Computing Endomorphism Rings of Abelian Varieties

Gaetan Bisson

Macquarie University, Sydney, Australia

ECC'11

Isogenies and Abelian Varieties

Let $\mathscr{H}$ be an ordinary hyperelliptic curve of genus $g = 1, 2$ over $\mathbb{F}_q$.

$\mathrm{Jac}(\mathscr{H})$ is a principally polarized abelian variety $(\mathscr{A}, \mathscr{P})$ of dimension g.

Isogenies and Abelian Varieties

Let $\mathscr{H}$ be an ordinary hyperelliptic curve of genus $g = 1, 2$ over $\mathbb{F}_q$.

$\mathrm{Jac}(\mathscr{H})$ is a principally polarized abelian variety $(\mathscr{A}, \mathscr{P})$ of dimension g.

$(\mathscr{A}, \mathscr{P})$ and $(\mathscr{A}', \mathscr{P}')$ are isomorphic if and only if $\mathscr{H}$ and $\mathscr{H}'$ are.

$\mathscr{A}$ and $\mathscr{A}'$ are isogenous if and only if π and π' are conjugate.

Isogenies and Abelian Varieties

Let $\mathscr{H}$ be an ordinary hyperelliptic curve of genus $g = 1, 2$ over $\mathbb{F}_q$.

$\mathrm{Jac}(\mathscr{H})$ is a principally polarized abelian variety $(\mathscr{A}, \mathscr{P})$ of dimension g.

$(\mathscr{A}, \mathscr{P})$ and $(\mathscr{A}', \mathscr{P}')$ are isomorphic if and only if $\mathscr{H}$ and $\mathscr{H}'$ are. (invariants)

$\mathscr{A}$ and $\mathscr{A}'$ are isogenous if and only if π and π' are conjugate. (point counting)

Isogenies and Abelian Varieties

Let $\mathscr{H}$ be an ordinary hyperelliptic curve of genus $g = 1, 2$ over $\mathbb{F}_q$.

$\mathrm{Jac}(\mathscr{H})$ is a principally polarized abelian variety $(\mathscr{A}, \mathscr{P})$ of dimension g.

$(\mathscr{A}, \mathscr{P})$ and $(\mathscr{A}', \mathscr{P}')$ are isomorphic if and only if $\mathscr{H}$ and $\mathscr{H}'$ are. (invariants)

$\mathscr{A}$ and $\mathscr{A}'$ are isogenous if and only if π and π' are conjugate. (point counting)

Crypto: *computable* isogenies transport the DLP.

Computing an isogeny with isotropic kernel $(\mathbb{Z}/\ell\mathbb{Z})^g$ takes roughly ℓ^{2g} time.

Isogenies and Abelian Varieties

Let $\mathscr{H}$ be an ordinary hyperelliptic curve of genus $g = 1, 2$ over $\mathbb{F}_q$.

$\mathrm{Jac}(\mathscr{H})$ is a principally polarized abelian variety $(\mathscr{A}, \mathscr{P})$ of dimension g.

$(\mathscr{A}, \mathscr{P})$ and $(\mathscr{A}', \mathscr{P}')$ are isomorphic if and only if $\mathscr{H}$ and $\mathscr{H}'$ are. (invariants)

$\mathscr{A}$ and $\mathscr{A}'$ are isogenous if and only if π and π' are conjugate. (point counting)

Crypto: *computable* isogenies transport the DLP.

Computing an $\underbrace{\text{isogeny with isotropic kernel } (\mathbb{Z}/\ell\mathbb{Z})^g}_{\ell\text{-isogeny}}$ takes roughly ℓ^{2g} time.

Endomorphism Rings

Let π be the Frobenius endomorphism of $\mathscr{A}$.

The ring of endomorphisms of $\mathscr{A}$ contains $\mathbb{Z}[\pi, \overline{\pi}]$ and is contained in $\mathscr{O}_{\mathbb{Q}(\pi)}$.

Endomorphism Rings

Let π be the Frobenius endomorphism of $\mathscr{A}$.

The ring of endomorphisms of $\mathscr{A}$ contains $\mathbb{Z}[\pi,\overline{\pi}]$ and is contained in $\mathscr{O}_{\mathbb{Q}(\pi)}$.

If $\mathscr{A} \to \mathscr{A}'$ is an ℓ-isogeny, then d divides ℓ^{4g-2} where

$$d = \left[\mathrm{End}(\mathscr{A}) + \mathrm{End}(\mathscr{A}') : \mathrm{End}(\mathscr{A}) \cap \mathrm{End}(A')\right].$$

Endomorphism Rings

Let π be the Frobenius endomorphism of $\mathscr{A}$.

The ring of endomorphisms of $\mathscr{A}$ contains $\mathbb{Z}[\pi, \overline{\pi}]$ and is contained in $\mathscr{O}_{\mathbb{Q}(\pi)}$.

If $\mathscr{A} \to \mathscr{A}'$ is an ℓ-isogeny, then d divides ℓ^{4g-2} where

$$d = \left[\mathrm{End}(\mathscr{A}) + \mathrm{End}(\mathscr{A}') : \mathrm{End}(\mathscr{A}) \cap \mathrm{End}(A')\right].$$

To find an isogeny from $\mathscr{A}$ to $\mathscr{A}'$:

– If $\mathrm{End}(\mathscr{A}) \neq \mathrm{End}(\mathscr{A}')$, take a d-isogeny, and then...

Endomorphism Rings

Let π be the Frobenius endomorphism of $\mathscr{A}$.

The ring of endomorphisms of $\mathscr{A}$ contains $\mathbb{Z}[\pi,\overline{\pi}]$ and is contained in $\mathscr{O}_{\mathbb{Q}(\pi)}$.

