A moduli interpretation for the non-split Cartan modular curve

Marusia Rebolledo, Christian Wuthrich

A moduli interpretation for the non-split Cartan modular curve

Marusia Rebolledo and Christian Wuthrich

28th November 2014

Abstract

Modular curves like $X_0(N)$ and $X_1(N)$ appear very frequently in arithmetic geometry. While their complex points are obtained as a quotient of the upper half plane by some subgroups of $\mathrm{SL}_2(\mathbb{Z})$, they allow for a more arithmetic description as a solution to a moduli problem. This description turns out to be very useful in many applications. We wish to give such a moduli description for two other modular curves, denoted here by $X_{\mathrm{nsp}}(p)$ and $X^+_{\mathrm{nsp}}(p)$ associated to non-split Cartan subgroups and their normaliser in $\mathrm{GL}_2(\mathbb{F}_p)$. These modular curves appear for instance in Serre's problem of classifying all possible Galois structures of p-torsion points on elliptic curves over number fields. We give then a moduli-theoretic interpretation and a new proof of a result of Chen [Che98, Che00].

1 Introduction

Let p be an odd prime. Let $Y(p)$ be the affine modular curve classifying elliptic curves with full level p structure. The completed modular curve $X(p)$ classifies generalised elliptic curves with full level p structure. Those two curves admit integral models over the ring of integers of the cyclotomic field $\mathbb{Q}(\zeta_p)$. See [DR73] and [KM85]. The modular curve $X(p)$ comes equipped with a natural action by $\mathrm{GL}_2(\mathbb{F}_p)$. For any subgroup $\mathcal{H}$ of $\mathrm{GL}_2(\mathbb{F}_p)$ the quotient $X(p)/\mathcal{H}$ defines an algebraic curve $X_{\mathcal{H}}$ over $\mathbb{Q}(\zeta_p)^{\det(\mathcal{H})}$. Hence the points on $X_{\mathcal{H}}$ over an algebraically closed field $\bar{k}$ of characteristic different from p are $\mathcal{H}$-orbits of $\bar{k}$-points of $X(p)$. However in some interesting cases, there is a nice description of a moduli problem for $X_{\mathcal{H}}$ too.

As an example, we explain the case when $\mathcal{H}$ is the Borel subgroup $\mathcal{B} = \left\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\right\}$ in $\mathrm{GL}_2(\mathbb{F}_p)$. First, the points in $Y(p)(\bar{k})$ are $\bar{k}$-isomorphism classes of pairs $\big(E, (P,Q)\big)$ where $E/\bar{k}$ is an elliptic curve and (P,Q) form a basis of $E[p]$. For a fixed E, all the pairs (P',Q') in the $\mathcal{B}$-orbit of (P,Q) are such that P' is in the subgroup C generated by P. Hence the $\bar{k}$-points on the quotient curve $Y_{\mathcal{B}}$ can be identified with $\bar{k}$-isomorphism classes of pairs (E,C) with E again an elliptic curve defined over $\bar{k}$ and C a cyclic subgroup of order p in $E[p]$. The latter description is now independent of the initial choice of the Borel subgroup $\mathcal{B}$ in $\mathrm{GL}_2(\mathbb{F}_p)$ and only uses the geometry of E. The curve $X_{\mathcal{B}}$ is usually denoted by $X_0(p)$.

Another example is the quotient by the split Cartan subgroup which consists of diagonal matrices in $\mathrm{GL}_2(\mathbb{F}_p)$. The corresponding curve is denoted here by $X_{\mathrm{sp}}(p)$ and it parametrises $\bar{k}$-isomorphism classes $\big(E, (A,B)\big)$ of generalised elliptic curves E endowed with two distinct cyclic subgroups A and B of order p in E. For its normaliser $\mathcal{S}$, we find the curve $X_{\mathcal{S}} = X^+_{\mathrm{sp}}(p)$ which classifies generalised elliptic curves with an unordered pair $\{A,B\}$ of cyclic subgroups A and B of order p. All these cases are easy to describe because the subgroups $\mathcal{H}$ can be defined as the stabiliser of some object under a natural action of $\mathrm{GL}\big(E[p]\big)$.

In view of Serre's problem to classify the possible Galois module structure of the p-torsion of an elliptic curve over a number field, there are two further modular curves of importance. The aim of this paper is to give a good moduli description for those, namely when $\mathcal{H}$ is a non-split Cartan subgroup or a normaliser of a non-split Cartan subgroup in $\mathrm{GL}_2(\mathbb{F}_p)$. We will denote the corresponding modular curves by $X_{\mathrm{nsp}}(p)$ and $X^+_{\mathrm{nsp}}(p)$ respectively. See the start of Section 2 for detailed definitions. These curves have been studied for instance by Ligozat [Lig77], Halberstadt [Hal98], Chen [Che98, Che00], Merel and Darmon [Mer99, DM97] and Baran [Bar10].

In our description, the modular curve $X^+_{\mathrm{nsp}}(p)$ will classify elliptic curves endowed with a level structure that we call a *necklace*. Roughly speaking, a necklace is a regular $(p+1)$-gon whose corners, called *pearls*,

are all cyclic subgroups of order p in E and such that there is an element in $\mathrm{PGL}\big(E[p]\big)$ that turns this necklace by one pearl. This will not depend on the choice of a non-split Cartan subgroup.

In Section 2, we will define these necklaces in detail and we will give an alternative and more geometric description using the cross-ratio in $\mathbb{P}\big(E[p]\big)$. The following Section 3 shows how classical results about the geometry of $X_{\mathrm{nsp}}(p)$ can be proven using this moduli interpretation. For instance, we can count the number of elliptic points, describe the cusps and the degeneracy maps. In Section 4, we reprove a result by Chen. He shows [Che98, Che00] that there is an isogeny between the Jacobian of $X_{\mathrm{sp}}^+(p)$ and the product of the Jacobians of $X_0(p)$ and $X_{\mathrm{nsp}}^+(p)$. The proof of this theorem is not entirely new, however we believe that it gives a better geometric vision of the maps involved and the representation-theoretic proof. We conclude the paper with some numerical data related to Chen's Theorem.

Since the prime p is fixed throughout the paper, we will now omit it from the notations and only write X_{nsp} and X_{nsp}^+. It is to note that there should be no real difficulty in generalising our moduli description to composite levels N. With view on the problem of Serre to classify the Galois structure of p-torsion subgroups of elliptic curves over $\mathbb{Q}$, prime levels are maybe the most interesting.

Notations

The following is a list of modular curves that appear in this paper and the notations we frequently use. The definitions will be given later. See also Sections 3.1 and 4.1 for degeneracy maps and correspondences between them.

Symbol	Description of $\mathcal{H} < \mathrm{GL}_2(\mathbb{F}_p)$	Level structure
$X(p)$	Full level structure, $\mathcal{H} = \{1\}$	Basis (P, Q) of $E[p]$
$X_{\mathcal{A}}$	Scalar matrices $\mathcal{A}$	Distinct triple (A, B, C) in $\mathbb{P}\big(E[p]\big)$
X_0	A Borel subgroup $\mathcal{B}$	Subgroup $C \in \mathbb{P}\big(E[p]\big)$
X_{sp}	A split Cartan	Distinct pair (A, B) in $\mathbb{P}\big(E[p]\big)$
X_{sp}^+	Normaliser of a split Cartan $\mathcal{S}$	Non-ordered pair $\{A, B\} \subset \mathbb{P}\big(E[p]\big)$
X_{nsp}	A non-split Cartan	Oriented necklace $\mathfrak{v}$
X_{nsp}^+	Normaliser of a non-split Cartan $\mathcal{N}$	Necklace $\mathfrak{v}$

Matrices in $\mathrm{GL}(\mathbb{F}_p)$ will be written as $\left(\begin{smallmatrix} \cdot & \cdot \\ \cdot & \cdot \end{smallmatrix}\right)$. Instead the coset of matrices in $\mathrm{PGL}(\mathbb{F}_p)$ will be represented by matrices of the form $\left[\begin{smallmatrix} \cdot & \cdot \\ \cdot & \cdot \end{smallmatrix}\right]$.

2 The moduli problem of necklaces

2.1 Non-split Cartan subgroups and their modular curves

We refer to [Ser97] for definitions and results about non-split Cartan subgroups and Dixon's classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$ and just briefly recall some facts. The group $\mathrm{GL}_2(\mathbb{F}_p)$ acts on the right on $\mathbb{P}^1(\mathbb{F}_{p^2})$ by $(x : y)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = (ax + cy : bx + dy)$. Any non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ can be defined as the stabiliser $\mathcal{H}_\alpha$ of $(1 : \alpha)$ in $\mathbb{P}^1(\mathbb{F}_{p^2}) \setminus \mathbb{P}^1(\mathbb{F}_p)$ for a choice of $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$. We see that $\mathcal{H}_\alpha$ has order $p^2 - 1$ as the action of $\mathrm{GL}_2(\mathbb{F}_p)$ is transitive on $\mathbb{P}^1(\mathbb{F}_{p^2}) \setminus \mathbb{P}^1(\mathbb{F}_p)$.

Alternatively, we can consider the basis $(1, \alpha)$ of $\mathbb{F}_{p^2}$ as a $\mathbb{F}_p$-vector space. Then we claim that $\mathcal{H}_\alpha$ is equal to the image of the map $i_\alpha \colon \mathbb{F}_{p^2}^\times \to \mathrm{GL}_2(\mathbb{F}_p)$ sending β to the matrix which represents the multiplication by β on $\mathbb{F}_{p^2}$ written in basis $(1, \alpha)$.[1] Indeed, let $\beta = x + y\alpha \in \mathbb{F}_{p^2}^\times$ with $x, y \in \mathbb{F}_p$. If $X^2 - tX + n$ is the minimal polynomial of α over $\mathbb{F}_p$, then

$$i_\alpha(\beta) = \begin{pmatrix} x & -ny \\ y & x + ty \end{pmatrix}$$

and so $(1 : \alpha) i_\alpha(\beta) = (x + y\alpha : -ny + (x + ty)\alpha) = (\beta : \beta\alpha) = (1 : \alpha)$. So the image of i_α is contained in $\mathcal{H}_\alpha$ and they are equal because they are of the same size.

[1] The multiplication of matrices in $\mathrm{GL}_2(\mathbb{F}_p)$ on the two-dimensional vector space happens from the left here.

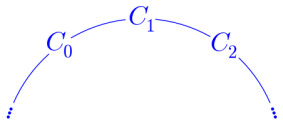
Given a choice of a non-split Cartan subgroup $\mathcal{H}$, we define the modular curve X_{nsp} as the quotient $X_{\mathcal{H}}$. Note that the quotient does not depend on the choice of $\mathcal{H}$ as these subgroups are all conjugate. However the description of points on X_{nsp} as $\mathcal{H}$-orbits do.

The normaliser $\mathcal{N}$ of a non-split Cartan subgroup $\mathcal{H}$ in $\mathrm{GL}_2(\mathbb{F}_p)$ contains $\mathcal{H}$ with index 2. It can be viewed as adding the image under i_α of the conjugation map in $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ on $\mathbb{F}_{p^2}^\times$. The corresponding quotient $X_{\mathcal{N}}$ will be denoted by X_{nsp}^+.

2.2 Necklaces

Let γ be a multiplicative generator of $\mathbb{F}_{p^2}^\times$. For any 2-dimensional $\mathbb{F}_p$-vector space V, we define $\mathcal{C}_\gamma$ to be the conjugacy class in $\mathrm{PGL}(V)$ of all elements h which have a representative in $\mathrm{GL}(V)$ whose characteristic polynomial is equal to the minimal polynomial of γ. In other words, all representatives of $h \in \mathcal{C}_\gamma$ have an eigenvalue in $\mathbb{F}_p^\times \cdot \gamma$. If $\bar\gamma$ is the conjugate of γ over $\mathbb{F}_p$, then $\mathcal{C}_{\bar\gamma} = \mathcal{C}_\gamma$. If a basis of V is chosen then $\mathcal{C}_\gamma$ consist of all classes of matrices $i_\alpha(\gamma)$ as α runs through $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. Note that the class of $i_\alpha(\bar\gamma) = i_{\bar\alpha}(\gamma) = \mathrm{N}(\gamma)^{-1}\, i_\alpha(\gamma)^{-1}$ is equal to the inverse of class of $i_\alpha(\gamma)$. In particular, in any non-split Cartan subgroup in $\mathrm{PGL}(V)$, there are exactly two generators h and h^{-1} that belong to $\mathcal{C}_\gamma$. As γ varies, we obtain the $\frac{1}{2}\varphi(p+1)$ conjugacy classes of elements of order $p+1$.

Let $\bar k$ be an algebraically closed field of characteristic 0 or different from p and let $E/\bar k$ be an elliptic curve. We know that there exists $p+1$ cyclic subgroups of order p in $E[p]$. We will consider lists $(C_0, C_1, \dots, C_p)$ of those cyclic subgroups and will say that two such lists are equivalent if we can obtain one from the other by a cyclic permutation; so $(C_0, C_1, \dots, C_p)$ and $(C_1, C_2, \dots, C_p, C_0)$ are equivalent.



