K3 surfaces: From counting points to rational curves

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

January 26, 2021

VaNTAGe: K3 surfaces

Slides available at `researchseminars.org`

Joint work with Andreas-Stephan Elsenhans, Francesc Fité, Jörg Jahnel, Emre Sertöz, and Andrew Sutherland.

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

What is a K3 surface?

There are several equivalent ways to define K3 surfaces.

Definition

An algebraic **K3 surface** is a smooth projective simply-connected surface with trivial canonical class.

They may arise in many ways:

- smooth quartic surface 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 $\mathbb{P}(3, 1, 1, 1)$

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

- Kummer surfaces, $\operatorname{Kummer}(A) := \widetilde{A/\pm}$, with A an abelian surface.

K3 surfaces — the sweet spot for surfaces™

In the classification of surfaces, they land in the middle.

Neither too simple nor too complicated, next level of difficulty past ruled surfaces

K3 surfaces share many common features with curves and abelian varieties, and at the same time provide new challenges!

- Trivial canonical bundle $\Rightarrow$ Calabi–Yau manifold, as for elliptic curves
  This provides us some constructions and insights coming from physics
  - mirror symmetry
  - curve counting heuristics

$$\prod_{n\geq 1}(1-q^n)^{-24} = q/\Delta = \sum_{n\geq 0} d_n q^n \qquad \text{Yau–Zaslow}$$

where d_n should “gives” the number of n-nodal rational curves in a K3 surface

K3 surfaces — the sweet spot for surfaces™

K3 surfaces also share many common features with curves and abelian varieties, and at the same time provide new challenges!

- Trivial canonical bundle $\Rightarrow$ Calabi–Yau manifold, as for elliptic curves
  This provides us some constructions and insights coming from physics
  - mirror symmetry
  - curve counting heuristics

$$\prod_{n\geq 1}(1-q^n)^{-24} = q/\Delta = \sum_{n\geq 0} d_n q^n \qquad \text{Yau–Zaslow}$$

  where d_n should "gives" the number of n-nodal rational curves in a K3 surface
- Torelli theorem: a K3 surface is determined by its Hodge structure
- Kuga–Satake construction: relates a K3 surface X to an abelian variety $KS(X)$ of dimension $\leq 2^{19}$, such that $H^2(X, \mathbb{Z}) \subset H^2(KS(X)^2, \mathbb{Z})$ as Hodge structures.
- a weaker analogy of Honda–Tate theory for abelian varieties.
- categorical description of ordinary K3 surfaces over a finite field

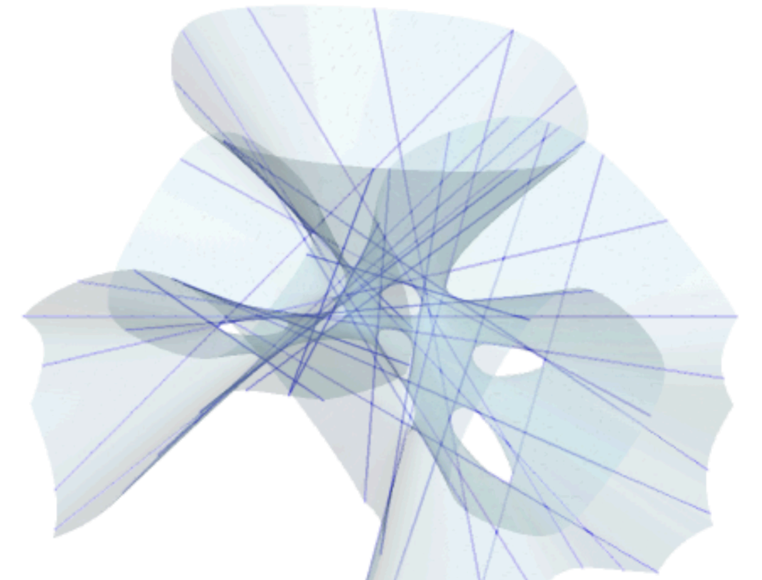
K3 surfaces — popular problems

- existence of rational points
  - Elkies: $x^4 + y^4 + z^4 = w^4$ has infinitely many rational points.
    Disproving Euler's conjectured generalization of Fermat's last theorem.
  - Elsenhans–Jahnel: $x^4 + 2y^4 = z^4 + 4w^4$ found the unique solution ≤ 100 million

