Mass formulae for supersingular abelian threefolds

Valentijn Karemaker
(Utrecht University & Stockholm University)

Joint work with F. Yobuko and C.-F. Yu

N^3 days XII

May 28, 2020

What is a mass (formula)?

Definition

Let S be a finite set of objects with finite automorphism groups. The MASS of S is the weighted sum

$$\mathrm{Mass}(S) = \sum_{s \in S} \frac{1}{|\mathrm{Aut}(s)|}.$$

A mass formula computes an expression for the mass.

Examples of mass formulae

Minkowski-Siegel mass formula

Let $S = \{$ even unimodular lattices of dimension $8k\}/\simeq$.
Then for $k > 0$,

$$\mathrm{Mass}(S) = \sum_{s \in S} \frac{1}{|\mathrm{Aut}(s)|} = \frac{|B_{4k}|}{8k} \prod_{j=1}^{4k-1} \frac{|B_{2k}|}{4j}.$$

Eichler-Deuring mass formula

Let $S = \{$ supersingular elliptic curves over $\overline{\mathbb{F}}_p\}/\simeq$. Then

$$\mathrm{Mass}(S) = \sum_{s \in S} \frac{1}{|\mathrm{Aut}(s)|} = \frac{p-1}{24}.$$

What set are we computing the mass of?

Let k be an algebraically closed field of characteristic p.

Let X/k be a three-dimensional abelian variety.
X/k is SUPERSINGULAR (resp. SUPERSPECIAL) if it is *isogenous* (resp. *isomorphic*) to a product of supersingular elliptic curves.

Let $\mathcal{S}_{3,1}$ be the moduli space of principally polarised supersingular abelian threefolds (X, λ).

For all primes $\ell \neq p$, we have $T_\ell(X) = X[\ell^\infty] \simeq \mathbb{Z}_\ell^6$.

Definition

For $x = (X_0, \lambda_0) \in \mathcal{S}_{3,1}(k)$, let

$$\Lambda_x = \{(X, \lambda) \in \mathcal{S}_{3,1}(k) : (X, \lambda)[p^\infty] \simeq (X_0, \lambda_0)[p^\infty]\}.$$

What set are we computing the mass of?

$$\Lambda_x = \{(X,\lambda) \in \mathcal{S}_{3,1}(k) : (X,\lambda)[p^\infty] \simeq (X_0,\lambda_0)[p^\infty]\}.$$

It is known that Λ_x is finite [Yu].

Goal

Compute $\mathrm{Mass}(\Lambda_x) = \sum_{x' \in \Lambda_x} |\mathrm{Aut}(x')|^{-1}$ for any $x \in \mathcal{S}_{3,1}$.

For $x = (X_0, \lambda_0) \in S_{3,1}(k)$, let $G_x/\mathbb{Z}$ be the automorphism group scheme such that for any commutative ring R,

$$G_x(R) = \{h \in (\mathrm{End}(X_0) \otimes_{\mathbb{Z}} R)^\times : h'h = 1\}.$$

Then there is a bijection

$$\Lambda_x \simeq G_x(\mathbb{Q}) \backslash G_x(\mathbb{A}_f) / G_x(\widehat{\mathbb{Z}}),$$

so $$\mathrm{Mass}(\Lambda_x) = \mathrm{vol}(G_x(\mathbb{Q}) \backslash G_x(\mathbb{A}_f)) = \mathrm{Mass}(G_x, G_x(\widehat{\mathbb{Z}})).$$

How do we describe $\mathcal{S}_{3,1}$?

Let $E/\mathbb{F}_{p^2}$ be a supersingular elliptic curve with $\pi_E = -p$.
Let μ be any principal polarisation of E^3.

Definition

A POLARISED FLAG TYPE QUOTIENT (PFTQ) WITH RESPECT TO μ is a chain

$$(E^3, p\mu) =: (Y_2, \lambda_2) \xrightarrow{\rho_2} (Y_1, \lambda_1) \xrightarrow{\rho_1} (Y_0, \lambda_0)$$

such that $\ker(\rho_1) \simeq \alpha_p$, $\ker(\rho_2) \simeq \alpha_p^2$, and $\ker(\lambda_i) \subseteq \ker(V^j \circ F^{i-j})$ for $0 \le i \le 2$ and $0 \le j \le \lfloor i/2 \rfloor$.

