Abelian varieties over $\mathbb{F}_q$ and their groups of rational points

Caleb Springer

University College London & Heilbronn Institute for Mathematical Research

13 April 2023

Heilbronn Institute for Mathematical Research

Prescriptions for abelian varieties

There was a flurry of activity in 2021.

Theorem (Howe, Kedlaya 2021)

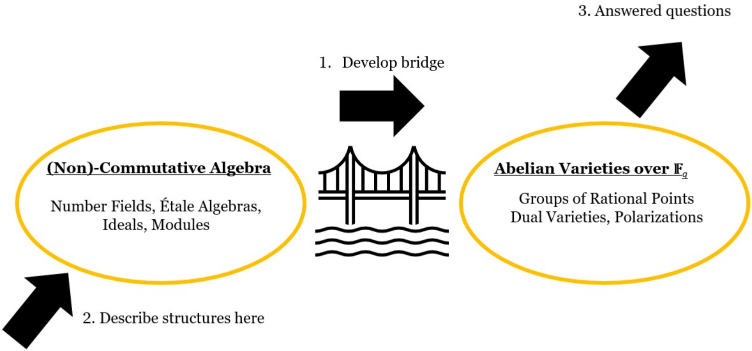
For every $n \geq 1$, there is an ordinary abelian variety over $\mathbb{F}_2$ with $\#A(\mathbb{F}_2) = n$.

Theorem (Marseglia-S. 2023)

For every finite abelian group G, there is an ordinary abelian variety over $\mathbb{F}_2$ with $A(\mathbb{F}_2) \cong G$.

- Also 2021: further results for prescribing point counts from Kedlaya and from vBCLPS. We also extended these results to analogous group-theoretic prescriptions.
- This talk's focus: General tools for understanding groups of rational points.

One Strategy for Proofs



Elliptic Curves over $\mathbb{F}_q$: Crash Course

- An elliptic curve E over $\mathbb{F}_q$ is a smooth projective curve whose group of rational points $E(\mathbb{F}_q)$ is an abelian group.
- E has a Frobenius endomorphism Frob induced by $x \mapsto x^q$.
- We can identify Frob with an algebraic integer $\pi \in \mathbb{C}$ of absolute value $\sqrt{q}$.
  - π is a root of the characteristic polynomial of Frob.
- The ($\mathbb{F}_q$-rational) endomorphism ring $\mathrm{End}(E) = \{\varphi : E \to E\}$ is isomorphic to either...

(If $\pi \notin \mathbb{Z}$) An order $\mathcal{O}$ satisfying $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_K$ for $K = \mathbb{Q}(\pi)$;

(If $\pi \in \mathbb{Z}$) A maximal order $\mathcal{O}$ in a quaternion algebra $\mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij$ with $i^2, j^2 \in \mathbb{Q}$ and $ij = -ji$.

- Actually, $E(\mathbb{F}_q)$ isn't just a group - it is a module over $\mathrm{End}(E)$.

Describing the Module Structure

Theorem (Lenstra, 1994)

Let E be an elliptic curve over $\mathbb{F}_q$ with Frobenius π.

(a) If $\mathrm{End}(E)$ is commutative, then

$$E(\mathbb{F}_q) \cong \mathrm{End}(E)/(1-\pi)$$

is an isomorphism of $\mathrm{End}(E)$-modules.

(b) If $\mathrm{End}(E)$ is noncommutative, then

$$E(\mathbb{F}_q) \cong (\mathbb{Z}/(1-\pi)\mathbb{Z})^2$$

is an isomorphism of groups whose $\mathrm{End}(E)$-module structure is given by $\mathrm{End}(E)/(1-\pi) \cong \mathrm{Mat}_2(\mathbb{Z}/(1-\pi)\mathbb{Z})$.

Remark: Galois theory says $E(\mathbb{F}_q) = \ker(1-\pi)$.

ABELIAN VARIETIES OF DIMENSION $g > 1$

- Abelian varieties provide a higher-dimensional analogue of elliptic curves: Smooth projective varieties with an abelian group structure on the rational points.
- In his 1994 paper, Lenstra showed that a naive generalization of his theorem fails even for abelian varieties of dimension 2.
- But the story continues nonetheless.

Describing the Module Structure

Theorem (S., 2021)

Let A be a simple abelian variety over $\mathbb{F}_q$ with Frobenius π.

(a) If $\mathrm{End}(A)$ is commutative **Gorenstein**, then

$$A(\mathbb{F}_q) \cong \mathrm{End}(A)/(1-\pi)$$

is an isomorphism of $\mathrm{End}(A)$-modules.

Remarks:

- The Gorenstein condition was already present, and automatically satisfied, in the elliptic curve version.
- The "simple" hypothesis can be deleted for part (a), and Gorenstein is only required locally at primes over $(1-\pi)$.
    - Joint work with Marseglia (2022).

Describing the Module Structure

Theorem (S., 2021) - Weak version for brevity

Let A be a simple abelian variety over $\mathbb{F}_q$ with Frobenius π.

(b) If the center Z of $\mathrm{End}(A)$ is a **maximal order** and $d = 2\dim(A)/[\mathbb{Q}(\pi) : \mathbb{Q}]$, then

$$A(\mathbb{F}_q) \cong (Z/(1-\pi)Z)^d$$

is an isomorphism of groups whose $\mathrm{End}(A)$-module structure is given by $\mathrm{End}(A)/(1-\pi) \cong \mathrm{Mat}_d(Z/(1-\pi)Z)$.

