Geometric invariants from counting points

Edgar Costa (MIT)
Simons Collaboration on Arithmetic Geometry, Number Theory, and Computation

June 10, 2022
Connecticut Summer School in Number Theory

Slides available at `edgarcosta.org`

Joint work with Andreas-Stephan Elsenhans, Francesc Fité, Jörg Jahnel, Davide Lombardo, Nicolas Mascot, Jeroen Sijsling, Andrew Sutherland, and John Voight.

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p?

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p?
- Given $\#E_p$ for many p, what can we say about E?

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p?
- Given $\#E_p$ for many p, what can we say about E?

$\rightsquigarrow$ studying the **statistical** properties of $\#E_p$

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p?
- Given $\#E_p$ for many p, what can we say about E?

$\rightsquigarrow$ studying the **statistical** properties of $\#E_p$

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p?
- Given $\#E_p$ for many p, what can we say about E?

$\rightsquigarrow$ studying the **statistical** properties of $\#E_p$

Theorem (Hasse)

$$\#E_p = p + 1 - a_p, \quad a_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p?
- Given $\#E_p$ for many p, what can we say about E?

$\rightsquigarrow$ studying the **statistical** properties of $\#E_p$ or $a_p := \operatorname{tr} \mathrm{Frob}_p$.

Theorem (Hasse)

$$\#E_p = p + 1 - a_p, \quad a_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

Elliptic curves

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Write $E_p := E \bmod p$, for p a prime of good reduction

- What can we say about $\#E_p$ for an arbitrary p?
- Given $\#E_p$ for many p, what can we say about E?

$\rightsquigarrow$ studying the **statistical** properties of $\#E_p$ or $a_p := \operatorname{tr} \mathrm{Frob}_p$.

Theorem (Hasse)

$$\#E_p = p + 1 - a_p, \quad a_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

Question

What can we say about the error term $a_p/\sqrt{p}$ as $p \to \infty$?

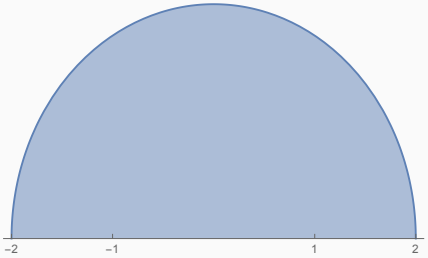
Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \operatorname{tr} \mathrm{Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for $a_p/\sqrt{p}$

non-CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$



CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-d})$

Checkout the gifs: rank 28 and generic

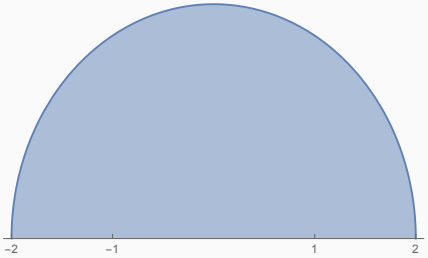
Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \operatorname{tr} \operatorname{Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for $a_p/\sqrt{p}$

non-CM

$\operatorname{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$



$\operatorname{Prob}(a_p = 0) \overset{?}{\sim} 1/\sqrt{p}$

CM

$\operatorname{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-d})$

$\operatorname{Prob}(a_p = 0) = 1/2$

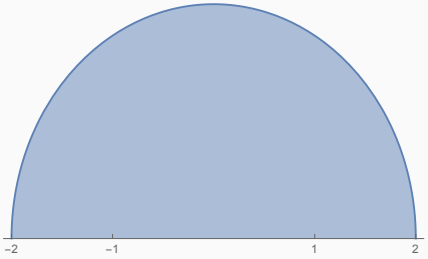
Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \operatorname{tr} \mathrm{Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for $a_p/\sqrt{p}$

non-CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$



CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-d})$

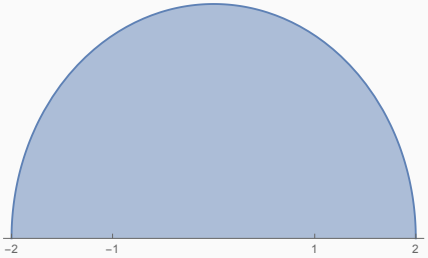
$$a_p = 0 \iff \mathbb{Q}(\mathrm{Frob}_p) := \mathbb{Q}(\sqrt{a_p^2 - 4p}) \subsetneq \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$$

Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \operatorname{tr} \mathrm{Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

non-CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$



CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-d})$

$$a_p = 0 \iff \mathbb{Q}(\mathrm{Frob}_p) := \mathbb{Q}(\sqrt{a_p^2 - 4p}) \subsetneq \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$$

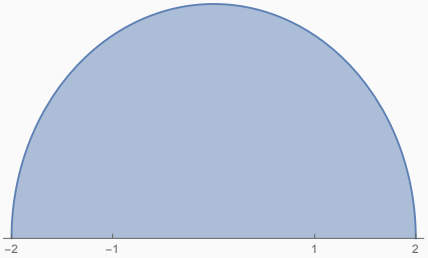
$$\iff \dim \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} > 2$$

Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \operatorname{tr} \mathrm{Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

non-CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$



CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-d})$

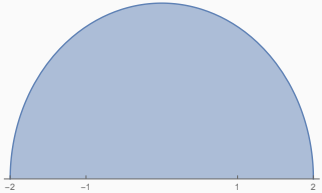
$$a_p = 0 \iff \mathbb{Q}(\mathrm{Frob}_p) := \mathbb{Q}(\sqrt{a_p^2 - 4p}) \subsetneq \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$$

$$\iff \dim \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} > 2 = \min_q \dim \mathrm{End}_{\mathbb{Q}} E_q^{\mathrm{al}}$$

How to distinguish between the two types?

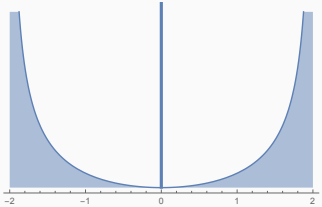
non-CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$



CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-d})$

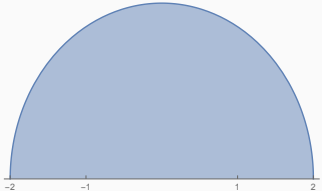


- $\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} \hookrightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} \hookleftarrow \mathbb{Q}(\mathrm{Frob}_p)$
- $a_p \neq 0 \iff \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$ is a quadratic field

How to distinguish between the two types?

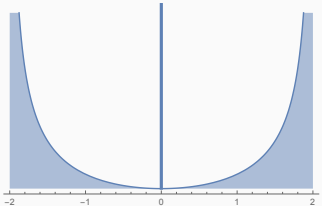
non-CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$



CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-d})$



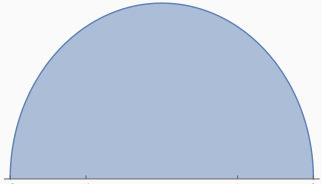
- $\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} \hookrightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} \hookleftarrow \mathbb{Q}(\mathrm{Frob}_p)$
- $a_p \neq 0 \iff \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$ is a quadratic field
- If E has CM by $\mathbb{Q}(\sqrt{-d})$, then

  $a_p \equiv 0 \bmod p \Leftrightarrow p$ inert or ramified in $\mathbb{Q}(\sqrt{-d}) \Leftrightarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} \not\simeq \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$

How to distinguish between the two types?