Let $\mathcal{P}_\mu$ be the moduli space of PFTQ's.
It is a two-dimensional geometrically irreducible scheme over $\mathbb{F}_{p^2}$.

How do we describe $\mathcal{S}_{3,1}$?

An PFTQ w.r.t. μ is $(E^3, p\mu) =: (Y_2, \lambda_2) \xrightarrow{\rho_2} (Y_1, \lambda_1) \xrightarrow{\rho_1} (Y_0, \lambda_0)$.

It follows that $(Y_0, \lambda_0) \in \mathcal{S}_{3,1}$, so there is a projection map

$$\begin{aligned} \mathrm{pr}_0 : \mathcal{P}_\mu &\to \mathcal{S}_{3,1} \\ (Y_2 \to Y_1 \to Y_0) &\mapsto (Y_0, \lambda_0) \end{aligned}$$

such that $\coprod_\mu \mathcal{P}_\mu \to \mathcal{S}_{3,1}$ is surjective and generically finite.

Slogan

Each $\mathcal{P}_\mu$ approximates a geom. irreducible component of $\mathcal{S}_{3,1}$.

How do we describe $\mathcal{P}_\mu$?

Let $C : t_1^{p+1} + t_2^{p+1} + t_3^{p+1} = 0$ be a Fermat curve in $\mathbb{P}^2$.
It has genus $p(p-1)/2$ and admits a left action by $U_3(\mathbb{F}_p)$.

Then $\pi : \mathcal{P}_\mu \simeq \mathbb{P}_C(\mathcal{O}(-1) \oplus \mathcal{O}(1)) \to C$ is a $\mathbb{P}^1$-bundle.
There is a section $s : C \to T \subseteq \mathcal{P}_\mu$.

Upshot

For each (X, λ) there exist a μ and a $y \in \mathcal{P}_\mu$ such that $\mathrm{pr}_0(y) = [(X, \lambda)]$.
This y is uniquely characterised by a pair (t, u) with $t = (t_1 : t_2 : t_3) \in C(k)$ and $u = (u_1 : u_2) \in \pi^{-1}(t) \simeq \mathbb{P}^1_t(k)$.

The structure of $\mathcal{P}_\mu$

$\pi : \mathcal{P}_\mu \simeq \mathbb{P}_C(\mathcal{O}(-1) \oplus \mathcal{O}(1)) \to C$ has section $s : C \to T \subseteq \mathcal{P}_\mu$

Definition

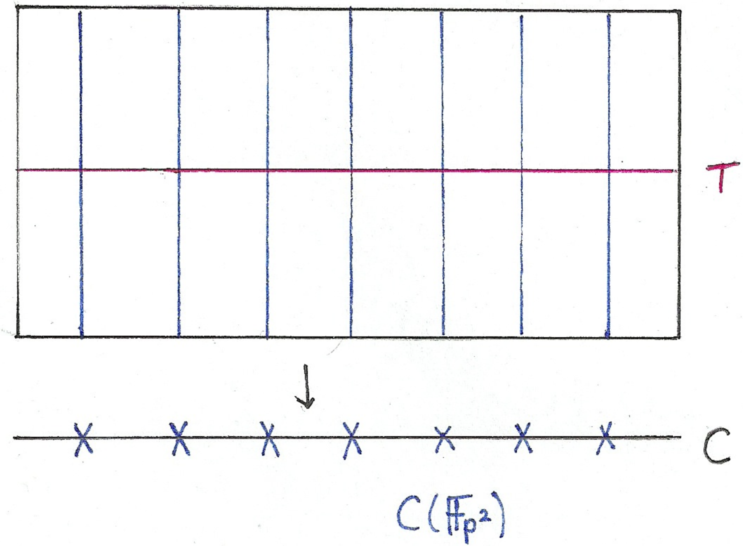
Let X/k be an abelian variety. Its a-NUMBER is

$$a(X) := \dim_k \mathrm{Hom}(\alpha_p, X).$$

For a PFTQ $y = (Y_2 \to Y_1 \to Y_0)$, we say $a(y) = a(Y_0)$.