If $\mathscr{A} \to \mathscr{A}'$ is an ℓ-isogeny, then d divides ℓ^{4g-2} where

$$d = \left[\mathrm{End}(\mathscr{A}) + \mathrm{End}(\mathscr{A}') : \mathrm{End}(\mathscr{A}) \cap \mathrm{End}(A')\right].$$

To find an isogeny from $\mathscr{A}$ to $\mathscr{A}'$:

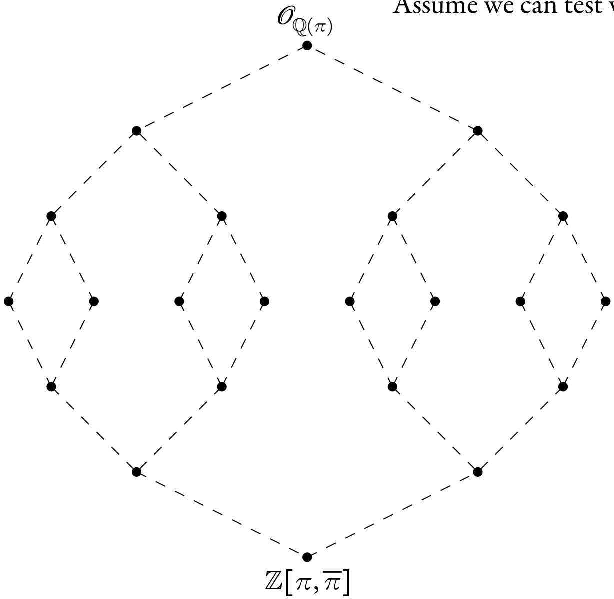
- If $\mathrm{End}(\mathscr{A}) \neq \mathrm{End}(\mathscr{A}')$, take a d-isogeny, and then...
- If $\mathrm{End}(\mathscr{A}) = \mathrm{End}(\mathscr{A}')$, use Pollard's rho (or a quantum computer).

Computing Endomorphism Rings (easy part)

Assume we can test whether $\mathscr{O} \subseteq \mathrm{End}(\mathscr{A})$...

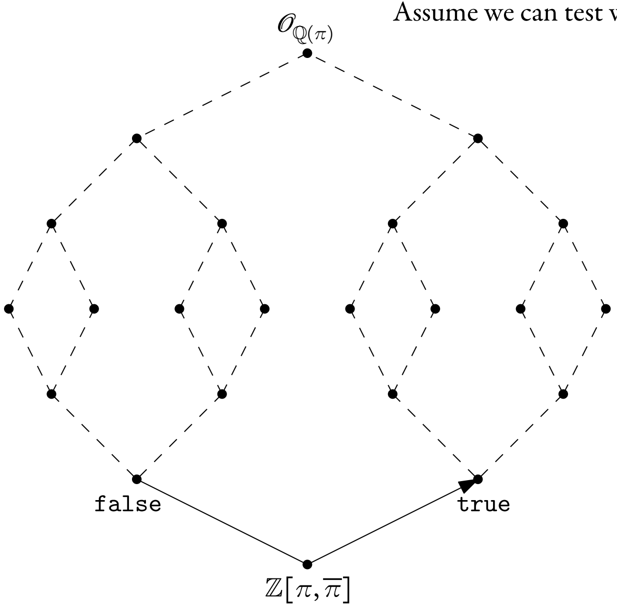
Computing Endomorphism Rings (easy part)

Assume we can test whether $\mathscr{O} \subseteq \mathrm{End}(\mathscr{A})$...



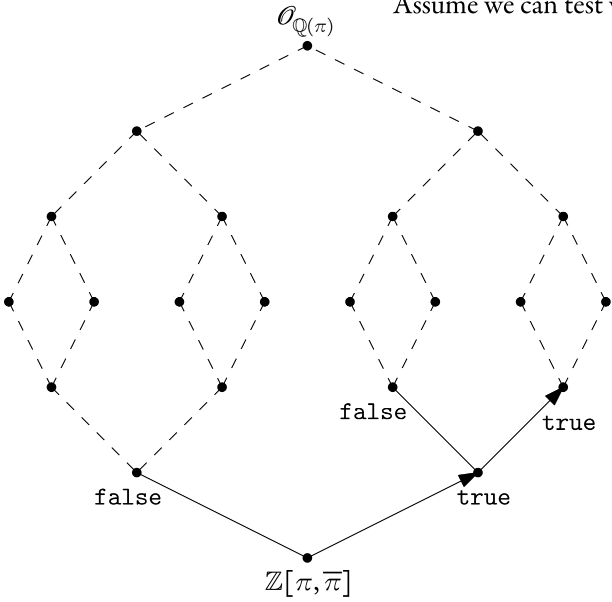
Computing Endomorphism Rings (easy part)

Assume we can test whether $\mathscr{O} \subseteq \mathrm{End}(\mathscr{A})$...



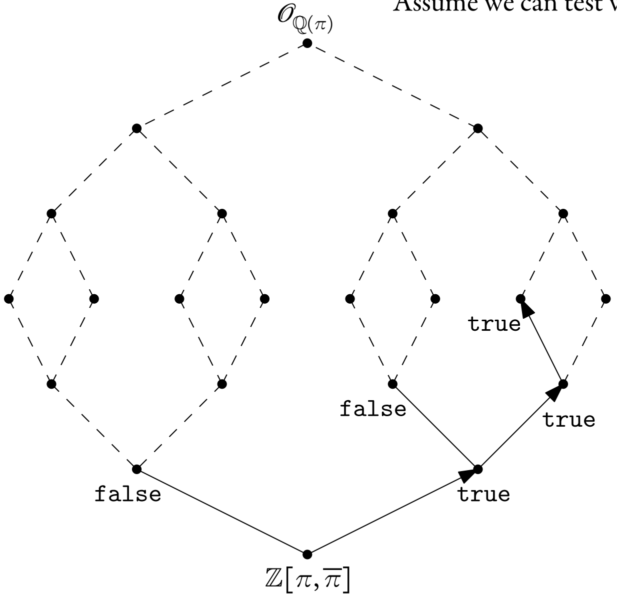
Computing Endomorphism Rings (easy part)

Assume we can test whether $\mathcal{O} \subseteq \mathrm{End}(\mathscr{A})$...



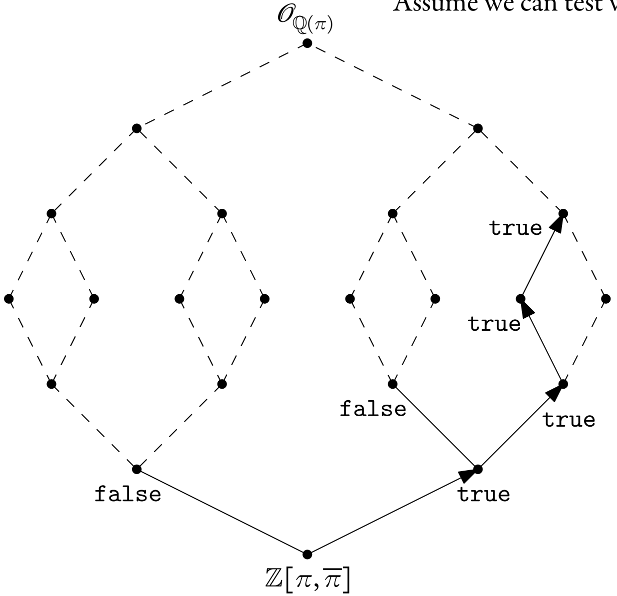
Computing Endomorphism Rings (easy part)

Assume we can test whether $\mathscr{O} \subseteq \mathrm{End}(\mathscr{A})$...



