Sato-Tate Groups, Elliptic Curves, and Second Moment Distributions

Lawrence Dillon (lvid@uw.edu)
Pramana Saldin (saldin@wisc.edu)

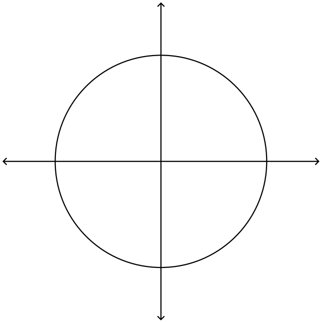
Joint work with Steve Zanetti (szanetti@umich.edu)
Advised by Steven J. Miller (sjm1@williams.edu)

SMALL REU 2025
Yale, July 23, 2025

Algebraic Curves

A **curve** is a zero set of some polynomial over a field. For example:

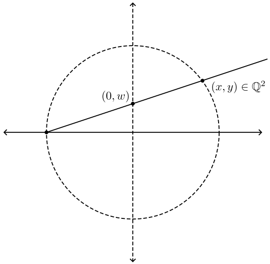
$$C\colon x^2 + y^2 = 1 \text{ over } \mathbb{R}.$$



Algebraic Curves (and Arithmetic!)

Solutions over $\mathbb{Q}$ correspond in some sense to solutions over $\mathbb{Z}$ (e.g. clear denominators), so it encodes arithmetic properties.

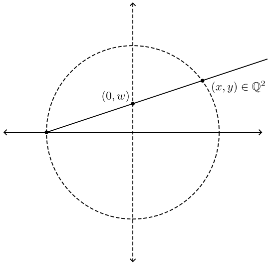
$$C\colon x^2 + y^2 = 1 \text{ over } \mathbb{Q}.$$



Algebraic Curves (and Arithmetic!)

Solutions over $\mathbb{Q}$ correspond in some sense to solutions over $\mathbb{Z}$ (e.g. clear denominators), so it encodes arithmetic properties.

$$C\colon x^2 + y^2 = 1 \text{ over } \mathbb{Q}.$$



The solution set to $x^2 + y^2 = 1$ in $\mathbb{Q}$ encodes the information of pythagorean triples $x^2 + y^2 = z^2$ in $\mathbb{Z}$.

An important invariant: genus

- **Idea:** A curve in $\mathbb{C}^2$ is 1 $\mathbb{C}$-dimensional, so it is 2 $\mathbb{R}$-dimensional. So every curve corresponds to a surface.

An important invariant: genus

- **Idea:** A curve in $\mathbb{C}^2$ is 1 $\mathbb{C}$-dimensional, so it is 2 $\mathbb{R}$-dimensional. So every curve corresponds to a surface.
- **Genus** is a topological invariant of surfaces. It counts the number of holes. This is an invariant of curves as well.

What's an Elliptic Curve?

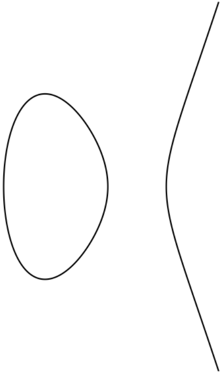
Formally, smooth curve of genus 1. Easier over $\mathbb{Q}$: an elliptic curve E is given by

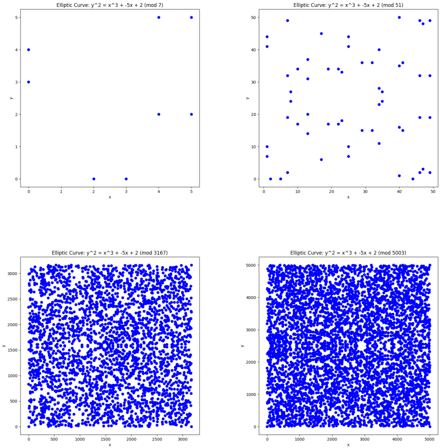
$$E\colon y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$, $4a^3 + 27b^2 \neq 0$.

