Canad. Math. Bull. Vol. **50** (2), 2007 pp. 196–205

Plane Quartic Twists of $X(5,3)$

Dedicated to Pilar Bayer on her sixtieth birthday

Julio Fernández, Josep González and Joan-C. Lario

Abstract. Given an odd surjective Galois representation $\varrho\colon \mathrm{G}_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{F}_3)$ and a positive integer N, there exists a twisted modular curve $X(N,3)_\varrho$ defined over $\mathbb{Q}$ whose rational points classify the quadratic $\mathbb{Q}$-curves of degree N realizing ϱ. This paper gives a method to provide an explicit plane quartic model for this curve in the genus-three case $N = 5$.

1 Introduction

Let p be an odd prime. The so-called $\mathbb{Q}$-curves (non-CM elliptic curves over $\overline{\mathbb{Q}}$ that are isogenous to all their Galois conjugates) are a source of representations of the absolute Galois group $\mathrm{G}_{\mathbb{Q}}$ into $\mathrm{PGL}_2(\mathbb{F}_p)$. We refer to [FLR02, Fer04] for a detailed construction of the odd representation $\varrho_{E,p}\colon \mathrm{G}_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{F}_p)$ arising from the p-torsion of a $\mathbb{Q}$-curve E. It seems natural to ask for the *frequency* of such representations $\varrho_{E,p}$ among all odd 2-dimensional projective mod p Galois representations. We say that a $\mathbb{Q}$-curve E *realizes* a given representation $\varrho\colon \mathrm{G}_{\mathbb{Q}} \to \mathrm{PGL}_2(\mathbb{F}_p)$ if $\varrho_{E,p} = \varrho$ up to conjugation in $\mathrm{PGL}_2(\mathbb{F}_p)$.

The moduli problem classifying the quadratic $\mathbb{Q}$-curves that realize such a representation ϱ is the subject of the Ph.D. thesis of the first author [Fer03]. The problem splits into different cases depending on the value mod p of the eventual degrees N for the isogeny from the $\mathbb{Q}$-curve to its Galois conjugate. For N non-square mod p, the representation ϱ cannot have cyclotomic determinant for it to be realized by quadratic $\mathbb{Q}$-curves of degree N, and such $\mathbb{Q}$-curves are then given by the rational points on some twist of a modular curve $X(N,p)$. The aim of this paper is to explain a method to obtain good models over $\mathbb{Q}$ for some of these twisted curves, namely for those corresponding to the octahedral genus-three case $N = 5$, $p = 3$.

In Section 2 we briefly introduce the modular curve $X(N,p)$ and its twists $X(N,p)_\varrho$. We refer to [Fer04] for this section. In Section 3 we give a plane quartic model for $X(5,3)$ along with an explicit description of the natural map $X(5,3) \to X^+(5)$. An algorithm to produce a plane quartic model for $X(5,3)_\varrho$ whenever ϱ is surjective is then explained in Section 4, where the input is given by a degree-four polynomial in $\mathbb{Z}[X]$ having the same splitting field as ϱ. Finally, in Section 5 we present an example illustrating that all computations can be carried out by any of the available standard algebraic manipulation systems. We also compute by hand some rational points on the resulting quartic model and show that the Chabauty–Coleman method fails to be of use in this case. The authors expect that some other developing

Received by the editors February 7, 2005.
AMS subject classification: 11F03, 11F80, 14G05.

techniques to determine the set of all rational points on small genus curves can be applied to the models provided by the method described in the paper.

2 The Twisted Modular Curve $X(N,p)_\varrho$

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 [Lig77, §II.3] and [Maz77, §2]. Its $\mathbb{Q}$-isomorphism class does not depend on the choice of such a matrix. We denote by $\mathcal{W}(N,p)$ the automorphism group of the covering $X(N,p) \longrightarrow X^+(N)$, where $X^+(N)$ is the quotient of $X_0(N)$ by the Atkin–Lehner involution w_N. We recall that the rational points on $X^+(N)$ yield the isomorphism classes of quadratic $\mathbb{Q}$-curves of degree N up to Galois conjugation.