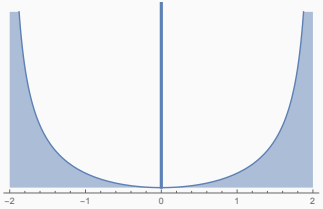
non-CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$



CM

$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-d})$



- $\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} \hookrightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} \hookleftarrow \mathbb{Q}(\mathrm{Frob}_p)$
- $a_p \neq 0 \iff \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$ is a quadratic field
- If E has CM by $\mathbb{Q}(\sqrt{-d})$, then

  $a_p \equiv 0 \bmod p \Leftrightarrow p$ inert or ramified in $\mathbb{Q}(\sqrt{-d}) \Leftrightarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} \not\simeq \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$
- If E is non-CM, then $\mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} \cap \mathrm{End}_{\mathbb{Q}} E_q^{\mathrm{al}} \simeq \mathbb{Q}$ with prob. 1;
  and we expect $\mathrm{Prob}(a_p \equiv 0 \bmod p) \sim 1/\sqrt{p}$

Examples

$E : y^2 + y = x^3 - x^2 - 10x - 20$ **(LMFDB label: 11.a2)**

- $\mathrm{End}_{\mathbb{Q}} E_2^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-1})$
- $\mathrm{End}_{\mathbb{Q}} E_3^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-11})$
- $\Rightarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$

Examples

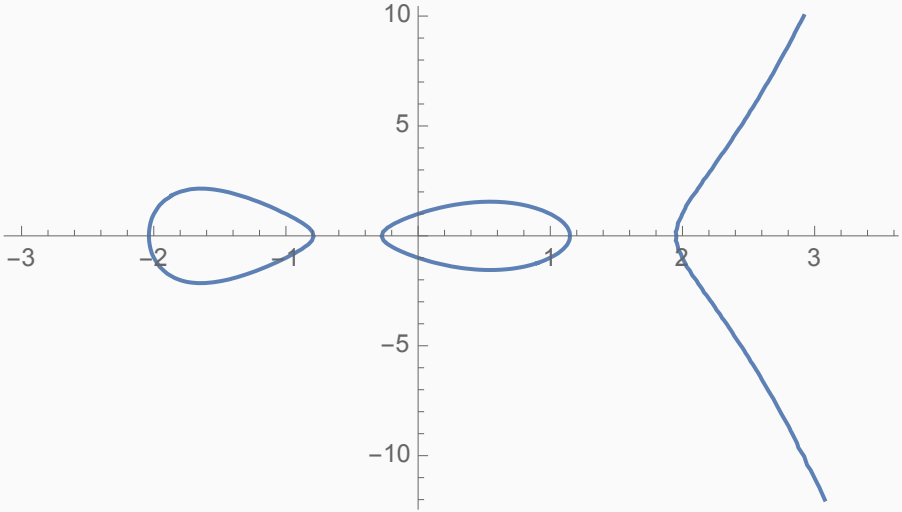
$E : y^2 + y = x^3 - x^2 - 10x - 20$ (LMFDB label: 11.a2)

- $\mathrm{End}_{\mathbb{Q}} E_2^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-1})$
- $\mathrm{End}_{\mathbb{Q}} E_3^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-11})$
- $\Rightarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}$

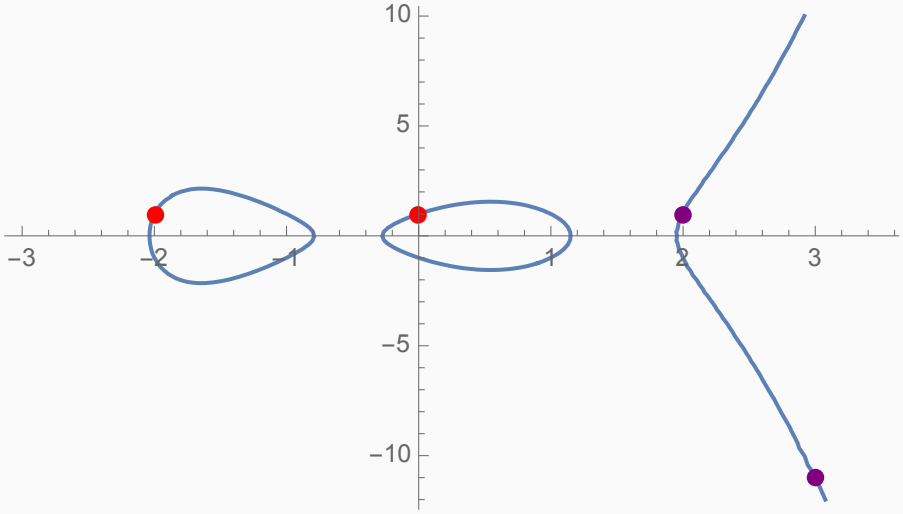
$E : y^2 + y = x^3 - 7$ (LMFDB label: 27.a2)

- $p = 2 \bmod 3 \Rightarrow a_p = 0 \Rightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$ is a Quaternion algebra
- $p = 1 \bmod 3 \Rightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-3})$
- $\rightsquigarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-3})$

