Murmurations of arithmetic L-functions

Andrew V. Sutherland

Massachusetts Institute of Technology
Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation

November 11, 2024

Joint work with Yang-Hui He, Kyu-Hwan Lee, Thomas Oliver, and Alexey Pozdnyakov,
with thanks to Eran Assaf, Jonathan Bober, Andrew Booker, Edgar Costa, Alex Cowan,
Min Lee, David Lowry-Duda, Kimball Martin, Peter Sarnak, Will Sawin, and Nina Zubrilina.

Elliptic curves and their L-functions

Let $E/\mathbb{Q}$ be an elliptic curve, say $E\colon y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$.
For primes $p \nmid \Delta(E) := -16(4A^3 + 27B^2)$ this equation defines an elliptic curve $E/\mathbb{F}_p$.
For all such primes p we have the trace of Frobenius $a_p(E) := p + 1 - \#E(\mathbb{F}_p) \in \mathbb{Z}$.

One can also define $a_p(E)$ for $p|\Delta(E)$, and then construct the L-function

$$L(E, s) := \prod_p (1 - a_p p^{-s} + \chi(p)p^{1-2s})^{-1} = \sum_{n \geq 1} a_n n^{-s}$$

where $\chi(p) = \begin{cases} 0 & p|N(E) \\ 1 & \text{otherwise} \end{cases}$ and the conductor $N(E)$ divides $\Delta(E)$.

But in fact the a_p for $p \nmid \Delta(E)$ determine $L(E, s)$ (via strong multiplicity one), as well as the conductor and root number $w(E) = \pm 1$ which appear in the functional equation

$$\Lambda(E, s) = w(E)N(E)^{1-s}\Lambda(E, 2 - s),$$

where $\Lambda(s) := \Gamma_{\mathbb{C}}(s)L(E, s)$. The L-function $L(E, s)$ determines the isogeny class of E.

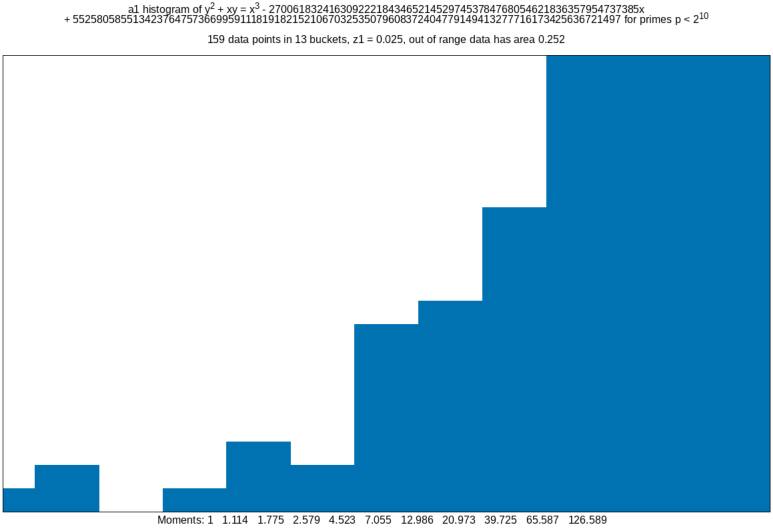
Arithmetic statistics of Frobenius traces of elliptic curves $E/\mathbb{Q}$

Three conjectures from the 1960s and 1970s (the first is now a theorem):

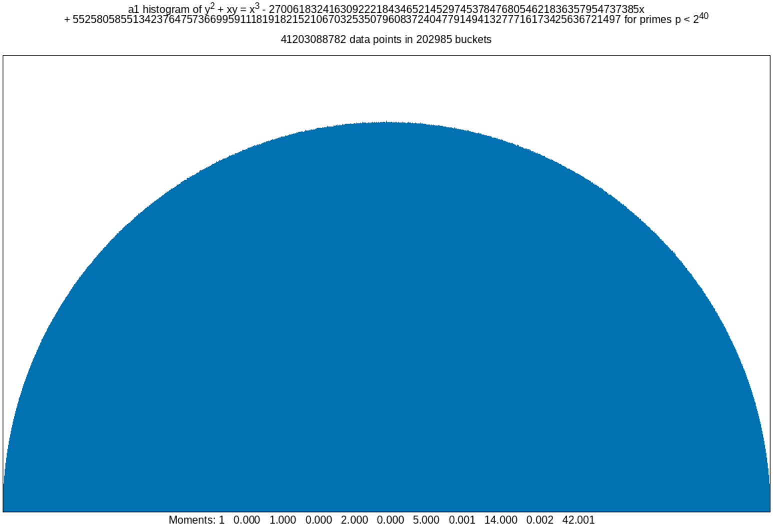
1. **Sato–Tate**: The sequence $x_p := a_p(E)/\sqrt{p}$ is equidistributed with respect to the pushforward of the Haar measure of $\mathrm{ST}(E)$ ($= \mathrm{SU}(2)$ if E does not have CM).
2. **Birch and Swinnerton-Dyer**:
$$\lim_{x\to\infty} \frac{1}{\log x} \sum_{p \le x} \frac{a_p(E) \log p}{p} = \frac{1}{2} - r,$$
3. **Lang–Trotter**: For every nonzero $t \in \mathbb{Z}$ there is a real number $C_{E,t}$ for which
$$\#\{p \le x : a_p(E) = t\} \sim C_{E,t} \frac{\sqrt{x}}{\log x}.$$

These conjectures depend only on $L(E, s)$ and generalize to other L-functions.

Example: Elkies-Klagsbrun curve of rank ≥ 29.



Example: Elkies-Klagsbrun curve of rank ≥ 29.



How rank effects trace distributions

An early form of the BSD conjecture implies that

$$\lim_{x\to\infty} \frac{1}{\log x} \sum_{p\leq x} \frac{a_p(E)\log p}{p} = \frac{1}{2} - r. \tag{1}$$

Sums of this form (Mestre-Nagao sums) are often used as a tool when searching for elliptic curves of large rank (which necessarily have large conductor N).[1] [2]

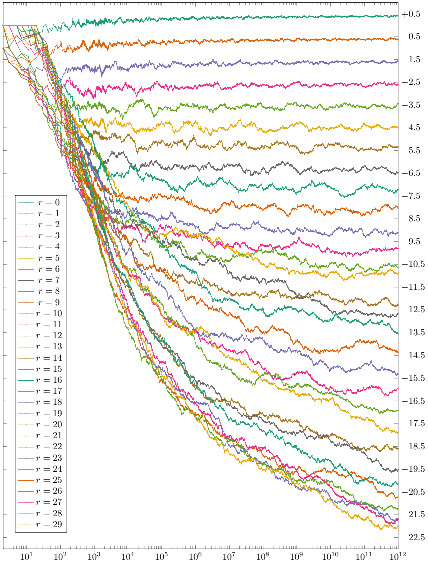
Theorem (Kim-Murty 2023)

If the limit on the LHS of (1) exists then it equals the RHS with r the analytic rank, and the L-function of E satisfies the Riemann hypothesis.

---

[1] See Sarnak's 2007 letter to Mazur.

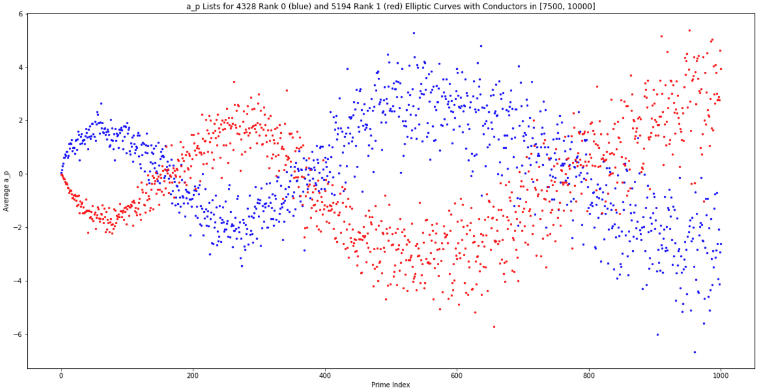
[2] See Kazalicki-Vlah for some recent machine-learning work on this topic.



+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}
$r = 0$
$r = 1$
$r = 2$
$r = 3$
$r = 4$
$r = 5$
$r = 6$
$r = 7$
$r = 8$
$r = 9$
$r = 10$
$r = 11$
$r = 12$
$r = 13$
$r = 14$
$r = 15$
$r = 16$
$r = 17$
$r = 18$
$r = 19$
$r = 20$
$r = 21$
$r = 22$
$r = 23$
$r = 24$
$r = 25$
$r = 26$
$r = 27$
$r = 28$
$r = 29$

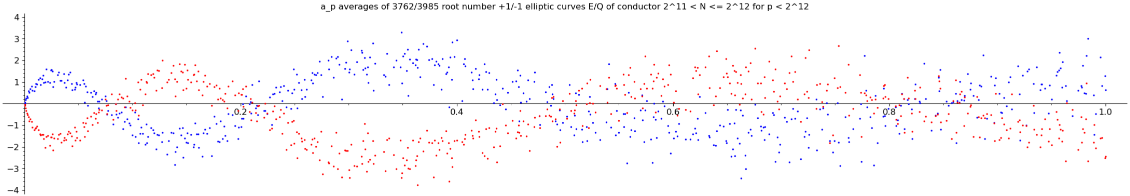
Murmurations of elliptic curves

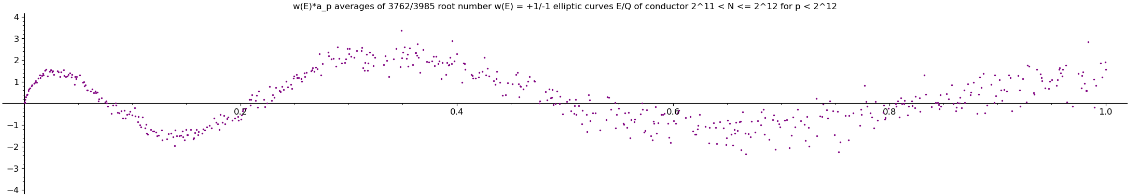
In their 2022 preprint *Murmurations of elliptic curves* (recently published), He, Lee, Oliver, and Pozdnyakov observed a curious fluctuation in average Frobenius traces of elliptic curves in a fixed conductor interval when separated by rank.



Murmurations of elliptic curves

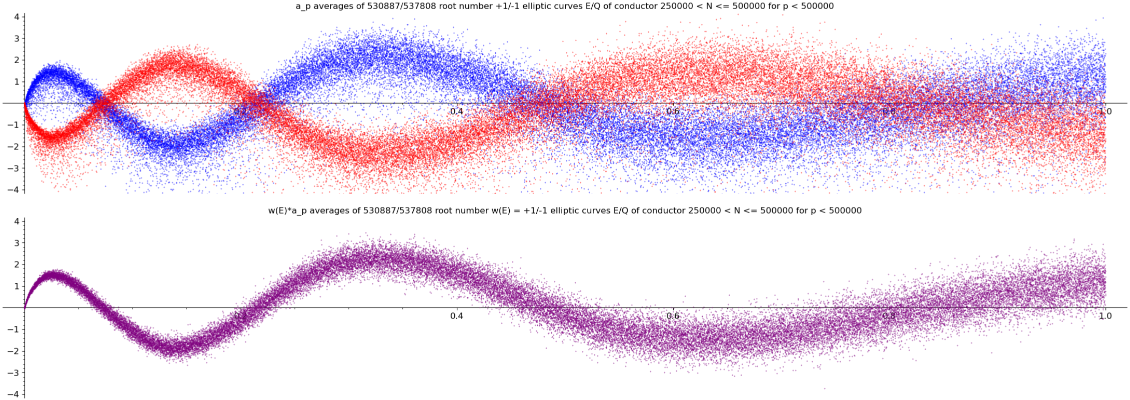
Elliptic curve L-functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \ldots, 2^{17}, 250000$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or $m_p := w(E)a_p(E)$ over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.





