Supersingular Elliptic Curve Isogeny Graphs with Level Structure

Sarah Arpin, University of Colorado Boulder

sarah.arpin@colorado.edu

WCNT 2021: Problems in Number Theory

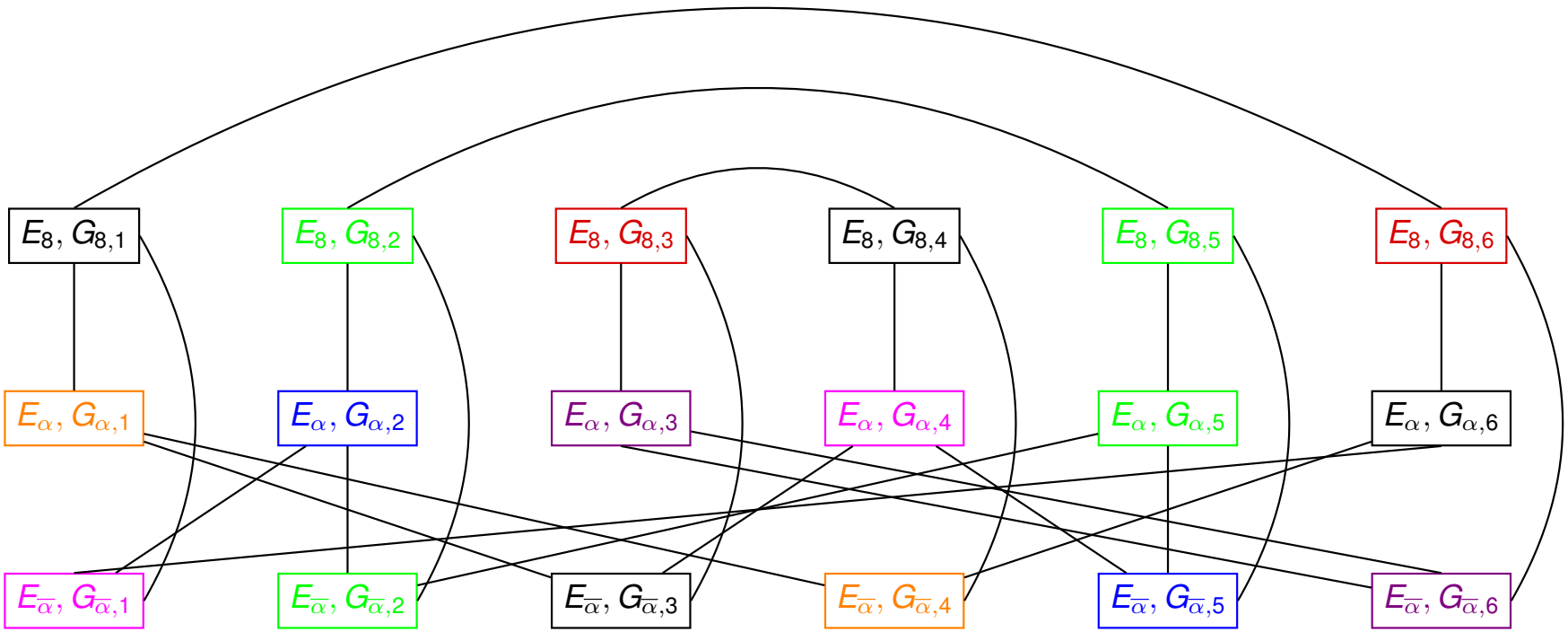
December 17th, 2021

Table of Contents

1 Background

2 Isogeny Graph With Level Structure

3 Summary



Supersingular Elliptic Curves

Definition (Chapter V[Sil09])

Let E be an elliptic curve defined over a field K of characteristic $p \neq \infty$. E is **supersingular** iff $\mathrm{End}(E)$ is a maximal order in a quaternion algebra.

For a given p, there are finitely many isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Each isomorphism class has a representative defined over $\mathbb{F}_{p^2}$.

