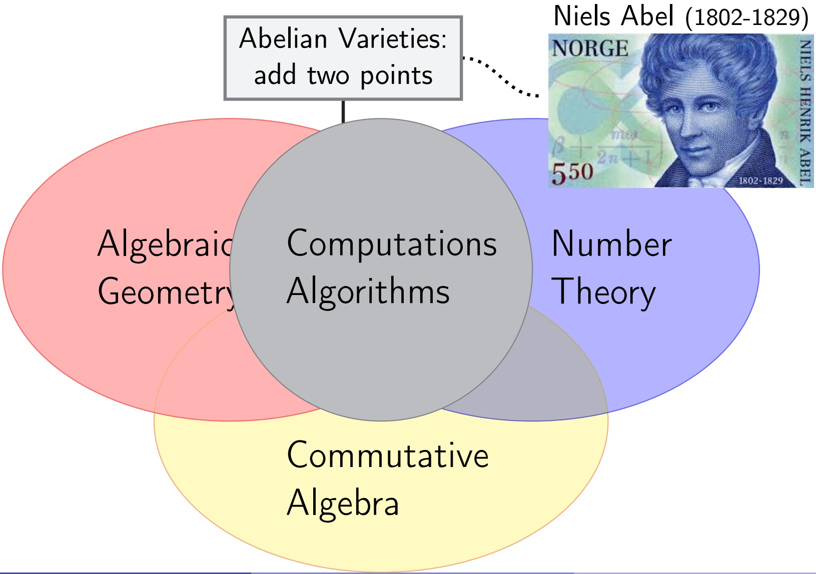
Abelian varieties over finite fields

Stefano Marseglia

UPF - Gaati Lab

14/02/2024

What do I do for a living?



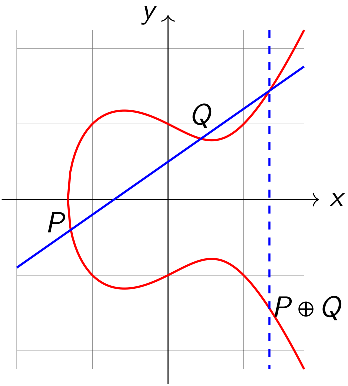
Abelian varieties: what are they ?

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.
- Then $A(\mathbb{C})$ is a **torus**: $T := \mathbb{C}^g/\Lambda$, where $\Lambda \simeq_{\mathbb{Z}} \mathbb{Z}^{2g}$.
- T admits a non-degenerate Riemann form $\longleftrightarrow$ polarization.
- In fact, $A \mapsto A(\mathbb{C})$ 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...
- ... which we are going to use to classify the AVs up to isomorphism.

Isogeny classification over $\mathbb{F}_q$

- An **isogeny** $A \to B$ is a surjective morphism with finite kernel.
- $A/\mathbb{F}_q$ 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

$$\text{isogeny class of } A \longmapsto h_A(x)$$

  is injective and allows us to enumerate all AVs up to isogeny.
- Also, $h_A(x)$ is squarefree $\iff$ $\mathrm{End}(A)$ is commutative.

Deligne's equivalence

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

Theorem (Deligne '69)

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

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

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

- 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.

- 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 $R = \mathcal{O}_K$

- ...and actually

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

- Hofmann-Sircana '19: computation of over-orders.

simplify the problem

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

- **weak equivalence**:

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

$$\Updownarrow$$

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

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

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

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

Compute $\mathrm{ICM}(R)$

Partition w.r.t. the multiplicator ring:

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

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

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 $R \subseteq S \subseteq \mathcal{O}_K$:

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

To sum up:

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

Remark

Let $\mathscr{C}_h$ be a **squarefree** *isogeny classes over the* **prime field** $\mathbb{F}_p$*. Building on work by Centeleghe-Stix, we get a bijection between the isomorphism classes of AVs in $\mathscr{C}_h$ and the ideal class monoid of $\mathbb{Z}[\pi, p/\pi]$, as above. But the functor is completely different! (eg. It is contravariant)*

Dual varieties and Polarizations

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

Theorem

Let $A \in \mathscr{C}_h$ with h ordinary and squarefree. If $A \leftrightarrow I$, 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);*
  - λ *is totally imaginary ($\overline{\lambda} = -\lambda$);*
  - λ *is Φ-positive, where Φ is a CM-type of K satisf. the Shimura-Taniyama formula.*

  Also: $\deg \mu = [\overline{I}^t : \lambda I]$.
- *if $(A,\mu) \leftrightarrow (I,\lambda)$ is a princ. polarized ab. var. and $S = (I : I)$ then*
$$\left\{ \begin{matrix} \text{non-isomorphic princ.} \\ \text{polarizations of } A \end{matrix} \right\} \longleftrightarrow \frac{\{\text{totally positive } u \in S^\times\}}{\{v\overline{v} : v \in S^\times\}},$$
- *and* $\mathrm{Aut}(A,\mu) = \{\text{torsion units of } S\}$.