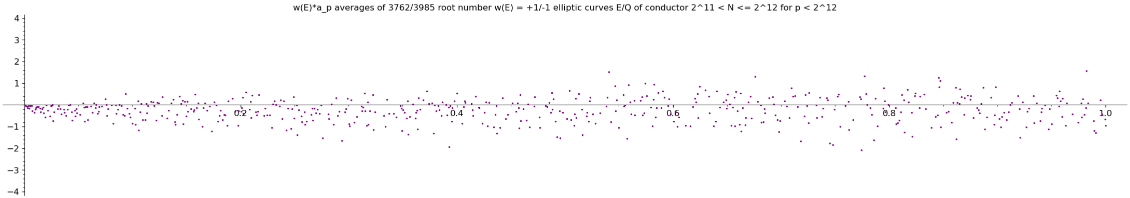
Murmurations of elliptic curves

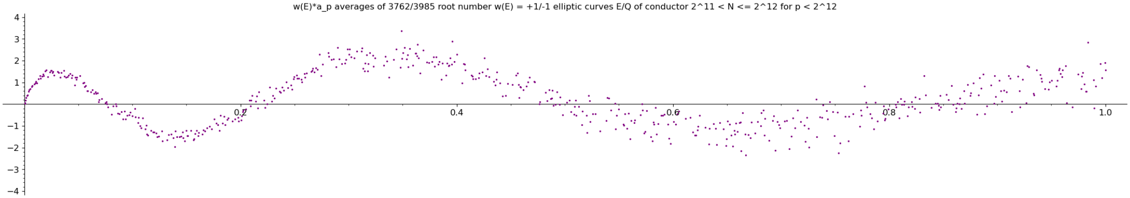
Elliptic curve L-functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \ldots, 2^{17}, 250000$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p \text{ or } \bar{m}_p)$ shows the average of a_p or $m_p := w(E)a_p(E)$ over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.



Bias cancellation

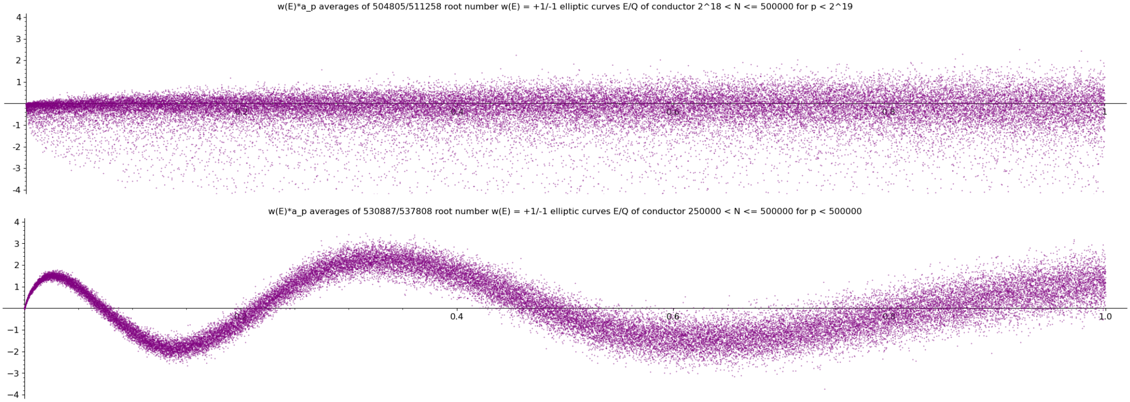
There is a negative bias in $\bar{a}_p$ that depends on p but is independent of the root number $w(E)$ and disappears in $\bar{m}_p$.





Bias cancellation

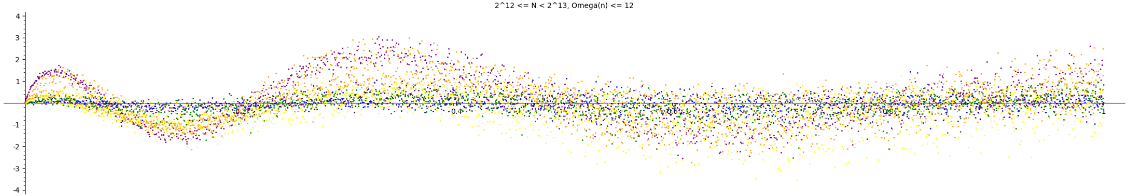
There is a negative bias in $\bar{a}_p$ that depends on p but is independent of the root number $w(E)$ and disappears in $\bar{m}_p$.



Murmurations of elliptic curves over a_n (not just a_p)

Elliptic curve L-functions of conductor $N \in (M, 2M]$ for $M = 2^{12}, \ldots, 2^{17}, 250000$. The x-axis range is $[0, 2M]$. Dots at $(n, \bar{m}_n)$ show the average of $m_n := w(E)a_n(E)$ over all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.

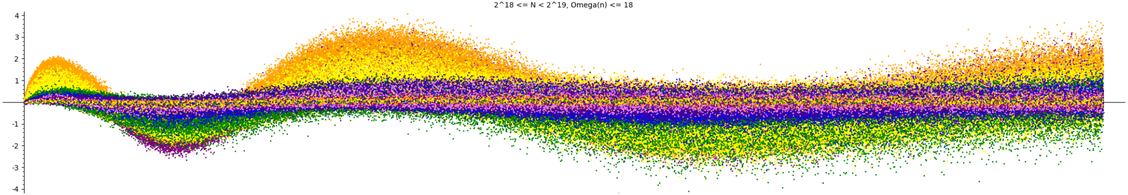
The color of the dot indicates the number of prime factors of n (with multiplicity).



Murmurations of elliptic curves over a_n (not just a_p)

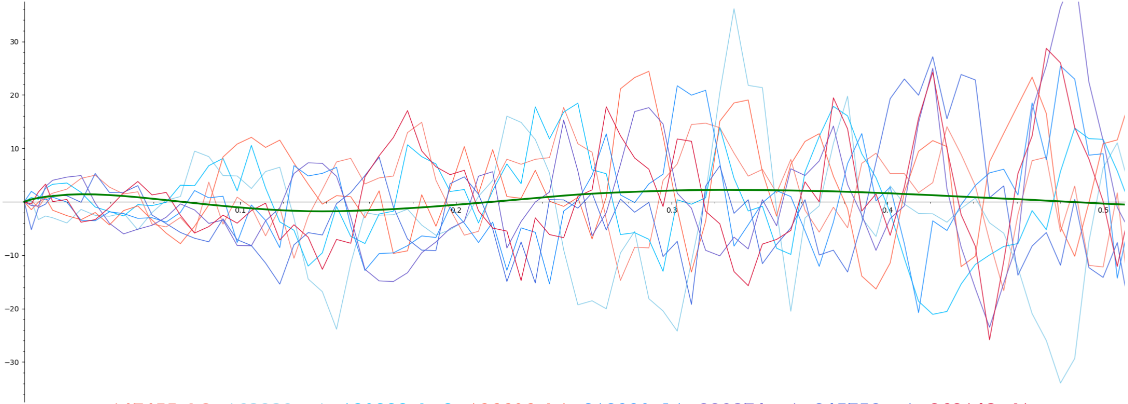
Elliptic curve L-functions of conductor $N \in (M, 2M]$ for $M = 2^{12}, \ldots, 2^{17}, 250000$. The x-axis range is $[0, 2M]$. Dots at $(n, \bar{m}_n)$ show the average of $m_n := w(E)a_n(E)$ over all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.

The color of the dot indicates the number of prime factors of n (with multiplicity).



Murmurations are an aggregate phenomenon

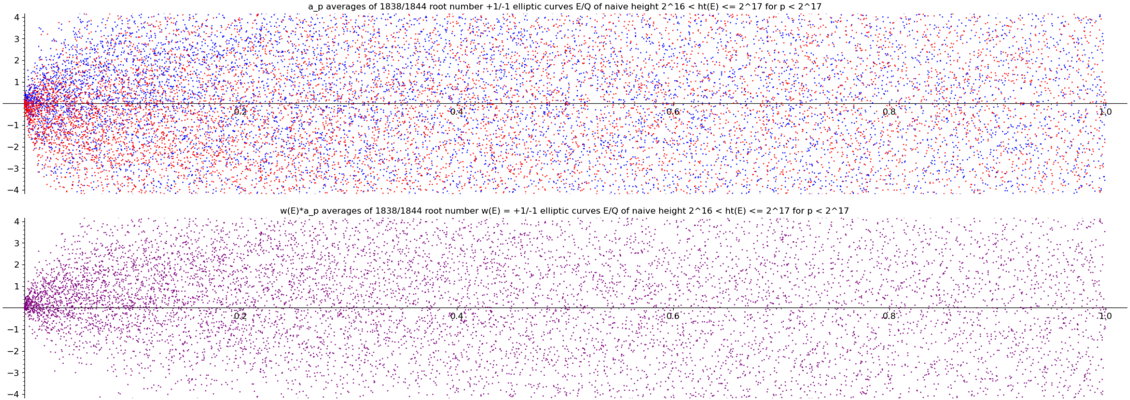
Moving average line plots of $\bar{m}_p$ for 8 individual and all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$, using subintervals of size $\sqrt{M}$ for $p \leq 2M$, with $M = 2^{17}$.



147455.b2, 163839.a1, 180222.be2, 196606.b1, 212990.l1, 229374.a1, 245758.a1, 262143.d1

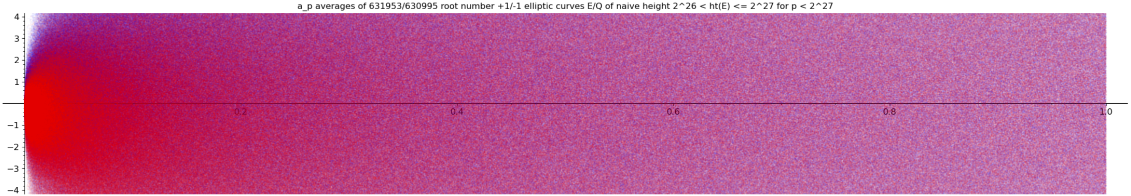
Ordering by height

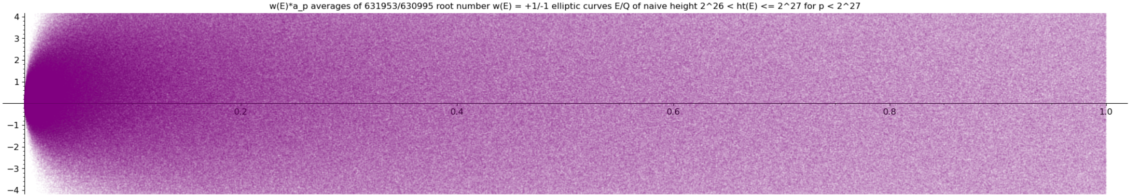
Elliptic curves with $\mathrm{ht}(E) := \max(4|A|^3, 27B^2)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{26}$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.



