A moduli approach to quadratic $\mathbb{Q}$-curves realizing projective mod p Galois representations

Julio Fernández

September 24, 2013

Abstract

For a fixed odd prime p and a representation ϱ of the absolute Galois group of $\mathbb{Q}$ into the projective group $\mathrm{PGL}_2(\mathbb{F}_p)$, we provide the twisted modular curves whose rational points supply the quadratic $\mathbb{Q}$-curves of degree N prime to p that realize ϱ through the Galois action on their p-torsion modules. The modular curve to twist is either the fiber product of the modular curves $X_0(N)$ and $X(p)$ or a certain quotient of Atkin-Lehner type, depending on the value of N mod p. For our purposes, a special care must be taken in fixing rational models for these modular curves and in studying their automorphisms. By performing some genus computations, we obtain from Faltings' theorem some finiteness results on the number of quadratic $\mathbb{Q}$-curves of a given degree N realizing ϱ.

1 Introduction

Throughout we fix an odd prime p and an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. For a subfield L of $\overline{\mathbb{Q}}$, we denote by G_L the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/L)$. We say that a non-CM elliptic curve defined over a quadratic field k is a $\mathbb{Q}$-*curve of degree* N if there is a cyclic isogeny of degree N from the curve to its Galois conjugate. The p-torsion of a $\mathbb{Q}$-curve $E_{/k}$ of degree N prime to p gives rise to a Galois representation

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

whose conjugacy class is an invariant of the isomorphism class of E and whose restriction to G_k is the projective representation obtained from the usual Galois action on the p-torsion points of the curve. The procedure to obtain ϱ_E is detailed in Section 2. The determinant of ϱ_E draws off two different cases, which we call *cyclotomic* and *non-cyclotomic*, and which correspond to N being a square mod p or not, respectively. These two cases rule most of the structure and contents of the rest of sections.

The situation just described raises the following inverse problem: find the $\mathbb{Q}$-curves of degree N realizing a given projective mod p Galois representation

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

namely those whose p-torsion points give rise to ϱ in the above sense. The aim of this paper is to explain in detail how to produce the moduli spaces whose rational points yield the solutions to this problem. Henceforth the term *rational* stands for $\mathbb{Q}$-*rational*.

The moduli spaces that we provide are either twists of the modular curve $X(N,p)$ obtained as the fiber product of the curves $X_0(N)$ and $X(p)$, in the non-cyclotomic case, or twists of a certain Atkin-Lehner quotient $X^+(N,p)$ in the cyclotomic case. In Section 3 we analyze the structure of the subgroup $\mathcal{W}(N,p)$ of automorphisms on $X(N,p)$ extending the group generated by the Atkin-Lehner involution w_N on $X_0(N)$. In Section 4 we fix a suitable rational model for $X(N,p)$ and then describe the Galois action on $\mathcal{W}(N,p)$. In order to do this, we need first to study the action of $\mathcal{W}(N,p)$ on the non-cuspidal points of the curve. The last two sections explain how to obtain the twisted curves whose non-cuspidal non-CM rational points give the $\mathbb{Q}$-curves of degree N realizing ϱ. Section 5 is devoted to the cyclotomic case and Section 6 to the non-cyclotomic case. They also include some finiteness results obtained from Faltings' theorem and from some genus computations performed in Section 3.

Our moduli approach turns out to be quite effective in the non-cyclotomic case, since the quadratic field of definition for the possible $\mathbb{Q}$-curves realizing the representation ϱ is uniquely determined and, for every fixed degree N, we just need one twist $X(N,p)_\varrho$. For an explicit application we refer to [FGL], where a plane quartic model is provided for the genus-three case $X(5,3)_\varrho$.

In the cyclotomic case, one should instead consider two twists $X^+(N,p)_\varrho$, $X^+(N,p)'_\varrho$ whose rational points include the cyclic isogenies of degree N between elliptic curves over $\mathbb{Q}$ realizing ϱ. One may also approach the problem by adding a given quadratic field k as extra data: the $\mathbb{Q}$-curves of degree N defined over k realizing ϱ are given by the non-cuspidal non-CM rational points on two other twisted curves $X(N,p)_{\varrho,k}$, $X(N,p)'_{\varrho,k}$.

2 Projective mod p Galois representations realized by p-admissible $\mathbb{Q}$-curves

The aim of this section is to review the construction of the representation

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

attached to a (p-admissible) $\mathbb{Q}$-curve E and to compute its determinant. Up to some minor points, the section is mostly a reformulation of known facts that

can mainly be found in [ES01] and go back to [Rib92]. The particular case of quadratic $\mathbb{Q}$-curves is written down in [Ser92] using the ideas of [Shi78].

Let E be a $\mathbb{Q}$-*curve*. By this we mean a non-CM elliptic curve defined over a number field L and with an isogeny

$$\lambda_\sigma : {}^\sigma E \longrightarrow E$$

for every σ in $\mathrm{G}_\mathbb{Q}$. Without loss of generality, we always take λ_σ equal to λ_τ whenever σ and τ restrict to the same embedding of L into $\overline{\mathbb{Q}}$, and one might also assume the isogenies λ_σ to be cyclic. We suppose here that the $\mathbb{Q}$-curve E is *p-admissible*, namely that the isogenies λ_σ can be chosen so that p does not divide the degree of any of them.

For an isogeny $\varphi : E' \longrightarrow E$, let us write φ^{-1} for the element $(\deg \varphi)^{-1} \otimes \widehat{\varphi}$ in $\mathbb{Q} \otimes \mathrm{Hom}(E, E')$, where $\widehat{\varphi}$ is the dual isogeny of φ. Since E has no CM, any isogeny $E' \longrightarrow E$ differs from φ by a rational number. Thus, the 2-cocycle of $\mathrm{G}_\mathbb{Q}$

$$c_E : (\sigma, \tau) \longmapsto \lambda_\sigma \, {}^\sigma\lambda_\tau \, \lambda_{\sigma\tau}^{-1}$$

takes values in $\mathbb{Q}^*$. Let α be a *splitting map* for the 2-cocycle c_E viewed inside the trivial cohomology group $H^2(\mathrm{G}_\mathbb{Q}, \overline{\mathbb{Q}}^*)$, that is, a continuous map $\mathrm{G}_\mathbb{Q} \longrightarrow \overline{\mathbb{Q}}^*$ satisfying

$$\lambda_\sigma \, {}^\sigma\lambda_\tau \, \lambda_{\sigma\tau}^{-1} \, = \, \alpha(\sigma) \, \alpha(\tau) \, \alpha(\sigma\tau)^{-1}$$

for all σ, τ in $\mathrm{G}_\mathbb{Q}$. By taking degrees, one deduces that the map $\sigma \mapsto \alpha(\sigma)^2 / \deg \lambda_\sigma$ is a Galois character. In particular, the values taken by α are algebraic integers prime to p. So there exist a finite extension $\mathbb{F}_\alpha$ of $\mathbb{F}_p$ and a mod p reduction map $\widetilde{\alpha} : \mathrm{G}_\mathbb{Q} \longrightarrow \mathbb{F}_\alpha^*$ obtained from a fixed embedding of $\overline{\mathbb{Q}}$ into a fixed algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$.

Consider now the $\mathbb{F}_\alpha$–linear action of $\mathrm{G}_\mathbb{Q}$ on $\mathbb{F}_\alpha \otimes_{\mathbb{F}_p} E[p]$ given by

$$(\sigma, \, 1 \otimes P) \longmapsto \widetilde{\alpha}(\sigma)^{-1} \otimes \lambda_\sigma({}^\sigma P).$$

By means of the choice of a basis for the $\mathbb{F}_p$–module $E[p]$, this action produces a linear representation

$$\rho_{E,\,\alpha} : \mathrm{G}_\mathbb{Q} \longrightarrow \mathbb{F}_\alpha^* \, \mathrm{GL}_2(\mathbb{F}_p)$$

defined up to conjugation by matrices in $\mathrm{GL}_2(\mathbb{F}_p)$. The corresponding projective Galois representation ϱ_E is actually given by the induced action

$$(\sigma, \, C) \longmapsto \lambda_\sigma({}^\sigma C)$$

on the projective line

$$\mathbb{P}\,(\,E[p]\,) \, = \, \big\{\, C \subset E[p] \;\big|\; C \simeq \mathbb{F}_p \,\big\}\,.$$

This projective representation ϱ_E depends on neither the p-admissible system of isogenies λ_σ nor the splitting map α. Further, the following proposition shows that ϱ_E is an invariant of the *p-admissible isogeny class* of E.

Proposition 2.1 *Let E' be an elliptic curve over $\overline{\mathbb{Q}}$ and $\varphi : E' \longrightarrow E$ be an isogeny of degree prime to p. Then $\varrho_{E'} = \varrho_E$.*

Proof. Let $\widehat{\varphi}$ be the dual isogeny of φ and let λ_σ and α be as before. Consider the 2-cocycle $c_{E'}$ attached to the p-admissible system of isogenies $\widehat{\varphi}\,\lambda_\sigma\,{}^\sigma\varphi$ for the $\mathbb{Q}$-curve E'. Then $\alpha \deg \varphi$ is a splitting map for $c_{E'}$ whose reduction mod p takes values in the same finite field $\mathbb{F}$ as $\widetilde{\alpha}$. The isomorphism $E'[p] \longrightarrow E[p]$ induced by φ extends naturally to an isomorphism $\mathbb{F}\otimes E'[p] \longrightarrow \mathbb{F}\otimes E[p]$ that is compatible with the corresponding $\mathbb{F}$–linear actions of $\mathrm{G}_\mathbb{Q}$. So $\rho_{E,\alpha}$ and $\rho_{E',\alpha\deg\varphi}$ are conjugated by a matrix in $\mathrm{GL}_2(\mathbb{F}_p)$, and the result follows. □

Remark 2.2 The (conjugacy class of the) representation $\rho_{E,\alpha}$ is the linear mod p representation obtained from the Galois action on the abelian variety of GL_2-type attached in [Rib92] to the $\mathbb{Q}$-curve E and the splitting map α. Moreover, any lifting of ϱ_E into $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ is of the form $\rho_{E,\alpha}$ for some splitting map α for c_E.

Note that the restriction of ϱ_E to G_L is the projective representation

$$\overline{\rho}_E : \mathrm{G}_L \longrightarrow \mathrm{PGL}_2(\mathbb{F}_p)$$

obtained from the usual Galois action on the p-torsion points of E. In terms of number fields, this provides the fixed field of ϱ_E with the following property: its composite with L is the splitting field of the modular polynomial $\Phi_p(j_E\,;\,X)$ over L, where j_E stands for the j-invariant of the elliptic curve E. Whenever L is normal over $\mathbb{Q}$ and $\overline{\rho}_E$ is surjective, this property singles out the fixed field of ϱ_E among all Galois extensions of $\mathbb{Q}$ with group $\mathrm{PGL}_2(\mathbb{F}_p)$.

We recall that the determinant of $\overline{\rho}_E$ is the restriction to G_L of the quadratic Galois character

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

obtained from the mod p cyclotomic character χ. The fixed field of ε is the only quadratic field $k_p = \mathbb{Q}(\sqrt{\pm p}\,)$ inside the p-th cyclotomic extension of $\mathbb{Q}$. Let us now show that the projective representation ϱ_E is odd by first computing the determinant of a lifting.

