Computing isomorphism classes and polarisations of abelian varieties over finite fields.

Stefano Marseglia

Utrecht University

Institut Fourier - Laboratoire de mathématiques
Grenoble - December 12, 2023

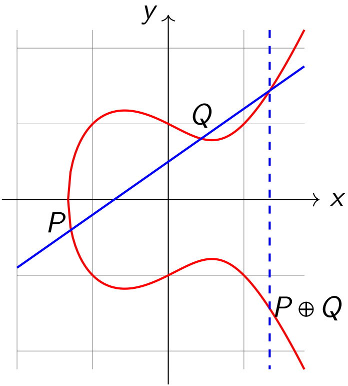
Abelian varieties: what are they ?

Abelian varieties are connected projective group varieties.

Abelian varieties: what are they ?

Abelian varieties are connected projective group varieties.

Abelian varieties of dim. 1 are called **elliptic curves**.
Eg: over $\mathbb{R}$, $y^2 = x^3 - x + 1$

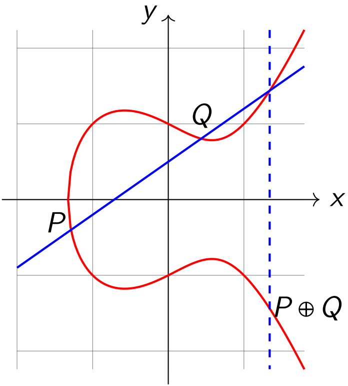


Abelian varieties: what are they ?

Abelian varieties are connected projective group varieties.

Abelian varieties of dim. 1 are called **elliptic curves**.
Eg: over $\mathbb{R}$, $y^2 = x^3 - x + 1$

We can add points:
$P, Q \rightsquigarrow P \oplus Q$



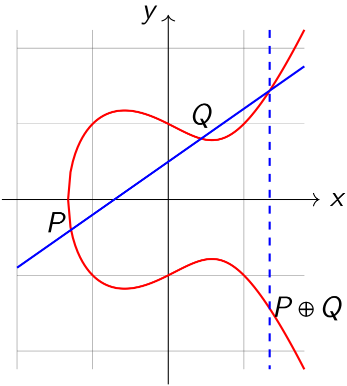
Abelian varieties: what are they ?

Abelian varieties are connected projective group varieties.

Abelian varieties of dim. 1 are called **elliptic curves**.
Eg: over $\mathbb{R}$, $y^2 = x^3 - x + 1$

We can add points:
$P, Q \rightsquigarrow P \oplus Q$

Equations are impractical in dim ≥ 2.
We need a better way to represent them...



Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension g.

Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension g.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.

Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension g.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- Also, T admits a non-degenerate **Riemann form** $\longleftrightarrow$ polarization.

Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension g.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- Also, T admits a non-degenerate **Riemann form** $\longleftrightarrow$ polarization.
- The functor $A \mapsto A(\mathbb{C})$ induces an equivalence of categories:

$$\{\text{abelian varieties } /\mathbb{C}\} \longleftrightarrow \left\{ \begin{array}{c} \mathbb{C}^g/\Lambda \text{ with } \Lambda \simeq \mathbb{Z}^{2g} \text{ admitting} \\ \text{a Riemann form} \end{array} \right\}.$$

Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension g.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- Also, T admits a non-degenerate **Riemann form** $\longleftrightarrow$ polarization.
- The functor $A \mapsto A(\mathbb{C})$ induces an equivalence of categories:

$$\{\text{abelian varieties } /\mathbb{C}\} \longleftrightarrow \left\{ \begin{matrix} \mathbb{C}^g/\Lambda \text{ with } \Lambda \simeq \mathbb{Z}^{2g} \text{ admitting} \\ \text{a Riemann form} \end{matrix} \right\}.$$

- In char. $p > 0$ such an equivalence cannot exist : there are (supersingular) elliptic curves with quaternionic endomorphism algebras.

Abelian varieties over $\mathbb{C}$ vs $\mathbb{F}_q$

- Let $A/\mathbb{C}$ be an abelian variety of dimension g.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- Also, T admits a non-degenerate **Riemann form** $\longleftrightarrow$ polarization.
- The functor $A \mapsto A(\mathbb{C})$ induces an equivalence of categories:

$$\{\text{abelian varieties } /\mathbb{C}\} \longleftrightarrow \left\{ \begin{array}{c} \mathbb{C}^g/\Lambda \text{ with } \Lambda \simeq \mathbb{Z}^{2g} \text{ admitting} \\ \text{a Riemann form} \end{array} \right\}.$$

- In char. $p > 0$ such an equivalence cannot exist : there are (supersingular) elliptic curves with quaternionic endomorphism algebras.
- Nevertheless, over finite fields, we obtain analogous results if we restrict ourselves to certain **subcategories** of AVs.

Isogeny classification over $\mathbb{F}_q$

- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism,

Isogeny classification over $\mathbb{F}_q$

- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism, that induces an action

$$\mathrm{Frob}_A : T_\ell A \to T_\ell A \text{ for any } \ell \neq p,$$

where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.

Isogeny classification over $\mathbb{F}_q$

- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism, that induces an action

$$\mathrm{Frob}_A : T_\ell A \to T_\ell A \text{ for any } \ell \neq p,$$

where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.
- $h_A(x) := \mathrm{char}(\mathrm{Frob}_A)$ is a q-Weil polynomial and **isogeny invariant**.

Isogeny classification over $\mathbb{F}_q$

- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism, that induces an action

$$\mathrm{Frob}_A : T_\ell A \to T_\ell A \text{ for any } \ell \neq p,$$

where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.

- $h_A(x) := \mathrm{char}(\mathrm{Frob}_A)$ is a q-Weil polynomial and **isogeny invariant**.
- By **Honda-Tate** theory, the association

$$A \longmapsto h_A(x)$$

is injective up to isogeny and allows us to enumerate all AVs up to isogeny.

Isogeny classification over $\mathbb{F}_q$

- $A/\mathbb{F}_q$ comes with a **Frobenius** endomorphism, that induces an action

$$\mathrm{Frob}_A : T_\ell A \to T_\ell A \text{ for any } \ell \neq p,$$

where $T_\ell(A) = \varprojlim A[\ell^n] \simeq \mathbb{Z}_\ell^{2g}$.

- $h_A(x) := \mathrm{char}(\mathrm{Frob}_A)$ is a q-Weil polynomial and **isogeny invariant**.
- By **Honda-Tate** theory, the association

$$A \longmapsto h_A(x)$$

is injective up to isogeny and allows us to enumerate all AVs up to isogeny.

- Also, $h_A(x)$ is squarefree $\iff$ End(A) is commutative.

Deligne's equivalence

Recall: $A/\mathbb{F}_q$ is **ordinary** if half of the p-adic roots of h_A are units.

Deligne's equivalence

Recall: $A/\mathbb{F}_q$ is **ordinary** if half of the p-adic roots of h_A are units.

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an equivalence of categories:

$$\left\{ \textbf{Ordinary } \textit{abelian varieties over } \mathbb{F}_q \right\} \qquad\qquad A$$

Deligne's equivalence

Recall: $A/\mathbb{F}_q$ is **ordinary** if half of the p-adic roots of h_A are units.

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an equivalence of categories:

$$\left\{ \textbf{Ordinary } \textit{abelian varieties over } \mathbb{F}_q \right\} \qquad A$$
$$\updownarrow \qquad \qquad \downarrow$$
$$\left\{ \textit{pairs } (T, F), \textit{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \textit{ and } T \xrightarrow{F} T \textit{ s.t.} \right.$$

Deligne's equivalence

Recall: $A/\mathbb{F}_q$ is **ordinary** if half of the p-adic roots of h_A are units.

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an equivalence of categories:

$$
\begin{array}{cc}
\{\textbf{Ordinary}\ \textit{abelian varieties over}\ \mathbb{F}_q\} & A \\
\updownarrow & \mapsto \\
\left\{\begin{array}{l}
\textit{pairs } (T,F), \textit{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \textit{ and } T \xrightarrow{F} T \textit{ s.t.} \\
\textit{- } F \otimes \mathbb{Q} \textit{ is semisimple} \\
\textit{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \textit{ have abs. value } \sqrt{q} \\
\textit{- } \textbf{half of them are } p\textbf{-adic units} \\
\textit{- } \exists V : T \to T \textit{ such that } FV = VF = q
\end{array}\right\} & (T(A), F(A))
\end{array}
$$

Deligne's equivalence

Recall: $A/\mathbb{F}_q$ is **ordinary** if half of the p-adic roots of h_A are units.

