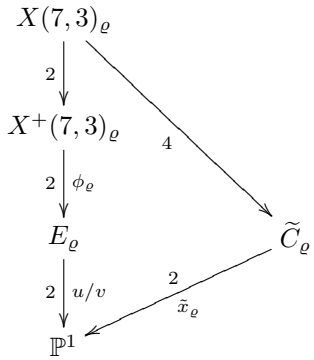
**Proposition 5.3.** *The functions* $\tilde{x}_\varrho = \Psi^*(R_\varrho/S_\varrho)$ *and* $\tilde{y}_\varrho = \alpha^3\, d\tilde{x}_\varrho/\Psi^*(S_\varrho)$ *lie in* $\mathbb{Q}(X(7,3)_\varrho)$ *and generate over* $\mathbb{Q}$ *the function field of the genus-two curve*

$$\widetilde{C}_\varrho :\ \tilde{y}_\varrho^2 = d^4\tilde{x}_\varrho^6 - 26\, d^2\tilde{x}_\varrho^3 - 27,$$

*where* $d = \alpha^3$.

*Proof.* It suffices to use Proposition 5.2 and equation (7) along with the equalities $\tilde{x}_\varrho = \Psi^*(\widetilde{x})/\alpha^2$ and $\tilde{y}_\varrho = \Psi^*(\widetilde{y})$. □

With the notation in Remark 5.2, we have the following commutative diagram, where the morphism degrees are displayed:




5.6. **The twisted curves** $X(7,3)_{\varrho,\,m}$**.** With the notation in Proposition 5.2, a rational projective model for the double cover

$$X(7,3)_{\varrho,\,m} \xrightarrow{\varphi_m} X(7,3)_\varrho \longrightarrow X^+(7,3)_\varrho$$

introduced in Section 2 is given by

$$R_{\varrho,\,m}^2 = m\, Q_{1,\varrho}\,(X_\varrho, Y_\varrho, Z_\varrho)\,,\ R_{\varrho,\,m}\, S_{\varrho,\,m} = m\, Q_{2,\varrho}\,(X_\varrho, Y_\varrho, Z_\varrho)\,,\ S_{\varrho,\,m}^2 = m\, Q_{3,\varrho}\,(X_\varrho, Y_\varrho, Z_\varrho)\,,$$

where $R_{\varrho,\,m} = \sqrt{m}\, R_\varrho$ and $S_{\varrho,\,m} = \sqrt{m}\, S_\varrho$. Multiplying by nonzero rational squares, if necessary, we can assume each polynomial $Q_{i,\varrho}(x_\varrho, y_\varrho, 1)$ in $\mathbb{Z}[x_\varrho, y_\varrho]$. Let $\mathcal{S}$ be the set of integers dividing the squarefree part of the greatest common divisor of the three resultants

$$\operatorname{Res}_{x_\varrho}\Big(\operatorname{Res}_{y_\varrho}\big(Q_{i,\varrho}(x_\varrho, y_\varrho, 1), Q_{j,\varrho}(x_\varrho, y_\varrho, 1)\big),\, \operatorname{Res}_{y_\varrho}\big(Q_{i,\varrho}(x_\varrho, y_\varrho, 1), Q_{k,\varrho}(x_\varrho, y_\varrho, 1)\big)\Big)$$

obtained for $1 \le i, j, k \le 3$ and $i \ne j \ne k$. Then, there are no quadratic $\mathbb{Q}$-curves of degree 7 realizing $\varrho$ whose field of moduli is $\mathbb{Q}(\sqrt{m}\,)$ when the squarefree parts of $m$ and $-3\,m$ are not in $\mathcal{S}$.

