pre-Talk: Effective obstruction to lifting algebraic classes from positive characteristic

Edgar Costa (MIT)

Simons Collab. on Arithmetic Geometry, Number Theory, and Computation

April 19, 2021

Columbia-CUNY-NYU joint number theory seminar

Slides available at `researchseminars.org`

Joint work with Davide Lombardo, Nicolas Mascot, Jeroen Sijsling, Emre Sertöz, and John Voight.

Riemann zeta function

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

- 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
  Visualizing the Riemann zeta function and analytic continuation:
  `https://www.youtube.com/watch?v=sD0NjbwqlYw`
- $\zeta(s)$ still keeps secret many of its properties

Hasse–Weil zeta functions

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

$$Z_X(s) := \prod_p Z_{X_p}(p^{-s})$$

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

$$Z_{X_p}(t) := exp\left(\sum_{i\geq 0} \#X_p(\mathbb{F}_{p^i})\frac{t^i}{i}\right) \in \mathbb{Q}(t)$$

Example: $X = \{\bullet\}$, a point, then $Z_{\{\bullet\}}(s) = \zeta(s)$

- What arithmetic properties of X can we read from $Z_{X_p}(s)$?
- $Z_{X_p}(t)$ obeys a functional equation and satisfies the Riemann hypothesis!
- What about $Z_X(s)$?

Elliptic curves

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

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

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

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

- $a_p \rightsquigarrow$ arithmetic information about $E_p \rightsquigarrow E$.
- Modularity theorem $\implies$ L_E satisfies a functional equation
- Birch–Swinnerton-Dyer conjecture predicts $\mathsf{ord}_{s=1} L_E(s) = \mathsf{rk}(E)$.

$\zeta(s)$ vs $Z_X(s)$

We always expect $Z_X(s)$ 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 $Z_{X_p}(t)$ for an arbitrary X

Problem

Given an *explicit* description of X, compute

$$Z_{X_p}(t) := exp\left(\sum_{i\geq 0} \#X_p(\mathbb{F}_{p^i})\frac{t^i}{i}\right) \in \mathbb{Q}(t)$$

The zeta function problem

Let X be a smooth variety over a finite field $\mathbb{F}_q$ of characteristic p, consider

$$Z_X(t) := exp\left(\sum_{i\geq 1} \#X(\mathbb{F}_{q^i})\frac{t^i}{i}\right)$$

Problem

Compute Z_X from an *explicit* description of X.

Theoretically this is “trivial”.
The degree of Z_X is bounded by the geometry of X, and we can then enumerate $X(\mathbb{F}_{q^i})$ for enough i to pinpoint Z_X.

This approach is only practical for very few classes of varieties, e.g., low genus curves and p small.

“Real life” applications

- Cryptography/Coding Theory, often interested in $\#X(\mathbb{F}_q)$
- Testing isomorphism/isogeny
- Computing $\mathsf{End}(A)$ for A an abelian variety.
  $\rightsquigarrow$ A couple of $Z_{A_p}(t)$ usually give away the shape of $\mathsf{End}(A)$.
  We will see this in the first half of the main talk.
- Computing Picard number for surfaces
  We will see this in the second half of the main talk.
- Testing the speciality of a cubic fourfold
- Computing L-functions and their special values, e.g.:
  - Birch–Swinnerton-Dyer conjecture $\rightsquigarrow \mathsf{rk}(A)$
  - searching for Langlands correspondences
- Arithmetic statistics
  - Sato–Tate (Click to see histograms: g1 g2 g3)
  - Lang–Trotter

The zeta function problem

Let $X \subset \mathbb{P}^n$ be a smooth **hypersurface** over a finite field $\mathbb{F}_q$ of characteristic p, consider

$$Z_X(t) := exp\left(\sum_{i\geq 1} \#X(\mathbb{F}_{q^i})\frac{t^i}{i}\right) = Q(t)^{(-1)^n}\prod_{i=0}^{n-1}\frac{1}{1-q^i t},$$

Problem

Compute Z_X from an *explicit* description of X.

Some data points:

- Elliptic curve, degree 3 polynomial in $\mathbb{P}^2$, $\deg Q = 2$
- Smooth plane curve, degree 4 polynomial in $\mathbb{P}^2$, $\deg Q = 6$
- K3 surface, degree 4 polynomial in $\mathbb{P}^3$, $\deg Q = 21$
- degree 5 polynomial in $\mathbb{P}^3$, $\deg Q = 52$
- Calabi-Yau 3fold, degree 5 polynomial in $\mathbb{P}^4$, $\deg Q = 204$

Attack the problem with algebraic topology

If rewrite

$$\#X(\mathbb{F}_{q^a}) = \{x \in \mathbb{F}_{q^a} : f(x) = 0\} = \{x \in X(\mathbb{F}_p{}^{\mathsf{al}}) : \mathsf{Frob}^a(x) = x\}$$

then we can use Lefschetz fixed point theorem:

- X be a nice space;
- H^* be a **nice** cohomology theory;
- $F : X \to X$ be a nice map.

then $\#\{x \in X : F(x) = x\} = \sum_i (-1)^i \operatorname{tr}\left(F^* | \mathsf{H}^i(X)\right)$.

