Journal of Number Theory 200 (2019) 185–204

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

# An explicit correspondence of modular curves[☆]

Imin Chen[*], Parinaz Salari Sharif

*Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, Canada*

ARTICLE INFO

*Article history:*
Received 5 March 2018
Received in revised form 27 November 2018
Accepted 7 December 2018
Available online 22 January 2019
Communicated by F. Pellarin

*MSC:*
primary 11G18
secondary 14G35

*Keywords:*
Modular curves
Elliptic curves

ABSTRACT

In this paper, we recall an alternative proof of Merel's conjecture which asserts that a certain explicit correspondence gives the isogeny relation between the Jacobians associated to the normalizer of split and non-split Cartan subgroups. This alternative proof does not require extensive representation theory and can be formulated in terms of finite field analogues of the complex plane minus the real line.

Secondly, we generalize these arguments to exhibit an explicit correspondence which gives the isogeny relation between the Jacobians associated to split and non-split Cartan subgroups. An interesting feature is that the required explicit correspondence is considerably more complicated but can expressed as a certain linear combination of double coset operators whose coefficients we are able to make explicit.

## 1. Introduction

Modular curves, which are coarse moduli spaces for elliptic curves with prescribed level structure, appear in the study of Galois torsion structures on elliptic curves.

[☆] Research supported by an NSERC Discovery Grant and a SFU VPR Bridging Grant.

[*] Corresponding author.
*E-mail addresses:* ichen@sfu.ca (I. Chen), psalaris@sfu.ca (P. Salari Sharif).

https://doi.org/10.1016/j.jnt.2018.12.003
0022-314X/© 2019 Published by Elsevier Inc.

Let $\ell$ be a prime, and $\mathbb{Z}/\ell\mathbb{Z} = \mathbb{F}_\ell$ be the finite field of cardinality $\ell$.

A well-known example is Mazur's Theorem [7] which states that there are no rational $\ell$-isogenies between rational elliptic curves if $\ell > 163$. This result is proven by showing the modular curve $X_0(\ell)$ has no non-cuspidal rational point if $\ell > 163$. Mazur's method is based on descent on the Jacobian of $X_0(\ell)$, but because of the rich arithmetic structure of these curves, the method is more powerful and efficient.

For a subgroup $H$ of $\mathrm{GL}_2(\mathbb{F}_\ell)$ which contains $-1$, it is possible to associate a modular curve $X_H := X/H$, where $X = X(\ell)$ is the modular curve with full level structure $\ell$. In the case when $H$ is a non-split Cartan subgroup $C'$ or its normalizer $N'$, it is relevant from the point of view of Mazur's method to understand the Jacobian of $X_H$. In [3], it was proven using the trace formula that $X_{N'}$ and $X_{C'}$ are related by an isogeny over $\mathbb{Q}$ to certain quotients of the Jacobian of the modular curve $X_0(\ell^2)$. Subsequently, a proof based on the representation theory of $\mathrm{GL}_2(\mathbb{F}_\ell)$ was given in [5].

In [4], it was conjectured that the above isogeny relation between the Jacobian of $X_{N'}$ and the Jacobian of $X_0(\ell^2)$ was given by a certain explicit correspondence. This was proven in [2] using the representation theory of $\mathrm{GL}_2(\mathbb{F}_\ell)$ and identities in finite double coset algebras.

Recently, a new moduli interpretation for $X_{N'}$ was given in [10], which explains and clarifies the representation-theoretic proof given in [2] in terms of 'necklaces'.

In this paper, we recall an alternative proof of Merel's conjecture, which does not require extensive representation theory, based on arguments given by B. Birch and D. Zagier [1]. The proof can be formulated in terms of finite field analogues of the complex plane minus the real line, and is largely elementary in its statement and proof, with the exception of one argument relying on algebraic number theory.

Secondly, we generalize these arguments to exhibit an explicit correspondence which gives the isogeny relation between the Jacobians associated to split and non-split Cartan subgroups. An interesting feature is that the required explicit correspondence is considerably more complicated, but can be expressed as a certain linear combination of double coset operators whose coefficients we are able to make explicit.

The precise statements of the theorems we prove are as follows.

- Let $\ell$ be an odd prime and $\epsilon$ a non-square in $\mathbb{F}_\ell^\times$.
- Let $G = \mathrm{GL}_2(\mathbb{F}_\ell)$.
- Let $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta$ denote the set of ordered pairs $(a, b)$ of distinct points in $\mathbb{P}^1(\mathbb{F}_\ell)$.
- Let $(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta)/\sim$, where $(a, b) \sim (b, a)$, denote the set of unordered pairs $\{a, b\}$ of distinct points in $\mathbb{P}^1(\mathbb{F}_\ell)$.
- Let $\mathfrak{C}_\ell = \left\{x + y\sqrt{\epsilon} : x \in \mathbb{F}_\ell, y \in \mathbb{F}_\ell^\times\right\}$.
- Let $\mathfrak{H}_\ell = \mathfrak{C}_\ell/\sim$, where $x + y\sqrt{\epsilon} \sim x - y\sqrt{\epsilon}$.
- When $S$ is a set, we denote by $\mathbb{Q}[S]$ the free $\mathbb{Q}$-vector space generated by the set $S$.
- For convenience, we write column vectors in the form $(x, y)^t$ for instance.

Given an unordered pair $\{a,b\}$ in $(\mathbb{P}^1(\mathbb{F}_\ell)\times\mathbb{P}^1(\mathbb{F}_\ell)\setminus\Delta)/\sim$, we define in (6) a 'geodesic' $\gamma_{\{a,b\}}$ in $\mathfrak{H}_\ell$ between $a$ and $b$.

**Theorem 1.** *The map*

$$\begin{aligned}\psi^+ : \mathbb{Q}[(\mathbb{P}^1(\mathbb{F}_\ell)\times\mathbb{P}^1(\mathbb{F}_\ell)\setminus\Delta)/\sim] &\to \mathbb{Q}[\mathfrak{H}_\ell]\\ \{a,b\} &\mapsto \sum_{x\in\gamma_{\{a,b\}}} x\end{aligned}$$

*is a surjective* $\mathbb{Q}[G]$*-module homomorphism.*

Given an ordered pair $(a,b)$ in $\mathbb{P}^1(\mathbb{F}_\ell)\times\mathbb{P}^1(\mathbb{F}_\ell)\setminus\Delta$ and a parameter $s\in\mathbb{F}_\ell^\times$, we define in (20) a 'path' $\gamma^s_{(a,b)}$ in $\mathfrak{C}_\ell$ from $a$ to $b$.

**Theorem 2.** *The map*

$$\begin{aligned}\psi : \mathbb{Q}[\mathbb{P}^1(\mathbb{F}_\ell)\times\mathbb{P}^1(\mathbb{F}_\ell)\setminus\Delta] &\to \mathbb{Q}[\mathfrak{C}_\ell]\\ (a,b) &\mapsto \sum_{s=1}^{\ell-1}(\alpha_s+\beta_s)\sum_{x\in\gamma^s_{(a,b)}} x\end{aligned}$$

*is a surjective* $\mathbb{Q}[G]$*-module homomorphism, where* $0\le\alpha_s,\beta_s\le\ell-1$ *are integers satisfying* $\alpha_s\equiv 1\ \ (\ell)$ *and* $\beta_s\equiv s^{-1}\ \ (\ell)$ *for* $s\in\{1,\dots,\ell-1\}$*.*

We explain in section 5 how Theorems 1 and 2 imply relations between the Jacobians of $X_{N'}$ and $X_{C'}$ and quotients of the Jacobian of the more standard modular curve $X_0(\ell^2)$.

