Equidistributions in arithmetic geometry

Edgar Costa

Dartmouth College

14th January 2016
Dartmouth College

Motivation: Randomness Principle

Rigidity/Randomness Dichotomy [Sarnak]

Given an arithmetic problem, either

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

Motivation: Randomness Principle

Rigidity/Randomness Dichotomy [Sarnak]

Given an arithmetic problem, either

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

- Understanding and providing the probability law $\rightsquigarrow$ deep understanding of the phenomenon
- Real world applications

Motivation: Problem

p a prime number
X an "integral" object, e.g.:

- a integer
- a polynomial with integer coefficients
- a curve or a surface defined by a polynomial equation with integer coefficients
- ...

Motivation: Problem

p a prime number

X an “integral” object, e.g.:

- a integer
- a polynomial with integer coefficients
- a curve or a surface defined by a polynomial equation with integer coefficients
- ...

We can consider X modulo p.

Motivation: Problem

p a prime number
X an "integral" object, e.g.:

- a integer
- a polynomial with integer coefficients
- a curve or a surface defined by a polynomial equation with integer coefficients
- ...

We can consider X modulo p.

Question

Given X mod p

- What can we say about X?

Motivation: Problem

p a prime number
X an "integral" object, e.g.:

- a integer
- a polynomial with integer coefficients
- a curve or a surface defined by a polynomial equation with integer coefficients
- ...

We can consider X modulo p.

Question

Given X mod p

- What can we say about X?
- What if we consider infinitely many primes?

Motivation: Problem

p a prime number
X an "integral" object, e.g.:

- a integer
- a polynomial with integer coefficients
- a curve or a surface defined by a polynomial equation with integer coefficients
- ...

We can consider X modulo p.

Question

Given X mod p

- What can we say about X?
- What if we consider infinitely many primes?
- How does it behave as $p \to \infty$?

Overview

1. Polynomials in one variable
2. Elliptic curves
3. Quartic surfaces

Counting roots of polynomials

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

p a prime number

Consider:

$$\begin{aligned} N_f(p) &:= \#\left\{x \in \{0, \dots, p-1\} \;:\; f(x) \equiv 0 \bmod p\right\} \\ &= \#\left\{x \in \mathbb{F}_p \;:\; f(x) = 0\right\} \end{aligned}$$

$$N_f(p) \in \{0, 1, \dots, d\}$$

Question

How often does each value occur?

Example: quadratic polynomials

$f(x) = ax^2 + bx + c$, $\Delta = b^2 - 4ac$, the discriminant of f.

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

Example: quadratic polynomials

$f(x) = ax^2 + bx + c$, $\Delta = b^2 - 4ac$, the discriminant of f.

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

Half of the numbers modulo p are squares.
Hence, if Δ isn't a square, then $\mathrm{Prob}(\Delta \text{ is a square modulo } p) = 1/2$

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

Example: quadratic polynomials

$f(x) = ax^2 + bx + c$, $\Delta = b^2 - 4ac$, the discriminant of f.

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

Half of the numbers modulo p are squares.
Hence, if Δ isn't a square, then Prob(Δ is a square modulo p) $= 1/2$

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

$$\text{For example, if } \Delta = 5 \text{ and } p > 2, \text{ then } N_f(p) = \begin{cases} 0 & \text{if } p \equiv 2, 3 \bmod 5 \\ 1 & \text{if } p = 5 \\ 2 & \text{if } p \equiv 1, 4 \bmod 5 \end{cases}$$

Example: cubic polynomials

In general one cannot find explicit formulas for $N_f(p)$, but we can still determine their average distribution!

Example: cubic polynomials

In general one cannot find explicit formulas for $N_f(p)$, but we can still determine their average distribution!

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

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

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

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

The Chebotarëv density theorem

$f(x) = (x - \alpha_1)\dots(x - \alpha_d)$, $\alpha_i \in \mathbb{C}$
$G := \mathrm{Aut}(\mathbb{Q}(\alpha_1, \dots, \alpha_d)/\mathbb{Q}) = \mathrm{Gal}(f/\mathbb{Q})$
$G \subset S_d$, as it acts on the roots $\alpha_1, \dots, \alpha_d$ by permutations.