Assume N to be a non-square mod p. The automorphism group $\mathcal{W}(N,p)$ is then canonically isomorphic to $\mathrm{PGL}_2(\mathbb{F}_p)$. If we put w for the involution on $X(N,p)$ corresponding through this isomorphism to the above matrix V and identify $\mathcal{W}(N,p)$ with its (inner) automorphism group, the Galois action on $\mathcal{W}(N,p)$ is given by the morphism

$$\varepsilon\colon \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathbb{F}_p^*/\mathbb{F}_p^{*2} \simeq \langle w\rangle \hookrightarrow \mathcal{W}(N,p)$$

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

Suppose that we are now given a surjective Galois representation

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

with non-cyclotomic determinant. A $\mathbb{Q}$-curve of degree N realizing ϱ must then be defined over the quadratic field attached to the Galois character

$$\varepsilon\det\varrho\colon \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathbb{F}_p^*/\mathbb{F}_p^{*2} \simeq \{\pm 1\}.$$

For the moduli classification of such $\mathbb{Q}$-curves, we produce a twist of $X(N,p)$ from a certain element in the cohomology set $H^1(\mathrm{G}_{\mathbb{Q}},\mathcal{W}(N,p))$. Specifically, we take the 1-cocycle $\xi = \varrho\varepsilon$, where we view ϱ as a map onto $\mathcal{W}(N,p)$ through the above canonical isomorphism:

$$\varrho\colon \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p) \xrightarrow{\simeq} \mathcal{W}(N,p).$$

For the twist of $X(N,p)$ attached to ξ, we fix a rational model $X(N,p)_\varrho$ along with an isomorphism

$$\Psi\colon X(N,p)_\varrho \longrightarrow X(N,p)$$

satisfying $\Psi = \xi_\sigma{}^\sigma\Psi$ for every σ in $\mathrm{G}_{\mathbb{Q}}$. We note that the $\mathbb{Q}$-isomorphism class of $X(N,p)_\varrho$ is an invariant of the conjugacy class of ϱ. In other words, it only depends on the splitting field of ϱ, since every automorphism of $\mathrm{PGL}_2(\mathbb{F}_p)$ is inner.

Theorem 2.1 *There exists a quadratic $\mathbb{Q}$-curve of degree N realizing ϱ if and only if the set of non-cuspidal non-CM rational points on the curve $X(N,p)_\varrho$ is nonempty. In this case, the composition*

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

https://doi.org/10.4153/CMB-2007-021-8 Published online by Cambridge University Press

defines a one-to-one correspondence between this set of points and the set of isomorphism classes of quadratic $\mathbb{Q}$-curves of degree N up to Galois conjugation realizing ϱ.

Remark 2.2 The genus of $X(N, p)$ is never two, and the only genus-three case appears for $N = 5$ and $p = 3$.

3 A Plane Quartic Model for $X(5, 3)$

The automorphism of the complex upper-half plane given by $\tau \mapsto \tau/3$ induces an isomorphism

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

defined over $\mathbb{Q}$, so that $\Phi^*(\mathbb{Q}(X_0(9N)))$ is the function field of the rational model for $X(N, 3)$ fixed in the previous section. Moreover, the above involution w on $X(N, 3)$ can be chosen to correspond through Φ to the Atkin–Lehner involution w_N on $X_0(9N)$. From now on, we take $N = 5$ and ease the notation as follows: for a function $x \in \mathbb{Q}(X_0(45))$, a regular differential $\omega \in \Omega^1(X_0(45))$ or an automorphism $W \in \mathrm{Aut}(X_0(45))$, we put $\overline{x} = \Phi^*(x)$, $\overline{\omega} = \Phi^*(\omega)$, $\overline{W} = \Phi^{-1}W\Phi$ for the corresponding function, differential or automorphism on $X(5, 3)$.

