Bruhat-Tits trees as a cryptanalitic tool for isogeny-based cryptography

ANNAMARIA IEZZI

Université de la Polynésie Française

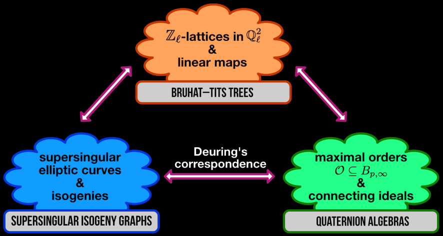
Cryptography and Coding Theory - First Annual Conference

September 22, 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).
- *Computing endomorphism rings of supersingular elliptic curves and connections to pathfinding in isogeny graphs* -Eisenträger, Hallgren, Leonardi, Morrison, Park (2020).

A little bit of context

Supersingular isogeny graphs were:

- First considered by Mestre and Oesterlé in the 1986: *La méthode des graphes. Exemples et applications.*
- 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*.
  $\downarrow$
  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:**

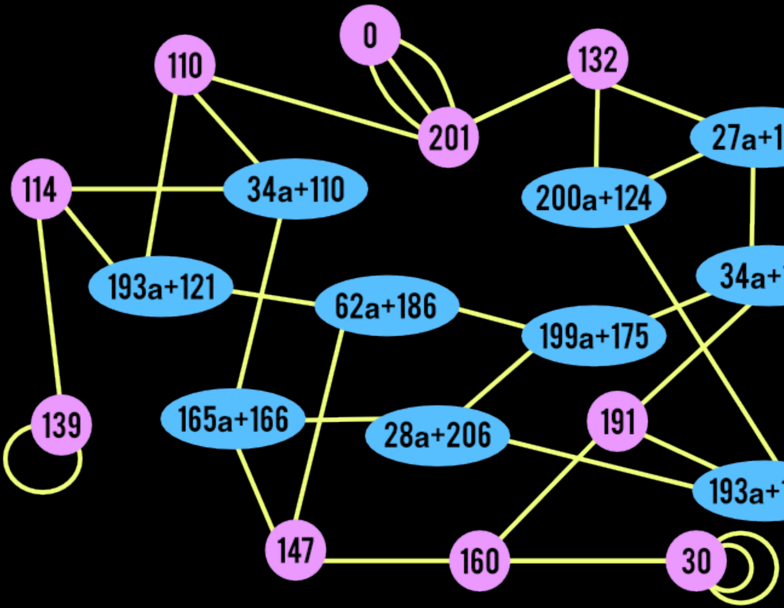
$$\left\{ \begin{array}{c} \overline{\mathbb{F}}_p\text{-isomorphism classes of supersingular elliptic curves} \\ \text{defined over } \overline{\mathbb{F}}_p \end{array} \right\}$$

$$\updownarrow$$

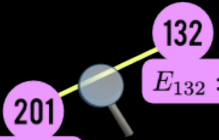
$$\{\text{supersingular } j\text{-invariants in } \mathbb{F}_{p^2}\}$$

