Counting isogenous principally-polarized abelian varieties over finite fields

Everett W. Howe

Center for Communications Research, La Jolla

Arithmetic of Low-Dimensional Abelian Varieties
ICERM, 3–7 June 2019

(Corrected and edited slides)

email: however@alumni.caltech.edu Web site: ewhowe.com Twitter: @howe

Motivations

Formative mathematical experiences

Undergraduate: Single-variable complex analysis

- Does a continuous $f\colon \mathbb{C} \to \mathbb{C}$ satisfy the Cauchy–Riemann relations?
  Then it's infinitely differentiable!
- Got an open simply-connected proper subset of $\mathbb{C}$?
  It's conformally equivalent to the interior of the unit disk!
- Got an intractable integral on the real line to compute?
  Use Cauchy's theorem to find its value!
- Life is beautiful and every nice thing is true.

Graduate school: Several complex variables

- Life is brutal and short. Give up now.
- That's literally all I remember from my several complex variables class.

Life lesson: One-dimensional objects are friendly and fun to work with.

One-dimensional objects and their friends

Number rings

- Maximal orders; non-maximal orders
- Ideals; ideal class groups
- Modules over number rings aren't necessarily one-dimensional, but they're still pretty friendly

Curves, and things to study about them

- Over $\mathbb{Q}$: Number of rational points; *finding* rational points; ...
- Over finite fields: Curves with many points for their genus, or few; distribution of Frobenius eigenvalues; ...
- Over any field: Automorphism groups; decomposition of Jacobians; ...

...Hold on there bucko, Jacobians are higher-dimensional objects!

The dream

Can we understand Jacobians, general abelian varieties, polarizations, and so forth, using *one-dimensional objects*?

Deligne (1969)

For ordinary abelian varieties over finite fields: *yes*.

Centeleghe and Stix (2015)

For (not quite completely general) abelian varieties over finite *prime* fields: *yes*.

This talk:

I will sketch Deligne's result and some follow-on work, and use it to address the question of determining the number of principally-polarized varieties in a simple ordinary isogeny class.

Deligne modules

Ordinary abelian varieties

Suppose

- k is a finite field of characteristic p,
- A is a g-dimensional abelian variety over k,
- f is the characteristic polynomial of Frobenius (the *Weil polynomial*) for A. ($f \in \mathbb{Z}[x]$ is monic, degree $2g$, and its complex roots have magnitude $\sqrt{q}$.)

We say that A is ordinary if one of the following equivalent conditions holds:

- $\#A(\overline{k})[p] = p^g$;
- The local-local group scheme α_p can't be embedded into A;
- Exactly half of the roots of f in $\overline{\mathbb{Q}}_p$ are p-adic units;
- The middle coefficient of f (that is, the coefficient of x^g) is coprime to p.

The category of Deligne modules

We define the category $\mathcal{L}_q$ of Deligne modules over $\mathbb{F}_q$ by specifying its objects and morphisms.

Objects

Pairs (T, F), where:

- T is a finitely-generated free $\mathbb{Z}$-module of even rank, and
- F is an endomorphism of T such that
  - The endomorphism $F \otimes \mathbb{Q}$ of the $\mathbb{Q}$-vector space $T \otimes \mathbb{Q}$ is semi-simple, and its complex eigenvalues have magnitude $\sqrt{q}$;
  - Exactly half of the roots in $\overline{\mathbb{Q}}_p$ of the characteristic polynomial of F are p-adic units;
  - There is an endomorphism V of T with $FV = q$.

Morphisms from (T_1, F_1) to (T_2, F_2)

$\mathbb{Z}$-module morphisms $\varphi\colon T_1 \to T_2$ such that $F_2\varphi(x) = \varphi(F_1 x)$ for all $x \in T_1$.

Deligne's equivalence of categories

Theorem (Deligne, 1969)

There is an equivalence between the category of ordinary abelian varieties over $\mathbb{F}_q$ and the category $\mathcal{L}_q$ that takes g-dimensional varieties to pairs (T, F) with $\operatorname{rank}_{\mathbb{Z}} T = 2g$.

The equivalence requires a nasty choice

Let W be the ring of Witt vectors over $\overline{\mathbb{F}}_q$. Let ε be an embedding of W into $\mathbb{C}$.

$$A/\mathbb{F}_q \rightsquigarrow \text{Serre–Tate canonical lift of } A \text{ over } W$$
$$\rightsquigarrow \widetilde{A}/\mathbb{C} := \text{base extension of the canonical lift to } \mathbb{C} \text{ via } \varepsilon$$

Let $T = H_1(\widetilde{A})$; let F be the lift of Frobenius. The equivalence sends A to (T, F).

