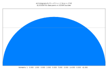
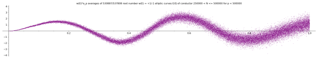
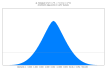
Sato–Tate distributions and murmurations

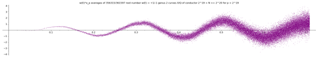
Andrew V. Sutherland
MIT

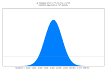
March 21, 2025

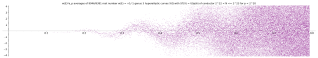












Sato

As explained by Ihara, in 1962 Mikio Sato returned to the University of Tokyo after visiting IAS with an interest in the following question about the sequence of Frobenius eigenangles ϑ_p associated to an elliptic curve $E/\mathbb{Q}$ at primes p of good reduction.

How is ϑ_p distributed on $[0, \pi]$ as p varies over primes?

The university had recently installed a HIPAC 103 computer, and several young researchers and students had started "playing" with it, including Kanji Namba.

> *... on a nice summer evening, Sato and some of his colleagues, including Namba, instead of parting at the Ikebukuro suburban train terminal were drawn to a roof beer garden on a department store. Then Sato, explaining the beauty of arithmetic of elliptic curves and modular forms, said to Namba something like "why not use the new computer for something more worthwhile than examining the Goldbach conjecture; for example, for collecting data for this question".*

HIPAC 103

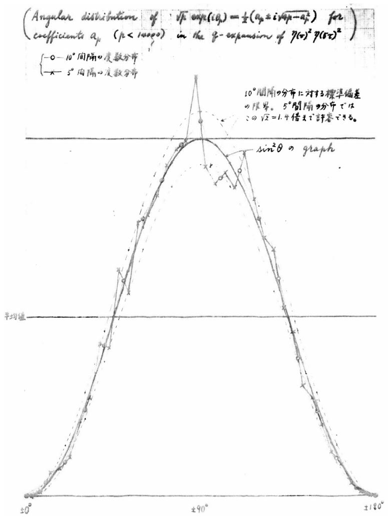
The **HI**tachi **P**arametron **A**utomatic **C**omputer used 48-bit words and had a 13-bit address space. It came equipped with 1024 words of core memory (6KB) and 8192 words of magnetic drum storage (48KB). It used resonant circuits ("parametrons") rather than vacuum tubes or transistors.

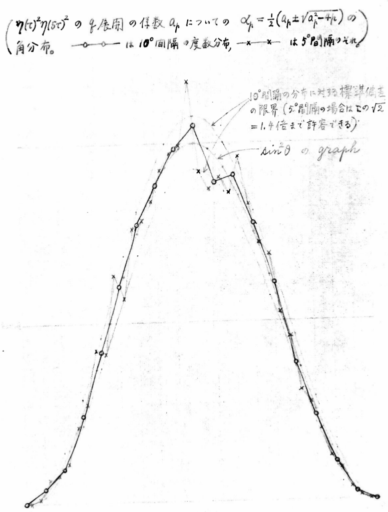
As explained by Namba, Mr. Nagashima, a staff member in the department of mathematics, ran a computer program that computed the q-expansion of the weight-2 Hecke eigenform $f(z)$ of level 20 (20.2.a.a) using the product formula

$$f(z) = \eta(2z)^2\eta(10z)^2 = \sum_{n\geq 1} a_n q^n = q\prod_{n=1}^{\infty}(1-q^{2n})^2(1-q^{10n})^2.$$

Since $a_n = 0$ for n even, they could store 7000 odd values of a_n, including a_p at 1650 primes of good reduction (they needed the other 1192 words of storage for the code).

The $\sin^2\vartheta$-law (May 15, 1963 letter from Sato to Namba)





The $\sin^2 \vartheta$-law

In the letter Sato wrote to Namba in May, 1963 (as translated by Namba in a March 2007 letter to Ralf Schmidt)

> *. . . according to the figure and table, it is estimated that the angular distribution of α_p is proportional to* $\sin^2 \vartheta$*. It could be said that the above hypothesis is very plausible.*

Here $\alpha_p = \sqrt{p}e^{i\vartheta_p}$ and $\bar{\alpha}_p = \sqrt{p}e^{-i\vartheta_p}$ are p-Weil numbers with $a_p = \alpha_p + \bar{\alpha}_p$. Sato continued

> *This fact is, I think, probably, if we spend sufficiently long time and deep conversation, even under our present knowledge, it would be possible to explain theoretically, but now, I would like to postpone such heavy brain work, and instead, collect experimental muscular obtainable data.*

Tate

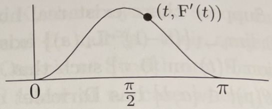
Let k be a finitely generated field, X/k a nice variety, and $\ell \neq \mathrm{char}(k)$ a prime.
In his 1964 Woods Hole lectures Tate presented several conjectures, including those denoted T^r, E^r, I^r, S^r in Poonen's talk, as well as

$$P^r : \zeta_X^{2r}(s) \text{ has a pole of order } \dim_{\mathbb{Q}_\ell} \mathrm{H}^{2r}(\overline{X}, \mathbb{Q}_\ell(r))^{\mathrm{Gal}_k} \text{ at } s = r.$$

In his August 1963 letters to Serre, Tate explains that under P^r, if $E/\mathbb{Q}$ is a non-CM elliptic curve, then its Frobenius eigenangles ϑ_p have a $\frac{2}{\pi}\sin^2\vartheta$ distribution. He writes

> *Mumford tells me that Sato has found* $c\sin^2\vartheta$ *experimentally by machine on one curve with thousands of p — many more p than your computation. Did you ever have your distribution analyzed and do they all look like* $\sin^2\vartheta$*????*

$$dF(t) = \frac{1}{\pi}(1 - \cos 2t)\, dt = \frac{2}{\pi}\sin^2 t\, dt.$$



The Sato-Tate distribution

Fix an elliptic curve $E/\mathbb{Q}$. For each good prime p the trace of Frobenius

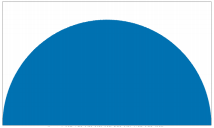
$$a_p := p + 1 - \#E_p(\mathbb{F}_p)$$

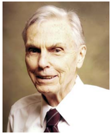
satisfies $|a_p| \leq 2\sqrt{p}$. Let $x_p := -a_p/\sqrt{p} \in [-2, 2]$. If E does not have CM then $(x_2, x_3, x_5, x_7, x_{11}, \ldots)$ should be equidistributed with respect to the measure

$$\frac{2}{\pi}\sqrt{4 - x^2}dx$$

If we construct a histogram of x_p-values for $p \leq B$ and rescale by $\frac{\pi}{2}$, as B tends to infinity our histogram should converge to a semicircle of radius 2.

