Distributions in arithmetic geometry

Edgar Costa (Dartmouth College)

June 21st, 2018
University of Washington

Presented at Communicating Mathematics Effectively

Slides available at `edgarcosta.org` under Research

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

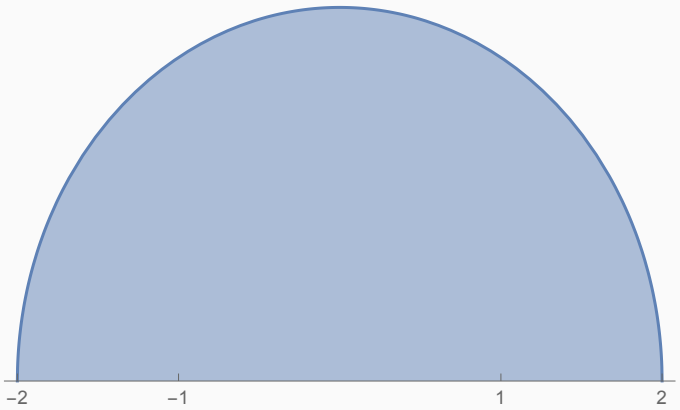
$$\lambda_p := \frac{p + 1 - \#E_p}{\sqrt{p}} \in [-2, 2]$$

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!



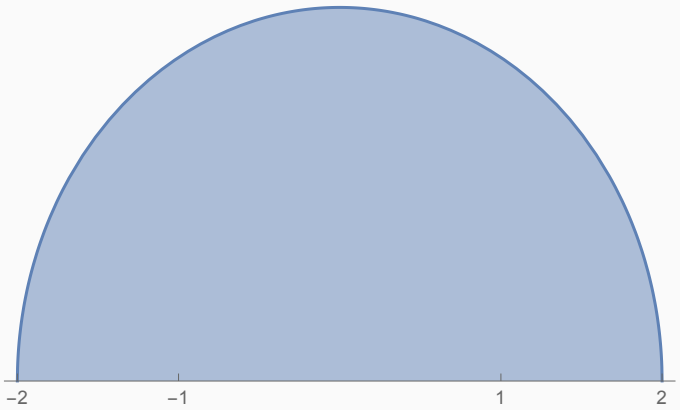
Two types of elliptic curves

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

There are two limiting distributions for λ_p!

non-CM

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



CM

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

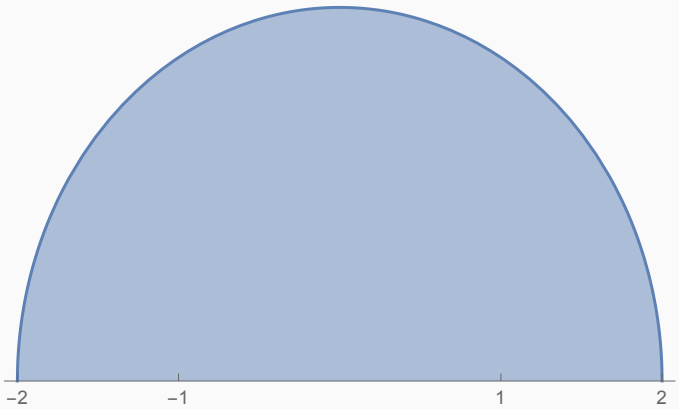
Two types of elliptic curves

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

There are two limiting distributions for λ_p!

non-CM

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



$\mathrm{Prob}(\lambda_p = 0) \sim 1/\sqrt{p}$

CM

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

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

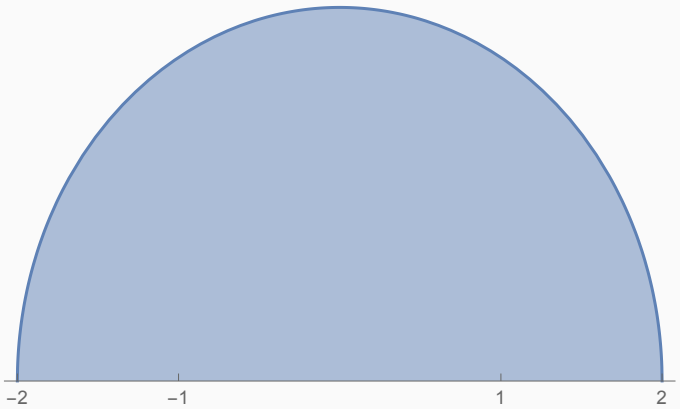
Two types of elliptic curves

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

There are two limiting distributions for λ_p!