Proposition 2.3 *The determinant of $\rho_{E,\alpha}$ is the product of the mod p cyclotomic character χ and the character $\mathrm{G}_\mathbb{Q} \longrightarrow \mathbb{F}_\alpha^*$ defined by $\sigma \mapsto \deg \lambda_\sigma / \widetilde{\alpha}(\sigma)^2$.*

Proof. By virtue of the properties of the Weil pairing $\langle\,\cdot\,,\cdot\,\rangle_{E,p}$, the equalities

$$\langle\,\lambda_\sigma({}^\sigma P),\,\lambda_\sigma({}^\sigma Q)\,\rangle_{E,p} \;=\; \langle\,{}^\sigma P,\,\widehat{\lambda}_\sigma\lambda_\sigma({}^\sigma Q)\,\rangle_{{}^\sigma E,p} \;=\; \Big(\langle\,P,\,Q\,\rangle_{E,p}\Big)^{\chi(\sigma)\deg\lambda_\sigma}$$

hold for any two points P, Q in $E[p]$ and any σ in $\mathrm{G}_\mathbb{Q}$. Whenever $[P,Q]$ is a basis of $E[p]$, so is $[\lambda_\sigma({}^\sigma P),\,\lambda_\sigma({}^\sigma Q)]$. Moreover, the left-hand term in the above equalities is the power of $\langle\,P,\,Q\,\rangle_{E,p}$ to the determinant of the basis change. Therefore, the result follows from the definition of $\rho_{E,\alpha}$. □

Corollary 2.4 *The Galois representation ϱ_E is odd.*

Proof. Since ϱ_E does not depend on the p-admissible system of isogenies λ_σ chosen, we can take λ_σ as the identity for all σ in G_L. Fix a splitting map α for the 2-cocycle c_E obtained from the isogenies λ_σ. Note that the restriction of α to G_L is then a Galois character. Write ς for the complex conjugation in $\mathrm{G}_\mathbb{Q}$ obtained by fixing an embedding $\overline{\mathbb{Q}} \longrightarrow \mathbb{C}$. We must prove the equality $\det \rho_{E,\alpha}(\varsigma) = -1$. Consider the isogeny $\lambda_\varsigma {}^\varsigma\lambda_\varsigma : E \longrightarrow E$. It is given, on the one hand, by multiplication by $\alpha(\varsigma)^2$ and, on the other hand, by multiplication by $\pm \deg \lambda_\varsigma$. All we have to do is to pin down the latter sign. As a complex elliptic curve, E is isomorphic to $E_z = \mathbb{C}/(\mathbb{Z} + z\,\mathbb{Z})$ for some z in the complex upper-half plane $\mathbb{H}$. Through this isomorphism, $\lambda_\varsigma {}^\varsigma\lambda_\varsigma$ translates into the isogeny $E_z \longrightarrow E_z$ induced by multiplication by $\delta\,{}^\varsigma\delta$ for some δ in $\mathbb{C}^*$. So the above sign is positive and thus $\widetilde{\alpha}(\varsigma)^2 = \deg \lambda_\varsigma$ in $\mathbb{F}_p$. Since $\chi(\varsigma) = -1$, the result follows from Proposition 2.3.□

Let $deg : \mathrm{G}_\mathbb{Q} \longrightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$ be the degree character induced by any p-admissible system of isogenies $\lambda_\sigma : {}^\sigma E \longrightarrow E$. Then, consider the mod p degree character

$$deg_p : \mathrm{G}_\mathbb{Q} \longrightarrow \mathbb{F}_p^*/\mathbb{F}_p^{*2} \simeq \{\pm 1\}$$

obtained from deg by composition with the natural map $\mathbb{Q}^*/\mathbb{Q}^{*2} \longrightarrow \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. The following statement is a straightforward consequence of Proposition 2.3.

Corollary 2.5 *The determinant of ϱ_E is the product $\varepsilon\, deg_p$.*

Remark 2.6 If the map deg is not trivial, its fixed field K_{deg} is a composite of quadratic fields $\mathbb{Q}(\sqrt{a_1}), \ldots, \mathbb{Q}(\sqrt{a_m})$, where 2^m is the degree of K_{deg} over $\mathbb{Q}$. For every $l = 1, \ldots, m$, take σ_l in $\mathrm{G}_\mathbb{Q}$ restricting to the non-trivial automorphism of K_{deg} that fixes $\sqrt{a_h}$ for $h \neq l$. Then, the map deg_p is the product of the quadratic Galois characters attached to the extensions $\mathbb{Q}(\sqrt{a_l})$ for which $\deg \lambda_{\sigma_l}$ is not a square mod p.

We say that a projective mod p Galois representation

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

is *realized by* a (p-admissible) $\mathbb{Q}$-curve E if $\varrho_E = \varrho$, where this equality makes only sense up to conjugation in $\mathrm{PGL}_2(\mathbb{F}_p)$. The rest of sections are devoted to the particular case of quadratic $\mathbb{Q}$-curves. Assume ϱ to be realized by a p-admissible $\mathbb{Q}$-curve of degree N, that is, by a non-CM elliptic curve defined over a quadratic field and with a cyclic isogeny to its Galois conjugate of degree N prime to p. From Corollary 2.5 and Remark 2.6, ϱ has determinant ε if and only if N is a square mod p, and otherwise any $\mathbb{Q}$-curves of degree N realizing ϱ must be defined over the fixed field of the quadratic character $\varepsilon \det \varrho$. We refer to the first case (N square mod p) as the *cyclotomic case*, and to the second one (N non-square mod p) as the *non-cyclotomic case*.

3 Automorphisms of the modular curve $X(N,p)$

Let $N>1$ be an integer prime to p. Let $X_0(N)$, $X(p)$ and $X(1)$ be the modular curves attached to the congruence subgroups $\Gamma_0(N)$, $\Gamma(p)$ and $\mathrm{SL}_2(\mathbb{Z})$, respectively. We denote by $X(N,p)$ the modular curve attached to the congruence subgroup $\Gamma_0(N)\cap\Gamma(p)$, namely the fiber product of $X_0(N)$ and $X(p)$ over $X(1)$:

$$\begin{array}{ccc} X(N,p) & & \\ \downarrow & \searrow & \\ X_0(N) & & X(p) \\ & \searrow & \downarrow \\ & & X(1) \end{array}$$

The aim of this section is to introduce a certain group $\mathcal{W}(N,p)$ of automorphisms on $X(N,p)$. We also compute the genus of this curve.

As a complex curve, $X(N,p)$ is a Galois covering of $X_0(N)$ with group $\mathcal{G}(N,p)$ given by the quotient $\Gamma_0(N)/\pm\Gamma_0(N)\cap\Gamma(p)$. Since the mod p reduction map $\mathrm{SL}_2(\mathbb{Z})\longrightarrow\mathrm{SL}_2(\mathbb{F}_p)$ induces the exact sequence

$$1 \;\longrightarrow\; \pm\Gamma_0(N)\cap\Gamma(p) \;\longrightarrow\; \Gamma_0(N) \;\longrightarrow\; \mathrm{PSL}_2(\mathbb{F}_p) \;\longrightarrow\; 1,$$

there is a canonical isomorphism

$$\mathcal{G}(N,p) \;\simeq\; \mathrm{PSL}_2(\mathbb{F}_p).$$

We recall that $\mathcal{G}(N,p)$ consists of the automorphisms g on $X(N,p)$ for which the following diagram commutes:

$$\begin{array}{ccc} X(N,p) & \xrightarrow{\;g\;} & X(N,p) \\ & \searrow \quad \swarrow & \\ & X_0(N) & \end{array}$$

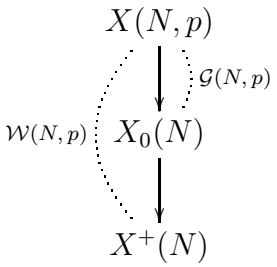
Let w_N be the Atkin-Lehner involution on $X_0(N)$ and denote by $X^+(N)$ the corresponding quotient. For any integers a,b,c,d satisfying $a\,d\,N-b\,c\,p^2=1$ and $d\equiv\pm1\,(\mathrm{mod}\;p)$, the action of the matrix

$$\begin{pmatrix} a\,N & b\,p \\ c\,p\,N & d\,N \end{pmatrix}$$

on the complex upper-half plane $\mathbb{H}$ defines an automorphism ϑ on $X(N,p)$ *extending* w_N, namely making the following diagram commutative:

$$\begin{array}{ccc} X(N,p) & \xrightarrow{\;\vartheta\;} & X(N,p) \\ \downarrow & & \downarrow \\ X_0(N) & \xrightarrow{\;w_N\;} & X_0(N) \end{array}$$

Indeed, one can check that the above matrix lies in the normalizer of $\Gamma_0(N) \cap \Gamma(p)$ inside $\mathrm{PSL}_2(\mathbb{R})$. Hence, the covering $X(N,p) \longrightarrow X^+(N)$ has as many automorphisms as its degree, which means that it is a Galois covering. Let $\mathcal{W}(N,p)$ denote its automorphism group:



The group $\mathcal{W}(N,p)$ contains $\mathcal{G}(N,p)$ as a subgroup of index two whose complement consists of the automorphisms on $X(N,p)$ extending w_N.

Proposition 3.1 *The group $\mathcal{G}(N,p)$ is a direct factor of $\mathcal{W}(N,p)$ if and only if N is a square mod p. More precisely, the structure of $\mathcal{W}(N,p)$ is as follows:*

- *In the cyclotomic case, there is a unique involution w on $X(N,p)$ such that*

$$\mathcal{W}(N,p) \;=\; \mathcal{G}(N,p) \times \langle w \rangle.$$

- *In the non-cyclotomic case,*

$$\mathcal{W}(N,p) \;\simeq\; \mathrm{PGL}_2(\mathbb{F}_p).$$

In the first case, the quotient curve $X(N,p)/w$ is a Galois covering of $X^+(N)$ with group $\mathcal{G}(N,p)$. In the second case, the quotient of $X(N,p)$ by an involution in $\mathcal{W}(N,p)$ is never a Galois covering of $X^+(N)$.