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

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



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

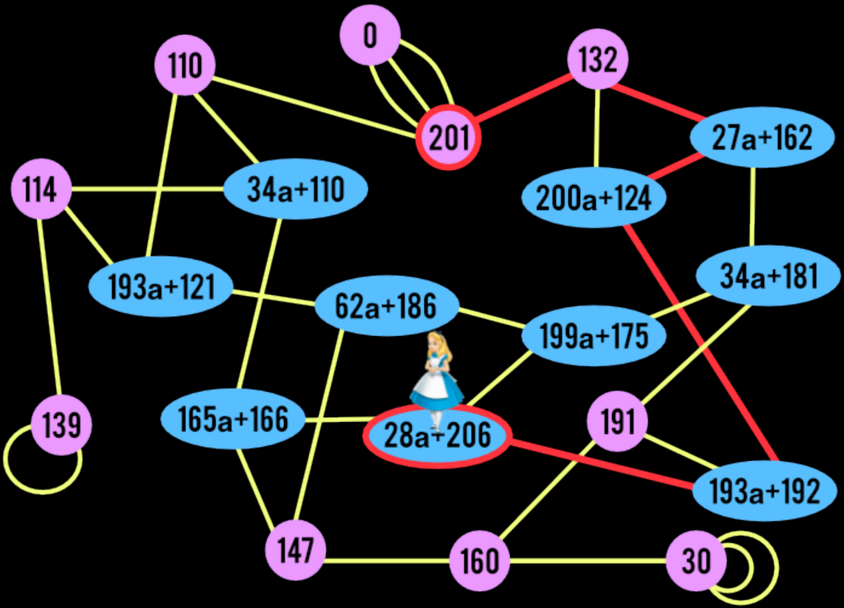


$E_{132} : y^2 = x^3 + 120x + 214$

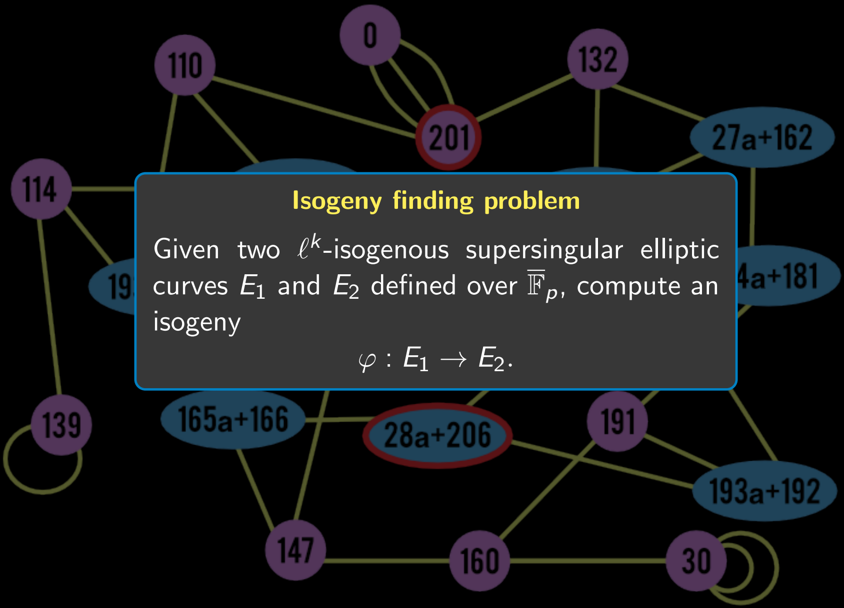
$E_{201} : y^2 = x^3 + 69x + 128$

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

Random walks



Random walks



Isogeny finding problem

Given two ℓ^k-isogenous supersingular elliptic curves E_1 and E_2 defined over $\overline{\mathbb{F}}_p$, compute an isogeny

$$\varphi : E_1 \to E_2.$$

Non-backtracking walks

$$\{\text{non-backtracking walks from } E/\mathbb{F}_{p^2} \text{ of length } n \text{ in } \mathcal{G}_\ell(\overline{\mathbb{F}}_p)\}$$
$$\updownarrow$$
$$\{\text{cyclic (separable) isogenies } \varphi : E \to E' \text{ of degree } \ell^n\}$$
$$\updownarrow$$
$$\{\text{ cyclic subgroups of order } \ell^n \text{ in } E[\ell^n]\}$$