Taking $\sigma^* = q$-th power Frobenius we get

$$Z_{Z_{\mathbb{F}_q}}(t) = \prod_i \det(1 - t\sigma | \mathsf{H}^i(X))^{(-1)^{i+1}} = \det(1 - q^{-1}t\sigma | \mathsf{H}^n(\mathbb{P}^n \backslash X))^{(-1)^n} \prod_{i=0}^{n-1} \frac{1}{1 - q^i t}$$

Common Approaches

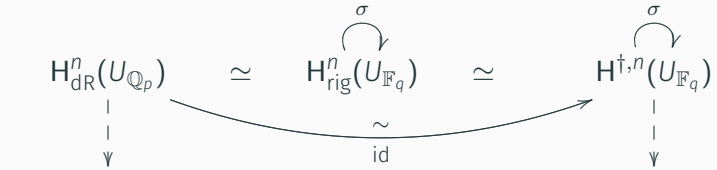
- ℓ-adic: by computing the action of Frobenius on mod-ℓ étale cohomology for many ℓ.
  - We need to have an effective *description* of the cohomology.
  - E.g.: for abelian varieties we have Schoof-Pila's method
    However, only practical if $g \leq 2$ or some extra structure is available.
- p-adic:
  - Dwork cohomology: based on Dwork's p-adic analytic proof that $Z_X(t) \in \mathbb{Q}(t)$
    One usually gets Frob by solving a p-adic differential equation
  - Monsky–Washnitzer cohomology: de Rham cohmology for smooth affine X.
    Achieves a striking balance between **practicality** and **generality**.
    Originally developed for hyperelliptic curves by Kedlaya.
    Now, we can handle nondegenerate hypersurfaces in toric varieties.
    We do this by computing a matrix representing the action of σ in $\mathrm{H}^{n,\dagger}(\mathbb{P}^n \backslash X)$
    with enough of p-adic precision to deduce

$$Q(t) = \det(1 - q^{-1} t \,\mathrm{Frob} \,|\mathrm{H}^{n,\dagger}(\mathbb{P}^n \backslash X)) \in 1 + \mathbb{Z}[t].$$

Overall picture

Goal

Compute the matrix representing the action of σ in $\mathrm{H}^{n,\dagger}(U)$ with enough p-adic precision, where $U := \mathbb{P}^n \backslash X$.



At the end of the day, we obtain an algorithm that runs in quasi-linear time in p.

“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 $\mathbb{P}^3$

$$X : f(x, y, z, w) = 0, \quad \deg f = 4$$

  e.g. Fermat quartic surface $x^4 + y^4 + z^4 + w^4 = 0$.
- double cover of $\mathbb{P}^2$ branched over a sextic curve $\mathbb{P}(3, 1, 1, 1)$

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

  e.g. Fermat like surface $w^2 = x^6 + y^6 + z^6$.
- Kummer surfaces, $\mathsf{Kum}(A) := \widetilde{A/\pm}$, 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 ⇒ 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 "give" 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 ⇒ 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 "give" 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 $\mathsf{KS}(X)$ of dimension $\leq 2^{19}$, such that $\mathrm{H}^2(X,\mathbb{Z}) \subset \mathrm{H}^2(\mathsf{KS}(X)^2,\mathbb{Z})$ as Hodge structures.
- a weaker analogue of Honda–Tate theory for abelian varieties.
- categorical description of ordinary K3 surfaces over a finite field

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

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

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

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

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

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

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

Picard lattice – over finite fields

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

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

From $\chi(t)$ we may deduce $\rho(X_{\mathbb{F}_{p^r}})$ for any r, via Tate conjecture (known for K3):

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

It implies that cohomological cycles invariant under Frobenius are algebraic.

Write

$$\chi(t) = h(t) \prod_i \Phi_{k_i}(pt)^{\gamma_i}$$

where $\Phi_{k_i}(t) \in \mathbb{Z}[t]$ is the k_i-th cyclotomic polynomial, then

$$\rho(X_{\mathbb{F}_{p^r}}) = \sum_{k_i | r} \deg \Phi_{k_i}.$$

Effective obstruction to lifting algebraic classes from positive characteristic

Edgar Costa (MIT)

Simons Collab. on Arithmetic Geometry, Number Theory, and Computation

April 19, 2021

Columbia-CUNY-NYU joint number theory seminar

Slides available at `researchseminars.org`

Joint work with Davide Lombardo, Nicolas Mascot, Jeroen Sijsling, Emre Sertöz, and John Voight.

Elliptic curves

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

- What can we say about $\#E(\mathbb{F}_p)$ for an arbitrary p?
- Given $\#E(\mathbb{F}_p)$ for many p, what can we say about E?

$\rightsquigarrow$ studying the **statistical** properties $\#E(\mathbb{F}_p)$.

Hasse's bound

Theorem (Hasse)

$$a_p := p + 1 - \#E(\mathbb{F}_p) \in [-2\sqrt{p}, 2\sqrt{p}]$$

Alternatively, we could also have written the formula above as

$$\begin{aligned} \#E(\mathbb{F}_p) &= L(1), \text{ where} \\ L(T) &= 1 - a_p T + pT^2 = \det(1 - T\,\mathrm{Frob}_p \,|\mathrm{H}^1(E)) \\ a_p &:= \operatorname{tr} \mathrm{Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}] \end{aligned}$$

Question

What can we say about the error term $a_p/\sqrt{p}$ as $p \to \infty$?

