Equidistributions in arithmetic geometry

Edgar Costa

ICERM/Dartmouth College

10th December 2015
IST

Motivation

Question

Given an "integral" object X, for example:

- an integer
- a one variable polynomial with integer coefficients
- an algebraic curves defined by one polynomial equation with integer coefficients
- a smooth surface defined over $\mathbb{Q}$
- ...

I can consider its reduction modulo a prime p.

- What kind of geometric properties of X can we read of X mod p?
- What if we consider infinitely many primes?
- How does X mod p behave when we take $p \to \infty$?
  Does it behave as random as it should?

Overview

Counting roots of polynomials

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

p a prime number

Consider:

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

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

Question

How often does each value occur?

Example: quadratic polynomials

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

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

If Δ isn't a square, then $\text{Prob}(N_f(p) = 0) = \text{Prob}(N_f(p) = 2) = \frac{1}{2}$

In this case, one can even give an explicit formula for $N_f(p)$, using the law of quadratic reciprocity.

For example, if $\Delta = 5$ (for $p > 2$):

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

Example: cubic polynomials

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

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

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

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

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

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.

Theorem (Chebotarëv, early 1920s)

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

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

where,

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

Example: Cubic polynomials, again

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

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

$$\begin{aligned} S_3 = \{&\text{id}, (1 \leftrightarrow 2), (1 \leftrightarrow 3), (2 \leftrightarrow 3), \\ &(1 \to 2 \to 3 \to 1), (1 \to 3 \to 2 \to 1)\} \end{aligned}$$

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

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

Prime powers

We may also define

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

Theorem (Chebotarëv continued)

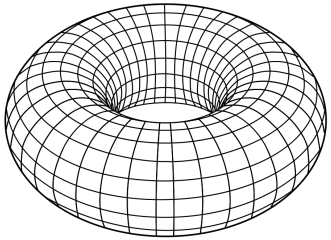
$$\text{Prob}\left(N_f(p) = c_1, N_f\left(p^2\right) = c_2, \cdots\right)$$
$$||$$
$$\text{Prob}\left(g \in G : g \textit{ fixes } c_1 \textit{ roots}, \ g^2 \textit{ fixes } c_2 \textit{ roots}, \ldots\right)$$

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

$$\text{Prob}\left(N_f(p) = N_f\left(p^2\right) = 0\right) = 1/3$$
$$\text{Prob}\left(N_f(p) = N_f\left(p^2\right) = 3\right) = 1/6$$
$$\text{Prob}\left(N_f(p) = 1, N_f\left(p^2\right) = 3\right) = 1/2$$

Elliptic curves

An *elliptic curve* over a field K is a smooth proper algebraic curve over K of genus 1.

Taking $K = \mathbb{C}$ we get a torus:  .

These are projective algebraic curves defined by equations of the form

$$y^2 = f(x)$$

$$f \in K[x],\ \deg f = 3,\ \text{and no repeated roots}$$

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

$$P + Q + R = 0.$$

Applications: cryptography, integer factorization ...

Counting points on elliptic curves

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

$$X : y^2 = f(x), \quad f(x) \in \mathbb{Z}[x]$$

We can consider its reduction modulo p (we will ignore the bad primes and $p = 2$).

As before, consider:

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

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

Instead, we will look for statistical properties of $N_X(p^e)$.

Hasse's bound

Theorem (Hasse, 1930s)

For any positive integer e

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

In other words,

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

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

Weil's theorem

Theorem (Hasse, 1930s)

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

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)