**Acknowledgments**

We would like to thank B. Birch and D. Zagier for explaining to us their alternative proof of Merel's conjecture, and the anonymous referee for detailed comments and suggestions made which greatly improved the text.

## 2. Double coset operators

**Lemma 3.** *Let* $G$ *be a group,* $H$ *and* $K$ *be subgroups of* $G$*, and* $g\in G$*. Then*

$$HgK = \bigcup_{\alpha\in H/H\cap gKg^{-1}} \alpha gK,$$

*where the union is disjoint. We call* $[H : H\cap gKg^{-1}]$ *the degree of* $HgK$*. This is independent of the choice of* $g$ *in the sense that* $deg(HgK) = deg(Hg'K)$ *if* $HgK = Hg'K$*.*

**Proof.** See [11, Proposition 3.1]. □

**Definition 4.** Let $G$ be a finite group with subgroups $H$ and $K$. Given a double coset $HgK$ and a decomposition into disjoint cosets

$$HgK = \bigcup_{\alpha\in\Omega} \alpha g K,$$

we obtain a $\mathbb{Z}[G]$-module homomorphism $\sigma = \sigma(HgK)$ given by

$$\begin{aligned} \sigma : \mathbb{Z}[G/H] &\to \mathbb{Z}[G/K] \\ xH &\mapsto \sum_{\alpha\in\Omega} x\alpha g K. \end{aligned} \tag{1}$$

The $\mathbb{Z}[G]$-module homomorphism $\sigma$ is called a double coset operator.

Let $C$ (resp. $C'$) be the split (resp. non-split) Cartan subgroup of $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ given respectively by

$$C = \left\{ \begin{pmatrix} \eta & 0 \\ 0 & \beta \end{pmatrix} : \eta, \beta \in \mathbb{F}_\ell^\times \right\},$$
$$C' = \left\{ \begin{pmatrix} x & \epsilon y \\ y & x \end{pmatrix} : x, y \in \mathbb{F}_\ell, (x,y) \neq (0,0) \right\}.$$

Let $N$ (resp. $N'$) be the normalizer in $G$ of $C$ (resp. $C'$) which is given respectively by

$$N = \left\{ \begin{pmatrix} \eta & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} 0 & \eta \\ \beta & 0 \end{pmatrix} : \eta, \beta \in \mathbb{F}_\ell^\times \right\},$$
$$N' = \left\{ \begin{pmatrix} x & \epsilon y \\ y & x \end{pmatrix}, \begin{pmatrix} x & -\epsilon y \\ y & -x \end{pmatrix} : x, y \in \mathbb{F}_\ell, (x,y) \neq (0,0) \right\}.$$

The finite field $\mathbb{F}_{\ell^2}$ is a vector space over $\mathbb{F}_\ell$ of dimension 2. The basis $\{1, \sqrt{\epsilon}\}$ gives us an identification $\mathbb{F}_{\ell^2} \cong \mathbb{F}_\ell + \sqrt{\epsilon}\mathbb{F}_\ell$. Thus, for every $z \in \mathbb{F}_{\ell^2}$, we can write $z = x + \sqrt{\epsilon}y$ for some $x, y \in \mathbb{F}_\ell$.

The group $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $\mathfrak{C}_\ell$, $\mathfrak{H}_\ell$, and $\mathbb{P}^1(\mathbb{F}_\ell)$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d},$$

(that is, by Möbius transformations), which is analogous to the facts that $\mathrm{GL}_2(\mathbb{R})$ acts on the complex plane minus the real line, and on $\mathbb{P}^1(\mathbb{R})$; its verification is similar.

We list the following bijections for later reference:

$$G/N \leftrightarrow (\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta)/\sim \tag{2}$$

$$G/N' \leftrightarrow \mathfrak{H}_\ell \tag{3}$$

$$G/C \leftrightarrow \mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta \tag{4}$$

$$G/C' \leftrightarrow \mathfrak{C}_\ell. \tag{5}$$

The above bijections are obtained by noting $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ acts transitively on each of the above sets on the right hand side. Picking the elements $\{0, \infty\}$, $\{\pm\sqrt{\epsilon}\}$, $(0, \infty)$, $(\sqrt{\epsilon}, -\sqrt{\epsilon})$, we obtain the desired bijections by computing the stabilizers of these elements.

## 3. Normalizer of Cartan subgroup case

In this section, we explain and give a detailed proof of Merel's conjecture for normalizers of Cartan subgroups using methods in [1]. In this situation, the conjectural explicit intertwining operator is given by a single double coset operator.

Define $\gamma_{\{0,\infty\}} := \mathbb{F}_\ell^\times \sqrt{\epsilon} \subseteq \mathfrak{H}_\ell$, which can be thought of as the geodesic in $\mathfrak{H}_\ell$ between 0 and $\infty$. Given an unordered pair $\{a, b\} \subseteq \mathbb{P}^1(\mathbb{F}_\ell)$, there is a $g \in G$ such that $\{a, b\} = \{g(0), g(\infty)\}$, which is unique up to multiplication on the right by $N$.

**Lemma 5.** *A choice for the element $g$ above is given by*

$$\begin{pmatrix} b & a \\ 1 & 1 \end{pmatrix},$$

*where if $a = \infty$ (resp. $b = \infty$), then the second (resp. first) column is replaced by $(1, 0)^t$.*

**Proof.** The point at infinity $\infty$ is denoted by $(1, 0)^t$ and the point 0 by $(0, 1)^t$. We require a matrix $g$ such that $g(0) = (a, 1)^t$ and $g(\infty) = (b, 1)^t$, which is given by the above matrix. □

Thus, we may define

$$\gamma_{\{a,b\}} := g(\gamma_{\{0,\infty\}}), \tag{6}$$

using the action of $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathfrak{H}_\ell$. The subset $\gamma_{\{a,b\}} \subseteq \mathfrak{H}_\ell$ can be thought of as the geodesic in $\mathfrak{H}_\ell$ between $a$ and $b$.