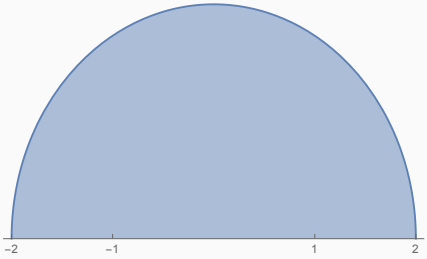
Two types of elliptic curves

$$a_p := p + 1 - \#E_p = \operatorname{tr} \mathrm{Frob}_p \in [-2\sqrt{p}, 2\sqrt{p}]$$

There are two limiting distributions for $a_p/\sqrt{p}$

non-CM

$\mathrm{End}_{\mathbb{Q}}\, E_{\mathbb{Q}^{\mathrm{al}}} = \mathbb{Q}$



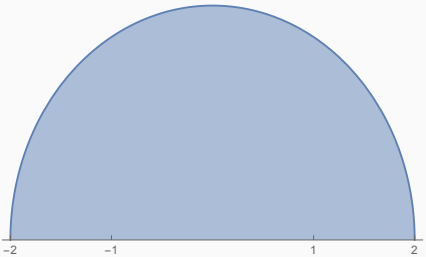
CM

$\mathrm{End}_{\mathbb{Q}}\, E_{\mathbb{Q}^{\mathrm{al}}} = \mathbb{Q}(\sqrt{-d})$

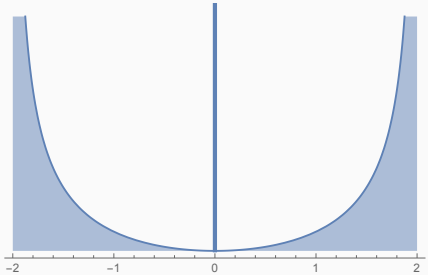
This is know as the Sato–Tate conjecture (a theorem for elliptic curves over $\mathbb{Q}$).

How to distinguish between the two types?

non-CM



CM by $\mathbb{Q}(\sqrt{-d})$



- $\mathrm{End}_{\mathbb{Q}} E_{\mathbb{Q}^{\mathrm{al}}} \hookrightarrow \mathrm{End}_{\mathbb{Q}} E_{\mathbb{F}_p^{\mathrm{al}}} \hookleftarrow \mathbb{Q}(\mathrm{Frob}_p)$
- $a_p \neq 0 \bmod p \iff \mathrm{End}_{\mathbb{Q}} E_{\mathbb{F}_p^{\mathrm{al}}}$ is a quadratic field
- If E has CM, then $a_p \equiv 0 \bmod p \Leftrightarrow p$ inert or ramified in $\mathbb{Q}(\sqrt{-d})$

  $$\Leftrightarrow \mathbb{Q}(\sqrt{-d}) \subsetneq \mathrm{End}_{\mathbb{Q}} E_{\mathbb{F}_p^{\mathrm{al}}}$$
- If E is non-CM, then $\mathrm{End}_{\mathbb{Q}} E_{\mathbb{F}_p^{\mathrm{al}}} \cap \mathrm{End}_{\mathbb{Q}} E_{\mathbb{F}_q^{\mathrm{al}}} \simeq \mathbb{Q}$ with prob. 1

Examples

$E : y^2 + y = x^3 - x^2 - 10x - 20$ (11.a2)

- $\mathrm{End}_{\mathbb{Q}} E_{\mathbb{F}_2^{\mathrm{al}}} \simeq \mathbb{Q}(\sqrt{-1})$
- $\mathrm{End}_{\mathbb{Q}} E_{\mathbb{F}_3^{\mathrm{al}}} \simeq \mathbb{Q}(\sqrt{-11})$

$\Rightarrow \mathrm{End}_{\mathbb{Q}} E_{\mathbb{Q}^{\mathrm{al}}} = \mathbb{Q}$

$E : y^2 + y = x^3 - 7$ (27.a2)

- $p = 2 \bmod 3 \Rightarrow a_p = 0 \Rightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}}$ is a Quaternion algebra
- $p = 1 \bmod 3 \Rightarrow \mathrm{End}_{\mathbb{Q}} E_p^{\mathrm{al}} \simeq \mathbb{Q}(\sqrt{-3})$
- $\rightsquigarrow \mathrm{End}_{\mathbb{Q}} E^{\mathrm{al}} = \mathbb{Q}(\sqrt{-3})$

Genus 2 curves/Abelian surfaces

There are 6 possibilities for the real endomorphism algebra:

Abelian surface	$\mathrm{End}_{\mathbb{R}} A^{\mathrm{al}}$
square of CM elliptic curve	$\mathrm{M}_2(\mathbb{C})$
• QM abelian surface • square of non-CM elliptic curve	$\mathrm{M}_2(\mathbb{R})$
• CM abelian surface • product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$
• RM abelian surface • product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$
generic abelian surface	$\mathbb{R}$

Can we distinguish between these by looking at A mod p?

Endomorphism algebra over finite fields

Over finite fields the Frobenius polynomial

$$\det(1 - t\,\mathrm{Frob}\,|\mathrm{H}^1(A))$$

uniquely determines the isogeny class of A and $\mathrm{End}_{\mathbb{Q}} A$ up to isomorphism.

For example, endomorphisms corresponds to a nontrivial graphs in $A \times A$, up to numerical equivalency, i.e.,

$$\mathrm{End}(A) \simeq \mathrm{DC}(A \times A) \subset \mathrm{H}^1(A) \otimes \mathrm{H}^1(A).$$

Thus, Tate conjectures, proved for abelian varieties by Tate, tells us

$$\mathrm{rk}\,\mathrm{End}(A) = \dim \ker(\mathrm{Frob} - p|\mathrm{H}^1(A) \otimes \mathrm{H}^1(A)).$$

Therefore, by factoring $\det(1 - t\,\mathrm{Frob}\,|\mathrm{H}^1(A) \otimes \mathrm{H}^1(A))$ we obtain $\mathrm{rk}\,\mathrm{End}(A_{\mathbb{F}_{q^r}}), \quad \forall_{r \geq 1}$.