3.1 An Equation for $X_0(45)$

The jacobian of $X_0(45)$ is $\mathbb{Q}$-isogenous to $J_0(15)^2 \times J_0(45)^{\mathrm{new}}$, where $J_0(15)$ and $J_0(45)^{\mathrm{new}}$ are elliptic curves over $\mathbb{Q}$ of conductors 15 and 45, respectively. A basis for the $\mathbb{Q}$-vector space $\Omega^1_{\mathbb{Q}}(X_0(45))$ is given by

$$\omega_1 = f_1(q)\frac{dq}{q}, \quad \omega_2 = f_1(q^3)\frac{dq}{q}, \quad \omega_3 = f_2(q)\frac{dq}{q},$$

where f_1 and f_2 are the normalized weight-two newforms of levels 15 and 45, respectively:

$$\begin{aligned} f_1 &= q - q^2 - q^3 - q^4 + q^5 + q^6 + 3q^8 + q^9 - q^{10} - 4q^{11} + q^{12} \\ &\quad - 2q^{13} - q^{15} - q^{16} + 2q^{17} + \cdots \\ f_2 &= q + q^2 - q^4 - q^5 - 3q^8 - q^{10} + 4q^{11} - 2q^{13} - q^{16} - 2q^{17} + \cdots \end{aligned}$$

The genus-three curve $X_0(45)$ is nonhyperelliptic (see [Ogg74]), so the image of $X_0(45)$ under the canonical embedding is the zero locus of a homogenous polynomial P in $\mathbb{Q}[X, Y, Z]$ of degree 4. Such a polynomial P, unique up to non-zero rational multiples, satisfies $P(\omega_1, \omega_2, \omega_3) = 0$ and can be explicitly determined using the first seventeen Fourier coefficients of each ω_i (see [BGGP, §2]). This yields the following affine equation for $X_0(45)$:

$$x^4 - 2x^2y^2 + 81y^4 - 2x^2 - 16xy - 18y^2 + 1 = 0, \tag{1}$$

where $x = \omega_1/\omega_3$ and $y = \omega_2/\omega_3$. In particular, $\mathbb{Q}(X(5, 3)) = \mathbb{Q}(\overline{x}, \overline{y})$.

https://doi.org/10.4153/CMB-2007-021-8 Published online by Cambridge University Press

3.2 The Group $\mathrm{Aut}(X_0(45))$

The group $\mathrm{Aut}\,(X_0(45))$ is generated by the Atkin–Lehner involutions w_5, w_9 and the automorphism S induced by the map $\tau \mapsto \tau + 1/3$ on the complex upper-half plane (see [KM88, LN64]). The action of these generators on $\Omega^1(X_0(45))$ is displayed in the following table:

	w_5	w_9	S
ω_1	$-\omega_1$	$3\omega_2$	$-1/2\omega_1 - 3/2\omega_2 + \sqrt{-3}/2\omega_3$
ω_2	$-\omega_2$	$1/3\omega_1$	ω_2
ω_3	ω_3	$-\omega_3$	$\sqrt{-3}/2\omega_1 + \sqrt{-3}/2\omega_2 - 1/2\omega_3$

It can be easily checked from these relations that $\mathrm{Aut}(X_0(45))$ has the same order as $\mathrm{PGL}_2(\mathbb{F}_3)$, so that $\mathrm{Aut}(X(5,3)) = \mathcal{W}(5,3) = \langle \overline{w}_5, \overline{w}_9, \overline{S}\rangle \simeq \mathrm{PGL}_2(\mathbb{F}_3)$. Let us also note that $\mathrm{Aut}_{\mathbb{Q}}(X_0(45))$ is the subgroup of Atkin–Lehner involutions, while the automorphism S is defined over the quadratic field $\mathbb{Q}(\sqrt{-3})$ and satisfies ${}^{\nu}S = S^2$ for the non-trivial automorphism $\nu \in \mathrm{Gal}(\mathbb{Q}(\sqrt{-3})/\mathbb{Q})$. In particular, the group $\langle w_9 S w_9\rangle$ is $\mathrm{G}_{\mathbb{Q}}$-stable. As a matter of fact, the degree-three covering $X_0(45) \to X_0(45)/\langle w_9 S w_9\rangle$ is the natural projection $X_0(45) \to X_0(15)$, since the pullback of $\Omega^1_{\mathbb{Q}}(X_0(45)/\langle w_9 S w_9\rangle)$ is $\langle \omega_1\rangle$.