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

We may thus focus our attention on

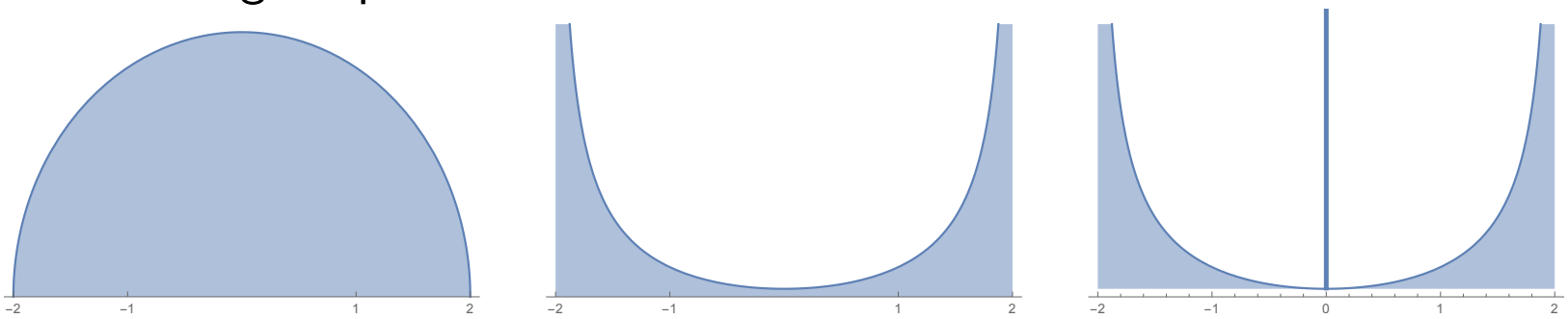
$$p \mapsto \alpha_p \in S^1 \quad \text{or} \quad p \mapsto \theta_p \in [0, \pi] \quad \text{or} \quad p \mapsto 2\cos\theta_p \in [-2, 2]$$

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!

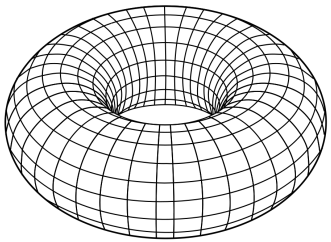


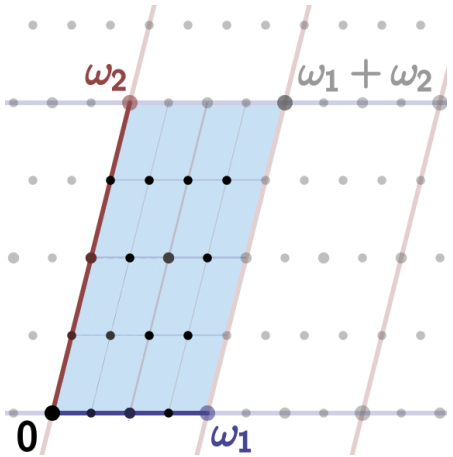
One can confirm the conjectured convergence with high numerical accuracy:
`http://math.mit.edu/~drew/g1SatoTateDistributions.html`

Classification of Elliptic curves

Elliptic curves can be divided in two classes: CM and non-CM

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

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

CM Elliptic curves

Theorem (Deuring 1940s)

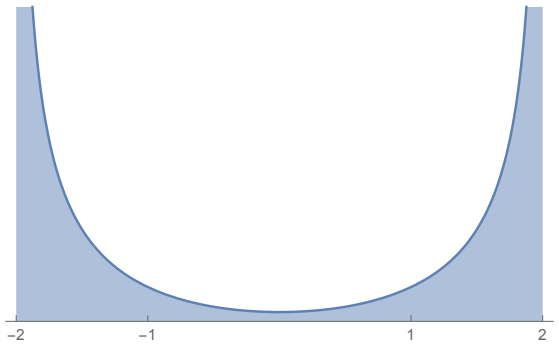
If X is a CM elliptic curve then $\alpha_p = e^{i\theta}$ are equidistributed with respect to the uniform measure on the semicircle, i.e.,

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

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 $t = 2\cos\theta$ is

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



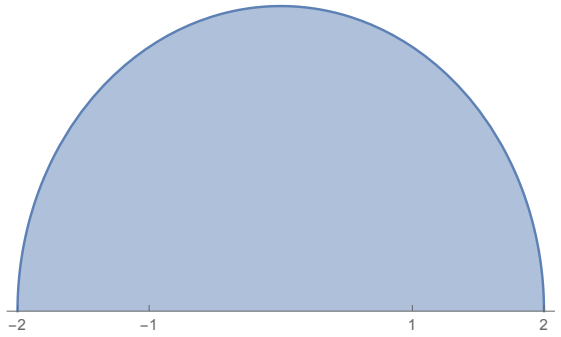
non-CM Elliptic curves

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 $t = 2cos\theta$ is

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



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).

