Sato-Tate Groups and Distributions of $y^2 = x^{p^2} - 1$

Rezwan Hoque
Joint work with Justin Chen, Heidi Goodson, and Sabeeha Malikah

Brooklyn College, City University of New York
PME Contributed Session on Research by Undergraduates, Jan. 5 2026

Proposed by Mikio Sato and John Tate around 1960.

Mikio Sato (1928 - 2023)

John Tate (1925 - 2019)

The Sato-Tate Conjecture (Cont.)

Let C be a smooth, projective, genus g curve over $\mathbb{Q}$.

- Originally posed when A is an elliptic curve ($g = 1$), can be extended to higher-genus curves via $\mathrm{Jac}(C)$.

Denote the normalized L-polynomial of primes p of good reduction for C as

$$\overline{L}_p(C, T) = T^{2g} + a_1 T^{2g-1} + a_2 T^{2g-2} + \ldots + a_2 T^2 + a_1 T + 1.$$

As $p \to \infty$, we can realize distributions of $\overline{L}_p(C, T)$'s coefficients as moment sequences.

Note: For each prime $p \nmid \ell$ of good reduction, $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{F}/F)$ is mapped to a conjugacy class under $\rho_{A,\ell}$ in $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))$. The conjecture is equivalent to talking about limiting distributions of Frobenius elements' conjugacy classes

The Sato-Tate Conjecture (Cont.)

Let C be a smooth, projective, genus g curve over $\mathbb{Q}$.

- Originally posed when A is an elliptic curve ($g = 1$), can be extended to higher-genus curves via $\mathsf{Jac}(C)$.

Denote the normalized L-polynomial of primes p of good reduction for C as

$$\overline{L}_p(C, T) = T^{2g} + a_1 T^{2g-1} + a_2 T^{2g-2} + \ldots + a_2 T^2 + a_1 T + 1.$$

As $p \to \infty$, we can realize distributions of $\overline{L}_p(C, T)$'s coefficients as moment sequences.

(Generalized) Sato-Tate Conjecture

As $p \to \infty$, the distribution of coefficients of $\overline{L}_p(C, T)$ converges to the distributions of $\mathsf{ST}(\mathsf{Jac}(C))$'s conjugacy classes' charpoly coefficients via the Haar measure.

Note: For each prime $p \nmid \ell$ of good reduction, $\mathbf{Frob}_p \in \mathsf{Gal}(\overline{F}/F)$ is mapped to a conjugacy class under $\rho_{A,\ell}$ in $\mathsf{ST}(\mathsf{Jac}(C_{p^2}))$. The conjecture is equivalent to talking about limiting distributions of Frobenius elements' conjugacy classes

Our Case

We are studying the family of (hyperelliptic) curves

$$C_{p^2} : y^2 = x^{p^2} - 1,$$

where p is an odd prime.

Our Case

We are studying the family of (hyperelliptic) curves

$$C_{p^2} : y^2 = x^{p^2} - 1,$$

where p is an odd prime.

C_{p^2} exhibits complex multiplication (CM) by $\mathbb{Q}(\zeta_{p^2})$. By the results of [Joh17], this means *the Sato-Tate conjecture is true for C_{p^2}!*

Our Case

We are studying the family of (hyperelliptic) curves

$$C_{p^2} : y^2 = x^{p^2} - 1,$$

where p is an odd prime.

C_{p^2} exhibits complex multiplication (CM) by $\mathbb{Q}(\zeta_{p^2})$. By the results of [Joh17], this means *the Sato-Tate conjecture is true for* C_{p^2}*!*

We want to see what $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))$ and its distributions look like.

Computing Sato-Tate Groups

We need to compute two objects:

$$\mathrm{ST}^0(\mathrm{Jac}(C_{p^2})) \quad \text{and} \quad \mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\,\mathrm{ST}^0(\mathrm{Jac}(C_{p^2})).$$

Computing $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$

First, we have that the endomorphism field of $\mathrm{Jac}(C_{p^2})$ is $\mathbb{Q}(\zeta_{p^2})$ ([GGL24, Prop. 3.5.1]). By [GGL25, Thm. 7.2.12], this is also its *connected monodromy field*. So,

$$\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\mathrm{ST}^0(\mathrm{Jac}(C_{p^2})) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}).$$

Moreover

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times,$$

so $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$ is cyclic (because $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is) and has order $\phi(p^2)$.

Computing $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\,\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$

First, we have that the endomorphism field of $\mathrm{Jac}(C_{p^2})$ is $\mathbb{Q}(\zeta_{p^2})$ ([GGL24, Prop. 3.5.1]). By [GGL25, Thm. 7.2.12], this is also its *connected monodromy field*. So,

$$\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\,\mathrm{ST}^0(\mathrm{Jac}(C_{p^2})) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}).$$

Moreover

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times,$$

so $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\,\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$ is cyclic (because $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is) and has order $\phi(p^2)$.

To find a generator of $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\,\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$, we study *endomorphisms* of $\mathrm{Jac}(C_{p^2})$ acted on by $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q})$.

Computing $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\,\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$ (Cont.)

Let $Z := -\,\mathrm{diag}(\zeta_{p^2}, \overline{\zeta}_{p^2})$. Endomorphisms of $\mathrm{Jac}(C_{p^2})$ are of the form

$$\alpha = \mathrm{diag}(Z, Z^2, Z^3, ..., Z^g),$$

where $g = (p^2 - 1)/2$ is the genus of C_{p^2}.

