https://eprint.iacr.org/2026/500
Joint work with **Thomas Decru**

Higher-dimensional isogeny graphs

and their problems

Krijn Reijnders
Ohrid Workshop 2026

KU LEUVEN

PART 1
Objects

PART 2
Morphisms

PART 3
Graphs

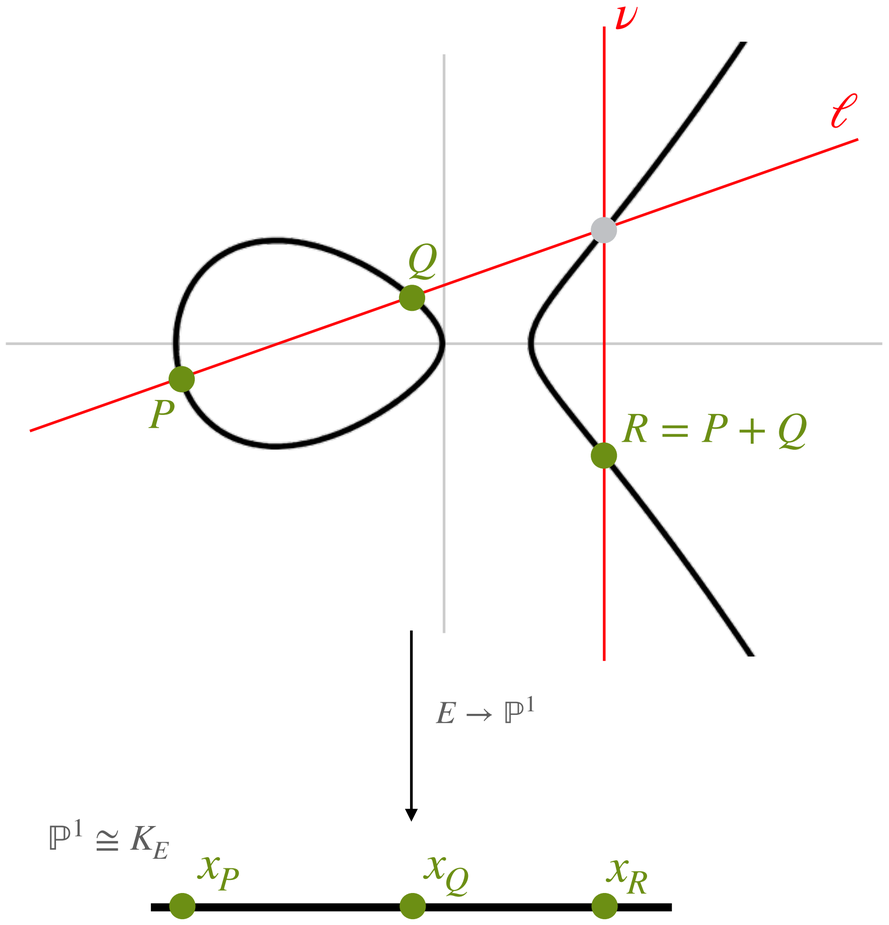
Dimension 1: Elliptic Curves

“Elliptic curves are very special.”
- K. Reijnders, 2025

PART 1

Objects

$$E : y^2 = x^3 + ax + b \qquad \cong \qquad J_E$$



1. Points on the curve $P, Q, R \in E(k)$, i.e. satisfying $y^2 = x^3 + ax + b$

2. Addition of divisors using lines from the function field $\ell, \nu \in k(E)$, essentially arithmetic on the Jacobian $J_E = \mathrm{Pic}^0(E)$

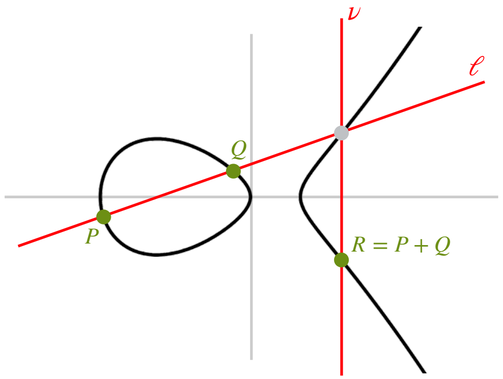
(in cryptography)

3. x-only arithmetic, i.e. working on the *Kummer line* K_E

PART 1

Objects

1. The set of points $E(k)$ of a **curve** $E : y^2 = f(x)$



2. The **Jacobian** $J_E = \mathrm{Pic}^0_k(E)$

$$J_E = \{\ (P) - (\mathcal{O})\ :\ P \in E(k)\ \}$$

3. The **Kummer line** $K_E = J_E/[-1]$

$\mathbb{P}^1 \cong K_E$

PART 1

Objects

Q

Given an elliptic curve E over $\mathbb{F}_q$,
what can we say about
$|E(\mathbb{F}_q)|$

- assume $E : y^2 = x^3 + ax + b$.
- for a random $x \in [0 \ldots q-1]$, assume $\texttt{rhs} = x^3 + ax + b$ is also random
- if this is square, we get **two** points (x, y) and $(x, -y)$
- if this is not square, we get **zero** points
- we always have the point at infinity

conclusion: we should on average get $q + 1$ points?

Example: if $q = 1073741827$, then any ell. curve has between 1073676292 and 1073807364 points.

Hasse's Theorem. For any elliptic curve E over a finite field $\mathbb{F}_q$, the size of $E(\mathbb{F}_q)$ is very strongly bounded:

$$q - 2\sqrt{q} + 1 \leq |E(\mathbb{F}_q)| \leq q + 2\sqrt{q} + 1$$

Any curve has "roughly" size q,

and $q + 1$ is in the middle of
the Hasse interval!

PART 1
Objects

Order

The map $[n] : P \mapsto P + \ldots + P$ allows us to define the **order** of $P \in E(\mathbb{F}_q)$:
the smallest positive integer n such that $[n]P = \mathcal{O}$.

We write the kernel of $[n]$ as $E[n] := \{P \in E(\overline{\mathbb{F}_q}) \mid [n]P = \mathcal{O}\}$.

Theorem 1. If E is an elliptic curve over $\mathbb{F}_q$, then

$$E(\mathbb{F}_q) \cong \mathbb{Z}_N \times \mathbb{Z}_M,$$

with $M \mid N$ and $M \mid q - 1$.

Theorem 2. If E is an elliptic curve over $\mathbb{F}_q$, then

$$E[n] = \mathbb{Z}_n \times \mathbb{Z}_n,$$

whenever n is coprime to p.

Lemma/Definition. The p-torsion is either

$$E[p] = \mathbb{Z}_p \text{ or } E[p] = \{\mathcal{O}\},$$

In the first case, we say E is **ordinary.**
In the second case, E is **supersingular.**

Q

Are the sizes or group structures different for **supersingular** curves?

A

YES!!
Every supersingular curve exists over $\mathbb{F}_{p^2}$ and has one of five orders;
$(p-1)^2,\ p^2-p+1,\ p^2+1,\ p^2+p+1,\ (p+1)^2$

A

For technical (but good) reasons, we can and do almost always use **maximal** curves of size $(p+1)^2$.
These **always** have $E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$

KU LEUVEN

Dimension 2: Abelian Surfaces

Principally Polarized

“There is nothing special about elliptic curves.”
- K. Reijnders, 2025

PART 1
Objects

facts

- A 2-dimensional abelian variety is an **abelian surface**
- Any (principally polarized) abelian surface is either a **Jacobian** or a **product** of elliptic curves, when seen over the algebraic closure

- take any smooth algebraic curve C of genus g over a field k
- **divisor**: formal sum of points $D = \sum n_P P$ with $P \in C(\bar{k})$
- degree of divisor, simply $\deg D = \sum n_p$
- define the group of divisors of degree 0 as $\mathrm{Div}^0(C)$

- functions $f \in k(C)^*$ have a divisor too!
- define $\mathrm{div} f = \sum \mathrm{ord}_P(f) P$
- define the group of (principal) divisors as $\mathrm{Princ}(C)$
- we get the g-dimensional Jacobian

$$\mathrm{Jac}(C) := \mathrm{Div}^0(C)/\mathrm{Princ}(C)$$

1

To get a dim-2 Jacobian, we need a genus-2 curve

2

Any genus-2 curve is a **hyperelliptic curve**

3

Any genus-2 **hyperell. curve** of is of the form $y^2 = f(x)$ w/ $\deg f = 5,6$ (when $p \neq 2$)

PART 1
Objects

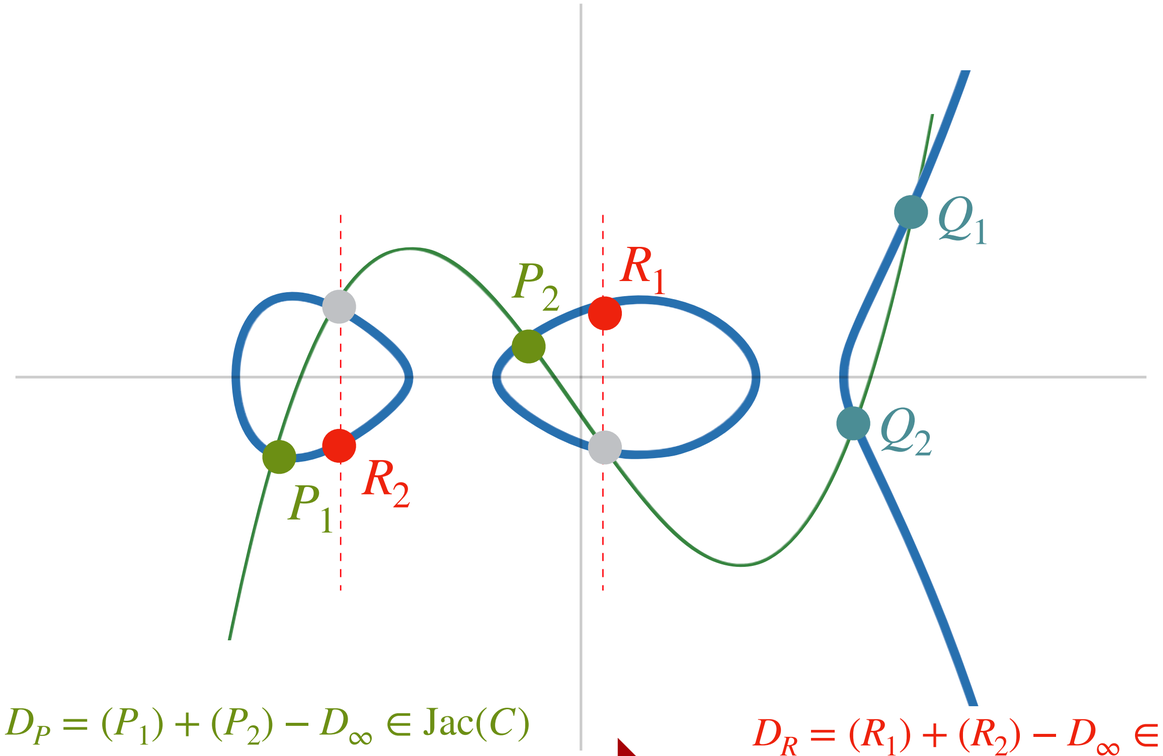
facts

- A 2-dimensional abelian variety is an **abelian surface**
- Any (principally polarized) abelian surface is either a **Jacobian** or a **product** of elliptic curves, when seen over the algebraic closure