Definition. An equivalence class $(C_0, C_1, \dots, C_p)$ is called an *oriented necklace* of E if there exists an element $h \in \mathcal{C}_\gamma \subset \mathrm{PGL}(E[p])$ such that $h(C_i) = C_{i+1}$ for all $i = 0, \dots, p-1$.

If h is such an element, then we must also have $h(C_p) = C_0$ as h is of order $p+1$. Note also that if $(C_0, C_1, \dots, C_p)$ is an oriented necklace with a certain $h \in \mathcal{C}_\gamma$, then so is $(C_p, C_{p-1}, \dots, C_0)$ because $h^{-1} \in \mathcal{C}_\gamma$.

Let us consider the dependence on γ; so to be more precise, we will call it now an oriented γ-necklace.

Lemma 1. *Let γ and γ' be two generators of $\mathbb{F}_{p^2}^\times$. There is a canonical bijection between oriented γ-necklaces and oriented γ'-necklaces.*

Proof. Since $\mathbb{F}_{p^2}^\times$ is cyclic, there exists an integer $k \in [0, p^2-1]$ such that $\gamma' = \gamma^k$ and such that k is coprime to $p+1$. In particular $\mathcal{C}_{\gamma'}$ is the set of all h^k with $h \in \mathcal{C}_\gamma$. So the requested bijection is given by

$$\begin{aligned} \{\text{oriented } \gamma\text{-necklaces}\} &\to \{\text{oriented } \gamma'\text{-necklaces}\} \\ (C_0, C_1, \dots, C_p) &\mapsto (C_0, C_k, C_{2k}, \dots) \end{aligned}$$

with the index taken modulo $p+1$. □

As a consequence, we may now fix a choice of γ for the rest of the paper.

In a picture, we arrange the subgroups $C_0, \dots, C_p$ like pearls on a necklace that can be turned around the neck using the automorphism h of $\mathbb{P}(E[p])$. If we allow the necklace to be worn in both directions, we get the notion of a necklace without orientation:

Definition. Let w denote the involution defined by

$$w(C_0, C_1, \dots, C_p) = (C_p, C_{p-1}, \dots, C_0)$$

which changes the orientation of an oriented necklace. A *necklace* is a w-orbit of oriented necklaces $\{\mathfrak{v}, w(\mathfrak{v})\}$.

Lemma 2. *Fix a generator γ of $\mathbb{F}_{p^2}^\times$. Let C_0, C_1, and C_2 be three distinct cyclic subgroups of order p in $E[p]$. Then there exists a unique element $h \in \mathcal{C}_\gamma$ in $\mathrm{PGL}(E[p])$ such that $h(C_0) = C_1$ and $h(C_1) = C_2$.*

Proof. Choose generators P_0 and P_1 in C_0 and C_1 respectively and consider them as a basis of $E[p]$. Write t and n for the trace and the norm of γ. Our class of matrices must contain a matrix of the form $\left(\begin{smallmatrix} 0 & y \\ x & t \end{smallmatrix}\right)$ for some x and y in $\mathbb{F}_p^\times$ if we want $h(C_0) = C_1$ and $\mathrm{tr}(h) = t$. As y varies the points $yP_0 + tP_1$ form an affine line and hence there is a unique $y \in \mathbb{F}_p^\times$ such that $yP_0 + tP_1$ belongs to C_2. Finally, we have no choice but to set $x = ny^{-1}$ if we also want $\det(h) = n$. □

This lemma implies that for any triple (C_0, C_1, C_2) of distinct cyclic subgroups of $E[p]$, there is a unique oriented necklace of the form $(C_0, C_1, C_2, \dots)$. We will denote it by $C_0 \to C_1 \to C_2$. Similarly there is a unique necklace with consecutive pearls C_0, C_1, C_2, which we denote by $C_0 - C_1 - C_2$.

There is a natural action of $\mathrm{PGL}(E[p])$ on the set of oriented necklaces by setting $g \cdot (C_0, \dots C_p) = \big(g(C_0), \dots, g(C_p)\big)$ for g in $\mathrm{PGL}(E[p])$. If $h \in \mathcal{C}_\gamma$ is such that $h(C_i) = C_{i+1}$ then $ghg^{-1} \in \mathcal{C}_\gamma$ can be used to show that $\big(g(C_0), \dots, g(C_p)\big)$ is indeed an oriented necklace. Since the action of $\mathrm{PGL}(E[p])$ on $\mathbb{P}(E[p])$ is simply 3-transitive, Lemma 2 implies that the action of $\mathrm{PGL}(E[p])$ is transitive on oriented necklaces. By definition, for every oriented necklace $\mathfrak{v}$, there exists $h \in \mathcal{C}_\gamma$ fixing it. Therefore, the group generated by h, which is a non-split Cartan subgroup in $\mathrm{PGL}(E[p])$ will belong to the stabiliser of $\mathfrak{v}$. It is clear that this is equal to the stabiliser of $\mathfrak{v}$. We have shown:

Corollary 3. *Let $\mathcal{G} = \mathrm{PGL}(E[p])$. The set of oriented γ-necklaces is isomorphic as a $\mathcal{G}$-set to $\mathcal{G}/\mathcal{H}$ where $\mathcal{H}$ is any non-split Cartan group in $\mathcal{G}$. Similarly, the set of γ-necklaces is $\mathcal{G}$-isomorphic to $\mathcal{G}/\mathcal{N}$ for the normaliser of a non-split Cartan group $\mathcal{N}$ in $\mathcal{G}$. In particular, there are exactly $p(p-1)$ oriented necklaces and $p(p-1)/2$ necklaces.*

2.3 Moduli description

Let $\mathcal{H}$ be a non-split Cartan subgroup in $\mathcal{G} = \mathrm{GL}_2(\mathbb{F}_p)$ and write $\mathcal{N}$ for its normaliser. Let $\bar{k}$ be an algebraically closed field of characteristic different from p. The moduli space $Y(p)(\bar{k})$ consists of $\bar{k}$-isomorphism classes of pairs $\big(E, (P, Q)\big)$ where E is an elliptic curve over $\bar{k}$ and (P, Q) is an $\mathbb{F}_p$-basis of $E[p]$. The group $\mathrm{GL}_2(\mathbb{F}_p)$ acts on a pair on the right as usual $\big(E, (P, Q)\big) \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \big(E, (aP+cQ, bP+dQ)\big)$. A point in $Y_{\mathcal{H}}(\bar{k})$ is an orbit under this action by the non-split Cartan subgroup $\mathcal{H}$. For a given elliptic curve $E/\bar{k}$, the $\mathcal{H}$-orbits of triples is a $\mathcal{G}$-set isomorphic to $\mathcal{G}/\mathcal{H}$. Corollary 3 has shown us that the set of oriented necklaces on E is also isomorphic to $\mathcal{G}/\mathcal{H}$. Hence we have:

Proposition 4. *Let $\mathcal{H}$ be a non-split Cartan subgroup in $\mathrm{GL}_2(\mathbb{F}_p)$. There is a bijection between the points in $Y_{\mathcal{H}}(\bar{k})$ and the set of $\bar{k}$-isomorphism classes of pairs $(E, \mathfrak{v})$ composed of an elliptic curve $E/\bar{k}$ together with an oriented necklace $\mathfrak{v}$ in E. Similarly $Y_{\mathcal{N}}(\bar{k})$ consists of pairs $(E, \mathfrak{v})$ where $\mathfrak{v}$ is a necklace in E.*

We will from now on informally say that Y_{nsp}^+ and Y_{nsp} are coarse moduli spaces for the moduli problem of elliptic curves endowed with a necklace and an oriented necklaces respectively. In order to make this absolutely precise, we would have to define necklaces for elliptic curves over arbitrary schemes and that is very cumbersome to do. There is a similar problem for the split Cartan subgroup, too. However, later in Section 3.3, we give the description of k-rational points for fields k which are not algebraically closed.

2.4 The cross-ratio

Let A, B, C be three distinct points in $\mathbb{P}\big(E[p]\big)$ and $D \in \mathbb{P}\big(E[p]\big)$. Recall that the cross-ratio of A, B, C, D is defined by $[A, B; C, D] = f(D)$ where $f : \mathbb{P}\big(E[p]\big) \longrightarrow \mathbb{P}^1(\mathbb{F}_p)$ is the unique isomorphism such that $f(A) = (1 : 0)$, $f(B) = (0 : 1)$ and $f(C) = (1 : 1)$. After a choice of basis of $E[p]$ identifying $\mathbb{P}\big(E[p]\big)$ with $\mathbb{P}^1(\mathbb{F}_p)$, we get

$$[A, B; C, D] = \frac{A - C}{B - C} \cdot \frac{B - D}{A - D}.$$

The choice of basis does not matter as the cross-ratio is $\mathrm{PGL}\big(E[p]\big)$-invariant. If $\mathfrak{v} = (C_0, C_1, \dots, C_p)$ is an oriented necklace, then $[C_0, C_1; C_2, C_3] = [C_i, C_{i+1}; C_{i+2}, C_{i+3}]$ for all $0 \leqslant i \leqslant p$ with the index taken modulo $p+1$. Hence we can attach a cross-ratio to each necklace. As described above, the action of $\mathrm{PGL}\big(E[p]\big)$ on oriented necklaces is transitive and hence this cross-ratio $[C_0, C_1; C_2, C_3]$ is the same for all oriented γ-necklaces.

Proposition 5. *Let γ be a generator of $\mathbb{F}_{p^2}^\times$ of trace t and norm n. Set $\xi_\gamma = t^2/(t^2-n)$. Then a list $(C_0, C_1, \dots, C_p)$ of all distinct cyclic subgroups of order p in E represents a γ-necklace if and only if $[C_i, C_{i+1}; C_{i+2}, C_{i+3}] = \xi_\gamma$ for all $0 \leqslant i \leqslant p$ with the index taken modulo $p+1$.*

This provides a new possibility of defining necklaces by-passing completely the use of the automorphism group of $E[p]$, but only relying on the projective geometry of $\mathbb{P}(E[p])$.

Proof. We only need to compute the cross-ratio for one necklace. We take the basis such that $h = \left[\begin{smallmatrix} 0 & -n \\ 1 & t \end{smallmatrix}\right]$ is in $\mathcal{C}_\gamma$. The necklace now contains the consecutive pearls $(1:0)$, $(0:1)$, $(-n:t)$ and $(-nt:-n+t^2)$ from which we obtain the above cross-ratio ξ_γ. □

Since to each triple (C_0, C_1, C_2) there is a unique C_3 such that $[C_0, C_1; C_2, C_3] = \xi_\gamma$, we have a second proof of Lemma 2.

2.5 Relation to other descriptions

We recall a different description of the $\mathcal{H}_\alpha$-orbits of points in $X(p)$ where α is a choice in $\mathbb{F}_{p^2} \setminus \mathbb{F}_p$. See [Mer99]. Let $E/\bar{k}$ be an elliptic curve. Choose a basis P_0, P_1 of $E[p]$ and identify $E[p]$ with $\mathbb{F}_{p^2}$ via $P_0 \mapsto 1$ and $P_1 \mapsto \alpha$. Any basis (P, Q) of $E[p]$ is equal to $(P_0, P_1)g$ for some $g \in \mathrm{GL}_2(\mathbb{F}_p)$. Consider the $\mathrm{GL}_2(\mathbb{F}_p)$-equivariant map which sends (P_0, P_1) to $(1:\alpha) \in \mathbb{P}^1(\mathbb{F}_{p^2}) \setminus \mathbb{P}^1(\mathbb{F}_p)$. Since the action of $\mathcal{H}_\alpha$ is now just the multiplication on $\mathbb{F}_{p^2}$, it induces a well defined $\mathrm{GL}_2(\mathbb{F}_p)$-equivariant map from the set of $\mathcal{H}_\alpha$-orbits of basis (P, Q) to $\mathbb{P}^1(\mathbb{F}_{p^2}) \setminus \mathbb{P}^1(\mathbb{F}_p)$. This is a $\mathrm{GL}_2(\mathbb{F}_p)$-equivariant bijection.

This leads now to a moduli problem description of X_{nsp}. Each point in $Y_{\mathrm{nsp}}(\bar{k})$ with $\bar{k}$ an algebraically closed field of characteristic different from p is a $\bar{k}$-isomorphism class of $(E, \mathfrak{C})$ where $E/\bar{k}$ is an elliptic curve and $\mathfrak{C}$ is an element in $\mathbb{P}\big(E[p] \otimes \mathbb{F}_{p^2}\big) \setminus \mathbb{P}\big(E[p]\big)$. The group $\mathrm{PGL}\big(E[p]\big)$ acts on the left on $\mathbb{P}\big(E[p] \otimes \mathbb{F}_{p^2}\big)$ by its action on $E[p]$.