Proof. Viewed as the quotient $\mathrm{SL}_2(\mathbb{F}_p)/\{\pm 1\}$, the group $\mathrm{PSL}_2(\mathbb{F}_p)$ is generated by the matrices

$$T \;=\; \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad U \;=\; \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

On the other hand, the determinant $\mathrm{GL}_2(\mathbb{F}_p) \longrightarrow \mathbb{F}_p^*$ induces an exact sequence

$$1 \;\longrightarrow\; \mathrm{PSL}_2(\mathbb{F}_p) \;\longrightarrow\; \mathrm{PGL}_2(\mathbb{F}_p) \;\xrightarrow{\det}\; \mathbb{F}_p^*/\mathbb{F}_p^{*2} \;\longrightarrow\; 1,$$

so that $\mathrm{PSL}_2(\mathbb{F}_p)$ can be identified with a subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ of index two whose complementary subgroups are those generated by a conjugate of the matrix

$$V \;=\; \begin{pmatrix} 0 & -v \\ 1 & 0 \end{pmatrix},$$

where v is a non-square in $\mathbb{F}_p^*$. Since one has the relations $V\,T = U^{-v^{-1}}\,V$ and $V\,U = T^{-v}\,V$, a system of generators for $\mathrm{PGL}_2(\mathbb{F}_p)$ is given by V and either T or U. Now, $\mathcal{G}(N,p)$ is generated by the automorphisms defined by the matrices

$$T_{\scriptscriptstyle N} \,=\, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad\qquad U_{\scriptscriptstyle N} \,=\, \begin{pmatrix} 1 & 0 \\ \tilde{N}\,N & 1 \end{pmatrix}$$

in $\Gamma_0(N)$, where $\tilde{N} \in \mathbb{Z}$ is any inverse of N mod p. To give a complementary subgroup for $\mathcal{G}(N,p)$ inside $\mathcal{W}(N,p)$, let us consider separately the two possibilities for N mod p:

- If N is a square mod p, then it is also a square mod p^2. Let a, b be any integers satisfying $a^2 N - b\,p^2 = 1$. Then, the matrix

$$Z_{\scriptscriptstyle N} \,=\, \begin{pmatrix} a\,N & b\,p \\ p\,N & a\,N \end{pmatrix}$$

  defines an involution w on $X(N,p)$ extending $w_{\scriptscriptstyle N}$. Moreover, w commutes with the automorphisms defined by $T_{\scriptscriptstyle N}$ and $U_{\scriptscriptstyle N}$, so it generates a direct cofactor of $\mathcal{G}(N,p)$ inside $\mathcal{W}(N,p)$. The uniqueness of w comes from the fact that $\mathrm{PSL}_2(\mathbb{F}_p)$ has trivial center.

- If N is not a square mod p, then neither is $\tilde{N}$. Moreover, the matrix

$$V_{\scriptscriptstyle N} \,=\, \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix},$$

  which defines an involution on $X(N,p)$ extending $w_{\scriptscriptstyle N}$, satisfies the relations $V_{\scriptscriptstyle N}\,T_{\scriptscriptstyle N} \,=\, U_{\scriptscriptstyle N}^{-N}\,V_{\scriptscriptstyle N}$ and $V_{\scriptscriptstyle N}\,U_{\scriptscriptstyle N} \,=\, T_{\scriptscriptstyle N}^{-\tilde{N}}\,V_{\scriptscriptstyle N}$ inside $\mathcal{W}(N,p)$. These are precisely the relations that the matrix V, for v equal to $\tilde{N}$ mod p, satisfies with the generators T, U of $\mathrm{PSL}_2(\mathbb{F}_p)$. Hence, the group $\mathcal{W}(N,p)$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_p)$.

The last assertion in the statement follows from the group structure of $\mathcal{W}(N,p)$: in the first case, the subgroup $\langle w \rangle$ is normal, while in the second case $\mathcal{W}(N,p)$ has no normal subgroups of order two because it has trivial center. $\square$

Remark 3.2 The matrices $Z_{\scriptscriptstyle N}$ and $V_{\scriptscriptstyle N}$ in the proof of Proposition 3.1 have determinant N. Thus, in the same way as the automorphisms in $\mathcal{G}(N,p)$ are defined by matrices in $\Gamma_0(N)$ acting on $\mathbb{H}$, the automorphisms on $X(N,p)$ extending $w_{\scriptscriptstyle N}$ are defined by matrices in $\mathrm{M}_2(\mathbb{Z})$ with determinant N and hence lying in $\mathrm{GL}_2(\mathbb{F}_p)$ when reduced mod p. So we have a mod p reduction map

$$\mathcal{W}(N,p) \;\longrightarrow\; \mathrm{PGL}_2(\mathbb{F}_p)$$

whose restriction to $\mathcal{G}(N,p)$ is the canonical isomorphism onto $\mathrm{PSL}_2(\mathbb{F}_p)$. In the non-cyclotomic case, this map is the isomorphism $\mathcal{W}(N,p) \,\simeq\, \mathrm{PGL}_2(\mathbb{F}_p)$ constructed in the proof of Proposition 3.1. We keep this *canonical* isomorphism throughout the rest of the paper.

Remark 3.3 In the non-cyclotomic case, all involutions on $X(N,p)$ extending w_N are conjugated inside $\mathcal{W}(N,p)$. Hence, their defining matrices in $\mathrm{M}_2(\mathbb{Z})$ can be obtained conjugating the matrix V_N in the proof of Proposition 3.1 by matrices in $\Gamma_0(N)$. So they can be chosen to be of the form

$$\begin{pmatrix} a\,N & b \\ c\,N & -a\,N \end{pmatrix},$$

where a, b, c are integers satisfying $a^2N + b\,c = -1$. This fact is used in the proof of Proposition 4.3.

In the cyclotomic case, let us write $X^+(N,p)$ for the quotient of $X(N,p)$ by the only involution w in the center of the group $\mathcal{W}(N,p)$. To conclude this section, we give a formula for the genus of $X(N,p)$ and compute the values of N and p for which the curves $X(N,p)$ and $X^+(N,p)$ have genus zero or one. In the proof of Proposition 3.4, we recall the description of the cusps of $X_0(N)$. We refer to [Gon91] for this, as well as for the action of the Atkin-Lehner involutions on the set of cusps. Both things are used in the proof of Proposition 3.7.

Proposition 3.4 *The genus of the modular curve $X(N,p)$ is*

$$1 \;+\; \frac{\psi(N)\,p\,(p^2-1)}{24} \;-\; \frac{p^2-1}{4} \sum_{0<n\,|N} \varphi\,(\,(n, N/n)\,)\,,$$

where (a,b), $\varphi(r)$ and $\psi(N)$ are the usual notations for the greatest common divisor of the integers a and b, the order of the group $(\mathbb{Z}/r\,\mathbb{Z})^*$ and the index of $\Gamma_0(N)/\{\pm 1\}$ in $\mathrm{PSL}_2(\mathbb{Z})$, respectively.

Proof. The number of cusps of $X_0(N)$ is $\sum \varphi(h_n)$, where the sum is taken over the positive divisors n of N, and h_n stands for $(n, N/n)$. For every divisor n, there is exactly one cusp for each integer m in a system of representatives in $\mathbb{Z}$ of the group $(\mathbb{Z}/h_n\,\mathbb{Z})^*$. We just take the integer $m = 1$ whenever $\varphi(h_n) = 1$. Any such integer m can be chosen prime to n, and the corresponding cusp is then represented by the rational number m/n. The ramification degree of this cusp over $X(1)$ is $N/(n\,h_n)$. On the other hand, the cusps of $X(p)$ have ramification degree p over $X(1)$. Thus, since N is prime to p, the cusps of $X(N,p)$ also have ramification degree p over $X_0(N)$. Moreover, $X(p)$ has no elliptic points, so neither has $X(N,p)$. Lastly, the degrees of the coverings $X(N,p) \longrightarrow X_0(N)$ and $X_0(N) \longrightarrow X(1)$ are $p\,(p^2-1)/2$ and $\psi(N)$, respectively. Hence, the proposition follows from the Hurwitz formula applied to the map $X(N,p) \longrightarrow X(1)$. $\square$

Corollary 3.5 *The modular curve $X(N,p)$ has genus greater than one, except for the genus-zero case $X(2,3)$ and the elliptic case $X(4,3)$.*

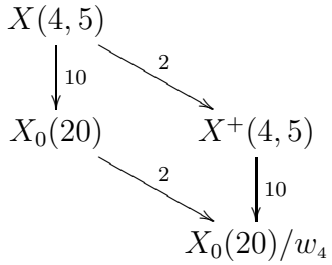
Proof. Since the genera of $X(p)$ and $X_0(N)$ are greater than one for $p > 5$ and $N > 49$, respectively, one only has to check the values that Proposition 3.4 yields in the remaining cases. □

Lemma 3.6 *For an odd prime p and an integer $N > 1$ prime to p, consider the Atkin-Lehner involution w_N on the modular curve $X_0(pN)$. The only pairs (N, p) for which the quotient curve $X_0(pN)/w_N$ has genus zero are $(2, 3)$, $(4, 3)$, $(5, 3)$, $(8, 3)$, $(11, 3)$, $(2, 5)$, $(4, 5)$ and $(3, 7)$.*

Proof. For every integer $D > 71$, the modular curve $X_0(D)$ has positive genus and is neither elliptic nor hyperelliptic [Ogg74]. For each odd prime p and each integer N prime to p such that $pN \leq 71$, one can then use the formulae in [Klu77] or the tables [STN92] to conclude the lemma. □

Proposition 3.7 *The curve $X^+(N, p)$ has genus greater than one, except for the genus-zero case $X^+(4, 3)$.*

Proof. The involution w, which is defined by the matrix Z_N in the proof of Proposition 3.1, restricts to the Atkin-Lehner involution w_N on $X_0(pN)$, so it induces a Galois covering $X^+(N, p) \longrightarrow X_0(pN)/w_N$. On the other hand, the cusps of $X_0(pN)$ that ramify on $X(N, p)$ are those of the form m/n with p dividing n, and the ramification degree is always p (cf. the proof of Proposition 3.4). In particular, the Hurwitz formula implies that $X_0(pN)/w_N$ has genus zero whenever $X^+(N, p)$ has genus less than two. By Lemma 3.6, the only pairs (N, p), with N prime to p and square mod p, for which $X_0(pN)/w_N$ has genus zero are $(4, 3)$ and $(4, 5)$. In the first case, the involution w fixes the cusp $1/2$, so $X^+(4, 3)$ is a genus-zero quotient of the elliptic curve $X(4, 3)$. Let us now study the second case, for which we consider the following commutative diagram:



The only ramified points of the covering $X(4, 5) \longrightarrow X_0(20)$ are cusps. Moreover, it can be checked that the points lying above the two cusps $1/2, 1/10$ fixed by w_4 are also fixed by the involution w. Thus, the only ramified cusps of the covering $X^+(4, 5) \longrightarrow X_0(20)/w_4$ are the points above $1/5$ and $1/10$, all of them with ramification degree 5. Then, the Hurwitz formula shows that there must be ten more ramified points, necessarily with ramification degree 2 and lying above the two non-cuspidal points on $X_0(20)$ fixed by w_4, hence the genus of $X^+(4, 5)$ is four. Notice that there are no other ramified points because the number of points on $X_0(20)$ fixed by w_4 is exactly four (cf. [Klu77] or [STN92]). □

4 A rational model for the modular curve $X(N,p)$

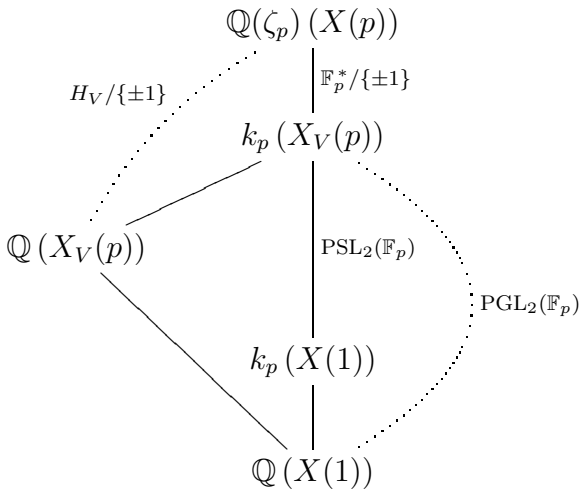
This section deals with the rationality over $\mathbb{Q}$ for the curve $X(N,p)$ as well as for the automorphism group $\mathcal{W}(N,p)$ introduced in the previous section: we fix a certain rational model for $X(N,p)$ that makes the automorphisms in $\mathcal{W}(N,p)$ be defined over k_p. Recall that k_p stands for the only quadratic field inside the p-th cyclotomic extension of $\mathbb{Q}$. We denote by ζ_p the root of unity $e^{2\pi i/p}$.