Convention

p: a fixed **large** prime (cryptographic size)
$p \equiv 3 \pmod 4$ (minor adjustments for other p)

Isogenies

Definition

An **isogeny** $\phi : E_1 \to E_2$ is a morphism between elliptic curves such that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. It has a dual $\widehat{\phi} : E_2 \to E_1$.

Theorem (Corollary III.4.9 and Proposition III.4.12 [Sil09])

The kernel of a nonzero isogeny is a finite group. A given finite subgroup of points uniquely determines a separable isogeny.

Theorem (Theorem III.4.10(c) [Sil09])

The degree of a separable isogeny is equal to the size of the kernel.

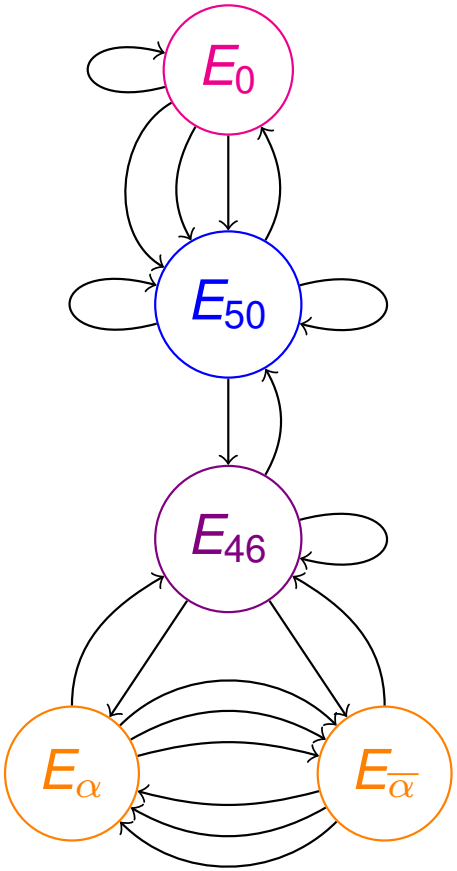
Convention

Isogenies will be degree ℓ or ℓ^r, with ℓ a small prime.

Supersingular elliptic curves over $\overline{\mathbb{F}}_p$ are all ℓ-power isogenous.

Supersingular ℓ-isogeny graph

$p = 53, \ell = 3$



- With the right conditions on p, can be taken to be *undirected* by identifying isogenies with their duals
- Connected
- Out-degree $\ell + 1$
- $\sim \lfloor \frac{p}{12} \rfloor$ nodes

Quaternion Algebras: A Comparison to Number Fields

For thorough background, see [Voi21]

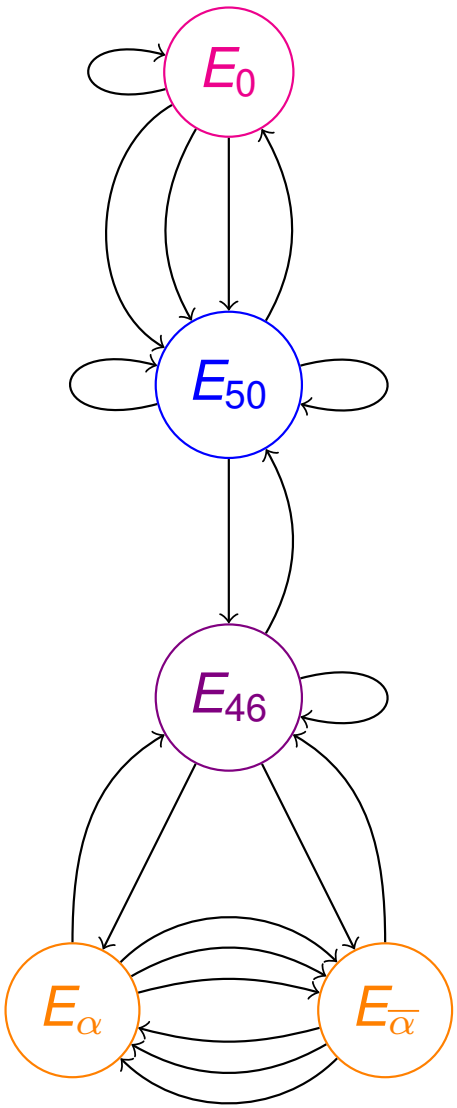
Quaternion Algebra $B_{p,\infty}$	**Imaginary Quadratic Field**
Noncommutative	Commutative
$\mathbb{Q}\langle i, j, ij\rangle : i^2 = -1, j^2 = -p, ij = -ji$	$\mathbb{Q}\langle\sqrt{-d}\rangle$
Maximal orders (finitely many)	$\mathcal{O}_K$
Eichler orders of level N	Orders of conductor N: $\mathbb{Z} + N\mathcal{O}_K$
Class set of left or right ideals Class group of two-sided ideals	Class group of ideals
End rings of supersingular EC's	End rings of ordinary EC's