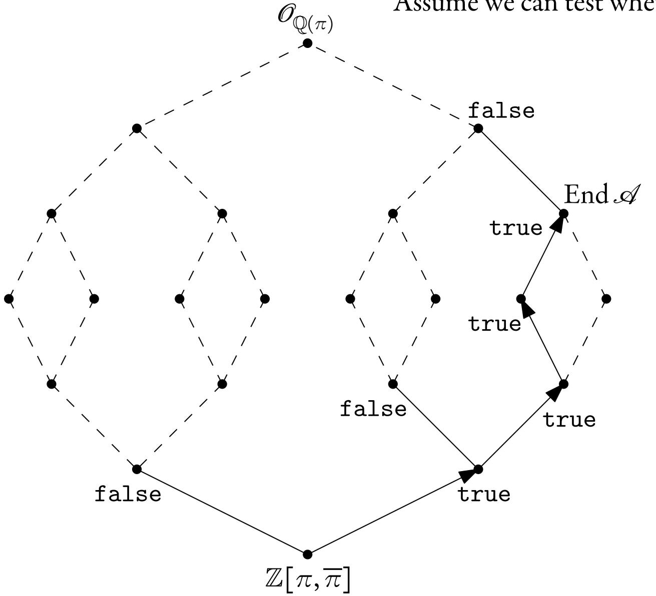
Computing Endomorphism Rings (easy part)

Assume we can test whether $\mathscr{O} \subseteq \mathrm{End}(\mathscr{A})$...



Computing Endomorphism Rings (easy part)

Assume we can test whether $\mathscr{O} \subseteq \operatorname{End}(\mathscr{A})$...



Computing Endomorphism Rings (hard part)

Previous work:

- Kohel's algorithm ($g = 1$)
- Eisenträger–Lauter method
- Wagner's algorithm

Computing Endomorphism Rings (hard part)

Previous work:

- Kohel's algorithm ($g = 1$)
- Eisenträger–Lauter method
- Wagner's algorithm

Exponential worst-case runtime as $d = [\mathcal{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]] \approx q^{g^2/2}$.

Computing Endomorphism Rings (hard part)

Previous work:

- Kohel's algorithm ($g = 1$)
- Eisenträger–Lauter method
- Wagner's algorithm

Exponential worst-case runtime as $d = [\mathscr{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]] \approx q^{g^2/2}$.

Using the *horizontal structure*, we design a subexponential algorithm:

- fast and proven under GRH for $g = 1$;
- slower and relies on more heuristics for $g = 2$.

(Partly joint work with Drew Sutherland.)

Vertical vs. Horizontal

An ℓ-isogeny $\phi : \mathscr{A} \to \mathscr{A}'$ is:

- *vertical* if $\mathrm{End}(\mathscr{A}) \neq \mathrm{End}(\mathscr{A}')$
- *horizontal* if $\mathrm{End}(\mathscr{A}) = \mathrm{End}(\mathscr{A}')$

Vertical vs. Horizontal

An ℓ-isogeny $\phi : \mathscr{A} \to \mathscr{A}'$ is:

- *vertical* if $\mathrm{End}(\mathscr{A}) \neq \mathrm{End}(\mathscr{A}') \Rightarrow \ell \mid [\mathscr{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]]$
- *horizontal* if $\mathrm{End}(\mathscr{A}) = \mathrm{End}(\mathscr{A}') \Leftarrow \ell \nmid [\mathscr{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]]$

Vertical vs. Horizontal

An ℓ-isogeny $\phi : \mathscr{A} \to \mathscr{A}'$ is:

- *vertical* if $\mathrm{End}(\mathscr{A}) \neq \mathrm{End}(\mathscr{A}') \Rightarrow \ell \mid [\mathscr{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]]$
- *horizontal* if $\mathrm{End}(\mathscr{A}) = \mathrm{End}(\mathscr{A}') \Leftarrow \ell \nmid [\mathscr{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]]$

Now, fix a base field $\mathbb{F}_q$, a conjugacy class for π, and a prime ℓ.

Right:

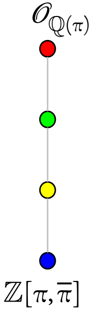
- $V = \{$orders containing $\mathbb{Z}[\pi, \overline{\pi}]\}$
- $E =$ inclusion

Left: (one connected component of)

- $V = \{$isomorphism classes of p.p. abelian varieties$\}$
- $E = \{\ell$-isogenies$\}$

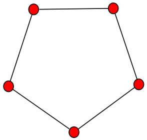
Vertical Structure for $g = 1$

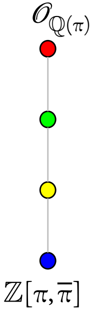
(Kohel's thesis)



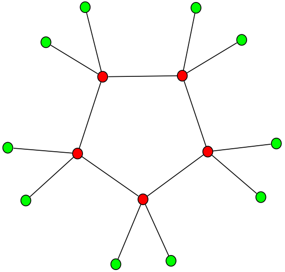
Vertical Structure for $g = 1$

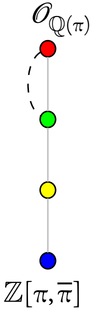
(Kohel's thesis)





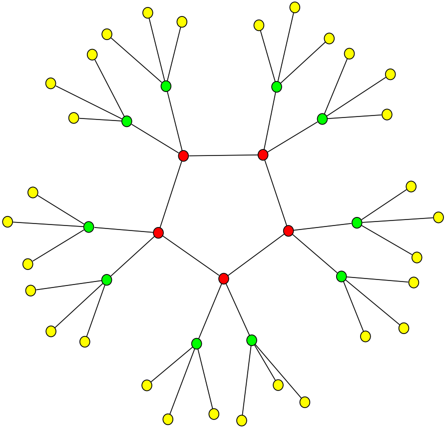
Vertical Structure for $g = 1$ (Kohel's thesis)

