

Can we use Bruhat-Tits trees to better understand supersingular isogeny graphs?

joint work with
Laia Amorós, Kristin Lauter, Chloe Martindale and Jana Sotáková

ANNAMARIA IEZZI

Université de la Polynésie Française

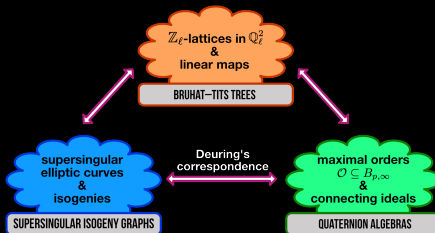
AGC²T

June 1, 2021

Goal of this talk

Explicit connections between supersingular isogeny graphs and Bruhat-Tits trees

Laia Amorós, Annamaria Iezzi, Kristin Lauter, Chloe Martindale, Jana Sotáková. (2021)
<https://eprint.iacr.org/2021/372>



Bruhat-Tits trees in the context of supersingular isogeny graphs also appear in:

- *Exploring isogeny graphs* - Luca De Feo's HDR thesis (2018).
- *Ramanujan Graphs in Cryptography* - Costache, Feigon, Lauter, Massierer, Puskás (2019).

A little bit of context

Supersingular isogeny graphs were:

- **Introduced** by Pizer in 1990: *Graphs and Hecke operators*.
- **Brought into cryptography** by Charles, Goren and Lauter in 2006: *Cryptographic Hash functions from expander graphs*.
- **Proposed for a Diffie-Hellman key exchange** by Jao and De Feo in 2011: *Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies*.



SIKE: NIST 3rd round alternate candidate (July 2020) for the public key encryption and key encapsulation mechanism.

Supersingular ℓ -isogeny graphs

Let $p > 3$ and ℓ be primes such that $p \neq \ell$ (p large, ℓ small).

We denote $\mathcal{G}_\ell(\overline{\mathbb{F}}_p)$ the supersingular ℓ -isogeny graph over $\overline{\mathbb{F}}_p$ with:

- **Vertices:**

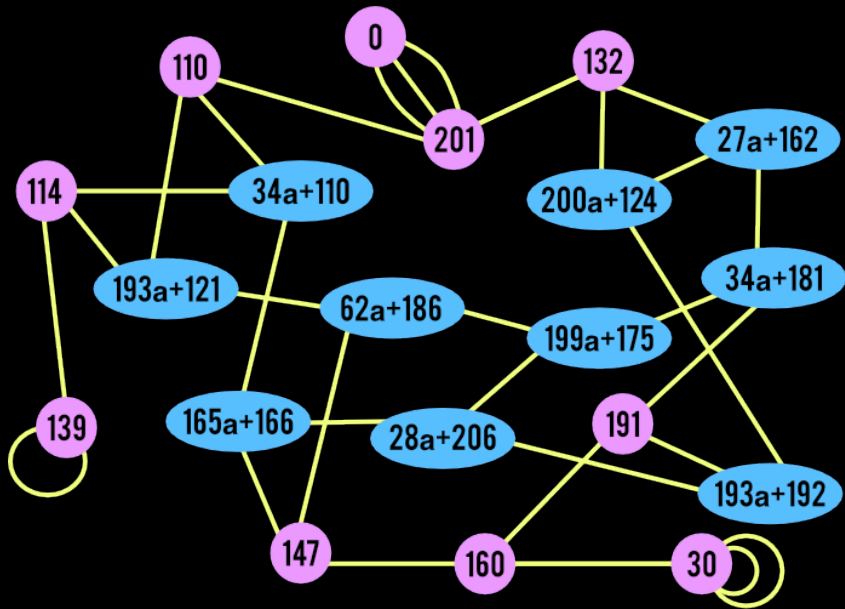
$$\left\{ \begin{array}{c} \overline{\mathbb{F}}_p\text{-isomorphism classes of supersingular elliptic curves} \\ \text{defined over } \overline{\mathbb{F}}_p \end{array} \right\}$$



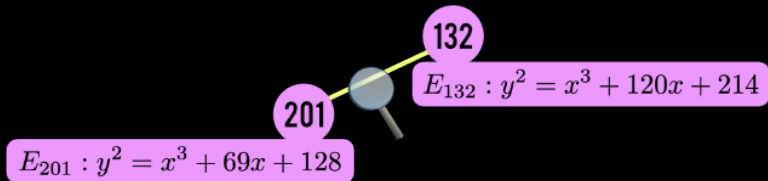
$$\{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}$$