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an equivalence of categories:

$$\left\{ \textbf{Ordinary } \textit{abelian varieties over } \mathbb{F}_q \right\} \qquad\qquad A$$

$$\updownarrow \qquad\qquad\qquad\qquad \downarrow$$

$$\left\{ \begin{array}{l} \textit{pairs } (T,F), \textit{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \textit{ and } T \xrightarrow{F} T \textit{ s.t.} \\ \textit{- } F \otimes \mathbb{Q} \textit{ is semisimple} \\ \textit{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \textit{ have abs. value } \sqrt{q} \\ \textit{- } \boldsymbol{\textit{half of them are } p\textit{-adic units}} \\ \textit{- } \exists V : T \to T \textit{ such that } FV = VF = q \end{array} \right\} \qquad (T(A), F(A))$$

- Ordinary $A/\mathbb{F}_q$ can be canonically lifted: $\rightsquigarrow \mathscr{A}_{\mathrm{can}}/\mathrm{Witt}(\mathbb{F}_q)$...

Deligne's equivalence

Recall: $A/\mathbb{F}_q$ is **ordinary** if half of the p-adic roots of h_A are units.

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an equivalence of categories:

$$\begin{array}{ccc} \left\{ \textbf{Ordinary } \textit{abelian varieties over } \mathbb{F}_q \right\} & & A \\ \updownarrow & & \downarrow \\ \left\{ \begin{array}{l} \textit{pairs } (T,F), \textit{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \textit{ and } T \xrightarrow{F} T \textit{ s.t.} \\ \textit{- } F \otimes \mathbb{Q} \textit{ is semisimple} \\ \textit{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \textit{ have abs. value } \sqrt{q} \\ \textit{- } \textbf{\textit{half of them are }} p\textbf{\textit{-adic units}} \\ \textit{- } \exists V : T \to T \textit{ such that } FV = VF = q \end{array} \right\} & & (T(A), F(A)) \end{array}$$

- Ordinary $A/\mathbb{F}_q$ can be canonically lifted: $\rightsquigarrow \mathscr{A}_{\mathrm{can}}/\mathrm{Witt}(\mathbb{F}_q)$...
- ... characterized by: $\mathrm{End}_{\mathbb{F}_q}(A) = \mathrm{End}_{\mathrm{Witt}(\mathbb{F}_q)}(\mathscr{A}_{\mathrm{can}})$.

Deligne's equivalence

Recall: $A/\mathbb{F}_q$ is **ordinary** if half of the p-adic roots of h_A are units.

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an equivalence of categories:

$$\left\{ \textbf{Ordinary } \textit{abelian varieties over } \mathbb{F}_q \right\} \qquad\qquad A$$

$$\updownarrow \qquad\qquad\qquad\qquad \mapsto$$

$$\left\{ \begin{array}{l} \textit{pairs } (T, F), \textit{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \textit{ and } T \xrightarrow{F} T \textit{ s.t.} \\ \textit{- } F \otimes \mathbb{Q} \textit{ is semisimple} \\ \textit{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \textit{ have abs. value } \sqrt{q} \\ \textit{- } \textbf{\textit{half of them are }} p\textbf{\textit{-adic units}} \\ \textit{- } \exists V : T \to T \textit{ such that } FV = VF = q \end{array} \right\} \qquad (T(A), F(A))$$

- Ordinary $A/\mathbb{F}_q$ can be canonically lifted: $\rightsquigarrow \mathscr{A}_{\mathrm{can}}/\mathrm{Witt}(\mathbb{F}_q)$...
- ... characterized by: $\mathrm{End}_{\mathbb{F}_q}(A) = \mathrm{End}_{\mathrm{Witt}(\mathbb{F}_q)}(\mathscr{A}_{\mathrm{can}})$.
- Put $T(A) := H_1(\mathscr{A}_{\mathrm{can}} \otimes \mathbb{C}, \mathbb{Z})$

Deligne's equivalence

Recall: $A/\mathbb{F}_q$ is **ordinary** if half of the p-adic roots of h_A are units.

Theorem (Deligne '69)

Let $q = p^r$, with p a prime. There is an equivalence of categories:

$$\begin{array}{ccc} \{\, \textbf{Ordinary } \textit{abelian varieties over } \mathbb{F}_q \} & & A \\ \updownarrow & & \downarrow \\ \left\{ \begin{array}{l} \textit{pairs } (T,F)\textit{, where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \textit{ and } T \xrightarrow{F} T \textit{ s.t.} \\ \textit{- } F \otimes \mathbb{Q} \textit{ is semisimple} \\ \textit{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \textit{ have abs. value } \sqrt{q} \\ \textit{- } \textbf{\textit{half of them are p-adic units}} \\ \textit{- } \exists V : T \to T \textit{ such that } FV = VF = q \end{array} \right\} & & (T(A), F(A)) \end{array}$$

- Ordinary $A/\mathbb{F}_q$ can be canonically lifted: $\rightsquigarrow \mathscr{A}_{\mathrm{can}}/\mathrm{Witt}(\mathbb{F}_q)$...
- ... characterized by: $\mathrm{End}_{\mathbb{F}_q}(A) = \mathrm{End}_{\mathrm{Witt}(\mathbb{F}_q)}(\mathscr{A}_{\mathrm{can}})$.
- Put $T(A) := H_1(\mathscr{A}_{\mathrm{can}} \otimes \mathbb{C}, \mathbb{Z})$ and $F(A) :=$ the induced Frobenius.

Squarefree case

- Fix an **ordinary squarefree** q-Weil polynomial h :

Squarefree case

- Fix an **ordinary squarefree** q-Weil polynomial h :
- $\rightsquigarrow$ an isogeny class $\mathscr{C}_h/\mathbb{F}_q$.

Squarefree case

- Fix an **ordinary squarefree** q-Weil polynomial h :
- $\rightsquigarrow$ an isogeny class $\mathscr{C}_h/\mathbb{F}_q$.
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$, an étale algebra = product of number fields.

Squarefree case

- Fix an **ordinary squarefree** q-Weil polynomial h :
- $\rightsquigarrow$ an isogeny class $\mathscr{C}_h/\mathbb{F}_q$.
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$, an étale algebra = product of number fields.
- Put $V = q/F$. Deligne's equivalence induces:

Squarefree case

- Fix an **ordinary squarefree** q-Weil polynomial h :
- $\rightsquigarrow$ an isogeny class $\mathscr{C}_h/\mathbb{F}_q$.
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$, an étale algebra = product of number fields.
- Put $V = q/F$. Deligne's equivalence induces:

Theorem

$$\left\{\text{abelian varieties over } \mathbb{F}_q \text{ in } \mathscr{C}_h\right\}_{/\simeq}$$
$$\updownarrow$$
$$\left\{\text{fractional ideals of } \mathbb{Z}[F,V] \subset K\right\}_{/\simeq}$$

Squarefree case

- Fix an **ordinary squarefree** q-Weil polynomial h :
- $\rightsquigarrow$ an isogeny class $\mathscr{C}_h/\mathbb{F}_q$.
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$, an étale algebra = product of number fields.
- Put $V = q/F$. Deligne's equivalence induces:

Theorem

$$\left\{\textit{abelian varieties over } \mathbb{F}_q \textit{ in } \mathscr{C}_h\right\}_{/\simeq}$$
$$\updownarrow$$
$$\left\{\textit{fractional ideals of } \mathbb{Z}[F,V] \subset K\right\}_{/\simeq} \quad =: \mathrm{ICM}(\mathbb{Z}[F,V])$$

ideal class monoid

Squarefree case

- Fix an **ordinary squarefree** q-Weil polynomial h :
- $\rightsquigarrow$ an isogeny class $\mathscr{C}_h/\mathbb{F}_q$.
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$, an étale algebra = product of number fields.
- Put $V = q/F$. Deligne's equivalence induces:

Theorem

$$\left\{\textit{abelian varieties over } \mathbb{F}_q \textit{ in } \mathscr{C}_h\right\}_{/\simeq}$$

$$\updownarrow$$

$$\left\{\textit{fractional ideals of } \mathbb{Z}[F,V] \subset K\right\}_{/\simeq} \qquad =: \mathrm{ICM}(\mathbb{Z}[F,V])$$

ideal class monoid

- Problem: $\mathbb{Z}[F,V]$ might not be maximal $\rightsquigarrow$ non-invertible ideals.

