Moduli spaces:
classifying, constructing and counting varieties

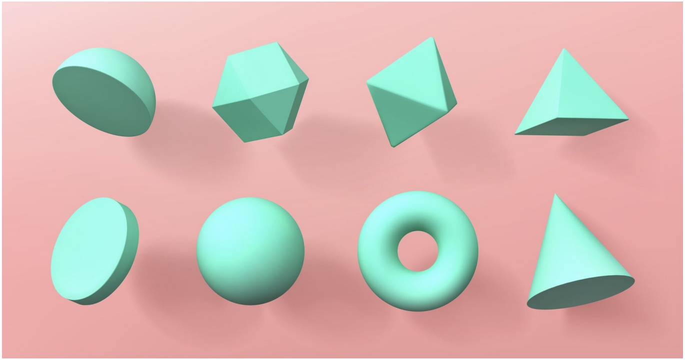
Valentijn Karemaker

University of Amsterdam

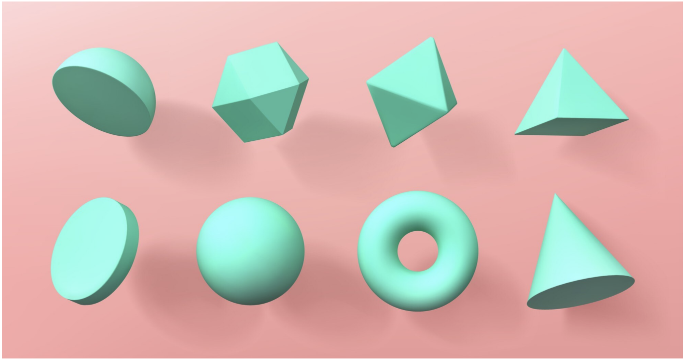
DIAMANT Symposium

21 November 2025

How do we classify geometric objects?



How do we classify geometric objects?



When are two objects the same?

When are two objects the same?

It depends who you ask!

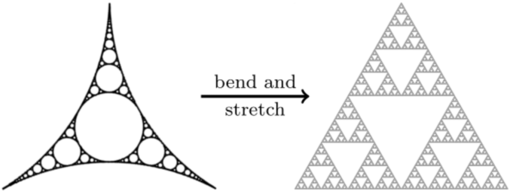
Example: triangles in the real plane ($\mathbb{R}^2$).

When are two objects the same?

It depends who you ask!

Example: triangles in the real plane ($\mathbb{R}^2$).

Topology: two triangles are the same (= homeomorphic) if you can continuously deform one into the other. So all triangles are the same, and they're also the same as all circles, squares, ...



When are two objects the same?

It depends who you ask!

Example: triangles in the real plane ($\mathbb{R}^2$) with non-zero area.

Geometry: we no longer allow all ways of deforming.
For example, we may call two triangles the same if they are:

1. Equal (= same vertices with same labelling), or
2. Similar (= congruent up to scaling).

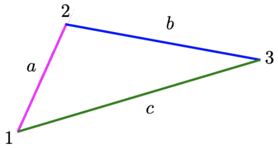


Figure: 1. Equal

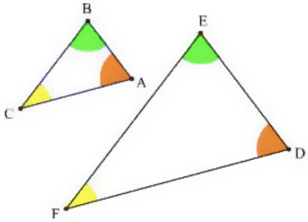


Figure: 2. Similar

How many different triangles are there?[1]

1. The set of all non-equal triangles in $\mathbb{R}^2$ is

$$M_1 = \{(x_1, y_1, x_2, y_2, x_3, y_3) : \det \begin{pmatrix} x_2 - x_1 & x_3 - x_1 \\ y_2 - y_1 & y_3 - y_1 \end{pmatrix} \neq 0\}.$$

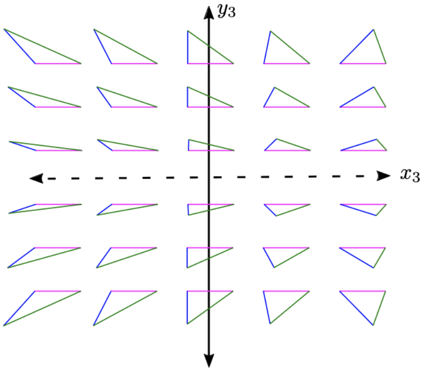


Figure: Slice of M_1 where $(x_1, y_1) = (0, 0), (x_2, y_2) = (1, 0)$.

