Randomness in number theory

Edgar Costa (MIT)

November 29th, 2018

Colorado State University

Slides available at `edgarcosta.org` under Research

Randomness principle in number theory

Number theoretic dichotomy [Sarnak]

Given a problem, either

1. there is a rigid structure $\rightsquigarrow$ rigid solution, or
2. the answer is difficult to determine $\rightsquigarrow$ random behaviour

Randomness principle in number theory

Number theoretic dichotomy [Sarnak]

Given a problem, either

1. there is a rigid structure $\rightsquigarrow$ rigid solution, or
2. the answer is difficult to determine $\rightsquigarrow$ random behaviour

- Understanding and/or proving the probability law
  $\rightsquigarrow$ deep understanding of the phenomenon

Randomness principle in number theory

Number theoretic dichotomy [Sarnak]

Given a problem, either

1. there is a rigid structure $\rightsquigarrow$ rigid solution, or
2. the answer is difficult to determine $\rightsquigarrow$ random behaviour

- Understanding and/or proving the probability law
  $\rightsquigarrow$ deep understanding of the phenomenon
- Real world applications
  - pseudo random numbers
  - cryptography
  - quasi-Monte Carlo methods

Counting roots of polynomials

$f(x) \in \mathbb{Z}[x]$ a monic irreducible polynomial of degree $d > 0$

Question

How many roots does f have?

Counting roots of polynomials

$f(x) \in \mathbb{Z}[x]$ a monic irreducible polynomial of degree $d > 0$

Question

How many roots does f have?

- At most d

Counting roots of polynomials

$f(x) \in \mathbb{Z}[x]$ a monic irreducible polynomial of degree $d > 0$

Question

How many roots does f have?

- Over $\mathbb{C}$ or $\mathbb{Q}^{\mathrm{al}}$ we know that it has d roots.

Counting roots of polynomials

$f(x) \in \mathbb{Z}[x]$ a monic irreducible polynomial of degree $d > 0$

Question

How many roots does f have?

- Over $\mathbb{C}$ or $\mathbb{Q}^{\mathsf{al}}$ we know that it has d roots.
- What about over $\mathbb{R}$?

Counting roots of polynomials

$f(x) \in \mathbb{Z}[x]$ a monic irreducible polynomial of degree $d > 0$

Question

How many roots does f have?

- Over $\mathbb{C}$ or $\mathbb{Q}^{\mathsf{al}}$ we know that it has d roots.
- What about over $\mathbb{R}$?

For quadratic polynomials, $x^2 + ax + b$, the answer just depends on the sign of $\Delta := a^2 - 4b$.

Counting roots of polynomials over finite fields

$f(x) \in \mathbb{Z}[x]$ a monic irreducible polynomial of degree $d > 0$

Question

How many roots does f have?

$$\begin{aligned} N_f(p) :=& \#\{x \in \{0, \ldots, p-1\} \ : \ f(x) \equiv 0 \bmod p\} \\ =& \#\{x \in \{0, \ldots, p-1\} \ : \ p \mid f(x)\} \\ =& \#\{x \in \mathbb{F}_p \ : \ f(x) = 0\} \in \{0, 1, \ldots, d\} \end{aligned}$$

Counting roots of polynomials over finite fields

$f(x) \in \mathbb{Z}[x]$ a monic irreducible polynomial of degree $d > 0$

Question

How many roots does f have?

$$\begin{aligned} N_f(p) :=& \#\{x \in \{0, \ldots, p-1\} \ : \ f(x) \equiv 0 \bmod p\} \\ =& \#\{x \in \{0, \ldots, p-1\} \ : \ p \mid f(x)\} \\ =& \#\{x \in \mathbb{F}_p \ : \ f(x) = 0\} \in \{0, 1, \ldots, d\} \end{aligned}$$

Question

How often does each value occur?

Quadratic polynomials

$$f(x) = x^2 + ax + b, \quad \Delta := a^2 - 4b$$

$$\text{Quadratic formula} \implies N_f(p) = \begin{cases} 0 & \text{if } \Delta \text{ is not a square modulo } p \\ 1 & \text{if } \Delta \equiv 0 \bmod p \\ 2 & \text{if } \Delta \text{ is a square modulo } p \end{cases}$$

Quadratic polynomials

$$f(x) = x^2 + ax + b, \quad \Delta := a^2 - 4b$$

$$\text{Quadratic formula} \implies N_f(p) = \begin{cases} 0 & \text{if } \Delta \text{ is not a square modulo } p \\ 1 & \text{if } \Delta \equiv 0 \bmod p \\ 2 & \text{if } \Delta \text{ is a square modulo } p \end{cases}$$

Half of the numbers modulo p are squares.

Quadratic polynomials

$$f(x) = x^2 + ax + b, \quad \Delta := a^2 - 4b$$

$$\text{Quadratic formula} \implies N_f(p) = \begin{cases} 0 & \text{if } \Delta \text{ is not a square modulo } p \\ 1 & \text{if } \Delta \equiv 0 \bmod p \\ 2 & \text{if } \Delta \text{ is a square modulo } p \end{cases}$$

Half of the numbers modulo p are squares.
Hence, if $\Delta \in \mathbb{Z}$ isn't a square, then

$$\mathsf{Prob}(\Delta \text{ is a square modulo } p) = 1/2$$

$$\implies \mathsf{Prob}(N_f(p) = 0) = \mathsf{Prob}(N_f(p) = 2) = \frac{1}{2}$$

Quadratic polynomials

$$f(x) = x^2 + ax + b, \quad \Delta := a^2 - 4b$$

$$\text{Quadratic formula} \implies N_f(p) = \begin{cases} 0 & \text{if } \Delta \text{ is not a square modulo } p \\ 1 & \text{if } \Delta \equiv 0 \bmod p \\ 2 & \text{if } \Delta \text{ is a square modulo } p \end{cases}$$

Half of the numbers modulo p are squares.
Hence, if $\Delta \in \mathbb{Z}$ isn't a square, then

$$\mathsf{Prob}(\Delta \text{ is a square modulo } p) = 1/2$$

$$\implies \mathsf{Prob}(N_f(p) = 0) = \mathsf{Prob}(N_f(p) = 2) = \frac{1}{2}$$

It is easy to describe for which primes Δ is a square $\bmod p$.
For example, 5 is a square for $p \equiv 1, 4 \bmod 5$ and $p = 2$.

Cubic polynomials

$$f(x) = x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x - \sqrt[3]{2}e^{2\pi i/3}\right)\left(x - \sqrt[3]{2}e^{4\pi i/3}\right)$$

$$\text{Prob}\left(N_f(p) = k\right) = \begin{cases} 1/3 & \text{if } k = 0 \\ 1/2 & \text{if } k = 1 \\ 1/6 & \text{if } k = 3. \end{cases}$$

$$g(x) = x^3 - x^2 - 2x + 1 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

$$\text{Prob}\left(N_g(p) = k\right) = \begin{cases} 2/3 & \text{if } k = 0 \\ 1/3 & \text{if } k = 3. \end{cases}$$

Cubic polynomials

$$f(x) = x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x - \sqrt[3]{2}e^{2\pi i/3}\right)\left(x - \sqrt[3]{2}e^{4\pi i/3}\right)$$

$$\text{Prob}\left(N_f(p) = k\right) = \begin{cases} 1/3 & \text{if } k = 0 \\ 1/2 & \text{if } k = 1 \\ 1/6 & \text{if } k = 3. \end{cases}$$

$$g(x) = x^3 - x^2 - 2x + 1 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

$$\text{Prob}\left(N_g(p) = k\right) = \begin{cases} 2/3 & \text{if } k = 0 \\ 1/3 & \text{if } k = 3. \end{cases}$$

Theorem (Frobenius)

$$\text{Prob}(N_f(p) = i) = \text{Prob}(g \in \text{Gal}(f) : g \textit{ fixes } i \textit{ roots}),$$

Cubic polynomials

$$f(x) = x^3 - 2 = \left(x - \sqrt[3]{2}\right)\left(x - \sqrt[3]{2}e^{2\pi i/3}\right)\left(x - \sqrt[3]{2}e^{4\pi i/3}\right)$$

$$\text{Prob}\left(N_f(p) = k\right) = \begin{cases} 1/3 & \text{if } k = 0 \\ 1/2 & \text{if } k = 1 \\ 1/6 & \text{if } k = 3. \end{cases} \Rightarrow \text{Gal}(f) = S_3$$

$$g(x) = x^3 - x^2 - 2x + 1 = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)$$

$$\text{Prob}\left(N_g(p) = k\right) = \begin{cases} 2/3 & \text{if } k = 0 \\ 1/3 & \text{if } k = 3. \end{cases} \Rightarrow \text{Gal}(g) = \mathbb{Z}/3\mathbb{Z}$$

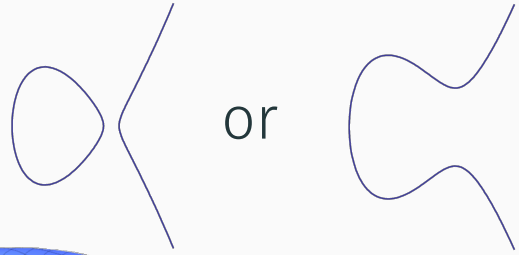
Theorem (Frobenius)

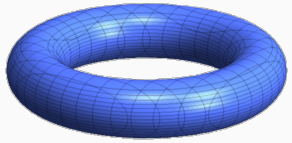
$$\text{Prob}(N_f(p) = i) = \text{Prob}(g \in \text{Gal}(f) : g \textit{ fixes } i \textit{ roots}),$$

Elliptic curves

An *elliptic curve* is a smooth curve defined by

$$y^2 = x^3 + ax + b$$

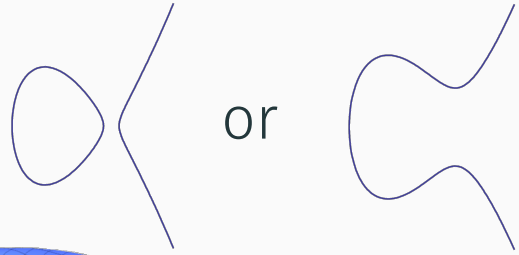
Over $\mathbb{R}$ it might look like  or

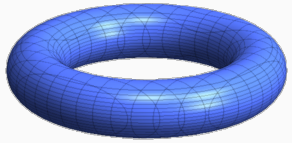
Over $\mathbb{C}$ this is a torus 

Elliptic curves

An *elliptic curve* is a smooth curve defined by

$$y^2 = x^3 + ax + b$$

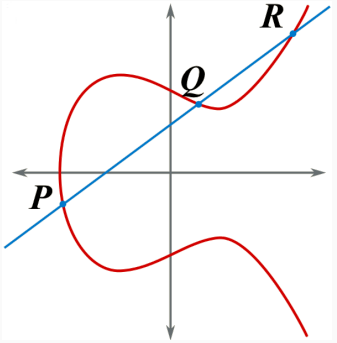
Over $\mathbb{R}$ it might look like  or

Over $\mathbb{C}$ this is a torus 

There is a natural *group structure*!