The Chebotarëv density theorem

$f(x) = (x - \alpha_1) \dots (x - \alpha_d)$, $\alpha_i \in \mathbb{C}$
$G := \mathrm{Aut}(\mathbb{Q}(\alpha_1, \dots, \alpha_d)/\mathbb{Q}) = \mathrm{Gal}(f/\mathbb{Q})$
$G \subset S_d$, as it acts on the roots $\alpha_1, \dots, \alpha_d$ by permutations.

Theorem (Chebotarëv, early 1920s)

For $i = 0, \dots, d$, we have

$$\mathrm{Prob}(N_f(p) = i) = \mathrm{Prob}(g \in G : g \textit{ fixes } i \textit{ roots}),$$

where

$$\mathrm{Prob}(N_f(p) = i) := \lim_{N \to \infty} \frac{\#\{p \textit{ prime}, p \leq N, N_f(p) = i\}}{\#\{p \textit{ prime}, p \leq N\}}.$$

Example: Cubic polynomials, again

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

$$\operatorname{Prob}\left(N_f(p) = x\right) = \begin{cases} 1/3 & \text{if } x = 0 \\ 1/2 & \text{if } x = 1 \\ 1/6 & \text{if } x = 3 \end{cases} \text{ and } G = S_3.$$

$$S_3 = \left\{ \begin{array}{c} \text{id}, \\ (1 \leftrightarrow 2), (1 \leftrightarrow 3), (2 \leftrightarrow 3), \\ (1 \to 2 \to 3 \to 1), (1 \to 3 \to 2 \to 1) \end{array} \right\}$$

Example: Cubic polynomials, again

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

$$\operatorname{Prob}\left(N_f(p) = x\right) = \begin{cases} 1/3 & \text{if } x = 0 \\ 1/2 & \text{if } x = 1 \\ 1/6 & \text{if } x = 3 \end{cases} \text{ and } G = S_3.$$

$$S_3 = \left\{ \begin{array}{c} \mathrm{id}, \\ (1 \leftrightarrow 2), (1 \leftrightarrow 3), (2 \leftrightarrow 3), \\ (1 \to 2 \to 3 \to 1), (1 \to 3 \to 2 \to 1) \end{array} \right\}$$

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

$$\operatorname{Prob}\left(N_f(p) = x\right) = \begin{cases} 2/3 & \text{if } x = 0 \\ 1/3 & \text{if } x = 3 \end{cases} \text{ and } G = \mathbb{Z}/3\mathbb{Z}.$$

Prime powers

We may also define

$$N_f\left(p^e\right) = \#\left\{x \in \mathbb{F}_{p^e} \;:\; f(x) = 0\right\}$$

Theorem (Chebotarëv continued)

$$\mathrm{Prob}\left(N_f\left(p\right) = c_1, N_f\left(p^2\right) = c_2, \cdots\right)$$
$$||$$
$$\mathrm{Prob}\left(g \in G : g \text{ fixes } c_1 \text{ roots}, \; g^2 \text{ fixes } c_2 \text{ roots}, \ldots\right)$$

Prime powers

We may also define

$$N_f\left(p^e\right) = \#\left\{x \in \mathbb{F}_{p^e} \ : \ f(x) = 0\right\}$$

Theorem (Chebotarëv continued)

$$\operatorname{Prob}\left(N_f\left(p\right) = c_1, N_f\left(p^2\right) = c_2, \cdots\right)$$

$$||$$

$$\operatorname{Prob}\left(g \in G : g \ \textit{fixes}\ c_1 \ \textit{roots},\ g^2 \ \textit{fixes}\ c_2 \ \textit{roots}, \ldots\right)$$

Let $f(x) = x^3 - 2$, then $G = S_3$ and:

$$\operatorname{Prob}\left(N_f\left(p\right) = N_f\left(p^2\right) = 0\right) = 1/3$$

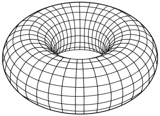
$$\operatorname{Prob}\left(N_f\left(p\right) = N_f\left(p^2\right) = 3\right) = 1/6$$

$$\operatorname{Prob}\left(N_f\left(p\right) = 1, N_f\left(p^2\right) = 3\right) = 1/2$$

Elliptic curves

An *elliptic curve* is a smooth plane algebraic curve defined by

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

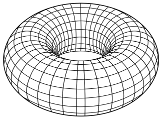
over the complex numbers $\mathbb{C}$ this is a torus: 