Extending the equivalence: Dual varieties

Definition

Given (T, F) in $\mathcal{L}_q$, let $\widehat{T} = \mathrm{Hom}(T, \mathbb{Z})$, so there is a natural pairing $T \times \widehat{T} \to \mathbb{Z}$. Let $\widehat{F}$ be the endomorphism of $\widehat{T}$ such that for all $x \in T$ and $y \in \widehat{T}$ we have

$$(x, \widehat{F}y) = (Vx, y).$$

The dual of (T, F) is $(\widehat{T}, \widehat{F})$.

Theorem (H., 1995)

Deligne's equivalence respects duality.

Extending the equivalence: Polarizations

Given $(T, F) \in \mathcal{L}_q$, let

$$R = \mathbb{Z}[F, V] \subseteq \mathrm{End}(T, F)$$
$$K = R \otimes \mathbb{Q} = \prod K_i$$

The p-adic valuation v on $\overline{\mathbb{Q}} \subset \mathbb{C}$ obtained from $\varepsilon\colon W \hookrightarrow \mathbb{C}$ gives a CM-type on K:

$$\Phi := \{\varphi : K \to \mathbb{C} \mid v(\varphi(F)) > 0\}.$$

Let ι be a totally imaginary element of K such that

$$\forall \varphi \in \Phi : \varphi(\iota) \text{ is positive imaginary.}$$

(We say that such an ι is Φ-positive.)

Polarizations, continued

Suppose λ is an isogeny from (T, F) to its dual $(\widehat{T}, \widehat{F})$.
This gives us a pairing $b : T \times T \to T \times \widehat{T} \to \mathbb{Z}$.

Definition

The isogeny λ is a polarization if

- The pairing b is alternating, and
- The pairing $(x, y) \mapsto b(\iota x, y)$ on $T \times T$ is symmetric and positive definite.

Theorem (H., 1995)

Deligne's equivalence takes polarizations to polarizations.

Applications

Principally-polarized varieties with maximal endomorphism rings

Consider a simple ordinary isogeny class I over $\mathbb{F}_q$ with Weil polynomial f.
Let K be the number field defined by f, and let $\mathcal{O}$ be the maximal order in K.
Let ι be a Φ-positive element as above, and let $\mathfrak{d}$ be the different of $\mathcal{O}$.

Under Deligne's equivalence:

$$\{A \in I \text{ with } \mathrm{End}\, A \cong \mathcal{O}\}/\cong \longleftrightarrow \{\text{fractional ideals } \mathfrak{A} \text{ of } \mathcal{O}\}/\sim$$

$$\text{dual } \widehat{A} \text{ of } A \longleftrightarrow \text{ideal } \mathfrak{d}^{-1}\overline{\mathfrak{A}}^{-1}$$

$$\text{principal polarization of } A \longleftrightarrow \text{totally positive } x \in K^+ \text{ with } \iota x\mathfrak{A} = \mathfrak{d}^{-1}\overline{\mathfrak{A}}^{-1}$$

So $x \gg 0$ gives a principal polarization of $\mathfrak{A}$ if and only if $x\mathfrak{A}\overline{\mathfrak{A}} = (\iota\mathfrak{d})^{-1}$.
That is, $\mathfrak{A}\overline{\mathfrak{A}}$ and $(\iota\mathfrak{d})^{-1}$ give the same element of the narrow class group of $\mathcal{O}^+$.

Maximal endomorphism rings, continued

Theorem (essentially Deligne plus Shimura, see [H. 1995])

If the norm map $\operatorname{Pic}\mathcal{O} \to \operatorname{Pic}^+\mathcal{O}^+$ *is surjective, there are* $\#\operatorname{Pic}\mathcal{O}/\#\operatorname{Pic}^+\mathcal{O}^+$ *principally-polarizable varieties* $A/\mathbb{F}_q$ *with Weil polynomial* f *and with* $\operatorname{End} A \cong \mathcal{O}$.

The number of non-isomorphic principal polarizations on such an A *is equal to the index of the norms of the units of* $\mathcal{O}$ *in the totally-positive units of* $\mathcal{O}^+$.