ICM : Ideal Class Monoid

Let R be an **order** in an étale $\mathbb{Q}$-algebra K.

ICM : Ideal Class Monoid

Let R be an **order** in an étale $\mathbb{Q}$-algebra K.

- Recall: for **fractional** R**-ideals** I and J

$$I \simeq_R J \Longleftrightarrow \exists x \in K^\times \text{ s.t. } xI = J$$

ICM : Ideal Class Monoid

Let R be an **order** in an étale $\mathbb{Q}$-algebra K.

- Recall: for **fractional** R**-ideals** I and J

$$I \simeq_R J \iff \exists x \in K^\times \text{ s.t. } xI = J$$

- We have

$$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R) = {}^{\{\text{invertible fractional } R\text{-ideals}\}}\!\big/_{\simeq_R}$$

with equality $\Updownarrow$ iff $R = \mathcal{O}_K$

ICM : Ideal Class Monoid

Let R be an **order** in an étale $\mathbb{Q}$-algebra K.

- Recall: for **fractional** R**-ideals** I and J

$$I \simeq_R J \iff \exists x \in K^\times \text{ s.t. } xI = J$$

- We have

$$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R) = {\{\text{invertible fractional } R\text{-ideals}\}}\big/{\simeq_R}$$

with equality $\updownarrow$ iff $R = \mathcal{O}_K$

- ...and actually

$$\mathrm{ICM}(R) \supseteq \bigsqcup_{\substack{R \subseteq S \subseteq \mathcal{O}_K \\ \text{over-orders}}} \mathrm{Pic}(S) \qquad \text{with equality iff } R \text{ is Bass}$$

ICM : Ideal Class Monoid

Let R be an **order** in an étale $\mathbb{Q}$-algebra K.

- Recall: for **fractional** R**-ideals** I and J

$$I \simeq_R J \Longleftrightarrow \exists x \in K^\times \text{ s.t. } xI = J$$

- We have

$$\mathrm{ICM}(R) \supseteq \mathrm{Pic}(R) = {}^{\{\text{invertible fractional } R\text{-ideals}\}}\big/_{\simeq_R}$$

with equality $\updownarrow$ iff $R = \mathscr{O}_K$

- ...and actually

$$\mathrm{ICM}(R) \supseteq \bigsqcup_{\substack{R \subseteq S \subseteq \mathscr{O}_K \\ \text{over-orders}}} \mathrm{Pic}(S) \qquad \text{with equality iff } R \text{ is Bass}$$

- Hofmann-Sircana : computation of over-orders.

simplify the problem

First, locally: Dade-Taussky-Zassenhaus.

simplify the problem

First, locally: Dade-Taussky-Zassenhaus.

- **weak equivalence**:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

simplify the problem

First, locally: Dade-Taussky-Zassenhaus.

- **weak equivalence**:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

$$\Updownarrow$$

$$1 \in (I : J)(J : I) \quad \text{easy to check!}$$

simplify the problem

First, locally: Dade-Taussky-Zassenhaus.

- **weak equivalence**:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \mathrm{mSpec}(R)$$

$$\Updownarrow$$

$$1 \in (I : J)(J : I) \quad \text{easy to check!}$$

- Let $\mathscr{W}(R)$ be the set of weak eq. classes...

simplify the problem

First, locally: Dade-Taussky-Zassenhaus.

- **weak equivalence**:

$$I_{\mathfrak{p}} \simeq_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \text{ for every } \mathfrak{p} \in \operatorname{mSpec}(R)$$

$$\Updownarrow$$

$$1 \in (I : J)(J : I)$$ easy to check!

- Let $\mathscr{W}(R)$ be the set of weak eq. classes...
  ...whose representatives can be found in

$$\left\{ \text{sub-}R\text{-modules of } {}^{\mathscr{O}_K}\!\big/_{\mathfrak{f}_R} \right\}$$ finite! and most of the time not-too-big ...

  where $\mathfrak{f}_R = (R : \mathscr{O}_K)$ is the conductor of R.

Compute ICM(R)

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathscr{W}_S(R)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathrm{ICM}_S(R)$$

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathscr{W}_S(R)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathrm{ICM}_S(R)$$

the "pedix" $-_S$ means "only classes with multiplicator ring S"

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

$$\mathscr{W}(R) = \bigsqcup_{R\subseteq S\subseteq \mathscr{O}_K} \mathscr{W}_S(R)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R\subseteq S\subseteq \mathscr{O}_K} \mathrm{ICM}_S(R)$$

the "pedix" $-_S$ means "only classes with multiplicator ring S"

Theorem (M.)

For every over-order S of R, $\mathrm{Pic}(S)$ acts freely on $\mathrm{ICM}_S(R)$ and

$$\mathscr{W}_S(R) = \mathrm{ICM}_S(R)/\mathrm{Pic}(S)$$

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

$$\mathscr{W}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathscr{W}_S(R)$$

$$\mathrm{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathscr{O}_K} \mathrm{ICM}_S(R)$$

the "pedix" $-_S$ means "only classes with multiplicator ring S"

Theorem (M.)

For every over-order S of R, $\mathrm{Pic}(S)$ acts freely on $\mathrm{ICM}_S(R)$ and

$$\mathscr{W}_S(R) = \mathrm{ICM}_S(R) / \mathrm{Pic}(S)$$

Repeat for every $R \subseteq S \subseteq \mathscr{O}_K$:

$$\rightsquigarrow \mathrm{ICM}(R).$$

To sum up:

- To sum up:

To sum up:

- To sum up:
- Given a **ordinary squarefree** q-Weil polynomial h ...

To sum up:

- To sum up:
- Given a **ordinary squarefree** q-Weil polynomial h ...
- ... $\rightsquigarrow$ algorithm to compute the isomorphism classes of AVs in $\mathscr{C}_h$.

To sum up:

- To sum up:
- Given a **ordinary squarefree** q-Weil polynomial h ...
- ... $\rightsquigarrow$ algorithm to compute the isomorphism classes of AVs in $\mathscr{C}_h$.
- What about polarizations?

Dual varieties and Polarizations

Howe : **dual** varieties and **polarizations** on Deligne modules.

Dual varieties and Polarizations

Howe : **dual** varieties and **polarizations** on Deligne modules.

Theorem (M.)

Let $A \in \mathscr{C}_h$ with h ordinary and squarefree. If $A \leftrightarrow I$, set $S = (I : I)$, then:

Dual varieties and Polarizations

Howe : **dual** varieties and **polarizations** on Deligne modules.

Theorem (M.)

Let $A \in \mathscr{C}_h$ with h ordinary and squarefree. If $A \leftrightarrow I$, set $S = (I : I)$, then:

- $A^\vee \leftrightarrow \overline{I}^t := \{\overline{x} \in K : \mathrm{Tr}(xI) \subseteq \mathbb{Z}\}$.

Dual varieties and Polarizations

Howe : **dual** varieties and **polarizations** on Deligne modules.

Theorem (M.)

Let $A \in \mathscr{C}_h$ with h ordinary and squarefree. If $A \leftrightarrow I$, set $S = (I : I)$, then:

- $A^\vee \leftrightarrow \overline{I}^t := \{\overline{x} \in K : \mathrm{Tr}(xI) \subseteq \mathbb{Z}\}$.
- *a polarization μ of A corresponds to a $\lambda \in K^\times$ such that*
  - $\lambda I \subseteq \overline{I}^t$ *(isogeny of* $\deg \mu = [\overline{I}^t : \lambda I]$*);*
  - λ *is totally imaginary* ($\overline{\lambda} = -\lambda$)*;*
  - λ *is* Φ*-positive* ($\Im\varphi(\lambda) > 0$ *for all* $\varphi \in \Phi$)*,*

  where Φ is a CM-type of K satisf. the Shimura-Taniyama formula.

Dual varieties and Polarizations

Howe : **dual** varieties and **polarizations** on Deligne modules.