non-CM

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



$\mathrm{Prob}(\lambda_p = 0) \sim 1/\sqrt{p}$

CM

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

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

$$\lambda_p = 0 \iff \mathrm{rk}\, \mathrm{End}\, {E_p}^{\mathrm{al}} > 2$$

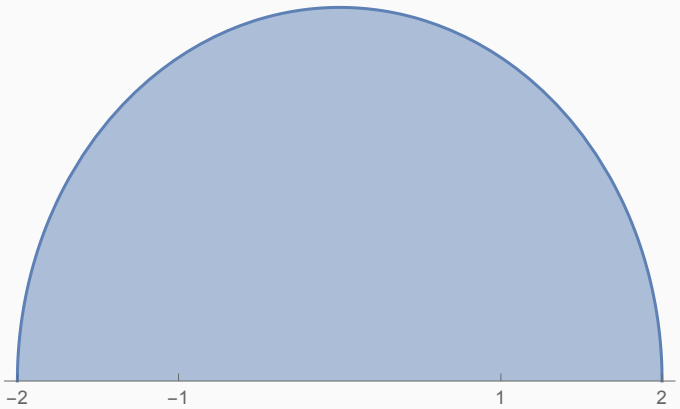
Two types of elliptic curves

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

There are two limiting distributions for λ_p!

non-CM

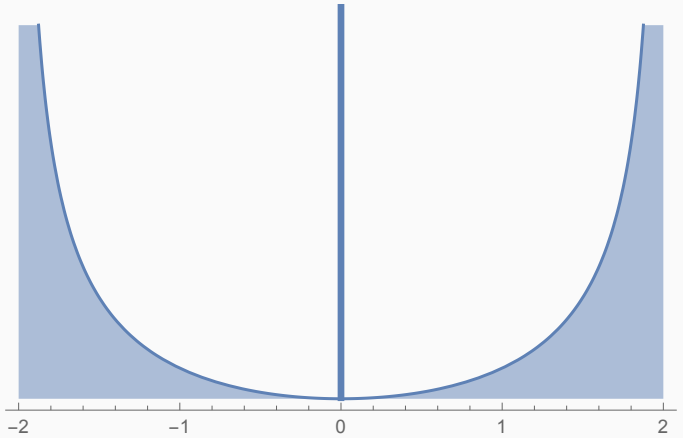
$\mathrm{End}\, E^{\mathrm{al}} = \mathbb{Z}$



$\mathrm{Prob}(\lambda_p = 0) \sim 1/\sqrt{p}$

CM

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



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

$$\lambda_p = 0 \iff \mathrm{rk}\,\mathrm{End}\, {E_p}^{\mathrm{al}} > 2 = \min_q \mathrm{rk}\,\mathrm{End}\, E_q^{\mathrm{al}}$$

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves

For example, **smooth quartic surfaces** in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad f \in \mathbb{Z}[x], \ \deg f = 4$$

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves

For example, **smooth quartic surfaces** in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad f \in \mathbb{Z}[x],\ \deg f = 4$$

In this case, instead of studying $\#X_p$, we study

$$p \longmapsto \operatorname{rk} \mathrm{NS}\, X_p{}^{\mathrm{al}}.$$

K3 surfaces

K3 surfaces are a possible generalization of elliptic curves

For example, **smooth quartic surfaces** in $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad f \in \mathbb{Z}[x], \ \deg f = 4$$

In this case, instead of studying $\#X_p$, we study

$$p \longmapsto \operatorname{rk} \mathrm{NS}\, {X_p}^{\mathrm{al}}.$$

This is analogous to studying $\operatorname{rk} \mathrm{End}\, {E_p}^{\mathrm{al}} = \operatorname{rk} \mathrm{NS}({E_p}^{\mathrm{al}} \times {E_p}^{\mathrm{al}})$

Néron–Severi group

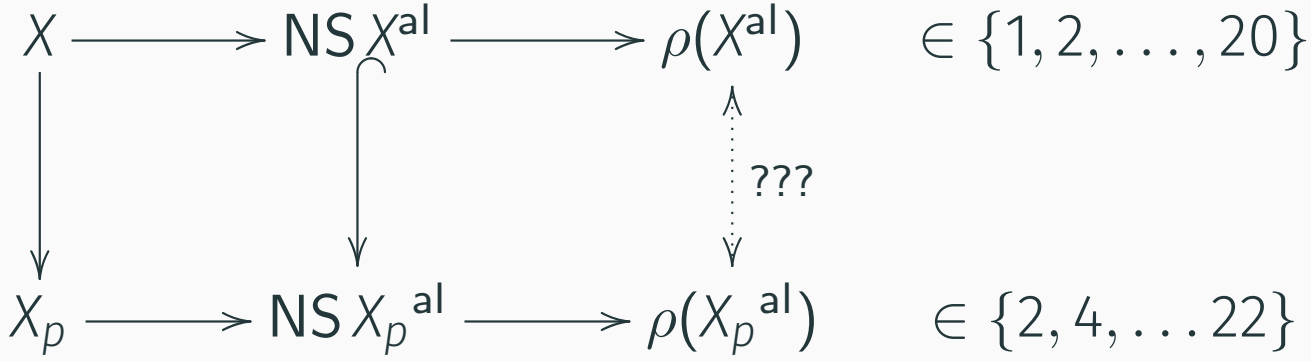
$\mathsf{NS}\,\bullet = \text{Néron–Severi group of } \bullet \simeq \{\text{curves on } \bullet\}/\sim$