3.3 The Covering $X(5,3) \to X^+(5)$

Consider the composition $X_0(45) \stackrel{\pi_1}{\to} X_0(15) \stackrel{\pi_2}{\to} X_0(5) \stackrel{\pi_3}{\to} X^+(5)$, where π_1, π_2 and π_3 are the natural projections. We fix for $X_0(45)$ the model given by equation (1). For $X_0(15)$, we take the minimal equation

$$v^2 + uv + v = u^3 + u^2 - 10u - 10 \tag{2}$$

given in [Cre97], where the functions $u, v \in \mathbb{Q}(X_0(15))$ have a unique pole at the cusp ∞ with respective multiplicities 2 and 3:

$$u = \frac{1}{q^2} + \frac{1}{q} + 1 + 2q + 4q^2 + \cdots \qquad v = \frac{1}{q^3} + \frac{1}{q^2} + \frac{2}{q} + 3 + 2q + 5q^2 + \cdots$$

As for the function fields of $X_0(5)$ and $X^+(5)$, we take the following generators over $\mathbb{Q}$, respectively:

$$G(\tau) = \left(\frac{\eta(\tau)}{\eta(5\tau)}\right)^6 = \frac{1}{q} - 6 + 9q + 10q^2 + \cdots$$

$$t(\tau) = G(\tau) + \frac{5^3}{G(\tau)} = \frac{1}{q} - 6 + 134q + 760q^2 + \cdots$$

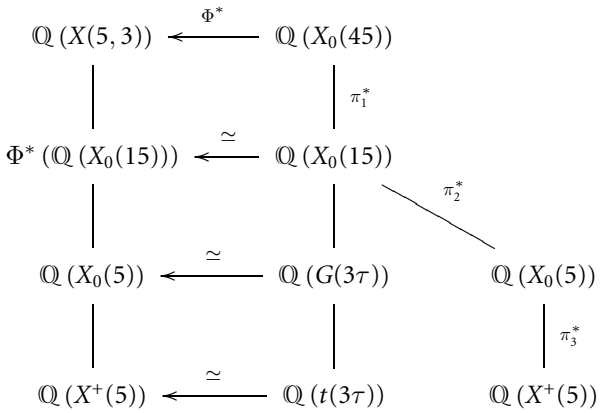
https://doi.org/10.4153/CMB-2007-021-8 Published online by Cambridge University Press

where η denotes the Dedekind function on the complex upper-half plane. The field $\mathbb{Q}(X_0(5))$ is generated over $\mathbb{Q}(X^+(5))$ by the elliptic modular function j, and the relation between the functions j and t can be computed by using the procedure described in [GL98]:

$$j^2 - (t^5 + 30t^4 - 310t^3 - 13700t^2 - 38424t + 614000)\,j + (t^2 + 260t + 5380)^3 = 0.$$

The j-invariants of quadratic $\mathbb{Q}$-curves of degree 5 are obtained from this equation by rational values of the function t.

Through the above isomorphism Φ, the functions $G(3\tau)$ and $t(3\tau)$ can be viewed inside $\mathbb{Q}(X(5,3))$, as the following diagram shows:



In order to give an explicit description of the extension $\mathbb{Q}(X(5,3))/\mathbb{Q}(X^+(5))$ on the left column of the diagram, we begin by recalling that π_1 is in fact the projection $X_0(45) \to X_0(45)/\langle w_9 S w_9 \rangle$. We now consider the following functions on $X_0(45)$:

$$U = \frac{(-3 + x + 9y)(3 + x + 9y)}{4x^2}, \quad V = \frac{9(3 + x^2 + 18xy + 81y^2)}{4x^3}.$$

They are invariant by $w_9 S w_9$ and satisfy $[\mathbb{Q}(X_0(45)) : \mathbb{Q}(U,V)] = 3$, so they generate the function field of $X_0(15)$ over $\mathbb{Q}$. Using the q-expansions of the above functions u and v, we obtain the following identities:

$$u = \frac{Q(U,V)}{2(10 + 2U + 3U^2 - 2V)^2}, \quad v = \frac{R(U,V)}{2(10 + 2U + 3U^2 - 2V)^3},$$

where

$$\begin{aligned} Q(U,V) &= -1300 - 520U - 477U^2 + 19U^3 - 17U^4 + (260 + 52U + 33U^2)V, \\ R(U,V) &= 9\left(1000 - 1900U - 630U^2 - 1237U^3 - 39U^4 - 121U^5 + 2U^6\right) \\ &\quad + 9(-200 + 420U + 82U^2 + 131U^3 + 2U^4)V. \end{aligned}$$

https://doi.org/10.4153/CMB-2007-021-8 Published online by Cambridge University Press