Genus 2 curve arithmetic, an example $C : y^2 = x^5 - 5x^3 + 4x + 1$

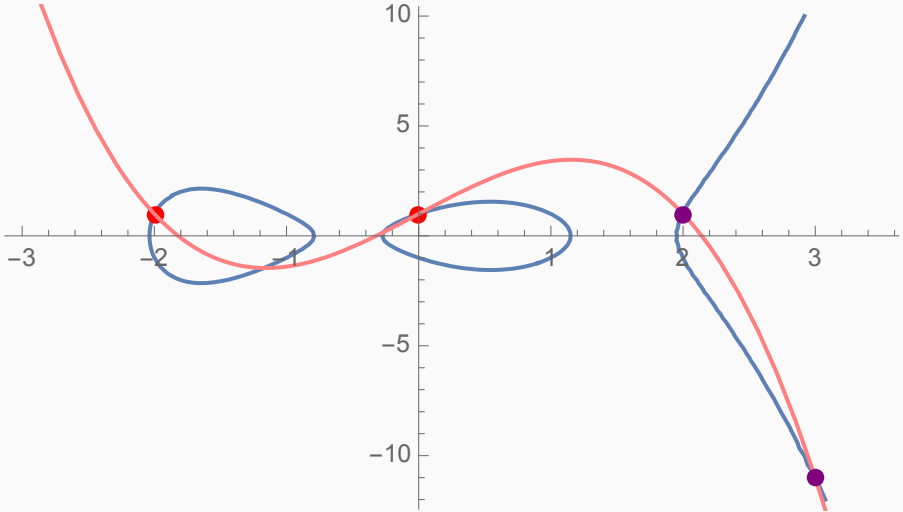


Genus 2 curve arithmetic, an example $C : y^2 = x^5 - 5x^3 + 4x + 1$

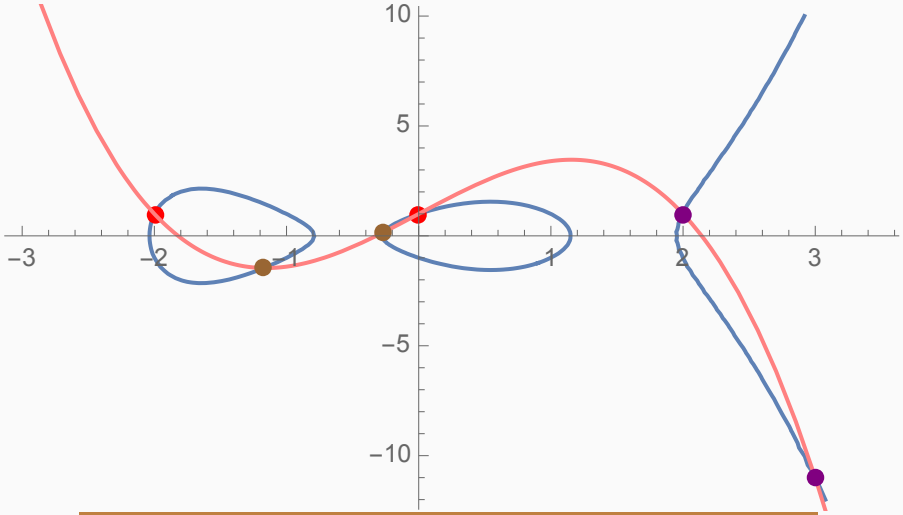


$D_1 := (-2, 1) + (0, 1)$ $D_2 := (2, 1) + (3, -11)$

Genus 2 curve arithmetic, an example $C : y^2 = x^5 - 5x^3 + 4x + 1$

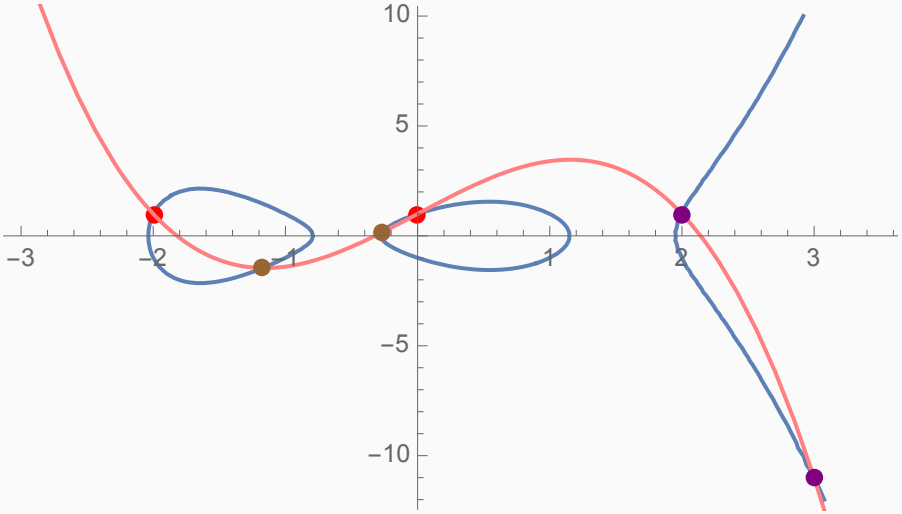


Genus 2 curve arithmetic, an example $C : y^2 = x^5 - 5x^3 + 4x + 1$



$$D_3 := \left(\frac{-\sqrt{209}-23}{32}, \frac{-115\sqrt{209}-1333}{2048}\right) + \left(\frac{\sqrt{209}-23}{32}, \frac{115\sqrt{209}-1333}{2048}\right)$$

Genus 2 curve arithmetic, an example $C : y^2 = x^5 - 5x^3 + 4x + 1$



$$(\bullet + \bullet) + (\bullet + \bullet) + (\bullet + \bullet) = 0$$

Genus 2 curves/Abelian surfaces

$$A := \mathsf{Jac}(C : y^2 = a_6x^6 + \cdots + a_0)$$

There are 6 possibilities for the real endomorphism algebra:

Abelian surface	$\mathsf{End}_{\mathbb{R}}\, A^{\mathsf{al}}$
square of CM elliptic curve	$\mathrm{M}_2(\mathbb{C})$
• QM abelian surface • square of non-CM elliptic curve	$\mathrm{M}_2(\mathbb{R})$
• CM abelian surface • product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$
• RM abelian surface • product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$
generic abelian surface	$\mathbb{R}$

Genus 2 curves/Abelian surfaces

$$A := \mathsf{Jac}(C : y^2 = a_6x^6 + \cdots + a_0)$$

There are 6 possibilities for the real endomorphism algebra:

Abelian surface	$\mathsf{End}_{\mathbb{R}}\, A^{\mathsf{al}}$
square of CM elliptic curve	$\mathrm{M}_2(\mathbb{C})$
• QM abelian surface • square of non-CM elliptic curve	$\mathrm{M}_2(\mathbb{R})$
• CM abelian surface • product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$
• RM abelian surface • product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$
generic abelian surface	$\mathbb{R}$

Can we distinguish between these by looking at A mod p?

Zeta functions and Frobenius polynomials

- $C/\mathbb{Q}$ a nice curve of genus g
- $A := \mathsf{Jac}(C)$
- p a prime of good reduction

$$Z_p(C,T) := \exp\left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r})T^r/r\right) \in \mathbb{Q}(t)$$

Zeta functions and Frobenius polynomials

- $C/\mathbb{Q}$ a nice curve of genus g
- $A := \mathsf{Jac}(C)$
- p a prime of good reduction

$$Z_p(C,T) := \exp\left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r})T^r/r\right) = \frac{L_p(T)}{(1-T)(1-pT)}$$

where $\deg L_p(T) = 2g$ and

$$L_p(T) = \det(1 - T\,\mathsf{Frob}_p \,|H^1(C)) = \det(1 - T\,\mathsf{Frob}_p \,|H^1(A)) \in 1 + T\mathbb{Z}[T]$$

Zeta functions and Frobenius polynomials

- $C/\mathbb{Q}$ a nice curve of genus g
- $A := \mathsf{Jac}(C)$
- p a prime of good reduction

$$Z_p(C,T) := \exp\left(\sum_{r=1}^{\infty} \#C(\mathbb{F}_{p^r})T^r/r\right) = \frac{L_p(T)}{(1-T)(1-pT)}$$

where $\deg L_p(T) = 2g$ and

$$L_p(T) = \det(1 - T\,\mathsf{Frob}_p \,|H^1(C)) = \det(1 - T\,\mathsf{Frob}_p \,|H^1(A)) \in 1 + T\mathbb{Z}[T]$$

- $g = 1 \rightsquigarrow L_p(T) = 1 - a_pT + pT^2$
- $g = 2 \rightsquigarrow L_p(T) = 1 - a_{1,p}T + a_{2,p}T^2 - a_{1,p}pT^3 + p^2T^4$

$L_p(T)$ gives us a lot of information about $A_p := A \bmod p$

Endomorphism algebras over finite fields

Let A be an abelian variety over $\mathbb{F}_q$.

Theorem

Given $L_p(T) := \det(1 - t\,\mathrm{Frob}\,|H^1(A))$, *we may compute:*

1. *(Tate)* $\mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{q^r}})$ *for all* $r \geq 1$;

Endomorphism algebras over finite fields

Let A be an abelian variety over $\mathbb{F}_q$.

Theorem

Given $L_p(T) := \det(1 - t\,\mathrm{Frob} \mid H^1(A))$, *we may compute:*

1. *(Tate)* $\mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{q^r}})$ *for all* $r \geq 1$;
2. *(Honda–Tate) the isomorphism class of* $\mathrm{End}_{\mathbb{Q}}(A_{\mathbb{F}_{q^r}})$ *for all* $r \geq 1$.

Endomorphism algebras over finite fields

Let A be an abelian variety over $\mathbb{F}_q$.

Theorem

Given $L_p(T) := \det(1 - t\,\mathrm{Frob} \mid H^1(A))$, we may compute:

1. *(Tate)* $\mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{q^r}})$ *for all* $r \geq 1$*;*
2. *(Honda–Tate) the isomorphism class of* $\mathrm{End}_{\mathbb{Q}}(A_{\mathbb{F}_{q^r}})$ *for all* $r \geq 1$.