**Lemma 6.** *Let $a, b \in \mathbb{F}_\ell$. The quadratic equation*

$$\left(x - \frac{a+b}{2}\right)^2 - \epsilon y^2 = \left(\frac{b-a}{2}\right)^2, \tag{7}$$

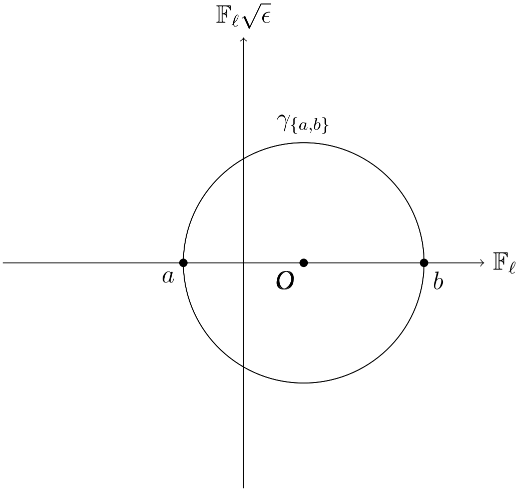

**Fig. 1.** A visual depiction of the geodesic $\gamma_{\{a,b\}}$ in $\mathfrak{H}_\ell$.

*gives the geodesic $\gamma_{\{a,b\}}$ with coordinates (see Fig. 1)*

$$x = \frac{a - \epsilon\lambda^2 b}{1 - \epsilon\lambda^2}, \tag{8}$$

$$y = \frac{\lambda(a - b)}{1 - \epsilon\lambda^2}, \tag{9}$$

$$y/(x - b) = \lambda. \tag{10}$$

**Proof.** The elements in $\gamma_{\{a,b\}}$ are given by $z = g(\lambda\sqrt{\epsilon})$ where $g = \begin{pmatrix} b & a \\ 1 & 1 \end{pmatrix}$; writing $z$ as a fraction and then rationalizing it, we obtain:

$$z = \frac{b\lambda\sqrt{\epsilon} + a}{\lambda\sqrt{\epsilon} + 1} = \frac{a - b\lambda^2\epsilon}{1 - \epsilon\lambda^2} + \sqrt{\epsilon}\frac{\lambda(b - a)}{1 - \epsilon\lambda^2}.$$

Therefore, $z = x + y\sqrt{\epsilon}$, where the $x, y$ are given by (8)–(10), which we may verify satisfy equation (6) (this equation can be found in analogy with the complex case).

The formulae (8)–(10) also give a parametrization of the conic in (6); thus every $(x, y) \in \mathbb{F}_\ell \times \mathbb{F}_\ell^\times$ (up to equivalence) satisfying (6) corresponds to an element in $\gamma_{\{a,b\}}$. □

**Lemma 7.** *The map $\psi^+ : \mathbb{Z}[(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta)/\sim] \to \mathbb{Z}[\mathfrak{H}_\ell]$ defined in Theorem 1 coincides with the double coset operator $NN' : \mathbb{Z}[G/N] \to \mathbb{Z}[G/N']$ and is hence a $\mathbb{Z}[G]$-module homomorphism.*

**Proof.** Since

$$N \cap N' = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \pm\alpha \end{pmatrix} : \alpha \in \mathbb{F}_\ell^\times \right\} \cup \left\{ \begin{pmatrix} 0 & \pm\epsilon\alpha \\ \alpha & 0 \end{pmatrix} : \alpha \in \mathbb{F}_\ell^\times \right\},$$

we have from Lemma 3 that

$$NN' = \cup_{\alpha \in \mathbb{F}_\ell^\times/\{\pm 1\}} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} N'.$$

The $\mathbb{Z}[G]$-module homomorphism from $\mathbb{Z}[G/N] \to \mathbb{Z}[G/N']$ induced by $NN'$ from (1) is then seen to be the map $\psi^+$ under the bijections (2)–(3). □

### *3.1. Coordinates for $G/N$ and $G/N'$*

We need more convenient coordinates to represent elements in (a certain subset of) $(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta)/\sim$ and $\mathfrak{H}_\ell$, where we recall $(\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta)/\sim$ is in bijection with $G/N$, and $\mathfrak{H}_\ell$ is in bijection with $G/N'$.

**Lemma 8.** *Let*

$$S_+ = \left\{(t, m) : m \text{ is a square in } \mathbb{F}_\ell^\times\right\}.$$

*Then there is a bijection from the set $(\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta)/\sim$ to the set $S_+$ given by*

$$\{a, b\} \mapsto (a + b, (a - b)^2).$$

**Proof.** The inverse map is given by sending $(t, m) \in S_+$ to the set of roots in $\mathbb{F}_\ell$ of $X^2 - tX + \frac{t^2 - m}{4}$. □

**Lemma 9.** *Let*

$$S'_+ = \left\{(T, M) : M \text{ is a non-square in } \mathbb{F}_\ell^\times\right\}.$$

*Then there is a bijection from the set $\mathfrak{H}_\ell$ to the set $S'_+$ given by*

$$x + \sqrt{\epsilon} y \mapsto (2x, 4\epsilon y^2).$$

**Proof.** The inverse map is given by sending $(T, M) \in S'_+$ to the class in $\mathfrak{H}_\ell$ of any root (in $\mathfrak{C}_\ell$) of $X^2 - TX + \frac{T^2 - M}{4}$. □

### *3.2. Proof of Theorem 1*

By Lemma 7, $\psi^+$ is a $\mathbb{Q}[G]$-module homomorphism. To prove Theorem 1, it suffices to prove that the restriction

$$\psi^+ \mid_{\mathbb{Q}[(\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta)/\sim]} : \mathbb{Q}[(\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta)/\sim] \to \mathbb{Q}[\mathfrak{H}_\ell], \tag{11}$$

is an isomorphism of $\mathbb{Q}$-vector spaces.

Using the bijections given by Lemmas 8–9, to prove (11) is equivalent to proving that

$$\psi^+ : \mathbb{Q}[S_+] \to \mathbb{Q}[S'_+],$$

is an isomorphism of $\mathbb{Q}$-vector spaces, where $\psi^+$ is the same map as $\psi^+ |_{\mathbb{Q}[(\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta)/\sim]}$ under the identifications given by the two bijections $(\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta)/\sim \leftrightarrow S_+$ and $\mathfrak{H}_\ell \leftrightarrow S'_+$.

The strategy of proving $\psi^+$ is an isomorphism will be to show its determinant is non-zero. This will be done by showing a matrix of $\psi^+$ has the form $(D_{m,M})$, where we can view each entry $D_{m,M} \in \mathbb{Z}[\zeta]$, where $\zeta$ is a primitive $\ell$th root of unity. We reduce these entries modulo a prime ideal $\mathfrak{L}$ above $\ell$ to obtain a matrix $(\overline{D}_{m,M})$ with entries in $\mathbb{F}_\ell$. After reindexing the rows and columns, we obtain a matrix $(D_{i,j})$ which is circulant, and compute its determinant to be non-zero in $\mathbb{F}_\ell$. This implies that the determinant of the original matrix of $\psi^+$ is non-zero.

To begin, recall the equation giving the geodesic between $a$ and $b$ is

$$\left(x - \frac{a+b}{2}\right)^2 - \epsilon y^2 = \left(\frac{b-a}{2}\right)^2,$$

by Lemma 6. This equation becomes

$$(T-t)^2 = (b-a)^2 + 4\epsilon y^2 = m + M,$$

in the new coordinates from Lemmas 8 and 9, namely

$$(t, m) = (a+b, (a-b)^2)$$
$$(T, M) = (2x, 4\epsilon y^2).$$

Here, $m$ and $M$ satisfy $(\frac{m}{\ell}) = 1$ and $(\frac{M}{\ell}) = -1$, where $(\frac{\cdot}{\ell})$ is the Legendre symbol modulo $\ell$.