$\rho(\bullet) = \operatorname{rk} \mathsf{NS}\,\bullet$

Néron–Severi group

$\mathsf{NS}\,\bullet = \text{Néron–Severi group of } \bullet \simeq \{\text{curves on } \bullet\}/\sim$

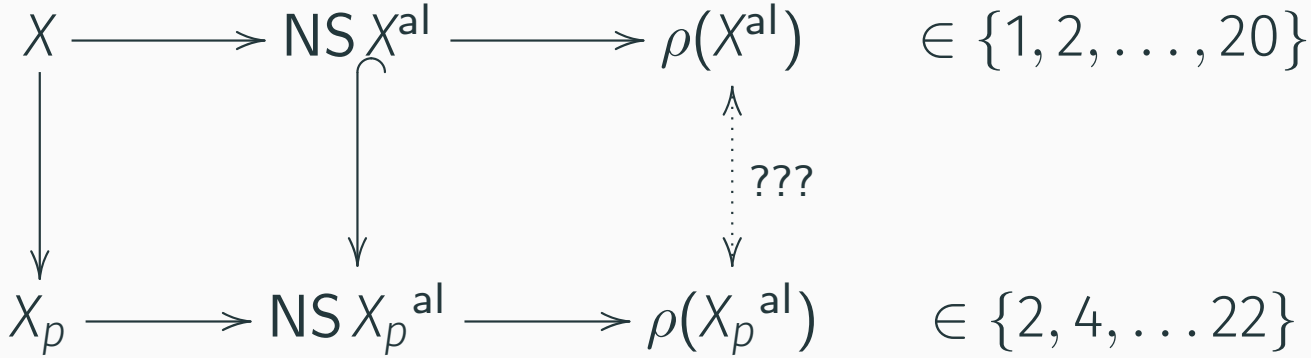
$\rho(\bullet) = \operatorname{rk} \mathsf{NS}\,\bullet$



Néron–Severi group

$\mathsf{NS}\,\bullet = $ Néron–Severi group of $\bullet \simeq \{\text{curves on } \bullet\}/\sim$

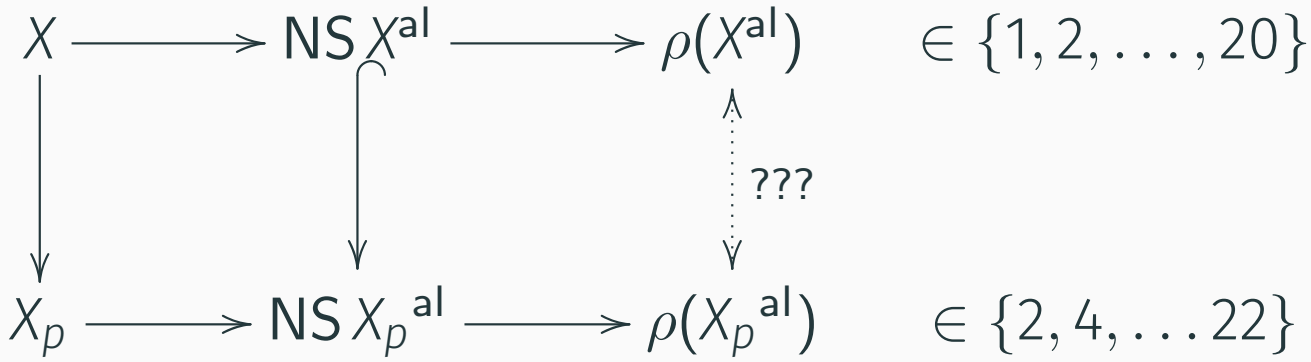
$\rho(\bullet) = \mathrm{rk}\,\mathsf{NS}\,\bullet$



Theorem (Charles)