Elliptic curves

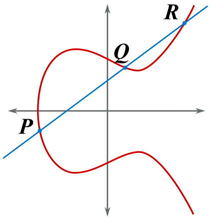
An *elliptic curve* is a smooth plane algebraic curve defined by

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

over the complex numbers $\mathbb{C}$ this is a torus:



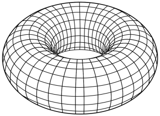
There is a natural *group structure*!
If P, Q, and R are colinear, then
$$P + Q + R = 0$$



Elliptic curves

An *elliptic curve* is a smooth plane algebraic curve defined by

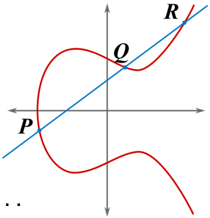
$$y^2 = x^3 + ax + b$$

over the complex numbers $\mathbb{C}$ 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, ...



Counting points on elliptic curves

Given an elliptic curve over $\mathbb{Q}$

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

We can consider its reduction modulo p (ignoring bad primes and $p = 2$).

Counting points on elliptic curves

Given an elliptic curve over $\mathbb{Q}$

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

We can consider its reduction modulo p (ignoring bad primes and $p = 2$).

As before, consider:

$$\begin{aligned} N_X(p) &:= \#X(\mathbb{F}_p) \\ &= \left\{(x, y) \in (\mathbb{F}_p)^2 : y^2 = f(x)\right\} + 1 \end{aligned}$$

One cannot hope to write $N_X(p)$ as an explicit function of p.

Counting points on elliptic curves

Given an elliptic curve over $\mathbb{Q}$

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

We can consider its reduction modulo p (ignoring bad primes and $p = 2$).

As before, consider:

$$\begin{aligned} N_X(p) &:= \#X(\mathbb{F}_p) \\ &= \left\{(x, y) \in (\mathbb{F}_p)^2 : y^2 = f(x)\right\} + 1 \end{aligned}$$

One cannot hope to write $N_X(p)$ as an explicit function of p.

Instead, we look for **statistical** properties of $N_X(p)$.

Hasse's bound

Theorem (Hasse, 1930s)

$$|p + 1 - N_X(p)| \leq 2\sqrt{p}.$$

Hasse's bound

Theorem (Hasse, 1930s)

$$|p+1-N_X(p)| \leq 2\sqrt{p}.$$

In other words,

$$N_x(p) = p + 1 - \sqrt{p}\lambda_p, \quad \lambda_p \in [-2, 2]$$

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

Weil's theorem

Theorem (Hasse, 1930s)

$$N_x(p) = p + 1 - \sqrt{p}\lambda_p, \quad \lambda_p \in [-2, 2].$$

Weil's theorem

Theorem (Hasse, 1930s)

$$N_x(p) = p + 1 - \sqrt{p}\lambda_p, \quad \lambda_p \in [-2, 2].$$

Taking $\lambda_p = 2\cos\theta_p$, with $\theta_p \in [0, \pi]$ we can rewrite

$$N_X(p) = p + 1 - \sqrt{p}(\alpha_p + \overline{\alpha_p}), \quad \alpha_p = e^{i\theta_p}.$$

Weil's theorem

Theorem (Hasse, 1930s)

$$N_x(p) = p + 1 - \sqrt{p}\lambda_p, \quad \lambda_p \in [-2, 2].$$

Taking $\lambda_p = 2\cos\theta_p$, with $\theta_p \in [0, \pi]$ we can rewrite

$$N_X(p) = p + 1 - \sqrt{p}(\alpha_p + \overline{\alpha_p}), \quad \alpha_p = e^{i\theta_p}.$$

Theorem (Weil, 1940s)

$$\begin{aligned} N_X(p^e) &= p^e + 1 - \sqrt{p^e}\left(\alpha_p^e + \overline{\alpha_p}^e\right) \\ &= p^e + 1 - \sqrt{p^e}\, 2\cos(e\,\theta_p) \end{aligned}$$

