Journal of Number Theory 286 (2026) 131–184

Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

General Section

Spectral theory of isogeny graphs

Giulio Codogni *, Guido Maria Lido

Università di Roma Tor Vergata, Italy

ARTICLE INFO

Article history:
Received 29 May 2025
Received in revised form 18 December 2025
Accepted 6 February 2026
Available online 1 April 2026
Communicated by F. Pellarin

Keywords:
Isogeny graphs
Elliptic curves
Isogeny based cryptography
Expander graphs
Modular forms
Hecke operators

ABSTRACT

We consider finite graphs whose vertices are supersingular elliptic curves, possibly with level structure, and edges are isogenies. They can be applied to the study of modular forms and to isogeny based cryptography. The main result of this paper is an upper bound on the absolute values of the eigenvalues of their adjacency matrices, which in particular implies that these graphs are Ramanujan. We also study the asymptotic distribution of the eigenvalues of the adjacency matrices, the number of connected components, the automorphisms of the graphs, and the connection between the graphs and modular forms.

Contents

* Corresponding author.
E-mail addresses: codogni@mat.uniroma2.it (G. Codogni), guidomaria.lido@gmail.com (G.M. Lido).

https://doi.org/10.1016/j.jnt.2026.02.006

1. Introduction

Given two distinct prime numbers p and ℓ, supersingular isogeny graphs are finite graphs whose vertices are isomorphism classes of supersingular elliptic curves defined over a field of characteristic p, possibly enriched with some level structure, and edges are degree ℓ isogeny (see Definitions 1.1 and 1.3). The number of vertices of these graphs grows linearly in p.

Theorems 1.4 and 1.6, our main results, give information about the spectrum of the adjacency matrices of these graphs. They rely on algebraic geometry constructions.

The spectrum of the adjacency matrix is not a complete invariant of a graph. Non-isomorphic graphs whose adjacency matrices have the same spectrum are sometimes called cospectral mates. Spectral graph theory allows to gather important information about the geometry of the graph only out of the spectrum of the adjacency matrix, and this is why our work provides a better understanding of isogeny graphs.

Isogeny graphs were first studied by Mestre [46] in the 80's. His goal was to study modular forms, in particular to compute eigenforms out of eigenvectors of adjacency matrices of isogeny graphs. This approach has been recently made very practical in [17]. Our Theorems 5.5.2, 5.5.5 generalize [46, Theorem 2.1], and we hope they lead to possible extensions of Mestre's "Méthode des graphes", even though an analogue for formula (1) in [46] is needed.

In the 90's people from graph theory were looking for explicit examples of graphs with optimal spectral gap, and consequently optimal expansion constant and mixing time. Surprisingly, classical isogeny graphs, i.e. without level structure, provided such examples! These facts are discussed in Section 1.2, where we also show, as corollary of our main results, that isogeny graphs with level structure also have this property.

More recently, isogeny graphs started to play an important role in cryptography, as many protocols from isogeny based cryptography rely on their features. For instance,

information about the spectrum of isogeny graphs with Borel level structure is used to prove Statistical Zero Knowledge for a proof of knowledge in [8] and for signature schemes in [9,18]. This is discussed in Section 1.3.

1.1. Main definitions and results

The vertices of the graphs we study are supersingular elliptic curves enriched with some torsion data. We start by specifying what kind of data we are interested in.

Definition 1.1 *(Level structure on elliptic curves).* Fix a positive integer N and a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) = \mathrm{Aut}((\mathbb{Z}/N\mathbb{Z})^2)$. Let k be a field where N is invertible. For an elliptic curve E/k, a *level H structure* on E is an isomorphism $\phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$ considered up to composition with an element of H, i.e. two isomorphisms ϕ and ϕ' are equivalent if there exists an element h in H such that $\phi = \phi' \circ h$.

Sometimes level H structures have more explicit interpretations, as illustrated below.

- *Trivial level structure*: when $H = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, there is a unique level structure on every elliptic curve;
- *Borel level structure:* when $H = \{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\}$ is the subgroup of lower triangular matrices, a level H structure is equivalent to the choice of a cyclic subgroup of order N in $E[N]$ (equivalently, Borel level structure can be defined using upper triangular matrices; we prefer the lower ones as they make some computations with modular forms less cumbersome);
- *Full level structure*: when $H = \{\mathrm{Id}\}$, an H structure is equivalent to the choice of a basis of $E[N]$;
- *Split Cartan level structure*: when $H = \{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)\}$, a level structure is equivalent to the choice of an ordered pair of cyclic subgroups $C_1, C_2 < E[N]$ having order N and trivial intersection. This level structure gives a graph isomorphic to a graph with Borel level structure, see Section 2.4, so we will not discuss it in details. If we instead consider $H = \{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)\} \cup \{\left(\begin{smallmatrix} 0 & * \\ * & 0 \end{smallmatrix}\right)\}$, which is equal to the normalizer of $\{\left(\begin{smallmatrix} * & 0 \\ 0 & * \end{smallmatrix}\right)\}$ when N is an odd prime power, an H-level structure corresponds to a non-ordered pair of cyclic subgroups; the corresponding graph is a quotient of the graph with Cartan level structure.
- *Torsion point level structure*: when $H = \{\left(\begin{smallmatrix} * & 0 \\ * & 1 \end{smallmatrix}\right)\}$, a level H structure is equivalent to the choice of a point of order N;
- *Non split Cartan level structure*: when H is a non-split Cartan subgroups of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, which is unique up to conjugation. Details are given [23] and in [52] these structures are interpreted as "necklaces" of subgroups of $E[N]$ for N prime.

Fix (E_1, ϕ_1) and (E_2, ϕ_2), where E_1, E_2 are elliptic curves over a common field k, and ϕ_i is a level H structure on E_i. A morphism $\alpha\colon (E_1, \phi_1) \to (E_2, \phi_2)$ is an isogeny

$\alpha\colon E_1 \to E_2$ such that $\alpha \circ \phi_1 = \phi_2$ as level H structures on E_2, or equivalently such that there exists an element $h \in H$ satisfying $\alpha \circ \phi_1 = \phi_2 \circ h$. The degree of such a morphism is the degree of the corresponding isogeny $E_1 \to E_2$. We call such an α a *morphism, or isogeny, of elliptic curves with level structures*. A morphism is an *isomorphism* if it is an isomorphism at the level of elliptic curves, i.e. it has degree one.

Remark 1.2. In the context pairs (E, ϕ) of elliptic curves with level H structure, if u is an automorphism of E, then the pairs (E, ϕ) and $(E, u \circ \phi)$ are always isomorphic. Nevertheless u does not always define an automorphism of (E, ϕ): it does if and only if

$$\phi^{-1} \circ u \circ \phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \to (\mathbb{Z}/N\mathbb{Z})^2$$

lies in H. In particular, if $\begin{pmatrix} -1 & \\ & -1 \end{pmatrix} \notin H$, then -1 is not an automorphism of (E, ϕ) even though $(E, \phi) \cong (E, -\phi)$.

Definition 1.3 *(Supersingular isogeny graph).* Fix a positive integer N, a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and distinct prime numbers p, ℓ not dividing N.

The isogeny graph with level structure $G = G(p, \ell, H)$ is the directed graph with:

- vertices $V = \{(E_1, \phi_1), \dots, (E_r, \phi_r)\}$ a set of representatives of isomorphism classes of supersingular elliptic curves $E/\overline{\mathbb{F}}_p$ with a level H structure ϕ;
- edges: given vertices (E_i, ϕ_i) and (E_j, ϕ_j), edges between them are degree ℓ morphisms $(E_i, \phi_i) \to (E_j, \phi_j)$, modulo postcomposition by automorphisms of (E_j, ϕ_j).

We denote by $A = (a_{ij})_{i,j}$ the adjacency matrix of G, namely the matrix whose entries a_{ij} are the number of edges $(E_j, \phi_j) \to (E_i, \phi_i)$.

In the context of the above definition, given a vertex (E_i, ϕ_i), taking the kernel of isogenies gives a bijection between cyclic subgroups of cardinality ℓ of $E_i[\ell]$, and edges coming out of the vertex (E_i, ϕ_i), since edges correspond to isogenies up to postcomposition by automorphisms. In particular, there are exactly $\ell+1$ edges coming out of each vertex. The graph does not depend on the choices of the representatives (E_i, ϕ_i).

The graph G might not be connected. For every connected component G_i, consider the vector v_i in $\mathbb{C}^V$ obtained as formal sum of the vertex of G_i. Then $A^t\, v_i = (\ell + 1)v_i$, where ^{t} denotes the transpose. This shows that $\ell+1$ is an eigenvalue of A.

Our first main result gives information about the eigenvalues of A in the cases where H contains the scalar matrices and its image $\det(H) \subset (\mathbb{Z}/N/\mathbb{Z})^\times$ under the determinant is maximal. For example, it covers the case of graphs with Borel, Cartan (both split and non-split) and trivial level structure (which give the classical isogeny graph). In particular, we recover Pizer's result [51, Theorem 1] (see also the detailed discussion in Section 1.4).

Theorem 1.4. *With the notation of Definition 1.3, if H contains the scalar matrices and $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$, then the graph $G(p,\ell,H)$ is connected, its adjacency matrix A is diagonalizable over $\mathbb{R}$, the eigenvalue $\ell+1$ has multiplicity one, and all the other eigenvalues have absolute value smaller than*

$$2\sqrt{\ell} - \left(4\sqrt{\ell}\right)^{-2|V|+3},$$

where $|V|$ is the number of vertices of $G(p,\ell,H)$. In particular, all eigenvalues different from $\ell+1$ are contained in the open Hasse interval $(-2\sqrt{\ell}, 2\sqrt{\ell})$.

When the graph contains pairs (E,ϕ) with non-trivial automorphisms (i.e. automorphisms not induced by $\pm 1 \in \mathrm{Aut}(E)$), the adjacency matrix A is not symmetric.

When $\det(H)$ is strictly contained in $(\mathbb{Z}/N\mathbb{Z})^\times$, we need to introduce some further notations to describe the connected components of the graphs, and their partitions. Let $\mu_N^\times(\overline{\mathbb{F}}_p)$ be the set of primitive N-th root of unity in $\overline{\mathbb{F}}_p$. This is a principal homogeneous space for the right action of $(\mathbb{Z}/N\mathbb{Z})^\times$ given by $\zeta \cdot a = \zeta^a$. The group $\det(H)$ is a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$, so it also acts on $\mu_N^\times(\overline{\mathbb{F}}_p)$ and we can form the quotient $R_H := \mu_N^\times(\overline{\mathbb{F}}_p)/\det(H)$.

Definition 1.5 *(Weil invariant of a level structure).* Consider an elliptic curve with level H structure (E,ϕ). Let w be the Weil pairing on the N-torsion of E and let

$$w(\phi) = w(\phi(\tbinom{1}{0}), \phi(\tbinom{0}{1})).$$

As ϕ is defined only modulo the action of H, the invariant $w(\phi)$ is an element of the quotient R_H. We call this invariant the Weil invariant of the level structure.

The Weil invariant gives an obstruction to $G = G(p,\ell,H)$ being connected: if two vertices v_1, v_2 are connected by a degree ℓ isogeny, then [57, Chapter III, Proposition 8.2] implies that their corresponding Weil invariants are connected by the action of ℓ, i.e. $w(v_2) = w(v_1)^\ell$. Hence in a connected component of G, the Weil invariant has image an orbit of the action of ℓ on R_H. Let $\{C_1, \dots, C_n\}$ be the orbits of ℓ acting on R_H and for each i we denote

$$G_i := w^{-1}(C_i)$$

which is a subgraph of G by the previous argument. Our second main result generalizes Theorem 1.4.

Theorem 1.6. *With the notation of Definition 1.3, let $G = G(p,\ell,H)$ with H any subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, and let $G_1, \dots, G_n$ be the subgraphs of G defined above.*

Connected components *Each G_i is connected, i.e. the graph G has n connected components. Let $\mathcal{N}_H$ be the normalizer of H in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. If p, ℓ and $\det(\mathcal{N}_H)$ together generate $(\mathbb{Z}/N\mathbb{Z})^\times$, then the G_i's are all isomorphic.*

Spectrum of the adjacency matrix *Denote by k the order of ℓ in $(\mathbb{Z}/N\mathbb{Z})^\times/\det(H)$, and by k' the smallest positive integer such that $\ell^{k'}\mathrm{Id} \in H$. The adjacency matrix A_i of G_i is diagonalizable over $\mathbb{C}$ and, for each k-th root of unity ζ, the number $(\ell+1)\zeta$ is an eigenvalue of A_i of multiplicity one. The other eigenvalues of A_i are complex numbers with angle in $\frac{\pi}{k'}\mathbb{Z}$ and absolute value smaller than*

$$2\sqrt{\ell} - \left(4\sqrt{\ell}\right)^{-2(d-k)k'+1},$$

where d is the number of vertices of G_i.

Theorem 1.6 applies to the case of full level structure, where the adjacency matrix has non-real eigenvalues. In this case $\mathcal{N}_H = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, hence all connected components are isomorphic. We also have that $k = k'$ is the multiplicative order of ℓ in $(\mathbb{Z}/N\mathbb{Z})^\times$, and the number of connected components is $n = \varphi(N)/k$, where φ is the Euler totient function.

We can also apply Theorem 1.6 to the isogeny graphs with torsion point level structure, namely $H = \{\left(\begin{smallmatrix} * & 0 \\ * & 1 \end{smallmatrix}\right)\}$. In this case $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$, hence G is connected and $k = 1$. One might have $k' > 1$, and indeed Corollary 1.14 implies that for p big enough the adjacency matrix has non-real eigenvalues.

Remark 1.7 *(Multipartite graphs).* Given a finite connected directed graph $G = (V, E)$, a *k-multipartition* is a partition of V into k disjoint subsets V_j such that vertices of V_j are connected only to vertices of $V_{j+1 \pmod k}$. A 2-partite graph is called bipartite. When G is d-regular, this is related to the spectrum of the adjacency matrix A of G in the following way. Let $u_j = \sum_{v \in V_j} v$, and U the span of $\{u_1, \dots, u_k\}$ in $\mathbb{C}^V$. Then U is stabilized by A^t, and A^t restricted to U acts as d times a cyclic permutation, hence the spectrum of A contains d times the group of k-th roots of unity.

The Weil invariant gives a k-multipartition of the vertices of G_i, and by the above discussion this is a k-multipartition of G_i; the existence of this partition implies the existence of the eigenvalues $(\ell+1)\zeta$'s appearing in the statement of Theorem 1.6. Theorem 1.6 also says that there are no other eigenvalues of absolute value equal to $\ell+1$, hence this partition can not be refined.

Organization of the paper

In Section 2, we reduce the proof of Theorems 1.4 and 1.6 to Theorem 2.3.8. Along the way, we prove a few elementary results about isogeny graphs.

Sections 3 and 4 are devoted to set-up a more general framework to study isogeny graphs, and to prove Theorem 2.3.8 (= Theorem 4.18). These sections rely on more advanced algebraic geometry notions.

In Section 5 we develop the connection between isogeny graphs and modular forms. This connection is of independent interest, and it is used to prove Corollary 1.14. Throughout the paper, we keep track of automorphisms of the graphs. We relate them to automorphisms of modular curves and modular forms, such as the Fricke and Atkin-Lehner automorphisms. These results are not used in the proof of our main theorems, but we think they could be useful for further developments.

1.2. Ramanujan graphs and expander sequences

In this section we discuss the implication of our results from the point of view of graph theory. We refer the reader to the textbooks [19,37,58], the papers [11,34] and references therein for detailed discussions of the concepts introduced here.

Let G be a d-regular non-bipartite (see Remark 1.7) connected finite graph with symmetric adjacency matrix A. The spectrum of A contains the eigenvalue d, called trivial eigenvalue, with multiplicity one. All other eigenvalues are called non-trivial and are contained in the interval $(-d, d)$ ([19, Proposition 1.1.2]). The *spectral gap* is the minimum of $d - |\lambda|$, where λ runs among all non-trivial eigenvalues. Notice that our main results give lower bounds on the spectral gap of isogeny graphs. Lower bounds on the spectral gap can be used, among the other things, to bound the diameter, the expansion constant and the mixing time of a graph, see [19,37].

A graph is called *Ramanujan* if all non-trivial eigenvalues of A are contained in the Hasse interval $[-2\sqrt{d-1}, 2\sqrt{d-1}]$. The Alon-Boppana inequality says that there exists a constant $c_d > 0$, depending only on d, such that for every d-regular graphs with n vertices there exists a non-trivial eigenvalue with absolute value at least $2\sqrt{d-1} - c_d/(\log(n))^2$; in a more colloquial language, it says that Ramanujan graphs have the largest possible spectral gap among big graphs ([37, Section 5.2], [19, Section 1.3], [11, Introduction]).

A key result, conjectured by Alon and proven in [34] and [11], says the following: fixing a strictly positive real number ε, using the uniform distribution on the set of d-regular simple graphs with n vertices, the probability that all non trivial eigenvalues of the adjacency matrix lie in the interval $[-2\sqrt{d-1} - \varepsilon, 2\sqrt{d-1} + \varepsilon]$ tends to 1 when n tends to infinity. In other words, a random graph is close to be Ramanujan. In [38], it is shown that, for n big enough, approximately 69% of the d-regular graphs are Ramanujan. It is however challenging to construct examples of Ramanujan graphs, as discussed for instance in [11, Introduction]. Our results give the following.

Corollary 1.8. *With the notation of Definition 1.3, if p is congruent to 1 modulo 12, H contains $\ell\cdot\mathrm{Id}$, and $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$, then the isogeny graph $G(p, \ell, H)$ is a Ramanujan graph.*

The first three conditions guarantee that the adjacency matrix is symmetric, see Proposition 2.2.2; if we drop them, our main results say that the graphs are Ramanujan

in some generalized sense. Corollary 1.8 can be applied for instance to isogeny graphs with Borel level structure.

With the same spirit, people have looked at *expander sequences of graphs*. A sequence of d-regular connected finite graphs G_i is an expander sequence if the adjacency matrices A_i are symmetric, the number of vertices tends to infinity, and there exists a constant $\varepsilon > 0$ independent of i such that the spectral gap of G_i is at least ε for every i. We again refer to [19,37] and references therein for a detailed discussion. Observe that in [19,37] the definition is given in terms of the expansion constant; our definition in terms of spectral gap is equivalent to the classical one because of the Cheeger inequality ([37, Sections 4.4 and 4.5] and [19, Section 1.2]). The importance of constructing explicit examples is highlighted for instance in [37, Section 2.1] or [41]. The following corollary of Theorem 1.6 and Proposition 2.2.2 provides many new examples of expander sequences of graphs.

Corollary 1.9. *Fix a prime ℓ and a sequence of graphs $\{G_i\} = \{G(p_i, \ell, H_i)\}$ with $p_i \equiv 1 \pmod{12}$ and $H_i < \mathrm{GL}_2(\mathbb{Z}/N_i\mathbb{Z})$ a subgroup containing $\ell \cdot \mathrm{Id}$, with determinant $\det(H_i) = (\mathbb{Z}/N_i\mathbb{Z})^\times$, and such that $[\mathrm{GL}_2(\mathbb{Z}/N_i\mathbb{Z}) : H_i] \cdot p_i$ tends to infinity. Then, $\{G_i\}$ is an expander sequence of graphs.*

The first example where Corollary 1.9 can be applied is the classical sequence of isogeny graphs: $N_i = 1$ for every i, and p_i grows. New examples are for instance when p_i is fixed and $[\mathrm{GL}_2(\mathbb{Z}/N_i\mathbb{Z}) : H_i] \to \infty$, which happens e.g. if N_i grows, and H_i is of a fixed type such as Borel or Cartan; or when p_i grows, N_i and H_i can be anything.

Again, if we drop the condition that p_i is congruent to 1 modulo 12, and that H_i contains ℓ, then the adjacency matrix might not be symmetric and the sequence is expander in a generalized sense.

Consider the largest number $\eta = \eta(p, \ell, H)$ such that the non-trivial eigenvalues of the adjacency matrix of $G(p, \ell, H)$ are contained in the Hasse interval shrunk by η, i.e. the interval $[-2\sqrt{\ell} + \eta, 2\sqrt{\ell} - \eta]$. In other words, we are interested in the gap

$$\eta(p, \ell, H) := 2\sqrt{\ell} - \max_{\lambda} |\lambda| \,, \tag{1.10}$$

where the maximum is taken over all non-trivial eigenvalues of the adjacency matrix of $G(p, \ell, H)$. The estimates in our Theorems 1.4 and 1.6 can be rephrased as lower bounds on η. Alon-Boppana inequality implies that there is a constant c_ℓ which depends only on ℓ such that $\eta(p, \ell, H) \leq c_\ell \log(|V(p, \ell, H)|)^{-2}$, where $V(p, \ell, H)$ is the set of vertexes of the graph $G(p, \ell, H)$. Numerical experiments from Appendix B show that our bounds are not sharp. Let us formulate the following general questions, which are open and interesting already in the case without level structure.

Question 1.11. *With the notations of Corollary 1.8, fix ℓ, N, and a subgroup H of level N. Let $v(p)$ be the number of vertices of $G(p, \ell, H)$, and $\eta(p) = \eta(p, \ell, H)$. What are good*

lower bounds for $\eta(p)$? What is the asymptotic of $\eta(p)$? Does this sequence achieve the Alon-Boppana bound (i.e. $\lim_{p\to\infty}\eta(p)\log(v(p))^2$ is equal to a positive constant)?

1.2.1. Non-backtracking random walks and mixing time

Random walks can be used to generate probability distributions on the vertices of a graph: one starts from a given distribution π and, after a length k random walk, the end vertex has distribution $\pi^{(k)}$. A distribution is stationary if it does not change after random walk. By general graph theory, if the graph is connected and not multipartite, the sequence $\pi^{(k)}$ converges to the unique stationary distribution; a general reference is [37]. The mixing time measures the speed of convergence, i.e. the number k of steps such that $\pi^{(k)}$ is distant at most a certain ε from the stationary distribution.

Motivated by applications to isogeny based cryptography, in Proposition 1.12 we give an upper bound for the mixing time of non-backtracking random walks on isogeny graphs.

Let us first recall the definition of non-backtracking walk on isogeny graphs. Assume that $\ell\cdot\mathrm{Id}\in H$; for each edge $(E,\phi)\xrightarrow{e}(E',\phi')$ we can choose an edge $(E',\phi')\xrightarrow{\overline{e}}(E,\phi)$ by choosing an isogeny α representing e and taking $\overline{e}=[\hat{\alpha}]$, where $\hat{\alpha}$ is the dual isogeny of α. A walk is non-backtracking if an edge e is never followed by $\overline{e}$.

(Note that if $j(E')=0,1728$ the definition of $\overline{e}$ is not necessarily canonical: if $u\in\mathrm{Aut}(E',\phi')$ is not $u\pm1$, the isogeny $\alpha\circ u$ still represents e, but $\hat{\alpha}$ and $\widehat{\alpha\circ u}=\hat{\alpha}\circ\hat{u}$ might have different kernels, hence correspond to different edges; more details in [8, Section 3.3].)

In this set-up, if we further assume that $\det(H)=(\mathbb{Z}/N\mathbb{Z})^\times$ so that $G(p,\ell,H)$ is connected and not multipartite, the distribution $\pi^{(k)}$ obtained after a non-backtracking random walk always converges to a stationary distribution s when k goes to infinity. The Borel case is treated in details in [8]: as consequence of the Ramanujan property of the graph, [8, Theorem 11] shows that the speed of convergence of $\pi^{(k)}$ to s is $O(\frac{k}{\ell^{k/2}})$, and compute the precise constants.

In our Theorem 1.6 we show that the non-trivial part of the spectrum is contained in an interval $[-2\sqrt{\ell}+\eta,2\sqrt{\ell}-\eta]$ for $\eta=(4\sqrt{\ell})^{-2|V|+3}$, see also (1.10), Question 1.11 and Appendix B. This result is stronger than the Ramanujan property, and it implies that the rate of convergence of $\pi^{(k)}$ to the stationary distribution is $O(\frac{1}{\ell^{k/2}})$. We give a precise statement.