- take any smooth algebraic curve C of genus g over a field k
- **divisor**: formal sum of points $D = \sum n_P P$ with $P \in C(\bar{k})$
- degree of divisor, simply $\deg D = \sum n_p$
- define the group of divisors of degree 0 as $\mathrm{Div}^0(C)$

- functions $f \in k(C)^*$ have a divisor too!
- define $\mathrm{div} f = \sum \mathrm{ord}_P(f) P$
- define the group of (principal) divisors as $\mathrm{Princ}(C)$
- we get the g-dimensional Jacobian

$$\mathrm{Jac}(C) := \mathrm{Div}^0(C)/\mathrm{Princ}(C)$$



$D_P = (P_1) + (P_2) - D_\infty \in \mathrm{Jac}(C)$

$D_Q = (Q_1) + (Q_2) - D_\infty \in \mathrm{Jac}(C)$

$D_R = (R_1) + (R_2) - D_\infty \in \mathrm{Jac}(C)$

$D_P + D_Q = D_R$

KU LEUVEN

PART 1

Objects

facts

- A 2-dimensional abelian variety is an **abelian surface**
- Any (principally polarized) abelian surface is either a **Jacobian** or a **product** of elliptic curves, when seen over the algebraic closure

Theorem 3. Let A be a 2-dimensional (principally polarized) abelian variety over $\mathbb{F}_q$. Then A is either

- the Jacobian J_C of a curve,
$$C : y^2 = f(x), \quad \deg f = 5,6$$
- the product of two elliptic curves

!

Jacobians always have a "**natural**" principal polarization, derived from the curve.
This does not hold **generally.**

PART 1

Objects

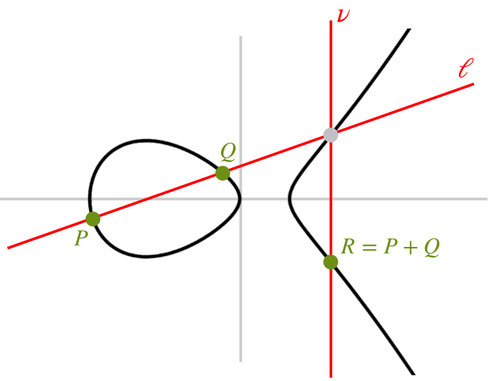
The geometric picture

1. The set of points $C(k)$ of a **curve** $C : y^2 = f(x)$

2. The **Jacobian variety** $J_C = \mathrm{Pic}^0_k(C)$

3. The **Kummer variety** $K_C = J_C/\pm$

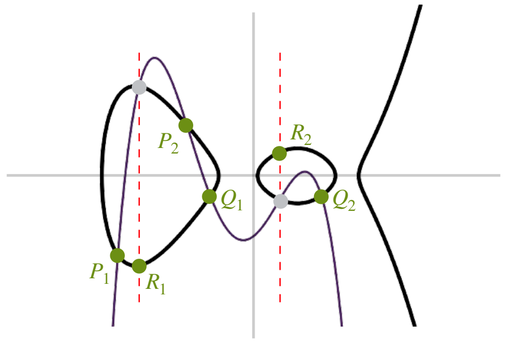
Dimension 1



$J_C = \{\ (P) - (\mathcal{O})\ :\ P \in C(k)\ \}$

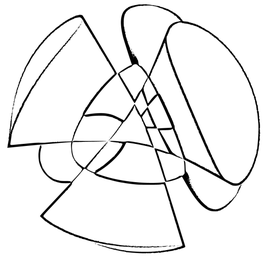
$\mathbb{P}^1 \cong K_C$

Dimension 2



$J_C = \{\ (P) + (Q) - D_\infty\ :\ P, Q \in C\ \}$

$K_C \hookrightarrow \mathbb{P}^3$



KU LEUVEN

PART 1
Objects

Some arithmetical properties of abelian varieties

Q

Given an abelian variety A over $\mathbb{F}_q$,
what can we say about $A(\mathbb{F}_q)$?

Hasse-Weil. For any abelian variety A of dimension g over a finite field $\mathbb{F}_q$, the size of $A(\mathbb{F}_q)$ is very strongly bounded:

$$(\sqrt{q}-1)^{2g} \leq |A(\mathbb{F}_q)| \leq (\sqrt{q}+1)^{2g}$$

Theorem 4. If A is an abelian variety over $\mathbb{F}_q$, then

$$A[n] = \mathbb{Z}_n^{2g},$$

whenever n is coprime to p.

Lemma/Definition. The p-torsion is

$$A[p] = \mathbb{Z}_p^r$$

where $0 \leq r \leq g$, called the p-rank.
All **supersingular** varieties have p-rank 0, but not vice versa!!

Corollary. If A is an abelian variety over $\mathbb{F}_q$, then

$$A(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \mathbb{Z}_{n_{2g}}$$

with $n_{i+1} \mid n_i$, and $n_i \mid q-1$ for $i > g$.

!

The notion of **supersingularity** gets very confusing in higher dim.
Let's **ditch** it (for this talk).

PART 1
Objects

We really want *superspecial* surfaces

mantra

superspecial surfaces
are the right dim-2 analogy to
supersingular elliptic curves
(for isogeny-based cryptography!)

facts

- Superspeciality is **stronger** than supersingularity;
  superspecial implies supersingular
- As for elliptic curves, superspecial varieties always have a **model** over $\mathbb{F}_{p^2}$
- Any **maximal** abelian surface, e.g., reaching the Hasse-Weil bound $(\sqrt{q}+1)^4 = (p+1)^4$ is automagically superspecial
- Any superspecial surface is the **twist** of a maximal surface

A

We essentially always use
maximal elliptic curves E over $\mathbb{F}_{p^2}$
which have group structure
$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$

!

We focus on
maximal abelian surfaces A over $\mathbb{F}_{p^2}$
which have group structure
$A(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$

PART 1

Objects

An abelian surface

Definition. The **Flynn embedding** is an embedding of J_C into $\mathbb{P}^{15}$ as the zero locus of a set of **72 quadratic equations** in **16 variables**.

We don't use it much in practice.

