Sato-Tate Groups and Distributions of $y^\ell = x(x^\ell - 1)$

Heidi Goodson   Rezwan Hoque

Brooklyn College, City University of New York

Objective

Define $C_\ell/\mathbb{Q}$ as the curve $y^\ell = x(x^\ell - 1)$, where ℓ is an odd prime.

Our goal is to study the limiting distributions of the coefficients of the normalized L-polynomials associated with C_ℓ. Motivated by the findings of this objective, we provide further results on the number of points on C_ℓ over various $\mathbb{F}_q$, where q is an odd prime.

Background

L-Polynomials

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

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

Define the normalized L-polynomial as

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

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*:

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

Goal: Find the limiting distribution of a_i as $p \to \infty$.

Moment Statistics

We can describe the distributions numerically via *moment statistics*.

The nth moment (about 0) of an independent random variable X is $M_n[X] = \mathbb{E}[X^n]$. For a dataset $X = \{x_i\}_{i=1}^m$, the nth moment can also be expressed as

$$M_n[X] = \frac{1}{m}\sum_{i=1}^{m} x_i^n,$$

and for any constant c, $M_n[c] = c^n$.

The Sato-Tate Conjecture

The Sato-Tate conjecture is a statistical statement about the distribution of the number of points on the reduction modulo primes of an elliptic curve defined over $\mathbb{Q}$.

The *generalized* Sato-Tate conjecture attempts to extend this statement to any abelian variety. This version claims the existence of a compact Lie group, the *Sato-Tate group*, that can determine the limiting distribution of the normalized L-polynomials' coefficients via the *Haar measure*.

Our curve, C_ℓ, and its Jacobian are equipped with

- complex multiplication (CM)
- nondegeneracy.

The conjecture is proven to be true for abelian varieties with CM. In addition, there are well-established techniques for computing Sato-Tate groups for nondegenerate abelian varieties.

Preliminaries

Our curve C_ℓ isn't an abelian variety. But, the *Jacobian*, $\mathrm{Jac}(C_\ell)$, is.

- $\mathrm{Jac}(C_\ell)$ is nondegenerate.

A curve automorphism of C_ℓ is

$$\alpha : (x, y) \mapsto (\zeta^\ell x, \zeta^{\ell+1} y),$$

where $\zeta := \zeta_{\ell^2}$.

We define a space of regular differential 1-forms, $\mathcal{B}$, as

$$\mathcal{B} = \left\{\omega_{a,b} := x^a \frac{dx}{y^b} \;\middle|\; \begin{array}{c} 0 \le a \le \ell - 2, \\ a + 1 \le b \le \ell - 1 \end{array}\right\} \implies \alpha^*\omega_{a,b} = \zeta^{\ell(a+1-b)-b}\omega_{a,b}.$$

An endomorphism, α, of $\mathrm{Jac}(C_\ell)$ is then

$$\alpha[j,j] = Z^{\ell(a_j+1-b_j)-b_j},$$

where $0 \le j \le g-1$, $e_j := \langle \ell(a_j + 1 - b_j) - b_j\rangle_{\ell^2}$, and $S := \{e_j\}$.

For $\langle \sigma_n \rangle = \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^2})/\mathbb{Q})$, define $g_i := \langle \ell n(a_i + 1 - b_i) - nb_i\rangle_{\ell^2} = \langle ne_i\rangle_{\ell^2}$. Then, the Galois action on the endomorphism α is

$$^{\sigma_n}\alpha[i,i] = \begin{cases} Z^{g_i} & \text{if } g_i \in S \\ \overline{Z}^{\ell^2 - g_i} & \text{if } g_i \notin S. \end{cases}$$

Since $\mathrm{Jac}(C_\ell)$ is nondegenerate, we can compute the *twisted Lefschetz group* to get $\mathrm{ST}(\mathrm{Jac}(C_\ell))$.

Theorem - The Sato-Tate Group [1]

The **Sato-Tate group**, up to isomorphism in $\mathrm{USp}(2g)$, of $\mathrm{Jac}(C_\ell)$ is

$$\mathrm{ST}(\mathrm{Jac}(C_\ell)) \cong \langle \mathrm{U}(1)^g, \gamma\rangle,$$

where γ is a $2g \times 2g$ block-signed permutation matrix whose ij^{th} block is

$$\gamma[i,j] = \begin{cases} I & \text{if } g_i = e_j \\ J & \text{if } g_i = \ell^2 - e_j \\ 0 & \text{otherwise,} \end{cases}$$

where $0 \le i, j \le g-1$.

Distributions

Let $U \in U(1)^g$ where $U = \mathrm{diag}(u_0, \overline{u}_0, u_1, \overline{u}_1, \ldots, u_{g-1}, \overline{u}_{g-1})$, and denote $\alpha_i := u_i + \overline{u}_i$.

We find the limiting distributions of the L-polynomials by the charpolys of the elements of $\mathrm{ST}(\mathrm{Jac}(C_\ell))$: $U \cdot \gamma^i$, where $0 \le i < \ell(\ell-1)$.

