

Isomorphism classes of abelian varieties over finite fields

Marseglia Stefano

Utrecht University

DIAMANT symposium - 28 November 2019

Introduction: Abelian Varieties

- An **abelian variety** over a field k is a projective connected group variety over k .

Introduction: Abelian Varieties

- An **abelian variety** over a field k is a projective connected group variety over k .
- e.g. AVs of dim 1 are elliptic curves:

$$\text{when } \text{char}(k) \neq 2, 3 \rightsquigarrow Y^2 = X^3 + AX + B$$

Introduction: Abelian Varieties

- An **abelian variety** over a field k is a projective connected group variety over k .
- e.g. AVs of dim 1 are elliptic curves:

$$\text{when } \text{char}(k) \neq 2, 3 \rightsquigarrow Y^2 = X^3 + AX + B$$

- **Goal**: compute **isomorphism classes** of abelian varieties over a **finite field** (+ extra structure, like polarizations, period matrices, etc.)

Introduction: Abelian Varieties

- An **abelian variety** over a field k is a projective connected group variety over k .
- e.g. AVs of dim 1 are elliptic curves:

$$\text{when } \text{char}(k) \neq 2, 3 \rightsquigarrow Y^2 = X^3 + AX + B$$

- **Goal**: compute **isomorphism classes** of abelian varieties over a **finite field** (+ extra structure, like polarizations, period matrices, etc.)
- in dimension $g > 1$ is not easy to produce equations.

Introduction: Abelian Varieties

- An **abelian variety** over a field k is a projective connected group variety over k .
- e.g. AVs of dim 1 are elliptic curves:

$$\text{when } \text{char}(k) \neq 2, 3 \rightsquigarrow Y^2 = X^3 + AX + B$$

- **Goal:** compute **isomorphism classes** of abelian varieties over a **finite field** (+ extra structure, like polarizations, period matrices, etc.)
- in dimension $g > 1$ is not easy to produce equations.
- over \mathbb{C} :

$$\{\text{abelian varieties } / \mathbb{C}\} \longleftrightarrow \left\{ \mathbb{C}^g / L \text{ with } L \simeq \mathbb{Z}^{2g} \text{ with } \right. \\ \left. \text{eq.cl. of Riemann form} \right\}$$

Introduction: Abelian Varieties

- An **abelian variety** over a field k is a projective connected group variety over k .
- e.g. AVs of dim 1 are elliptic curves:

$$\text{when } \text{char}(k) \neq 2, 3 \rightsquigarrow Y^2 = X^3 + AX + B$$

- **Goal:** compute **isomorphism classes** of abelian varieties over a **finite field** (+ extra structure, like polarizations, period matrices, etc.)
- in dimension $g > 1$ is not easy to produce equations.
- over \mathbb{C} :

$$\{\text{abelian varieties } / \mathbb{C}\} \longleftrightarrow \left\{ \mathbb{C}^g / L \text{ with } L \simeq \mathbb{Z}^{2g} \text{ with } \right. \\ \left. \text{eq.cl. of Riemann form} \right\}$$

- in positive characteristic we don't have such equivalence.

Classification problem

- A and B are **isogenous** if $\dim A = \dim B$ and there exists a surjective homomorphism $\varphi : A \rightarrow B$.

Classification problem

- A and B are **isogenous** if $\dim A = \dim B$ and there exists a surjective homomorphism $\varphi: A \rightarrow B$.
- Being isogenous is an equivalence relation.

Classification problem

- A and B are **isogenous** if $\dim A = \dim B$ and there exists a surjective homomorphism $\varphi: A \rightarrow B$.
- Being isogenous is an equivalence relation.
- A/\mathbb{F}_{p^r} comes with a **Frobenius endomorphism**, that induces an action

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

$\mathrm{char}(\mathrm{Frob}_A)$ is a **p^r -Weil polynomial**.

Classification problem

- A and B are **isogenous** if $\dim A = \dim B$ and there exists a surjective homomorphism $\varphi: A \rightarrow B$.
- Being isogenous is an equivalence relation.
- A/\mathbb{F}_{p^r} comes with a **Frobenius endomorphism**, that induces an action

$$\text{Frob}_A: T_\ell A \rightarrow T_\ell A \text{ for any } \ell \neq p.$$

$\text{char}(\text{Frob}_A)$ is a **p^r -Weil polynomial**.

- By **Honda-Tate** theory, the association

$$\text{isogeny class of } A \mapsto \text{char}(\text{Frob}_A)$$

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

Deligne's equivalence

Theorem (Deligne '69)

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

$$\{ \text{Ordinary abelian varieties over } \mathbb{F}_q \} \quad A$$

Deligne's equivalence

Theorem (Deligne '69)

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

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

Deligne's equivalence

Theorem (Deligne '69)

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

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

Remark

- If $\dim(A) = g$ then $\text{Rank}(T(A)) = 2g$;
- $\text{Frob}(A) \rightsquigarrow F(A)$.