Ordering by height

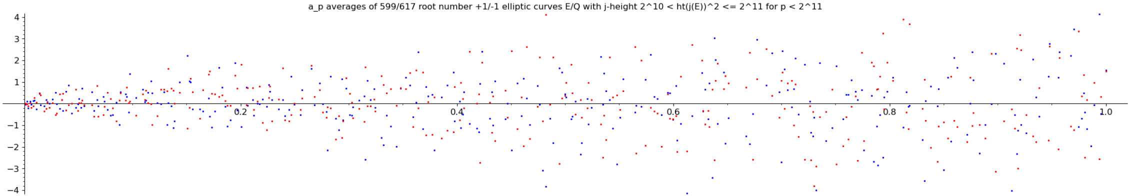
Elliptic curves with $\mathrm{ht}(E) := \max(4|A|^3, 27B^2)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{26}$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.

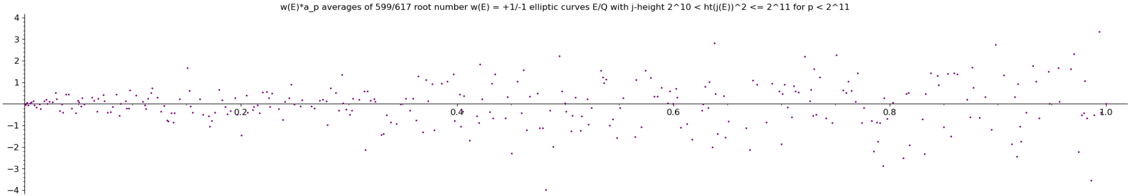




Ordering by j-invariant

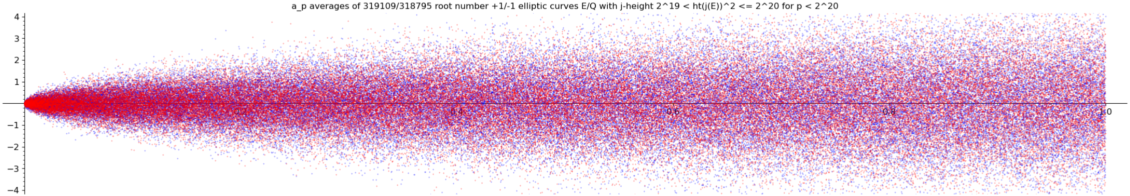
Elliptic curves with $\mathrm{ht}(j(E))^{12/5}$ in $(M, 2M]$ for $M = 2^{11}, \ldots, 2^{19}$.
The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.

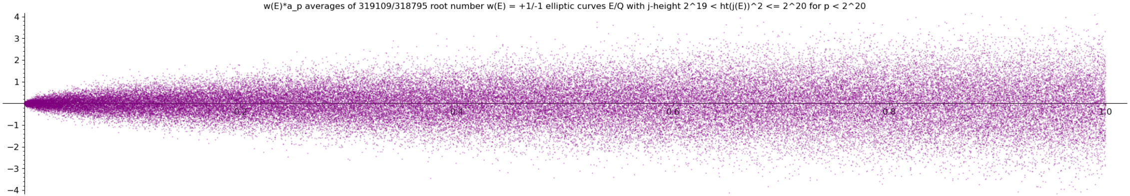




Ordering by j-invariant

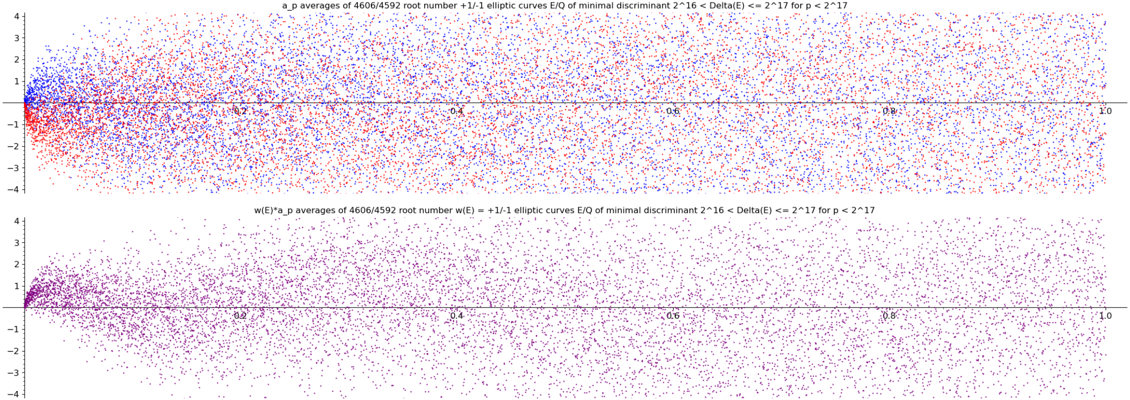
Elliptic curves with $\mathrm{ht}(j(E))^{12/5}$ in $(M, 2M]$ for $M = 2^{11}, \ldots, 2^{19}$.
The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.





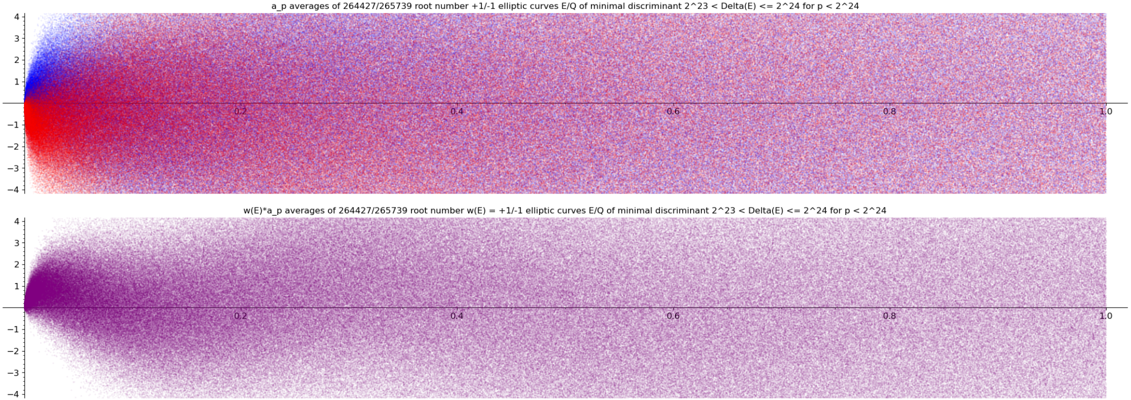
Ordering by minimal discriminant

Elliptic curves with minimal discriminant $\Delta(E)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{23}$. 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 $N_E \in (M, 2M]$.



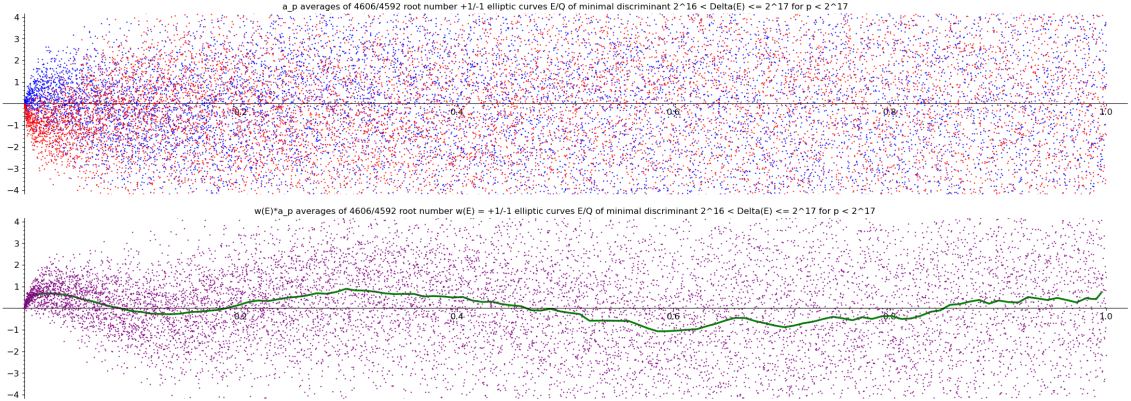
Ordering by minimal discriminant

Elliptic curves with minimal discriminant $\Delta(E)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{23}$. 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 $N_E \in (M, 2M]$.



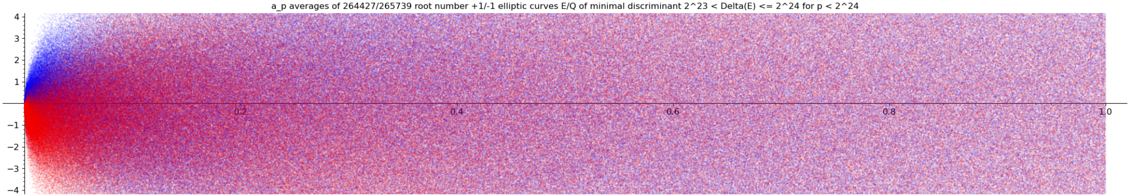
Ordering by minimal discriminant

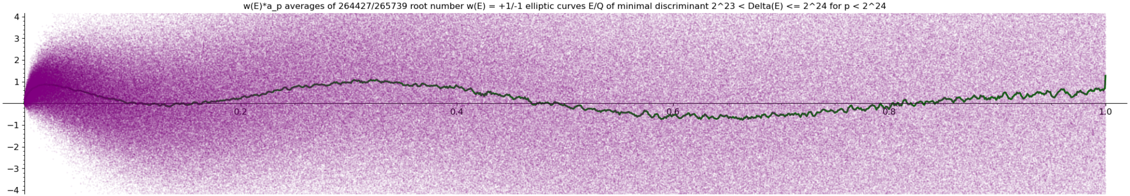
Elliptic curves with minimal discriminant $\Delta(E)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{23}$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.



Ordering by minimal discriminant

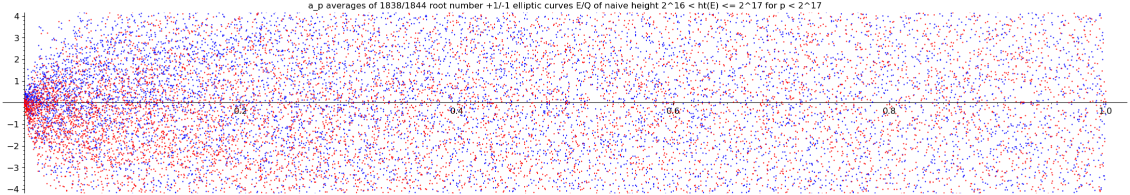
Elliptic curves with minimal discriminant $\Delta(E)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{23}$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.

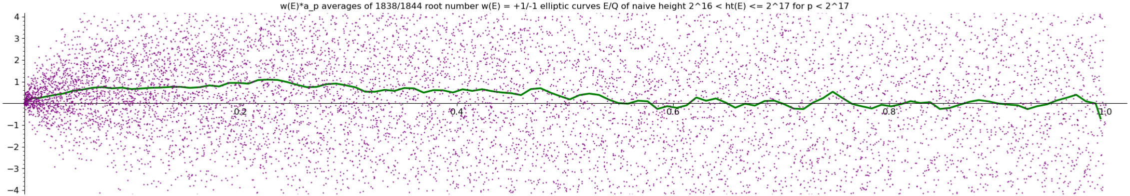




Ordering by height (redux)

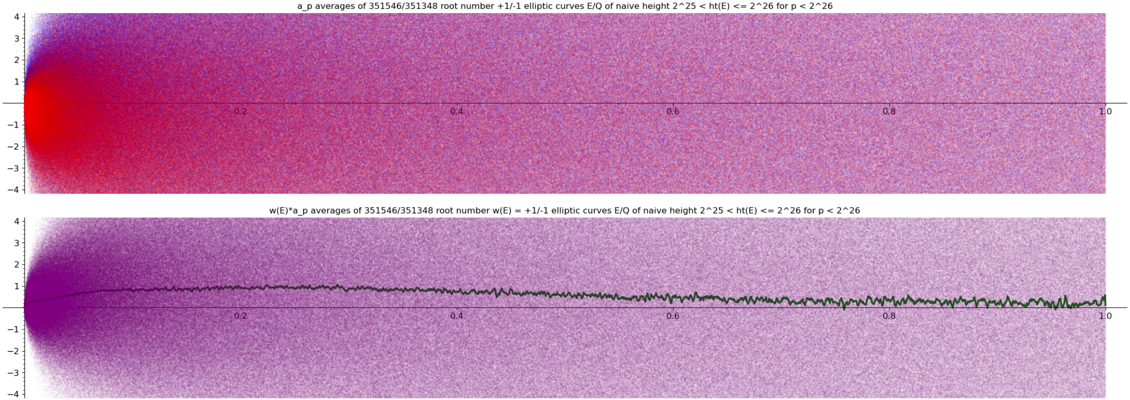
Elliptic curves with $\text{ht}(E) := \max(4|A|^3, 27B^2)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{25}$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p \text{ or } \bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.