Since $X(N,p)$ is the fiber product of the modular curves $X(p)$ and $X_0(N)$ over $X(1)$, a rational model for the first curve is determined by fixing rational models for the other three curves. Recall that the function field of $X(1)$ is generated over $\mathbb{Q}$ by the elliptic modular function j. For $X_0(N)$, consider the canonical rational model given by the function field $\mathbb{Q}(j, j_N)$, where j_N is the modular function defined by $j_N(z) = j(Nz)$ for z in the complex upper-half plane $\mathbb{H}$. As for $X(p)$, the rational model that we fix satisfies the following property: its extension to k_p gives by specialization over an elliptic curve E in $X(1)(\overline{\mathbb{Q}})$ the fixed field of the projective mod p Galois representation $\overline{\rho}_E$ attached to the p-torsion points of E. This model for $X(p)$ is obtained as the following particular case of a general procedure that follows Section II.3 in [Lig77] and Section 2 in [Maz77].

Fix a non-square v in $\mathbb{F}_p^*$ and take a matrix V in $\mathrm{GL}_2(\mathbb{F}_p)$ of order two in $\mathrm{PGL}_2(\mathbb{F}_p)$ and with $\det(V) = v$. Without risk of confusion, we often identify the matrix V, up to a sign, with its image in $\mathrm{PGL}_2(\mathbb{F}_p)$. Define H_V as the inverse image in $\mathrm{GL}_2(\mathbb{F}_p)$ of the subgroup generated by V in $\mathrm{PGL}_2(\mathbb{F}_p)$:

$$H_V \;=\; \mathbb{F}_p^* \,\cup\, \mathbb{F}_p^*\, V.$$

Up to conjugation, H_V is the only subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ containing the center $\mathbb{F}_p^*$ and reducing inside $\mathrm{PGL}_2(\mathbb{F}_p)$ to a complementary subgroup of $\mathrm{PSL}_2(\mathbb{F}_p)$. The group H_V defines, as shown in the following diagram, a rational model $X_V(p)$ whose $\mathbb{Q}$-isomorphism class does not depend on the choice of the matrix V:



Here $\mathbb{Q}(\zeta_p)\,(X(p))$ stands for the field of modular functions for $\Gamma(p)$ whose Fourier expansions have coefficients in $\mathbb{Q}(\zeta_p)$. This is a Galois extension of $\mathbb{Q}\,(X(1))$ with group $\mathrm{GL}_2(\mathbb{F}_p)/\{\pm 1\}$ and the function field of $X_V(p)$ is then the fixed field by the subgroup $H_V/\{\pm 1\}$.

Although we should denote by $X_V(N,p)$ the rational model for $X(N,p)$ obtained from $X_V(p)$, we just write $X(N,p)$ for simplicity. Without loss of generality, we always take the above non-square v equal to N^{-1} mod p in the non-cyclotomic case. Note that the map $X(N,p) \longrightarrow X_0(N)$ is defined over $\mathbb{Q}$ and that the function field $k_p\,(X(N,p))$ is a Galois extension of $\mathbb{Q}\,(X_0(N))$ with group $\mathrm{PGL}_2(\mathbb{F}_p)$. In particular, the Galois action on the automorphism group $\mathcal{G}(N,p)$ factors through $\mathrm{Gal}(k_p/\mathbb{Q})$.

The non-cuspidal complex points on $X(N,p)$ are in bijection with the isomorphism classes of triples

$$(E,\, C,\, [T_1,T_2]_V),$$

where E is a complex elliptic curve, C is a cyclic subgroup of $E(\mathbb{C})$ of order N, $[T_1,T_2]$ is a basis for $E[p]$ and $[T_1,T_2]_V$ is the corresponding orbit inside $E[p]\times E[p]$ by the action of H_V. Here H_V is viewed as a subgroup of automorphisms of $E[p]$ through the isomorphism $\mathrm{GL}_2(\mathbb{F}_p) \simeq \mathrm{Aut}(E[p])$ fixed by the basis $[T_1,T_2]$, so that

$$[T_1,T_2]_V \;=\; \left\{\, [r\,T_1, r\,T_2],\, [r\,T_1, r\,T_2]\,V \;\middle|\; r \in \mathbb{F}_p^* \,\right\}.$$

Two triples of the form $(E,\, C,\, [T_1,T_2]_V)$ are isomorphic if there is an isomorphism between the corresponding elliptic curves interchanging the cyclic subgroups and the H_V–orbits.

This bijection is compatible with the usual Galois actions. Thus, a point on $X(N,p)$ given by a triple as above with $j_E \neq 0, 1728$ is defined over a number field L if and only if the elliptic curve E is defined over L, the subgroup C is G_L-invariant and the image of the linear Galois representation

$$\rho_E :\, \mathrm{G}_L \;\longrightarrow\; \mathrm{GL}_2(\mathbb{F}_p)$$

attached to $E[p]$ lies inside a conjugate of the subgroup H_V.

We can always assume that the basis $[T_1,T_2]$ in a triple $(E,\, C,\, [T_1,T_2]_V)$ is, inside the corresponding H_V–orbit, the only one up to a sign that is sent to ζ_p by the Weil pairing. The Galois action on the non-cuspidal points of $X(N,p)$ should then be written accordingly: an automorphism σ of $\mathbb{C}$ takes any such a triple to that given by the elliptic curve ${}^{\sigma}E$, the subgroup ${}^{\sigma}C$ and the H_V–orbit of either the basis $[r^{-1}\,{}^{\sigma}T_1, r^{-1}\,{}^{\sigma}T_2]$ or the basis $[(v\,r)^{-1}\,{}^{\sigma}T_1, (v\,r)^{-1}\,{}^{\sigma}T_2]\,V$, depending on whether ${}^{\sigma}\zeta_p = \zeta_p^{\,r^2}$ or ${}^{\sigma}\zeta_p = \zeta_p^{\,v\,r^2}$ for some r in $\mathbb{F}_p^*$, respectively.

The action of the automorphism group $\mathcal{G}(N,p)$ on the non-cuspidal points of $X(N,p)$, and then the Galois action on $\mathcal{G}(N,p)$, are stated in Proposition 4.1 and Corollary 4.2, respectively. The symbol $\hat{}$ stands henceforth for the matrix (anti)involution given by

$$\hat{M} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} {}^{\mathrm{t}}M \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

where ${}^{\mathrm{t}}M$ is the transpose of the matrix M. Alternatively, it can be defined as follows:

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \longmapsto \hat{M} = \begin{pmatrix} d & c \\ b & a \end{pmatrix}.$$

Proposition 4.1 *An automorphism in $\mathcal{G}(N,p)$ represented through the canonical isomorphism $\mathcal{G}(N,p) \simeq \mathrm{PSL}_2(\mathbb{F}_p)$ by a matrix γ in $\mathrm{SL}_2(\mathbb{F}_p)$ takes a point $(E,\, C,\, [T_1,T_2]_V)$ on $X(N,p)$ to the point given by the elliptic curve E, the subgroup C and the H_V–orbit of the p-torsion basis $[T_1,T_2]\,\hat{\gamma}$.*

Proof. Take any matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z})$ reducing mod p to γ. The triple $(E,\, C,\, [T_1,T_2]_V)$ is isomorphic to one of the form

$$(E_z\,,\, \langle 1/N\rangle,\, [\,1/p,\, z/p\,]_V)$$

for some z in $\mathbb{H}$, where E_z stands for the complex elliptic curve defined by the lattice $\mathbb{Z} + z\,\mathbb{Z}$. The automorphism in the statement sends the pair given by z to that given by

$$z' \;=\; \frac{a\,z+b}{c\,z+d}\,.$$

Then, the endomorphism of $\mathbb{C}$ defined by multiplication by $c\,z+d$ extends to an isomorphism $E_{z'} \longrightarrow E_z$ that preserves the subgroup $\langle 1/N\rangle$ and sends the basis $[\,1/p,\, z'/p\,]$ of $E_{z'}[p]$ to the basis

$$[\,(d+c\,z)/p,\, (b+a\,z)/p\,] \;=\; [\,1/p,\, z/p\,]\,\hat{\gamma}$$

of $E_z[p]$, so the result follows. □

Corollary 4.2 *An automorphism in $\mathcal{G}(N,p)$ represented through the canonical isomorphism $\mathcal{G}(N,p) \simeq \mathrm{PSL}_2(\mathbb{F}_p)$ by a matrix γ in $\mathrm{SL}_2(\mathbb{F}_p)$ is sent by the non-trivial element in $\mathrm{Gal}(k_p/\mathbb{Q})$ to the automorphism in $\mathcal{G}(N,p)$ corresponding to the matrix $\hat{V}\gamma\hat{V}$ in $\mathrm{PSL}_2(\mathbb{F}_p)$.*

Proof. Denote by g the automorphism represented by the matrix γ. Take any element σ in $\mathrm{G}_{\mathbb{Q}}$ such that ${}^{\sigma}\zeta_p = \zeta_p^{\,v}$ and let γ_σ be a matrix in $\mathrm{SL}_2(\mathbb{F}_p)$ representing the automorphism ${}^{\sigma}g \in \mathcal{G}(N,p)$. Take also any point P in $X(N,p)(\overline{\mathbb{Q}})$ given by a triple $(E,\, C,\, [T_1,T_2]_V)$ with $j_E \neq 0, 1728$. The identity ${}^{\sigma}(\,g\,(P)\,) = {}^{\sigma}g\,({}^{\sigma}P)$ leads, by means of Proposition 4.1, to an automorphism of the elliptic curve ${}^{\sigma}E$ interchanging the H_V–orbits of the p-torsion bases $[v^{-1}\,{}^{\sigma}T_1, v^{-1}\,{}^{\sigma}T_2]\,\hat{\gamma}\,V$ and $[v^{-1}\,{}^{\sigma}T_1, v^{-1}\,{}^{\sigma}T_2]\,V\hat{\gamma}_\sigma$. This yields the identity $\hat{\gamma}_\sigma = V\hat{\gamma}\,V$ in $\mathrm{PSL}_2(\mathbb{F}_p)$. □

From now on, we fix as follows an involution w on $X(N,p)$ extending the Atkin-Lehner involution w_N on $X_0(N)$. Recall that $\mathcal{W}(N,p)$ stands for the group of the Galois covering $X(N,p) \longrightarrow X^+(N)$, where $X^+(N)$ is the quotient of $X_0(N)$

by w_N. In the cyclotomic case, we take as w the only involution in the center of $\mathcal{W}(N,p)$ (cf. Proposition 3.1) and denote by $\sqrt{N}$ a square root of N mod p. In the non-cyclotomic case, we take as w the involution corresponding to the matrix $\hat{V}$ through the canonical isomorphism $\mathcal{W}(N,p) \simeq \mathrm{PGL}_2(\mathbb{F}_p)$ (cf. Remark 3.2). Recall that, in the second case, $\det(V)$ is taken to be N^{-1} mod p.