If P, Q, and R are colinear, then

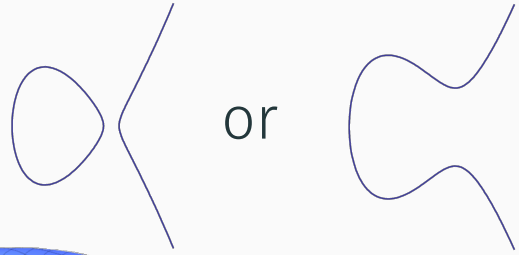
$$P + Q + R = 0$$

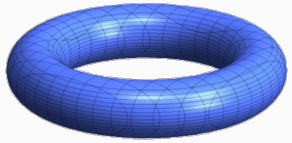


Elliptic curves

An *elliptic curve* is a smooth curve defined by

$$y^2 = x^3 + ax + b$$

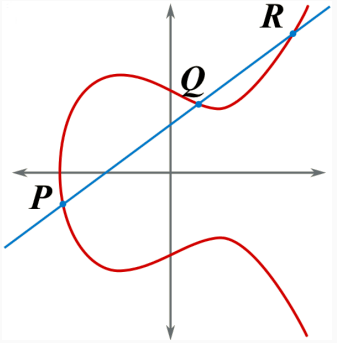
Over $\mathbb{R}$ it might look like  or

Over $\mathbb{C}$ this is a torus 

There is a natural *group structure*!

If P, Q, and R are colinear, then

$$P + Q + R = 0$$



Applications:

- cryptography
- integer factorization
- pseudorandom numbers, ...

Elliptic curves

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

Write $E_p := E \bmod p$

- 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 $E_p := E \bmod p$

- 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 $E_p := E \bmod p$

- 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 $\#E_p$.

Hasse's bound

Theorem (Hasse, 1930s)

$$|p + 1 - \#E_p| \leq 2\sqrt{p}.$$

Hasse's bound

Theorem (Hasse, 1930s)

$$|p + 1 - \#E_p| \leq 2\sqrt{p}.$$

In other words,

$$\lambda_p := \frac{p + 1 - \#E_p}{\sqrt{p}} \in [-2, 2]$$

What can we say about the error term, λ_p, as $p \to \infty$?

Two types of elliptic curves

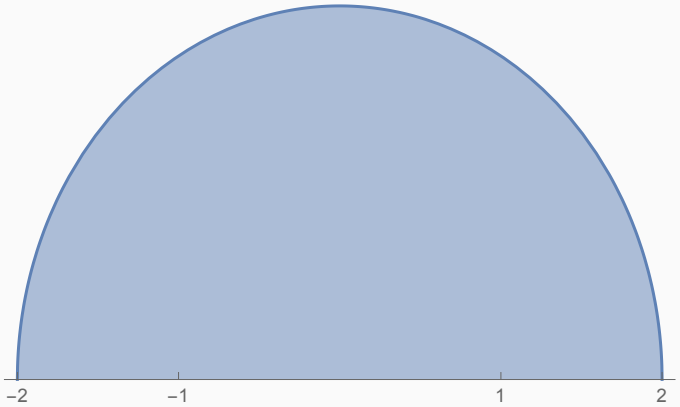
$$\lambda_p := \frac{p+1-\#E_p}{\sqrt{p}} \in [-2,2]$$

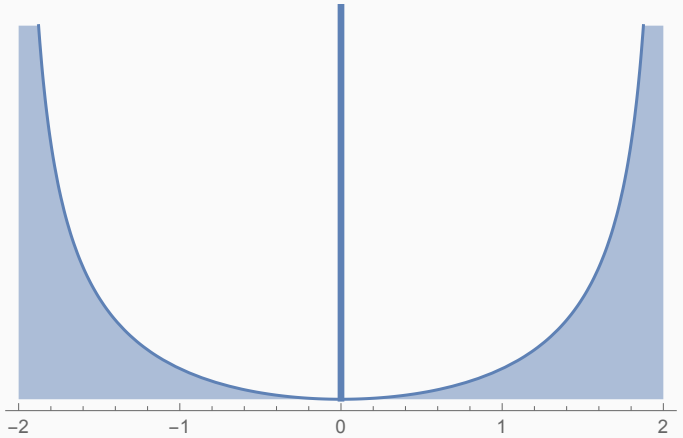
There are two limiting distributions for λ_p

Two types of elliptic curves

$$\lambda_p := \frac{p+1-\#E_p}{\sqrt{p}} \in [-2,2]$$

There are two limiting distributions for λ_p





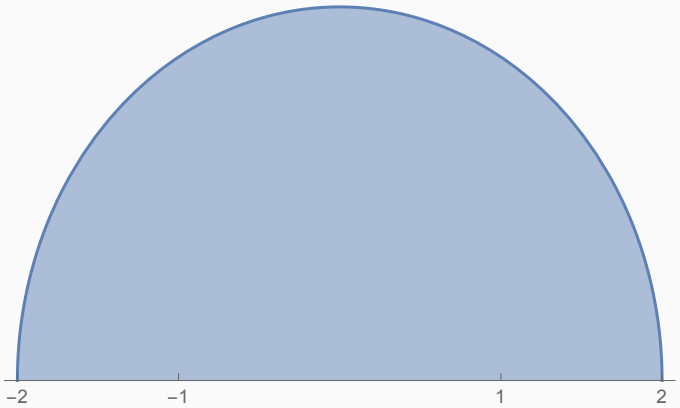
Two types of elliptic curves

$$\lambda_p := \frac{p+1-\#E_p}{\sqrt{p}} \in [-2,2]$$

There are two limiting distributions for λ_p

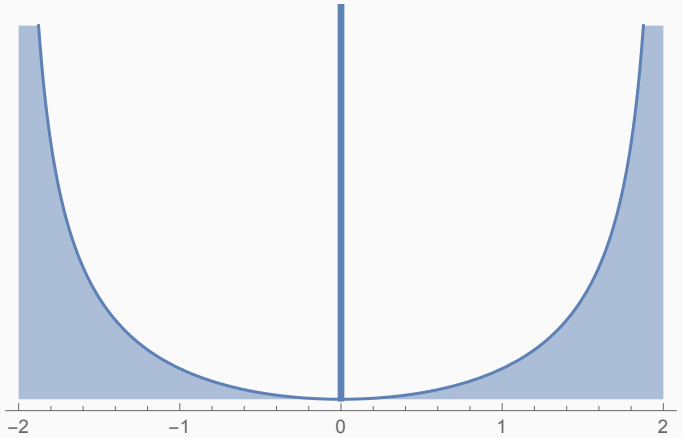
ordinary

$\mathsf{End}\, E^{\mathsf{al}} = \mathbb{Z}$



special

$\mathsf{End}\, E^{\mathsf{al}} \neq \mathbb{Z}$



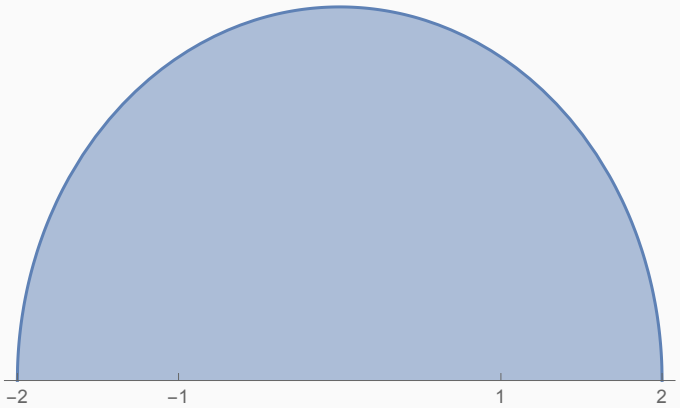
Two types of elliptic curves

$$\lambda_p := \frac{p+1-\#E_p}{\sqrt{p}} \in [-2,2]$$

There are two limiting distributions for λ_p

ordinary

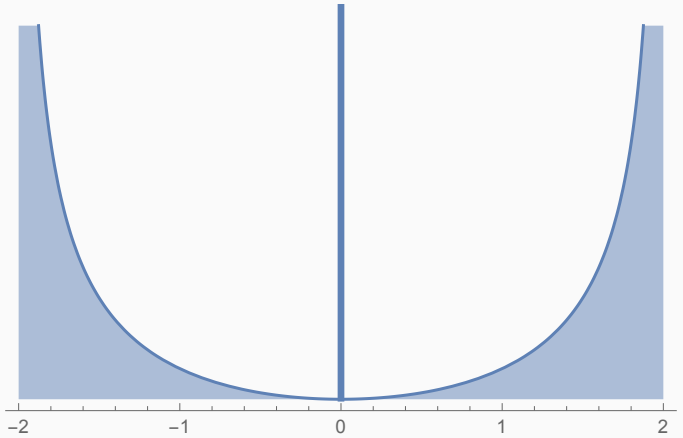
$\mathsf{End}\, E^{\mathsf{al}} = \mathbb{Z}$