We will now give an explicit $\mathrm{PGL}\big(E[p]\big)$-equivariant bijection between the set of oriented γ-necklaces of E and $\mathbb{P}\big(E[p] \otimes \mathbb{F}_{p^2}\big) \setminus \mathbb{P}\big(E[p]\big)$. Write n and t for the norm and trace of the fixed element γ in $\mathbb{F}_{p^2}$. Consider the map

$$\begin{array}{ccc} \{\gamma\text{-necklaces}\} & \longrightarrow & \mathbb{P}\big(E[p] \otimes \mathbb{F}_{p^2}\big) \\ (C_0, C_1, C_2, \dots) & \mapsto & \langle P \otimes (-\gamma) + Q \otimes 1 \rangle \end{array} \tag{1}$$

where (P, Q) is a basis of $E[p]$ such that $C_0 = \langle P \rangle$, $C_1 = \langle Q \rangle$ and $C_2 = \langle -nP + tQ \rangle$. Note that such a basis exists because neither n nor t could be zero when γ is a multiplicative generator of $\mathbb{F}_{p^2}$. We have to show that this map is well-defined. Let h be a generator in the stabiliser of $\mathfrak{v}$ which belongs to $\mathcal{C}_\gamma$. In the basis (P, Q) this element h is represented by the matrix $\left[\begin{smallmatrix} 0 & -n \\ 1 & t \end{smallmatrix}\right]$. Now

$$h\Big(P \otimes (-\gamma) + Q \otimes 1\Big) = Q \otimes (-\gamma) + (-nP + tQ) \otimes 1 = (t - \gamma) \cdot \Big(P \otimes (-\gamma) + Q \otimes 1\Big)$$

as $(t-\gamma)(-\gamma) = \gamma^2 - t\gamma = -n$. This shows that the line in $\mathbb{P}\big(E[p] \otimes \mathbb{F}_{p^2}\big)$ does not depend on the choices made in the construction. It also is evident from this that the stabiliser of $\mathfrak{v}$ is equal to the stabiliser of the image. From the construction we see that the map is $\mathrm{PGL}\big(E[p]\big)$-equivariant. Since the actions are transitive, it follows that it is surjective and hence bijective.

Since we have no geometric object linked to E which can be thought of directly as an element in $E[p] \otimes \mathbb{F}_{p^2}$, we believe that the moduli problem of necklaces has its advantages.

While finalising this article, we learnt of yet another moduli interpretation given by Kohen and Pacetti in [KP14]: Fix a choice of a quadratic non-residue ε modulo p. They represent each point in $Y^+_{\mathrm{nsp}}(\bar{k})$ by a $\bar{k}$-isomorphism class of (E, ϕ) where $E/\bar{k}$ is an elliptic curve and $\phi \in \mathrm{GL}\big(E[p]\big)$ is an element such that ϕ^2 is the multiplication by ε. See Proposition 1.1 and Remark 1.3 in [KP14]. The following defines a

$\mathrm{PGL}\big(E[p]\big)$-equivariant bijection between the set of such endomorphisms ϕ and the set of necklaces on E. The endomorphism ϕ defines an element of order two in $\mathrm{PGL}\big(E[p]\big)$ without fixed point; so it belongs to a unique non-split Cartan subgroup $\mathcal{H}$ whose normaliser is the stabiliser of a necklace $\mathfrak{v}$. Conversely, every stabiliser of a necklace contains a unique element in $\mathrm{PGL}\big(E[p]\big)$ that lifts to an element $\phi \in \mathrm{GL}\big(E[p]\big)$ with $\phi^2 = \varepsilon$.

3 Describing the geometry and arithmetic with necklaces

3.1 Degeneracy maps

Let $\mathcal{A}$ be the group of scalars in $\mathrm{GL}_2(\mathbb{F}_p)$ and consider the associated modular curve $X_{\mathcal{A}}$. Because the group $\mathrm{PGL}_2(\mathbb{F}_p)$ acts sharply 3-transitive on $\mathbb{P}^1(\mathbb{F}_p)$, the curve $X_{\mathcal{A}}$ represents the moduli problem associating to each elliptic curve E a triple of distinct cyclic subgroups (C_0, C_1, C_2) of order p in E, which is also called a projective frame in $\mathbb{P}(E[p])$.

The map $\pi_{\mathcal{A}} \colon X(p) \to X_{\mathcal{A}}$ can be chosen to be the following. Let n and t be the norm and trace of our fixed generator γ in $\mathbb{F}_{p^2}$. To each basis (P, Q) of the p-torsion of an elliptic curve E, we associate the triple $\big(\langle P\rangle, \langle Q\rangle, \langle -n\,P + t\,Q\rangle\big)$. From the fact that $t \neq 0$, it is clear that this gives a map $X(p) \to X_{\mathcal{A}}$. Next we describe the map $\pi_{\mathrm{nsp}} \colon X_{\mathcal{A}} \to X_{\mathrm{nsp}}$. We have a natural choice to send the triple (C_0, C_1, C_2) to the unique oriented necklace $C_0 \to C_1 \to C_2$ given by Lemma 2. Similarly, we will send it to the necklace $C_0 - C_1 - C_2$ to define the map $\pi^+_{\mathrm{nsp}} \colon X_{\mathcal{A}} \to X^+_{\mathrm{nsp}}$.

The advantage of our choices is that $\pi_{\mathrm{nsp}} \circ \pi_{\mathcal{A}}$ provides an explicit bijection between the set of orbits of isomorphism classes $(E, (P, Q))$ under a particular non-split Cartan subgroup $\mathcal{H}_0$ and the set of isomorphism classes $(E, \mathfrak{v})$ of elliptic curves endowed with an oriented necklace. Let $\mathcal{H}_0$ be the non-split Cartan subgroup in $\mathrm{GL}_2(\mathbb{F}_p)$ generated by the matrix $h_0 = \left(\begin{smallmatrix} 0 & -n \\ 1 & t \end{smallmatrix}\right) = i_\gamma(\gamma)$, which is an element in our chosen class $\mathcal{C}_\gamma$ for $V = \mathbb{F}_p^2$. Let E be an elliptic curve and (P, Q) a basis of $E[p]$. Denote by $h \in \mathrm{PGL}(E[p])$ the element of order $p+1$ defining the necklace $\mathfrak{v} = \pi_{\mathrm{nsp}} \circ \pi_{\mathcal{A}}(P, Q)$. Then, by construction of $\pi_{\mathcal{A}}$,

$$\pi_{\mathcal{A}}\big((P, Q) \cdot h_0\big) = h \cdot \pi_{\mathcal{A}}(P, Q).$$

This insures that the map which sends an orbit $(E, (P, Q))\,\mathcal{H}_0$ to $(E, \mathfrak{v})$ where $\mathfrak{v} = \pi_{\mathrm{nsp}} \circ \pi_{\mathcal{A}}(P, Q)$ is well defined and it gives the expected bijection.

Under the map (1) in Section 2.5, identifying necklaces with elements in $\mathbb{P}\big(E[p] \otimes \mathbb{F}_{p^2}\big) \setminus \mathbb{P}\big(E[p]\big)$, the degeneracy map above can also be described as sending the basis (P, Q) of $E[p]$ to the projective line $\langle P \otimes (-\gamma) + Q \otimes 1\rangle$ in $E[p] \otimes \mathbb{F}_{p^2}$. This provides an explicit bijection between the set of orbits of isomorphism classes $(E, (P, Q))$ under $\mathcal{H}_0$ and the set of isomorphism classes $(E, \mathfrak{C})$ of elliptic curves endowed with an element $\mathfrak{C}$ in $\mathbb{P}\big(E[p] \otimes \mathbb{F}_{p^2}\big) \setminus \mathbb{P}\big(E[p]\big)$.

We will see later in Section 4.7 another naturally defined degeneracy map $\tilde{\pi}^+_{\mathrm{nsp}} \colon X_{\mathcal{A}} \to X^+_{\mathrm{nsp}}$.

3.2 Cusps

The following proposition, quoted (but not proved) in [Ser97] Appendix A.5, can be proved using necklaces:

Proposition 6. *The modular curve X_{nsp} has $p-1$ cusps, each ramified of degree p over the cusp ∞ in $X(1)$.*

Proof. In order to determine the structure of the cusps, we use the Tate curve E_q over $\mathbb{Q}(\!(q)\!)$. Formally, one can deduce the proposition using Theorem 10.9.1 in [KM85] from the fact that a non-split Cartan subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$ acts transitively on $\mathbb{P}^1(\mathbb{F}_p)$ and that it contains no non-trivial element from any Borel subgroup. In particular, the formal completion of X_{nsp} along the cusps is the formal spectrum of $\mathbb{Q}(\zeta)[\![\alpha]\!]$, where $\alpha^p = q$ and ζ is a p-th root of unity.

However, we can also view it on the necklaces of E_q. The Tate curve has a distinguished cyclic subgroup μ_p of order p. Any oriented necklace $\mathfrak{v}$ can be turned in such a way that $C_0 = \mu_p$. The two following pearls C_1 and C_2 have each a generator which is a p-th root of q, say $\alpha\zeta^i$ and $\alpha\zeta^j$, respectively,

where $0 \leqslant i \neq j < p$. From the action of the inertia group of the extension $\mathbb{Q}(\!(q)\!)[\alpha, \zeta]$ over $\mathbb{Q}(\!(q)\!)$, we see that all the p necklaces with a given $i - j \in \mathbb{F}_p^\times$ meet at the same cusp in the special fibre at (q). □

The cusps are not defined over $\mathbb{Q}$ but over the cyclotomic field $\mathbb{Q}(\mu_p)$ only, forming one orbit under the action of the Galois group, despite the fact that X_{nsp} is defined over $\mathbb{Q}$. See Appendix A.5 in [Ser97]. As a consequence there are $p-1$ choices of embeddings $X_{\mathrm{nsp}} \hookrightarrow \mathrm{Jac}(X_{\mathrm{nsp}})$, all defined over $\mathbb{Q}(\mu_p)$ only and none of them is a canonical choice.

With the same proof we show that X_{nsp}^+ has $(p-1)/2$ cusps defined over the maximal real subfield of $\mathbb{Q}(\mu_p)$.

3.3 Galois action

Let k be a field of characteristic different from p and write G_k for its absolute Galois group. For any σ in G_k and point $x \in Y_{\mathrm{nsp}}(\bar{k})$, represented by the pair $(E, \mathfrak{v})$, we define $\sigma(x)$ in the obvious way as the $\bar{k}$-isomorphism class of the pair $\big(E^\sigma, \sigma(\mathfrak{v})\big)$. Here $\sigma\big((C_0, C_1, \dots)\big)$ is the necklace $\big(\sigma(C_0), \sigma(C_1), \dots\big)$. Write $Y_{\mathrm{nsp}}(k)$ for the elements in $Y_{\mathrm{nsp}}(\bar{k})$ fixed by G_k.

Proposition 7. *Let $x \in Y_{\mathrm{nsp}}(k)$. Then there exists a pair $(E, \mathfrak{v})$ representing x such that E is defined over k. If $j(E) \notin \{0, 1728\}$ then the oriented necklace $\mathfrak{v}$ is also defined over k, in the sense that $\sigma(\mathfrak{v}) = \mathfrak{v}$ for all $\sigma \in G_k$. In particular, the image of the residual Galois representation $\bar{\rho}_p(E)\colon G_k \to \mathrm{GL}\big(E[p]\big)$ has its image in a non-split Cartan subgroup.*

Proof. Let $(E, \mathfrak{v})$ be a representation of x. So E^σ is $\bar{k}$-isomorphic to E. As usual $\sigma\big(j(E)\big) = j(E^\sigma) = j(E)$, shows that $j(E) \in k$ and hence we may assume that E is defined over k.

For every $\sigma \in G_k$ there is an automorphism $\Psi_\sigma \in \mathrm{Aut}_{\bar{k}}(E)$ such that $\Psi_\sigma(\mathfrak{v}) = \sigma(\mathfrak{v})$. If $j(E) \notin \{0, 1728\}$ then there are no additional automorphisms besides $[\pm 1]$. Therefore they all act by scalars on $E[p]$ and thus they act trivially on $\mathbb{P}\big(E[p]\big)$. It follows that $\mathfrak{v} = \sigma(\mathfrak{v})$. So the image of $\bar{\rho}_p(E)$ lands in the stabiliser of $\mathfrak{v}$, which is a non-split Cartan subgroup. □

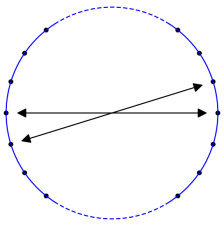
If $\mathfrak{v}$ is defined over k then there exists a cyclic extension L/k of degree dividing $p+1$ such that all cyclic subgroups C of $E[p]$ are defined over L.

The analogous statement holds for $Y_{\mathrm{nsp}}^+(k)$: Every point in $Y_{\mathrm{nsp}}^+(k)$ can be represented by a pair $(E, \mathfrak{v})$ with E being defined over k. If $j(E) \notin \{0, 1728\}$, then the necklace $\mathfrak{v}$ has also to be defined over k and the residual Galois representation takes values in the normaliser of a non-split Cartan subgroup of $\mathrm{GL}\big(E[p]\big)$.