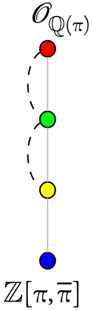




Vertical Structure for $g = 1$

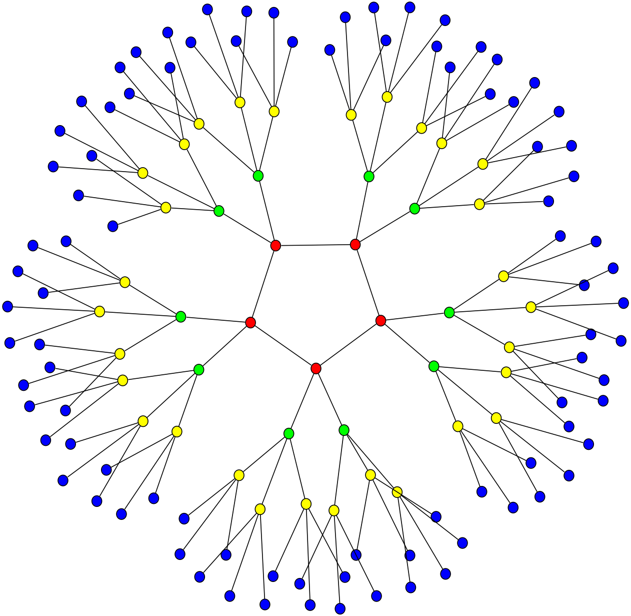
(Kohel's thesis)

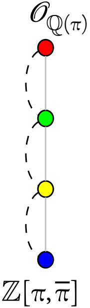




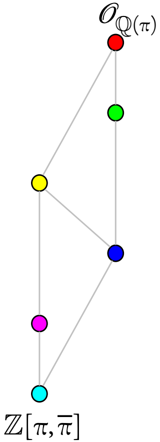
Vertical Structure for $g = 1$

(Kohel's thesis)

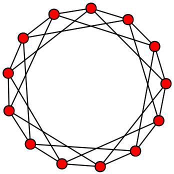


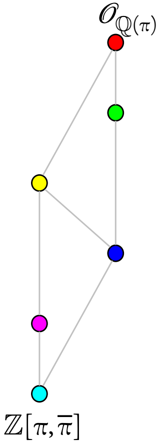


Vertical Structure for $g = 2$

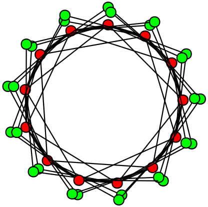


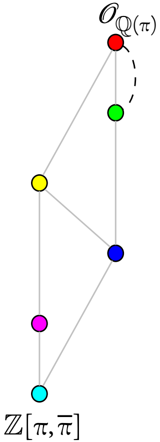
Vertical Structure for $g = 2$



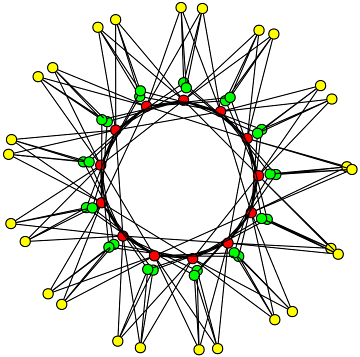


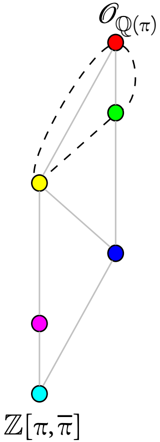
Vertical Structure for $g = 2$



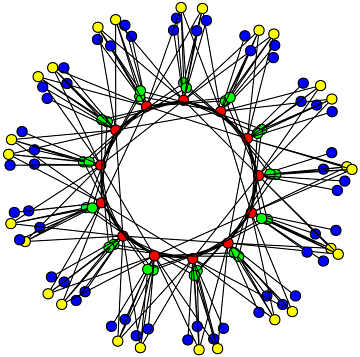


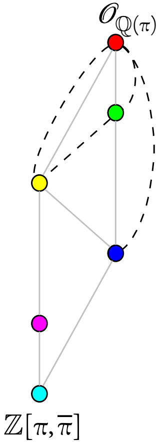
VERTICAL STRUCTURE FOR $g = 2$



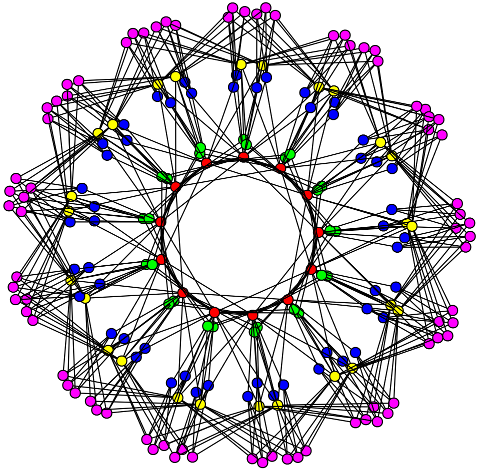


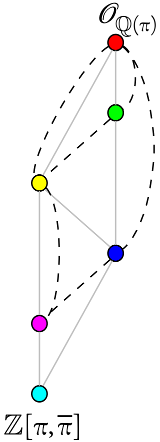
Vertical Structure for $g = 2$



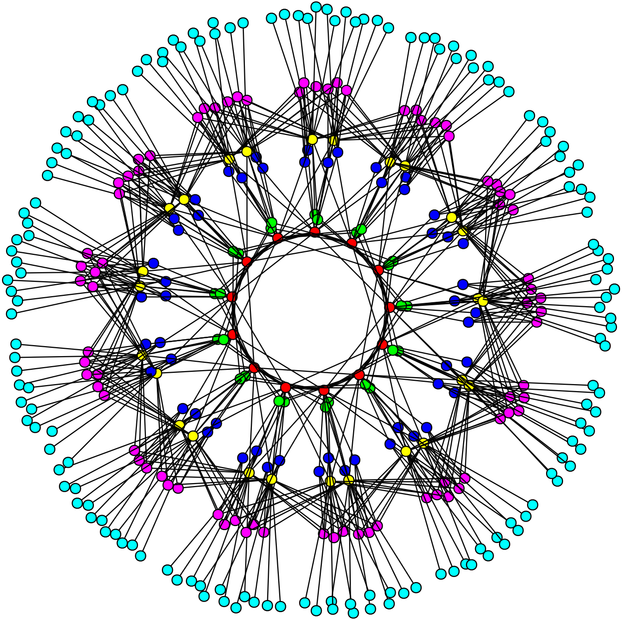


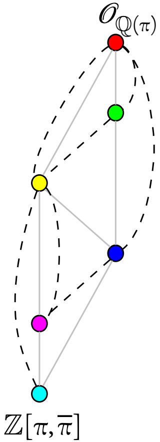
Vertical Structure for $g = 2$





Vertical Structure for $g = 2$





Complex Multiplication

Ideals $\mathfrak{a}$ such that $\mathfrak{a}\bar{\mathfrak{a}} = \ell\mathscr{O}$ act as ℓ-isogenies on $\{\mathscr{A} : \mathrm{End}(\mathscr{A}) \simeq \mathscr{O}\}$.
Principal ideals map $\mathscr{A}$ to an isomorphic variety.