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

The Problem



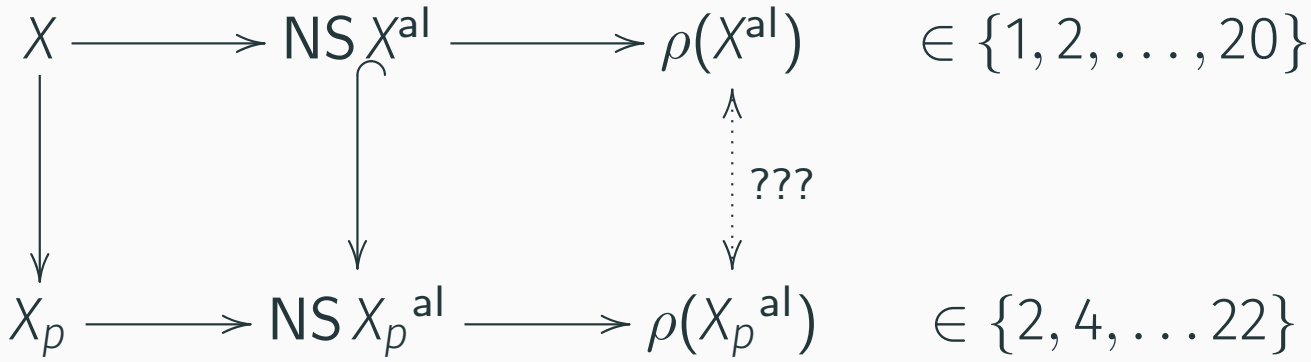
Theorem (Charles)

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



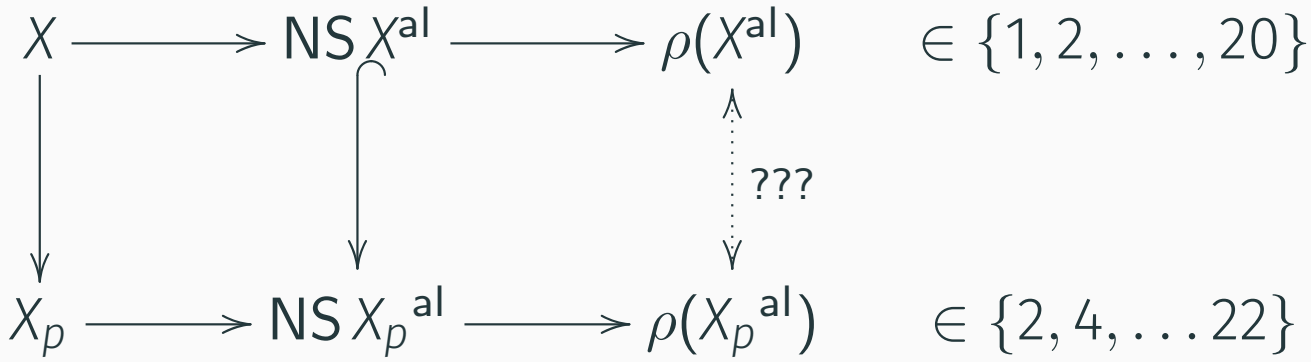
Theorem (Charles)

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)

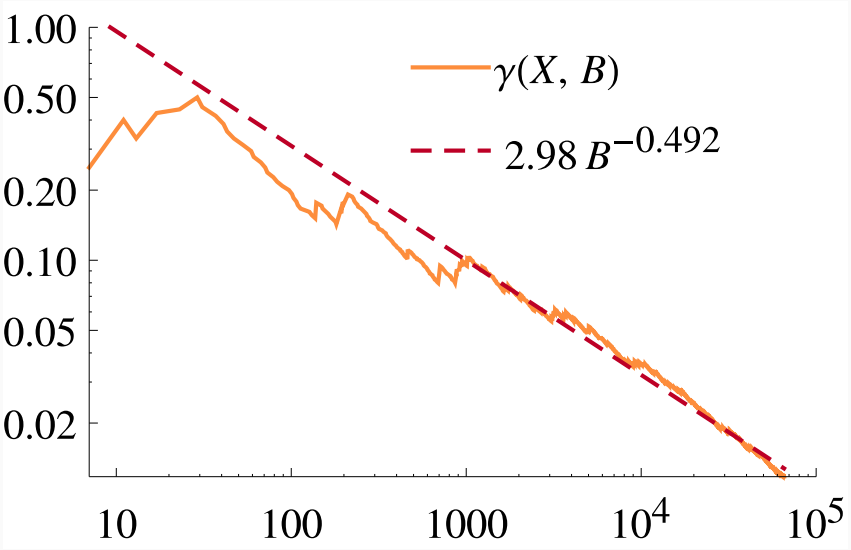
For infinitely many p we have $\rho({X_p}^{\mathsf{al}}) = \mathsf{min}_q\, \rho({X_q}^{\mathsf{al}})$.

