Abelian varieties over $\mathbb{F}_2$ of prescribed order

Kiran S. Kedlaya
work in progress (draft available)

Department of Mathematics, University of California San Diego
kedlaya@ucsd.edu
These slides can be downloaded from https://kskedlaya.org/slides/.

Explicit Methods in Number Theory
Mathematisches Forschungsinstitut Oberwolfach (hybrid meeting)
July 22, 2021

Supported by NSF (grants DMS-1802161, DMS-2053473) and UC San Diego (Warschawski Professorship). Thanks to the SIMONS FOUNDATION for the Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation.

The UC San Diego campus sits on unceded ancestral land of the Kumeyaay Nation, whom I thank for their stewardship.

The order of an abelian variety

Let A be an abelian variety over $\mathbb{F}_q$. Then the **order of** A is given by

$$\#A(\mathbb{F}_q) = P(1)$$

where $P \in \mathbb{Z}[T]$ is the charpoly of Frobenius on A.*

By a theorem of Weil, for $g = \dim(A)$, in $\mathbb{C}[T]$ we have

$$P(T) = (T - \alpha_1) \cdots (T - \alpha_{2g})$$

where $|\alpha_i| = \sqrt{q}$ and $\alpha_{g+i} = \overline{\alpha}_i$.

Conversely, by Honda–Tate, given a polynomial $P \in \mathbb{Z}[T]$ of this form, some power of it occurs as the charpoly of Frobenius of some A. When $q = p$, P itself always occurs.

---

*Or more precisely, on the ℓ-adic Tate module of A for any prime $\ell \nmid q$.

A closer look at the Weil bound

Weil's theorem implies that for $g = \dim(A)$,

$$(\sqrt{q} - 1)^{2g} \leq \#A(\mathbb{F}_q) \leq (\sqrt{q} + 1)^{2g}.$$

For fixed q, as $g \to \infty$ these intervals start to overlap, so there does not appear to be an obstruction to realizing **every** sufficiently large integer as the order of an abelian variety over $\mathbb{F}_q$ (of arbitrary order).

One can turn this intuition into a theorem by giving systematic constructions of Weil polynomials. This leads to results as on the next slide.

Acknowledgment: these are partly inspired by the tables of isogeny classes of abelian varieties in LMFDB (Dupuy–K–Roe–Vincent).

Realization of orders

Theorem (Howe–K, March 2021)

Every positive integer (with no exceptions!) is the order of an abelian variety over $\mathbb{F}_2$, which may even taken to be ordinary.

Theorem (van Bommel–Costa–Li–Poonen–Smith, June 2021)

For any given q, every sufficiently large positive integer[a] is the order of an abelian variety over $\mathbb{F}_q$, which may even taken to be ordinary, geometrically simple, and principally polarizable.

[a] Of course the cutoff for "sufficiently large" depends on q as well as on which side conditions you add. In any case it is principle effective; with no side conditions you can realize all orders beyond $q^{3\sqrt{q}\log q}$.

An improved Weil bound

It is possible to improve the Weil bounds for **simple** abelian varieties. For example, Kadets (following Aubry–Haloui–Lachaud) showed that for $q > 2$, if A is simple of dimension g, then with finitely many exceptions[†]

$$\#A(\mathbb{F}_q) \geq 1.359^g.$$

In particular, for $q > 2$ any given positive integer can only occur as the order of **finitely many** simple abelian varieties over $\mathbb{F}_q$.

By contrast, Madan–Pal (1970s) found[‡] **infinitely many** simple abelian varieties over $\mathbb{F}_2$ of order 1 (and even classified the Weil polynomials).

Kadets (2020) asked whether there are infinitely many simple abelian varieties over $\mathbb{F}_2$ of order 2. It is also natural to consider higher orders...

[†] Sample exceptions: over $\mathbb{F}_3$ and $\mathbb{F}_4$ there are elliptic curves of order 1.

[‡] Motivated by the class number one problem for function fields.

The main result

Theorem (K, July 2021)

For every positive integer m, there exist infinitely many simple abelian varieties over $\mathbb{F}_2$ of order m.

The method of proof is constructive: for **every** m we exhibit an explicit sequence of Weil polynomials corresponding to abelian varieties over $\mathbb{F}_2$ of order m. With some care, we can also ensure that these polynomials are (nearly) irreducible.

By contrast, I expect there are only finitely many Jacobians over $\mathbb{F}_2$ of order m, but this only seems to be known for $m = 1$ (Madan–Queen, Stirpe, Mercuri–Stirpe, Shen–Shi).

The method of proof does not ensure that we get **ordinary**, **geometrically simple**, or **principally polarizable** AVs.

Reduction steps

Any Weil polynomial of degree $2g$ for $q = 2$ has the form

$$T^g P(T + 2/T)$$

where $P(T) \in \mathbb{Z}[T]$ is a monic polynomial with all roots in $[-2\sqrt{2}, 2\sqrt{2}]$ and satisfies $\#A(\mathbb{F}_2) = P(3)$.

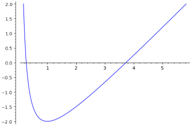
Following Madan–Pal (and R. Robinson), consider the polynomial

$$Q(T) = (-1)^{\deg P} P(3 - T),$$

which has roots in $[3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ and satisfies $\#A(\mathbb{F}_2) = |Q(0)|$. The roots of $Q(x)$ are totally positive algebraic integers of small norm, with all conjugates in a short interval.