- **Edges:** isogenies of degree ℓ (up to a certain equivalence).

$$\mathcal{G}_2(\overline{\mathbb{F}}_{227})$$



$$\mathcal{G}_2(\overline{\mathbb{F}}_{227})$$



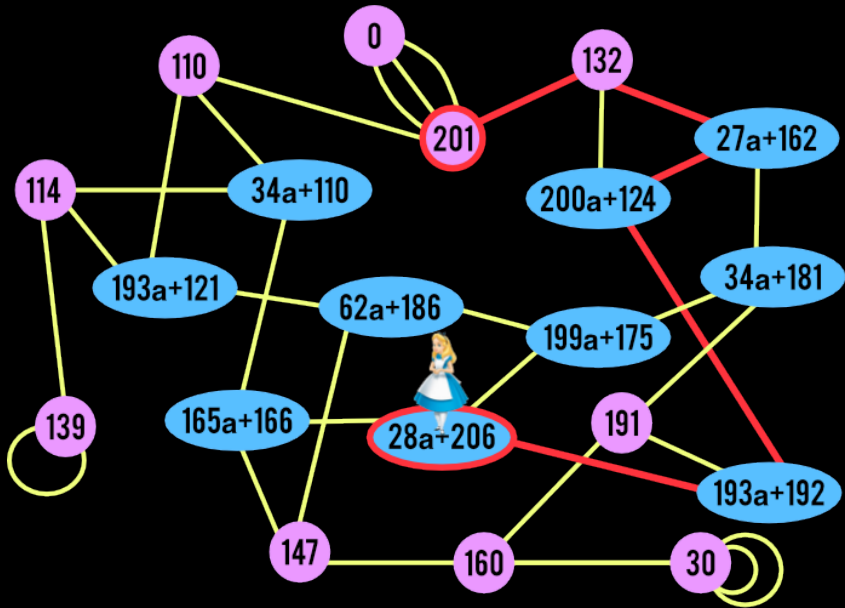
$$\begin{aligned} \varphi : E_{201} &\rightarrow E_{132} \\ (x, y) &\mapsto \left(\frac{x^2 + 84x - 101}{x + 84}, y \frac{x^2 - 59x - 107}{x^2 - 59x + 19} \right) \end{aligned}$$

Properties of supersingular isogeny graphs

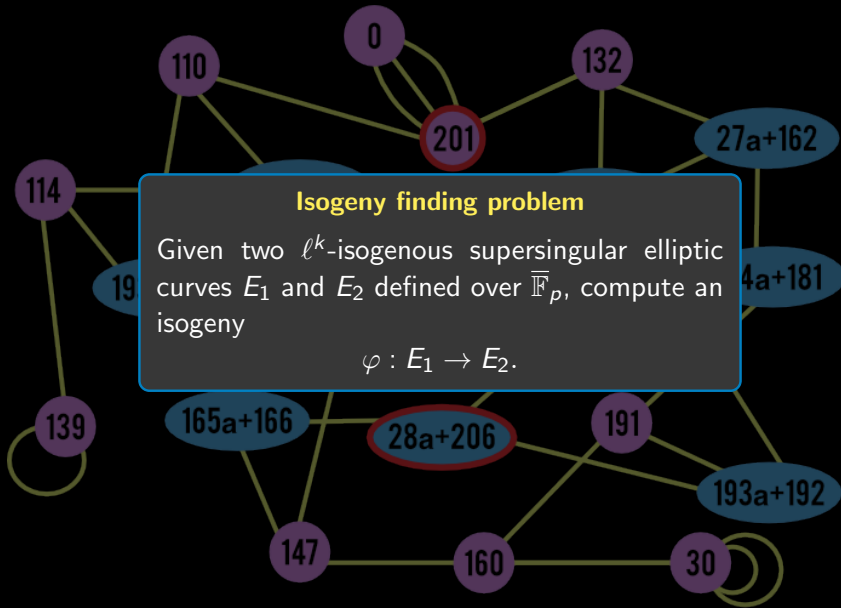
A supersingular ℓ -isogeny graph over $\overline{\mathbb{F}}_p$ is:

- Exponentially large
Approximately $\frac{p}{12}$ vertices
- Connected with diameter $O(\log(p))$
- $\ell + 1$ -regular
Except possibly at $j = 0$, $j = 1728$ and their neighbors (because of the extra automorphisms).
- Ramanujan graph (i.e. optimal expander graphs)
Relatively short walks on the graph approximate the uniform distribution.

