Toric point counting and applications

Edgar Costa (Dartmouth College)

16th March 2017

Presented at BIRS, New Trends in Arithmetic and Geometry of Algebraic Surfaces
Joint work with David Harvey (UNSW) and Kiran Kedlaya (UCSD)

Motivation

Riemann zeta function

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{7^s} \cdots$$
$$= \frac{1}{1-2^{-s}} \cdot \frac{1}{1-3^{-s}} \cdot \frac{1}{1-5^{-s}} \cdots$$

- One of the most famous examples of a global zeta function
- Together with the functional equation

$$\xi(s) := \pi^{-s/2}\Gamma(s/2)\zeta(s) = \xi(1-s)$$

encodes a lot of the arithmetic information of $\mathbb{Z}$.
e.g.: Zeros of $\zeta(s) \rightsquigarrow$ precise prime distribution

- $\zeta(s)$ still keeps secret many of its properties

Hasse–Weil zeta functions

Hasse and Weil generalized $\zeta(s)$ for algebraic varieties

$$\zeta_X(s) := \prod_p \zeta_{X_p}(p^{-s})$$

If $X_p := X \bmod p$ is smooth, then

$$\zeta_{X_p}(t) := exp\left(\sum_{i\geq 1} \#X_p(\mathbb{F}_{p^i})\frac{t^i}{i}\right) = \prod_i \det\left(1 - t\,\mathrm{Frob}\,|H^i_{\mathrm{et}}(\overline{X_p}, \mathbb{Q}_\ell)\right)^{(-1)^{i+1}}$$

Example: $X = \{\bullet\}$, a point over $\mathbb{Q}$, then $\zeta_{\{\bullet\}}(s) = \zeta(s)$

	$\zeta_{X_p}(t)$	$\zeta_X(s)$
functional equation	✓	?
Riemann hypothesis	✓	?
arithmetic information	✓	?

What arithmetic properties of X can we read from $\zeta_X(s)$?

Elliptic curves

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

$$\zeta_E(s) := \prod_p \zeta_{E_p}(p^{-s}) \quad \text{and} \quad \zeta_{E_p}(t) = \frac{L_p(t)}{(1-t)(1-pt)}$$

$$L_p(t) = \begin{cases} 1 - a_p t + pt^2, & \text{good reduction, } a_p = p + 1 - \#E_p(\mathbb{F}_p) \\ 1 \pm t, & \text{non-split/split multiplicative reduction;} \\ 1 & \text{additive reduction;} \end{cases}$$

$$\zeta_E(s) = \prod_p \frac{L_p(p^{-s})}{(1-p^{-s})(1-p^{-s+1})} = \frac{\zeta(s)\zeta(s-1)}{L_E(s)}$$

- $L_E(s)$ is the interesting factor
- Modularity theorem $\implies$ $L_E(s)$ satisfies a functional equation
- Birch–Swinnerton-Dyer conjecture predicts $\operatorname{ord}_{s=1} L_E(s) = \operatorname{rk}(E)$.

$\zeta(s)$ vs $\zeta_X(s)$

We always expect $\zeta_X(s)$ to satisfy a functional equation.

- zero-dimensional varieties (number fields) ✓
- elliptic curves over $\mathbb{Q}$ ✓
- genus 2 curves ? numerically ✓
- surfaces ?

Major difference

- easy to explicitly write down $\zeta(s)$
- extremely difficult to calculate $\zeta_{X_p}(t)$ for an arbitrary X

Today

New method to compute $\zeta_{X_p}(t)$ that achieves a good balance between practicality and generality.