Tate also showed that $\mathbb{Q}(\mathrm{Frob})$ is the center of $\mathrm{End}_{\mathbb{Q}} A$

Endomorphism algebra over finite fields

Theorem (Tate)

$$\operatorname{rk}\operatorname{End}(A) = \dim\ker(\mathrm{Frob} - p | \mathrm{H}^1(A) \otimes \mathrm{H}^1(A))$$

Example

$A/\mathbb{F}_5$ and $\det(1 - t\,\mathrm{Frob}\,|\mathrm{H}^1(A)) = 1 - 2T^2 + 25T^4$

- $\det(1 - t\,\mathrm{Frob}\,|\mathrm{H}^1(A) \otimes \mathrm{H}^1(A)) = (1-5T)^4(1+5T)^4(1-2T+25T^2)^2(1+2T+25T^2)^2$
- $\operatorname{rk}\operatorname{End} A = 4$ and thus $\operatorname{End} A = \mathbb{Q}(\mathrm{Frob}) = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$
- all endomorphisms are defined over $\mathbb{F}_{25}$, and
- $A_{\mathbb{F}_{25}}$ is isogenous to a square of an elliptic curve given by $1 - 2T + 25T^2$
- $\operatorname{End}_{\mathbb{Q}} A_{\mathbb{F}_{25}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

Example continued, now over $\mathbb{Q}$

$$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.d.524288.1)$$

For $p = 5$, $\det(1 - T\,\mathrm{Frob}_5 \,|\mathrm{H}^1(A)) = 1 - 2T^2 + 25T^4$, and:

- all endomorphisms of $A_{\mathbb{F}_5^{\mathrm{al}}}$ are defined over $\mathbb{F}_{25}$
- $\det(1 - T\,\mathrm{Frob}_5^2 \,|\mathrm{H}^1(A)) = (1 - 2T + 25T^2)^2$
- over $\mathbb{F}_{25}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}}\, A_{\mathbb{F}_5^{\mathrm{al}}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$

For $p = 7$, $\det(1 - T\,\mathrm{Frob}_7 \,|\mathrm{H}^1(A)) = 1 + 6T^2 + 49T^4$, and:

- all endomorphisms of $A_{\mathbb{F}_7^{\mathrm{al}}}$ are defined over $\mathbb{F}_{49}$
- $\det(1 - T\,\mathrm{Frob}_7^2 \,|\mathrm{H}^1(A)) = (1 + 6T + 49T^2)^2$
- $\mathbb{F}_{49}$ is isogenous to a square of an elliptic curve
- $\mathrm{End}_{\mathbb{Q}}\, A_{\mathbb{F}_7^{\mathrm{al}}} \simeq M_2(\mathbb{Q}(\sqrt{-10}))$

$\Rightarrow \mathrm{End}_{\mathbb{R}}\, A^{\mathrm{al}} \neq M_2(\mathbb{C})$

Same Frobenius polynomials, different approach

We could have looked at the Néron–Severi lattice.

$$\mathrm{NS}(A_{\mathbb{Q}^{\mathrm{al}}}) \hookrightarrow \mathrm{NS}(A_{\mathbb{F}_p^{\mathrm{al}}})$$

- $\mathrm{rk}\,\mathrm{NS}(A_{\mathbb{Q}^{\mathrm{al}}}) \in \{1, 2, 3, 4\}$
- $\mathrm{rk}\,\mathrm{NS}(A_{\mathbb{F}_p^{\mathrm{al}}}) \in \{2, 4, 6\}$

Example

- $\mathrm{rk}\,\mathrm{NS}(A_{\mathbb{F}_5^{\mathrm{al}}}) = \mathrm{rk}\,\mathrm{NS}(A_{\mathbb{F}_7^{\mathrm{al}}}) = 4$
- $\left.\begin{array}{l} \mathrm{disc}\,\mathrm{NS}(A_{\mathbb{F}_5^{\mathrm{al}}}) = -6 \bmod \mathbb{Q}^{\times 2} \\ \mathrm{disc}\,\mathrm{NS}(A_{\mathbb{F}_7^{\mathrm{al}}}) = -10 \bmod \mathbb{Q}^{\times 2} \end{array}\right\} \Rightarrow \mathrm{rk}\,\mathrm{NS}(A_{\mathbb{Q}^{\mathrm{al}}}) \leq 3$

By a theorem of Charles, we know that at some point this method will attain a tight upper bound for $\mathrm{rk}\,\mathrm{NS}\,A_{\mathbb{Q}^{\mathrm{al}}}$.

Real endomorphisms algebras and Picard numbers

Abelian surface	$\mathrm{End}_{\mathbb{R}} A^{\mathrm{al}}$	$\mathrm{rk}\,\mathrm{NS}(A^{\mathrm{al}})$
square of CM elliptic curve	$\mathrm{M}_2(\mathbb{C})$	4
• QM abelian surface • square of non-CM elliptic curve	$\mathrm{M}_2(\mathbb{R})$	3
• CM abelian surface • product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$	2
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$	2
• RM abelian surface • product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$	2
generic abelian surface	$\mathbb{R}$	1

Higher genus

- K be a numberfield such that $\mathsf{End}\, A_K = \mathsf{End}\, A^{\mathsf{al}}$
- $A_K \sim \prod_{i=1}^{t} A_i^{n_i}$, A_i simple and unique up to isogeny (over K),
- $B_i := \mathsf{End}_{\mathbb{Q}}\, A_i$ central simple algebra over $L_i := Z(B_i)$,
- $\mathsf{dim}_{L_i}\, B_i = e_i^2$,
- $\mathsf{End}_{\mathbb{Q}}\, A_K = \prod_{i=1}^{t} M_{n_i}(B_i)$

Theorem (C–Mascot–Sijsling–Voight, C–Lombardo–Voight)

If Mumford–Tate conjecture holds for A, then we can compute

- t
- $\{(e_i n_i, n_i \dim A_i)\}_{i=1}^{t}$
- L_i

This is practical and we just need two well chosen Frobenius polynomials.
Without Mumford–Tate conjecture we only obtain upper bounds.

