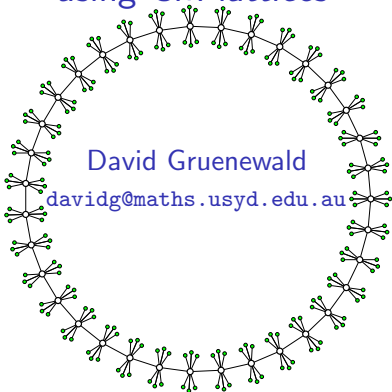


# Computing “isogeny graphs” in genus 2 using CM lattices



ECC workshop, Querétaro, México  
31st October 2012

# Motivation for computing isogenies

1. Point counting.
2. Computing CM invariants.
3. Computing modular polynomials.
4. Endomorphism ring computations.
5. Transporting discrete log problems.
6. Computing canonical lifts.

These are all interrelated, for example for computing CM invariants using:

- ▶ the  $p$ -adic method: need 3 and 6.
- ▶ the CRT method: need 1, 3 and 4.

# History of isogenies

Genus 1, we have Vélu's formulae (1971).

Genus 2, from a computational perspective we had:

- ▶ Richelot  $(2, 2)$ -isogenies
- ▶  $(3, 3)$ -isogenies (Carls-Kohel-Lubicz, Bröker-G.-Lauter)

And more recently (2010-),

- ▶  $(l^2, l^2)$ -isogenies for  $l \lesssim 40$  (Lubicz-Robert)
- ▶  $(l, l)$ -isogenies for  $l \lesssim 1000$  now possible using the Magma package AVIsogenies (Bisson-Cosset-Robert)

## Other types of isogenies:

- ▶ Explicit endomorphisms for RM families:
  - ▶  $\sqrt{2}$  in genus 2 (Bending, Gaudry, Mestre,...)
  - ▶  $\frac{1+\sqrt{5}}{2}$  in genus 2 (Kohel-Smith, Takashima,...)
  - ▶  $\zeta_{2g+1} + \zeta_{2g+1}^{-1}$  in genus  $g$  (Mestre, Smith, Tautz-Top-Verberkmoes,...)
- ▶ (2, 2, 2)-isogenies for generic genus 3 curves (Lehavi-Ritzenthaler)

## Other types of isogenies:

- ▶ Explicit endomorphisms for RM families:
  - ▶  $\sqrt{2}$  in genus 2 (Bending, Gaudry, Mestre,...)
  - ▶  $\frac{1+\sqrt{5}}{2}$  in genus 2 (Kohel-Smith, Takashima,...)
  - ▶  $\zeta_{2g+1} + \zeta_{2g+1}^{-1}$  in genus  $g$  (Mestre, Smith, Tautz-Top-Verberkmoes,...)
- ▶ (2, 2, 2)-isogenies for generic genus 3 curves (Lehavi-Ritzenthaler)
- ▶ and all the crypto ones!

## Motivation for computing isogeny graphs in genus 2

For ordinary elliptic curves over finite fields, we are in the know (Kohel, Fouquet-Morain, Miret et al., Ionica-Joux,...)

- ▶ The CM theory is completely explicit and realisable.
  - ▶ For example, isogeny cycles correspond to relations in the ideal class group. (“horizontal isogenies”)
- ▶ We have “ $l$ -isogeny volcano” graphs. In particular the endomorphism ring can be read off the graph.
- ▶ We can navigate these graphs “vertically” using Velu’s formulae, knowing the kernel of the isogeny.
- ▶ There is a path of isogenies reaching an elliptic curve whose endomorphism ring is the maximal order.

## Motivation for computing isogeny graphs in genus 2

For ordinary **genus 2 Jacobians** over finite fields, we know less (Bisson, Bröker-G.-Lauter, Ionica, Lauter-Robert)

- ▶ The CM theory is completely explicit and realisable.
  - ▶ For example, isogeny cycles correspond to relations in the ideal class group. (“horizontal isogenies”)
- ▶ We have “ $l$ -isogeny volcano” graphs. In particular the endomorphism ring can be read off the graph.
- ▶ We can navigate these graphs “vertically” using Velu-type formulae, knowing the kernel of the isogeny.
- ▶ There is a path of isogenies reaching an elliptic curve whose endomorphism ring is the maximal order.

Explicit CM in genus 2 is more complicated due to the CM field degree being 4 ( $> 2$ ) and the dimension of the moduli space of abelian surfaces has dimension 3 ( $> 1$ ), amongst other things.