Remarks:

- Like before, the hypothesis that Z is maximal was automatically satisfied in the elliptic curve version.
- This part is proven via kernel ideals in the sense of Waterhouse.

Describing the Group Structure

A different piece of machinery is built upon the foundation of categorical equivalences developed by Deligne, Howe, and Centeleghe–Stix.

Theorem (Marseglia., 2021)

Let A be an abelian variety over $\mathbb{F}_q$ with Frobenius π. If $\mathrm{End}(A)$ is commutative and either A is ordinary or $q = p$ is prime, then there is an equivalence of categories

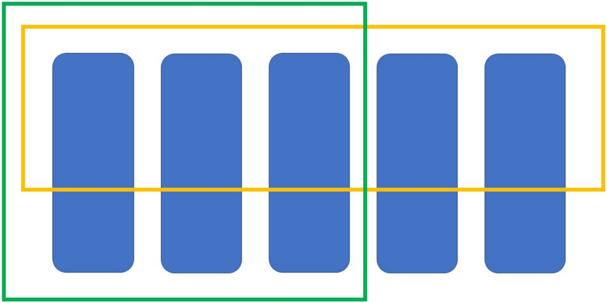
$$\mathcal{F} : \{\mathbb{F}_q - \text{isogeny class of } A\}/\cong \;\longrightarrow \{\text{ ideals of } \mathbb{Z}[\pi, \overline{\pi}]\}/\sim .$$

If $\mathcal{F}(A) = I$, then $A(\mathbb{F}_q) \cong I/I(1-\pi)$ are isomorphic groups.

- **Remark:** The righthand side is a so-called *ideal class monoid*, which is similar to a class group except that there are non-invertible ideals.

Combination of Tools

When looking towards applications, these tools have complementary strengths.



S. 2021:
In every simple isogeny class, applies to some of the abelian varieties.

Marseglia 2021: In certain isogeny classes, applies to all abelian varieties.

First consequence

Theorem (Marseglia-S. 2021)

For every finite abelian group G, there is an ordinary abelian variety over $\mathbb{F}_2$ with $A(\mathbb{F}_2) \cong G$.

Proof Sketch: Let $n \geq 1$.

1. Howe and Kedlaya: there is ordinary $A/\mathbb{F}_2$ with $A(\mathbb{F}_2) = n$ and $\mathrm{End}(A)$ commutative.
2. The isogeny class of A is defined by Weil polynomial $f(x)$ with $f(1) = n$ and $\mathbb{Q}[\pi] = \mathbb{Q}[x]/(f)$.
3. Algebra: show $\mathbb{Z}[\pi, \overline{\pi}]/(1-\pi) \cong \mathbb{Z}/n\mathbb{Z}$ is a cyclic group.
4. Using either of our tools, this algebraic fact is translated to the world of abelian varieties: we have $B \sim A$ with
$$B(\mathbb{F}_2) \cong \mathbb{Z}[\pi, \overline{\pi}]/(1-\pi) \cong \mathbb{Z}/n\mathbb{Z}.$$
5. Every finite abelian group is the product of cyclic groups. QED.

Pointers Towards Additional Consequences

Joint work with Stefano Marseglia (2022).

1. Explicit examples of $A/\mathbb{F}_q$ with $A(\mathbb{F}_q) \ncong A^\vee(\mathbb{F}_q)$.
   - Answers a question of Poonen from AMS MRC 2019.
   - Examples are easy to find for dimensions $2 \leq g \leq 5$.
   - Context: none of the arrows below are reversible in general.

$$A \cong \mathrm{Jac}(C) \Longrightarrow A \text{ is princ. pol.} \Longrightarrow A \cong A^\vee \Longrightarrow A(\mathbb{F}_q) \cong A^\vee(\mathbb{F}_q)$$

On the other hand, we prove that $A(\mathbb{F}_q) \cong A^\vee(\mathbb{F}_q)$ whenever $\mathrm{End}(A)$ satisfies certain hypotheses concerning its so-called Cohen-Macaulay type and complex conjugation.

POINTERS TOWARDS ADDITIONAL CONSEQUENCES

2. Sufficient conditions for the group structure of $A(\mathbb{F}_q)$ to be uniquely determined by $\mathrm{End}(A)$ in terms of Cohen-Macaulay type.
3. Characterization of isogeny classes $\mathcal{I}$ over $\mathbb{F}_q$ in which $A(\mathbb{F}_q)$ is *cyclic* for every $A \in \mathcal{I}$.
   - Theorem: If $A/\mathbb{F}_q$ has cyclic isogeny class, then $A \sim A_1 \times A_{\text{com}}$ where $\#A_1(\mathbb{F}_q) = 1$ and $\mathrm{End}(A_{\text{com}})$ is commutative.
   - When $\mathrm{End}(A)$ is commutative, the characterization is in terms of conductor ideals.
4. Characterization of isogeny classes $\mathcal{I}$ over $\mathbb{F}_q$ in which *every* abelian group of order N occurs as $A(\mathbb{F}_q)$ for some $A \in \mathcal{I}$.