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

special

$\mathsf{End}\, E^{\mathsf{al}} \neq \mathbb{Z}$

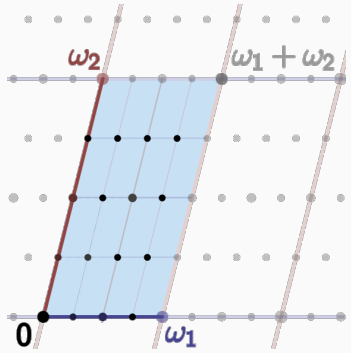


$\mathsf{Prob}(\lambda_p = 0) = 1/2$

Two types of elliptic curves

Over $\mathbb{C}$ an elliptic curve E is a torus

$E_{\mathbb{C}} \simeq \mathbb{C}/\Lambda, \quad$ where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 =$

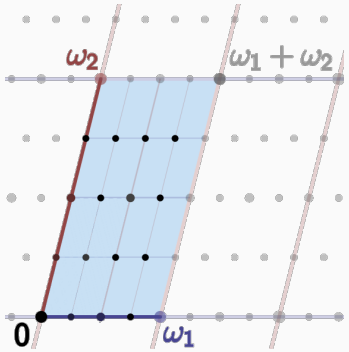


and we have $\mathsf{End}\, E^{\mathsf{al}} = \mathsf{End}\, \Lambda$

Two types of elliptic curves

Over $\mathbb{C}$ an elliptic curve E is a torus

$E_{\mathbb{C}} \simeq \mathbb{C}/\Lambda, \quad$ where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 =$



and we have $\mathbf{End}\, E^{\mathsf{al}} = \mathbf{End}\, \Lambda$

ordinary

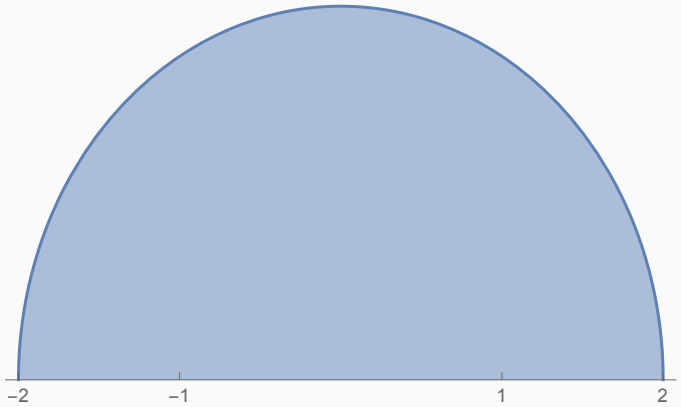
$\mathbf{End}\, \Lambda = \mathbb{Z}$

special

$\mathbb{Z} \subsetneq \mathbf{End}(\Lambda) \subset \mathbb{Q}(\sqrt{-d})$

$\omega_2/\omega_1 \in \mathbb{Q}(\sqrt{-d})$ for some $d > 0$

non-CM

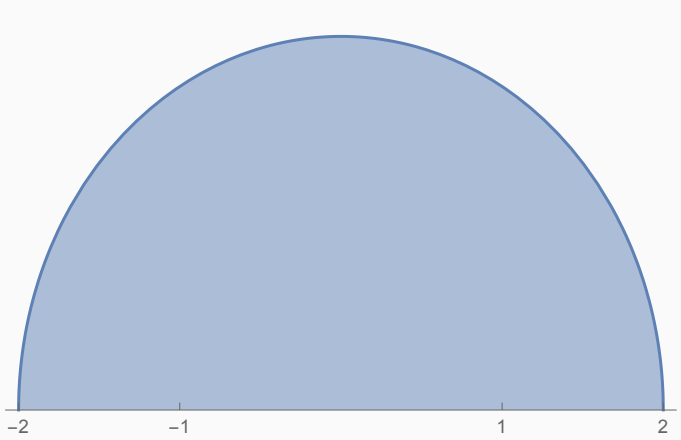


CM

How to distinguish between the two types?

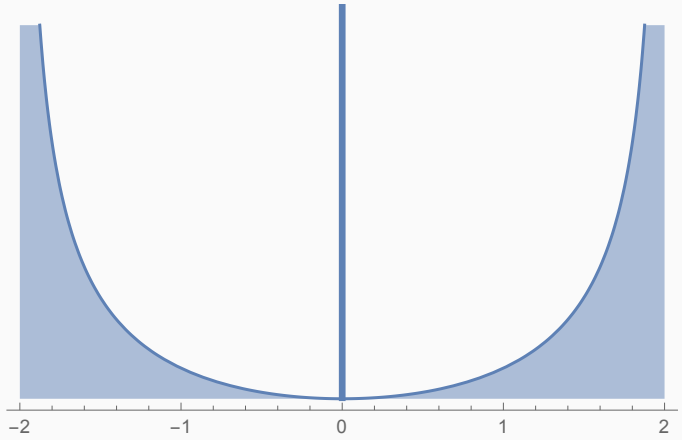
non-CM

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



CM

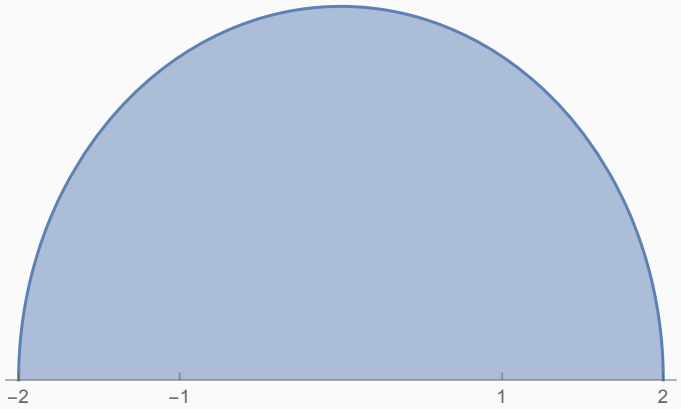
$\mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-d})$



How to distinguish between the two types?

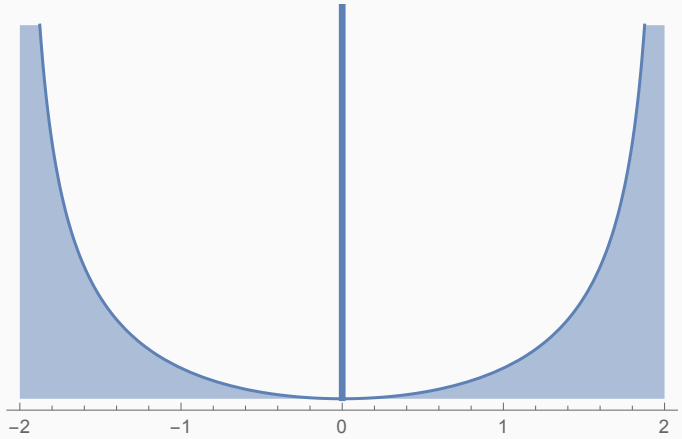
non-CM

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



CM

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



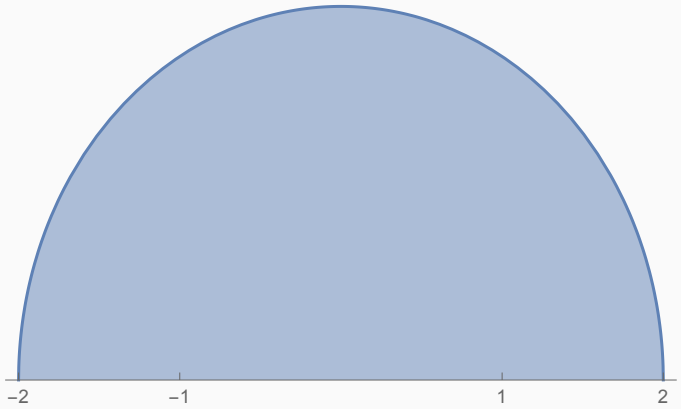
It is enough to count points!

$$p + 1 - \#E_p =: a_p \neq 0 \Longrightarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} \subset \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right)$$

How to distinguish between the two types?

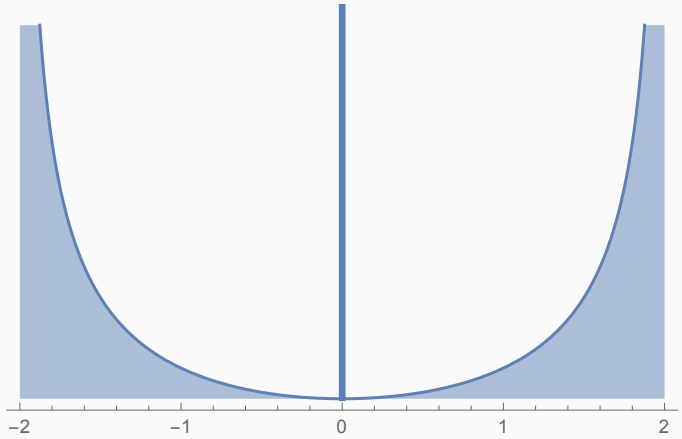
non-CM

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



CM

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



It is enough to count points!

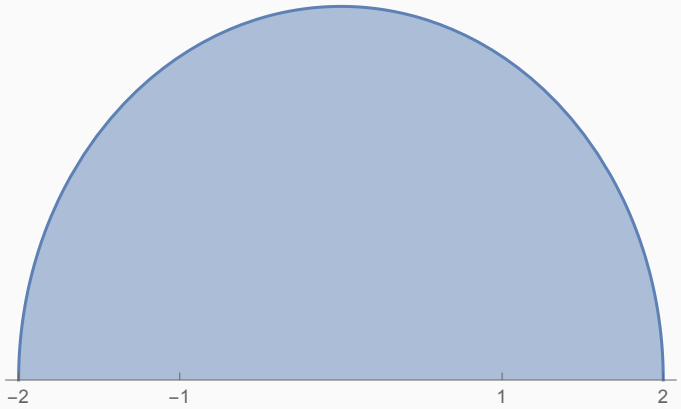
$$p + 1 - \#E_p =: a_p \neq 0 \Longrightarrow \mathsf{End}_{\mathbb{Q}} E^{\mathsf{al}} \subset \mathbb{Q}\left(\sqrt{a_p^2 - 4p}\right)$$

- If E is non-CM, then $\mathbb{Q}(\sqrt{a_p^2 - 4p}) \not\simeq \mathbb{Q}(\sqrt{a_q^2 - 4q})$ for $p \neq q$ with prob. 1.