[1] Jarod Alper, *Stacks and Moduli*, version July 2025.

How many different triangles are there?

2. The set of all non-similar triangles in $\mathbb{R}^2$ is

$$M_2 = \{(a, b, c) : 0 < a \leq b \leq c < a + b, a + b + c = 2\}.$$

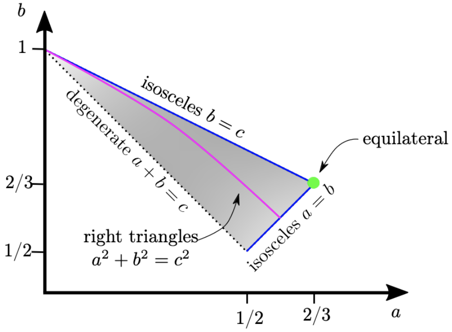


Figure: M_2 with some special triangles marked

How many different triangles are there?

2. The set of all non-similar triangles in $\mathbb{R}^2$ is

$$M_2 = \{(a,b,c) : 0 < a \leq b \leq c < a+b, a+b+c = 2\}.$$

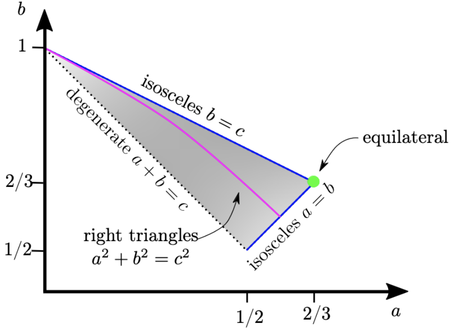


Figure: M_2 with some special triangles marked

Question: What does the set of all non-congruent triangles look like?

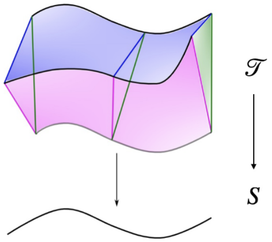
What have we just done?

- We chose a suitable notion of “being the same” for our objects.
- We found a description of the set of objects that are not the same.
- Every point in the set is a unique object.

What have we just done?

- We chose a suitable notion of "being the same" for our objects.
- We found a description of the set of objects that are not the same.
- Every point in the set is a unique object.

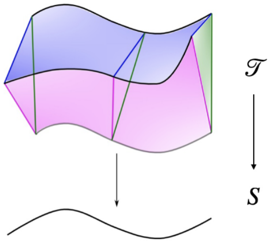
This set is (roughly) a moduli space!



What have we just done?

- We chose a suitable notion of "being the same" for our objects.
- We found a description of the set of objects that are not the same.
- Every point in the set is a unique object.

This set is (roughly) a moduli space!



Slogan: In a moduli space every point corresponds with a unique object that is different (= not the same) as all other objects.

What's next?

Algebraic geometry is not only about triangles, but about:

Varieties: Solution sets of polynomial equations

What's next?

Algebraic geometry is not only about triangles, but about:

Varieties: Solution sets of polynomial equations,

of a certain *dimension* (= "number of equations")

What's next?

Algebraic geometry is not only about triangles, but about:

Varieties: Solution sets of polynomial equations,

of a certain *dimension* (= "number of equations"):

Curves (dim 1), surfaces (dim 2), ...

What's next?

Algebraic geometry is not only about triangles, but about:

Varieties: Solution sets of polynomial equations,

of a certain *dimension* (= "number of equations"):

Curves (dim 1), surfaces (dim 2), ...

Curves have a *genus* (= "complexity of the equation")

What's next?

Algebraic geometry is not only about triangles, but about:

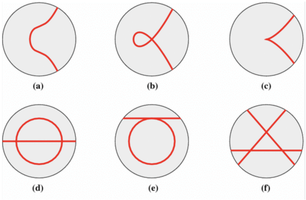
Varieties: Solution sets of polynomial equations,

of a certain *dimension* (="number of equations"):

Curves (dim 1), surfaces (dim 2), ...