Complex Multiplication

Ideals $\mathfrak{a}$ such that $\mathfrak{a}\bar{\mathfrak{a}} = \ell\mathscr{O}$ act as ℓ-isogenies on $\{\mathscr{A} : \mathrm{End}(\mathscr{A}) \simeq \mathscr{O}\}$.
Principal ideals map $\mathscr{A}$ to an isomorphic variety.

For instance, if $\ell\mathscr{O} = \mathfrak{p}\bar{\mathfrak{p}}\mathfrak{q}\bar{\mathfrak{q}}$, ℓ-isogenies correspond to $\mathfrak{p}\mathfrak{q}$, $\mathfrak{p}\bar{\mathfrak{q}}$, and $\bar{\mathfrak{p}}\bar{\mathfrak{q}}$, $\bar{\mathfrak{p}}\mathfrak{q}$.

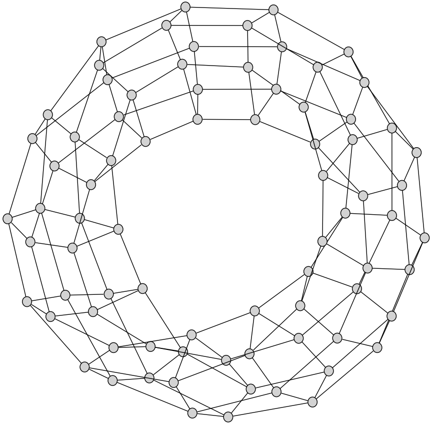
The ℓ-isogeny graph of $\mathscr{A} : \mathrm{End}(\mathscr{A}) \simeq \mathscr{O}$
is their Cayley graph in $\mathrm{cl}(\mathscr{O})$.

Complex Multiplication

Ideals $\mathfrak{a}$ such that $\mathfrak{a}\bar{\mathfrak{a}} = \ell\mathscr{O}$ act as ℓ-isogenies on $\{\mathscr{A} : \mathrm{End}(\mathscr{A}) \simeq \mathscr{O}\}$.
Principal ideals map $\mathscr{A}$ to an isomorphic variety.

For instance, if $\ell\mathscr{O} = \mathfrak{p}\bar{\mathfrak{p}}\mathfrak{q}\bar{\mathfrak{q}}$, ℓ-isogenies correspond to $\mathfrak{p}\mathfrak{q}$, $\mathfrak{p}\bar{\mathfrak{q}}$, and $\bar{\mathfrak{p}}\bar{\mathfrak{q}}$, $\bar{\mathfrak{p}}\mathfrak{q}$.

The ℓ-isogeny graph of $\mathscr{A} : \mathrm{End}(\mathscr{A}) \simeq \mathscr{O}$ is their Cayley graph in $\mathrm{cl}(\mathscr{O})$.



Example:
$(\mathfrak{p}\mathfrak{q})^{26} = 1$
$(\mathfrak{p}\bar{\mathfrak{q}})^{6} = 1$
$(\mathfrak{p}\mathfrak{q})^{13}(\mathfrak{p}\bar{\mathfrak{q}})^{3} = 1$

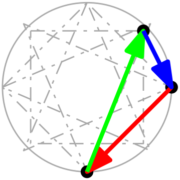
Probing Class Groups

$$\mathfrak{a}\ \mathfrak{b}\ \mathfrak{c} = 1 \in \mathrm{cl}(\mathscr{O}')$$

$$\mathfrak{a}\ \mathfrak{b}\ \mathfrak{c} \neq 1 \in \mathrm{cl}(\mathscr{O})$$

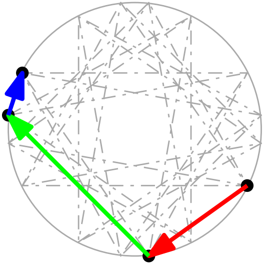
Probing Class Groups

$\mathfrak{a}\,\mathfrak{b}\,\mathfrak{c} = 1 \in \mathrm{cl}(\mathscr{O}') \iff$



$\mathrm{End}(\mathscr{A}') \simeq \mathscr{O}'$

$\mathfrak{a}\,\mathfrak{b}\,\mathfrak{c} \neq 1 \in \mathrm{cl}(\mathscr{O}) \iff$



$\mathrm{End}(\mathscr{A}) \simeq \mathscr{O}$

Relations

Let $\mathfrak{P}$ be a generating set of ideals for $\mathrm{cl}(\mathbb{Z}[\pi, \overline{\pi}])$.

Define $\Lambda_{\mathscr{O}} = \{x \in \mathbb{Z}^{\mathfrak{P}} : \prod (\mathfrak{p}\mathscr{O})^{x_{\mathfrak{p}}} \text{ principal}\}$; thus $\mathbb{Z}^{\mathfrak{P}} / \Lambda_{\mathscr{O}} = \mathrm{cl}(\mathscr{O})$.

Relations

Let $\mathfrak{P}$ be a generating set of ideals for $\mathrm{cl}(\mathbb{Z}[\pi,\overline{\pi}])$.

Define $\Lambda_{\mathcal{O}} = \{x \in \mathbb{Z}^{\mathfrak{P}} : \prod(\mathfrak{p}\mathcal{O})^{x_{\mathfrak{p}}} \text{ principal}\}$; thus $\mathbb{Z}^{\mathfrak{P}}/\Lambda_{\mathcal{O}} = \mathrm{cl}(\mathcal{O})$.

We have $\mathcal{O} \subseteq \mathcal{O}' \Rightarrow \Lambda_{\mathcal{O}} \subseteq \Lambda_{\mathcal{O}'}$. (Almost an equivalence.)