Ordering by height (redux)

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 $N_E \in (M, 2M]$.



Local averaging

Rather than averaging a_p's for L-functions with conductor in an interval, we may instead compute local averages of a_p for each L-function in our family with p/N varying over some interval, and then average these local averages.

For example, we may divide the interval $[0,1]$ into n intervals $(x, x+\frac{1}{n}]$, with $x = 0, \frac{1}{n}, \frac{2}{n}, \ldots, \frac{n-1}{n}$. For each L-function in our family we compute a_p for all primes $p \leq N$, and then for $x = 0, \frac{1}{n}, \ldots, \frac{n-1}{n}$ we compute the average $\alpha_x(E)$ of $a_p(E)$ for

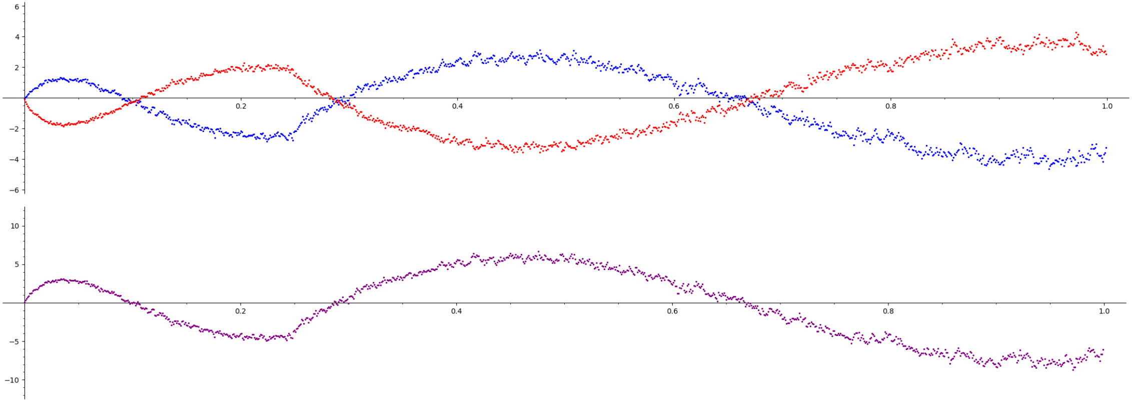
$$\frac{p}{N} \in \Big(x, x+\frac{1}{n}\Big],$$

yielding a vector of n real numbers. We then average these vectors over all L-functions in our family of a given root number or rank, up to an increasing bound $X \to \infty$.

With this setup, we do not need to order by conductor, but the order matters.

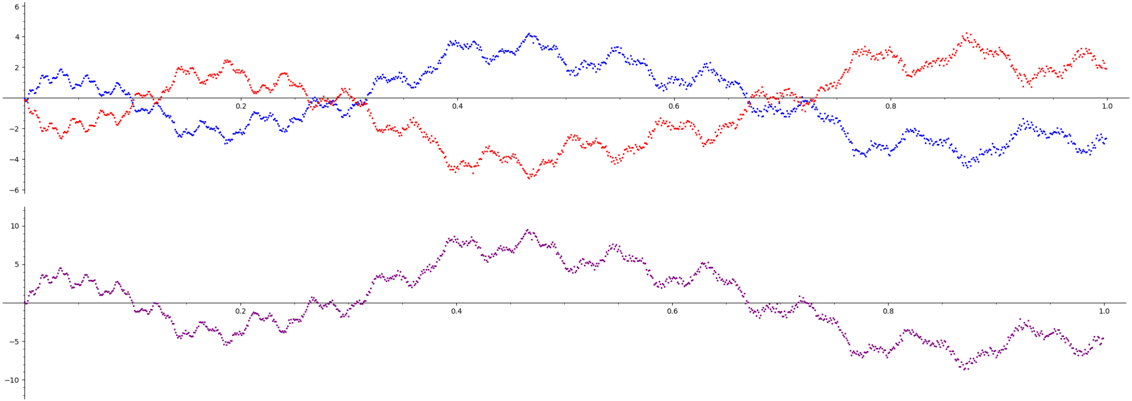
Local averaging: elliptic curves ordered by conductor

Elliptic curve L-functions of conductor $N \leq M$ for $M = 2^{12}, 2^{13}, \ldots, 2^{17}, 2^{18}$. The x-axis range is $[0, 1]$. A blue/red (or purple) dot at $(x, \bar{\alpha}_x)$ shows the average $\bar{\alpha}_x$ of $\alpha_x(E)$ (or $w_p(E)\alpha_x(E)$) over even/odd rank (or all) $E/\mathbb{Q}$ with $N_E \leq M$.

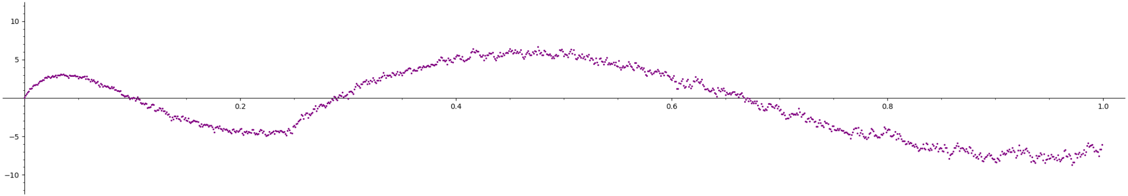


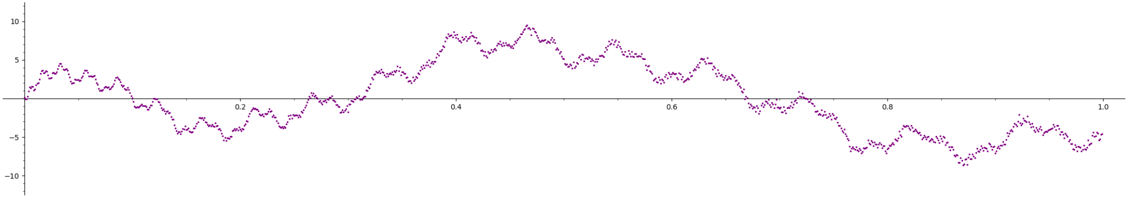
Local averaging: elliptic curves ordered by height

Elliptic curves with $\mathrm{ht}(E) := \max(4|A|^3, 27|B|^2) \leq M$ for $M = 2^{18}, \ldots, 2^{27}$.
The x-axis range is $[0, 1]$. A blue/red (or purple) dot at $(x, \bar{\alpha}_x)$ shows the average $\bar{\alpha}_x$ of $\alpha_x(E)$ (or $w_p(E)\alpha_x(E)$) over even/odd rank (or all) $E/\mathbb{Q}$ with $\mathrm{ht}(E) \leq M$.



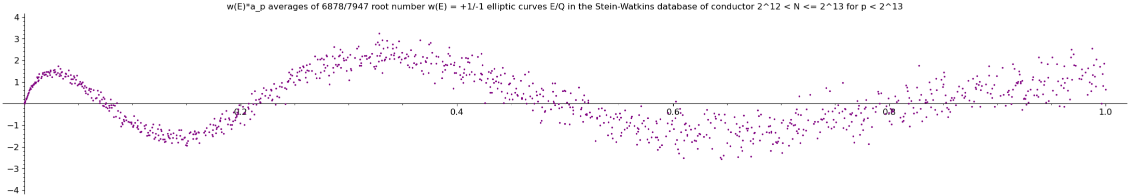
Local averaging: elliptic curves ordered by conductor vs height

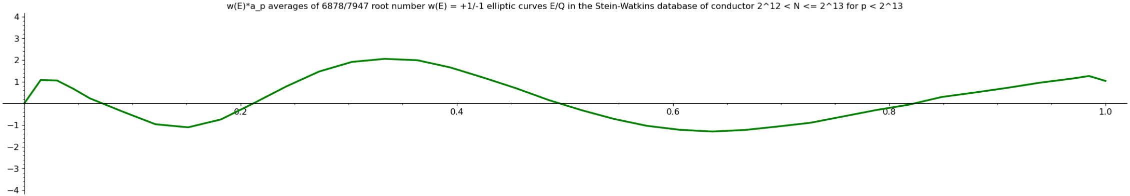




Murmurations scale

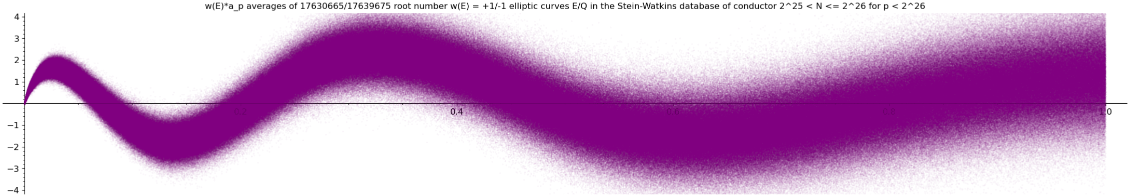
Elliptic curves in the SWDB of conductor $N \in (M, 2M]$ for $M = 2^{12}, \ldots, 2^{25}$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p \text{ or } \bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.

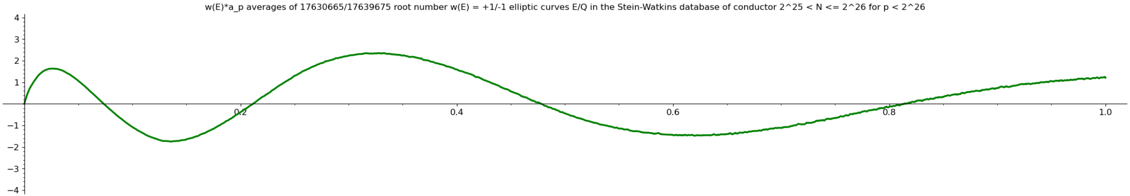




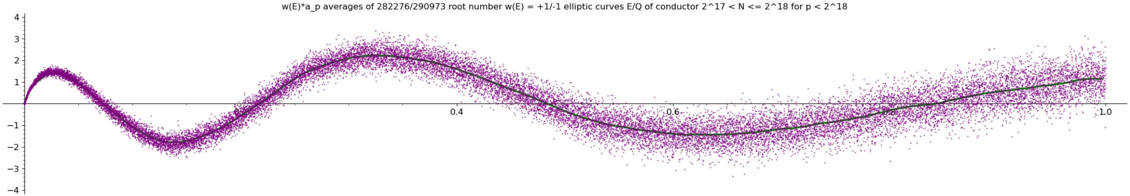
Murmurations scale

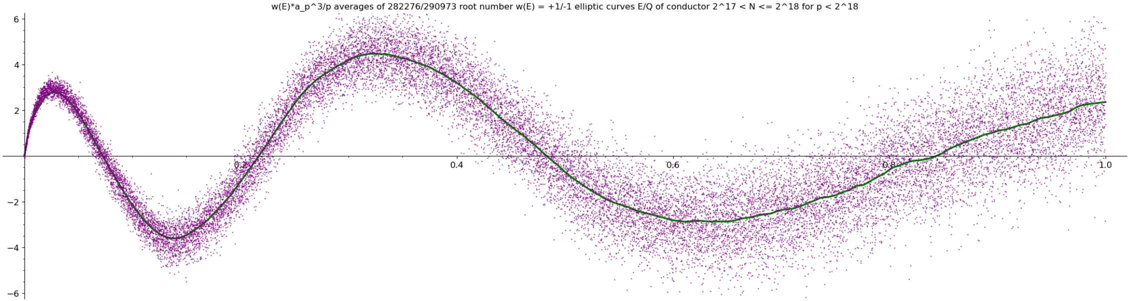
Elliptic curves in the SWDB of conductor $N \in (M, 2M]$ for $M = 2^{12}, \ldots, 2^{25}$.
The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p \text{ or } \bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.