Introduction/Motivation

Genus 1

Genus 2

Examples

# Lattices of elliptic curves

## isomorphisms

Let  $E$  be an elliptic curve over  $\mathbb{C}$ .

$E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ , where  $\Lambda = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z} \subset \mathbb{C}$  is a lattice.

In particular,  $\{\alpha_1, \alpha_2\} \subset \mathbb{C}$  are  $\mathbb{R}$ -linearly independent, so one of

$$(\alpha_1/\alpha_2)^{\pm 1} \in \mathbb{H}_1 := \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}.$$

Order our basis  $\langle \alpha_1, \alpha_2 \rangle$  so that  $\alpha_1/\alpha_2 \in \mathbb{H}_1$ .

The set of lattices  $\Lambda_0$  with ordered bases such that  $\mathbb{C}/\Lambda_0 \cong E(\mathbb{C})$  is given by the orbit

$$\mathbb{C}^* \backslash \Lambda / \mathrm{SL}_2(\mathbb{Z})$$

- ▶ Left action : rescale basis by  $\lambda \in \mathbb{C}^*$   
 $\lambda \cdot \langle \alpha_1, \alpha_2 \rangle = \langle \lambda \alpha_1, \lambda \alpha_2 \rangle$
- ▶ Right action: change basis by  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$   
 $\langle \alpha_1, \alpha_2 \rangle \cdot M = \langle a\alpha_1 + b\alpha_2, c\alpha_1 + d\alpha_2 \rangle$

In particular,  $\langle \tau, 1 \rangle \cdot M \cong \langle M \cdot \tau, 1 \rangle$  where

$$M \cdot \tau := \frac{a\tau + b}{c\tau + d}$$

From this, we see the usual  $\mathrm{SL}_2(\mathbb{Z})$ -action on the upper half plane.

# Lattices of elliptic curves

## isogenies

- ▶ An isogeny  $\mathbb{C}/\Lambda \rightarrow \mathbb{C}/\Lambda'$  is induced by a  $\mathbb{C}$ -linear map  $\varphi : \mathbb{C} \rightarrow \mathbb{C}$  with  $\varphi\Lambda \subseteq \Lambda'$ .
- ▶ Fixing a basis for  $\Lambda'$  we can represent this by  $R_\varphi = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{M}_2(\mathbb{Z})$  with  $ad - bc = n > 0$ .
- ▶ The degree/kernel of the isogeny is given by the elementary divisors of  $R_\varphi$ .
- ▶  $n = 1 \implies R_\varphi \in \mathrm{SL}_2(\mathbb{Z})$  is an isomorphism, as expected.

# Lattices of elliptic curves

“Isogeny graphs”

Usual definition of a  $T$ -isogeny graph:

- ▶ Vertices: isomorphism classes of elliptic curves
- ▶ Edges: isogenies of type  $T$

“Equivalent” definition:

- ▶ Vertices: lattices upto homothety
- ▶ Edges:  $T$ -isogenies between lattices

## Example: 2-isogeny graphs

For  $l$  prime, there are  $l + 1$  cyclic  $l$ -isogenies

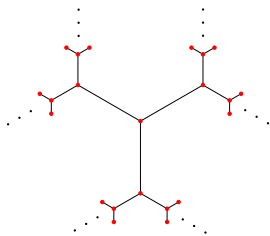
$$\mathcal{R}_l = \left\{ \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix} x \mid x \in \mathrm{SL}_2(\mathbb{Z})/\Gamma_0(l) \right\}$$

where  $\Gamma_0(l) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{l} \right\}$

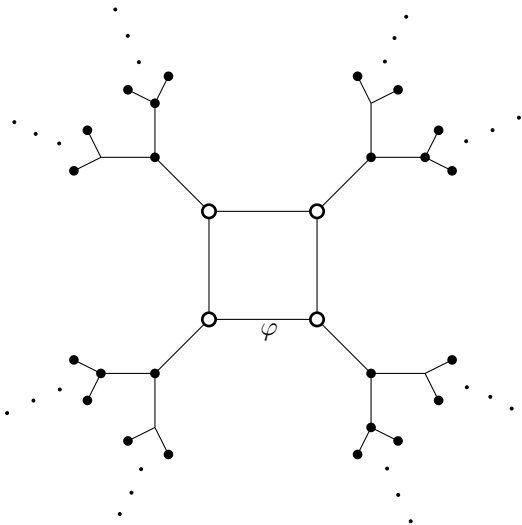
Up to isomorphism, the 2-isogenies can be represented by:

$$\mathcal{R}_2 = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\}$$

For a generic  $\tau \in \mathbb{H}_1$  (the case where  $\mathrm{End}(\langle\tau, 1\rangle) \cong \mathbb{Z}$ ) the isogeny graph is a 3-ary tree