Proposition 1.12. *In the notation of Definition 1.3, suppose that H contains $\ell\cdot\mathrm{Id}$ and that $\det(H)=(\mathbb{Z}/N\mathbb{Z})^\times$. Let G be the graph $G(p,\ell,H)$ with set of vertices V.*

Let s be the probability distribution on V, where each vertex (E,ϕ) has probability proportional to $|\mathrm{Aut}(E,\phi)|^{-1}$. Then s is a stationary distribution and for each probability distribution π on V, the distribution $\pi^{(k)}$ defined above converges to s. More precisely for $p\neq2,3$ we have the following inequality

$$d_{TV}(\pi^{(k)},s)\leq\frac{1}{4}\sqrt{(p-1)[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}):H]}\cdot\min\left(\left(\frac{\eta}{\sqrt{\ell}}-\frac{\eta^2}{4\ell}\right)^{-\frac{1}{2}},\frac{(\ell+1)(k+1)-2}{(\ell+1)}\right)\cdot\frac{1}{\sqrt{\ell^k}},$$

where $d_{TV}(p_1,p_2)=\frac{1}{2}\sum_{v\in V}|p_1(v)-p_2(v)|$ *is the total variation distance and* $\eta>0$ *is such that all the non-trivial eigenvalues of* G *lie in* $[-2\sqrt{\ell}+\eta, 2\sqrt{\ell}-\eta]$.

For $p=2$, *respectively* $p=3$, *the above inequality is true after substituting "*$\leq \frac{1}{4}\dots$*" with "*$\leq \frac{1}{2}\dots$*", respectively with "*$\leq \frac{1}{\sqrt{2}}\dots$*".*

The proof follows the same strategy as in [8, Theorem 11], the main difference is that we bound the value in Equation (5) in [8] not only as in Equation (6), but also using the inequalities $|\sin((k+1)\theta)|\leq 1$, $|\sin((k-1)\theta)|\leq 1$ and

$$|\sin(\theta)|=\sqrt{1-(\cos\theta)^2}=\sqrt{1-\tfrac{\lambda_i^2}{4\ell}}\geq\sqrt{1-\tfrac{(2\sqrt{\ell}-\eta)^2}{4\ell}}\,.$$

To connect with the notation in [8, Theorem 11], the quadratic form Q in that theorem is the same as $\frac{1}{2}H$ here (see Equation (2.2.1)) and the constants K, M, related to $||\cdot||_{TV}$ and Q, can be computed or bounded as in [8, Theorem 7]:

$$K=\left(\tfrac{p-1}{12}[\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}):H]\right)^{-1/2}\,,\qquad M\leq\left(\max_i\tfrac{|\mathrm{Aut}(E_i,\phi_i)|}{2}\right)^{1/2}\,,$$

so that $M\leq\sqrt{3}$ for $p\neq 2,3$, $M\leq\sqrt{6}$ for $p=3$ and $M\leq\sqrt{12}$ for $p=2$.

1.2.2. Asymptotic distribution of the eigenvalues

Let us now look at the distribution of all eigenvalues, the bulk of the spectrum following the terminology of [37, Section 7.1], see also [56, Section 8]. Given a sequence G_i of graphs as above and an angle θ, we introduce the probability measure

$$\mu(G_i,\theta):=\frac{1}{|\sigma(A_i,\theta)|}\sum_{\lambda\in\sigma(A_i,\theta)}\delta_\lambda\,,$$

where $\sigma(A_i,\theta)$ is the set of eigenvalues of the adjacency matrix A_i with phase θ or $\theta+\pi$, and δ_λ is a Dirac mass at λ; of course the definition makes sense only if $|\sigma(A_i,\theta)|\neq 0$. The limits of the sequences $\{\mu(G_i,\theta)\}$, if they exist, give the asymptotic distribution of the spectrum of G_i. If all eigenvalues of A_i are real, we omit the dependence from θ.

Let us also introduce the Kesten–McKay measure (also known as Kesten–McKay law or distribution)

$$\mu_\ell:=\frac{\ell+1}{\pi}\frac{\sqrt{\ell-x^2/4}}{\ell(\ell^{1/2}+\ell^{-1/2})^2-x^2}dx \tag{1.13}$$

supported in the Hasse interval $[-2\sqrt{\ell},2\sqrt{\ell}]$; it is the asymptotic distribution of the eigenvalues of a random sequence of $(\ell+1)$-regular graphs with increasing number of vertices, see [45], [37, Theorem 7.2] and references therein.

The following result, which relies on the theory of modular forms, is a corollary of Theorems 5.5.5 and 5.7.1.

Corollary 1.14. *Fix a subgroup $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, a prime number ℓ coprime with N, and let $\{p_i\}$ be an increasing sequence of prime numbers not dividing $N\ell$. Let $G_i = G(p_i, \ell, H)$,*

- *If $H = \{\mathrm{Id}\}$, i.e. G_i are isogeny graphs with full level structure, given k' the order of ℓ in $(\mathbb{Z}/N\mathbb{Z})^\times$, then for every θ in $\frac{\pi}{k'}\mathbb{Z}$ we have*

$$\lim_{i\to\infty} \mu(G_i, \theta) = e^{i\theta}\mu_\ell \ ,$$

  and for all other choices of θ there are no eigenvalues.
- *If H is the Borel subgroup, then all eigenvalues are real and*

$$\lim_{i\to\infty} \mu(G_i) = \mu_\ell \ ,$$

- *If $H = \{\left(\begin{smallmatrix} * & 0 \\ * & 1 \end{smallmatrix}\right)\}$, i.e. the G_i's are graphs with torsion point structure, denoting k' the order of ℓ in $(\mathbb{Z}/N\mathbb{Z})^\times$, then for every θ in $\frac{\pi}{k'}\mathbb{Z}$ we have*

$$\lim_{i\to\infty} \mu(G_i, \theta) = e^{i\theta}\mu_\ell \ ,$$

  and for all other choices of θ there are no eigenvalues.
- *If H is a non-split Cartan, then all eigenvalues are real and*

$$\lim_{i\to\infty} \mu(G_i) = \mu_\ell \ .$$

It is instructive to note that Corollary 1.14 alone does not imply that all eigenvalues are contained in the Hasse interval: it does not prevent a small number of eigenvalues to lie outside the support of the asymptotic distribution.

By general graph theory, Corollary 1.14 implies that G_i has few cycles, more precisely the number of cycles of a fixed length divided by the number of vertices of G_i tends to zero when i tends to infinity, see [45] and [56, Theorem 10].

1.3. Relation with isogeny based cryptography

Usually the security and sometime the design of protocols from isogeny-based cryptography relies on features of isogeny graphs. Often the security is related to the mixing time, the number of cycles, or to the spectral gap of the graphs. All these features can be studied looking at the spectrum of the adjacency matrix. We again refer to [37] or other textbooks in Graph Theory or Markov Chains for a general discussion of this topic, see also our Section 1.2

The first appearance of isogeny graphs in cryptography is the Charles–Goren–Lauter hash function [15], where the digest of a message is computed through a walk on a classical isogeny graph.

An important instance of isogeny based cryptography is the key exchange protocol SIDH [32]. In this protocol, the public key is a pair of vertices on the isogeny graph with full level structure and the private key is a walk between them. This protocol has been broken [13,44,54]: if N is big enough with respect to the length of the walk, as in SIDH, there are efficient algorithms to find a path between the two vertices. If N is small with respect to the length of the walk, still we do not know an efficient algorithm to find a path.

Given the importance of the full level structure in the SIDH attacks, new light has been shed on the torsion and on how to leverage it: new key exchanges, some with the intent of "fixing" SIDH, have been proposed and once again public and private keys can be represented using a convenient isogeny graph $G(p, \ell, H)$, now with H different from $\{\mathrm{Id}\}$ and $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. For instance, in [28], the group H defining the level structure is the group of scalar matrices. In [10] the authors use a commutative H to hide information: they mainly use a split Cartan subgroup and they also propose the group of circulant invertible matrices; we notice that the non-split Cartan subgroup could be considered as a viable option. Another scheme leveraging early torsion attacks is proposed in [31]. The article [29] discusses the security of various level structures in cryptographic protocols.

It is not known if there is some intrinsic property of the isogeny graphs which makes the path finding problem more difficult for some level structure rather than others. Let us recall that the efficiency of general path find algorithms on graphs depends on the spectral gap.

From a different perspective, estimates on the mixing time of random walks on isogeny graph, as the one from Proposition 1.12, are used to ensure that certain schemes are secure. For example, in [8] non-backtracking random walks on the isogeny graph with Borel level structure are used to define a Zero Knowledge Proof. The length of the walk is a parameter of the scheme, let us denote it by k. As discussed in Section 1.2.1, these walks give a probability distribution $\pi^{(k)}$ on the graph. Following [8], the statistical security of the Zero Knowledge Proof is determined by the total variation distance between $\pi^{(k)}$ and the stationary distribution: the closer they are, more statistically secure is the Proof. The analysis of the mixing time from [8, Theorem 7] is thus used to give a precise relation between the length of the walk and the security of the Proof.

The last isogeny based protocol being submitted to the NIST for standardization is the signature scheme SQISign (see [30] and the recent developments [18], [9], [25] and [49]). In SQISign, a random walk on an isogeny graph with trivial level structure is used to choose a supersingular elliptic curve. In the same fashion of the Zero Knowledge Proof discussed above, the length of the walk is related to the security of the scheme via an estimate of the mixing time. The estimate used in SQIsign is discussed in [9, Lemma 20] and [18, Proposition 29], which again rely on [8, Theorem 11].

Proposition 1.12 improves [8, Theorem 7]; in principle, it could imply that to achieve a certain security level one needs shorter walks than the ones requested in the above cited papers, and this could improve the efficiency of the schemes. Looking at the commonly used parameters and the dependence on p of the constants in Proposition 1.12, right now

it seems that our result does not give relevant improvements. However, the numerical experiments from Appendix B suggest that the constants in Proposition 1.12 could be improved.

To conclude this section, we explain how Theorem 1.6 implies Conjectures 1 and 2 from [33] (as long as the restriction from [33, Section 4] about the Weil pairing is taken into account). These conjectures are about valid keys in isogeny based cryptography are true. Their proof will rely on the following corollary of Theorem 1.6 applied to the case $H = \{\mathrm{Id}\} \times B_0(M)$ in $\mathrm{GL}_2(\mathbb{Z}/NM\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ for M, N coprime integers (we actually need only the description of the connected components of the isogeny graphs from Theorem 1.6).

Corollary 1.15. *Let p, ℓ, N and M be pairwise coprime numbers such that p and ℓ are prime; let (E, P, Q, C) and (E', P', Q', C') be two supersingular elliptic curves over $\overline{\mathbb{F}}_p$ endowed with basis of the N torsion and cyclic subgroups of order M.*

Then, there exists $m \in \mathbb{Z}$ and an isogeny $\phi\colon E \to E'$ of degree ℓ^m such that $\phi(P) = P'$, $\phi(Q) = Q'$ and $\phi(C) = C'$ if and only if for some integer $k > 0$ we have $w(P, Q) = w(P', Q')^{\ell^k}$, where w is the Weil pairing on the N-torsion.

Let us now explain and prove the conjectures in [33]. Fix a supersingular elliptic curve E with a basis $\{P, Q\}$ of the N-torsion. A valid degree insensitive public key is a supersingular elliptic curve with level N structure (E', P', Q') such that there exists $m \in \mathbb{Z}$ and an isogeny of degree ℓ^m $\phi\colon E \to E'$ such that $\phi(P) = P'$ and $\phi(Q) = Q'$. Conjecture 1 in [33], taking into account the obstruction presented in Section 4 in [33], states that all supersingular elliptic curves with level N structure are valid degree insensitive key as long as for some integer $k > 0$ we have $w(P, Q) = w(P', Q')^{\ell^k}$. This is a direct application of the corollary with $M = 1$.

Conjecture 2 is about degree insensitive SIDH squares (these squares are now often called isogeny diamonds). Fix two different primes ℓ_A and ℓ_B, and two numbers e_A and e_B. A SIDH square is a commutative diagram

$$\begin{array}{ccc} (E, P_A, Q_A, P_B, Q_B) & \xrightarrow{\varphi_A} & (E'_A, P'_B, Q'_B) \\ \downarrow{\scriptstyle \varphi_B} & & \downarrow{\scriptstyle \varphi_{BA}} \\ (E'_B, P'_A, Q'_A) & \xrightarrow[\varphi_{AB}]{} & E_{AB} \end{array}$$

where $\{P_A, Q_A\}$ and $\{P'_A, Q'_A\}$ are basis of the $\ell_A^{e_A}$-torsion, and $\{P_B, Q_B\}$ and $\{P'_B, Q'_B\}$ are basis of the $\ell_B^{e_B}$-torsion; the isogeny ϕ_A has degree $\ell_A^{m_A}$ and ϕ_B has degree $\ell_B^{m_B}$ for some integers m_A and m_B, and respect the level structure. [33, Conjecture 2] says that any four curves with level structure (E, P_A, Q_A, P_B, Q_B), (E'_A, P'_B, Q'_B), (E'_B, P'_A, Q'_A), and E_{AB} can be put in such a diagram as long as there are no obstructions from the

Weil pairing, i.e. $w(P_A, Q_A) = w(P'_A, Q'_A)^{\ell_A^{k_A}}$ and $w(P_B, Q_B) = w(P'_B, Q'_B)^{\ell_B^{k_B}}$ for some integers k_A and k_B. Let us show it.

There exist infinitely many isogenies $\phi_B \colon E \to E_B$ of degree ℓ_B^m sending $(P_A, Q_A) \mapsto (P'_A, Q'_A)$ (for the "infinitely many" part we can compose closed non-backtracking walks in the graph with full level structure with a walk from Corollary 1.15). For m big enough, by Proposition 1.12 we can find a cyclic isogeny $\psi \colon E_A \to E_{AB}$ of the same degree ℓ_B^m. Denoting $C_B = \ker(\phi_B)$, $K = \ker(\psi)$ and using that $w(P'_B, Q'_B) = w(P_B, Q_B)^{\ell_A^k}$ for some k, Corollary 1.15 gives isogeny $\phi_A \colon E \to E_A$ of degree a power of ℓ_A, sending $P_B \mapsto P'_B$, $Q_B \mapsto Q'_B$ and $C_B \mapsto K$. This last condition implies that we can complete the square with a map $E_B \to E_{AB}$, forming the requesting diagram and completing the proof.

1.4. Relation with other works

The Ramanujan property of isogeny graphs without level structure is usually attributed to A. K. Pizer [51]. There, the result is stated for graphs constructed using Brandt matrices. These matrices are defined using quaternion algebras and theta series; they represent the action of Hecke operators on spaces of modular forms. Using the moduli space of elliptic curves over $\mathbb{Z}$, one can deduce the bound of the spectra of Hecke operators on modular forms from Deligne's proof of the Weil's conjecture. Finally, the Deuring correspondence provides the relations between Brandt matrices and isogeny graphs. This approach is taken up in full details in [8, Section 3], where it is extended to the case of isogeny graph with Borel level structure. A few weeks after this article appeared on ArXiv, A. Page and B. Wesolowski in [50] further generalize this approach and gave an independent proof of a variant of our Theorem 1.6. They use a generalization of the Deuring correspondence - the adelic Deuring correspondence - to relate isogeny graphs with level structure to graphs defined using quaternion algebras. They then use the Jacquet–Langlands correspondence to relate the adjacency matrices of this graph to the action of Hecke operators on spaces of modular forms. As in the case without level structure, the bound on the spectra of these operators is a consequence of Deligne's proof of Weil conjecture. Similar arguments can also be found in [14].

Here we follow ideas from [53,26]. Using the moduli space of elliptic curves over $\mathbb{Z}$, we directly relate the adjacency matrix of the isogeny graphs with level structure to the action of certain Hecke operators on the cohomology of the moduli space of elliptic curves over $\mathbb{F}_\ell$. We then directly apply Deligne's proof of Weil conjecture. Our approach does not involve quaternion algebras, the Deuring and the Jaquet-Langlands correspondences, and modular forms, but still boils down to Deligne's Theorem.

Let us also briefly survey a few papers on isogeny graphs which do not focus on the spectrum of the adjacency matrix. The Borel level structure case is studied by Arpin in [4]. The zeta-function of isogeny graphs with Borel level structure is studied in [42].

Other interesting papers are [5,3,43]. In [36,6], there is nice bound on the number of cycles on classical isogeny graphs obtained using different methods from ours.

Isogeny graphs of ordinary curves are studied by Kohel [40], they have a rather different (and simpler!) structure from the supersingular ones, sometime they go by the names of volcano graphs or jellyfish graphs.

Remark 1.16 *(Relation with the graphs $X^{p,q}$ from [19]).* Fixing $p = 2$ and taking H to be the group of scalar matrices modulo N for a prime level N, we get graphs closely related to the Cayley graphs $X^{\ell,N}$ from [19, Chapter 4], and references therein. Indeed, there is only one supersingular elliptic curve $E/\overline{\mathbb{F}}_2$ up to isomorphism, that is the one with equation $y^2 + y = x^3$, whose endomorphism ring of E is a quaternion order $\mathcal{O}$ that contains the integral Hermite quaternions $\mathbb{Z}[i,j,k]$ and it is contained in $\frac{1}{2}\mathbb{Z}[i,j,k]$, so that all ℓ-isogenies of our graphs can be represented as elements of norm ℓ in $\mathcal{O}$, and actually, up to postcomposition by automorphisms, they are the elements of $S_\ell \subset \mathbb{Z}[i,j,k]$ defined in [19, page 68].[1] Moreover, the isomorphism $\mathbb{F}_N[i,j,k] \cong M_2(\mathbb{F}_N)$ in [19] keeps track of the action of $\mathrm{End}(E)$ on $E[N]$: we get a bijection between $\mathrm{PGL}_2(\mathbb{F}_N)$ and H-structures on E, and also a bijection isomorphism classes of supersingular elliptic over $\overline{\mathbb{F}}_2$ together with an H-structure with the quotient of $\mathrm{PGL}_2(\mathbb{F}_q)$ by the image of $\mathrm{Aut}(E)$. In particular, a connected component of the isogeny graph $G(2,\ell,H)$ (all components are isomorphic) is a quotient of the Cayley graph $X^{\ell,N}$ obtained in [19] reducing the elements of S_ℓ modulo N.

Acknowledgments

We have had the pleasure and the benefit of conversations about the topics of this paper with S. Arpin, A. Basso, P. Caputo, L. De Feo, T. B. Fouotsa, T. Morrison, M. Sala, M. Salvi, R. Schoof, S. Vigogna and F. Viviani. The first author also would like to thank the organizers and the participants of the Banff/Bristol 2023 workshop "Isogeny graphs in Cryptography" for many discussions on the topics of this paper. We also thank the anonymous referee for his/her suggestions.

Both authors are supported by the MUR Excellence Department Project MatMod@TOV, CUP E83C23000330006, awarded to the Department of Mathematics, University of Rome Tor Vergata, the "National Group for Algebraic and Geometric Structures and their Applications" (GNSAGA - INdAM), and the PRIN PNRR 2022 "Mathematical Primitives for Post Quantum Digital Signatures" CUP D53D23018900001. The second author is also supported by "Programma Operativo Nazionale (PON) "Ricerca e Innovazione" 2014-2020.

[1] Indeed all elements γ_i of such an S_ℓ define an ℓ-isogeny of E and they are all distinct up to postcomposition by automorphism because for $i \neq j$ the element $\gamma_i^{-1}\gamma_j = \frac{1}{\ell}\overline{\gamma_i}\gamma_j$ is in $\frac{1}{\ell}\mathbb{Z}[i,j,k]$ but not in $\mathbb{Z}[i,j,k]$, hence it is not in $\frac{1}{2}\mathbb{Z}[i,j,k]$ which contains $\mathcal{O}$.

2. First properties of isogeny graphs and reduction of Theorems 1.4 and 1.6 to Theorem 2.3.8

We fix p and ℓ distinct prime numbers, N a positive integer coprime to $p\ell$ and H a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, together with the isogeny graph $G = G(p, \ell, H)$ in Definition 1.3 and its vertex set V. The adjacency matrix A defines a linear operator $A\colon \mathbb{Q}^V \to \mathbb{Q}^V$, hence also an operator $\mathbb{C}^V \to \mathbb{C}^V$, which maps a vertex v to $\sum v_i$, where the sum runs over all edges $v \to v_i$ coming out of v.

2.1. Automorphisms of isogeny graphs

All isogeny graphs have the following automorphism, which is usually called Galois or Frobenius automorphism.

Definition 2.1.1 *(Frobenius automorphism).* Let σ be the Frobenius automorphism of $\overline{\mathbb{F}}_p/\mathbb{F}_p$, then

$$\langle\sigma\rangle\colon G \to G$$

maps a vertex (E, ϕ) to the conjugated $(E^\sigma, \phi^\sigma := \sigma\circ\phi)$, and an isogeny to the conjugated by σ.

Adding level structure, naturally enriches isogeny graphs with the following automorphisms.

Definition 2.1.2 *(Diamond and matricial automorphisms).* Let G be as in Definition 1.3. For every g in the normalizer $\mathcal{N}_H$ of H in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we define an automorphism

$$\begin{aligned}\langle g\rangle\colon G &\to G\\ (E,\phi) &\mapsto (E, \phi\circ g)\end{aligned}$$

In particular, for every d in $(\mathbb{Z}/N\mathbb{Z})^\times$, the diamond operator $\langle d\rangle$ is the automorphism associated with the diagonal matrix $\left(\begin{smallmatrix} d & \\ & d\end{smallmatrix}\right)$.

Observe that if $d = \left(\begin{smallmatrix} d & \\ & d\end{smallmatrix}\right)$ belongs to H, then $\langle d\rangle$ is the identity. Moreover, even if $-1 \notin H$, then $\langle -1\rangle$ is the identity because $(E, -\phi)$ is always isomorphic to (E, ϕ).

Notice that, up to isomorphism, we can suppose that each elliptic curve E_i in our graph is defined over $\mathbb{F}_{p^2}$ and that the Frobenius endomorphism $\mathrm{Frob}_{p^2}\colon E_i \to E_i$ acts as $[-p]$. Since the map $\sigma\colon E(\overline{\mathbb{F}}_p) \to E^\sigma(\overline{\mathbb{F}}_p)$ coincides with the action of $\mathrm{Frob}_p\colon E \to E^\sigma$, we deduce that $\langle\sigma\rangle^2 = \langle p\rangle$ on the graph: indeed, for each vertex (E_i, ϕ_i) we have

$$\begin{aligned}\langle\sigma\rangle^2(E_i,\phi_i) &= (E_i^{\sigma^2}, \sigma^2\circ\phi_i) = (E_i, \mathrm{Frob}_{p^2}\circ\phi_i) = (E_i, [-p]\circ\phi_i)\\ &= \langle -p\rangle(E_i,\phi_i) = \langle p\rangle(E_i,\phi_i)\,,\end{aligned}$$

where the last equality is true because $\langle -1 \rangle$ is the identity.

Proposition 2.1.3. *For every p, ℓ, N, and H, the isogeny graph $G(p, \ell, H)$ is the quotient of the isogeny graph with full level structure $G(p, \ell, \{\mathrm{Id}\})$ by the action of H given in Definition 2.1.2. In particular, the spectrum of the adjacency matrix of $G(p, \ell, H)$ is a subset of the spectrum of the adjacency matrix of $G(p, \ell, \{\mathrm{Id}\})$.*

Using Proposition 2.1.3, one could deduce most of our results from the case of full level structure. However, we prefer to give proofs that directly work for any level structure.

To introduce the Atkin-Lehner automorphisms we need some more notations. If $N = N'q$, with N' and q coprime, and the group H is a product $H' \times B$ in $\mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/q\mathbb{Z})$, then a level H structure consist of a level H' and a level B structure. Now assume that q is a prime power, and B is a Borel subgroup of $E[q]$; then a level B structure consists of a cyclic subgroup C of $E[q]$ of rank q.

Definition 2.1.4 *(Atkin-Lehner automorphism).* With the above notation, the Atkin-Lehner automorphism

$$w_q \colon G \to G$$

maps (E, ϕ, C) to $(E/C, \pi \circ \phi, E[q]/\pi(C))$, where ϕ is a level H' structure, C is a level B structure, and π is the quotient map $E \to E/C$.

When $N = N'q_1 \cdots q_r$ with $N, q_1, \dots, q_r$ coprime and q_i prime powers, and $H = H' \times \prod B_i$ in $\mathrm{GL}_2(\mathbb{Z}/N'\mathbb{Z}) \times \prod \mathrm{GL}_2(\mathbb{Z}/q_i\mathbb{Z})$, the above definition gives r Atkin-Lehner automorphisms $w_{q_1}, \dots, w_{q_r}$.