$$
\begin{aligned}
F_1 &: -a_0a_{11} + f_1a_{14}a_3 + f_3a_{10}a_5 + f_5a_3a_{10} + 2a_4a_3 \\
F_2 &: -a_0a_{10} + a_3^2 \\
F_3 &: -a_0a_{12} + a_3a_5 \\
F_4 &: -f_0f_2a_{14}^2 - f_0a_{14}a_5 - 8f_0f_6a_{12}^2 - f_3f_5a_{12}a_{10} - f_1f_6a_{13}a_{10} - f_2f_5a_{13}a_{10} - f_1f_5a_{13}a_{11} - 3f_5f_0a_{13}a_{12} \\
&\quad - f_1f_3a_{14}a_{12} - f_3f_0a_{14}a_{13} - f_0f_6a_{14}a_{10} - f_2f_4a_{14}a_{10} + a_4^2 - a_0a_{12} - 6f_0f_6a_{12}a_{15} - f_2f_6a_{10}a_{15} \\
&\quad - f_1f_6a_{11}a_{15} - f_5f_0a_{13}a_{15} - f_1f_4a_{14}a_{11} - f_2a_{12}a_5 - f_4f_0a_{13}^2 - f_0f_6a_{15}^2 - f_4f_6a_{10}^2 - f_6a_{10}a_3 \\
&\quad - f_4a_{10}a_5 - f_3f_6a_{10}a_{11} - 4f_2f_6a_{10}a_{12} - 2f_1f_6a_{11}a_{12} \\
F_5 &: -a_0a_{13} + f_1a_{14}a_5 + f_3a_{14}a_3 + f_5a_{10}a_5 + 2a_5a_4 \\
F_6 &: -a_0a_{14} + a_5^2 \\
F_7 &: -4f_0f_2a_{14}^2 - 4f_0a_{14}a_5 + a_0a_{15} - 36f_0f_6a_{12}^2 - 4f_3f_5a_{12}a_{10} - 4f_1f_6a_{13}a_{10} - 4f_2f_5a_{13}a_{10} - 12f_5f_0a_{13}a_{12} \\
&\quad - 2f_1f_3a_{14}a_{12} - 4f_3f_0a_{14}a_{13} - 4f_2f_4a_{14}a_{10} - 4f_5a_{10}a_4 - f_5^2a_{10}^2 - 24f_0f_6a_{12}a_{15} - 4f_2f_6a_{10}a_{15} - 4f_1f_6a_{11}a_{15} \\
&\quad - 4f_5f_0a_{13}a_{15} - 4f_1f_4a_{14}a_{11} + f_3^2a_{14}a_{10} - 2f_3a_{11}a_5 - 16f_1f_5a_{12}^2 - 2f_1a_{13}a_5 - 4f_2a_{12}a_5 - 4f_0f_6a_{15}^2 \\
&\quad - 4f_4f_6a_{10}^2 - 4f_6a_{10}a_3 - 4f_4a_{10}a_5 - 4f_3f_6a_{10}a_{11} - 16f_2f_6a_{10}a_{12} - 8f_1f_6a_{11}a_{12} + f_1^2a_{14}^2 - 16f_0f_4a_{14}a_{12} \\
&\quad - 4f_1f_5a_{12}a_{15} - 4f_0f_4a_{14}a_{15} \\
F_8 &: -f_1a_{14}^2 - f_3a_{14}a_{12} + 2f_4a_{13}a_{12} - f_5a_{12}^2 - 2a_4a_{14} - 2f_4a_{14}a_{11} + a_5a_{13} \\
F_9 &: -f_1a_{14}a_{12} - f_3a_{14}a_{10} - f_5a_{12}a_{10} - 2a_4a_{12} + a_5a_{11} \\
F_{10} &: 2f_4a_{14}a_{10} + 2f_5a_{12}a_{11} - 4a_5a_{12} - 2f_4a_{12}^2 - a_5a_{15} + f_1a_{14}a_{13} + f_3a_{14}a_{11} - f_5a_{13}a_{10} \\
&\quad + 2a_4a_{13} \\
F_{11} &: -f_5a_{10}^2 - f_3a_{10}a_{12} + 2f_2a_{11}a_{12} - f_1a_{12}^2 - 2a_4a_{10} - 2f_2a_{13}a_{10} + a_3a_{11} \\
F_{12} &: f_2a_{12}^2 + f_1a_{13}a_{12} - a_5a_{10} - f_1a_{14}a_{11} - f_2a_{10}a_{14} + a_3a_{12} \\
F_{13} &: f_5a_{13}a_{10} + f_4a_{14}a_{10} - a_5a_{12} - f_4a_{12}^2 - f_5a_{12}a_{11} + a_3a_{14} \\
F_{14} &: -f_1a_{14}a_{12} - f_3a_{14}a_{10} - f_5a_{12}a_{10} - 2a_4a_{12} + a_3a_{13} \\
F_{15} &: 4f_1a_{13}a_{12} - 2a_5a_{10} - 3f_1a_{14}a_{11} - a_3a_{15} - 2a_3a_{12} + f_5a_{10}a_{11} + f_3a_{10}a_{13} + 2a_4a_{11} \\
F_{16} &: -a_{14}a_{15} - 4a_{12}a_{14} + a_{13}^2 \\
F_{17} &: -a_{10}a_{14} + a_{12}^2 \\
F_{18} &: -a_{10}a_{15} - 4a_{10}a_{12} + a_{11}^2 \\
F_{19} &: -a_{11}a_{13} + 2a_{10}a_{14} + a_{12}a_{15} + 2a_{12}^2 \\
F_{20} &: -a_{12}a_{13} + a_{11}a_{14} \\
F_{21} &: -a_{11}a_{12} + a_{10}a_{13} \\
F_{22} &: -a_{10}^2f_2f_5^2 - a_{11}^2f_0f_5^2 + a_1^2 - a_0a_3 + 8f_0f_6a_4a_{11} - a_{10}^2f_3^2f_6 - f_4a_3^2 - f_0a_5^2 \\
&\quad + 4a_{10}^2f_1f_5f_6 + 4a_{10}^2f_2f_4f_6 - a_{10}a_3f_3f_5 + 4a_{10}a_3f_2f_6 + 8f_1f_6a_{10}a_4 + f_1f_5a_{10}a_5 + 4a_{11}^2f_0f_4f_6 - a_{10}a_{11}f_1f_5^2 \\
&\quad + 4a_{10}a_{11}f_0f_5f_6 + 4a_{10}a_{11}f_1f_4f_6 + 4f_0f_5a_{12}a_4 + 2a_{12}a_{10}f_0f_5^2 + 6a_{12}a_{10}f_1f_3f_6 + 8f_0f_3f_6a_{12}a_{11} + 4a_{14}a_{10}f_0f_2f_6 + 2a_{14}a_{10}f \\
&\quad + 3a_{14}a_{10}f_1^2f_6 + 4f_0f_1f_6a_{14}a_{11} + 2f_0f_1f_5a_{14}a_{12} \\
F_{23} &: a_1a_2 - a_0a_4 + 3a_{13}a_{10}f_0f_5^2 + a_{13}a_{10}f_1f_3f_6 + 2a_{10}^2f_2f_5f_6 + f_3f_6a_{10}a_3 + 4f_2f_6a_{10}a_4 + a_{10}a_5f_2f_5 \\
&\quad + 5a_{10}a_5f_1f_6 + 4f_1f_6a_{12}a_3 + 20f_0f_6a_{12}a_4 + 10f_0f_5f_6a_{10}a_{12} + 2a_{12}^2f_1f_3f_5 + 28a_{12}^2f_0f_3f_6 + 4a_{12}^2f_1f_2f_6 + 3f_1f_5a_{12}a_4 \\
&\quad + 2a_{12}a_{10}f_1f_4f_6 + 2a_{12}a_{10}f_2f_3f_6 + a_{12}a_{10}f_1f_5^2 - 4f_0f_5^2a_{12}a_{11} - 4f_0f_6f_4a_{12}a_{11} + 2f_0f_4a_{13}a_5 + 8a_{10}a_{13}f_0f_4f_6 + 8a_{13}a_{12}f_0f_2 \\
&\quad + 3a_{13}a_{12}f_0f_3f_5 - a_{13}a_{12}f_1^2f_6 + 9a_{14}a_3f_0f_5 + a_{14}a_3f_1f_4 + f_0f_3a_{14}a_5 - 2f_1f_6f_2a_{14}a_{10} - 8f_0f_6f_3a_{14}a_{10} - 2f_0f_5f_3a_{14}a_{11} \\
&\quad - 4f_0f_6f_2a_{14}a_{11} + 10f_1f_6f_0a_{14}a_{12} + 2a_{14}a_{12}f_0f_2f_5 + a_{14}a_{12}f_1^2f_5 + 2f_1f_6a_3a_{15} + 4f_0f_6a_4a_{15} + 2f_0f_5a_5a_{15} + 2f_0f_5f_6a_{10}a_{15}
\end{aligned}
$$

PART 1
Objects

The arithmetical picture

	Dimension 1	Dimension 2
The variety	The elliptic curve $E : y^2 = x^3 + ax + b$	The Jacobian J_C of $C : y^2 = f(x), \quad \deg f = 5,6$ or $E_1 \times E_2$ for ell. curves
The n-torsion	$E[n] = \mathbb{Z}_n^2$ (n coprime to p)	$A[n] = \mathbb{Z}_n^4$ (n coprime to p)
The p-torsion	$E[p] = \begin{cases} \mathbb{Z}, \text{ if ordinary} \\ \mathcal{O}, \text{ if supersingular} \end{cases}$	$A[p] = \begin{cases} \mathbb{Z}^2, \text{ if ordinary} \\ \mathbb{Z}, \text{ if non-ordinary} \\ \mathcal{O}, \text{ if supersingular} \end{cases}$
The maximal variety (superspecial, used in isogeny-based crypto)	$E(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$	$A(\mathbb{F}_{p^2}) \cong \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1} \times \mathbb{Z}_{p+1}$

PART 1
Objects

PART 2
Morphisms

PART 3
Graphs

KU LEUVEN

Dimension 1: ℓ-isogenies

PART 2

Morphisms

$a, b \in \mathbb{F}_q$

$E : y^2 = x^3 + ax + b$

$a', b' \in \mathbb{F}_q$

$E' : y^2 = x^3 + a'x + b'$

$$\varphi : E \to E'$$

Definition 1 (sketch). An *isogeny* is a "nice" map between elliptic curves.

(it preserves the group structures we have on E and E')

It has a *degree* $\deg \varphi$, which measures its complexity.

It is given by rational functions: a point $(x, y) \in E$ is mapped to

$$\left(\, f_1(x)/f_2(x) \, , \, g_1(x,y)/g_2(x,y) \, \right)$$

PART 2

Morphisms

$$\varphi : E \to E'$$

Definition 2. The **kernel** $\ker \varphi$ are the points $P \in E$ that are mapped to infinity $\mathcal{O}' \in E'$. For all isogenies we will care about, the **degree** $\deg \varphi$ is equal to the size of $\ker \varphi$.

$$\ker \varphi := \{\ P \in E \ \mid\ \varphi(P) = \mathcal{O}'\ \}.$$

The kernel is **cyclic** if

$$\ker \varphi = \{\ K, [2]K, [3]K, \ \ldots, [n]K\ \}$$

for some point $K \in E[n]$.

Definition 3. An ℓ**-isogeny** is an isogeny $\varphi : E \to E'$ of degree ℓ.

If ℓ is a prime different from p, then an ℓ-isogeny is necessarily cyclic.

Hence, $\ker \varphi = \langle K \rangle$ for some $K \in E[\ell]$.

PART 2

Morphisms

toy example 1

over $\mathbb{F}_{11}$

$$E : y^2 = x^3 + x \xrightarrow{\varphi} E' : y^2 = x^3 + 5$$

$$(x, y) \mapsto \left(\frac{x^3 + x^2 + x + 2}{(x-5)^2}, \frac{y(x^3 - 4x^2 + 2)}{(x-5)^3} \right)$$

Can check

- this is a group homomorphism: $\varphi(\mathcal{O}) = \mathcal{O}'$ and $\varphi(P + Q) = \varphi(P) + \varphi(Q)$
- kernel: $\varphi(P) = \mathcal{O}'$ when $P = \mathcal{O}$ or $x_P = 5$, so $P = (5,3)$ and $P = (5, -3)$
- φ is of degree 3 and we can say E and E' are 3-isogenous

toy example 2

over $\mathbb{F}_q$

$$E \xrightarrow{\pi} E$$

$$(x, y) \mapsto (x^q, y^q)$$

- this is a group homomorphism: $\pi(\mathcal{O}) = \mathcal{O}$ and $\pi(P + Q) = \pi(P) + \pi(Q)$
- it doesn't have a kernel (as we can see it…)
- **inseperable** isogeny: degree q

toy example 3

over k

$$E \xrightarrow{[n]} E$$

$$P \mapsto [n]P = P + \ldots + P$$

- again: $[n]\mathcal{O} = \mathcal{O}$ and $[n](P + Q) = [n]P + [n]Q$
- we already know the kernel is $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$
- so degree is n^2

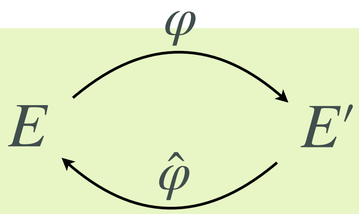
PART 2
Morphisms

GREAT THINGS ABOUT ISOGENIES

1

THE DUAL

$\hat{\varphi}$



If you have an ℓ-isogeny $\varphi : E \to E'$,
there exists a **dual** ℓ-isogeny $\hat{\varphi} : E' \to E$
such that $\hat{\varphi} \circ \varphi : E \to E$ is just $[\ell]$

2

HONDA-TATE THEOREM

$$|E(\mathbb{F}_q)| = |E'(\mathbb{F}_q)|$$
$$\Leftrightarrow$$
$$E \heartsuit E'$$

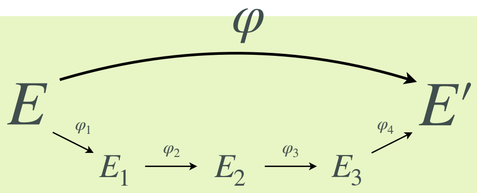
If E and E' have the same number of points over $\mathbb{F}_q$,
then they are isogenous over $\mathbb{F}_q$

!