Hence, the matrix of $\psi^+ |_{\mathbb{Q}[S_+]}$ with respect to the basis $S_+$ is given by $(a_{(T,M),(t,m)})$ where

$$a_{(T,M),(t,m)} = \begin{cases} 1 & \text{if } (T-t)^2 = m + M, \\ 0 & \text{otherwise.} \end{cases} \tag{12}$$

Thus, the above matrix is an $\frac{\ell-1}{2} \times \frac{\ell-1}{2}$ matrix $(D_{m,M})$, with entries being the $\ell \times \ell$ matrices given by

$$(D_{m,M})_{t,T} := \begin{cases} 1 & \text{if } (T-t)^2 = m + M, \\ 0 & \text{otherwise.} \end{cases}$$

**Remark 10.** At this point in the proof, we index the entries of the matrices using the variables $T, t \in \mathbb{F}_\ell$ and $m, M \in \mathbb{F}_\ell^\times$ where $\left(\frac{m}{\ell}\right) = 1$ and $\left(\frac{M}{\ell}\right) = -1$. Strictly speaking, this requires specifying an ordering on the indexing elements, which we do in the paragraph before (13) for $m, M$, and for $T, t$ we use the least non-negative residue.

Let $D$ be the matrix obtained from the $\ell \times \ell$ identity matrix by permuting its columns according to the cycle $(1\,2\,3 \ldots \ell)$.

**Lemma 11.** *We have that*

$$D_{m,M} = \sum_{u^2=m+M} D^u.$$

**Proof.** As $D$ has order $\ell$, $D^u$ is well-defined for $u \in \mathbb{F}_\ell$.

If $m + M$ is not a square in $\mathbb{F}_\ell$, therefore $D_{m,M}$ is a zero matrix due to 0 entries, so $D_{m,M} = \sum_{u^2=m+M} D^u = 0$.

If $m + M = u^2$ is a square in $\mathbb{F}_\ell$. Then $T - t = \pm u$ and

$$(D_{m,M})_{t,T} = \begin{cases} 1 & \text{if } T = t \pm u, \\ 0 & \text{otherwise.} \end{cases}$$

In this case, $D_{m,M}$ coincides with $\sum_{u^2=m+M} D^u$. □

Let $\zeta$ be a primitive $\ell$-th root of unity. The matrix $(D_{m,M})$ has entries in $\mathbb{Q}[D]$, but we can replace the matrix $D$ by an element in the cyclotomic field $\mathbb{Q}(\zeta)$ in the following manner: the minimal polynomial of $D$ over $\mathbb{Q}$ is given by $m(X) = X^{\ell-1} + \cdots + X + 1$, so we have that

$$\mathbb{Q}[D] \cong \frac{\mathbb{Q}[X]}{(m(X))} \cong \mathbb{Q}[\zeta] \cong \mathbb{Q}(\zeta).$$

**Lemma 12.** *Let $\mathfrak{L}$ be a prime ideal of $\mathbb{Q}(\zeta)$ above $\ell$. Then the residue field $\mathbb{Z}[\zeta]/\mathfrak{L} \cong \mathbb{F}_\ell$ and $\zeta \equiv 1 \pmod{\mathfrak{L}}$.*

**Proof.** [9, Lemma 10.1]. □

From the above discussion, we see that each block $D_{m,M}$ may be replaced by the element $\sum_{u^2=m+M} 1 \in \mathbb{F}_\ell$, after identifying it with an element of $\mathbb{Z}[\zeta]$ and reducing modulo $\mathfrak{L}$, yielding a matrix $(\overline{D}_{m,M})$ with entries in $\mathbb{F}_\ell$.

We label $m, M$ as $m = g^{2i}$ for $0 \leq i \leq r - 1$ and $M = \epsilon g^{2j}$ for $0 \leq j \leq r - 1$, where $r = \frac{\ell-1}{2}$ and $g \in \mathbb{F}_\ell^\times$ is a primitive root. This gives us a new matrix denoted by $(D_{i,j})$ whose entries are:

$$D_{i,j} = \sum_{u^2=g^{2i}+\epsilon g^{2j}} 1 \in \mathbb{F}_\ell. \tag{13}$$

**Definition 13.** A circulant matrix is a matrix with entries in a field $F$ of the form

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{r-1} \\ a_{r-1} & a_0 & a_1 & \dots & a_{r-2} \\ \vdots & & & & \vdots \\ a_1 & a_2 & \dots & a_{r-1} & a_0 \end{pmatrix}, \tag{14}$$

that is, a matrix whose $i$-th row is obtained from the $(i-1)$-th row by cyclically shifting the entries one position to the right.

**Proposition 14.** *Let $F$ be a field which contains all $r$th roots of unity and suppose these are distinct. Then determinant of the circulant matrix in (14) is given by*

$$\prod_{k=0}^{r-1}(a_0 + a_1\omega_k + a_2\omega_k^2 + \dots + a_{r-1}\omega_k^{r-1}) = \prod_{k=0}^{r-1}\left(\sum_{j=0}^{r-1} a_j\omega_k^j\right), \tag{15}$$

*where $\omega_k = \omega^k, r \geq 1$, and $\omega$ is a primitive $r$th root of unity in $F$.*

For later reference, we call each factor in the above formula *an eigenvalue* for $k$. We also let $r = \frac{\ell-1}{2}$ for the rest of this section.

**Lemma 15.** *The matrix $(D_{i,j})$ is an $r \times r$ circulant matrix with entries in $\mathbb{F}_\ell$.*

**Proof.** This follows because

$$D_{i,j} = \sum_{u^2=g^{2i}+\epsilon g^{2j}} 1 = \sum_{u^2=g^2(g^{2(i-1)}+\epsilon g^{2(j-1)})} 1 = D_{i-1,j-1},$$

where the indices $i, j$ are taken modulo $r$. □

Remark that $D_{0,j} = a_j$ is equal to the number of solutions of $u^2 = 1 + \epsilon g^{2j}$. To show that $(D_{i,j})$ has non-zero determinant, it suffices to show, by the determinant formula for a circulant matrix, that we have

$$a_0 + a_1\omega_k + a_2\omega_k^2 + \dots + a_{r-1}\omega_k^{r-1} \neq 0 \tag{16}$$

for every $0 \leq k \leq r-1$, where $\omega_k = g^{2k}$. This is proven in the next lemma.

**Lemma 16.**

$$\sum_{j=0}^{r-1} a_j(g^{2k})^j \neq 0,$$

*for every $0 \leq k \leq r-1$.*

**Proof.** The above sum can be calculated as:

$$\begin{aligned}\sum_{j=0}^{r-1} D_{0,j}(g^{2k})^j &= \sum_{j=0}^{r-1} a_j (g^{2k})^j = \sum_{j=0}^{r-1}\left(\sum_{u^2=1+\epsilon g^{2j}} 1\right)(g^{2j})^k \\ &= \sum_{\substack{j=0,\dots,r-1\\ u\in\mathbb{F}_\ell\\ u^2=1+\epsilon g^{2j}}} (g^{2j})^k = \frac{1}{2}\sum_{\substack{u\in\mathbb{F}_\ell\\ y\in\mathbb{F}_\ell^\times\\ u^2=1+4\epsilon y^2}}\left(\frac{u^2-1}{\epsilon}\right)^k. \end{aligned} \tag{17}$$

Now, we need to show that (17) is non-zero for every $0 \le k \le r-1$.