The fibres in Y_{nsp} and Y_{nsp}^+ above the points $j = 0$ or $j = 1728$, contain ramified points and elliptic points. We will discuss these later in detail in Section 3.5. A ramified point x in one of those fibres can still be represented by $(E, \mathfrak{v})$ with E defined over $\mathbb{Q}$. However we will show now that the field of definition of x is not equal to the field of definition of $\mathfrak{v}$ if $p > 3$: In both cases, the curve E has complex multiplication and by a general result (see Corollary 5.20 in Rubin's part in [CGRR99]), the image of the Galois representation $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}\big(E[p]\big)$ contains the image of all the automorphisms of E. Since x is ramified, there is an automorphism g such that $g(\mathfrak{v}) \neq \mathfrak{v}$. Hence there is an element $\sigma \in G_{\mathbb{Q}}$ that sends $\mathfrak{v}$ to $g(\mathfrak{v})$. Now σ does not fix $\mathfrak{v}$, but it fixes x, which is also represented by $\big(E, g(\mathfrak{v})\big)$.

3.4 A lemma on antipodal pearls and cross-ratios

Let E an elliptic curve over an algebraically closed field $\bar{k}$ of characteristic different from p. The following definition and lemma will be used in many places later on.



Definition. Let $\mathfrak{v} = (C_0, C_1, \dots, C_p)$ be a necklace in E. Two pearls C_i and C_j are called *antipodal in* $\mathfrak{v}$ if $i \equiv j + \frac{p+1}{2} \pmod{p+1}$. In other words if they are diametrically opposed when we represent the necklace as a regular $(p+1)$-gon. If A and B are antipodal in $\mathfrak{v}$, we write $A \leftrightarrow B \in \mathfrak{v}$.

Lemma 8. *Let A, B, C, D be four distinct cyclic subgroups of order p in an elliptic curve E. There are $(p-1)/2$ necklaces in which $A \leftrightarrow B$. If the cross-ratio $[A,B;C,D]$ is a square in $\mathbb{F}_p^\times$, then there is no necklace $\mathfrak{v}$ such that $A \leftrightarrow B \in \mathfrak{v}$ and $C \leftrightarrow D \in \mathfrak{v}$. If instead $[A,B;C,D]$ is a non-square in $\mathbb{F}_p^\times$, then there is exactly one necklace $\mathfrak{v}$ such that $A \leftrightarrow B \in \mathfrak{v}$ and $C \leftrightarrow D \in \mathfrak{v}$.*

Proof. We may choose a basis of $E[p]$ in such a way that $A = (1:0)$, $B = (0:1)$ and $C = (1:1)$. Then $D = (d:1)$ for some $d \in \mathbb{F}_p^\times \setminus \{1\}$. Now $[A,B;C,D] = d$.

If d is a non-square, then the matrix $g = \left[\begin{smallmatrix} 0 & d \\ 1 & 0 \end{smallmatrix}\right]$ is an element of order two without a fixed point in $\mathbb{P}^1(\mathbb{F}_p)$. Hence it belongs to a unique non-split Cartan subgroup $\mathcal{H}$. Then the necklace $\mathfrak{v}$ whose stabiliser is the normaliser of $\mathcal{H}$ is a necklace such that $A \leftrightarrow B \in \mathfrak{v}$ and $C \leftrightarrow D \in \mathfrak{v}$ as $g(A) = B$ and $g(C) = D$.

Conversely, if we have such a necklace $\mathfrak{v}$ for A, B, C, D, then the unique element of order 2 which preserves the orientation on $\mathfrak{v}$, must send A to B and C to D. Hence it is of the form $g = \left[\begin{smallmatrix} 0 & d \\ 1 & 0 \end{smallmatrix}\right]$. However if it has no fixed points in $\mathbb{P}^1(\mathbb{F}_p)$, then d has to be a non-square in $\mathbb{F}_p^\times$.

Finally, we have to count how many necklaces have $A \leftrightarrow B \in \mathfrak{v}$. By the above proof, this is the same as to count how many matrices $g = \left[\begin{smallmatrix} 0 & d \\ 1 & 0 \end{smallmatrix}\right]$ belong to a non-split Cartan subgroup. That is $\frac{p-1}{2}$ as there are that many non-squares d in $\mathbb{F}_p^\times$. □

3.5 Elliptic points

We proceed to count elliptic points using our moduli description. Our results in Propositions 9 and 12 below agree with the more general calculations by Baran in Proposition 7.10 in [Bar10]. Assume for this that $p > 3$.

Consider the canonical coverings $X_{\mathrm{nsp}} \longrightarrow X(1)$ and $X^+_{\mathrm{nsp}} \longrightarrow X(1)$. An *elliptic point* on X_{nsp} or X^+_{nsp} is a point in the fibre of a point in $X(1)$ represented by an elliptic curve E with $\mathrm{Aut}(E) \neq \{\pm 1\}$. Hence, an elliptic point on X_{nsp} can be represented by a pair $(E, \mathfrak{v})$ such that there is an automorphism on E that induces a non-trivial element $g \in \mathrm{PGL}\big(E[p]\big)$ which fixes $\mathfrak{v}$. Consider the involution w on X_{nsp} which reverses the orientation of the oriented necklaces. An elliptic point on X^+_{nsp} can be viewed as a pair $(E, \{\mathfrak{v}, w\mathfrak{v}\})$ with an automorphism $g \in \mathrm{PGL}\big(E[p]\big)$ and an oriented necklace $\mathfrak{v}$ such that either $g(\mathfrak{v}) = \mathfrak{v}$ or $g(\mathfrak{v}) = w(\mathfrak{v})$. In the latter case, we say that $\mathfrak{v}$ and its necklace $\{\mathfrak{v}, w(\mathfrak{v})\}$ is *flipped* by g.

First note that if $(E, \cdot)$ is a elliptic point then $j(E) = 1728$ and g is of order two or $j(E) = 0$ and g is of order three. These are elliptic curves with complex multiplication and $E[p]$ becomes a free $\mathrm{End}(E)/p$-module of rank 1. So if g is of order 2 and $p \equiv 3 \pmod 4$ or if g is of order 3 and $p \equiv 2 \pmod 3$, then $\mathrm{End}(E)/p \cong \mathbb{F}_{p^2}$ and hence g belongs to a unique non-split Cartan subgroup of $\mathrm{PGL}\big(E[p]\big)$. Instead, if g is of order 2 and $p \equiv 1 \pmod 4$ or if g is of order 3 and $p \equiv 1 \pmod 3$ then $\mathrm{End}(E)/p \cong \mathbb{F}_p \oplus \mathbb{F}_p$ and therefore g belongs to a unique split Cartan subgroup as it will have exactly two fixed points.

3.5.1 Fixed oriented necklaces

Let $(E, \mathfrak{v})$ be an elliptic point on X_{nsp} with the oriented necklace $\mathfrak{v}$ fixed by g. Then g is in the non-split Cartan subgroup stabilising $\mathfrak{v}$. Hence by the above, $p \equiv 3 \pmod 4$ if g has order 2 and $p \equiv 2 \pmod 3$ if g has order 3. Conversely, if these congruence conditions are satisfied then g is in a unique non-split Cartan subgroup which is the stabiliser of exactly two oriented necklaces, namely $\mathfrak{v}$ and $w\mathfrak{v}$. This gives the following result:

Proposition 9. *For $r = 2$ and 3, let e_r be the number of elliptic points in X_{nsp} with g of order r. Then*

$$e_2 = 1 - \left(\frac{-1}{p}\right) = \begin{cases} 0 & \text{if } p \equiv 1 \pmod 4, \\ 2 & \text{if } p \equiv 3 \pmod 4, \end{cases} \quad \text{and} \quad e_3 = 1 - \left(\frac{-3}{p}\right) = \begin{cases} 0 & \text{if } p \equiv 1 \pmod 3, \\ 2 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

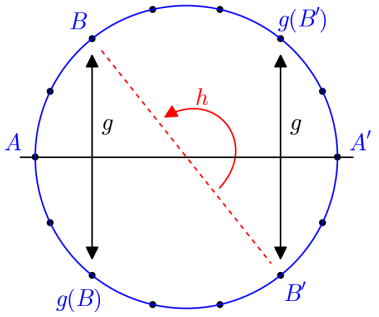
In the cases where $e_r = 2$ the two corresponding oriented necklaces are in the same w-orbit.

3.5.2 Flipped necklaces

Let $(E, \mathfrak{v})$ be an elliptic point on X_{nsp}^+ where the necklace $\mathfrak{v} = \{\vec{\mathfrak{v}}, w\vec{\mathfrak{v}}\}$ is flipped by g. If g were of order 3, we would have $\vec{\mathfrak{v}} = g^3(\vec{\mathfrak{v}}) = w(\vec{\mathfrak{v}})$. Hence g is of order 2. The involution g is in a split Cartan subgroup if $p \equiv 1 \pmod 4$ and in a non-split Cartan subgroup if $p \equiv 3 \pmod 4$.

Lemma 10. *Suppose that $p \equiv 1 \pmod 4$ and let A, A' denote the two fixed points of g in $\mathbb{P}(E[p])$. A necklace $\mathfrak{v}$ is flipped by g if and only if A and A' are antipodal in $\mathfrak{v}$. Consequently, there are $\frac{p-1}{2}$ necklaces flipped by g.*

Proof. Let $\vec{\mathfrak{v}} = (C_0, C_1, C_2, \ldots, C_p)$ be a flipped oriented necklace with $C_0 = A$. From $g(\vec{\mathfrak{v}}) = w(\vec{\mathfrak{v}})$, we get $g(C_k) = C_{p+1-k}$ for all k, where the indices are taken modulo $p+1$. It follows that if $A' = C_k$ then $A' = g(A') = C_{p+1-k}$, so $k = (p+1)/2$ and A and A' are antipodals in $\mathfrak{v} = \{\vec{\mathfrak{v}}, w\vec{\mathfrak{v}}\}$. Moreover from $g(C_k) = C_{p+1-k}$, we see that g will act on $\mathfrak{v}$, represented as a regular $(p+1)$-gon, as the reflection through the axis passing through A and A'.



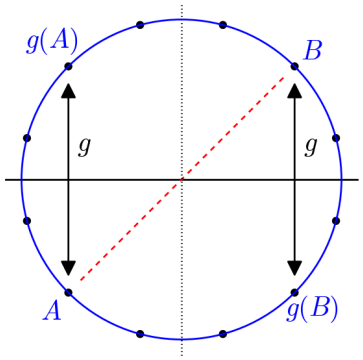
Conversely, let $\mathfrak{v}$ be a necklace in which $A \leftrightarrow A'$. Let $B \leftrightarrow B'$ be two other antipodal pearls in $\mathfrak{v}$. Let h be the element of order 2 in the normaliser of the non-split Cartan subgroup stabilising $\mathfrak{v}$. As it exchanges antipodal pairs in $\mathfrak{v}$, we have $h(A) = A'$ and $h(B) = B'$. Since hgh^{-1} is also an involution that fixes A and A', it follows that $hgh^{-1} = g$ as there is a unique involution fixing two given points. Therefore $hg(B) = gh(B) = g(B')$ which implies that $g(B) \leftrightarrow g(B') \in \mathfrak{v}$.

As g sends antipodal pairs in $\mathfrak{v}$ to antipodal pairs in $g(\mathfrak{v})$, we also have $A \leftrightarrow A'$ and $g(B) \leftrightarrow g(B')$ in $g(\mathfrak{v})$. Hence, by Lemma 8, either $g(\vec{\mathfrak{v}}) = \vec{\mathfrak{v}}$ or $g(\vec{\mathfrak{v}}) = w\vec{\mathfrak{v}}$ where $\{\vec{\mathfrak{v}}, w\vec{\mathfrak{v}}\} = \mathfrak{v}$. The first case is excluded because g does not belong to a non-split Cartan subgroup if $p \equiv 1 \pmod 4$.

The end of the proof follows from the fact that there are $(p-1)/2$ necklaces such that A and A' are antipodal, again by Lemma 8. □

Lemma 11. *Suppose that $p \equiv 3 \pmod 4$. Let $A \in \mathbb{P}\big(E[p]\big)$. Consider the map sending a necklace $\mathfrak{v}$ to the pearl antipodal to A in $\mathfrak{v}$. This is a bijection between necklaces $\mathfrak{v}$ flipped by g and the set of pearls $B \notin \{A, g(A)\}$ such that $\big[A, B; g(A), g(B)\big]$ is a non-square in $\mathbb{F}_p$.*

Proof. Let $\mathfrak{v}$ be a necklace flipped by g. As above, from $g(\vec{\mathfrak{v}}) = w(\vec{\mathfrak{v}})$ we get $g(C_k) = C_{p+1-k}$ for all k and one can see that, since $p \equiv 3 \pmod 4$, g will act on $\mathfrak{v}$ as a reflection through an axis that does not pass through a corner of the regular $(p+1)$-gon. Let B be antipodal to A in $\mathfrak{v}$. So $B \neq A$. If B were equal to $g(A)$, then A and B would be on the line orthogonal to the axis of reflection of g. But this would imply that $p+1 \equiv 2 \pmod 4$, and hence $B \neq g(A)$. Finally, since g flips $\mathfrak{v}$, we see that $g(A) \leftrightarrow g(B) \in \mathfrak{v}$. By Lemma 8, it follows that $\big[A, B; g(A), g(B)\big]$ is a non-square modulo p. The same lemma also shows that our map $\mathfrak{v} \mapsto B$ is injective.