Outline

Nondegenerate toric hypersurfaces

p-adic Cohomology

Applications

Nondegenerate toric hypersurfaces

Lattices and differentials

- R a domain
- Consider the Laurent polynomial ring

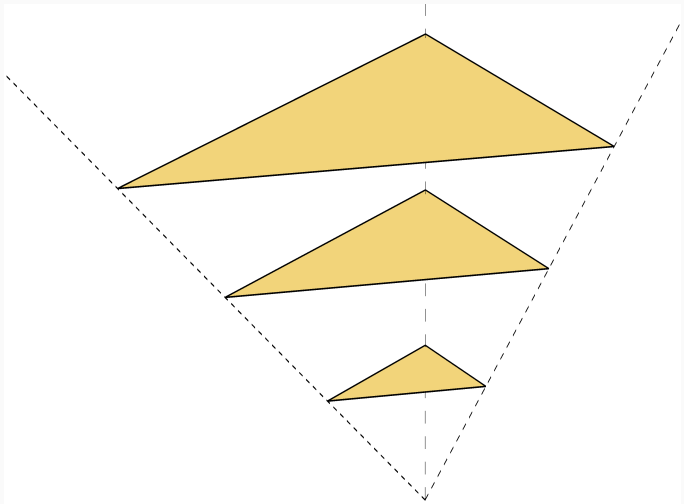
$$L := R[x_1^{\pm}, \ldots, x_n^{\pm}]$$

  the R-algebra generated by monomials with exponents in $\mathbb{Z}^n$.
- If $R = \mathbb{C}$, then $\mathrm{Spec}(L) = (\mathbb{C}^*)^n$, the n-dimensional torus
- We define a degree preserving derivation in L

$$\partial_i = x_i \frac{\partial}{\partial x_i}$$

Toric varieties

- Δ a convex polytope in $\mathbb{R}^n$ (the convex hull of a finite subset of $\mathbb{Z}^n$).
- If Δ is "nice" we can associate to it a graded ring (and a projective variety).



$$P_\Delta := \bigoplus_{d \geq 0} P_d, \quad P_d := R[d\Delta \cap \mathbb{Z}^n]$$

$$X_\Delta := \operatorname{Proj} P_\Delta$$

Examples

Δ	X_Δ
$\operatorname{Conv}(0, e_1, \ldots, e_n)$	$\mathbb{P}^n$
$\operatorname{Conv}(0, e_1, \ell e_2, \ldots, \ell e_n)$	$\mathbb{P}^n(\ell, 1, \ldots, 1)$
$\operatorname{Conv}(0, e_1, e_2, e_1 + e_2)$	$\mathbb{P}^1 \times \mathbb{P}^1$

Nondegenerate hypersurfaces

Definition

$f \in P_d$, $J_f := \langle f, \partial_1 f, \ldots, \partial_n f \rangle$.
We say that f is nondenegerate if the ideal J_f is irrelevant in P_Δ.

$\iff$ $(P_\Delta)_\ell = (J_f)_\ell$ for $\ell \gg 0$

$\iff$ if for every face $\sigma \subset \Delta$ (including Δ itself) f restricted to the torus associated to σ is nonsingular of codimension 1.

$\implies$ Nondegeneracy is a generic condition.

Example

$\mathrm{supp}(f) \subset \mathrm{conv}(0, de_1, de_2)$, f defines a plane curve C in $\mathbb{P}^2$.
C is nondegenerate if:

- C does not pass through the points $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$;
- C intersects the coordinate axes $x = 0$, $y = 0$, $z = 0$ transversally;
- C is smooth on the complement of the coordinate axes.

Examples

Vertices of Δ	Resulting hypersurface
$0, de_1, de_2$	Smooth plane curve of genus $\binom{d-1}{2}$
$0, (2g+1)e_1, 2e_2$	Odd hyperelliptic curve of genus g
$0, ae_1, be_2$	$C_{a,b}$-curve
$0, 4e_1, 4e_2, 4e_3$	Quartic K3 surface
$0, 2e_1, 6e_2, 6e_3$	Degree 2 K3 surface
$0, 5e_1, \ldots, 5e_5$	Quintic Calabi-Yau threefold
$0, 3e_1, \ldots, 3e_6$	Cubic fourfold

Remark

There are 95 different polytopes that give rise to a K3 surface.

p-adic Cohomology

Goal

Setup

- $R = \mathbb{Z}_p$
- $f \in P_1$ nondegenerate with respect to $\Delta = \text{conv}(\text{supp}\, f)$
- $Z := V(f) = \{x \in X_\Delta : f(x) = 0\}$

Goal

Compute

$$\zeta_{Z_{\mathbb{F}_p}}(t) := exp\left(\sum_{i\geq 1} \#Z(\mathbb{F}_{p^i})\frac{t^i}{i}\right) \in \mathbb{Q}(t)$$

$$:= Q(t)^{(-1)^n} \prod_{i=0}^{n-1} \left(\frac{1}{1-p^i t}\right)^{b_i},$$

where $Q(t) = \det\left(1 - p^{-1}t\,\text{Frob}\,|H^n_{\text{et}}(\overline{X_\Delta \backslash Z}, \mathbb{Q}_\ell)\right) \in 1 + \mathbb{Z}[t]$.