For a CM point  $\tau \in \mathbb{H}_1$  (the case where  $\text{End}(\langle \tau, 1 \rangle) \cong \mathcal{O}$  is an order in  $\mathbb{Q}(\sqrt{-D})$ ) the isogeny graph is determined by  $\text{Pic}(\mathcal{O})$



$$\ker \varphi = \mathfrak{a}, [\mathfrak{a}^4] = [\mathcal{O}] \in \text{Pic}(\mathcal{O})$$



Introduction/Motivation

Genus 1

Genus 2

Examples

# Lattices of abelian surfaces

## isomorphisms

Let  $A$  be a principally polarized (PP) abelian surface over  $\mathbb{C}$ .

$$A(\mathbb{C}) \cong \mathbb{C}^2/\Lambda, \text{ where } \Lambda \cong \mathbb{Z}^4 \text{ is a PP lattice}$$

Such a lattice comes equipped with a symplectic basis (wrt the polarization). Using this basis we can then write  $\Lambda = \Pi\mathbb{Z}^4$  where  $\Pi = \langle \Pi_1 \ \Pi_2 \rangle \in \text{Mat}(2 \times 4, \mathbb{C})$  called the **period matrix**. This matrix satisfies the *Riemann relations*:

$$\Pi_2 {}^t \Pi_1 - \Pi_1 {}^t \Pi_2 = 0 \quad (\text{RR1})$$

$$i(\Pi_2 {}^t \overline{\Pi_1} - \Pi_1 {}^t \overline{\Pi_2}) > 0 \quad (\text{RR2})$$

The set of PP lattices  $\Lambda_0$  for which  $\mathbb{C}/\Lambda_0 \cong A(\mathbb{C})$  as PPAS's is given by the orbit

$$\mathrm{GL}_2(\mathbb{C}) \backslash \Lambda / \mathrm{Sp}_4(\mathbb{Z})$$

- ▶ Left action :  $\lambda \in \mathrm{GL}_2(\mathbb{C})$  sends  $\Pi$  to  $\lambda\Pi$
- ▶ Right action:  $M \in \mathrm{Sp}_4(\mathbb{Z})$  sends  $\Pi$  to  $\Pi {}^tM$

(RR  $\Rightarrow$ ) each orbit has a representative of the form  $\langle \tau \ I \rangle$  where

$$\tau \in \mathbb{H}_2 := \{ Z \in \mathbb{M}_2(\mathbb{C}) \mid {}^tZ = Z \text{ and } \mathrm{Im} Z > 0 \}$$

From this we derive the action of  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{Z})$  on  $\tau \in \mathbb{H}_2$ :

$$M \cdot \tau := (a\tau + b)(c\tau + d)^{-1}$$

# Lattices of abelian surfaces

## Isogenies

Let  $A = (\mathbb{C}^2/\Lambda, \chi)$  be a polarized abelian surface over  $\mathbb{C}$ .

- ▶ An isogeny  $\varphi : \mathbb{C}^2/\Lambda \rightarrow \mathbb{C}^2/\Lambda'$  induces a  $\mathbb{C}$ -linear map  $\varphi : \mathbb{C}^2 \rightarrow \mathbb{C}^2$  with  $\varphi\Lambda \subseteq \Lambda'$ .
- ▶ Fixing a basis of  $\Lambda'$  we can represent this by  $R_\varphi \in \mathbb{M}_4(\mathbb{Z})$ , with  $\deg \varphi = \det R_\varphi = n > 0$ .