We may thus focus our attention on

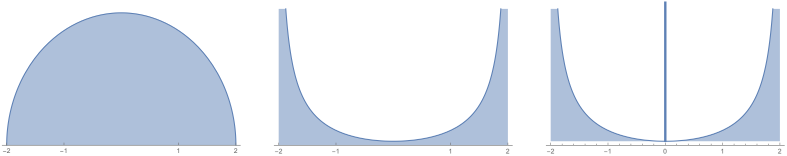
$$p \mapsto \alpha_p \in S^1 \quad \text{or} \quad p \mapsto \theta_p \in [0, \pi] \quad \text{or} \quad p \mapsto 2\cos\theta_p \in [-2, 2]$$

Histograms

If one picks an elliptic curve and computes a histogram for the values

$$\frac{N_X(p) - 1 - p}{\sqrt{p}} = 2\,\mathrm{Re}\,\alpha_p = 2\cos\theta_p$$

over a large range of primes, one always observes convergence to one of three limiting shapes!

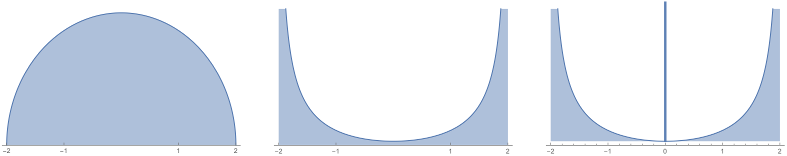


Histograms

If one picks an elliptic curve and computes a histogram for the values

$$\frac{N_X(p) - 1 - p}{\sqrt{p}} = 2\,\mathrm{Re}\,\alpha_p = 2\cos\theta_p$$

over a large range of primes, one always observes convergence to one of three limiting shapes!



One can confirm the conjectured convergence with high numerical accuracy:
`http://math.mit.edu/~drew/g1SatoTateDistributions.html`

Classification of Elliptic curves

Elliptic curves can be divided in two classes: special and ordinary

Classification of Elliptic curves

Elliptic curves can be divided in two classes:

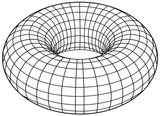
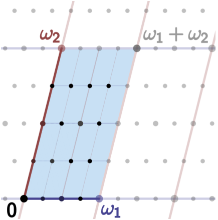
- CM (special)
- non-CM (ordinary)

Classification of Elliptic curves

Elliptic curves can be divided in two classes:

- CM (special)
- non-CM (ordinary)

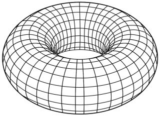
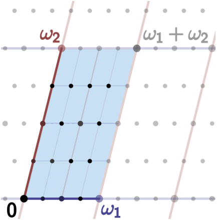
Consider the elliptic curve over $\mathbb{C}$

$X/\mathbb{C} \simeq$  $\simeq \mathbb{C}/\Lambda$ and $\Lambda = \mathbb{Z}\omega_1 \otimes \mathbb{Z}\omega_2 =$ 

Classification of Elliptic curves

Elliptic curves can be divided in two classes:
- CM (special)
- non-CM (ordinary)

Consider the elliptic curve over $\mathbb{C}$

$X/\mathbb{C} \simeq$  $\simeq \mathbb{C}/\Lambda$ and $\Lambda = \mathbb{Z}\omega_1 \otimes \mathbb{Z}\omega_2 =$ 

non-CM the generic case, $\mathrm{End}(\Lambda) = \mathbb{Z}$

CM Λ has extra symmetries,
$\mathbb{Z} \subsetneq \mathrm{End}(\Lambda)$ and $\omega_2/\omega_1 \in \mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{N}$.

CM Elliptic curves

Theorem (Deuring 1940s)

If X is a CM elliptic curve then $\alpha_p = e^{i\theta}$ are equidistributed with respect to the uniform measure on the semicircle, i.e.,

$$\left\{ e^{i\theta} \in \mathbb{C} : \operatorname{Im}(z) \geq 0 \right\} \text{ with } \mu = \frac{1}{2\pi}\, \mathrm{d}\theta$$

If the extra endomorphism is not defined over the base field one must take $\mu = \frac{1}{\pi}\, \mathrm{d}\theta + \frac{1}{2}\delta_{\pi/2}$

In both cases, the probability density function for $2\cos\theta$ is

$$\frac{\{1,2\}}{4\pi\sqrt{4-z^2}} =$$

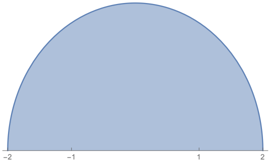
non-CM Elliptic curves

Conjecture (Sato–Tate, early 1960s)

If X does not have CM then $\alpha_p = e^{i\theta}$ are equidistributed in the semi circle with respect to $\mu = \frac{2}{\pi} \sin^2 \theta \, \mathrm{d}\theta$.