Computing $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\,\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$ (Cont.)

Let $Z := -\operatorname{diag}(\zeta_{p^2}, \overline{\zeta}_{p^2})$. Endomorphisms of $\mathrm{Jac}(C_{p^2})$ are of the form

$$\alpha = \operatorname{diag}(Z, Z^2, Z^3, \dots, Z^g),$$

where $g = (p^2 - 1)/2$ is the genus of C_{p^2}.

By computing a $\langle \sigma_a \rangle = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q})$ (through Sage), the action of σ_a on α (${}^{\sigma_a}Z^t = Z^{at}$) either *only* permutes or permutes *and* conjugates entries of α. Tracking this behavior gives the component group generator.

Computing $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\,\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$ (Cont.)

Let $Z := -\,\mathrm{diag}(\zeta_{p^2}, \overline{\zeta}_{p^2})$. Endomorphisms of $\mathrm{Jac}(C_{p^2})$ are of the form

$$\alpha = \mathrm{diag}(Z, Z^2, Z^3, ..., Z^g),$$

where $g = (p^2 - 1)/2$ is the genus of C_{p^2}.

By computing a $\langle \sigma_a \rangle = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^2})/\mathbb{Q})$ (through Sage), the action of σ_a on α (${}^{\sigma_a}Z^t = Z^{at}$) either *only* permutes or permutes *and* conjugates entries of α. Tracking this behavior gives the component group generator.

Let I be the 2×2 identity matrix,

$$J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

and $\langle n \rangle_{p^2}$ denote $n \pmod{p^2}$.

Computing $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))/\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$ (Cont.)

Proposition [CGHM25]

The $2g \times 2g$ matrix γ (in $\mathrm{USp}(2g)$) defined by

$$\gamma[i,j] = \begin{cases} I & \text{if } j = \langle ai \rangle_{p^2} \\ J & \text{if } j = p^2 - \langle ai \rangle_{p^2} \\ 0 & \text{otherwise.} \end{cases}$$

generates the component group of $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))$.

Proof idea:

- Show that $\gamma\alpha\gamma^{-1} = {}^{\sigma_a}\alpha$ (shows that $\gamma \in \mathrm{ST}(\mathrm{Jac}(C_{p^2}))$)
- $|\gamma| = \phi(p^2)$ (order is equal to that of the component group).

Example of a Component Group Generator: C_{25}

When $p = 5$, using σ_2 as a generator for $\mathrm{Gal}(\mathbb{Q}(\zeta_{25})/\mathbb{Q})$ (found via Sage) gives

$$\gamma = \begin{pmatrix} 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & I \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & J & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & J & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & J & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & J & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & J & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ J & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Here, $g = (25 - 1)/2 = 12$. So, γ is a 24×24 matrix. For $p = 7$, γ is a 48×48 matrix!

The Identity Component, $\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$

Since $\mathrm{Jac}(C_{p^2})$ is an abelian variety with CM, we have that

$$\mathrm{ST}^0(\mathrm{Jac}(C_{p^2})) \cong \mathrm{Hg}(\mathrm{Jac}(C_{p^2})),$$

where $\mathrm{Hg}(\mathrm{Jac}(C_{p^2}))$ is the Hodge group of $\mathrm{Jac}(C_{p^2})$.

Note: We embed $\mathbf{U}(1)$ in $\mathbf{SU}(2)$ via $u \mapsto U = \mathbf{diag}(u, \overline{u})$, and $\mathbf{U}(1)^n := \langle \mathbf{diag}(U_1, \ldots, U_n) \mid U_i \in \mathbf{U}(1) \rangle$

The Identity Component, $\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$

Since $\mathrm{Jac}(C_{p^2})$ is an abelian variety with CM, we have that

$$\mathrm{ST}^0(\mathrm{Jac}(C_{p^2})) \cong \mathrm{Hg}(\mathrm{Jac}(C_{p^2})),$$

where $\mathrm{Hg}(\mathrm{Jac}(C_{p^2}))$ is the Hodge group of $\mathrm{Jac}(C_{p^2})$.

We have that

Proposition [CGHM25]

$\mathrm{Hg}(\mathrm{Jac}(C_{p^2})) \cong \mathrm{U}(1)^{g'}$, where $g' = \phi(p^2)/2$.

Proof idea:

- $\mathrm{Jac}(C_{p^2}) \sim \mathrm{Jac}(C_p) \times X_{p^2}$ and $\mathrm{MT}(\mathrm{Jac}(C_{p^2})) \cong \mathrm{MT}(X_{p^2})$ by [GGL24]
- $\mathrm{Hg}(\mathrm{Jac}(C_{p^2})) \cong \mathrm{Hg}(X_{p^2}) \cong \mathrm{L}(X_{p^2}) \cong \mathrm{U}(1)^{g'}$.

Note: We embed $\mathbf{U}(1)$ in $\mathbf{SU}(2)$ via $u \mapsto U = \mathbf{diag}(u, \overline{u})$, and $\mathbf{U}(1)^n := \langle \mathbf{diag}(U_1, \ldots, U_n) \mid U_i \in \mathbf{U}(1) \rangle$

The Identity Component (Cont.)