    $$(\pm 1\,484\,801, \pm 1\,203\,120, \pm 1\,169\,407, \pm 1\,157\,520)$$

    Counter example to a conjecture of Swinnerton-Dyer.
- Zariski (potential) density of rational points
  - Bogomolov–Tschinkel: if X admits an elliptic fibration or $\#\,\mathbf{Aut}(X) = \infty$, then the rational points are potentially dense.
- existence of rational curves
  - Examples with many lines $\Rightarrow$ curves with many rational points
  - Elkies: the record number of lines in quartic surface is 46 lines defined over $\mathbb{Q}$
    for a double cover of $\mathbb{P}^2$ the record is 53 lines defined over $\mathbb{Q}$
  - Bogomolov–Tschinkel: if X admits an elliptic fibration or $\#\,\mathbf{Aut}(X) = \infty$, then X contains infinitely many rational curves.

Example: Quartic K3 surface with 42 lines, by Elkies



K3 surfaces — popular problems

- Zariski (potential) density of rational points
  - Bogomolov–Tschinkel: if X admits an elliptic fibration or $\# \operatorname{Aut}(X) = \infty$, then the rational points are potentially dense.
- existence of rational curves
  - Examples with many lines $\Rightarrow$ curves with many rational points
  - Elkies: the record number of lines in quartic surface over $\mathbb{Q}$ is 46
  - Bogomolov–Tschinkel: if X admits an elliptic fibration or $\# \operatorname{Aut}(X) = \infty$, then X contains infinitely many rational curves.
- understanding obstructions to Hasse's local–global principle
  - The Brauer group $\operatorname{Br}(X)$ usually plays a key role in such obstructions, somehow analogous to the Tate–Shafarevich group for an elliptic curve.
- classification of automorphism groups
  - Mukai: If $\operatorname{Aut}(X) < \infty$, then $\operatorname{Aut}(X) \subsetneq M_{23}$ iff induces a faithful symplectic action

K3 surfaces — popular problems

- understanding obstructions to Hasse's local–global principle
  - The Brauer group usually plays a key role in such obstructions, somehow analogous to the Tate–Shafarevich group for an elliptic curve.
- classification of automorphism groups
  - Mukai: If $\mathrm{Aut}(X) < \infty$, then $\mathrm{Aut}(X) \subsetneq M_{23}$ iff induces a faithful symplectic action
- Compute geometric invariants
  - Automorphism group $\mathrm{Aut}(X)$
  - Period map
  - Brauer group $\mathrm{Br}(X)$
  - Picard lattice $\mathrm{Pic}(X) \simeq \mathbb{Z}^\rho$

Picard lattice

A key geometric invariant for an algebraic K3 surface is its Picard lattice

$$\mathrm{Pic}(X) = \mathrm{NS}(X) \simeq \mathbb{Z}^{\rho}, \qquad \rho(X) := \mathrm{rk}\,\mathrm{Pic}(X)$$

Geometrically it describes the algebraic cycles on X under linear/algebraic/numerical equivalency.

Plays a similar role as $\mathrm{End}(A)$ for an abelian variety A

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

where $\dagger$ denotes the Rosati involution.

Over $\mathbb{Q}^{\mathrm{al}}$, we have

$$\mathrm{Pic}(X_{\mathbb{Q}^{\mathrm{al}}}) \simeq H^{1,1}(X_{\mathbb{C}}) \cap H^2(X_{\mathbb{C}}, \mathbb{Z}) \subsetneq H^2(X_{\mathbb{C}}, \mathbb{Z}) \simeq (-E_8)^2 \oplus U^3 \simeq \mathbb{Z}^{22}$$

and $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) \in \{1, 2, \ldots, 20\}$.