We can rewrite $\frac{u^2-1}{\epsilon}$ as $4y^2$. Here, we are computing $D_{i,j}$ for $i = 0$, which corresponds to $m = 1 = (a-b)^2$ and $u = 2x - (a+b)$. The conic $u^2 = 1 + 4\epsilon y^2$ then becomes

$$\begin{aligned} u^2 = 1+4\epsilon y^2 &\iff (2x-(a+b))^2 = 1+4\epsilon y^2 \\ &\iff \left(x-\frac{a+b}{2}\right)^2 - \epsilon y^2 = \left(\frac{b-a}{2}\right)^2, \end{aligned}$$

which is parametrized by $x = \frac{a-\epsilon\lambda^2 b}{1-\epsilon\lambda^2}, y = \frac{\lambda(a-b)}{1-\epsilon\lambda^2}$ from (7). Thus, we can rewrite (17) as

$$\sum_{\lambda\in\mathbb{F}_\ell^\times}\frac{4^k}{2}\left(\frac{\lambda}{1-\epsilon\lambda^2}\right)^{2k} = \sum_{\lambda\in\mathbb{F}_\ell^\times}\frac{4^k}{2}\cdot(\lambda^{-1}-\epsilon\lambda)^{-2k} = \sum_{\lambda\in\mathbb{F}_\ell^\times}\frac{4^{k'}}{2}\cdot(\lambda^{-1}-\epsilon\lambda)^{2k'},$$

where $-2k' \equiv 2k \ (\ell-1)$ and $0 \le 2k' \le \ell-2$, hence $0 \le k' \le \frac{\ell-3}{2}$.

The sum of all terms except the constant terms will be zero. Therefore, we just have to compute the sum of the constant terms which is

$$\sum_{\lambda\in\mathbb{F}_\ell^\times}\frac{(2k')!}{k'!k'!}(-1)^{k'}\epsilon^{k'} = \frac{(2k')!}{k'!k'!}(-1)^{k'+1}\epsilon^{k'}. \tag{18}$$

This is non-zero since $2k' < \ell$ for all values of $k'$, hence (18) is non-zero in $\mathbb{F}_\ell$. □

This concludes the proof of Theorem 1.

## 4. Cartan subgroup case

In this section, we generalize Merel's conjecture to Cartan subgroups and give a proof by generalizing the methods in Section 3. A new feature is that the conjectural explicit intertwining operator is now a linear combination of double coset operators (rather than a single double coset operator) whose coefficients we are able to make explicit.

Define $\gamma_{(0,\infty)} := \mathbb{F}_\ell^\times\sqrt{\epsilon} \subseteq \mathfrak{C}_\ell$, which can be thought of as a path in $\mathfrak{C}_\ell$ from 0 to $\infty$. Given an ordered pair $(a, b)$, there is a $g \in G$ by Lemma 5 such that $(a, b) = (g(0), g(\infty))$, which is unique up to multiplication on the right by $C$. Thus, we may define

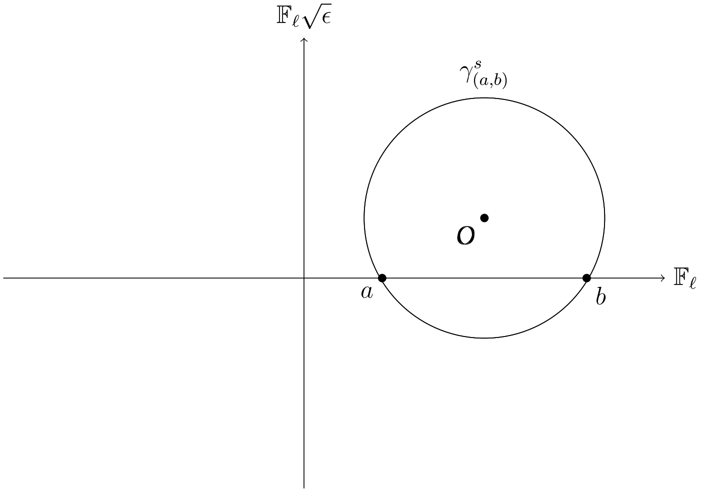

**Fig. 2.** A visual depiction of the path $\gamma^s_{(a,b)}$ in $\mathfrak{C}_\ell$.

$$\gamma_{(a,b)} := g(\gamma_{(0,\infty)}), \tag{19}$$

using the action of $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathfrak{C}_\ell$. The subset $\gamma_{(a,b)} \subseteq \mathfrak{C}_\ell$ can be thought of as a path in $\mathfrak{C}_\ell$ from $a$ to $b$.

**Definition 17.** For $s \in \mathbb{F}_\ell^\times$, define $\gamma^s_{(0,\infty)}$ to be $\left\{(\lambda s + \lambda\sqrt{\epsilon}, 1)^t : \lambda \in \mathbb{F}_\ell^\times\right\} \subseteq \mathfrak{C}_\ell$. This is a path in $\mathfrak{C}_\ell$ which is a line with slope $s^{-1}$.

By Lemma 5, the path in $\mathfrak{C}_\ell$ from $a$ to $b$ with parameter $s$ is defined as

$$\gamma^s_{(a,b)} := g(\gamma^s_{(0,\infty)}) = \left\{g(\lambda s + \lambda\sqrt{\epsilon}) : \lambda \in \mathbb{F}_\ell^\times\right\}, \tag{20}$$

where $g = \begin{pmatrix} b & a \\ 1 & 1 \end{pmatrix}$, which is represented by an equation defined in the next lemma.

**Lemma 18.** *The quadratic equation*

$$\left(x - \frac{a+b}{2}\right)^2 - \epsilon\left(y - \frac{s(b-a)}{2\epsilon}\right)^2 = \frac{(\epsilon - s^2)(a-b)^2}{4\epsilon}, \tag{21}$$

*gives the path $\gamma^s_{(a,b)}$ with coordinates (see Fig. 2)*

$$x = \frac{(b\lambda s + a)(\lambda s + 1) - b\lambda^2\epsilon}{(\lambda s + 1)^2 - \lambda^2\epsilon}, \tag{22}$$

$$y = \frac{\lambda(b-a)}{(\lambda s + 1)^2 - \lambda^2\epsilon}, \tag{23}$$

$$y/(x-b) = \mu = -\lambda/(1 + s\lambda). \tag{24}$$

**Proof.** The elements in $\gamma^s_{(a,b)}$ are given by $z = g(\lambda s + \lambda\sqrt{\epsilon})$, where $g = \begin{pmatrix} b & a \\ 1 & 1 \end{pmatrix}$ and $\lambda \in \mathbb{F}_\ell^\times$; writing $z$ as a fraction and then rationalizing it, we obtain:

$$\frac{(b\lambda s + a) + b\lambda\sqrt{\epsilon}}{(\lambda s + 1) + \lambda\sqrt{\epsilon}} = \frac{(b\lambda s + a)(\lambda s + 1) - b\lambda^2\epsilon}{(\lambda s + 1)^2 - \lambda^2\epsilon} + \sqrt{\epsilon}\frac{\lambda(b - a)}{(\lambda s + 1)^2 - \lambda^2\epsilon}.$$

Therefore, $z = x + y\sqrt{\epsilon}$, where the $x, y$ are given by (22)–(24), which we may verify satisfy equation (21) (this was found by solving for an undetermined conic with the given parametrization).