This result tells us that $\mathrm{Hg}(\mathrm{Jac}(C_{p^2}))$ is smaller than expected—since $\mathrm{Jac}(C_{p^2})$ has CM, it'd "normally" be isomorphic to $\mathrm{U}(1)^g$.

The Identity Component (Cont.)

This result tells us that $\mathrm{Hg}(\mathrm{Jac}(C_{p^2}))$ is smaller than expected—since $\mathrm{Jac}(C_{p^2})$ has CM, it'd "normally" be isomorphic to $\mathrm{U}(1)^g$.

This is reflected by the fact that $\mathrm{Jac}(C_{p^2})$ is degenerate (by [Goo24]).

Definition

An abelian variety A is *degenerate* if its Hodge ring

$$\mathscr{B}^*(A) := \sum_{d=0}^{\dim(A)} \mathscr{B}^d(A),$$

where $\mathscr{B}^d(A)$ is the $\mathbb{C}$-span of the Hodge classes of codimension d on A, contains exceptional (Hodge) classes—Hodge classes not generated by classes of codimension $d = 1$ (i.e., divisor classes).

The Identity Component (Cont.)

This result tells us that $\mathrm{Hg}(\mathrm{Jac}(C_{p^2}))$ is smaller than expected—since $\mathrm{Jac}(C_{p^2})$ has CM, it'd "normally" be isomorphic to $\mathrm{U}(1)^g$.

This is reflected by the fact that $\mathrm{Jac}(C_{p^2})$ is degenerate (by [Goo24]).

Definition

An abelian variety A is *degenerate* if its Hodge ring

$$\mathscr{B}^*(A) := \sum_{d=0}^{\dim(A)} \mathscr{B}^d(A),$$

where $\mathscr{B}^d(A)$ is the $\mathbb{C}$-span of the Hodge classes of codimension d on A, contains exceptional (Hodge) classes—Hodge classes not generated by classes of codimension $d = 1$ (i.e., divisor classes).

Since $\mathrm{ST}(\mathrm{Jac}(C_{p^2})) \subseteq \mathrm{USp}(2g)$ and $g - g' = (p-1)/2$, if we identified an element of $\mathrm{Hg}(\mathrm{Jac}(C_{p^2}))$ with a $U \in \mathrm{U}(1)^g$, $p - 1$ entries of U are dependent on other entries of U.

Extracting the Dependencies

Informally, the Hodge ring is made up of the classes that are *fixed* by the Hodge group ([BL04, Thm. 17.3.3]). So, if $U \in \mathrm{Hg}(\mathrm{Jac}(C_{p^2}))$ (as a matrix) and v is a Hodge class (in the Hodge ring), then

$$U \cdot v = v.$$

This action is how we'll extract the extra relations.

Extracting the Dependencies

Informally, the Hodge ring is made up of the classes that are *fixed* by the Hodge group ([BL04, Thm. 17.3.3]). So, if $U \in \mathrm{Hg}(\mathrm{Jac}(C_{p^2}))$ (as a matrix) and v is a Hodge class (in the Hodge ring), then

$$U \cdot v = v.$$

This action is how we'll extract the extra relations.

Identifying the Hodge group with an element from $\mathrm{U}(1)^{g'}$ already incorporates the relations from the divisor classes—it's just

$$\mathrm{diag}(U_1, \overline{U}_1, U_2, \overline{U}_2, ...U_{g'}, \overline{U}_{g'}),$$

where $U_i \in \mathrm{U}(1)$ and $U_i\overline{U}_i = 1$. The non-divisor class Hodge classes have to come from higher codimensions.

Extracting the Dependencies

Informally, the Hodge ring is made up of the classes that are *fixed* by the Hodge group ([BL04, Thm. 17.3.3]). So, if $U \in \mathrm{Hg}(\mathrm{Jac}(C_{p^2}))$ (as a matrix) and v is a Hodge class (in the Hodge ring), then

$$U \cdot v = v.$$

This action is how we'll extract the extra relations.

Identifying the Hodge group with an element from $\mathrm{U}(1)^{g'}$ already incorporates the relations from the divisor classes—it's just

$$\mathrm{diag}(U_1, \overline{U}_1, U_2, \overline{U}_2, \ldots U_{g'}, \overline{U}_{g'}),$$

where $U_i \in \mathrm{U}(1)$ and $U_i\overline{U}_i = 1$. The non-divisor class Hodge classes have to come from higher codimensions.

We look at the indecomposable Hodge classes—exceptional classes not generated by classes of lower codimension.

Redefining Indecomposable Classes

In [Shi82], Shioda defines a set of tuples that act as an index set for Hodge classes of codimension d:

Definition [CGHM25]

Let m be a positive, odd integer and d be an integer satisfying $1 \leq d \leq \frac{m-1}{2}$. We define the set

$$\mathfrak{B}_m^d := \{\beta = (b_1, b_2, \ldots, b_{2d})\}$$

to be the set of tuples of length $2d$ satisfying the following properties:

1. $1 \leq b_1 < b_2 < \cdots < b_{2d} \leq m - 1$;
2. $\sum_{i=1}^{2d} b_i \equiv 0 \pmod{m}$;
3. $|t \cdot \beta| = d$ for all $t \in (\mathbb{Z}/m\mathbb{Z})^\times$, where $|t \cdot \beta| = \sum_{i=1}^{2d} \langle tb_i \rangle_m / m$.