For a generic K3 surface we have $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) = 1$

Picard lattice

Over $\mathbb{Q}^{\text{al}}$, we have

$$\mathrm{Pic}(X_{\mathbb{Q}^{\text{al}}}) \simeq H^{1,1}(X_{\mathbb{C}}) \cap H^2(X_{\mathbb{C}}, \mathbb{Z}) \subset H^2(X_{\mathbb{C}}, \mathbb{Z}) \simeq (-E_8)^2 \oplus U^3 \simeq \mathbb{Z}^{22}$$

and $\rho(X_{\mathbb{Q}^{\text{al}}}) \in \{1, 2, \ldots, 20\}$.

For a generic K3 surface we have $\rho(X_{\mathbb{Q}^{\text{al}}}) = 1$

The degree of "difficulty" is negatively correlated with $\rho(X)$

$$H^2(X_{\mathbb{C}}, \mathbb{Q}) \simeq Pic(X_{\mathbb{Q}^{\text{al}}})_{\mathbb{Q}} \oplus T(X)_{\mathbb{Q}}$$

The "new and interesting" Galois representations arise from $T(X)$.

Picard lattice – over finite fields

Over $\mathbb{F}_p^{\mathrm{al}}$ we have $\rho(X_{\mathbb{F}_p^{\mathrm{al}}}) \in \{2, 4, \ldots, 22\}$ (Over $\mathbb{Q}^{\mathrm{al}}$ it was $\{1, 2, \ldots, 20\}$)

The Hasse–Weil zeta function $Z_X(t)$ plays a key role for the computation of $\rho(X_{\mathbb{F}_{p^n}})$

$$Z_X(t) := \exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{p^m})}{m} t^m\right) = \frac{1}{(1-t)\chi(t)(1-p^2 t)}$$

where $\chi(t) = \mathbf{det}(1 - t\,\mathbf{Frob} \,|H^2_{\mathrm{et}}(X_{\mathbb{F}_p^{\mathrm{al}}}, \mathbb{Q}_\ell)) \in \mathbb{Z}[t]$ and $\mathbf{deg}\,\chi = 22$.

One may deduce $Z_X(t)$ by naively computing $\#X(\mathbb{F}_{p^m})$ for $m \leq 11$.

From $\chi(t)$ we may deduce $\rho(X_{\mathbb{F}_{p^n}})$ for any n, via Tate conjecture:

$$\mathrm{Pic}(X_{\mathbb{F}_p})_{\mathbb{Q}_\ell} = \ker(\mathrm{Frob}_p - p \cdot \mathrm{id} \,|H^2_{\mathrm{et}}(X_{\mathbb{F}_p^{\mathrm{al}}}, \mathbb{Q}_\ell))$$

Tate conjecture is a theorem for K3 surfaces over finite fields.
[Charles, Madapusi, Kim–Madapusi]

Picard lattice – over finite fields

$$Z_X(t) := \exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{p^m})}{m} t^m\right) = \frac{1}{(1-t)\chi(t)(1-p^2 t)}$$

where $\chi(t) = \det(1 - t\,\mathrm{Frob}\,|H^2_{\mathrm{et}}(X_{\mathbb{F}_p^{\mathrm{al}}}, \mathbb{Q}_\ell)) \in \mathbb{Z}[t]$ and $\deg \chi = 22$.

One may deduce $Z_X(t)$ by naively computing $\#X(\mathbb{F}_{p^m})$ for $m \leq 11$.

From $\chi(t)$ we may deduce $\rho(X_{\mathbb{F}_{p^n}})$ for any n, via Tate conjecture:

$$\mathrm{Pic}(X_{\mathbb{F}_p})_{\mathbb{Q}_\ell} = \ker(\mathrm{Frob}_p - p \cdot \mathrm{id}\,|H^2_{\mathrm{et}}(X_{\mathbb{F}_p^{\mathrm{al}}}, \mathbb{Q}_\ell))$$

Tate conjecture is a theorem for K3 surfaces over finite fields.