The probability density function for $2cos\theta$ is

$$\frac{\sqrt{4 - z^2}}{2\pi} =$$



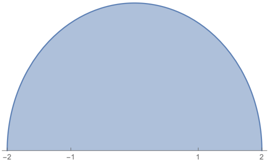
non-CM Elliptic curves

Conjecture (Sato–Tate, early 1960s)

If X does not have CM then $\alpha_p = e^{i\theta}$ are equidistributed in the semi circle with respect to $\mu = \frac{2}{\pi}\sin^2\theta\,\mathrm{d}\theta$.

The probability density function for $2cos\theta$ is

$$\frac{\sqrt{4-z^2}}{2\pi} =$$



Theorem (Clozel, Harris, Taylor, et al., late 2000s; very hard!)

The Sato–Tate conjecture holds for $K = \mathbb{Q}$ (and more generally for K a totally real number field).

Group-theoretic interpretation

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

Group-theoretic interpretation

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

There is compact Lie **group** associated to X called the *Sato–Tate* group ST_X.
It can be interpreted as the "Galois" group of X.

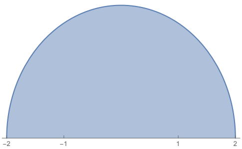
Group-theoretic interpretation

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

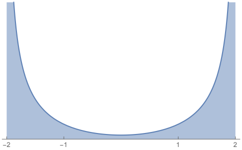
There is compact Lie **group** associated to X called the *Sato–Tate* group ST_X.
It can be interpreted as the "Galois" group of X.

The pairs $\{\alpha_p, \overline{\alpha_p}\}$ are distributed like the eigenvalues of a matrix chosen at random from ST_X with respect to its Haar measure.

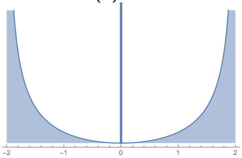
non-CM
$\mathrm{SU}(2)$



CM
$\mathrm{U}(1)$



CM (with the δ)
$\mathrm{N}_{\mathrm{SU}(2)}(\mathrm{U}(1))$



1. Polynomials in one variable

2. Elliptic curves

3. Quartic surfaces

K3 surfaces

K3 surfaces are a 2-dimensional analog of elliptic curves.

K3 surfaces

K3 surfaces are a 2-dimensional analog of elliptic curves.

For simplicity we will focus on **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 2-dimensional analog of elliptic curves.

For simplicity we will focus on **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 $N_X(p^e)$ are associated to a 22×22 orthogonal matrix!

K3 surfaces

K3 surfaces are a 2-dimensional analog of elliptic curves.

For simplicity we will focus on **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 $N_X(p^e)$ are associated to a 22×22 orthogonal matrix!

Instead, we study other geometric invariant.

Picard lattice

We will be studying a lattice associated to X and X mod p.

Picard lattice

We will be studying a lattice associated to X and X mod p.

$\operatorname{Pic} \bullet =$ Picard lattice of $\bullet \simeq \{\text{curves on } \bullet\}/\sim$
$\rho(\bullet) = \operatorname{rk} \operatorname{Pic} \bullet$
$\rho(\overline{X})$ is known as the geometric Picard number

Picard lattice

We will be studying a lattice associated to X and X mod p.

$\operatorname{Pic} \bullet =$ Picard lattice of $\bullet \simeq \{$curves on $\bullet\}/\sim$
$\rho(\bullet) = \operatorname{rk} \operatorname{Pic} \bullet$
$\rho(\overline{X})$ is known as the geometric Picard number

$$\begin{tikzcd}
X \arrow[r, dashed] \arrow[d] & \operatorname{Pic} \overline{X} \arrow[r, dashed] \arrow[d, hook] & \rho(\overline{X}) \in [1, \ldots, 20] \arrow[d, dotted, "???"] \\
X_p := X \bmod p \arrow[r, dashed] & \operatorname{Pic} \overline{X}_p \arrow[r, dashed] & \rho(\overline{X}_p) \in [2, 4, \ldots 22]
\end{tikzcd}$$

Picard lattice

We will be studying a lattice associated to X and $X \bmod p$.