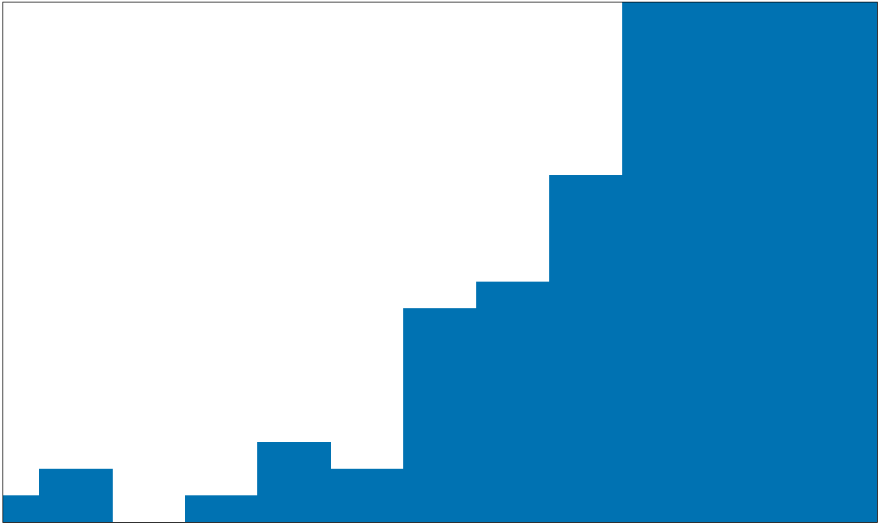

Mikio Sato




John Tate

a1 histogram of $y^2 + xy = x^3 - 27006183241630922218434652145297453784768054621836357954737385x$
$+ 55258058551342376475736699591118191821521067032535079608372404779149413277716173425636721497$ for primes $p < 2^{10}$

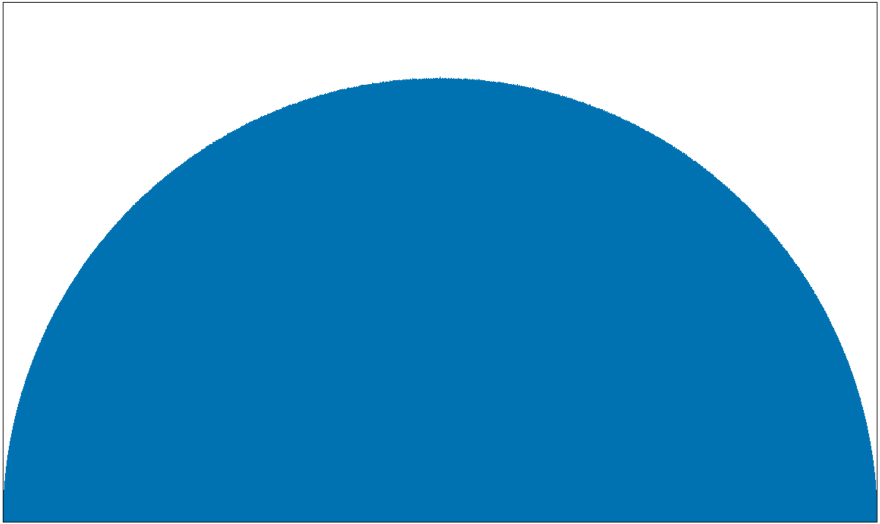
159 data points in 13 buckets, z1 = 0.025, out of range data has area 0.252



Moments: 1 1.114 1.775 2.579 4.523 7.055 12.986 20.973 39.725 65.587 126.589

a1 histogram of $y^2 + xy = x^3 - 27006183241630922218434652145297453784768054621836357954737385x + 55258058551342376475736699591118191821521067032535079608372404779149413277716173425636721497$ for primes $p < 2^{40}$

41203088782 data points in 202985 buckets



Moments: 1 0.000 1.000 0.000 2.000 0.000 5.000 0.001 14.000 0.002 42.001

Sato–Tate theorems

Theorem (Barnet–Lamb, Clozel, Gee, Geraghty, Harris, Shepherd–Barron, Taylor 2008, 2010, 2011)

Let E be an elliptic curve without complex multiplication over a totally real field. The sequence x_p converges to the semi-circular distribution.

Theorem (Allen, Calegari, Caraiani, Gee, Helm, Le Hung, Newton, Scholze, Taylor, Thorne 2022)

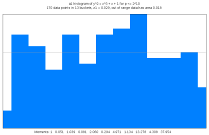
Let E be an elliptic curve without complex multiplication over a CM field. The sequence x_p converges to the semi-circular distribution.

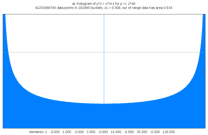
The Sato–Tate conjecture remains open for elliptic curves over number fields that are neither totally real nor CM. The first such field (ordered by $|D_k|$) is $\mathbb{Q}[x]/(x^3 - x^2 + 1)$.

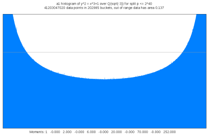
Sato-Tate groups in dimension 1

The Sato-Tate group of E is a closed subgroup G of $\mathrm{SU}(2) = \mathrm{USp}(2)$ that is determined by the ℓ-adic Galois representation attached to E (as we will explain).

G	G/G^0	E	k	$\mathrm{M}_{2n}[\mathrm{tr}(g)]_{n\geq 0}$
$\mathrm{SU}(2)$	C_1	$y^2 = x^3 + x + 1$	$\mathbb{Q}$	$1, 1, 2, 5, 14, 42, \ldots$
$N(\mathrm{U}(1))$	C_2	$y^2 = x^3 + 1$	$\mathbb{Q}$	$1, 1, 3, 10, 35, 126, \ldots$
$\mathrm{U}(1)$	C_1	$y^2 = x^3 + 1$	$\mathbb{Q}(\zeta_3)$	$1, 2, 6, 20, 70, 252, \ldots$







Fun fact: $\displaystyle\int_{\mathrm{SU}(2)} \mathrm{tr}(g)^n dg = \frac{1}{2\pi}\int_0^\pi (2\cos\vartheta)^n \sin^2\vartheta\, d\vartheta$ is the $\frac{n}{2}$th Catalan number!

Zeta functions and L-polynomials

For a nice curve $X/\mathbb{Q}$ of genus g and each good prime p we have the zeta function

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

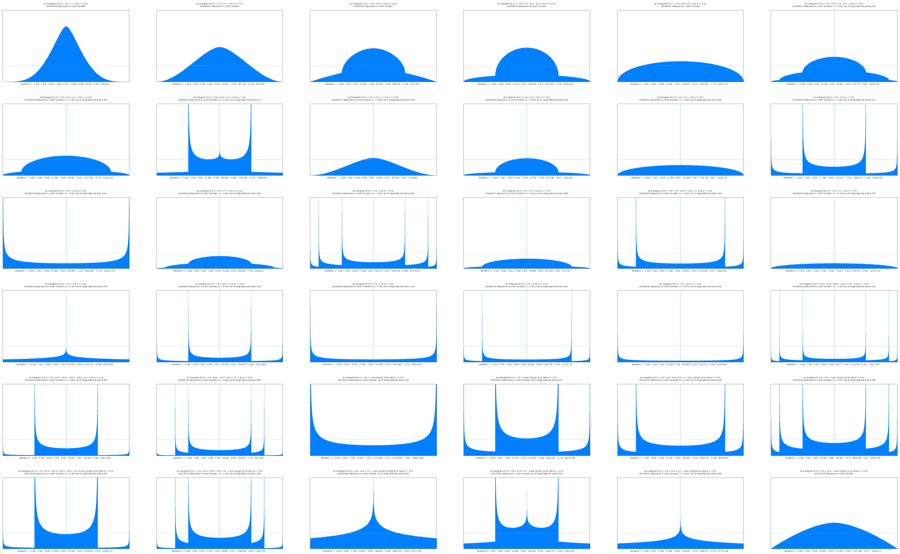
where $L_p \in \mathbb{Z}[T]$ has degree $2g$. The normalized L-polynomial