In fact,

$$\varphi : (A, \chi) \rightarrow C/\Lambda' = (A', \chi')$$

is an isogeny of PAS's, but **not** necessarily polarization preserving.  
(In general  $\chi \neq \varphi^*\chi'$ )

## $(l, l)$ -isogenies

- ▶ Isogenies  $\varphi : A \rightarrow A'$  for which  $\ker \varphi \cong (\mathbb{Z}/l\mathbb{Z})^2$  is a maximal Weil-isotropic  $l$ -subgroup of  $A[l]$  preserve the polarization class and are called  $(l, l)$ -isogenies.
- ▶ For  $l$  prime there are

$$l^3 + l^2 + l + 1$$

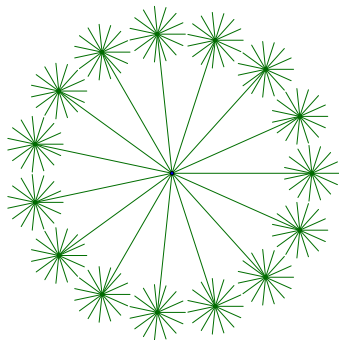
$(l, l)$ -isogenies up to isomorphism, represented by:

$$\mathcal{R}_{l,l}^{(2)} = \left\{ \text{diag}(l, l, 0, 0)x \mid x \in \text{Sp}_4(\mathbb{Z})/\Gamma_0^{(2)}(l) \right\}$$

where  $\Gamma_0^{(2)}(l) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{Sp}_4(\mathbb{Z}) \mid c \equiv 0 \pmod{l} \right\}$ .

## Generic example

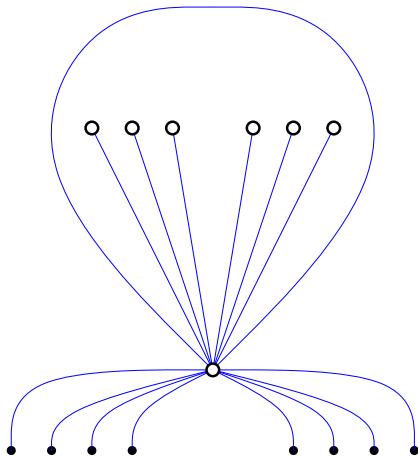
For a generic  $\tau \in \mathbb{H}_2$  (the case where  $\text{End}(\langle \tau, I \rangle) \cong \mathbb{Z}$ ) the  $(2, 2)$ -isogeny graph is a 15-ary tree



## RM example - squiddy the 6-eyed octopus

Here's part of the  $(2, 2)$  isogeny graph of an RM lattice:

$$\text{End}(\langle \tau, I \rangle) = \mathbb{Z}[\sqrt{2}]$$

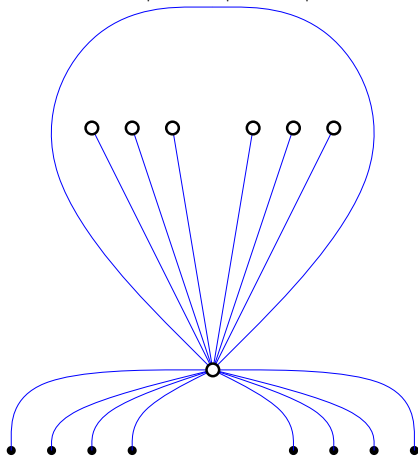


## RM example - squiddy the 6-eyed octopus

Here's part of the  $(2, 2)$  isogeny graph of an RM lattice:

$\text{End}(\langle \tau, I \rangle) = \mathbb{Z}[\sqrt{2}] = \text{Jac}(C)$  where

$C : y^2 = x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$  over  $\mathbb{C}$



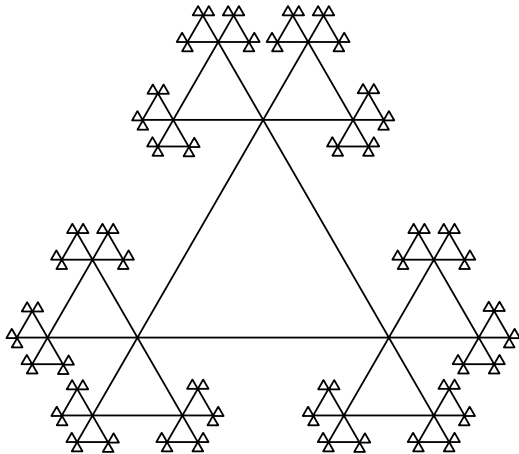


## RM example - squiddy the 6-eyed octopus

Here's part of the  $(2, 2)$  isogeny graph of an RM lattice:

$\text{End}(\langle \tau, I \rangle) = \mathbb{Z}[\sqrt{2}] = \text{Jac}(C)$  where