$\operatorname{Pic} \bullet$ = Picard lattice of $\bullet \simeq \{\text{curves on } \bullet\}/\sim$
$\rho(\bullet) = \operatorname{rk} \operatorname{Pic} \bullet$
$\rho(\overline{X})$ is known as the geometric Picard number

$$\begin{tikzcd}
X \arrow[r, dashed] \arrow[d] & \operatorname{Pic} \overline{X} \arrow[r, dashed] \arrow[d, hook] & \rho(\overline{X}) \in [1, \ldots, 20] \arrow[d, dotted, "???"] \\
X_p := X \bmod p \arrow[r, dashed] & \operatorname{Pic} \overline{X}_p \arrow[r, dashed] & \rho(\overline{X}_p) \in [2, 4, \ldots 22]
\end{tikzcd}$$

Theorem (Charles 2011)

We have $\min_q \rho(\overline{X}_q) = \rho(\overline{X}_p)$ *for infinitely many* p.

Problem

$$
\begin{tikzcd}
X \arrow[r, dashed] \arrow[d] & \operatorname{Pic} \overline{X} \arrow[r, dashed] \arrow[d, hook] & \rho(\overline{X}) \in [1, \ldots, 20] \arrow[d, dotted, "???"] \\
X_p := X \bmod p \arrow[r, dashed] & \operatorname{Pic} \overline{X}_p \arrow[r, dashed] & \rho(\overline{X}_p) \in [2, 4, \ldots 22]
\end{tikzcd}
$$

Theorem (Charles 2011)

We have $\min_q \rho(\overline{X}_q) = \rho(\overline{X}_p)$ *for infinitely many* p.

What can we say about the following:

- $\Pi_{\mathrm{jump}}(X) := \{p : \min_q \rho(\overline{X}_q) < \rho(\overline{X}_p)\}$

Problem

$$\begin{tikzcd}
X \arrow[r, dashed] \arrow[d] & \operatorname{Pic} \overline{X} \arrow[r, dashed] \arrow[d, hook] & \rho(\overline{X}) \in [1, \ldots, 20] \arrow[d, dotted, "???"] \\
X_p := X \bmod p \arrow[r, dashed] & \operatorname{Pic} \overline{X}_p \arrow[r, dashed] & \rho(\overline{X}_p) \in [2, 4, \ldots 22]
\end{tikzcd}$$

Theorem (Charles 2011)

We have $\min_q \rho(\overline{X}_q) = \rho(\overline{X}_p)$ *for infinitely many* p.

What can we say about the following:

- $\Pi_{\mathrm{jump}}(X) := \left\{ p : \min_q \rho(\overline{X}_q) < \rho(\overline{X}_p) \right\}$
- $\gamma(X, B) := \dfrac{\#\left\{ p \leq B : p \in \Pi_{\mathrm{jump}}(X) \right\}}{\#\left\{ p \leq B \right\}}$ as $B \to \infty$

Problem

What can we say about the following:

- $\Pi_{\mathrm{jump}}(X) := \left\{ p : \min_q \rho(\overline{X}_q) < \rho(\overline{X}_p) \right\}$
- $\gamma(X, B) := \dfrac{\#\left\{ p \leq B : p \in \Pi_{\mathrm{jump}}(X) \right\}}{\#\left\{ p \leq B \right\}}$ as $B \to \infty$

Information about $\Pi_{\mathrm{jump}}(X) \rightsquigarrow$ Geometric statements

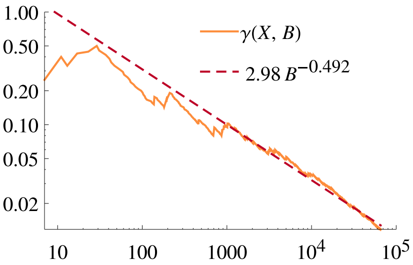
- How often an elliptic curve has $p + 1$ points modulo p?
- How often two elliptic curves have the same number of points modulo p?
- Does $\overline{X}$ have infinitely many rational curves ?
- ...

