Second Moment Distributions Associated to Elliptic Surfaces

Lawrence Dillon (lvid@uw.edu)

Joint work with Pramana Saldin (saldin@wisc.edu), Bartosz Naskręcki (nasqret@gmail.com), and Matija Kazalicki (matija.kazalicki@gmail.com).

Advised by Steven J. Miller (sjm1@williams.edu)

SMALL REU 2025, Maine-Québec 2025

Elliptic Surface

- Define an elliptic surface $\pi : \mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}}$ (proper, flat, etc.).
- The generic fiber $\pi^{-1}(\eta)$ gives an elliptic curve over the function field $\mathbb{Q}(T)$.
- This curve has discriminant $\Delta(T)$, finitely many singular specializations over the base.
- Define $U = \{t \in \mathbb{P}^1 : \Delta(t) \neq 0\}$. Then $\pi : \mathcal{E} \to U$ is smooth locus.

Trace of Frobenius

- For a a fixed $E/\mathbb{Q}$, we care about $a(p) = p + 1 - \#E(\mathbb{F}_p)$.
- Why? Because they encode a ton of arithmetic information, both algebraically (cohomology) and analytically (coefficients of Hasse-Weil L-function).

Moments

- For the surface $\pi : \mathcal{E} \to U$, we may care to understand $a_t(p)$ as $t \in U$ varies over the base.
- First, reduce mod p by a base change $\mathcal{E}' \to \mathbb{P}^1(\mathbb{F}_p)$, then there are only finitely many fibers.
- Now define

$$A_1(p) = \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} a_t(p) - a_\infty(p), \quad A_2(p) = \sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} a_t(p)^2 - a_\infty^2(p).$$

Michel's Result

Theorem ([Mic95])

For an elliptic surface $\pi : \mathcal{E}_T \to \mathbb{P}^1$ with non-constant j-invariant, we have

$$A_2(p) = p^2 + O(p^{3/2}).$$

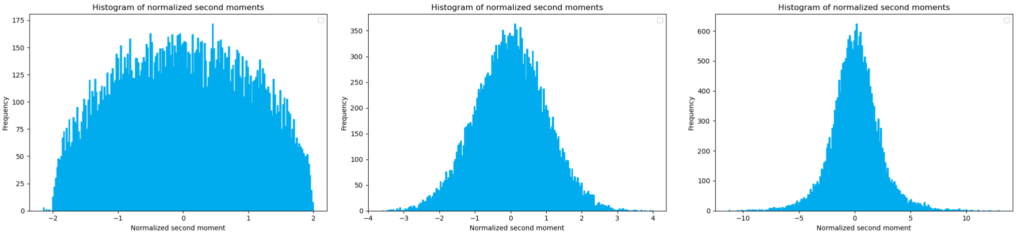
Moreover, there are exactly four lower-order terms; they are $O(p^{3/2})$, $O(p)$, $O(p^{1/2})$, and $O(1)$ respectively and each has a cohomological interpretation.

This suggests that we can normalize to isolate some weight-3 contribution, defining

$$B_2(p) := \frac{A_2(p) - p^2}{p^{3/2}}.$$

$B_2(p)$ as a random variable

- Cheek et al. [CGJ$^+$24] plotted $B_2(p)$ as $p \to \infty$ over the primes.
- Treating $B_2(p)$ as a *random variable*, we may be interested in the moments of its distribution.



Conjecture

They conjectured the following:

Conjecture

For an elliptic surface $\mathcal{E}_T$, the variance of $B_2(p)$ is always an integer.

After collecting more data, we believe that all moments should be integral.

Pencils of Cubics

- We say an elliptic surface $\pi : \mathcal{E} \to \mathbb{P}^1_{\mathbb{Q}}$ is a *pencil of cubics* if the generic fiber $E/\mathbb{Q}(T)$ has a model of the form

$$E : y^2 = P(x)T + Q(x)$$

  where $\deg P(x), \deg Q(x) \leq 3$ That is, we need the Weierstrass equation to be linear in the varying parameter.
- Professors Matija Kazalicki and Bartosz Naskręcki recently confirmed Steven J. Miller's *bias conjecture* for the class of pencils of cubics [KN25].
- In doing so, they give explicit formulae for the second moment $A_2(p)$ of such families.

Confirmation of the integral moment conjecture

- Using their work, we were able to confirm our conjecture in this case.
- Moreover, the distribution of $B_2(p)$ always ended up being distributed as $-b(p)$, where $b(p)$ is the trace on a fixed genus one or two curve.
- The only issue arises in the so-called *typical* case.