Redefining Indecomposable Classes (Cont.)

Namely, he showed that there is a correspondence between tuples in $\mathfrak{B}_m^d$ to Hodge classes:

[Shi82, Thm. 5.2]

Assume m is odd. The Hodge classes on the Jacobian variety $\mathrm{Jac}(C_m)$ have the following description:

$$\mathscr{B}^d(\mathrm{Jac}(C_m)) = \bigoplus_{(b_1,\ldots,b_{2d})\in\mathfrak{B}_m^d} \mathbb{C}\,\omega_{b_1}\wedge\cdots\wedge\omega_{b_{2d}}.$$

So

$$(b_1, b_2, \ldots, b_{2d}) \longleftrightarrow \omega_{b_1}\wedge\omega_{b_2}\wedge\cdots\wedge\omega_{b_{2d}}.$$

Redefining Indecomposable Classes (Cont.)

So we can frame *exceptional*-ness and *indecomposible*-ness in terms of tuples:

Definition [CGHM25]

We say that a tuple $\beta \in \mathfrak{B}_m^d$ is **exceptional** if it's not entirely made up of pairs b_i, b_j such that $b_i + b_j \equiv 0 \pmod{m}$.

We say that $\beta \in \mathfrak{B}_m^d$ is **indecomposable** if no proper subset (with an even number of elements) of $\{b_1, b_2, \ldots, b_{2d}\}$ adds to a multiple of m. Otherwise, we say that β is *decomposable*.

Example: $m = p^2 = 9$, $d = (3+1)/2 = 2$

- $(1, 4, 6, 7)$ and $(2, 3, 5, 8)$ are exceptional and indecomposable, but $(1, 2, 7, 8)$ isn't exceptional

Example: $m = p^2 = 25$, $d = 4$

- $(1, 2, 6, 11, 16, 20, 21, 23)$ is exceptional, but not indecomposable

Our Case: $m = p^2$

In the proof of [Shi82, Lemma 5.5], Shioda defined a family of indecomposable tuples of codimension $d = (p+1)/2$: For $1 \leq i \leq p-1$, define

$$\beta_i := (i, i+p, i+2p, \ldots, i+(p-1)p, p(p-i)).$$

(We write β_i to signify the tuple's entries have been permuted to be an element of $\mathfrak{B}_m^d$)

Our Case: $m = p^2$

In the proof of [Shi82, Lemma 5.5], Shioda defined a family of indecomposable tuples of codimension $d = (p+1)/2$: For $1 \leq i \leq p-1$, define

$$\beta_i := (i, i+p, i+2p, \ldots, i+(p-1)p, p(p-i)).$$

(We write β_i to signify the tuple's entries have been permuted to be an element of $\mathfrak{B}_m^d$)

It turns out, *all* indecomposable tuples (when $m = p^2$) come from β_i. Meaning, the only codimension where indecomposable classes exist is $d = (p+1)/2$ ([CGHM25, Thm. 3.21]).

Our Case: $m = p^2$

In the proof of [Shi82, Lemma 5.5], Shioda defined a family of indecomposable tuples of codimension $d = (p+1)/2$: For $1 \leq i \leq p-1$, define

$$\beta_i := (i, i+p, i+2p, \ldots, i+(p-1)p, p(p-i)).$$

(We write β_i to signify the tuple's entries have been permuted to be an element of $\mathfrak{B}_m^d$)

It turns out, *all* indecomposable tuples (when $m = p^2$) come from β_i. Meaning, the only codimension where indecomposable classes exist is $d = (p+1)/2$ ([CGHM25, Thm. 3.21]).

Furthermore, there are exactly $p-1$ many of these tuples when $m = p^2$ ([CGHM25, Thm. 3.21]).

The Indecomposable Classes Characterized

Using the above correspondence, this means

[CGHM25, Cor. 3.22]

From each indecomposable tuple

$$\beta_i := (i, i+p, i+2p, \dots, i+(p-1)p, p(p-i)),$$

the indecomposable Hodge classes of codimension $(p+1)/2$ are given by

$$\nu_i = \omega_i \wedge \omega_{i+p} \wedge \omega_{i+2p} \wedge \cdots \wedge \omega_{i+(p-1)p} \wedge \omega_{p(p-i)},$$

where $1 \leq i \leq p-1$.

An Adjustment

We'll modify the elements of β_i such that every entry b_j with $j > d = \frac{p+1}{2}$ is written as $b_j - p^2$. This modification will negate elements of the tuple whose value is greater than $\frac{p^2}{2}$. This corresponds to expressing the differential ω_{b_j} as $\overline{\omega}_{p^2 - b_j}$.

After modifying the tuples in this way, we obtain pairs of tuples such that each β_i is paired with the corresponding tuple β_{p-i}, where both are negatives of each other.
Ex: $p^2 = 9$

- $\beta_1 = (1, 4, 6, 7) \to (1, 4, -3, -2) \longleftrightarrow \nu_1 = \omega_1 \wedge \omega_4 \wedge \overline{\omega}_3 \wedge \overline{\omega}_2$
- $\beta_2 = (2, 3, 5, 8) \to (2, 3, -4, -1) \longleftrightarrow \nu_2 = \omega_2 \wedge \omega_3 \wedge \overline{\omega}_4 \wedge \overline{\omega}_1$

We read off the effect of the Hodge group in every new β_i. So, it's sufficient to just focus on the tuples β_i where $1 \leq i \leq \frac{p-1}{2}$.