Main result

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

Main result

- Fix an **ordinary squarefree** q -Weil polynomial h :
- \rightsquigarrow an isogeny class \mathcal{C}_h .

Main result

- Fix an **ordinary squarefree** q -Weil polynomial h :
- \rightsquigarrow an isogeny class \mathcal{C}_h .
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$.

Main result

- Fix an **ordinary squarefree** q -Weil polynomial h :
- \rightsquigarrow an isogeny class \mathcal{C}_h .
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$.
- Deligne's equivalence induces:

Theorem (M.)

$$\begin{array}{c} \{ \text{abelian varieties over } \mathbb{F}_q \text{ in } \mathcal{C}_h \} / \simeq \\ \updownarrow \\ \{ \text{fractional ideals of } \mathbb{Z}[F, q/F] \subset K \} / \simeq \end{array}$$

Main result

- Fix an **ordinary squarefree** q -Weil polynomial h :
- \rightsquigarrow an isogeny class \mathcal{C}_h .
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$.
- Deligne's equivalence induces:

Theorem (M.)

$$\begin{array}{c} \{ \text{abelian varieties over } \mathbb{F}_q \text{ in } \mathcal{C}_h \} / \simeq \\ \updownarrow \\ \{ \text{fractional ideals of } \mathbb{Z}[F, q/F] \subset K \} / \simeq \end{array} =: \text{ICM}(\mathbb{Z}[F, q/F])$$

ideal class monoid

Main result

- Fix an **ordinary squarefree** q -Weil polynomial h :
- \rightsquigarrow an isogeny class \mathcal{C}_h .
- Put $K := \mathbb{Q}[x]/(h) = \mathbb{Q}[F]$.
- Deligne's equivalence induces:

Theorem (M.)

$$\begin{array}{c} \{ \text{abelian varieties over } \mathbb{F}_q \text{ in } \mathcal{C}_h \} / \simeq \\ \updownarrow \\ \{ \text{fractional ideals of } \mathbb{Z}[F, q/F] \subset K \} / \simeq \end{array} =: \text{ICM}(\mathbb{Z}[F, q/F])$$

ideal class monoid

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

ICM : Ideal Class Monoid

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

ICM : Ideal Class Monoid

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

- Recall: for fractional R -ideals I and J

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

ICM : Ideal Class Monoid

Let R be an **order** in a finite 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

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

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

ICM : Ideal Class Monoid

Let R be an **order** in a finite 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

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

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

- ...and actually

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

simplify the problem

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

simplify the problem

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

- **weak equivalence:**

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

simplify the problem

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

- **weak equivalence:**

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



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

simplify the problem

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

- **weak equivalence:**

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



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

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

simplify the problem

Study the isomorphism problem locally: (Dade, Taussky, Zassenhaus '62)

- **weak equivalence:**

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



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

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

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

Compute $ICM(R)$

Compute $\text{ICM}(R)$

Partition w.r.t. the multiplier ring:

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

$$\text{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \text{ICM}_S(R)$$

Compute $\text{ICM}(R)$

Partition w.r.t. the multiplier ring:

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

$$\text{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \text{ICM}_S(R)$$

the “pedix” $-_S$ means
“only classes with multiplier ring S ”

Compute $\text{ICM}(R)$

Partition w.r.t. the multiplier ring:

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

$$\text{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \text{ICM}_S(R)$$

the “pedix” $-_S$ means
“only classes with multiplier ring S ”

Theorem (M.)

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

$$\mathcal{W}_S(R) = \text{ICM}_S(R) / \text{Pic}(S)$$

Compute $\text{ICM}(R)$

Partition w.r.t. the multiplier ring:

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

$$\text{ICM}(R) = \bigsqcup_{R \subseteq S \subseteq \mathcal{O}_K} \text{ICM}_S(R)$$

the “pedix” $-_S$ means
“only classes with multiplier ring S ”

Theorem (M.)

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

$$\mathcal{W}_S(R) = \text{ICM}_S(R) / \text{Pic}(S)$$

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

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

back to AV's: Dual variety/Polarization

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

Theorem (M.)

If $A \leftrightarrow I$, then:

back to AV's: Dual variety/Polarization

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

Theorem (M.)

If $A \leftrightarrow I$, then:

- $A^\vee \leftrightarrow \bar{I}^t.$

back to AV's: Dual variety/Polarization

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

Theorem (M.)

If $A \leftrightarrow I$, then:

- $A^\vee \leftrightarrow \bar{I}^t$.
 - a polarization μ of A corresponds to a $\lambda \in K^\times$ such that
 - $\lambda I \subseteq \bar{I}^t$ (isogeny);
 - λ is totally imaginary ($\bar{\lambda} = -\lambda$);
 - λ is Φ -positive, where Φ is a specific CM-type of K .
- Also: $\deg \mu = [\bar{I}^t : \lambda I]$.

back to AV's: Dual variety/Polarization

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

Theorem (M.)