All maximal curves
are isogenous over $\mathbb{F}_{p^2}$!

3

FACTORING ISOGENIES



An isogeny φ of degree $d = \prod p_i^{e_i}$
factors as $\varphi = \varphi_n \circ \ldots \circ \varphi_1$,
the composition of e_i isogenies of degree p_i.

KU LEUVEN

PART 2

Morphisms

Definition 3. An ℓ-isogeny is an isogeny $\varphi : E \to E'$ of degree ℓ.

If ℓ is a prime different from p, then an ℓ-isogeny is necessarily cyclic.

Hence, $\ker \varphi = \langle K \rangle$ for some $K \in E[\ell]$.

Q

For E over $\mathbb{F}_q$,
how many ℓ-isogenies
does E have?

A

$$\ell + 1$$

- we know $E[\ell] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$
- let $\langle P, Q \rangle = E[\ell]$
- we get ℓ isogenies with
  $$\ker \phi = \langle P + aQ \rangle$$
  with $a \in [1, \ldots, \ell]$
- and 1 isogeny w/ $\ker \phi = \langle Q \rangle$

PART 2

Morphisms

Definition 3. An ℓ-isogeny is an isogeny $\varphi : E \to E'$ of degree ℓ.

If ℓ is a prime different from p, then an ℓ-isogeny is necessarily cyclic.

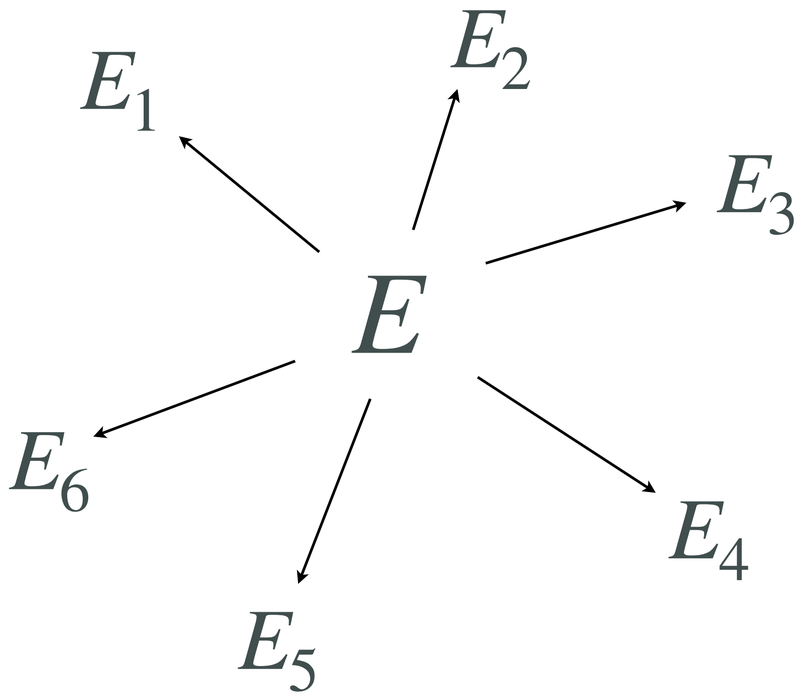
Hence, $\ker \varphi = \langle K \rangle$ for some $K \in E[\ell]$.

A

$$\ell + 1$$

- we know $E[\ell] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$
- let $\langle P, Q \rangle = E[\ell]$
- we get ℓ isogenies with
  $$\ker \phi = \langle P + aQ \rangle$$
  with $a \in [1, \ldots, \ell]$
- and 1 isogeny w/ $\ker \phi = \langle Q \rangle$

$\ell = 5$

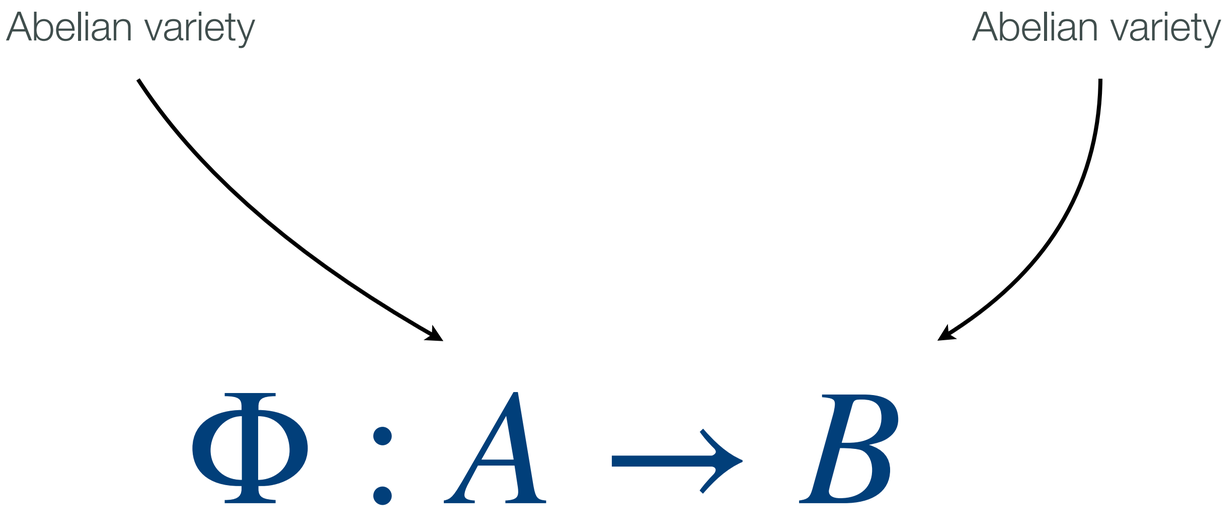


Dimension 2: (ℓ, ℓ)-isogenies

“Lasciate ogne speranza, voi ch’intrate.”
- D. Alighieri, 1321

PART 2

Morphisms



Definition 4 (sketch). A (higher-dimensional) **isogeny** is a “nice” map between abelian varieties.

- Zero is mapped to zero, i.e., $\Phi : \mathbf{0}_A \mapsto \mathbf{0}_B$,
- The map Φ is surjective
- We have a finite kernel $|\Phi^{-1}(\mathbf{0}_B)| < \infty$

PART 2

Morphisms

The right generalisation of ℓ-isogenies to dimension 2 are (ℓ, ℓ)-isogenies:

$$\Phi : A \to B \qquad \ker \Phi \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

DUAL

For every abelian variety A,
there exists a dual variety $\hat{A}$.

But in *practice,* we need a (principal polarization) to even write down **coordinates** of the varieties, or to "compute" on them!

- to compute **pairings**
- to compute **isogenies**

For any elliptic curve
$E \cong \hat{E}$
so we never talk
about polarizations

PRINCIPAL POLARIZATION

A principal polarization λ
is a "special" isomorphism
$\lambda : A \to \hat{A}$.

Claim: cryptographers essentially only work with principally polarized abelian varieties.

Mantra: A principal polarization on A gives you a model for A so that you can compute on it.

An abelian variety A,
can have many princ. pol.,
so think of a p.p.a.v. as
(A, λ)

PART 2

Morphisms

The right generalisation of ℓ-isogenies to dimension 2 are (ℓ, ℓ)-isogenies:

$$\Phi : A \to B \qquad \ker \Phi \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

For any elliptic curve
$E \cong \hat{E}$
so we never talk
about polarizations

An abelian variety A,
can have many princ. pol.,
so think of a p.p.a.v. as
(A, λ)

PART 2

Morphisms

The right generalisation of ℓ-isogenies to dimension 2 are (ℓ, ℓ)-isogenies:

$$\Phi : A \to B \qquad \ker \Phi \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

For any elliptic curve
$E \cong \hat{E}$
so we never talk
about polarizations

For a product of ell. curves
$E_1 \times E_2$,
we naturally get a p.p
from each E_i

An abelian variety A,
can have many princ. pol.,
so think of a p.p.a.v. as
(A, λ)

For a Jacobian J_C,
we naturally get a p.p.
from C

!

We have a problem when we go to
pairings

PART 2
Morphisms

The Weil pairing gives a symplectic structure to $A[n]$

Definition 5. The Weil pairing for n coprime to p

$$e_n : E[n] \times E[n] \to \mu_n$$

is a bilinear, alternating non-degenerate pairing, taking values in n-th roots of unity.

Theorem 5. The Weil pairing is superhandy when you want to find a basis for $E[n]$ because:

$e_n(P, Q) = 1$ only if $Q = [k]P$

and

$e_n(P, Q)$ has order n only if (P, Q) is basis for $E[n]$

However, on abelian varieties…

$$e_n : A[n] \times \hat{A}[n] \to \mu_n$$

We need a principal polarization $\lambda : A \xrightarrow{\sim} \hat{A}$ to get

$$e_n^\lambda : A[n] \times A[n]$$

This makes $A[n]$ into a **symplectic space**: we can find a basis $(P_1, \ldots, P_g, Q_1 \ldots, Q_g)$ such that

- the Weil pairing e_n^λ is trivial on $\langle P_1, \ldots, P_g \rangle$,
- also trivial on $\langle Q_1, \ldots, Q_g \rangle$
- and for all i, we have $e_n^\lambda(P_i, Q_i)$ of order n

!