How can we do this?

Naively computing $\#Z(\mathbb{F}_{p^a})$ to deduce $Q(t)$ is not practical!

In general, to recover $Q(t)$ we need $\#X(\mathbb{F}_{p^a})$ for $a = 1, \ldots, \lceil \deg Q/2 \rceil$.

Some data points:

- Elliptic curve, $Q(t) = 1 - a_p t + p t^2$
- genus 2 curve, $Q(t) = 1 + a_{p,1} t + a_{p,2} t^2 + p a_{p,1} t^3 + p^2 t^4$
- K3 surface, $\deg Q = 21$
- Calabi-Yau 3fold, $\deg Q = 204$

Instead, we will switch cohomology theory.

$$\begin{aligned} Q(t) &= \det\left(1 - p^{-1} t \operatorname{Frob} \,|\, H^n_{\mathrm{et}}(\overline{X_\Delta \setminus Z}, \mathbb{Q}_\ell)\right) \\ &= \det\left(1 - p^{-1} t \operatorname{Frob} \,|\, H^n_{\mathrm{rig}}(X_\Delta \setminus Z)\right) \\ &= \det\left(1 - p^{-1} t \operatorname{Frob} \,|\, H^{\dagger,n}(X_\Delta \setminus Z)\right) \end{aligned}$$

Master plan

Setup

- $R = \mathbb{Z}_p$, $\in P_1$ nondegenerate
- $Z := V(f) = \{x \in X_\Delta : f(x) = 0\}$
- $U := X_\Delta \backslash Z$ a smooth affine variety
- $\mathbb{Z}_p(U) = \bigoplus_{i \geq 0} f^{-i} P_i$
- σ = p-th power Frobenius

Goal

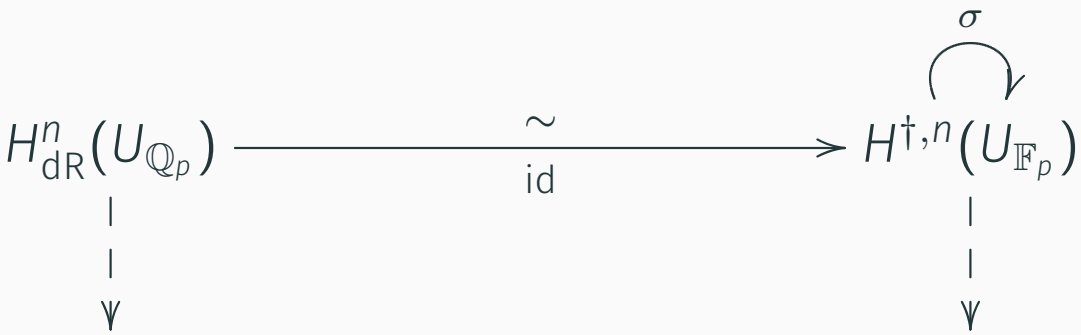
Compute the matrix representing the action of Frob in $H^{\dagger,n}(U_{\mathbb{F}_p})$ with enough of p-adic precision to deduce

$$\det\left(1 - p^{-1} t \,\mathrm{Frob} \,|H^{\dagger,n}(U_{\mathbb{F}_p})\right).$$

Overall picture

Goal

Compute the matrix representing the action of σ in $H^{\dagger,n}(U_{\mathbb{F}_p})$ with enough of p-adic precision.



explicit description over $\mathbb{C}$
[Dwork–Griffiths, Batyrev–Cox]

de Rham cohomology
with overconvergent power series

cohomology relations

+

commutative algebra

$\Longrightarrow$

basis for $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p}) = \left\{x^\beta \omega / f^i\right\}_\beta$