Proof idea in the isotypical setting

- K be a numberfield such that $\mathsf{End}\, A_K = \mathsf{End}\, A^{\mathsf{al}}$
- $A_K \sim A_{\mathrm{rad}}^n$, A_{rad} geometrically simple,
- $B := \mathsf{End}_{\mathbb{Q}}\, A_{\mathrm{rad}}$ central simple algebra over $L := Z(B)$,
- $\dim_L B = e^2$,

Then we claim we can compute en and L.

Zywina showed that for $\mathfrak{p}$ in a set of density 1 in K we have

$$A_{\mathbb{F}_{\mathfrak{p}}} \sim C^{en},$$

with C geometrically simple, and thus we may effectively compute en.

Furthemore, for $\mathfrak{q}$ in a set of density 1 depending on $\mathfrak{p}$, we have

$$L = \mathbb{Q}(\mathsf{Frob}_{\mathfrak{p}}) \cap \mathbb{Q}(\mathsf{Frob}_{\mathfrak{q}})$$

Zywina has recently refined our method to compute the Sato–Tate group of A_K.

Real endomorphisms algebras, $\{e_i n_i, n_i \dim A_i\}_{i=1}^t$, and $\dim L_i$

Recall, $A_K \sim \prod_{i=1}^t A_i^{n_i}$, $L_i = Z(\mathsf{End}_{\mathbb{Q}} A_i)$, and $\dim_{L_i} \mathsf{End}_{\mathbb{Q}} A_i = e_i^2$

Abelian surface	$\mathsf{End}_{\mathbb{R}} A^{\mathsf{al}}$	tuples	$\dim L_i$
square of CM elliptic crv	$\mathrm{M}_2(\mathbb{C})$	$\{(2,2)\}$	2
• QM abelian surface • square of non-CM elliptic crv	$\mathrm{M}_2(\mathbb{R})$	$\{(2,2)\}$	1
• CM abelian surface	$\mathbb{C} \times \mathbb{C}$	$\{(1,2)\}$	4
• product of CM elliptic crv		$\{(1,1),(1,1)\}$	2, 2
CM $\times$ non-CM elliptic crvs	$\mathbb{C} \times \mathbb{R}$	$\{(1,1),(1,1)\}$	2, 1
• RM abelian surface	$\mathbb{R} \times \mathbb{R}$	$\{(1,2)\}$	2
• prod. of non-CM elliptic crv		$\{(1,1),(1,1)\}$	1, 1
generic abelian surface	$\mathbb{R}$	$\{(1,1)\}$	1

Example continued

$$A = \mathrm{Jac}(y^2 = x^5 - x^4 + 4x^3 - 8x^2 + 5x - 1) \quad (262144.\mathrm{d}.524288.1)$$

- $\mathrm{End}_{\mathbb{Q}} A_{\mathbb{F}_3^{\mathrm{al}}} \simeq M_2(\mathbb{Q}(\sqrt{-3}))$
- $\mathrm{End}_{\mathbb{Q}} A_{\mathbb{F}_5^{\mathrm{al}}} \simeq M_2(\mathbb{Q}(\sqrt{-6}))$
- $\Rightarrow \mathrm{End}_{\mathbb{R}} A_{\mathbb{Q}^{\mathrm{al}}} \neq M_2(\mathbb{C})$

Question

Write $B := \mathrm{End}_{\mathbb{Q}} A_{\mathbb{Q}^{\mathrm{al}}}$ and assume that B is a quaternion algebra.
Can we guess $\mathrm{disc}\, B$?

If ℓ is ramified in $B \Rightarrow \ell$ cannot split in $\mathbb{Q}(\mathrm{Frob}_p)$

- $5, 13, 17 \nmid \mathrm{disc}\, B$, as they split in $\mathbb{Q}(\sqrt{-3})$
- $7, 11 \nmid \mathrm{disc}\, B$, as they split in $\mathbb{Q}(\sqrt{-6})$

We can rule out all the primes except 2 and 3 (up to some bnd).
Indeed, $\mathrm{disc}\, B = 6$.

Picard numbers of surfaces over $\mathbb{Q}^{\mathrm{al}}$

Let $X := Z(f) \subset \mathbb{P}^3_{\mathbb{Q}}$ be a smooth surface of degree d.

Picard group $\mathsf{Pic}(X_{\mathbb{Q}^{\mathrm{al}}}) \simeq \mathbb{Z}^\rho$ and Picard number $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) := \mathsf{rk}\,\mathsf{Pic}(X_{\mathbb{Q}^{\mathrm{al}}})$

- $d = 2$: $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) = 2$ and $X_{\mathbb{Q}^{\mathrm{al}}} \simeq \mathbb{P}^1 \times \mathbb{P}^1$
- $d = 3$: $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) = 7$ and $X_{\mathbb{Q}^{\mathrm{al}}} \simeq \mathsf{Bl}_{p_1,\dots,p_6}\,\mathbb{P}^2$
- $d = 4$: $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) \in \{1, 2, \dots, 20\}$ and X is a K3 surface
- $d = 5$: $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) \in \{1, 2, \dots, 45\}$

In general, $\mathsf{Pic}(X_{\mathbb{Q}^{\mathrm{al}}}) \simeq \mathsf{H}^{1,1}(X_{\mathbb{C}}) \cap \mathsf{H}^2(X_{\mathbb{C}}, \mathbb{Z}) \subset \mathsf{H}^2(X_{\mathbb{C}}, \mathbb{Z})$ and $1 \leq \rho(X_{\mathbb{Q}^{\mathrm{al}}}) \leq h_{1,1}$.