- For a threefold X we have $a(X) \in \{1, 2, 3\}$, and $a(X) = 3 \Leftrightarrow X$ is superspecial.
- If $y \in T$, then $a(y) = 3$.
- For $t \in C(k)$, we have $t \in C(\mathbb{F}_{p^2}) \Leftrightarrow a(y) \geq 2$ for any $y \in \pi^{-1}(t)$.
- For $y \in \mathcal{P}_\mu$, we have $a(y) = 1 \Leftrightarrow y \notin T$ and $\pi(y) \notin C(\mathbb{F}_{p^2})$.

The structure of $\mathcal{P}_\mu$: a picture



Using PFTQ's to construct minimal isogenies

Any supersingular abelian variety X admits a MINIMAL ISOGENY

$$\varphi : Y \to X$$

from a *superspecial* abelian variety Y.

Idea

Construct the minimal isogeny for X from its corresponding PFTQ

$$Y_2 \xrightarrow{\rho_2} Y_1 \xrightarrow{\rho_1} Y_0 = X.$$

(If $Y_2 \to Y_1 \to Y_0$ is a PFTQ, then Y_2 is superspecial!)

- If $a(X) = 3$ then X is superspecial and $\varphi = \mathrm{id}$.
- If $a(X) = 2$, then $a(Y_1) = 3$ and $\varphi = \rho_1$ of degree p.
- If $a(X) = 1$, then $\varphi = \rho_1 \circ \rho_2$ of degree p^3.

From minimal isogenies to masses

Let $x = (X, \lambda)$ be supersingular and $\varphi : Y \to X$ a minimal isogeny. Write $\tilde{x} = (Y, \varphi^* \lambda)$.

Through φ, we may view both $G_{\tilde{x}}(\widehat{\mathbb{Z}})$ and $\varphi^* G_x(\widehat{\mathbb{Z}})$ as open compact subgroups of $G_{\tilde{x}}(\mathbb{A}_f)$, which differ only at p. Hence:

Lemma

$$\begin{aligned}\mathrm{Mass}(\Lambda_x) &= \frac{[G_{\tilde{x}}(\widehat{\mathbb{Z}}) : G_{\tilde{x}}(\widehat{\mathbb{Z}}) \cap \varphi^* G_x(\widehat{\mathbb{Z}})]}{[\varphi^* G_x(\widehat{\mathbb{Z}}) : G_{\tilde{x}}(\widehat{\mathbb{Z}}) \cap \varphi^* G_x(\widehat{\mathbb{Z}})]} \cdot \mathrm{Mass}(\Lambda_{\tilde{x}}) \\ &= [\mathrm{Aut}((Y, \phi^* \lambda)[p^\infty]) : \mathrm{Aut}((X, \lambda)[p^\infty])] \cdot \mathrm{Mass}(\Lambda_{\tilde{x}}).\end{aligned}$$

So we can compare any supersingular mass to a superspecial mass.

From minimal isogenies to masses

Moreover, the superspecial masses are known in any dimension!

Lemma [Ekedahl, Harashita, Hashimoto, Ibukiyama, Yu]

Let $\tilde{x} = (Y, \lambda)$ be a superspecial abelian threefold.

- If λ is a principal polarisation, then
$$\mathrm{Mass}(\Lambda_{\tilde{x}}) = \frac{(p-1)(p^2+1)(p^3-1)}{2^{10} \cdot 3^4 \cdot 5 \cdot 7}.$$
- If $\ker(\lambda) \simeq \alpha_p \times \alpha_p$, then
$$\mathrm{Mass}(\Lambda_{\tilde{x}}) = \frac{(p-1)(p^3+1)(p^3-1)}{2^{10} \cdot 3^4 \cdot 5 \cdot 7}.$$

It remains to compute $[\mathrm{Aut}((Y, \phi^* \lambda)[p^\infty]) : \mathrm{Aut}((X, \lambda)[p^\infty])]$.