Example

If $L_5(T) = 1 - 2T^2 + 25T^4$, then:

- all endomorphisms are defined over $\mathbb{F}_{25}$, and
- $A_{\mathbb{F}_{25}}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}}\, A^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

Example continued

$$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

For $p = 5$, $L_5(T) = 1 - 2T^2 + 25T^4$, and:

- all endomorphisms of A_5 are defined over $\mathbb{F}_{25}$
- $\det(1 - T\,\mathrm{Frob}_5^2 \,|H^1(A)) = (1 - 2T + 25T^2)^2$
- A_5 over $\mathbb{F}_{25}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}}\, A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

Example continued

$$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

For $p = 5$, $L_5(T) = 1 - 2T^2 + 25T^4$, and:

- all endomorphisms of A_5 are defined over $\mathbb{F}_{25}$
- $\det(1 - T\,\mathrm{Frob}_5^2 \,|H^1(A)) = (1 - 2T + 25T^2)^2$
- A_5 over $\mathbb{F}_{25}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}}\, A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

For $p = 7$, $L_7(T) = 1 + 6T^2 + 49T^4$, and:

- all endomorphisms of A_7 are defined over $\mathbb{F}_{49}$
- $\det(1 - T\,\mathrm{Frob}_7^2 \,|H^1(A)) = (1 + 6T + 49T^2)^2$
- A_7 over $\mathbb{F}_{49}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}}\, A_7^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-10}))$

Example continued

$$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

For $p = 5$, $L_5(T) = 1 - 2T^2 + 25T^4$, and:

- all endomorphisms of A_5 are defined over $\mathbb{F}_{25}$
- $\det(1 - T\,\mathrm{Frob}_5^2 \,|H^1(A)) = (1 - 2T + 25T^2)^2$
- A_5 over $\mathbb{F}_{25}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}} A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

For $p = 7$, $L_7(T) = 1 + 6T^2 + 49T^4$, and:

- all endomorphisms of A_7 are defined over $\mathbb{F}_{49}$
- $\det(1 - T\,\mathrm{Frob}_7^2 \,|H^1(A)) = (1 + 6T + 49T^2)^2$
- A_7 over $\mathbb{F}_{49}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}} A_7^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-10}))$

$\Rightarrow \mathrm{End}_{\mathbb{R}} A^{\mathrm{al}} \neq M_2(\mathbb{C})$

Same L_p, different approach

We could have looked at the Néron–Severi lattice $\mathsf{NS}(A)$.

$$\mathsf{End}_{\mathbb{Q}}(A)^{\dagger} \simeq \mathsf{NS}(A) \otimes \mathbb{Q} \qquad \mathsf{NS}(A^{\mathsf{al}}) \hookrightarrow \mathsf{NS}(A_p^{\mathsf{al}})$$

Same L_p, different approach

We could have looked at the Néron–Severi lattice $\mathsf{NS}(A)$.

$$\mathsf{End}_{\mathbb{Q}}(A)^{\dagger} \simeq \mathsf{NS}(A) \otimes \mathbb{Q} \qquad \mathsf{NS}(A^{\mathsf{al}}) \hookrightarrow \mathsf{NS}(A_p^{\mathsf{al}})$$

- $\operatorname{rk} \mathsf{NS}(A^{\mathsf{al}}) \in \{1, 2, 3, 4\}$
- $\operatorname{rk} \mathsf{NS}(A_p^{\mathsf{al}}) \in \{2, 4, 6\}$

Same L_p, different approach

We could have looked at the Néron–Severi lattice $\mathrm{NS}(A)$.

$$\mathrm{End}_{\mathbb{Q}}(A)^{\dagger} \simeq \mathrm{NS}(A) \otimes \mathbb{Q} \qquad \mathrm{NS}(A^{\mathrm{al}}) \hookrightarrow \mathrm{NS}(A_p^{\mathrm{al}})$$

- $\mathrm{rk}\,\mathrm{NS}(A^{\mathrm{al}}) \in \{1, 2, 3, 4\}$
- $\mathrm{rk}\,\mathrm{NS}(A_p^{\mathrm{al}}) \in \{2, 4, 6\}$

Example

- $\mathrm{rk}\,\mathrm{NS}(A_5^{\mathrm{al}}) = \mathrm{rk}\,\mathrm{NS}(A_7^{\mathrm{al}}) = 4$
- $\left.\begin{array}{l} \mathrm{disc}\,\mathrm{NS}(A_5^{\mathrm{al}}) = -6 \bmod \mathbb{Q}^{\times 2} \\ \mathrm{disc}\,\mathrm{NS}(A_7^{\mathrm{al}}) = -10 \bmod \mathbb{Q}^{\times 2} \end{array}\right\} \Rightarrow \mathrm{rk}\,\mathrm{NS}(A^{\mathrm{al}}) \leq 3$

Fact

By a theorem of Charles, we know that at some point this method will attain a tight upper bound for $\mathrm{rk}\,\mathrm{NS}(A^{\mathrm{al}})$.

Real endomorphisms algebras and Picard numbers

Abelian surface	$\mathrm{End}_{\mathbb{R}} A^{\mathrm{al}}$	$\mathrm{rk}\,\mathrm{NS}(A^{\mathrm{al}})$
square of CM elliptic curve	$\mathrm{M}_2(\mathbb{C})$	4
• QM abelian surface • square of non-CM elliptic curve	$\mathrm{M}_2(\mathbb{R})$	3
• CM abelian surface • product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$	2
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$	2
• RM abelian surface • product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$	2
generic abelian surface	$\mathbb{R}$	1

Higher genus

Let K be a numberfield such that $\mathbf{End}\, A_K = \mathbf{End}\, A^{\mathrm{al}}$

Higher genus

Let K be a numberfield such that $\mathsf{End}\, A_K = \mathsf{End}\, A^{\mathsf{al}}$, then

- $A_K \sim \prod_{i=1}^{t} A_i^{n_i}$,
- A_i unique and simple up to isogeny (over K),
- $B_i := \mathsf{End}_{\mathbb{Q}}\, A_i$ central simple algebra over $L_i := Z(B_i)$,
- $\mathsf{dim}_{L_i}\, B_i = e_i^2$,
- $\mathsf{End}_{\mathbb{Q}}\, A_K = \prod_{i=1}^{t} M_{n_i}(B_i)$

Higher genus

Let K be a numberfield such that $\mathsf{End}\, A_K = \mathsf{End}\, A^{\mathsf{al}}$, then

- $A_K \sim \prod_{i=1}^{t} A_i^{n_i}$,
- A_i unique and simple up to isogeny (over K),
- $B_i := \mathsf{End}_{\mathbb{Q}}\, A_i$ central simple algebra over $L_i := Z(B_i)$,
- $\dim_{L_i} B_i = e_i^2$,
- $\mathsf{End}_{\mathbb{Q}}\, A_K = \prod_{i=1}^{t} M_{n_i}(B_i)$

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight)

If Mumford–Tate conjecture holds for A, then we can compute

- t
- $\{(e_i n_i, n_i \dim A_i)\}_{i=1}^{t}$
- L_i

This is practical and its done by counting points (=computing L_p)

Real endomorphisms algebras, $\{e_i n_i, n_i \dim A_i\}_{i=1}^t$, and $\dim L_i$

Abelian surface	$\mathrm{End}_{\mathbb{R}} A^{\mathrm{al}}$	tuples	$\dim L_i$
square of CM elliptic crv	$\mathrm{M}_2(\mathbb{C})$	$\{(2,2)\}$	2
• QM abelian surface • square of non-CM elliptic crv	$\mathrm{M}_2(\mathbb{R})$	$\{(2,2)\}$	1
• CM abelian surface • product of CM elliptic crv	$\mathbb{C} \times \mathbb{C}$	$\{(1,2)\}$ $\{(1,1),(1,1)\}$	4 2, 2
CM $\times$ non-CM elliptic crvs	$\mathbb{C} \times \mathbb{R}$	$\{(1,1),(1,1)\}$	2, 1
• RM abelian surface • prod. of non-CM elliptic crv	$\mathbb{R} \times \mathbb{R}$	$\{(1,2)\}$ $\{(1,1),(1,1)\}$	2 1, 1
generic abelian surface	$\mathbb{R}$	$\{(1,1)\}$	1

Example continued: QM vs (non-CM)^2

$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1)$ (LMFDB label: 262144.d.524288.1)

- $\mathrm{End}_{\mathbb{Q}} A_3^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\mathrm{End}_{\mathbb{Q}} A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \mathrm{End}_{\mathbb{R}} A^{\mathrm{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \mathrm{End}_Q A^{\mathrm{al}}$ and assume that B is a quaternion algebra.
Can we guess $\mathrm{disc}\, B$?