2.2. Hermitian form and diagonalization

With keep the notation of Definition 1.3. We introduce the following Hermitian form H on $\mathbb{C}^V$

$$H\left((E_i, \phi_i), (E_j, \phi_j)\right) = \delta_{ij} a_i \,, \tag{2.2.1}$$

with $a_j = |\mathrm{Aut}(E_i, \phi_i)|$ and δ_{ij} is the Kronecker delta.

Proposition 2.2.2 *(Adjoint of the adjacency matrix). Let G and A be as in Definition 1.3 and let A^* be its adjoint with respect to the Hermitian form (2.2.1). Then,*

$$A^* = \langle \ell^{-1} \rangle A \,.$$

The adjacency matrix A is diagonalizable, and the angles of its eigenvalues lie in $\frac{\pi}{k'}\mathbb{Z}$, where k' is the minimum positive integer such that $\ell^{k'} \mathrm{Id} \in H$. In particular:

- *the operators A and A^* commute, are both diagonalizable, have the same spectrum, and are conjugate;*
- *if ℓ belongs to H, then $A = A^*$ and the spectrum of A is real;*
- *if ℓ belongs to H and p is congruent to 1 modulo 12, the adjacency matrix is symmetric.*

Proof. For the first part, we need to prove that, given vertices (E_i, ϕ_i) and (E_j, ϕ_j) we have

$$H\big(A\cdot(E_i,\phi),(E_j,\phi_j)\big) = H\big((E_i,\phi_i),\langle \ell^{-1}\rangle A\cdot(E_j,\phi_j)\big)\,, \tag{2.2.3}$$

where we interpret (E_i, ϕ_i) and (E_j, ϕ_j) as elements of $\mathbb{C}^V$. Let L be the set of degree ℓ morphisms $(E_i, \phi_i) \to (E_j, \phi_j)$, and let M be the set of degree ℓ morphisms $(E_j, \phi_j) \to (E_i, [\ell]\phi_i)$. Then, using the definition of A, and the definition (2.2.1) of H, we find that

$$H(A\cdot(E_i,\phi),(E_j,\phi_j)) = \frac{\#L\cdot\#\mathrm{Aut}(E_j,\phi_j)}{\#\mathrm{Aut}(E_j,\phi_j)}\,,$$
$$H((E_i,\phi_i),\langle\ell\rangle A\cdot(E_j,\phi_j)) = \frac{\#M\cdot\#\mathrm{Aut}(E_i,\phi_i)}{\#\mathrm{Aut}(E_i,[\ell]\phi_i)}\,.$$

We notice that $\mathrm{Aut}(E_i, \ell\phi_i)$ equals $\mathrm{Aut}(E_i, \phi_i)$ as subgroup of $\mathrm{Aut}(E_i)$. Hence equation (2.2.3) is equivalent to the fact that L and M have the same cardinality: indeed duality of isogenies gives a bijection between the two.

Since diamond operators commute with A, then A is a normal operator, hence diagonalizable. Moreover, the adjoint of $A^{k'}$ is equal to $\langle \ell^{k'}\rangle A^{k'} = A^{k'}$, hence $A^{k'}$ is Hermitian and has real eigenvalues. We deduce that for each λ in the spectrum of A, its power $\lambda^{k'}$ is real, hence the angle of λ lies in $\frac{\pi}{k'}\mathbb{Z}$.

The operator A^* is also diagonalizable. Since A and A^* commute, they have the same eigenvectors. The corresponding eigenvalues are conjugated. Since A is real, its spectrum is invariant under conjugation, hence A and A^* have the same spectrum. Since A and A^* are both diagonalizable with the same spectrum, they are conjugate.

If p is congruent to 1 modulo 12, all supersingular elliptic curves have $\{\pm 1\}$ as automorphism group, and hence all vertices (E_i, ϕ_i) have the same number a_i of automorphisms: if $-1 \in H$, then $a_i = 2$, otherwise $a_i = 1$. Then, the Hermitian form from Equation (2.2.1) is a multiple of the standard form, and being self-adjoint coincides with being symmetric. □

Remark 2.2.4. Since the Hermitian form (2.2.1) is presented in diagonal form, it is easy to write down the entries of A^*: for each i we have

$$A^*((E_i,\phi_i)) = a_i\sum_j a_j^{-1}(E_j,\phi_j)\,, \tag{2.2.5}$$

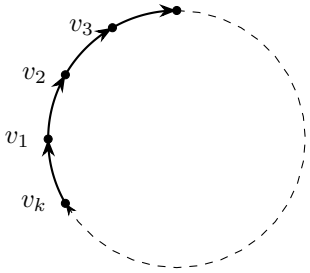
where a_i, a_j are as in Equation (2.2.1), and the sum runs over all edges $(E_j, \phi_j) \to (E_i, \phi_i)$, namely all the edges in G with end-point (E_i, ϕ_i). We notice that the entries of A^* are integers: any vertex (E_j, ϕ_j) appearing in the right hand side of (2.2.5) has multiplicity $a_i a_j^{-1} \cdot (\#S/a_i) = \#S/a_j$, for S the set of degree ℓ isogenies $(E_j, \phi_j) \to (E_i, \phi_i)$; since $\mathrm{Aut}(E_j, \phi_j)$ acts freely on S by precomposition, then $\#S/a_j$ is an integer.

2.3. Weil pairing and reduction of Theorems 1.4 and 1.6 to Theorem 2.3.8

To formulate the arguments in this subsection, we look at the following graph.

Definition 2.3.1. Given H a subgroup $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\ell \in (\mathbb{Z}/N\mathbb{Z})^\times$, the oriented Caley graph $C = C(N, \det(H), \ell)$ is the graph whose vertices are the element of $R_H = \mu_N^\times(\overline{\mathbb{F}}_p)/\det(H)$ and such that there is an edge from ξ_1 to ξ_2 if and only if $\xi_2 = \xi_1^\ell$.

Since $\mu_N^\times(\overline{\mathbb{F}}_p)$ is a principal homogeneous space for the right action of $(\mathbb{Z}/N\mathbb{Z})^\times$, the graph $C(N, \det(H), \ell)$ has simple structure: it is the disjoint union of n cycles $C_1, \dots C_n$, each having the form of a loop:

$C_i \cong$ 

with k the order of ℓ in $(\mathbb{Z}/N\mathbb{Z})^\times/\det(H)$ and $n = \varphi(N)/(k\,|\det(H)|)$. In particular, the adjacency matrix P_i of each C_i is the cyclic permutation matrix on k elements; its spectrum in $\mathbb{C}$ is thus the set $\mu_k(\mathbb{C})$ of the k-th roots of unity in $\mathbb{C}$.

If two elliptic curves with level structure are connected by a degree ℓ isogeny, then [57, Chapter III, Proposition 8.2] implies that the Weil invariants of the level structures are one the ℓ-th power of the other, hence we have the following result.

Proposition 2.3.2. *The Weil invariant (see Definition 1.5) of a level structure gives a surjective map of graphs*

$$w\colon G(p, \ell, H) \to C(N, \det(H), \ell)\,. \tag{2.3.3}$$

Moreover, in the language of Definitions 2.1.2 and 2.1.1, for every matrix g in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that normalizes of H we have $w(\langle g\rangle(E, \phi)) = w((E, \phi))^{\det(g)}$ and, denoting σ the Frobenius automorphism of $\overline{\mathbb{F}}_p/\mathbb{F}_p$, we have $w(\sigma(E, \phi)) = w((E, \phi))^p$.

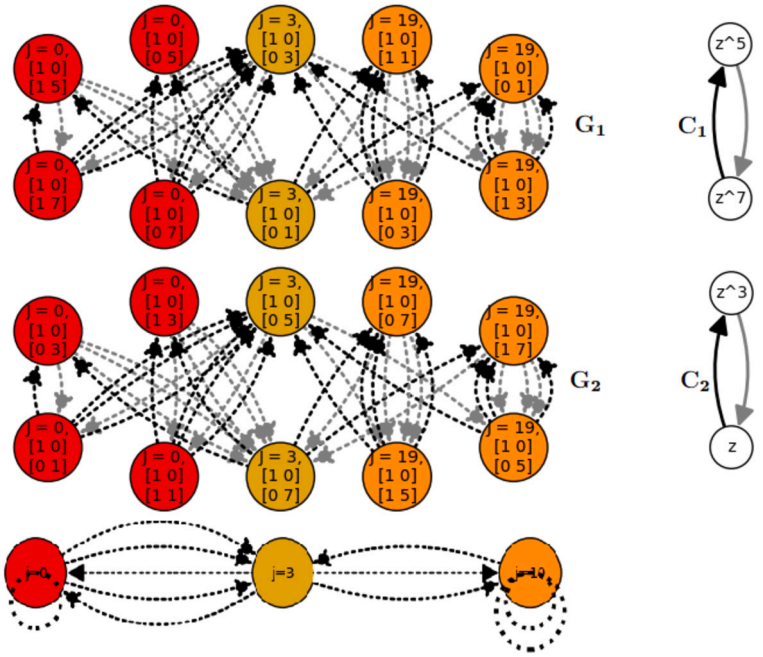


Fig. 1. This is an example of isogeny graph $G(p, \ell, H)$ with $p = 23$, $\ell = 3$ and $H = \langle \left(\begin{smallmatrix} 5 & 6 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 7 & 0 \\ 2 & 7 \end{smallmatrix}\right), \left(\begin{smallmatrix} 5 & 0 \\ 0 & 5 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 7 \\ 7 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 4 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 4 & 1 \end{smallmatrix}\right) \rangle$ the only index 8 subgroup of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$.
The color indicates the elliptic curve, or equivalently the j-invariant. The level structure is given through a matrix: for each of the three elliptic curves we have chosen a (non-canonical) basis of the 8-torsion, and the matrix gives the change of basis. For mere visual clarity, arrows going up are black, arrows going down are gray. (For colored figure(s), the reader is referred to the web version of this article.)
The graph $G(p, \ell, H)$ has two components, G_1 and G_2, which correspond via the Weil invariant to the two connected components C_1 and C_2 of the Cayley graph, depicted on the right. Since each C_i has two vertices, each G_i is bipartite, see Remark 1.7. At the bottom, the graph without level structure.

An example of isogeny graph together with the map w is given in Fig. 1.

Denoting $V(\cdot)$ the set of vertices of a graph, the above map extends to linear maps

$$w_* \colon \mathbb{Q}^{V(G)} \longrightarrow \mathbb{Q}^{V(C)} . \tag{2.3.4}$$

Fix connected components C_i of C, let $G_i := w^{-1}(C_i)$ (this definition of G_i coincides with the one in the Introduction), then the above map restricts to a morphism

$$w_{i,*} \colon \mathbb{Q}^{V(G_i)} \longrightarrow \mathbb{Q}^{V(C_i)} . \tag{2.3.5}$$

Remark 2.3.6 *(Description of* $\ker(w_{i,*})$*).* The kernel of the map $w_{i,*}$ defined in Equation (2.3.5) will play an important role in this paper, so let us describe it explicitly.

If, as in the Borel case, $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$, then $\ker(w_{i,*})$ is the space of linear combination of vertices of the graphs whose coefficient sum up to zero, i.e. the orthogonal complement of the vector $(1, \dots, 1)$ in $\mathbb{Q}^{V(G)}$ for the standard scalar product.

In general, $\ker(w_{i,*})$ is equal to the subspace of $\mathbb{Q}^{V(G_i)}$ spanned by linear combinations of elements of $V(G_i)$ with the same Weil invariant and such that the coefficients sum up to zero. In other words, calling V_ξ the set of vertices of G with Weil invariant $\xi \in R_H$, then

$$\ker(w_*) = \bigoplus_{\xi \in R_H} \left\{ x \in \mathbb{Q}^{V_\xi} : \sum x_v = 0 \right\}, \quad \ker(w_{i,*}) = \bigoplus_{\xi \in V(C_i)} \left\{ x \in \mathbb{Q}^{V_\xi} : \sum x_v = 0 \right\}$$

where we identify $\mathbb{Q}^{V(G)}$ with the direct sum of the various $\mathbb{Q}^{V_\xi}$.

Since w_i is a map of regular graphs, $\ker(w_{i,*})$ is stable for the action of the adjacency matrix A_i of G_i.

Proposition 2.3.7. *Let G be an isogeny graph as in Definition 1.3, G_i be one of its subgraphs defined above, and A_i the adjacency matrix of G_i.*

The spectrum of A_i over $\mathbb{C}$ is equal to the union of $(\ell+1)\mu_k(\mathbb{C})$ and the spectrum of A_i restricted to $\ker(w_{i,*}) \otimes \mathbb{C}$, where k is as in Theorem 1.6 and $\mu_k(\mathbb{C})$ is the group of k-th roots of unity in $\mathbb{C}$.

Proof. The spectrum of A_i is the union of the spectra of A_i restricted to $\ker(w_{i,*})$ and of A_i when acting on the quotient $\mathbb{C}^{V(G_i)}/\ker(w_{i,*})$. Since w_i is a map of graphs and G_i is $\ell+1$ regular while C_i is 1 regular, the action of A_i on $\mathbb{C}^{V(G_i)}/\ker(w_{i,*}) \cong \mathbb{C}^{V(C_i)}$ is $\ell+1$ times the adjacency matrix of C_i, that is

$$\begin{pmatrix} 0 & & \\ \vdots & & (\ell+1)\mathrm{Id}_{k-1} \\ 0 & & \\ (\ell+1) & 0 \quad \cdots & 0 \end{pmatrix}$$

which is diagonalizable with spectrum $(\ell+1)\mu_k(\mathbb{C})$. □

The study of the spectrum of A_i to $\ker(w_{i,*})$ is rather delicate; Sections 3 and 4 are devoted to the proof of the following result.

Theorem 2.3.8 *(see Theorem 4.18). Let G be as in Definition 1.3, let G_i be one of its subgraphs defined above, with adjacency matrix A_i, acting on the kernel $\ker(w_{i,*})$ of the map (2.3.5). Then the absolute values of the eigenvalues of A_i restricted to $\ker(w_{i,*}) \otimes \mathbb{C}$ are strictly smaller than $2\sqrt{\ell}$.*

Let us see how this statement implies the other theorems described in the Introduction.

Corollary 2.3.9. *With the notation as in Theorem 2.3.8, each G_i is connected. If p, ℓ and $\det \mathcal{N}_H$ generate $(\mathbb{Z}/N\mathbb{Z})^\times$, then all G_i's are isomorphic.*

Proof. By general graph theory, e.g the argument from [19, Proposition 1.1.2], the number of connected component of an $\ell+1$ regular graph is the multiplicity of the eigenvalues $\ell+1$ for the adjacency matrix, hence Proposition 2.3.7 and Theorem 2.3.8 implies that G_i is connected.

For the second part we notice that p, ℓ and $\det \mathcal{N}_H$ generate $(\mathbb{Z}/N\mathbb{Z})^\times$ if and only if $\langle p, \det \mathcal{N}_H \rangle$ acts transitively on the set of orbits $\{C_1, \dots, C_n\}$. If, for g in $\mathcal{N}_H$, $\det(g)$ maps C_i to C_j, then $\langle g \rangle$ and $\langle g^{-1} \rangle$ give an isomorphism between G_i and G_j. Analogously, if p maps C_i to C_j, then $\langle \sigma \rangle$ gives an isomorphism between G_i and G_j. □

To prove Theorem 1.4 and Theorem 1.6 we will use the following lemma.

Lemma 2.3.10. *Let $p(x) \in \mathbb{Z}[x]$ be a monic polynomial of degree d, and let ℓ and k' two positive integers such that for every complex root λ of $p(x)$ one has $|\lambda| < 2\sqrt{\ell}$ and the phase of λ is in $\frac{\pi}{k'}\mathbb{Z}$. Then we have*

$$|\lambda| < 2\sqrt{\ell} - \left(4\sqrt{\ell}\right)^{-2dk'+1}.$$

Proof. Let F be the subfield of $\mathbb{C}$ obtained adding to $\mathbb{Q}$ all roots of $p(x)$, all k'th roots of unity and $\sqrt{\ell}$. The field F is a Galois extension of $\mathbb{Q}$ of degree at most $2dk'$.

Let λ be a root of $p(x)$ of phase ξ. Consider the product

$$P := \prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \sigma(2\sqrt{\ell} - \xi^{-1}\lambda).$$

Observe first that P is $\mathrm{Gal}(F/\mathbb{Q})$-invariant, hence it is in $\mathbb{Q}$. It is a product of algebraic integers, hence it is in $\mathbb{Z}$. Because of the assumption on the absolute values of the roots of $p(x)$, P is different from 0, hence $|P| \geq 1$. Furthermore, $|\sigma(2\sqrt{\ell} - \xi^{-1}\lambda)| \leq |\sigma(2\sqrt{\ell})| + |\sigma(\xi^{-1})||\sigma(\lambda)| < 4\sqrt{\ell}$, hence

$$|2\sqrt{\ell} - \xi^{-1}\lambda| = \frac{|P|}{\prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q}) \setminus \{1\}} |\sigma(2\sqrt{\ell} - \lambda)|} > \left(4\sqrt{\ell}\right)^{-|G|+1}. \quad \square$$

Proof of Theorems 1.4 and 1.6 The statement about the connected components is Corollary 2.3.9. Diagonalizability and the angles of the eigenvalues are given in Proposition 2.2.2. The eigenvalues of absolute value $\ell+1$ are described in Proposition 2.3.7.

To bound the absolute values of the other eigenvalues, we first apply Theorem 2.3.8, and then we apply Lemma 2.3.10 to the characteristic polynomial of the adjacency matrix A_i restricted to $\ker(w_{i,*}) \otimes \mathbb{C}$.

2.4. Isomorphism between Borel and Cartan level structure

Here we define an isomorphism between graphs with Borel and Cartan level structure; because of this isomorphism, in the sequel, when we spell out our results in special cases, we will consider the Borel level structures and not the Cartan ones.

Fix p and ℓ distinct primes; let N be a positive integer coprime with p and ℓ; let $B_0(N^2)$ be the Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/N^2\mathbb{Z})$ and $T(N)$ the split Cartan of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Consider the map

$$\begin{aligned} F\colon G(p,\ell,B_0(N^2)) &\longrightarrow G(p,\ell,T(N)) \\ (E,C) &\longmapsto (E/NC, C/NC, E[N]/NC)\ . \end{aligned}$$

Proposition 2.4.1. *The map F defined above gives an isomorphism of graphs.*

Proof. The map F naturally extends to edges: given vertices (E,C) and (E',C') in the Borel graph, for each ℓ-isogeny $\varphi\colon E \to E'$ such that $\varphi(C) = C'$, we also have $\varphi(NC) = NC'$, hence there exists an isogeny $\tilde{\varphi}$ of degree ℓ that fits in the commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\varphi} & E' \\ \downarrow & & \downarrow \\ E/NC & \xrightarrow{\tilde{\varphi}} & E'/NC \end{array}$$

In particular, the isogeny $\tilde{\varphi}$ has degree ℓ and sends the subgroups C/NC, $E[N]/NC$ respectively to C'/NC', $E'[N]/NC'$. The inverse of F, at the level of vertices, is the map sending (E,C_1,C_2) to $(E/C_2,(N^{-1}C_1)/C_2)$, where $N^{-1}C_1$ is the set of points $P \in E[N^2]$ such that NP lies in C_1. □

3. Preliminary results on modular curves

In this section we collect some facts about the compactified moduli space of elliptic curves with level structure, and Hecke operators. Our main reference is [21], as it treats these concepts in the generality that we need. There are however many other references about these classical topics.

We need the construction of the moduli space as stack: first we need the definition of (generalized) elliptic curve over an arbitrary scheme S; then, as usual, the moduli space will be the space M such that maps from S to M are equivalent to (generalized) elliptic curves over S. A modern reference about stacks is [2], it contains also an introduction with a high level description of moduli spaces and stacks.

Following [21, Chapter II page 173], a generalized elliptic curve is either an elliptic curve or a Néron polygon. A Néron polygon is a curve obtained taking n copies of $\mathbb{P}^1$

indexed by $\mathbb{Z}/n$, and gluing the point 0 of the i-th copy, with the point ∞ of the $i+1$-copy; its smooth locus has a natural group structure.

A generalized elliptic curves $\pi\colon E \to S$ over an arbitrary scheme S is a family of genus one curves, whose geometric fibers are either elliptic curves or Néron polygons, and with a group structure on the smooth locus [21, Definition 1.12 page 36].

Fix a positive integer N and a subgroup H of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. A level H structure on an elliptic curve or on a Néron polygon with N edges E is an isomorphism ϕ between the N torsion of E and $(\mathbb{Z}/N\mathbb{Z})^{\oplus 2}$; two level structures ϕ_1 and ϕ_2 are isomorphic if there exists an h in H such that $\phi_1 = \phi_2 \circ h$. Observe that to have such a level structure the characteristic of the base field can not divide N.

A level H structure on a generalized elliptic curves $\pi\colon E \to S$ over an arbitrary scheme S is an isomorphism ϕ of the N torsion of E with $(\mathbb{Z}/N\mathbb{Z})_S^{\oplus 2}$; two level structures ϕ_1 and ϕ_2 are isomorphic if étale locally on S there exists an h in H such that $\phi_1 = \phi_2 \circ h$.

A key result of [21] is that the moduli stack $\mathcal{M}_H$ parameterizing generalized elliptic curve with level H structure is a proper and smooth Deligne-Mumford stack over $\mathbb{Z}[1/N]$, see [21, Section IV.3, and Theorem 3.4]. The moduli space of elliptic curves is an open substack of $\mathcal{M}_H$; in particular, it is not proper.

For the proofs of our results, we need a more general definition of level structure that works also when the characteristic divides the level. The most general notion is the one of Drinfeld level structure, see [39]; in this paper we will only need a generalization of Borel level structure, already discussed in [21], which we recall below.

For every positive integer k, let $B_0(k) = \{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\}$ be the standard Borel subgroup of $\mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})$. Given $M = Nq_1 \cdots q_r$, with q_i prime powers that are pairwise coprime and prime to N, we will consider level structures associated with subgroups K of $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ of the form

$$K = H \times B_0(q_1) \times \cdots \times B_0(q_r) \quad < \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \times \prod_{i=1}^{r} \mathrm{GL}_2(\mathbb{Z}/q_i\mathbb{Z}), \quad (3.1)$$

for H a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. When $r = 1$ and $q_1 = p$ is prime, we write

$$H_p := H \times B_0(p) \quad < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/Np\mathbb{Z})\,. \quad (3.2)$$

For these kinds of subgroups, a level K structure on a generalized elliptic curve $\pi\colon E \to S$ is the datum of a level H structure ϕ, and, for each q_i, a cyclic locally free subgroup scheme C_i of rank q_i such that the subgroup generated by C_i and the image of ϕ intersects every irreducible component of every geometric fiber of π (see [21, 1.4.1, page 100]).

Since a Borel subgroup $B_0(q)$ is the stabilizer of a line in $(\mathbb{Z}/q\mathbb{Z})^2$, we observe that over $\mathbb{Z}[1/M]$ this second definition of level K structure is equivalent to the previous one, i.e. to an isomorphism between the M-torsion and $(\mathbb{Z}/M\mathbb{Z})^{\oplus 2}$ up to the action of K. On the other hand, if, for example, q_i is prime, over $\overline{\mathbb{F}}_{q_i}$ the kernel of the Frobenius is a "new" example of $B_0(q_i)$-structure for an elliptic curve which does not fit in the previous definition.

The stack $\mathcal{M}_K$ parametrizes generalized elliptic curves with level K structure such that the Néron polygons have only M edges. It is a proper and regular Deligne-Mumford stack over $\mathbb{Z}[1/N]$, it is smooth outside the $\overline{\mathbb{F}}_{q_i}$ points parametrizing supersingular elliptic curves, see [21, Chapter V, Theorem 1.6, Proposition 1.10, Variants 1.14 and 1.20].

For d in $(\mathbb{Z}/N\mathbb{Z})^\times$, we define an automorphism $\langle d\rangle$ of $\mathcal{M}_K$ called diamond operator. A point of $\mathcal{M}_K$ is a generalized elliptic curve with level K structure $(E, \phi, C_1, \dots, C_r)$; we let[2]

$$\langle d\rangle(E, \phi, C_1, \dots, C_r) := (E, d\phi, C_1, \dots, C_r)\,, \tag{3.3}$$

where $d\phi$ is the level H structure obtained composing ϕ with the multiplication by d. This definition makes sense for curves over an arbitrary scheme S, so gives an automorphism of $\mathcal{M}_K$. The inverse of $\langle d\rangle$ is $\langle e\rangle$, where e is a multiplicative inverse of d modulo N.