Conversely, suppose that $B \notin \{A, g(A)\}$ is such that the cross-ratio $\big[A, B; g(A), g(B)\big]$ is a non-square modulo p. Since A, B, $g(A)$ and $g(B)$ are all distinct, Lemma 8 applies to show that there is a necklace $\mathfrak{v}$ with $A \leftrightarrow B$ and $g(A) \leftrightarrow g(B)$. Now $g(\mathfrak{v})$ has also $g(A) \leftrightarrow g(B)$ and $A \leftrightarrow B$. The same lemma now shows that $g(\mathfrak{v}) = \mathfrak{v}$. If the orientation of $\mathfrak{v}$ were fixed rather than flipped, then $g(A)$ would be B. Hence our map is surjective, too. □

Proposition 12. *For $r = 2$ or 3, let e_r^+ be the number of elliptic points with g of order r in X_{nsp}^+. Then*

$$e_2^+ = \frac{p+1}{2} - \left(\frac{-1}{p}\right) = \begin{cases} \frac{p-1}{2} & \text{if } p \equiv 1 \pmod 4, \\ \frac{p+3}{2} & \text{if } p \equiv 3 \pmod 4, \end{cases}$$

and

$$e_3^+ = \frac{1}{2} - \frac{1}{2}\left(\frac{-3}{p}\right) = \begin{cases} 0 & \text{if } p \equiv 1 \pmod 3, \\ 1 & \text{if } p \equiv 2 \pmod 3. \end{cases}$$

Proof. The number of elliptic points for X_{nsp}^+ is the sum of the number of fixed and the number of flipped necklaces. In Proposition 9 we counted the fixed ones. We have already counted the flipped necklaces for $p \equiv 1 \pmod 4$ in Lemma 10. Now suppose $p \equiv 3 \pmod 4$ and let $A \in \mathbb{P}\big(E[p]\big)$. By Lemma 11, we must count how many pearls B there are such that $B \notin \{A, g(A)\}$ and $\big[A, B; g(A), g(B)\big]$ is a non-square in $\mathbb{F}_p$.

Let us choose a basis of $E[p]$ such that $A = (1:0)$ and $g(A) = (0:1)$. Let $b \in \mathbb{F}_p^\times$ such that $B = (1:b)$. Then $g = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$ and $g(B) = (-b:1)$. Hence $\big[A, B; g(A), g(B)\big] = 1 + b^2$. So we have to count the number of $b \in \mathbb{F}_p^\times$ such that $1 + b^2$ is a non-square. One finds that there are $\frac{p+1}{2}$ such b by counting the cases when $1 + b^2$ is a square using that there are $p + 1$ points on a projective conic $a^2 + b^2 = c^2$. □

3.6 Genus

From the above, we can now proceed to compute the genus of our modular curves. Of course, we find the well-known formulae, as for instance in Appendix A.5 to [Ser97], [Bar10] or [Che98]. The reader can also find tables for the genus of X_{nsp} and X_{nsp}^+ for small primes p in [Bar10].

The Riemann-Hurwitz formula applied to the modular curve $X_{\mathcal{H}}$ associated to a subgroup of finite index $\mathcal{H}$ of $\mathrm{GL}_2(\mathbb{F}_p)$ and with the canonical morphism $X_{\mathcal{H}} \to X(1)$ of degree d, gives the following formula for the genus $g(X_{\mathcal{H}})$ of $X_{\mathcal{H}}$:

$$g(X_{\mathcal{H}}) = 1 + \frac{d}{12} - \frac{e_2}{4} - \frac{e_3}{3} - \frac{e_\infty}{2}$$

where e_r is the number of elliptic points in X_H of order r and e_∞ is the number of cusps.

With the results of Sections 3.5 and 3.2, a straightforward computation gives the following.

Proposition 13. *The genera of X_{nsp} and X_{nsp}^+ are*

$$g(X_{\mathrm{nsp}}) = \frac{1}{12}\left(p^2 - 7p + 11 + 3\left(\frac{-1}{p}\right) + 4\left(\frac{-3}{p}\right)\right)$$

and

$$g(X_{\mathrm{nsp}}^+) = \frac{1}{24}\left(p^2 - 10p + 23 + 6\left(\frac{-1}{p}\right) + 4\left(\frac{-3}{p}\right)\right).$$

With the same method, one can compute the genus of other modular curves, for instance X_0 and X_{sp}^+. The classical results (see for instance [Shi94] and [Che98]) for their genus are

$$g\big(X_{\mathrm{sp}}^+\big) = \frac{1}{24}\left(p^2 - 8p + 11 - 4\left(\frac{-3}{p}\right)\right) \quad \text{and} \quad g\big(X_0\big) = \frac{1}{12}\left(p - 6 - 3\left(\frac{-1}{p}\right) - 4\left(\frac{-3}{p}\right)\right).$$

Then one can verify easily the relation noticed by Birch following Chen's calculation of genus and confirmed by Chen's isogeny

$$g\big(X_{\mathrm{nsp}}^+\big) + g\big(X_0\big) = g\big(X_{\mathrm{sp}}^+\big). \tag{2}$$

3.7 Hecke operators

Let ℓ be any prime distinct from p. Denote by $X_{0,\mathrm{nsp}}^+(\ell, p) = X_0(\ell) \times_{X(1)} X_{\mathrm{nsp}}^+(p)$. We recall how the Hecke correspondence T_ℓ is defined through the following two natural degeneracy maps ρ and $\rho' \colon X_{0,\mathrm{nsp}}^+(\ell, p) \longrightarrow X_{\mathrm{nsp}}^+(p)$. The modular curve $X_{0,\mathrm{nsp}}^+(\ell, p)$ parametrises isomorphism classes $\big(E, (f, \mathfrak{v})\big)$ of elliptic curves E endowed with an ℓ-isogeny $f \colon E \to E'$ and a necklace $\mathfrak{v}$. Let ρ be the map obtained by forgetting the ℓ-structure and ρ' the map which sends $(E, (f, \mathfrak{v}))$ to $\big(E', f(\mathfrak{v})\big)$. The image $f(\mathfrak{v})$, defined as $\big(f(C_0), f(C_1), \ldots, f(C_p)\big)$ when $\mathfrak{v} = (C_0, \ldots, C_p)$, is indeed a necklace on $E' = f(E)$ since $\ell \neq p$.

The correspondence T_ℓ on X^+_{nsp} is now defined as $\rho^* \circ \rho'_*$. It induces an endomorphism on $\mathrm{Pic}(X^+_{\mathrm{nsp}})$ by Picard functoriality. On the divisor (z) with the point z in X^+_{nsp} represented by $(E, \mathfrak{v})$, it is defined as

$$T_\ell(z) = \sum_{\substack{f\colon E \to E' \\ \deg f = \ell}} \big(E', f(\mathfrak{v})\big)$$

where the sum runs over all isogenies f from E of degree ℓ.

We will now verify that this moduli-theoretic description of T_ℓ via these correspondences coincide with the Hecke operators defined by double coset.

Let us denote by $\mathcal{N}$ a normaliser of a non-split Cartan in $\mathrm{GL}_2(\mathbb{F}_p)$, by Γ the congruence subgroup of matrices in $\mathrm{SL}_2(\mathbb{Z})$ with image in $\mathcal{N}$ modulo p, and by Δ the set of integral matrices whose determinant is positive and coprime to p and which reduce to a matrix in $\mathcal{N}$ modulo p. Then T_ℓ as a double coset is defined by $\Gamma\alpha\Gamma$ for any $\alpha \in \Delta$ of determinant ℓ. Since such an element α reduces modulo ℓ to a non-zero matrix of determinant 0, there exist γ and γ' in Γ such that $\gamma\alpha\gamma'$ is of the form $\left(\begin{smallmatrix} a & b\ell \\ c\ell & d\ell \end{smallmatrix}\right)$ with integers a, b, c, and d. (Note that we can impose conditions modulo p on γ, γ' because p and ℓ are coprime.) In other words, $\Gamma\alpha\Gamma$ contains an element of the form $\beta \left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right)$ with $\beta \in \Gamma_0(\ell)$, so we may now suppose that $\alpha = \beta \left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right)$, with $\beta \in \Gamma_0(\ell)$.

We will then prove that $\Gamma \cap \alpha^{-1}\Gamma\alpha = \Gamma \cap \Gamma^0(\ell)$, where we denote by $\Gamma^0(\ell)$ the matrices in $\mathrm{SL}_2(\mathbb{Z})$ with right upper entry equal to 0 modulo ℓ: Since $\beta \in \mathrm{SL}_2(\mathbb{Z})$, we have $\beta^{-1}\Gamma\beta \subset \mathrm{SL}_2(\mathbb{Z})$, hence $\left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right)^{-1} \beta^{-1}\Gamma\beta \left(\begin{smallmatrix} 1 & 0 \\ 0 & \ell \end{smallmatrix}\right)$ are matrices of the form $\left(\begin{smallmatrix} a & b\ell \\ c/\ell & d \end{smallmatrix}\right)$ and this shows the first inclusion. Conversely, if $\gamma \in \Gamma \cap \Gamma^0(\ell)$, since α and γ belong to C modulo p, the product $\alpha\gamma\alpha^{-1}$ also belongs to it, so $\alpha\gamma\alpha^{-1} \in \Gamma$.

Similarly, one can show that $\Gamma \cap \alpha\Gamma\alpha^{-1} = \Gamma \cap \Gamma_0(\ell)$. Now, from the fact that $\Gamma \cap \alpha^{-1}\Gamma\alpha = \Gamma \cap \Gamma^0(\ell)$ or $\Gamma \cap \alpha\Gamma\alpha^{-1} = \Gamma \cap \Gamma_0(\ell)$, we deduce in a classical manner, as explained for instance in Section 6.3 in [DS05] taking $\Gamma_1 = \Gamma_2 = \Gamma$, that the double coset description of T_ℓ coincide with the moduli-theoretic description we gave above. Compare with Theorem 1.11 in [KP14] for a different proof.

3.8 A pairing

Given two necklaces $\mathfrak{v}$ and $\mathfrak{w}$ in E, we set

$$\langle \mathfrak{v}, \mathfrak{w} \rangle = \#\Big\{ \{A, B\} \;\Big|\; A \leftrightarrow B \in \mathfrak{v} \text{ and } A \leftrightarrow B \in \mathfrak{w} \Big\}.$$

It is the number of antipodal pearls that $\mathfrak{v}$ and $\mathfrak{w}$ have in common. We can extend it linearly to $\bigoplus_{\text{all } \mathfrak{v}} \mathbb{Z}\mathfrak{v}$ regarded as an abelian group with an action by $\mathrm{PGL}\big(E[p]\big)$.

Proposition 14. *The pairing $\langle \cdot, \cdot \rangle$ is a positive non-degenerate symmetric $\mathrm{PGL}\big(E[p]\big)$-equivariant bilinear form on $\bigoplus_{\mathfrak{v}} \mathbb{Z}\mathfrak{v}$. We have $\langle \mathfrak{v}, \mathfrak{v} \rangle = \frac{p+1}{2}$ and $\langle \mathfrak{v}, \mathfrak{w} \rangle \in \{0, 1\}$ for all necklaces $\mathfrak{v} \neq \mathfrak{w}$.*

First, we note that we are left to prove that the pairing is positive, takes value 0 or 1 on distinct necklaces, and is non-degenerate. In this section, we only give the proof of the two first facts. The proof of non-degeneracy will be given in Section 4.5 and numerical examples are in Section 5. We will see that this pairing gives a more conceptual understanding of the eigenvalues computed by Chen [Che00] in his table 2.

Proof. The statement that $\langle \mathfrak{v}, \mathfrak{w} \rangle \in \{0, 1\}$ for $\mathfrak{v} \neq \mathfrak{w}$ is a direct consequence of Lemma 8: If $\langle \mathfrak{v}, \mathfrak{w} \rangle \geqslant 2$, then there are four distinct A, B, C, D with both $A \leftrightarrow B$ and $C \leftrightarrow D$ in $\mathfrak{v}$ and $\mathfrak{w}$, contradicting the lemma.