The main tool: Dieudonné modules

Let $W = W(k)$ be the ring of Witt vectors over k.
Let σ be the Frobenius acting on W.

Definition (Dieudonné module)

A DIEUDONNÉ MODULE over k is a finite W-module M, with a σ-linear operator F and a σ^{-1}-linear operator V such that

$$FV = VF = p.$$

There is an antiequivalence

$$\{p\text{-divisible groups}/k\} \leftrightarrow \{W\text{-free Dieudonné modules}/k\}.$$

Let A be an abelian variety over k.
Instead of $A[p^\infty]$, we study its Dieudonné module $M = M(A[p^\infty])$.

The case $a(X) = 2$

Let $x = (X, \lambda) \in \mathcal{S}_{3,1}$ such that $a(X) = 2$.
Its PFTQ $(Y_2, \lambda_2) \to (Y_1, \lambda_1) \to (X, \lambda)$ is characterised by a pair $t \in C(\mathbb{F}_{p^2})$ and $u \in \mathbb{P}^1_t(k) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^2})$.
The minimal isogeny is $\varphi = \rho_1 : Y_1 \to X$.

So we need to compute $[\mathrm{Aut}((Y_1, \lambda_1)[p^\infty]) : \mathrm{Aut}((X, \lambda)[p^\infty])]$.
Write $M_1 = M(Y_1[p^\infty])$ and $M = M(X[p^\infty])$.
Then equivalently we need to compute $[\mathrm{Aut}(M_1) : \mathrm{Aut}(M)]$.

Let $M_1^\diamond := \{m \in M_1 : Fm + Vm = 0\}$ be the SKELETON of M_1.
Then $V = M_1^\diamond / M_1^{\diamond, t}$ is an $\mathbb{F}_{p^2}$-vector space.
We have (reduction) maps

$$\mathrm{Aut}(M_1) = \mathrm{Aut}(M_1^\diamond) \xrightarrow{m} \mathrm{Aut}_{\mathbb{F}_{p^2}}(V) = \mathrm{SL}_2(\mathbb{F}_{p^2}).$$

The case $a(X) = 2$

We further have

$$\mathrm{Aut}(M) \xrightarrow{m} \mathrm{SL}_2(\mathbb{F}_{p^2}) \cap \mathrm{End}(u)^{\times},$$

where

$$\mathrm{End}(u) = \{g \in M_2(\mathbb{F}_{p^2}) : g \cdot u \subseteq k \cdot u\} \simeq \begin{cases} \mathbb{F}_{p^4} \text{ if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ \mathbb{F}_{p^2} \text{ if } u \in \mathbb{P}^1_t(k) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^4}). \end{cases}$$

So $[\mathrm{Aut}(M_1) : \mathrm{Aut}(M)] =$

$$[\mathrm{SL}_2(\mathbb{F}_{p^2}) : \mathrm{SL}_2(\mathbb{F}_{p^2}) \cap \mathrm{End}(u)^{\times}] =$$

$$\begin{cases} p^2(p^2 - 1) & \text{if } u \in \mathbb{P}^1_t(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ |\mathrm{PSL}_2(\mathbb{F}_{p^2})| & \text{if } u \in \mathbb{P}^1_t(k) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^4}). \end{cases}$$

The case $a(X) = 2$

Theorem (K.-Yobuko-Yu)

Let $x = (X, \lambda) \in \mathcal{S}_{3,1}$ such that $a(X) = 2$,
whose PFTQ $(Y_2, \lambda_2) \to (Y_1, \lambda_1) \to (X, \lambda)$ is characterised by a pair $t \in C(\mathbb{F}_{p^2})$ and $u \in \mathbb{P}^1_t(k) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^2})$.
Write $x_1 = (Y_1, \lambda_1)$, $M_1 = M(Y_1[p^\infty])$, and $M = M(X[p^\infty])$.
Let $e(p) = 0$ if $p = 2$ and $e(p) = 1$ if $p > 2$.