Random walks



Random walks



Non-backtracking walks

$\{\text{non-backtracking walks from } E/\mathbb{F}_{p^2} \text{ of length } n \text{ in } \mathcal{G}_\ell(\overline{\mathbb{F}}_p)\}$



$\{\text{cyclic (separable) isogenies } \varphi : E \rightarrow E' \text{ of degree } \ell^n\}$



$\{\text{cyclic subgroups of order } \ell^n \text{ in } E[\ell^n]\}$

Let $E[\ell^n] = \langle P_n, Q_n \rangle \cong \frac{\mathbb{Z}}{\ell^n \mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^n \mathbb{Z}}$ and let $G \leq E[\ell^n]$ be a cyclic subgroup of order ℓ^n . Then:

- $G = \langle P_n + aQ_n \rangle$, $0 \leq a < \ell^n$ or
- $G = \langle Q_n + bP_n \rangle$, $0 \leq b < \ell^n$, $b \equiv 0 \pmod{\ell}$.

So there are

$$\ell^n + \ell^{n-1} = (\ell + 1)\ell^{n-1}$$

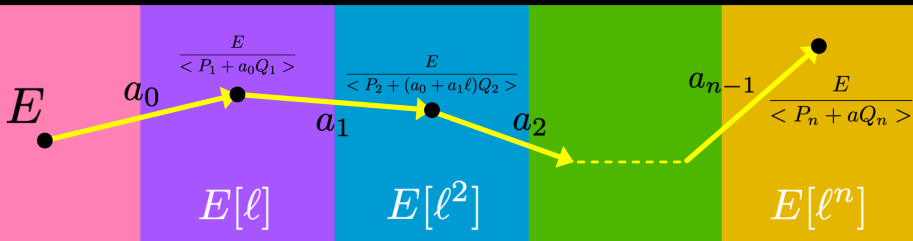
cyclic subgroups of order ℓ^n in $E[\ell^n]$.

Let's have a look to one of these walks

- $E[\ell^n] = \langle P_n, Q_n \rangle$
- For $i = 1, \dots, n-1$:
 $P_i = \ell^{n-i} P_n, Q_i = \ell^{n-i} Q_n \Rightarrow E[\ell^i] = \langle P_i, Q_i \rangle$
- $G = \langle P_n + aQ_n \rangle, 0 \leq a < \ell^n$

The ℓ -adic representation of a can be used to reconstruct each step of the walk:

$$a = \sum_{i=0}^{n-1} a_i \ell^i, 0 \leq a_i < \ell.$$



An infinite tree (for $\ell = 3$)