For $p > 7$ computing $Z_X(t)$ by naive point counting is unpractical.

Instead, one relies in a infrastructure of methods in crystalline cohomology [Abbott–Kedlaya–Roe, C, C–Harvey–Kedlaya, Tuitman–Pancratz]

Computing Picard lattice over $\mathbb{Q}^{\mathrm{al}}$

Computing $\rho(X_{\mathbb{Q}^{\mathrm{al}}})$ is in principle, solved.
[Charles, Poonen–Testa–van Luijk, Hassett–Kresch–Tschinkel, Shioda, Lairez–Sertöz]
These algorithms are not practical.
Usually rely on searching for explicit generators for the Picard lattice.
We do not know how to do that efficiently.

To terminate such a search, one makes use of the specialization being injective

$$\mathrm{Pic}(X_{\mathbb{Q}^{\mathrm{al}}}) \hookrightarrow \mathrm{Pic}(X_{\mathbb{F}_p^{\mathrm{al}}}) \quad \text{and} \quad \rho(X_{\mathbb{Q}^{\mathrm{al}}}) \leq \rho(X_{\mathbb{F}_p^{\mathrm{al}}}),$$

for a prime of good reduction.

Various ad hoc methods exist to improve the inequality above.

Improving upper bounds — using two specializations [van Luijk]

$$\operatorname{Pic}(X_{\mathbb{Q}^{\mathrm{al}}}) \hookrightarrow \operatorname{Pic}(X_{\mathbb{F}_p^{\mathrm{al}}}) \quad \text{and} \quad \rho(X_{\mathbb{Q}^{\mathrm{al}}}) \leq \rho(X_{\mathbb{F}_p^{\mathrm{al}}})$$

If p and q are two primes of good reduction, and

$$\rho(X_{\mathbb{F}_p^{\mathrm{al}}}) = \rho(X_{\mathbb{F}_q^{\mathrm{al}}}) = 2r,$$
$$\operatorname{disc}\operatorname{Pic}(X_{\mathbb{F}_p^{\mathrm{al}}}) \neq \operatorname{disc}\operatorname{Pic}(X_{\mathbb{F}_q^{\mathrm{al}}}).$$

then

$$\operatorname{Pic}(X_{\mathbb{Q}^{\mathrm{al}}}) < 2r.$$

van Luijk, used this technique with $r = 1$, to provide the first known examples of K3 surfaces over $\mathbb{Q}$ such that $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) = 1$

Improving upper bounds — torsion-free cokernel [Elsenhans–Jahnel]

Elsenhans–Jahnel showed that the specialization map

$$\mathrm{Pic}(X_{\mathbb{Q}^{\mathrm{al}}}) \hookrightarrow \mathrm{Pic}(X_{\mathbb{F}_p^{\mathrm{al}}})$$

has torsion-free cokernel for $p \neq 2$.

Thus, if $\rho(X_{\mathbb{F}_p^{\mathrm{al}}}) = \rho(X_{\mathbb{Q}^{\mathrm{al}}})$ every invertible sheaf lifts.

For example, if $\rho(X_{\mathbb{F}_p^{\mathrm{al}}}) = 2$, Elsenhans–Jahnel approach is

1. compute $\mathrm{Pic}(X_{\mathbb{F}_p^{\mathrm{al}}})$
2. estimate the degree of a hypothetical effective divisor of the lift
3. use Gröbner bases to verify that such a divisor does or does not exist

This approach is only practical if one can compute $\mathrm{Pic}(X_{\mathbb{F}_p^{\mathrm{al}}})$ and if the obtained estimates are low.