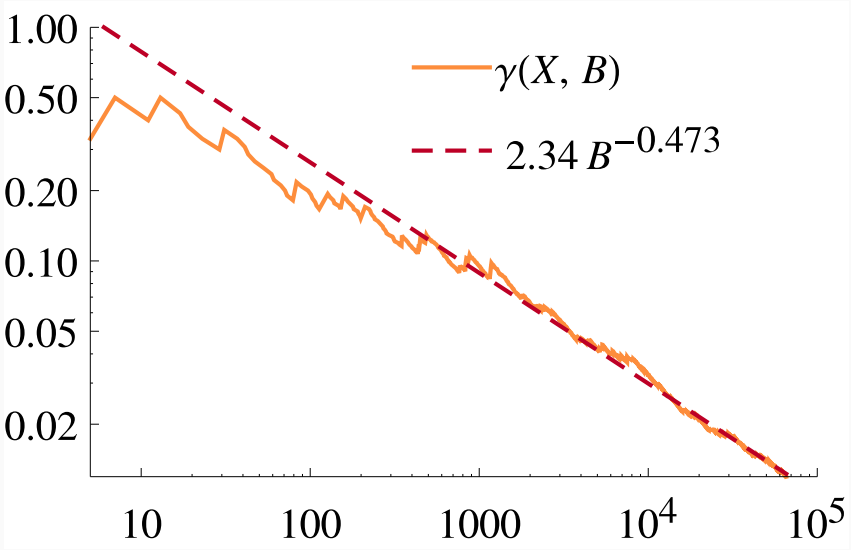
What can we say about the following:

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

Let's do some numerical experiments!

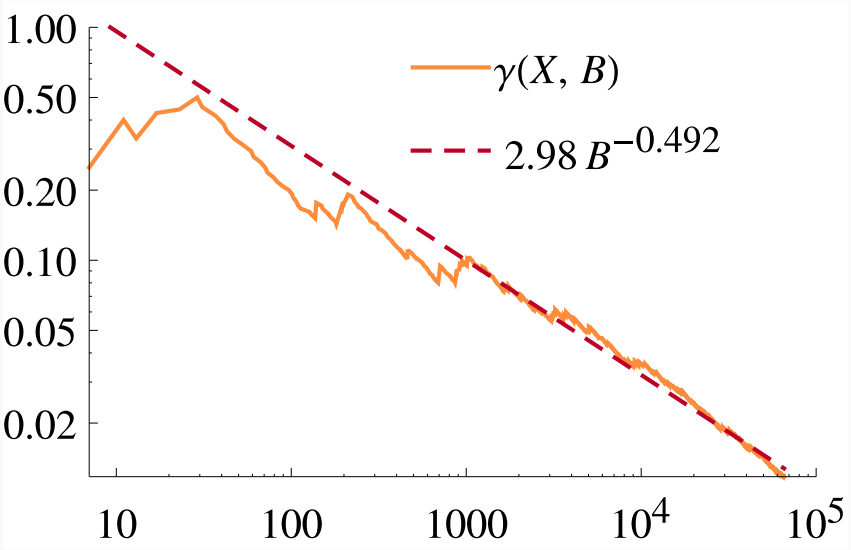
Generic K3 surfaces, $\rho(X^{\mathrm{al}}) = 1$