To build the infinite tree

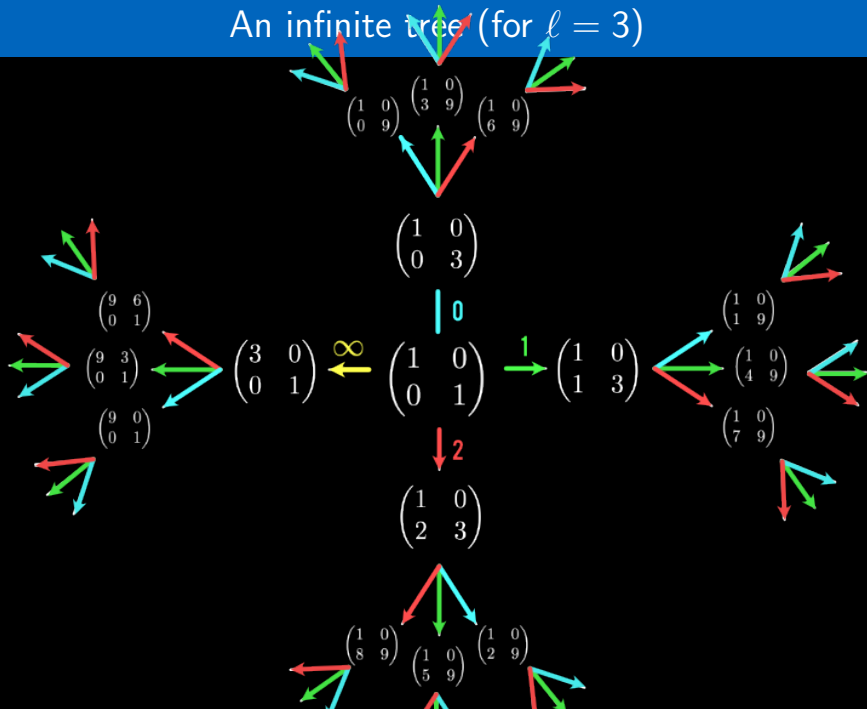
Fix a basis of the ℓ -adic Tate module

$$T_\ell(E) = \langle P, Q \rangle \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell,$$

where $P = (P_1, P_2, P_3, \dots)$, $Q = (Q_1, Q_2, Q_3, \dots)$ and

$$E[\ell^i] = \langle P_i, Q_i \rangle.$$

An infinite tree (for $\ell = 3$)



Bruhat-Tits trees

We use here the notation \mathbb{Q}_ℓ for matching the notation coming from supersingular isogeny graphs.

For each prime ℓ , we can define the **Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_\ell)$** . We can look at its vertices from different perspectives:

- classes of homothetic \mathbb{Z}_ℓ -lattices in \mathbb{Q}_ℓ^2 ;
- classes of matrices in $\mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$;
- maximal orders in the quaternion algebra $M_2(\mathbb{Q}_\ell)$.

Homothetic lattices of \mathbb{Q}_ℓ^2

- A **lattice** L of \mathbb{Q}_ℓ^2 is a free \mathbb{Z}_ℓ -module of rank 2 of \mathbb{Q}_ℓ^2 :

$$L = \langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{Z}_\ell} = \mathbb{Z}_\ell \mathbf{u} + \mathbb{Z}_\ell \mathbf{v} = \{x\mathbf{u} + y\mathbf{v} : x, y \in \mathbb{Z}_\ell\}$$

- We say that two lattices L_1 and L_2 are **homothetic** if there exists $\lambda \in \mathbb{Q}_\ell^\times$ such that $L_1 = \lambda L_2$. We denote $[L]$ the homothety class of a lattice L .
- Two homothety classes $[L_1]$ and $[L_2]$ are said to be **adjacent** if their representatives L_1 and L_2 can be chosen so that

$$\ell L_1 \subsetneq L_2 \subsetneq L_1.$$

EXAMPLE:

Given $L = \langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{Z}_\ell}$ there are $\ell + 1$ -lattices L_i such that $\ell L \subsetneq L_i \subsetneq L$:

$$(\mathbf{u} \quad \mathbf{v}) \begin{pmatrix} 1 & 0 \\ i & \ell \end{pmatrix}, i = 0, \dots, \ell - 1 \quad \text{and} \quad (\mathbf{u} \quad \mathbf{v}) \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$$

The Bruhat-Tits tree for $\mathrm{PGL}_2(\mathbb{Q}_\ell)$

The Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ is the graph \mathcal{T}_ℓ with

- $\mathrm{Ver}(\mathcal{T}_\ell)$: homothety classes of lattices of \mathbb{Q}_ℓ^2 .
- $\mathrm{Ed}(\mathcal{T}_\ell)$: set of pairs of adjacent homothety classes.

The (undirected) graph \mathcal{T}_ℓ is a $(\ell + 1)$ -regular infinite tree.