Curves have a *genus* (="complexity of the equation"):

Lines (genus 0), **elliptic curves** (genus 1), ...


(a) (b) (c)
(d) (e) (f)

What is an elliptic curve?

Definition (elliptic curve)

An elliptic curve is a curve of genus 1,
given by a Weierstrass equation:

$$E : y^2 + axy + by = x^3 + cx^2 + dx + e$$

for parameters a, b, c, d, e, together with a point $\mathcal{O}$ ("at infinity").

What is an elliptic curve?

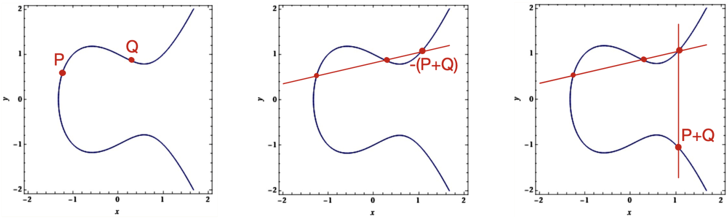
Definition (elliptic curve)

An elliptic curve is a curve of genus 1,
given by a Weierstrass equation:

$$E : y^2 + axy + by = x^3 + cx^2 + dx + e$$

for parameters a, b, c, d, e, together with a point $\mathcal{O}$ ("at infinity").

The solutions of the equation, i.e. the points on the curve, can be added together via a geometric process (where $\mathcal{O} = 0$).



When are two elliptic curves the same?

Two elliptic curves

$$E_1 : y^2 + axy + by = x^3 + cx^2 + dx + e$$
$$E_2 : \tilde{y}^2 + f\tilde{x}\tilde{y} + g\tilde{y} = \tilde{x}^3 + h\tilde{x}^2 + i\tilde{x} + j$$

are the same (= *isomorphic*) if we can go from E_1 to E_2 via

$$\boldsymbol{\tilde{x} = u^2 x + r, \quad \tilde{y} = u^3 y + u^2 s x + t},$$

for constants u, r, s, t with $u \neq 0$.

Then we have

$$\begin{aligned} ua &= f + 2s, \\ u^2 c &= h - sf + 3r - s^2, \\ u^3 b &= g + rf + 2t, \\ u^4 d &= i - sg + 2rh - (t + rs)f + 3r^2 - 2st, \\ u^6 e &= j + ri + r^2 h + r^3 - tg - t^2 - rtf. \end{aligned}$$

A family of elliptic curves

After a coordinate change we write the Weierstrass equation as

$$E_\lambda : y^2 = x(x-1)(x-\lambda),$$

for $\lambda \neq 0, 1$.

This is called the **Legendre normal form** of the elliptic curve.

A family of elliptic curves

After a coordinate change we write the Weierstrass equation as

$$E_\lambda : y^2 = x(x-1)(x-\lambda),$$

for $\lambda \neq 0, 1$.
This is called the **Legendre normal form** of the elliptic curve.

We obtain the family $\{E_\lambda\}_\lambda$ of elliptic curves with parameter λ.
Is $\{\lambda\}$ a moduli space?

A family of elliptic curves

After a coordinate change we write the Weierstrass equation as

$$E_\lambda : y^2 = x(x-1)(x-\lambda),$$

for $\lambda \neq 0, 1$.
This is called the **Legendre normal form** of the elliptic curve.

We obtain the family $\{E_\lambda\}_\lambda$ of elliptic curves with parameter λ.
Is $\{\lambda\}$ a moduli space? No!

To find an elliptic curve $\tilde{y}^2 = \tilde{x}(\tilde{x}-1)(\tilde{x}-\mu)$ isomorphic to E_λ we take

$$\tilde{x} = u^2 x + r \text{ en } \tilde{y} = u^3 y,$$

so that

$$x(x-1)(x-\mu) = \left(x + \frac{r}{u^2}\right)\left(x + \frac{r-1}{u^2}\right)\left(x + \frac{r-\lambda}{u^2}\right).$$

A family of elliptic curves

After a coordinate change we write the Weierstrass equation as

$$E_\lambda : y^2 = x(x-1)(x-\lambda),$$

for $\lambda \neq 0, 1$.
This is called the **Legendre normal form** of the elliptic curve.