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

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

So there are

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

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

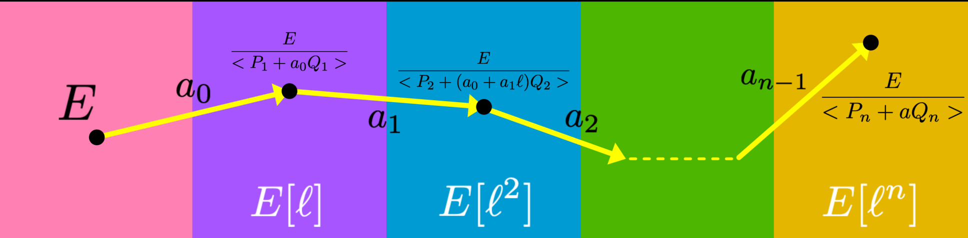
Let's have a look to one of these walks

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

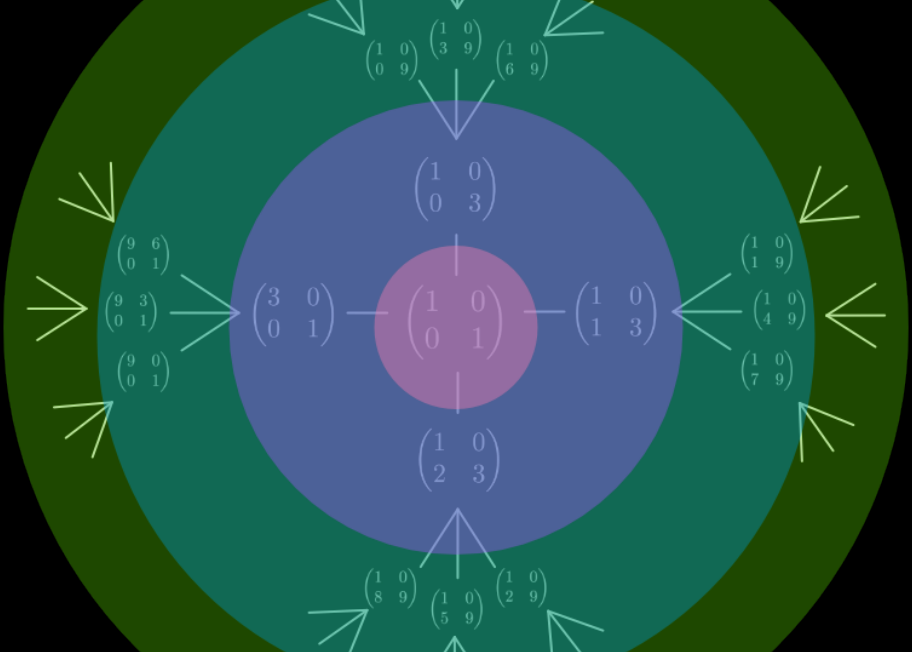
Consider the walk associated to the cyclic isogeny $\varphi : E \to \frac{E}{<P_n + aQ_n>}$.

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

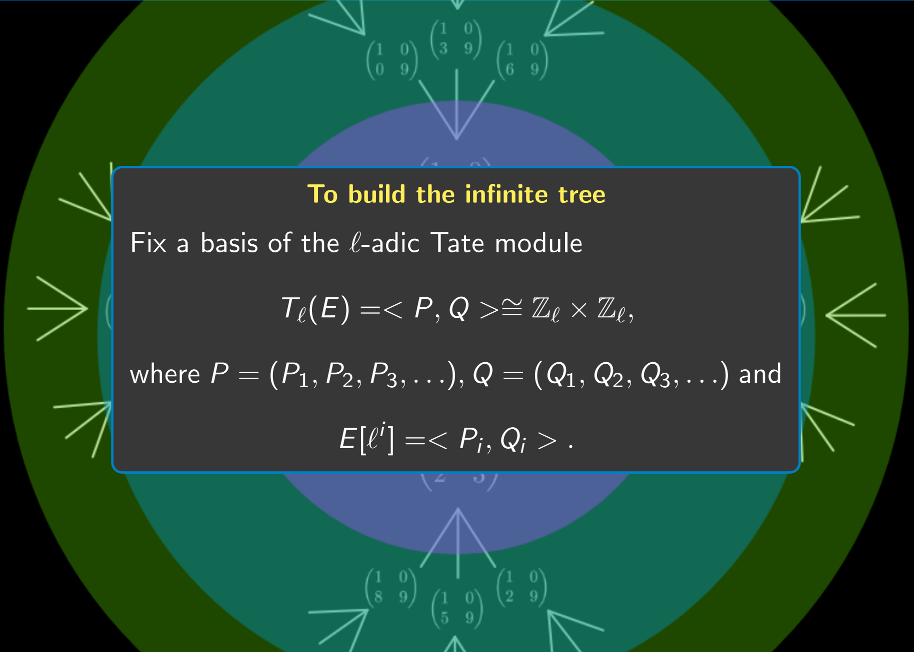
$$a = \sum_{i=0}^{n-1} a_i \ell^i, 0 \leq a_i < \ell.$$