We have now a rational map onto a genus-two curve

$$X(7,3)_{\varrho,\,m} \longrightarrow \widetilde{C}_{\varrho,\,m}\,, \qquad \widetilde{C}_{\varrho,\,m} :\ m\,\tilde{y}_{\varrho,\,m}^2 = d^4\tilde{x}_{\varrho,\,m}^6 - 26\, d^2\tilde{x}_{\varrho,\,m}^3 - 27,$$

where

$$\tilde{x}_{\varrho,\,m} \,=\, \Psi^*(R_{\varrho\,,m}/S_{\varrho\,,m}) \,=\, \tilde{x}_\varrho\,, \qquad \tilde{y}_{\varrho,\,m} \,=\, \alpha^3\, d\tilde{x}_{\varrho\,,m}/\Psi^*(S_{\varrho\,,m}) \,=\, \tilde{y}_\varrho/\sqrt{m}$$

and $d = \alpha^3$ (cf. Proposition 5.3). Thus, to get the above $\mathbb{Q}$-curves for a given integer $m$ such that the squarefree part of $m$ or $-3\,m$ lies in the set $\mathcal{S}$, we only need to determine $\widetilde{C}_{\varrho,m}(\mathbb{Q})$, $\widetilde{C}_{\varrho,-3m}(\mathbb{Q})$ and then use the following remark.

**Remark 5.3.** The diagram in Subsection 5.5 still holds if we replace $X(7,3)_\varrho$ and $\widetilde{C}_\varrho$ by $X(7,3)_{\varrho,\,m}$ and $\widetilde{C}_{\varrho,\,m}$, respectively. Given a lifting to $X(7,3)_{\varrho,\,m}$ of a point $(X_0 : Y_0 : Z_0)$ in $X^+(7,3)_\varrho$, denote by $(\tilde{x}_0, \tilde{y}_0)$ its image in $\widetilde{C}_{\varrho,\,m}$. Then, the liftings to $X(7,3)_{\varrho,\,m}$ of any other point in $X^+(7,3)_\varrho$ map to $(\tilde{x}_0, \pm\tilde{y}_o)$ if and only if this point is a zero of the function $R_\varrho/S_\varrho - \tilde{x}_0$, that is, if and only if it also lies in the conique

$$Q_{2,\varrho}(X,Y,Z)/Q_{3,\varrho}(X,Y,Z) = Q_{2,\varrho}(X_0,Y_0,Z_0)/Q_{3,\varrho}(X_0,Y_0,Z_0). \tag{9}$$

This is used in the second example of next section.

Finally, note that the composition

$$X(7,3)'_{\varrho,\,m} \xrightarrow{\Psi'\varphi_m} X(7,3) \xrightarrow{\overline{W}} X(7,3) \xrightarrow{(\Psi\,\varphi_{-3m})^{-1}} X(7,3)_{\varrho,\,-3m}$$

is defined over $\mathbb{Q}$, where we use any lifting to $X(7,3)$ of the automorphism $\overline{W}$. Thus, to get all quadratic $\mathbb{Q}$-curves of degree 7 realizing $\varrho$ and with field of moduli $\mathbb{Q}(\sqrt{m}\,)$, it suffices to compute the $t$-values obtained from both the rational points on $X(7,3)_{\varrho,\,m}$ and the image by $\overline{W}$ of the rational points on $X(7,3)_{\varrho,\,-3m}$. Proposition 5.1, which can be useful for this computation, yields then the $t$-values of quadratic $\mathbb{Q}$-curves of degree 7 realizing $\varrho$ and with field of moduli $\mathbb{Q}(\sqrt{-3m}\,)$.

## 6. Two examples

The computations involved in the following examples have been performed with the computer algebra system Magma v2.11 [Mag]. The first example uses a genus-one strategy following Subsection 5.3, while the second one uses a genus-two strategy following Subsection 5.6.

**Example 1.** Consider the surjective Galois representation $\varrho : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_3)$ defined up to conjugation by the splitting field of the irreducible polynomial

$$f(X) = X^4 + 2\,X^3 - 3\,X^2 + 2\,X + 7.$$

The discriminant of $f$ equals $-2^6\,3^7$. A projective model for $X(7,3)_\varrho \longrightarrow X^+(7,3)_\varrho$ is given by

$$R^2 = Q_{1,\varrho}(X,Y,Z)\,, \quad S^2 = Q_{3,\varrho}(X,Y,Z)\,, \quad R\,S = Q_{2,\varrho}(X,Y,Z)\,,$$

where

$$\begin{aligned} Q_{1,\varrho} &= \phantom{-}2\left(X^2 + 2\,X\,Y + 4\,X\,Z + 8\,Y^2 + 2\,Z^2\right), \\ Q_{3,\varrho} &= -6\left(26\,X^2 + 50\,X\,Y + 24\,X\,Z + 11\,Y^2 + 24\,Y\,Z + 6\,Z^2\right), \\ Q_{2,\varrho} &= \phantom{-}3\left(15\,X^2 - 4\,X\,Y + 20\,X\,Z - 11\,Y^2 + 4\,Y\,Z + 6\,Z^2\right). \end{aligned}$$