Theorem (M.)

Let $A \in \mathscr{C}_h$ with h ordinary and squarefree. If $A \leftrightarrow I$, set $S = (I : I)$, then:

- $A^\vee \leftrightarrow \overline{I}^t := \{\overline{x} \in K : \mathrm{Tr}(xI) \subseteq \mathbb{Z}\}$.
- *a polarization μ of A corresponds to a $\lambda \in K^\times$ such that*
  - $\lambda I \subseteq \overline{I}^t$ *(isogeny of* $\deg \mu = [\overline{I}^t : \lambda I]$*);*
  - λ *is totally imaginary* ($\overline{\lambda} = -\lambda$)*;*
  - λ *is Φ-positive* ($\Im\varphi(\lambda) > 0$ *for all* $\varphi \in \Phi$*),*

  where Φ is a CM-type of K satisf. the Shimura-Taniyama formula.
- *if $(A, \mu) \leftrightarrow (I, \lambda)$ is a princ. polarized ab. var. and $S = (I : I)$ then*

$$\left\{\begin{matrix} \text{non-isomorphic princ.} \\ \text{polarizations of } A \end{matrix}\right\} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{v\overline{v} : v \in S^\times\}},$$

Dual varieties and Polarizations

Howe : **dual** varieties and **polarizations** on Deligne modules.

Theorem (M.)

Let $A \in \mathscr{C}_h$ with h ordinary and squarefree. If $A \leftrightarrow I$, set $S = (I : I)$, then:

- $A^\vee \leftrightarrow \overline{I}^t := \{\overline{x} \in K : \mathrm{Tr}(xI) \subseteq \mathbb{Z}\}$.
- *a polarization μ of A corresponds to a $\lambda \in K^\times$ such that*
  - $\lambda I \subseteq \overline{I}^t$ *(isogeny of* $\deg \mu = [\overline{I}^t : \lambda I]$*);*
  - λ *is totally imaginary* $(\overline{\lambda} = -\lambda)$*;*
  - λ *is* Φ*-positive* $(\Im\varphi(\lambda) > 0$ *for all* $\varphi \in \Phi)$*,*

  where Φ is a CM-type of K satisf. the Shimura-Taniyama formula.
- *if $(A, \mu) \leftrightarrow (I, \lambda)$ is a princ. polarized ab. var. and $S = (I : I)$ then*

$$\left\{\begin{matrix}\text{non-isomorphic princ.}\\ \text{polarizations of } A\end{matrix}\right\} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{v\overline{v} : v \in S^\times\}},$$

similar statement for $\deg \mu > 1$

Dual varieties and Polarizations

Howe : **dual** varieties and **polarizations** on Deligne modules.

Theorem (M.)

Let $A \in \mathscr{C}_h$ with h ordinary and squarefree. If $A \leftrightarrow I$, set $S = (I : I)$, then:

- $A^\vee \leftrightarrow \overline{I}^t := \{\overline{x} \in K : \mathrm{Tr}(xI) \subseteq \mathbb{Z}\}$.
- *a polarization μ of A corresponds to a $\lambda \in K^\times$ such that*
  - $\lambda I \subseteq \overline{I}^t$ *(isogeny of* $\deg \mu = [\overline{I}^t : \lambda I]$*);*
  - λ *is totally imaginary* ($\overline{\lambda} = -\lambda$)*;*
  - λ *is* Φ*-positive* ($\Im\varphi(\lambda) > 0$ *for all* $\varphi \in \Phi$*),*

  where Φ is a CM-type of K satisf. the Shimura-Taniyama formula.
- *if $(A,\mu) \leftrightarrow (I,\lambda)$ is a princ. polarized ab. var. and $S = (I : I)$ then*

$$\left\{\begin{matrix}\text{non-isomorphic princ.}\\ \text{polarizations of } A\end{matrix}\right\} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{v\overline{v} : v \in S^\times\}},$$

similar statement for $\deg \mu > 1$

- *and* $\mathrm{Aut}(A,\mu) = \{\text{torsion units of } S\}$.

Principal Polarizations

We have an **algorithm** to enumerate principal polarizations up to isomorphism:

Principal Polarizations

We have an **algorithm** to enumerate principal polarizations up to isomorphism:

1. Compute i_0 such that $i_0 I = \overline{I}^t$.

Principal Polarizations

We have an **algorithm** to enumerate principal polarizations up to isomorphism:

1. Compute i_0 such that $i_0 I = \overline{I}^t$.
2. Loop over the representatives u of the finite quotient

$$\frac{S^\times}{\{v\overline{v} : v \in S^\times\}}.$$

Principal Polarizations

We have an **algorithm** to enumerate principal polarizations up to isomorphism:

1. Compute i_0 such that $i_0 I = \overline{I}^t$.
2. Loop over the representatives u of the finite quotient
$$\frac{S^\times}{\{v\overline{v} : v \in S^\times\}}.$$
3. If $\lambda := i_0 u$ is totally imaginary and Φ-positive ...

Principal Polarizations

We have an **algorithm** to enumerate principal polarizations up to isomorphism:

1. Compute i_0 such that $i_0 I = \overline{I}^t$.
2. Loop over the representatives u of the finite quotient
$$\frac{S^\times}{\{v\overline{v} : v \in S^\times\}}.$$
3. If $\lambda := i_0 u$ is totally imaginary and Φ-positive ...
4. ... then we have one principal polarization.

Principal Polarizations

We have an **algorithm** to enumerate principal polarizations up to isomorphism:

1. Compute i_0 such that $i_0 I = \overline{I}^t$.
2. Loop over the representatives u of the finite quotient
$$\frac{S^\times}{\{v\overline{v} : v \in S^\times\}}.$$
3. If $\lambda := i_0 u$ is totally imaginary and Φ-positive ...
4. ... then we have one principal polarization.
5. By the previous Theorem, we have all princ. polarizations up to isom.

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81.$

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$.
- $\rightsquigarrow$ isogeny class of an simple ordinary abelian varieties over $\mathbb{F}_3$ of dimension 4.

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$.
- $\rightsquigarrow$ isogeny class of an simple ordinary abelian varieties over $\mathbb{F}_3$ of dimension 4.
- Let F be a root of $h(x)$ and put $R := \mathbb{Z}[F, 3/F] \subset \mathbb{Q}(F)$.

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$.
- $\rightsquigarrow$ isogeny class of an simple ordinary abelian varieties over $\mathbb{F}_3$ of dimension 4.
- Let F be a root of $h(x)$ and put $R := \mathbb{Z}[F, 3/F] \subset \mathbb{Q}(F)$.
- 8 over-orders of R: two of them are not Gorenstein.

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$.
- $\rightsquigarrow$ isogeny class of an simple ordinary abelian varieties over $\mathbb{F}_3$ of dimension 4.
- Let F be a root of $h(x)$ and put $R := \mathbb{Z}[F, 3/F] \subset \mathbb{Q}(F)$.
- 8 over-orders of R: two of them are not Gorenstein.
- $\#\mathrm{ICM}(R) = 18 \rightsquigarrow 18$ isom. classes of AV in the isogeny class.

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$.
- $\rightsquigarrow$ isogeny class of an simple ordinary abelian varieties over $\mathbb{F}_3$ of dimension 4.
- Let F be a root of $h(x)$ and put $R := \mathbb{Z}[F, 3/F] \subset \mathbb{Q}(F)$.
- 8 over-orders of R: two of them are not Gorenstein.
- $\#\mathrm{ICM}(R) = 18 \rightsquigarrow 18$ isom. classes of AV in the isogeny class.
- 5 are not invertible in their multiplicator ring.

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$.
- $\rightsquigarrow$ isogeny class of an simple ordinary abelian varieties over $\mathbb{F}_3$ of dimension 4.
- Let F be a root of $h(x)$ and put $R := \mathbb{Z}[F, 3/F] \subset \mathbb{Q}(F)$.
- 8 over-orders of R: two of them are not Gorenstein.
- $\#\mathrm{ICM}(R) = 18 \rightsquigarrow 18$ isom. classes of AV in the isogeny class.
- 5 are not invertible in their multiplicator ring.
- 8 classes admit principal polarizations.

