Murmurations of Arithmetic L-functions

Andrew V. Sutherland

Massachusetts Institute of Technology

May 17, 2023

Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation

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

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 the Sato-Tate group of E (typically SU(2)).

2. **Birch and Swinnerton-Dyer**:

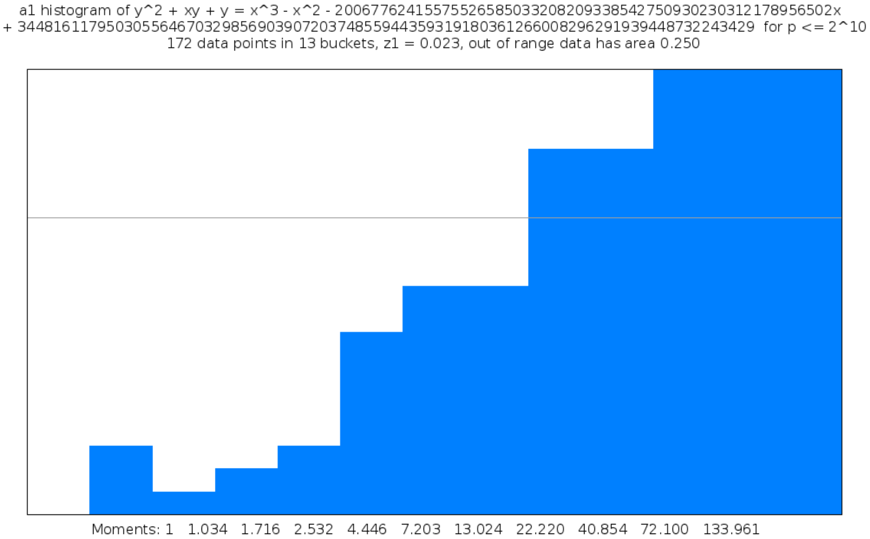
$$\lim_{x\to\infty} \frac{\log x}{2\sqrt{x}} \sum_{p\le x} \frac{a_p(E)}{\sqrt{p}} = \frac{1}{2} - r_{\mathrm{an}}(E).$$

3. **Lang–Trotter**: For every nonzero $t \in \mathbb{Z}$ there is a real number $C_{E,t}$ for which

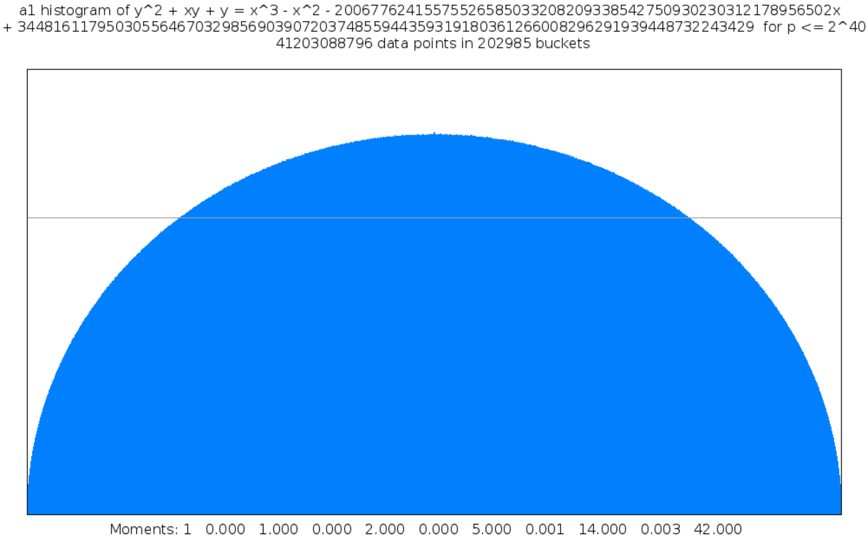
$$\#\{p \le x : a_p(E) = t\} \sim C_{E,t} \frac{\sqrt{x}}{\log x}.$$

These depend only on $L_E(s) = \sum a_n n^{-s}$ and generalize to other L-functions.

Example: Elkies' curve of rank ≥ 28 ($= 28$ under GRH).



Example: Elkies' curve of rank ≥ 28 ($= 28$ under GRH).



How rank effects trace distributions

One formulation of the BSD conjecture implies that

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

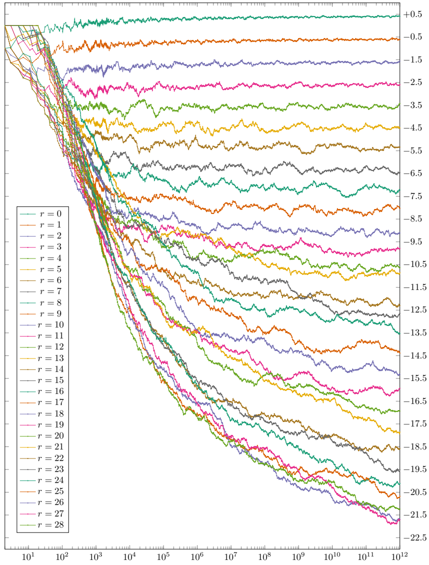
and sums of this form (Mestre-Nagao sums) are often used as a tool when searching for elliptic curves of large rank (which necessarily have large conductor N).[1] [2]