By applying Φ^* to the resulting expressions of u and v in terms of x, y, that is, by changing x, y, u, v by $\overline{x}, \overline{y}, \overline{u}, \overline{v}$, respectively, in the above relations, we get a description of the subextension $\mathbb{Q}(X(5,3))/\Phi^*(\mathbb{Q}(X_0(15)))$. All we have to do then is to give 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. Now, $G(3\tau)$ has exactly two poles at the cusps $1/5$ and ∞ of $X_0(15)$ with multiplicities 1 and 3, respectively. Since the function

$$H(\tau) = \frac{\eta(3\tau)\eta(5\tau)^5}{\eta(\tau)\eta(15\tau)^5} = \frac{1}{q^2} + \frac{1}{q} + 2 + 2q + 4q^2 + \cdots$$

lies in $\mathbb{Q}(X_0(15))$ and has divisor $2(1/5) - 2(\infty)$, we get $H = u + 1$. Then, the function $(u+1)G(3\tau)$ has a unique pole at ∞ (with multiplicity 5), so it must be a polynomial in u and v. Using again the q-expansions of u and v, we obtain

$$G(3\tau) = \frac{uv - u^2 - 9u - 8}{u+1},$$

hence

$$t = \frac{189 + 205\overline{u} + 7\overline{u}^2 + \overline{u}^3 + \overline{u}^4 - 16\overline{uv} - 3\overline{u}^2\overline{v}}{\overline{uv} - \overline{u}^2 - 9\overline{u} - 8}. \tag{3}$$

4 A Plane Quartic Model for $X(5,3)_\varrho$

The background strategy in this section is the same as in Subsection 3.1: a plane quartic model for $X(5,3)_\varrho$ over $\mathbb{Q}$ can be theoretically obtained from a basis of the 3-dimensional $\mathbb{Q}$-vector space $\Omega^1_{\mathbb{Q}}(X(5,3)_\varrho)$. So our problem amounts to giving an explicit enough description of this space.

We recall that ϱ stands for any fixed representation of $\mathrm{G}_{\mathbb{Q}}$ onto $\mathrm{PGL}_2(\mathbb{F}_3)$ with non-cyclotomic determinant. It is determined by its splitting field L up to conjugation in $\mathrm{PGL}_2(\mathbb{F}_3)$, and the condition on the determinant amounts to saying that L does not contain $\sqrt{-3}$. Put $K = L(\sqrt{-3})$ and denote by ν the non-trivial element in $\mathrm{Gal}(K/L)$. Since $\mathrm{PGL}_2(\mathbb{F}_3)$ is isomorphic to the symmetric group $\mathfrak{S}_4$, we can take as input data a quartic polynomial $f \in \mathbb{Z}[X]$ with splitting field L and identify $\mathrm{Gal}(L/\mathbb{Q})$ with $\mathfrak{S}_4$ by fixing an order of the roots of f. For convenience, we take as generators for this Galois group the following permutations:

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

Consider on $\Omega^1_{\overline{\mathbb{Q}}}(X(5,3)) = \Omega^1_{\mathbb{Q}}(X(5,3)) \otimes \overline{\mathbb{Q}}$ the Galois action twisted by the 1-cocycle ξ obtained from ϱ as in Section 2. It is defined by

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

for $\omega \in \Omega^1_{\mathbb{Q}}(X(5,3))$, $\gamma \in \overline{\mathbb{Q}}$ and $\sigma \in \mathrm{G}_{\mathbb{Q}}$. This action factors through $\mathrm{Gal}(K/\mathbb{Q})$, and the regular differentials on $X(5,3)_\varrho$ defined over $\mathbb{Q}$ can be identified via the isomorphism $\Psi\colon X(5,3)_\varrho \to X(5,3)$ with the fixed elements in $\Omega^1_K(X(5,3))$:

$$\Omega^1_{\mathbb{Q}}\left(X(5,3)_\varrho\right) = \left(\Omega^1_{\mathbb{Q}(\sqrt{-3})}(X(5,3)) \otimes L\right)^{\mathrm{Gal}(K/\mathbb{Q})}_\xi.$$

https://doi.org/10.4153/CMB-2007-021-8 Published online by Cambridge University Press

