Isogeny graphs with level structure and their spectrum

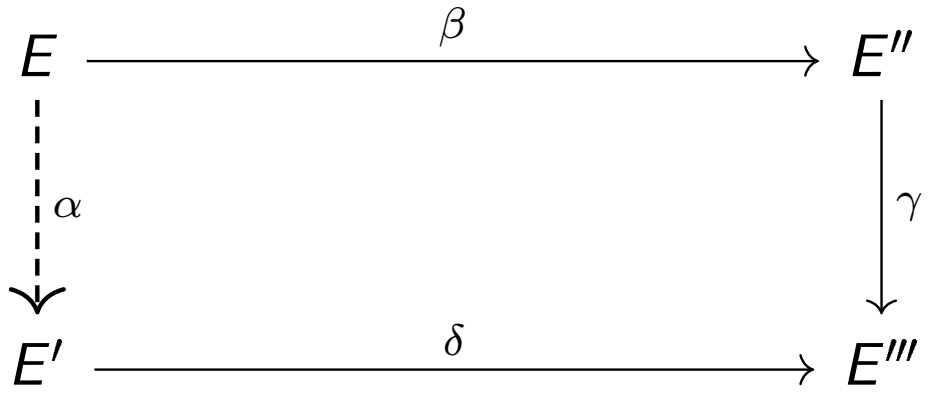
Guido Maria Lido joint work with Giulio Codogni

Università di Roma Tor Vergata

11 October 2023

A ZK proof of knowledge of an isogeny

with Basso, Connolly, De Feo, Fouotsa, Morrison, Panny, Patranabis, Wesolowski



Commit to E'', E''' and reveal β, γ or δ, depending on a challenge

Statistical Zero Knowledge: β, γ, δ are uniformly distributed?

- easy for β, δ because β is chosen at random
- Need equidistribution for $\gamma \leftrightarrow (E'', \ker \gamma)$

  Idea: form an isogeny graph where vertices are pairs (E, C), with $C \cong \mathbb{Z}/N\mathbb{Z}$.

  ... to be continued after the theory

Torsion structures

$$(P, Q) \text{ basis of } E[N] \longleftrightarrow \Phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N],$$
$$\text{change of basis by } h \longleftrightarrow \Phi \circ h$$

Definition (H-structure)

Let E/k be an elliptic curve and let $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, for N coprime to $\operatorname{char} k$. An H-structure on E is an isomorphism

$$\Phi\colon (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N], \qquad \text{up to equivalence } \Phi \sim \Phi \circ h \quad \forall h \in H.$$

- $H = \{\mathrm{Id}\} \to$ Basis — *full level*
- $H = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to$ one structure for each E — *trivial*
- $H = \left\{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\right\} \to C < E[N]$ cyclic of order N — *Borel*
  Take $C = \left\langle \Phi \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \right\rangle \quad \rightsquigarrow \quad$ isogenies.
- $H = \left\{\left(\begin{smallmatrix} * & 0 \\ * & 1 \end{smallmatrix}\right)\right\} \to P \in E[N]$ of order N — *torsion point*

Isogeny graphs with torsion structure

Definition (Isogeny graphs with torsion structure)

Fix p, ℓ distinct primes, and $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for N coprime to $p\ell$. Then $G(p, \ell, H)$ is the oriented graph with

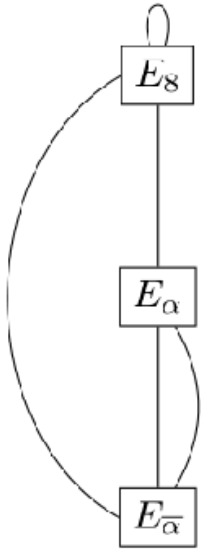
- Vertices $(E_1, \Phi_1), \ldots, (E_r, \Phi_r)$: supersingular elliptic curves $E/\overline{\mathbb{F}_p}$ with a level H-structure Φ, up to isomorphism.
- Edges $(E_i, \Phi_i) \to (E_j, \Phi_j)$: degree ℓ isogenies, up to $\mathrm{Aut}(E_j, \Phi_j)$.