Relations

Let $\mathfrak{P}$ be a generating set of ideals for $\mathrm{cl}(\mathbb{Z}[\pi, \overline{\pi}])$.

Define $\Lambda_{\mathcal{O}} = \{x \in \mathbb{Z}^{\mathfrak{P}} : \prod (\mathfrak{p}\mathcal{O})^{x_{\mathfrak{p}}} \text{ principal}\}$; thus $\mathbb{Z}^{\mathfrak{P}} / \Lambda_{\mathcal{O}} = \mathrm{cl}(\mathcal{O})$.

We have $\mathcal{O} \subseteq \mathcal{O}' \Rightarrow \Lambda_{\mathcal{O}} \subseteq \Lambda_{\mathcal{O}'}$. (Almost an equivalence.)

To test if $\Lambda_{\mathcal{O}} \subseteq \Lambda_{\mathrm{End}(\mathscr{A})}$, select *random relations* $x \in \Lambda_{\mathcal{O}}$ and compute

$$\underbrace{\phi_{\mathfrak{p}_1} \circ \cdots \circ \phi_{\mathfrak{p}_1}}_{x_{\mathfrak{p}_1} \text{ times}} \circ \underbrace{\phi_{\mathfrak{p}_2} \circ \cdots \circ \phi_{\mathfrak{p}_2}}_{x_{\mathfrak{p}_2} \text{ times}} \circ \cdots (\mathscr{A})$$

Relations

Let $\mathfrak{P}$ be a generating set of ideals for $\mathrm{cl}(\mathbb{Z}[\pi,\overline{\pi}])$.

Define $\Lambda_{\mathscr{O}} = \{x \in \mathbb{Z}^{\mathfrak{P}} : \prod(\mathfrak{p}\mathscr{O})^{x_\mathfrak{p}} \text{ principal}\}$; thus $\mathbb{Z}^{\mathfrak{P}}/\Lambda_{\mathscr{O}} = \mathrm{cl}(\mathscr{O})$.

We have $\mathscr{O} \subseteq \mathscr{O}' \Rightarrow \Lambda_{\mathscr{O}} \subseteq \Lambda_{\mathscr{O}'}$. (Almost an equivalence.)

To test if $\Lambda_{\mathscr{O}} \subseteq \Lambda_{\mathrm{End}(\mathscr{A})}$, select *random relations* $x \in \Lambda_{\mathscr{O}}$ and compute

$$\underbrace{\phi_{\mathfrak{p}_1} \circ \cdots \circ \phi_{\mathfrak{p}_1}}_{x_{\mathfrak{p}_1} \text{ times}} \circ \underbrace{\phi_{\mathfrak{p}_2} \circ \cdots \circ \phi_{\mathfrak{p}_2}}_{x_{\mathfrak{p}_2} \text{ times}} \circ \cdots (\mathscr{A})$$

Remains to:

- Obtain random relations with bounded coefficients.
- Evaluate $\phi_{\mathfrak{p}}$.
- Ensure $\Lambda_{\mathscr{O}}$ determines $\mathscr{O}$.

Relations

Let $\mathfrak{P}$ be a generating set of ideals for $\mathrm{cl}(\mathbb{Z}[\pi,\overline{\pi}])$.

Define $\Lambda_{\mathcal{O}} = \{x \in \mathbb{Z}^{\mathfrak{P}} : \prod(\mathfrak{p}\mathcal{O})^{x_\mathfrak{p}} \text{ principal}\}$; thus $\mathbb{Z}^{\mathfrak{P}}/\Lambda_{\mathcal{O}} = \mathrm{cl}(\mathcal{O})$.

We have $\mathcal{O} \subseteq \mathcal{O}' \Rightarrow \Lambda_{\mathcal{O}} \subseteq \Lambda_{\mathcal{O}'}$. (Almost an equivalence.)

To test if $\Lambda_{\mathcal{O}} \subseteq \Lambda_{\mathrm{End}(\mathscr{A})}$, select *random relations* $x \in \Lambda_{\mathcal{O}}$ and compute

$$\underbrace{\phi_{\mathfrak{p}_1} \circ \cdots \circ \phi_{\mathfrak{p}_1}}_{x_{\mathfrak{p}_1} \text{ times}} \circ \underbrace{\phi_{\mathfrak{p}_2} \circ \cdots \circ \phi_{\mathfrak{p}_2}}_{x_{\mathfrak{p}_2} \text{ times}} \circ \cdots (\mathscr{A})$$

Remains to:

- Obtain random relations with bounded coefficients.
- Evaluate $\phi_\mathfrak{p}$. $\longrightarrow$ `AVIsogenies`
- Ensure $\Lambda_{\mathcal{O}}$ determines $\mathcal{O}$. $\longrightarrow$ vertical methods

Finding Relations

Find products of elements of $\mathfrak{P}$ that are principal in $\mathscr{O}$.

Finding Relations

Find products of elements of $\mathfrak{P}$ that are principal in $\mathcal{O}$.

1. Let $\mathfrak{P} = \{\mathfrak{p} \text{ prime of norm} < N\}$
2. While true do:
3. Draw $x \in \{0, \ldots, h-1\}^{\mathfrak{P}}$ uniformly at random.
4. Let $y \leftarrow \prod \mathfrak{p}^{x_\mathfrak{p}}$.
5. Let $y' \leftarrow \mathrm{Reduce}(y)$.
6. If $y' = \prod \mathfrak{p}^{z_\mathfrak{p}}$ for some z, return $x - z$.

Finding Relations

Find products of elements of $\mathfrak{P}$ that are principal in $\mathcal{O}$.

1. Let $\mathfrak{P} = \{\mathfrak{p} \text{ prime of norm} < N\}$
2. While true do:
3. Draw $x \in \{0, \dots, h-1\}^{\mathfrak{P}}$ uniformly at random.
4. Let $y \leftarrow \prod \mathfrak{p}^{x_\mathfrak{p}}$.
5. Let $y' \leftarrow \text{Reduce}(y)$.
6. If $y' = \prod \mathfrak{p}^{z_\mathfrak{p}}$ for some z, return $x - z$.

Time: $L(\Delta)^\gamma + L(\Delta)^{1/(4\gamma)}$ when $N = L(\Delta)^\gamma$, $\Delta = \text{disc}(\mathcal{O})$.