We obtain the family $\{E_\lambda\}_\lambda$ of elliptic curves with parameter λ.
Is $\{\lambda\}$ a moduli space? No!

To find an elliptic curve $\tilde{y}^2 = \tilde{x}(\tilde{x}-1)(\tilde{x}-\mu)$ isomorphic to E_λ we take

$$\tilde{x} = u^2 x + r \text{ en } \tilde{y} = u^3 y,$$

so that

$$x(x-1)(x-\mu) = \left(x + \frac{r}{u^2}\right)\left(x + \frac{r-1}{u^2}\right)\left(x + \frac{r-\lambda}{u^2}\right).$$

So we have six choices of μ! They are:

$$\lambda,\ 1/\lambda,\ 1-\lambda,\ 1/(1-\lambda),\ \lambda/(\lambda-1),\ (\lambda-1)/\lambda.$$

The j-invariant

We look for another expression in the coefficients of an elliptic curve that describes it uniquely up to isomorphism.

After another coordinate change we simplify the general equation to

$$E : y^2 = x^3 + Ax + B.$$

Definition (j-invariant)

An elliptic curve given by a Weierstrass equation

$$E : y^2 = x^3 + Ax + B$$

with parameters A, B has j-invariant

$$j(E) = 12^3 \frac{4A^3}{4A^3 + 27B^2}.$$

The moduli space of elliptic curves

$E : y^2 = x^3 + Ax + B$ has j-invariant $j(E) = 12^3 \frac{4A^3}{4A^3+27B^2}$.

The j-invariant is constructed such that elliptic curves are isomorphic if and only if they have the same j-invariant.

Moreover, for every value J of the j-invariant there exists a unique elliptic curve with that j-invariant. It is:

$$E_J : y^2 = x^3 - \frac{27J}{4(J-12^3)}x - \frac{27J}{4(J-12^3)}.$$

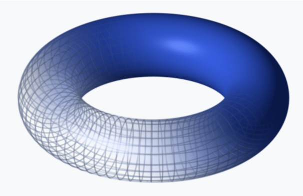
This means:

Conclusion

The line $\{j\}$ is (isomorphic to) the moduli space of elliptic curves. Every point on this line (i.e. every j-value) corresponds to a unique elliptic curve up to isomorphism.

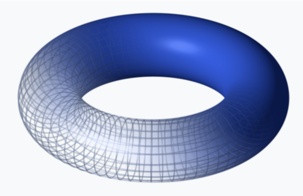
Elliptic curves over $\mathbb{C}$

Working over the complex numbers, we can give an alternative description.
This is because an elliptic curve over $\mathbb{C}$ is a torus:



Elliptic curves over $\mathbb{C}$

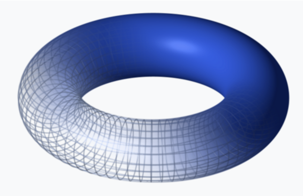
Working over the complex numbers, we can give an alternative description.
This is because an elliptic curve over $\mathbb{C}$ is a torus:



A complex torus can be written as $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ for τ in $\mathbb{C}$.
This means: we call two points c_1, c_2 in $\mathbb{C}$ the same if there exist integers z_1, z_2 such that $c_1 = c_2 + (z_1 + z_2 \cdot \tau)$.

Elliptic curves over $\mathbb{C}$

Working over the complex numbers, we can give an alternative description.
This is because an elliptic curve over $\mathbb{C}$ is a torus:



A complex torus can be written as $\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ for τ in $\mathbb{C}$.
This means: we call two points c_1, c_2 in $\mathbb{C}$ the same if there exist integers z_1, z_2 such that $c_1 = c_2 + (z_1 + z_2 \cdot \tau)$.

The points in $\Lambda = \mathbb{Z}+\mathbb{Z}\tau$ describe a lattice.
Tori $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are the same (isomorphic) $\Leftrightarrow$
there exists c in $\mathbb{C}$ such that $\Lambda_1 = c \cdot \Lambda_2$.
Then Λ_1 and Λ_2 are **homothetic** lattices.