Chebyshev polynomials and a substitution

Note that $x \mapsto x + x^{-1} - 4$ carries $[3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$ onto $[-2, 2]$.



Let T_n be the n-th Chebyshev polynomial for the normalization

$$T_n(2\cos\theta) = 2\cos n\theta.$$

Then

$$f_n(x) := x^n T_n(x + x^{-1} - 4)$$

is a polynomial with constant term 1 and all roots in $[3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$. Madan–Pal show[§] that this accounts for all AVs over $\mathbb{F}_2$ of order 1.

§ By reducing to Kronecker's theorem: every algebraic integer whose complex conjugates all have norm 1 is a root of unity.

A modified construction

Define

$$g_{n,k}(x) := (x-1)^{-k} \sum_{j=0}^{k} \binom{k}{j} f_{n+j}(x) \in \mathbb{Z}[x].$$

We will see shortly that $g_{n,k}(x)$ also has all roots in $[3-2\sqrt{2}, 3+2\sqrt{2}]$. Note that $|g_{n,k}(0)| = 2^k$.

More generally, we will give a condition on a sequence $a_0, \dots, a_k = 1$ of real numbers under which the polynomial

$$\sum_i a_i g_{n,i}(x)$$

has all roots in $[3-2\sqrt{2}, 3+2\sqrt{2}]$; see next slide.

Sketch of a proof (via winding numbers)

Theorem (K, July 2021)

For $a_0, \dots, a_k = 1 \in \mathbb{R}$ such that $\sum_{i=0}^k a_i z^i$ all $\mathbb{C}$-roots in the disc $|z| \leq \sqrt{2}$, $P_n(x) = \sum_i a_i g_{n,i}(x)$ has all $\mathbb{C}$-roots in $[3-2\sqrt{2}, 3+2\sqrt{2}]$.

Sketch of proof: for $\theta \in [0, 2\pi]$, put $y(\theta) = e^{2\pi i \theta}$ and let $x(\theta)$ be a root of

$$x(\theta) + x(\theta)^{-1} - 4 = 2\cos\theta = y(\theta) + y(\theta)^{-1}$$

varying continuously from $3+2\sqrt{2}$ to $3-2\sqrt{2}$. Now write

$$P_n(x(\theta)) = 2x(\theta)^n \mathrm{Re}\left(y(\theta)^n s(\theta)^k \sum_{i=0}^k a_i s(\theta)^{i-k} \right), \; s(\theta) = \frac{x(\theta)y(\theta)+1}{x(\theta)-1}$$

and compute complex arguments; since $|s(\theta)| = \sqrt{2}$, the sum over i is dominated by the term $i = k$.

A convenient choice

Each positive integer m has a unique **nonadjacent binary representation** (Reitwiesner, 1960):

$$m = \sum_{i=0}^{k} a_i 2^i \quad \text{where} \quad a_i \in \{-1, 0, 1\}, a_k = 1, \, a_i a_{i+1} = 0 \quad (i \geq 0).$$

The previous theorem applies to

$$h_{n,m}(x) := \sum_{i=0}^{k} (-1)^{i+k} a_i g_{n,i}(x),$$

for which $|h_{n,m}(0)| = m$: the nonadjacent condition implies

$$\sum_{i=0}^{k-1} |a_i| 2^{(i-k)/2} < 2^{-1} + 2^{-2} + \cdots = 1,$$

which implies that $\sum_{i=0}^{k} a_i z^i$ has all roots in $|z| \leq \sqrt{2}$.

Proof of the theorem: even order case

For any fixed choice of the a_i, the polynomials $P_n(x) = \sum_i a_i g_{n,i}(x)$ satisfy a second-order linear recurrence. This implies that any irreducible factor shared by two of the $P_n(x)$ must be a factor of some $f_n(x)$ (and so corresponds to a simple AV of order 1).

For m even, we can arrange (using either $h_{n,m}(x)$ or a slight variant) that the 2-adic Newton polygon forces an irreducible factor over $\mathbb{Q}_2$ of bounded codegree, and hence likewise over $\mathbb{Q}$. The cofactor is limited to a finite set, in which only polynomials with constant term ± 1 occur more than once; so the big irreducible factor usually has constant term $\pm m$.

Proof of the theorem: odd order case

For m odd, we can force $P_n(x+1)$ to be Eisenstein at 2!

Lemma

There exists a monic integer polynomial $Q(z)$ such that:

- $Q(2) = m$;
- $Q(z) \equiv (z-1)^{\deg Q(z)} \pmod{2}$; *and*
- $Q(z)$ *has all complex roots in the disc* $|z| < \sqrt{2}$.

(Then write $\sum_{i=0}^{k} a_i z^i = Q(z)$ and use these to form $P_n(x)$.)

Our proof of this is computational: we find explicit examples for $m \leq 350$, then compute larger examples by keeping track of the "quality"

$$\min\{|Q(z)| : |z| \geq \sqrt{2}\}.$$

Given enough examples of quality at least 7, we can continue via the rule

$$m \mapsto 15m + c \qquad (|c| \leq 7), \qquad Q(z) \mapsto (z^4 - 1)Q(z) + c.$$