+

reduction algorithm

Generic algorithm – Abbott–Kedlaya–Roe type

$$H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p}) \xrightarrow[\mathrm{id}]{\sim} H^{\dagger,n}(U_{\mathbb{F}_p}) \quad \overset{\sigma}{\circlearrowright} \qquad \approx \begin{matrix} H^n_{\mathrm{dR}}(U) \\ \text{with overconvergent} \\ \text{power series} \end{matrix}$$

1. Compute $\left\{ \frac{x^\beta}{f^m}\omega \right\}_\beta$ a monomial basis for $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p})$
2. In $H^{\dagger,n}$ compute a series approximation for

$$\sigma\left(\frac{x^\beta}{f^m}\omega\right) = p^n \frac{x^{p\beta}}{f^{pm}}\omega \sum_{i\geq 0} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i$$

3. Write the approximation in terms of basis elements, i.e., apply the de Rham relations

Explicit description of H^n_{dR}

Set $\omega := \frac{dx_1}{x_1} \wedge \cdots \wedge \frac{dx_n}{x_n} \in \Omega^n(\mathbb{T})$, $\mathbb{T} := \operatorname{Spec} \mathbb{Q}_p[x_1^{\pm}, \ldots, x_n^{\pm}] \simeq (\mathbb{Q}_p^*)^n$.

For $g \in P_m$ we have

$$\frac{gf}{f^{m+1}}\omega = \frac{g}{f}\omega$$

$$m\frac{g\,\partial_i f}{f^{m+1}}\omega \equiv \frac{\partial_i g}{f^m} \qquad \text{for } i = 1, \ldots, n, \text{ and } m > 0 \text{ in } H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p} \cap \mathbb{T}).$$

If $h \in (J_f)_{m+1} := \langle f, \partial_1 f, \ldots, \partial_n f \rangle_{m+1}$ then

$$m\frac{h}{f^{m+1}}\omega = m\frac{c_0 f + \sum_i c_i \partial_i f}{f^{m+1}} \equiv \frac{m c_0 f + \sum_i \partial_i c_i}{f^m} = \frac{\tilde{h}}{f^m}\omega \text{ with } \tilde{h} \in P_m$$

The nondenegeracy condition $\implies$ $P_\ell \subset (J_f)_\ell$ for $\ell > n$

$\implies$ we may always reduce the pole order to n or less

Same equations hold for $U_{\mathbb{Q}_q}$, if $g \in P_m^{\mathrm{int}} := R[\mathrm{int}(m\Delta) \cap L]$.

Generic algorithm – Abbott–Kedlaya–Roe

$$H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p}) \xrightarrow[\mathrm{id}]{\sim} H^{\dagger,n}(U_{\mathbb{F}_p}) \qquad \overset{\sigma}{\curvearrowright} \qquad H^n_{\mathrm{dR}}(U) \approx \text{ with overconvergent power series}$$

1. Compute $\left\{ \frac{x^\beta}{f^m}\omega \right\}_{\beta \in P^{\mathrm{int}}_m \setminus (J_f)_m,\, m \leq n}$ a monomial basis for $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_p})$
2. In $H^{\dagger,n}$ compute a series approximation for

$$\sigma\left(\frac{x^\beta}{f^m}\omega\right) = p^n \frac{x^{p\beta}}{f^{pm}}\omega \sum_{i \geq 0} \binom{-m}{i} \left(\frac{\sigma(f) - f^p}{f^p}\right)^i$$

3. Write the approximation in terms of basis elements, i.e., apply the reduction algorithm

A sparse representation of Frobenius

Unfortunately, the truncation of the series expansion to K terms

$$\sigma\left(\frac{x^\beta}{f^m}\omega\right) \approx p^n \frac{x^{p\beta}\omega}{f^{pm}} \sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i$$