Problem

Compute $\rho(X_{\mathbb{Q}^{\mathrm{al}}})$ from $f \in \mathbb{Z}[x, y, z, w]$

In principle, solved, if given the Tate conjecture.

[Charles, Poonen–Testa–van Luijk, Hassett–Kresch–Tschinkel, Shioda, Lairez–Sertöz]

Picard lattice – over finite fields

Tate conjecture

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

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

One may deduce χ by naively computing $\#X(\mathbb{F}_{p^m})$ for $m \leq b_2/2 + 1$.

Since Frob_p acts semisimply, we have:

$$\rho\big(X_{\mathbb{F}_{p^n}}\big) = \#\{z : \chi(1/z) = 0 \text{ and } z^n = p^n\}.$$

Note: $\rho(X_{\mathbb{F}_p^{\mathrm{al}}}) \equiv b_2 \bmod 2$

For $p > 7$ computing $\chi(t)$ by naive point counting is not practical.

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

Reduction to finite characteristic

Take $f \in \mathbb{Z}[x, y, z, w]$ and $X := Z(f) \subset \mathbb{P}^3_{\mathbb{Q}}$.

We may consider the surface $X_{\mathbb{F}_p} := Z(f \bmod p) \subset \mathbb{P}^3(\mathbb{F}_p)$.

Theorem

If X and $X_{\mathbb{F}_p}$ are smooth then the specialization map is injective

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

Goal

For a given f and p, improve the inequality $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) \leq \rho(X_{\mathbb{F}_p^{\mathrm{al}}})$.

Parity reasons might already force the inequality to not be sharp.

Endomorphisms of the transcendental lattice can complicate things even further.

Improving upper bounds — using two specializations [van Luijk]

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

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

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

then

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

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

Under the right conditions we know that this method will not succeed to give a tight upper bound (parity + endomorphisms of the transcendental lattice).

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

Elsenhans–Jahnel showed that the specialization map

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

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

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

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

1. compute $\mathrm{Pic}(X_{\overline{\mathbb{F}_p}})$
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 $\mathrm{Pic}(X_{\overline{\mathbb{F}_p}})$ and if the obtained estimates are low.

Reduction to finite characteristic

Take $f \in \mathbb{Z}[x, y, z, w]$ and $X := Z(f) \subset \mathbb{P}^3_{\mathbb{Z}}$.

We may consider the surface $X_{\mathbb{F}_p} := Z(f \bmod p) \subset \mathbb{P}^3(\mathbb{F}_p)$.

Theorem

If X and $X_{\mathbb{F}_p}$ are smooth then $\rho(X_{\mathbb{Q}^{\mathsf{al}}}) = \rho(X_{\mathbb{Q}_p^{\mathsf{al}}}) \leq \rho(X_{\mathbb{F}_p^{\mathsf{al}}})$.

Goal

For a given f and p, improve the inequality above.

Idea, try to lift algebraic cycles (curves) from $\mathbb{F}_p^{\mathsf{al}}$ to $\mathbb{Q}_p^{\mathsf{al}}$.

We will do this by considering the thickenings

$$Z(f \bmod p^i) \subset P^3_{\mathbb{Z}/(p)^i} \quad i = 1, 2, \ldots$$

1st ingredient: Cohomology

For simplicity, assume that all curve classes are defined over the base field, i.e.,

$$\rho(X) = \rho(X_{\mathbb{Q}^{\mathrm{al}}}) \quad \text{and} \quad \rho(X_{\mathbb{F}_p}) = \rho(X_{\mathbb{F}_p^{\mathrm{al}}})$$

Over characteristic zero we have:

- $\mathrm{H}^2_{\mathrm{dR}}(X/\mathbb{Q}) = \mathrm{F}^0 \supset \mathrm{F}^1 \supset \mathrm{F}^2$, the Hodge filtration
- $\mathrm{Pic}(X) \hookrightarrow \mathrm{F}^1(X)$
- For $d = 4$, $\dim \mathrm{F}^i(X) = 22, 21, 1$.

Over characteristic p we have:

- $\mathrm{Pic}(X_{\mathbb{F}_p}) \hookrightarrow \mathrm{H}^2_{\mathrm{crys}}(X_{\mathbb{F}_p}/\mathbb{Z}_p) \otimes \mathbb{Q}_p \simeq \mathrm{H}^2_{\mathrm{dR}}(X/\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{Q}_p = \mathrm{F}^0_{\mathbb{Q}_p} \supset \mathrm{F}^1_{\mathbb{Q}_p} \supset \mathrm{F}^2_{\mathbb{Q}_p}$

Theorem (Berthelot, Ogus 1978; Raynaud 1979)

$$\mathrm{Pic}(X)_{\mathbb{Q}} = \mathrm{Pic}(X_{\mathbb{F}_p})_{\mathbb{Q}} \cap \mathrm{F}^1_{\mathbb{Q}_p}$$

2nd ingredient: Approximate $\mathrm{Pic}(X_{\mathbb{F}_p}) \otimes_{\mathbb{Z}} \mathbb{Q}_p$