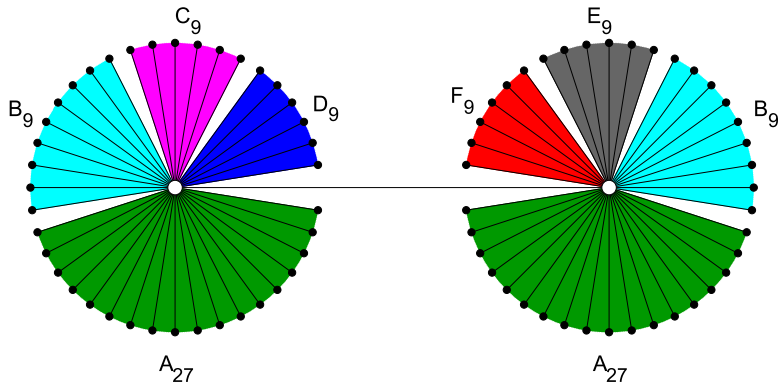
$C : y^2 = x^6 - 4x^5 - 12x^4 + 2x^3 + 8x^2 + 8x - 7$  over  $\mathbb{C}$



part of graph with only (some) maximal RM points shown

## CM example: a $(3, 3)$ -isogeny graph

$K = \mathbb{Q}[X]/(X^4 + 12X^2 + 18)$ , cyclic Galois group, class number 2.  
 $3\mathcal{O}_K = \mathfrak{p}^2 \Rightarrow$  the two CM lattices with  $\mathcal{O}_K$ -multiplication are connected by a  $(3, 3)$ -isogeny.



$A_{27}, B_9, C_9, D_9, E_9, F_9$  are the endomorphism rings of the nonmaximal “leaf” vertices (appearing with multiplicities 18, 9, 6, 6, 6, 6 resp.)  $18 + 9 + 6 + 6 + 1 = 40$  isogenous points.

## Connection to isogeny graphs over finite fields

An ordinary PPAS over  $\mathbb{F}_q$  is the reduction of an abelian surface over  $\mathbb{C}$  having CM by an order in  $K = \mathbb{Q}(\pi)$  where  $\pi$  is an ordinary Weil number of norm  $q^2$ .

To obtain an  $(l, l)$ -isogeny graph for PPAS's over  $\mathbb{F}_q$  in the isogeny class given by  $\pi \in K$ , do the following:

## Connection to isogeny graphs over finite fields

An ordinary PPAS over  $\mathbb{F}_q$  is the reduction of an abelian surface over  $\mathbb{C}$  having CM by an order in  $K = \mathbb{Q}(\pi)$  where  $\pi$  is an ordinary Weil number of norm  $q^2$ .

To obtain an  $(l, l)$ -isogeny graph for PPAS's over  $\mathbb{F}_q$  in the isogeny class given by  $\pi \in K$ , do the following:

1. Take a principally polarizable ideal class of  $\mathcal{O}_K$ :  $(\mathfrak{a}, \xi)$  where  $\xi \in K$  is purely imaginary and  $\xi \mathfrak{a} \bar{\mathfrak{a}} = \mathfrak{D}_{K/\mathbb{Q}}^{-1}$ , the inverse different. This is our starting point.

## Connection to isogeny graphs over finite fields

An ordinary PPAS over  $\mathbb{F}_q$  is the reduction of an abelian surface over  $\mathbb{C}$  having CM by an order in  $K = \mathbb{Q}(\pi)$  where  $\pi$  is an ordinary Weil number of norm  $q^2$ .

To obtain an  $(l, l)$ -isogeny graph for PPAS's over  $\mathbb{F}_q$  in the isogeny class given by  $\pi \in K$ , do the following:

1. Take a principally polarizable ideal class of  $\mathcal{O}_K$ :  $(\mathfrak{a}, \xi)$  where  $\xi \in K$  is purely imaginary and  $\xi \mathfrak{a} \bar{\mathfrak{a}} = \mathfrak{D}_{K/\mathbb{Q}}^{-1}$ , the inverse different. This is our starting point.
2. Compute a Frobenius basis  $\Pi \mathbb{Z}^4$  for the rank four  $\mathbb{Z}$ -module  $\mathfrak{a}$  with respect to  $\xi$ ; the symplectic form is

$$E: (x, y) \mapsto \mathrm{Tr}_{K/\mathbb{Q}}(\xi \bar{x}y)$$

and we want the matrix of  $E$  to be  $\begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ .

3. Compute  $(l, l)$ -isogenous images:

For each isogeny transformation  $M \in \mathcal{R}_{l,l}^{(2)}$ :

- ▶ Compute the isogenous period matrix

$$\Pi' = \Pi^t M.$$

The principally polarized CM lattice is  $(\mathfrak{a}', \xi') = (\Pi' \mathbb{Z}^4, l^{-1} \xi)$ .

3. Compute  $(l, l)$ -isogenous images:

For each isogeny transformation  $M \in \mathcal{R}_{l,l}^{(2)}$ :

- ▶ Compute the isogenous period matrix

$$\Pi' = \Pi^t M.$$

The principally polarized CM lattice is  $(\mathfrak{a}', \xi') = (\Pi' \mathbb{Z}^4, l^{-1} \xi)$ .

- ▶ Test whether

$$\pi \mathfrak{a}' \subset \mathfrak{a}'.$$

If true, this means that  $\pi \in \text{End}(\mathfrak{a}')$  and that the reduction of this isogenous PPAS  $\mathbb{C}^2 / \Pi' \mathbb{Z}^4$  is defined over  $\mathbb{F}_q$ .

Throw away the lattices which fail the test.

### 3. Compute $(l, l)$ -isogenous images:

For each isogeny transformation  $M \in \mathcal{R}_{l,l}^{(2)}$ :

- ▶ Compute the isogenous period matrix

$$\Pi' = \Pi^t M.$$

The principally polarized CM lattice is  $(\mathfrak{a}', \xi') = (\Pi' \mathbb{Z}^4, l^{-1} \xi)$ .

- ▶ Test whether

$$\pi \mathfrak{a}' \subset \mathfrak{a}'.$$

If true, this means that  $\pi \in \text{End}(\mathfrak{a}')$  and that the reduction of this isogenous PPAS  $\mathbb{C}^2 / \Pi' \mathbb{Z}^4$  is defined over  $\mathbb{F}_q$ .

Throw away the lattices which fail the test.

Recursively run algorithm on unexplored isomorphism classes of CM lattices. Isomorphism test:

$$(\mathfrak{a}, \xi) \cong (\mathfrak{a}', \xi') \text{ iff } \begin{cases} \mathfrak{a}' = \gamma \mathfrak{a} \\ \xi' = (\gamma \bar{\gamma})^{-1} \xi \end{cases} \quad (\exists \gamma \in K)$$



## Disadvantages:

- ▶ We can compute complex approximations of absolute invariants for CM lattices, but constructing CM moduli over  $\mathbb{F}_q$  seems rather intractable.
- ▶ Slow

## Advantages:

## Disadvantages:

- ▶ We can compute complex approximations of absolute invariants for CM lattices, but constructing CM moduli over  $\mathbb{F}_q$  seems rather intractable.
- ▶ Slow

## Advantages:

- ▶ Endomorphism rings of CM lattices are easy to compute (= multiplier ring of lattice)

## Generalisations:

- ▶ Use a different set  $\mathcal{R}$  of isogeny transformations, not necessarily always polarization preserving (e.g. cyclic  $l$ -isogenies).
- ▶ Higher genus.

Introduction/Motivation

Genus 1

Genus 2

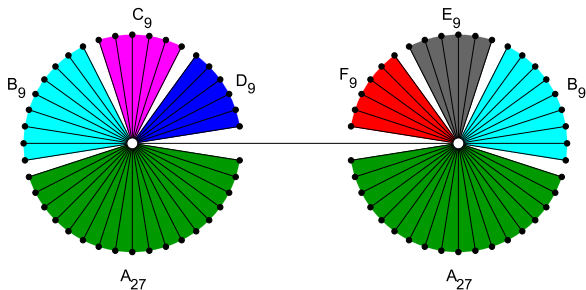
Examples

# Example 1: our old friend $K = \mathbb{Q}[X]/(X^4 + 12X^2 + 18)$

$\text{Gal}(K/\mathbb{Q}) = C_4 = \langle \sigma \rangle$  and  $\text{Cl}(\mathcal{O}_K) = \mathbb{Z}/2\mathbb{Z}$ .

Let  $q = 127$ . We have  $K = \mathbb{Q}(\pi)$  where

$\pi^4 + 28\pi^3 + 378\pi^2 + 28q\pi + q^2 = 0$  is an ordinary Weil number.