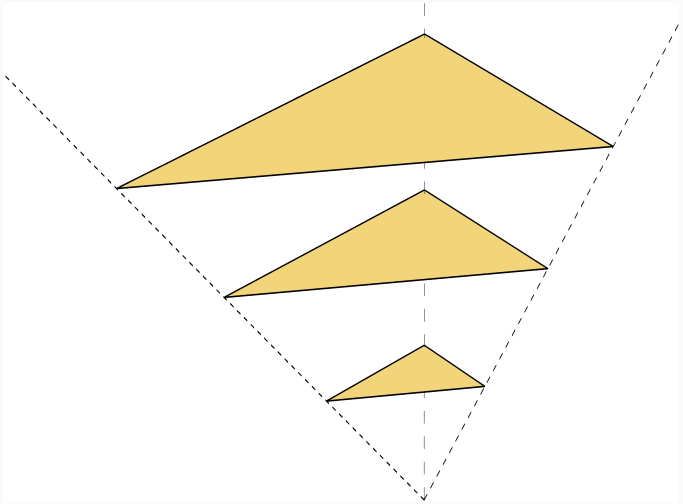
involves dense polynomials of degree $p(K-1)$ in n variables, and thus an unavoidable factor of p^n in the runtime.

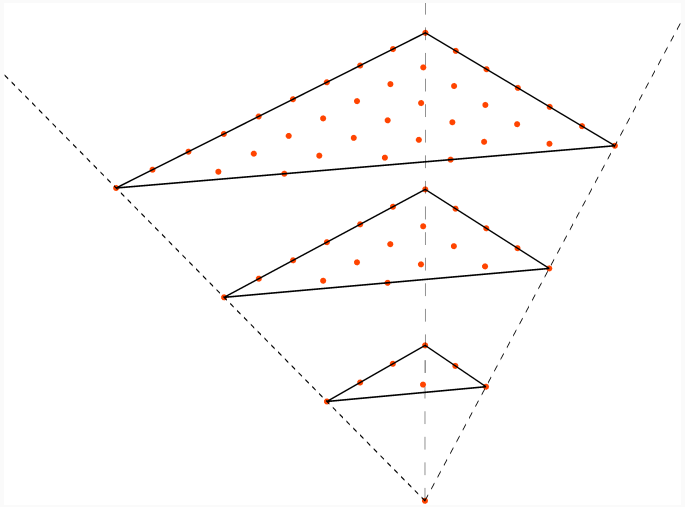
But there is another way...

$$\begin{aligned}
\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i &= \sum_{i=0}^{K-1} \binom{-m}{i} f^{-pi} \sum_{j=0}^{i} (-1)^{i-j} \binom{i}{j} \sigma(f)^j f^{p(i-j)} \\
&= \sum_{j=0}^{K-1} \binom{-m}{j} \sigma(f)^i f^{-p(m+j)} \sum_{i=j}^{K-1} \binom{m+i-1}{m+j-1} \\
&= \sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}
\end{aligned}$$

Schematically

Abbott–Kedlaya–Roe	vs	C.–Harvey–Kedlaya
$\sum_{i=0}^{K-1} \binom{-m}{i} \left(\frac{\sigma(f)-f^p}{f^p}\right)^i$		$\sum_{i=0}^{K-1} \binom{-m}{i} \binom{m+K-1}{K-i-1} \sigma(f)^i f^{-p(m+i)}$
$(pdK)^{n+O(1)}$ terms		$(dK)^{n+O(1)}$ terms





$\rho : P_{\ell+1} \longmapsto P_\ell$	$\pi : P_n \longmapsto P_n$
$\ell \frac{g\omega}{f^{\ell+1}} \equiv \frac{\rho(g)\omega}{f^\ell}$	$\ell x^{\alpha+\beta} \frac{g\omega}{f^{\ell+1}} \equiv x^\beta \frac{\pi(g)\omega}{f^\ell},\ x^\alpha \in P_1$

Generic algorithm – C.–Harvey–Kedlaya

$$H^n_{\mathrm{dR}}(U) \xrightarrow[\mathrm{id}]{\sim} H^{\dagger,n}(U_{\mathbb{F}_p}), \qquad \sigma \circlearrowright H^{\dagger,n}(U_{\mathbb{F}_p})$$