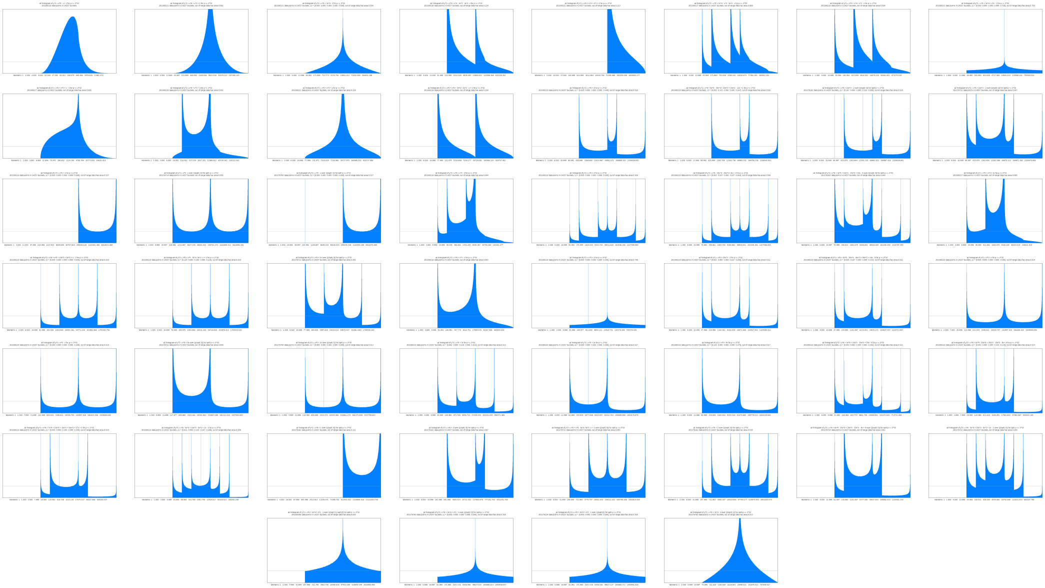
$$\bar{L}_p(T) := L_p(T/\sqrt{p}) = \sum_{i=0}^{2g} a_i T^i \in \mathbb{R}[T]$$

is monic, reciprocal, and unitary, with $|a_i| \le \binom{2g}{i}$ (better bounds hold for even i).

Now consider the limiting distribution of $a_1, a_2, \ldots, a_g$ over good primes $p \le B \to \infty$.

Sato-Tate trace distributions of genus 2 curves





The Sato-Tate group of an abelian variety

Let A be an abelian variety over a number field k. The Zariski closure of the image of

$$\rho_\ell\colon \mathrm{Gal}_k \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell(A)) \simeq \mathrm{GSp}_{2g}(\mathbb{Q}_\ell)$$

is a $\mathbb{Q}_\ell$-algebraic group $G_\ell^{\mathrm{zar}} \subseteq \mathrm{GSp}_{2g}$, and we let $G_\ell^{1,\mathrm{zar}} := G_\ell^{\mathrm{zar}} \cap \mathrm{Sp}_{2g}$.
Now fix $\iota\colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$, and let $G_{\ell,\iota}^{\mathrm{zar}}$ and $G_{\ell,\iota}^{1,\mathrm{zar}}$ denote base changes to $\mathbb{C}$.

Definition

$\mathrm{ST}(A) \subseteq \mathrm{USp}(2g)$ is a maximal compact subgroup of $G_{\ell,\iota}^{1,\mathrm{zar}}(\mathbb{C})$ equipped with the map $s\colon \mathfrak{p} \mapsto \mathrm{conj}(\|\mathfrak{p}\|^{-1/2}\rho_{\ell,\iota}(\mathrm{Frob}_\mathfrak{p})) \in \mathrm{conj}(\mathrm{ST}(A))$.

- $\mathrm{ST}(A)$ is unique up to conjugacy and conjecturally independent of ι and ℓ.
- $s(\mathfrak{p})$ is the normalized L-polynomial $\bar{L}_\mathfrak{p}(T)$.
- $\rho_{\ell,\iota}(\mathrm{Frob}_\mathfrak{p})$ is semisimple (by a theorem of Tate), so conjugate to a $g \in \mathrm{ST}(A)$.

The Sato-Tate conjecture for abelian varieties

Algebraic Sato–Tate Conjecture

$(G_\ell^{\mathrm{zar}})^0 = \mathrm{MT}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$, equivalently, $(G_\ell^{1,\mathrm{zar}})^0 = \mathrm{Hg}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.
More generally, $(G_\ell^{\mathrm{zar}}) = \mathrm{AST}(A) \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$.

The algebraic Sato-Tate conjecture is known for $g \leq 3$ [Banaszak–Kedlaya 2015].
It follows from the Mumford–Tate conjecture [Cantoral-Farfán–Commelin 2022].

Sato-Tate conjecture for abelian varieties

The conjugacy classes $s(\mathfrak{p})$ are equidistributed with respect to $\mu_{\mathrm{ST}(A)}$.

The Sato-Tate conjecture implies that the distribution of normalized L-polynomials converges to the distribution of characteristic polynomials in $\mathrm{ST}(A)$.

Sato-Tate axioms for abelian varieties

$G \subseteq \mathrm{USp}(2g)$ satisfies the Sato-Tate axioms (for abelian varieties of dimension g) if:

1. **Compact**: G is closed;
2. **Hodge**: G contains a Hodge circle $\vartheta\colon \mathrm{U}(1) \to G^0$ whose elements $\vartheta(u)$ have eigenvalues u, $1/u$ with multiplicity g, such that the conjugates of ϑ generate a dense subset of G;
3. **Rationality**: For each component H of G and each irreducible character χ of $\mathrm{GL}_{2g}(\mathbb{C})$ we have $\mathrm{E}[\chi(\gamma) : \gamma \in H] \in \mathbb{Z}$;
4. **Lefschetz**: The subgroup of $\mathrm{USp}(2g)$ fixing $\mathrm{End}(\mathbb{C}^{2g})^{G_0}$ is G^0.

Theorem (FKRS 2012, FKS 2019)

Sato-Tate groups of abelian varieties of dimension ≤ 3 satisfy the Sato-Tate axioms.

Axioms 1-3 are expected to hold in general, but Axiom 4 fails for $g = 4$.
For any g, the set of G satisfying axioms 1-3 is **finite**.

Galois endomorphism types

Let A be an abelian variety defined over a number field k.
Let K be the minimal extension of k for which $\mathrm{End}(A_K) = \mathrm{End}(A_{\bar{k}})$.
$\mathrm{Gal}(K/k)$ acts on the $\mathbb{R}$-algebra $\mathrm{End}(A_K)_\mathbb{R} = \mathrm{End}(A_K) \otimes_\mathbb{Z} \mathbb{R}$.

Definition

The Galois endomorphism type of A is the isomorphism class of $[\mathrm{Gal}(K/k), \mathrm{End}(A_K)_\mathbb{R}]$, where $[G, E] \simeq [G', E']$ iff we have compatible isomorphisms $G \simeq G'$ and $E \simeq E'$.

Theorem (FKRS 2012)

For abelian varieties A/k of dimension ≤ 3 there is a one-to-one correspondence between Sato-Tate groups and Galois endomorphism types.

More precisely, the identity component G^0 is uniquely determined by $\mathrm{End}(A_K)_\mathbb{R}$, and we have $G/G^0 \simeq \mathrm{Gal}(K/k)$ (with compatible actions).