Finding Relations

Find products of elements of $\mathfrak{P}$ that are principal in $\mathcal{O}$.

1. Let $\mathfrak{P} = \{\mathfrak{p} \text{ prime of norm} < N\}$
2. While true do:
3. Draw $x \in \{0, \dots, h-1\}^{\mathfrak{P}}$ uniformly at random.
4. Let $y \leftarrow \prod \mathfrak{p}^{x_\mathfrak{p}}$.
5. Let $y' \leftarrow \mathrm{Reduce}(y)$.
6. If $y' = \prod \mathfrak{p}^{z_\mathfrak{p}}$ for some z, return $x - z$.

Time: $L(\Delta)^\gamma + L(\Delta)^{1/(4\gamma)}$ when $N = L(\Delta)^\gamma$, $\Delta = \mathrm{disc}(\mathcal{O})$.

For any $\mathcal{O}' \subseteq \mathcal{O}$, this gives random relations of $\Lambda_\mathcal{O}/\Lambda_{\mathcal{O}'}$.
(Rests on GRH for $g = 1$, more for $g = 2$)

Finding Relations

Find products of elements of $\mathfrak{P}$ that are principal in $\mathcal{O}$.

1. Let $\mathfrak{P} = \{\mathfrak{p} \text{ prime of norm} < N\}$
2. While true do:
3. Draw $x \in \{0, \dots, h-1\}^{\mathfrak{P}}$ uniformly at random.
4. Let $y \leftarrow \prod \mathfrak{p}^{x_\mathfrak{p}}$.
5. Let $y' \leftarrow \text{Reduce}(y)$.
6. If $y' = \prod \mathfrak{p}^{z_\mathfrak{p}}$ for some z, return $x - z$.

Time: $L(\Delta)^\gamma + L(\Delta)^{1/(4\gamma)}$ when $N = L(\Delta)^\gamma$, $\Delta = \text{disc}(\mathcal{O})$.

For any $\mathcal{O}' \subseteq \mathcal{O}$, this gives random relations of $\Lambda_{\mathcal{O}}/\Lambda_{\mathcal{O}'}$.
(Rests on GRH for $g = 1$, more for $g = 2$)

Bounded Relations

To bound coefficients while retaining randomness, we use:

Under GRH, for all $\varepsilon > 0$ there exists $c > 1$ such that for any order $\mathcal{O}$:
products of at least $c \log(\Delta)/\log\log(\Delta)$ elements of $\{\mathfrak{p}$ of norm $< \log^{2+\varepsilon}\Delta\}$
are quasi-uniformly distributed in $\mathrm{cl}(\mathcal{O})$.

Bounded Relations

To bound coefficients while retaining randomness, we use:

Under GRH, for all $\varepsilon > 0$ there exists $c > 1$ such that for any order $\mathcal{O}$:
products of at least $c \log(\Delta)/\log\log(\Delta)$ elements of $\{\mathfrak{p}$ of norm $< \log^{2+\varepsilon}\Delta\}$
are quasi-uniformly distributed in $\mathrm{cl}(\mathcal{O})$.

So each ideal class not only has a smooth representant,
but also one with exponents $o(\log(\Delta))$.

Bounded Relations

To bound coefficients while retaining randomness, we use:

Under GRH, for all $\varepsilon > 0$ there exists $c > 1$ such that for any order $\mathcal{O}$:
products of at least $c \log(\Delta)/\log\log(\Delta)$ elements of $\{\mathfrak{p}$ of norm $< \log^{2+\varepsilon}\Delta\}$
are quasi-uniformly distributed in $\mathrm{cl}(\mathcal{O})$.

So each ideal class not only has a smooth representant,
but also one with exponents $o(\log(\Delta))$.

This implies $\mathrm{diam}(\Lambda_{\mathcal{O}}) = o(\log^{4+\varepsilon}\Delta)$, from which we deduce
that *random* relations with small coefficients can be generated.

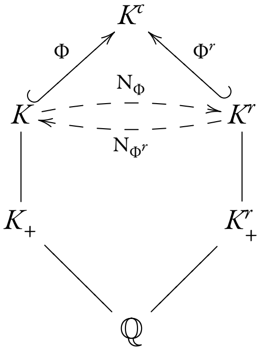
Restricting to ℓ-isogenies

PROBLEM: This might not generate relations with ideals $\mathfrak{a}$ such that $\mathfrak{a}\bar{\mathfrak{a}} = \ell\mathcal{O}$.

Restricting to ℓ-isogenies

Problem: This might not generate relations with ideals $\mathfrak{a}$ such that $\mathfrak{a}\overline{\mathfrak{a}} = \ell\mathcal{O}$.

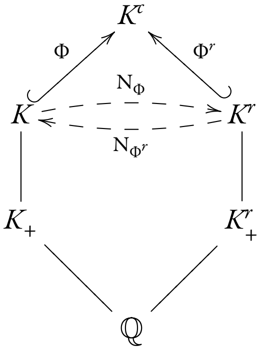
Theoretical Solution:
Generate relations in $\mathrm{cl}(\mathcal{O}^r)$ and fetch them via the reflex typenorm.



Restricting to ℓ-isogenies

Problem: This might not generate relations with ideals $\mathfrak{a}$ such that $\mathfrak{a}\bar{\mathfrak{a}} = \ell\mathcal{O}$.

Theoretical Solution:
Generate relations in $\mathrm{cl}(\mathcal{O}^r)$ and fetch them via the reflex typenorm.



Practical Solution: Use BSGS.

Theoretical Results

Heuristics (only GRH needed for $g = 1$):

- GRH and smoothness of reduced ideals;
- our relations determine $\Lambda_{\mathcal{O}}$ which determines $\mathcal{O}$;
- complex multiplication holds for non-maximal orders.

Theoretical Results

Heuristics (only GRH needed for $g = 1$):

- GRH and smoothness of reduced ideals;
- our relations determine $\Lambda_{\mathcal{O}}$ which determines $\mathcal{O}$;
- complex multiplication holds for non-maximal orders.

Finding relations: $L(\Delta)^{\gamma} + L(\Delta)^{1/4\gamma}$ for one with norm $L(\Delta)^{\gamma}$

Computing isogenies: ℓ^{4g}

Theoretical Results

Heuristics (only GRH needed for $g = 1$):

- GRH and smoothness of reduced ideals;
- our relations determine $\Lambda_{\mathscr{O}}$ which determines $\mathscr{O}$;
- complex multiplication holds for non-maximal orders.

