Orders of abelian varieties over $\mathbb{F}_2$: a drama in five acts

Kiran S. Kedlaya

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

Number Theory Web Seminar
December 2, 2021

Supported by NSF (grants DMS-1802161, DMS-2053473) and UC San Diego (Warschawski Professorship).

The UC San Diego campus sits on unceded ancestral land of the Kumeyaay Nation. The Kumeyaay people continue to have an important and thriving presence in the region: https://www.kumeyaay.info. I am speaking from Washington, DC, the ancestral land of the Piscataway-Nacotchtank (Anacostian) people. For ancestral lands in your area, see https://native-land.ca/.

Orders and a formula of Weil

Throughout, let A be an abelian variety over a finite field $\mathbb{F}_q$. By the **order** of A, we mean the order of the group $A(\mathbb{F}_q)$ of rational points.

By Weil, the order of A equals $P(1)$ where $P(T) \in \mathbb{Z}[T]$ is* the characteristic polynomial of Frobenius acting on the ℓ-adic Tate module of A for any prime $\ell \nmid q$. This polynomial is monic of degree $2g$ where $g = \dim(A)$; its $\mathbb{C}$-roots lie on the circle $|T| = q^{1/2}$.

We call such a polynomial a q-**Weil polynomial**. There is built-in code in SageMath to enumerate Weil polynomials for specific q and g (or rather $d = 2g$):

```
sage: P.<x> = QQ[]
sage: l = P.weil_polynomials(q=2, d=12)
```

*This interpretation will play no further role in this talk! You can safely ignore it.

A converse theorem due to Honda–Tate

Theorem (Honda–Tate)

There is a one-to-one correspondence between isogeny classes of simple abelian varieties over $\mathbb{F}_q$ and irreducible q-Weil polynomials. Specifically, if A is a simple abelian variety over $\mathbb{F}_q$, then the characteristic polynomial of Frobenius on A equals $P(T)^e$ for some irreducible q-Weil polynomial $P(T)$ and some positive integer e.

Reminder: an **isogeny** of abelian varieties is a morphism $A \to A'$ which is surjective with finite kernel.

The integer e can be read off from $P(T)$; it is the Brauer index of the endomorphism algebra of A. When $q = p$, we always have $e = 1$ with the sole exception where $P(T) = T^2 - p$.

May algebraic number theory reign!

The upshot of Honda–Tate is that problems about existence of abelian varieties of a given order over a given $\mathbb{F}_q$ are really problems about existence of Weil polynomials with certain properties. We will thus not see (m)any abelian varieties in the sequel!

Aside: the order of the group $A(\mathbb{F}_q)$ is an isogeny invariant, but the isomorphism class of this group is not. Hence questions about existence of abelian varieties with a given group structure require additional ideas; cf. work of Marseglia–Springer.

An order estimate derived from Weil

Let A be an abelian variety of dimension g over $\mathbb{F}_q$. By Weil,

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

For $q \gg 0$ this means that certain integers get "skipped over" when we consider the possible orders of abelian varieties over $\mathbb{F}_q$. But this doesn't happen for $q = 2$...

All orders can be found over $\mathbb{F}_2$

Theorem (Howe–K)

Every positive integer is the order of **at least one** *abelian variety over* $\mathbb{F}_2$.

More precisely, we show that every positive integer in the range

$$\left[\left\lceil \frac{4}{3}2^{d-1}+1 \right\rceil, \left\lfloor \frac{4}{3}2^{d}+1 \right\rfloor\right]$$

occurs as $P(1)$ for some 2-Weil polynomial of degree $2d$.

We can also ensure that the Weil polynomial is **ordinary**, meaning that its middle coefficient is coprime to q (i.e., odd). Geometrically, this means that the resulting abelian variety has 2-torsion subgroup over $\overline{\mathbb{F}}_2$ of rank d, the largest possible.

A polynomial's complex roots, controlled

Lemma (DiPippo–Howe)

For q a prime power, let $(a_1, \dots, a_n)$ be a sequence of real numbers with

$$\left|\frac{a_n}{q^{n/2}}\right| + \sum_{i=1}^{n-1} \left|\frac{a_i}{q^{i/2}}\right| < 1.$$

Then the complex roots of the polynomial

$$f(z) = z^{2n} + a_1 z^{2n-1} + \cdots + a_{n-1} z^{n+1} + a_n z^n + q a_{n-1} z^{n-1} + \cdots + q^{n-1} a_1 z + q^n$$

are pairwise distinct and lie on the circle $|z| = \sqrt{q}$.

Key idea:[†] on the circle $|z| = \sqrt{q}$, $f(z)/z^n$ is real-valued and its values at $2n$-th roots of unity alternate in sign.