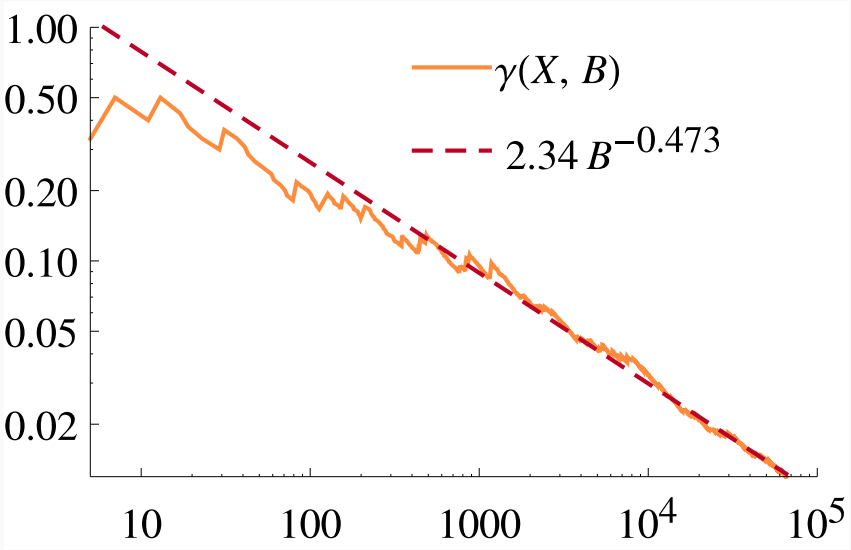




$$\gamma(X, B) \sim \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

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

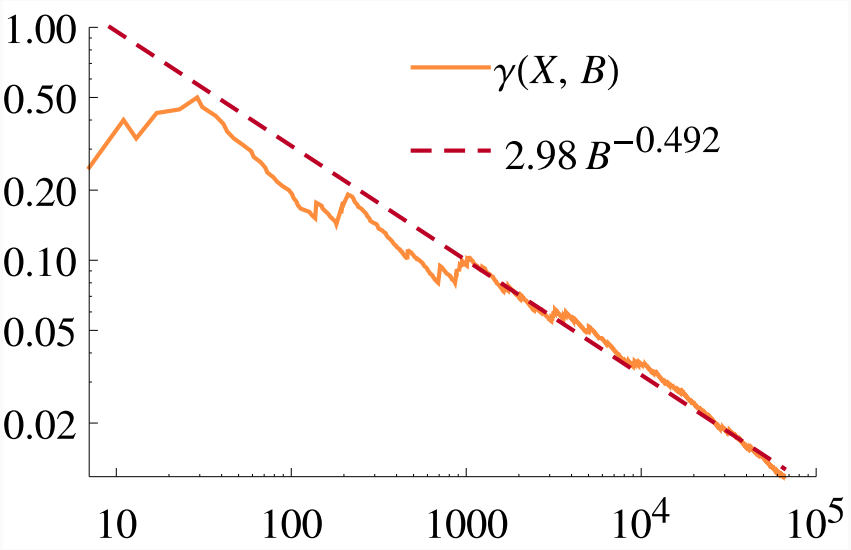


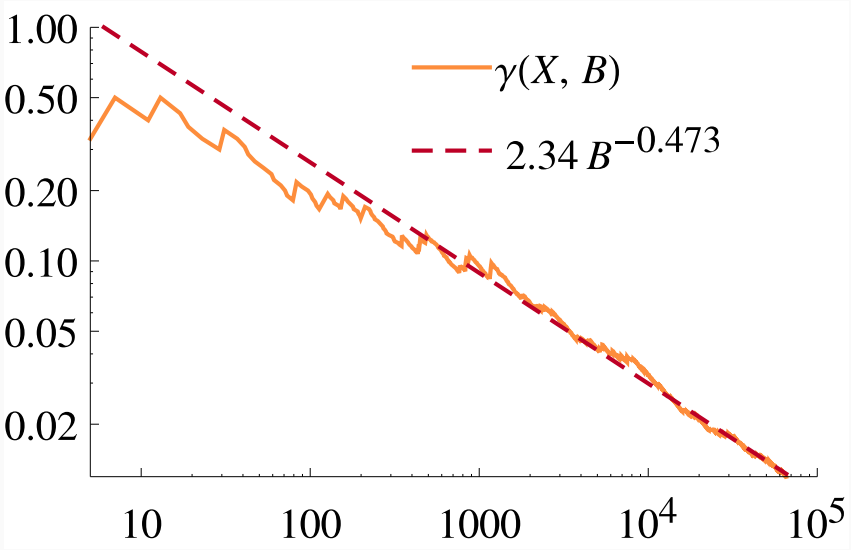


$$\gamma(X, B) \sim \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

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

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



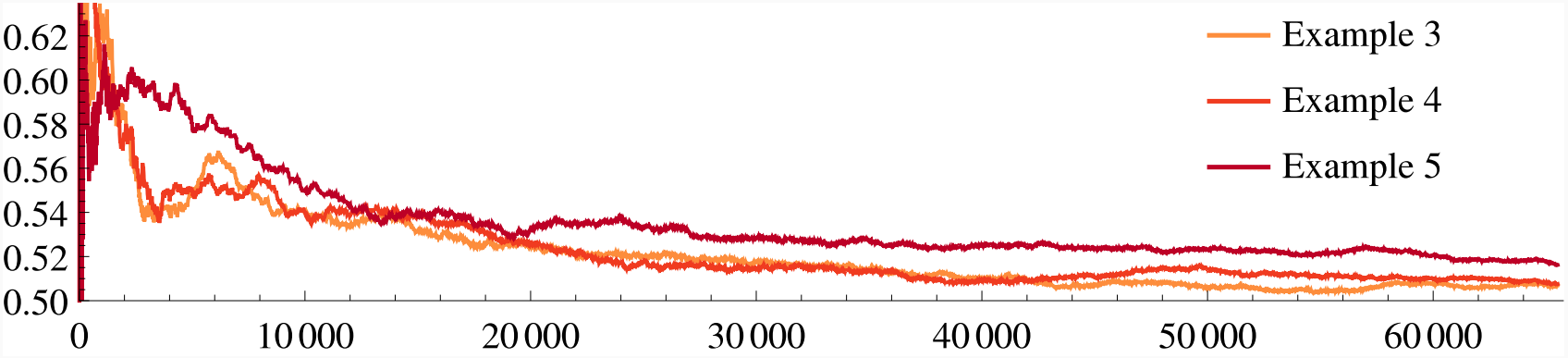


$$\gamma(X, B) \sim \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

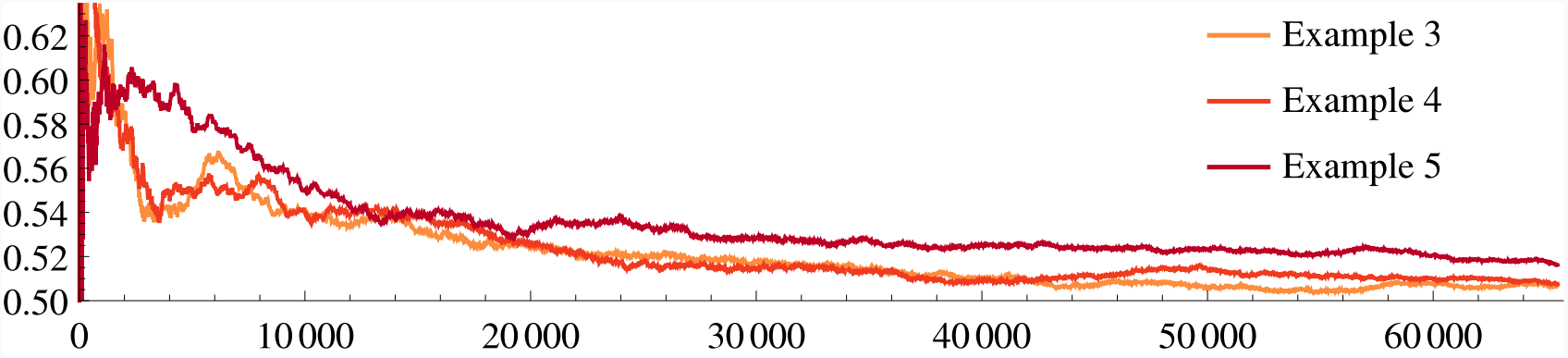
$$\Longrightarrow \ \mathrm{Prob}(p \in \Pi_{\mathrm{jump}}(X)) \sim 1/\sqrt{p}$$

Why?

Data for $\rho(X^{\mathrm{al}}) = 2$

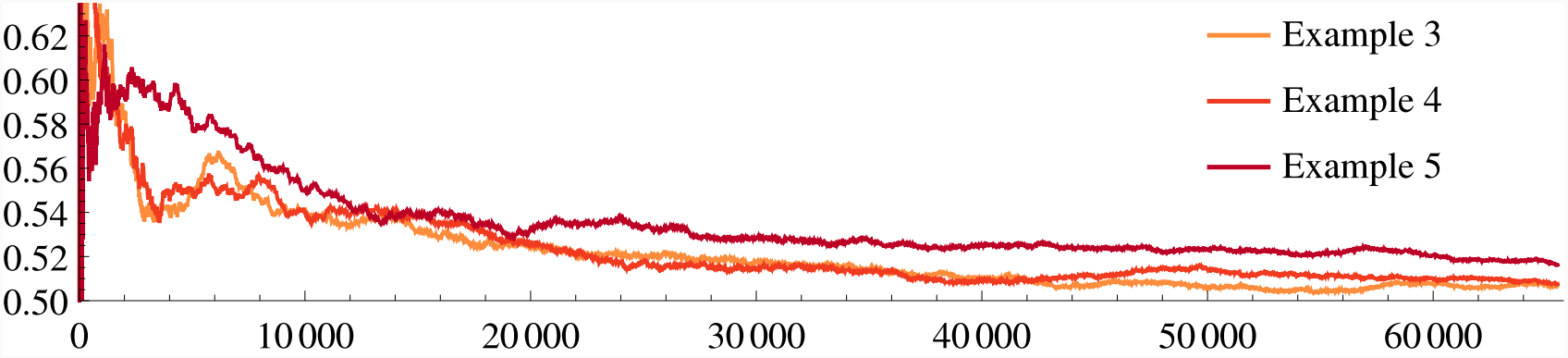


Data for $\rho(X^{\mathrm{al}}) = 2$