Real endomorphism algebras of abelian surfaces

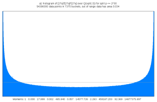
abelian surface	$\mathbf{End}(A_K)_{\mathbb{R}}$	$\mathbf{ST}(A)^0$
square of CM elliptic curve	$\mathrm{M}_2(\mathbb{C})$	$\mathrm{U}(1)_2$
• QM abelian surface • square of non-CM elliptic curve	$\mathrm{M}_2(\mathbb{R})$	$\mathrm{SU}(2)_2$
• CM abelian surface • product of CM elliptic curves	$\mathbb{C} \times \mathbb{C}$	$\mathrm{U}(1) \times \mathrm{U}(1)$
product of CM and non-CM elliptic curves	$\mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{SU}(2)$
• RM abelian surface • product of non-CM elliptic curves	$\mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{SU}(2)$
generic abelian surface	$\mathbb{R}$	$\mathrm{USp}(4)$

(factors in products are assumed to be non-isogenous)

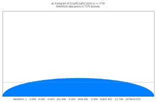
Real endomorphism algebras of abelian threefolds

abelian threefold	$\mathbf{End}(A_K)_{\mathbb{R}}$	$\mathbf{ST}(A)^0$
cube of a CM elliptic curve	$\mathrm{M}_3(\mathbb{C})$	$\mathrm{U}(1)_3$
cube of a non-CM elliptic curve	$\mathrm{M}_3(\mathbb{R})$	$\mathrm{SU}(2)_3$
product of CM elliptic curve and square of CM elliptic curve	$\mathbb{C} \times \mathrm{M}_2(\mathbb{C})$	$\mathrm{U}(1) \times \mathrm{U}(1)_2$
product of non-CM elliptic curve and square of CM elliptic curve	$\mathbb{R} \times \mathrm{M}_2(\mathbb{C})$	$\mathrm{SU}(2) \times \mathrm{U}(1)_2$
• product of CM elliptic curve and QM abelian surface • product of CM elliptic curve and square of non-CM elliptic curve	$\mathbb{C} \times \mathrm{M}_2(\mathbb{R})$	$\mathrm{U}(1) \times \mathrm{SU}(2)_2$
• product of non-CM elliptic curve and QM abelian surface • product of non-CM elliptic curve and square of non-CM elliptic curve	$\mathbb{R} \times \mathrm{M}_2(\mathbb{R})$	$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$
• CM abelian threefold • product of CM elliptic curve and CM abelian surface • product of three CM elliptic curves	$\mathbb{C} \times \mathbb{C} \times \mathbb{C}$	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$
• product of non-CM elliptic curve and CM abelian surface • product of non-CM elliptic curve and two CM elliptic curves	$\mathbb{C} \times \mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{SU}(2)$
• product of CM elliptic curve and RM abelian surface • product of CM elliptic curve and two non-CM elliptic curves	$\mathbb{C} \times \mathbb{R} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$
• RM abelian threefold • product of non-CM elliptic curve and RM abelian surface • product of 3 non-CM elliptic curves	$\mathbb{R} \times \mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{SU}(3) \times \mathrm{SU}(3)$
product of CM elliptic curve and abelian surface	$\mathbb{C} \times \mathbb{R}$	$\mathrm{U}(1) \times \mathrm{USp}(4)$
product of non-CM elliptic curve and abelian surface	$\mathbb{R} \times \mathbb{R}$	$\mathrm{SU}(2) \times \mathrm{USp}(4)$
quadratic CM abelian threefold	$\mathbb{C}$	$\mathrm{U}(3)$
generic abelian threefold	$\mathbb{R}$	$\mathrm{USp}(6)$

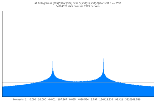
Connected Sato-Tate groups of abelian threefolds:



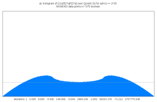
$U(1)_3$



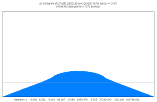
$SU(2)_3$



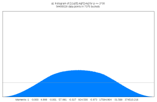
$U(1) \times U(1)_2$



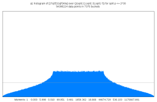
$SU(2) \times U(1)_2$



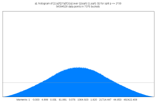
$U(1) \times SU(2)_2$



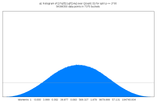
$SU(2) \times SU(2)_2$



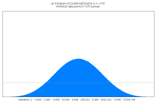
$U(1) \times U(1) \times U(1)$



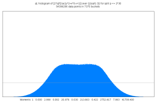
$U(1) \times U(1) \times SU(2)$



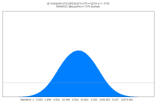
$U(1) \times SU(2) \times U(1)$



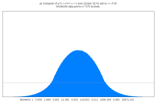
$SU(2) \times SU(2) \times SU(2)$



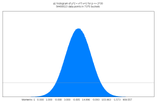
$U(1) \times USp(4)$



$SU(2) \times USp(4)$



$U(3)$



$USp(6)$

Classification of Sato-Tate groups of abelian varieties over number fields

Theorem (FKRS 2012, FKS 2019)

For $g = 1, 2, 3$ the table below lists the number of subgroups of $\mathrm{USp}(2g)$ that satisfy the Sato-Tate axioms, and the subset of these that arise as $\mathrm{ST}(A)$ for an abelian variety A over a number field k. Among those that arise as $\mathrm{ST}(A)$, it lists the number that are connected, the number that are maximal, the number that arise over $\mathbb{Q}$, and the size of the largest component group.

g	axioms	$\#\{\mathrm{ST}(A)\}$	$\#\{\mathrm{ST}^0(A)\}$	maximal	over $\mathbb{Q}$	$\max\{\mathrm{ST}(A)/\mathrm{ST}^0(A)\}$
1	3	3	2	2	2	2
2	55	53	6	9	34	48
3	433	410	14	33	?	432

See the LMFDB for more details, including generators, moments, and other invariants.

This theorem says nothing about the Sato–Tate conjecture. For abelian surfaces $A/\mathbb{Q}$ the Sato–Tate conjecture is known for $\mathrm{ST}(A) \neq \mathrm{USp}(4)$ [Johansson 2017, Taylor 2020].

Mumford exceptional abelian varieties

Things are much harder for $g > 3$ because $\mathrm{MT}(A)$, and therefore $\mathrm{ST}(A)$, is no longer determined by endomorphisms. Mumford proved the existence of abelian fourfolds A/k with $\mathrm{End}(A_{\overline{k}}) = \mathbb{Z}$ for which $\mathrm{MT}(A) \neq \mathrm{GSp}_{2g}$, and Shioda showed that the Jacobian of the curve $y^2 = x^9 - 1$ (isogenous to the product of a CM threefold and a CM elliptic curve) admits an algebraic cycle that makes its Mumford–Tate group exceptional.

It has been challenging to find a similarly explicit example of a generic abelian fourfold of Mumford type, ideally one that arises as the Jacobian of a genus 4 curve over $\mathbb{Q}$.

Bouchet–Hanselman–Pieper–Schiavone have constructed a one-parameter family of hyperelliptic genus 4 curves whose Jacobians are generically expected to be of Mumford type (this is work in progress). This includes the example

$$X\colon y^2 = 7x^9 + 63x^8 + 36x^7 - 252x^6 + 1890x^5 - 1134x^4 + 756x^3 + 6804x^2 + 5103x + 3591$$

with $\mathrm{End}(\mathrm{Jac}(X_{\overline{\mathbb{Q}}})) = \mathbb{Z}$, whose Sato–Tate group does not appear to be $\mathrm{USp}(8)$.