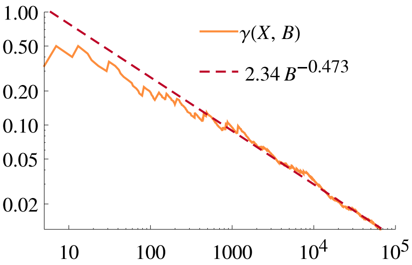
Numerical experiments for a generic K3, $\rho(\overline{X}) = 1$

$\rho(\overline{X})$ is very hard to compute
$\rho(\overline{X}_p)$ only now computationally feasible for large p [C.-Harvey]

Numerical experiments for a generic K3, $\rho(\overline{X}) = 1$

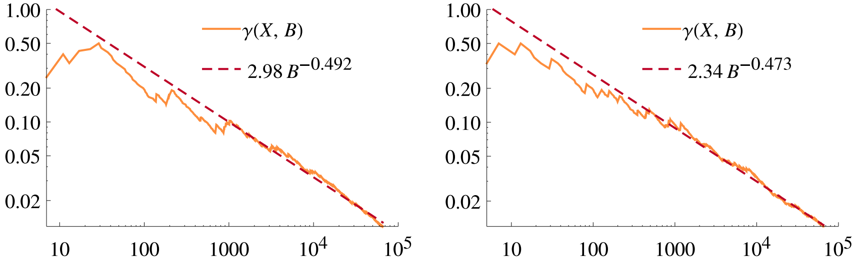
$\rho(\overline{X})$ is very hard to compute
$\rho(\overline{X}_p)$ only now computationally feasible for large p [C.-Harvey]





Numerical experiments for a generic K3, $\rho(\overline{X}) = 1$

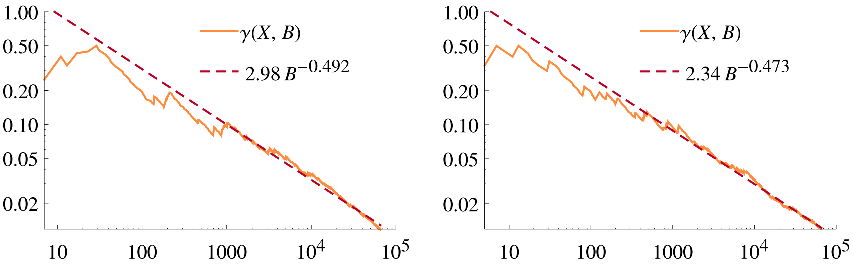
$\rho(\overline{X})$ is very hard to compute
$\rho(\overline{X}_p)$ only now computationally feasible for large p [C.-Harvey]



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

Numerical experiments for a generic K3, $\rho(\overline{X}) = 1$

$\rho(\overline{X})$ is very hard to compute
$\rho(\overline{X}_p)$ only now computationally feasible for large p [C.-Harvey]

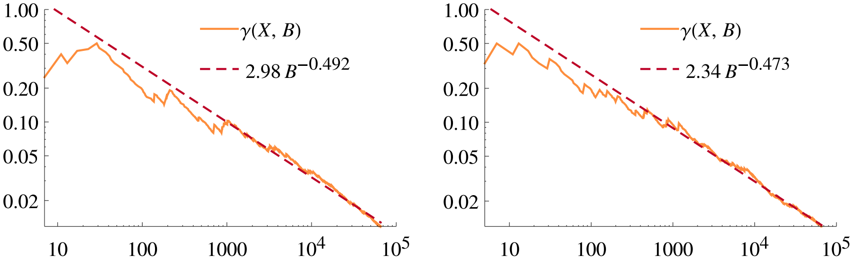


$$\gamma(X, B) \sim \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

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

Numerical experiments for a generic K3, $\rho(\overline{X}) = 1$

$\rho(\overline{X})$ is very hard to compute
$\rho(\overline{X}_p)$ only now computationally feasible for large p [C.-Harvey]



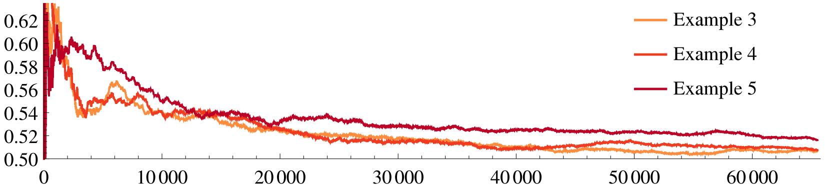
$$\gamma(X, B) \sim \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

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

Similar behaviour observed in other examples with $\rho(\overline{X})$ odd.