How to distinguish between the two types?

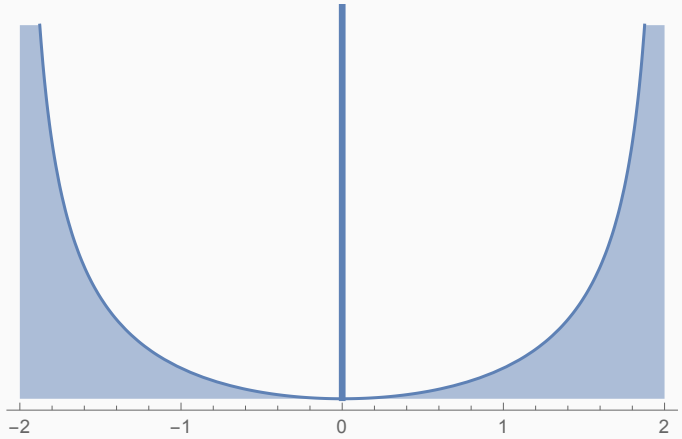
non-CM

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



CM

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



It is enough to count points!

$$p + 1 - \#E_p =: a_p \neq 0 \Longrightarrow \mathsf{End}_{\mathbb{Q}} E^{\mathsf{al}} \subset \mathbb{Q}(\sqrt{a_p^2 - 4p})$$

- If E is non-CM, then $\mathbb{Q}(\sqrt{a_p^2 - 4p}) \not\simeq \mathbb{Q}(\sqrt{a_q^2 - 4q})$ for $p \neq q$ with prob. 1.
- If E has CM, then $\mathbb{Q}(\sqrt{-d}) \simeq \mathbb{Q}(\sqrt{a_p^2 - 4p})$.

Group-theoretic interpretation

There is a simple group-theoretic descriptions for these histograms!

Group-theoretic interpretation

There is a simple group-theoretic descriptions for these histograms!

- To E we associate a compact Lie group $\mathrm{ST}_E \subset \mathrm{SU}(2)$
- This group is know as the *Sato–Tate* group of E.
- You may think of it as the “Galois” group of E.

Group-theoretic interpretation

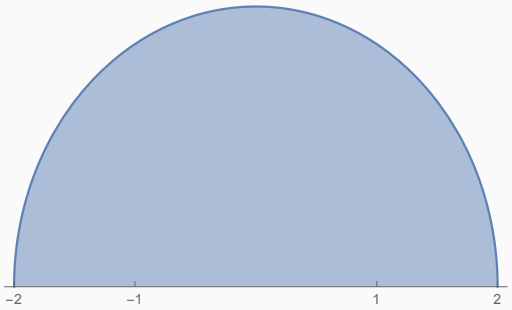
There is a simple group-theoretic descriptions for these histograms!

- To E we associate a compact Lie group $\mathrm{ST}_E \subset \mathrm{SU}(2)$
- This group is know as the *Sato–Tate* group of E.
- You may think of it as the "Galois" group of E.

Then, the a_p are distributed as the trace of a matrix chosen at random from ST_E with respect to its Haar measure.

non-CM

$\mathrm{SU}(2)$

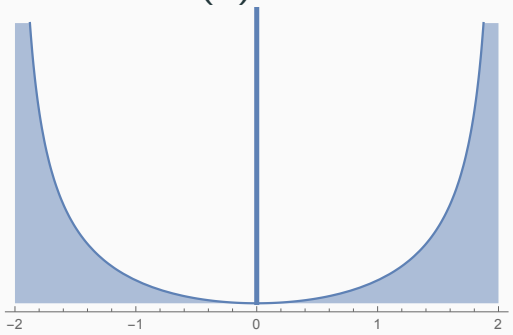


CM

$\mathrm{U}(1)$

CM (with the δ)

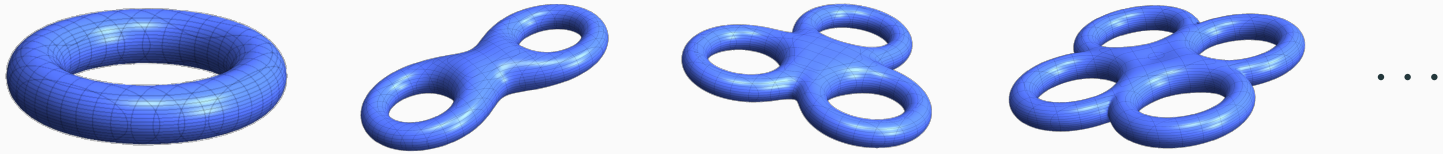
$\mathrm{N}_{\mathrm{SU}(2)}(\mathrm{U}(1))$



Higher Genus curves

Let's now consider curves with higher genus = #handles.

$g = 1$ $g = 2$ $g = 3$ $g = 4$ $\cdots$

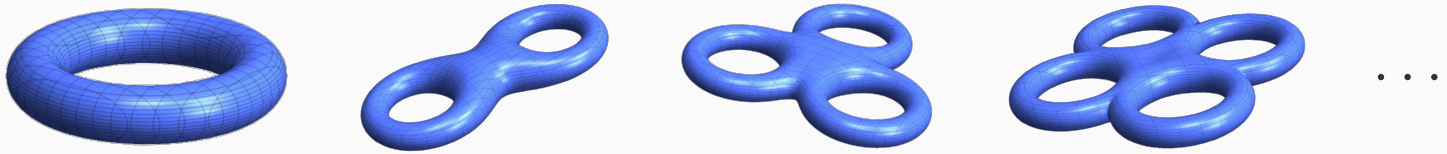


$\cdots$

Higher Genus curves

Let's now consider curves with higher genus = #handles.

$g = 1$ $g = 2$ $g = 3$ $g = 4$ $\cdots$



$\cdots$

For example, an hyperelliptic curve:

$$C : y^2 = a_{2g+2}x^{2g+2} + \cdots + a_0$$

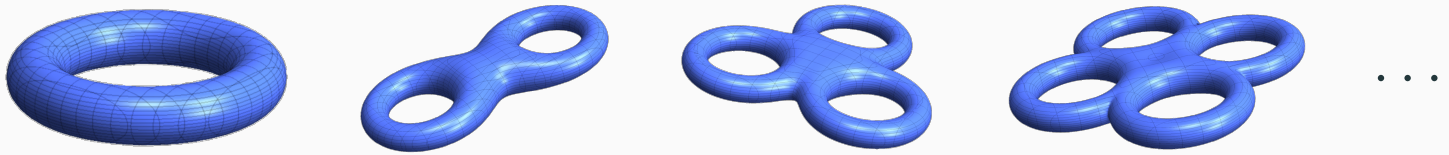
We may the Jacobian to obtain an object with a group structure

$$A := \mathsf{Jac}(C) \simeq_{\mathbb{C}} \mathbb{C}^g/\Lambda$$

Higher Genus curves

Let's now consider curves with higher genus = #handles.

$g = 1$ $g = 2$ $g = 3$ $g = 4$ $\cdots$



$\cdots$

For example, an hyperelliptic curve:

$$C : y^2 = a_{2g+2}x^{2g+2} + \cdots + a_0$$

We may the Jacobian to obtain an object with a group structure

$$A := \mathsf{Jac}(C) \simeq_{\mathbb{C}} \mathbb{C}^g/\Lambda$$

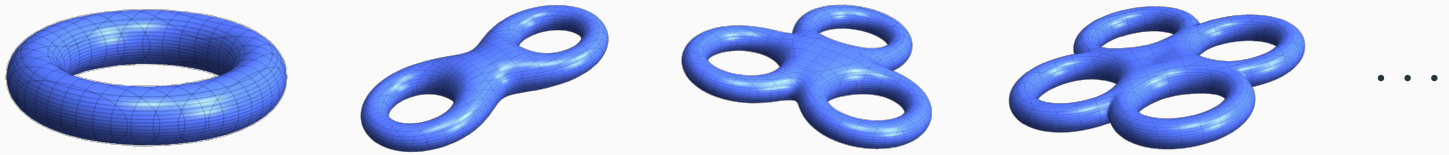
Question

Can we repeat the same experiment?

Higher Genus curves

Let's now consider curves with higher genus = #handles.

$g = 1$ $g = 2$ $g = 3$ $g = 4$ $\cdots$



$\cdots$

For example, an hyperelliptic curve:

$$C : y^2 = a_{2g+2}x^{2g+2} + \cdots + a_0$$

We may the Jacobian to obtain an object with a group structure

$$A := \mathsf{Jac}(C) \simeq_{\mathbb{C}} \mathbb{C}^g/\Lambda$$

Question

Can we repeat the same experiment?

Now we will need to count solutions over $\mathbb{F}_{p^i}$ for $i = 1, \cdots, g$.

Zeta functions and Frobenius polynomials

Question

Can we repeat the same experiment?

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

Zeta functions and Frobenius polynomials

Question

Can we repeat the same experiment?

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

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

Zeta functions and Frobenius polynomials

Question

Can we repeat the same experiment?

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

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

$$L_p(T) = \det(1 - t\,\mathrm{Frob}_p \,|H^1(C)) = \det(1 - t\,\mathrm{Frob}_p \,|H^1(A))$$

Zeta functions and Frobenius polynomials

Question

Can we repeat the same experiment?

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

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

$$L_p(T) = \det(1 - t\,\mathrm{Frob}_p \,|H^1(C)) = \det(1 - t\,\mathrm{Frob}_p \,|H^1(A))$$

- $g = 1 \rightsquigarrow L_p(T) = 1 - a_pT + pT^2$

Zeta functions and Frobenius polynomials

Question

Can we repeat the same experiment?

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

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

$$L_p(T) = \det(1 - t\,\mathrm{Frob}_p \,|H^1(C)) = \det(1 - t\,\mathrm{Frob}_p \,|H^1(A))$$

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

Zeta functions and Frobenius polynomials

Question

Can we repeat the same experiment?