The a_1 Characteristc Polynomial Coefficient

For $i > 0$, $U \cdot \gamma^i = 0$, so $M_n[{}^i\mu_1] = 0$. For $i = 0$, the a_1 coefficient is $\mathrm{tr}(U) = -(\alpha_0 + \alpha_1 + \ldots + \alpha_{g-1})$.

The moment sequence for each α_i is that of the unitary group $\mathrm{U}(1)$:

$$M[\mu_{\mathrm{U}(1)}] = [1, 0, 2, 0, 6, 0, 20, \ldots].$$

By properties of the expected value, we get

$$M_n[\mu_1] = \frac{1}{\ell(\ell-1)} \sum_{b_0+b_1+\ldots+b_{g-1}=n} \binom{n}{b_0, b_1, \ldots, b_{g-1}} M_{b_0}[\alpha_0] M_{b_1}[\alpha_1] \ldots M_{b_{g-1}}[\alpha_{g-1}].$$

Example: $\ell = 5$

The genus of C_5 is $g = \phi(5^2)/2 = 5(4)/2 = 10$, meaning

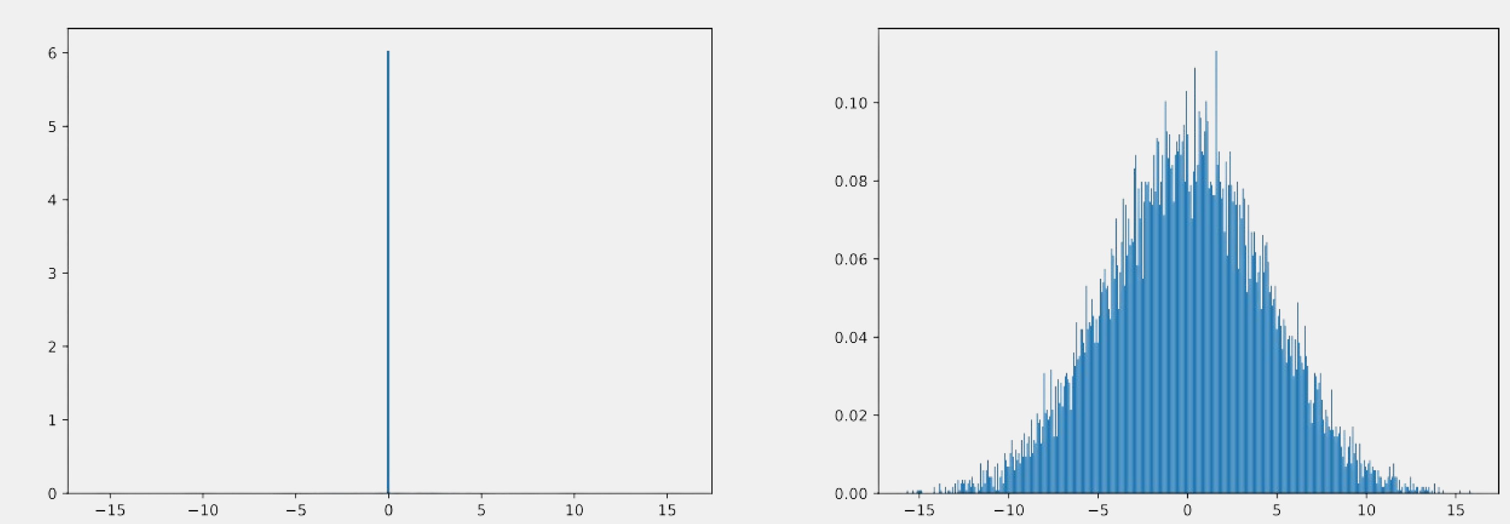
$$\mathrm{ST}(\mathrm{Jac}(C_5)) \cong \langle \mathrm{U}(1)^{10}, \gamma\rangle.$$

The μ_1 moment statistics generated by $\mathrm{ST}(\mathrm{Jac}(C_5))$ are

$$[1, 0, 1, 0, 57, 0, 5140, 0, 615545, \ldots].$$

	M_2	M_4	M_6	M_8
a_1	1.00479	58.4085	5363.22	646563
μ_1	1	57	5140	615545

Table 1. The a_1 and μ_1 moments ($p < 2^{22}$).



(a) For all primes q.

(b) For primes $q \equiv 1 \pmod{25}$.

Figure 1. Histograms of the a_1 coefficients over different $\mathbb{F}_q$.

Theorem - Point Count [1]

If $q \not\equiv 1 \pmod{\ell^2}$, then $\#C_\ell(\mathbb{F}_q) = q + 1$.

Next Steps

- Compute moment statistics for the $a_2, a_3, \ldots, a_g$ coefficients when $\ell = 5, 7, \ldots$
- Improve bounds for computing the numerical moments.
- Study other families of curves!

Acknowledgements

This research collaboration initiated through the Tow Mentoring and Research Program at Brooklyn College, City University of New York. We are grateful for this support provided by the Tow Foundation. Our research was also supported by a grant from the National Science Foundation (DMS - 2201085).

References

[1] Heidi Goodson and Rezwan Hoque. Sato-tate groups and distributions of $y^\ell = x(x^\ell - 1)$. *arXiv e-prints*, page arXiv:2412.02522, 2024.