Example (Typical Case)

$$\mathcal{A}_{2,\mathcal{E}}(p) = p^2 - p \cdot d_p - p \cdot \#S(\mathbb{F}_p) - a_\infty^2(p)$$

Example (Typical Case)

$$\mathcal{A}_{2,\mathcal{E}}(p) = p^2 - p \cdot d_p - p \cdot \#S(\mathbb{F}_p) - a_\infty^2(p)$$

$$\mathcal{B}_{2,\mathcal{E}}(p) = \frac{\mathcal{A}_{2,\mathcal{E}}(p) - p^2}{p^{3/2}} = -\frac{d_p}{\sqrt{p}} - \frac{\#S(\mathbb{F}_p)}{\sqrt{p}} - \frac{a_\infty^2}{p^{3/2}}.$$

Average over p to compute moments. We find that $B_2(p)$ is distributed exactly as $d_p/\sqrt{p}$.

Distribution of $d_p/\sqrt{p}$

$\mathcal{B}_{2,\mathcal{E}}(p) \sim d_p/\sqrt{p}$, so it suffices to show all moments are integers.

- In the "typical" case considered in their paper, $\overline{D}$ is genus 2.

Distribution of $d_p/\sqrt{p}$

$\mathcal{B}_{2,\mathcal{E}}(p) \sim d_p/\sqrt{p}$, so it suffices to show all moments are integers.

- In the "typical" case considered in their paper, $\overline{D}$ is genus 2.
- Hence, we can use the classification of Sato-Tate distributions for genus 2 curves [FKRS12].

Distribution of $d_p/\sqrt{p}$

$\mathcal{B}_{2,\mathcal{E}}(p) \sim d_p/\sqrt{p}$, so it suffices to show all moments are integers.

- In the "typical" case considered in their paper, $\overline{D}$ is genus 2.
- Hence, we can use the classification of Sato-Tate distributions for genus 2 curves [FKRS12].
- All of these distributions have integer moments.

Distribution of $d_p/\sqrt{p}$

$\mathcal{B}_{2,\mathcal{E}}(p) \sim d_p/\sqrt{p}$, so it suffices to show all moments are integers.

- In the "typical" case considered in their paper, $\overline{D}$ is genus 2.
- Hence, we can use the classification of Sato-Tate distributions for genus 2 curves [FKRS12].
- All of these distributions have integer moments.
- For generic curves, whose Jacobian has small endomorphism group, the Sato-Tate conjecture has been verified and so we're done.

Distribution of $d_p/\sqrt{p}$

$\mathcal{B}_{2,\mathcal{E}}(p) \sim d_p/\sqrt{p}$, so it suffices to show all moments are integers.

- In the "typical" case considered in their paper, $\overline{D}$ is genus 2.
- Hence, we can use the classification of Sato-Tate distributions for genus 2 curves [FKRS12].
- All of these distributions have integer moments.
- For generic curves, whose Jacobian has small endomorphism group, the Sato-Tate conjecture has been verified and so we're done.
- In general, assuming Sato-Tate for genus two curves, we have the result. ■
- It turns out that all other (non-typical) cases can be proven unconditionally.

Algebraic Approach

Let $i : U \hookrightarrow \mathbb{P}^1_{\mathbb{Q}}$ be the inclusion.

- For any $\ell \neq p$, form the ℓ-adic lisse sheaf $\mathcal{F} := R^1\pi_*\mathbb{Q}_\ell$ on the base U.
- By Deligne, $i_*\mathrm{Sym}^m\mathcal{F}$ is rank two and pure of weight m. [Del80]
- We have the following results [KN25]:

Algebraic Approach

Putting $W_{m,\ell} = H^1_{\text{ét}}(\mathbb{P}^1 \otimes \overline{\mathbb{Q}}, i_*\mathrm{Sym}^m\mathcal{F}_\ell)$ and letting $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ denote a geometric Frobenius, we can compute traces fiber by fiber:

$$\mathrm{Trace}(\mathrm{Frob}_p | W_{m,\ell}) = -\sum_{t \in \mathbb{P}^1(\mathbb{F}_p)} \mathrm{Trace}(\mathrm{Frob}_p | (i_*\mathrm{Sym}^m\mathcal{F}_\ell)_t). \tag{1}$$