Improving upper bounds — p-adic obstruction map [C–Sertöz]

Compute an p-adic approximation of the obstruction map

$$\pi : \operatorname{Pic}(X_{\mathbb{F}_p}) \subset H^2_{\mathbf{crys}}(X/\mathbb{Z}_p) \to H^2_{\mathbf{crys}}(X/\mathbb{Z}_p)/F^1 H^2_{\mathbf{crys}}(X/\mathbb{Z}_p)$$

If $\pi(C) \neq 0$, then $C \notin \operatorname{Pic}(X)$. (analogous to $\operatorname{Pic}(X_{\mathbb{C}}) = H^{1,1}(X_{\mathbb{C}}) \cap H^2(X, \mathbb{Z})$)

1. compute a p-adic approximation of Frob_p
2. compute an approximation of

$$\operatorname{Pic}(X_{\mathbb{F}_p})_{\mathbb{Q}_p} = \ker(\operatorname{Frob}_p - p \cdot \operatorname{id} | H^2_{\mathrm{dR}}(X/\mathbb{Q}_p))$$

3. compute an approximation of

$$\pi_{\mathbb{Q}_p} : \operatorname{Pic}(X_{\mathbb{F}_p})_{\mathbb{Q}_p} \to H^2_{\mathrm{dR}}(X/\mathbb{Q}_p)/F^1 H^2_{\mathrm{dR}}(X/\mathbb{Q}_p)$$

4. $\dim \operatorname{Pic}(X) \leq \dim_{\mathbb{Q}_p} \ker \pi_{\mathbb{Q}_p}$

Picard number via Sato–Tate moments

Theorem (C–Fité–Sutherland)

Let X be a K3 surface over a number field k, then we have

$$\begin{aligned}\dim \operatorname{Pic}(X) &= \mathrm{M}_1[a_1] = \mathrm{E}_{\mathrm{ST}_X}[\mathrm{tr}] \\ &\stackrel{?}{=} \mathrm{E}[\mathrm{tr}(\mathrm{Frob}_p \,|H^2(X)(1))] = \lim_{N\to\infty} \pi_k(N)^{-1} \sum_{\mathrm{Nm}(\mathfrak{p})\leq N} \frac{\mathrm{tr}(\mathrm{Frob}_{\mathfrak{p}})}{\mathrm{Nm}(\mathfrak{p})}\end{aligned}$$

The Sato–Tate group of X is a compact Lie group $G \subset O(22)$ containing (as a dense subset) the image of a representation that maps Frobenius elements to conjugacy classes.

K3 surfaces

So far we have been trying to improve the inequality $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) \leq \rho(X_{\mathbb{F}_p^{\mathrm{al}}})$.
Can we use the inequality to our advantage?

Theorem [Li–Liedtke]

If there are infinitely many p primes such that

$$\rho(X_{\mathbb{Q}^{\mathrm{al}}}) < \rho(X_{\mathbb{F}_p^{\mathrm{al}}}) \text{ and } \rho(X_{\mathbb{F}_p^{\mathrm{al}}}) \neq 22,$$

then $X_{\mathbb{Q}^{\mathrm{al}}}$ contains infinitely many rational curves.

Theorem [Bogomolov–Zarhin]

The set $\{p : \rho(X_{\mathbb{F}_p^{\mathrm{al}}}) \neq 22\}$ has positive density (density 1 after finite extension).

Corollary [Li–Liedtke]

If $\rho(X_{\mathbb{Q}^{\mathrm{al}}})$ is odd, then $X_{\mathbb{Q}^{\mathrm{al}}}$ contains infinitely many rational curves.

Jumping Picard ranks

Theorem [Charles]

We have

$$\rho(X_{\mathbb{Q}^{\mathrm{al}}}) + \eta(X_{\mathbb{Q}^{\mathrm{al}}}) \leq \rho(X_{\mathbb{F}_p^{\mathrm{al}}})$$

for some $\eta(X_{\mathbb{Q}^{\mathrm{al}}}) \geq 0$. Equality occurs infinitely often (density 1 after some finite extension).