1. Compute $\left\{ \frac{x^\beta}{f^m}\omega \right\}_{\beta \in P_m^{\mathrm{int}} \setminus (J_f)_m,\, m \le n}$ a monomial basis for $H^n_{\mathrm{dR}}(U)$
2. In $H^{\dagger,n}$ compute a series approximation for

$$\sigma\left(\frac{x^\beta}{f^m}\omega\right) \approx p^n \frac{x^{p\beta}}{f^{pm}} \sum_{i=0}^{N-1} \binom{-m}{i} \binom{m+N-1}{N-i-1} \sigma(f)^i f^{-p(m+i)}$$

3. Apply reduction algorithm in H^n_{dR} to reduce to basis elements.
   - Strip out $x^{p\alpha}$, with $x^\alpha \in P_1$, by multiplying together p matrices of size $\#(n\Delta \cap L) \sim n^n \operatorname{vol} \Delta$
   - In a more convolved process, we can reduce the matrix size to $n! \operatorname{vol} \Delta$, saving a factor of $e^n \approx n^n/n!$ (e.g. $220 \rightsquigarrow 64$)

For large p, all the work is in step 3

Some Remarks

- **Complexity**
  First version of our new algorithm has complexity roughly

$$p^{1+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

  and space complexity is only

$$\log p \operatorname{vol}(\Delta)^{O(n)}.$$

  This allows us to handle examples with much larger p than any found in the literature.
- **Implementation**
  - Projective hypersurfaces (∼2014): C++ with NTL and Flint
  - Toric hypersurfaces: Sage ✓, C++ with NTL ~~underway~~ ✓

Other versions

- **Space-time tradeoff**
  We can reduce the time dependence on p to

$$p^{0.5+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

- **Average polynomial time**
  Given an hypersurface defined over $\mathbb{Q}$, we may compute the zeta functions of its reductions modulo various primes at once. The average time complexity for each prime p < N is

$$\log(N)^{4+o(1)} \operatorname{vol}(\Delta)^{O(n)}$$

  These have not been implemented yet.

Applications

Modularity

E an elliptic curve over $\mathbb{Q}$ of conductor N

What can we say about E if we know $\#E_p(\mathbb{F}_p)$ for almost all p?

If we know $\#E(\mathbb{F}_p)$ for all good primes up to $\sim \sqrt{N}$, then we can guess:

- the functional equation for $\zeta_E(s)$
- the conductor N
- local zeta function at the bad primes
- the rank of E
- the corresponding modular form
- etc...

We can also do the "same" for Abelian surfaces

We would like to do the same for K3 surfaces!

Design of K3 surfaces

To have some hope to develop similar toolkit for K3 surfaces, we first need to try it out in some easy examples.

Question: How can we design a K3 surfaces?

For example, if one restricts to quartic K3 surfaces then usually there is a compromise between arithmetic complexity (aka conductor) and generality, i.e.,

- surfaces with interesting invariants $\rightsquigarrow$ huge conductor
- surfaces with small conductor $\rightsquigarrow$ trivial examples

Approach: Use Reid's list to expand our search to toric hypersurfaces.

Design of K3 surfaces

Example

I would like a nice equation for a K3 surface such that

$$\operatorname{Pic} X = D_9 \oplus D_5 \oplus U$$

$$X : x^2z + xw^4 + y^4 + yw^5 + z^5 + z^2w^4 = 0 \text{ in } \mathbb{P}(8,5,4,3)$$

$$\det(1 - t \operatorname{Frob}_p | T_X) = p^6t^6 - 14662p^4t^5 - 31559p^3t^4 - 5620p^2t^3 \ldots$$

$$\text{with } p = 49999$$

Other Applications/Questions

- **Picard Jumps** [C. – Tschinkel, C.–Elsenhans–Jahnel]
  How often $\operatorname{rk} \mathrm{NS}(\overline{X}_p) > \min_q \operatorname{rk}(\mathrm{NS}\,\overline{X}_q)$?
- **Numerical evidence for Sato–Tate conjecture**
  How are the eigenvalues of Frobenius acting on T_X equidistributed?
  What are the possible Sato–Tate groups?
- **Computing** $\mathrm{NS}(X)$**?**
  Can we lift $\mathrm{NS}(X_p) \cap H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$ to $\mathbb{Q}$ using the Frobenius approximation?
- **You tell me**

Questions?