Conjectures of Birch and Swinnerton-Dyer

Based on early computer experiments Birch and Swinnerton-Dyer conjectured that

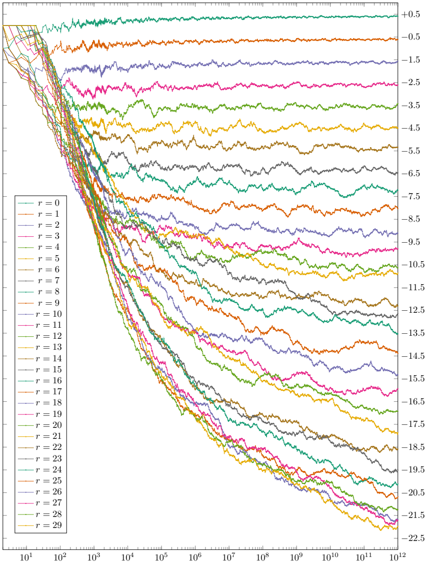
$$\lim_{x\to\infty} \prod_{p\le x} \frac{\#E(\mathbb{F}_p)}{p} = c_E (\log x)^r$$

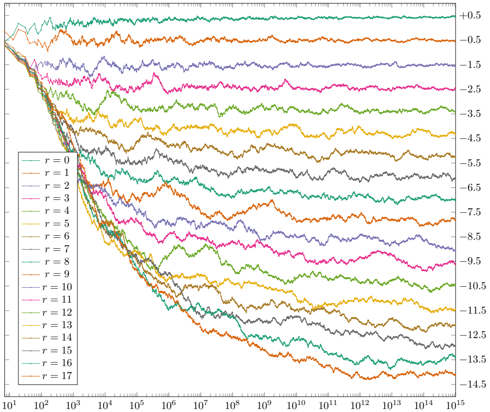
for some constant c_E, where r is the analytic rank. This implies

$$\lim_{x\to\infty} \frac{1}{\log x} \sum_{p\le x} \frac{a_p \log p}{p} = -r + \tfrac{1}{2},$$

and suggests that one can compute (or at least predict) r by counting points.

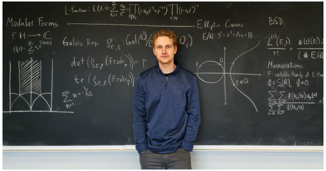
Birch and Swinnerton-Dyer eventually formulated a more precise (weaker!) conjecture that became more well known (the conjecture above implies RH for $L_E(s)$, in fact this must hold if the limit on the LHS exists [Kim–Murty 2023]).


+0.5
−0.5
−1.5
−2.5
−3.5
−4.5
−5.5
−6.5
−7.5
−8.5
−9.5
−10.5
−11.5
−12.5
−13.5
−14.5
−15.5
−16.5
−17.5
−18.5
−19.5
−20.5
−21.5
−22.5
10^1
10^2
10^3
10^4
10^5
10^6
10^7
10^8
10^9
10^{10}
10^{11}
10^{12}
$r = 0$
$r = 1$
$r = 2$
$r = 3$
$r = 4$
$r = 5$
$r = 6$
$r = 7$
$r = 8$
$r = 9$
$r = 10$
$r = 11$
$r = 12$
$r = 13$
$r = 14$
$r = 15$
$r = 16$
$r = 17$
$r = 18$
$r = 19$
$r = 20$
$r = 21$
$r = 22$
$r = 23$
$r = 24$
$r = 25$
$r = 26$
$r = 27$
$r = 28$
$r = 29$


+0.5
−0.5
−1.5
−2.5
−3.5
−4.5
−5.5
−6.5
−7.5
−8.5
−9.5
−10.5
−11.5
−12.5
−13.5
−14.5
10^1
10^2
10^3
10^4
10^5
10^6
10^7
10^8
10^9
10^{10}
10^{11}
10^{12}
10^{13}
10^{14}
10^{15}
$r = 0$
$r = 1$
$r = 2$
$r = 3$
$r = 4$
$r = 5$
$r = 6$
$r = 7$
$r = 8$
$r = 9$
$r = 10$
$r = 11$
$r = 12$
$r = 13$
$r = 14$
$r = 15$
$r = 16$
$r = 17$

Murmurations of elliptic curves

In 2022, He, Lee, Oliver, and Pozdnyakov ran a series of machine learning experiments in an attempt to predict ranks of elliptic curves over $\mathbb{Q}$ using Frobenius traces.

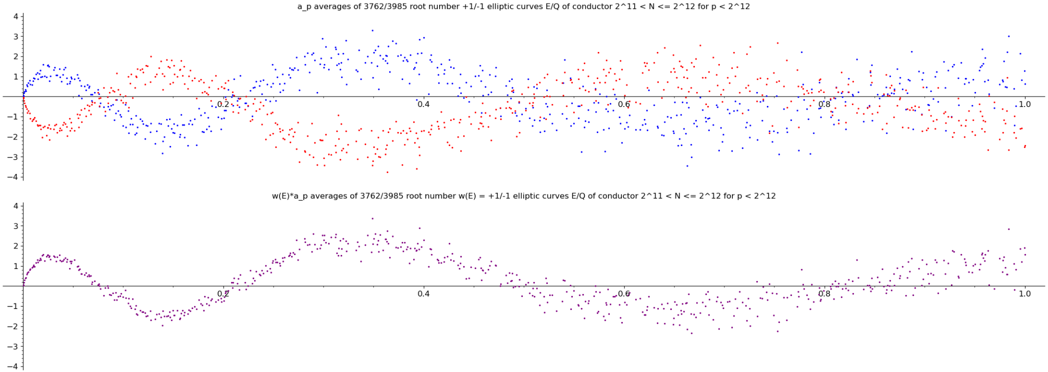


Their efforts to predict ranks worked for curves of small conductor, but not in general. However, they noticed a previously unobserved oscillation in average Frobenius traces in families of elliptic curves ordered by conductor when separated by rank.

You can read more about their discovery in this 2024 Quanta article.

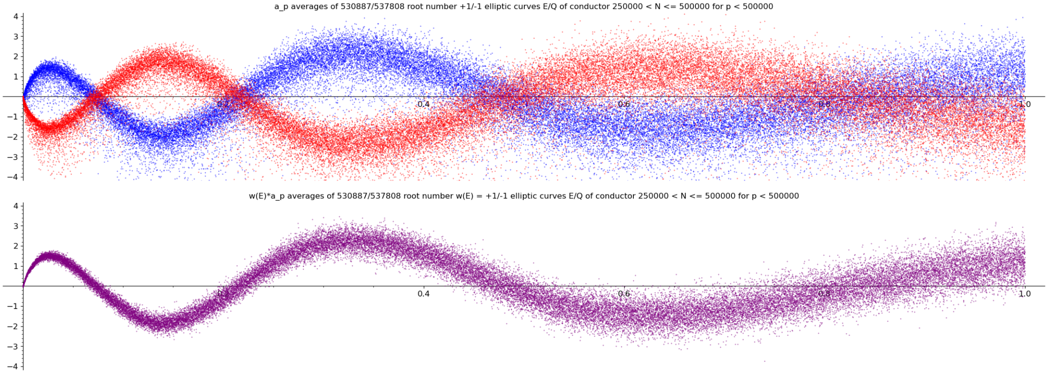
Murmurations of elliptic curves

Elliptic curves of conductor $N \in (2^n, 2^{n+1}]$ for $11 \le n \le 18$. Blue/red/purple dots at $(p, \bar{a}_p$ or $\bar{m}_p)$ are averages of a_p or $m_p := (-1)^r a_p(E)$ over even/odd/all $E/\mathbb{Q}$.