This symplectic structure on $A[n]$ is **crucial** to everything we do on p.p.a.v.'s but fully **hidden** on ell. curves!

!

An isogeny $(A, \lambda) \to (B, \lambda')$ that respects the polarization **must** have a kernel $K \subset A[n]$ that is **maximally isotropic**

e_n^λ is trivial on K

there is no larger isotropic $K \subset K' \subset A[n]$

PART 2

Morphisms

The Weil pairing gives a symplectic structure to $A[n]$

!

This symplectic structure on $A[n]$
is **crucial** to everything we do
on p.p.a.v.'s
but fully **hidden** on ell. curves!

!

An isogeny $(A, \lambda) \to (B, \lambda')$
that respects the polarization
must have a kernel $K \subset A[n]$
that is **maximally isotropic**

e_n^λ is trivial on K

there is no larger isotropic
$K \subset K' \subset A[n]$

back to very concrete things

Dim 2: (principally polarized) abelian surface is a **Jacobian** J,

Let's look at **simplest** non-trivial isogenies: $(2,2)$-isogenies.

Central object:

$$J[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

which is now naturally equipped with a symplectic structure
thanks to the Weil pairing $e_2 : J[2] \times J[2] \to \{-1,1\}$

In general, we can take **35** subgroups $K \subset J[2]$ such that

$$K = \langle P, Q \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

but only **15** of these subgroups are actually isotropic!

PART 2
Morphisms

The Weil pairing gives a symplectic structure to $A[n]$

back to very concrete things

Dim 2: (principally polarized) abelian surface is a **Jacobian** J,

Let's look at **simplest** non-trivial isogenies: $(2,2)$-isogenies.

Central object:

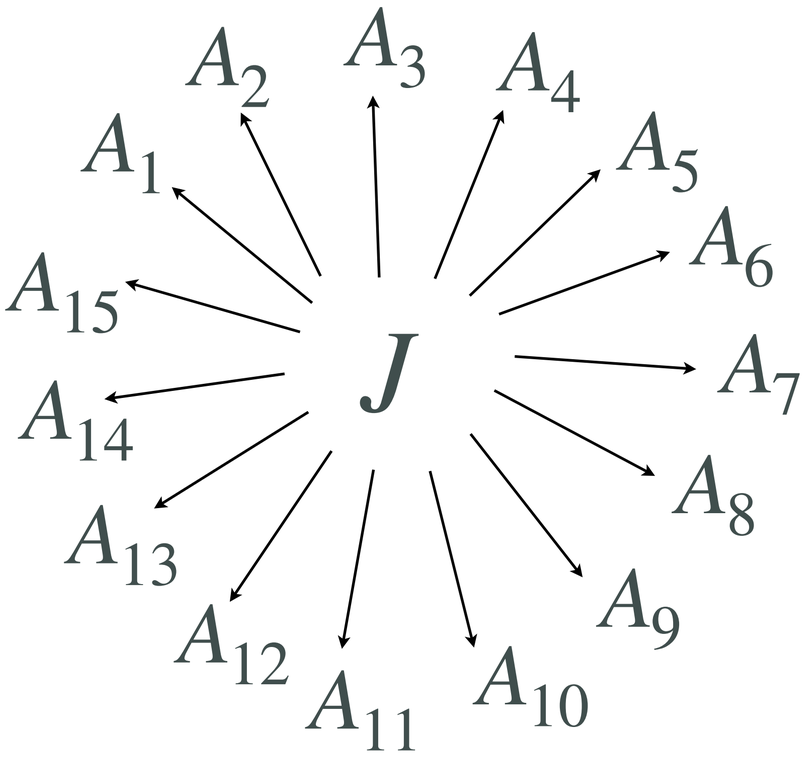
$$J[2] \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

which is now naturally equipped with a symplectic structure thanks to the Weil pairing $e_2 : J[2] \times J[2] \to \{-1,1\}$

In general, we can take **35** subgroups $K \subset J[2]$ such that

$$K = \langle P, Q \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

but only **15** of these subgroups are actually isotropic!



PART 2

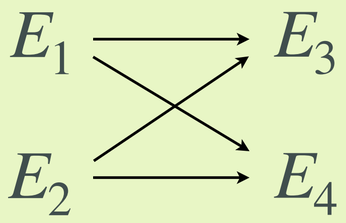
Morphisms

Even the “nice” (ℓ, ℓ)-isogenies are kinda funky…

What are the domains and codomains of an (ℓ, ℓ)-isogeny?

$$J \longrightarrow A$$

1. An isogeny $\Phi : J \to J$ is called **generic isogeny**
2. An isogeny $\Phi : J \to E_1 \times E_2$ is called a **splitting isogeny**
3. An isogeny $\Phi : E_1 \times E_2 \to J$ is called a **gluing isogeny**
4. An isogeny $\Phi : E_1 \times E_2 \to E_3 \times E_4$ is called a **diagonal isogeny** when its the composition of $\varphi_1 : E_1 \to E_3$ and $\varphi_2 : E_2 \to E_4$
5. An isogeny $\Phi : E_1 \times E_2 \to E_3 \times E_4$ associated to a **Kani diagram**

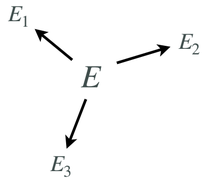
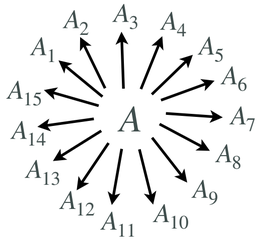


which induces a matrix of isogenies

$$\begin{pmatrix} \varphi_{1,3} & \varphi_{2,3} \\ \varphi_{1,4} & \varphi_{2,4} \end{pmatrix} : E_1 \times E_2 \to E_3 \times E_4$$

PART 2
Morphisms

Comparison of isogenies

	Dimension 1	Dimension 2
The torsion	$E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$	$A[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n \times \mathbb{Z}_n$
The kernel	Kernel of (sep.) ℓ-isogeny of form $\ker \varphi = \langle K \rangle \cong \mathbb{Z}_\ell$ (always max. isotropic)	Kernel of (sep.) (ℓ, ℓ)-isogeny of form $\ker \varphi = \langle K_1, K_2 \rangle \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ and we must have $e_\ell(K_1, K_2) = 1$.
Number of isogenies	Per prime ℓ, we have $\ell + 1$ such isogenies e.g. **3** 2-isogenies	Per prime ℓ, we have $\ell^3 + \ell^2 + \ell + 1$ such isogenies e.g. **15** 2-isogenies
Looks like (for $\ell = 2$)		

PART 1
Objects

PART 2
Morphisms

PART 3
Graphs

Dimension 1: The supersingular ℓ-isogeny graph $\mathcal{G}_p(\ell)$

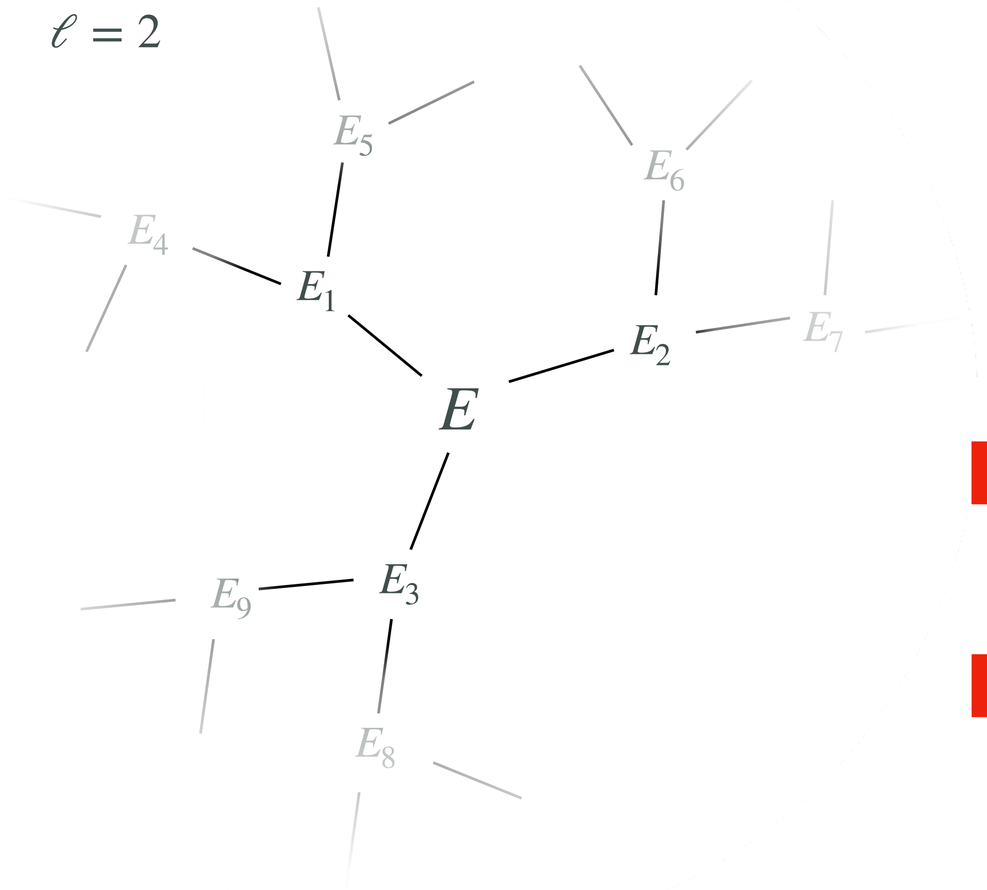
PART 3

Graphs

Definition 6. The supersingular isogeny graph $\mathcal{G}_p(\ell)$ is the graph with