New Expression of Indecomposable Classes

From that adjustment of each β_i, we obtain a new expression of the indecomposable Hodge classes

[CGHM25, Cor. 3.26]

Let $1 \leq i \leq \frac{p-1}{2}$. Then

$$\nu_i = \omega_i \wedge \omega_{i+p} \wedge \omega_{i+2p} \wedge \cdots \wedge \omega_{i+p\frac{p-1}{2}} \wedge \overline{\omega}_{p\frac{p-1}{2}-i} \wedge \cdots \wedge \overline{\omega}_{p-i} \wedge \overline{\omega}_{pi}.$$

The Indecomposable Classes Characterized (Cont.)

By the group action $U \cdot \nu_i = \nu_i$, when ν_i is an indecomposable class we have

$$
\begin{aligned}
U \cdot \nu_i &= U \cdot (\omega_i \wedge \omega_{i+p} \wedge \omega_{i+2p} \wedge \cdots \wedge \omega_{i+p\frac{p-1}{2}} \wedge \overline{\omega}_{p\frac{p-1}{2}-i} \wedge \cdots \wedge \overline{\omega}_{p-i} \wedge \overline{\omega}_{pi}) \\
&= (u_i u_{i+p} u_{i+2p} \cdots u_{i+p\frac{p-1}{2}} \overline{u}_{p\frac{p-1}{2}-i} \cdots \overline{u}_{p-i} \overline{u}_{pi}) \nu_i .
\end{aligned}
$$

The Indecomposable Classes Characterized (Cont.)

By the group action $U \cdot \nu_i = \nu_i$, when ν_i is an indecomposable class we have

$$\begin{aligned} U \cdot \nu_i &= U \cdot (\omega_i \wedge \omega_{i+p} \wedge \omega_{i+2p} \wedge \cdots \wedge \omega_{i+p\frac{p-1}{2}} \wedge \overline{\omega}_{p\frac{p-1}{2}-i} \wedge \cdots \wedge \overline{\omega}_{p-i} \wedge \overline{\omega}_{pi}) \\ &= (u_i u_{i+p} u_{i+2p} \cdots u_{i+p\frac{p-1}{2}} \overline{u}_{p\frac{p-1}{2}-i} \cdots \overline{u}_{p-i} \overline{u}_{pi}) \nu_i. \end{aligned}$$

Since the Hodge group fixes elements from the Hodge ring, we have that

$$u_i u_{i+p} u_{i+2p} \cdots u_{i+p\frac{p-1}{2}} \overline{u}_{p\frac{p-1}{2}-i} \cdots \overline{u}_{p-i} \overline{u}_{pi} = 1.$$

The Indecomposable Classes Characterized (Cont.)

By the group action $U \cdot \nu_i = \nu_i$, when ν_i is an indecomposable class we have

$$U \cdot \nu_i = U \cdot (\omega_i \wedge \omega_{i+p} \wedge \omega_{i+2p} \wedge \cdots \wedge \omega_{i+p\frac{p-1}{2}} \wedge \overline{\omega}_{p\frac{p-1}{2}-i} \wedge \cdots \wedge \overline{\omega}_{p-i} \wedge \overline{\omega}_{pi})$$

$$= (u_i u_{i+p} u_{i+2p} \cdots u_{i+p\frac{p-1}{2}} \overline{u}_{p\frac{p-1}{2}-i} \cdots \overline{u}_{p-i} \overline{u}_{pi}) \nu_i.$$

Since the Hodge group fixes elements from the Hodge ring, we have that

$$u_i u_{i+p} u_{i+2p} \cdots u_{i+p\frac{p-1}{2}} \overline{u}_{p\frac{p-1}{2}-i} \cdots \overline{u}_{p-i} \overline{u}_{pi} = 1.$$

The largest subscript is $i + p\frac{p-1}{2}$, so isolating it gives

$$u_{i+p\frac{p-1}{2}} = \overline{u}_i \overline{u}_{i+p} \overline{u}_{i+2p} \cdots \overline{u}_{i+p\frac{p-3}{2}} u_{p\frac{p-1}{2}-i} \cdots u_{p-i} u_{pi}$$

and

$$\overline{u}_{i+p\frac{p-1}{2}} = u_i u_{i+p} u_{i+2p} \cdots u_{i+p\frac{p-3}{2}} \overline{u}_{p\frac{p-1}{2}-i} \cdots \overline{u}_{p-i} \overline{u}_{pi}.$$

The Indecomposable Classes Characterized (Cont.)