An isogeny $(E_i, \Phi_i) \to (E_j, \Phi_j)$ is an isogeny $\alpha\colon E_i \to E_j$ s.t.

$$\Phi_j^{-1} \circ \alpha \circ \Phi_i \in H \qquad \text{in } \mathrm{End}\left((\mathbb{Z}/N\mathbb{Z})^2\right)$$

It is a $(\ell+1)$-**regular graph**, i.e. from each vertex (E_i, Φ_i) there are $\ell+1$ outgoing edges.

An example with $p = 37$, $\ell = 2$



the classical isogeny graph $= G(p, \ell, \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}))$

the Borel graph $G(p, \ell, \{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\})$ for $N = 3$

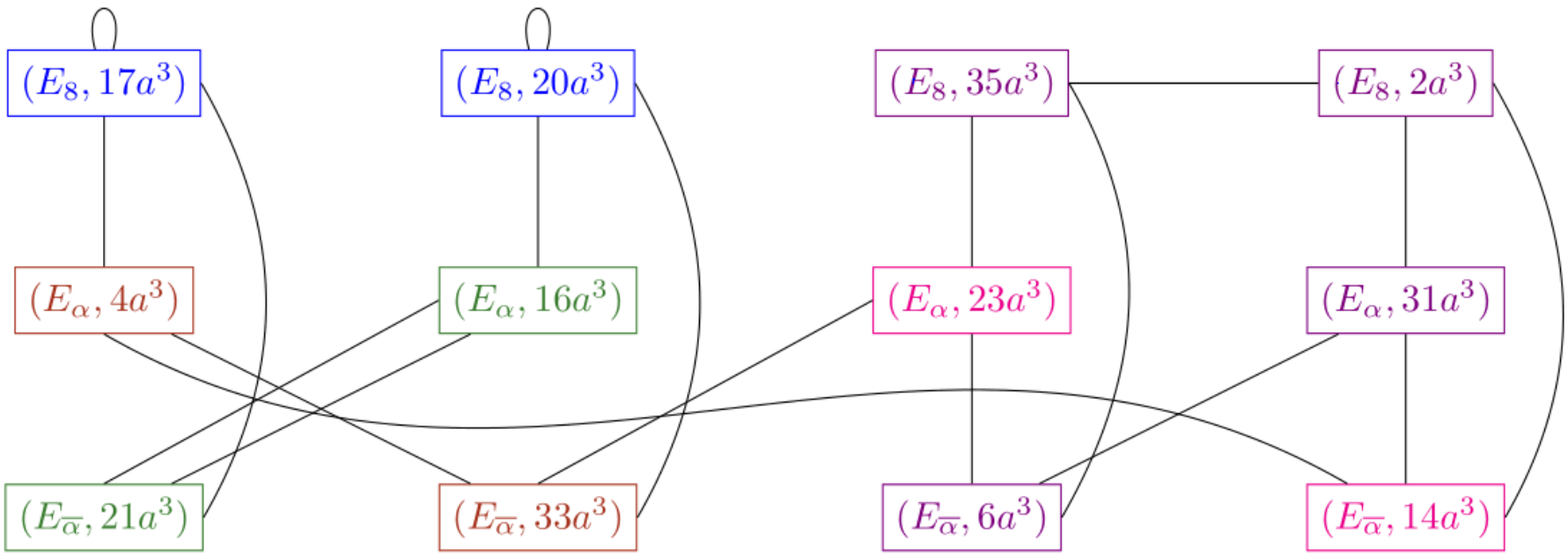


Image by Sarah Arpin

A little more motivation

Remark: keys in SIDH are walks in $G = G(p, \ell, \{Id_N\})$

$$\begin{array}{ccc} (E,\Phi_A,\Phi_B) = (E,P_A,Q_A,P_B,Q_B) & \xrightarrow{\alpha} & (E'',P''_B,Q''_B) = (E'',\Phi''_B) \\ \downarrow \beta & & \downarrow \beta' \\ (E',\Phi'_A) = (E',P'_A,Q'_A) & \xrightarrow{\alpha'} & (E''') \end{array}$$

$$\Phi'_A = \beta \circ \Phi_A\,, \quad \Phi'_B = \alpha \circ \Phi_B \tag{1}$$

$$\text{secret } C_A \subset (\mathbb{Z}/N\mathbb{Z})^2 \rightsquigarrow \ker\alpha = \Phi_A(C_A),\ \ker\alpha' = \Phi'_A(C_A) \tag{2}$$

Castryck-Decru, Maino-Martindale, Robert find short walks in G.