Example continued: QM vs (non-CM)^2

$A = \mathsf{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1)$ (LMFDB label: 262144.d.524288.1)

- $\mathsf{End}_{\mathbb{Q}} A_3^{\mathsf{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\mathsf{End}_{\mathbb{Q}} A_5^{\mathsf{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \mathsf{End}_{\mathbb{R}} A^{\mathsf{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \mathsf{End}_{Q} A^{\mathsf{al}}$ and assume that B is a quaternion algebra.
Can we guess $\mathsf{disc}\, B$?

If ℓ is ramified in $B \Rightarrow \ell$ cannot split in $\mathbb{Q}(\mathsf{Frob}_p)$

Example continued: QM vs (non-CM)^2

$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1)$ (LMFDB label: 262144.d.524288.1)

- $\mathrm{End}_{\mathbb{Q}} A_3^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\mathrm{End}_{\mathbb{Q}} A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \mathrm{End}_{\mathbb{R}} A^{\mathrm{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \mathrm{End}_Q A^{\mathrm{al}}$ and assume that B is a quaternion algebra.
Can we guess $\mathrm{disc}\, B$?

If ℓ is ramified in $B \Rightarrow \ell$ cannot split in $\mathbb{Q}(\mathrm{Frob}_p)$

- $5, 13, 17 \nmid \mathrm{disc}\, B$, as they split in $\mathbb{Q}(\sqrt{-3})$
- $7, 11 \nmid \mathrm{disc}\, B$, as they split in $\mathbb{Q}(\sqrt{-6})$

We can rule out all the primes except 2 and 3 (up to some bnd).

Example continued: QM vs (non-CM)^2

$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1)$ (LMFDB label: 262144.d.524288.1)

- $\mathrm{End}_{\mathbb{Q}} A_3^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\mathrm{End}_{\mathbb{Q}} A_5^{\mathrm{al}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \mathrm{End}_{\mathbb{R}} A^{\mathrm{al}} \neq M_2(\mathbb{C})$

Question

Write $B := \mathrm{End}_{Q} A^{\mathrm{al}}$ and assume that B is a quaternion algebra.
Can we guess $\mathrm{disc}\, B$?

If ℓ is ramified in $B \Rightarrow \ell$ cannot split in $\mathbb{Q}(\mathrm{Frob}_p)$

- $5, 13, 17 \nmid \mathrm{disc}\, B$, as they split in $\mathbb{Q}(\sqrt{-3})$
- $7, 11 \nmid \mathrm{disc}\, B$, as they split in $\mathbb{Q}(\sqrt{-6})$

We can rule out all the primes except 2 and 3 (up to some bnd). Indeed, $\mathrm{disc}\, B = 6$.

Using Sato–Tate distributions

Abelian surface	$\mathsf{End}_{\mathbb{R}} A$	$\mathrm{rk}\,\mathsf{NS}(A)$	$M_2[a_1] \stackrel{?}{=} E[a_{1,p}^2/p]$	$M_1[a_2] \stackrel{?}{=} E[a_{2,p}/p]$
CM^2	$\mathrm{M}_2(\mathbb{C})$	4	8	4
• QM abelian surface • $(\text{non-CM})^2$	$\mathrm{M}_2(\mathbb{R})$	3	4	3
• CM abelian surface • CM $\times$ CM	$\mathbb{C} \times \mathbb{C}$	2	4	2
CM $\times$ non-CM	$\mathbb{C} \times \mathbb{R}$	2	3	2
• RM abelian surf. • non-CM $\times$ non-CM	$\mathbb{R} \times \mathbb{R}$	2	2	2
generic abelian surface	$\mathbb{R}$	1	1	1

Question

Can you spot the pattern?

Arithmetic invariants from Sato-Tate moments

Theorem (Fité–C–Sutherland)

Let A be an abelian variety, then we have

- $\operatorname{rk}\operatorname{End}(A) = \mathsf{M}_2[a_1] = \mathsf{E}_{\mathrm{ST}_A}[\mathrm{tr}^2]$
- $\operatorname{rk}\mathrm{NS}(A) = \mathsf{M}_1[a_2] = \mathsf{E}_{\mathrm{ST}_A}[\mathrm{tr}(\Lambda^2)]$

This does not depend on any classification.

Arithmetic invariants from Sato-Tate moments

Theorem (Fité–C–Sutherland)

Let A be an abelian variety, then we have

- $\operatorname{rk}\operatorname{End}(A) = \mathrm{M}_2[a_1] = \mathrm{E}_{\mathrm{ST}_A}[\mathrm{tr}^2] \stackrel{?}{=} \mathrm{E}[\mathrm{tr}(\mathrm{Frob}_p\, p^{-1/2} | H^1(A))^2]$
- $\operatorname{rk}\mathrm{NS}(A) = \mathrm{M}_1[a_2] = \mathrm{E}_{\mathrm{ST}_A}[\mathrm{tr}(\Lambda^2)] \stackrel{?}{=} \mathrm{E}[\mathrm{tr}(\mathrm{Frob}_p\, | H^2(A)(1))]$

This does not depend on any classification.

Arithmetic invariants from Sato-Tate moments

Theorem (Fité–C–Sutherland)

Let A be an abelian variety, then we have

- $\operatorname{rk}\operatorname{End}(A) = \mathrm{M}_2[a_1] = \mathrm{E}_{\mathrm{ST}_A}[\mathrm{tr}^2] \stackrel{?}{=} \mathrm{E}[\mathrm{tr}(\mathrm{Frob}_p\, p^{-1/2} | H^1(A))^2]$
- $\operatorname{rk}\mathrm{NS}(A) = \mathrm{M}_1[a_2] = \mathrm{E}_{\mathrm{ST}_A}[\mathrm{tr}(\Lambda^2)] \stackrel{?}{=} \mathrm{E}[\mathrm{tr}(\mathrm{Frob}_p\, | H^2(A)(1))]$

This does not depend on any classification.

Theorem (Fité–C–Sutherland)

Let X be a K3 surface, then we have

$$\operatorname{rk}\mathrm{NS}(X) = \mathrm{M}_1[a_1] = \mathrm{E}_{\mathrm{ST}_X}[\mathrm{tr}]$$

Arithmetic invariants from Sato-Tate moments

Theorem (Fité–C–Sutherland)

Let A be an abelian variety, then we have

- $\operatorname{rk}\operatorname{End}(A) = \mathrm{M}_2[a_1] = \mathrm{E}_{\mathrm{ST}_A}[\mathrm{tr}^2] \overset{?}{=} \mathrm{E}[\mathrm{tr}(\mathrm{Frob}_p\, p^{-1/2} | H^1(A))^2]$
- $\operatorname{rk}\mathrm{NS}(A) = \mathrm{M}_1[a_2] = \mathrm{E}_{\mathrm{ST}_A}[\mathrm{tr}(\Lambda^2)] \overset{?}{=} \mathrm{E}[\mathrm{tr}(\mathrm{Frob}_p\, | H^2(A)(1))]$

This does not depend on any classification.