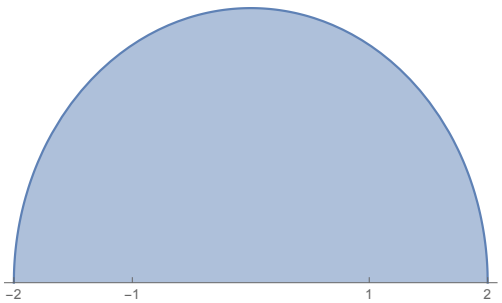
Group-theoretic interpretation

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

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.

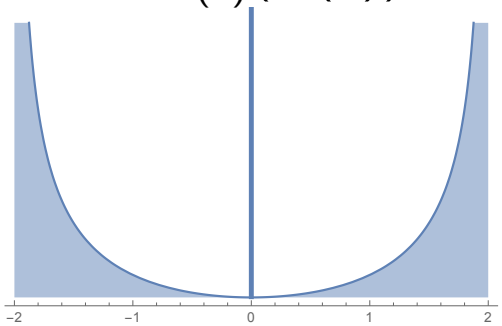
Then, the pairs $\{\alpha_p, \overline{\alpha_p}\}$ are distributed like the eigenvalues of a matrix chosen at random from ST_X with respect to its Haar measure.

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



CM
$\mathrm{U}(1)$

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



K3 surfaces

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

For simplicity we will focus on **smooth quartic surfaces** in $\mathbb{P}^3$

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

$N_X(p^e)$ can be read of some matrix in the Sato–Tate group of X.

However, now $\mathrm{ST}_X \subseteq \mathrm{O}(21)$ and with equality in the generic case.

To get the full picture we would need to study

$$N_X(p^e) \text{ for } 1 \leq e \leq 11$$

Instead, we study other geometric invariant.

Picard group

Put $X_p = X \bmod p$
Let $\mathrm{Pic}(\overline{X}) =$ be the Picard group of X

- $\mathrm{Pic}(\overline{X})$ is a $\mathbb{Z}$ lattice $\simeq \{\text{curves on } X\}/\sim$
- $\rho\left(\overline{X}\right) := \mathrm{rk}\,\mathrm{Pic}\left(\overline{X}\right)$, the geometric Picard number
- $\rho(\overline{X}) \in [1, \ldots, 20]$
- $\rho(\overline{X_p}) \in [2, 4, \ldots 22]$

Theorem (Charles 2011)

There is a $\eta(\overline{X}) \geq 0$ *such that*

$$\min_p \rho(\overline{X}_p) = \rho(\overline{X}) + \eta(\overline{X}) \leq \rho(\overline{X}_p)$$

and ***equality occurs infinitely often****!*

Problem

What can we say about the following:

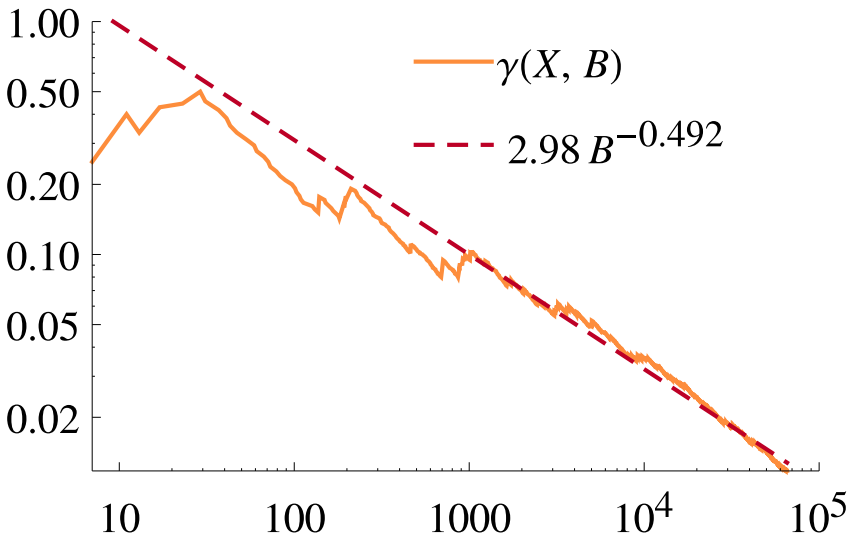
- $\Pi_{\mathrm{jump}}(X) := \left\{p : \rho(\overline{X}) + \eta(\overline{X}) < \rho(\overline{X}_p)\right\}$
- $\gamma(X, B) := \dfrac{\#\left\{p \leq B : p \in \Pi_{\mathrm{jump}}(X)\right\}}{\#\left\{p \leq B\right\}}$ as $B \to \infty$

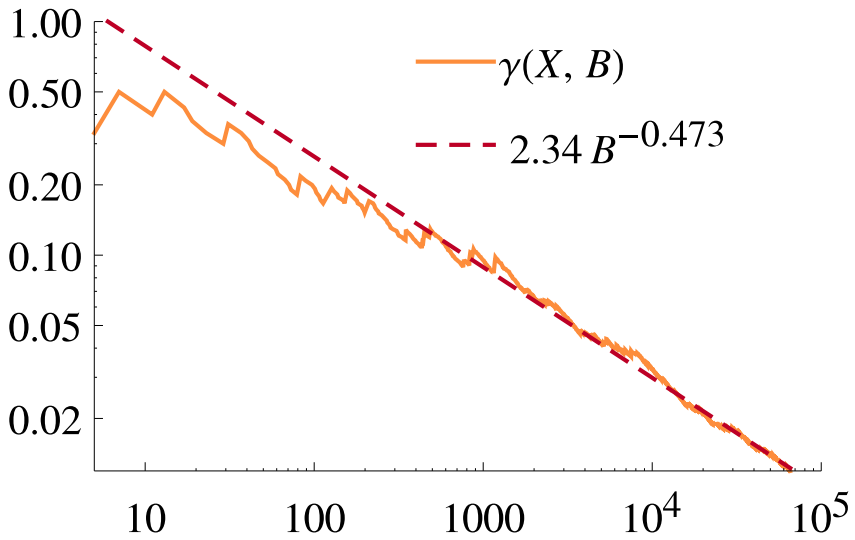
Information about $\Pi_{\mathrm{jump}}(X) \rightsquigarrow$ Geometric statements

- 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, $\rho(\overline{X}) = \eta(\overline{X}) = 1$

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





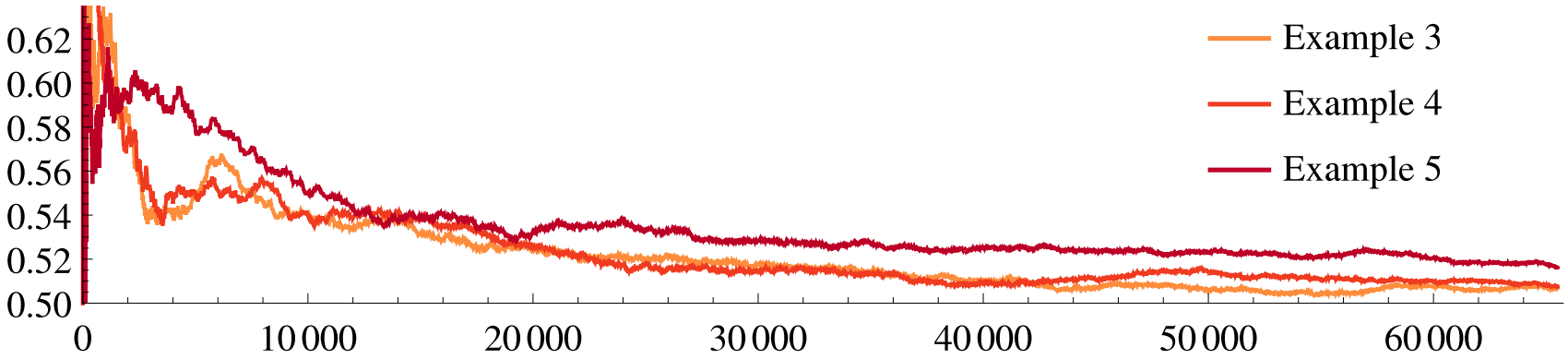
$$\gamma(X, B) \sim \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