Via the isomorphism $\mathrm{H}^2_{\mathrm{crys}}(X_{\mathbb{F}_p}/\mathbb{Z}_p) \otimes \mathbb{Q}_p \simeq \mathrm{H}^2_{\mathrm{dR}}(X/\mathbb{Q})$, we have

$$\mathrm{Frob}_p : \mathrm{H}^2_{\mathrm{dR}}(X/\mathbb{Q}_p) \to \mathrm{H}^2_{\mathrm{dR}}(X/\mathbb{Q}_p).$$

Tate conjecture

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

By computing a p-adic approximation of Frob_p, we may compute a p-adic approximation of

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

thus

$$\dim_{\mathbb{Q}} \mathrm{Pic}(X) \leq \dim_{\mathbb{Q}_p} \ker \pi.$$

By picking a basis that respects the Hodge filtration, the map

$$\mathrm{H}^2_{\mathrm{dR}}(X/\mathbb{Q}_p) \to \mathrm{H}^2_{\mathrm{dR}}(X/\mathbb{Q}_p)/\,\mathrm{F}^1_{\mathbb{Q}_p}$$

is a coordinate projection.

Abelian surface

$A = \mathrm{Jac}(y^2 = 4x^5 - 36x^4 + 56x^3 - 76x^2 + 44x - 23)$

$$\mathrm{Frob}\,|_{\mathsf{H}^1_{\mathrm{dR}}(A/\mathbb{Q}_p)} \equiv \begin{pmatrix} 31\cdot 482 & 31\cdot 284 & 16241 & 3075 \\ 31\cdot 386 & 31\cdot 886 & 2644 & 12126 \\ 31\cdot 284 & 31\cdot 659 & 6336 & 9750 \\ 31\cdot 194 & 31\cdot 876 & 27408 & 10841 \end{pmatrix} \pmod{31^3},$$

$$L(t) = \det(1 - t\,\mathrm{Frob}\,|\mathsf{H}^1) = 1 - 3t + 14t^2 - 93t^3 + 961t^4.$$

From this we deduce $\mathrm{Frob}\,|_{\mathsf{H}^2_{\mathrm{dR}}(A/\mathbb{Q}_p)}$ and

$$\det(1 - t31^{-1}\,\mathrm{Frob}\,|\mathsf{H}^2_{\mathrm{dR}}(A/\mathbb{Q}_p)) = (t-1)^2(31t^4 + 48t^3 + 43t^2 + 48t + 31)/31$$

Thus, $\rho\big(A_{\mathbb{F}_p^{\mathrm{al}}}\big) = 2$.

Since the basis of H^1 respects the Hodge filtration, the induced basis in H^2 will also respect it.

Abelian Surface

$A = \mathrm{Jac}(y^2 = 4x^5 - 36x^4 + 56x^3 - 76x^2 + 44x - 23)$

$$\det(1 - t31^{-1}\,\mathrm{Frob}\,|\mathrm{H}^2_{\mathrm{dR}}(A/\mathbb{Q}_p)) = (t-1)^2(31t^4 + 48t^3 + 43t^2 + 48t + 31)/31$$

Thus, $\rho(A_{\mathbb{F}_p^{\mathrm{al}}}) = 2$.

Compute 2 eigenvectors

$$v_1 \equiv (356,\ 37,\ 831,\ 0,\ 295,\ 31) \pmod{31^2}$$
$$v_2 \equiv (4,\ 957,\ 3,\ 1,\ 0,\ 0) \pmod{31^2}.$$

The last coordinate of the vectors above gives the projection to H^2/F_1.

Therefore, $v_1 \notin F^1$ and the corresponding algebraic cycle cannot lift to $\mathbb{Q}_p$.

Thus, we improved $\mathrm{rk}\,\mathrm{NS}(A_{\mathbb{Q}^{\mathrm{al}}}) \leq 2$ to $\mathrm{rk}\,\mathrm{NS}(A_{\mathbb{Q}^{\mathrm{al}}}) \leq 1$, and therefore $\mathrm{End}(A_{\mathbb{Q}^{\mathrm{al}}}) = \mathbb{Z}$.

van Luijk's method would have succeed in this example by using a second prime.

Abelian surface

$A = \mathrm{Jac}(y^2 = 4x^5 - 36x^4 + 56x^3 - 76x^2 + 44x - 23)$

We have automated this process and the SageMath package is available at

`github.com/edgarcosta/crystalline_obstruction`

```
sage: f = ZZ['x,y']('4*x^5 - 36*x^4 + 56*x^3 - 76*x^2 + 44*x - 23 -y^2')
sage: crystalline_obstruction(f=f, p=31, precision=3)
(1,
 {'precision': 3,
  'p': 31,
  'rank T(X_Fpbar)': 2,
  'factors': [(t - 1, 2)],
  'dim Ti': [2],
  'dim Li': [1]})
```

As we had observed before:

- $\rho\left(A_{\mathbb{F}_p^{\mathrm{al}}}\right) = 2$
- $\rho(A_{\mathbb{Q}^{\mathrm{al}}}) \leq 1 \Longrightarrow \mathrm{rk}\,\mathrm{End}(A_{\mathbb{Q}^{\mathrm{al}}}) = 1.$