Theorem (Fité–C–Sutherland)

Let X be a K3 surface, then we have

$$\operatorname{rk}\mathrm{NS}(X) = \mathrm{M}_1[a_1] = \mathrm{E}_{\mathrm{ST}_X}[\mathrm{tr}] \overset{?}{=} \mathrm{E}[\mathrm{tr}(\mathrm{Frob}_p\, | H^2(X)(1))]$$

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves

They may arise in many ways:

- smooth quartic surfaces in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

- double cover of $\mathbb{P}^2$ branched over a sextic curve

$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

“Dans la seconde partie de mon rapport, il s’agit des variétés kählériennes dites K3, ainsi nommées en l’honneur de Kummer, Kähler, Kodaira et de la belle montagne K2 au Cachemire.” —André Weil

(Photo credit: Waqas Anees)

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves
They may arise in many ways:

- smooth quartic surfaces in $\mathbb{P}^3$
$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$
- double cover of $\mathbb{P}^2$ branched over a sextic curve
$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

Can we play similar game as before?

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves
They may arise in many ways:

- smooth quartic surfaces in $\mathbb{P}^3$
$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$
- double cover of $\mathbb{P}^2$ branched over a sextic curve
$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

Can we play similar game as before?
In this case, instead of studying $\#X_p$ or $\operatorname{tr} \mathrm{Frob}_p$ we study

$$p \longmapsto \operatorname{rk} \mathrm{NS}\, X_p{}^{\mathrm{al}} \in \{2, 4, \ldots, 22\}$$

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves
They may arise in many ways:

- smooth quartic surfaces in $\mathbb{P}^3$
$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$
- double cover of $\mathbb{P}^2$ branched over a sextic curve
$$X : w^2 = f(x, y, z), \quad \deg f = 6$$

Can we play similar game as before?
In this case, instead of studying $\#X_p$ or $\operatorname{tr} \mathrm{Frob}_p$ we study

$$p \longmapsto \operatorname{rk} \mathrm{NS}\, {X_p}^{\mathrm{al}} \in \{2, 4, \ldots, 22\}$$

We are still counting points

$$\operatorname{rk} \mathrm{NS}\, {X_p}^{\mathrm{al}} = \sum_{\zeta} \operatorname{ord}_{T=\zeta/p} Z_p(X, T), \text{ where } Z_p(X, T) := \exp\left(\sum_{r=1}^{\infty} \#X(\mathbb{F}_{p^r}) T^r / r\right)$$

The analogous problem for elliptic curves

$X/\mathbb{Q}$ a K3 surface

$$p \longmapsto \operatorname{rk} \mathrm{NS}\, X_p{}^{\mathrm{al}} \in \{2, 4, \ldots, 22\}$$

This is analogous to studying:

$$p \longmapsto \operatorname{rk} \mathrm{End}\, E_p^{\mathrm{al}} \in \{2, 4\}$$

The analogous problem for elliptic curves

$X/\mathbb{Q}$ a K3 surface

$$p \longmapsto \operatorname{rk} \mathrm{NS}\, X_p{}^{\mathrm{al}} \in \{2, 4, \ldots, 22\}$$

This is analogous to studying:

$$p \longmapsto \operatorname{rk} \mathrm{End}\, E_p^{\mathrm{al}} \in \{2, 4\}$$

Recall that:

- $\operatorname{rk} \mathrm{End}\, E_p^{\mathrm{al}} = 4 \iff a_p = 0$
- $\mathrm{Prob}(a_p = 0) = \begin{cases} \overset{?}{\sim} \frac{1}{\sqrt{p}} & \text{if } E \text{ is non-CM (Lang–Trotter)} \\ 1/2 & \text{if } E \text{ has CM by } \mathbb{Q}(\sqrt{-d}) \end{cases}$

In the latter case,

$$\{p : a_p = 0\} = \{p : p \text{ is ramified or inert in } \mathbb{Q}(\sqrt{-d})\}$$

The analogous problem for abelian surfaces

$X/\mathbb{Q}$ a K3 surface

$$p \longmapsto \operatorname{rk} \mathrm{NS}\, X_p{}^{\mathrm{al}} \in \{2, 4, \ldots, 22\}$$

For an abelian surface A we have:

$$\mathrm{NS}(A)_{\mathbb{Q}} \simeq \{\phi \in \mathrm{End}(A)_{\mathbb{Q}} : \phi^{\dagger} = \phi\},$$

where † denotes the Rosati involution.

The analogous problem for abelian surfaces

$X/\mathbb{Q}$ a K3 surface

$$p \longmapsto \operatorname{rk} \mathrm{NS}\, X_p{}^{\mathrm{al}} \in \{2, 4, \ldots, 22\}$$

For an abelian surface A we have:

$$\mathrm{NS}(A)_{\mathbb{Q}} \simeq \{\phi \in \mathrm{End}(A)_{\mathbb{Q}} : \phi^{\dagger} = \phi\},$$

where † denotes the Rosati involution. Thus for $A/\mathbb{Q}$ this is equivalent to

$$p \longmapsto \operatorname{rk} \mathrm{End}(A_p^{\mathrm{al}})_{\mathbb{Q}}^{\dagger} = \operatorname{rk} \mathrm{NS}\, A_p^{\mathrm{al}} \in \{2, 4, 6\}$$

Now

- $\operatorname{rk} \mathrm{NS}\, A_p^{\mathrm{al}} \geq 4 \iff A_p^{\mathrm{al}} \sim E^2$
- $\operatorname{rk} \mathrm{NS}\, A_p^{\mathrm{al}} = 6 \iff A_p^{\mathrm{al}} \sim E^2$, E supersingular, i.e., $a_p = 0$

If $\operatorname{rk} \mathrm{NS}\, A^{\mathrm{al}} = 1$, what is the "probability" of $\operatorname{rk} \mathrm{NS}\, A_p^{\mathrm{al}} \geq 4$?

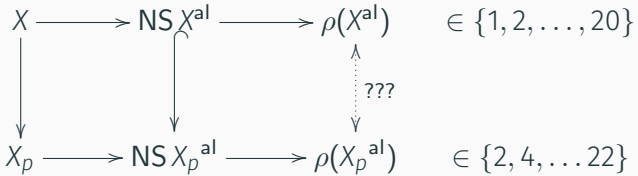
Néron–Severi group

- $\mathrm{NS}\,\bullet = $ Néron–Severi group of $\bullet \simeq \{\text{curves on } \bullet\}/\sim$
- $\rho(\bullet) = \operatorname{rk} \mathrm{NS}\,\bullet$
- $X_p := X \bmod p$

$$\begin{array}{ccccc} X & \longrightarrow & \mathrm{NS}\, X^{\mathrm{al}} & \longrightarrow & \rho(X^{\mathrm{al}}) \quad \in \{1, 2, \ldots, 20\} \\ \downarrow & & \downarrow & & \uparrow \\ & & & & ??? \\ \downarrow & & \downarrow & & \downarrow \\ X_p & \longrightarrow & \mathrm{NS}\, X_p{}^{\mathrm{al}} & \longrightarrow & \rho(X_p{}^{\mathrm{al}}) \quad \in \{2, 4, \ldots 22\} \end{array}$$

Néron–Severi group

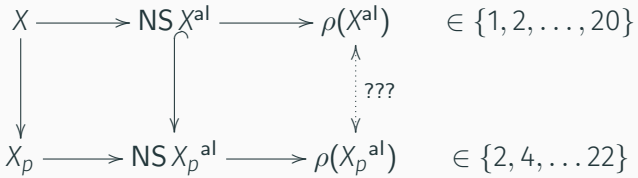
- $\mathrm{NS}\,\bullet$ = Néron–Severi group of $\bullet \simeq \{\text{curves on } \bullet\}/\sim$
- $\rho(\bullet) = \mathrm{rk}\,\mathrm{NS}\,\bullet$
- $X_p := X \bmod p$



Theorem (Charles)

For infinitely many p we have $\rho(X_p{}^{\mathrm{al}}) = \min_q \rho(X_q{}^{\mathrm{al}})$.