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

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

$$L_p(T) = \det(1 - t\,\mathrm{Frob}_p \,|H^1(C)) = \det(1 - t\,\mathrm{Frob}_p \,|H^1(A))$$

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

Sato–Tate conjecture

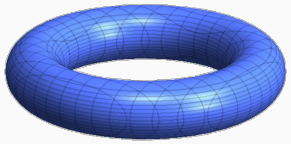
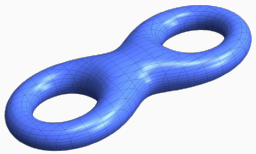
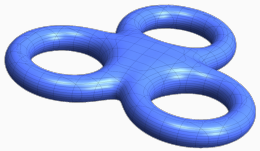
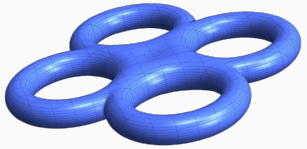
$L_p(T/\sqrt{p})$ are equidistributed according to $\mathrm{ST}_A \subset \mathrm{USp}(2g)$

Possible distributions out there

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

Sato–Tate conjecture

$L_p(T/\sqrt{p})$ are equidistributed according to $\mathrm{ST}_A \subset \mathrm{USp}(2g)$

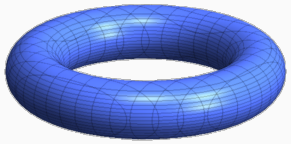
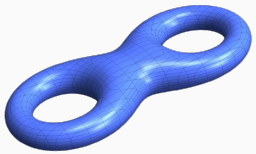
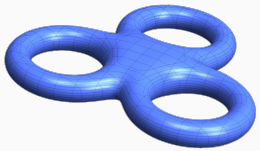
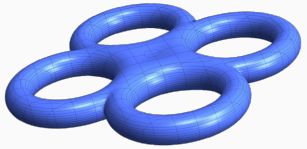
	$g=1$	$g=2$	$g=3$	$g=4$	$\cdots$
					$\cdots$
$\#\{\mathrm{ST}_A\}$	3	52	$\overset{?}{\sim}$ 400	$\overset{?}{\geq}$ 1000	$\cdots$

Possible distributions out there

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

Sato–Tate conjecture

$L_p(T/\sqrt{p})$ are equidistributed according to $\mathrm{ST}_A \subset \mathrm{USp}(2g)$

	$g=1$	$g=2$	$g=3$	$g=4$	$\cdots$
					$\cdots$
$\#\{\mathrm{ST}_A\}$	3	52	$\overset{?}{\sim}$ 400	$\overset{?}{\geq}$ 1000	$\cdots$

Question

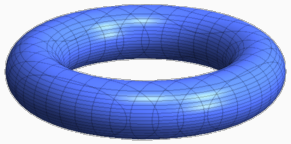
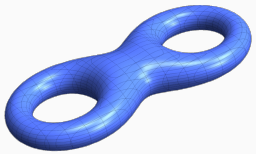
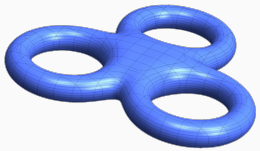
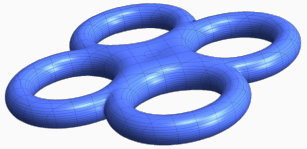
Given C can we compute ST_A?

Possible distributions out there

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

Sato–Tate conjecture

$L_p(T/\sqrt{p})$ are equidistributed according to $\mathrm{ST}_A \subset \mathrm{USp}(2g)$

	$g=1$	$g=2$	$g=3$	$g=4$	$\cdots$
					$\cdots$
$\#\{\mathrm{ST}_A\}$	3	52	$\overset{?}{\sim}$ 400	$\overset{?}{\geq}$ 1000	$\cdots$

Question

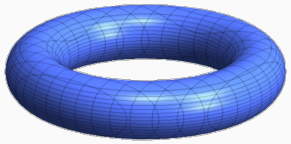
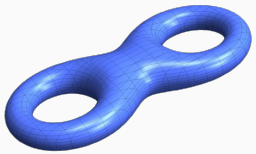
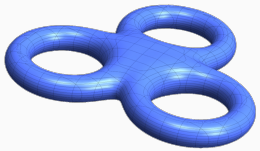
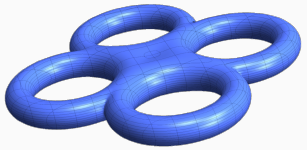
Given C can we compute ST_A or $\mathbf{End}\, A^{\mathrm{al}}$?

Possible distributions out there

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

Sato–Tate conjecture

$L_p(T/\sqrt{p})$ are equidistributed according to $\mathrm{ST}_A \subset \mathrm{USp}(2g)$

	$g=1$	$g=2$	$g=3$	$g=4$	$\cdots$
					$\cdots$
$\#\{\mathrm{ST}_A\}$	3	52	$\overset{?}{\sim}$ 400	$\overset{?}{\geq}$ 1000	$\cdots$

Question

Given C can we compute ST_A or $\mathbf{End}\, A^{\mathrm{al}}$?

Yes, we can compute $\mathbf{End}\, A^{\mathrm{al}}$!

Lower bounds for the endomorphism ring

- C be a nice curve over a number field
- $A := \mathrm{Jac}(C) \simeq_{\mathbb{C}} \mathbb{C}^g/\Lambda$
- $\mathrm{End}\, A^{\mathrm{al}} \simeq \mathrm{End}\, \mathbb{C}^g/\Lambda \simeq \mathrm{End}\, \Lambda$

Theorem (C–Mascot–Sijsling–Voight)

There exists a deterministic algorithm that, given input $\alpha \in \mathrm{M}_g(\mathbb{Q}^{\mathrm{al}})$, *returns*

$$\begin{cases} \texttt{true} & \alpha \in \mathrm{End}\, A^{\mathrm{al}} \text{ and } \alpha \text{ is nondegenerate}^1, \\ \texttt{false} & \alpha \notin \mathrm{End}\, A^{\mathrm{al}} \text{ or } \alpha \text{ is degenerate.} \end{cases}$$

[1] i.e., not in the locus of indeterminancy of the Mumford map

Lower bounds for the endomorphism ring

- C be a nice curve over a number field
- $A := \mathsf{Jac}(C) \simeq_{\mathbb{C}} \mathbb{C}^g/\Lambda$
- $\mathsf{End}\, A^{\mathsf{al}} \simeq \mathsf{End}\, \mathbb{C}^g/\Lambda \simeq \mathsf{End}\, \Lambda$

Theorem (C–Mascot–Sijsling–Voight)

There exists a deterministic algorithm that, given input $\alpha \in \mathrm{M}_g(\mathbb{Q}^{\mathsf{al}})$, returns

$$\begin{cases} \texttt{true} & \alpha \in \mathsf{End}\, A^{\mathsf{al}} \text{ and } \alpha \text{ is nondegenerate}^1, \\ \texttt{false} & \alpha \notin \mathsf{End}\, A^{\mathsf{al}} \text{ or } \alpha \text{ is degenerate.} \end{cases}$$

In practice, we first compute $\mathsf{End}\, \mathbb{C}^g/\Lambda$ numerically.

[1] i.e., not in the locus of indeterminancy of the Mumford map

Upper bounds for the endomorphism ring

We may factor $\mathbf{End}\, A^{\mathsf{al}}$ uniquely as

$$\mathbf{End}\, A^{\mathsf{al}} \simeq \prod_{i=1}^{t} \mathrm{M}_{n_i}(B_i),$$

where B_i are division algebras

Upper bounds for the endomorphism ring

We may factor $\mathbf{End}\, A^{\mathsf{al}}$ uniquely as

$$\mathbf{End}\, A^{\mathsf{al}} \simeq \prod_{i=1}^{t} \mathrm{M}_{n_i}(B_i),$$

where B_i are division algebras with center L_i.
Set $e_i^2 := \mathbf{dim}_{L_i} B_i$, then

$$\mathbf{rk}\, \mathbf{End}(A_K) = \sum_{i=1}^{t} e_i^2 n_i^2 [L_i : \mathbb{Q}].$$

Upper bounds for the endomorphism ring

We may factor $\mathsf{End}\, A^{\mathsf{al}}$ uniquely as

$$\mathsf{End}\, A^{\mathsf{al}} \simeq \prod_{i=1}^{t} \mathrm{M}_{n_i}(B_i),$$

where B_i are division algebras with center L_i.
Set $e_i^2 := \mathsf{dim}_{L_i} B_i$, then

$$\mathsf{rk}\, \mathsf{End}(A_K) = \sum_{i=1}^{t} e_i^2 n_i^2 [L_i : \mathbb{Q}].$$

Theorem (C–Mascot–Sijsling–Voight)

We can effectively compute

$$t, \qquad \{e_i n_i\}_{i=1,\dots,t}, \quad \text{and} \quad \{L_i\}_{i=1,\dots,t},$$

if the Mumford–Tate conjecture holds for A.

Upper bounds for the endomorphism ring

We may factor $\mathsf{End}\, A^{\mathsf{al}}$ uniquely as

$$\mathsf{End}\, A^{\mathsf{al}} \simeq \prod_{i=1}^{t} \mathrm{M}_{n_i}(B_i),$$

where B_i are division algebras with center L_i.
Set $e_i^2 := \mathsf{dim}_{L_i} B_i$, then

$$\mathsf{rk}\, \mathsf{End}(A_K) = \sum_{i=1}^{t} e_i^2 n_i^2 [L_i : \mathbb{Q}].$$

Theorem (C–Mascot–Sijsling–Voight)

We can effectively compute

$$t, \qquad \{e_i n_i\}_{i=1,\dots,t}, \quad \text{and} \quad \{L_i\}_{i=1,\dots,t},$$

if the Mumford–Tate conjecture holds for A.

This is done by just counting points.

Upshot

We can efficiently compute $\mathbf{End}\, A^{\mathrm{al}}$ as a Galois module.

Upshot

We can efficiently compute $\mathbf{End}\, A^{\mathsf{al}}$ as a Galois module.

Remark

For $g \leq 3$ this is sufficient to determine ST_A.

	$g=1$	$g=2$	$g=3$	$g=4$	$\cdots$
$\#\{\mathrm{ST}_A\}$	3	52	$\overset{?}{\sim} 400$	$\overset{?}{\geq} 1000$	$\cdots$

Upshot

We can efficiently compute $\mathsf{End}\, A^{\mathsf{al}}$ as a Galois module.