We now introduce two key maps, that will play more than one role for us

$$\begin{aligned} &\mathrm{pr}_p\colon \mathcal{M}_{H_p} \to \mathcal{M}_H\,, && \mathrm{pr}_p(E \to S, \phi, C) = (E \to S, \phi)\,, \\ &\mathrm{quot}_p\colon \mathcal{M}_{H_p} \to \mathcal{M}_H && \mathrm{quot}_p(E \to S, \phi, C) = (E/C \to S, \pi_C \circ \phi)\,, \end{aligned} \tag{3.4}$$

where π_C is the quotient map $E \to E/C$.

Following [21, Section V], we first use them to study the fiber $\mathcal{M}_{H_p,\mathbb{F}_p} = \mathcal{M}_{H_p} \times \operatorname{Spec}\mathbb{F}_p$. The maps pr_p and quot_p have right inverses when restricted to $\mathcal{M}_{H_p,\mathbb{F}_p}$. Indeed, an elliptic curve E over $\overline{\mathbb{F}}_p$ has only two subgroup or rank p: the kernel of the Frobenius and the kernel of the Verschiebung. Recall that, by definition, the Verschiebung is the dual isogeny of the Frobenius; we denote it by Ver. They are equal if and only if the curve is supersingular. We obtain two morphisms

$$\begin{aligned} \mathrm{pr}_{p,p}^{-1}\colon \mathcal{M}_{H,\mathbb{F}_p} &\longrightarrow \mathcal{M}_{H_p,\mathbb{F}_p}\,, && (E/S/\mathbb{F}_p, \phi) \mapsto (E/S/\mathbb{F}_p, \phi, \ker(\mathrm{Frob}))\,, \\ \mathrm{quot}_{p,p}^{-1}\colon \mathcal{M}_{H,\mathbb{F}_p} &\longrightarrow \mathcal{M}_{H_p,\mathbb{F}_p}\,, && (E/S/\mathbb{F}_p, \phi) \mapsto (E^{(p)}/S/\mathbb{F}_p, \phi \circ (\cdot\tfrac{1}{p}) \circ \mathrm{Frob}, \ker(\mathrm{Ver}))\,, \end{aligned} \tag{3.5}$$

which provide a description of $\mathcal{M}_{H_p,\mathbb{F}_p}$ as the union of two copies of $\mathcal{M}_{H,\mathbb{F}_p}$ nodally attached at the supersingular elliptic curves, see [21, Section 5, Theorem 1.16 and Variant 1.18]. Here we apologize for an abuse of notations: $\mathrm{pr}_{p,p}^{-1}$ and $\mathrm{quot}_{p,p}^{-1}$ are not the inverse of $\mathrm{pr}_{p,p} = \mathrm{pr}_{p,\mathbb{F}_p}$ and $\mathrm{quot}_{p,p} = \mathrm{quot}_{p,\mathbb{F}_p}$, but just the right inverse.

Every Deligne-Mumford stack $\mathcal{M}$ admits a coarse space M, in particular $\mathcal{M}_K$ has a coarse space M_K. Every map between stacks, such as pr_p and quot_p, induces a map between coarse spaces. A key fact is that in our set-up the formation of the coarse space is compatible with base change. More precisely, let ℓ be any prime number not dividing

[2] This definition of the diamond operator generalizes the one from [22, Section 7.9], which is given just for torsion point level structures. It differs slightly from the one given in [55, Appendix A] for full level structures. Our definition applies to arbitrary level structure, and it is compatible with the Eichler-Shimura relation 3.7.

N (possibly it can also be a divisor of the q_i's); the universal property of coarse spaces gives a map from the coarse space of $\mathcal{M}_{K,\mathbb{F}_\ell}$ to $M_{K,\mathbb{F}_\ell} := M_K \times \mathbb{F}_\ell$. In [21, Cor 6.10 page 145] it is shown that this map is an isomorphism (observe that if ℓ divides N then this compatibility is not known for general H, see for instance [39, Section 8.5]).

The definition of Picard group generalizes in a standard way from varieties to Deligne-Mumford stack, see e.g. [2, Section 4.1.7]. We use the Picard group of $\mathcal{M}_K$ and the maps (3.4) to define the *Hecke operator* T_ℓ.

Definition 3.6 *(Hecke operators).* With K as in Equation (3.1), and for a prime ℓ which does not divide M, the Hecke operator T_ℓ is the map

$$T_\ell := (\mathrm{quot}_\ell)_* \circ \mathrm{pr}_\ell^* \colon \mathrm{Pic}(\mathcal{M}_K/\mathbb{Z}[1/N]) \to \mathrm{Pic}(\mathcal{M}_K/\mathbb{Z}[1/N])\,,$$

where the push-forward is a cycle push-forward.

The analogue definition works for the coarse space M_K.

Observe that the diamond operator $\langle d\rangle$, which is defined for every d which does not divide N, commutes with pr_ℓ, quot_ℓ and T_ℓ.

The moduli space $\mathcal{M}_{K,\mathbb{F}_\ell}$ is one dimensional, and we have the following celebrated description of the restriction of the Hecke operator T_ℓ to the Jacobian $\mathrm{Pic}^0(\mathcal{M}_{K,\mathbb{F}_\ell})$ of $\mathcal{M}_{K,\mathbb{F}_\ell}$.

Theorem 3.7 *(Eichler-Shimura relation). With the notations of Definition 3.6, denoting by $T_{\ell,\mathbb{F}_\ell}$ the restriction of T_ℓ to either $\mathrm{Pic}^0(\mathcal{M}_{K,\mathbb{F}_\ell})$ or $\mathrm{Pic}^0(M_{K,\mathbb{F}_\ell})$, we have*

$$T_{\ell,\mathbb{F}_\ell} = \mathrm{Frob}_* + \langle \ell\rangle_* \mathrm{Frob}^*$$

where $\langle\ell\rangle$ is the diamond automorphism (3.3) and Frob *is the Frobenius of the curve $\mathcal{M}_{K,\mathbb{F}_\ell}$ or $M_{K,\mathbb{F}_\ell}$.*

Proof. We first prove the result on the stacks. Looking at the description of $\mathrm{quot}_{\ell,\mathbb{F}_\ell}$ and $\mathrm{pr}_{\ell,\mathbb{F}_\ell}$ on the two irreducible components of $\mathcal{M}_{K_\ell}$, we can write

$$T_{\ell,\mathbb{F}_\ell} = (\mathrm{quot}_{\ell,\mathbb{F}_\ell} \circ \mathrm{pr}_{\ell,\mathbb{F}_\ell}^{-1})_* \circ (\mathrm{pr}_{\ell,\mathbb{F}_\ell} \circ \mathrm{pr}_{\ell,\mathbb{F}_\ell}^{-1})^* + (\mathrm{quot}_{\ell,\mathbb{F}_\ell} \circ \mathrm{quot}_{\ell,\mathbb{F}_\ell}^{-1})_* \circ (\mathrm{pr}_{\ell,\mathbb{F}_\ell} \circ \mathrm{quot}_{\ell,\mathbb{F}_\ell}^{-1})^*$$

Both $\mathrm{pr}_{\ell,\mathbb{F}_\ell} \circ \mathrm{pr}_{\ell,\mathbb{F}_\ell}^{-1}$ and $\mathrm{quot}_{\ell,\mathbb{F}_\ell} \circ \mathrm{quot}_{\ell,\mathbb{F}_\ell}^{-1}$ are the identity on $\mathrm{Pic}^0\mathcal{M}_{K,\mathbb{F}_\ell}$, so we are left with

$$T_{\ell,\mathbb{F}_\ell} = (\mathrm{quot}_{\ell,\mathbb{F}_\ell} \circ \mathrm{pr}_{\ell,\ell}^{-1})_* + (\mathrm{pr}_{\ell,\mathbb{F}_\ell} \circ \mathrm{quot}_{\ell,\ell}^{-1})^*$$

We observe that $(\mathrm{quot}_{\ell,\mathbb{F}_\ell} \circ \mathrm{pr}_{\ell,\ell}^{-1})_* = \mathrm{Frob}_*$ because it maps (E,ϕ) to $(E^{(\ell)}, \mathrm{Frob}\circ\phi)$. To conclude, $(\mathrm{pr}_{\ell,\mathbb{F}_\ell} \circ \mathrm{quot}_{\ell,\ell}^{-1})^* = \langle\ell\rangle_*\mathrm{Frob}^*$ because it maps (E,ϕ) to $(E^{(\ell)}, \mathrm{Frob}\circ\phi\circ(\cdot\frac{1}{\ell}))$.

The property on the coarse spaces follows from their universal property. □

The spectral bounds in Theorem 2.3.8 will eventually be a consequence of the following bound, which in turn is a consequence of the above mentioned Eichler-Schimura relation and Weil's conjectures. A reference for the étale cohomology used below is [47]. For Weil's conjectures we refer to [20].

Theorem 3.8 *(Bound on the eigenvalues of the Hecke operator). With the above notations, let ℓ, ℓ' be different primes not diving M, then the roots of the characteristic polynomial of the action T_ℓ on $H^{i,\acute{e}t}(\mathrm{Pic}^0(M_{K,\mathbb{F}_\ell}), \mathbb{Q}_{\ell'})$ have complex absolute value less than or equal to $2\ell^{i/2}$.*

Proof. The curve $M_{K,\mathbb{F}_\ell}$ is proper and smooth, hence $X := \mathrm{Pic}^0(M_{K,\mathbb{F}_\ell})$ is an abelian variety defined over $\mathbb{F}_\ell$. Weil's conjectures, proved by Deligne [20, Theoreme 1.6], imply that the roots of the characteristic polynomial of the action Frob_X, which is the Frobenius of X, on $H^{i,\text{ét}}(X, \mathbb{Q}_{\ell'})$ have complex absolute value $\ell^{i/2}$ (in [20] Deligne uses the term variety to denote also possibly non-irreducible reduced schemes).

The Frobenius Frob_X is the endomorphism Frob_* appearing in Theorem 3.7. The maps Frob_* and Frob^* commutes, $\mathrm{Frob}^* \circ \mathrm{Frob}_*$ is the multiplication by ℓ, hence also Frob_* has eigenvalues of complex absolute value $\ell^{i/2}$. The map $\langle \ell \rangle$ is an automorphism of finite order of X, hence its eigenvalues are roots of unity.

Since the maps Frob_*, Frob^* and $\langle \ell \rangle$ commute, the claim follows from Theorem 3.7. □

We close this section by introducing some automorphisms of modular curves. They will be related to the automorphisms of isogeny graphs from Section 2.1, see Theorem 4.17.

The following automorphisms will correspond to the automorphisms from Section 2.1 with the same name.

Definition 3.9 *(Matricial automorphisms).* Given a level structure $K = H \times \prod B_0(q_i)$ as in (3.1), for any element g in the normalizer $\mathcal{N}_H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ of H, the automorphism $\langle g \rangle \colon \mathcal{M}_K \to \mathcal{M}_K$ maps a curve $(E, \phi, C_1, \dots C_r)$ to $(E, \phi \circ g, C_1, \dots C_r)$.
In particular, for every d in $(\mathbb{Z}/N\mathbb{Z})^\times$, the diamond operator $\langle d \rangle$ in (3.3) is the automorphism associated with the diagonal matrix $\left(\begin{smallmatrix} d & \\ & d \end{smallmatrix}\right)$.

Definition 3.10 *(Atkin-Lehner automorphisms).* Given $K = H \times \prod B_0(q_i)$ as in (3.1), each q_i yields the Atkin-Lehner map

$$w_{q_i} \colon \mathcal{M}_K \to \mathcal{M}_K\,, \quad (E, \phi, C_1, \dots C_r) \mapsto (E/C_i, \pi_i \circ \phi, \pi_i(C_1), \dots, E[q_i]/C_i, \dots, \pi_i(C_r)) \tag{3.11}$$

where $\pi_i \colon E \to E/C_i$ is the projection.

For a level structure H_p, the Atkin-Lehner automorphism w_p plays a special role, and it is related to the Galois or Frobenius automorphism of the graphs. We will call it Fricke automorphism because it is equal to the classical Fricke involution when $K = B_0(p)$, and to highlight its special role.

Definition 3.12 *(Fricke automorphism).* For a level structure H_p, the Fricke automorphism $\sigma\colon \mathcal{M}_{H_p} \to \mathcal{M}_{H_p}$ maps a curve (E, ϕ, C) to $(E/C, \pi \circ \phi, E[p]/C)$, where $\pi\colon E \to E/C$ is the projection.

4. Relation between modular curves and isogeny graphs and proof of Theorem 2.3.8

In this section we explain the relation between the isogeny graph, together with its adjacency matrix, and the coarse moduli space $M_{H_p,\mathbb{F}_p}$, together with the Hecke operator T_ℓ (see Remark 4.10 for the analysis on the stack).

We fix p, N, H as in Definition 1.3: p is a prime number, N is an integer not divisible by p, and H is a subgroup of $GL_2(\mathbb{Z}/N\mathbb{Z})$. The maps (3.4) give the desingularization

$$\mathrm{pr}_{p,p}^{-1} \sqcup \mathrm{quot}_{p,p}^{-1}\colon M_{H,\mathbb{F}_p} \sqcup M_{H,\mathbb{F}_p} \to M_{H_p,\mathbb{F}_p}\,. \tag{4.1}$$

Since the singularities of $M_{H_p,\mathbb{F}_p}$ are nodal, the pull-back induces an exact sequence

$$0 \to T \to \mathrm{Pic}^0\left(M_{H_p,\mathbb{F}_p}\right) \longrightarrow \mathrm{Pic}^0\left(M_{H,\mathbb{F}_p}\right)^2 \to 0 \tag{4.2}$$

with T the toric part of the semi-abelian variety $\mathrm{Pic}^0\left(M_{H_p,\mathbb{F}_p}\right)$.

To analyze T, we need first to count the connected components of $M_{H,\overline{\mathbb{F}}_p}$. To this end, recall that the Weil invariant of a level structure, see Definition 1.5, gives a morphism

$$w\colon M_H \to \mathrm{Spec}\left(\mathbb{Z}[\tfrac{1}{N}, \zeta_N]^{\det(H)}\right)$$

where ζ_N is a primitive N-th root of the unity, see [21, Chapter 3, Subsection 3.20], and the exponentiation to $\det(H)$ means that we take invariants of $\det(H) \subset (\mathbb{Z}/N\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. If we base change to a field of characteristic prime to N, the fibers of w are irreducible, see [21, Chapter 3, Corollary 5.6]. In particular, there is a bijection between the connected components of $\mathcal{M}_{H,\overline{\mathbb{F}}_p}$ and $R_H = \mu_N^\times(\overline{\mathbb{F}}_p)/\det(H)$, see Definition 1.5 and above.

Call these components M_ξ, for ξ in R_H. The discussion below Equation (3.5) implies that the map $\mathrm{pr}_{p,\mathbb{F}_p}$ is surjective and gives a bijection between the connected components of $M_{H,\overline{\mathbb{F}}_p}$ and the ones of $M_{H_p,\overline{\mathbb{F}}_p}$.

By definition, points on T correspond to line bundles L over M_{H_p} such that both $\left(\mathrm{pr}_{p,p}^{-1}\right)^* L$ and $\left(\mathrm{quot}_{p,p}^{-1}\right)^* L$ are trivial. As recalled in Appendix A, to describe such an L we need to give a scalar for each node of $M_{H_p,\mathbb{F}_p}$, modulo a diagonal action of $\mathbb{G}_\mathrm{m}$ for every connected component M_ξ. Recall that the nodes of $M_{H_p,\mathbb{F}_p}$ are the points representing supersingular curves. Call V_ξ the set of vertices of $G = G(p, \ell, H)$ with Weil invariant ξ, which are in turn the points of M_ξ such that $\mathrm{pr}_{p,p}^{-1}(v)$ is singular in $M_{H_p,\overline{\mathbb{F}}_p}$. With this notation we have a canonical isomorphism

$$T \cong \prod_{\xi \in R_H} T_\xi \quad \text{with} \quad T_\xi := \mathbb{G}_\mathrm{m}^{V_\xi}/\mathbb{G}_\mathrm{m}\,. \tag{4.3}$$

For the groups of characters $T^\vee := \mathrm{Hom}(T, \mathbb{G}_\mathrm{m})$ and $T_\xi^\vee := \mathrm{Hom}(T_\xi, \mathbb{G}_\mathrm{m})$, we obtain

$$T^\vee = \bigoplus_{\xi \in R_H} T_\xi^\vee \quad \text{with} \quad T_\xi^\vee \cong \left\{ x \in \mathbb{Z}^{V_\xi} \,:\, \textstyle\sum_{v \in V_\xi} x_v = 0 \right\}. \tag{4.4}$$

This identifies $T^\vee$ with a submodule of $\mathbb{Z}^V$ and, comparing with Remark 2.3.6, we have a canonical isomorphism $T_\xi^\vee \otimes \mathbb{Q} = \ker(w_*)$ inside $\mathbb{Q}^V$. Moreover, the decomposition $R_H = C_1 \sqcup \ldots \sqcup C_n$ of R_H into the orbits of $\xi \to \xi^\ell$, as in the discussion below Proposition 2.3.2 provides a more refined canonical isomorphism

$$\bigoplus_{\xi \in C_i} T_\xi^\vee \otimes \mathbb{Q} = \ker(w_{i,*}), \tag{4.5}$$

where $\ker(w_{i,*})$ is the subspace of $\mathbb{Q}^V$ described in Remark 2.3.6.

Theorem 4.6. *Let $G = G(p, \ell, H)$ be the graph in Definition 1.3, with G_i the subgraphs defined above Theorem 1.6, and let $T = \prod_{\xi \in R_H} T_\xi$ be the maximal torus of $\mathrm{Pic}^0(M_{H_p, \overline{\mathbb{F}}_p})$, as in Equations (4.2) and (4.3).*

For each i, the isomorphism (4.5) conjugates the action of the Hecke operator T_ℓ to the adjoint action of the adjacency matrix of the graph G_i: i.e. the following diagram is commutative

$$\begin{array}{ccc} \displaystyle\bigoplus_{\xi \in C_i} T_\xi^\vee \otimes \mathbb{Q} & \xrightarrow{T_\ell} & \displaystyle\bigoplus_{\xi \in C_i} T_\xi^\vee \otimes \mathbb{Q} \\ \| & & \| \\ \ker(w_{i,*}) & \xrightarrow{A_i^*} & \ker(w_{i,*}) \end{array}$$

where $\ker(w_{i,*})$ is the subspace of $\mathbb{Q}^V$ described in Remark 2.3.6, and A^* is the adjoint of the adjacency matrix A with respect to the Hermitian form (2.2.3), see also Proposition 2.2.2.

Proof. Let V be the set of vertices of G. Equation (4.4) gives an embedding of $T^\vee$ and $\bigoplus_{\xi \in C_i} T_\xi^\vee$ inside $\mathbb{Z}^V$.

In the Appendix A we described the Picard group of a nodal curve, and how morphism such as the Hecke operator acts on it (it is a rather general theory, and this is why we have discussed it in an appendix). In particular, Proposition A.7 tells us that $T_\ell \colon T^\vee \to T^\vee$ (and in particular also its restriction to $\bigoplus_{\xi \in C_i} T_\xi^\vee$) extends to a map $T_\ell \colon \mathbb{Z}^V \to \mathbb{Z}^V$. It is enough to prove the commutativity of the diagram

$$\begin{array}{ccc} \mathbb{Z}^V \otimes \mathbb{Q} & \xrightarrow{T_\ell \otimes \mathbb{Q}} & \mathbb{Z}^V \otimes \mathbb{Q} \\ \wr\downarrow & & \wr\downarrow \\ \mathbb{Q}^V & \xrightarrow{A^*} & \mathbb{Q}^V \end{array}.$$

In particular, it is enough checking the commutativity on the elements (E_i, ϕ_i) of the canonical basis of $\mathbb{Z}^V$.

On M_{H_p} we have $T_\ell = (\mathrm{quot}_\ell)_* \circ \mathrm{pr}_\ell^*$. Writing $M_{H_p,\mathbb{F}_p}$ as the union of two copies of $M_{H,\mathbb{F}_p}$, Proposition A.7 allows us to describe T_ℓ on $\mathbb{Z}^V$ only looking at what is happening on one of the two copies of $M_{H,\mathbb{F}_p}$. In particular, for each supersingular point (E_i, ϕ_i) on $M_H(\overline{\mathbb{F}}_p)$ we have

$$\begin{aligned} T_\ell(E_i,\phi_i) &= \sum_{(E_j,\phi_j,C)} \mathrm{ord}_{(E_j,\phi_j,C)}(\mathrm{quot}_\ell)\cdot \mathrm{pr}_\ell(E_j,\phi_j,C) \\ &= \sum_{(E_j,\phi_j,C)} \mathrm{ord}_{(E_j,\phi_j,C)}(\mathrm{quot}_\ell)\cdot (E_j,\phi_j)\,, \end{aligned} \tag{4.7}$$

where (E_j, ϕ_j, C) varies in the fiber $\mathrm{quot}_\ell^{-1}(E_i, \phi_i) \subset M_{H_\ell}(\overline{\mathbb{F}}_p)$.

To compute the orders $\mathrm{ord}(\mathrm{quot}_\ell)$ we start by noticing that when H structures are rigid (i.e. when $\mathrm{Aut}(E, \phi) = \{1\}$ for each (E, ϕ) in $M_H(\overline{\mathbb{F}}_p)$), then $\mathrm{ord}(\mathrm{quot}_\ell) = 1$: indeed quot_ℓ has degree $\ell{+}1$ and duality of isogenies gives a bijection between the set of points $(E_j, \phi_j, C) \in \mathrm{quot}_\ell^{-1}(E_i, \phi_i)$ and the set of points $(E_i, \frac{1}{\ell}\phi_i, C) \in M_{H_\ell}(\overline{\mathbb{F}}_p)$ which has cardinality $\ell{+}1$ because $\mathrm{Aut}(E_i, \phi_i)$ is trivial, hence for different subgroups $C_1, C_2 \subset E_i[\ell]$ the triples $(E_i, \frac{1}{\ell}\phi_i, C_1)$ and $(E_i, \frac{1}{\ell}\phi_i, C_2)$ are not isomorphic.

For general H structure, even not rigid, write $M_{H,\mathbb{F}_p} = M_{K,\mathbb{F}_p}/G$ for K a rigid level structure and G a finite group, with quotient map π_G (for example take K to be full-level structures of level $3N$, see [39, Corollary 4.7.2], and $G < \mathrm{GL}_2(\mathbb{Z}/3N\mathbb{Z})$ to be the inverse image of H under reduction modulo N). Analogously we have $M_{H_\ell} = M_{K_\ell}/G$, with quotient map $\pi_{G,\ell}$. Now, given (E_j, ϕ_j, C) supersingular point on M_{H_ℓ}, we can lift it to a point (E_j, ψ_j, C) on M_{K_ℓ}, and, using the commutation $\mathrm{quot}_\ell \circ \pi_{G,\ell} = \pi_G \circ \mathrm{quot}_\ell$, we compute

$$\begin{aligned} \mathrm{ord}_{(E_j,\phi_j,C)}\mathrm{quot}_\ell &= \frac{\mathrm{ord}_{(E_j,\psi_j,C)}(\mathrm{quot}_\ell \circ \pi_{G,\ell})}{\mathrm{ord}_{(E_j,\psi_j,C)}\pi_{G,\ell}} = \frac{\mathrm{ord}_{(E_j,\psi_j,C)}(\pi_G \circ \mathrm{quot}_\ell)}{\mathrm{ord}_{(E_j,\psi_j,C)}\pi_{G,\ell}} \\ &= \frac{\mathrm{ord}_{(E_j,\psi_j,C)}(\mathrm{quot}_\ell)\cdot \mathrm{ord}_{(E_i,\psi_i)}\pi_G}{\mathrm{ord}_{(E_j,\psi_j,C)}\pi_{G,\ell}} = \frac{1\cdot|\mathrm{Aut}(E_i,\phi_i)|}{|\mathrm{Aut}(E_j,\phi_j,C)|}\,. \end{aligned}$$

Substituting in Equation (4.7), and using the definition of a_i in (2.2.1), we get

$$T_\ell(E_i,\phi_i) = \sum_{(E_j,\phi_j,C)} \frac{|\mathrm{Aut}(E_i,\phi_i)|}{|\mathrm{Aut}(E_j,\phi_j,C)|}\cdot(E_j,\phi_j) = a_i \sum_{(E_j,\phi_j,C)} |\mathrm{Aut}(E_j,\phi_j,C)|^{-1}\cdot(E_j,\phi_j)\,, \tag{4.8}$$

where the sums run over the isomorphism classes of triples $(E_j, \phi_j, C) \in M_{H_\ell}(\overline{\mathbb{F}}_p)$ such that $\mathrm{quot}_\ell(E_j, \phi_j, C) := (E_j/C, \pi_C \circ \phi_j)$ is isomorphic to (E_i, ϕ_i). We want to compare the last term of Equation (4.8) with the description of A^* given in Remark 2.2.4.