No obvious trend...

Data for $\rho(X^{\mathrm{al}}) = 2$



No obvious trend...

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

Numerical experiments $\rightsquigarrow$ Theoretical Results

In most cases we can explain the 1/2!

Numerical experiments $\rightsquigarrow$ Theoretical Results

In most cases 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.*

Numerical experiments $\rightsquigarrow$ Theoretical Results

In most cases 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.*

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

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

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

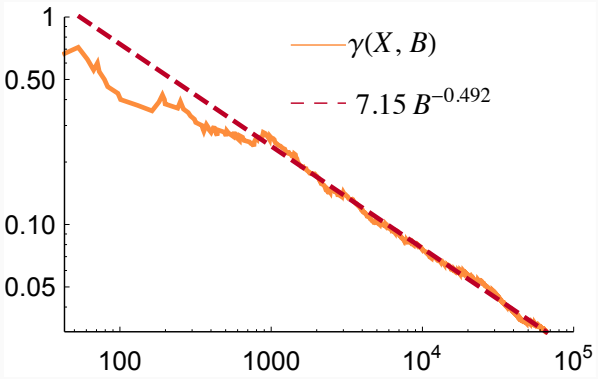
What if we ignore $\{p > 2 : p \text{ inert in } \mathbb{Q}(\sqrt{d_X})\} \subset \Pi_{\mathrm{jump}}(X)$?