Fouotsa, Moriya, Petit: M-SIDH in $G\left(p, \ell, \left\{\begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix}\right\}\right)$.

Basso, Fouotsa: binSIDH in $G\left(p, \ell, \left\{\begin{pmatrix} \lambda & \\ & \mu \end{pmatrix}\right\}\right)$.

Spectrum of graphs: generalities

Definition (Adjacency matrix)

The adjacency matrix of a graph G with vertices $v_1, \ldots, v_n$ is

$$A = (a_{ij})_{ij} = (\text{number of edges } v_i \to v_j)_{ij} \in \mathbb{Z}^{n \times n}.$$

Theorem

Suppose G is k-regular.

1. k is an eigenvalue, it has multiplicity 1 iff G is connected
2. All walks converge to the same distribution iff all other eigenvalues have absolute value $< k$

1. If $\{v_i, \ldots, v_j\}$ is a component, consider its indicator vector $w = (0, \ldots, 0, 1, \ldots 1, 0 \ldots, 0)$. Then $A^t w = kw$
2. $w_1, \ldots, w_n$ eigenvectors. With B steps a distribution changes

$$D = \sum_{i=1}^{n} a_i w_i \quad \longmapsto \quad A^B D = \sum_{i=1}^{n} \left(\frac{\lambda_i}{k}\right)^B w_i$$

Our result

Theorem (Main)

Fix p, ℓ distinct primes, and $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for N coprime to $p\ell$:

The Weil pairing defines a splitting $G(p, \ell, H) = G_1 \sqcup \ldots \sqcup G_r$.

- *each G_i is connected*
- *the adjacency matrix of G_i is diagonalizable.*
- *it has multiplicity 1 eigenvalues of the shape $(\ell+1)z$, with z a root of unity;*
- *all the other eigenvalues $\lambda_i \in \mathbb{C}$ satisfy $|\lambda_i| \leqslant 2\sqrt{\ell}$*

A similar result also obtained by Aurel Page and Benjamin Wesolowski in *The supersingular Endomorphism Ring and One Endomorphism problems are equivalent*

Classical supersingular isogeny graphs

Theorem (Eichler, 1955)

Let $G(p,\ell) = G(p,\ell,\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}))$. *Then*

- *the graph is connected*
- *the adjacency matrix is diagonalizable with real eigenvalues*
- *all eigenvalues except* $\ell+1$ *are contained in* $[-2\sqrt{\ell}, 2\sqrt{\ell}]$

Random walks converge to limit distribution with speed at least

$$\left(\frac{2\sqrt{\ell}}{ell+1}\right)^{\#\text{ steps}}$$

This speed is optimal:

Theorem (Alon-Boppana and Serre)

G a connected graph, k-regular, with coming back arrows.
G sufficiently$_\epsilon$ *large* $\implies$ $\exists$ *non-trivial eigenvalue* $> 2\sqrt{k-1} - \epsilon$

Weil pairing and isogeny graphs

$w_N(P,Q) = w(\Phi)$ in $\{\text{primitive } N\text{-th roots of unity}\} \cong (\mathbb{Z}/N\mathbb{Z})^\times$

The Weil pairing transforms as

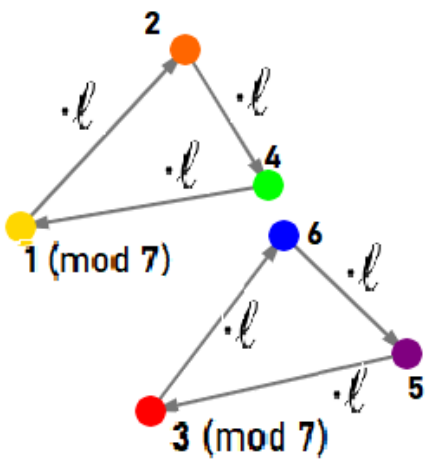
$$w(\Phi \circ h) = w(\Phi)^{\det h} \quad \text{for a change of basis } h \tag{3}$$