$$\sum_{p \le B} \frac{1}{\sqrt{p}} \sim c \frac{\sqrt{B}}{\log B} \implies \text{Prob}(p \in \Pi_{\text{jump}}(X)) \sim 1/\sqrt{p}$$

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 ...

Similar behaviour observed in other examples with $\rho(\overline{X})$ even. Could it be related to a quadratic polynomial and its reductions mod p?

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

$\sim$9000 CPU hours per example.

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

Assume $\rho(\overline{X}) = 2r$ *and* $\eta(\overline{X}) = 0$, *there is a* $d_X \in \mathbb{Z}$ *such that:*

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

The set of X *for which* d_X *is not a square is Zariski dense.*

Corollary

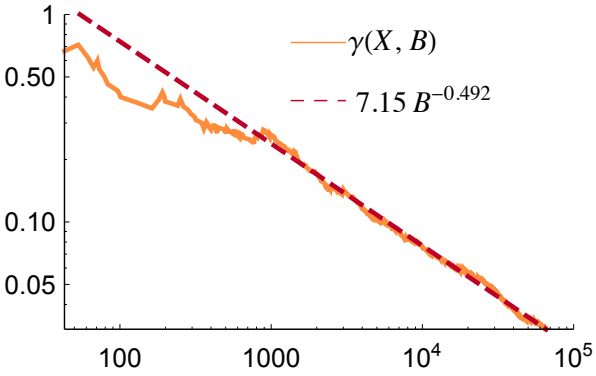
If d_X *is not a square:*

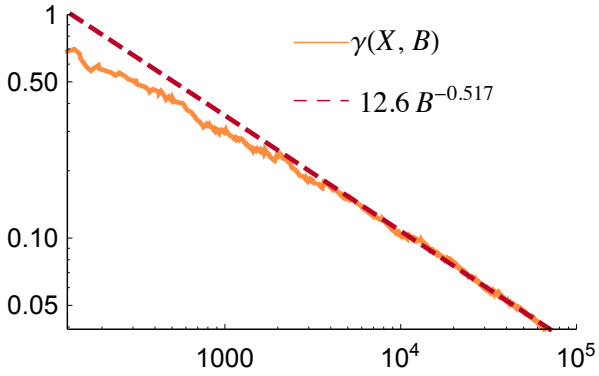
- $\liminf_{B\to\infty} \gamma(X, B) \geq 1/2$
- $\overline{X}$ *has infinitely many rational curves.*

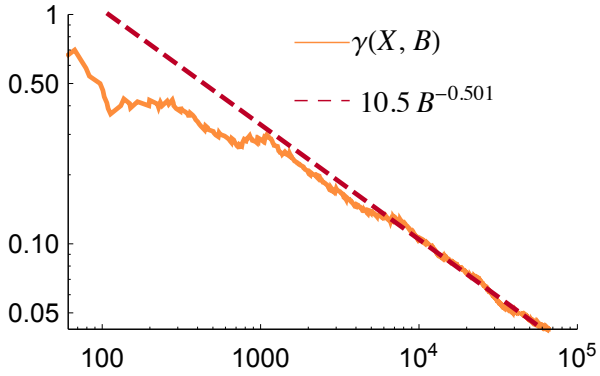
Numerical experiments for $\rho(\overline{X}) = 2$, again

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

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







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

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!