- They are of study throughout number theory.
- They are one of the main objects used in the proof of Fermat's Last Theorem.

What's an Elliptic Curve?





Counting Points

The mod p reductions looked very chaotic, we need tools to help understand them.

Define the Legendre symbol: for $a \in \mathbb{N}$ and p a prime,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a non-zero square mod p} \\ -1 & \text{if a is not a non-zero square mod p} \\ 0 & \text{if } a \equiv 0 \mod p \end{cases}$$

Important observation: $1 + \left(\frac{a}{p}\right)$ is the number of solutions to $y^2 = a \mod p$.

Sato-Tate Distributions over $\mathbb{Q}$

That is, $\#E(\mathbb{F}_p) = \sum_{x=0}^{p-1}\left[1 + \left(\frac{x^3+ax+b}{p}\right)\right] + \text{point at } \infty = p + 1 + a(p)$.

We wish to understand how $a(p)$ varies with p.

Sato-Tate Distributions over $\mathbb{Q}$

That is, $\#E(\mathbb{F}_p) = \sum_{x=0}^{p-1}\left[1 + \left(\frac{x^3+ax+b}{p}\right)\right] + \text{point at } \infty = p + 1 + a(p)$.

We wish to understand how $a(p)$ varies with p.

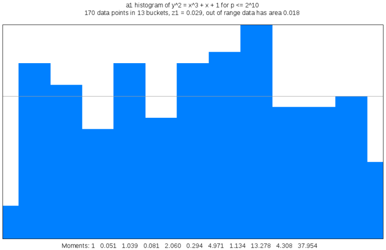
Theorem (Sato-Tate Conjecture, 2011)

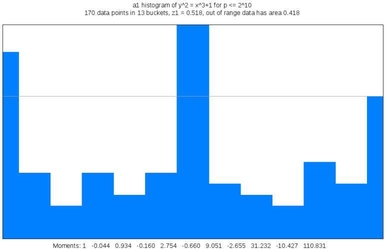
Let E be an elliptic curve without complex multiplication. As $p \to \infty$, the sequence $\{\frac{a(p)}{\sqrt{p}}\}_p$ becomes equidistributed according to the density

$$\mathrm{d}\mu_{ST} = \frac{\sqrt{4-x^2}}{2\pi}\mathrm{d}x$$

which is compactly supported on $[-2, 2]$.

Sato-Tate Distributions over $\mathbb{Q}$

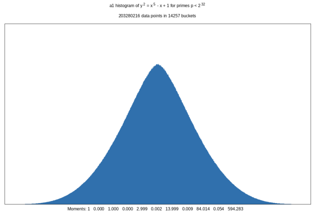


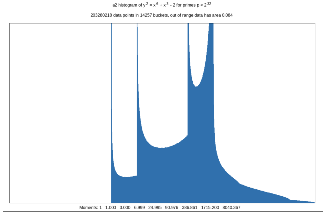


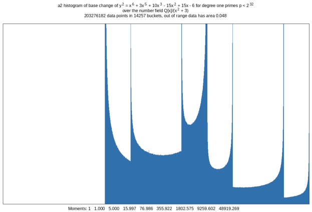
https://math.mit.edu/~drew/g1_D1_a1f.gif
https://math.mit.edu/~drew/g1_D2_a1f.gif

Genus 2

The above come from the Haar measure on certain subgroups of the compact group USp(2). To classify Sato-Tate distributions of genus 2 curves, use USp(4). Exactly 34 possibilities over $\mathbb{Q}$.