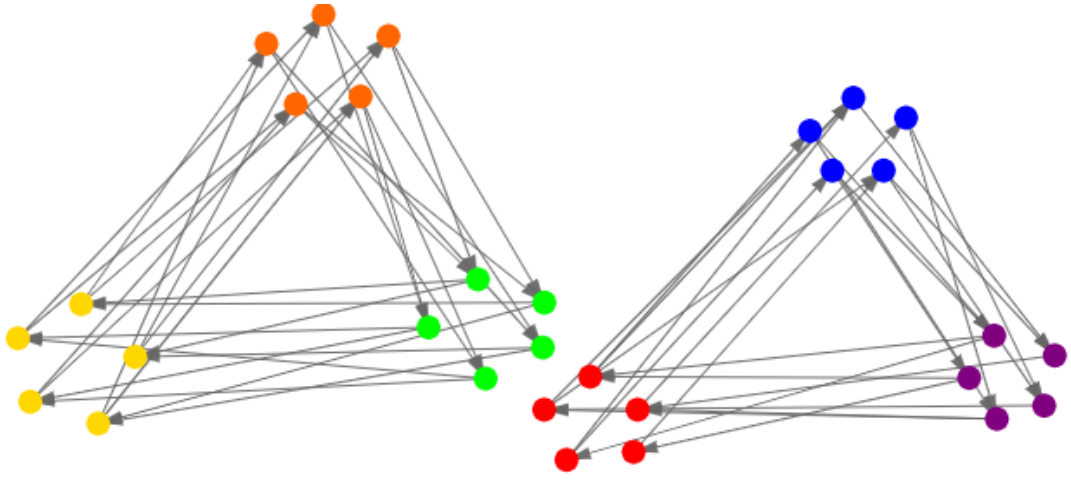
$$w(\Psi) = w(\Phi)^{\deg \alpha} \quad \text{for an isogeny } \alpha\colon (E,\Phi) \to (E',\Psi) \tag{4}$$

Definition

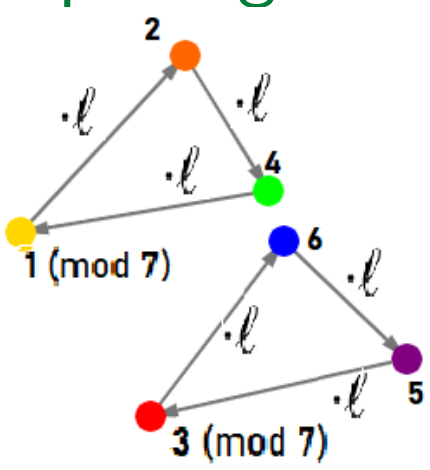
For (E,Φ) an elliptic curve with H-structure, we define

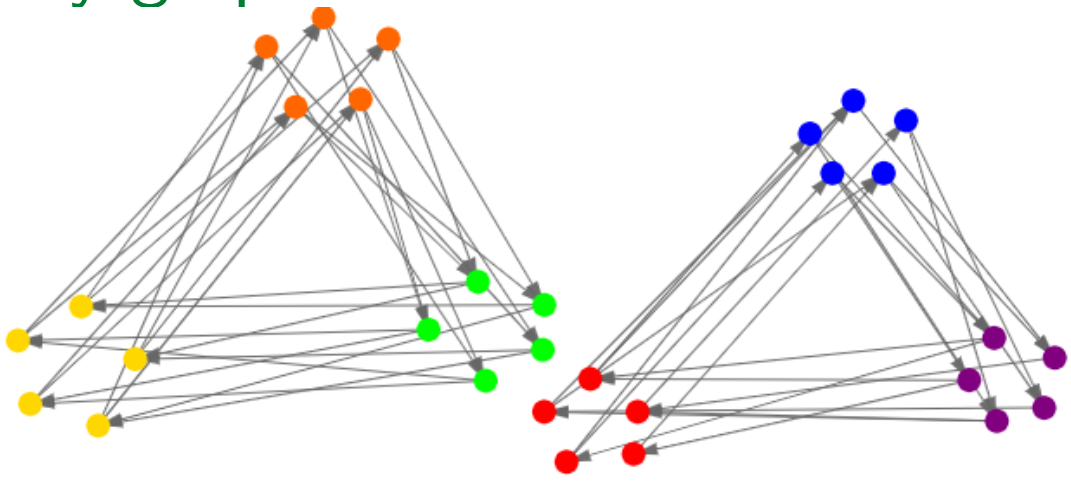
$$w(\Phi) \quad \in \mu_N^\times(\overline{\mathbb{F}_p})/\det H \cong (\mathbb{Z}/N\mathbb{Z})^\times/\det H$$