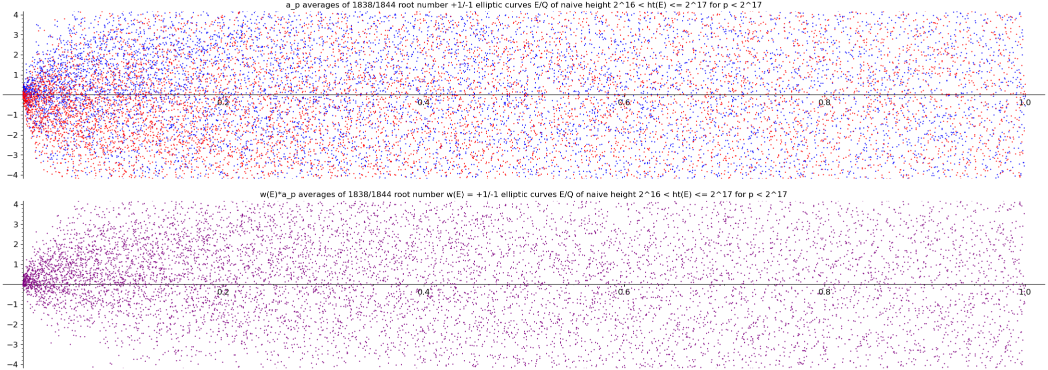
Murmurations of elliptic curves

Elliptic curves of conductor $N \in (2^n, 2^{n+1}]$ for $11 \leq n \leq 18$. Blue/red/purple dots at $(p, \bar{a}_p$ or $\bar{m}_p)$ are averages of a_p or $m_p := (-1)^r a_p(E)$ over even/odd/all $E/\mathbb{Q}$.



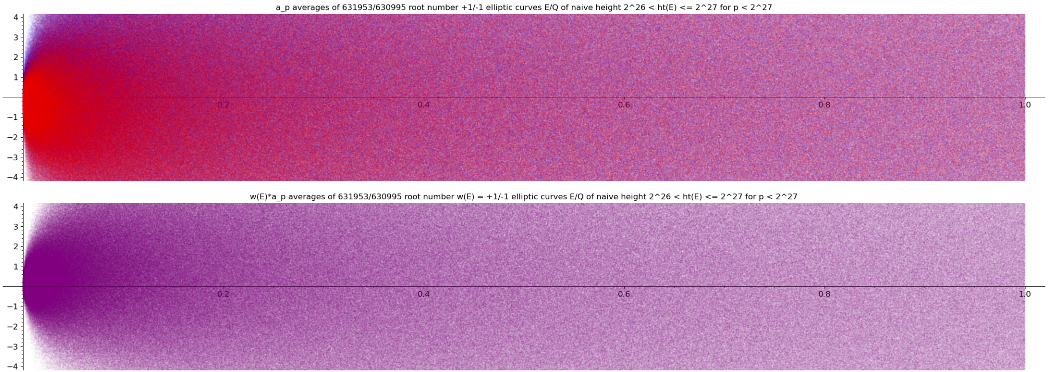
Ordering by naive height

Elliptic curves with $\mathrm{ht}(E) := \max(4|A|^3, 27B^2)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{25}$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.

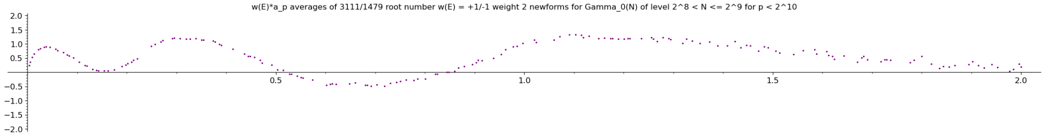


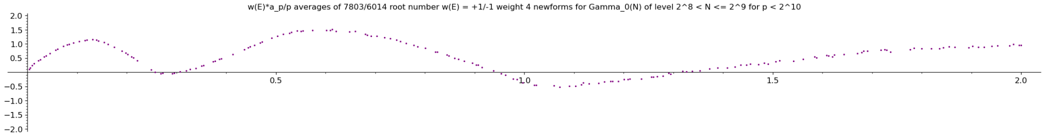
Ordering by naive height

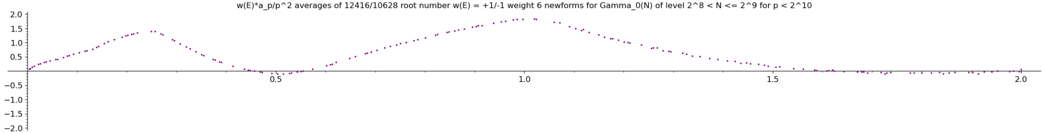
Elliptic curves with $\mathrm{ht}(E) := \max(4|A|^3, 27B^2)$ in $(M, 2M]$ for $M = 2^{16}, \dots, 2^{25}$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.

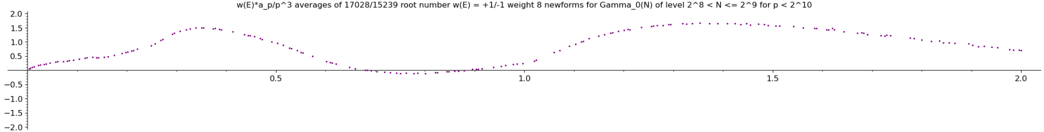


Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6, 8$.

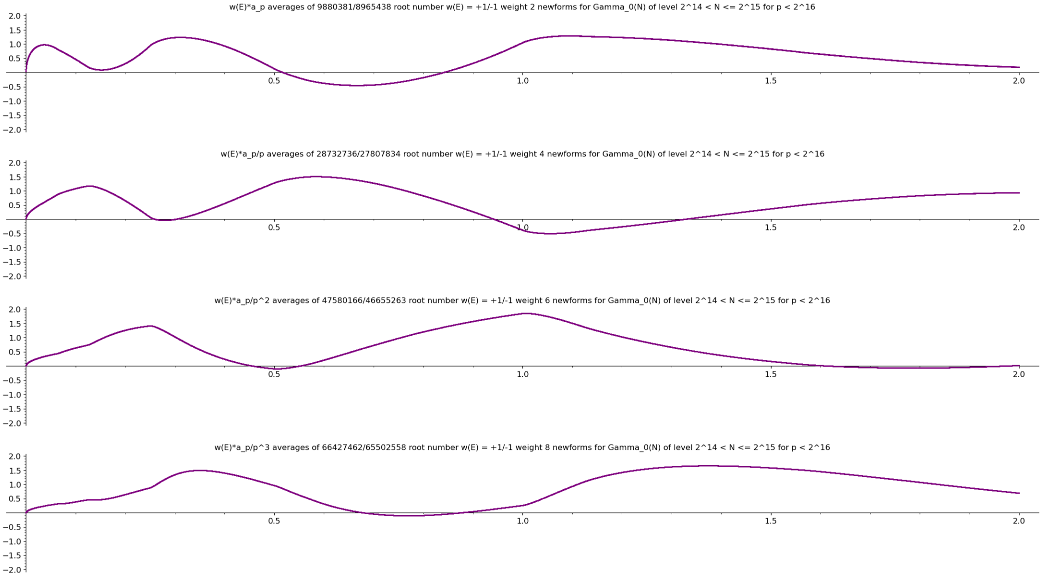








Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6, 8$.