The moduli space of elliptic curves over $\mathbb{C}$

Tori $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic $\Leftrightarrow \Lambda_1 = c \cdot \Lambda_2$ are homothetic.

To understand the moduli space of elliptic curves (= tori $\mathbb{C}/\Lambda$),
it suffices to describe the moduli space of lattices $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$.

We may choose $\tau = a + bi$ such that $b > 0$.
(Otherwise $-1 \cdot \Lambda_\tau = \Lambda_{\overline{\tau}}$ is a homothetic lattice that satisfies this.)

The moduli space of elliptic curves over $\mathbb{C}$

Tori $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic $\Leftrightarrow \Lambda_1 = c \cdot \Lambda_2$ are homothetic.

To understand the moduli space of elliptic curves ($=$ tori $\mathbb{C}/\Lambda$),
it suffices to describe the moduli space of lattices $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$.

We may choose $\tau = a + bi$ such that $b > 0$.
(Otherwise $-1 \cdot \Lambda_\tau = \Lambda_{\overline{\tau}}$ is a homothetic lattice that satisfies this.)
But this does not render the choice of τ unique!
One shows that Λ_{τ_1} is homothetic to Λ_{τ_2}, for $\tau_1 = a_1 + b_1 i$ and $\tau_2 = a_2 + b_2 i$ (with $b_1, b_2 > 0$) if and only if

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} Aa_2 + Bb_2 \\ Ca_2 + Db_2 \end{pmatrix} \tag{1}$$

for a matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ of determinant 1. Also, $\pm\mathrm{Id}_2$ act trivially.

The moduli space of elliptic curves over $\mathbb{C}$

Tori $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic $\Leftrightarrow \Lambda_1 = c \cdot \Lambda_2$ are homothetic.

To understand the moduli space of elliptic curves ($=$ tori $\mathbb{C}/\Lambda$), it suffices to describe the moduli space of lattices $\Lambda_\tau = \mathbb{Z} + \mathbb{Z}\tau$.

We may choose $\tau = a + bi$ such that $b > 0$.
(Otherwise $-1 \cdot \Lambda_\tau = \Lambda_{\overline{\tau}}$ is a homothetic lattice that satisfies this.)
But this does not render the choice of τ unique!
One shows that Λ_{τ_1} is homothetic to Λ_{τ_2}, for $\tau_1 = a_1 + b_1 i$ and $\tau_2 = a_2 + b_2 i$ (with $b_1, b_2 > 0$) if and only if

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} Aa_2 + Bb_2 \\ Ca_2 + Db_2 \end{pmatrix} \tag{1}$$

for a matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ of determinant 1. Also, $\pm\mathrm{Id}_2$ act trivially.

Conclusion

The moduli space of elliptic curves over $\mathbb{C}$ is (isomorphic to) the set $\{\tau = a + bi : b > 0\}$ up to the equivalence in (1), i.e. to

$$(\mathrm{SL}_2(\mathbb{Z})/\pm\mathrm{Id}_2) \setminus \mathbb{H}.$$

Abelian varieties over finite fields

An abelian variety is a higher-dimensional elliptic curve.

Definition (abelian variety)

An abelian variety is a non-singular projective group variety.

Abelian varieties over finite fields

An abelian variety is a higher-dimensional elliptic curve.

Definition (abelian variety)

An abelian variety is a non-singular projective group variety.

I mostly consider abelian varieties which (i.e., whose defining equations) are defined over finite fields.

Definition/notation

Let $\mathbb{F}_q$ be the finite field of cardinality $q = p^r$, where p is a prime.

All elements $x \in \mathbb{F}_q$ satisfy $x^q = x$.

Abelian varieties over finite fields have interesting applications in cryptography and coding theory.

First classification: abelian varieties up to isogeny

When are two abelian varieties X, Y of dimension $g \geq 1$ the same?

First answer: when they are **isogenous**, denoted $X \sim Y$.
An isogeny $\varphi : X \to Y$ is a surjective map with finite kernel.
Isogeny defines an equivalence relation on abelian varieties.

First classification: abelian varieties up to isogeny

When are two abelian varieties X, Y of dimension $g \geq 1$ the same?