Consider

$$\Pi_{\mathrm{jump}}(X) := \left\{ p : \rho(X_{\mathbb{F}_p^{\mathrm{al}}}) > \rho(X_{\mathbb{Q}^{\mathrm{al}}}) + \eta(X_{\mathbb{Q}^{\mathrm{al}}}) \right\}$$

Is this set infinite? What is its density?

What about

$$\gamma(X, B) := \frac{\#\{p \leq B : p \in \Pi_{\mathrm{jump}}(X)\}}{\#\{p \leq B\}} \quad \text{as } B \to \infty \quad ?$$

Jumping Picard ranks for Kummer surfaces

Let $X \simeq \mathrm{Kummer}(A) := \widetilde{A/\pm}$ be a Kummer surface, where A is an abelian surface.

We have

- $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) = \rho(A_{\mathbb{Q}^{\mathrm{al}}}) + 16$
- $\rho(X_{\mathbb{F}_p^{\mathrm{al}}}) = \rho(A_{\mathbb{F}_p^{\mathrm{al}}}) + 16$
- $\eta(X_{\mathbb{Q}^{\mathrm{al}}}) = \eta(A_{\mathbb{Q}^{\mathrm{al}}}) = (\rho(A_{\mathbb{Q}^{\mathrm{al}}}) \bmod 2)$

Thus, $\Pi_{\mathrm{jump}}(X) = \Pi_{\mathrm{jump}}(A)$

Moreover

$$\mathrm{Pic}(A_k)/\,\mathrm{Pic}^0(A_k) \simeq \mathrm{NS}(A_k)_{\mathbb{Q}} \simeq \{\phi \in \mathrm{End}(A_k)_{\mathbb{Q}} : \phi^\dagger = \phi\},$$

where $\dagger$ denotes the Rosati involution and

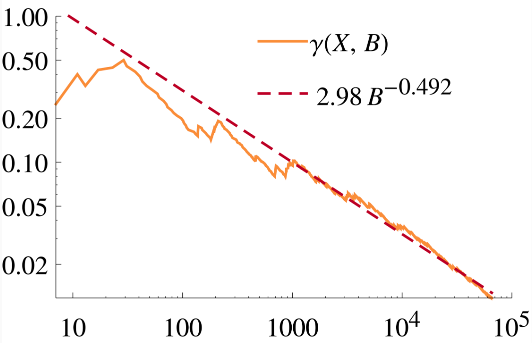
- $\rho(A_{\mathbb{F}_p^{\mathrm{al}}}) \geq 4 \iff A_{\mathbb{F}_p^{\mathrm{al}}} \sim E^2$, E an elliptic curve
- $\rho(A_{\mathbb{F}_p^{\mathrm{al}}}) = 6 \iff A_{\mathbb{F}_p^{\mathrm{al}}} \sim E^2$, E a supersingular elliptic curve

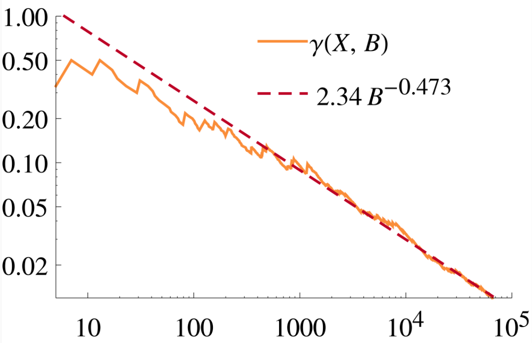
Jumping Picard ranks for Kummer surfaces