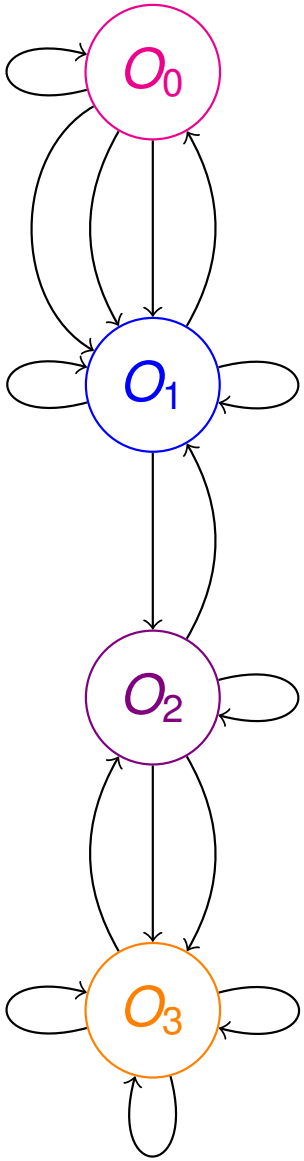
Theorem (Deuring Correspondence [Deu41])

If $E/\overline{\mathbb{F}}_p$ is supersingular, then there is a maximal order $\mathcal{O}$ of $B_{p,\infty}$ such that $End(E) \cong \mathcal{O}$. This association is either 2-1 or 1-1, depending on the size of the two-sided ideal class group of $\mathcal{O}$.

Hard to compute.

Quaternion Analog of Supersingular ℓ-Isogeny Graph





Isogeny Graph $\mathcal{E}_{p,\ell}^{N}$ With Level Structure

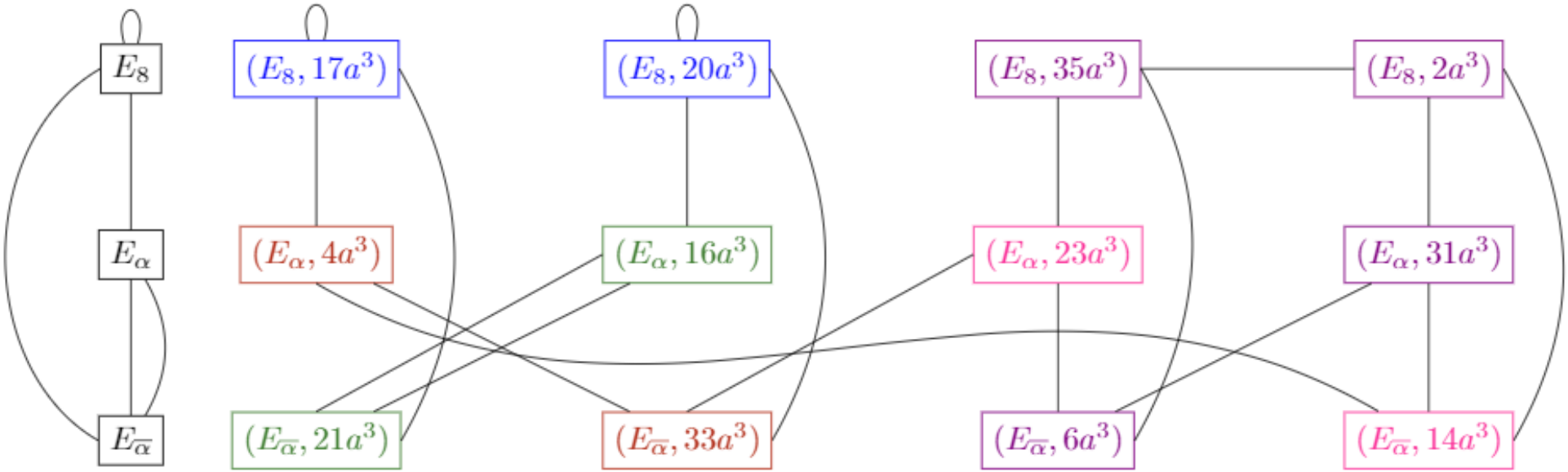
Idea: Keep track of N-torsion subgroups in the supersingular ℓ-isogeny graph