By the group action $U \cdot \nu_i = \nu_i$, when ν_i is an indecomposable class we have

$$U \cdot \nu_i = U \cdot (\omega_i \wedge \omega_{i+p} \wedge \omega_{i+2p} \wedge \cdots \wedge \omega_{i+p\frac{p-1}{2}} \wedge \overline{\omega}_{p\frac{p-1}{2}-i} \wedge \cdots \wedge \overline{\omega}_{p-i} \wedge \overline{\omega}_{pi})$$
$$= (u_i u_{i+p} u_{i+2p} \cdots u_{i+p\frac{p-1}{2}} \overline{u}_{p\frac{p-1}{2}-i} \cdots \overline{u}_{p-i} \overline{u}_{pi})\nu_i.$$

Since the Hodge group fixes elements from the Hodge ring, we have that

$$u_i u_{i+p} u_{i+2p} \cdots u_{i+p\frac{p-1}{2}} \overline{u}_{p\frac{p-1}{2}-i} \cdots \overline{u}_{p-i} \overline{u}_{pi} = 1.$$

The largest subscript is $i + p\frac{p-1}{2}$, so isolating it gives

$$u_{i+p\frac{p-1}{2}} = \overline{u}_i \overline{u}_{i+p} \overline{u}_{i+2p} \cdots \overline{u}_{i+p\frac{p-3}{2}} u_{p\frac{p-1}{2}-i} \cdots u_{p-i} u_{pi}$$

and

$$\overline{u}_{i+p\frac{p-1}{2}} = u_i u_{i+p} u_{i+2p} \cdots u_{i+p\frac{p-3}{2}} \overline{u}_{p\frac{p-1}{2}-i} \cdots \overline{u}_{p-i} \overline{u}_{pi}.$$

These are *exactly* the missing relations!

The Identity Component, Revisited

By the previous slide, we can now express $\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$:

[CGHM25, Prop. 4.1]

The identity component of the Sato-Tate group of $\mathrm{Jac}(C_{p^2})$ is isomorphic to $\mathrm{U}(1)^{g'}$. We can identify elements of the identity component with matrices $U = \mathrm{diag}(U_1, U_2, \ldots, U_g)$ in $\mathrm{U}(1)^g$ where

$$U_{i+p\frac{p-1}{2}} = \overline{U}_i \overline{U}_{i+p} \overline{U}_{i+2p} \cdots \overline{U}_{i+p\frac{p-3}{2}} U_{p\frac{p-1}{2}-i} \cdots U_{p-i} U_{pi}$$

for $1 \leq i \leq \frac{p-1}{2}$.

Recall $U_i = \mathbf{diag}(u_i, \overline{u}_i)$

Example of Identity Component: C_{25}

Let $p = 5$. The genus of C_{25} is $g = (25 - 1)/2 = 12$. The only indecomposable tuples are

$$(1, 6, 11, 16, 20, 21),\ (2, 7, 12, 15, 17, 22),\ (3, 8, 10, 13, 18, 23),\ (4, 5, 9, 14, 19, 24)$$

and they're all of the form β_i with $1 \leq i \leq 4$.

We select the first two tuples and adjust each entry of the tuple whose value is greater than $p^2/2 = 12.5$ to obtain

$$\beta_1 = (1, 6, 11, -9, -5, -4) \qquad \beta_2 = (2, 7, 12, -10, -8, -3).$$

These correspond to the Hodge classes

$$\nu_1 = \omega_1 \wedge \omega_6 \wedge \omega_{11} \wedge \overline{\omega}_9 \wedge \overline{\omega}_5 \wedge \overline{\omega}_4 \quad \text{and} \quad \nu_2 = \omega_2 \wedge \omega_7 \wedge \omega_{12} \wedge \overline{\omega}_{10} \wedge \overline{\omega}_8 \wedge \overline{\omega}_3.$$

Let $U \in \mathrm{U}(1)^g$. We get the following relations among entries of U

$$u_{11} = \overline{u}_1 u_4 u_5 \overline{u}_6 u_9 \quad \text{and} \quad u_{12} = \overline{u}_2 u_3 \overline{u}_7 u_8 u_{10},$$

giving us the identity component

$$U = \mathrm{diag}(U_1, U_2, \ldots, U_{10},\ \overline{U}_1 U_4 U_5 \overline{U}_6 U_9,\ \overline{U}_2 U_3 \overline{U}_7 U_8 U_{10}).$$

The Sato-Tate Group of $\mathrm{Jac}(C_{p^2})$

[CGHM25, Thm. 4.6]

Let $g = \frac{p^2-1}{2}$ be the genus of the curve C_{p^2} and let $g' = \frac{p(p-1)}{2}$. The Sato-Tate group of $\mathrm{Jac}(C_{p^2})$, up to isomorphism in $\mathrm{USp}(2g)$, is given by

$$\mathrm{ST}(\mathrm{Jac}(C_{p^2})) \simeq \langle \mathrm{U}(1)^{g'}, \gamma \rangle,$$

where the embedding of $\mathrm{U}(1)^{g'}$ in $\mathrm{USp}(2g)$ is described in Slide 21.

(a_1) Moment Statistics of C_{25}

The numerical moments coming from the a_1 coefficient of the normalized L-polynomial were computed up to primes $p < 2^{25}$

	M_2	M_4	M_6	M_8
a_1	2.009	90.848	9452.007	1438061.241
μ_1	2	90	9344	1419866

Table 1: Table of a_1- and μ_1-moments for $C_{25} : y^2 = x^{25} - 1$ (with $p < 2^{25}$).

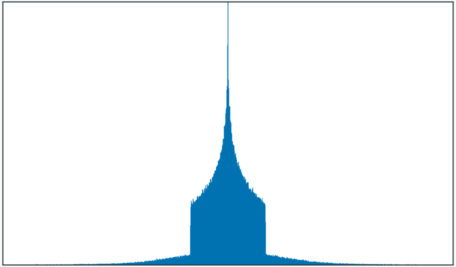

Figure 1: Histogram of the a_1-coefficients for $C_{25} : y^2 = x^{25} - 1$.