The formulae (22)–(24) also give a parametrization of the conic in (21) (in particular, $\mu$ gives a parametrization, which is a Möbius transformation of $\lambda$); thus every $(x, y) \in \mathbb{F}_\ell \times \mathbb{F}_\ell^\times$ satisfying (21) corresponds to an element in $\gamma^s_{(a,b)}$. □

For each $s \in \mathbb{F}_\ell^\times$, we define the linear operator $H_s$ by:

$$\begin{aligned} H_s : \mathbb{Q}[\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta] &\to \mathbb{Q}[\mathfrak{C}_\ell] \\ (a, b) &\longmapsto \sum_{x \in \gamma^s_{(a,b)}} x. \end{aligned} \tag{25}$$

**Lemma 19.** *The map $H_s : \mathbb{Z}[\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta] \to \mathbb{Z}[\mathfrak{C}_\ell]$ defined in (25) coincides with the double coset operator $C \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} C' : \mathbb{Z}[G/C] \to \mathbb{Z}[G/C']$ and is hence a $\mathbb{Z}[G]$-module homomorphism.*

**Proof.** For $g = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$, we have that

$$C \cap gC'g^{-1} = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} : \alpha \in \mathbb{F}_\ell^\times \right\}.$$

Thus, from Lemma 3, we have that

$$C \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} C' = \cup_{\alpha \in \mathbb{F}_\ell^\times} \begin{pmatrix} \alpha & \alpha s \\ 0 & 1 \end{pmatrix} C'.$$

The $\mathbb{Z}[G]$-module homomorphism from $\mathbb{Z}[G/C] \to \mathbb{Z}[G/C']$ induced by $CgC'$ from (1) is then seen to be the map $H_s$ under the bijections (4)–(5). □

### *4.1. Coordinates for $G/C$ and $G/C'$*

We need more convenient coordinates to represent elements in (a certain subset of) $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta$ and $\mathfrak{C}_\ell$, where we recall $\mathbb{P}^1(\mathbb{F}_\ell) \times \mathbb{P}^1(\mathbb{F}_\ell) \setminus \Delta$ is in bijection with $G/C$, and $\mathfrak{C}_\ell$ is in bijection with $G/C'$.

**Lemma 20.** *Let $\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta$ and $S = \{(t,t') : t \in \mathbb{F}_\ell, t' \in \mathbb{F}_\ell^\times\}$. Then there is a bijection between the sets $\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta$ and $S$ given by:*

$$(a,b) \mapsto (a+b, a-b).$$

**Proof.** The inverse map is given by $a = \frac{t+t'}{2}$ and $b = \frac{t-t'}{2}$. □

**Lemma 21.** *Let $\mathfrak{C}_\ell$ and $S' = \{(T,T') : T \in \mathbb{F}_\ell, T' \in \mathbb{F}_\ell^\times\}$. Then there is a bijection between the sets $\mathfrak{C}_\ell$ and $S'$ given by:*

$$x + \sqrt{\epsilon}y \mapsto (2x, y).$$

**Proof.** The inverse map is given by $z = \frac{T}{2} + \sqrt{\epsilon}T'$. □

### *4.2. Proof of Theorem 2*

By Lemma 19, $\psi$ is a $\mathbb{Q}[G]$-module homomorphism. To prove Theorem 2, it suffices to prove that the restriction

$$\psi \mid_{\mathbb{Q}[\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta]} : \mathbb{Q}[\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta] \to \mathbb{Q}[\mathfrak{C}_\ell], \tag{26}$$

is an isomorphism of $\mathbb{Q}$-vector spaces.

Using the bijections given by Lemma 20 and Lemma 21, to prove (26) is equivalent to proving that

$$\psi : \mathbb{Q}[S] \to \mathbb{Q}[S'],$$

is an isomorphism of $\mathbb{Q}$-vector spaces, where $\psi$ is the same map as $\psi \mid \mathbb{Q}[\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta]$ under identifications given by the two bijections $\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta \leftrightarrow S$ and $\mathfrak{C}_\ell \leftrightarrow S'$.

Recall the equation giving the path $\gamma^s_{(a,b)}$ from $a$ to $b$ with parameter $s$ is

$$\left(x - \frac{a+b}{2}\right)^2 - \epsilon\left(y - \frac{s(b-a)}{2\epsilon}\right)^2 = \frac{(\epsilon - s^2)(a-b)^2}{4\epsilon},$$

by Lemma 18. By the bijections $\mathbb{F}_\ell \times \mathbb{F}_\ell \setminus \Delta \leftrightarrow S$ and $\mathfrak{C}_\ell \leftrightarrow S'$, this equation becomes

$$(T-t)^2 = t'^2 + 4\epsilon T'^2 + 4sT't', \tag{27}$$

in the new coordinates from Lemma 20 and Lemma 21. Hence, the matrix of $H_s$ restricted to $\mathbb{Q}[S]$ with respect to the basis $S$ is given by $(a_{(t,t'),(T,T')}(s))$, where

$$a_{(t,t'),(T,T')}(s) = \begin{cases} 1 & \text{if } (T-t)^2 = t'^2 + 4\epsilon T'^2 + 4sT't', \\ 0 & \text{otherwise.} \end{cases} \tag{28}$$

The above matrix is an $(\ell-1)\times(\ell-1)$ matrix $(X_{t',T'}(s))$, with entries being the $\ell\times\ell$ matrices $((X_{t',T'}(s))_{t,T})$, where

$$(X_{t',T'}(s))_{t,T} = \begin{cases} 1 & \text{if } (T-t)^2 = t'^{\,2} + 4\epsilon T'^{\,2} + 4sT't', \\ 0 & \text{otherwise.} \end{cases}$$

**Remark 22.** At this point in the proof, we index the entries of the matrices using the variables $T, t \in \mathbb{F}_\ell$ and $T', t' \in \mathbb{F}_\ell^\times$. The ordering for $T', t'$ is specified in the paragraph before Lemma 24, and for $T, t$, we use the least non-negative residue.

Recall $D$ is the matrix which permutes columns of the $\ell\times\ell$ identity matrix according to the cycle $(1\,2\,3\cdots\ell)$.

**Lemma 23.** *We have that*

$$X_{t',T'}(s) = \sum_{v^2 = t'^{\,2} + 4\epsilon T'^{\,2} + 4sT't'} D^v.$$

**Proof.** If $t'^{\,2} + 4\epsilon T'^{\,2} + 4sT't'$ is not square in $\mathbb{F}_\ell$, then $X_{t,T}(s)$ is a zero matrix due to 0 entries. Therefore, $X_{t',T'}(s) = \sum_{v^2=t'^{\,2}+4\epsilon T'^{\,2}+4sT't'} D^v = 0$.

If $t'^{\,2} + 4\epsilon T'^{\,2} + 4sT't' = v^2$ is a square in $\mathbb{F}_\ell$, then $T - t = \pm v$ and

$$(X_{t',T'})_{t,T}(s) = \begin{cases} 1 & \text{if } T = t \pm v, \\ 0 & \text{otherwise.} \end{cases}$$

In this case, $X_{t',T'}(s)$ coincides with $\sum_{v^2=t'^{\,2}+4\epsilon T'^{\,2}+4sT't'} D^v$. □

Arguing similarly as in the discussion preceding Lemma 12, we obtain that each block $X_{t',T'}(s)$ may be replaced by the element $\sum_{v^2=t'^{\,2}+4\epsilon T'^{\,2}+4sT't'} 1 \in \mathbb{F}_\ell$, after identifying it with an element of $\mathbb{Z}[\zeta]$ and reducing modulo $\mathfrak{L}$, yielding a matrix $(\overline{X}_{t',T'}(s))$ with entries in $\mathbb{F}_\ell$.