Abelian threefold $A := \mathrm{Jac}(y^4 + x^3z + 2y^3z - yz^3)$

Recall that $\mathrm{End}(A) \simeq \mathrm{H}^1(A) \otimes \mathrm{H}^1(A) \subset \mathrm{H}^2(A \times A)$.
Thus, we may bound $\mathrm{rk}\,\mathrm{End}(A)$ directly by inspecting $\mathrm{H}^1(A) \otimes \mathrm{H}^1(A)$.

```
sage: crystalline_obstruction(f=f, p=31, precision=3)
(4, {'rank T(X_Fpbar)': 5,
     'factors': [(t - 1, 3), (t^2 + t + 1, 1)],
     'dim Ti': [3, 2],
     'dim Li': [2, 2],
     'precision': 5, 'p': 31})
sage: crystalline_obstruction(f=f, p=31, precision=3, tensor=True)
(6, {'rank T(X_Fpbar)': 10,
     'factors': [(t - 1, 6), (t^2 + t + 1, 2)],
     'dim Ti': [6, 4],
     'dim Li': [4, 2],
     'precision': 5, 'p': 31})
```

- Improved, $\mathrm{rk}\,\mathrm{NS}(A_{\mathbb{Q}^{\mathrm{al}}}) \leq 5$ to $\mathrm{rk}\,\mathrm{NS}(A_{\mathbb{Q}^{\mathrm{al}}}) \leq 4$
- Improved, $\mathrm{rk}\,\mathrm{End}(A_{\mathbb{Q}^{\mathrm{al}}}) \leq 10$ to $\mathrm{rk}\,\mathrm{End}(A_{\mathbb{Q}^{\mathrm{al}}}) \leq 6$
- indeed, $\mathrm{End}(A_{\mathbb{Q}^{\mathrm{al}}})_{\mathbb{Q}} = \mathbb{Q}(\sqrt{-3}) \times B$, B is a quaternion algebra with $\mathrm{disc}\,B = 6$.

K3 surface

$X := Z(y^4 - x^3z + yz^3 + zw^3 + w^4) \subset \mathbb{P}^3_{\mathbb{C}}$

```
sage: crystalline_obstruction(f, p=89, precision=3)
(4,
 {'rank T(X_Fpbar)': 10,
  'factors': [(t - 1, 1), (t + 1, 1), (t - 1, 4), (t^4 + 1, 1)],
  'dim Ti': [1, 1, 4, 4],
  'dim Li': [1, 0, 3, 0]},
  'precision': 3, 'p': 89})
```

- $\rho(X_{\mathbb{F}_{89}^{\mathrm{al}}}) = 10$
- $\mathrm{Pic}(X_{\mathbb{F}_{89}^{\mathrm{al}}})$ decomposes as $P_{\zeta_1} \oplus P_{\zeta_2} \oplus P_{\zeta_8}$
- By studying each factor independent, we show $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) \leq 4$
- In fact, $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) = 4$ as there are four lines in $z = 0$.
- previous approaches would have not used $p = 89$

Quartic surface

$X = Z(y^4 - x^3z + yz^3 + zw^3 + w^4) \subset \mathbb{P}^3_{\mathbb{C}}$

```
sage: crystalline_obstruction(f, p=31, precision=5)
(4,
 {'rank T(X_Fpbar)': 4,
  'factors': [(t - 1, 1), (t - 1, 1), (t + 1, 2)],
  'dim Ti': [1, 1, 2],
  'dim Li': [1, 1, 2]},
  'precision': 5, 'p': 31})
```

- $\rho(X_{\mathbb{F}_{31}^{\mathrm{al}}}) = 4$
- no cycle obstruction found while working $\mathbb{Z}/(p)^5$
- $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) \leq 4$, with some extra confidence that the equality might hold.
- by searching for lines Elsenhans–Jahnel's method would have succeeded in this example

Quintic surface

$X := Z(9xy^4 + 3x^4z + 9y^2z^3 + z^5 + 5w^5) \subset \mathbb{P}^3$

```
sage: crystalline_obstruction(f, p=23, precision=6)
(1, {'rank T(X_Fpbar)': 5,
     'factors': [(t - 1, 1), (t - 1, 1), (t + 1, 1), (t^2 + 1, 1)],
     'dim Ti': [1, 1, 1, 2],
     'dim Li': [1, 0, 0, 0],
    'precision': 6, 'p': 23})
```

```
sage: crystalline_obstruction(f, p=29, precision=20)
(3, {'rank T(X_Fpbar)': 5,
     'factors': [(t - 1, 1), (t - 1, 2), (t + 1, 2)],
     'dim Ti': [1, 2, 2],
     'dim Li': [1, 1, 1]})
     'precision': 20, 'p': 29})
```

- $\rho(X_{\mathbb{Q}^{\mathrm{al}}}) = 1$
- However, we cannot deduce this from $p = 29$, not even with infinite precision.
- The surface has *CM* by $\mathbb{Q}(\zeta_5)$

Final thoughts

- Is there a prime for which the bound will be tight?
  In general, no.
  For example, take a K3 X surface with real multiplication, defined over a number field where all the algebraic cycles in X and $X \times X$ are defined.
  However, we are hopeful for K3 surfaces and abelian 3folds defined over $\mathbb{Q}$.
- Can we combine both approaches?
  At the moment we are only computing an approximation of $\mathrm{Pic}(X)_{\mathbb{Q}_p}$.
  To combine several primes we need at least $\mathrm{Pic}(X_{\mathbb{F}_p})_{\mathbb{Q}}$, to be able to use

$$\mathrm{Pic}(X)_{\mathbb{Q}} = \mathrm{Pic}(X_{\mathbb{F}_p})_{\mathbb{Q}} \cap \mathrm{F}^1_{\mathbb{Q}_p}$$

  in its full strength.
  At the moment we are only using

$$\mathrm{Pic}(X)_{\mathbb{Q}_p} \subset \mathrm{Pic}(X_{\mathbb{F}_p})_{\mathbb{Q}_p} \cap \mathrm{F}^1_{\mathbb{Q}_p}$$