Theorem 6.1 below proves that $(-5 : 1 : 5)$ is the only rational point on $X^+(7,3)_\varrho$. The $t$-values corresponding to this point are $t_1 = -10$ and $t_2 = -22$, and the corresponding $j$-invariants for the associated quadratic $\mathbb{Q}$-curves of degree 7 are

$$j_1 = 3\,(-23 \pm 10\,\sqrt{-6}\,)^3, \qquad j_2 = -9\,(139 \pm 102\,\sqrt{2}\,)^3.$$

**Theorem 6.1.** *With the above notations, we have* $X^+(7,3)_\varrho(\mathbb{Q}) = \{(-5:1:5)\}$.

*Proof.* For this case, it turns out that $L_3 = \mathbb{Q}(\alpha)$, with $\alpha^3 = -3$. We consider the following morphism (cf. Remark 5.2):

$$\begin{array}{ccc} X^+(7,3)_\varrho & \stackrel{\phi_\varrho}{\longrightarrow} & \mathbb{P}^2 \\ (x:y:z) & \longmapsto & (u:v:w) = (Q_{1,\varrho} : Q_{2,\varrho} : (1609x + (-12\alpha^2 + 147\alpha + 1015)z)^2). \end{array}$$

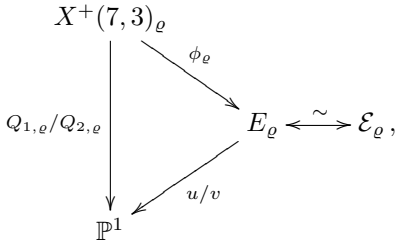
Using the rational point $\phi_\varrho(-5:1:5)$, the genus-one curve $E_\varrho = \phi_\varrho\left(X^+(7,3)_\varrho\right)$ can be shown to be isomorphic to

$$\mathcal{E}_\varrho:\ Y^2 = X^3 + (-2\alpha^2 + 2\alpha - 2)X^2 + (-189\alpha^2 + 315\alpha - 441)X.$$

The equation for $E_\varrho$ and the map $X^+(7,3)_\varrho \longrightarrow \mathcal{E}_\varrho$ are both too horrible to reproduce here, but the information above is sufficient to recover them using a computer algebra system. We find that

$$\frac{u}{v} = \frac{(2\alpha^2 - 6\alpha + 2)Y - X^2 + (-8\alpha^2 + 4\alpha - 8)X - 9\alpha^2 - 9\alpha - 45}{3(X^2 + (-14\alpha^2 + 22\alpha - 30)X + (15\alpha^2 - 9\alpha - 45))}.$$

We have the following commutative diagram:




where $Q_{1,\varrho}/Q_{2,\varrho} : X^+(7,3)_\varrho \longrightarrow \mathbb{P}^1$ is defined over $\mathbb{Q}$ and all other maps are defined over $L_3$. It follows that

$$X^+(7,3)_\varrho(\mathbb{Q}) \subseteq (Q_{1,\varrho}/Q_{2,\varrho})^{-1}\left(\mathbb{P}^1(\mathbb{Q}) \cap (u/v)(E_\varrho(L_3))\right).$$

We can then use Chabauty-type methods as developed in [Bru03] to compute the intersection $\mathbb{P}^1(\mathbb{Q}) \cap (u/v)(E_\varrho(L_3))$.

First note that a full 2-descent on the curve

$$\mathcal{E}'_\varrho:\ y^2 = x^3 + (4\alpha^2 - 4\alpha + 4)x^2 + (768\alpha^2 - 1280\alpha + 1792)x,$$

which is isogenous to $\mathcal{E}_\varrho$ over $L_3$, shows that $\mathcal{E}'_\varrho(L_3)$ is of rank at most one, and therefore $\mathcal{E}_\varrho(L_3)$ is as well. In fact, one can check that

$$\mathcal{E}_\varrho(L_3) \simeq \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z},$$

where

$$\mathfrak{t}_1 = (0,0) \ \text{ and } \ \mathfrak{t}_2 = (-7\alpha^2 + 7\alpha - 7, 0)$$

generate the 2-torsion and

$$\mathfrak{g} = ((-3\alpha^2 + 18\alpha - 27)/4, (111\alpha^2 - 243\alpha + 360)/8)$$

is a non-torsion point in $\mathcal{E}_\varrho(L_3)$.