Weil pairing and isogeny graphs





$G(p, \ell, H)$ is multipartite with $\#(\mathbb{Z}/N\mathbb{Z})^\times / \det H$ parts

Corollary 1: "possible non-connectedness"

$G(p, \ell, H)$ can be subdivided in subgraphs $G_1, \ldots, G_r$ for $r = \#(\mathbb{Z}/N\mathbb{Z})^\times / \langle \ell, \det H \rangle$.

Corollary 2: "spectrum possibly non-real"

Let k be the order of ℓ in $(\mathbb{Z}/N\mathbb{Z})^\times / \det H$.
Then $(\ell+1)z$ is an eigenvalue for each k-root of unity $z \in \mathbb{C}$.

Our result

Theorem (Main)

Fix p, ℓ distinct primes, and $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for N coprime to $p\ell$. Let $G_1, \ldots, G_r$ be the subgraphs of $G(p, \ell, H)$ given by the Weil. Then

- *Each G_i is connected*
- *The adjacency matrix of G_i is diagonalizable.*
- *Each eigenvalue of the shape $(\ell+1)z$ has multiplicity 1; all the other eigenvalues $\lambda_i \in \mathbb{C}$ satisfy $|\lambda_i| \leqslant 2\sqrt{\ell}$*

- Weil pairing (multipartition) not the only reason for $\lambda_i \notin \mathbb{R}$: if $H = \{\left(\begin{smallmatrix} * & 0 \\ * & 1 \end{smallmatrix}\right)\}$ and $N \gg 0$, then trivial partition and $\lambda_i \notin \mathbb{R}$

- if $\left(\begin{smallmatrix} \ell & \\ & \ell \end{smallmatrix}\right) \in H$ the graph has coming back arrows $\implies$ random walks converge quickly to uniform distribution.

Proof: modular curves

Definition (Modular curves)

Fix $K < \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. The modular curve X_K is the normalization of the coarse moduli space for elliptic curves with K-structure.

$$X_K(\overline{\mathbb{F}}) = \{\text{cusps}\} \sqcup \left\{(E/\overline{\mathbb{F}}, \Phi) : \Phi \text{ a } K\text{-structure}\right\}/\sim$$

for $\mathrm{char}\,\mathbb{F} \nmid m$ and the cusps coming from the normalization.

Take $m = Np$ and

$$K = H_p = H \times \left\{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\right\} < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/Np\mathbb{Z})$$

$$H_q\text{-structures} \quad \leftrightarrow \quad (\Phi, C),\ \Phi \text{ a } H\text{-structure}, \ C < E[p] \text{ cyclic of order } p$$

$$X_{H_p}(\overline{\mathbb{F}}) = \{\text{cusps}\} \sqcup \left\{(E/\overline{\mathbb{F}}, \Phi, C)\right\}/\sim \quad \text{if } \mathrm{char}(\mathbb{F}) \nmid N$$