Thank you!

Read our paper!

or search Degeneracy and Sato-Tate Groups of $y^2 = x^{p^2} - 1$

Bonus: Sato-Tate Group Definition

For an abelian variety A of dimension g over a field F and prime ℓ, the Galois action on the Tate module is given by an ℓ-adic representation

$$\rho_{A,\ell} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{Aut}(V_\ell) \cong \mathrm{GL}_{2g,\mathbb{Q}_\ell},$$

where V_ℓ is the rational Tate module.

The ℓ-adic monodromy group of A, denoted as $G_{A,\ell}$, is the Zariski closure of the image of this map over $\mathrm{GL}_{2g,\mathbb{Q}_\ell}$. Additionally, let $G^1_{A,\ell} := G_{A,\ell} \cap \mathrm{Sp}_{2g,\mathbb{Q}_\ell}$.

Definition [Goo24, Sec. 2.4]

The Sato-Tate group of A, denoted as $\mathrm{ST}(A)$, is a maximal compact Lie subgroup of $G^1_{A,\ell} \otimes_{\mathbb{Q}_\ell} \mathbb{C}$ contained in $\mathrm{USp}(2g)$.

Bonus: Moment Statistics

Moment statistics from the $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))$ are called theoretical moments, whereas those from the normalized L-polynomials are called numerical moments.

Bonus: Moment Statistics

Moment statistics from the $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))$ are called theoretical moments, whereas those from the normalized L-polynomials are called numerical moments.

By the isomorphism of $\mathrm{ST}(\mathrm{Jac}(C_{p^2}))$, we can compute moments by working with $\langle \mathrm{U}(1)^{g'}, \gamma \rangle$ instead.

Bonus: Moment Statistics (Cont. + Some Background)

For the unitary group $\mathrm{U}(1)$, the trace map tr on a random element $U \in \mathrm{U}(1)$ is given by $z := \mathrm{tr}(U) = u + \overline{u} = 2\cos(\theta)$, where $u = e^{i\theta}$. Then $dz = -2\sin(\theta)d\theta$ and

$$\mu_{\mathrm{U}(1)} = \frac{1}{2\pi}\frac{dz}{\sqrt{4-z^2}} = \frac{1}{2\pi}d\theta$$

gives a uniform measure of $\mathrm{U}(1)$ on the eigenangle $\theta \in [-\pi, \pi]$ (see [Sut19, Section 2]). The n^{th} moment $M_n[\mu]$ is the expected value of $\phi_n : z \mapsto z^n$ with respect to μ, computed as

$$M_n[\mu] = \int_I z^n \mu(z),$$

where $I = [-2, 2]$.

Bonus: Moment Statistics (Cont.)

Let U be a random matrix in $\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$ and γ be the component group generator. Denote

$$g_i^k$$

to be the coefficient of T^i in the characteristic polynomial of $U\gamma^k$ (where $0 \leq k \leq \phi(p^2)$).

Note: Frob_p is defined up to conjugacy, so we can think of $\rho_{A,\ell}(\mathrm{Frob}_p)$–a matrix–as representing a conjugacy class. Thus, working with $\mathrm{ST}(A)$ charpolys means inherently working with its conjugacy classes.

Bonus: Moment Statistics (Cont.)

Let U be a random matrix in $\mathrm{ST}^0(\mathrm{Jac}(C_{p^2}))$ and γ be the component group generator. Denote

$$g_i^k$$

to be the coefficient of T^i in the characteristic polynomial of $U\gamma^k$ (where $0 \leq k \leq \phi(p^2)$).

The nth moment $M_n[\mu_i^k]$ is then the expected value of $(g_i^k)^n$, and we compute this by integrating against the Haar measure. Once done, we obtain moment statistics for the entire Sato-Tate group by taking the average of the moments for $U\gamma^k$.

Note: Frob_p is defined up to conjugacy, so we can think of $\rho_{A,\ell}(\mathrm{Frob}_p)$–a matrix–as representing a conjugacy class. Thus, working with $\mathrm{ST}(A)$ charpolys means inherently working with its conjugacy classes.

Bonus: Example of Moment Statistics: C_{25}

Let $p = 5$ ($g = 12$). We first compute the characteristic polynomial of each $U\gamma^k$, where $0 \leq k \leq \phi(25) = 20$.

Bonus: Example of Moment Statistics: C_{25}

Let $p = 5$ ($g = 12$). We first compute the characteristic polynomial of each $U\gamma^k$, where $0 \leq k \leq \phi(25) = 20$.

We found that the g_1^k coefficient (the charpoly of $U\gamma^k$) is 0, unless k is a multiple of 4.

Bonus: Example of Moment Statistics: C_{25}

Let $p = 5$ ($g = 12$). We first compute the characteristic polynomial of each $U\gamma^k$, where $0 \leq k \leq \phi(25) = 20$.

We found that the g_1^k coefficient (the charpoly of $U\gamma^k$) is 0, unless k is a multiple of 4.

Even more surprising, g_1^0 ($k = 0$) has the *largest* number of terms. Naturally, this creates the most complicated integral...

Bonus: Example of Moment Statistics: C_{25}

Let $p = 5$ ($g = 12$). We first compute the characteristic polynomial of each $U\gamma^k$, where $0 \le k \le \phi(25) = 20$.