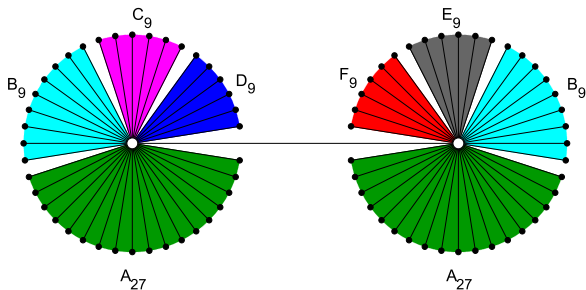
$A_{27}, B_9, C_9, D_9, E_9, F_9$  are the endomorphism rings of the nonmaximal “leaf” vertices (appearing with multiplicities 18,9,6,6,6,6 resp.)

# Example 1: our old friend $K = \mathbb{Q}[X]/(X^4 + 12X^2 + 18)$

$\text{Gal}(K/\mathbb{Q}) = C_4 = \langle \sigma \rangle$  and  $\text{Cl}(\mathcal{O}_K) = \mathbb{Z}/2\mathbb{Z}$ .

Let  $q = 127$ . We have  $K = \mathbb{Q}(\pi)$  where

$\pi^4 + 28\pi^3 + 378\pi^2 + 28q\pi + q^2 = 0$  is an ordinary Weil number.



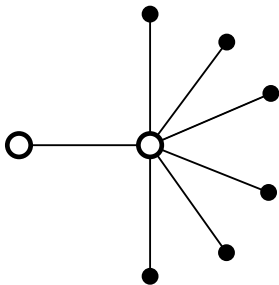
$A_{27}, B_9, C_9, D_9, E_9, F_9$  are the endomorphism rings of the nonmaximal “leaf” vertices (appearing with multiplicities 18,9,6,6,6,6 resp.) Of the six proper suborders, only  $F_9$  contains  $\pi$ .

Example 1: our old friend  $K = \mathbb{Q}[X]/(X^4 + 12X^2 + 18)$

$\text{Gal}(K/\mathbb{Q}) = C_4 = \langle \sigma \rangle$  and  $\text{Cl}(\mathcal{O}_K) = \mathbb{Z}/2\mathbb{Z}$ .

Let  $q = 127$ . We have  $K = \mathbb{Q}(\pi)$  where

$\pi^4 + 28\pi^3 + 378\pi^2 + 28q\pi + q^2 = 0$  is an ordinary Weil number.



**Lesson:** graph structure alone is not sufficient information to determine the endomorphism ring.

Example 2:  $K = \mathbb{Q}[X]/(X^4 + 22X + 73)$

(3, 3)-isogeny graph over  $\mathbb{F}_{1609}$

$\text{Gal}(K/\mathbb{Q}) \cong$  dihedral group of order 8.

Let  $q = 1609$ . We have  $K = \mathbb{Q}(\pi) = \mathbb{Q}(\psi)$  where

$\pi^4 + 76\pi^3 + 2934\pi^2 + 76q\pi + q^2 = 0$  and

$\psi^4 + 32\psi^3 - 414\psi^2 + 32q\psi + q^2 = 0$  are ordinary Weil numbers.

## Example 2: $K = \mathbb{Q}[X]/(X^4 + 22X + 73)$

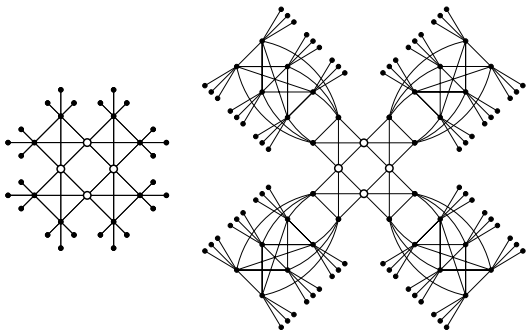
(3, 3)-isogeny graph over  $\mathbb{F}_{1609}$

$\text{Gal}(K/\mathbb{Q}) \cong$  dihedral group of order 8.

Let  $q = 1609$ . We have  $K = \mathbb{Q}(\pi) = \mathbb{Q}(\psi)$  where

$\pi^4 + 76\pi^3 + 2934\pi^2 + 76q\pi + q^2 = 0$  and

$\psi^4 + 32\psi^3 - 414\psi^2 + 32q\psi + q^2 = 0$  are ordinary Weil numbers.