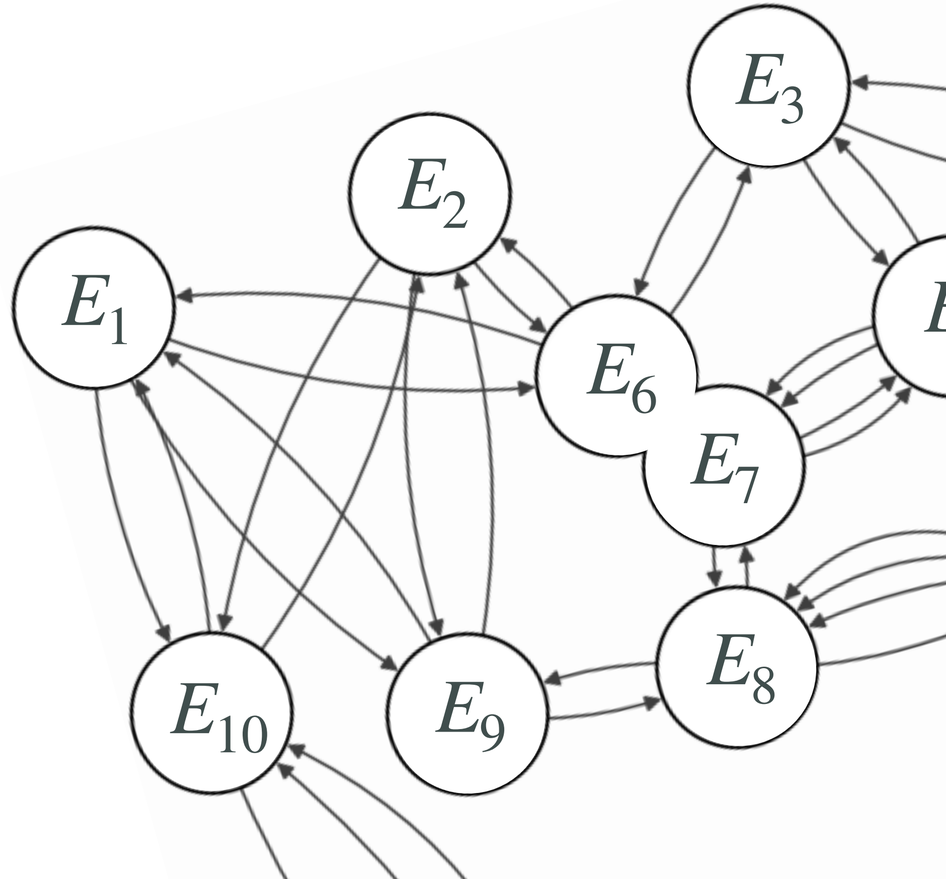
- nodes V, the set of supersingular elliptic curves over $\mathbb{F}_{p^2}$, up to isomorphism,
- edges E, the ℓ-isogenies between such nodes.

$\ell = 2$



$\mathbb{F}_{p^2}$ with $p = 131$

$\ell = 2$



1. looks $\ell + 1$ regular!

2. looks very random!

KU LEUVEN

PART 3

Graphs

Definition 6. The supersingular isogeny graph $\mathcal{G}_p(\ell)$ is the graph with

- nodes V, the set of supersingular elliptic curves over $\mathbb{F}_{p^2}$, up to isomorphism,
- edges E, the ℓ-isogenies between such nodes.

1 looks $\ell + 1$ regular!

2 looks very random!

Lemma. The curve

$$E_0 : y^2 = x^3 + 1$$

has extra **automorphisms** generated by $[-1]$ and

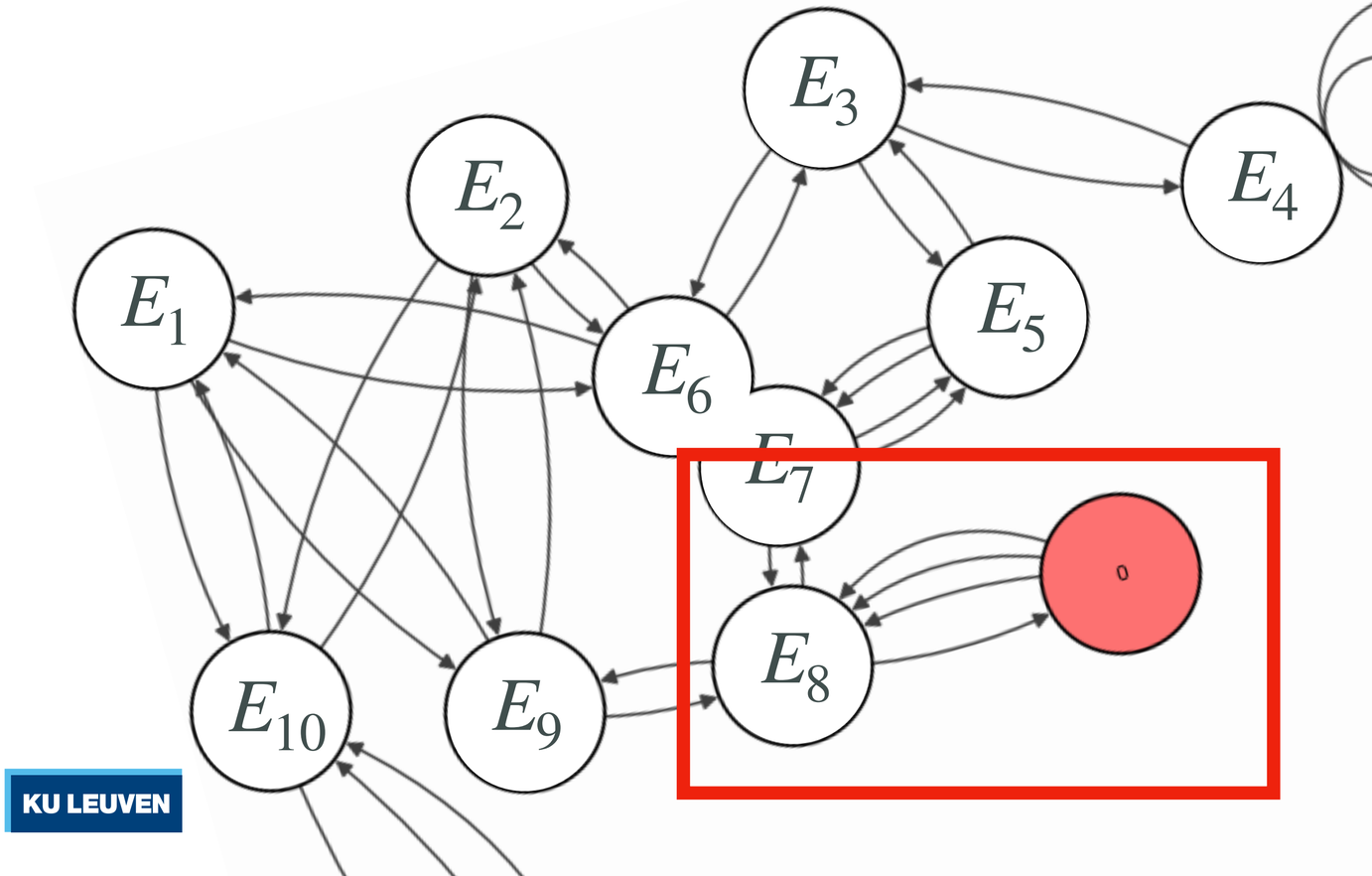
$$\Omega : (x, y) \mapsto (\omega x, y), \quad \text{with } \omega^3 = 1.$$

Write $E_0[2] = \{\mathcal{O}, P_1, P_2, P_3\}$, then the three 2-isogenies are given by kernels $\langle P_i \rangle$, but Ω permutes these kernels:

$$P_2 = \Omega(P_1), \quad P_3 = \Omega(P_2), \quad P_1 = \Omega(P_3).$$

$\mathbb{F}_{p^2}$ with $p = 131$

$\ell = 2$



KU LEUVEN

PART 3
Graphs

Why are automorphisms so annoying?

Lemma. The curve

$$E_0 : y^2 = x^3 + 1$$

has extra **automorphisms** generated by $[-1]$ and

$$\Omega : (x, y) \mapsto (\omega x, y), \quad \text{with } \omega^3 = 1.$$

Write $E_0[2] = \{\mathcal{O}, P_1, P_2, P_3\}$, then the three 2-isogenies are given by kernels $\langle P_i \rangle$, but Ω permutes these kernels:

$$P_2 = \Omega(P_1), \quad P_3 = \Omega(P_2), \quad P_1 = \Omega(P_3).$$

1 If an automorphism α maps $\ker \varphi_1 \mapsto \ker \varphi_2$, then the codomains are isomorphic!

2 $[-1] \in \mathrm{Aut}(E)$, which is boring. Only two curves have **extra** automorphisms: E_0 and $E_{1728} : y^2 = x^3 + x$

3 Only 2 curves out of $\sim \frac{p}{12}$, (if they are supersingular)

! In dimension 1, we can (and do) mostly **ignore** E_0 and E_{1728} without any impact

PART 3

Graphs

Definition 7. Ignore the nodes E_0 and E_{1728}, and define the **adjacency matrix** A of $\mathcal{G}_p(\ell)$ by

$$A_{ij} = |\text{number of edges between } E_i \text{ and } E_j\ |.$$

The size-sorted **eigenvalues** $\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n$ of A describe its expansion properties.