[†]Thanks to Bjorn Poonen for suggesting this argument

Integers in binary, but signed

Lemma (Howe–K)

Every positive integer can be realized as $f(1)$ for some integer polynomial $f(z)$ as above. We can further ensure that the central coefficient is odd.

This is an easy variation on the fact that every positive integer m admits a unique **nonadjacent binary representation**[‡] (Reitwiesner, 1960):

$$m = \sum_{i=0}^{n} a_i 2^i, \qquad a_i \in \{-1, 0, 1\}, \qquad a_i a_{i+1} = 0.$$

By Honda–Tate, $f(z)$ is the Weil polynomial of an abelian variety of order $f(1)$.

[‡]This fact is handy in computer algebra, particularly for efficient arithmetic in elliptic curve cryptography.

But what about the case of larger q?

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

For every prime power q, every **sufficiently large** *positive integer is the order of at least one abelian variety over $\mathbb{F}_q$. One can further ensure that the AV is ordinary, simple (or even geometrically simple), and principally polarizable (at the expense of changing the "sufficiently large" cutoff).*

The point is that for fixed q, the Weil bounds

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

do start to overlap once g is large enough. While not every integer permitted by the Weil bounds occurs, one can construct a large enough subinterval consisting of integers that do occur to achieve the desired overlap (improving on results of Aubry–Haloui–Lachaud and Kadets).

Simplicity means Weil's bound isn't best

Theorem (Kadets, after Aubry–Haloui–Lachaud)

For every prime power $q > 2$, for every **simple** *abelian variety A over $\mathbb{F}_q$ of dimension g, we have $\#A(\mathbb{F}_q) > 2^{g/2}$* **unless** *$q \in \{3, 4\}$ and $g = 1$.*

For $q \geq 7$ this is immediate from the Weil bound. For smaller q, this uses a standard technique of Cassels to identify algebraic integers of small trace/norm.

For $q = 2$, this is totally false! We end up running into a "threshold" of a sort studied in detail by R. Robinson.[§]

[§]Tangential note: A. Smith has recently made some progress on the closely related **Schur–Siegel–Smyth trace problem**.

The order 1 case: work of Madan–Pal

Theorem (Madan–Pal, Robinson)

Let A be a simple abelian variety over $\mathbb{F}_q$ of order 1.

(a) *We have $q \leq 4$.*

(b) *If $q \in \{3, 4\}$, then $\dim(A) = 1$; moreover, there is a unique isogeny class that occurs.*

(c) *If $q = 2$, then every Frobenius eigenvalue α of A satisfies*

$$\alpha^2 + (\eta - 1)\alpha - 2\eta = 0$$

for some root of unity η. The roots of unity of order n give rise to two distinct isogeny classes when $n = 7, 30$ and otherwise to one.

Key idea: $\eta = \frac{\alpha-1}{\overline{\alpha}-1}$ is an algebraic unit (because $\mathrm{Norm}(\alpha - 1) = 1$) whose conjugates all have $\mathbb{C}$-norm 1, so by Kronecker η is a root of unity.

Each order shows up many, many times

Theorem (K)

Every positive integer is the order of **infinitely many** *simple abelian varieties over* $\mathbb{F}_2$.

The main step is to construct infinite sequences of 2-Weil polynomials realizing a particular order. It seems quite hard to do this by direct methods; we instead proceed by tweaking the polynomials given by the Madan–Pal construction.

Some difficulty arises in trying to ensure that we produce enough **irreducible** Weil polynomials for a fixed order. We handle this by ensuring irreducibility[¶] over $\mathbb{Q}_2$ (variants of the Schönemann–Eisenstein criterion).

[¶] Technical note: we only prove irreducibility up to a bounded cofactor. We then use the fact that our sequence of polynomials satisfies a second-order linear recurrence to show that any factor which occurs more than once corresponds to an AV of order 1.

Some sequences derived from Chebyshëv

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

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

For $n \geq 0$, define the polynomial $f_n(x)$ of degree $2n$ by the formula

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

For $n, k \geq 0$, define the rational function (actually a polynomial)

$$g_{n,k}(x) = (x-1)^{-k} \sum_{j=0}^{k} \binom{k}{j} f_{n+j}(x);$$

note that $g_{n,k}(x) = (-2)^k$.

Another case of complex root control

Lemma (K)

Let $a_0, \dots, a_k$ be a sequence of real numbers with $a_k = 1$, such that the polynomial $Q(z) = \sum_{i=0}^{k} a_i z^i$ has all of its complex roots inside the disc $|z| < \sqrt{2}$. Then for each $n \geq 0$, the roots of the polynomial

$$P_n(x) = \sum_{i=0}^{k} a_i g_{n,i}(x)$$

are real, pairwise distinct, and contained in $[3 - 2\sqrt{2}, 3 + 2\sqrt{2}]$.