Moreover, the twisted action of $\mathrm{Gal}(K/\mathbb{Q})$ can be restricted to the 6-dimensional $\mathbb{Q}$-vector space $\Omega^1_{\mathbb{Q}(\sqrt{-3})}(X(5,3))$, for which we take the basis

$$\{\overline{\omega}_1, \overline{\omega}_2, \overline{\omega}_3, \sqrt{-3}\overline{\omega}_1, \sqrt{-3}\overline{\omega}_2, \sqrt{-3}\overline{\omega}_3\}.$$

Recall that $\omega_1, \omega_2, \omega_3$ are the forms in $\Omega^1_{\mathbb{Q}}(X_0(45))$ introduced in the previous section, while $\overline{\omega}_1, \overline{\omega}_2, \overline{\omega}_3$ are the corresponding forms in $\Omega^1_{\mathbb{Q}}(X(5,3))$. The action of the Galois generators $\sigma_1, \sigma_2, \sigma_3$ and ν on this basis is given by the matrices

$$s_1 = \begin{pmatrix} -\frac{1}{2} & 0 & 0 & 0 & 0 & -\frac{3}{2} \\ -\frac{3}{2} & 1 & 0 & 0 & 0 & -\frac{3}{2} \\ 0 & 0 & -\frac{1}{2} & -\frac{3}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & -\frac{1}{2} & 0 & 0 \\ 0 & 0 & \frac{1}{2} & -\frac{3}{2} & 1 & 0 \\ \frac{1}{2} & 0 & 0 & 0 & 0 & -\frac{1}{2} \end{pmatrix}, \quad s_2 = \begin{pmatrix} 0 & \frac{1}{3} & 0 & 0 & 0 & 0 \\ 3 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{1}{3} & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix},$$

$$s_3 = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad s_4 = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix},$$

respectively. This comes from the table in Subsection 3.2 and from the definition of the 1-cocyle ξ. Indeed, the (conjugacy class of the) representation ϱ translates into the isomorphism $\mathrm{Gal}(L/\mathbb{Q}) \simeq \mathrm{Aut}(X(5,3))$ sending $\sigma_1, \sigma_2, \sigma_3$ to $\overline{S}^{-1}, \overline{w}_9, \overline{w}_5$, respectively.

We must now look for three elements in $\Omega^1_{\mathbb{Q}(\sqrt{-3})}(X(5,3)) \otimes L$ which are linearly independent over $\mathbb{Q}$ and invariant by the above Galois action. To that end, we follow the next steps:

Step 1 Compute a basis for the ring of integers $\mathcal{O}_L$.

Step 2 Compute the 24×24 matrices $\Sigma_1, \Sigma_2, \Sigma_3$ with entries in $\mathbb{Z}$ giving the action of $\sigma_1, \sigma_2, \sigma_3$, respectively, on the integral basis of $\mathcal{O}_L$.

Step 3 Form the Kronecker products

$$\mathcal{W}_1 := s_1 \otimes \Sigma_1, \quad \mathcal{W}_2 := s_2 \otimes \Sigma_2, \quad \mathcal{W}_3 := s_3 \otimes \Sigma_3, \quad \mathcal{W}_4 := s_4 \otimes \Sigma_4,$$

where Σ_4 stands for the identity matrix Id_{24}. Then compute a basis $X_\varrho, Y_\varrho, Z_\varrho$ for the 3-dimensional vector subspace of $\Omega^1_{\mathbb{Q}(\sqrt{-3})(X(5,3))} \otimes L$ corresponding to the subspace $\bigcap_{i=1}^4 \ker(\mathcal{W}_i - \mathrm{Id}_{144})$ of $\mathbb{Q}^{144}$.