We consider the rank-one module $\overline{\mathcal{E}_\varrho(L_3)}$ that $\mathcal{E}_\varrho(L_3)$ generates over $\mathbb{Z}_5$ inside $\mathcal{E}_\varrho(L_3 \otimes \mathbb{Q}_5)$, viewed as a three-dimensional compact algebraic group $A$ over $\mathbb{Q}_5$. The inverse image of $\mathbb{P}^1(\mathbb{Q}_5)$ under $u/v$ yields a one-dimensional subvariety $R$ over $A$. The points we are interested in lie in the intersection $\overline{\mathcal{E}_\varrho(L_3)} \cap R$, which

is an intersection of two one-dimensional 5-adic analytic varieties inside a compact three-dimensional ambient space $A$. One would expect only finitely many points in this intersection, and this is indeed the case.

In fact, one can check that, from the fact that $\langle \mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{g} \rangle \subset \mathcal{E}_\varrho(L_3)$ is 5-saturated, it follows that $\langle \mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{g} \rangle$ generates $\overline{\mathcal{E}_\varrho(L_3)}$. By making 5-adic power series expansions locally for $\langle \mathfrak{t}_1, \mathfrak{t}_2, \mathfrak{g} \rangle \cap R$, one can verify that all points $P \in \overline{\mathcal{E}_\varrho(L_3)}$ mapping to $\mathbb{P}^1(\mathbb{Q}_5)$ under $u/v$ have $(u/v)(P) = -1/3$. There are routines available in Magma to verify these computations.

Finally, it is easily checked that the only rational point on $X^+(7,3)_\varrho$ satisfying $Q_{1,\varrho}/Q_{2,\varrho} = -1/3$ is $(-5:1:5)$, which proves our claim. □

**Example 2.** Consider the surjective Galois representation $\varrho : \mathrm{G}_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{F}_3)$ defined up to conjugation by the splitting field of the irreducible polynomial

$$f(X) = X^4 - X^3 - 6X^2 + 10X - 10\,.$$

The discriminant of $f$ equals $-2^2\,3^3\,5^2\,11^2$. A model for $X(7,3)_\varrho \longrightarrow X^+(7,3)_\varrho$ is given by

$$R^2 = 11\,Q_{1,\varrho}(X,Y,Z)\,, \quad S^2 = 11\,Q_{3,\varrho}(X,Y,Z)\,, \quad RS = 11\,Q_{2,\varrho}(X,Y,Z)\,,$$

where

$$\begin{aligned} Q_{1,\varrho} &= 495\left(19X^2 - 180XY - 6XZ + 412Y^2 + 4YZ + 3Z^2\right), \\ Q_{3,\varrho} &= 660\left(-23X^2 + 172XY - 6XZ - 508Y^2 + 60YZ + Z^2\right), \\ Q_{2,\varrho} &= 990\left(-X^2 + 68XY - 8XZ - 244Y^2 + 16YZ + Z^2\right). \end{aligned}$$

The curve $X^+(7,3)_\varrho$ has (at least) the rational points $(0:0:1)$ and $(5:1:1)$. The $t$-values corresponding to these points are $t_1 = 19$, $t_2 = 41$, $t_3 = -27/2$ and $t_4 = -443/32$, and the corresponding $j$-invariants for the associated quadratic $\mathbb{Q}$-curves of degree 7 are

$$\begin{aligned} j_1 &= 4\left(360 \pm 24\sqrt{165}\right)^3, \\ j_2 &= 2\left(2685 \pm 207\sqrt{165}\right)^3, \\ j_3 &= 1/2^7\left(\left(-75 \pm 17\sqrt{-55}\right)/2\right)^3, \\ j_4 &= 1/2^{35}\left(\left(-81195 \pm 7641\sqrt{-55}\right)/2\right)^3. \end{aligned}$$

We now find that $L_3 = \mathbb{Q}(\alpha)$, where $\alpha^3 = 2$, and that $E_\varrho$ is isomorphic to the quadratic twist of $X_0(21)$ by $7\alpha^2 + 16\alpha + 13$. As it turns out, $E_\varrho(L_3)$ is of rank three, so an argument along the line of the proof of Theorem 6.1 does not work.