Observe that (E_j, ϕ_j) appears in the right hand side of (4.8) if and only if there is an arrow $(E_j, \phi_j) \to (E_i, \phi_i)$. The number of such arrows equals the number of nontrivial

subgroups $C \subset E_i[\ell]$ such that $(E_j/C, \pi_C \circ \phi_j) \cong (E_i, \phi_i)$. Two triples (E_j, ϕ_j, C_1) and (E_j, ϕ_j, C_2) give the same element of $M_{H_\ell}(\overline{\mathbb{F}}_p)$ if and only if there exist σ in $\mathrm{Aut}(E_j, \phi_j)/\mathrm{Aut}(E_j, \phi_j, C_1)$ such that $\sigma(C_1) = C_2$. Such σ, if it exists, is unique because we quotiented out exactly by the stabilizer of (E_j, ϕ_j, C_1) in $\mathrm{Aut}(E_j, \phi_j)$. We conclude that the coefficient of (E_j, ϕ_j) in the right hand side of Equation (4.8) is

$$a_i \sum_{\substack{0 \subsetneq C \subsetneq E_j[\ell] \text{ s.t.} \\ (E_j/C, \pi_C \circ \phi_j) \cong (E_i, \phi_i)}} |\mathrm{Aut}(E_j, \phi_j)/\mathrm{Aut}(E_j, \phi_j, C)|^{-1} |\mathrm{Aut}(E_j, \phi_j, C)|^{-1} .$$

As in Remark 2.2.4 we have $a_i = |\mathrm{Aut}(E_j, \phi_j)|$, we have the claim. □

The automorphisms of modular curves act on the Picard groups, and hence on $T^\vee$, via pull-back. The following proposition explains how the canonical isomorphism (4.5) relates the automorphisms of the isogeny graph and the automorphism of the modular curve.

Proposition 4.9. *The sum of the canonical isomorphisms from Equation* (4.5)

$$T^\vee \otimes \mathbb{Q} \xrightarrow{\quad\quad} \oplus_{i=1}^n \ker(w_{i,*})$$

conjugates the Galois map 2.1.1 to the Fricke map 3.12, and the automorphisms from Section 2.1 to the automorphisms from 3.9 and 3.10 with the same name.

Proof. This is an application of Proposition A.7 in the case where G is the identity of $M_{H_p,\mathbb{F}_p}$ and F is one of the automorphisms of $M_{H_p,\mathbb{F}_p}$ we have considered. In particular, it is enough checking that the action of matricial automorphisms, respectively Atkin-Lehner automorphisms and Fricke map, on the supersingular points of $M_{H_p,\mathbb{F}_p}$ is exactly the action of the corresponding automorphisms of the graph. In the first two cases this is straightforward. For the Fricke map σ, we observe that, given a point $(E, \phi, \ker(\mathrm{Frob}_p))$ of $M_{H_p,\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ representing a supersingular elliptic curve, we have

$$\sigma\big(E, \phi, \ker(\mathrm{Frob}_p)\big) = \big(E/\ker(\mathrm{Frob}_p), \pi \circ \phi, E[p]/\ker(\mathrm{Frob}_p)\big) .$$

This is equal to $\big(E^\sigma, \sigma \circ \phi, \ker \mathrm{Frob}_p\big)$ since $E/\ker(\mathrm{Frob}_p)$ is supersingular, hence $E[p]/\ker(\mathrm{Frob}_p)$ must be equal to the kernel of its Frobenius, and the quotient map $\pi\colon E \to E/\ker(\mathrm{Frob}_p)$ is exactly the Frobenius map $\mathrm{Frob}_p\colon E \to E^\sigma$. We conclude that the action of the Fricke map on the points of $M_{H_p,\mathbb{F}_p}$ representing superingular elliptic curves is equal to the Galois action on the corresponding points of the graph. □

Remark 4.10 *(Analogous construction on the moduli stack).* One could carry out the constructions of this section on the stack $\mathcal{M}_{H_p,\mathbb{F}_p}$ rather than the coarse space $M_{H_p,\mathbb{F}_p}$. Observe that when $p \geq 5$, so the characteristic of the base field does not divide the automorphism group, this stack is a twisted curve, as in [1, Section 2]. Twisted curves

are also called stacky curves in the literature. At least in these cases, in [1] is explained how the Picard group is an extension of the Picard group of the coarse space by a finite étale group over $\mathbb{F}_p$ related to the automorphism groups. The study of this extension might give further information about isogeny graphs.

Definition 4.11. Let p be a prime number, N is an integer coprime with p, and H is a subgroup of $GL_2(\mathbb{Z}/N\mathbb{Z})$ as in Definition 1.3, let $\mathcal{A} = \mathcal{A}_{H,p}$ over $\mathbb{Z}[1/N]$ be the connected component of the identity of the kernel of the map

$$\left(\mathrm{pr}_{p,*}, \mathrm{quot}_{p,*}\right) : \mathrm{Pic}^0\left(M_{H_p}\right) \longrightarrow \mathrm{Pic}^0\left(M_H\right) \times \mathrm{Pic}^0\left(M_H\right)$$

The action of the Hecke operator T_ℓ, and the automorphism from Definitions 3.12, 3.9 and 3.10 preserve $\mathcal{A}$, hence we can and do consider their restriction to $\mathcal{A}$.

Proposition 4.12. *Let p be a prime number, N is an integer coprime with p, and H is a subgroup of $GL_2(\mathbb{Z}/N\mathbb{Z})$ as in Definition 1.3. The fiber $\mathcal{A}_{\mathbb{F}_p}$ is equal to the torus T introduced in Equation (4.2).*

Proof. Since $\mathrm{Pic}^0\left(M_{H,\mathbb{F}_p}\right)$ is an abelian variety, and there are no non-trivial maps from a torus to an abelian variety, we have the inclusion $T \subseteq \mathcal{A}_{\mathbb{F}_p}$.

Since $\dim T = \dim \mathrm{Pic}^0\left(M_{H_{p,\overline{\mathbb{F}}_p}}\right) - \dim\left(\mathrm{Pic}^0\left(M_{H_{\overline{\mathbb{F}}_p}}\right) \times \mathrm{Pic}^0\left(M_{H_{\overline{\mathbb{F}}_p}}\right)\right)$, to conclude we have to show that the reduction modulo p of $\left(\mathrm{pr}_{p,*}, \mathrm{quot}_{p,*}\right)$ is surjective.

We look at the resolution given by Equation (4.1) and we consider the map

$$\lambda\colon \mathrm{Pic}^0(M_{H,\mathbb{F}_p})^2 \longrightarrow \mathrm{Pic}^0(M_{H_p,\mathbb{F}_p}), \quad (x,y) \longmapsto (\mathrm{pr}_{p,p}^{-1})_*(x) + (\mathrm{quot}_{p,p}^{-1})_*(y).$$

By the same arguments used in the proof of Theorem 3.7, (or see also the diagram in [21, page 145]), we have that $\left(\mathrm{pr}_{p,*}, \mathrm{quot}_{p,*}\right)_{\mathbb{F}_p} \circ \lambda$ equals $\left(\begin{smallmatrix} \mathrm{Id} & \mathrm{Frob} \\ \mathrm{Frob} & \mathrm{Id} \end{smallmatrix}\right)$ as endomorphism of $\mathrm{Pic}^0(M_{H,\mathbb{F}_p})^2$; this endomorphism is surjective, hence the same is true for $\left(\mathrm{pr}_{p,*}, \mathrm{quot}_{p,*}\right)_{\mathbb{F}_p}$. □

The following key technical lemma uses the theory of Néron models, a general reference for Néron models is [12].

Lemma 4.13. *Fix p, N, H as in Definition 1.3 and let $\mathcal{A} = \mathcal{A}_{H_p}$. Then, for every endomorphism F of $\mathcal{A}$ and every prime number q not dividing N, we have*

$$\dim(\mathrm{Im}\,(F|_{\mathcal{A}_{\mathbb{C}}})) = \dim\left(\mathrm{Im}\left(F|_{\mathcal{A}_{\overline{\mathbb{F}}_q}}\right)\right).$$

Proof. By [21, Proposition 6.7 and Theorem 6.9, pages 143-145], both $M_H/\mathbb{Z}[\frac{1}{N}]$ and $M_{H_p}/\mathbb{Z}[\frac{1}{N}]$ have reduced fibers, and geometrically irreducible generic fiber. Again by [21], M_H is regular, but M_{H_p} might not be: it is smooth away from supersingular elliptic

curves (E, ϕ, C) in characteristic p, and locally around such points it is isomorphic to $\mathbb{Z}_p[[w,z]]/(wz - p^k)$, where k is either $\#Aut(E,\phi,C)$, or half of it if -1 is an automorphism. To reduce to the regular case we can blow-up the non-regular points. In this way, we introduce a chain of $\mathbb{P}^1$'s on the fiber over p; this chain does not alter the Pic^0, hence we can assume by abuse of notation that also M_{H_p} is regular.

We now localize at q and apply [12, Theorem 4 (b), Section 9.5, page 267]: both $\mathrm{Pic}^0\left(M_{H_p}\right)$ and $\mathrm{Pic}^0\left(M_H\right)$ are the connected component of the identity of the Néron models of $\mathrm{Pic}^0\left(M_{H_p}\right)_{\mathbb{Q}}$ and $\mathrm{Pic}^0\left(M_H\right)_{\mathbb{Q}}$, hence $\mathcal{A}$ is the connected component of the identity of the Néron model of $\mathcal{A}_{\mathbb{Q}}$ (this last assertion can be checked using the universal property of Néron models). Moreover, by Lemma 4.14 and [21, Proposition 6.7, page 143], $\mathcal{A}$ has semi-abelian reduction.

When there is semi-abelian reduction, by [12, Proposition 3, section 7.5, page 186], taking Néron models is exact up to isogeny, so we have the claim. □

Now, we start looking at the singular cohomology of the complex variety $\mathcal{A}(\mathbb{C})$, we will denote it by $H^{1\mathrm{sing}}(\mathcal{A}(\mathbb{C}),\mathbb{Z})$. This cohomology group will be used to compare the adjacency matrix of the graph with the action of the Hecke operator on the étale cohomology $H^{1,\text{ét}}(\mathcal{A}_{\overline{\mathbb{F}}_\ell},\mathbb{Q}_{\ell'})$, where we have the bound on the eigenvalues from Theorem 3.8.

Lemma 4.14. *Fix p, ℓ, H as in Definition 1.3. Let $\mathcal{A}$ be the abelian variety in Definition 4.11 and let $T^\vee$ be the group of characters of the torus T introduced in Equation (4.2).*

There is a (non-canonical) isomorphism of T_ℓ modules

$$(T^\vee \otimes \mathbb{Q})^{\oplus 2} \cong H^{1,sing}(\mathcal{A}(\mathbb{C}),\mathbb{Z}) \otimes \mathbb{Q}$$

which is equivariant for the automorphisms from Definitions 3.9, 3.12 and 3.10.

Proof. First we show that there exists a non-canonical isomorphism γ of T_ℓ-modules. For this it is enough showing a $\mathbb{Q}$-linear isomorphism between $T^\vee \otimes \mathbb{Q}$ and $H^{1,\mathrm{sing}}(\mathcal{A}(\mathbb{C}),\mathbb{Z}) \otimes \mathbb{Q}$, as $\mathbb{Q}[x]$-modules, with x acting as T_ℓ. Since $\mathbb{Q}[x]$ is a PID, it is enough showing that for every polynomial q in $\mathbb{Z}[x]$, the rank of $F := q(T_\ell)$ is equal on both spaces. The morphism F is an endomorphism of $\mathcal{A}$. The rank of F restricted to $T^\vee \otimes \mathbb{Q}$ is equal to $\dim(\mathrm{Im}\left(F|_{\mathcal{A}_{\overline{\mathbb{F}}_\ell}}\right))$. The rank of F on $H^{1,\mathrm{sing}}(\mathcal{A}(\mathbb{C}),\mathbb{Q}) = H^{1,\mathrm{sing}}(\mathcal{A}(\mathbb{C}),\mathbb{Z}) \otimes \mathbb{Q}$ is equal to twice $\dim(\mathrm{Im}\left(F|_{\mathcal{A}_{\mathbb{C}}}\right))$. We obtain the claim by Lemma 4.13.

We now show that γ can be chosen equivariant for all automorphisms. Let G be the group formed by these automorphisms. Theorem 4.6 and Proposition 2.2.2 imply that T_ℓ is semi-simple: we can decompose both $V = (T^\vee \otimes \mathbb{Q})^{\oplus 2}$ and $W = H^{1,\mathrm{sing}}(\mathcal{A}(\mathbb{C}),\mathbb{Z}) \otimes \mathbb{Q}$ in "eigenspaces", i.e. subspaces V_μ, W_μ of the form $\ker(\mu(T_\ell))$ for $\mu \in \mathbb{Q}[x]$ an irreducible polynomial. Notice that $\mathbb{Q}[T_\ell]$ acts as the field $K = \mathbb{Q}[x]/\mu$ on V_μ and W_μ. Since G commutes with T_ℓ, then it preserves such eigenspaces and we are left to prove that $V_\mu \cong W_\mu$ as $K[G]$-modules. To this end, since G is finite, it is enough to show that the

characters of these two representations are the same. Since each $g \in G$ has finite order, the actions of g on V_μ, W_μ are separable, and the traces over K are equal if for each $p \in K[x]$ the ranks of $p(g)$ are equal: this is a consequence of the fact that V_μ and W_μ can be described as the images of a certain polynomial in T_ℓ and of Lemma 4.13 applied to endomorphisms induced by polynomials in g and T_ℓ. □

The following lemma is a rather general fact.

Lemma 4.15. *Fix p, ℓ, H as in Definition 1.3. Let $\mathcal{A}$ be the abelian variety in Definition 4.11 and denote $H^{*,sing}$ the singular cohomology.*

For any prime ℓ' which does not divide $p\ell N$, we have an isomorphism of T_ℓ modules

$$H^{1,\acute{e}t}(\mathcal{A}_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_{\ell'}) \cong H^{1,sing}(\mathcal{A}(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Q}_{\ell'}\,,$$

which is equivariant for the automorphisms from Definitions 3.12, 3.9 and 3.10.

Proof. The isomorphism is given by the cospecialization map, let us explain the argument. By proper-smooth base change theorem (see [47, Theorem 20.4]), the cospecialization map

$$H^{1,\text{ét}}(\mathcal{A}_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_{\ell'}) \longrightarrow H^{1,\text{ét}}(\mathcal{A}_{\mathbb{C}}, \mathbb{Q}_{\ell'})\,, \tag{4.16}$$

is an isomorphism. Since the cospecialization map is functorial, then it is an isomorphism of T_ℓ modules.

Moreover, since $\mathcal{A}_{\mathbb{C}}$ is a smooth variety over $\mathbb{C}$, then the comparison theorem [47, Theorem 21.1] tells us that, for each positive integer k, we have isomorphisms

$$H^{1,\text{ét}}(\mathcal{A}_{\mathbb{C}}, \mathbb{Z}/(\ell')^k\mathbb{Z}) \cong H^{1,\text{sing}}(\mathcal{A}(\mathbb{C}), \mathbb{Z}/(\ell')^k\mathbb{Z})$$

Since the above isomorphism is functorial, then, again, it also an isomorphism of T_ℓ modules. The proof of the second statement is analogous. □

The following result sums up Theorem 4.6, Lemma 4.14 and Lemma 4.15

Theorem 4.17 *(Relation between isogeny graphs and modular curves). Fix p, ℓ, H as in Definition 1.3. Let $\mathcal{A}$ be the abelian variety in Definition 4.11, and $\ker(w_{i,*})$ as in Remark 2.3.6.*

For any prime ℓ' which does not divide $p\ell N$, there is a non-canonical isomorphism

$$H^{1,\acute{e}t}(\mathcal{A}_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_{\ell'}) \cong (\ker(w_{i,*}) \otimes \mathbb{Q}_{\ell'})^{\oplus 2}$$

which conjugates the action of the Hecke operator T_ℓ to the action of the adjacency matrix of the isogeny graph.

Moreover, one can find an isomorphism that conjugates the Galois map 2.1.1 to the Fricke map 3.12, and the automorphisms from Section 2.1 to the automorphisms from 3.9 and 3.10 with the same name.

(As funny byproduct, this result shows the well-known fact that the minimal polynomial of the Hecke operator is defined over $\mathbb{Z}$.)

We are now ready to prove Theorem 2.3.8 about isogeny graphs used in Section 2.

Theorem 4.18 *(see Theorem 2.3.8). The absolute values of the eigenvalues of A_i restricted to $\ker(w_{i,*}) \otimes \mathbb{C}$ are strictly smaller than $2\sqrt{\ell}$.*

Proof. Because of Theorem 4.17, the eigenvalues of A_i are the eigenvalue of the Hecke operator T_ℓ acting on cohomology a sub-abelian variety $\mathcal{A}$ of the Jacobian of a modular curve. Then, the combination of Eichler-Shimura relation and Weil conjectures stated in Theorems 3.7, 3.8 implies that the absolute values of the eigenvalues are less or equal than $2\sqrt{\ell}$.

In the spirit of the proof of [16, Theorem 2.1], we prove arguing by contradiction that the absolute values of the eigenvalues cannot be equal to $2\sqrt{\ell}$. Suppose that $T_\ell \circlearrowright H^{1,\text{ét}}(\mathcal{A}_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_{\ell'})$ has a complex eigenvalue of absolute value $2\sqrt{\ell}$. By Proposition 2.2.2, such an eigenvalue, has an angle in $\frac{\pi}{k'}\mathbb{Z}$ for k' an integer, implying that $T_\ell^{2k'} - (4\ell)^{k'}$ is not surjective on $H^{1,\text{ét}}(\mathcal{A}_{\overline{\mathbb{F}}_\ell}, \mathbb{Q}_{\ell'})$ nor, by Lemma 4.15, on $H^{1,\text{sing}}(\mathcal{A}(\mathbb{C}), \mathbb{Q})$. We deduce that $\ker(T_\ell^{2k'} - (4\ell)^{k'})$ in $\mathcal{A}$ is not finite, hence its connected component of identity B is a sub-abelian variety of $\mathcal{A}$ defined over $\mathbb{Q}$ of positive dimension.

The abelian variety B has good reduction modulo ℓ, since it is a quotient of the Jacobian of a modular curve which has good reduction modulo ℓ (indeed having good reduction is stable under isogeny and quotients).

On the cohomology of $B_{\mathbb{F}_\ell}$ we have the Eichler-Shimura relation 3.7 $T_\ell = \text{Frob} + \langle \ell \rangle \text{Ver}$. Because of this, if an eigenvalue of T_ℓ has absolute value $2\sqrt{\ell}$, then Frob and $\langle \ell \rangle$Ver must have exactly the same eigenvalues relative to the same eigenvectors; we conclude that $T_\ell = 2\text{Frob}$ on $B_{\mathbb{F}_\ell}$. This implies that the action $T_\ell \circlearrowright H^0(B_{\mathbb{F}_\ell}, \Omega^1)$ is zero. Furthermore, in the case $\ell = 2$, it implies that the action of T_ℓ on $H^0(B, \Omega^1)$ is a multiple of 2, and also the action $\frac{T_\ell}{2} \circlearrowright H^0(B_{\mathbb{F}_\ell}, \Omega^1)$ is zero. By the good reduction, we can consider the free $\mathbb{Z}_\ell$-module $M := H^0(B_{\mathbb{Z}_\ell}, \Omega^1)$, and $M \otimes_{Z_\ell} \mathbb{F}_\ell = H^0(B_{\mathbb{F}_\ell}, \Omega^1)$. Knowing the action of T_ℓ and $\frac{T_\ell}{2}$ on $M \otimes \mathbb{F}_\ell$, we deduce that the action $T_\ell \circlearrowright M$ must be a multiple of 2ℓ, hence its determinant must be a multiple of $(2\ell)^{\text{rank}M} = 2^{\dim B} \ell^{\dim B}$. This is absurd since by looking at the eigenvalues, the determinant of $T_\ell \circlearrowright M$ is a root of unity times $(2\sqrt{\ell})^{\dim B} = 2^{\dim B} \ell^{\dim B/2}$. Hence there are no eigenvalues of T_ℓ of absolute value $2\sqrt{\ell}$. □

5. Relation with modular forms

In this section we identify our spaces $\ker(w_{i,*})$ from Remark 2.3.6 with spaces of modular forms. We start from the following lemma.

Lemma 5.1. *Fix p, ℓ, H as in Definition 1.3. Let $\mathcal{A}$ be the abelian variety in Definition 4.11 and let $T^\vee$ be the group of characters of the torus T introduced in Equation (4.2).*

We have a (non-canonical) isomorphism of T_ℓ modules

$$T^\vee \otimes \mathbb{C} \cong H^0(\mathcal{A}_{\mathbb{C}}, \Omega^1)$$

which is equivariant for the automorphisms u from Definitions 3.9, 3.12 and 3.10, acting by pullback on $\mathcal{A}$, hence as $u^{*,\vee}$ on $T^\vee$ and as $(u^*)^*$ (see Remark 5.2) on the differentials of $\mathcal{A}_{\mathbb{C}}$.

Proof. It is enough giving an isomorphism $T^\vee \otimes \mathbb{C} \cong H^0(\mathcal{A}_{\mathbb{C}}, \Omega^1)$, which is analogous to Lemma 4.14. □

Remark 5.2. For a map of curves $u\colon X \to Y$, we have the pullback $u^*\colon \mathrm{Pic}^0(Y) \to \mathrm{Pic}^0(X)$ and its pullback

$$(u^*)^*\colon H^0(\mathrm{Pic}^0(X), \Omega^1) = H^0(X, \Omega^1) \longrightarrow H^0(\mathrm{Pic}^0(Y), \Omega^1) = H^0(Y, \Omega^1)\,.$$

Then, the above map is equal to the pushforward of differentials $u_*\colon H^0(X, \Omega^1) \to H^0(Y, \Omega^1)$. In particular, in Lemma 5.1, an automorphism u acts as the restriction of u_* on $H^0(\mathcal{A}_{\mathbb{C}}, \Omega^1)$

The above Lemma, together with Theorem 4.6, suggests the study differentials on $\mathcal{A}$: in Theorems 5.5.2 and 5.5.5 we relate these differentials with modular forms.

To include non-connected modular curves in our analysis, in Subsections 5.1 - 5.4 we recall the notation, mainly following [22], and collect some slightly cumbersome computations.

5.1. Complex points on modular curves

Analogously to [21, IV.5.3], using the definition $\mathbb{H}^\pm := \mathbb{C} - \mathbb{R}$ and its "compactification" $\overline{\mathbb{H}}^\pm := \mathbb{H}^\pm \cup \mathbb{P}^1(\mathbb{Q})$, we have a (canonical) isomorphism of Riemann surfaces

$$\mathrm{GL}_2(\mathbb{Z})\backslash\left(\overline{\mathbb{H}}^\pm \times (\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/H)\right) \xrightarrow{\sim} M_H(\mathbb{C}), \tag{5.1.1}$$

where for each τ's in $\mathbb{H}^\pm$ (on proper elliptic curves) the map identifies

$$(\tau, \gamma H) \longmapsto (E_\tau, \phi_\tau \circ \gamma) = (\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau), \phi_\tau \circ \gamma), \quad \phi_\tau \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right) = \tfrac{\tau}{N}\,, \phi_\tau \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right) = \tfrac{1}{N}\,.$$

In the above isomorphism $\mathrm{GL}_2(\mathbb{Z})$ acts by

$$\begin{aligned} g \cdot (\tau, \gamma H) &:= (g(\tau), \bar{g}^{-T}\gamma H) \qquad \text{i.e.} \\ \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)(\tau, \gamma H) &= \left(\tfrac{a\tau+b}{c\tau+d},\ \tfrac{1}{\det g}\left(\begin{smallmatrix}d & -c\\ -b & a\end{smallmatrix}\right)\gamma H\right)\,. \end{aligned} \tag{5.1.2}$$

For the subgroup $H_p < \mathrm{GL}_2(\mathbb{Z}/Np\mathbb{Z})$, Equation (5.1.1) can be rephrased as

$$\Gamma^0(p)\backslash\big(\overline{\mathbb{H}}^{\pm} \times \tfrac{\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})}{H}\big) \xrightarrow{\sim} M_{H_p}(\mathbb{C})\,, \qquad (\tau,\gamma) \longmapsto (E_\tau, \phi_\tau \circ \gamma, \langle \tfrac{\tau}{p}\rangle)\,, \tag{5.1.3}$$

where $\Gamma^0(p)$ is the subgroup of $\mathrm{GL}_2(\mathbb{Z})$ made of matrices congruent to $\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)$ modulo p.