Let $u = \sum a_{\mathfrak{v}}\, \mathfrak{v}$ be an element in $\bigoplus \mathbb{Z}\, \mathfrak{v}$. We have

$$\langle u, u \rangle = \sum_{\mathfrak{v}} \sum_{\mathfrak{w}} a_{\mathfrak{v}}\, a_{\mathfrak{w}}\, \langle \mathfrak{v}, \mathfrak{w} \rangle = \sum_{\{A,B\}} \sum_{\substack{\mathfrak{v} \text{ with} \\ A \leftrightarrow B \in \mathfrak{v}}} \sum_{\substack{\mathfrak{w} \text{ with} \\ A \leftrightarrow B \in \mathfrak{w}}} a_{\mathfrak{v}}\, a_{\mathfrak{w}} = \sum_{\{A,B\}} \Big(\sum_{\substack{\mathfrak{v} \text{ with} \\ A \leftrightarrow B \in \mathfrak{v}}} a_{\mathfrak{v}} \Big)^2 \geqslant 0,$$

where $\sum_{\{A,B\}}$ is the sum running over all unordered pairs of distinct cyclic subgroups of $E[p]$. Hence the pairing is positive. The non-degeneracy of the pairing will be shown in Section 4.5. □

4 Chen's isogeny

4.1 Definitions and statement

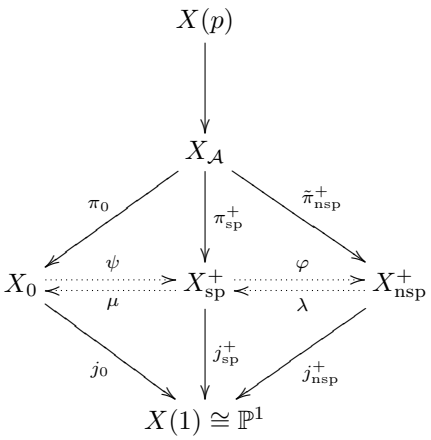
In [Che98], Chen proved that $\mathrm{Jac}(X^+_{\mathrm{nsp}}) = \mathrm{Jac}(X_0^+(p^2))^{\mathrm{new}}$. Edixhoven and de Smit [dSE00, Edi96] found a different and rather elegant proof. Finally Chen gave in [Che00] an explicit description of his morphism

$$\mathrm{Jac}(X^+_{\mathrm{sp}}) \to \mathrm{Jac}(X^+_{\mathrm{nsp}}) \times \mathrm{Jac}(X_0).$$

With our new moduli description this morphism can be described yet in another manner. Let $\bar{k}$ be an algebraically closed field of characteristic different from p. In Section 3.6, we have given the definitions of the modular curves X_0 and X^+_{sp}. The points in $X^+_{\mathrm{sp}}(\bar{k})$ can be represented as $\bar{k}$-isomorphism classes of the form $\big(E, \{A, B\}\big)$ where $\{A, B\}$ is a unordered pair of distinct cyclic subgroups of order p in E. Let $y = \big(E, \{A, B\}\big)$ be a point in X^+_{sp}. We define $\varphi(y)$ on the divisor (y) to be the sum of $(E, \mathfrak{v})$ where $\mathfrak{v}$ runs over all necklaces in which the pearls A and B are antipodal. This extends linearly to a map on the Jacobians.

Further we define the maps ψ, μ, and λ in the diagram on the right as follows. If y is the point $\big(E, \{A, B\}\big)$ as above, then $\mu(y)$ is the sum of the points (E, A) and (E, B) in X_0. If $x = (E, A)$ with A a cyclic subgroup of order p in E is a point on X_0, then we set $\psi(x)$ equal to the sum of $\big(E, \{A, B\}\big)$ where B runs through all cyclic subgroups of order p in E distinct from A. Finally if $z = (E, \mathfrak{v})$ is a point on X_{nsp} for some necklace $\mathfrak{v}$, then $\lambda(z)$ is the sum of all $\big(E, \{A, B\}\big)$ where A and B run through all pairs of antipodal pearls in the necklace $\mathfrak{v}$. All these three correspondences extend linearly to the corresponding Jacobians. As explained in Section 4.7, those correspondences comes from degeneracy maps (where we replace π^+_{nsp} by $\tilde{\pi}^+_{\mathrm{nsp}}$ which will be defined in Section 4.7).

To recapitulate, we list in Figure 1 the definitions for future reference next to a diagram involving all relevant maps.



$$\psi\big(E, A\big) = \sum_{\substack{B \text{ with} \\ B \neq A}} \big(E, \{A, B\}\big)$$

$$\mu\big(E, \{A, B\}\big) = \big(E, A\big) + \big(E, B\big)$$

$$\varphi\big(E, \{A, B\}\big) = \sum_{\substack{\mathfrak{v} \text{ with} \\ \mathfrak{v} \ni A \leftrightarrow B}} \big(E, \mathfrak{v}\big)$$

$$\lambda\big(E, \mathfrak{v}\big) = \sum_{\substack{\{A,B\} \text{ with} \\ A \leftrightarrow B \in \mathfrak{v}}} \big(E, \{A, B\}\big)$$

Figure 1: The various maps in Chen's theorem

We proceed to reprove Chen's result. Even if we believe that our proof is simpler and conceptually better visualised than the original proof in [Che00], we have to emphasise that it is mostly a reformulation or translation of Chen's proof into our new language. The crucial argument at the end is the same.

Theorem 15 (Chen-Edixhoven). *There are two complexes of abelian varieties over* $\mathbb{Q}$

$$0 \longrightarrow \mathrm{Jac}\big(X_0\big) \xrightarrow{\psi} \mathrm{Jac}\big(X^+_{\mathrm{sp}}\big) \xrightarrow{\varphi} \mathrm{Jac}\big(X^+_{\mathrm{nsp}}\big) \longrightarrow 0$$

$$0 \longleftarrow \mathrm{Jac}\big(X_0\big) \xleftarrow[\mu]{} \mathrm{Jac}\big(X^+_{\mathrm{sp}}\big) \xleftarrow[\lambda]{} \mathrm{Jac}\big(X^+_{\mathrm{nsp}}\big) \longleftarrow 0$$

whose cohomologies are finite groups.

We could also reformulate the theorem by saying that

$$\mathrm{Jac}\big(X_0\big) \oplus \mathrm{Jac}\big(X^+_{\mathrm{nsp}}\big) \underset{\mu\oplus\varphi}{\overset{\psi+\lambda}{\rightleftarrows}} \mathrm{Jac}\big(X^+_{\mathrm{sp}}\big)$$

are isogenies defined over $\mathbb{Q}$; however they are not dual to each other.

4.2 The easier part of the proof

Lemma 16. *The two sequences in Theorem 15 are complexes and $\mu\circ\psi = [p-1]$ on the Jacobian of X_0.*

Proof. Let $x = (E, A)$ be a point in X_0. Then

$$\varphi\circ\psi(x) = \varphi\Big(\sum_{B\neq A}\big(E,\{A,B\}\big)\Big) = \sum_{B\neq A}\sum_{\mathfrak{v}\ni A\leftrightarrow B}(E,\mathfrak{v})$$

where the last sum runs over all necklaces $\mathfrak{v}$ in which A and B are antipodal. Now A will appear in each necklace once and for each necklace there is a unique B which is antipodal to A in $\mathfrak{v}$. Hence $\varphi\circ\psi(x)$ is equal to the sum over all possible necklaces of E. But

$$\varphi\circ\psi(x) = \sum_{\mathfrak{v}}(E,\mathfrak{v}) = j^*_{\mathrm{nsp}}(E)$$

is the pullback of a divisor (E) on $X(1)$ by the natural projection $j^+_{\mathrm{nsp}}\colon X^+_{\mathrm{nsp}}\to X(1)$. Since $X(1)\cong\mathbb{P}^1$ has trivial Jacobian, we find $\varphi\circ\psi = 0$ on the Jacobians. This proof was already noted by Merel on page 189 in [Mer99].

Next, for a point $z = (E,\mathfrak{v})$ in X^+_{nsp}, we have

$$\mu\circ\lambda(z) = \mu\Big(\tfrac{1}{2}\sum_A\big(E,\{A,B\}\big)\Big) = \frac{1}{2}\sum_A\Big((E,A)+(E,B)\Big) = \sum_A(E,A) = j_0^*(E)$$

where B in the sums denotes the unique pearl which is antipodal to A in $\mathfrak{v}$ and where $j_0\colon X_0\to X(1)$. Hence $\mu\circ\lambda = 0$ on the Jacobians.

Finally, we obtain

$$\begin{aligned}\mu\circ\psi(x) &= \mu\Big(\sum_{B\neq A}\big(E,\{A,B\}\big)\Big) = \sum_{B\neq A}\Big((E,A)+(E,B)\Big)\\ &= (p-1)\cdot(E,A) + \sum_B(E,B) = (p-1)\cdot x + j_0^*(E)\end{aligned}$$

and hence $\mu\circ\psi = [p-1]$ on the Jacobian of X_0. □

Corollary 17. *The kernel $\ker\psi\subset\mathrm{Jac}(X_0)[p-1]$ and the cokernel $\mathrm{coker}(\mu) = 0$ are finite.*

4.3 Making use of antipodal pearls

We deduce from the earlier Lemma 8 the following result:

Corollary 18. *For every $\big(E,\{A,B\}\big)\in X^+_{\mathrm{sp}}$, we have*

$$\lambda\circ\varphi\,\big(E,\{A,B\}\big) = \frac{p-1}{2}\cdot\big(E,\{A,B\}\big) + \sum_{\substack{\{C,D\}\ \text{with}\\ [A,B;C,D]\notin\square}}\big(E,\{C,D\}\big)$$

with the sum running over all $\{C,D\}$ disjoint from $\{A,B\}$ such that the cross-ratio $[A,B;C,D]$ is a non-square in $\mathbb{F}_p^\times$.

Proof. Since

$$\lambda \circ \varphi\left(E, \{A, B\}\right) = \sum_{\substack{\mathfrak{v} \text{ with} \\ A \leftrightarrow B \in \mathfrak{v}}} \sum_{\substack{\{C,D\} \text{ with} \\ C \leftrightarrow D \in \mathfrak{v}}} \left(E, \{C, D\}\right)$$

we are asked to count how many necklaces have both $\{A, B\}$ and $\{C, D\}$ as antipodal pairs in common. If the four pearls are distinct, Lemma 8 gives the answer. If $A = B$, but $C \neq D$, then there are no such $\mathfrak{v}$ and if $\{A, B\} = \{C, D\}$, then we have to count how many necklaces have $A \leftrightarrow B \in \mathfrak{v}$, this is $\frac{p-1}{2}$ by Lemma 8 again. □

We now define yet another map $\alpha\colon \mathrm{Jac}\big(X^+_{\mathrm{sp}}\big) \to \mathrm{Jac}\big(X^+_{\mathrm{sp}}\big)$. For a point $y = (E, \{A, B\})$, we define $\alpha\big(E, \{A, B\}\big)$ to be the sum $\sum\{C, D\}$ running over all unordered pairs $\{C, D\}$ such that $[A, B; C, D] = -1$.

Lemma 19. *We have*

$$\alpha \circ \alpha\left(E, \{A, B\}\right) = \frac{p-1}{2} \cdot \left(E, \{A, B\}\right) + \sum_{\substack{\{C,D\} \text{ with} \\ [A,B;C,D] \in \square}} \left(E, \{C, D\}\right)$$

where the second sum runs over all unordered pairs $\{C, D\}$ such that the cross-ratio $[A, B; C, D]$ is a square in $\mathbb{F}_p^\times$.

Proof. By definition, we have

$$\alpha \circ \alpha\left(E, \{A, B\}\right) = \sum_{\substack{\{X,Y\} \text{ with} \\ [A,B;X,Y]=-1}} \sum_{\substack{\{C,D\} \text{ with} \\ [X,Y;C,D]=-1}} \{C, D\}.$$

Given $\{C, D\}$, we wish to determine how many $\{X, Y\}$ exist with $[A, B; X, Y] = [X, Y; C, D] = -1$. Assume first that A, B, C, D are all distinct. It follows that X and Y are distinct from any of the four. Then we choose a basis such that $A = (1 : 0)$, $B = (0 : 1)$ and $C = (1 : 1)$. We write $D = (d : 1)$, $X = (x : 1)$ and $Y = (y : 1)$. The two equations give

$$\begin{aligned} -1 &= [A, B; X, Y] = x/y \\ -1 &= [X, Y; C, D] = \frac{x-1}{y-1} \cdot \frac{y-d}{x-d}. \end{aligned}$$

They simplify to $x = -y$ and $x^2 = d = [A, B; C, D]$. Hence if $[A, B; C, D]$ is a non-square in $\mathbb{F}_p$, then there are no $\{X, Y\}$ and if it is a square then there is exactly one pair $\{X, Y\}$.

Finally, suppose they are not all distinct, say $C = A$. If $D \neq B$, then there can not be any $\{X, Y\}$. If $\{A, B\} = \{C, D\}$, then all pairs $\{X, Y\}$ with $[A, B; X, Y] = -1$ will contribute to the sum, and there are $\frac{p-1}{2}$ such pairs. □

Proposition 20. *Let $j_{\mathrm{sp}}\colon X^+_{\mathrm{sp}} \to X(1)$ be the natural projection. The relation*

$$\Big(\lambda \circ \varphi + \alpha \circ \alpha + \psi \circ \mu\Big)\big(E, \{A, B\}\big) = p \cdot \big(E, \{A, B\}\big) + j^*_{\mathrm{sp}}(E) \tag{3}$$

holds for all $\big(E, \{A, B\}\big) \in X^+_{\mathrm{sp}}$.