If $\operatorname{Pic}\mathcal{O} \to \operatorname{Pic}^+\mathcal{O}^+$ is *not* surjective, then there are either no such A or there are $2(\#\operatorname{Pic}\mathcal{O}/\#\operatorname{Pic}^+\mathcal{O}^+)$ of them. [H. 1995] says how to determine which.

[$\operatorname{Pic}\mathcal{O} \to \operatorname{Pic}^+\mathcal{O}^+$ is surjective exactly when K/K^+ is ramified at a finite prime.]

Generalizing to non-maximal orders

Suppose $A/\mathbb{F}_q$ is a simple ordinary abelian variety with Weil polynomial f,
let K be the number field defined by f,
and let $\pi \in K$ be a root of f.

We know that $\mathbb{Z}[\pi, \overline{\pi}] \subseteq \mathrm{End}\, A \subseteq \mathcal{O}$.

If A has a principal polarization then $\mathrm{End}\, A$ is stable under complex conjugation.

Question

If R is an order with $\mathbb{Z}[\pi, \overline{\pi}] \subseteq R \subseteq \mathcal{O}$ that is stable under complex conjugation, is there a Picard group formula for the number of principally-polarized varieties with endomorphism ring R?

Digression on Gorenstein rings

An order R in a number field is Gorenstein if every fractional R-ideal $\mathfrak{A}$ with $\operatorname{End}\mathfrak{A} = R$ is actually an *invertible* R-ideal.

Convenient facts about Gorenstein rings

- An order R is Gorenstein if and only if its trace dual is invertible (as a fractional R-ideal).
- A ring that is a complete intersection over $\mathbb{Z}$ is Gorenstein.
- In particular, every monogenic order $\mathbb{Z}[\alpha]$ is Gorenstein.

Picard groups are formed from invertible ideals, so...

If we want a Picard group formula for the number of (polarized) Deligne modules with a given endomorphism ring, Gorenstein rings come up naturally.

Convenient orders

An order R in K is convenient if it satisfies the following properties:

1. R is stable under complex conjugation;
2. the order $R^+ := R \cap K^+$ of K^+ is Gorenstein; and
3. the trace dual of R is generated (as a fractional R-ideal) by its pure imaginary elements.

Originally I included a fourth assumption — that R be Gorenstein — but Marseglia observed that that follows from (1)–(3).

Note that $\mathcal{O}$ and $\mathbb{Z}[\pi, \overline{\pi}]$ are both convenient.

Principally-polarized varieties with convenient endomorphism rings

Theorem (H., 2019?)

Let $R \supseteq \mathbb{Z}[\pi, \overline{\pi}]$ be a convenient order.

If the norm map $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is surjective, there are $\#\operatorname{Pic} R / \#\operatorname{Pic}^+ R^+$ principally-polarizable varieties $A/\mathbb{F}_q$ with Weil polynomial f and with $\operatorname{End} A \cong R$.

The number of non-isomorphic principal polarizations on such an A is equal to the index of the norms of the units of R in the totally-positive units of R^+.

If $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ is not surjective, we will still have principally-polarizable varieties with endomorphism ring R as long as $\iota R^\dagger$ (which can be viewed as an ideal of R^+) lies in the image of $\operatorname{Pic} R$ under the norm map. This is a computable condition. [H. 1995]

Remarks

Some useful ancillary results:

Theorem

Suppose $R \supseteq \mathbb{Z}[\pi, \overline{\pi}]$ is an order that is stable under complex conjugation and such that R^+ is Gorenstein.

If there are elements α, β of R and fractional ideals $\mathfrak{A}$ and $\mathfrak{B}$ of R^+ such that $R = \mathfrak{A} \cdot \alpha + \mathfrak{B} \cdot \beta$, then R is convenient.

Theorem

Let $R \supseteq \mathbb{Z}[\pi, \overline{\pi}]$ be a convenient order.

If K/K^+ is ramified at a finite prime that does not divide the conductor of R^+, then the norm map $\mathrm{Pic}\, R \to \mathrm{Pic}^+ R^+$ is surjective.

(*At this point in the talk, I gave an example on the whiteboard of a simple application of the ideas I had discussed, one that showed that having these Picard group formulas can be useful. In particular, I reviewed the argument of my 2004 paper* On the nonexistence of certain curves of genus two *in light of the idea of convenient orders.*)

(*Afterwards, I skipped the following section on "Rough estimates" and went straight to the slide on "Further questions."*)

Rough estimates

Estimating the number of principally-polarized varieties

If R is convenient, define the *minus class number* $h^-(R)$ to be $\#\operatorname{Pic} R / \#\operatorname{Pic} R^+$.