Remark

For $g \leq 3$ this is sufficient to determine ST_A.

	$g=1$	$g=2$	$g=3$	$g=4$	$\cdots$
$\#\{\mathrm{ST}_A\}$	3	52	$\overset{?}{\sim} 400$	$\overset{?}{\geq} 1000$	$\cdots$

Publicly available for you to try out

`github.com/edgarcosta/endomorphisms/`

Already used on more than 250000 curves, coming soon to

`LMFDB.org`

K3 surfaces

These provide another natural 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

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

K3 surfaces

These provide another natural 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

These provide another natural 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 $a_p := \operatorname{Tr} \mathrm{Frob}_p$ we study

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

K3 Surfaces

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

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

This is analogous to studying:

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

K3 Surfaces

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

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

This is analogous to studying:

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

As we have

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

K3 Surfaces

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

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

This is analogous to studying:

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

As we have

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

In the later case,

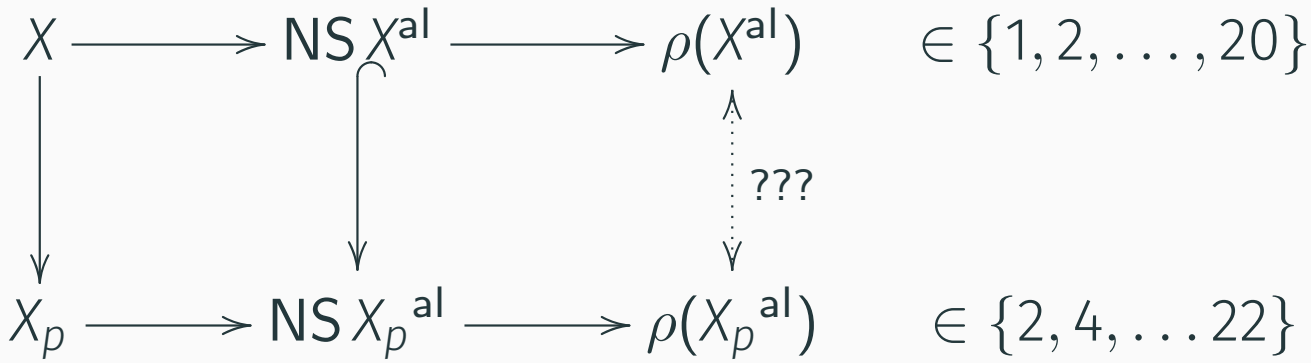
$$\{p : a_p = 0\} = \{p : p \text{ is ramified or inert in } \mathbb{Q}(\sqrt{-d})\}$$

Néron–Severi group

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

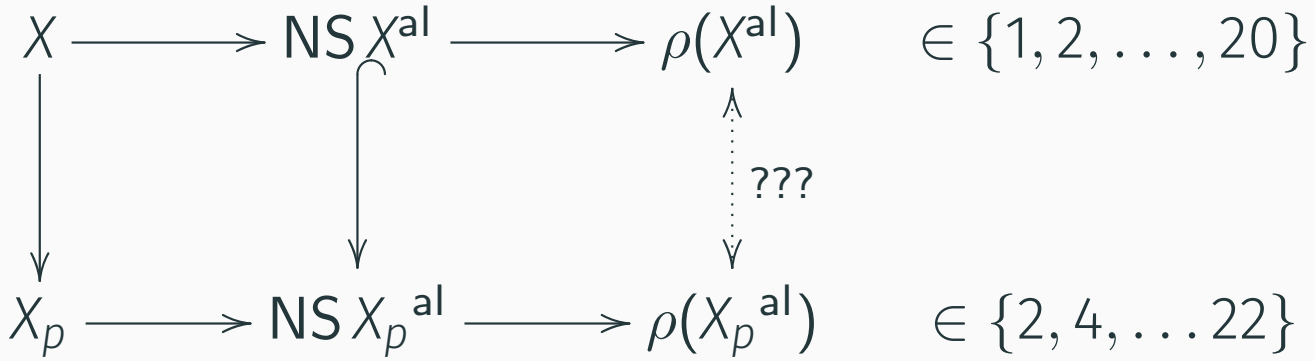
Néron–Severi group

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



Néron–Severi group

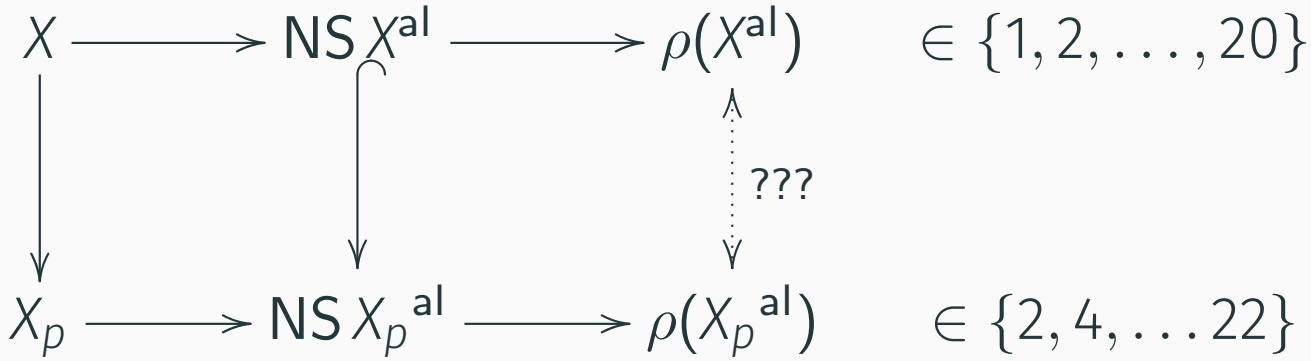
- $\mathsf{NS}\,\bullet$ = Néron–Severi group of $\bullet \simeq \{\text{curves on } \bullet\}/\sim$
- $\rho(\bullet) = \mathsf{rk}\,\mathsf{NS}\,\bullet$
- $X_p := X \bmod p$



Theorem (Charles)

For infinitely many p we have $\rho({X_p}^{\mathsf{al}}) = \mathsf{min}_q\, \rho({X_q}^{\mathsf{al}})$.

The Problem



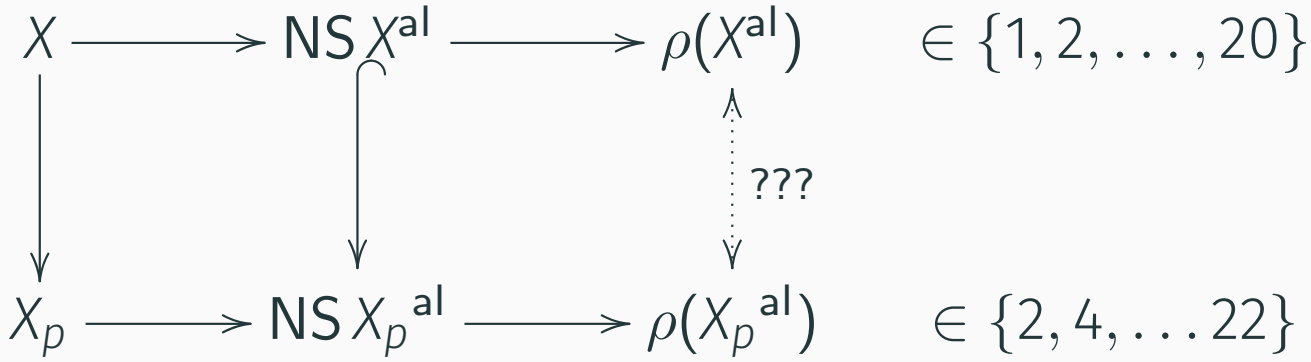
Theorem (Charles)

For infinitely many p we have $\rho({X_p}^{\mathsf{al}}) = \mathsf{min}_q\, \rho({X_q}^{\mathsf{al}})$.

What can we say about the following:

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

The Problem



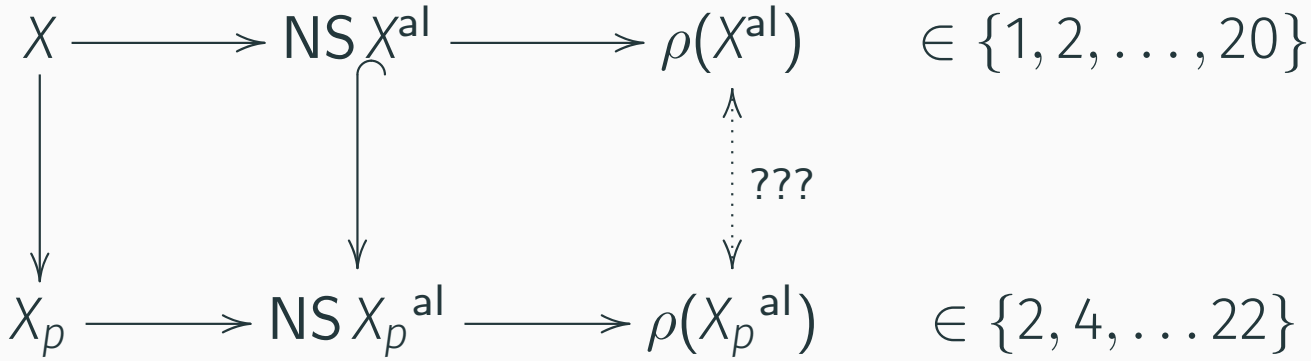
Theorem (Charles)

For infinitely many p we have $\rho({X_p}^{\mathsf{al}}) = \mathsf{min}_q\, \rho({X_q}^{\mathsf{al}})$.

