Abelian Varieties and their endomorphism rings

Caleb Springer (Penn State)

Abelian Varieties are simultaneously

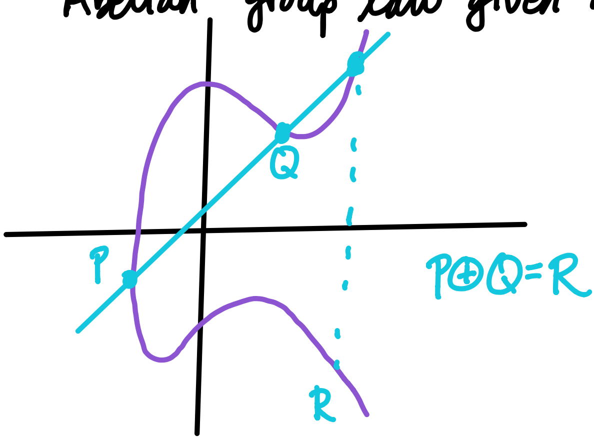
- Smooth projective Varieties
- abelian groups.

Motivating example: elliptic curves!

$$E: \left\{ (x,y) \in \overline{\mathbb{F}}_q^2 \;\middle|\; y^2 = \underbrace{x^3 + ax + b}_{\text{distinct roots}} \right\} \cup \{\infty\}$$

$$E(\mathbb{F}_q) = \left\{ (x,y) \in \mathbb{F}_q^2 \;\middle|\; \cdots \right\} \cup \{\infty\}.$$ group of rational points.

- Smooth projective curve
- Abelian group law given geometrically.



Finite fields are perfect for Computation and crypto!

Let A be an abelian variety over $\mathbb{F}_q$.

An isogeny $\varphi: A \to A$ (endomorphism) is both a morphism of varieties and a homomorphism of groups.

Examples: 1. $n \in \mathbb{Z}$ $\quad [n]: A \to A$

$$P \mapsto \underbrace{P \oplus \cdots \oplus P}_{n \text{ times}}$$

2. Over $\mathbb{F}_q$, Frobenius π induced by $x \mapsto x^q$.

The set of all endomorphisms forms a ring:

$$\mathrm{End}(A) = \{ \text{isogenies } \varphi: A \to A \}$$

(defined over $\mathbb{F}_q$)

The group of rational points $A(\mathbb{F}_q)$ is a module over $\mathrm{End}(A)$.

What is this module structure?

First, the ring structure of End(E) for an elliptic curve $E/\mathbb{F}_q$.

We can naturally identify the Frobenius π with a Weil q-integer: An algebraic integer whose $\underbrace{\text{Conjugates}}_{\text{(roots of min poly over } \mathbb{Q}.)}$ all have absolute value $\sqrt{q}$.

① If $\pi \notin \mathbb{Z}$, then End(E) is (isomorphic to) an order in the quadratic imaginary field $K = \mathbb{Q}(\pi)$

In fact, $\mathbb{Z}[\pi] \subseteq \text{End}(E) \subseteq \mathcal{O}_K$.

② If $\pi \in \mathbb{Z}$, then End(E) is (isomorphic to) an order in a quaternion algebra

$\mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$ $\qquad ij = -ji$

$i^2, j^2 \in \mathbb{Q}$.

Theorem (Lenstra) $E/\mathbb{F}_q$ elliptic curve, Frobenius π.

① If $\pi \notin \mathbb{Z}$ then $E(\mathbb{F}_{q^n}) \cong \mathrm{End}(E)/(\pi^n - 1)$

② If $\pi \in \mathbb{Z}$ then $E(\mathbb{F}_{q^n}) \cong \left(\mathbb{Z}/(\pi^n - 1)\right)^2$ as ab. gps.

End(E)-mod structure from $\mathrm{End}(E)/(\pi^n - 1) \cong \mathrm{Mat}_2\left(\mathbb{Z}/(\pi^n - 1)\right)$

NOTE: ① is a nontrivial statement, even when ignoring all but the abelian group structure.

Corollary (Galbraith) Every isogeny class of ordinary elliptic curves over $\mathbb{F}_q$ contains some $E/\mathbb{F}_q$ where $E(\mathbb{F}_q)$ is a cyclic group.

More generally, if $A/\mathbb{F}_q$ is simple with Frob π,
End(A) is contained in a division algebra D with center $\mathbb{Q}(\pi)$.

Theorem (S.): $R = \mathrm{End}(A)$
$Z = $ Center of $R \subseteq \mathbb{Q}(\pi) = K$

① If $R = Z$ commutative is Gorenstein (e.g. $R = \mathcal{O}_K$.)
then

$$A(\mathbb{F}_{q^n}) \cong R/(\pi^n - 1)$$

② If $Z = \mathcal{O}_K$, $\quad d = \dfrac{2\dim(A)}{[K:\mathbb{Q}]}$

$$A(\mathbb{F}_{q^n}) \cong \left(Z/(\pi^n - 1) \right)^d \qquad Z\text{-mods.}$$

R-mod structure from $R/(\pi^n-1) \cong \mathrm{Mat}_d\left(Z/(\pi^n-1) \right)$

Corollary (S.) Every simple ordinary isogeny class over $\mathbb{F}_q$ contains some $A/\mathbb{F}_q$ where $A(\mathbb{F}_q)$ is a cyclic group.