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.

Can modify to compute polarizations of any degree.

Example

- Let $h(x) = x^8 - 5x^7 + 13x^6 - 25x^5 + 44x^4 - 75x^3 + 117x^2 - 135x + 81$, LMFDB label: 4.3.af_n_az_bs.
- $\rightsquigarrow$ isogeny class of a 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.
- More info at

  `https://abvar.lmfdb.xyz/Variety/Abelian/Fq/4/3/af_n_az_bs`

- The equivalence is not just useful to classify the AVs!
- It can be used to compute polarizations, isogenies, and group of $\mathbb{F}_q$-points.
- In the rest of the talk, we will prove

Theorem (M.-Springer)

Let k be $\mathbb{F}_2$, $\mathbb{F}_3$ or $\mathbb{F}_5$. Let G be a finite abelian group. Then there exists an ordinary A/k with $A(k) = G$.

Cyclic abelian varieties

Recall that we have an equivalence

$$\mathscr{C}_h \longleftrightarrow \{\text{fractional ideals of } \mathbb{Z}[F, q/F]\}.$$

Corollary

If A corresponds to the fractional $\mathbb{Z}[F, q/F]$-ideal J then

$$A(\mathbb{F}_q) \simeq \frac{J}{(1-F)J}.$$

Proposition (M.-Springer)

Every ordinary squarefree isogeny class contains a cyclic abelian variety.

Proof: Take $A \longleftrightarrow J = \mathbb{Z}[F, q/F]$.

$$A(\mathbb{F}_q) \simeq \frac{\mathbb{Z}[F, q/F]}{(1-F)} \simeq \frac{\mathbb{Z}[x, y]}{(h(x), xy - q, 1 - x)} \simeq \frac{\mathbb{Z}}{h(1)\mathbb{Z}}. \quad \square$$

Number of points

Theorem (Howe-Kedlaya)

Let $m \in \mathbb{Z}_{\geq 0}$. Then there is a squarefree ordinary $A/\mathbb{F}_2$ such that $\#A(\mathbb{F}_2) = m$.

Theorem (van Bommel-Costa-Li-Poonen-Smith)

Let $m \in \mathbb{Z}_{\geq 0}$ and k be $\mathbb{F}_3$ or $\mathbb{F}_5$. Then there is a squarefree ordinary A/k such that $\#A(k) = m$.

They use extremely clever constructions that allows them to construct characteristic polynomials h_A such that $h_A(1) = m$.

Group of points

Theorem (M.-Springer)

Let k be $\mathbb{F}_2$, $\mathbb{F}_3$ or $\mathbb{F}_5$. Let G be a finite abelian group. Then there exists an ordinary A/k with $A(k) = G$.

Proof: Write

$$G \simeq \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{m_s\mathbb{Z}}.$$

By H-K or vBCLPS, for each i there is an isogeny class with m_i points.
By Proposition, within each of the isogeny classes, there is a cyclic A_i.
Take $A = \prod_i A_i$. □

Corollary

If G is cyclic we can take A to be ordinary and squarefree.

Further results (building on vBCLPS)

- Over $\mathbb{F}_4$: for every abelian $G \neq 0$ there exists an ordinary or almost ordinary $A/\mathbb{F}_4$ such that $A(\mathbb{F}_4) \simeq G$.
- Over $\mathbb{F}_7$: for every cyclic $G \neq 0$ with $\#G \not\in \{2, 8, 14, 16, 17, 73\}$ there exists a squarefree ordinary $A/\mathbb{F}_7$ such that $A(\mathbb{F}_7) \simeq G$.
- vBCLPS: For an arbitrary q, every integer $m \geq q^{3\sqrt{q}\log q}$ arises as $m = \#A(\mathbb{F}_q)$ for some ordinary squarefree $A/\mathbb{F}_q$.

Theorem (M.-Springer)

Let $m_1, \ldots, m_r$ be integers satisfying $m_i \geq q^{3\sqrt{q}\log q}$. Put

$$G = \frac{\mathbb{Z}}{m_1\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{m_r\mathbb{Z}}.$$

Then there is an ordinary $A/\mathbb{F}_q$ such that $G = A(\mathbb{F}_q)$.

Thank you!