$$\begin{aligned}
\mathrm{Mass}(\Lambda_x) &= \mathrm{Mass}(\Lambda_{x_1}) \cdot [\mathrm{Aut}(M_1) : \mathrm{Aut}(M)] \\
&= \frac{1}{2^{10} \cdot 3^4 \cdot 5 \cdot 7}. \\
&\begin{cases} (p-1)(p^3+1)(p^3-1)(p^4-p^2) & : u \in \mathbb{P}^1_t(\mathbb{F}_{p^4}) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^2}); \\ 2^{-e(p)}(p-1)(p^3+1)(p^3-1)p^2(p^4-1) & : u \in \mathbb{P}^1_t(k) \setminus \mathbb{P}^1_t(\mathbb{F}_{p^4}). \end{cases}
\end{aligned}$$

The case $a(X) = 1$

Let $x = (X, \lambda) \in \mathcal{S}_{3,1}$ such that $a(X) = 1$.
Its PFTQ $(Y_2, \lambda_2) \to (Y_1, \lambda_1) \to (X, \lambda)$ is characterised by a pair $t \in C^0(k) := C(k) \setminus C(\mathbb{F}_{p^2})$ and $u \in \mathbb{P}^1_t(k)$.

We need to compute $[\mathrm{Aut}((Y_2, \lambda_2)[p^\infty]) : \mathrm{Aut}((X, \lambda)[p^\infty])]$.
Write $M_2 = M(Y_2[p^\infty])$and $M = M(X[p^\infty])$.
Then equivalently we need to compute $[\mathrm{Aut}(M_2) : \mathrm{Aut}(M)]$.

Let $D_p = \mathbb{Q}_{p^2}[\Pi]$ be the division quaternion algebra over $\mathbb{Q}_p$, and let $\mathcal{O}_{D_p}$ its maximal order. (We have $\Pi^2 = -p$.) Then

$$\begin{aligned} \mathrm{Aut}(M_2) &\simeq \{A \in \mathrm{GL}_3(\mathcal{O}_{D_p}) : A^* A = \mathbb{I}_3\}; \\ \mathrm{Aut}(M) &\simeq \{g \in \mathrm{Aut}(M_2) : g(M) = M\}. \end{aligned}$$

The case $a(X) = 1$

Let m_p be the reduction-modulo-pM_2 map. We obtain

$$\begin{aligned}\overline{G}_2 &= m_p(\mathrm{Aut}(M_2)) \\ &= \{A + B\Pi \in \mathrm{GL}_3(\mathbb{F}_{p^2}[\Pi]) : A^*A = \mathbb{I}_3, B^TA^* = A^{*T}B\}; \\ \overline{G} &= m_p(\mathrm{Aut}(M)) \\ &= \{g \in \overline{G}_2 : g(M/pM_2) \subseteq M/pM_2\}.\end{aligned}$$

We see that

$$|\overline{G}_2| = |U_3(\mathbb{F}_p)| \cdot |S_3(\mathbb{F}_{p^2})| = p^{15}(p+1)(p^2-1)(p^3+1).$$

Moreover,

$$[\mathrm{Aut}(M_2) : \mathrm{Aut}(M)] = [\overline{G}_2 : \overline{G}].$$

The case $a(X) = 1$

We prove that

$$\overline{G} \simeq \left\{ \left(\begin{smallmatrix} A & 0 \\ SA & A^{(p)} \end{smallmatrix} \right) : A \in U_3(\mathbb{F}_p), A \cdot t = \alpha \cdot t, \right.$$
$$\left. S \in S_3(\mathbb{F}_{p^2}), \psi_t(S) = u_2 u_1^{-1}(1 - \alpha^{p^3-1}) \right\},$$

where

$$\psi_t : S_3(\mathbb{F}_{p^2}) \to k$$
$$S \mapsto \text{ the } (1,1)\text{-component of } \mathbb{T}^{-1} S \mathbb{T},$$
$$\text{for } \mathbb{T} = \begin{pmatrix} t_1 & t_1^p & t_1^{p^{-1}} \\ t_2 & t_2^p & t_2^{p^{-1}} \\ t_3 & t_3^p & t_3^{p^{-1}} \end{pmatrix},$$

is a homomorphism depending on t. So

$$|\overline{G}| = |\{A \in U_3(\mathbb{F}_p) : A \cdot t = \alpha \cdot t, u_2 u_1^{-1}(1 - \alpha^{p^3-1}) \in \mathrm{Im}(\psi_t)\}| \cdot |\ker(\psi_t)|.$$