Instead, we pass to the unramified double covers $X(7,3)_{\varrho,\,m}$. Recall that any rational point on $X^+(7,3)_\varrho$ lifts to $X(7,3)_{\varrho,\,m}$ for some $m$. Local arguments show that $X(7,3)_{\varrho,\,m}(\mathbb{Q})$ is empty if $m$ is not equivalent to $-55$ or 165. In fact, $(5:1:1)$ and $(0:0:1)$ give rise to $m = -55$ and $m = 165$, respectively. The corresponding genus-two quotients $\widetilde{C}_{\varrho,\,m}$ admit models

$$\begin{aligned} C_{\varrho,-55} \quad &: \quad y^2 = -220\Big(x^3 - \frac{1}{2}\Big)\Big(x^3 + \frac{27}{2}\Big), \\ C_{\varrho,165} \quad &: \quad y^2 = \phantom{-}660\Big(x^3 - \frac{1}{2}\Big)\Big(x^3 + \frac{27}{2}\Big). \end{aligned}$$

In the two lemmata below, we prove that each of these curves has exactly two rational points, sharing the same $x$-coordinate. Moreover, for $(X_0 : Y_0 : Z_0)$ equal to $(5 : 1 : 1)$ or $(0 : 0 : 1)$, the only rational point on $X^+(7,3)_\varrho$ satisfying equation (9) is $(X_0 : Y_0 : Z_0)$. It follows then the following result.

**Theorem 6.2.** *With the above notations,* $X^+(7,3)_\varrho(\mathbb{Q}) = \{(5 : 1 : 1), (0 : 0 : 1)\}$.

**Lemma 6.1.** *The genus-two curve* $C_{\varrho,-55}$ *has* $C_{\varrho,-55}(\mathbb{Q}) = \{(3/4, \pm 495/32)\}$.

*Proof.* We write $\alpha = \sqrt[3]{2}$ and $C = C_{\varrho,-55}$. It is easily checked that the nonsingular projective closure of $C$ does not have rational points above $x = \infty$. We note that, for any rational point $(x, y) \in C(\mathbb{Q})$, there exist $\delta, y_1, y_2 \in \mathbb{Q}(\alpha)$ such that

$$\begin{cases} \delta\, y_1^2 &= (x^2 - \frac{3}{2}\,\alpha^2 x + \frac{9}{2}\,\alpha) \\ -220\,\mathrm{Norm}(\delta)\,\delta\, y_2^2 &= (x - \frac{1}{2}\,\alpha^2)(x + \frac{3}{2}\,\alpha^2)(x^2 + \frac{1}{2}\,\alpha^2 x + \frac{1}{2}\,\alpha) \end{cases}$$

In fact, local considerations show that, without loss of generality, we can assume $\delta = 4\alpha^2 + 6\alpha + 9$. Hence, the question is reduced to proving that $x = 3/4$ is the only rational value such that

$$D\colon\ y_2^2 = (4\alpha^2 + 6\alpha + 9)\Big(x^4 + \frac{3\alpha^2}{2}\,x^3 - \frac{1}{2}\,x - \frac{3\alpha^2}{4}\Big)$$

has a solution with $y_2 \in \mathbb{Q}(\alpha)$. We find that the curve $D$ is isomorphic to

$$V^2 = (-10\alpha^2 - 5)\big(U^3 + 2U^2 + \frac{7}{3}\,U\big).$$

A 2-descent on this elliptic curve gives a rank bound of three, but a 2-descent on the 2-isogenous curve shows that the rank of this curve over $\mathbb{Q}(\alpha)$ is actually one. A maximal rank subgroup is generated by

$$\begin{aligned}(U, V) = \quad & (0, 0), \\ & ((-72\alpha^2 - 96\alpha - 123)/5, (2872\alpha^2 + 3616\alpha + 4548)/5).\end{aligned}$$