Finding relations: $L(\Delta)^{\gamma} + L(\Delta)^{1/4\gamma}$ for one with norm $L(\Delta)^{\gamma}$

Computing isogenies: ℓ^{4g}

Computing $\mathrm{End}(\mathscr{A})$ for an abelian variety $\mathscr{A}/\mathbb{F}_q$ takes time

$$L(q)^{g^{3/2}} \quad \text{for } g = 2$$

$$L(q)^{1/\sqrt{2}} \quad \text{for } g = 1 \quad \text{(faster isogenies, besides factoring)}$$

Practical Results for $g = 1$

Let $\mathscr{A}/\mathbb{F}_q$ be the elliptic curve $Y^2 = X^3 - 3X + c$ where

$$c = 66089717007102549448903693691119613107552207997068089804952 8$$
$$q = 160693804425899027555081234320605007554655094341590901447829 9$$

$$[\mathcal{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]] = 2 \cdot 127 \cdot 524287 \cdot 7195777666870732918103.$$

Practical Results for $g = 1$

Let $\mathscr{A}/\mathbb{F}_q$ be the elliptic curve $Y^2 = X^3 - 3X + c$ where

$$c = 660897170071025494489036936911196131075522079970680898049528$$
$$q = 1606938044258990275550812343206050075546550943415909014478299$$

$$[\mathscr{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]] = 2 \cdot 127 \cdot 524287 \cdot 7195777666870732918103.$$

Using further improvements for $g = 1$ yield the timings:

- four minutes to find relations;
- five minutes to evaluate the corresponding isogenies.

A typical relation was:

$$\mathfrak{p}_2^{1798}\mathfrak{p}_{23}^{3}\mathfrak{p}_{29}^{1}\mathfrak{p}_{37}^{2}\mathfrak{p}_{53}^{29}\mathfrak{p}_{137}^{1}\mathfrak{p}_{149}^{1}\mathfrak{p}_{233}^{1}\mathfrak{p}_{263}^{2}\mathfrak{p}_{547}^{1}$$

Practical Results for $g = 2$

Best Case: $\mathrm{Jac}\left(y^2 = 80742x^5 + 56078x^4 + 76952x^3 + 134685x^2 + 60828x + 119537\right)$ over $\mathbb{F}_{161983}$

$$[\mathcal{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]] = 156799$$

The ideal $\mathfrak{p}_3^{115}$ is principal in $\mathcal{O}_{\mathbb{Q}(\pi)}$ but not in $\mathbb{Z}[\pi, \overline{\pi}]$.
Testing that relation took under four minutes.

Practical Results for $g = 2$

Best Case: $\mathrm{Jac}\big(y^2 = 80742x^5 + 56078x^4 + 76952x^3 + 134685x^2 + 60828x + 119537\big)$ over $\mathbb{F}_{161983}$

$$[\mathscr{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]] = 156799$$

The ideal $\mathfrak{p}_3^{115}$ is principal in $\mathscr{O}_{\mathbb{Q}(\pi)}$ but not in $\mathbb{Z}[\pi, \overline{\pi}]$.
Testing that relation took under four minutes.

Average Case: $\mathrm{Jac}\big(y^2 = 2987x^5 + 1680x^4 + 3443x^3 + 1918x^2 + 2983x + 489\big)$ over $\mathbb{F}_{3499}$

$$[\mathscr{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]] = 13^2 \cdot 37 \cdot 79$$

Horizontal 3, 5, and 7-isogenies take 1, 3.5, and 5.5 seconds to compute.
Using $\mathfrak{p}_3^5 \mathfrak{p}_7^7 = 1$ and $\mathfrak{p}_5^{10} = 1$ suffices to conclude.

Practical Results for $g = 2$

Best Case: $\mathrm{Jac}\left(y^2 = 80742x^5 + 56078x^4 + 76952x^3 + 134685x^2 + 60828x + 119537\right)$ over $\mathbb{F}_{161983}$

$$[\mathcal{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]] = 156799$$

The ideal $\mathfrak{p}_3^{115}$ is principal in $\mathcal{O}_{\mathbb{Q}(\pi)}$ but not in $\mathbb{Z}[\pi, \overline{\pi}]$.
Testing that relation took under four minutes.

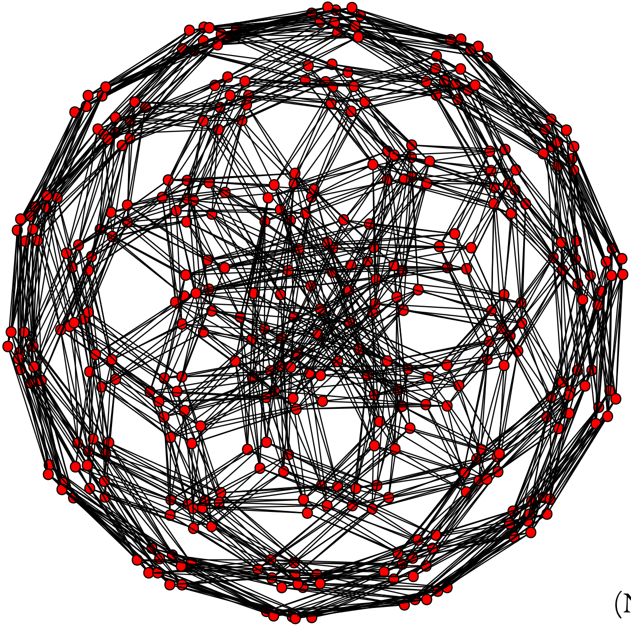
Average Case: $\mathrm{Jac}\left(y^2 = 2987x^5 + 1680x^4 + 3443x^3 + 1918x^2 + 2983x + 489\right)$ over $\mathbb{F}_{3499}$

$$[\mathcal{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]] = 13^2 \cdot 37 \cdot 79$$

Horizontal 3, 5, and 7-isogenies take 1, 3.5, and 5.5 seconds to compute.
Using $\mathfrak{p}_3^5 \mathfrak{p}_7^7 = 1$ and $\mathfrak{p}_5^{10} = 1$ suffices to conclude.

Worst Case: $[\mathcal{O}_{\mathbb{Q}(\pi)} : \mathbb{Z}[\pi, \overline{\pi}]] = 2 \cdot 3 \cdot 5$; slower than other methods.

NEXT YEAR: $g = 3$?!



(Not a chance.)