Zubrilina's theorem

Definition. Let $U_n \in \mathbb{Z}[x]$ denote the Chebyshev polynomial defined by $U_n(\cos\vartheta)\sin\vartheta = \sin((n+1)\vartheta)$. The murmuration density function is

$$M_k(y) := D_k\Big(Ay \;-(-1)^{k/2}B\sum_{1\le r\le 2y} c(r)\sqrt{4y^2-r^2}\;U_{k-2}\big(\tfrac{r}{2y}\big) - \pi y^2\delta_{k=2}\Big),$$

$A := \prod_p\big(1+\frac{p}{(p+1)^2(p-1)}\big)$, $B := \prod_p \frac{p^4-2p^2-p+1}{(p^2-1)^2}$, $c(r) := \prod_{p|r}\big(1+\frac{p^2}{p^4-2p^2-p+1}\big)$, $D_k := \frac{12}{(k-1)\pi\prod_p\left(1-\frac{1}{p^2+p}\right)}$.

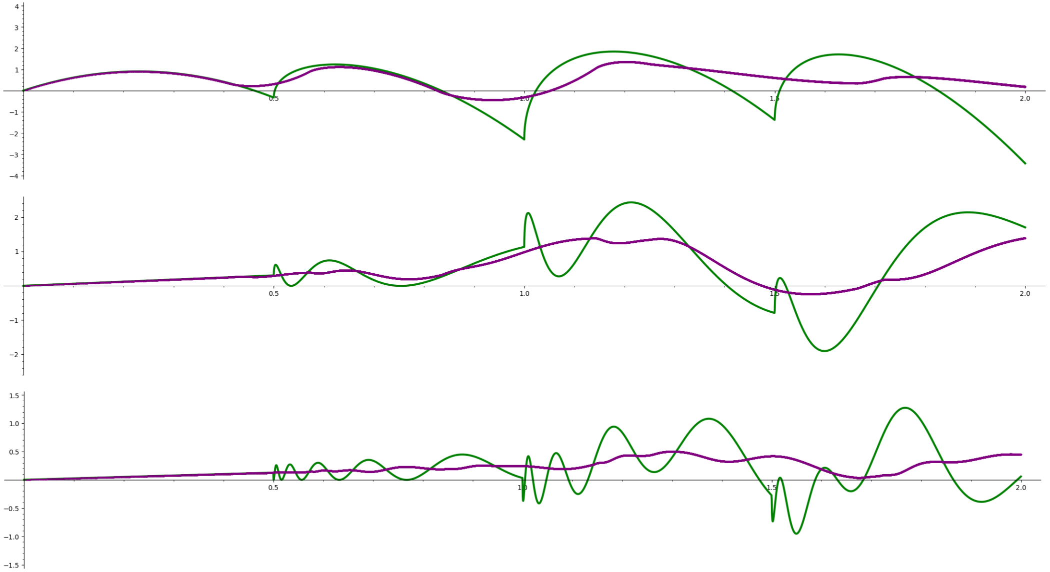
Theorem (Zubrilina 2023)

Let $\sum a_n(f)q^n$ denote a weight-k newform for $\Gamma_0(N)$ with root number $w(f)$. Let $X, Y, P \to \infty$ with P prime, $Y \sim X^{1-\delta}$, $P \ll X^{1+\delta_1}$, $\delta, \delta_1 > 0$ and $2\delta_1 < \delta < 1$, and put $y := \sqrt{P/X}$. Then for every $\varepsilon > 0$ we have

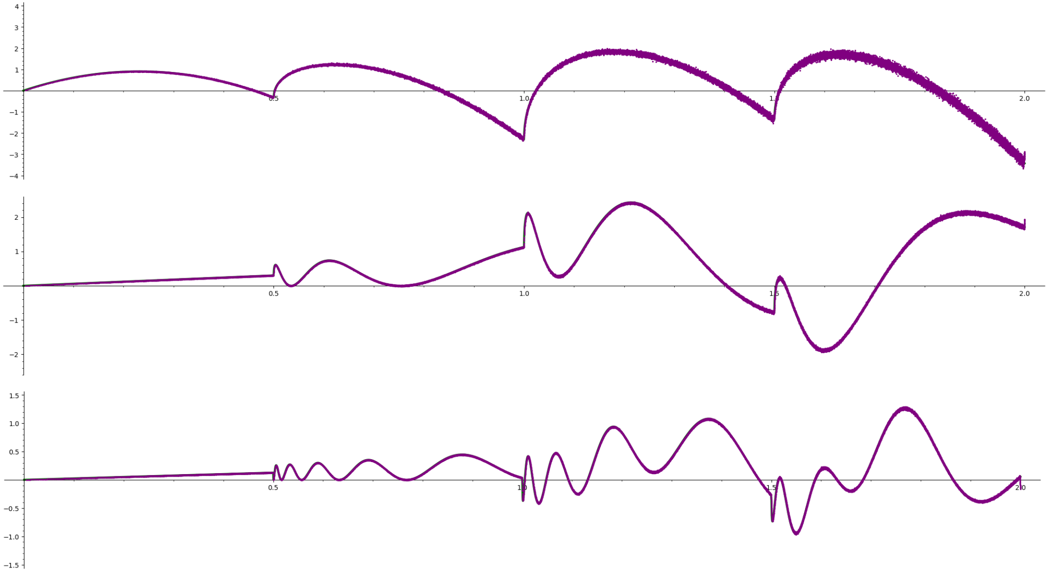
$$\frac{\sum_{N\in[X,X+Y]}^{\square\text{-free}}\sum_f w(f)a_P(f)P^{(1-k/2)}}{\sum_{N\in[X,X+Y]}^{\square\text{-free}}\sum_f 1} = M_k(y) + O_\varepsilon(X^{-\delta'+\varepsilon}+P^{-1})$$

where $\delta' := \max(\delta/2-\delta_1, (\delta+1)/9-\delta_1)$; for $\delta_1 < 2/9$ we can choose δ so $\delta' > 0$.

Zubrilina's theorem for $k = 2, 14, 32$ (click here for other k)



Zubrilina's theorem for $k = 2, 14, 32$ (click here for other k)



A murmuration theorem for elliptic curves

Let $\mathcal{E}(X) := \left\{ y^2 = x^3 + ax + b : a, b \in \mathbb{Z}, p^4 | a \Rightarrow p^6 \nmid b, \max(4|a|^3, 27b^2) \leq X \right\}$ be the set of isomorphism classes of elliptic curves over $\mathbb{Q}$ of naive height at most X.