Using this, it is straightforward to verify using a Chabauty-type argument locally at 31 that there are only two points in $D(\mathbb{Q}(\alpha))$ with $\mathbb{Q}$-rational $x$-coordinate. □

**Lemma 6.2.** *The genus-two curve* $C_{\varrho,165}$ *has* $C_{\varrho,165}(\mathbb{Q}) = \{(-3, \pm 495)\}$.

*Proof.* We proceed similarly to the proof of Lemma 6.1. We use two factorisations, however. When we find a point $(x, y) \in C(\mathbb{Q}(\alpha))$ with $x \in \mathbb{Q}$, then there exist $y_1, y_2, y_3, y_4, \epsilon, \delta \in \mathbb{Q}(\alpha)$ such that

$$\begin{cases} \delta\, y_1^2 &= (x^2 - \frac{3}{2}\,\alpha^2 x + \frac{9}{2}\,\alpha) \\ 660\,\mathrm{Norm}(\delta)\,\delta\, y_2^2 &= (x - \frac{1}{2}\,\alpha^2)(x + \frac{3}{2}\,\alpha^2)(x^2 + \frac{1}{2}\,\alpha^2 x + \frac{1}{2}\,\alpha) \\ \epsilon\, y_3^2 &= (x^2 + \frac{1}{2}\,\alpha^2 x + \frac{1}{2}\,\alpha) \\ 660\,\mathrm{Norm}(\epsilon)\,\epsilon\, y_4^2 &= (x - \frac{1}{2}\,\alpha^2)(x + \frac{3}{2}\,\alpha^2)(x^2 - \frac{3}{2}\,\alpha^2 x + \frac{9}{2}\,\alpha) \end{cases}$$

In fact, using local arguments, we can limit ourselves to the cases

$$(\delta, \epsilon) \in \{(9\alpha^2 - 3\alpha + 1, \alpha^2 + \alpha + 1), (4\alpha^2 + 6\alpha + 9, -\alpha^2 + 2\alpha + 1), (\alpha^2 + \alpha + 1, 9\alpha^2 - 3\alpha + 1)\}.$$

For $\delta = 9\alpha^2 - 3\alpha + 1$, we find that the corresponding quartic is isomorphic to

$$V^2 = (3\alpha + 1)\big(U^3 + 2U^2 + \frac{7}{3}\,U\big),$$

that its Mordell-Weil group is of rank two and that a subgroup of index prime to 12 is generated by

$$\begin{aligned}(U,V) = \quad & (0,0),\\ & ((8\alpha^2+4\alpha-13)/15, (4\alpha^2-8\alpha+36)/15),\\ & ((589\alpha^2-805\alpha+184)/198, (2084\alpha^2-5080\alpha+2489)/198).\end{aligned}$$

A simple combinatorial argument mod 43 shows that none of the $\mathbb{Q}(\alpha)$-points have $\mathbb{Q}$-rational $x$-coordinate.

For $\delta = 4\alpha^2+6\alpha+9$, we find that the corresponding quartic is isomorphic to

$$V^2 = (-10\alpha+15)\big(U^3+2U^2+\frac{7}{3}U\big).$$

A 2-isogeny descent on this curve yields a rank bound of three, but a further second descent on the homogeneous spaces resulting from the 2-isogeny descent show that the rank is really one. A maximal rank subgroup of index prime to 2 is generated by

$$\begin{aligned}(U,V) = \quad & (0,0),\\ & ((-7\alpha^2+28\alpha-7)/15, (-7\alpha^2+168\alpha-140)/15).\end{aligned}$$

Again, a simple combinatorial argument mod 43 shows that none of the $\mathbb{Q}(\alpha)$-points have $\mathbb{Q}$-rational $x$-coordinate.