Step 4 Compute the 3×3 matrix Θ with entries in K giving the basis change

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

https://doi.org/10.4153/CMB-2007-021-8 Published online by Cambridge University Press

Replacing $X_\varrho, Y_\varrho, Z_\varrho$ by projective variables X, Y, Z, then plugging $\overline{\omega}_1, \overline{\omega}_2, \overline{\omega}_3$ into the homogenization of equation (1), and finally factoring out, one gets a plane quartic equation $F(X,Y,Z) = 0$ for the twist $X(5,3)_\varrho$ over $\mathbb{Q}$.

Remark 4.1 The interest of working with an integral basis of $\mathcal{O}_L$, instead of just using the power-basis attached to a primitive element of the extension $L/\mathbb{Q}$, is due to the fact that one obtains experimentally better models in the sense of shrinking the set of bad reduction primes for the twisted curve.

Remark 4.2 It can be easily checked that $\{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid {}^\sigma\Psi = \Psi\} = \langle \nu\sigma_3 \rangle$. Thus, the isomorphism Ψ is defined over $K^{\langle \nu\sigma_3 \rangle}$ and the entries of the above matrix Θ all belong to this extension of degree 24. We also have

$$\{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid {}^\sigma\Psi\Psi^{-1} \in \langle \overline{w}_9 \overline{S} \overline{w}_9 \rangle\} = \langle \nu\sigma_3, \sigma_2\sigma_1\sigma_2 \rangle,$$

which means that the composition

$$X(5,3)_\rho \xrightarrow{\Psi} X(5,3) \longrightarrow X(5,3)/\langle \overline{w}_9 \overline{S} \overline{w}_9 \rangle \simeq X_0(15)$$

is defined over a number field of degree 8 which is the compositum of the quadratic field k attached to the character $\varepsilon \det \varrho$ and the number field L_0 generated by the root of the quartic polynomial f fixed by the permutation $\sigma_2\sigma_1\sigma_2$.

5 An Explicit Example

All the steps in the previous section can be performed using a software package for algebraic manipulation such as Pari or Magma. As an example, we consider the surjective Galois representation $\varrho\colon \mathrm{G}_\mathbb{Q} \to \mathrm{PGL}_2(\mathbb{F}_3)$ defined up to conjugation by the splitting field of the irreducible polynomial

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

Since the discriminant of f equals -33 up to squares, the field k over which the quadratic $\mathbb{Q}$-curves realizing ϱ must be defined is $\mathbb{Q}(\sqrt{11})$ (see Section 2).

Note that if the rank of $X_0(15)(kL_0)$ is zero, where L_0 is the quartic number field defined by f (*cf.* Remark 4.2), then we do not need to compute an equation for $X(5,3)_\varrho$. Indeed, in this case the values $t \in X^+(5)(\mathbb{Q})$ obtained from the torsion points of $X_0(15)(kL_0)$ using (3) would provide us with a finite set of candidate $\mathbb{Q}$-curves E, and then it would suffice to check whether $\varrho_{E,3} = \varrho$ or not for each of them. In our example, this strategy does not apply, since the rank of $X_0(15)(k)$, which can be computed using Magma v2.11, is one.

The procedure described in the previous section allows us to obtain the following projective model for $X(5,3)_\varrho$:

$$\begin{aligned} &-9XY(2X+Y)(9X+8Y) + 9(6X^3 + 62X^2Y + 66XY^2 + 15Y^3)Z \\ &\qquad + 3(27X^2 - 104XY - 83Y^2)Z^2 - 3(94X + 7Y)Z^3 + 191Z^4 = 0. \end{aligned}$$

https://doi.org/10.4153/CMB-2007-021-8 Published online by Cambridge University Press

We have found four rational points on the line at infinity, namely

$$P_1 = [0:1:0], \quad P_2 = [1:0:0], \quad P_3 = [1:-2:0], \quad P_4 = [8:-9:0].$$