Proposition 4.3 *The involution w takes a point $(E,\, C,\, [T_1, T_2]_V)$ on $X(N,p)$ to the point given by the elliptic curve E/C, the subgroup $E[N]/C$ and the H_V–orbit of the image in E/C of the following p-torsion basis:*

- $[\sqrt{N}^{-1} T_1, \sqrt{N}^{-1} T_2]$ *in the cyclotomic case.*
- $[T_1, T_2]\, V$ *in the non-cyclotomic case.*

Proof. According to Remark 3.3 and the proof of Proposition 3.1, the involution w is always defined by the action on $\mathbb{H}$ of a matrix in $\mathrm{M}_2(\mathbb{Z})$ of the form

$$\begin{pmatrix} a\,N & b \\ c\,N & d\,N \end{pmatrix},$$

with $a\,d\,N - b\,c = 1$. Denote by γ the reduction mod p of this matrix. We now proceed as in the proof of Proposition 4.1 : the given triple is isomorphic to one of the form

$$(E_z\,,\, \langle 1/N\rangle,\, [\,1/p,\, z/p\,]_V)$$

for some z in $\mathbb{H}$, where E_z stands for the complex elliptic curve defined by the lattice $\mathbb{Z} + z\,\mathbb{Z}$. The involution w sends the triple given by z to that given by

$$z' \;=\; \frac{a\,N\,z + b}{c\,N\,z + d\,N}\,.$$

Then, the endomorphism of $\mathbb{C}$ defined by multiplication by $c\,z + d$ extends to an isomorphism

$$E_{z'} \;\longrightarrow\; E_z\big/\langle 1/N\rangle.$$

This isomorphism sends the subgroup $\langle 1/N\rangle$ of $E_{z'}$ to the image of $E_z[N]$ under the isogeny $E_z \longrightarrow E_z\big/\langle 1/N\rangle$. Also, it sends the basis $[\,1/p,\, z'/p\,]$ of $E_{z'}[p]$ to the image of the basis

$$[\,(d + c\,z)/p,\, (N^{-1}b + a\,z)/p\,] \;=\; [\,1/p,\, z/p\,]\,N^{-1}\,\hat{\gamma}$$

of $E_z[p]$. In the cyclotomic case, $d = a$, $c = p$ and b is a multiple of p, so that a^2 equals N^{-1} mod p and the matrix $\sqrt{N}^{-1}\hat{\gamma}$ is trivial in $\mathrm{PSL}_2(\mathbb{F}_p)$. In the non-cyclotomic case, we have $\gamma = \pm N\,\hat{V}$. This completes the proof. □

Corollary 4.4 *The involution w is defined over $\mathbb{Q}$.*

Proof. Take any automorphism σ in $\mathrm{G}_{\mathbb{Q}}$. Since w_N is defined over $\mathbb{Q}$, ${}^{\sigma}w$ is still an involution in $\mathcal{W}(N,p) \setminus \mathcal{G}(N,p)$. Let P be a non-CM point in $X(N,p)(\overline{\mathbb{Q}})$ given by a triple $(E,\, C,\, [T_1,T_2]_V)$. For a fixed model of the elliptic curve E/C, an isogeny $\lambda : E \longrightarrow E/C$ with kernel C is determined up to a sign. One has the conjugate isogeny ${}^{\sigma}\lambda\colon {}^{\sigma}E \longrightarrow {}^{\sigma}(E/C)$. Using Proposition 4.3 and the isomorphism ${}^{\sigma}E/{}^{\sigma}C \longrightarrow {}^{\sigma}(E/C)$ induced by ${}^{\sigma}\lambda$, we can verify case by case that ${}^{\sigma}P$ has the same image by both w and ${}^{\sigma}w$. Consider, for instance, the cyclotomic case and assume ${}^{\sigma}\zeta_p = \zeta_p^{r^2}$ for some r in $\mathbb{F}_p^*$. Then, the point ${}^{\sigma}P$ is sent to the isomorphism class of the triple given by the elliptic curve ${}^{\sigma}(E/C)$, the cyclic group ${}^{\sigma}\lambda({}^{\sigma}E[N])$ and the H_V–orbit of the basis

$$[\,(r\sqrt{N}\,)^{-1}\ {}^{\sigma}\lambda({}^{\sigma}T_1),\ (r\sqrt{N}\,)^{-1}\ {}^{\sigma}\lambda({}^{\sigma}T_2)\,].$$

By Proposition 4.1, this implies that the matrix in $\mathrm{PSL}_2(\mathbb{F}_p)$ corresponding to the automorphism ${}^{\sigma}w\, w$ in $\mathcal{G}(N,p)$ is the identity, and the result follows. □

Remark 4.5 We can conclude that the Galois covering $X(N,p) \longrightarrow X^+(N)$ is defined over k_p. In other words, the function field $k_p\,(X(N,p))$ is a Galois extension of $k_p\,(X^+(N))$, with group (anti)isomorphic to $\mathcal{W}(N,p)$. As a matter of fact, $k_p\,(X(N,p))$ is a Galois extension of $\mathbb{Q}\,(X^+(N))$.

Let us finish this section by reviewing the moduli interpretation of the rational points on $X^+(N)$. The non-cuspidal points of $X_0(N)(\mathbb{C})$ are in bijection with the isomorphism classes of pairs (E,C), where E is a complex elliptic curve and C is a cyclic subgroup of $E(\mathbb{C})$ of order N. Such a point is defined over a number field L if and only if E and C are defined over L, which means that ${}^{\sigma}E = E$ and ${}^{\sigma}C = C$ for all σ in G_L. A point on $X(N,p)$ given by a triple $(E,\, C,\, [T_1,T_2]_V)$ has image on $X_0(N)$ given by the pair (E,C). In particular, the involution w_N sends this pair to $(E/C,\, E[N]/C)$.

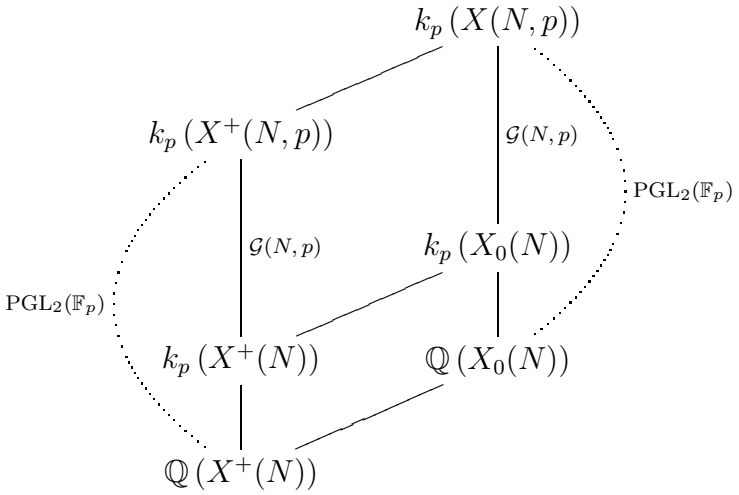
Let E be an elliptic curve defined over L, and let $E \longrightarrow E'$ be an isogeny with cyclic kernel C of order N. Assume that E has no CM, so that an isogeny from E to any elliptic curve is determined up to a sign by its degree. Then, the subgroup C is defined over L if and only if E' admits a model over L.

Now, suppose that E and E' are defined over a quadratic field k, so that the pair (E,C) defines a k-rational point P on $X_0(N)$. This point is rational if and only if both E and E' have a model over $\mathbb{Q}$. In this case we say that the couple $\{E,E'\}$ is a *fake $\mathbb{Q}$-curve of degree N*. Otherwise, the image of P on $X^+(N)$ is rational if and only if E' is isomorphic to the Galois conjugate ${}^{\nu}E$ of E. Indeed, since E has no CM, an isogeny $\mu\colon E \longrightarrow {}^{\nu}E$ with kernel C sends $E[N]$ to ${}^{\nu}C$, so the existence of such an isogeny μ amounts to the equality $w_N(P) = {}^{\nu}P$ in $X_0(N)(k)$. Thus, every non-cuspidal non-CM rational point on $X^+(N)$ comes from a pair (E,C) on $X_0(N)$ defined over some quadratic field and yielding a (possibly fake) $\mathbb{Q}$-curve of degree N.

5 The twisted curves in the cyclotomic case

Assume N to be a square mod p. The structure of this section is as follows. We first obtain from a modular point of view the fixed field of the Galois representation ϱ_E attached in Section 2 to a $\mathbb{Q}$-curve E of degree N. Next, we produce the twisted modular curves whose non-cuspidal non-CM rational points give the $\mathbb{Q}$-curves of degree N realizing a fixed projective mod p Galois representation with cyclotomic determinant. We also include a result on the finiteness of the number of such $\mathbb{Q}$-curves.

Recall that $X^+(N,p)$ denotes the quotient of $X(N,p)$ by the involution w. The induced map $X^+(N,p) \longrightarrow X^+(N)$ is a Galois covering with automorphism group $\mathcal{G}(N,p)$ and hence defined over k_p (cf. Proposition 3.1 and Remark 4.5). The function field $k_p\,(X^+(N,p))$ is in fact a Galois extension of $\mathbb{Q}\,(X^+(N))$, with group $\mathrm{PGL}_2(\mathbb{F}_p)$:



Proposition 5.1 *The function field $k_p\,(X^+(N,p))$ produces, by specialization over a rational point on $X^+(N)$ corresponding to a $\mathbb{Q}$-curve E, the fixed field of the Galois representation ϱ_E.*

Proof. Let E be a $\mathbb{Q}$-curve of degree N defined over a quadratic field k. Fix an automorphism ν in $\mathrm{G}_{\mathbb{Q}} \setminus \mathrm{G}_k$ and an isogeny $\mu\colon E \longrightarrow {}^{\nu}E$ of degree N. If we let C be the kernel of μ, the pair (E,C) defines a k-rational point on $X_0(N)$ with rational image on $X^+(N)$. The preimages on $X^+(N,p)$ of this rational point are given by the couples $\{P, w(P)\}$ for all points P on $X(N,p)$ represented by a triple of the form $(E,\, C,\, [T_1,T_2]_V)$. If we denote by H the subgroup of G_{k_p} fixing those couples, what the proposition asserts is that H equals the kernel of ϱ_E. This kernel is indeed a subgroup of G_{k_p} because the fixed field of $\det \varrho_E$ is k_p (cf. Corollary 2.5). For a point P as above, $w(P)$ is given by the triple $({}^{\nu}E,\, {}^{\nu}C,\, [\sqrt{N}^{-1}\mu(T_1), \sqrt{N}^{-1}\mu(T_2)]_V)$. Take now any σ in G_{k_p}, so that ${}^{\sigma}\zeta_p = \zeta_p^{r^2}$ for some r in $\mathbb{F}_p^*$. If $\sigma \in \mathrm{G}_k$, then $\sigma \in H$ if and only if ${}^{\sigma}P = P$, namely if and

only if ${}^{\sigma}T = \pm r\,T$ for all points T in $E[p]$. If $\sigma \notin \mathrm{G}_k$, then $\sigma \in H$ if and only if ${}^{\sigma}P = w(P)$, namely if and only if ${}^{\sigma}T = \pm r\,\sqrt{N}^{-1}\mu(T)$ for all points T in $E[p]$. Therefore, the result follows from the definition of ϱ_E. $\square$

Suppose that we are now given a Galois representation

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

with cyclotomic determinant, which means that the fixed field of $\det\varrho$ is k_p. For the moduli problem of classifying the $\mathbb{Q}$-curves of degree N realizing ϱ, we twist the curve $X^+(N,p)$ by certain elements in the cohomology set $H^1(\mathrm{G}_{\mathbb{Q}}, \mathcal{G}(N,p))$. Recall that the twists of a curve defined over $\mathbb{Q}$, up to $\mathbb{Q}$-isomorphism, are in bijection with the elements in the first cohomology set of $\mathrm{G}_{\mathbb{Q}}$ with values in the automorphism group of the curve.