For the third case, we were unable to find sufficient generators for the Mordell-Weil group of the quartic involving $\delta$. Therefore, we use the curve associated with the corresponding value of $\epsilon$, for which we were able to find all generators. We find that the quartic corresponding to $\epsilon = 9\alpha^2-3\alpha+1$ is isomorphic to

$$V^2 = (-8\alpha^2-11\alpha-15)\big(U^3+2U^2+\frac{7}{3}U\big),$$

with a Mordell-Weil group of rank two. A maximal rank subgroup of index prime to 2 and to 127 is generated by

$$\begin{aligned}(U,V) = \quad & (0,0),\\ & (-4\alpha^2-4\alpha-7, (-304\alpha^2-380\alpha-484)/3),\\ & ((-865\alpha^2-2645\alpha+2990)/594, (40825\alpha^2-21565\alpha+5575)/1782).\end{aligned}$$

A Chabauty-type argument at 127, along with combinatorial information mod 31 and 43, shows that $x=-3$ is the only rational $x$-coordinate occurring for points on the above elliptic curve which are defined over $\mathbb{Q}(\alpha)$. This completes the proof. □

## References


[Bar99] F. Bars. Bielliptic modular curves. *J. Number Theory*, 76(1):154–165, 1999.

[BGGP05] Matthew H. Baker, Enrique González-Jiménez, Josep González, and Bjorn Poonen. Finiteness results for modular curves of genus at least 2. *Amer. J. Math.*, 127(6):1325–1387, 2005.

[BH03] M. Baker and Y. Hasegawa. Automorphisms of $X_0^*(p)$. *J. Number Theory*, 100(1):72–87, 2003.

[Bru03] N. Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[Bru04] N. Bruin. The arithmetic of Prym varieties in genus 3. *Preprint*, 2004.

[Dol] I. Dolgachev. *Topics in Classical Algebraic Geometry. Part I.* Private Lecture Notes in: http://www.math.Isa.umich.edu/ idolga/.

[Elk90] N.D. Elkies. The automorphism group of the modular curve $X_0(63)$. *Compositio Math.*, 74(2):203–208, 1990.

[ES01] J.S. Ellenberg and C. Skinner. On the modularity of $\mathbb{Q}$-curves. *Duke Math. J.*, 109(1):97–122, 2001.

[Fer04] J. Fernández. A moduli approach to quadratic $\mathbb{Q}$-curves realizing projective mod $p$ Galois representations. *Preprint*, 2004. Available at `http://www.math.leidenuniv.nl/gtem`.

[FGL] J. Fernández, J. González, and J.-C. Lario. Plane quartic twists of $X(5,3)$. *To appear in Canad. Math. Bull.*

[FLR02] J. Fernández, J.-C. Lario, and A. Rio. Octahedral Galois representations arising from $\mathbb{Q}$-curves of degree 2. *Canad. J. Math.*, 54(6):1202–1228, 2002.

[GJG03] E. González-Jiménez and J. González. Modular curves of genus 2. *Math. Comp.*, 72(241):397–418 (electronic), 2003.

[GJGG02] E. González-Jiménez, J. González, and J. Guàrdia. Computations on modular Jacobian surfaces. In *Algorithmic number theory (Sydney, 2002)*, volume 2369 of *Lecture Notes in Comput. Sci.*, pages 189–197. Springer, Berlin, 2002.

[GL98] J. González and J.-C. Lario. Rational and elliptic parametrizations of $\mathbb{Q}$-curves. *J. Number Theory*, 72(1):13–31, 1998.

[Gon91] J. González. Equations of hyperelliptic modular curves. *Ann. Inst. Fourier (Grenoble)*, 41(4):779–795, 1991.

[KM88] M. A. Kenku and F. Momose. Automorphism groups of the modular curves $X_0(N)$. *Compositio Math.*, 65(1):51–80, 1988.

[Lig77] G. Ligozat. Courbes modulaires de niveau 11. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 149–237. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.

[Mag] Magma. The magma computational algebra system. `Available from http://magma.maths.usyd.edu.au/magma/`.

[Maz77] B. Mazur. Rational points on modular curves. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 107–148. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.

[Ogg74] A. P. Ogg. Hyperelliptic modular curves. *Bull. Soc. Math. France*, 102:449–462, 1974.

[Shi71] G. Shimura. *Introduction to the arithmetic theory of automorphic functions.* Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.

Department of Mathematics, Simon Fraser University, Burnaby, BC, Canada V5A 1S6
*E-mail address*: `nbruin@cecm.sfu.ca`

Facultat de Matemàtiques i Estadística, Universitat Politècnica de Catalunya, Pau Gargallo 5, 08028 Barcelona, Spain
*E-mail address*: `julio@mat.upc.edu, josepg@mat.upc.edu, joan.carles.lario@upc.edu`