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$.
- $\rightsquigarrow$ isogeny class of an simple ordinary abelian varieties over $\mathbb{F}_3$ of dimension 4.
- Let F be a root of $h(x)$ and put $R := \mathbb{Z}[F, 3/F] \subset \mathbb{Q}(F)$.
- 8 over-orders of R: two of them are not Gorenstein.
- $\#\mathrm{ICM}(R) = 18 \rightsquigarrow 18$ isom. classes of AV in the isogeny class.
- 5 are not invertible in their multiplicator ring.
- 8 classes admit principal polarizations.
- 10 isomorphism classes of princ. polarized AV.

Example

Concretely:

$$\begin{aligned} I_1 = & 2645633792595191\mathbb{Z} \oplus (F + 836920075614551)\mathbb{Z} \oplus (F^2 + 1474295643839839)\mathbb{Z}\oplus \\ & \oplus (F^3 + 1372829830503387)\mathbb{Z} \oplus (F^4 + 1072904687510)\mathbb{Z}\oplus \\ & \oplus \frac{1}{3}(F^5 + F^4 + F^3 + 2F^2 + 2F + 670480698614361\,0)\mathbb{Z}\oplus \\ & \oplus \frac{1}{9}(F^6 + F^5 + F^4 + 8F^3 + 2F^2 + 2991665243621169)\mathbb{Z}\oplus \\ & \oplus \frac{1}{27}(F^7 + F^6 + F^5 + 17F^4 + 20F^3 + 9F^2 + 6801531251872220\,1)\mathbb{Z} \end{aligned}$$

principal polarizations:

$$\begin{aligned} x_{1,1} = & \frac{1}{27}(-121922F^7 + 588604F^6 - 1422437F^5 + \\ & + 1464239F^4 + 1196576F^3 - 7570722F^2 + 15316479F - 12821193) \\ x_{1,2} = & \frac{1}{27}(3015467F^7 - 17689816F^6 + 35965592F^5 - \\ & - 64660346F^4 + 121230619F^3 - 191117052F^2 + 315021546F - 300025458) \end{aligned}$$

$\mathrm{End}(I_1) = R$

$\#\mathrm{Aut}(I_1, x_{1,1}) = \#\mathrm{Aut}(I_1, x_{1,2}) = 2$

Example

$$
\begin{aligned}
I_7 =& 2\mathbb{Z} \oplus (F+1)\mathbb{Z} \oplus (F^2+1)\mathbb{Z} \oplus (F^3+1)\mathbb{Z} \oplus (F^4+1)\mathbb{Z} \oplus \frac{1}{3}(F^5+F^4+F^3+2F^2+2F+3)\mathbb{Z}\oplus \\
& \oplus \frac{1}{36}(F^6+F^5+10F^4+26F^3+2F^2+27F+45)\mathbb{Z}\oplus \\
& \oplus \frac{1}{216}(F^7+4F^6+49F^5+200F^4+116F^3+105F^2+198F+351)\mathbb{Z}
\end{aligned}
$$

principal polarization:

$$
x_{7,1} = \frac{1}{54}(20F^7 - 43F^6 + 155F^5 - 308F^4 + 580F^3 - 1116F^2 + 2205F - 1809)
$$

$$
\begin{aligned}
\mathrm{End}(I_7) = & \mathbb{Z} \oplus F\mathbb{Z} \oplus F^2\mathbb{Z} \oplus F^3\mathbb{Z} \oplus F^4\mathbb{Z} \oplus \frac{1}{3}(F^5+F^4+F^3+2F^2+2F)\mathbb{Z}\oplus \\
& \oplus \frac{1}{18}(F^6+F^5+10F^4+8F^3+2F^2+9F+9)\mathbb{Z}\oplus \\
& \oplus \frac{1}{108}(F^7+4F^6+13F^5+56F^4+80F^3+33F^2+18F+27)\mathbb{Z}
\end{aligned}
$$

$$\#\mathrm{Aut}(I_7, x_{7,1}) = 2$$

I_1 is invertible in R, but I_7 is not invertible in $\mathrm{End}(I_7)$.

Outside of the ordinary...

Outside of the ordinary...

Theorem (Centeleghe-Stix '15)

There is an equivalence of categories:

$$\begin{array}{ccc}
\{\text{abelian varieties } A \text{ over } \mathbb{F}_p \text{ with } \boldsymbol{h_A(\sqrt{p}) \neq 0}\} & & A \\
\updownarrow & & \downarrow \\
\left\{\begin{array}{l}
\text{pairs } (T, F), \text{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \text{ and } T \xrightarrow{F} T \text{ s.t.} \\
\text{- } F \otimes \mathbb{Q} \text{ is semisimple} \\
\text{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \text{ have abs. value } \sqrt{p} \\
\text{- } \boldsymbol{\mathrm{char}_F(\sqrt{p}) \neq 0} \\
\text{- } \exists V : T \to T \text{ such that } FV = VF = p
\end{array}\right\} & & (T(A), F(A))
\end{array}$$

Outside of the ordinary...

Theorem (Centeleghe-Stix '15)

There is an equivalence of categories:

$$\begin{array}{ccc} \{\text{abelian varieties } A \text{ over } \mathbb{F}_p \text{ with } \boldsymbol{h_A(\sqrt{p}) \neq 0}\} & & A \\ \updownarrow & & \downarrow \\ \left\{\begin{array}{l} \text{pairs } (T,F), \text{ where } T \simeq_{\mathbb{Z}} \mathbb{Z}^{2g} \text{ and } T \xrightarrow{F} T \text{ s.t.} \\ \text{- } F \otimes \mathbb{Q} \text{ is semisimple} \\ \text{- the roots of } \mathrm{char}_{F\otimes\mathbb{Q}}(x) \text{ have abs. value } \sqrt{p} \\ \text{- } \boldsymbol{\mathrm{char}_F(\sqrt{p}) \neq 0} \\ \text{- } \exists V : T \to T \text{ such that } FV = VF = p \end{array}\right\} & & (T(A), F(A)) \end{array}$$

- Now, $T(A) := \mathrm{Hom}(A, A_w)$, where A_w has minimal End among the varieties with Weil support $w = w(A)$.
- $F(A)$ is the induced Frobenius.

Outside of the ordinary...isomorphism classes

- Everything I told so far about isomorphism classes works in the same way using the Centeleghe-Stix functor.

Outside of the ordinary...isomorphism classes

- Everything I told so far about isomorphism classes works in the same way using the Centeleghe-Stix functor.

Outside of the ordinary...isomorphism classes

- Everything I told so far about isomorphism classes works in the same way using the Centeleghe-Stix functor.
- For polarizations, the results by Howe do not apply immediately to the Centeleghe-Strix case:

Outside of the ordinary...isomorphism classes

- Everything I told so far about isomorphism classes works in the same way using the Centeleghe-Stix functor.
- For polarizations, the results by Howe do not apply immediately to the Centeleghe-Strix case:
- in general we cannot lift canonically each abelian variety.

Outside of the ordinary...polarizations

- New strategy: jt. Jonas Bergström and Valentijn Karemaker.

Outside of the ordinary...polarizations

- New strategy: jt. Jonas Bergström and Valentijn Karemaker.
- Consider $\mathscr{C}_h$ with h squarefree $/\mathbb{F}_q \rightsquigarrow K = \mathbb{Q}[F]$.

Outside of the ordinary...polarizations

- New strategy: jt. Jonas Bergström and Valentijn Karemaker.
- Consider $\mathscr{C}_h$ with h squarefree $/\mathbb{F}_q \rightsquigarrow K = \mathbb{Q}[F]$.
- Chai-Conrad-Oort: A (p-adic) CM-type (K, Φ) satisfies the **Residual Reflex Condition** if:

Outside of the ordinary...polarizations

- New strategy: jt. Jonas Bergström and Valentijn Karemaker.
- Consider $\mathscr{C}_h$ with h squarefree $/\mathbb{F}_q \rightsquigarrow K = \mathbb{Q}[F]$.
- Chai-Conrad-Oort: A (p-adic) CM-type (K, Φ) satisfies the **Residual Reflex Condition** if:
  1. the Shimura-Taniyama formula holds for Φ.