Algebraic Approach

Secondly, we have the following formulas. If the fiber $E_t = \pi^{-1}(t)$ is smooth, then

$$\mathrm{Trace}(\mathrm{Frob}_p|(i_*\mathrm{Sym}^1\mathcal{F}_\ell)_t) = p + 1 - \#E_t(\mathbb{F}_p) = a_t(p) \tag{2}$$

and

$$\mathrm{Trace}(\mathrm{Frob}_p|(i_*\mathrm{Sym}^2\mathcal{F}_\ell)_t) = \mathrm{Trace}(\mathrm{Frob}_p|(i_*\mathrm{Sym}^1\mathcal{F}_\ell)_t)^2 - p = a_t(p)^2 - p \tag{3}$$

If the fiber E_t is singular, then

$$\mathrm{Trace}(\mathrm{Frob}_p|(i_*\mathrm{Sym}^1\mathcal{F}_\ell)_t) = \begin{cases} 1 & \text{if the fiber is split multiplicative} \\ -1 & \text{if the fiber is nonsplit multiplicative} \\ 0 & \text{if the fiber is additive.} \end{cases}$$

Analogy

- Putting this all together, we have

$$-\,\mathrm{Trace}(\mathrm{Frob}_p | W_{2,\ell}) = \sum_{t \notin S} a_t(p)^2 - p^2 + O(p). \tag{4}$$

- Averaging over primes, this gives that the moments of $B_2(p)$ are the same as those of $-\mathrm{Trace}(\mathrm{Frob}_p | W_{2,\ell})/p^{3/2}$.
- This is analogous with our above results, assuming some equidistribution on the left.

The idea

- Condier an elliptic surface with fibers $\mathcal{E}_T : y^2 = x^3 + A(T)x + B(T)$.
- We can form a sequence of families by considering

$$\mathcal{E}_{T^n} : y^2 = x^3 + A(T^n)x + B(T^n).$$

- How does the variance of $B_2(p)$ change as n varies? There are some nice patterns.

Examples

- The family $\mathcal{E}_T : y^2 = x^3 + (T+1)x + (T+1)$ has nice properties.
- When $n = q^m$ is a prime power, we noticed numerically that the variance of $B_2(p)$ over $\mathcal{E}_{T^{q^m}}$ seems to always be m, the exponent in the prime power.
- There aren't a ton of tools to prove observations like this hold in general. There are heuristics. The map $t \mapsto t^n$ has degree $\gcd(n, p-1)$ on $\mathbb{F}_p$. We average
$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} \gcd(q^m, p-1) = m+1.$$
Using this and assuming the achieved fibers are *random enough*, we can prove the observation.

Modular Example

1. Another tractable case is 2-covers of universal elliptic curves.
2. Example: consider the universal elliptic curve over $\Gamma_1(6)$.
3. Deligne: traces on $\mathrm{Sym}^2\mathcal{F} \longleftrightarrow$ coefficients of unique newform $f \in S_4(\Gamma_1(6))$. [Del71]
4. Rankin-Selberg method and "guessing representations": Let $g \in S_4(\Gamma_1(12))$ be the unique newform, then the trace we want to compute is

$$= \begin{cases} 2a_f(p) + a_g(p) & p \equiv 1 \mod 4 \\ -a_g(p) & p \equiv 3 \mod 4. \end{cases}$$

Averaging over primes gives variance of original family 1 with variance of 2-cover 3. This matches our data.

Acknowledgements

We are grateful to Professor Steven J. Miller for introducing us to this area of research and for his continued mentorship.

We're additionally grateful to Professors Kazalicki and Naskręcki for their frequent correspondence.

This research was supported by the National Science Foundation, under grant DMS2241623, the University of Washington, and the University of Wisconsin.

References I

Timothy Cheek, Pico Gilman, Kareem Jaber, Steven J. Miller, Vismay Sharan, and Marie-Hélène Tomé, *Lower order biases in moment expansions of one parameter families of elliptic curves*, 2024.

Pierre Deligne, *Formes modulaires et représentations ℓ-adiques*, Séminaire Bourbaki : vol. 1968/69, exposés 347-363, Séminaire Bourbaki : vol. 1980/81, exposés 561-578, no. 11, Springer-Verlag, Berlin/Heidelberg, 1971, talk:355, pp. 139–172 (fr).

______, *La conjecture de Weil : II*, Publications Mathématiques de l'IHÉS **52** (1980), 137–252 (fr). MR 601520

Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland, *Sato-tate distributions and galois endomorphism modules in genus 2*, Compositio Mathematica **148** (2012), no. 5, 1390–1442.

References II

- Matija Kazalicki and Bartosz Naskręcki, *Second moments and the bias conjecture for the family of cubic pencils*, 2025.
- Philippe Michel, *Rang moyen de familles de courbes elliptiques et lois de sato-tate*, Monatshefte für Mathematik **120** (1995), no. 2, 127–136.