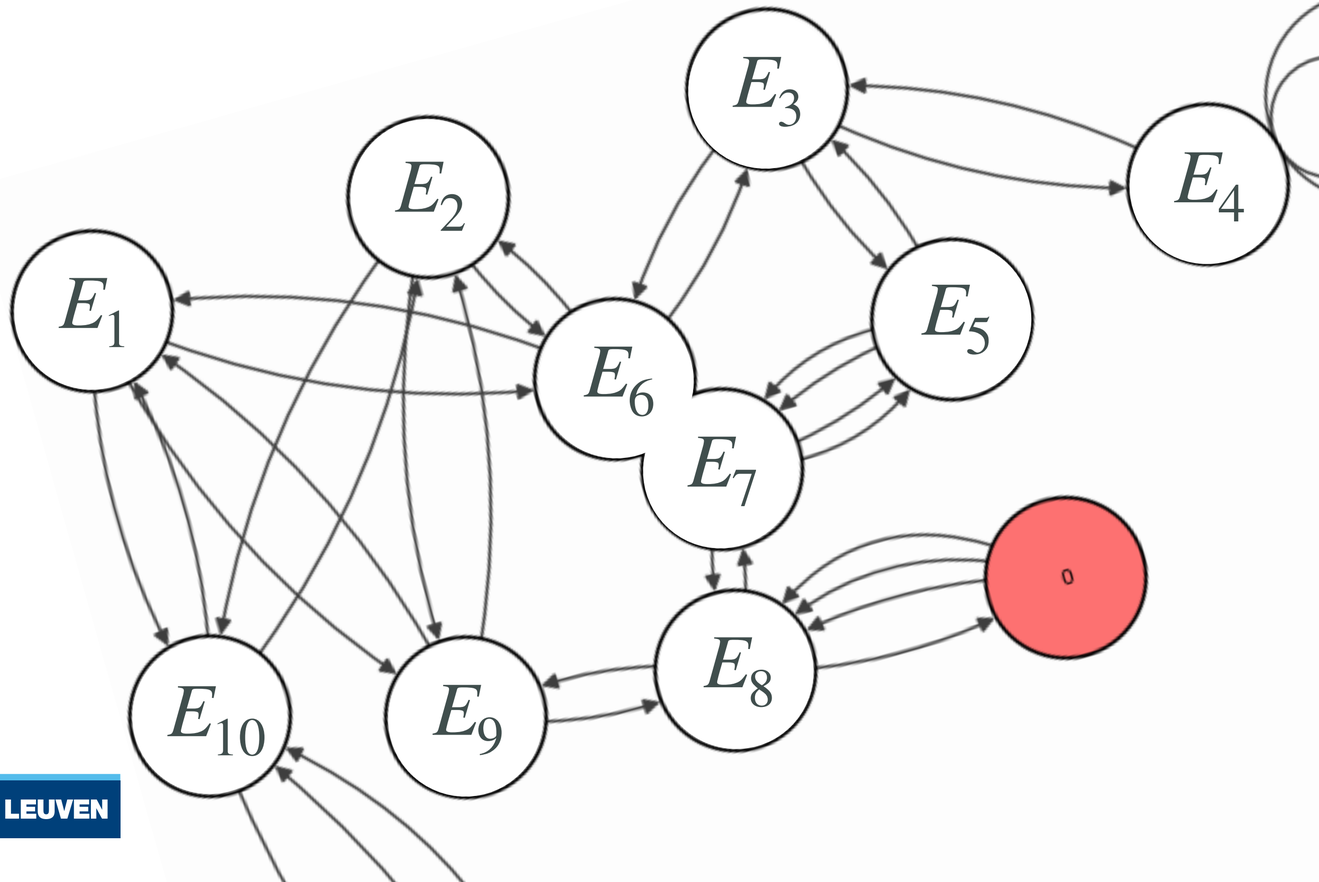
1 $\ell + 1$ regular implies $\lambda_1 = \ell + 1$

2 Ramanujan if $|\lambda_2| \leq \sqrt{\ell}$

3 $\mathcal{G}_p(\ell)$ is regular, connected, and Ramanujan!

$\mathbb{F}_{p^2}$ with $p = 131$

$\ell = 2$



KU LEUVEN

Dimension 2: The supersingular (ℓ, ℓ)-isogeny graph $\mathcal{G}_{2,p}(\ell)$

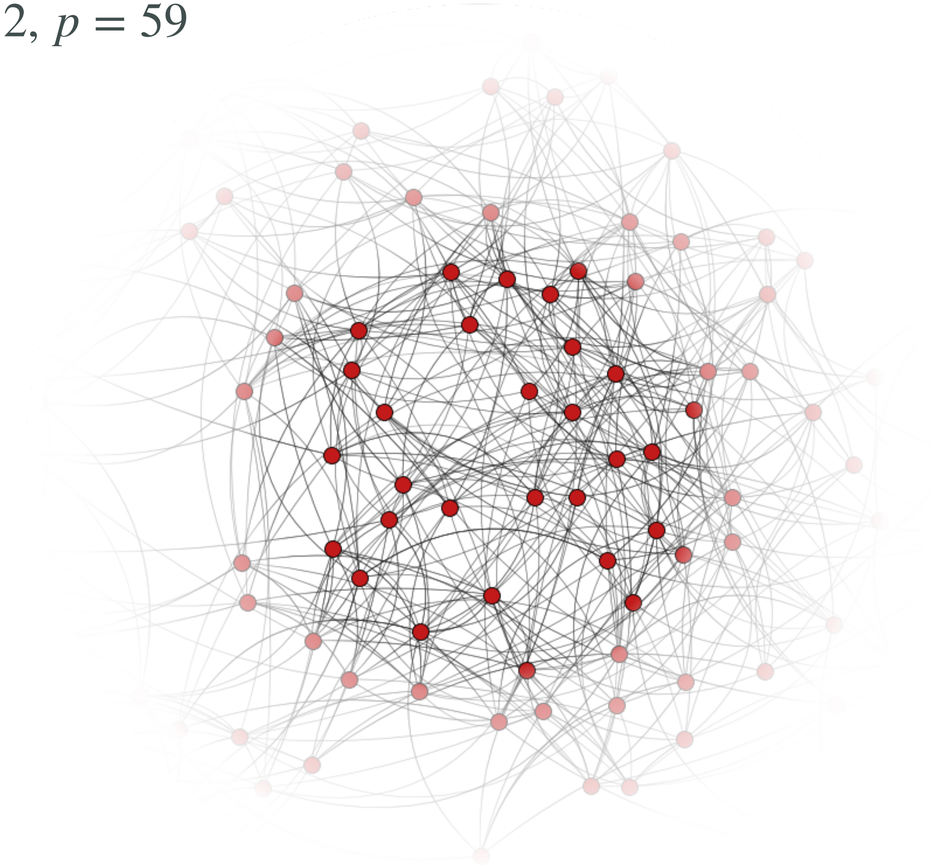
PART 3

Graphs

Definition 7. The (big) superspecial isogeny graph $\mathcal{G}_{2,p}(\ell)$ is the graph with

- nodes V, the set of superspecial principally polarized abelian surfaces over $\mathbb{F}_{p^2}$, up to isomorphism,
- edges E, the (ℓ, ℓ)-isogenies between them.

$\ell = 2,\ p = 59$



1 $\ell + 1$ regular!

2 Connected!

3 **NOT** Ramanujan!

! Bad cycles.

! Automorphisms ruin edges!

KU LEUVEN

PART 3

Graphs

$$E \xrightarrow{\varphi_1} E' \xrightarrow{\varphi_2} E''$$

In dim 1:

Lemma 8. If φ_1 and φ_2 are ℓ-isogenies, then $\varphi_2 \circ \varphi_1 : E \to E''$ is

- if φ_2 is dual of φ_1, then $\varphi_2 \circ \varphi_1 = [\ell]$, notice $\ker[\ell] = E[\ell] \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$,
- otherwise, $\varphi_2 \circ \varphi_1$ is an ℓ^2-isogeny, with $\ker(\varphi_2 \circ \varphi_1) \cong \mathbb{Z}_{\ell^2}$.

$$A \xrightarrow{\Phi_1} A' \xrightarrow{\Phi_2} A''$$

In dim 2:

Lemma 9. If Φ_1 and Φ_2 are (ℓ, ℓ)-isogenies, then $\Phi_2 \circ \Phi_1 : A \to A''$ is

- if Φ_2 is dual of Φ_1, then $\Phi_2 \circ \Phi_1 = [\ell]$, notice $\ker[\ell] = A[\ell] \cong \mathbb{Z}_\ell^4$,
- otherwise, two options:
  1. **Good extension:** we get (ℓ^2, ℓ^2)-isogeny $\Phi_2 \circ \Phi_1$, with $\ker(\Phi_2 \circ \Phi_1) \cong \mathbb{Z}_{\ell^2}^2$,
  2. **Bad extension:** we get (ℓ^2, ℓ, ℓ)-isogeny $\Phi_2 \circ \Phi_1$, with $\ker(\Phi_2 \circ \Phi_1) \cong \mathbb{Z}_{\ell^2} \times \mathbb{Z}_\ell^2$.

! Bad cycles.

! Automorphisms ruin edges!

PART 3

Graphs

$$E_1 \times E_2 \xrightarrow{\varphi_1 \times \varphi_2} E_3 \times E_4 \xrightarrow{\varphi_3 \times \hat{\varphi}_2} E_5 \times E_2$$

(ℓ, ℓ)-isogeny

(ℓ, ℓ)-isogeny

$$E_1 \times E_2 \xrightarrow{(\varphi_3 \circ \varphi_1) \times [\ell]} E_5 \times E_2$$

(ℓ^2, ℓ, ℓ)-isogeny, ker is $\mathbb{Z}_{\ell^2}$ times $E_2[\ell] \cong \mathbb{Z}_\ell^2$

! Bad cycles.

! Automorphisms ruin edges!

In dim 2:

$$A \xrightarrow{\Phi_1} A' \xrightarrow{\Phi_2} A''$$

Lemma 9. If Φ_1 and Φ_2 are (ℓ, ℓ)-isogenies, then $\Phi_2 \circ \Phi_1 : A \to A''$ is

- if Φ_2 is dual of Φ_1, then $\Phi_2 \circ \Phi_1 = [\ell]$, notice $\ker[\ell] = A[\ell] \cong \mathbb{Z}_\ell^4$,
- otherwise, two options:
  1. **Good extension:** we get (ℓ^2, ℓ^2)-isogeny $\Phi_2 \circ \Phi_1$, with $\ker(\Phi_2 \circ \Phi_1) \cong \mathbb{Z}_{\ell^2}^2$,
  2. **Bad extension:** we get (ℓ^2, ℓ, ℓ)-isogeny $\Phi_2 \circ \Phi_1$, with $\ker(\Phi_2 \circ \Phi_1) \cong \mathbb{Z}_{\ell^2} \times \mathbb{Z}_\ell^2$.

PART 3

Graphs

$$A \xrightarrow{\Phi_1} A' \xrightarrow{\Phi_2} A''$$

In dim 2:

Lemma 9. If Φ_1 and Φ_2 are (ℓ, ℓ)-isogenies, then $\Phi_2 \circ \Phi_1 : A \to A''$ is

- if Φ_2 is dual of Φ_1, then $\Phi_2 \circ \Phi_1 = [\ell]$, notice $\ker[\ell] = A[\ell] \cong \mathbb{Z}_\ell^4$,
- otherwise, two options:
  1. **Good extension:** we get (ℓ^2, ℓ^2)-isogeny $\Phi_2 \circ \Phi_1$, with $\ker(\Phi_2 \circ \Phi_1) \cong \mathbb{Z}_{\ell^2}^2$,
  2. **Bad extension:** we get (ℓ^2, ℓ, ℓ)-isogeny $\Phi_2 \circ \Phi_1$, with $\ker(\Phi_2 \circ \Phi_1) \cong \mathbb{Z}_{\ell^2} \times \mathbb{Z}_\ell^2$.