If $A \leftrightarrow I$, then:

- $A^\vee \leftrightarrow \bar{I}^t$.
- a polarization μ of A corresponds to a $\lambda \in K^\times$ such that
 - $\lambda I \subseteq \bar{I}^t$ (isogeny);
 - λ is totally imaginary ($\bar{\lambda} = -\lambda$);
 - λ is Φ -positive, where Φ is a specific CM-type of K .

Also: $\deg \mu = [\bar{I}^t : \lambda I]$.

- if $(A, \mu) \leftrightarrow (I, \lambda)$ and $S = (I : I)$ then

$$\left\{ \begin{array}{l} \text{non-isomorphic} \\ \text{polarizations of } A \\ \text{of degree} = \deg \lambda \end{array} \right\} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{v\bar{v} : v \in S^\times\}}.$$

back to AV's: Dual variety/Polarization

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

Theorem (M.)

If $A \leftrightarrow I$, then:

- $A^\vee \leftrightarrow \bar{I}^t$.
- a polarization μ of A corresponds to a $\lambda \in K^\times$ such that
 - $\lambda I \subseteq \bar{I}^t$ (isogeny);
 - λ is totally imaginary ($\bar{\lambda} = -\lambda$);
 - λ is Φ -positive, where Φ is a specific CM-type of K .

Also: $\deg \mu = [\bar{I}^t : \lambda I]$.

- if $(A, \mu) \leftrightarrow (I, \lambda)$ and $S = (I : I)$ then

$$\left\{ \begin{array}{l} \text{non-isomorphic} \\ \text{polarizations of } A \\ \text{of degree} = \deg \lambda \end{array} \right\} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{v\bar{v} : v \in S^\times\}}.$$

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

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.
- $\# \text{ICM}(R) = 18 \rightsquigarrow 18$ isom. classes of AV in the isogeny class.
- 5 are not invertible in their multiplier ring.
- 8 classes admit principal polarizations.
- 10 isomorphism classes of princ. polarized AV.

Example

Concretely:

$$\begin{aligned} I_1 = & 2645633792595191\mathbb{Z} \oplus (F + 836920075614551)\mathbb{Z} \oplus (F^2 + 1474295643839839)\mathbb{Z} \oplus \\ & \oplus (F^3 + 1372829830503387)\mathbb{Z} \oplus (F^4 + 1072904687510)\mathbb{Z} \oplus \\ & \oplus \frac{1}{3}(F^5 + F^4 + F^3 + 2F^2 + 2F + 6704806986143610)\mathbb{Z} \oplus \\ & \oplus \frac{1}{9}(F^6 + F^5 + F^4 + 8F^3 + 2F^2 + 2991665243621169)\mathbb{Z} \oplus \\ & \oplus \frac{1}{27}(F^7 + F^6 + F^5 + 17F^4 + 20F^3 + 9F^2 + 68015312518722201)\mathbb{Z} \end{aligned}$$

principal polarizations:

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

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

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

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:

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

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

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

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

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in \mathcal{C}_h over \mathbb{F}_p where h is **square-free** and **without real roots**.

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in \mathcal{C}_h over \mathbb{F}_p where h is **square-free** and **without real roots**.
much larger subcategory!!!

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in \mathcal{C}_h over \mathbb{F}_p where h is **square-free** and **without real roots**.
much larger subcategory!!!
- isogeny classes \mathcal{C}_{h^d} (with h square-free) when $\mathbb{Z}[F, q/F]$ is Bass.

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in \mathcal{C}_h over \mathbb{F}_p where h is **square-free** and **without real roots**.
much larger subcategory!!!
- isogeny classes \mathcal{C}_{h^d} (with h square-free) when $\mathbb{Z}[F, q/F]$ is Bass.
- base field extensions and **twists** (ordinary case) (soon on arXiv).

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in \mathcal{C}_h over \mathbb{F}_p where h is **square-free** and **without real roots**.
much larger subcategory!!!
- isogeny classes \mathcal{C}_{h^d} (with h square-free) when $\mathbb{Z}[F, q/F]$ is Bass.
- base field extensions and **twists** (ordinary case) (soon on arXiv).
- **period matrices** (ordinary case) of the canonical lift.

Final remarks

- Using Centeleghe-Stix '15 we can compute the isomorphism classes in \mathcal{C}_h over \mathbb{F}_p where h is **square-free** and **without real roots**.
much larger subcategory!!!
- isogeny classes \mathcal{C}_{h^d} (with h square-free) when $\mathbb{Z}[F, q/F]$ is Bass.
- base field extensions and **twists** (ordinary case) (soon on arXiv).
- **period matrices** (ordinary case) of the canonical lift.
- results of computations will appear on the LMFDB.

Thank you!