The Galois action on $\mathcal{G}(N,p)$ is known from Corollary 4.2. Now, the action by conjugation of $\mathrm{PGL}_2(\mathbb{F}_p)$ makes this group isomorphic to the automorphism group of $\mathrm{PSL}_2(\mathbb{F}_p)$. Hence, the canonical isomorphism $\mathcal{G}(N,p) \simeq \mathrm{PSL}_2(\mathbb{F}_p)$ induces an isomorphism $\mathrm{Aut}\,(\mathcal{G}(N,p)) \simeq \mathrm{PGL}_2(\mathbb{F}_p)$ through which the Galois action on $\mathcal{G}(N,p)$ can be described by the morphism

$$\eta : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(k_p/\mathbb{Q}) \simeq \langle \hat{V} \rangle \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_p).$$

Consider then the 1-cocycles $\xi = \varrho_*\eta$ and $\xi' = \varrho'_*\eta$, where $\varrho_*(\sigma) = {}^{\mathrm{t}}\varrho(\sigma^{-1})$ and $\varrho'_*(\sigma) = \hat{V}\,\varrho_*(\sigma)\,\hat{V}$ for all σ in $\mathrm{G}_{\mathbb{Q}}$. The cyclotomic hypothesis allows us to regard them, through the above canonical isomorphism, as cocycles with values in $\mathcal{G}(N,p)$. The cocycle condition for ξ, namely $\xi_{\sigma\tau} = \xi_\sigma\,{}^{\sigma}\xi_\tau$ for all σ, τ in $\mathrm{G}_{\mathbb{Q}}$, can be easily checked case by case, depending on whether σ and τ belong to G_{k_p} or not. The same holds for ξ'. The cocycle ξ defines a rational model $X^+(N,p)_\varrho$ for the corresponding twist of $X^+(N,p)$, together with an isomorphism

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

satisfying $\psi_+ = \xi_\sigma\,{}^{\sigma}\psi_+$ for every σ in $\mathrm{G}_{\mathbb{Q}}$. Let us denote by $X^+(N,p)'_\varrho$ and ψ'_+ the analogous twist and isomorphism defined by the cocycle ξ'.

Theorem 5.2 *There exists a (possibly fake) $\mathbb{Q}$-curve of degree N realizing ϱ 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 of the isomorphisms ψ_+ and ψ'_+ with the natural map $X^+(N,p) \longrightarrow X^+(N)$ define a surjective map from this set of points to the set of isomorphism classes of:*

- *$\mathbb{Q}$-curves of degree N up to Galois conjugation realizing ϱ,*
- *fake $\mathbb{Q}$-curves of degree N realizing ϱ.*

This map is bijective if and only if the centralizer in $\mathrm{PGL}_2(\mathbb{F}_p)$ of the image of ϱ is trivial.

Proof. The rational points on $X^+(N,p)_\varrho$ correspond via ψ_+ to the couples of the form $\{P, w(P)\}$, where P is an algebraic point on $X(N,p)$ such that, for each given automorphism σ in $\mathrm{G}_\mathbb{Q}$, either $\xi_\sigma({}^\sigma P) = P$ or $\xi_\sigma({}^\sigma P) = w(P)$.

Let P be a non-CM point in $X(N,p)(\overline{\mathbb{Q}})$ given by a triple $(E,\, C,\, [T_1, T_2]_V)$. We use the basis $[T_1, T_2]$ of $E[p]$ to fix the isomorphism $\mathrm{Aut}\,(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$. By virtue of Proposition 4.1, the condition ${}^\sigma P = \xi_\sigma^{-1}(P)$ for all σ in $\mathrm{G}_\mathbb{Q}$ amounts to saying that $\{E, E/C\}$ is a fake $\mathbb{Q}$-curve of degree N such that the equality

$$\varrho_E(\sigma) \;=\; \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \varrho(\sigma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{1}$$

holds in $\mathrm{PGL}_2(\mathbb{F}_p)$ for every σ in $\mathrm{G}_\mathbb{Q}$. Here, we extend the notation ϱ_E to the case of elliptic curves over $\mathbb{Q}$ by putting $\varrho_E = \overline{\rho}_E$.

If, on the other hand, there exists ν in $\mathrm{G}_\mathbb{Q}$ for which $\xi_\nu({}^\nu P) = w(P)$, then E must be a quadratic $\mathbb{Q}$-curve for the point $\psi_+^{-1}(\{P, w(P)\})$ on $X^+(N,p)_\varrho$ to be rational. Indeed, in this case the subgroup of $\mathrm{G}_\mathbb{Q}$ consisting of those automorphisms σ which satisfy $\xi_\sigma({}^\sigma P) = P$ has index two, so it is of the form G_k for some quadratic field k, and then the condition ${}^\sigma P = \xi_\sigma^{-1}(P)$ for all σ in G_k forces the elliptic curve E and the subgroup C to be defined over k, while the condition $w({}^\nu P) = \xi_\nu^{-1}(P)$ gives an isogeny $\lambda : {}^\nu E \longrightarrow E$ with kernel ${}^\nu C$.

So assume now E and C to be defined over a quadratic field k and let λ be an isogeny as above. Then, for $\sigma \notin \mathrm{G}_k$, the point $w({}^\sigma P)$ is represented by the triple given by the elliptic curve E, the cyclic group C and the H_V–orbit of the basis

$[\,(r\sqrt{N}\,)^{-1}\,\lambda({}^\sigma T_1),\, (r\sqrt{N}\,)^{-1}\,\lambda({}^\sigma T_2)\,]$	if ${}^\sigma\zeta_p = \zeta_p^{r^2}$
$[\,(v\,r\sqrt{N}\,)^{-1}\,\lambda({}^\sigma T_1),\, (v\,r\sqrt{N}\,)^{-1}\,\lambda({}^\sigma T_2)\,]\,V$	if ${}^\sigma\zeta_p = \zeta_p^{v\,r^2}$

This comes from Proposition 4.3 and the isomorphism ${}^\nu E/{}^\nu C \longrightarrow E$ induced by the isogeny λ. Notice that the second case does not occur whenever $k = k_p$.

On the other hand, the automorphism ξ_σ^{-1} is given by ${}^{\mathrm{t}}\varrho(\sigma)$, if $\sigma \in \mathrm{G}_{k_p}$, or by $\hat{V}\,{}^{\mathrm{t}}\varrho(\sigma)$, if $\sigma \notin \mathrm{G}_{k_p}$. Then, by applying Proposition 4.1 to each case, we obtain that the point $\psi_+^{-1}(\{P, w(P)\})$ on $X^+(N,p)_\varrho$ is rational if and only if condition (1) holds for every σ in $\mathrm{G}_\mathbb{Q}$.

Similarly, consider a point on $X^+(N,p)'_\varrho$ corresponding via ψ'_+ to a point on $X^+(N,p)$ obtained from a triple $(E,\, C,\, [T_1, T_2]_V)$. By the same reasoning as above, this point is rational if and only if the pair (E, C) represents a (possibly fake) $\mathbb{Q}$-curve of degree N such that, for every σ in $\mathrm{G}_\mathbb{Q}$,

$$\varrho_E(\sigma) \;=\; V \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \varrho(\sigma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} V. \tag{2}$$

Let us now consider a (possibly fake) $\mathbb{Q}$-curve of degree N given by some point (E, C) on $X_0(N)$ and assume $\varrho_E = \varrho$. Since this is an equality up to

conjugation in $\mathrm{PGL}_2(\mathbb{F}_p)$, it amounts to the existence of a basis $[T_1, T_2]$ of $E[p]$ for which condition (1) holds for every σ in $\mathrm{G}_{\mathbb{Q}}$. Moreover, we can suppose that such a basis is sent to either ζ_p or $\zeta_p^{v^{-1}}$ by the Weil pairing. In the first case, the image on $X^+(N,p)$ of the triple $(E,\, C,\, [T_1,T_2]_V)$ defines through ψ_+ a rational point on $X^+(N,p)_\varrho$. In the second case, take $[T_1', T_2'] = [T_1, T_2]\, V$. For this new basis, which is sent to ζ_p under the Weil pairing, condition (2) is satisfied for every σ in $\mathrm{G}_{\mathbb{Q}}$. So the image on $X^+(N,p)$ of the triple $(E,\, C,\, [T_1',T_2']_V)$ defines through ψ_+' a rational point on $X^+(N,p)_\varrho'$.

This proves the first part of the statement, including the surjectivity of the map whenever it is defined. To discuss its injectivity, consider a point (E,C) on $X_0(N)$ yielding a (possibly fake) $\mathbb{Q}$-curve of degree N. Suppose that one can take two different rational points on the twists, corresponding (via ψ_+ or ψ_+') to points on $X^+(N,p)$ obtained from two triples of the form $(E,\, C,\, [T_1,T_2]_V)$. Three different cases must be distinguished to complete the proof:

- Both rational points are on $X^+(N,p)_\varrho$ if and only if there is a non-trivial element γ in $\mathrm{PSL}_2(\mathbb{F}_p)$, representing a basis change in $E[p]$, such that

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \varrho(\sigma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \;=\; \gamma \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \varrho(\sigma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \gamma^{-1}$$

  for all σ in $\mathrm{G}_{\mathbb{Q}}$. This amounts to the existence of a non-trivial element in $\mathrm{PSL}_2(\mathbb{F}_p)$ commuting with all the elements in the image of ϱ.

- The same characterization is obtained if both points lie on $X^+(N,p)_\varrho'$.

- One of the points is on $X^+(N,p)_\varrho$ and the other on $X^+(N,p)_\varrho'$ if and only if there exists γ in $\mathrm{PSL}_2(\mathbb{F}_p)$ such that

$$V \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \varrho(\sigma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} V \;=\; \gamma \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \varrho(\sigma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \gamma^{-1}$$

  for every σ in $\mathrm{G}_{\mathbb{Q}}$. This amounts to the existence of an element in $\mathrm{PGL}_2(\mathbb{F}_p)$ not lying in $\mathrm{PSL}_2(\mathbb{F}_p)$ and commuting with all the elements in the image of ϱ. □

Note that the set of points in Theorem 5.2 is always finite whenever the genus of $X^+(N)$ is greater than one. One can assure this for $N > 131$: indeed, the modular curve $X_0(N)$ has genus at least two and is neither hyperelliptic [Ogg74] nor bielliptic [Bar99] for any such integer N. Using Proposition 3.7, one actually gets the following improvement.