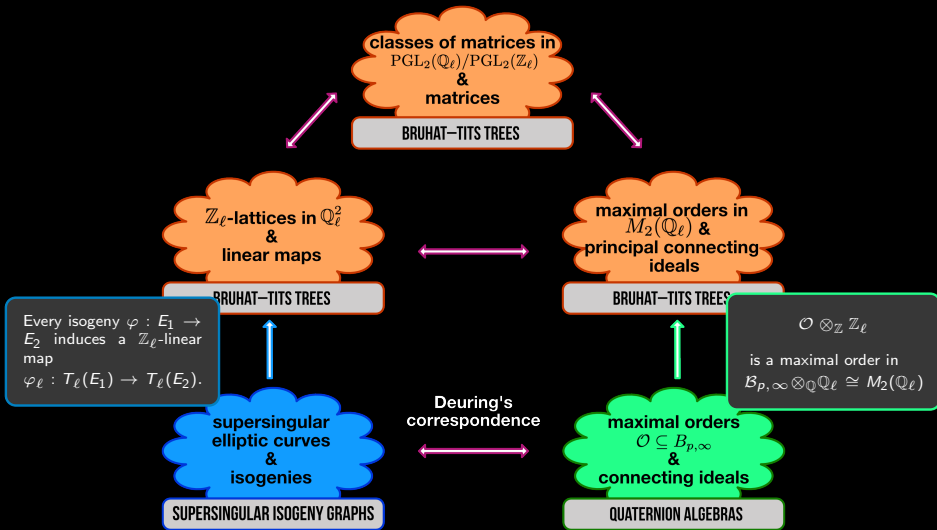
- From lattices to matrices:

$$\begin{array}{ccc} \{\text{homothety classes of lattices of } \mathbb{Q}_\ell^2\} & \longleftrightarrow & \mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell) \\ [L] = [\langle \mathbf{u}, \mathbf{v} \rangle_{\mathbb{Z}_\ell}] & \mapsto & [(\mathbf{u}|\mathbf{v})] \end{array}$$

- From lattices to maximal orders in $M_2(\mathbb{Q}_\ell)$:

$$\begin{array}{ccc} \{\text{homothety classes of lattices of } \mathbb{Q}_\ell^2\} & \longleftrightarrow & \{\text{maximal orders in } M_2(\mathbb{Q}_\ell)\} \\ [L] & \mapsto & \mathrm{End}(L) \end{array}$$

Connections



How to fold the Bruhat–Tits trees?

Fix an embedding

$$\phi_\ell : B_{p,\infty} \rightarrow M_2(\mathbb{Q}_\ell)$$

and let \mathcal{O} a maximal order in $B_{p,\infty}$.

Let $\Gamma_\ell = \phi_\ell(\mathcal{O} \begin{bmatrix} 1 & \\ & \ell \end{bmatrix}^\times)$. Then

$$\Gamma_\ell \backslash \mathcal{T}_\ell = \Gamma_\ell \backslash \mathrm{PGL}_2(\mathbb{Q}_\ell) / \mathrm{PGL}_2(\mathbb{Z}_\ell)$$

is isomorphic to the supersingular ℓ -isogeny graph over $\overline{\mathbb{F}}_p$.

One can define a subgroup $\Gamma_{\ell,+} \subseteq \Gamma_\ell$ such that

$$\Gamma_{\ell,+} \backslash \mathcal{T}_\ell$$

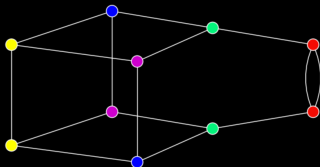
is the graph of the special fiber of a certain Shimura curve which is a 2-covering of the supersingular ℓ -isogeny graph.

Sage can compute this quotient using the **BTQuotient** module based on the algorithm given by:

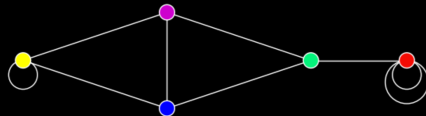
- Cameron Franc and Marc Masdeu, *Computing fundamental domains for the Bruhat–Tits tree for $GL_2(\mathbb{Q}_p)$, p -adic automorphic forms, and the canonical embedding of Shimura curves* (2014).

How to fold the Bruhat–Tits trees?

$$p = 61, \quad \ell = 2$$



$$\Gamma_{2,+} \setminus \mathcal{T}_2$$



$$\mathcal{G}_2(\overline{\mathbb{F}}_{61})$$

One can define a subgroup $\Gamma_{\ell,+} \subseteq \Gamma_{\ell}$ such that

$$\Gamma_{\ell,+} \setminus \mathcal{T}_{\ell}$$

is the graph of the special fiber of a certain Shimura curve which is a **2-covering of the supersingular ℓ -isogeny graph**.

Sage can compute this quotient using the **BTQuotient** module based on the algorithm given by:

- Cameron Franc and Marc Masdeu, *Computing fundamental domains for the Bruhat–Tits tree for $GL_2(\mathbb{Q}_p)$, p -adic automorphic forms, and the canonical embedding of Shimura curves* (2014).