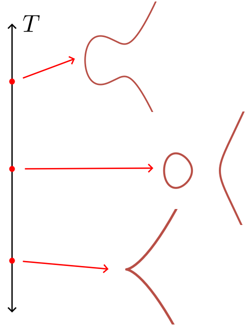
Families of curves

Idea: Allow a free parameter T to vary. One elliptic curve for each T:

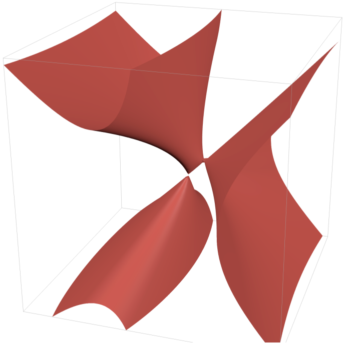
$$\mathcal{E}_T\colon y^2 = x^3 + A(T)x + B(T),$$

where $A(T), B(T) \in \mathbb{Q}(T)$.

Families of curves



(a) Elliptic curve fibers



(b) Plot of $\mathcal{E}_T$ in $\mathbb{R}^3$

Figure: $t \in \mathbb{Q}$ gives an elliptic curve $y^2 = x^3 + A(t)x + B(t)$.

The Bias Conjecture

Definition

The second moment of the bias is defined as

$$\mathcal{A}_{2,\mathcal{E}}(p) := \sum_{t \in \mathbb{F}_p} a_{\mathcal{E}(t)}(p)^2.$$

The Bias Conjecture

Definition

The second moment of the bias is defined as

$$\mathcal{A}_{2,\mathcal{E}}(p) := \sum_{t \in \mathbb{F}_p} a_{\mathcal{E}(t)}(p)^2.$$

Theorem (Second moment asymptotic (Michel) [Mic95])

For families $\mathcal{E}$ with $j(T)$ non-constant,

$$\mathcal{A}_{2,\mathcal{E}}(p) = p^2 + O(p^{3/2}).$$

The Bias Conjecture

Definition

The second moment of the bias is defined as

$$\mathcal{A}_{2,\mathcal{E}}(p) := \sum_{t \in \mathbb{F}_p} a_{\mathcal{E}(t)}(p)^2.$$

Theorem (Second moment asymptotic (Michel) [Mic95])

For families $\mathcal{E}$ with $j(T)$ non-constant,

$$\mathcal{A}_{2,\mathcal{E}}(p) = p^2 + O(p^{3/2}).$$

The lower order terms are $p^{3/2}$, p, $p^{1/2}$ and 1.

The Bias Conjecture

Theorem (Second moment asymptotic (Michel) [Mic95])

For families $\mathcal{E}$ with $j(T)$ non-constant,

$$\mathcal{A}_{2,\mathcal{E}}(p) = p^2 + O(p^{3/2}).$$

Conjecture (Bias conjecture, Steven J. Miller ’02)

The largest non-zero lower order term in $\mathcal{A}_{2,\mathcal{E}}(p)$ is on average negative as p runs through the primes.

The Bias Conjecture

Theorem (Second moment asymptotic (Michel) [Mic95])

For families $\mathcal{E}$ with $j(T)$ non-constant,

$$\mathcal{A}_{2,\mathcal{E}}(p) = p^2 + O(p^{3/2}).$$

Conjecture (Bias conjecture, Steven J. Miller '02)

The largest non-zero lower order term in $\mathcal{A}_{2,\mathcal{E}}(p)$ is on average negative as p runs through the primes.

One way to disprove the bias conjecture: $\mathcal{E}_T$ such that

$$\mathcal{B}_{2,\mathcal{E}}(p) := \frac{\mathcal{A}_{2,\mathcal{E}}(p) - p^2}{p^{3/2}}$$

averages to a negative value.

Why Do We Care?

- "Rank" of elliptic surface (family of elliptic curves) related to first moment
- Applications to Katz-Sarnak conjecture
- Order of vanishing of L-functions associated to the family
- Higher moments show family-specific behavior (rate of convergence)

Pencils of cubics

Given a family $y^2 = x^3 + A(T)x + B(T)$, we can think of it as a surface $\pi \colon \mathcal{E}_T \to \mathbb{P}^1$ fibered in elliptic curves.