The Problem



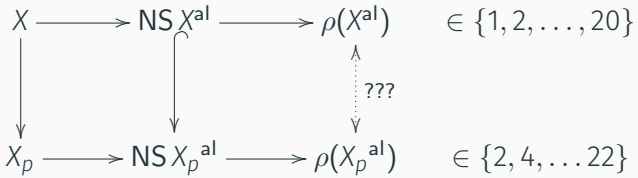
Theorem (Charles)

For infinitely many p we have $\rho({X_p}^{\mathrm{al}}) = \min_q \rho({X_q}^{\mathrm{al}})$.

What can we say about:

- $\Pi_{\mathrm{jump}}(X) := \left\{p : \rho({X_p}^{\mathrm{al}}) > \min_q \rho({X_q}^{\mathrm{al}})\right\}$

The Problem



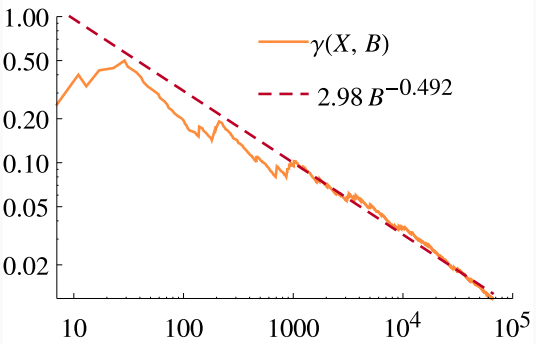
Theorem (Charles)

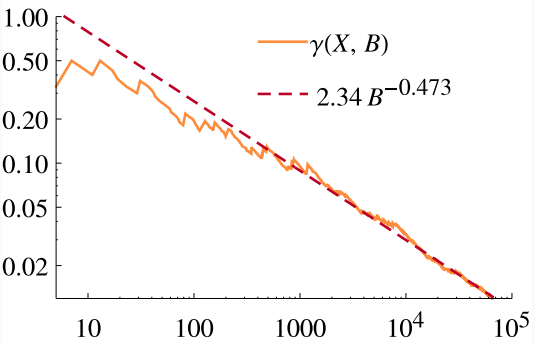
For infinitely many p we have $\rho({X_p}^{\mathrm{al}}) = \min_q \rho({X_q}^{\mathrm{al}})$.

What can we say about:

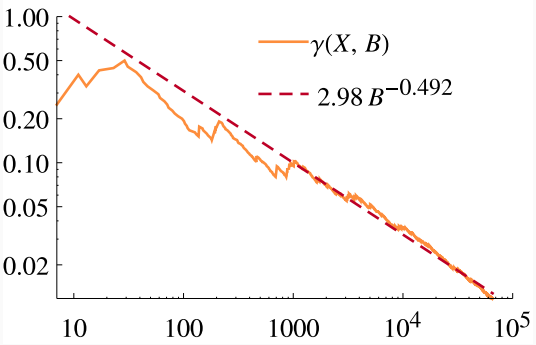
- $\Pi_{\mathrm{jump}}(X) := \left\{p : \rho({X_p}^{\mathrm{al}}) > \min_q \rho({X_q}^{\mathrm{al}})\right\}$
- $\gamma(X, B) := \dfrac{\#\left\{p \leq B : p \in \Pi_{\mathrm{jump}}(X)\right\}}{\#\left\{p \leq B\right\}}$ as $B \to \infty$

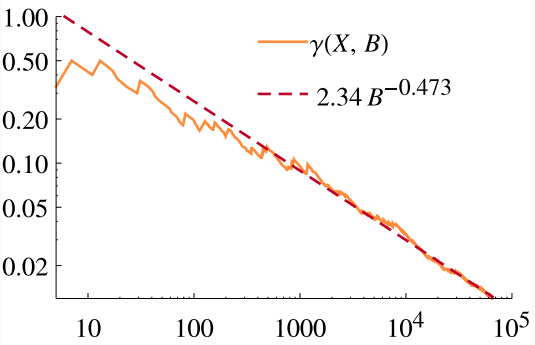
Two generic K3 surfaces with $\rho(X^{\mathrm{al}}) = 1$





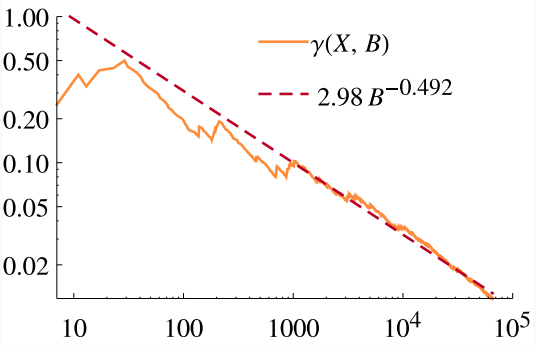
Two generic K3 surfaces with $\rho(X^{\mathrm{al}}) = 1$

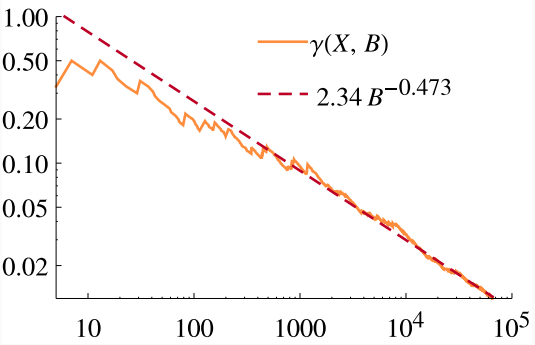




$$\gamma(X, B) \overset{?}{\sim} \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

Two generic K3 surfaces with $\rho(X^{\mathrm{al}}) = 1$

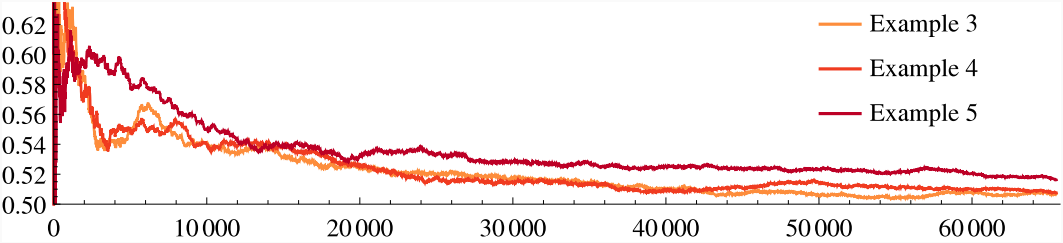




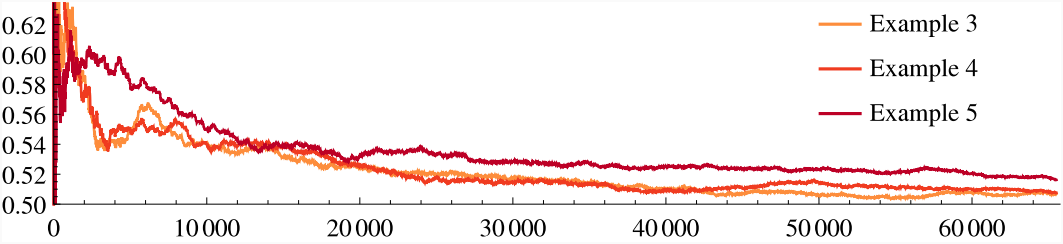
$$\gamma(X, B) \overset{?}{\sim} \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

$$\Longrightarrow \ \mathrm{Prob}(p \in \Pi_{\mathrm{jump}}(X)) \overset{?}{\sim} 1/\sqrt{p}$$