Outside of the ordinary...polarizations

- New strategy: jt. Jonas Bergström and Valentijn Karemaker.
- Consider $\mathscr{C}_h$ with h squarefree $/\mathbb{F}_q \rightsquigarrow K = \mathbb{Q}[F]$.
- Chai-Conrad-Oort: A (p-adic) CM-type (K, Φ) satisfies the **Residual Reflex Condition** if:
  1. the Shimura-Taniyama formula holds for Φ.
  2. the residuel field k_E of the reflex field E of (K, Φ) satisfies: $k_E \subseteq \mathbb{F}_q$.

Outside of the ordinary...polarizations

- New strategy: jt. Jonas Bergström and Valentijn Karemaker.
- Consider $\mathscr{C}_h$ with h squarefree $/\mathbb{F}_q \rightsquigarrow K = \mathbb{Q}[F]$.
- Chai-Conrad-Oort: A (p-adic) CM-type (K,Φ) satisfies the **Residual Reflex Condition** if:
  1. the Shimura-Taniyama formula holds for Φ.
  2. the residuel field k_E of the reflex field E of (K,Φ) satisfies: $k_E \subseteq \mathbb{F}_q$.

Theorem (Chai-Conrad-Oort)

If (K,Φ) satisfies the RRC then in $\mathscr{C}_h$ there exists an abelian variety A admitting a canonical lifting $\mathscr{A}$.

Outside of the ordinary...polarizations

- New strategy: jt. Jonas Bergström and Valentijn Karemaker.
- Consider $\mathscr{C}_h$ with h squarefree $/\mathbb{F}_q \rightsquigarrow K = \mathbb{Q}[F]$.
- Chai-Conrad-Oort: A (p-adic) CM-type (K, Φ) satisfies the **Residual Reflex Condition** if:
  1. the Shimura-Taniyama formula holds for Φ.
  2. the residuel field k_E of the reflex field E of (K, Φ) satisfies: $k_E \subseteq \mathbb{F}_q$.

Theorem (Chai-Conrad-Oort)

If (K, Φ) satisfies the RRC then in $\mathscr{C}_h$ there exists an abelian variety A admitting a canonical lifting $\mathscr{A}$.

- If we understand the polarizations of A we can 'spread' them to the whole isogeny class.

Outside of the ordinary...polarizations

Now $\mathscr{C}_h$ over $\mathbb{F}_p$: let $\mathscr{G}$ be the Centeleghe-Stix functor.
Assume that there exists A admitting a canonical lifting $\mathscr{A}$.

Outside of the ordinary...polarizations

Now $\mathscr{C}_h$ over $\mathbb{F}_p$: let $\mathscr{G}$ be the Centeleghe-Stix functor.
Assume that there exists A admitting a canonical lifting $\mathscr{A}$.

$$\begin{tikzcd}
\mathrm{Hom}(\mathscr{A},\mathscr{A}^\vee) \arrow[d, "\text{red}"] \arrow[dr, "\text{complex unif.}"] & \\
\mathrm{Hom}(A,A^\vee) & (\bar{I}^t : I)
\end{tikzcd}$$

Outside of the ordinary...polarizations

Now $\mathscr{C}_h$ over $\mathbb{F}_p$: let $\mathscr{G}$ be the Centeleghe-Stix functor.
Assume that there exists A admitting a canonical lifting $\mathscr{A}$.

$$
\begin{tikzcd}
\mathrm{Hom}(\mathscr{A},\mathscr{A}^\vee) \arrow[d, "\text{red}"] \arrow[drr, "\text{complex unif.}"] & & \\
\mathrm{Hom}(A,A^\vee) \arrow[d, "\mathscr{G}"] & & (\bar{I}^t : I) \arrow[d, "\simeq"', "{\color{red}\alpha=\bar{\alpha}}"] \\
(\mathscr{G}(A):\mathscr{G}(A^\vee)) \arrow[rr, equal] & & (\bar{I}^t : I)
\end{tikzcd}
$$

Outside of the ordinary...polarizations

Now $\mathscr{C}_h$ over $\mathbb{F}_p$: let $\mathscr{G}$ be the Centeleghe-Stix functor.
Assume that there exists A admitting a canonical lifting $\mathscr{A}$.
Let $f : A \to B$ be an isogeny.

$$\begin{tikzcd}
 & \mathrm{Hom}(\mathscr{A}, \mathscr{A}^\vee) \arrow[d, "\mathrm{red}"] \arrow[dr, "\text{complex unif.}"] & \\
\mathrm{Hom}(B, B^\vee) \arrow[r, "f^* := f^\vee \circ - \circ f"] & \mathrm{Hom}(A, A^\vee) \arrow[d, "\mathscr{G}"] & (\bar{I}^t : I) \arrow[d, "\simeq"', "\color{red}{\alpha = \overline{\alpha}}"] \\
 & (\mathscr{G}(A) : \mathscr{G}(A^\vee)) \arrow[r, equal] & (\bar{I}^t : I)
\end{tikzcd}$$

Outside of the ordinary...polarizations

Now $\mathscr{C}_h$ over $\mathbb{F}_p$: let $\mathscr{G}$ be the Centeleghe-Stix functor.
Assume that there exists A admitting a canonical lifting $\mathscr{A}$.
Let $f : A \to B$ be an isogeny.

$$\begin{tikzcd}
 & \mathrm{Hom}(\mathscr{A},\mathscr{A}^\vee) \arrow[d, "\text{red}"] \arrow[dr, "\text{complex unif.}"] & \\
\mathrm{Hom}(B,B^\vee) \arrow[r, "f^*:=f^\vee\circ - \circ f"] \arrow[d, "\mathscr{G}"] & \mathrm{Hom}(A,A^\vee) \arrow[d, "\mathscr{G}"] & (\overline{I}^t : I) \arrow[d, "\alpha=\overline{\alpha}", "\simeq"'] \\
(\mathscr{G}(B):\mathscr{G}(B^\vee)) \arrow[r, "\mathscr{G}(f^*)"] & (\mathscr{G}(A):\mathscr{G}(A^\vee)) \arrow[r, equal] & (\overline{I}^t : I)
\end{tikzcd}$$

Outside of the ordinary...polarizations

Now $\mathscr{C}_h$ over $\mathbb{F}_p$: let $\mathscr{G}$ be the Centeleghe-Stix functor.
Assume that there exists A admitting a canonical lifting $\mathscr{A}$.
Let $f : A \to B$ be an isogeny.

$$
\begin{tikzcd}
 & \mathrm{Hom}(\mathscr{A},\mathscr{A}^\vee) \arrow[d, "\text{red}"] \arrow[dr, "\text{complex unif.}"] & \\
\mathrm{Hom}(B,B^\vee) \arrow[r, "f^*:=f^\vee\circ-\circ f"] \arrow[d, "\mathscr{G}"] & \mathrm{Hom}(A,A^\vee) \arrow[d, "\mathscr{G}"] & (\bar{I}^t : I) \arrow[d, "\simeq"', "\color{red}\alpha=\overline{\alpha}"] \\
(\mathscr{G}(B):\mathscr{G}(B^\vee)) \arrow[r, "\mathscr{G}(f^*)"] & (\mathscr{G}(A):\mathscr{G}(A^\vee)) \arrow[r, equal] & (\bar{I}^t : I)
\end{tikzcd}
$$

Note that $\mathscr{G}(f^*)$ is multiplication by the totally positive element $\overline{\mathscr{G}(f)}\mathscr{G}(f)$:

Outside of the ordinary...polarizations

Now $\mathscr{C}_h$ over $\mathbb{F}_p$: let $\mathscr{G}$ be the Centeleghe-Stix functor.
Assume that there exists A admitting a canonical lifting $\mathscr{A}$.
Let $f : A \to B$ be an isogeny.

$$\begin{tikzcd}
 & \mathrm{Hom}(\mathscr{A}, \mathscr{A}^\vee) \arrow[d, "\mathrm{red}"] \arrow[dr, "\text{complex unif.}"] & \\
\mathrm{Hom}(B, B^\vee) \arrow[r, "f^* := f^\vee \circ - \circ f"] \arrow[d, "\mathscr{G}"] & \mathrm{Hom}(A, A^\vee) \arrow[d, "\mathscr{G}"] & (\bar{I}^t : I) \arrow[d, "\alpha = \overline{\alpha}", "\simeq"'] \\
(\mathscr{G}(B) : \mathscr{G}(B^\vee)) \arrow[r, "\mathscr{G}(f^*)"] & (\mathscr{G}(A) : \mathscr{G}(A^\vee)) \arrow[r, equal] & (\bar{I}^t : I)
\end{tikzcd}$$

Note that $\mathscr{G}(f^*)$ is multiplication by the totally positive element $\overline{\mathscr{G}(f)}\mathscr{G}(f)$: it sends totally imaginary elements to totally imaginary elements and Φ-positive elements to Φ-positive elements.