Using the above isomorphisms the maps pr_p and quot_p in (3.4) become

$$\begin{gathered} \mathrm{pr}_p,\, \mathrm{quot}_p : \Gamma^0(p)\backslash\big(\mathbb{H}^{\pm} \times \tfrac{\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})}{H}\big) \longrightarrow \mathrm{GL}_2(\mathbb{Z})\backslash\big(\mathbb{H}^{\pm} \times \tfrac{\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})}{H}\big)\,, \\ \mathrm{pr}_p(\tau,\gamma) = (\tau,\gamma)\,, \qquad \mathrm{quot}_p(\tau,\gamma) = \big(\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\tau, \left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)\gamma\big) \end{gathered} \tag{5.1.4}$$

The isomorphisms (5.1.1) (5.1.3) also help us recognize the components, over $\mathbb{C}$, of modular curves: choosing representatives $g_1, \dots, g_r$ for the quotient $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/(H \cdot \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$, we get the following (non-canonical) decomposition into connected components

$$\begin{aligned} M_H(\mathbb{C}) &\cong \coprod_{j=1}^{r} \Gamma_{g_j H g_i^{-1}}\backslash\overline{\mathbb{H}}\,, \qquad (E_\tau, \phi_\tau \circ g_j) \longleftarrow\!\shortmid (\tau, g_j)\,, \\ M_{H_p}(\mathbb{C}) &\cong \coprod_{j=1}^{r} \big(\Gamma^0(p) \cap \Gamma_{g_j H g_i^{-1}}\big)\backslash\overline{\mathbb{H}}\,, \qquad \Big(E_\tau, \phi_\tau \circ g_j, \langle \tfrac{\tau}{p}\rangle\Big) \longleftarrow\!\shortmid (\tau, g_j)\,, \end{aligned} \tag{5.1.5}$$

where $\overline{\mathbb{H}} = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ is the "compactification" of $\mathbb{H} = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}$, and where

$$\Gamma_H := \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma^T \pmod n \text{ lies in } H\}.$$

Remark 5.1.6. In Equation (5.1.3) we use $\Gamma^0(p) = \Gamma_{B^0(p)}$, with $B^0(p)$ the Borel group $\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\}$ (notice the transposition in (5.1.2)). Since conjugation of the H_p gives an isomorphic modular curve, we can also use $B_0(p) = \{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\} = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) B^0(p) \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)^{-1}$, yielding a variant of (5.1.3):

$$\Gamma_0(p)\backslash\big(\overline{\mathbb{H}}^{\pm} \times \tfrac{\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})}{H}\big) \xrightarrow{\sim} M_{H_p}(\mathbb{C})\,, \qquad (E_\tau, \phi_\tau \circ \gamma, \langle \tfrac{1}{p}\rangle) \longleftarrow\!\shortmid (\tau,\gamma)\,, \tag{5.1.7}$$

for $\Gamma_0(p) = \Gamma_{B_0(p)} = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}) : c \equiv 0 \pmod p\}$.

5.2. Modular forms and differentials

For any congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$, the map $f \mapsto f\mathrm{d}\tau$ gives an isomorphism between the space $S_2(\Gamma)$ of cuspidal modular forms of weight 2 and the space $H^0(\Gamma\backslash\overline{\mathbb{H}}, \Omega^1)$ of holomorphic differentials on $\Gamma\backslash\overline{\mathbb{H}}$, see [22, Section 3.3 and Excercise 3.3.6] or [48, Theorem 2.3.2]. This, together with (5.1.5) implies the isomorphisms

$$H^0(M_{H,\mathbb{C}},\Omega^1)\cong\bigoplus_{j=1}^{r}S_2\left(\Gamma_{g_jHg_i^{-1}}\right),\qquad H^0(M_{H_p,\mathbb{C}},\Omega^1)\cong\bigoplus_{j=1}^{r}S_2\left(\Gamma_{g_jHg_i^{-1}}\cap\Gamma^0(p)\right).\tag{5.2.1}$$

5.3. Full level case

When $H=\{\mathrm{Id}\}$, we write M_N for M_H and $\Gamma(N)$ for Γ_H, which contains matrices in $\mathrm{SL}_2(\mathbb{Z})$ congruent to $\left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ modulo N. Choosing $\{g_i\}=\{\left(\begin{smallmatrix}a&0\\0&1\end{smallmatrix}\right):a\in(\mathbb{Z}/N\mathbb{Z})^\times\}$, Equation (5.1.5) gives

$$M_N(\mathbb{C})\cong\bigsqcup_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\Gamma(N)\backslash\overline{\mathbb{H}},\quad M_{\{\mathrm{Id}\}\times B_0(p)}(\mathbb{C})\cong\bigsqcup_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\big(\Gamma^0(p)\cap\Gamma(N)\big)\backslash\overline{\mathbb{H}},\tag{5.3.1}$$

and, compatibly with these isomorphisms, the maps pr, quot are

$$\begin{aligned}\mathrm{pr}_p,\,\mathrm{quot}_p:\bigsqcup_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\big(\Gamma^0(p)\cap\Gamma(N)\big)\backslash\overline{\mathbb{H}}&\longrightarrow\bigsqcup_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}\Gamma(N)\backslash\overline{\mathbb{H}},\\ \mathrm{pr}_p(\tau,a)=(\tau,a),\qquad\mathrm{quot}_p(\tau,a)&=(\left(\begin{smallmatrix}1&0\\0&q\end{smallmatrix}\right)\tau,pa)\end{aligned}\tag{5.3.2}$$

Moreover, Equation (5.2.1) becomes

$$\begin{aligned}H^0(M_{N,\mathbb{C}},\Omega^1)&\cong\bigoplus_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}S_2\left(\Gamma(N)\right)=S_2\left(\Gamma(N)\right)\otimes_{\mathbb{C}}\mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times},\\ H^0(M_{\{\mathrm{Id}\}\times B^0(p),\mathbb{C}},\Omega^1)&\cong\bigoplus_{a\in(\mathbb{Z}/N\mathbb{Z})^\times}S_2\left(\Gamma(N)\cap\Gamma^0(p)\right)=S_2\left(\Gamma(N)\cap\Gamma^0(p)\right)\otimes_{\mathbb{C}}\mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}\end{aligned}\tag{5.3.3}$$

5.4. Hecke operators

As in [22, Section 5.1], we recall the definition of double coset operators: given $\Gamma_1,\Gamma_2<\mathrm{SL}_2(\mathbb{Z})$ congruence subgroups, and given $\alpha\in\mathrm{GL}_2^{\det>0}(\mathbb{Q})$, we have the operator

$$[\Gamma_1\alpha\Gamma_2]_2\colon M_2(\Gamma_1)\to M_2(\Gamma_2),\quad f[\Gamma_1\alpha\Gamma_2]_2=\sum_j f[\alpha\gamma_j]_2,\tag{5.4.1}$$

where $f[\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)]_2(\tau)=\det\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\frac{1}{(c\tau+d)^2}f\left(\frac{a\tau+b}{c\tau+d}\right)$, and $\{\gamma_j\}$ is a set of representatives for $\Gamma_3\backslash\Gamma_2$, with $\Gamma_3=\alpha^{-1}\Gamma_1\alpha\cap\Gamma_2$. We can interpret the operator (5.4.1) as follows: we have maps

$$\begin{array}{ccc}\Gamma_3\backslash\overline{\mathbb{H}}&\xrightarrow{\alpha\colon\tau\mapsto\alpha\tau}&\alpha\Gamma_3\alpha^{-1}\backslash\overline{\mathbb{H}}\\ \downarrow{\scriptstyle\pi_2\colon\tau\mapsto\tau}&&\downarrow{\scriptstyle\pi_1\colon\tau\mapsto\tau}\\ \Gamma_2\backslash\overline{\mathbb{H}}&&\Gamma_1\backslash\overline{\mathbb{H}}\end{array}\tag{5.4.2}$$

and, under the isomorphism (5.2.1), we have $[\Gamma_1\alpha\Gamma_2]_2 = \pi_{2,*}\circ(\pi_1\alpha)^*$. A particular case are the classical Hecke operators in the theory of modular forms, see [22, Section 5.2]:

$$\tilde{T}_\ell := [\Gamma \left(\begin{smallmatrix}1&0\\0&\ell\end{smallmatrix}\right)\Gamma]_2 = \pi_*\circ\left(\begin{smallmatrix}1&0\\0&\ell\end{smallmatrix}\right)^*, \qquad \left(\begin{smallmatrix}1&0\\0&\ell\end{smallmatrix}\right),\pi\colon \left(\Gamma^0(\ell)\cap\Gamma\right)\backslash\overline{\mathbb{H}} \to \Gamma\backslash\overline{\mathbb{H}} \tag{5.4.3}$$

where $\left(\begin{smallmatrix}1&0\\0&\ell\end{smallmatrix}\right)\tau = \frac{\tau}{\ell}$, $\pi\tau = \tau$, and we consider $\Gamma = \Gamma_H$ for $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ any subgroup that is normalized by diagonal matrices.

In the case $\Gamma = \Gamma(N)$, we want to compare $\tilde{T}_\ell$ with the Hecke operator T_ℓ in Definition 3.6. Indeed T_ℓ acts as $\mathrm{quot}_{\ell,*}\circ\mathrm{pr}_\ell^*$ on $\mathrm{Pic}^0(M_N)$, hence it acts by pull back as $\mathrm{pr}_{\ell,*}\circ\mathrm{quot}_\ell^*$ on $H^0(\mathrm{Pic}^0(M_{N,\mathbb{C}}),\Omega^1) = H^0(M_{N,\mathbb{C}},\Omega^1)$. By (5.3.3), this space of differentials is isomorphic to $S_2(\Gamma(N))\otimes_{\mathbb{C}}\mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}$ and, under this identification, Equation (5.3.2) tells that $\mathrm{pr}_{\ell,*} = \pi_*\otimes\mathrm{Id}$ and that $\mathrm{quot}_\ell^* = \left(\begin{smallmatrix}1&0\\0&\ell\end{smallmatrix}\right)^*\otimes\sigma_\ell$, where $\sigma_\ell\colon \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times} \to \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}$ is the "shift by ℓ" namely $(z_a)\mapsto(z_{a\ell})$, and the maps $\pi, \left(\begin{smallmatrix}1&0\\0&\ell\end{smallmatrix}\right)$ are the same appearing in (5.4.3). We deduce that

$$T_\ell = \tilde{T}_\ell\otimes_{\mathbb{C}}\sigma_\ell \quad \text{ in } H^0(\mathrm{Pic}^0(M_{N,\mathbb{C}}),\Omega^1) = S_2(\Gamma(N))\otimes_{\mathbb{C}}\mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}. \tag{5.4.4}$$

We have an analogous equality for $H = \{\mathrm{Id}\}\times B_0(p)$: using the second line in (5.3.3)

$$T_\ell = \tilde{T}_\ell\otimes_{\mathbb{C}}\sigma_\ell \quad \text{ in } H^0(\mathrm{Pic}^0(M_{\{\mathrm{Id}\}\times B_0(p),\mathbb{C}}),\Omega^1) = S_2(\Gamma^0(p)\cap\Gamma(N))\otimes_{\mathbb{C}}\mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}. \tag{5.4.5}$$

5.5. Graphs versus modular forms

In this section we study $H^0(\mathcal{A}_{\mathbb{C}},\Omega^1)$. Definition 4.11 gives the canonical isomorphism

$$H^0(\mathcal{A}_{\mathbb{C}},\Omega^1) = \frac{H^0(M_{H_p,\mathbb{C}},\Omega^1)}{\mathrm{pr}_p^*H^0(M_{H,\mathbb{C}},\Omega^1) + \mathrm{quot}_p^*H^0(M_{H_p,\mathbb{C}},\Omega^1)}.$$

We start by looking at the case $H = \{\mathrm{Id}\}$, where Equation (5.3.2) gives an explicit description of $\mathrm{pr}_p^*, \mathrm{quot}_p^*$. Instead of taking a quotient, we can take the orthogonal complement with respect to the Petersson inner product (see [22, Section 5.5]): following [53], we define the space of p-new forms as

$$S_2^{p\text{-new}}(\Gamma^0(p)\cap\Gamma(N)) := \left(S_2(\Gamma(N)) + S_2(\Gamma(N)[\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)]_2)\right)^\perp \subset S_2(\Gamma^0(p)\cap\Gamma(N)),$$

which, by the same arguments in [22, Proposition 5.5.2 and Proposition 5.6.2], is $\tilde{T}_\ell$-stable. In particular, using the description ((5.4.5) of the Hecke operator, we get the isomorphism

$$T_\ell \curvearrowright H^0(\mathcal{A}_{\{\mathrm{Id}\},p,\mathbb{C}},\Omega^1) \cong S_2^{p\text{-new}}(\Gamma^0(p)\cap\Gamma(N))\otimes_{\mathbb{C}}\mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times} \curvearrowleft \tilde{T}_\ell\otimes\sigma_\ell.$$

To treat the case of a general H, we recall that $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $M_{\{\mathrm{Id}\}\times B_0(p)}$ by the law $(E,\phi,C)^g = (E,\phi\circ g, C)$. Using (5.1.2) and (5.3.1), we can characterize this action as follows:

$$\begin{aligned}(\tau, \left(\begin{smallmatrix} a & 0 \\ 0 & 1\end{smallmatrix}\right))^g &= (\tau, \left(\begin{smallmatrix} ad & 0 \\ 0 & 1\end{smallmatrix}\right)) \qquad \text{if } g = \left(\begin{smallmatrix} d & 0 \\ 0 & 1\end{smallmatrix}\right),\\ (\tau, \left(\begin{smallmatrix} a & 0 \\ 0 & 1\end{smallmatrix}\right))^g &= (\tilde{g_a}\tau, \left(\begin{smallmatrix} a & 0 \\ 0 & 1\end{smallmatrix}\right)) \qquad \text{if } \det g = 1,\end{aligned}$$

where $\tilde{g_a}$ is any matrix in $\Gamma^0(p)$ that is congruent to $\left(\left(\begin{smallmatrix} a & 0 \\ 0 & 1\end{smallmatrix}\right) g \left(\begin{smallmatrix} a & 0 \\ 0 & 1\end{smallmatrix}\right)^{-1}\right)^t$ modulo N. We get an action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ by pullback on $H^0(\mathcal{A}_{\{\mathrm{Id}\},p,\mathbb{C}},\Omega^1) \subset H^0(M_{\{\mathrm{Id}\}\times B_0(p)})$ as follows:

$$\begin{gathered}\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \curvearrowright S_2^{p\text{-new}}(\Gamma^0(p)\cap\Gamma(N)) \otimes_{\mathbb{C}} \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times} = \bigoplus_{a\in(\mathbb{Z}/N\mathbb{Z})^\times} S_2^{p\text{-new}}(\Gamma^0(p)\cap\Gamma(N)),\\ \left(\begin{smallmatrix} d & 0 \\ 0 & 1\end{smallmatrix}\right)\cdot(f_a)_a = (f_{ad})_a, \quad g\cdot(f_a)_a = (f_a[\tilde{g_a}]_2)_a \text{ if } \det g = 1,\end{gathered} \tag{5.5.1}$$

where the operation $[\cdot]_2$ is as in (5.4.1), and $\tilde{g_a}$ is chosen as above. Since pullback of differentials along the natural projection $M_{\{\mathrm{Id}\}\times B_0(p)} \to M_{H_p}$ identifies $H^0(\mathcal{A}_{H,p},\Omega^1)$ with the subspace of $H^0(\mathcal{A}_{\{\mathrm{Id}\},p},\Omega^1)$ made of H-invariant differentials, we get the isomorphism

$$T_\ell \curvearrowright H^0(\mathcal{A}_{H,p,\mathbb{C}},\Omega^1) \cong \left(S_2^{p\text{-new}}(\Gamma^0(p)\cap\Gamma(N)) \otimes_{\mathbb{C}} \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}\right)^H \curvearrowleft \tilde{T}_\ell \otimes \sigma_\ell .$$

This, together with Lemma 5.1, Theorem 4.6 and the fact that A is conjugate to A^* (Proposition 2.2.2) implies the following result.

Theorem 5.5.2. *Let $G = G(p,\ell,H)$ be the graph in Definition 1.3, let $\ker(w_*), \ker(w_{i,*})$ be the subspaces of $\mathbb{C}^{V(G)}$ described in 2.3.6 and let S be the p-new part of $S_2(\Gamma^0(p)\cap\Gamma(N))$. Then*

$$A \curvearrowright \bigoplus_{i=1}^n \ker(w_{i,*}) \xleftrightarrow{\ \sim\ } \left(S\otimes_{\mathbb{C}} \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}\right)^H \curvearrowleft \tilde{T}_\ell\otimes\sigma_\ell .$$

In words $\ker(w_*) = \oplus_i \ker(w_{i,*})$, as a module over the adjacency matrix of the graph, is isomorphic to the subspace of $S\otimes_{\mathbb{C}} \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}$ fixed by H, as a module over $\tilde{T}_\ell\otimes\sigma_\ell$ (for the action of $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ see (5.5.1)).

Remark 5.5.3. In Remark 5.1.6 we pointed out that M_{H_p} can be described using either $\Gamma^0(p)$ or $\Gamma_0(p)$. Following the same lines, Theorem 5.5.2 remains true after substituting $S_2^{p\text{-new}}(\Gamma^0(p)\cap\Gamma(N))$ with

$$S_2^{p\text{-new}}(\Gamma_0(p)\cap\Gamma(N)) := \left(S_2(\Gamma(N)) + S_2(\Gamma(N))[\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_2\right)^{\perp} \quad \subset S_2(\Gamma_0(p)\cap\Gamma(N))\,,$$

and after slightly modifying the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ in (5.5.1), i.e. asking that $\tilde{g_a} \in \Gamma_0(p)$.

We also rephrase Theorem 5.5.2, for certain choices of H, using modular forms for

$$\Gamma_1(k) = \{m \in \mathrm{SL}_2(\mathbb{Z}) : m \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \bmod k\}\,, \quad \Gamma_0(k) = \{m \in \mathrm{SL}_2(\mathbb{Z}) : m \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod k\}.$$

Such modular forms received more attention in the literature, e.g. in the asymptotic estimates in [56] which we later use. We use the decomposition, (see [22, Section 4.3, page 119]),

$$S_2(\Gamma_1(k)) = \bigoplus_{\chi \in (\mathbb{Z}/k\mathbb{Z})^{\times,\vee}} S_2(\Gamma_1(k), \chi)\,, \tag{5.5.4}$$

where χ varies across all characters modulo k. In particular, it follows from the definitions that $S_2(\Gamma_0(p) \cap \Gamma_1(N))$ is a subspace of $S_2(\Gamma_1(Np))$ and precisely the subspace fixed by all the diamond operators (in the sense of [22, Section 5.2]) $\langle d \rangle$ for $d \equiv 1 \bmod N$. This implies that

$$S_2(\Gamma_0(p) \cap S_2(\Gamma_1(N)) = \bigoplus_{\chi \in (\mathbb{Z}/N\mathbb{Z})^{\times,\vee}} S_2(\Gamma_1(pN), \chi)\,,$$

where we notice that we are not summing over all characters χ modulo Np, as in (5.5.4), instead we only look at the characters $\chi\colon (\mathbb{Z}/Np\mathbb{Z})^{\times} \to \mathbb{C}^{\times}$ that factor through the projection $(\mathbb{Z}/Np\mathbb{Z})^{\times} \to (\mathbb{Z}/N\mathbb{Z})^{\times}$. Moreover, if f is a modular form in $S_2(\Gamma_1(N), \chi)$ for some character χ modulo N, then both f and $f[\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_1$ belong to $S_2(\Gamma_1(Np), \chi)$ by [22, Proposition 5.6.2]. Using this fact we define the spaces of p-new forms

$$S_2^{p-\mathrm{new}}(\Gamma_0(p) \cap \Gamma_1(N)) := \left(S_2(\Gamma_1(N)) + S_2(\Gamma_1(N))[\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_2\right)^{\perp} \quad \subset S_2(\Gamma_0(p)\cap\Gamma_1(N))\,,$$

$$S_2^{p-\mathrm{new}}(\Gamma_1(pN), \chi) := \left(S_2(\Gamma_1(N), \chi) + S_2(\Gamma_1(N), \chi)[\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)]_2\right)^{\perp} \quad \subset S_2(\Gamma_1(pN), \chi)\,,$$

where χ is modulo N and the orthogonal is taken with respect to the Petersson inner product.

Theorem 5.5.5. *Let $G(p, \ell, H)$ be the graph in Definition 1.3, with vertices V and adjacency matrix A, and let $\ker(w_{1,*}), \dots, \ker(w_{n,*})$ be the subspaces of $\mathbb{C}^V$ described in Remark 2.3.6.*

Then,

- *if* $H = \{\mathrm{Id}\} < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, *each* $\ker(w_{i,*})$, *as an* A*-module, is isomorphic to* $S' \otimes_{\mathbb{C}} \mathbb{C}^L$, *as a module over* $\tilde{T}_\ell \otimes \sigma_\ell$, *where* $L = \langle \ell \rangle \subset (\mathbb{Z}/N\mathbb{Z})^\times$, $\sigma_\ell \colon \mathbb{C}^L \to \mathbb{C}^L$ *sends* $(a_x)_{x\in L}$ *to* $(a_{x\ell})_{x\in L}$, *and* S' *is the following space of modular forms*

$$S' = \bigoplus_{\chi \in (\mathbb{Z}/N\mathbb{Z})^{\times,\vee}} S_2^{p\text{-}new}(\Gamma_1(pN^2), \chi)\,,$$

  with χ *varying across the characters that factor through the projection* $(\mathbb{Z}/pN^2\mathbb{Z})^\times \to (\mathbb{Z}/N\mathbb{Z})^\times$.
- *if* $H = B_0(N) = \{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\}$ *then* $n = 1$ *and* $\ker(w_{1,*}) = \{(x_v)_v \in \mathbb{C}^V : \sum_v x_v = 0\}$, *as a module over* A *is isomorphic to* $S_2^{p-\mathrm{new}}(\Gamma_0(pN))$ *as a module over* $\tilde{T}_\ell$.
- *if* $H = B_1(N) = \{\left(\begin{smallmatrix} * & 0 \\ * & 1 \end{smallmatrix}\right)\}$ *then* $n = 1$ *and* $\ker(w_{1,*}) = \{(x_v)_v \in \mathbb{C}^V : \sum_v x_v = 0\}$, *as a module over* A *is isomorphic to* S' *as a module over* $\tilde{T}_\ell$, *with*

$$S' = S_2^{p-\mathrm{new}}(\Gamma_0(p) \cap \Gamma_1(N)) = \bigoplus_{\chi \in (\mathbb{Z}/N\mathbb{Z})^{\times,\vee}} S_2^{p-\mathrm{new}}(\Gamma_1(pN), \chi).$$

- *if* H *is a non-split Cartan of level* N, *then* $n{=}1$ *and* $\ker(w_{1,*})$ *as an* A*-module, is isomorphic to*

$$\bigoplus_{d|N} S_2^{\mathrm{new}}(\Gamma_0(pd^2))\,,$$

  as a $\tilde{T}_\ell$*-module (see [22, Section 5.6] for the definition of* S_2^{new}*).*

Proof. By Lemma 5.1 it is enough to describe the T_ℓ-module $H^0(\mathcal{A}_{H,p}, \Omega^1)$.