We label $t', T'$ as $t' = g^i$ and $T' = g^j$ for $0 \le i, j \le \ell - 2$, where $g \in \mathbb{F}_\ell^\times$ is a primitive root. This gives us a new matrix denoted by $(X_{i,j}(s))$ which is given by

$$X_{i,j}(s) = \sum_{v^2 = g^{2i} + 4\epsilon g^{2j} + 4sg^{i+j}} 1.$$

**Lemma 24.** *The matrix $X_{i,j}(s)$ is a $(\ell-1)\times(\ell-1)$ circulant matrix.*

**Proof.** This follows since

$$X_{i,j}(s) = \sum_{v^2=g^{2i}+4\epsilon g^{2j}+4sg^{i+j}} 1 = \sum_{v^2=g^2(g^{2(i-1)}+4\epsilon g^{2(j-1)}+4sg^{i+j-2})} 1 = X_{i-1,j-1}(s),$$

where the indices $i, j$ are taken modulo $\ell - 1$. □

Let $a_j(s) = X_{0,j}(s)$ and $\omega = g \in \mathbb{F}_\ell^\times$. Remark, $X_{0,j}(s) = a_j(s)$ is equal to the number of solutions of $v^2 = 1 + 4\epsilon g^{2j} + 4sg^j$.

The eigenvalue of $X_{i,j}(s)$ for $0 \leq k \leq \ell - 2$ can be calculated as (see Proposition 14):

$$\begin{aligned}\sum_{j=0}^{\ell-2} a_j(s)\omega^{kj} &= \sum_{j=0}^{\ell-2} a_j(s)(g^k)^j = \sum_{j=0}^{\ell-2}\left(\sum_{v^2=1+4\epsilon g^{2j}+4sg^j} 1\right)(g^k)^j \\ &= \sum_{j=0}^{\ell-2}\sum_{v^2=1+4\epsilon g^{2j}+4sg^j} g^{kj} = \sum_{\lambda\in\mathbb{F}_\ell^\times} y(\lambda)^k = \sum_{\lambda\in\mathbb{F}_\ell^\times}\frac{\lambda^k(a-b)^k}{((\lambda s+1)^2-\lambda^2\epsilon)^k}. \qquad (29)\end{aligned}$$

Here, $a_j(s) = X_{0,j}(s)$, which corresponds to $t' = a - b = 1$. In the second last equality above, we use $y = T' = g^j$ and the parametrization in Lemma 18.

We now consider a linear combination $\sum_{s=1}^{\ell-1}\delta_s H_s : \mathbb{Q}[\mathbb{P}^1(\mathbb{F}_\ell)\times\mathbb{P}^1(\mathbb{F}_\ell)\setminus\Delta] \to \mathbb{Q}[\mathfrak{C}_\ell]$ of the maps $H_s$ where $\delta_s \in \mathbb{Z}$. Note that a linear combination of circulant matrices is circulant. Hence, the eigenvalue for $k$ of $\sum_{s\in\mathbb{F}_\ell^\times}\delta_s X_{i,j}(s)$ is thus given by $\sum_{j=0}^{\ell-2} b_j\omega^{kj}$, where $b_j = \sum_{s=1}^{\ell-1}\delta_s a_j(s)$. Then, we have that

$$\begin{aligned}\sum_{j=0}^{\ell-2} b_j\omega^{kj} &= \sum_{j=0}^{\ell-2}\left(\sum_{s\in\mathbb{F}_\ell^\times}\delta_s a_j(s)\right)\omega^{kj} = \sum_{s\in\mathbb{F}_\ell^\times}\delta_s\sum_{j=0}^{\ell-2} a_j(s)\omega^{kj} \\ &= \sum_{s\in\mathbb{F}_\ell^\times}\delta_s\sum_{\lambda\in\mathbb{F}_\ell^\times} y(\lambda,s)^k = \sum_{\lambda\in\mathbb{F}_\ell^\times}\sum_{s\in\mathbb{F}_\ell^\times}\delta_s y(\lambda,s)^k \\ &= \sum_{s\in\mathbb{F}_\ell^\times}\delta_s\sum_{\lambda\in\mathbb{F}_\ell^\times}\left(\frac{\lambda}{(\lambda s+1)^2-\epsilon\lambda^2}\right)^k.\end{aligned}$$

**Lemma 25.** *Let $\eta \in \{0,1\}$. We have that*

$$\sum_{s\in\mathbb{F}_\ell^\times} s^{-\eta}\sum_{\lambda\in\mathbb{F}_\ell^\times}\left(\frac{\lambda}{(\lambda s+1)^2-\epsilon\lambda^2}\right)^k \quad \begin{cases}\neq 0 & \text{if } k-\eta \text{ is even,}\\ = 0 & \text{if } k-\eta \text{ is odd.}\end{cases} \qquad (30)$$

**Proof.** Choose $k' \in \mathbb{Z}$ such that $k \equiv -k' \ (\ell - 1)$ and $0 \leq k' \leq \ell - 2$. Note $k$ and $k'$ have the same parity. Then

$$\begin{aligned}&\sum_{s\in\mathbb{F}_\ell^\times} s^{-\eta}\sum_{\lambda\in\mathbb{F}_\ell^\times}\left(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\right)^{-k} \\ &= \sum_{s\in\mathbb{F}_\ell^\times} s^{-\eta}\sum_{\lambda\in\mathbb{F}_\ell^\times}\left(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\right)^{k'},\end{aligned}$$

where

$$\begin{aligned}
&\left(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\right)^{k'} \\
&\quad = \left(\frac{\lambda^2 s^2+2\lambda s+1-\epsilon\lambda^2}{\lambda}\right)^{k'} \\
&\quad = (\lambda s^2+2s+\lambda^{-1}-\epsilon\lambda)^{k'} \\
&\quad = (\lambda(s^2-\epsilon)+2s+\lambda^{-1})^{k'}.
\end{aligned}$$

Here, we just need the constant terms of $\left(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\right)^{k'}$ as the other terms are powers of $\lambda$ not divisible by $\ell-1$, and the sum of these powers is zero in $\mathbb{F}_\ell$. Now, the constant term of

$$(\lambda(s^2-\epsilon)+2s+\lambda^{-1})^{k'}$$

is equal to

$$\sum_{i=0}^{\left\lfloor\frac{k'}{2}\right\rfloor} \frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon).$$

Thus, we obtain that

$$\sum_{s\in\mathbb{F}_\ell^\times} s^{-\eta}\sum_{\lambda\in\mathbb{F}_\ell^\times}\left(\frac{(\lambda s+1)^2-\epsilon\lambda^2}{\lambda}\right)^{-k} = \sum_{s\in\mathbb{F}_\ell^\times} s^{-\eta}\sum_{i=0}^{\left\lfloor\frac{k'}{2}\right\rfloor}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i.$$

If $k-\eta$ is even, we have that

$$\begin{aligned}
&\sum_{s\in\mathbb{F}_\ell^\times} s^{-\eta}\sum_{i=0}^{\left\lfloor\frac{k'}{2}\right\rfloor}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i \qquad (31)\\
&\quad = \sum_{s\in\mathbb{F}_\ell^\times} s^{-\eta}\sum_{i=0}^{\frac{k'}{2}}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i \\
&\quad = \sum_{i=0}^{\left\lfloor\frac{k'}{2}\right\rfloor}\sum_{s\in\mathbb{F}_\ell^\times}\frac{k'!}{i!i!(k'-2i)!}(2s)^{k'-2i}(s^2-\epsilon)^i s^{-\eta} \\
&\quad = \epsilon^{\frac{k'}{2}}\frac{k'!}{\frac{k'}{2}!\frac{k'}{2}!} \neq 0.
\end{aligned}$$

The last equality holds because the only power of $s$ whose exponent is divisible by $\ell-1$ happens when $i=\lfloor k'/2\rfloor$.