**Lesson:** we can have cycles involving nonmaximal points (invertible ideals of norm  $l^2$  can exist in non  $l$ -maximal orders).



### Example 3: $K = \mathbb{Q}[X]/(X^4 + 598X^2 + 70969)$

(2, 2)-isogenies over  $\mathbb{F}_{3^7}$

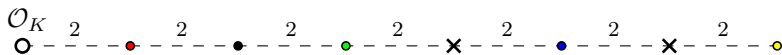
Let  $q = 3^7$ . We have  $K = \mathbb{Q}(\pi)$  where  $\pi^4 + 124\pi^3 + 7418\pi^2 + 124q\pi + q^2 = 0$  is an ordinary Weil number.

$$\text{Cl}(K) = \mathbb{Z}/35\mathbb{Z}$$

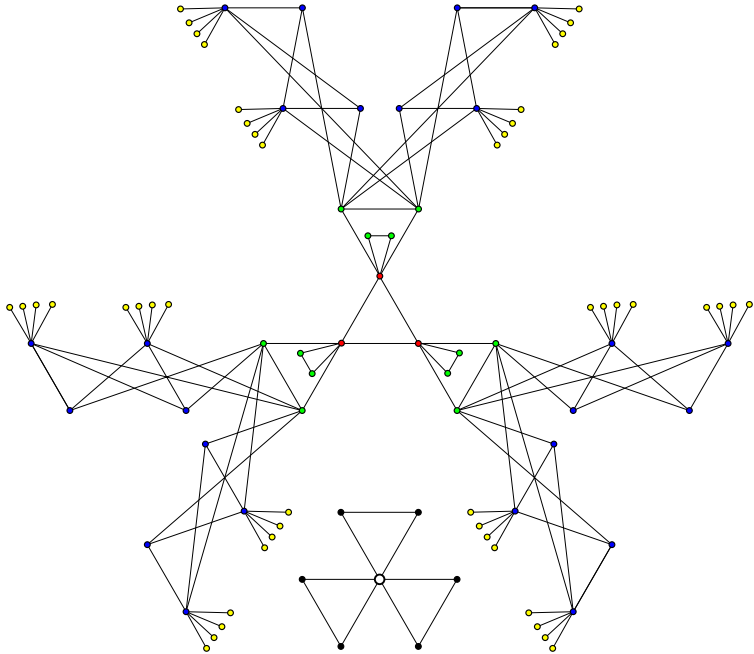
$\text{Gal}(K/\mathbb{Q}) \cong$  dihedral group of order 8

$$[\mathcal{O}_K : \mathbb{Z}[\pi, \bar{\pi}]] = 2^7 \cdot 5^2$$

The sublattice of suborders containing  $\mathbb{Z}[\pi, \bar{\pi}]$  having 2-power index in  $\mathcal{O}_K$  is



On the next slide we'll see that in this example, it is **not** always possible to find a “upward” path to reach a 2-maximal endomorphism ring (here  $\mathcal{O}_K$ ) using (2, 2)-isogenies.

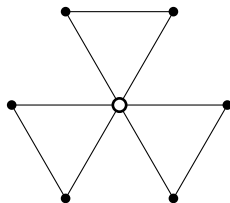


### Example 3: $K = \mathbb{Q}[X]/(X^4 + 598X^2 + 70969)$

(1, 2)-isogenies over  $\mathbb{F}_{3^7}$

Let  $q = 3^7$ . We have  $K = \mathbb{Q}(\pi)$  where  $\pi^4 + 124\pi^3 + 7418\pi^2 + 124q\pi + q^2 = 0$  is an ordinary Weil number.

(2, 2)-isogeny graph:

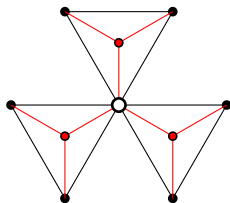


### Example 3: $K = \mathbb{Q}[X]/(X^4 + 598X^2 + 70969)$

(1, 2)-isogenies over  $\mathbb{F}_{3^7}$

Let  $q = 3^7$ . We have  $K = \mathbb{Q}(\pi)$  where  $\pi^4 + 124\pi^3 + 7418\pi^2 + 124q\pi + q^2 = 0$  is an ordinary Weil number.

(1, 2)-isogeny graph:



The end

Genus 3 isogeny graphs?

# The end

Genus 3 isogeny graphs? Perhaps they look like this:



Thanks for your attention.