!

Bad cycles.

!

Automorphisms ruin edges!

Lemma 10. Let $\ell = 2$. If $\Phi_1 : A \to A'$ is given, then there are **8 good extensions** $\Phi : A' \to A''$ out of the 15 general $(2,2)$-isogenies. They are easy to describe:

$\Phi : A' \to A''$ is a good extension of $\Phi_1 : A \to A'$

if and only if

$\ker \Phi$ does not overlap with $\ker \hat{\Phi}_1$, the dual $\hat{\Phi}_1 : A' \to A$

!

Think of $\ker \hat{\Phi}_1$ as any max. isotropic $(2,2)$-subgroup $G \subset A'[2]$, then look at the surface as **pair** (A', G): a $(2,2)$-level structure.

KU LEUVEN

PART 3
Graphs

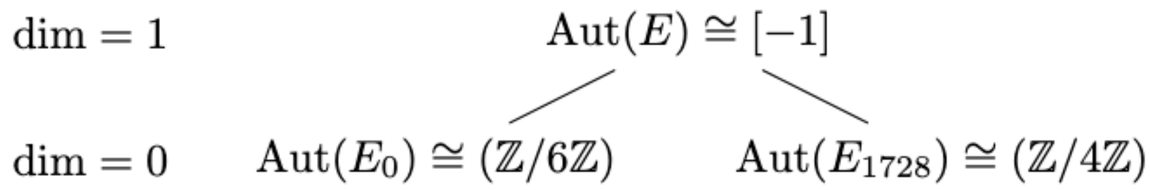
Definition 11. The superspecial (ℓ, ℓ)-isogeny digraph $\mathbf{G}_{2,p}(\ell)$ is the graph with

- nodes V, the pairs (A, G) with p.p.a.s. A and $G \subset A[\ell]$ max. isotropic, up to isomorphism
- edges E, the **good (ℓ, ℓ)-extensions**: isogenies $\Phi : A \to A'$ with $\ker \Phi \cap G = \{\mathbf{0}_A\}$.

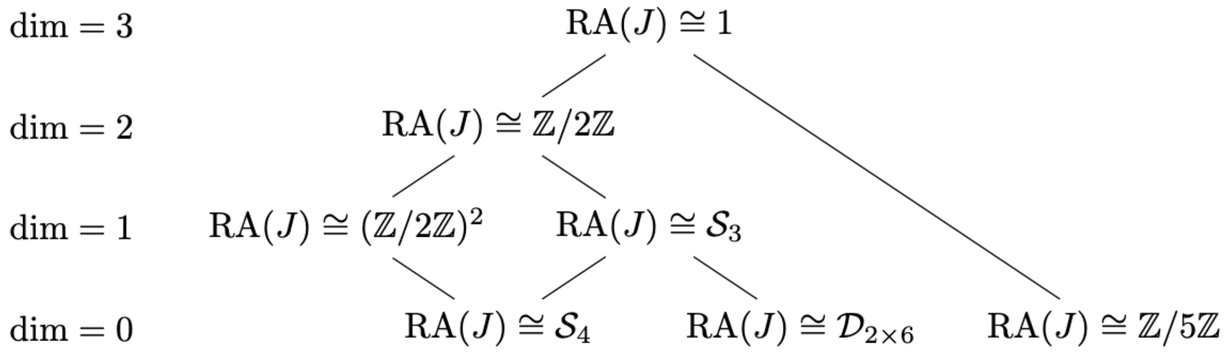
✓ Bad cycles are **removed**.

✓ Don't **ignore** autom., study carefully!

In dim 1:



In dim 2:



KU LEUVEN

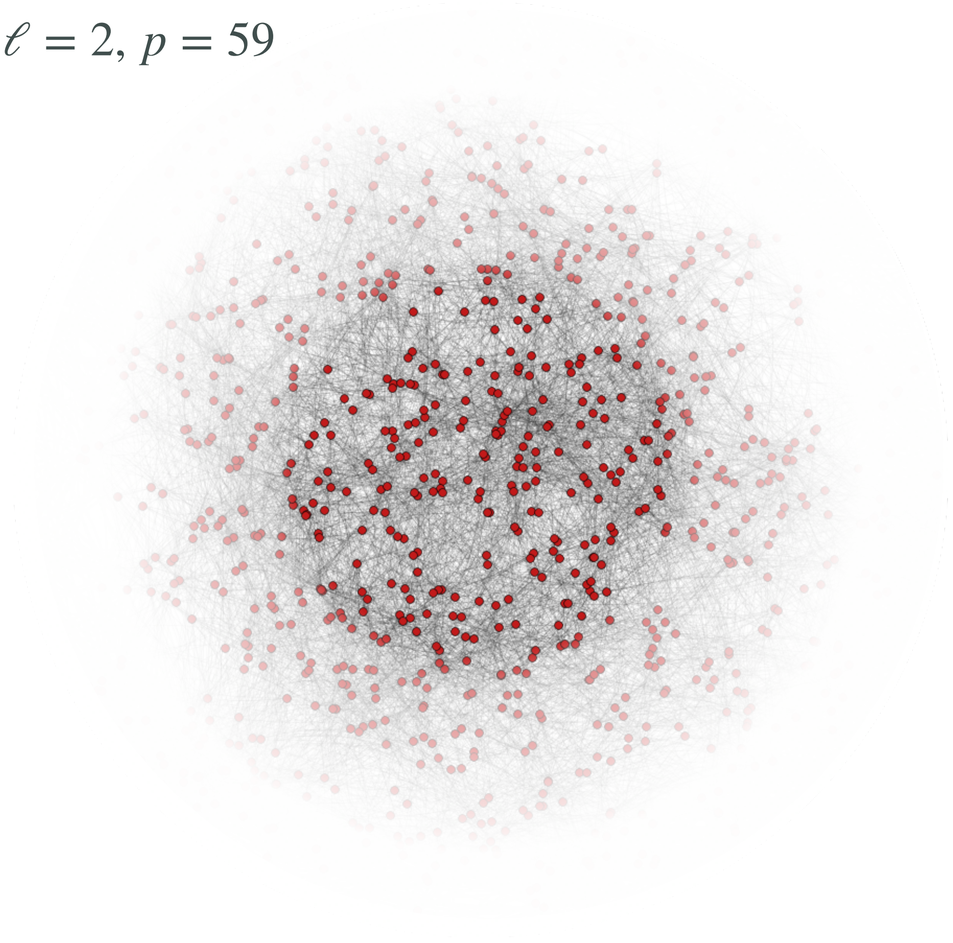
PART 3

Graphs

Definition 11. The superspecial (ℓ, ℓ)-isogeny digraph $\mathbf{G}_{2,p}(\ell)$ is the graph with

- nodes V, the pairs (A, G) with p.p.a.s. A and $G \subset A[\ell]$ max. isotropic, up to isomorphism
- edges E, the **good** (ℓ, ℓ)**-extensions**: isogenies $\Phi : A \to A'$ with $\ker \Phi \cap G = \{\mathbf{0}_A\}$.

$\ell = 2$, $p = 59$



1 Again regular!

2 Connected?

3 Ramanujan, for $\ell = 2$…

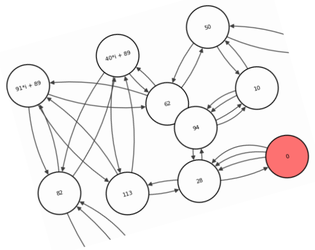
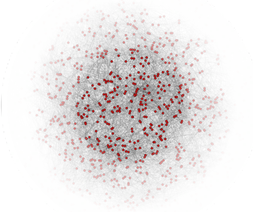
! Graph is **much** larger, harder to compute!

! Eigenvalues are very strange…

KU LEUVEN

PART 2
Morphisms

Comparison of graphs

	Dimension 1	Dimension 2
The nodes	Supersingular elliptic curves up to isomorphism	Pairs (A, G) with A superspecial ppas, and isotropic (ℓ, ℓ)-subgroup $G \subset A[\ell]$, up to isomorphism of (A, G)
The edges	ℓ-isogenies, essentially always good extensions	(ℓ, ℓ)-isogenies $\Phi : A \to A'$ with trivial overlap of $\ker \Phi$ with G
Properties	Regular, connected, and Ramanujan!	Regular! Connected? Expander properties?
Looks like (for $\ell = 2$)		

KU LEUVEN

PART 1
Objects

PART 2
Morphisms

PART 3
Graphs

KU LEUVEN

Beyond Dimension 2?

BONUS

Dim. 3 & 4

Overview of principally polarized abelian varieties in current-day isogeny-based cryptography

	General Variety	Description	Non-trivial Automorphisms	Other Varieties
Dimension 1	Elliptic curves	$E : y^2 = x^3 + ax + b$	Only 2 curves, well-understood	N/A
Dimension 2	Jacobian of hyp. ell. curve	$\mathrm{Jac}(C)$, where $C : y^2 = x^5 + ax^3 + bx^2 + cx + d$	2-dimensional space, well-understood	Products of dim. 1
Dimension 3	Jacobian of hyp. ell. curve or plane quartic	$\mathrm{Jac}(C)$, either $C : y^2 = f(x)$ with $\deg f = 7, 8$ or $C : q(x, y, z)^2 = xyzt$ with $q = ax^2 + by^2 + cz^2 + dxy + eyz + fzx$	(work in progress)	Products of dim. 1 and 2
Dimension 4	Prym variety! (no longer Jacobians!!)	Technical description in terms of double cover $\phi : C \to C'$	Don't ask me.	Jacobians of genus-4 curves, (hyp. ell. or space sextics) and products of dim 1, 2, and 3

BONUS

Dim. 3 & 4

Some mild ideas for this week

7 Connectedness of $\mathbf{G}_{g,p}(\ell)$?

1 Compute superspecial $(3,3)$-digraph?

5 Compute $(3,3,3)$-isogeny?

2 Kummer varieties in dimension 3 and 4?

6 Implement arithmetic Jacobian of smooth plane quartic?

3 Arithmetic of (simple) Prym varieties?

4 Automorphisms in dimension 4?