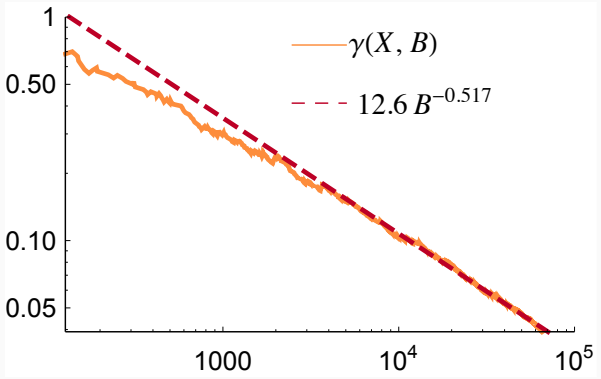
$$\gamma\left(X_{\mathbb{Q}(\sqrt{d_X})}, B\right) \sim \frac{c}{\sqrt{B}}, \quad B \to \infty$$

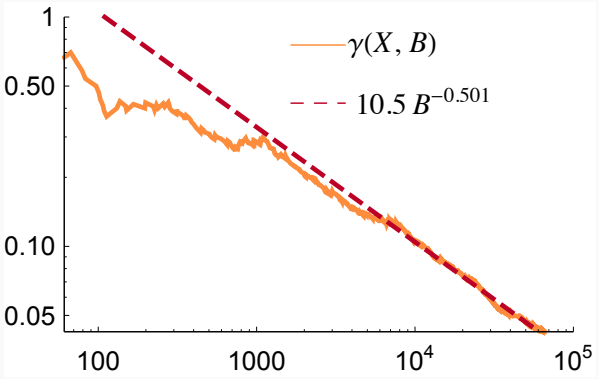
Experimental data for $\rho(X^{\mathrm{al}}) = 2$ (again)

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

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





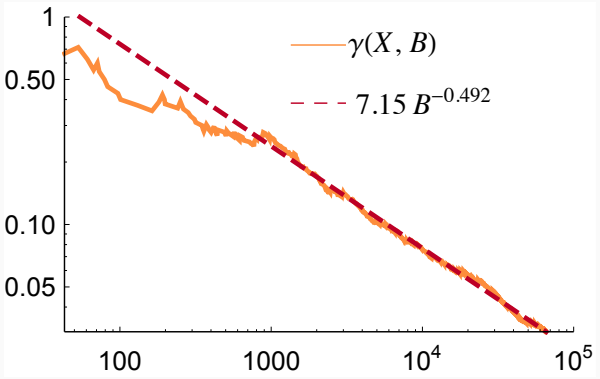


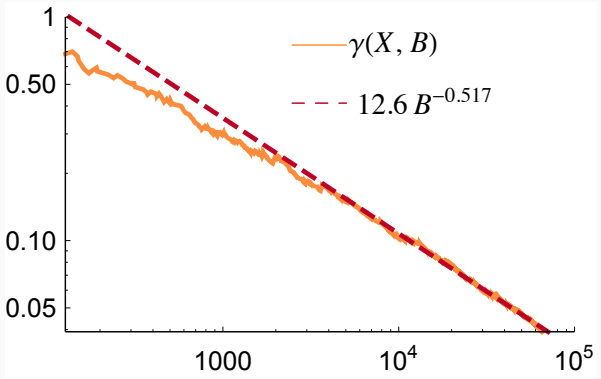
$$\mathrm{Prob}(p \in \Pi_{\mathrm{jump}}(X)) = \begin{cases} 1 & \text{if } d_X \text{ is not a square modulo } p \\ \sim \frac{1}{\sqrt{p}} & \textit{otherwise} \end{cases}$$

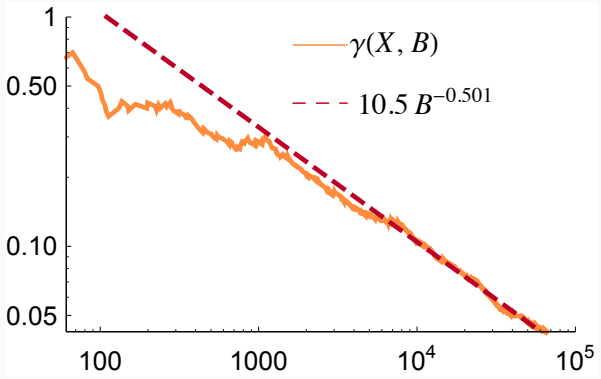
Experimental data for $\rho(X^{\mathrm{al}}) = 2$ (again)

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

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







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

Why?!?