Proof. This is just the combination of Corollary 18, Lemma 19, the equality

$$\psi \circ \mu\big(E, \{A, B\}\big) = 2 \cdot \big(E, \{A, B\}\big) + \sum_{C \neq A, B} \Big(\big(E, \{A, C\}\big) + \big(E, \{B, C\}\big)\Big),$$

and counting how often $\big(E, \{A, B\}\big)$ appears on both sides. □

4.4 Representation theoretic argument

The main argument in [Edi96, dSE00] that an isogeny must exist between the Jacobians, and even some information about its degree, is directly deduced from the Brauer relation between certain permutation representation. Denote by $\mathcal{B}$, $\mathcal{S}$, and $\mathcal{N}$ a Borel subgroup, a normaliser of a split Cartan subgroup and a normaliser of a non-split Cartan subgroup of a group $\mathcal{G}$ isomorphic to $\mathrm{PGL}_2(\mathbb{F}_p)$, respectively. Then (see [Edi96, dSE00])

$$\mathbb{Q}[\mathcal{G}/\mathcal{S}] \oplus \mathbb{Q}[\mathcal{G}/\mathcal{G}] \cong \mathbb{Q}[\mathcal{G}/\mathcal{N}] \oplus \mathbb{Q}[\mathcal{G}/\mathcal{B}].$$

We fix an elliptic curve E over an algebraically closed field of characteristic different from p. Write $\mathcal{G} = \mathrm{PGL}\big(E[p]\big)$. We consider the $\mathbb{Q}[\mathcal{G}]$-modules $U = \bigoplus_{\mathfrak{v}} \mathbb{Q}\,(E, \mathfrak{v})$, which is isomorphic to $\mathbb{Q}[\mathcal{G}/\mathcal{N}]$, and $V = \bigoplus_{\{A,B\}} \mathbb{Q}\,\big(E, \{A, B\}\big) \cong \mathbb{Q}[\mathcal{G}/\mathcal{S}]$. The equation (3) is a relation between $\mathbb{Q}[\mathcal{G}]$-endomorphisms of V: $\lambda\circ\varphi+\alpha\circ\alpha+\psi\circ\mu = [p]+j$, where we still denote by $\psi, \varphi, \alpha, \lambda, \mu$ the morphisms induced on $\mathbb{Q}[\mathcal{G}]$-modules and where $j\colon V \to V$ sends $\big(E, \{A, B\}\big)$ to the sum over all $\big(E, \{C, D\}\big)$.

From the fact that the middle line (for T') in table 2.2 in [Edi96] only contains 0 and 1, we see that $V \otimes \mathbb{C}$ decomposes into a sum of *distinct* irreducible $\mathbb{C}[\mathcal{G}]$-modules. We denote by χ_W the character and $e_W = 1/|\mathcal{G}| \cdot \sum_{g\in\mathcal{G}} \chi_W(g)\, g^{-1}$ the idempotent associated to such an irreducible $\mathbb{C}[\mathcal{G}]$-submodule W of V. For f a $\mathbb{Q}[\mathcal{G}]$-endomorphism of V, Schur's Lemma implies that $f|_W$ is the multiplication by a scalar $c_W(f) \in \mathbb{C}$. Let K be the cyclotomic field $\mathbb{Q}(\zeta_{p-1}, \zeta_{p+1})$. A look at the character table (for instance table 2.1 in [Edi96]) of $\mathcal{G} \cong \mathrm{PGL}_2(\mathbb{F}_p)$ shows that all values of characters are contained in K. Since $c_W(f) = 1/\dim(W) \cdot \mathrm{tr}(e_W \circ f)$, we see that $c_W(f)$ belongs to $\mathbb{Q}(\chi_W) \subset K$.

We will now consider these scaling factors for the $\mathbb{Q}[\mathcal{G}]$-endomorphisms in equation (3). Let W be an irreducible complex representation which appears in the decomposition of $V \otimes \mathbb{C}$ but not in the image of $\psi\otimes\mathbb{C}\colon \bigoplus_A \mathbb{C}\,(E, A) \to V\otimes\mathbb{C}$. Then $c_W(\psi\circ\mu) = 0$. By the Brauer relation, since $\bigoplus_A \mathbb{Q}\,(E, A) \cong \mathbb{Q}[\mathcal{G}/\mathcal{B}]$, the representation W also appears in the decomposition of $U \otimes \mathbb{C}$. Then similarly $c_W(j) = 0$. Hence the equation (3) gives

$$c_W(\lambda \circ \varphi) = c_W([p]) - c_W(\alpha \circ \alpha) = p - c_W(\alpha)^2.$$

However, since $c_W(\alpha) \in K$, it can not be equal to $\pm\sqrt{p}$. This shows that $c_W(\lambda\circ\varphi) \neq 0$ for all irreducible W which do not appear in the image of ψ.

Therefore the map φ is a $\mathcal{G}$-isomorphism from $V/\operatorname{im}\psi$ into the non-trivial part of U. Moreover, the map $\varphi \circ \lambda\colon U \to U$ has the same scalar factors $c_W(\varphi \circ \lambda) = c_W(\lambda \circ \varphi) \neq 0$ and on the trivial part it is the scalar multiplication by $(p^2 - 1)/4 \neq 0$. It follows that $\varphi \circ \lambda$ is a $\mathcal{G}$-automorphism of U.

4.5 End of proof of Proposition 14

We compute

$$\varphi \circ \lambda\,(\mathfrak{v}) = \varphi\Big(\sum_{\substack{\{A,B\} \text{ with} \\ A \nleftrightarrow B \in \mathfrak{v}}} \{A, B\}\Big) = \sum_{\substack{\{A,B\} \text{ with} \\ A \nleftrightarrow B \in \mathfrak{v}}} \sum_{\substack{\mathfrak{w} \text{ with} \\ A \nleftrightarrow B \in \mathfrak{w}}} \mathfrak{w} = \sum_{\mathfrak{w}} \langle \mathfrak{v}, \mathfrak{w} \rangle \cdot \mathfrak{w}.$$

We deduce from the above representation theoretic input that the pairing in Section 3.8 is non-degenerate.

This concludes the proof of Proposition 14. It is to note that the non-degeneracy of the pairing is equivalent to the difficult part of the proof of Chen's isogeny in Theorem 15. It would be nice to find a purely combinatorial proof of the non-degeneracy of this pairing.

4.6 End of proof of Theorem 15

In Section 4.4, we have shown that the map $\varphi \circ \lambda\colon \bigoplus_{\mathfrak{v}} \mathbb{Z}\,(E, \mathfrak{v}) \to \bigoplus_{\mathfrak{v}} \mathbb{Z}\,(E, \mathfrak{v})$ has finite kernel and cokernel. In other words the map

$$\varphi \circ \lambda\colon \mathrm{Div}(X^+_{\mathrm{nsp}}) \to \mathrm{Div}(X^+_{\mathrm{nsp}})$$

has finite kernel and cokernel in each fibre. Since the size of them is independent of the fibre, the above map has kernel and cokernel of finite exponent. Now consider the induced map

$$\varphi \circ \lambda\colon \mathrm{Jac}(X^+_{\mathrm{nsp}}) \to \mathrm{Jac}(X^+_{\mathrm{nsp}})$$

on the Jacobian. If $[D]$ is a divisor class in $\mathrm{Jac}(X^+_{\mathrm{nsp}})$, then there is a multiple $[mD]$ which is in the image of $\varphi \circ \lambda$. Therefore the map $\varphi \circ \lambda$ has finite cokernel on the Jacobians. Comparing the dimensions it follows that it has finite kernel, too. This implies that φ has finite cokernel and λ has finite kernel in the sequences in Theorem 15.

To conclude we have to verify that the sequences have finite cohomology in the middle term. This can be deduced from counting the dimension together with all the known parts of the theorem: We know from (2) in Section 3.6 that the dimension of $\mathrm{Jac}(X^+_{\mathrm{sp}})$ is equal to the sum of the dimensions of $\mathrm{Jac}(X_0)$ and $\mathrm{Jac}(X^+_{\mathrm{nsp}})$. Since φ has finite cokernel, its kernel has now the same dimension as $\mathrm{Jac}(X_0)$, which is also the dimension of the image of ψ. Because the sequence is a complex, we have $\operatorname{im}\psi \subset \ker\varphi$ and the quotient is finite because they have the same dimension. The argument for the second sequence is similar. This concludes the proof of Theorem 15.

4.7 Relation to Chen's computations

To relate our proof to the previous proof in [Che00], we need first to establish a translation. The first difference is that we work with $\mathrm{PGL}_2(\mathbb{F}_p)$ rather than with $\mathrm{GL}_2(\mathbb{F}_p)$, but that does not make any real difference.

Fix an elliptic curve E over an algebraically closed field of characteristic different from p. Let us fix two distinct subgroups A_0 and B_0 in E. Further we choose a necklace $\mathfrak{v}_0$ in which A_0 is antipodal to B_0. Let $\mathcal{B}$ be the stabiliser of A_0 in $\mathcal{G} = \mathrm{PGL}\big(E[p]\big)$, which is a Borel subgroup, let $\mathcal{S}$ be the stabiliser of $\{A_0, B_0\}$, which is the normaliser of a split Cartan subgroup, and let $\mathcal{N}$ be the stabiliser of $\mathfrak{v}_0$, which is the normaliser of a non-split Cartan. Then we define three $\mathcal{G}$-isomorphisms

$$\iota_0 : \mathbb{Q}\big[\mathcal{G}/\mathcal{B}\big] \longrightarrow \bigoplus_A \mathbb{Q}\,A\,, \qquad \iota_{\mathrm{sp}} : \mathbb{Q}\big[\mathcal{G}/\mathcal{S}\big] \longrightarrow \bigoplus_{\{A,B\}} \mathbb{Q}\,\{A,B\}\,, \qquad \iota_{\mathrm{nsp}} : \mathbb{Q}\big[\mathcal{G}/\mathcal{N}\big] \longrightarrow \bigoplus_{\mathfrak{v}} \mathbb{Q}\,\mathfrak{v}$$

by $\iota_0(\mathcal{B}) = A_0$, $\iota_{\mathrm{sp}}(\mathcal{S}) = \{A_0, B_0\}$ and $\iota_{\mathrm{nsp}}(\mathcal{N}) = \mathfrak{v}_0$. The importance of the exact choices here is that $\mathcal{N} \cap \mathcal{S}$ contains 4 elements. Had we taken "adjacent" rather than "antipodal" pearls in the necklace, we would only have 2 elements. Compare with remarque 3 in [dSE00].

Recall from [Che00] that for each double coset $\mathcal{H}g\mathcal{H}'$ for some subgroups $\mathcal{H}$ and $\mathcal{H}'$ of $\mathcal{G}$ and $g \in \mathcal{G}$, there is a $\mathcal{G}$-morphism $\Theta(\mathcal{H}g\mathcal{H}')\colon \mathbb{Q}[\mathcal{G}/\mathcal{H}] \to \mathbb{Q}[\mathcal{G}/\mathcal{H}']$ sending $\mathcal{H}$ to the sum $\sum_{s\in\Omega} s\mathcal{H}'$ such that $\bigcup_{s\in\Omega} s\mathcal{H}' = \mathcal{H}g\mathcal{H}'$ is a disjoint union.

Lemma 21. *We have*

$$\psi = \iota_{\mathrm{sp}} \circ \Theta(\mathcal{B}1\mathcal{S}) \circ \iota_0^{-1}, \quad \mu = \iota_0 \circ \Theta(\mathcal{S}1\mathcal{B}) \circ \iota_{\mathrm{sp}}^{-1}, \quad \varphi = \iota_{\mathrm{nsp}} \circ \Theta(\mathcal{S}1\mathcal{N}) \circ \iota_{\mathrm{sp}}^{-1}, \quad \textit{and} \quad \lambda = \iota_{\mathrm{sp}} \circ \Theta(\mathcal{N}1\mathcal{S}) \circ \iota_{\mathrm{nsp}}^{-1}.$$

Further we have $\alpha = \iota_{\mathrm{sp}} \circ \Theta(\mathcal{S}g\mathcal{S}) \circ \iota_{\mathrm{sp}}^{-1}$ *with* $g = \left[\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right]$.