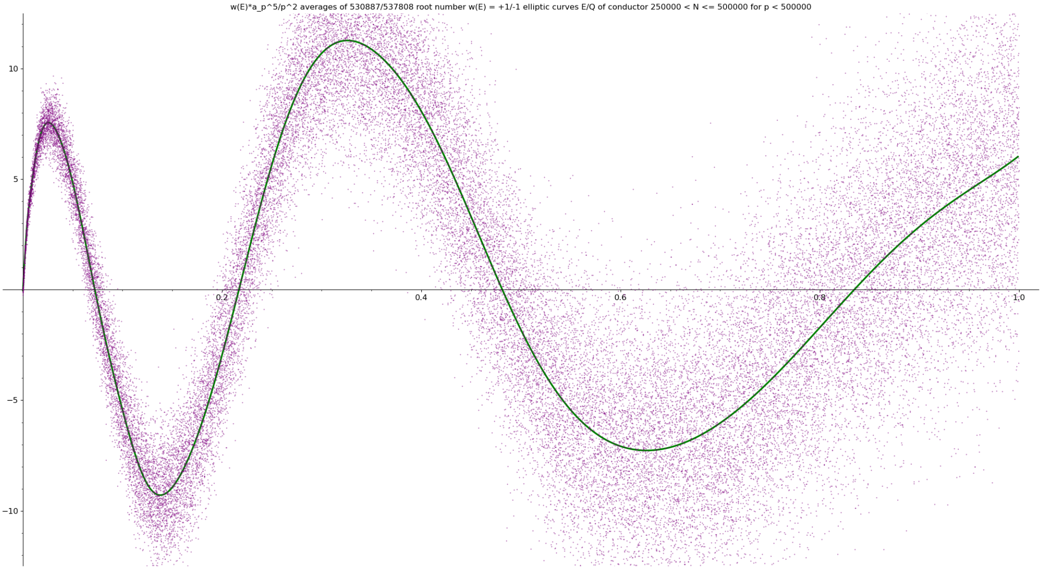


Higher moments $(w_p(E)a_p(E)$ and $w_p(E)a_p(E)^3/p)$





Higher moments $(w_p(E)a_p(E)^5/p^2)$



Arithmetic L-functions

We call an L-function is analytic if it has the properties every good L-function should: analytic continuation, functional equation, Euler product, temperedness, central character; see FPRS18; it is analytically normalized if its central value is at $s = 1/2$.

An analytically normalized L-function $L_{\rm an}(s) = \sum a_n n^{-s}$ is arithmetic if $a_n n^{\omega/2} \in \mathcal{O}_K$ for some number field K and $\omega \in \mathbb{Z}_{\geq 0}$. The least such ω is the motivic weight.
Its arithmetic normalization $L(s) := L_{\rm an}(s + \omega/2)$ has coefficients in $\mathcal{O}_K$ and satisfies

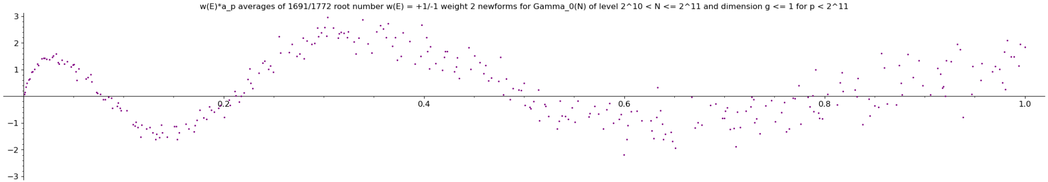
$$\Lambda(s) = N^{1-s} w \bar{\Lambda}(1 + \omega - s).$$

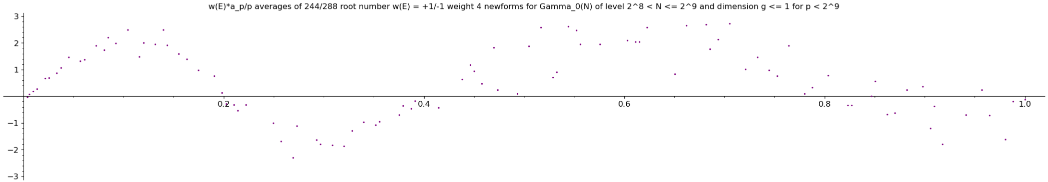
L-functions of abelian varieties have motivic weight $\omega = 1$.
L-functions of weight-k holomorphic cuspforms have motivic weight $\omega = k - 1$.

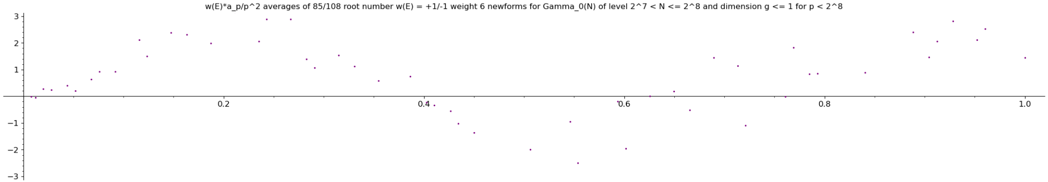
We consider Galois-closed families of self-dual arithmetically normalized L-functions.
In any such family the values of a_p and m_p are integers and $w = \pm 1$.

When averaging a_p's in motivic weight $\omega > 1$ we normalize them via $a_p \mapsto a_p/p^{(\omega-1)/2}$.
This ensures that we always have $|a_p| = O(\sqrt{p})$, as with elliptic curves.

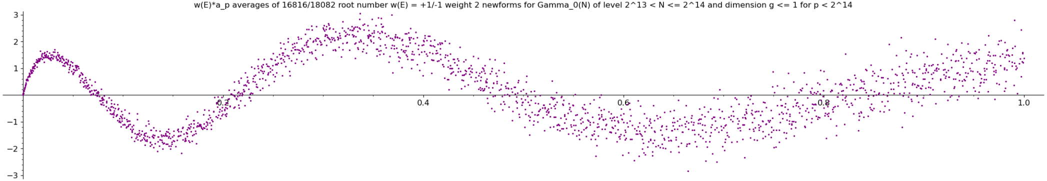
Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6$ with rational coefficients.

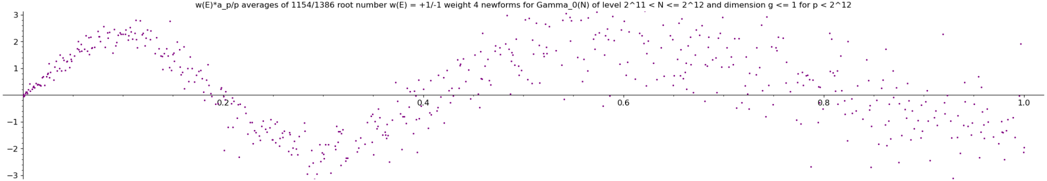


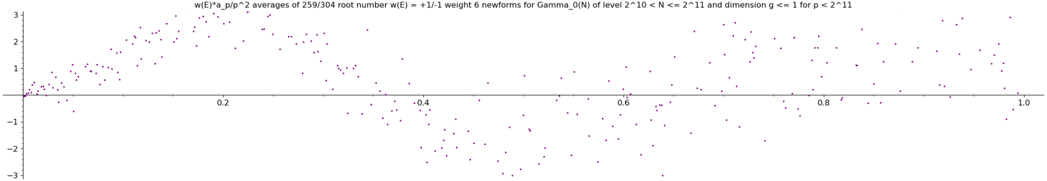




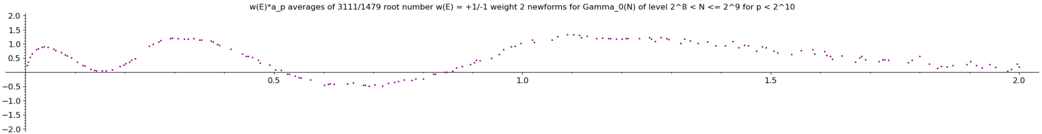
Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6$ with rational coefficients.

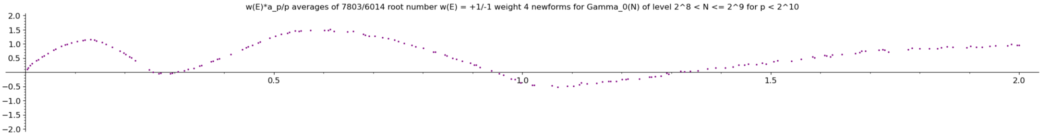


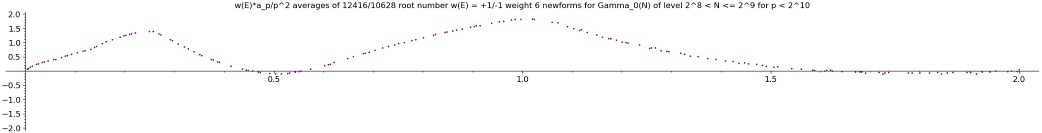


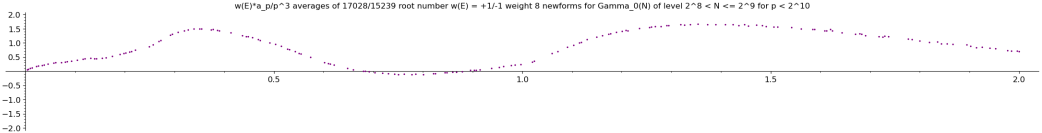


Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6, 8$.

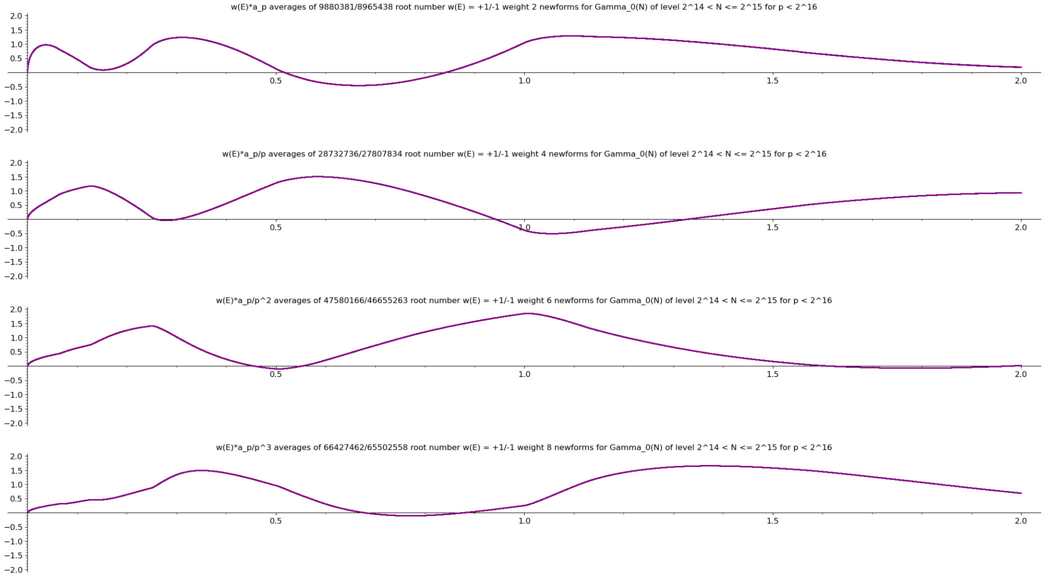








Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6, 8$.