What can we say about the following:

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

The Problem



Theorem (Charles)

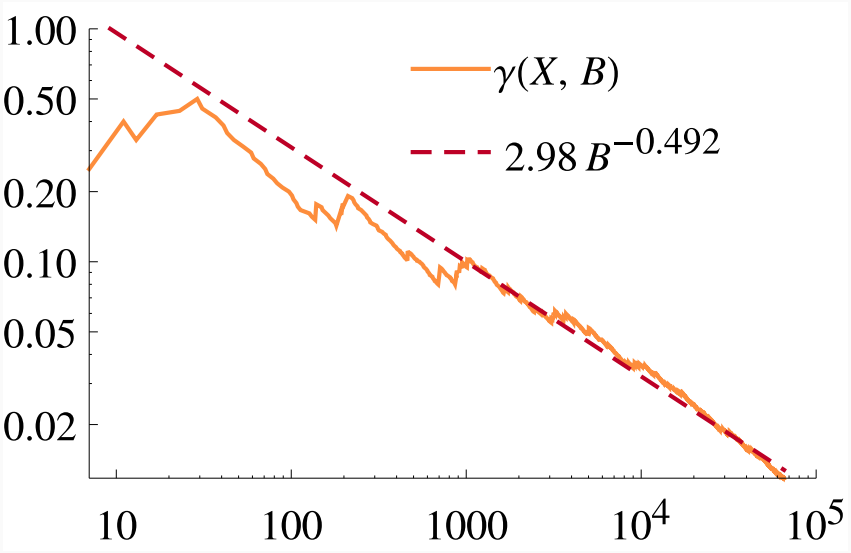
For infinitely many p we have $\rho({X_p}^{\mathsf{al}}) = \mathsf{min}_q\, \rho({X_q}^{\mathsf{al}})$.

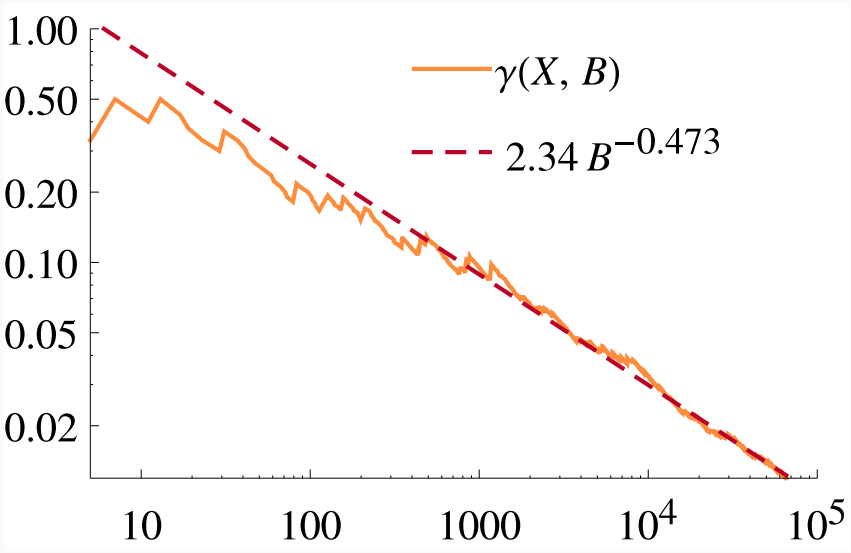
What can we say about the following:

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

Let's do some numerical experiments!

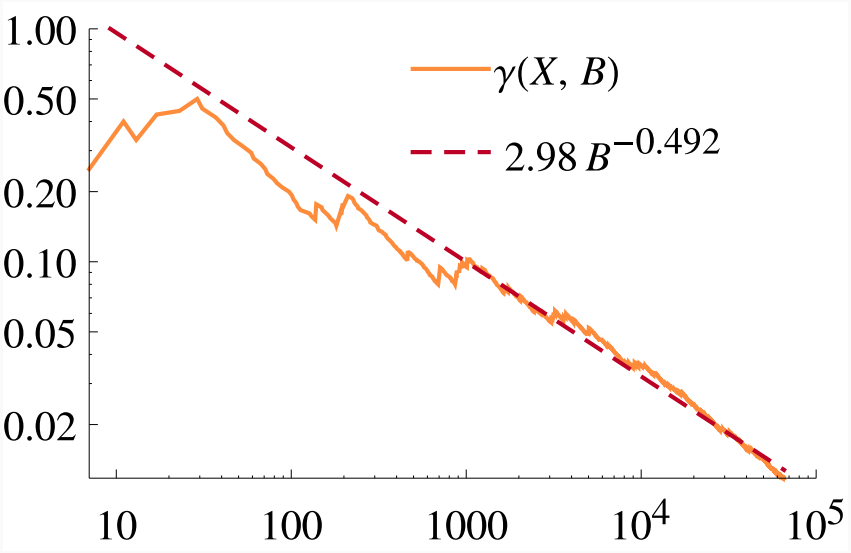
Two generic K3 surfaces, $\rho(X^{\mathrm{al}}) = 1$

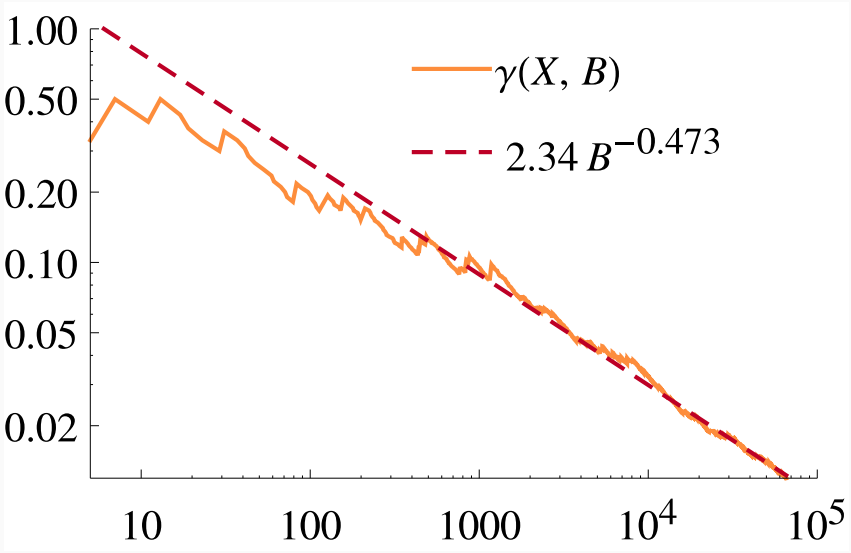




$$\gamma(X, B) \overset{?}{\sim} \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

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

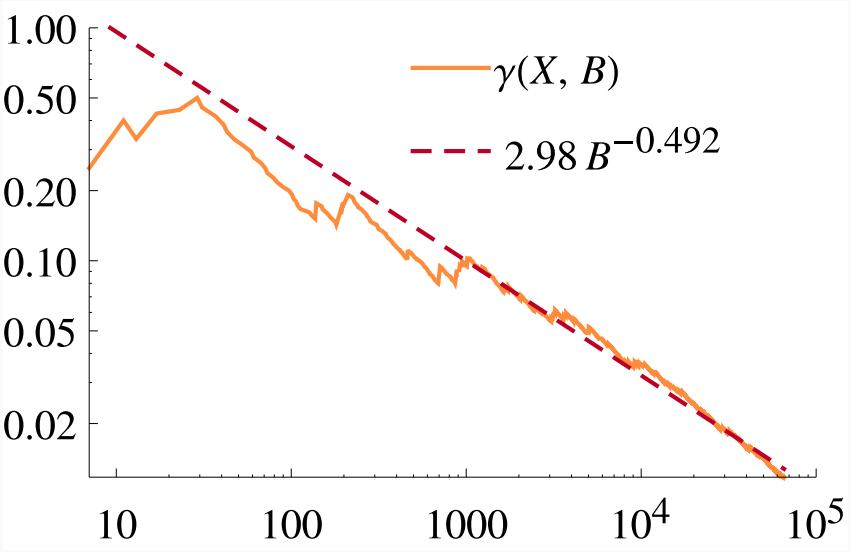


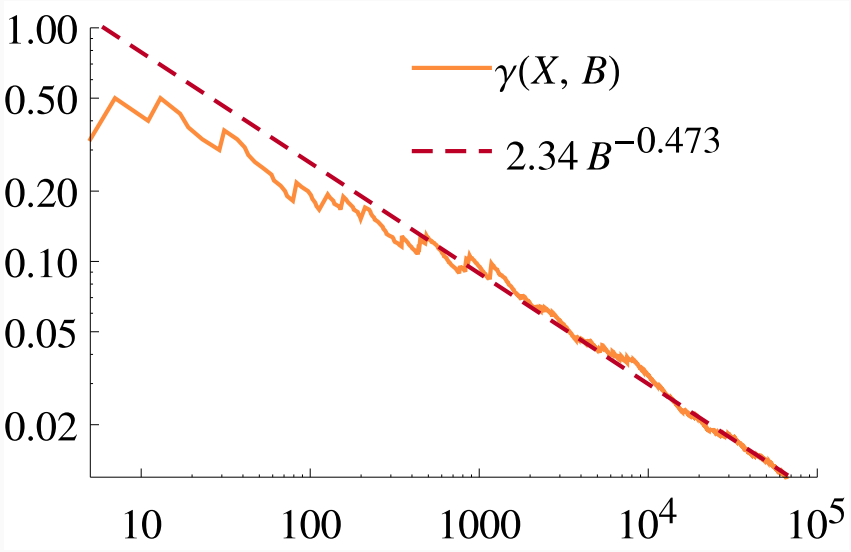


$$\gamma(X, B) \overset{?}{\sim} \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

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

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





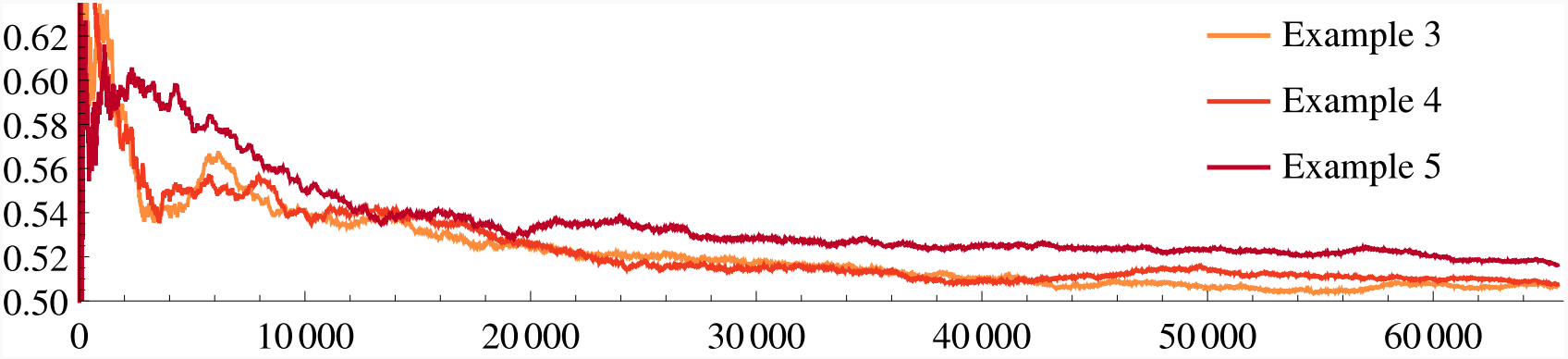
$$\gamma(X, B) \overset{?}{\sim} \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