Combining the formulas for the number of principally-polarizable varieties and the number of principal polarizations for a given variety, we find:

Theorem

Let $R \supseteq \mathbb{Z}[\pi, \overline{\pi}]$ be a convenient order with $\operatorname{Pic} R \to \operatorname{Pic}^+ R^+$ surjective.

The number of principally-polarized varieties (A, λ) with $\operatorname{End} A \cong R$ is equal to either $h^-(R)$ or $h^-(R)/2$.

Estimates of minus class numbers

For convenient orders R, let Δ_R^- denote $|\Delta_R/\Delta_{R^+}|$.

Theorem (Louboutin 2006)

For every $\varepsilon > 0$, as K ranges over CM-fields of fixed degree we have

$$(\Delta_{\mathcal{O}_K}^-)^{1/2-\varepsilon} \ll h^-(\mathcal{O}_K) \ll (\Delta_{\mathcal{O}_K}^-)^{1/2+\varepsilon}.$$

Remarks

- Louboutin's actual statements are much more precise than "$\pm\varepsilon$".
- This rough version is easily extended to convenient orders.

We will simply write $h^-(\mathcal{O}_K) \approxeq (\Delta_{\mathcal{O}_K}^-)^{1/2}$ for the relation in the theorem.

Estimates of minus discriminants

When $R = \mathbb{Z}[\pi, \overline{\pi}]$, we have a formula for Δ_R^- in terms of the Frobenius angles

$$0 \le \theta_1 < \theta_2 < \cdots < \theta_n \le \pi$$

for the n-dimensional abelian variety $A/\mathbb{F}_q$.

Theorem (See Gerhard–Williams 2017, for example)

If $R = \mathbb{Z}[\pi, \overline{\pi}]$, we have

$$(\Delta_R^-)^{1/2} = 2^{n(n+1)/2} q^{n(n+1)/4} \prod_{i<j} (\cos\theta_i - \cos\theta_j) \prod_i \sin\theta_i.$$

Heuristic connections to Katz–Sarnak distribution

For fixed dimension, and for $R = \mathbb{Z}[\pi, \overline{\pi}]$, the number of principally-polarized (A, λ) with $\mathrm{End}\, A \cong R$ is roughly

$$h^-(R) \approxeq (\Delta_R^-)^{1/2} \approxeq q^{n(n+1)/4} \prod_{i<j} (\cos\theta_i - \cos\theta_j) \prod_i \sin\theta_i.$$

Theorem (Vlăduţ 2001)

Fix n and $(\theta_1, \ldots, \theta_n)$. As $q \to \infty$, the number of isogeny classes of abelian varieties with Frobenius angles near $(\theta_1, \ldots, \theta_n)$ is better and better approximated by

$$c_n q^{n(n+1)/4} \prod_{i<j} (\cos\theta_i - \cos\theta_j) \prod_i \sin\theta_i \, \Delta\theta_1 \cdots \Delta\theta_n,$$

for an explicit constant c_n.

Combining rough estimates

Reckless and impetuous, we combine the first "equality" with Vlăduţ's result and boldly assert that the number of principally-polarized n-dimensional abelian varieties with Frobenius angles near $(\theta_1, \ldots, \theta_n)$ is approximately

$$d_n q^{n(n+1)/2} \prod_{i<j} (\cos\theta_i - \cos\theta_j)^2 \prod_i \sin^2\theta_i \, \Delta\theta_1 \cdots \Delta\theta_n$$

for some constant d_n.

This is exactly what is given by the Katz–Sarnak distribution [Katz–Sarnak 1999]!

Further questions

- Can the shady heuristics confirming the Katz–Sarnak distribution be made into an actual argument that proves anything at all?
- Are there formulas for the number of principally-polarized (A, λ) with $\mathrm{End}\, A$ an inconvenient order?
  (There are algorithms for computing this [Marseglia 2018].)
- What happens when you sum up over all orders between $\mathbb{Z}[\pi, \overline{\pi}]$ and $\mathcal{O}$?
- How to deal with the complications for non-simple isogeny classes?
- What analogous results do we get for the Centeleghe–Stix functor?