First answer: when they are **isogenous**, denoted $X \sim Y$.
An isogeny $\varphi : X \to Y$ is a surjective map with finite kernel.
Isogeny defines an equivalence relation on abelian varieties.

Honda and Tate showed:
$\{$ isogeny classes of abelian varieties over $\mathbb{F}_q$ $\} \leftrightarrow \{$ Weil q-polynomials $\}$

where a Weil q-polynomial is some monic $f \in \mathbb{Z}[x]$ whose complex roots all have absolute value $\sqrt{q}$.

First classification: abelian varieties up to isogeny

When are two abelian varieties X, Y of dimension $g \geq 1$ the same?

First answer: when they are **isogenous**, denoted $X \sim Y$.
An isogeny $\varphi : X \to Y$ is a surjective map with finite kernel.
Isogeny defines an equivalence relation on abelian varieties.

Honda and Tate showed:
$\{$ isogeny classes of abelian varieties over $\mathbb{F}_q$ $\} \leftrightarrow \{$ Weil q-polynomials $\}$

where a Weil q-polynomial is some monic $f \in \mathbb{Z}[x]$ whose complex roots all have absolute value $\sqrt{q}$.

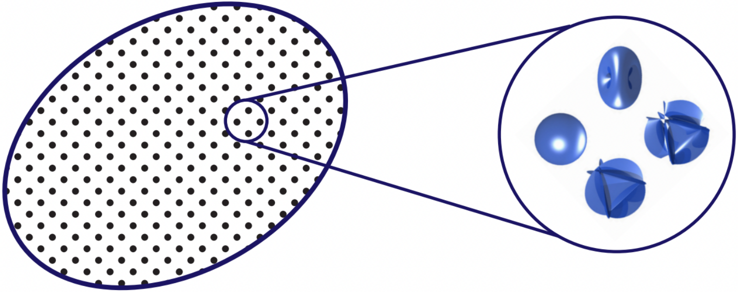
Conclusion

We can parametrise isogeny classes by Weil q- polynomials.
The "space of Weil q-polynomials" is not a nice moduli space, however.

Open problem: describe all abelian varieties in a fixed isogeny class.

Moduli spaces of abelian varieties (over finite fields)

Stronger: X, Y are the same when they are isomorphic, denoted $X \simeq Y$. This yields a nice moduli space, denoted $\mathcal{A}_g$ (in dim g).



Geometry of moduli space $\Rightarrow$ **arithmetic** of families of abelian varieties.

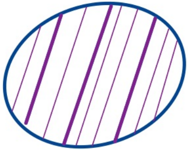
Arithmetic invariants and their induced stratifications

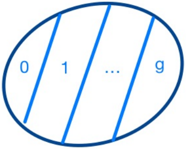
Idea: Study loci in $\mathcal{A}_g$ of fixed value of arithmetic invariant.

Arithmetic invariants and their induced stratifications

Idea: Study loci in $\mathcal{A}_g$ of fixed value of arithmetic invariant.
Finite fields have characteristic p, so p-(power) torsion is interesting.
Consider the p-torsion group scheme $X[p]$ and p-divisible group $X[p^\infty]$.

$X[p^\infty]/\sim$: p-rank stratification, refined by Newton stratification

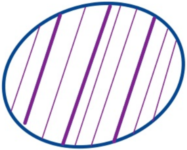


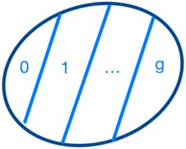


Arithmetic invariants and their induced stratifications

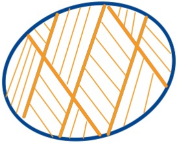
Idea: Study loci in $\mathcal{A}_g$ of fixed value of arithmetic invariant.
Finite fields have characteristic p, so p-(power) torsion is interesting.
Consider the p-torsion group scheme $X[p]$ and p-divisible group $X[p^\infty]$.

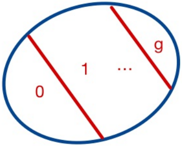
$X[p^\infty]/\sim$: p-rank stratification, refined by Newton stratification





$X[p]/\simeq$: a-number stratification, refined by EO stratification.