The j-invariants, up to Galois conjugation, for the corresponding $\mathbb{Q}$-curves of degree 5 realizing ϱ are

$$\begin{aligned}
j_1 &= \left(-8\sqrt{11}\right)^3(10+3\sqrt{11}),\\
j_2 &= \left(6(110+31\sqrt{11})\right)^3(10+3\sqrt{11}),\\
j_3 &= \left(12(10-\sqrt{11})\right)^3(10+3\sqrt{11}),\\
j_4 &= \left(2(-6878815950+2118474913\sqrt{11})/53^5\right)^3(10+3\sqrt{11}).
\end{aligned}$$

Let us finish by showing that the Chabauty–Coleman method to determine the set of rational points on a curve of genus at least two cannot be applied to $X(5,3)_\varrho$ for the representation ϱ in this example, since the requirement that the rank of the jacobian $J(X(5,3)_\varrho)$ be smaller than the genus of the curve is not fulfilled. Indeed, consider the projection $X(5,3)_\varrho \to X_0(15)$ in Remark 4.2 and the corresponding images Q_1, Q_2, Q_3, Q_4 in $X_0(15)(kL_0)$ of the above points P_1, P_2, P_3, P_4. The morphism

$$X(5,3)_\varrho \hookrightarrow J(X(5,3)_\varrho), \qquad P \mapsto (P) - (P_1)$$

is defined over $\mathbb{Q}$ and produces three rational points in $J\left(X(5,3)_\varrho\right)(\mathbb{Q})$ whose images in the elliptic curve $J_0(15)$ are Q_2-Q_1, Q_3-Q_1 and Q_4-Q_1. Now, using Magma again, one can compute the 3×3 matrix obtained by applying the Néron–Tate pairing

$$\langle P, Q\rangle = \frac{1}{2}(h(P+Q) - h(P) - h(Q))$$

over the points $Q_2 - Q_1$, $Q_3 - Q_1$, $Q_4 - Q_1$. An approximation for the determinant of this matrix turns out to be 6.460235. Since it is nonzero, these three points are linearly independent on $J_0(15)$. It follows that the rank of $J(X(5,3)_\varrho)(\mathbb{Q})$ is at least three.

References

[BGGP] M. Baker, E. González, J. González, and B. Poonen, *Finiteness results for modular curves of genus at least* 2. Amer. J. Math. **127**(2005), no. 6, 1325–1387.

[Cre97] J. E. Cremona, *Algorithms for Modular Elliptic Curves*. Second edition. Cambridge University Press, Cambridge, 1997.

[Fer03] J. Fernández, *Elliptic Realization of Galois Representations*. Ph.D. thesis, Universitat Politècnica de Catalunya, 2003.

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

[FLR02] J. Fernández, J.-C. Lario, and A. Rio, *Octahedral Galois representations arising from $\mathbb{Q}$-curves of degree* 2. Canad. J. Math. **54**(2002), no. 6, 1202–1228.

[GL98] J. González and J.-C. Lario, *Rational and elliptic parametrizations of $\mathbb{Q}$-curves.* J. Number Theory, **72**(1998), no. 1, 13–31.

https://doi.org/10.4153/CMB-2007-021-8 Published online by Cambridge University Press

[KM88] M. A. Kenku and F. Momose, *Automorphism groups of the modular curves* $X_0(N)$. Compositio Math. **65**(1988), no. 1, 51–80.
[Lig77] G. Ligozat, *Courbes modulaires de niveau* 11. In: Modular Functions of One Variable. Lecture Notes in Math. 601, Springer, Berlin, 1977, 149–237.
[LN64] J. Lehner and M. Newman, *Weierstrass points of* $\Gamma_0(n)$. Ann. of Math. **79**(1964), 360–368.
[Maz77] B. Mazur, *Rational points on modular curves.* In: Modular Functions of One Variable. Lecture Notes in Math. 601, Springer, Berlin, 1977, pp. 107–148.
[Ogg74] A. P. Ogg, *Hyperelliptic modular curves.* Bull. Soc. Math. France **102**(1974), 449–462.

Facultat de Matemàtiques i Estadística
Universitat Politècnica de Catalunya
Pau Gargallo 5
08028 Barcelona
Spain
e-mail: julio@ma4.upc.edu
josepg@ma4.upc.edu
joan.carles.lario@upc.edu

https://doi.org/10.4153/CMB-2007-021-8 Published online by Cambridge University Press