Proof: reduction of modular curves

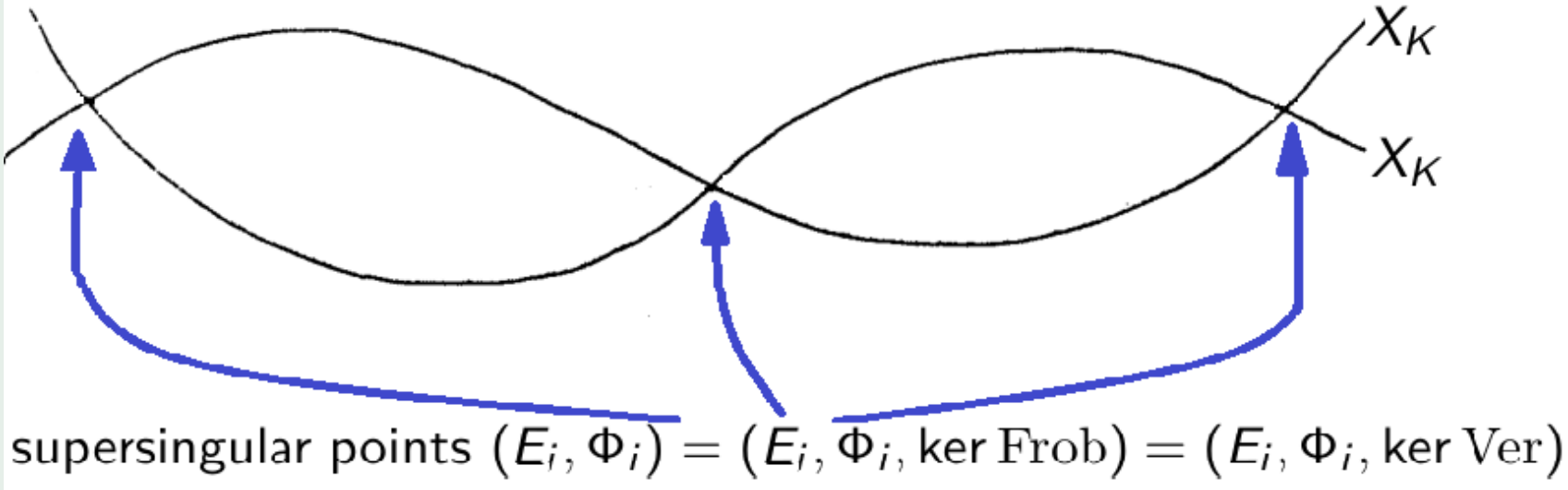
$$X_{H_p}(\overline{\mathbb{F}}) = \{\text{cusps}\} \sqcup \{(E/\overline{\mathbb{F}}, \Phi, C)\}/\sim \qquad \text{if } \operatorname{char}(\mathbb{F}) \nmid N$$

It also makes sense over $\overline{\mathbb{F}_p}$. Then there are two kinds of points:

$$X_H(\overline{\mathbb{F}_p}) \hookrightarrow X_{H_p}(\overline{\mathbb{F}_p}), \quad (E, \Phi) \mapsto (E, \Phi, \ker \mathrm{Frob})$$
$$X_H(\overline{\mathbb{F}_p}) \hookrightarrow X_{H_p}(\overline{\mathbb{F}_p}), \quad (E, \Phi) \mapsto (E, \Phi, \ker \mathrm{Ver})$$

Theorem (Eichler-Shimura 1)

The reduction of X_{H_p} modulo p is as follows



Proof: Hecke operators (general subgroup K)

$$\mathrm{pr}_q \colon X_{K_q} \longrightarrow X_K\,, \quad (E,\Phi,C) \mapsto (E,\Phi)\,,$$
$$\mathrm{quot}_q \colon X_{K_q} \longrightarrow X_K\,, \quad (E,\Phi,C) \mapsto (E/C, \pi_C \circ \Phi), \quad \pi_C \colon E \to E/C$$

Definition (Hecke operator)

Fix $K < \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and q prime to m. Let $J_K = \mathrm{Pic}^0(X_K)$.

$$T_q = \mathrm{quot}_{q,*} \circ \mathrm{pr}_q^* \colon J_K \longrightarrow J_K$$
$$\Longrightarrow \quad T_q(E,\phi) = \sum_{C < E[q]} (E/C, \pi_C \circ \Phi) \quad \text{as divisors}$$

Theorem (Eichler-Shimura 2)

If q is prime, the reduction modulo q of T_q satisfies

$$\overline{T_q} = \mathrm{Frob} + \langle q \rangle_* \,\mathrm{Ver} \quad \textit{in } \mathrm{End}(J_{K,\mathbb{F}_q})$$

where $\langle q \rangle \colon X_K \to X_K$ is the automorphism $(E,\phi) \mapsto (E, q\phi)$.