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

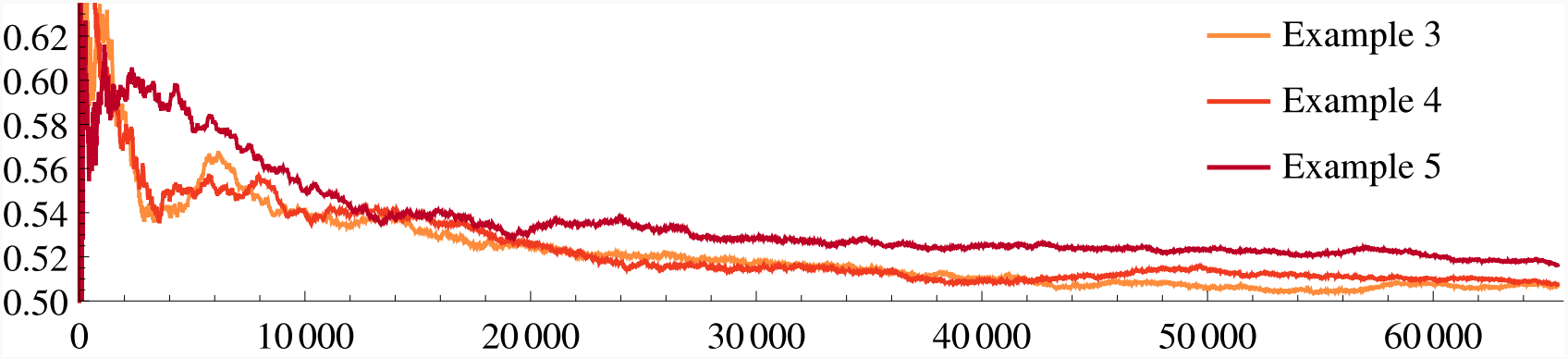
$\sim$ 1 CPU year per example

`github.com/edgarcosta/controlled-reduction/`

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

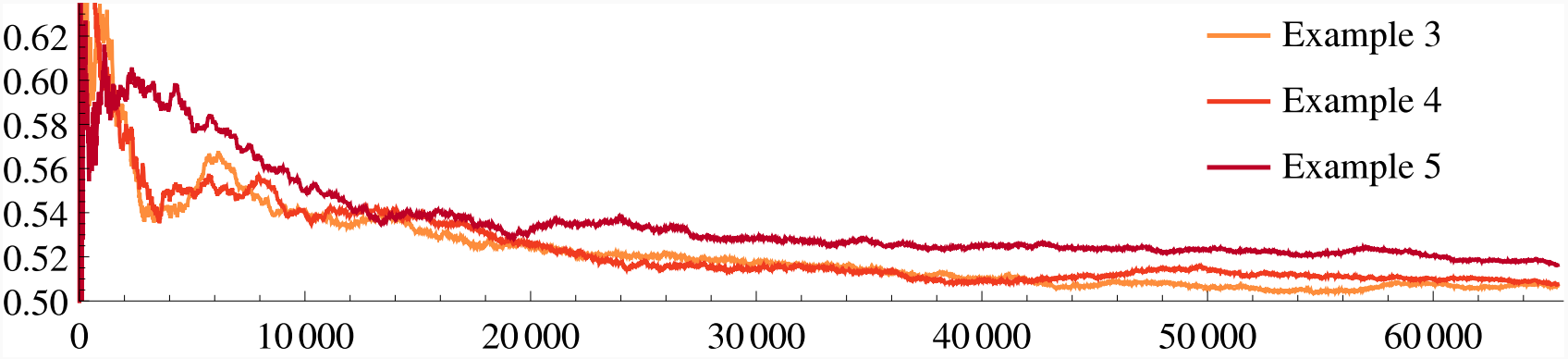


Three K3 surfaces with $\rho(X^{\mathrm{al}}) = 2$



Do you see a trend?

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



Do you see a 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.*

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.*

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.*

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.*

$d_3 = -1 \cdot 5 \cdot 151 \cdot 2249081735741437104 1 \cdot 3873084974301493372336663$

$d_4 = 53 \cdot 2624174618795407 \cdot 5128545618469648171394942020727783 41 \cdot$

$d_5 = -1 \cdot 47 \cdot 3109 \cdot 4969 \cdot 14857095849982608071 \cdot 44541027766092834$

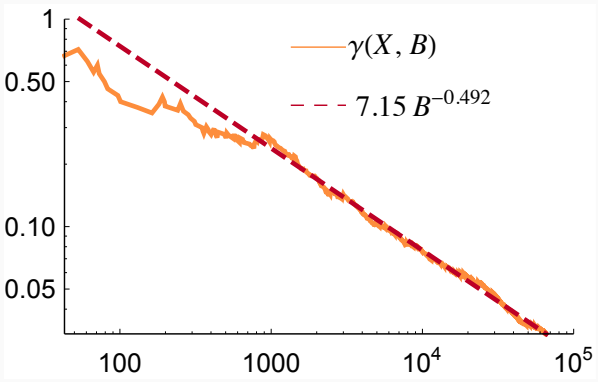
Experimental data for $\rho(X^{\mathrm{al}}) = 2$ (again)

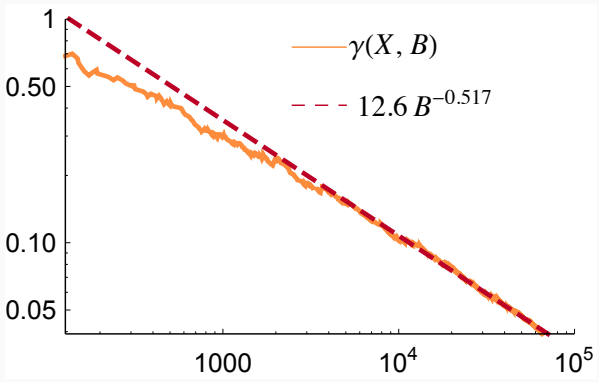
What if we ignore $\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\} \subset \Pi_{\mathrm{jump}}(X)$?

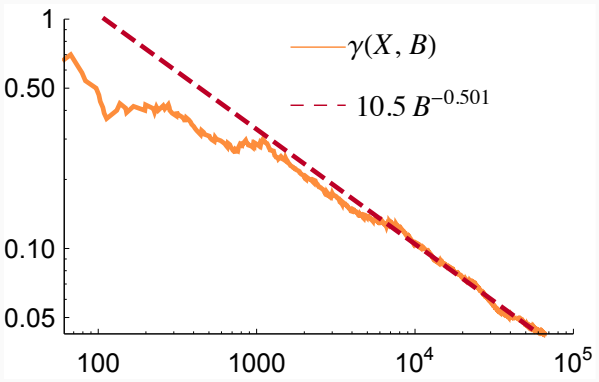
Experimental data for $\rho(X^{\mathrm{al}}) = 2$ (again)

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

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



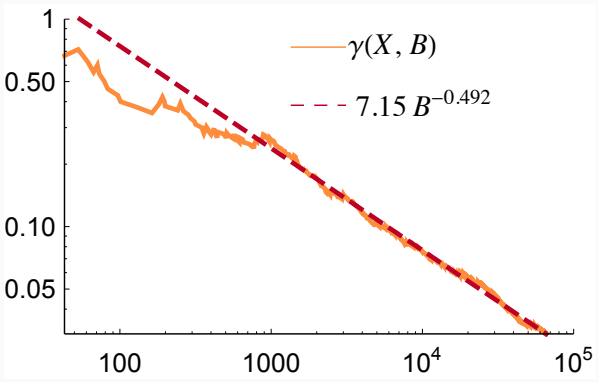


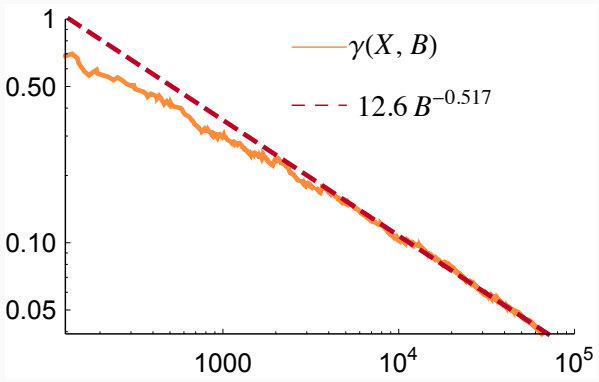


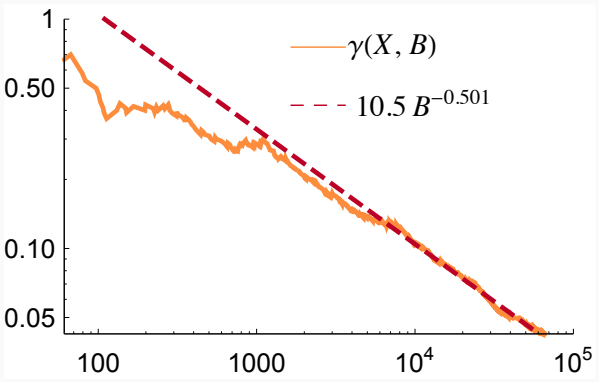
Experimental data for $\rho(X^{\mathrm{al}}) = 2$ (again)

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

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







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