Zubrilina's theorem (click me!)

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

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

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

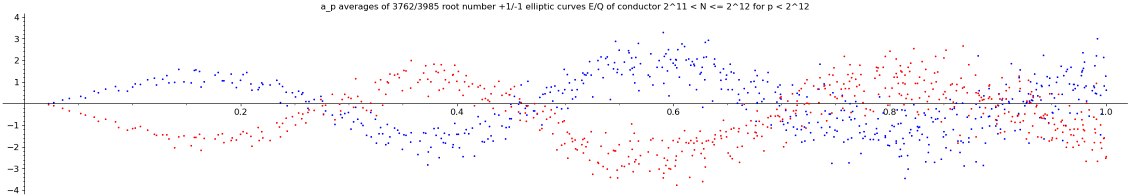
Theorem [Zubrilina 2023]. Let $\sum a_n(f)q^n$ denote a weight-k newform for $\Gamma_0(N)$ with root number $w(f)$. Let $X, Y, P \to \infty$ with P prime, $Y \sim X^{1-\delta}$, $P \ll X^{1+\delta_1}$, $\delta, \delta_1 > 0$ and $2\delta_1 < \delta < 1$, and put $y := \sqrt{P/X}$. Then for every $\varepsilon > 0$ we have

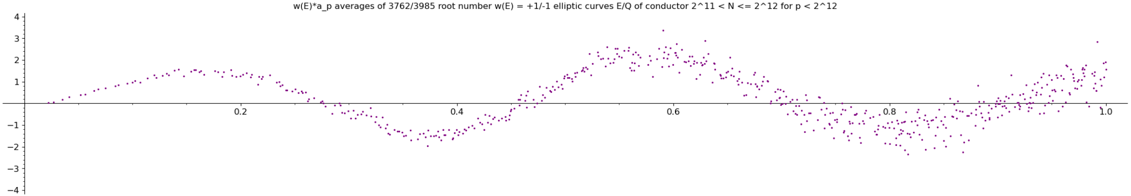
$$\frac{\sum_{N\in[X,X+Y]}^{\square\text{-free}} \sum_f w(f)a_P(f)P^{(1-k/2)}}{\sum_{N\in[X,X+Y]}^{\square\text{-free}} \sum_f 1} = M_k(y) + O_\varepsilon(X^{-\delta'+\varepsilon} + P^{-1})$$

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

Murmurations of elliptic curves with squareroot normalization

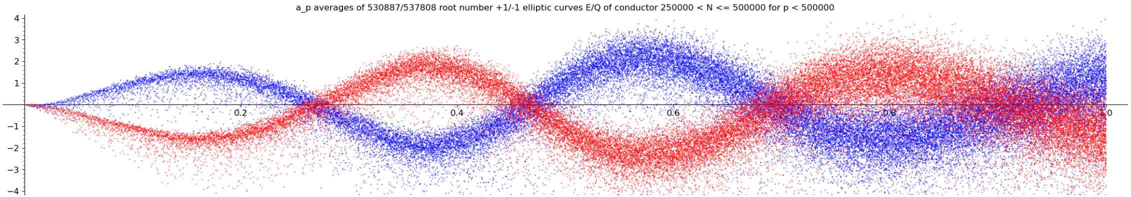
Elliptic curve L-functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \ldots, 2^{17}, 250000$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(\sqrt{p}, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or $m_p := w(E)a_p(E)$ over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.

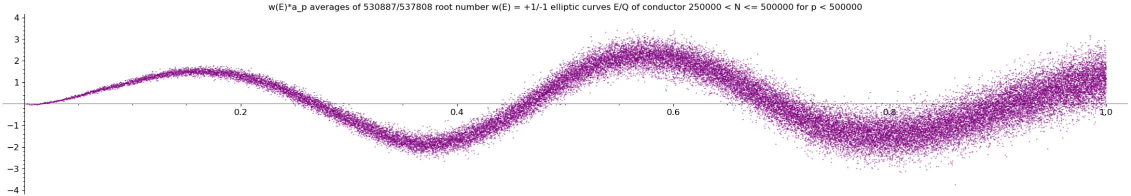




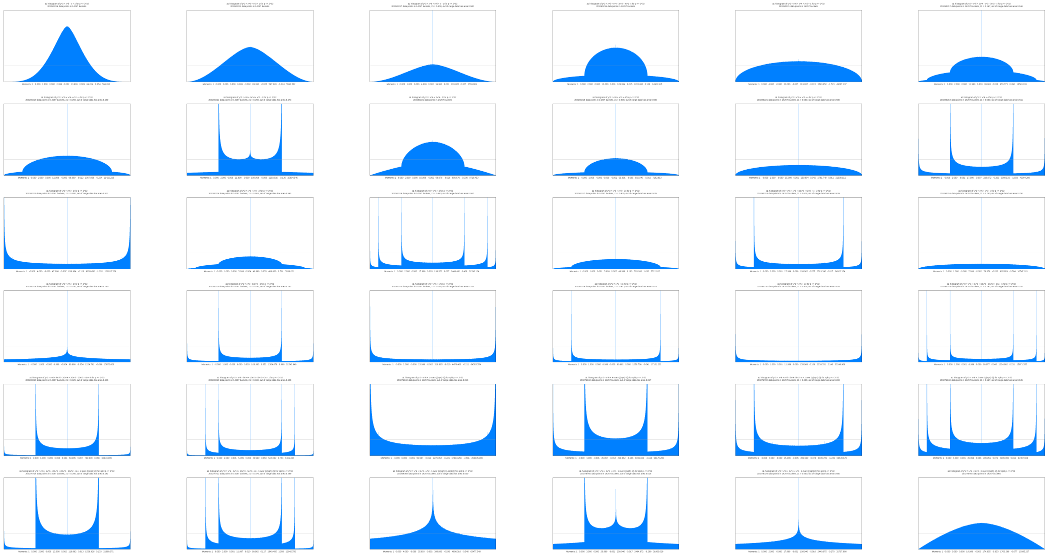
Murmurations of elliptic curves with squareroot normalization

Elliptic curve L-functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \ldots, 2^{17}, 250000$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(\sqrt{p}, \bar{a}_p \text{ or } \bar{m}_p)$ shows the average of a_p or $m_p := w(E)a_p(E)$ over even/odd or all $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.



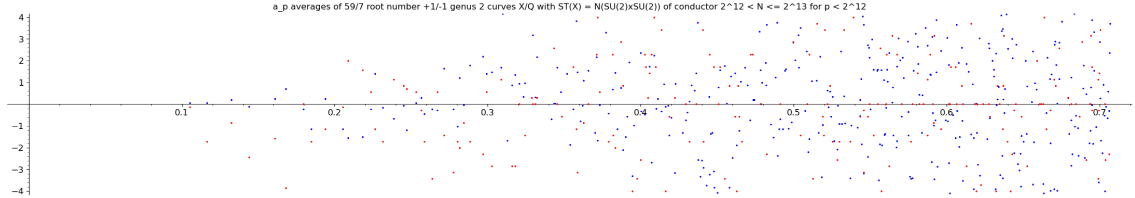


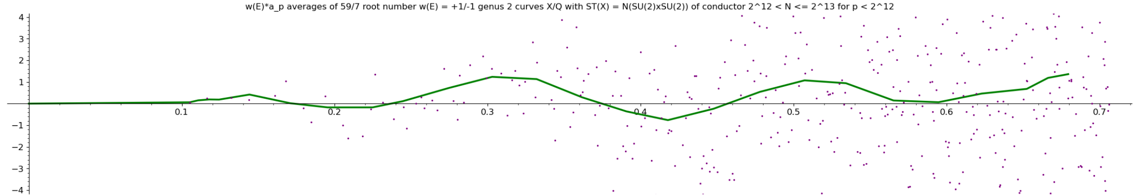
Trace distributions of genus 2 curves



L-functions of genus 2 curves over $\mathbb{Q}$, Sato-Tate group $N(\mathrm{SU}(2) \times \mathrm{SU}(2))$.

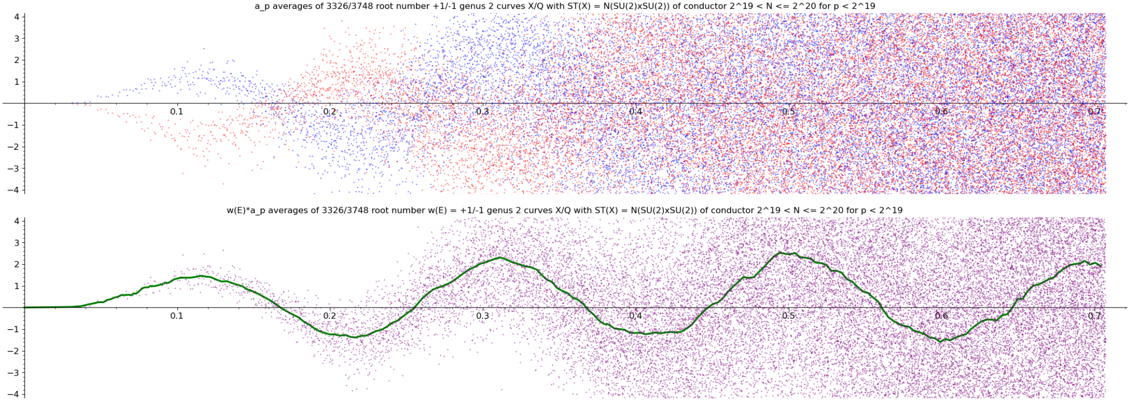
These are primitive L-functions arising from Hilbert or Bianchi modular forms.
Conductor of $L(X, s)$ in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{19}$ with x-axis range $[0, M/2]$.





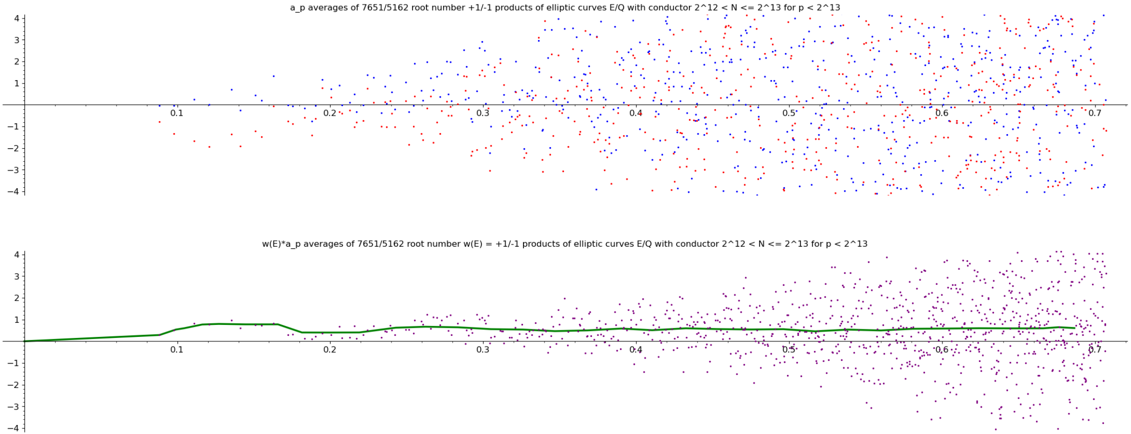
L-functions of genus 2 curves over $\mathbb{Q}$, Sato-Tate group $N(\mathrm{SU}(2) \times \mathrm{SU}(2))$.