We found that the g_1^k coefficient (the charpoly of $U\gamma^k$) is 0, unless k is a multiple of 4.

Even more surprising, g_1^0 ($k = 0$) has the *largest* number of terms. Naturally, this creates the most complicated integral...

When $k = 0$, $M_n[\mu_1^0]$ is equal to the value of the following integral

$$\frac{2^n}{(2\pi)^{10}} \int_0^{2\pi} \cdots \int_0^{2\pi} (\cos(\theta_1) + \cdots + \cos(\theta_{10}) \\ + \cos(-\theta_1 + \theta_4 + \theta_5 - \theta_6 + \theta_9) + \cos(-\theta_2 + \theta_3 - \theta_7 + \theta_8 + \theta_{10}))^n \, d\theta_1 \cdots d\theta_{10}.$$

We can see degeneracy manifesting in the last two terms, since we're taking the nth moment of just U here.

Bonus: Example of Moment Statistics: C_{25} (Cont.)

To compute $M_n[\mu_1^k]$ for $k = 4, 8, 12, 16$, we integrate

$$\frac{(\pm 2)^n}{(2\pi)^2} \int_0^{2\pi} \int_0^{2\pi} (\cos(\theta_5) + \cos(\theta_{10}))^n \, d\theta_5 d\theta_{10},$$

where the numerator of the coefficient is 2^n when $k = 4, 12$ and $(-2)^n$ when $k = 8, 12$.

Bonus: Example of Moment Statistics: C_{25} (Cont.)

To compute $M_n[\mu_1^k]$ for $k = 4, 8, 12, 16$, we integrate

$$\frac{(\pm 2)^n}{(2\pi)^2} \int_0^{2\pi} \int_0^{2\pi} (\cos(\theta_5) + \cos(\theta_{10}))^n \, d\theta_5 d\theta_{10},$$

where the numerator of the coefficient is 2^n when $k = 4, 12$ and $(-2)^n$ when $k = 8, 12$.

We then derive the full moment statistics $M_n[\mu_1]$ of the full Sato-Tate group by averaging over the size of the group (i.e., compute up to some moment for each restriction, then divide said moments by the size of the group).

Bonus: L-Polynomials

For primes p of good reduction for C, the zeta function of C is

$$Z(C/\mathbb{F}_p, T) := \exp\left(\sum_{k=1}^{\infty} \frac{\#C(\mathbb{F}_{p^k})T^k}{k}\right) = \frac{\mathrm{L_p(C, T)}}{(1-T)(1-pT)}.$$

Define the normalized L-polynomial as

$$\begin{aligned}\overline{L}_p(C, T) &:= \mathrm{L_p(C, T/\sqrt{p})} \\ &= T^{2g} + a_1 T^{2g-1} + a_2 T^{2g-2} + \cdots + a_2 T^2 + a_1 T + 1,\end{aligned}$$

where $a_i \in \left[-\binom{2g}{i}, \binom{2g}{i}\right]$ and g denotes the genus of C.

The coefficients of $\overline{L}_p(C, T)$ contain important arithmetic information about C

- The a_1 coefficient is the *trace of Frobenius*:

$$a_1 = p + 1 - \#C(\mathbb{F}_p).$$

Bonus: Cyclicity of $(\mathbb{Z}/p^2\mathbb{Z})^\times$

- The map
$$f : \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$$
is a surjective ring homomorphism which restricts to a surjective group homomorphism
$$g : (\mathbb{Z}/p^2\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times.$$
- From the group homomorphism,
$$(\mathbb{Z}/p^2\mathbb{Z})^\times \cong \ker(g) \times (\mathbb{Z}/p\mathbb{Z})^\times,$$
where $\ker(g)$ and $(\mathbb{Z}/p\mathbb{Z})^\times$ are finite cyclic groups of coprime orders.
- Product of two cyclic groups of coprime orders is itself a cyclic group, so $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is a cyclic group.

Christina Birkenhake and Herbert Lange.
Complex abelian varieties, volume 302 of *Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*.
Springer-Verlag, Berlin, second edition, 2004.

Justin Chen, Heidi Goodson, Rezwan Hoque, and Sabeeha Malikah.
Degeneracy and sato-tate groups of $y^2 = x^{p^2} - 1$, 2025.

Andrea Gallese, Heidi Goodson, and Davide Lombardo.
Monodromy groups and exceptional hodge classes, i: Fermat jacobians.
arXiv e-prints, 2024.
arxiv:2405.20394 (95 pages).

Andrea Gallese, Heidi Goodson, and Davide Lombardo.
Monodromy groups and exceptional hodge classes, i: Fermat jacobians.
2025.

Heidi Goodson.
An Exploration of Degeneracy in Abelian Varieties of Fermat Type.
Experimental Mathematics, pages 1–17, June 2024.

Christian Johansson.
On the Sato-Tate conjecture for non-generic abelian surfaces.
Trans. Amer. Math. Soc., 369(9):6303–6325, 2017.
With an appendix by Francesc Fité.

Tetsuji Shioda.
Algebraic cycles on abelian varieties of Fermat type.
Math. Ann., 258(1):65–80, 1981/82.

Andrew V. Sutherland.
Sato-Tate distributions.
In *Analytic methods in arithmetic geometry*, volume 740 of *Contemp. Math.*, pages 197–248. Amer. Math. Soc., Providence, RI, 2019.