The case $a(X) = 1$

The images of ψ_t for varying t define a divisor $D \subseteq C^0 \times \mathbb{P}^1$:

$$D = \sum_{S \in S_3(\mathbb{F}_{p^2})} \{(t^{(p)}, (1 : \psi_t(S)^p)) : t \in C^0\}.$$

For $t \in C^0(k)$, let $d(t) = \dim_{\mathbb{F}_{p^2}}(\mathrm{Im}(\psi_t))$ and $D_t = \pi^{-1}(t) \cap D$.
Then $u = (u_1 : u_2) \in D_t \Leftrightarrow u_2 u_1^{-1} \in \mathrm{Im}(\psi_t)$.
Also, $|\ker(\psi_t)| = p^{2(6-d(t))}$. Hence,

$$|\overline{G}| = \begin{cases} 2^{e(p)} p^{2(6-d(t))} & \text{if } u \notin D_t; \\ (p+1)p^{2(6-d(t))} & \text{if } u \in D_t \text{ and } t \notin C(\mathbb{F}_{p^6}); \\ (p^3+1)p^6 & \text{if } u \in D_t \text{ and } t \in C(\mathbb{F}_{p^6}), \end{cases}$$

where $e(p) = 0$ if $p = 2$ and $e(p) = 1$ if $p > 2$.

The case $a(X) = 1$

Theorem (K.-Yobuko-Yu)

Let $x = (X, \lambda) \in \mathcal{S}_{3,1}$ such that $a(X) = 1$, whose PFTQ $(Y_2, \lambda_2) \to (Y_1, \lambda_1) \to (X, \lambda)$ is characterised by a pair $t \in C^0(k) := C(k) \setminus C(\mathbb{F}_{p^2})$ and $u \in \mathbb{P}^1_t(k)$.
Write $x_2 = (Y_2, \lambda_2)$, $M_2 = M(Y_2[p^\infty])$, and $M = M(X[p^\infty])$.
Let $e(p) = 0$ if $p = 2$ and $e(p) = 1$ if $p > 2$.

$$\begin{aligned}\mathrm{Mass}(\Lambda_x) &= \mathrm{Mass}(\Lambda_{x_2}) \cdot [\mathrm{Aut}(M_2) : \mathrm{Aut}(M)] \\ &= \frac{p^3}{2^{10} \cdot 3^4 \cdot 5 \cdot 7}. \\ &\begin{cases} 2^{-e(p)} p^{2d(t)} (p^2-1)(p^4-1)(p^6-1) & : u \notin D_t; \\ p^{2d(t)} (p-1)(p^4-1)(p^6-1) & : u \in D_t, t \notin C(\mathbb{F}_{p^6}); \\ p^6 (p^2-1)(p^3-1)(p^4-1) & : u \in D_t, t \in C(\mathbb{F}_{p^6}). \end{cases}\end{aligned}$$

What else can we use all these computations for?

Application: Oort's conjecture

Oort's conjecture

Every generic g-dimensional principally polarised supersingular abelian variety (X, λ) over k of characteristic p has automorphism group $C_2 \simeq \{\pm 1\}$.

This fails in general: counterexamples for $(g, p) = (2, 2)$ and $(3, 2)$.

Theorem (K.-Yobuko-Yu)

When $g = 3$, Oort's conjecture holds precisely when $p \neq 2$.

- A *generic* threefold X has $a(X) = 1$.
  Its PFTQ is characterised by $t \in C^0(k)$ and $u \notin D_t$.
- Our computations show for such (X, λ) that

$$\mathrm{Aut}((X, \lambda)) \simeq \begin{cases} C_2^3 & \text{for } p = 2; \\ C_2 & \text{for } p \neq 2. \end{cases}$$