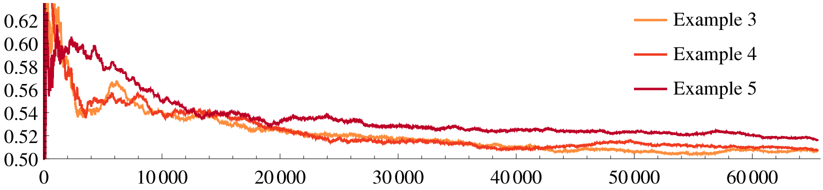
In this case, data $\rightsquigarrow$ equidistribution in $\mathrm{O}(21)$!

Numerical experiments for $\rho(\overline{X}) = 2$



No obvious trend ...

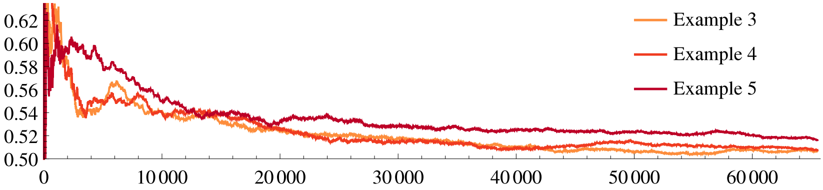
Numerical experiments for $\rho(\overline{X}) = 2$



No obvious trend ...

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

Numerical experiments for $\rho(\overline{X}) = 2$

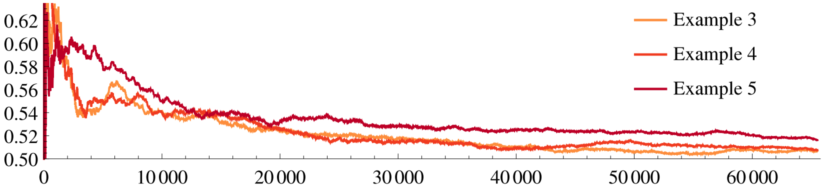


No obvious trend ...

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

Similar behaviour observed in other examples with $\rho(\overline{X})$ even.

Numerical experiments for $\rho(\overline{X}) = 2$



No obvious trend ...

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

Similar behaviour observed in other examples with $\rho(\overline{X})$ even.

Data $\rightsquigarrow$ equidistribution in $\mathrm{O}(20)$!

$\sim$1 CPU year per example.

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.] and [C.-Elsenhans-Jahnel])

Assume $\rho(\overline{X})$ is even and $\rho(\overline{X}) = \min_q \rho(\overline{X}_q)$, there is a $d_X \in \mathbb{Z}$ such that:

$$\{p > 2 : d_X \text{ is not a square modulo } p\} \subset \Pi_{\mathrm{jump}}(X).$$

In general, d_X is not a square.

Corollary

If d_X is not a square:

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

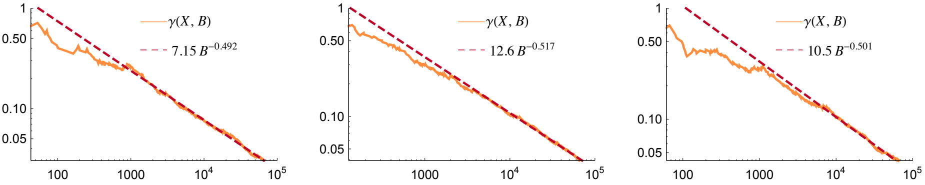
Numerical experiments for $\rho(\overline{X}) = 2$, again

What if we ignore $\{p : d_X \text{ is not a square modulo } p\} \subset \Pi_{\mathrm{jump}}(X)$?

Numerical experiments for $\rho(\overline{X}) = 2$, again

What if we ignore $\{p : d_X \text{ is not a square modulo } p\} \subset \Pi_{\mathrm{jump}}(X)$?

$$\gamma(X, B) \sim c/\sqrt{B}, \quad B \to \infty$$



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

Summary

Computing zeta functions of K3 surfaces via p-adic cohomology$\rightsquigarrow$

- Experimental data for $\Pi_{\mathrm{jump}}(X)$
- Results regarding $\Pi_{\mathrm{jump}}(X)$
- New class of examples of K3 surfaces with infinitely many rational curves

Thank you!