Key step: reduce to an instance of Rouché's theorem on winding numbers.

The point: $P_n(3 - x)$ has roots in $[-2\sqrt{2}, 2\sqrt{2}]$, which are of the form $\alpha + \overline{\alpha}$ where α is a root of a 2-Weil polynomial $R(T)$ with $R(1) = \pm P_n(1)$.

Simplicity: the geometric case

An abelian variety A over $\mathbb{F}_q$ is **geometrically simple** if its base extension to any finite extension of $\mathbb{F}_q$ (or equivalently, to an algebraic closure) is simple. If the characteristic polynomial of A is irreducible, this happens if and only if there are no two Frobenius eigenvalues α_1, α_2 of A such that α_1/α_2 is a nontrivial root of unity.

We expect that for any given $m > 1$, there exist infinitely many geometrically simple abelian varieties of order m. However, for $m = 1$ we have no control over the Weil polynomials; all we can do is look at the Madan–Pal construction to see what happens.

Inspection of the list of Madan–Pal

Theorem (D'Nelly-Warady–K)

Let A_n be a simple abelian variety[a] of order 1 over $\mathbb{F}_2$ corresponding to a primitive n-th root of unity. Then $A_{\overline{\mathbb{F}}_2}$ is isogenous to B^f for some simple abelian variety B over $\overline{\mathbb{F}}_2$, where

$$f = \begin{cases} 1 & n \text{ is a power of } 2 \text{ and } n \neq 4 \\ 2 & n = 4, \text{ or } n \text{ is not a power of } 2 \text{ and } n \neq 7, 30 \\ 3 & n = 7 \\ 4 & n = 30. \end{cases}$$

[a] Reminder: A_n is determined by n up to isogeny unless $n = 7, 30$.

Aside: A is ordinary if and only if n is not a power of 2. Hence no simple abelian variety of order 1 over $\mathbb{F}_2$ is both ordinary and geometrically simple.

Equations solved for roots of unity

Let α_1, α_2 be Frobenius eigenvalues of (possibly different) simple abelian varieties of order 1 over $\mathbb{F}_2$. If α_1/α_2 is a root of unity, then there exist three roots of unity η_1, η_2, η_3 satisfying

$$\alpha_1^2 + (\eta_1 - 1)\alpha_1 - 2\eta_1 = \alpha_2^2 + (\eta_2 - 1)\alpha_2 - 2\eta_2 = \alpha_1 - \eta_3\alpha_2 = 0.$$

Eliminating α_1, α_2 yields a polynomial in the three variables η_1, η_2, η_3, which we want to solve in roots of unity. We use the method of Conway–Jones, plus some SageMath code from the classification of tetrahedra with rational dihedral angles (K–Kolpakov–Poonen–Rubinstein).

The function fields whose class number is one

Theorem (Leitzel–Madan–Queen, Mercuri–Stirpe, Shen–Shi)

There are exactly ~~seven~~ eight isomorphism classes of function fields of positive genus over finite fields for which the class number is equal to 1*. That is, these fields correspond to curves whose Jacobians have order* 1*.*

Except for elliptic curves over $\mathbb{F}_3$ and $\mathbb{F}_4$, all of these are over $\mathbb{F}_2$. Leitzel–Madan–Queen found five examples of genera ≤ 3 and claimed this list was complete; later Stirpe found a new example of genus 4, and Mercuri–Stirpe and Shen–Shi corrected the proof.

Extensions coming from the constant field

Theorem (K, in preparation)

Let C be a curve of genus g over $\mathbb{F}_q$ such that $\#J(C)(\mathbb{F}_q) = \#J(C)(\mathbb{F}_{q^d})$ for some $d > 1$. Then

$$(q, d, g) \in \{(2,2,1), (2,2,2), (2,2,3), (2,3,1), (3,2,1), (4,2,1)\}.$$

There is a natural map from $J(C)$ to the Weil restriction of its base extension to $\mathbb{F}_{q^d}$; the cokernel A is an abelian variety of order 1. The Frobenius eigenvalues of A are of the form $\zeta_d^i \alpha$ where α is a Frobenius eigenvalue of C and $i \in \{1, \dots, d-1\}$. The analysis with D'Nelly-Warady now handles the case $d > 2$.

When $d = 2$, A is the quadratic twist of $J(C)$. The inequality

$$\#C(\mathbb{F}_{q^2}) \geq \#C(\mathbb{F}_q)$$

restricts A enough to complete the classification.