On the other hand, if $k-\eta$ is odd, then (31) is zero in $\mathbb{F}_\ell$ because there are no powers of $s$ whose exponent is divisible by $\ell-1$. This proves the lemma. □

**Corollary 26.** *Let $\alpha_s, \beta_s \in \mathbb{Z}$ be as in Theorem 2. Then the matrix $\sum_{s=1}^{\ell-1}(\alpha_s+\beta_s)X_{i,j}(s)$ has non-zero eigenvalue in $\mathbb{F}_\ell$ for all $0 \leq k \leq \ell-2$ in its circulant determinant formula.*

**Proof.** By Lemma 25, the eigenvalue of $\sum_{s=1}^{\ell-1}(\alpha_s+\beta_s)X_{i,j}(s)$ is non-zero in $\mathbb{F}_\ell$, since the eigenvalue of $\sum_{s=1}^{\ell-1}(\alpha_s+\beta_s)X_{i,j}(s)$ for $k$ is the sum of the eigenvalues for $k$ of $\sum_{s=1}^{\ell-1}\alpha_s X_{i,j}(s)$ and $\sum_{s=1}^{\ell-1}\beta_s X_{i,j}(s)$. □

The above corollary implies that determinant of $\sum_{s=1}^{\ell-1}(\alpha_s+\beta_s)H_s$ is non-zero. This concludes the proof of Theorem 2.

## 5. Relations between Jacobians of certain modular curves

In this section, we summarize some applications of the main results of this paper to Jacobians of modular curves.

Let $X = X(\ell)$ denote the modular curve of full level $\ell$ structure which has the structure of a projective algebraic curve over $\mathbb{Q}$ for $\ell \geq 3$ (cf. [8, p. 241] or [6, Theorem 3.7.1]).

The group $G = \mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $X$ and the quotients $X_H := X/H$ by subgroups $H$ of $G$ (which contain $-1$) exist as projective algebraic curves over $\mathbb{Q}$ [8, p. 244] and [6, Proposition 8.1.6].

Let $J$ denote the Jacobian of $X$ and $J_H$ denote the Jacobian of $X_H$.

**Proposition 27.** *Let $\sigma : \mathbb{Z}[G/H'] \to \mathbb{Z}[G/H]$ be a $\mathbb{Z}[G]$-module homomorphism. Then $\sigma$ induces a homomorphism of Jacobians $\sigma^* : J_H \to J_{H'}$.*

**Proof.** This is proved in [2, Lemma 3.3]. □

**Proposition 28.** *Suppose a cochain complex of $\mathbb{Z}[G]$-modules*

$$\ldots \to \mathbb{Z}[G/H_{i-1}] \to \mathbb{Z}[G/H_i] \to \mathbb{Z}[G/H_{i+1}] \to \ldots$$

*has finite cohomology groups. Then the induced sequence of Jacobians by applying Proposition 27 yields a chain complex*

$$\ldots \leftarrow J_{H_{i-1}} \leftarrow J_{H_i} \leftarrow J_{H_{i+1}} \leftarrow \ldots$$

*with finite homology groups.*

**Proof.** This is proved in [2, Proposition 3.7]. □

Theorems 1 and 2 imply that

$$\mathbb{Q}[G/N] \xrightarrow{\psi^+} \mathbb{Q}[G/N'] \to 0 \tag{32}$$

$$\mathbb{Q}[G/C] \xrightarrow{\psi} \mathbb{Q}[G/C'] \to 0 \tag{33}$$

are exact cochain complexes of $\mathbb{Q}[G]$-modules.

**Proposition 29.** *The following are cochain complexes*

$$\mathbb{Z}[G/N] \xrightarrow{\psi^+} \mathbb{Z}[G/N'] \to 0 \tag{34}$$

$$\mathbb{Z}[G/C] \xrightarrow{\psi} \mathbb{Z}[G/C'] \to 0 \tag{35}$$

*with finite cohomology groups.*

**Proof.** This follows from tensoring the cochain complexes above by $\mathbb{Q}$. If the cohomology groups were not finite, this would contradict the exactness of the cochain complexes in (32)–(33). □

Applying Proposition 28, we obtain:

**Corollary 30.** *The following are chain complexes*

$$0 \to J_{N'} \xrightarrow{\psi^{+*}} J_N \tag{36}$$

$$0 \to J_{C'} \xrightarrow{\psi^*} J_C \tag{37}$$

*with finite homology groups.*

From [3], we have that

$$J_N \sim J_{N'} \times J_B \tag{38}$$

$$J_C \sim J_{C'} \times J_B^2, \tag{39}$$

where $\sim$ denotes the relation of isogeny over $\mathbb{Q}$, and $B$ is the subgroup of upper triangular matrices in $G$. Hence, Corollary 30 describes the main part of the well-known relations between $J_N$ and $J_{N'}$ (resp. $J_C$ and $J_{C'}$) using explicit correspondences.

It is known that $X_C \cong X_0(\ell^2)$ and $X_N \cong X_0(\ell^2)/\langle w_\ell \rangle$, which are the more standard modular curves studied in the literature.

## References

[1] B. Birch, D. Zagier, Personal communication with I. Chen, 2000.

[2] I. Chen, On relations between Jacobians of certain modular curves, J. Algebra 231 (2000) 414–448.

[3] I. Chen, The Jacobians of non-split Cartan modular curves, Proc. Lond. Math. Soc. (3) 77 (1) (1998) 1–38.

[4] H. Darmon, L. Merel, Winding quotients and some variants of Fermat's Last Theorem, J. Reine Angew. Math. 490 (1997) 81–100.

[5] B. de Smit, B. Edixhoven, Sur un résultat d'Imin Chen (French) [On a result of Imin Chen], Math. Res. Lett. 7 (2–3) (2000) 147–153.

[6] N. Katz, B. Mazur, Arithmetic Moduli of Elliptic Curves, Princeton University Press, 1985.

[7] B. Mazur, Rational isogenies of prime degree, Invent. Math. 44 (1978) 129–162.

[8] B. Mazur, A. Wiles, Class fields of abelian extensions of $\mathbb{Q}$, Invent. Math. 76 (1984) 179–330.

[9] J. Neukirch, Algebraic Number Theory, Springer-Verlag, New York, 1999.

[10] M. Rebolledo, C. Wuthrich, A moduli interpretation for the non-split Cartan modular curve, Glasg. Math. J. 60 (2018) 411–434.

[11] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Forms, Princeton University Press, 1971.