Outside of the ordinary...polarizations

Now $\mathscr{C}_h$ over $\mathbb{F}_p$: let $\mathscr{G}$ be the Centeleghe-Stix functor.
Assume that there exists A admitting a canonical lifting $\mathscr{A}$.
Let $f : A \to B$ be an isogeny.

$$\begin{tikzcd}
 & \mathrm{Hom}(\mathscr{A},\mathscr{A}^\vee) \arrow[d, "\text{red}"] \arrow[dr, "\text{complex unif.}"] & \\
\mathrm{Hom}(B,B^\vee) \arrow[r, "f^*:=f^\vee\circ-\circ f"] \arrow[d, "\mathscr{G}"] & \mathrm{Hom}(A,A^\vee) \arrow[d, "\mathscr{G}"] & (\bar{I}^t : I) \arrow[d, "\simeq"', "\color{red}\alpha=\overline{\alpha}"] \\
(\mathscr{G}(B):\mathscr{G}(B^\vee)) \arrow[r, "\mathscr{G}(f^*)"] & (\mathscr{G}(A):\mathscr{G}(A^\vee)) \arrow[r, equal] & (\bar{I}^t : I)
\end{tikzcd}$$

Note that $\mathscr{G}(f^*)$ is multiplication by the totally positive element $\overline{\mathscr{G}(f)}\mathscr{G}(f)$: it sends totally imaginary elements to totally imaginary elements and Φ-positive elements to Φ-positive elements. The only 'issue' is the $\color{red}\alpha$.

Outside of the ordinary...polarizations

Now $\mathscr{C}_h$ over $\mathbb{F}_p$: let $\mathscr{G}$ be the Centeleghe-Stix functor.
Assume that there exists A admitting a canonical lifting $\mathscr{A}$.
Let $f : A \to B$ be an isogeny.

$$\begin{tikzcd}
 & \mathrm{Hom}(\mathscr{A},\mathscr{A}^\vee) \arrow[d, "\mathrm{red}"] \arrow[dr, "\text{complex unif.}"] & \\
\mathrm{Hom}(B,B^\vee) \arrow[r, "f^*:=f^\vee\circ-\circ f"] \arrow[d, "\mathscr{G}"] & \mathrm{Hom}(A,A^\vee) \arrow[d, "\mathscr{G}"] & (\bar{I}^t : I) \arrow[d, "\simeq"', "\alpha=\overline{\alpha}"] \\
(\mathscr{G}(B):\mathscr{G}(B^\vee)) \arrow[r, "\mathscr{G}(f^*)"] & (\mathscr{G}(A):\mathscr{G}(A^\vee)) \arrow[r, equal] & (\bar{I}^t : I)
\end{tikzcd}$$

Note that $\mathscr{G}(f^*)$ is multiplication by the totally positive element $\overline{\mathscr{G}(f)}\mathscr{G}(f)$: it sends totally imaginary elements to totally imaginary elements and Φ-positive elements to Φ-positive elements. The only 'issue' is the α.
We study when we can 'pretend' $\alpha = 1$.

Effective Results : when can we ignore α?

Assume A admits a canonical lifting. Put $S := \mathrm{End}(A)$
Let B be isogenous to A. Put $T = \mathrm{End}(B)$. The previous diagram tells us that the princ. polarisations of B (up-to-iso) are in bijections with

$$\mathscr{P}_\Phi^\alpha(B) := \{ i_0 \cdot u : u \in T^\times / \left\{ v\overline{v} : v \in T^\times \right\} \text{ s.t. } \alpha^{-1} i_0 u \text{ is tot. img. and } \Phi\text{-pos.} \}$$

Effective Results : when can we ignore α?

Assume A admits a canonical lifting. Put $S := \mathrm{End}(A)$
Let B be isogenous to A. Put $T = \mathrm{End}(B)$. The previous diagram tells us that the princ. polarisations of B (up-to-iso) are in bijections with

$$\mathscr{P}^{\alpha}_{\Phi}(B) := \{i_0 \cdot u : u \in T^{\times} / \{v\overline{v} : v \in T^{\times}\} \text{ s.t. } \alpha^{-1} i_0 u \text{ is tot. img. and } \Phi\text{-pos.}\}$$

Theorem (1)

Denote by $S^*_{\mathbb{R}}$ (resp. $T^*_{\mathbb{R}}$) the group of totally real units of S (resp. T).

Effective Results : when can we ignore α?

Assume A admits a canonical lifting. Put $S := \mathrm{End}(A)$
Let B be isogenous to A. Put $T = \mathrm{End}(B)$. The previous diagram tells us that the princ. polarisations of B (up-to-iso) are in bijections with

$$\mathscr{P}^{\alpha}_{\Phi}(B) := \{i_0 \cdot u : u \in T^{\times} / \{v\bar{v} : v \in T^{\times}\} \text{ s.t. } \alpha^{-1} i_0 u \text{ is tot. img. and } \Phi\text{-pos.}\}$$

Theorem (1)

Denote by $S^*_{\mathbb{R}}$ (resp. $T^*_{\mathbb{R}}$) the group of totally real units of S (resp. T). If $S^*_{\mathbb{R}} \subseteq T^*_{\mathbb{R}}$, then the set $\mathscr{P}^{\alpha}_{\Phi}(B)$

Effective Results : when can we ignore α?

Assume A admits a canonical lifting. Put $S := \mathrm{End}(A)$
Let B be isogenous to A. Put $T = \mathrm{End}(B)$. The previous diagram tells us that the princ. polarisations of B (up-to-iso) are in bijections with

$\mathscr{P}^{\alpha}_{\Phi}(B) := \{i_0 \cdot u : u \in T^{\times} / \{v\bar{v} : v \in T^{\times}\}$ s.t. $\alpha^{-1} i_0 u$ is tot. img. and Φ-pos.$\}$

Theorem (1)

Denote by $S^*_{\mathbb{R}}$ (resp. $T^*_{\mathbb{R}}$) the group of totally real units of S (resp. T). If $S^*_{\mathbb{R}} \subseteq T^*_{\mathbb{R}}$, then the set $\mathscr{P}^{\alpha}_{\Phi}(B)$ is in bijection with the set

$$\mathscr{P}^{1}_{\Phi}(B) = \{i_0 \cdot u : u \in T^{\times} / \{v\bar{v} : v \in T^{\times}\} \text{ s.t. } i_0 u \text{ is tot. img. and } \Phi\text{-pos.}\}.$$

(which does not depend on α!)

Effective Results : when can we ignore α?

Assume A admits a canonical lifting. Put $S := \mathrm{End}(A)$
Let B be isogenous to A. Put $T = \mathrm{End}(B)$. The previous diagram tells us that the princ. polarisations of B (up-to-iso) are in bijections with

$\mathscr{P}_\Phi^\alpha(B) := \{i_0 \cdot u : u \in T^\times / \{v\bar{v} : v \in T^\times\}$ s.t. $\alpha^{-1} i_0 u$ is tot. img. and Φ-pos.$\}$

Theorem (1)

Denote by $S_\mathbb{R}^*$ (resp. $T_\mathbb{R}^*$) the group of totally real units of S (resp. T). If $S_\mathbb{R}^* \subseteq T_\mathbb{R}^*$, then the set $\mathscr{P}_\Phi^\alpha(B)$ is in bijection with the set

$$\mathscr{P}_\Phi^1(B) = \{i_0 \cdot u : u \in T^\times / \{v\bar{v} : v \in T^\times\} \text{ s.t. } i_0 u \text{ is tot. img. and } \Phi\text{-pos.}\}.$$

(which does not depend on α!)

Corollary

If $S = \mathbb{Z}[F, V]$ (eg. $\mathrm{AV}_h(p)$ is ordinary or almost-ordinary) then we can ignore α.

Effective Results : when can we ignore α?