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



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



To build the infinite tree

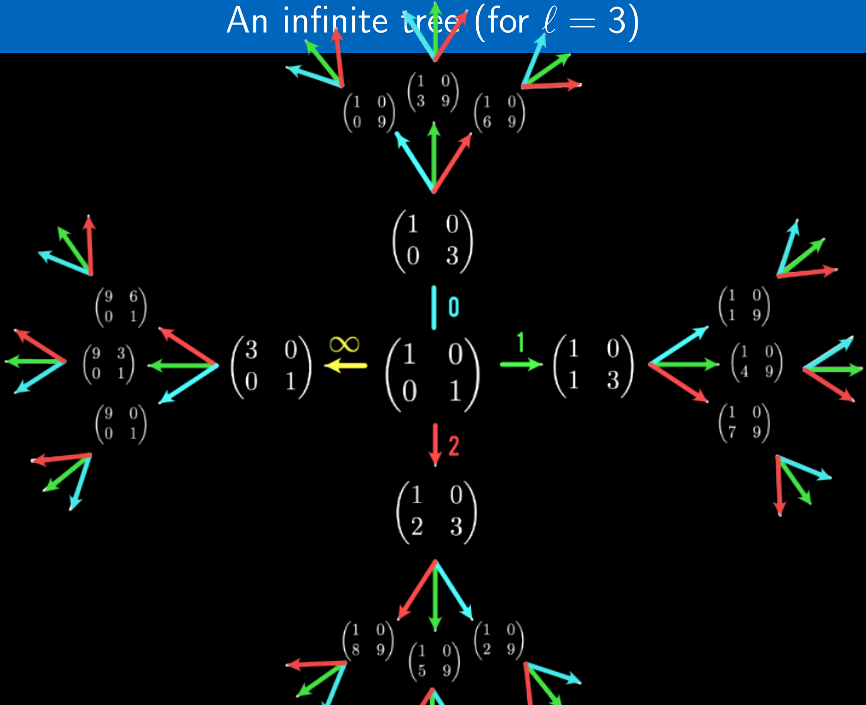
Fix a basis of the ℓ-adic Tate module

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

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

$$E[\ell^i] =< P_i, Q_i > .$$

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



Bruhat-Tits trees

We use here the notation $\mathbb{Q}_\ell$ 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 $\mathbb{Z}_\ell$-lattices in $\mathbb{Q}_\ell^2$;
- classes of matrices in $\mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$;
- maximal orders in the quaternion algebra $\mathrm{M}_2(\mathbb{Q}_\ell)$.

Homothetic lattices of $\mathbb{Q}_\ell^2$

- A lattice L of $\mathbb{Q}_\ell^2$ is a free $\mathbb{Z}_\ell$-module of rank 2 of $\mathbb{Q}_\ell^2$:

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

- 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 $\ell L \subsetneq L_i \subsetneq L$:

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

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 $\mathcal{T}_\ell$ with

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

> The (undirected) graph $\mathcal{T}_\ell$ 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