Theorem (S–Sawin 2025)

For any smooth $W : \mathbb{R}_{>0} \to \mathbb{R}$ with compact support, the limit

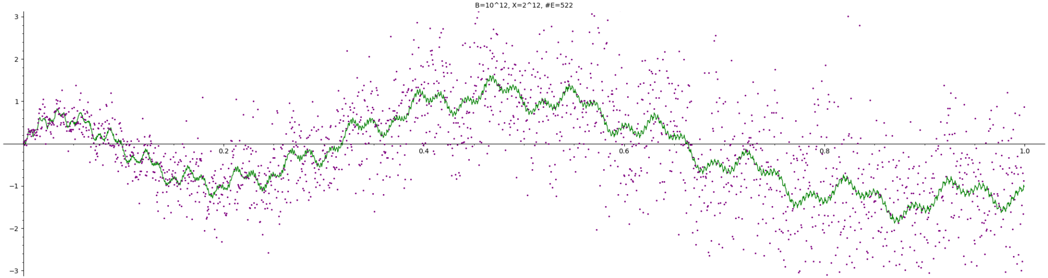
$$\lim_{X\to\infty} \frac{1}{\#\mathcal{E}(X)} \sum_{E\in\mathcal{E}(X)} \frac{\varepsilon(E)}{N_E} \sum_{n\geq 1} W(n/N_E) a_n(E)$$

exists and is equal to

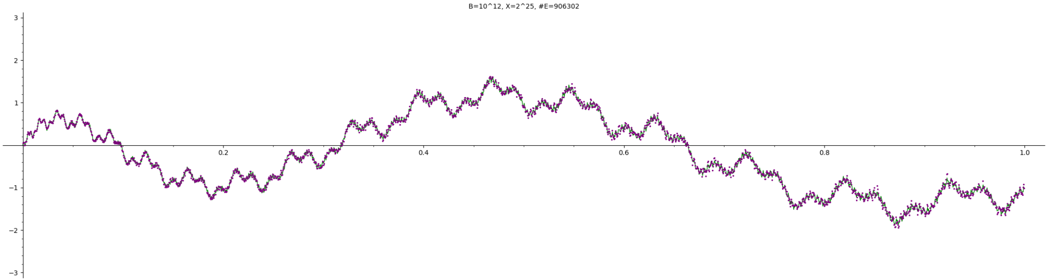
$$\int_0^\infty 2\pi W(u) \sum_{n=1}^{\infty} \frac{\prod_{p|n} \ell_{p^{\nu_p(n)}}}{\sqrt{n}} \sqrt{u} J_1(4\pi\sqrt{un}) du,$$

with $\ell_{2^\nu} = \frac{t_2(\nu+2)}{1023}, \ell_{3^\nu} = \cdots, \ell_{p^\nu} = \frac{p^9 - p^8}{p^{10}-1} t_p(\nu + 2)$, *where* $t_p(k) = \mathrm{tr}(T_p)$ *on* $S_k(1)$.

A murmuration theorem for elliptic curves

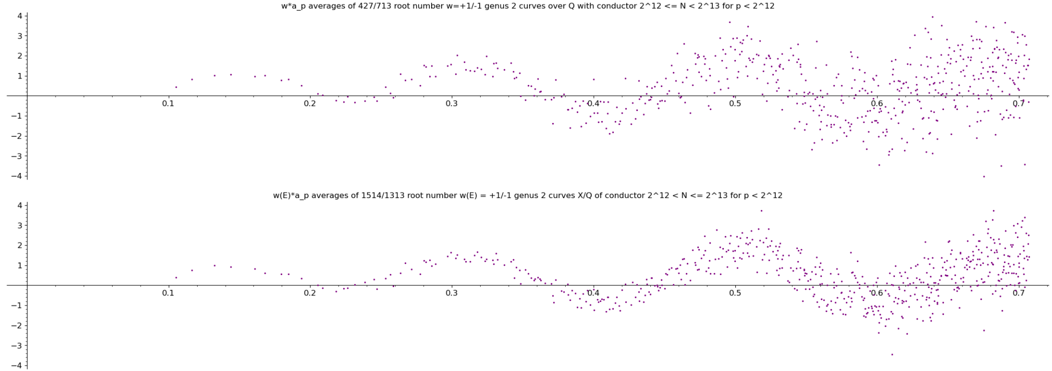


A murmuration theorem for elliptic curves



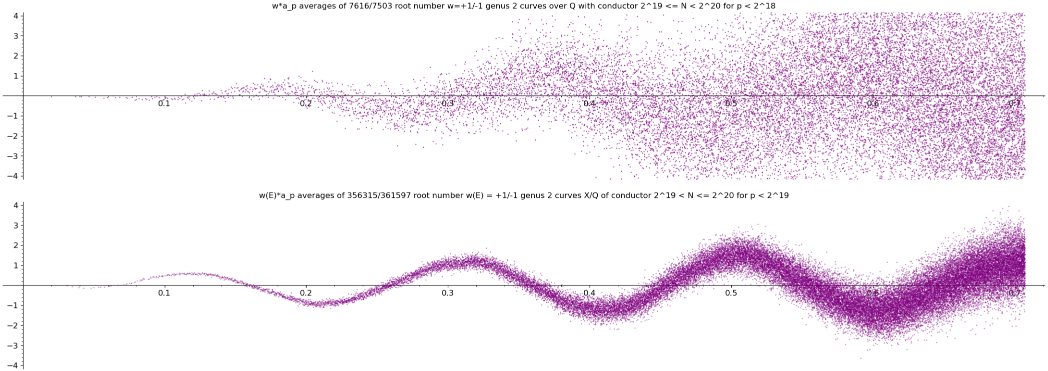
L-functions of genus 2 curves over $\mathbb{Q}$ with Sato-Tate group USp(4).

Before and after genus 2 murmuration plots (top LMFDB, bottom new dataset).

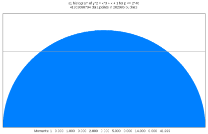


L-functions of genus 2 curves over $\mathbb{Q}$ with Sato-Tate group USp(4).

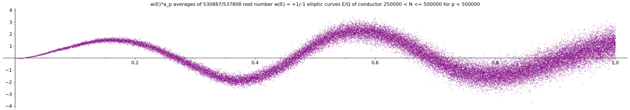
Before and after genus 2 murmuration plots (top LMFDB, bottom new dataset).



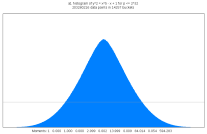
Thank you!



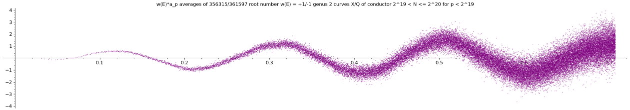
a1 histogram of y^2 = x^3 + x + 1 for p <= 2^40
41203088794 data points in 202985 buckets
Moments: 1 0.000 1.000 0.000 2.000 0.000 5.000 0.000 14.000 0.000 41.999



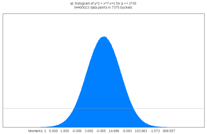
w(E)*a_p averages of 530887/537808 root number w(E) = +1/-1 elliptic curves E/Q of conductor 250000 < N <= 500000 for p < 500000



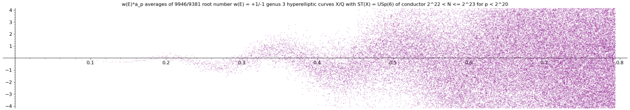
a1 histogram of y^2 = x^5 - x + 1 for p <= 2^32
203280216 data points in 14257 buckets
Moments: 1 0.000 1.000 0.000 2.999 0.002 13.999 0.009 84.014 0.054 594.283



w(E)*a_p averages of 356315/361597 root number w(E) = +1/-1 genus 2 curves X/Q of conductor 2^19 < N <= 2^20 for p < 2^19



a1 histogram of y^2 = x^7-x+1 for p <= 2^30
54400023 data points in 7375 buckets
Moments: 1 0.000 1.000 -0.000 3.000 -0.005 14.996 -0.093 103.963 -1.573 908.557



w(E)*a_p averages of 9946/9381 root number w(E) = +1/-1 genus 3 hyperelliptic curves X/Q with ST(X) = USp(6) of conductor 2^22 < N <= 2^23 for p < 2^20