Proof. We only illustrate the first equality as the proof is very similar for all of the first four equalities. The map $\Theta(\mathcal{B}1\mathcal{S})$ sends $\mathcal{B} = \iota_0^{-1}(A_0)$ to the sum of $s\mathcal{S}$ where s runs over a system Ω of representatives of $\mathcal{B}/(\mathcal{B}\cap\mathcal{S})$. The quotient group is the group of elements in $\mathcal{G}$ fixing A_0 modulo the subgroup of elements also fixing B_0. So

$$\iota_{\mathrm{sp}} \circ \Theta(\mathcal{B}1\mathcal{S})(\mathcal{B}) = \sum_{s\in\Omega} \{A_0, sB_0\}.$$

Since $\mathcal{B}$ acts transitively on $\mathbb{P}\big(E[p]\big) \setminus \{A_0\}$, each $\{A_0, B\}$ with $B \neq A_0$ will appear exactly once in this sum. Hence

$$\iota_{\mathrm{sp}} \circ \Theta(\mathcal{B}1\mathcal{S})(\mathcal{B}) = \sum_{B\neq A_0} \{A_0, B\} = \psi(A_0).$$

To prove the last equality, note that with $C_0 = gA_0$ and $D_0 = gB_0$, we get $[A_0, B_0; C_0, D_0] = -1$ and $g\mathcal{S}g^{-1}$ is the stabiliser in $\mathcal{G}$ of $\{C_0, D_0\}$. So the quotient $\mathcal{S}/(\mathcal{S}\cap g\mathcal{S}g^{-1})$ is the group of elements fixing $\{A_0, B_0\}$ modulo elements also fixing $\{C_0, D_0\}$. It follows that

$$\iota_{\mathrm{sp}} \circ \Theta(\mathcal{S}g\mathcal{S})(\mathcal{S}) = \sum_{s\in\Omega'} sg\{A_0, B_0\} = \sum_{s\in\Omega'} \{sC_0, sD_0\}$$

where Ω' is a system of representatives of $\mathcal{S}/(\mathcal{S} \cap g\mathcal{S}g^{-1})$. This is exactly the sum of all $\{C, D\}$ with $[A_0, B_0; C, D] = -1$, because the action of $\mathcal{S}$ on the set of pairs $\{C, D\}$ is transitive and for $s \in \Omega$, we have $[A_0, B_0; sC_0, sD_0] = [sA_0, sB_0; sC_0, sD_0] = [A_0, B_0; C_0, D_0] = -1$. □

Now it is clear that equation (3) is exactly what Chen proves in Proposition 8.6 and Proposition 8.7. His proof is a computation in double coset operators. He then goes on to give formulae for the values of $c_W(\lambda \circ \varphi)$ in terms of character sums. However, his final argument that they are non-zero can be shortened as we did in Section 4.4 without making the values more explicit.

Finally, we wish to point out that Chen also describes the maps using the degeneracy morphisms. See his Theorem 2 in [Che00]. For instance, let consider the usual degeneracy morphisms $\pi_0 : X_{\mathcal{A}} \longrightarrow X_0$ defined by $(E, (A, B, C)) \mapsto (E, A)$ and $\pi_{\mathrm{sp}}^+ : X_{\mathcal{A}} \longrightarrow X_{\mathrm{sp}}^+$ defined by $(E, (A, B, C) \mapsto (E, \{A, B\})$, it is easy to see from our definitions that

$$(p-1) \cdot \psi = (\pi_{\mathrm{sp}}^+)_* \circ (\pi_0)^* \qquad \text{and} \qquad (p-1) \cdot \mu = (\pi_0)_* \circ (\pi_{\mathrm{sp}}^+)^*$$

hold as maps on divisors. To explain φ and λ, we have to replace π_{nsp}^+ by another degeneracy map. Let ε be a non-square in $\mathbb{F}_p$. We define $\tilde{\pi}_{\mathrm{nsp}}^+ \colon X_{\mathcal{A}} \to X_{\mathrm{nsp}}^+$ by sending $\big(E, (A, B, C)\big)$ to the following necklace $\mathfrak{v}$ in E. First there exist a unique D distinct from A, B, and C such that $[A, B; C, D] = \varepsilon$. Then, by Lemma 8 there is a unique $\mathfrak{v}$ such that $A \leftrightarrow B \in \mathfrak{v}$ and $C \leftrightarrow D \in \mathfrak{v}$. It is also this lemma which shows that this map is $\mathrm{PGL}\big(E[p]\big)$-equivariant.

Lemma 22. *We have*

$$4 \cdot \varphi = (\tilde{\pi}_{\mathrm{nsp}}^+)_* \circ (\pi_{\mathrm{sp}}^+)^* \qquad \textit{and} \qquad 4 \cdot \lambda = (\pi_{\mathrm{sp}}^+)_* \circ (\tilde{\pi}_{\mathrm{nsp}}^+)^*.$$

Proof. Let A and B be two distinct cyclic subgroups of order p of some elliptic curve E. By definition, we have

$$\begin{aligned}(\tilde{\pi}_{\mathrm{nsp}}^+)_* \circ (\pi_{\mathrm{sp}}^+)^*\big(E, \{A, B\}\big) &= \sum_{C \notin \{A,B\}} \tilde{\pi}_{\mathrm{nsp}}^+\big(E, (A, B, C)\big) + \sum_{D \notin \{A,B\}} \tilde{\pi}_{\mathrm{nsp}}^+\big(E, (B, A, D)\big) \\ &= 2 \sum_{X \notin \{A,B\}} \tilde{\pi}_{\mathrm{nsp}}^+\big(E, (A, B, X)\big)\end{aligned}$$

since $[A, B; C, D] = [B, A; D, C]$ for all C, D. Each necklace in this sum will have A and B as antipodal pearls. Let $\mathfrak{v}$ be a necklace with $A \leftrightarrow B \in \mathfrak{v}$. We wish to determine how often $\mathfrak{v}$ appears in the above sum, that is to say how many $X \notin \{A, B\}$ are there such that $\mathfrak{v} = \tilde{\pi}_{\mathrm{nsp}}^+\big(E, (A, B, X)\big)$. In other words, we wish to count the X such that $[A, B; X, X'] = \varepsilon$ where X' is the antipodal pearl to X in $\mathfrak{v}$. We can choose a basis of $E[p]$ such that $A = (1 : 0)$, $B = (0 : 1)$ and the subgroups $X \notin \{A, B\}$ are $X = (1 : a)$ for some $a \in \mathbb{F}_p^\times$. The involution in the stabiliser of $\mathfrak{v}$ is then represented by a matrix $g = \left[\begin{smallmatrix} 0 & d \\ 1 & 0 \end{smallmatrix}\right]$ with d non-square and the antipodal pearl to X in $\mathfrak{v}$ is $X' = (da : 1)$. It follows that $[A, B; X, X'] = da^2$. Since ε and d are non-squares, the equation $da^2 = \varepsilon$ has two solutions in $\mathbb{F}_p^\times$. Hence there are two pearls $X \notin \{A, B\}$ such that $\mathfrak{v} = \tilde{\pi}_{\mathrm{nsp}}^+\big(E, (A, B, X)\big)$ and consequently

$$(\tilde{\pi}_{\mathrm{nsp}}^+)_* \circ (\pi_{\mathrm{sp}}^+)^*\big(E, \{A, B\}\big) = 4 \sum_{\substack{\mathfrak{v} \text{ with} \\ A \leftrightarrow B \in \mathfrak{v}}} \mathfrak{v}.$$

The second equality follows from an analogous argument. □

5 Examples

We add some numerical examples for small primes, mainly on the eigenvalues of the pairing in Section 3.8.

5.1 Necklaces for $p = 5$

There is a unique conjugacy class C_γ in $\mathrm{PGL}_2(\mathbb{F}_5)$. We have $t = 1$ and $n = 2$. We spell out the 10 necklaces below by giving them as a list of all points in $\mathbb{P}^1(\mathbb{F}_5)$:

$$\begin{gathered}(0,1,2,4,\infty,3),\ (0,1,3,\infty,2,4),\ (0,1,4,2,3,\infty),\ (0,1,\infty,3,4,2),\ (0,2,1,\infty,4,3),\\ (0,3,1,2,\infty,4),\ (0,3,2,1,4,\infty),\ (0,2,3,4,1,\infty),\ (0,2,\infty,1,3,4),\ (0,4,1,3,2,\infty).\end{gathered}$$

It is now easy to read off the pairing $\langle\cdot,\cdot\rangle$ defined in Section 3.8. Let $\mathfrak{v}$ be the first necklace in the list. Of course, we have $\langle\mathfrak{v},\mathfrak{v}\rangle = 3$. On the one hand, we have $\langle\mathfrak{v},\mathfrak{w}\rangle = 0$ for $\mathfrak{w}$ being any of the necklaces from the second to the seventh and, on the other hand, $\langle\mathfrak{v},\mathfrak{w}\rangle = 1$ when $\mathfrak{w}$ is any of the last three necklaces.

The resulting matrix $(\langle\mathfrak{v},\mathfrak{w}\rangle)_{\mathfrak{v},\mathfrak{w}}$ is non-singular. Its eigenvalues are 6, four times 1, and five times 4.

5.2 Necklaces for $p = 7$

For $p = 7$, we have two choices for γ. We take $t = 1$ and $n = 3$, here.

$$\begin{gathered}(0,\infty,2,3,5,1,4,6),\ (0,6,3,5,\infty,2,4,1),\ (0,\infty,3,1,4,5,6,2),\ (0,\infty,1,5,6,4,2,3),\\ (0,3,\infty,2,5,4,6,1),\ (0,3,4,5,1,6,\infty,2),\ (0,2,1,4,\infty,3,6,5),\ (0,2,3,\infty,5,6,1,4),\\ (0,5,4,\infty,2,1,6,3),\ (0,5,\infty,1,6,2,3,4),\ (0,3,5,6,\infty,1,2,4),\ (0,5,1,2,3,6,4,\infty),\\ (0,3,1,\infty,4,2,5,6),\ (0,1,\infty,3,4,6,2,5),\ (0,\infty,5,4,2,6,3,1),\ (0,2,4,3,6,\infty,5,1),\\ (0,6,2,\infty,1,4,3,5),\ (0,4,\infty,5,2,3,1,6),\ (0,\infty,6,2,1,3,5,4),\ (0,4,6,\infty,3,5,2,1),\\ (0,6,\infty,4,3,1,5,2).\end{gathered}$$

Again the pairing is degenerate with eigenvalues 12, six times $4+2\sqrt{2}$, six times $4-2\sqrt{2}$, and eight times 3.

5.3 Larger primes

We list the characteristic polynomial of the matrix $(\langle\mathfrak{v},\mathfrak{w}\rangle)_{\mathfrak{v},\mathfrak{w}}$ for the next few primes.

p	char. polynomial of $\langle\cdot,\cdot\rangle$
11	$(X-30)\cdot(X-2)^{10}\cdot(X-8)^{20}\cdot(X^2-10X+5)^{12}$
13	$(X-42)\cdot(X^3-19X^2+83X-1)^{12}\cdot(X-12)^{14}\cdot(X-4)^{27}$
17	$(X-72)\cdot(X-1)^{16}\cdot(X^3-27X^2+195X-361)^{16}\cdot(X-16)^{17}\cdot$ $\cdot(X-8)^{18}\cdot(X^2-16X+32)^{18}$
19	$(X-90)\cdot(X-18)^{18}\cdot(X^4-32X^3+304X^2-768X+256)^{18}\cdot$ $\cdot(X-3)^{20}\cdot(X^3-33X^2+315X-867)^{20}$

These values for the eigenvalues $c_W(\varphi\circ\lambda)$ coincide with Chen's computation in his table 2 in [Che00].

References

[Bar10] Burcu Baran, *Normalizers of non-split Cartan subgroups, modular curves, and the class number one problem*, J. Number Theory **130** (2010), no. 12, 2753–2772.

[CGRR99] J. Coates, R. Greenberg, K. A. Ribet, and K. Rubin, *Arithmetic theory of elliptic curves*, Lecture Notes in Mathematics, vol. 1716, Springer-Verlag, Berlin; Centro Internazionale Matematico Estivo (C.I.M.E.), Florence, 1999, Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12–19, 1997, Edited by C. Viola.

[Che98] Imin Chen, *The Jacobians of non-split Cartan modular curves*, Proc. London Math. Soc. (3) **77** (1998), no. 1, 1–38.

[Che00] ———, *On relations between Jacobians of certain modular curves*, J. Algebra **231** (2000), no. 1, 414–448.

[DM97] Henri Darmon and Loïc Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81–100.

[DR73] Pierre Deligne and Michael Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[dSE00] Bart de Smit and Bas Edixhoven, *Sur un résultat d'Imin Chen*, Math. Res. Lett. **7** (2000), no. 2-3, 147–153.

[Edi96] Bas Edixhoven, *On a result of Imin Chen*, unpublished preprint, available at `http://arxiv.org/abs/alg-geom/9604008`, 1996.

[Hal98] Emmanuel Halberstadt, *Sur la courbe modulaire* $X_{ndép}(11)$, Experiment. Math. **7** (1998), no. 2, 163–174.

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

[KP14] D. Kohen and A. Pacetti, *Heegner points on Cartan non-split curves*, `http://arxiv.org/abs/1403.7801`, 2014.

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

[Mer99] Loïc Merel, *Arithmetic of elliptic curves and Diophantine equations*, J. Théor. Nombres Bordeaux **11** (1999), no. 1, 173–200, Les XXèmes Journées Arithmétiques (Limoges, 1997).

[Ser97] Jean-Pierre Serre, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1.