These are primitive L-functions arising from Hilbert or Bianchi modular forms.
Conductor of $L(X, s)$ in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{19}$ with x-axis range $[0, M/2]$.



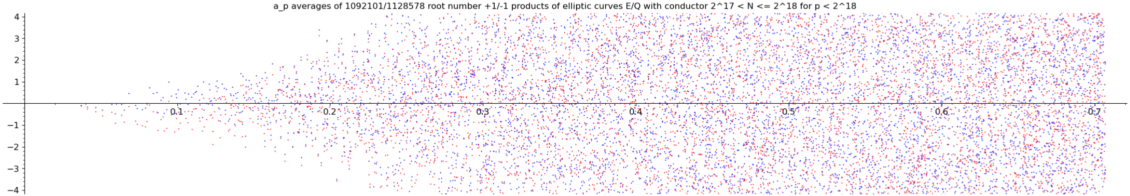
L-functions of products of $E/\mathbb{Q}$, Sato-Tate group $\mathrm{SU}(2) \times \mathrm{SU}(2)$.

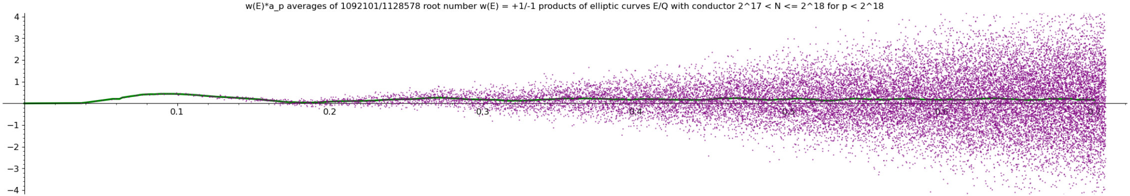
Conductor of $L(X,s)$ in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{17}$ with x-axis range $[0, M/2]$.



L-functions of products of $E/\mathbb{Q}$, Sato-Tate group $\mathrm{SU}(2) \times \mathrm{SU}(2)$.

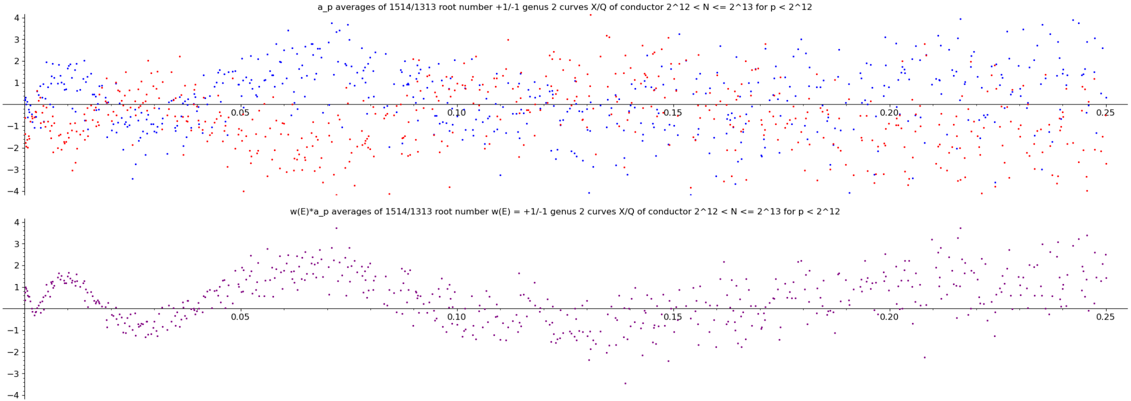
Conductor of $L(X,s)$ in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{17}$ with x-axis range $[0, M/2]$.





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

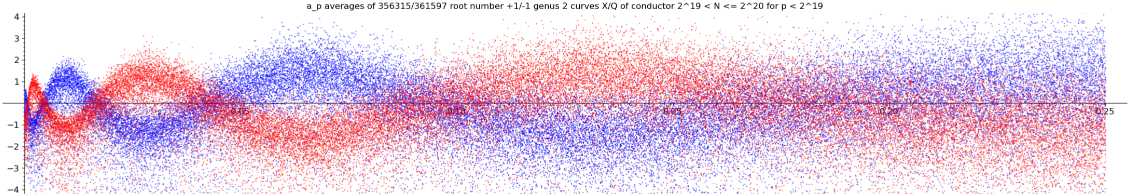
Recently constructed database of more than 6 million genus 2 curves $X/\mathbb{Q}$ of conductor at most 2^{20} includes about 1.7 million isogeny classes with Sato–Tate group USp(4). Conductor of $L(X, s)$ in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{19}$ with x-axis range $[0, M/2]$.

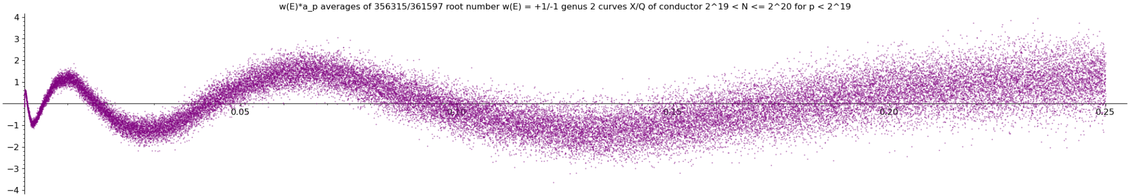


Coming soon to the LMFDB.

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

Recently constructed database of more than 6 million genus 2 curves $X/\mathbb{Q}$ of conductor at most 2^{20} includes about 1.7 million isogeny classes with Sato–Tate group USp(4). Conductor of $L(X,s)$ in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{19}$ with x-axis range $[0, M/2]$.

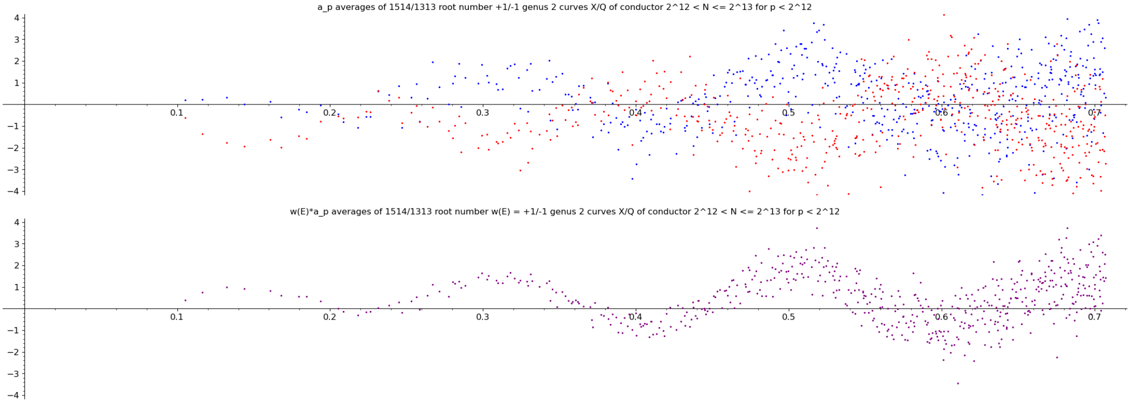




Coming soon to the LMFDB.

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

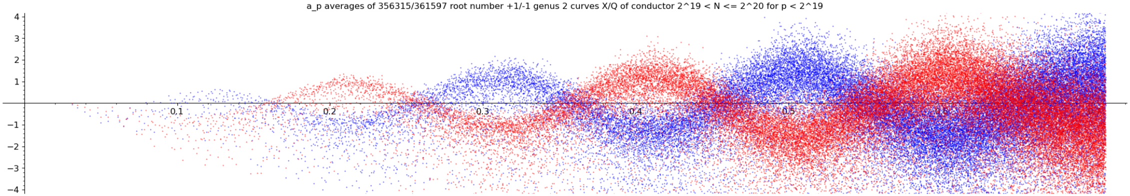
Recently constructed database of more than 6 million genus 2 curves $X/\mathbb{Q}$ of conductor at most 2^{20} includes about 1.7 million isogeny classes with Sato–Tate group USp(4). Conductor of $L(X, s)$ in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{19}$ with x-axis range $[0, M/2]$.

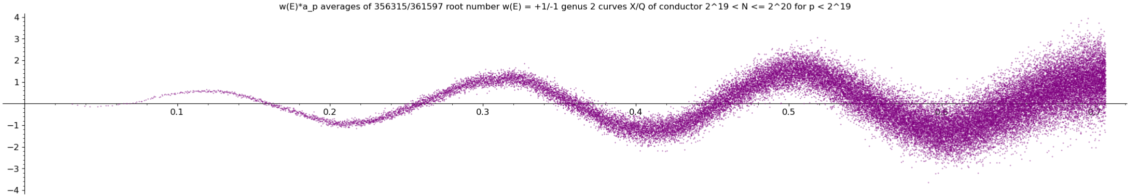


Coming soon to the LMFDB.

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

Recently constructed database of more than 6 million genus 2 curves $X/\mathbb{Q}$ of conductor at most 2^{20} includes about 1.7 million isogeny classes with Sato–Tate group USp(4). Conductor of $L(X,s)$ in $(M,2M]$ for $M = 2^{12},\ldots,2^{19}$ with x-axis range $[0, M/2]$.

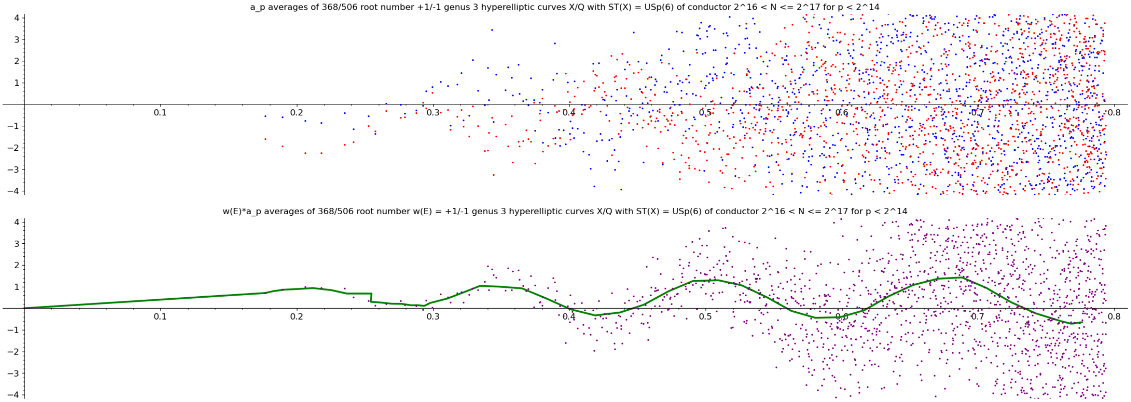




Coming soon to the LMFDB.