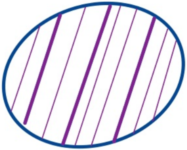


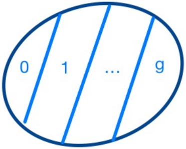


Arithmetic invariants and their induced stratifications

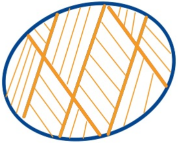
Idea: Study loci in $\mathcal{A}_g$ of fixed value of arithmetic invariant.
Finite fields have characteristic p, so p-(power) torsion is interesting.
Consider the p-torsion group scheme $X[p]$ and p-divisible group $X[p^\infty]$.

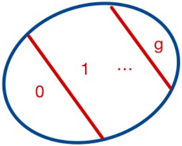
$X[p^\infty]/\sim$: p-rank stratification, refined by Newton stratification





$X[p]/\simeq$: a-number stratification, refined by EO stratification.





Open problem: How do the Newton and EO strata intersect?

Abelian varieties determined by their p-divisible group

We saw $X[p]/\simeq$ and $X[p^\infty]/\sim$, now $X[p^\infty]/\simeq$.
The **central leaf** passing through abelian variety X_0 is

$$\Lambda_{X_0} = \{X \in \mathcal{A}_g : X[p^\infty] \simeq X_0[p^\infty]\}.$$

Question: For which abelian varieties X_0 do we have $\#\Lambda_{X_0} = 1$?

Theorem (Ibukiyama-K.-Yu)

For a **supersingular** abelian variety X_0 of dimension g, we have $\#\Lambda_{X_0} = 1$ if and only if one of the following holds:

1. $g = 1$ and $p \in \{2, 3, 5, 7, 13\}$;
2. $g = 2$ and $p \in \{2, 3\}$;
3. $g = 3$, $p = 2$, and $a(X_0) \geq 2$.

(Here we work over the algebraically closed field $k = \overline{\mathbb{F}}_p$.)

Masses, or (weighted) counting on moduli spaces

The **mass** of a central leaf $\Lambda_{X_0} = \{X \in \mathcal{A}_g : X[p^\infty] \simeq X_0[p^\infty]\}$ is

$$\mathrm{Mass}(\Lambda_{X_0}) = \sum_{X \in \Lambda_{X_0}} \frac{1}{|\mathrm{Aut}(X)|}.$$

Masses, or (weighted) counting on moduli spaces

The **mass** of a central leaf $\Lambda_{X_0} = \{X \in \mathcal{A}_g : X[p^\infty] \simeq X_0[p^\infty]\}$ is

$$\mathrm{Mass}(\Lambda_{X_0}) = \sum_{X \in \Lambda_{X_0}} \frac{1}{|\mathrm{Aut}(X)|}.$$

Theorem (K.-Yobuko-Yu)

For a generic **supersingular** abelian variety X_0 of dimension 3, we have

$$\mathrm{Mass}(\Lambda_{X_0}) = \frac{p^{3+2d}(p^2-1)(p^4-1)(p^6-1)}{2^{11} \cdot 3^4 \cdot 5 \cdot 7}.$$

Masses, or (weighted) counting on moduli spaces

The **mass** of a central leaf $\Lambda_{X_0} = \{X \in \mathcal{A}_g : X[p^\infty] \simeq X_0[p^\infty]\}$ is

$$\mathrm{Mass}(\Lambda_{X_0}) = \sum_{X \in \Lambda_{X_0}} \frac{1}{|\mathrm{Aut}(X)|}.$$

Theorem (K.-Yobuko-Yu)

For a generic **supersingular** abelian variety X_0 of dimension 3, we have

$$\mathrm{Mass}(\Lambda_{X_0}) = \frac{p^{3+2d}(p^2-1)(p^4-1)(p^6-1)}{2^{11} \cdot 3^4 \cdot 5 \cdot 7}.$$

Consequence: every such X_0 has automorphism group $\mathrm{Aut}(X_0) = \{\pm 1\}$.

This was conjectured by Oort for any dimension g and characteristic p.
Oort's conjecture is **still open** for $g \geq 5$ odd. (We proved the rest :))

Thank you for your attention!