The cases $H = B_0(N) = \{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\}$ and $B_1(N) = \{\left(\begin{smallmatrix} * & 0 \\ * & 1 \end{smallmatrix}\right)\}$ can be treated with the same arguments used for the full level structure in Theorem 5.5.2, even slightly easier: $M_{B_0(N)_p}(\mathbb{C})$ and $M_{B_1(N)_p}(\mathbb{C})$ are connected and isomorphic to $\Gamma_0(pN)\backslash\overline{\mathbb{H}}$ and $(\Gamma_0(p)\cap\Gamma_1(N))\backslash\overline{\mathbb{H}}$, and, since $\left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right)$ belongs to H, the graph is connected and then T_ℓ acts exactly as $\tilde{T}_\ell$.

The full level structure case is a consequence of the Hecke-equivariant isomorphisms

$$\begin{aligned} \mathcal{M}_{B'(N^2)} &\longrightarrow \mathcal{M}_N\,, & (E,(P,Q)) &\longmapsto (E/\langle nQ\rangle, (nP,Q)) \\ \mathcal{M}_{B'(N^2)_p} &\longrightarrow \mathcal{M}_{\{\mathrm{Id}\}\times B_0(p)}\,, & (E,(P,Q),G) &\longmapsto (E/\langle nQ\rangle, (nP,Q), G)\,, \end{aligned}$$

where $B'(N^2)$ is the subgroup $\{\left(\begin{smallmatrix} 1+N* & 0 \\ * & 1+N* \end{smallmatrix}\right)\}$ of $\mathrm{GL}_2(\mathbb{Z}/N^2\mathbb{Z})$ and where we identify isomorphisms $\phi \colon (\mathbb{Z}/k\mathbb{Z})^2 \to E[k]$ with basis (P,Q) of the group $E[k]$.

We reduced to $B'(N^2)$ structures. The inclusion $B'(N^2) \supset B_2(N^2) := \{\left(\begin{smallmatrix} 1 & 0 \\ * & 1 \end{smallmatrix}\right)\}$ induces a map $M_{B_2(N^2)} \to M_{B'(N^2)}$ that identifies $H^0(M_{B'(N^2)}, \Omega^1)$ with the $B'(N^2)/M_{B_2(N^2)}$-invariant subspace of $H^0(M_{B'(N^2)}, \Omega^1)$. Choosing $\{g_i\} = \{\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) : a \in (\mathbb{Z}/N^2\mathbb{Z})^\times\}$, Equation (5.1.5) gives

$$M_{B_2(N^2)}(\mathbb{C}) \cong \bigcup_{a\in(\mathbb{Z}/N^2\mathbb{Z})^\times} \Gamma_1(N^2)\backslash\overline{\mathbb{H}}\,, \qquad \left(\mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau, (\tfrac{a\tau}{N}, \tfrac{1}{N})\right) \leftrightarrow (\tau, a)\,,$$

$$M_{B_2(N^2)_p}(\mathbb{C}) \cong \bigcup_{a\in(\mathbb{Z}/N^2\mathbb{Z})^\times} \big(\Gamma_1(N^2)\cap\Gamma_0(p)\big)\backslash\overline{\mathbb{H}}\,, \qquad \left(\mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau, (\tfrac{a\tau}{N}, \tfrac{1}{N}), \langle\tfrac{1}{p}\rangle\right) \leftrightarrow (\tau, a)\,.$$

The action of $B'(N^2)/B_2(N^2)$ identifies certain components (two points (τ, a), (τ, a') are identified iff $a \equiv a' \pmod N$) and that within the same components identifies a point (τ, a) with the point $(\widetilde{\langle d\rangle}\tau, a)$ for $d \equiv 1 \pmod N$ and $\widetilde{\langle d\rangle}$ the diamond operator in [22, Section 5.2]. We deduce the following isomorphism of Hecke-modules

$$\begin{aligned} H^0(\mathcal{A}_{\{\mathrm{Id}\},p}, \Omega^1) &\cong H^0(\mathcal{A}_{B_2(N^2),p}, \Omega^1)^{B'(N^2)/B_2(N^2)} \\ &= \bigoplus_{a\in(\mathbb{Z}/N\mathbb{Z})^\times} \bigoplus_{\chi\in(\mathbb{Z}/N\mathbb{Z})^{\times,\vee}} S_2^{p-\mathrm{new}}(\Gamma_1(pN^2), \chi) \\ &= \left(\bigoplus_{\chi\in(\mathbb{Z}/N\mathbb{Z})^{\times,\vee}} S_2^{p-\mathrm{new}}(\Gamma_1(pN^2), \chi)\right) \otimes \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}\,, \end{aligned}$$

on which, by the same arguments used in Theorem 5.5.2, the Hecke operator acts as $\tilde{T}_\ell \otimes \sigma_\ell$.

For H a non-split Cartan our result follows from the T_ℓ-equivariant isogenies [24, Lemma 3.1 and Theorem 3.8]

$$\mathrm{Pic}^0(M_H) \sim \prod_{d|N} J_0^{\mathrm{new}}(d^2)\,, \quad \mathrm{Pic}^0(M_{H_p}) \sim \prod_{d|N} \left(J_0^{\mathrm{new}}(d^2)^2 \times J_0^{\mathrm{new}}(pd^2)\right)\,,$$

where $J_0^{\mathrm{new}}(k)$ denotes the new part of the Jacobian of $M_{B_0(k)}$. □

5.6. *Automorphisms of the graphs versus automorphisms of spaces modular forms*

We now study how the automorphisms in Definitions 3.12, 3.9 and 3.10 act on a point of $M_{\{\mathrm{Id}\}\times B_0(p)}$ (or a quotient M_{H_p}) under the isomorphism (5.3.1). Recall that a point (a, τ) corresponds to the elliptic curve $E_\tau = \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau$ together with the subgroup $\langle\frac{\tau}{p}\rangle$ and the basis $(\frac{a\tau}{N}, \frac{1}{N})$ of $E[N]$ (such a basis corresponds to the isomorphism $\phi_\tau\colon (\mathbb{Z}/N\mathbb{Z})^2 \to E[N]$ sending the standard basis to it).

The Fricke automorphism σ sends the point (a, τ) to the elliptic curve $\mathbb{C}/\mathbb{Z}+\mathbb{Z}\frac{\tau}{p}$, with the subgroup $\langle\frac{1}{p}\rangle$ and with the basis $(\frac{a\tau}{N}, \frac{1}{N})$ of the N-torsion. The multiplication by $\tau' = -\frac{p}{\tau}$ inside $\mathbb{C}$ induces an isomorphism between this elliptic curve and the elliptic curve $E_{\tau'}$, with the subgroup $\langle\frac{\tau'}{p}\rangle$ and the basis $(-\frac{ap}{N}, \frac{\tau'}{N})$, namely the point of $(\tau', \left(\begin{smallmatrix} 0 & 1 \\ -ap & 0 \end{smallmatrix}\right))$ under the canonical isomorphism (5.1.3). If we now apply the action (5.1.2) of a matrix

$$\tilde{m} \in \Gamma^0(p) \quad \text{ such that } \tilde{m} \equiv \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \bmod N\,,$$

we see that this point is equivalent to the point $(\tilde{m}(\tau'), \left(\begin{smallmatrix} ap & 0 \\ 0 & 1 \end{smallmatrix}\right))$, that is the point $(\tilde{m}\left(\begin{smallmatrix} 0 & -p \\ 1 & 0 \end{smallmatrix}\right)\tau, ap)$. We deduce that

$$\sigma^* = [\tilde{m}\left(\begin{smallmatrix} 0 & -p \\ 1 & 0 \end{smallmatrix}\right)]_2 \otimes \sigma_p \quad \text{in } H^0(M_{\{\mathrm{Id}\}\times B^0(p),\mathbb{C}}, \Omega^1) \cong S_2\left(\Gamma(N)\cap\Gamma^0(p)\right) \otimes_{\mathbb{C}} \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}$$

where $\sigma_p \circlearrowright \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}$ is the shift $(x_a) \mapsto (x_{ap})$. Inspired by the above discussion we give the following

Definition 5.6.1. The Fricke automorphism on full level modular forms is

$$w_p \colon S_2\left(\Gamma(N)\cap\Gamma^0(p)\right) \longrightarrow S_2\left(\Gamma(N)\cap\Gamma^0(p)\right), \quad f \longmapsto f[m_\sigma]_2$$

for $m_\sigma = \tilde{m}\left(\begin{smallmatrix} 0 & -p \\ 1 & 0 \end{smallmatrix}\right)$ and $\tilde{m} \in \Gamma^0(p)$ a matrix congruent to $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ modulo N.

For matricial automorphisms as in Definition 3.9 we have already computed their action in Equation (5.5.1). In particular, diamond operators $\langle d\rangle$ act as $\widetilde{\langle d\rangle} \otimes \sigma_{d^2}$ for $\widetilde{\langle d\rangle}$ as in the next definition (which coincides with the diamond operator in [22, Section 5.2])

Definition 5.6.2. Given $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, for each $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have a diamond operator

$$\widetilde{\langle d\rangle} \colon S_2(\Gamma_H) \longrightarrow S_2(\Gamma_H), \quad f \longmapsto f[\tilde{m}_d]_2,$$

for $\tilde{m}_d \in \mathrm{SL}_2(\mathbb{Z})$ a matrix congruent to $\left(\begin{smallmatrix} d^{-1} & 0 \\ 0 & d \end{smallmatrix}\right)$ modulo N.

Let us now suppose that $N = Mq$ for M, q coprime, q a prime power, and that $H = \tilde{H} \times B_0(q)$ as in (3.1). Under the canonical isomorphism (5.1.3), a point $(\tau, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) \in M_{H_p}(\mathbb{C})$ corresponds to the elliptic curve $E_\tau = \mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau$ together with the subgroups $\langle\frac{\tau}{p}\rangle \subset E_\tau[p]$ and $\langle\frac{b\tau+d}{q}\rangle \subset E_\tau[q]$ and the basis $(\frac{a\tau+c}{M}, \frac{b\tau+d}{M})$ of $E_\tau[M]$. The image of a point (τ, a) under the q-th Atkin-Lehner w_q is the elliptic curve $\mathbb{C}/\mathbb{Z}\frac{1}{q}+\mathbb{Z}\tau$ together with the subgroups $\langle\frac{\tau}{p}\rangle$ and $\langle\frac{\tau}{q}\rangle$ and the basis $(\frac{a\tau}{M}, \frac{1}{M})$ of the M-torsion, which, for $\tau' = p\tau$ is isomorphic (under the map $z \to qz$) to the elliptic curve $\mathbb{C}/\mathbb{Z}+\mathbb{Z}\tau'$ together with the subgroups $\langle\frac{\tau'}{p}\rangle$ and $\langle\frac{\tau'}{q}\rangle$ and the basis $(\frac{a\tau'}{M}, \frac{q}{M})$ of the M-torsion. This last datum corresponds to a point $(q\tau, m)$ for $m \in \mathrm{GL}_2(\mathbb{Z}/qM\mathbb{Z})$ that is congruent to $\left(\begin{smallmatrix} a & 0 \\ 0 & q \end{smallmatrix}\right)$ modulo M and congruent to $\left(\begin{smallmatrix} * & * \\ * & 0 \end{smallmatrix}\right)$ modulo q. If we apply the action (5.1.2) by a matrix

$$\tilde{m}_q \in \Gamma^0(p) \quad \text{such that } \tilde{m}_q \equiv \left(\begin{smallmatrix} q & 0 \\ 0 & q^{-1} \end{smallmatrix}\right) \bmod M, \tilde{m}_q \equiv \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \bmod q, \tag{5.6.3}$$

the same point is moved to the point $(\tilde{m}_q\left(\begin{smallmatrix} q & 0 \\ 0 & 1 \end{smallmatrix}\right)\tau, \left(\begin{smallmatrix} a(q+M) & 0 \\ 0 & 1 \end{smallmatrix}\right))$. We deduce that

$$w_q^* = [\tilde{m}_q\left(\begin{smallmatrix} q & 0 \\ 0 & 1 \end{smallmatrix}\right)]_2 \otimes \sigma_{q+M} \circlearrowright \left(S_2\left(\Gamma(N)\cap\Gamma^0(p)\right) \otimes_{\mathbb{C}} \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}\right)^H, \tag{5.6.4}$$

where $\sigma_{q+M} \circlearrowright \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}$ is the shift $(x_a) \mapsto (x_{a(q+M)})$.

This discussion, together with Proposition 4.9, Theorem 4.6, and Lemma 5.1 implies the following result. Notice that by Remark 5.2 the automorphisms act by pushforward, or equivalently by pullback of their inverses, on the 1-forms.

Theorem 5.6.5. *Let $G = G(p, \ell, H)$ be the graph in Definition 1.3, with V the set of vertices and $\ker(w_{1,*}), \dots, \ker(w_{n,*})$ the subspaces of $\mathbb{C}^V$ described in Remark 2.3.6.*

Then there is an isomorphism

$$\bigoplus_{i=1}^{n} \ker(w_{i,*}) \cong \left(S_2^{p\text{-}new}(\Gamma^0(p) \cap \Gamma(N)) \otimes_{\mathbb{C}} \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times} \right)^H ,$$

that simultaneously intertwines the action of the adjoint of the adjacency matrix A^* (see also Proposition 2.2.2), the matricial automorphisms $\langle g \rangle$ in Definition 2.1.2, the Galois action in Definition 2.1.1 and, if there, the Atkin-Lehner involutions w_q in Definition 3.10 on the left, with the action of $\tilde{T}_\ell \otimes \sigma_\ell$, the action of a matrix g^{-1} in (5.5.1), the map $w_p \otimes \sigma_{1/p}$ (see Definition 5.6.1) and, if there, the inverse of the map (5.6.4) on the right (we denote $\sigma_d \circlearrowright \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}$ is the shift $(x_a)_a \mapsto (x_{ad})_a$).

In some special cases we can be slightly more explicit.

Theorem 5.6.6. *Keep the notation as in Theorem 5.5.5 and let A^* be the adjoint of the adjacency matrix, as in Proposition 2.2.2.*

- *if $H = \{\mathrm{Id}\}$, then $\oplus_i \ker(w_{i,*})$, as module over A^*, over the Galois action, and over the diamond operators $\langle d \rangle$, is isomorphic to $S' \otimes_{\mathbb{C}} \mathbb{C}^{(\mathbb{Z}/N\mathbb{Z})^\times}$, as a module over $\tilde{T}_\ell \otimes \sigma_\ell$, over $w_p \otimes \sigma_{1/p}$ and over $\widetilde{\langle d \rangle}^{-1} \otimes \sigma_{d^{-2}}$.*
- *if $H = B_0(N) = \{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\}$ then $n = 1$ and $\ker(w_{1,*})$, as a module over A^*, over the Galois action, and over the Atkin-Lehner involutions w_q, is isomorphic to $S_2^{p-\mathrm{new}}(\Gamma_0(pN))$ as a module over $\tilde{T}_\ell$, over the Fricke involution w_p, and over the other Atkin-Lehner involutions w_q in [7].*
- *if $H = B_1(N) = \{\left(\begin{smallmatrix} * & 0 \\ * & 1 \end{smallmatrix}\right)\}$ then $n = 1$ and $\ker(w_{1,*})$, as a module over A^*, over the Galois action, and over the diamond operators $\langle d \rangle$, is isomorphic to S', as a module over $\tilde{T}_\ell$, over w_p and over $\widetilde{\langle d^{-1} \rangle}$.*
- *if H is a non-split Cartan, then $n = 1$ and $\ker(w_{1,*})$ as a module over A^*, over the Galois action, and over the nontrivial matricial automorphisms $\langle g_q \rangle$ for q^e a prime power in the factorization of N and g_q the only elements in the normalizer of H such that $g_q \equiv \mathrm{Id} \pmod{N/q^e}$, is isomorphic to $\bigoplus_{d|N} S_2^{\mathrm{new}}(\Gamma_0(pd^2))$ as a module over $\tilde{T}_\ell$-module, over the p-th Atkin Lehner involution (see [7]) and over the q-th Atkin-Lehner involution (that acts trivially on $S_2^{\mathrm{new}}(\Gamma_0(pd^2))$ when $q \nmid d$)*

Remark 5.6.7. To have an isomorphism which is *simultaneously* equivariant with respect to all automorphisms, in Theorems 5.6.5 and 5.6.6 we used the adjoint A^* of the adjacency matrix. Instead, in Theorems 5.5.2 and 5.5.5, for merely aesthetic reasons, we preferred using the adjacency matrix, which is conjugate to its adjoint.

5.7. Asymptotic distribution of the eigenvalues

Following Serre [56], given a linear diagonalizable operator P with spectrum $\sigma(P)$ and domain V of finite dimension r, we introduce the probability measure

$$\mu(P,V) := \frac{1}{r}\sum_{\lambda\in\sigma(P)} \delta_\lambda\,,$$

where δ_λ is a Dirac mass at λ. Let us also recall the Kesten-McKay measure supported on the Hasse interval $[-2\sqrt{\ell}, 2\sqrt{\ell}]$ from Equation (1.13)

$$\mu_\ell = \frac{\ell+1}{\pi}\frac{\sqrt{\ell - x^2/4}}{\ell(\ell^{1/2}+\ell^{-1/2})^2 - x^2}dx\,.$$

We are interested in $\mu(P,V)$ when P is a Hecke operator and V is one of the spaces appearing in Theorem 5.5.5. The following theorem gives asymptotics, implying Corollary 1.14.

Theorem 5.7.1. *Fix a prime ℓ, a positive integer N coprime with ℓ, and let p_i be an increasing sequence of prime numbers coprime with $N\ell$. Then*

$$\lim_{i\to\infty}\mu\left(T_\ell, S_2^{p_i\text{-}new}(\Gamma_0(p_iN))\right) = \lim_{i\to\infty}\mu\left(T_\ell, \bigoplus_{d|N} S_2^{\mathrm{new}}(\Gamma_0(p_id^2))\right) = \mu_\ell\,,$$

and, for each character χ modulo N,

$$\lim_{i\to\infty}\mu\left(T_\ell, S_2^{p_i\text{-}new}(\Gamma_1(p_iN),\chi)\right) = \lim_{i\to\infty}\mu\left(T_\ell, S_2^{p_i\text{-}new}(\Gamma_1(p_iN^2),\chi)\right) = \sqrt{\chi(\ell)}\mu_\ell\,.$$

Observe that $\mu_\ell = -\mu_\ell$, so it does not matter which sign of the square root of $\chi(\ell)$ we choose.

Proof. Let us first prove the theorem for $S_2^{p_i\text{-}new}(\Gamma_0(p_iN))$. As Hecke modules we have

$$S_2(\Gamma_0(p_iN)) = S_2^{p_i\text{-new}}(\Gamma_0(p_iN)) \oplus S_2(\Gamma_0(N))^{\oplus 2}\,.$$

Passing to measures, and denoting $d(k) = \dim S_2(\Gamma_0(k))$, $d(p,k) = \dim S_2^{p\text{-new}}(\Gamma_0(pk))$, we get

$$\mu(T_\ell, S_2(\Gamma_0(p_iN)) = \frac{d(p_i,N)}{d(p_iN)}\mu(T_\ell, S_2(\Gamma_0(p_iN))^{p_i-new}) + 2\frac{d(N)}{d(p_iN)}\mu(T_\ell, S_2(\Gamma_0(N)))\,,$$

the second summand on the right hand side goes to zero when i goes to infinity, hence we deduce the claim from [56, Theorem 1].

The other cases are proved in the same way, replacing [56, Theorem 1] first with [56, Theorem 1] and then with [56, Theorem 4]. □

Appendix A. Correspondences on nodal curves

In the first part of this Appendix we recall for the reader convenience well-known facts and notations about the Picard group of nodal curves. We then use it to state and prove Proposition A.7.

Suppose we are given two smooth projective curves C_1, C_2 over a field $k = \overline{k}$. We allow for C_1 and C_2 to be disconnected with the same number of connected components which we denote $C_1^1, \dots, C_1^r$ of C_1, and $C_2^1, \dots, C_2^r$. We suppose that for each $j = 1, \dots, r$, we are given distinct points $x_1^j, \dots x_{n_j}^j \in C_1^j(k)$ and $y_1^j, \dots y_{n_j}^j \in C_2^j(k)$, and we look at the nodal curve

$$X = (C_1 \sqcup C_2)/x_i^j = y_i^j\,. \tag{A.1}$$

For simplicity we assume that $n_j \geq 1$, so that X has exactly r connected components, namely the curves $X_j = (C_1^j \sqcup C_2^j)/x_i^j = y_i^j$, each having 2 irreducible components. Anyway Proposition A.7 remains true if we suppose that the number of indices j such that $n_j \geq 1$ (keeping the notation r for this number) is strictly smaller than the number of components of C_1 and of C_2, possibly different.

Let $J = \mathrm{Pic}^0_{X/k}$ be the scheme representing invertible sheaves on X having degree 0 when restricted to each irreducible component of X. In particular, the natural maps $C_1 \to X$ and $C_2 \to X$ induce by pull back a map

$$J \longrightarrow \mathrm{Pic}^0_{C_1/k} \times \mathrm{Pic}^0_{C_2/k}\,. \tag{A.2}$$

Such a map is surjective: given invertible sheaves $\mathcal{L}_i$ over C_i, we can construct a (non-canonical) lift of $(\mathcal{L}_1, \mathcal{L}_2)$ by choosing generators v_i^j, w_i^j of $(x_i^j)^*\mathcal{L}_1, (y_i^j)^*\mathcal{L}_2$ and defining the invertible sheaf $\mathcal{L} = \mathcal{L}_{\mathcal{L}_1,\mathcal{L}_2,(v_i^j,w_i^j)_{i,j}}$ on X associating to each open $U \subset X$, the module

$$\mathcal{L}(U) = \{(f,g) \in \mathcal{L}_1(U \cap C_1) \times \mathcal{L}_2(U \cap C_2) :\ f(x_i^j)/v_i^j = g(y_i^j)/w_i^j \text{ for each } i,j\}\,. \tag{A.3}$$

We notice that the structure sheaf is a particular case of the above construction, namely when $\mathcal{L}_i = \mathcal{O}_{C_i}$ and $v_i = x_i^*1, w_i = y_i^*1$. Moreover, all the lifts of $(\mathcal{L}_1, \mathcal{L}_2)$ are obtained with this construction: given a lift $\mathcal{M}$, we choose for each i a section trivializing $\mathcal{M}_{x_i}$,

which determines by pull back sections v_i, w_i; then the pull back of sections to C_i determines a morphism of $\mathcal{O}$-modules $\mathcal{M} \to \mathcal{L}_{\mathcal{L}_1,\mathcal{L}_2,(v_i,w_i)_i}$, which is an isomorphism because of how the structure sheaf is defined.

Since map (A.2) is surjective, we have an exact sequence of group schemes over k

$$0 \longrightarrow T \longrightarrow J \longrightarrow \mathrm{Pic}^0_{C_1/k} \times \mathrm{Pic}^0_{C_2/k} \longrightarrow 0\,, \tag{A.4}$$

for a certain group scheme T. For every k-algebra A we can describe the points on T explicitly using (A.3): for every choice of i, j, the line bundle $(y_i^j)^*_{\mathrm{Spec}\,A}\mathcal{O}_{C_2,\mathrm{Spec}\,A}$ is canonically trivial, hence its generating sections are canonically elements of $A^\times$; in particular, every line bundle on $X_{\mathrm{Spec}\,A}$ that is trivial on the C_i's is isomorphic to

$$\mathcal{L}_a := \mathcal{L}_{\mathcal{O}_{C_1},\mathcal{O}_{C_2},(1,a(y_i^j))} \qquad \text{for some function } a\colon Y = \{y_1^1, \dots, y_r^{n_r}\} \longrightarrow A^\times\,.$$

More formally, denoting by $\mathbb{G}_m^Y$ the set of maps from Y to $\mathbb{G}_m$, we have a surjective map

$$\begin{aligned} \mathbb{G}_{\mathrm{m}}^Y &\longrightarrow T \\ a &\longmapsto \mathcal{L}_a \end{aligned}$$

Let us study the kernel. Which of the invertible sheaves $\mathcal{L}_a$ are trivial? Exactly those where $a(y_i^j)$ does not depend on i but only on j: indeed $\mathcal{L}_a$ is trivial if an only if it is trivial when restricted to each connected component X^j of X, and, since $\mathcal{L}_a|_{X^j}$ has degree 0, then it is trivial if and only if it has a non trivial global section, which implies our claim using (A.3) and the fact the only global functions on C_1^j and C_2^j are constant. This discussion implies that the following sequence of group schemes over k is exact

$$0 \longrightarrow \mathbb{G}_{\mathrm{m}}^r \xrightarrow{\Delta} \mathbb{G}_{\mathrm{m}}^Y \longrightarrow T \longrightarrow 0 \tag{A.5}$$

where $\Delta(b_1, \dots, b_r)(y_i^j) = b_j$.