Assume A admits a canonical lifting. Put $S := \mathrm{End}(A)$
Let B be isogenous to A. Put $T = \mathrm{End}(B)$. The previous diagram tells us that the princ. polarisations of B (up-to-iso) are in bijections with

$\mathscr{P}^{\alpha}_{\Phi}(B) := \{i_0 \cdot u : u \in T^\times / \{v\bar{v} : v \in T^\times\}$ s.t. $\alpha^{-1} i_0 u$ is tot. img. and Φ-pos.$\}$

Theorem (1)

Denote by $S^*_{\mathbb{R}}$ (resp. $T^*_{\mathbb{R}}$) the group of totally real units of S (resp. T). If $S^*_{\mathbb{R}} \subseteq T^*_{\mathbb{R}}$, then the set $\mathscr{P}^{\alpha}_{\Phi}(B)$ is in bijection with the set

$$\mathscr{P}^{1}_{\Phi}(B) = \{i_0 \cdot u : u \in T^\times / \{v\bar{v} : v \in T^\times\} \text{ s.t. } i_0 u \text{ is tot. img. and } \Phi\text{-pos.}\}.$$

(which does not depend on α!)

Corollary

If $S = \mathbb{Z}[F, V]$ (eg. $\mathrm{AV}_h(p)$ is ordinary or almost-ordinary) then we can ignore α. We recover Deligne+Howe and Oswal-Shankar

We run computations over all squarefree isogeny classes over small prime fields of dim 2,3 and 4.

We run computations over all squarefree isogeny classes over small prime fields of dim 2,3 and 4.

squarefree dimension 3			$p=2$	$p=3$	$p=5$	$p=7$
total			185	621	2863	7847
ordinary			82	390	2280	6700
almost ordinary			58	170	474	996
p-rank 1	no RRC		0	0	0	0
	yes RRC	Thm 1 yes	20	26	76	118
		Thm 1 no	4	16	12	8
p-rank 0	no RRC		0	3	2	1
	yes RRC	Thm 1 yes	20	15	17	23
		Thm 1 no	1	1	2	1

We run computations over all squarefree isogeny classes over small prime fields of dim 2,3 and 4.

squarefree dimension 3			$p=2$	$p=3$	$p=5$	$p=7$
total			185	621	2863	7847
ordinary			82	390	2280	6700
almost ordinary			58	170	474	996
p-rank 1	no RRC		0	0	0	0
	yes RRC	Thm 1 yes	20	26	76	118
		Thm 1 no	4	16	12	8
p-rank 0	no RRC		0	3	2	1
	yes RRC	Thm 1 yes	20	15	17	23
		Thm 1 no	1	1	2	1

Among the 45 isogeny classes which we cannot 'handle' with Thm 1, we can compute the number of PPAV for 32 of them using other techniques. For the remaining 13 (all over $\mathbb{F}_2$ and $\mathbb{F}_3$) we only get partial info.

squarefree dimension 4			$p = 2$	$p = 3$
total			1431	10453
ordinary			656	6742
almost ordinary			392	2506
p-rank 2	no RRC		0	0
	yes RRC	Thm 1 yes	149	500
		Thm 1 no	49	312
p-rank 1	no RRC		6	36
	yes RRC	Thm 1 yes	80	184
		Thm 1 no	14	40
p-rank 0	no RRC		3	6
	yes RRC	Thm 1 yes	73	88
		Thm 1 no	9	39

squarefree dimension 4			$p = 2$	$p = 3$
total			1431	10453
ordinary			656	6742
almost ordinary			392	2506
p-rank 2	no RRC		0	0
	yes RRC	Thm 1 yes	149	500
		Thm 1 no	49	312
p-rank 1	no RRC		6	36
	yes RRC	Thm 1 yes	80	184
		Thm 1 no	14	40
p-rank 0	no RRC		3	6
	yes RRC	Thm 1 yes	73	88
		Thm 1 no	9	39

Thm 1 ($S_{\mathbb{R}}^* \subseteq T_{\mathbb{R}}^*$) doesn't handle $72/\mathbb{F}_2$ and $391/\mathbb{F}_3$.

squarefree dimension 4			$p=2$	$p=3$
total			1431	10453
ordinary			656	6742
almost ordinary			392	2506
p-rank 2	no RRC		0	0
	yes RRC	Thm 1 yes	149	500
		Thm 1 no	49	312
p-rank 1	no RRC		6	36
	yes RRC	Thm 1 yes	80	184
		Thm 1 no	14	40
p-rank 0	no RRC		3	6
	yes RRC	Thm 1 yes	73	88
		Thm 1 no	9	39

Thm 1 ($S^*_{\mathbb{R}} \subseteq T^*_{\mathbb{R}}$) doesn't handle $72/\mathbb{F}_2$ and $391/\mathbb{F}_3$. Out of these, we can use other techniques for $20/\mathbb{F}_2$ and $214/\mathbb{F}_3$.

<table>
<tr><td colspan="3">squarefree dimension 4</td><td>$p = 2$</td><td>$p = 3$</td></tr>
<tr><td colspan="3">total</td><td>1431</td><td>10453</td></tr>
<tr><td colspan="3">ordinary</td><td>656</td><td>6742</td></tr>
<tr><td colspan="3">almost ordinary</td><td>392</td><td>2506</td></tr>
<tr><td rowspan="3">p-rank 2</td><td colspan="2">no RRC</td><td>0</td><td>0</td></tr>
<tr><td rowspan="2">yes RRC</td><td>Thm 1 yes</td><td>149</td><td>500</td></tr>
<tr><td>Thm 1 no</td><td>49</td><td>312</td></tr>
<tr><td rowspan="3">p-rank 1</td><td colspan="2">no RRC</td><td>6</td><td>36</td></tr>
<tr><td rowspan="2">yes RRC</td><td>Thm 1 yes</td><td>80</td><td>184</td></tr>
<tr><td>Thm 1 no</td><td>14</td><td>40</td></tr>
<tr><td rowspan="3">p-rank 0</td><td colspan="2">no RRC</td><td>3</td><td>6</td></tr>
<tr><td rowspan="2">yes RRC</td><td>Thm 1 yes</td><td>73</td><td>88</td></tr>
<tr><td>Thm 1 no</td><td>9</td><td>39</td></tr>
</table>

Thm 1 ($S^*_{\mathbb{R}} \subseteq T^*_{\mathbb{R}}$) doesn't handle $72/\mathbb{F}_2$ and $391/\mathbb{F}_3$. Out of these, we can use other techniques for $20/\mathbb{F}_2$ and $214/\mathbb{F}_3$. For the remaining $52/\mathbb{F}_2$ and $171/\mathbb{F}_3$ we can only get information about certain endomorphism rings (723 out of 946 and 3481 out of 4636, respectively).

Thank you!

Effective Results II

Theorem (2)

Assume that there are r isomorphism classes of abelian varieties in $\mathrm{AV}_h(p)$ with endomorphism ring T, represented under $\mathscr{G}$ by the fractional ideals $I_1, \dots, I_r$. For any CM-type Φ', we put

$$\mathscr{P}^1_{\Phi'}(I_i) = \{ i_0 \cdot u : u \in \mathscr{T} \text{ such that } i_0 u \text{ is totally imaginary and } \Phi'\text{-positive} \}.$$

If there exists a non-negative integer N such that for every CM-type Φ' we have

$$|\mathscr{P}^1_{\Phi'}(I_1)| + \ldots + |\mathscr{P}^1_{\Phi'}(I_r)| = N$$

then there are exactly N isomorphism classes of principally polarized abelian varieties with endomorphism ring T.

Proof.

- Consider the association $\Phi' \mapsto b$ where $b \in L^*$ is tot. imaginary and Φ'-positive.
- We can go back: for every b tot. imaginary there exists a unique CM-type Φ_b s.t. b is Φ_b-positive.
- Hence the totally real elements of L^* acts on the set of CM-types.
- If $\Phi = \Phi_b$ is the CM-type for which we have a canonical lift (as before) then $\mathscr{P}^{\alpha}_{\Phi_b}(I_i) \longleftrightarrow \mathscr{P}^{1}_{\Phi_{\alpha b}}(I_i)$.
- If the we get the 'same sum' (over the I_i's) for every CM-type we know that the result must be the correct one!

$\square$

Note: even if the sum is not the same for all Φ''s then we know that one of the outputs is the correct one!