NOTE: In Lenstra's original paper, counterexamples are given to ① if Gorenstein is dropped.

Key to proof: Since $A(\mathbb{F}_{q^n})$ is the kernel of $\pi^n - 1$ we study and describe the kernels of separable isogenies.

See also: S. Marseglia.

Uses equivalence of categories to obtain "similar" result in commutative case, without Gorenstein or simplicity conditions.

Some other Uses of End(A)

- Construct abelian varieties with desired properties.
- Attacking Cryptosystems.
- investigate isogeny graphs.

Wanted: An algorithm to compute End(A) for $A/\mathbb{F}_q$.

Let's focus on the ordinary case.

Again, we start with elliptic curves.

$E/\mathbb{F}_q$, Frobenius π $\qquad K = \mathbb{Q}(\pi)$.

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_K$$

<u>Objective</u>: determine this order.

<u>Fact</u>: Orders of K are uniquely determined by their index in $\mathcal{O}_K$, i.e. their conductors.

<u>Idea #1</u>: Factor $[\mathcal{O}_K : \mathbb{Z}[\pi]] = p_1^{r_1} \cdots p_k^{r_k}$

Determine for $0 \le i \le k$ the $0 \le s_i \le r_i$

s.t. $[\mathcal{O}_K : \mathrm{End}(E)] = p_1^{s_1} \cdots p_k^{s_k}$

one prime at a time

<u>Problem</u>:

The "straightforward" methods fail if p_j is large.

Fact #2: The class group $Cl(\mathcal{O})$ acts freely and transitively on all $E'/\mathbb{F}_q$ in the isog. class with $\mathrm{End}(E') = \mathcal{O}$.

The action explicitly associates ideals $\longleftrightarrow$ isogenies

An ideal is principal $\Leftrightarrow$ the isogeny is an endomorphism $E \to E$.

Idea #2 (Bisson-Sutherland)
Investigate $\mathrm{End}(E)$ vs. orders $\mathcal{O} \subseteq \mathcal{O}_K$.
by testing $Cl(\mathrm{End}\, E)$ by computing isogenies.

Theorem: $Cl(\mathrm{End}\, E)$ contains enough information to determine $[\mathcal{O}_K : \mathrm{End}(E)]$ at large primes.

Theorem (Bisson - Sutherland)

Subexponential algorithm to compute endomorphism ring of ordinary elliptic curves.

Theorem (S.)

Subexponential algorithm to compute endomorphism ring of ordinary 2-dimensional abelian varieties (under some technical assumptions) using the class group method.

Some additional challenges for dim > 1:

① Principal polarizability!

② Computation of isogenies is more difficult
- See Dudeanu, Jetchev, Robert & Vuille

For dim > 2, I still show Computing End(A) reduces to Computing isogenies
But it is not currently known how to compute all necessary isogenies.

③ $\mathbb{Q}(\pi)$ is a quartic CM field here.

$\Rightarrow$ Orders $\mathcal{O} \subseteq \mathbb{Q}(\pi)$ are not uniquely defined by their index!

Theorem (Brooks, Jetchev, Wesolowski)

$K =$ CM field (e.g. $\mathbb{Q}(\pi)$.)

$F =$ max. totally real subfield (e.g. $\mathbb{Q}(\pi + \bar{\pi})$)

$$\left\{ \begin{array}{c} \text{orders} \\ \mathcal{O}_F \subseteq \mathcal{O} \subseteq \mathcal{O}_K \end{array} \right\} \xleftrightarrow{\text{bijection}} \left\{ \begin{array}{c} \text{nonzero ideals} \\ I \subseteq \mathcal{O}_F \end{array} \right\}$$

$$\mathcal{O} = \mathcal{O}_F + I\mathcal{O}_K \longleftarrow\!\shortmid\; I$$

Restrict to maximal real multiplication

i.e. $\mathrm{End}(A) \supseteq \mathcal{O}_F$.

So that the Theorem applies, and we can loop through primes dividing the corresponding ideal

Comparison: $K =$ quadratic imaginary field.

$F = \mathbb{Q}$

$$\left\{ \begin{array}{c} \text{orders} \\ (\mathbb{Z} \subseteq)\, \mathcal{O} \subseteq \mathcal{O}_K \end{array} \right\} \longleftrightarrow \underbrace{\left\{ \begin{array}{c} \text{positive} \\ \text{nonzero} \\ f \in \mathbb{Z} \end{array} \right\}}_{\text{nonzero ideals of } \mathbb{Z}.}$$