The above exact sequence, allows us to describe the characters of T. We have canonical isomorphisms $(\mathbb{G}_{\mathrm{m}}^Y)^\vee = \mathrm{Hom}(\mathbb{G}_{\mathrm{m}}^Y, \mathbb{G}_{\mathrm{m}}) = \mathbb{Z}^Y = \bigoplus_{i,j} \mathbb{Z} y_i^j$ and $(\mathbb{G}_{\mathrm{m}}^r)^\vee = \mathrm{Hom}(\mathbb{G}_{\mathrm{m}}^r, \mathbb{G}_{\mathrm{m}}) = \mathbb{Z}^r$ and the map Δ induces

$$\Sigma = \Delta^\vee\colon \bigoplus_{i,j} \mathbb{Z} y_i^j \longrightarrow \mathbb{Z}^r\,, \quad \sum_{i,j} m_i^j y_i^j \longmapsto \Big(\sum_{i=1}^{n_1} m_i^1, \dots, \sum_{i=1}^{n_r} m_i^r\Big)\,.$$

Then, the exact sequence (A.5) gives the following isomorphism

$$\begin{array}{ccccc} T^\vee = \mathrm{Hom}(T, \mathbb{G}_{\mathrm{m}}) & = & \ker(\Delta^\vee\colon \mathbb{G}_{\mathrm{m}}^{T,\vee} \to \mathbb{G}_{\mathrm{m}}^{r,\vee}) & = & \ker(\Sigma) \\ \mathcal{L}_a \mapsto \prod_{i,j} a(y_i^j)^{m_i^j} & \longleftarrow\!\shortmid & & \longleftarrow\!\shortmid & \sum_{i,j} m_i^j y_i^j\,. \end{array} \tag{A.6}$$

In the next proposition we describe how certain correspondences act on T and on its characters, which is applied in the proof of Theorem 4.6 to the Hecke operator 3.6. In the notation of the proposition, we do not keep track of the connected components.

Proposition A.7. *Let k be an algebraically closed field and let $C = (C_1 \sqcup C_2)/(x_i = y_i)_{i=1}^n$ and $D = (D_1 \sqcup D_2)/(v_j = w_j)_{i=1}^m$ be curves over k described as in (A.1), with C_i, D_i smooth.*

Let $F, G\colon D \to C$ be maps restricting to $F_i, G_i\colon D_i \to C_i$ and sending the smooth part of D into the smooth part of C and the nodal points to the nodal points. Then, for each $a\colon \{y_1, \dots, y_n\} \to k^\times$ we have

$$G_* F^* \mathcal{L}_a \cong \mathcal{L}_b \qquad \text{for } b := a \circ F_{2*} G_2^*\colon\ y_i \mapsto \prod_{G_2(v)=y_i} a(F_2(v))^{\operatorname{ord}_v(G_2)}\,, \tag{A.8}$$

where G_* is a cycle push-forward.

Let T be the maximal torus of $\operatorname{Pic}_{C/k}$, as in (A.5), and let $T^\vee$ be its groups of characters. Keeping track of how the points y_i are distributed among the components of C_2, we get an isomorphism, analogous to (A.6),

$$T^\vee = \ker\left(\Sigma\colon \bigoplus_{i=1}^n \mathbb{Z} y_i \to \mathbb{Z}^r\right).$$

Using the above isomorphism, the map $(G_* F^*)^\vee$ is the restriction of the map H below

$$\begin{array}{ccc} T^\vee & \hookrightarrow & \bigoplus_{i=1}^n \mathbb{Z} y_i \\ \downarrow{\scriptstyle (G_* F^*)^\vee} & & \downarrow{\scriptstyle H} \\ T^\vee & \hookrightarrow & \bigoplus_{i=1}^n \mathbb{Z} y_i \end{array} \qquad\qquad \begin{array}{c} y_i \\ \downarrow \\ \displaystyle\sum_{G_2(v)=y_i} \operatorname{ord}_v(G_2) F_2(v)\,. \end{array} \tag{A.9}$$

Proof. We first give a description of T in terms of Cartier divisors. For a function $a\colon \{y_i\} \to k^\times$, take a meromorphic function $f \in k(C_2)$ such that $f(y_i) = a(y_i)$ for every i. By (A.3), the pair $(1, f)$ defines a meromorphic section of $\mathcal{L}_a$. The divisor attached to this section is supported in $C_2 \setminus \{v_1, \dots v_n\}$, and can be identified with the divisor $\operatorname{div} f$. As explained for instance in [35, Section 1, Proposition 1.4 (b)], the push-forward of a cycle attached to a meromorphic function can be computed using the norm, so

$$G_* F^* \mathcal{L}_a \cong G_* F^* (\operatorname{div}(1, f)) = G_* \operatorname{div}(F^*(1, f)) = \operatorname{div}((1, \operatorname{Norm}_{G_2}(F_2^* f))) = \mathcal{L}_c\,, \tag{A.10}$$

for

$$c = \mathrm{Norm}_{G_2}(F_2^* f)|_{\{y_i\}}\,.$$

To prove (A.8), it remains to prove $c = b$. The norm is compatible with pull-backs, i.e. if we want to compute $\mathrm{Norm}_{G_2}(F_2^* f))(y_i)$ we can look at the base change $G_2\colon G_2^{-1}(y_i) \to y_i$, the pull-back of $F_2^* f$ to $G_2^{-1}(y_i)$ and then compute the norm; we conclude that

$$(\mathrm{Norm}_{G_2}(F_2^* f))(y_i) = \prod_{G_2(v)=y_i} (F_2^* f)(v)^{\mathrm{ord}_v G_2}\,.$$

Since G_2 and F_2 send the smooth part of D_2 in the smooth part of C_2 (and analogously for the inverse images), then all the v's appearing above lie in the set $\{w_j\}$ and consequently the points $F_2(v)$ lie in the set $\{y_j\}$, so

$$\prod_{G_2(v)=y_i} (F_2^* f)(v)^{\mathrm{ord}_v G_2} = \prod_{G_2(v)=y_i} f(F_2(v))^{\mathrm{ord}_v G_2} = \prod_{G_2(v)=y_i} a(F_2(v))^{\mathrm{ord}_v G_2}\,.$$

For the second part of the proposition, namely Equation (A.9), it is enough proving that for each i, j we have $(G_* F^*)^\vee(y_i - y_j) = H(y_i - y_j)$, which is true since

$$\begin{aligned}
&(G_* F^*)^\vee(y_i - y_j)(\mathcal{L}_a)\\
&\quad = (y_i - y_j)(\mathcal{L}_b) = \tfrac{b(y_i)}{b(y_j)} = \prod_{G_2(v)=y_i} a(F_2(v))^{\mathrm{ord}_v(G_2)} \cdot \prod_{G_2(v)=y_j} a(F_2(v))^{-\mathrm{ord}_v(G_2)}\\
&\quad = a\left(\sum_{G_2(v)=y_i} \mathrm{ord}_v(G_2) F_2(v) - \sum_{G_2(v)=y_j} \mathrm{ord}_v(G_2) F_2(v)\right)\\
&\quad = a\left(H(y_i - y_j)\right) = H(y_i - y_j)(\mathcal{L}_a)\,. \quad \square
\end{aligned}$$

Appendix B. Numerical experiments on the largest non-trivial eigenvalue

In this appendix we focus on isogeny graphs with trivial level structure, so we omit H from the notations. We study the value $\eta = \eta(p, \ell)$ for the graph $G(p, \ell)$. Recall from Equation (1.10) that

$$\eta(p, \ell) := \min\{2\sqrt{\ell} - |\lambda|\}\,,$$

where the minimum ranges among all non-trivial eigenvalues of the adjacency matrix of the graph $G(p, \ell)$. In other words, $\eta(p, \ell)$ is the biggest number such that all non-trivial eigenvalues of the adjacency matrix of $G(p, \ell)$ lie in the shrunk Hasse interval $[-2\sqrt{\ell} + \eta(p, \ell), 2\sqrt{\ell} - \eta(p, \ell)]$.

For a fixed ℓ, the number of vertexes of $G(p, \ell)$ is linear in p, and Alon-Boppana inequality implies that $\eta \leq C \log(p)^{-2}$, for some constant C which depends only on ℓ. Recall that lower bounds on η give bounds on the mixing time of the graph via

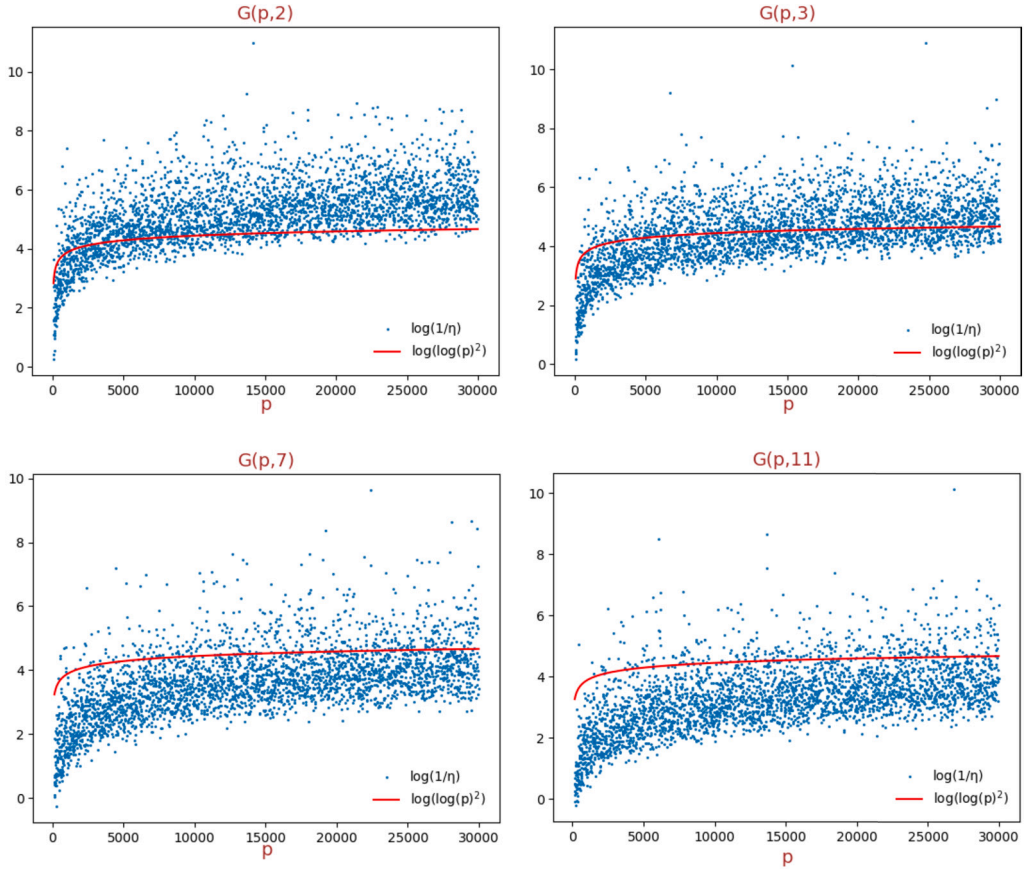


Fig. 2. Numerical experiments on $\eta(p,\ell)$. (For a colored figure, the reader is referred to the web version of this article.)

Proposition 1.12. To best of our knowledge, sharp lower bounds and the asymptotic of η are not known, see Question 1.11.

We have computed some values of $\eta(p,\ell)$ using the database [27], which lists graphs with $\ell = 2,3,5,7,11$ and $p < 30.000$. The results are displayed in Fig. 2.

For fixed ℓ, the order of magnitude of η varies a lot, so it is more convenient for graphical reasons to plot $\log(1/\eta)$ (we plot these values with light blue dots). Under the transformation $x \mapsto \log(1/x)$, our bound in Theorem 2.3.8 on η is linear in p, reaching the thousands; being quite far from the data below, we do not even plot it.

Alon-Boppana bound becomes $2\log(\log(p))$ up to an additive constant. We plot the function $2\log(\log(p))$ with a red line, to compare its shape with the data on η.

Data availability

No data was used for the research described in the article.

References

[1] D. Abramovich, M.C. Olsson, A. Vistoli, Twisted stable maps to tame Artin stacks, J. Algebr. Geom. 20 (3) (2011) 399–477.
[2] J. Alper, Stack and moduli, https://sites.math.washington.edu/~jarod/moduli.pdf.
[3] L. Amorós, A. Iezzi, K. Lauter, C. Martindale, J. Sotáková, Explicit connections between supersingular isogeny graphs and Bruhat-Tits trees, in: Women in Numbers Europe III—Research Directions in Number Theory, in: Assoc. Women Math. Ser., vol. 24, Springer, Cham, 2021, pp. 39–73.
[4] S. Arpin, Adding level structure to supersingular elliptic curve isogeny graphs, J. Théor. Nr. Bordx. 36 (2) (2024) 405–443.
[5] S. Arpin, C. Camacho-Navarro, K. Lauter, J. Lim, K. Nelson, T. Scholl, J. Sotáková, Adventures in supersingularland, Exp. Math. 32 (2) (2023) 241–268.
[6] S. Arpin, M. Chen, K.E. Lauter, R. Scheidler, K.E. Stange, H.T. Nguyen Tran, Orientations and cycles in supersingular isogeny graphs, in: Research Directions in Number Theory, in: Assoc. Women Math. Ser., vol. 33, Springer, Cham, 2022, pp. 25–86.
[7] A.O.L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. 185 (1970) 134–160.
[8] A. Basso, G. Codogni, D. Connolly, L. De Feo, T.B. Fouotsa, G.M. Lido, T. Morrison, L. Panny, S. Patranabis, B. Wesolowski, Supersingular curves you can trust, in: Advances in Cryptology—EUROCRYPT 2023. Part II, in: Lecture Notes in Comput. Sci., vol. 14005, Springer, Cham, 2023, pp. 405–437.
[9] A. Basso, L. De Feo, P. Dartois, A. Leroux, L. Maino, G. Pope, D. Robert, B. Wesolowski, SQIsign2D-West, in: Advances in Cryptology—ASIACRYPT 2024. Part III, in: Lecture Notes in Comput. Sci., vol. 15486, Springer, Singapore, 2024, pp. 339–370.
[10] A. Basso, L. Maino, G. Pope, FESTA: fast encryption from supersingular torsion attacks, in: Advances in Cryptology—ASIACRYPT 2023. Part VII, in: Lecture Notes in Comput. Sci., vol. 14444, Springer, Singapore, 2023, pp. 98–126.
[11] C. Bordenave, A new proof of Friedman's second eigenvalue theorem and its extension to random lifts, Ann. Sci. Éc. Norm. Supér. (4) 53 (6) (2020) 1393–1439.
[12] S. Bosch, W. Lütkebohmert, M. Raynaud, Néron Models, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 21, Springer, Berlin, 1990.
[13] W. Castryck, T. Decru, An efficient key recovery attack on SIDH, in: Advances in Cryptology—EUROCRYPT 2023. Part V, in: Lecture Notes in Comput. Sci., vol. 14008, Springer, Cham, 2023, pp. 423–447.
[14] D.X. Charles, E.Z. Goren, K.E. Lauter, Families of Ramanujan graphs and quaternion algebras, in: Groups and Symmetries, in: CRM Proc. Lecture Notes, vol. 47, Amer. Math. Soc., Providence, RI, 2007, pp. 53–80.
[15] D.X. Charles, K.E. Lauter, E.Z. Goren, Cryptographic hash functions from expander graphs, J. Cryptol. 22 (1) (2009) 93–113.
[16] R.F. Coleman, B. Edixhoven, On the semi-simplicity of the U_p-operator on modular forms, Math. Ann. 310 (1) (1998) 119–127.
[17] A. Cowan, Computing newforms using supersingular isogeny graphs, Res. Number Theory 8 (4) (2022) 96.
[18] P. Dartois, A. Leroux, D. Robert, B. Wesolowski, SQIsignHD: new dimensions in cryptography, in: Advances in Cryptology—EUROCRYPT 2024. Part I, in: Lecture Notes in Comput. Sci., vol. 14651, Springer, Cham, 2024, pp. 3–32.
[19] G.P. Davidoff, P.C. Sarnak, A.J. Valette, Elementary Number Theory, Group Theory, and Ramanujan Graphs, London Mathematical Society Student Texts, vol. 55, Cambridge Univ. Press, Cambridge, 2003.
[20] P. Deligne, La conjecture de Weil. I, Publ. Math. Inst. Hautes Études Sci. 43 (1974) 273–307.
[21] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques, in: Modular Functions of One Variable, II, Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972, in: Lecture Notes in Math., vol. 349, Springer, Berlin-New York, 1973, pp. 143–316.
[22] F.I. Diamond, J. Shurman, A First Course in Modular Forms, Graduate Texts in Mathematics, vol. 228, Springer, New York, 2005.
[23] V. Dose, G.M. Lido, P. Mercuri, Automorphisms of Cartan modular curves of prime and composite level, Algebra Number Theory 16 (6) (2022) 1423–1461.
[24] V. Dose, G. Lido, P. Mercuri, C. Stirpe, Modular curves with many points over finite fields, J. Algebra 635 (2023) 790–821.

[25] M. Duparc, T.B. Fouotsa, SQIPrime: a dimension 2 variant of SQISignHD with non-smooth challenge isogenies, in: Advances in Cryptology—ASIACRYPT 2024. Part III, in: Lecture Notes in Comput. Sci., vol. 15486, Springer, Singapore, 2024, pp. 396–429.
[26] M. Emerton, Supersingular elliptic curves, theta series and weight two modular forms, J. Am. Math. Soc. 15 (3) (2002) 671–714.
[27] G. Finol, E. Florit, Isogeny database, https://zenodo.org/doi/10.5281/zenodo.4303870, available at, https://isogenies.enricflorit.com/index.html.
[28] T.B. Fouotsa, T. Moriya, C. Petit, M-SIDH and MD-SIDH: countering SIDH attacks by masking information, in: Advances in Cryptology—EUROCRYPT 2023. Part V, in: Lecture Notes in Comput. Sci., vol. 14008, Springer, Cham, 2023, pp. 282–309.
[29] L. De Feo, T.B. Fouotsa, L. Panny, Isogeny problems with level structure, in: Advances in Cryptology—EUROCRYPT 2024. Part VII, in: Lecture Notes in Comput. Sci., vol. 14657, Springer, Cham, 2024, pp. 181–204.
[30] L. De Feo, D. Kohel, A. Leroux, C. Petit, B. Wesolowski, SQISign: compact post-quantum signatures from quaternions and isogenies, in: Advances in Cryptology—ASIACRYPT 2020. Part I, in: Lecture Notes in Comput. Sci., vol. 12491, Springer, Cham, 2020, pp. 64–93.
[31] L. De Feo, C. Guilhem, T.B. Fouotsa, P. Kutas, A. Leroux, C. Petit, J. Silva, B. Wesolowski, Séta: supersingular encryption from torsion attacks, in: Advances in Cryptology—ASIACRYPT 2021. Part IV, in: Lecture Notes in Comput. Sci., vol. 13093, Springer, Cham, 2021, pp. 249–278.
[32] L. De Feo, D. Jao, J. Plût, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies, J. Math. Cryptol. 8 (3) (2014) 209–247.
[33] S. Dobson, S.D. Galbraith, On the degree-insensitive SI-GDH problem and assumption, Cryptology ePrint Archive, Report 2019/929, https://eprint.iacr.org/2019/929, 2019.
[34] J. Friedman, A Proof of Alon's Second Eigenvalue Conjecture and Related Problems, vol. 195, Mem. Am. Math. Soc., 2008, 910, viii+100 pp.
[35] W. Fulton, Intersection Theory, second edition, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A (Series of Modern Surveys in Mathematics), vol. 2, Springer, Berlin, 1984.
[36] W. Ghantous, S. Katsumata, F. Pintore, M. Veroni, Collisions in supersingular isogeny graphs and the SIDH-based identification protocol, Cryptology ePrint Archive, Report 2021/1051, https://eprint.iacr.org/2021/1051, 2021.
[37] S. Hoory, N. Linial, A. Wigderson, Expander graphs and their applications, Bull. Am. Math. Soc. (N.S.) 43 (4) (2006) 439–561.
[38] J. Huang, T. McKenzie, Horng-Tzer Yau, Ramanujan property and edge universality of random regular graphs, arXiv preprint, arXiv:2412.20263, 2024, https://arxiv.org/abs/2412.20263.
[39] N.M. Katz, B.C. Mazur, Arithmetic Moduli of Elliptic Curves, Annals of Mathematics Studies, vol. 108, Princeton Univ. Press, Princeton, NJ, 1985.
[40] D. Kohel, Endomorphism rings of elliptic curves over finite fields, Ph.D. Thesis, University of California, Berkeley, December 1996.
[41] A. Lubotzky, R.S. Phillips, P.C. Sarnak, Ramanujan graphs, Combinatorica 8 (3) (1988) 261–277.
[42] A. Lei, K. Müller, On the zeta functions of supersingular isogeny graphs and modular curves, Arch. Math. (Basel) 122 (3) (2024) 285–294.
[43] A. Lei, K. Müller, On towers of isogeny graphs with full level structures, Res. Math. Sci. 12 (1) (2025) 4.
[44] L. Maino, C. Martindale, L. Panny, G. Pope, B. Wesolowski, A direct key recovery attack on SIDH, in: Advances in Cryptology—EUROCRYPT 2023. Part V, in: Lecture Notes in Comput. Sci., vol. 14008, Springer, Cham, 2023, pp. 448–471.
[45] B.D. McKay, The expected eigenvalue distribution of a large regular graph, Linear Algebra Appl. 40 (1981) 203–216.
[46] J.-F. Mestre, La méthode des graphes. Exemples et applications, in: Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields, Katata, 1986, Nagoya Univ., Nagoya, 2024, pp. 217–242.
[47] J.S. Milne, Lectures on étale cohomology, http://www.jmilne.org/math/CourseNotes/LEC.pdf.
[48] T. Miyake, Modular Forms, translated from the Japanese by Yoshitaka Maeda, Springer, Berlin, 1989.
[49] K. Nakagawa, H. Onuki, W. Castryck, M. Chen, R. Invernizzi, G. Lorenzon, F. Vercauteren, SQIsign2D-East: a new signature scheme using 2-dimensional isogenies, in: Advances in Cryptology—ASIACRYPT 2024. Part III, in: Lecture Notes in Comput. Sci., vol. 15486, Springer, Singapore, 2024, pp. 272–303.

[50] A. Page, B. Wesolowski, The supersingular endomorphism ring and one endomorphism problems are equivalent, in: Advances in Cryptology—EUROCRYPT 2024. Part VI, in: Lecture Notes in Comput. Sci., vol. 14656, Springer, Cham, 2024, pp. 388–417.
[51] A.K. Pizer, Ramanujan graphs and Hecke operators, Bull. Am. Math. Soc. (N.S.) 23 (1) (1990) 127–137.
[52] M. Rebolledo Hochart, C. Wuthrich, A moduli interpretation for the non-split Cartan modular curve, Glasg. Math. J. 60 (2) (2018) 411–434.
[53] K.A. Ribet, On modular representations of $\mathrm{Gal}(\overline{Q}/Q)$ arising from modular forms, Invent. Math. 100 (2) (1990) 431–476.
[54] D. Robert, Breaking SIDH in polynomial time, in: Advances in Cryptology—EUROCRYPT 2023. Part V, in: Lecture Notes in Comput. Sci., vol. 14008, Springer, Cham, 2023, pp. 472–503.
[55] J.A. Rouse, A.V. Sutherland, D. Zureick-Brown, ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight), Forum Math. Sigma 10 (2022) e62.
[56] J.-P. Serre, Répartition asymptotique des valeurs propres de l'opérateur de Hecke T_p, J. Am. Math. Soc. 10 (1) (1997) 75–102.
[57] J.H. Silverman, The Arithmetic of Elliptic Curves, second edition, Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[58] L. Trevisan, Lecture notes on graph partitioning, expanders and spectral methods, https://lucatrevisan.github.io/books/expanders-2016.pdf.