Proof

Theorem (Main)

Fix p, ℓ distinct primes, and $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for N coprime to $p\ell$. Let $G_1, \ldots, G_r$ be the subgraphs of $G(p, \ell, H)$ given by the Weil. Then

- *Each G_i is connected*
- *The adjacency matrix of G_i is diagonalizable.*
- *Each eigenvalue of the shape $(\ell+1)z$ has multiplicity 1; all the other eigenvalues $\lambda_i \in \mathbb{C}$ satisfy $|\lambda_i| \leqslant 2\sqrt{\ell}$*

Proof

Theorem (Main')

Fix p, ℓ distinct primes, and $H < \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for N coprime to $p\ell$. The non-trivial eigenvalues of $G(p, \ell, H)$ satisfy $|\lambda_i| \leqslant 2\sqrt{\ell}$

Consider X_K for $K = H_p$.

Hecke on singular points of $X_K(\overline{\mathbb{F}_p})$ $\leftrightarrow$ adjacency matrix

$$T_\ell(E, \Phi) = \sum_{C < E[\ell]} (E/C, \pi_C \circ \Phi) \tag{5}$$

Singular points of $X_K(\overline{\mathbb{F}_p})$ $\rightsquigarrow$ toric part $T = \tilde{J}_{\mathbb{F}_p}$ of $J_{K,\mathbb{F}_p}$ (6)

(5) + (6) $\implies$ {non-trivial λ_i} = spectrum of $T_\ell \circlearrowright \mathrm{Hom}(T, \mathbb{G}_\mathrm{m})$

{non-trivial λ_i} = spectrum of $T_\ell \circlearrowright T_{\ell'} T := \varprojlim T[\ell'^k]$

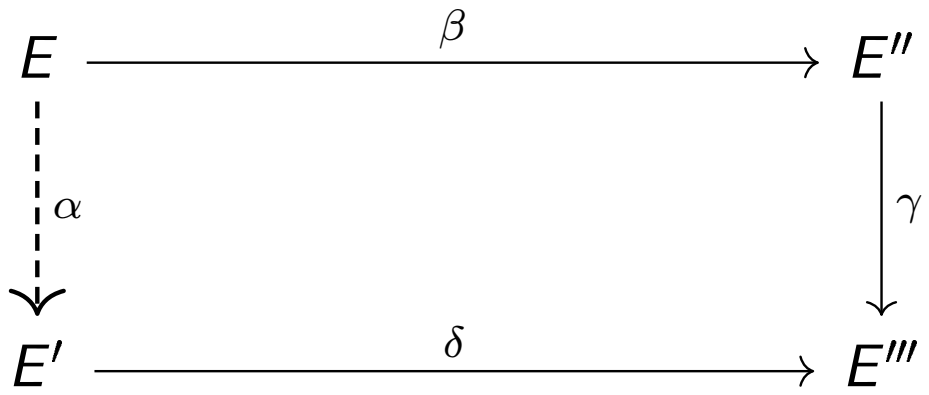
{non-trivial λ_i}$^{\sqcup 2}$ = spectrum of $T_\ell \circlearrowright T_{\ell'} \tilde{J}_{\mathbb{Q}} = T_{\ell'} \tilde{J}_{\mathbb{F}_\ell}$

{non-trivial λ_i}$^{\sqcup 2}$ = spectrum of $\mathrm{Frob} + \langle \ell \rangle_* \mathrm{Ver} \circlearrowright T_{\ell'} \tilde{J}_{\mathbb{F}_\ell}$

$\lambda_i = \mu + \xi\overline{\mu}$ with $|\mu| = \sqrt{\ell}$ and $|\xi| = 1$ $\implies$ $|\lambda_i| \leqslant 2\sqrt{\ell}$ $\square$

A ZK proof of knowledge of an isogeny (2)

with Basso, Connolly, De Feo, Fouotsa, Morrison, Panny, Patranabis, Wesolowski



Commit to E'', E''' and reveal β, γ or δ, depending on a challenge

Statistical Zero Knowledge: β, γ, δ are uniformly distributed?

- easy for β, δ because β is chosen at random
- Need equidistribution for $\gamma \leftrightarrow (E'', \ker \gamma)$

β is a random walk in $G(p, \ell, \{\left(\begin{smallmatrix} * & 0 \\ * & * \end{smallmatrix}\right)\})$, with degree ℓ^k

Main Theorem $\implies$ γ (close to) uniformly distributed if $k \gg 0$

Thank you!