Corollary 5.3 *For N square mod p, the number of isomorphism classes of $\mathbb{Q}$-curves of degree N realizing ϱ is finite, except possibly in the case $N = 4$, $p = 3$.*

For $\mathbb{Q}$-curves of degree N realizing ϱ, a different moduli description that gets rid of fake $\mathbb{Q}$-curves can be given for every quadratic field of definition. In order to do that, we twist $X(N,p)$ by two certain elements in the cohomology set $H^1(\mathrm{G}_{\mathbb{Q}}, \mathcal{W}(N,p))$ that are naturally obtained from the above cocycles ξ and ξ' as follows. By Proposition 3.1 and Corollary 4.4, the $\mathrm{G}_{\mathbb{Q}}$-group $\mathcal{W}(N,p)$ equals the direct product of $\mathrm{G}_{\mathbb{Q}}$-groups $\mathcal{G}(N,p) \times \langle w \rangle$. Then, $H^1(\mathrm{G}_{\mathbb{Q}}, \mathcal{W}(N,p))$ is also the direct product of the corresponding cohomology sets. Fix now a quadratic field k and take the Galois character

$$\chi_k : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(k/\mathbb{Q}) \simeq \langle w \rangle.$$

We then consider the 1-cocycle $\xi\,\chi_k$ and the rational model $X(N,p)_{\varrho,\,k}$ for the corresponding twist, along with the isomorphism

$$\psi_k : X(N,p)_{\varrho,\,k} \longrightarrow X(N,p)$$

satisfying $\psi_k = (\xi\,\chi_k)_\sigma\, {}^\sigma\psi_k$ for every σ in $\mathrm{G}_{\mathbb{Q}}$. Analogously, let us denote by $X(N,p)'_{\varrho,\,k}$ and ψ'_k the twist and the isomorphism defined by the cocycle $\xi'\chi_k$.

Theorem 5.4 *There exists a $\mathbb{Q}$-curve of degree N defined over k realizing ϱ if and only if the set of non-cuspidal non-CM rational points on the curves $X(N,p)_{\varrho,\,k}$ and $X(N,p)'_{\varrho,\,k}$ is not empty. In this case, the compositions of the isomorphisms ψ_k and ψ'_k with the natural map $X(N,p) \longrightarrow X_0(N)$ define a surjective map from this set of points to the set of isomorphism classes of $\mathbb{Q}$-curves of degree N defined over k realizing ϱ. This map is bijective if and only if the centralizer in $\mathrm{PGL}_2(\mathbb{F}_p)$ of the image of ϱ is trivial.*

Proof. The rational points on $X_{\varrho,\,k}(N,p)$ correspond via ψ_k to the algebraic points P on $X(N,p)$ such that

$$\xi_\sigma^{-1}(P) = \begin{cases} {}^\sigma P & \text{for } \sigma \in \mathrm{G}_k\,, \\ w({}^\sigma P) & \text{for } \sigma \notin \mathrm{G}_k\,. \end{cases}$$

The proof runs then in a very similar way to that of Theorem 5.2, so we omit the details. In the current case, a non-CM point on $X(N,p)_{\varrho,\,k}$ corresponding via ψ_k to a triple $(E,\, C,\, [T_1,T_2]_V)$ is rational if and only if E is defined over k, there exists an isogeny from E to its Galois conjugate with kernel C and condition (1) holds for every σ in $\mathrm{G}_{\mathbb{Q}}$ whenever one uses the basis $[T_1,T_2]$ to fix the isomorphism $\mathrm{Aut}\,(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$. The same characterization is valid for the rational points on $X(N,p)'_{\varrho,\,k}$ if we replace ψ_k by ψ'_k and condition (1) by condition (2). $\square$

Remark 5.5 One can check that ξ and ξ' are cohomologous as 1-cocycles with values in $\mathcal{G}(N,p)$ if and only if the centralizer in $\mathrm{PGL}_2(\mathbb{F}_p)$ of the image of ϱ does not lie in $\mathrm{PSL}_2(\mathbb{F}_p)$. Thus, the twists $X^+(N,p)_\varrho$ and $X^+(N,p)'_\varrho$ are not a priori isomorphic over $\mathbb{Q}$. The same holds for the twisted curves $X(N,p)_{\varrho,\,k}$ and $X(N,p)'_{\varrho,\,k}$. Moreover, it can be shown that the involution w does not switch the rational points on $X(N,p)_{\varrho,\,k}$ and $X(N,p)'_{\varrho,\,k}$, so finding the underlying $\mathbb{Q}$-curves requires in general the rational points on both twists.

6 The twisted curve in the non-cyclotomic case

Assume N to be a non-square mod p. This section is the analogue of the previous one for the non-cyclotomic case. Unlike the cyclotomic case, now the quadratic field of definition for the potential $\mathbb{Q}$-curves of degree N realizing a given projective mod p Galois representation is fixed by the determinant. Moreover, only one twist is needed for the moduli classification of such $\mathbb{Q}$-curves. We prove this in Theorem 6.4 below. For the sake of completeness, let us begin as before with the modular construction of the fixed field of the Galois representation ϱ_E attached to a $\mathbb{Q}$-curve E of degree N. The procedure is now more intricate.

Recall that the group $\mathcal{W}(N,p)$ of the covering $X(N,p) \longrightarrow X^+(N)$ is canonically isomorphic to $\mathrm{PGL}_2(\mathbb{F}_p)$. The action by conjugation of this group makes it isomorphic to its automorphism group. Thus, by virtue of Corollary 4.2 and Corollary 4.4, the Galois action on $\mathcal{W}(N,p)$ is given by the morphism

$$\eta : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(k_p/\mathbb{Q}) \simeq \langle w \rangle \hookrightarrow \mathcal{W}(N,p),$$

where we identify $\mathcal{W}(N,p)$ with its (inner) automorphism group.

Let $\widetilde{X}(N,p)$ be the twist of $X(N,p)$ defined by the 1-cocycle η. Likewise, denote by $\widetilde{X}_0(N)$ the twist of $X_0(N)$ defined by the 1-cocycle

$$\mathrm{G}_{\mathbb{Q}} \longrightarrow \mathrm{Gal}(k_p/\mathbb{Q}) \simeq \langle w_N \rangle.$$

We write $\widetilde{X}^+(N)$ for the quotient of $\widetilde{X}_0(N)$ by the involution corresponding to w_N. Consider the following commutative diagram, where the morphisms are the natural ones:

$$\begin{array}{ccc} \widetilde{X}(N,\,p) & \xrightarrow{\simeq} & X(N,\,p) \\ \downarrow & & \downarrow \\ \widetilde{X}_0(N) & \xrightarrow{\simeq} & X_0(N) \\ \downarrow & & \downarrow \\ \widetilde{X}^+(N) & \xrightarrow{\simeq} & X^+(N) \end{array}$$

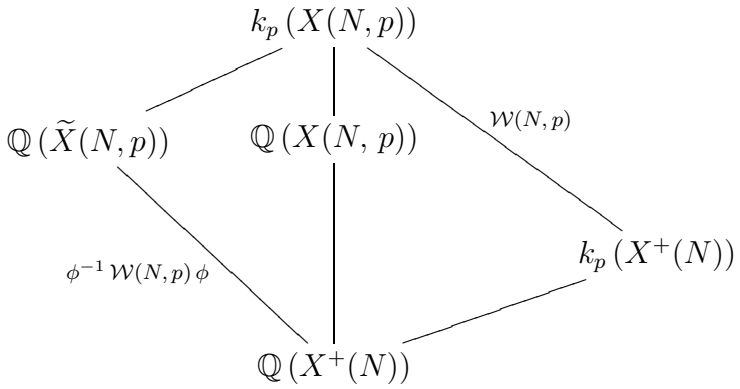
As remarked in the proof of the next lemma, the isomorphism $\widetilde{X}^+(N) \longrightarrow X^+(N)$ is actually defined over $\mathbb{Q}$.

Lemma 6.1 *The Galois covering $\widetilde{X}(N,p) \longrightarrow \widetilde{X}^+(N)$ is defined over $\mathbb{Q}$.*

Proof. Denote by $\phi : \widetilde{X}(N,p) \longrightarrow X(N,p)$ and $\phi_0 \colon \widetilde{X}_0(N) \longrightarrow X_0(N)$ the isomorphisms in the above diagram. They are defined over k_p and satisfy ${}^{\sigma}\phi\,\phi^{-1} = w$ and ${}^{\sigma}\phi_0\,\phi_0^{-1} = w_N$ for $\sigma \notin \mathrm{G}_{k_p}$. Then, the involution $\phi_0^{-1}\, w_N\, \phi_0$ on $\widetilde{X}_0(N)$ is defined over $\mathbb{Q}$. Hence, so is the corresponding quotient map $\widetilde{X}_0(N) \longrightarrow \widetilde{X}^+(N)$. The isomorphism $\phi_+ \colon X^+(N) \longrightarrow \widetilde{X}^+(N)$ induced by ϕ_0^{-1}

sends a couple $\{P, w_N(P)\}$ to $\{\phi_0^{-1}(P), \phi_0^{-1}\, w_N(P)\}$. It is easily checked to satisfy ${}^\sigma\phi_+ = \phi_+$ for all σ in $\mathrm{G}_\mathbb{Q}$. The same is true for the morphism $\widetilde{X}(N,p) \longrightarrow \widetilde{X}_0(N)$ induced from the natural map $X(N,p) \longrightarrow X_0(N)$ by the isomorphisms ϕ and ϕ_0. Finally, the automorphisms of the covering $\widetilde{X}(N,p) \longrightarrow \widetilde{X}^+(N)$ are also defined over $\mathbb{Q}$. Indeed, the relation ${}^\sigma(\phi^{-1}\,\vartheta\,\phi) = \phi^{-1}\, w\,(w\,\vartheta\, w)\, w\,\phi = \phi^{-1}\,\vartheta\,\phi$ holds for $\vartheta \in \mathcal{W}(N,p)$ and $\sigma \notin \mathrm{G}_{k_p}$. For another proof of the existence of such a rational covering we refer to [Shi74]. □

Remark 6.2 The function field of $\widetilde{X}(N,p)$ over $\mathbb{Q}$ is identified, through the isomorphism ϕ in the proof of Lemma 6.1, with a subfield of $k_p\,(X(N,p))$. As shown in the following diagram, it is a Galois extension of $\mathbb{Q}\,(X^+(N))$ with group isomorphic to $\mathrm{PGL}_2(\mathbb{F}_p)$:



Proposition 6.3 *The function field $\mathbb{Q}\,(\widetilde{X}(N,p))$ gives, by specialization over a rational point on $X^+(N)$ corresponding to a $\mathbb{Q}$-curve E, the fixed field of the representation ϱ_E.*