- Nodes: (E, G)
  - E: supersingular elliptic curve
  - $G \subset E(\overline{\mathbb{F}}_p)$ of (small) prime order N
- Edges: $(E, G) - (E', G')$ corresponding to an ℓ-isogeny φ:
  - $\varphi(E) = E'$
  - $\varphi(G) = G'$

Graph Properties

- $(N+1)$ nodes for every node of $\mathcal{G}_{p,\ell}$.
- $(\ell+1)$-regular, just like $\mathcal{G}_{p,\ell}$
- $\mathcal{E}_{p,\ell}^{N}$ is connected, just like $\mathcal{G}_{p,\ell}$

$p = 37, \ell = 2, N = 3$



- Black graph on the left: $\mathcal{G}_{p,\ell}$ Supersingular 2-isogeny graph for $p = 37$
- Colorful graph on the right: $\mathcal{E}^3_{37,2}$ Supersingular 2-isogeny graph for $p = 37$ with added level structure for $N = 3$.
- We can see how 2-isogenies act (differently) on 3-torsion points
- What about a quaternion analog?

The Quaternion Picture

What is the endomorphism ring of a node of $\mathcal{E}_{p,\ell}^N$?

$\mathrm{End}(E, G) := \{\alpha \in \mathrm{End}(E) : \alpha(G) \subseteq G\}$

Theorem (Arpin)

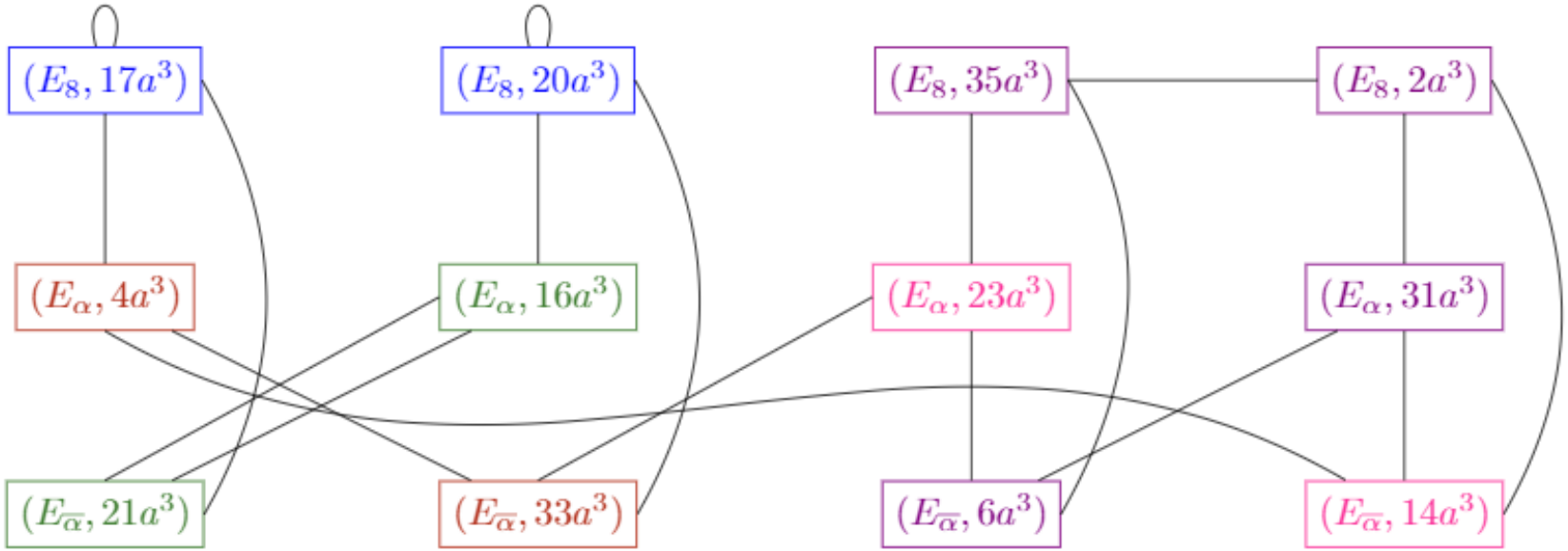
$\mathrm{End}(E, G)$ is isomorphic to an Eichler order of level $|G|$ of $B_{p,\infty}$.