- $\rho(A_{\mathbb{F}_p^{\mathrm{al}}}) \geq 4 \iff A_{\mathbb{F}_p^{\mathrm{al}}} \sim E^2$, E an elliptic curve
- $\rho(A_{\mathbb{F}_p^{\mathrm{al}}}) = 6 \iff A_{\mathbb{F}_p^{\mathrm{al}}} \sim E^2$, E a supersingular elliptic curve
- If $A \sim E^2$, then $p \in \Pi_{\mathrm{jump}}(A)$ iff p is supersingular for E
  This is related to the Lang–Trotter conjecture
  It states that p should be supersingular with probability proportional to $1/\sqrt{p}$
  Elkies has shown that there are infinitely many supersingular primes for $E/\mathbb{Q}$.
- If $A \sim E_1 \times E_2$ with $E_1 \not\sim E_2$, then $p \in \Pi_{\mathrm{jump}}(A)$ iff $E_1 \sim E_2$ over ${\mathbb{F}_p}^{\mathrm{al}}$
  Charles has shown that there are also infinitely many such primes.
- If $\mathrm{End}(A_{\mathbb{Q}^{\mathrm{al}}}) = \mathbb{Z}$, then $p \in \Pi_{\mathrm{jump}}(A)$ iff $A_{\mathbb{F}_p^{\mathrm{al}}} \sim E^2$
  What do you think it should happen in this case?

Let's do some numerical experiments for some non Kummer surfaces!

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

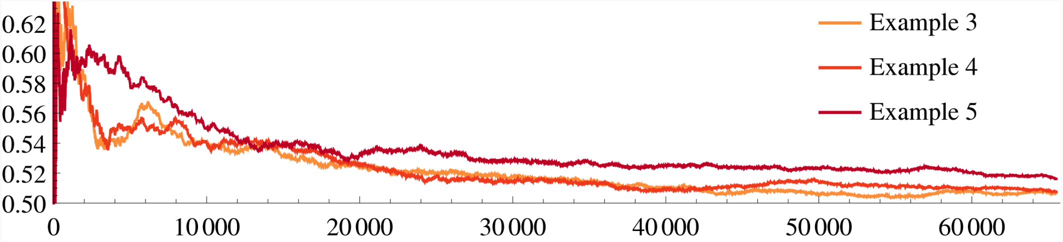




$$\gamma(X, B) \overset{?}{\sim} \frac{c_X}{\sqrt{B}}, \quad B \to \infty$$

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

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



No obvious trend...

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

We can explain the $1/2$

Theorem (C, C–Elsenhans–Jahnel)

If $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) = \min_p \rho(X_{\mathbb{F}_p^{\mathrm{al}}})$*, then there is* $d_X \in \mathbb{Z}$ *such that:*

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

d_X *represents the quadratic character* $p \mapsto \det(\mathrm{Frob}_p \,|T(X)(1)) \in \pm 1.$

Corollary

If d_X *is not a square:*

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

$d_{X_3} = -1 \cdot 5 \cdot 151 \cdot 22490817357414371041 \cdot 387308497430149337233666358807996260780875056740850984213276970343278935342068889706146733313789$

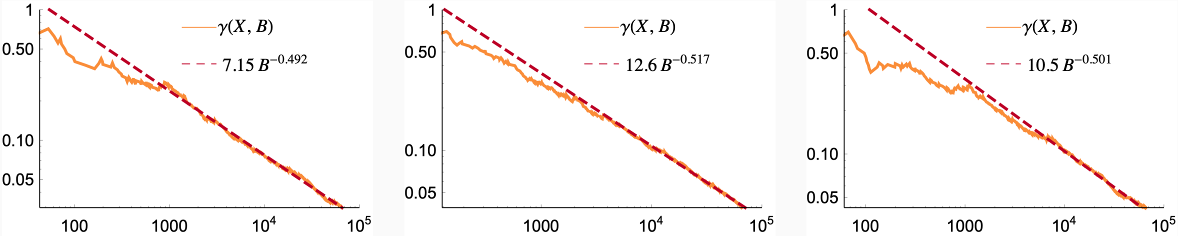
$d_{X_4} = 53 \cdot 2624174618795407 \cdot 512854561846964817139494202072778341 \cdot 1215218370089028769076718102126921744353362873 \cdot 6847124397158950456921300435158$

$d_{X_5} = -1 \cdot 47 \cdot 3109 \cdot 4969 \cdot 14857095849982608071 \cdot 445410277660928347762586764331874432202584688016149 \cdot 65865270852505269999342419873884248599811$

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

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

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



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