Three K3 surfaces with $\rho(X^{\mathrm{al}}) = 2$

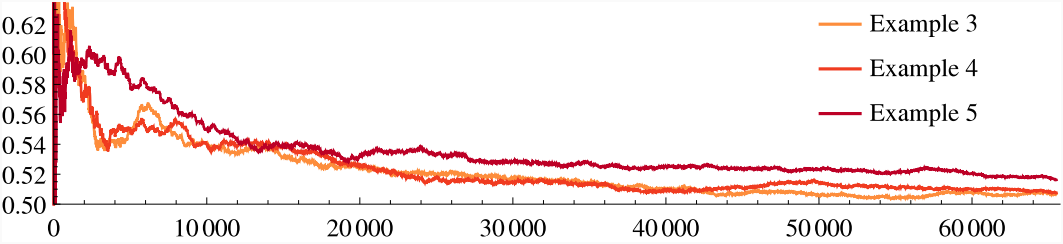


Three K3 surfaces with $\rho(X^{\mathrm{al}}) = 2$



Do you see an obvious trend?

Three K3 surfaces with $\rho(X^{\mathrm{al}}) = 2$



Do you see an obvious trend?

Could it be related to some integer being a square modulo p?

We can explain the 1/2

Theorem (C, C–Elsenhans–Jahnel)

If $\rho(X^{\mathrm{al}}) = \min_q \rho({X_p}^{\mathrm{al}})$, *then there is a* $d_X \in \mathbb{Z}$ *such that:*

$$\left\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\right\} \subset \Pi_{\mathrm{jump}}(X).$$

In general d_X *is not a square, and it can be described as the discriminant of a sub Galois representation associated to X.*

We can explain the 1/2

Theorem (C, C–Elsenhans–Jahnel)

If $\rho(X^{\mathrm{al}}) = \min_q \rho({X_p}^{\mathrm{al}})$, *then there is a* $d_X \in \mathbb{Z}$ *such that:*

$$\left\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\right\} \subset \Pi_{\mathrm{jump}}(X).$$

In general d_X *is not a square, and it can be described as the discriminant of a sub Galois representation associated to* X.

Corollary

If d_X *is not a square:*

- $\liminf_{B\to\infty} \gamma(X, B) \geq 1/2$
- X^{al} *has infinitely many rational curves.*

We can explain the 1/2

Theorem (C, C–Elsenhans–Jahnel)

If $\rho(X^{\mathrm{al}}) = \min_q \rho({X_p}^{\mathrm{al}})$, *then there is a* $d_X \in \mathbb{Z}$ *such that:*

$$\left\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\right\} \subset \Pi_{\mathrm{jump}}(X).$$

In general d_X *is not a square, and it can be described as the discriminant of a sub Galois representation associated to* X.

Corollary

If d_X *is not a square:*

- $\liminf_{B\to\infty} \gamma(X, B) \geq 1/2$
- X^{al} *has infinitely many rational curves.*

$D_3 = -1 \cdot 5 \cdot 151 \cdot 22490817357414371041 \cdot 387308497430149337233666358807996260780875056740850984213276970343278935342068889706146733313789$

$D_4 = 53 \cdot 2624174618795407 \cdot 5128545618469648171394942020727783 41 \cdot 12152183700890287690767181021269217443533628 73 \cdot 6847124397158950456921300435158$

$D_5 = -1 \cdot 47 \cdot 3109 \cdot 4969 \cdot 14857095849982608071 \cdot 44541027766092834776258676433187443220258468801614 9 \cdot 6586527085250526999934241987388424859981 15$

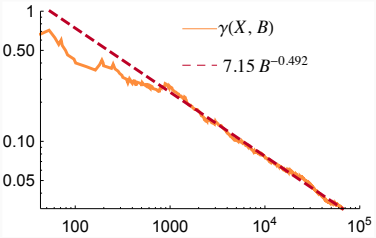
Experimental data for $\rho(X^{\mathrm{al}}) = 2$ (again)

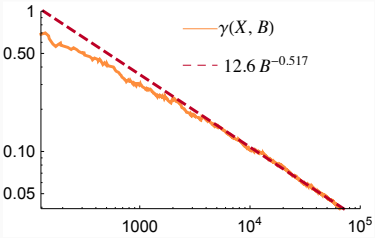
What if we ignore $\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\} \subset \Pi_{\mathrm{jump}}(X)$?

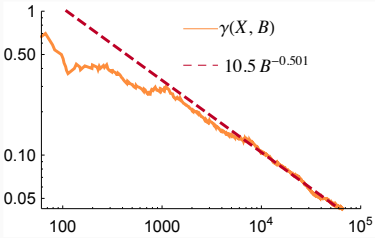
Experimental data for $\rho(X^{\mathrm{al}}) = 2$ (again)

What if we ignore $\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\} \subset \Pi_{\mathrm{jump}}(X)$?

$$\gamma\left(X_{\mathbb{Q}(\sqrt{d_X})}, B\right) \overset{?}{\sim} \frac{c}{\sqrt{B}}, \quad B \to \infty$$



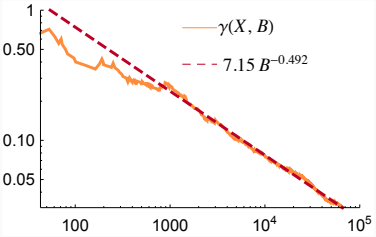


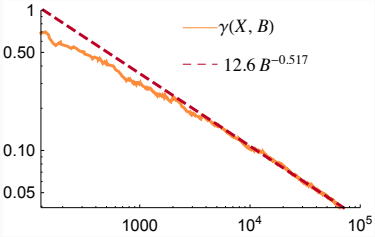


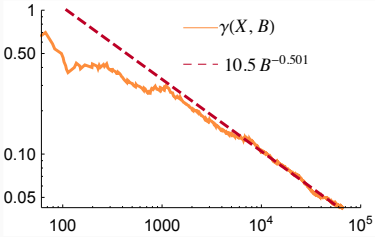
Experimental data for $\rho(X^{\mathrm{al}}) = 2$ (again)

What if we ignore $\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\} \subset \Pi_{\mathrm{jump}}(X)$?

$$\gamma\left(X_{\mathbb{Q}(\sqrt{d_X})}, B\right) \overset{?}{\sim} \frac{c}{\sqrt{B}}, \quad B \to \infty$$







$$\mathrm{Prob}(p \in \Pi_{\mathrm{jump}}(X)) = \begin{cases} 1 & \text{if } d_X \text{ is not a square modulo } p \\ \overset{?}{\sim} \frac{1}{\sqrt{p}} & \textit{otherwise} \end{cases}$$