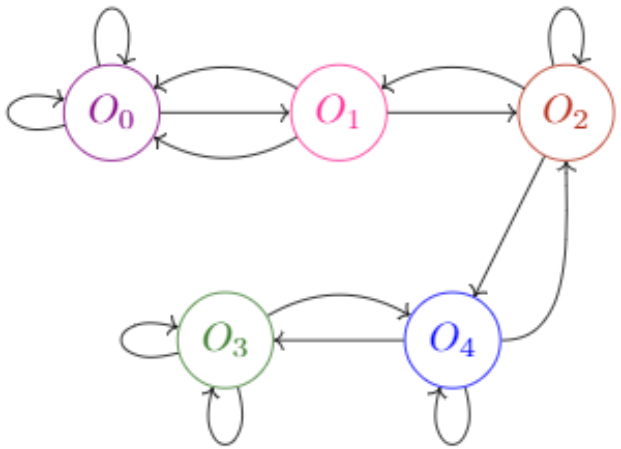
Theorem (Arpin)

Given a pair $(E, G) \in \mathcal{E}_{p,\ell}^N$, there is an Eichler order $\mathcal{O}$ of level N in $B_{p,\infty}$ such that $\mathrm{End}(E, G) \cong \mathcal{O}$. This association is either 4-1, 2-1, or 1-1, depending on the size of the two-sided ideal class group of $\mathcal{O}$.*

*Curves with extra automorphisms ($j = 0, 1728$) may not conform.

$p = 37$, $N = 3$, $\ell = 2$


$(E_8, 17a^3)$
$(E_8, 20a^3)$
$(E_8, 35a^3)$
$(E_8, 2a^3)$
$(E_\alpha, 4a^3)$
$(E_\alpha, 16a^3)$
$(E_\alpha, 23a^3)$
$(E_\alpha, 31a^3)$
$(E_{\overline{\alpha}}, 21a^3)$
$(E_{\overline{\alpha}}, 33a^3)$
$(E_{\overline{\alpha}}, 6a^3)$
$(E_{\overline{\alpha}}, 14a^3)$


O_0
O_1
O_2
O_3
O_4

Summary

- The structure of $\mathcal{G}_{p,\ell}$ can be analyzed through properties of $\mathcal{E}^N_{p,\ell}$.
- The quaternion analog of supersingular elliptic curves extends to those with level structure.

Thank You !

Reference I

[Deu41] Max Deuring. “Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.”. In: **Abh. Math. Sem. Hansischen Univ.** 14 (1941), pp. 197–272.

[Sil09] Joseph H. Silverman. **The arithmetic of elliptic curves**. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6.

[Voi21] John Voight. **Quaternion algebras**. Vol. 288. Graduate Texts in Mathematics. Springer, Cham, [2021] ©2021, pp. xxiii+885. ISBN: 978-3-030-56692-0; 978-3-030-56694-4. DOI: 10.1007/978-3-030-56694-4.