L-functions of genus 3 curves over $\mathbb{Q}$ with Sato-Tate group USp(6).

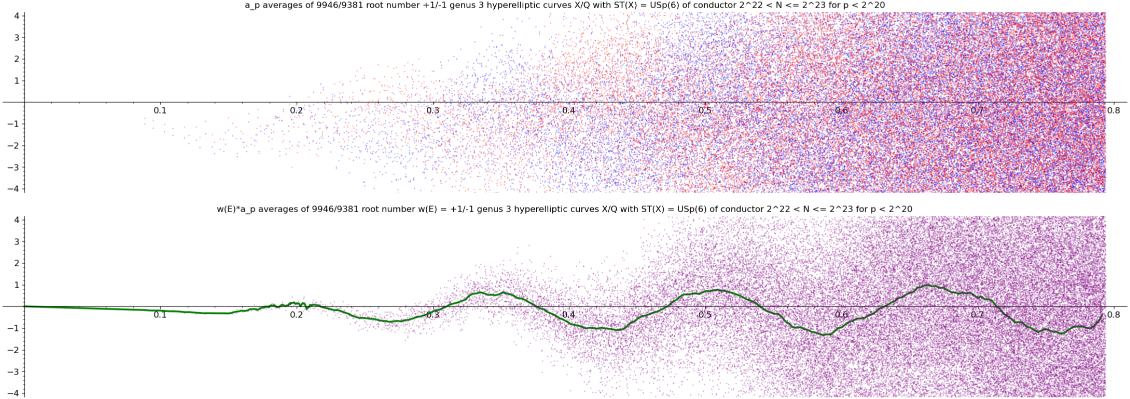
Recently constructed database of genus 3 curves $X/\mathbb{Q}$ of conductor at most 10^7 includes 59,214 isogeny classes of hyperelliptic curves with ST group USp(6). Conductor of $L(X,s)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{22}$ with x-axis range $[0, M/2]$.



Coming soon to the LMFDB.

L-functions of genus 3 curves over $\mathbb{Q}$ with Sato-Tate group USp(6).

Recently constructed database of genus 3 curves $X/\mathbb{Q}$ of conductor at most 10^7 includes 59,214 isogeny classes of hyperelliptic curves with ST group USp(6). Conductor of $L(X,s)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{22}$ with x-axis range $[0, M/2]$.



Coming soon to the LMFDB.

Computing murmurations of elliptic curves

When computing $a_p(E)$ for many $E/\mathbb{Q}$ we construct a lookup table $T[j] = a_p(E)$ for $E\colon y^2 = x^3 + Ax + B$ with $j(E) = j \neq 0, 1728$ and $B = \square$.

Average costs per curve, ignoring $O(\log\log p)$ factors:

- Naive: $O(p)$
- Mestre BSGS: $O(p^{1/4}\log p)$
- Schoof: $O(\log^5 p)$, Schoof–Elkies–Atkin: $O(\log^4 p)$
- CM torsor (isogenies): $O(\log^3 p)$ (GRH), $O(\log^2 p)$ (heuristic).
- CM torsor (GCDs): $O(\log p)$ per curve (heuristic).

We are extending the Stein–Watkins database using Elkies' lattice reduction method to include (conjecturally) all $E/\mathbb{Q}$ with $|\Delta(E)| \leq 10^{17}$ and $N(E)| \leq 10^9$ (versus 10^{12} and 10^8 with no claim of completeness).

Computing murmurations of modular forms

The sum of $w(f)a_p(f)$ over $f \in S_k^{\mathrm{new}}(N)$ is equal to the trace of $T_n \circ W$ acting on $S_k^{\mathrm{new}}(N)$, where the Fricke involution W is defined by $W(f) := f \mid \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$.

By massaging a theorem of Popa, one obtains

$$\mathrm{tr}(T_n \circ W, S_k(N)) = -\frac{1}{2} \sum_{\substack{t^2 N < 4n \\ D := t^2N^2 - 4nN}} g_k(t^2N, n) h^*(D, N) - \frac{1}{2} s_k(N, n) + \delta_{k=2}\, \sigma_N(n) - \delta_{\substack{N=1 \\ n=\square}} \frac{k-1}{12} n^{k/2-1}.$$

We compute $h^*(D, N)$ as the product of a multiplicative function and a class number

The class numbers for $|D| \le 2^{40}$ have been computed by Jacobson and Mosunov and can be downloaded from the LMFDB, and can be crammed into a 1.125TB lookup table. Using a memory mapped file on fast SSD it takes 40s to load.

It then takes less than a minute to compute $\mathrm{tr}(T_p \circ W, S_k^{\mathrm{new}}(N))$ for $2^{18} \le N < 2^{19}$ and $p \le 2^{19}$ for any reasonably small k (on 256 cores).

Computing murmurations of genus 2 and genus 3 curves

The average polynomial time algorithms described in [Harvey-S 2016] and [Costa-Harvey-S 2022] can readily compute the desired trace sums.

The main challenge is finding curves (and abelian varieties) of small conductor.

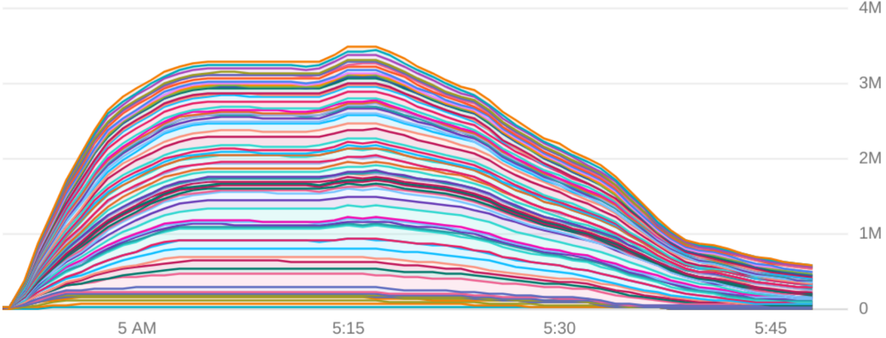
The algorithms described in [BSSVY 2016] and [S 2018] enumerate curves by discriminant, but curves with very large discriminants can have very small conductors.

This is already an issue in genus 1 with the Stein-Watkins database: it misses about $1/4$ of the isogeny classes of conductor up to $5 \cdot 10^5$, despite ranging up to 10^8, but the situation is much worse in higher genus.

Curves may have bad reduction at primes of good reduction for the Jacobian (this happens a lot!). The genus 2 murmurations here use a new dataset of more than six million curves with conductor below 10^6 (99% of these are not in the LMFDB yet!).

Searching for genus 2 curves

Over the past several years we have conducted several searches for genus 2 curves of small conductor. Below is CPU histogram from a computation from the largest of these computations, run on Google's Cloud Platform.



We used a total of 4,034,560 Intel/AMD vCPUs in 73 data centers across the globe.

Expanding the LMFDB

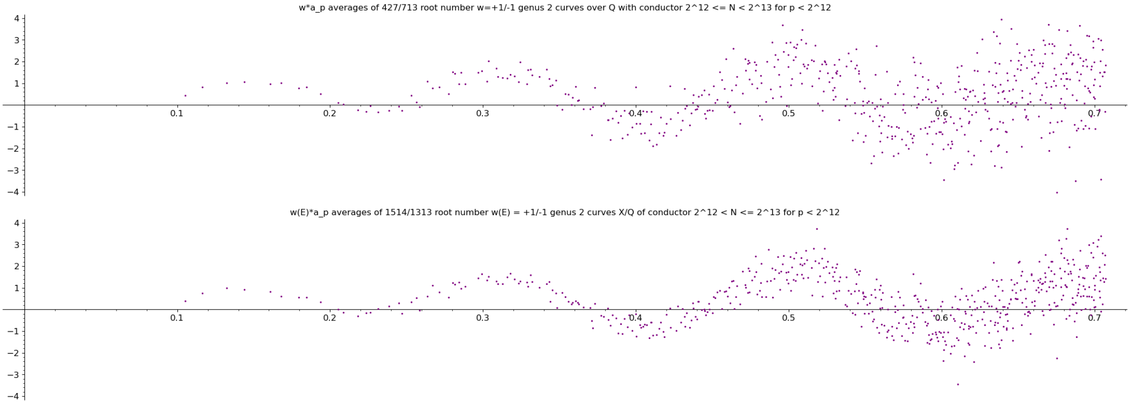
We found curves of conductor 657, 760, 775, 903, and 924 not previously known to occur, and many new genus-2 L-functions of small conductor:

conductor bound	1000	10000	100000	1000000
curves in LMFDB	159	3069	20265	66158
curves found	942	29514	493899	6075571
L-functions in LMFDB	109	2807	19775	65534
L-functions found	201	9534	194612	2559187

Standard divisibility test for $p < 2^{10}$	$\approx$ 2700 clock cycles
Montgomery divisibility test for $p < 2^{10}$	$\approx$ 960 clock cycles
AVX-512FMA divisiblity test for $p < 2^{10}$	$\approx$ 120 clock cycles
AVX-512FMA prime power testing (using mod-p tests)	$\approx$ 20 clock cycles

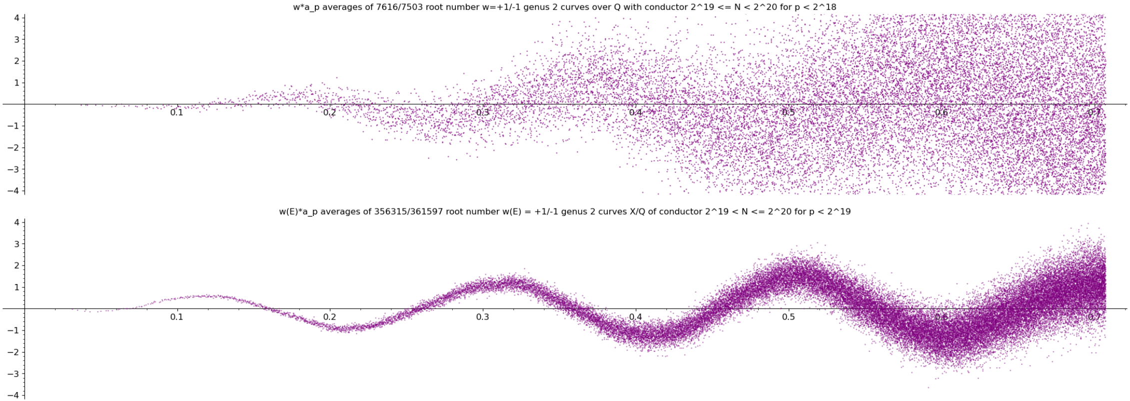
L-functions of genus 2 curves over $\mathbb{Q}$ with Sato-Tate group USp(4).

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

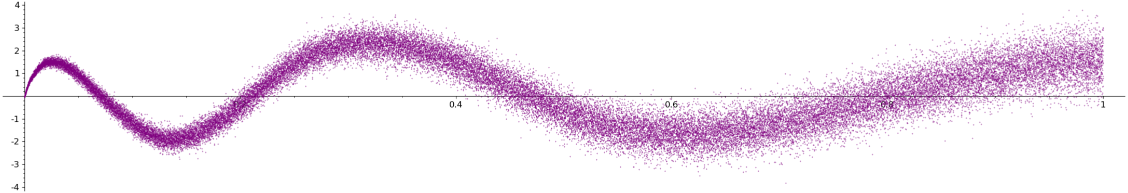


L-functions of genus 2 curves over $\mathbb{Q}$ with Sato-Tate group USp(4).

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



Thank you!



Animations available at https://math.mit.edu/~drew/murmurations.html.