

Every finite abelian group is the group of rational points
of an ordinary abelian variety over \mathbb{F}_2 , \mathbb{F}_3 and \mathbb{F}_5

Stefano Marseglia

Utrecht University

DIAMANT Symposium - 21 April 2022
joint work with
Caleb Springer

Abelian Varieties

- An **abelian variety** over a field k is a projective geometrically connected group variety over k .
- Fun fact: the group of rational points of an AV is commutative...
- ... but this is not why they are called abelian.
- e.g. AVs of dim 1 are elliptic curves:

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

- Annoying fact: in dimension $g > 1$, the equations are typically horrible.

Isogeny classes

- 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.
- Let q be a power of a prime p .
- A/\mathbb{F}_q comes with a **Frobenius endomorphism**, that induces an action

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

where $T_\ell A = \varprojlim A[\ell^n](\overline{\mathbb{F}}_p)$ is the ℓ -adic Tate module.

- $T_\ell A \simeq \mathbb{Z}_\ell^{2 \dim A}$. Put $h_A = \text{char}(\text{Frob}_A)$.
- h_A satisfies:
 - the definition of h_A does not depend on ℓ .
 - $h_A \in \mathbb{Z}[x]$.
 - $\deg h_A = 2 \dim A$
 - the complex roots of h_A have absolute value \sqrt{q} .

Isogeny classes

- By Honda-Tate theory, the association

$$A \mapsto h_A = \text{char}(\text{Frob}_A)$$

is **injective up to isogeny**, and...

...allows us to enumerate all AVs up to isogeny.

- Tate: h_A **squarefree** (no multiple roots) iff $\text{End}_{\mathbb{F}_q}(A)$ is commutative.
- The number of rational points is $\#A(\mathbb{F}_q) = h_A(1)$ isogeny invariant.
- ..but the group $A(\mathbb{F}_q)$ is not.
- We say that A/\mathbb{F}_q is **cyclic** if $A(\mathbb{F}_q)$ is cyclic.

Ordinary abelian varieties

- A/\mathbb{F}_q is **ordinary** if the coefficient of $x^{\dim A}$ in $h_A(x)$ is coprime to q .
- Being ordinary is an isogeny invariant.

Theorem (Deligne)

Let $h_A(x)$ be ordinary and squarefree. Put $K = \mathbb{Q}[F] = \mathbb{Q}[x]/(h_A(x))$. Then we have an **equivalence** of categories:

$$\begin{array}{c} \{ \text{abelian varieties } B/\mathbb{F}_q \text{ with } h_B(x) = h_A(x) \} \\ \updownarrow \\ \{ \text{fractional ideals of } \mathbb{Z}[F, q/F] \subset K \} \\ \parallel \\ \{ \text{fin. gen. } \mathbb{Z}[F, q/F]\text{-module in } K, \text{ free of max rank}_{\mathbb{Z}} \} \end{array}$$

Note: $F \leftrightarrow \text{Frob}$ (and $q/F \leftrightarrow \text{Verschiebung}$).

Cyclic abelian varieties

Corollary

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

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

Proposition (M.-Springer)

Every ordinary squarefree isogeny class contains a cyclic abelian variety.

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

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

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 an abelian group. Then there exists an ordinary A/k with $A(k) = G$.

Proof: Write

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

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 $\#G \notin \{2, 8, 14, 16, 17, 73\}$ 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, \dots, m_r be integers satisfying $m_i \geq q^{3\sqrt{q}\log q}$. Put

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

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

Thank you!