Pencils of cubics

Given a family $y^2 = x^3 + A(T)x + B(T)$, we can think of it as a surface $\pi\colon \mathcal{E}_T \to \mathbb{P}^1$ fibered in elliptic curves.

Let's specialize to the case

$$\mathcal{E}_T\colon y^2 = P(x)T + Q(x)$$

where $\deg P(x), \deg Q(x) \leq 3$. This is a **pencil of cubics.**

Some Algebraic Geometry

Proposition (SMALL 2025)

Let

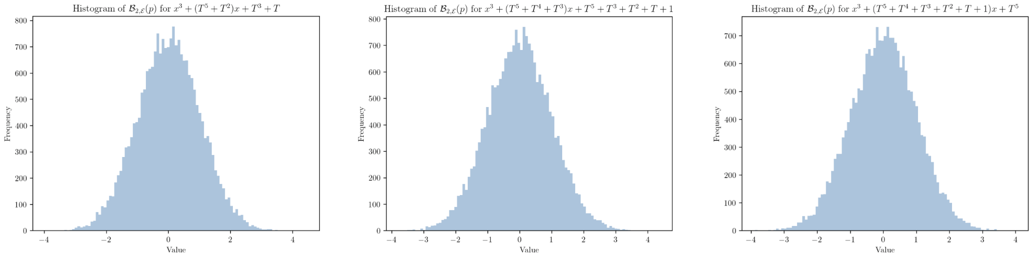
$$\mathcal{E}_T : y^2 = P(x)T + Q(x)$$

be a pencil of cubics. If the curve is "generic"[a] *all moments of* $\mathcal{B}_{2,\mathcal{E}}$ *are integers.*

[a] and the associated pair $(\widetilde{\Delta}, \widetilde{C})$ to $\mathcal{E}$ is K*-typical*,

Previous numerical investigations/motivation

Motivation from last year's SMALL [CGJ$^+$24]:



Variance = 1.0151610262691482 | Variance = 1.0046817588446215 | Variance = 0.9891139950619033

Figure: SMALL 2024's numerical evidence suggests the second moment converges to an integer.

Some Algebraic Geometry

The following approach is taken from Professors Bartosz Naskręcki and Matija Kazalicki's paper [KN25].

Proof. To the elliptic surface $\pi : \mathcal{E}_T \to \mathbb{P}^1$ associate a threefold

$$M \subset \mathbb{A}^1 \times \mathbb{A}^1 \times \mathbb{P}^1 \times \mathbb{A}^1$$

whereby they show in [Theorem 2.2] that

$$\#M(\mathbb{F}_p) = p^3 + p^2 + \widetilde{A}_{2,\mathcal{E}}(p).$$

This allows us to attack the problem through arithmetic geometry.

Computing the distribution of $\mathcal{B}_2(p)$

It follows from their main results, [Prop 3.15, Cor 3.19] that in our special case we have the explicit formula

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

where

1. d_p is the trace on some curve $\overline{D}$,
2. S is a polynomial,
3. $a_\infty^2(p)$ is the contribution of the fiber at infinity.

Computing the distribution of $\mathcal{B}_2(p)$

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

Computing the distribution of $\mathcal{B}_2(p)$

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

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

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 the generalized Sato-Tate conjecture allows us to compute the distribution. ∎

Our Other Work

- Again, assuming the generalized Sato-Tate conjecture, we prove this result for more families of elliptic curves.

Our Other Work

- Again, assuming the generalized Sato-Tate conjecture, we prove this result for more families of elliptic curves.
- We have expanded data from SMALL 2024: $p \leq 250\,000 \to p \leq 1\,000\,000$. This allows for deeper numerical investigations.

Acknowledgements

We are grateful to Professor Steven J. Miller for suggesting this problem and for his mentorship.

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.
- 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.
- 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.