Extensions coming from geometry

Theorem (K, in preparation)

Let $C' \to C$ be a morphism of curves of degree > 1 over $\mathbb{F}_q$ such that $\#J(C)(\mathbb{F}_q) = \#J(C')(\mathbb{F}_q)$. Let g, g' be the genera of C, C'. If $g' > g$ and $q > 2$, then $q \in \{3, 4\}$ and

$$(g, g') \in \begin{cases} \{(0,1),(1,2),(1,3),(2,3),(2,4),(3,5)\} & q = 3 \\ \{(0,1),(1,2),(2,3),(2,4)\} & q = 4; \end{cases}$$

moreover, the complete list of possible isomorphism classes of C and C' is known (there are 21 such pairs).

Sketch: the Prym variety A of $C' \to C$ has order 1. Use this plus the bound $\#C'(\mathbb{F}_q) \geq 0$ to get a lower bound on $\#C(\mathbb{F}_q)$, then compare with a "linear programming" bound on $\#C(\mathbb{F}_q)$ (Oesterlé, Serre).

The last frontier: the case over $\mathbb{F}_2$

Theorem (K, in preparation)

Let $C' \to C$ be a morphism of curves of degree $d > 1$ over $\mathbb{F}_2$ such that $g' > g$ and $\#J(C)(\mathbb{F}_2) = \#J(C')(\mathbb{F}_2)$. Then $g \leq 7, g' \leq 13$.

Again, the Prym variety has order 1, but this leaves many options. From the linear programming method, we get bounds on certain weighted combinations of $\#C(\mathbb{F}_2), \#C(\mathbb{F}_4), \ldots$; tuning parameters to get a bound which is suitably compatible with the Madan–Pal list gives roughly this bound. (A bit of exhaustion over Weil polynomials is needed to sharpen the result.)

The morphisms of this type are all Galois

Theorem (K, in preparation)

Let $f : C' \to C$ be a morphism of curves of degree $d > 1$ over $\mathbb{F}_q$ such that $g(C) > 1$ and $\#J(C)(\mathbb{F}_2) = \#J(C')(\mathbb{F}_2)$. Then f is Galois (but not necessarily étale) and cyclic.

We first collect all possible pairs of possible Weil polynomials of C and C'; there are about 70 such pairs with $d > 2$. We then work out how closed points of C split in C', then transfer this knowledge to other quotients of the Galois closure (and to isogeny factors of their Jacobians).

To complete the classification, it thus remains to find all the cyclic covers. This would be straightforward in Magma **if** we had a complete census of curves of genus ≤ 7 over $\mathbb{F}_2$. To date this is only done up to genus 4 (Xarles); genus 5 is in progress (Dragutinović), and genus 6 and 7 should be feasible thanks to Mukai's descriptions of canonical curves.

The list of papers that I drew upon

R. van Bommel, E. Costa, W. Li, B. Poonen, and A. Smith, Abelian varieties of prescribed order over finite fields, arXiv:2106.13651v1 (2021).
J.H. Conway and A.J. Jones, Trigonometric diophantine equations (On vanishing sums of roots of unity), *Acta Arith.* **30** (1976), 229–240.
T. D'Nelly-Warady and K.S. Kedlaya, Geometric decomposition of abelian varieties of order 1, arXiv:2109.03986v1 (2021).
D. Dragutinović, Supersingular curves of genera four and five in characteristic two, Masters thesis, Utrecht University, 2021.
E.W. Howe[‖] and K.S. Kedlaya, Every positive integer is the order of an ordinary abelian variety over $\mathbb{F}_2$, *Research in Number Theory* **7** (2021), article number 59.
K.S. Kedlaya, Search techniques for root-unitary polynomials, in *Computational Arithmetic Geometry*, Contemporary Math. 463, Amer. Math. Soc., 2008, 71–82.
K.S. Kedlaya, Abelian varieties over $\mathbb{F}_2$ of prescribed order, arXiv:2107.12453v2 (2021).
K.S. Kedlaya, The relative class number one problem for function fields, I, draft preprint.
K.S. Kedlaya, The relative class number one problem for function fields, II, in preparation.
K.S. Kedlaya, A. Kolpakov, B. Poonen, and M. Rubinstein, Space vectors forming rational angles, arXiv:2011.14232v1 (2020).
S. Marseglia and C. Springer, Every finite abelian group is the group of rational points of an ordinary abelian variety over $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_5$, arXiv:2105.08125v2 (2021).
S. Mukai, Curves and Grassmannians, in *Algebraic Geometry and Related Topics*, International Press, Cambridge, MA, 1993, 19–40.
S. Mukai, Curves and symmetric spaces, I, *Amer. J. Math.* **117** (1995), 1627–1644.
J.-P. Serre, *Rational Points on Curves over Finite Fields*, Doc. Math. 8, Soc. Math. France, 2020.
A. Smith, Algebraic integers with conjugates in a prescribed distribution, preprint.
X. Xarles, A census of all genus 4 curves over the field with 2 elements, arXiv:2007.07822v1 (2020).

[‖] That's **Reverend** Everett W. Howe to the rest of us.