Proof. With the same notations as in the proof of Proposition 5.1, take a cyclic isogeny $\mu : E \longrightarrow {}^\nu E$ with kernel C of order N. Consider the isomorphism $\phi : \widetilde{X}(N,p) \longrightarrow X(N,p)$ in the proof of Lemma 6.1. Let H be the subgroup of $\mathrm{G}_\mathbb{Q}$ fixing the points on $\widetilde{X}(N,p)$ corresponding through ϕ to the points on $X(N,p)$ of the form P or $w(P)$, where P is given by a triple of the form $(E,\, C,\, [T_1, T_2]_V)$. We must show that H is the kernel of ϱ_E. For a point P as above, $w(P)$ is represented by the triple given by ${}^\nu E$, ${}^\nu C$ and the H_V–orbit of the basis $[\mu(T_1), \mu(T_2)]V$. Using the definition of ϕ, we see that the group H consists of those $\sigma \in \mathrm{G}_{k_p}$ satisfying ${}^\sigma P = P$ and those $\sigma \notin \mathrm{G}_{k_p}$ satisfying ${}^\sigma P = w(P)$. Moreover, any such σ lies in G_k if and only if it lies in G_{k_p}. Take now any automorphism σ in $\mathrm{G}_\mathbb{Q}$. If ${}^\sigma\zeta_p = \zeta_p^{\,r^2}$ for some r in $\mathbb{F}_p^*$, then $\sigma \in H$ if and only if ${}^\sigma P = P$, namely if and only if ${}^\sigma T = \pm r\, T$ for all points T in $E[p]$. If ${}^\sigma\zeta_p = \zeta_p^{\,r^2 N^{-1}}$ for some r in $\mathbb{F}_p^*$, then $\sigma \in H$ if and only if ${}^\sigma P = w(P)$, namely if and only if ${}^\sigma T = \pm r\, N^{-1}\,\mu(T)$ for all points T in $E[p]$. So the result follows from the definition of ϱ_E. □

Suppose that we have now a Galois representation

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

with non-cyclotomic determinant. Recall that any $\mathbb{Q}$-curves of degree N realizing ϱ must be defined over the fixed field of $\varepsilon \det \varrho$, where ε is the character attached to k_p (cf. Corollary 2.5). Denote this quadratic field by k. 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 $H^1(\mathrm{G}_{\mathbb{Q}}, \mathcal{W}(N,p))$, as follows. The canonical isomorphism $\mathcal{W}(N,p) \simeq \mathrm{PGL}_2(\mathbb{F}_p)$ allows us to regard the projective representation ϱ_* in Section 5 as a morphism taking values in $\mathcal{W}(N,p)$. As before, let η stand for the morphism giving the Galois action on $\mathcal{W}(N,p)$. Then, consider the 1-cocycle $\xi = \varrho_* \eta$. For the twist of $X(N,p)$ defined by ξ, we fix a rational model $X(N,p)_\varrho$ along with an isomorphism

$$\psi : X(N,p)_\varrho \longrightarrow X(N,p)$$

satisfying $\psi = \xi_\sigma {}^\sigma\psi$ for every σ in $\mathrm{G}_{\mathbb{Q}}$.

Theorem 6.4 *There exists a $\mathbb{Q}$-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 not empty. In this case, the composition of ψ with the natural map $X(N,p) \longrightarrow X^+(N)$ defines a surjective map from this set of points to the set of isomorphism classes of $\mathbb{Q}$-curves of degree N up to Galois conjugation realizing ϱ. This map is bijective if and only if the centralizer in $\mathrm{PGL}_2(\mathbb{F}_p)$ of the image of ϱ is trivial.*

Proof. The first part of the proof goes along the lines of those of Theorem 5.2 and Theorem 5.4. Let us fix an automorphism ν in $\mathrm{G}_{\mathbb{Q}} \backslash \mathrm{G}_k$. The rational points on $X_\varrho(N,p)$ correspond via ψ to the algebraic points P on $X(N,p)$ satisfying

$$\varrho_*(\sigma)^{-1}(P) \;=\; \begin{cases} {}^\sigma P & \text{for } \sigma \in \mathrm{G}_{k_p}\,, \\ w({}^\sigma P) & \text{for } \sigma \notin \mathrm{G}_{k_p}\,. \end{cases}$$

Note that the automorphism $\varrho_*(\sigma)^{-1}$ belongs to $\mathcal{G}(N,p)$ if and only if σ lies in either both G_k and G_{k_p} or none of them. In particular, a non-CM point P given by a triple $(E,\, C,\, [T_1, T_2]_V)$ can satisfy the above condition only if E and C are defined over k and there is an isogeny $\lambda : {}^\nu E \longrightarrow E$ with kernel ${}^\nu C$. With these hypotheses on E and C, and for $\sigma \notin \mathrm{G}_k$, the point $w({}^\sigma P)$ is represented by the triple given by $E,\ C$ and the H_V–orbit of the basis

$[\, r^{-1}\, \lambda({}^\sigma T_1),\, r^{-1}\, \lambda({}^\sigma T_2)\,]\, V$	if ${}^\sigma\zeta_p = \zeta_p^{r^2}$
$[\, r^{-1}\, \lambda({}^\sigma T_1),\, r^{-1}\, \lambda({}^\sigma T_2)\,]$	if ${}^\sigma\zeta_p = \zeta_p^{r^2 N^{-1}}$

In the second case, and also for $\sigma \in \mathrm{G}_k \cap \mathrm{G}_{k_p}$, the automorphism $\varrho_*(\sigma)^{-1}$ is given by the matrix ${}^{\mathrm{t}}\varrho(\sigma)$ in $\mathrm{PSL}_2(\mathbb{F}_p)$. In the other case, and also for $\sigma \in \mathrm{G}_k \setminus \mathrm{G}_{k_p}$, the automorphism $w\,\varrho_*(\sigma)^{-1}$ is given by the matrix $\hat{V}\ {}^{\mathrm{t}}\varrho(\sigma)$ in $\mathrm{PSL}_2(\mathbb{F}_p)$. So, taking as in the proof of Theorem 5.2 the basis $[T_1, T_2]$ to fix the isomorphism $\mathrm{Aut}\,(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$, condition (1) is again seen to characterize the rationality of the point $\psi^{-1}(P)$.

Consider now a non-CM elliptic curve E defined over k and an isogeny $\mu : E \longrightarrow {}^{\nu}E$ with kernel C, and assume $\varrho_E = \varrho$. This equality amounts to the existence of a basis $[T_1, T_2]$ of $E[p]$ for which condition (1) holds for every σ in $\mathrm{G}_{\mathbb{Q}}$. We can further suppose that such a basis is sent to either ζ_p or ζ_p^{N-1} by the Weil pairing. In the first case, the point P on $X(N,p)$ given by the triple $(E,\, C,\, [T_1, T_2]_V)$ defines through ψ a rational point on $X(N,p)_{\varrho}$. In the second case, the triple $({}^{\nu}E,\, {}^{\nu}C,\, [\mu(T_1), \mu(T_2)]_V)$ represents a point on $X(N,p)$ lying above the same point on $X^+(N)$ as P and corresponding via ψ to a rational point on $X(N,p)_{\varrho}$. Indeed, if we choose the basis $[\mu(T_1), \mu(T_2)]$ to fix the isomorphism $\mathrm{Aut}({}^{\nu}E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$, we get the equality $\varrho_{\,{}^{\nu}E}(\sigma) = \varrho_E(\sigma)$ for all σ in $\mathrm{G}_{\mathbb{Q}}$.

Lastly, let us consider two different rational points on $X(N,p)_{\varrho}$ corresponding via ψ to non-CM points P and Q on $X(N,p)$ with the same image on $X^+(N)$. Let the triple $(E,\, C,\, [T_1, T_2]_V)$ represent the point P and fix an isogeny $\mu : E \longrightarrow {}^{\nu}E$ with kernel C. We must then distinguish two cases for the point Q:

- It lies over the pair (E, C) on $X_0(N)$ if and only if there is a non-trivial element γ in $\mathrm{PSL}_2(\mathbb{F}_p)$, representing a basis change in $E[p]$, such that

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \varrho(\sigma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \;=\; \gamma \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \varrho(\sigma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \gamma^{-1}$$

  for all σ in $\mathrm{G}_{\mathbb{Q}}$. This amounts to the existence of a non-trivial element in $\mathrm{PSL}_2(\mathbb{F}_p)$ commuting with all the elements in the image of ϱ.

- Otherwise, a triple representing Q is given by the elliptic curve ${}^{\nu}E$, the subgroup ${}^{\nu}C$ and the H_V–orbit of a basis obtained from $[\mu(T_1), \mu(T_2)]\, V$ by a basis change preserving the Weil pairing. Thus, this case amounts to the existence of an element γ in $\mathrm{PSL}_2(\mathbb{F}_p)$ such that

$$V \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \varrho(\sigma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} V \;=\; \gamma \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \varrho(\sigma) \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \gamma^{-1}$$

  for all σ in $\mathrm{G}_{\mathbb{Q}}$. This is in turn equivalent to the existence of an element in $\mathrm{PGL}_2(\mathbb{F}_p) \backslash \mathrm{PSL}_2(\mathbb{F}_p)$ commuting with all the elements in the image of ϱ. □

By the same reasoning as in Section 5, the set of points in Theorem 6.4 is always finite whenever $N > 131$. A stronger result is obtained from Corollary 3.5.

Corollary 6.5 *For N non-square mod p, the number of isomorphism classes of $\mathbb{Q}$-curves of degree N realizing ϱ is finite, unless $N = 2$ and $p = 3$.*

Acknowledgements

I wish to express my gratitude to Joan-Carles Lario for his help and encouragement through this work. I am most indebted to René Schoof and the *Dipartimento di Matematica* of the *Università di Roma "Tor Vergata"* as well as to the *Département de Mathématiques de Besançon*, where this research was carried out with financial support from the RTN European Network *Galois Theory and Explicit Methods in Arithmetic*. It is also a pleasure to thank Gabriel Cardona for some helpful comments on an earlier version of the paper.

References

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

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

[FGL] J. Fernández, J. González, and J.-C. Lario. Plane quartic twists of $X(5,3)$. *To appear in Canad. Math. Bull.* Preprint available at `http://arxiv.org/abs/math.NT/0501520`.

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

[Klu77] P. G. Kluit. On the normalizer of $\Gamma_0(N)$. In *Modular functions of one variable V.* Lecture Notes in Math., vol. 601, pages 239–246. Springer, 1977.

[Lig77] G. Ligozat. Courbes modulaires de niveau 11. In *Modular functions of one variable V.* Lecture Notes in Math., vol. 601, pages 149–237. Springer, 1977.

[Maz77] B. Mazur. Rational points on modular curves. In *Modular functions of one variable V.* Lecture Notes in Math., vol. 601, pages 107–148. Springer, 1977.

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

[Rib92] K. A. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *Algebra and topology 1992 (Taejŏn)*, pages 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.

[Ser92] J.-P. Serre. *Topics in Galois theory.* Jones and Bartlett Publishers, 1992. Lecture notes prepared by Henri Darmon.

[Shi74] K.-Y. Shih. On the construction of Galois extensions of function fields and number fields. *Math. Ann.*, 207:99–120, 1974.

[Shi78] K.-Y. Shih. p-division points on certain elliptic curves. *Comp. Math.*, 36(2):113–129, 1978.

[STN92] STNB. *Corbes modulars: taules*. Barcelona, 1992. Notes del Seminari de Teoria de Nombres de Barcelona, UB-UAB-UPC.

Julio Fernández
Departament de Matemàtica Aplicada 4
Universitat Politècnica de Catalunya
EPSEVG, av. Víctor Balaguer
E-08800 Vilanova i la Geltrú (Barcelona)
julio@mat.upc.edu