Theorem (Kim-Murty 2023)

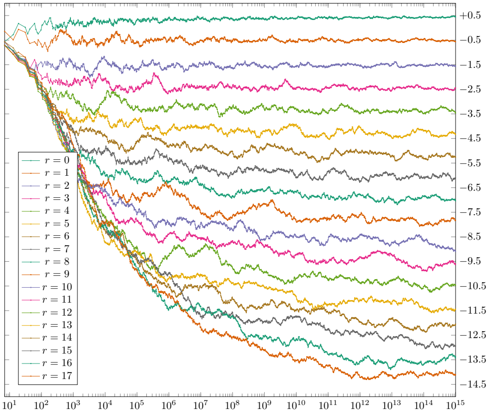
If the limit on the LHS of (1) exists then it equals the RHS with r the analytic rank, and the L-function of E satisfies the Riemann hypothesis.

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

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



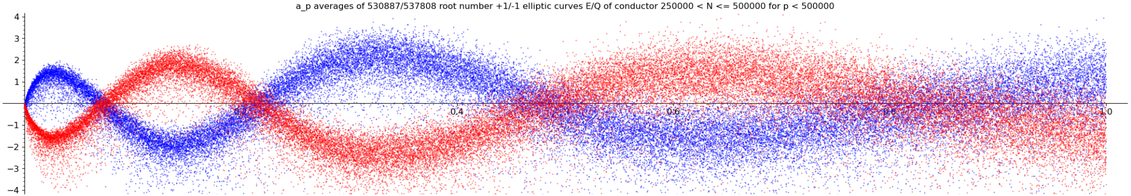
+0.5
−0.5
−1.5
−2.5
−3.5
−4.5
−5.5
−6.5
−7.5
−8.5
−9.5
−10.5
−11.5
−12.5
−13.5
−14.5
10^1 10^2 10^3 10^4 10^5 10^6 10^7 10^8 10^9 10^{10} 10^{11} 10^{12} 10^{13} 10^{14} 10^{15}
$r = 0$
$r = 1$
$r = 2$
$r = 3$
$r = 4$
$r = 5$
$r = 6$
$r = 7$
$r = 8$
$r = 9$
$r = 10$
$r = 11$
$r = 12$
$r = 13$
$r = 14$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

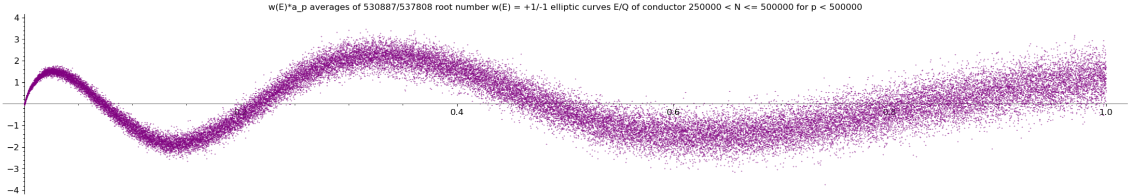
Murmurations of elliptic curves

In their 2022 preprint *Murmurations of elliptic curves*, Yang-Hui He, Kyu-Hwan Lee, Thomas Oliver, and Alexey Pozdnyakov observed a curious fluctuation in average Frobenius traces of elliptic curves in a given conductor interval depending on the rank.

Murmurations of elliptic curves

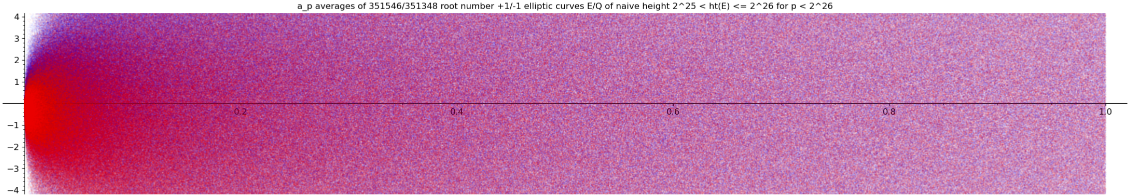
Elliptic curve L-functions of conductor $N \in (M, 2M]$ for $M = 2^{12}, 2^{13}, \ldots, 2^{17}, 250000$. The x-axis range is $[0, 2M]$. A blue/red (or purple) dot at $(p, \bar{a}_p)$ shows the average $\bar{a}_p$ of $a_p(E)$ (or $w_p(E)a_p(E)$) over even/odd rank (or all) $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.

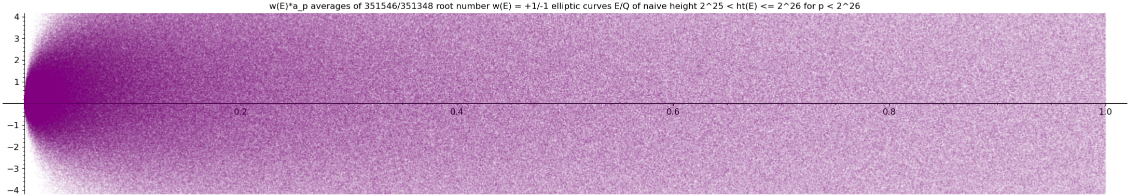




Ordering by naive height

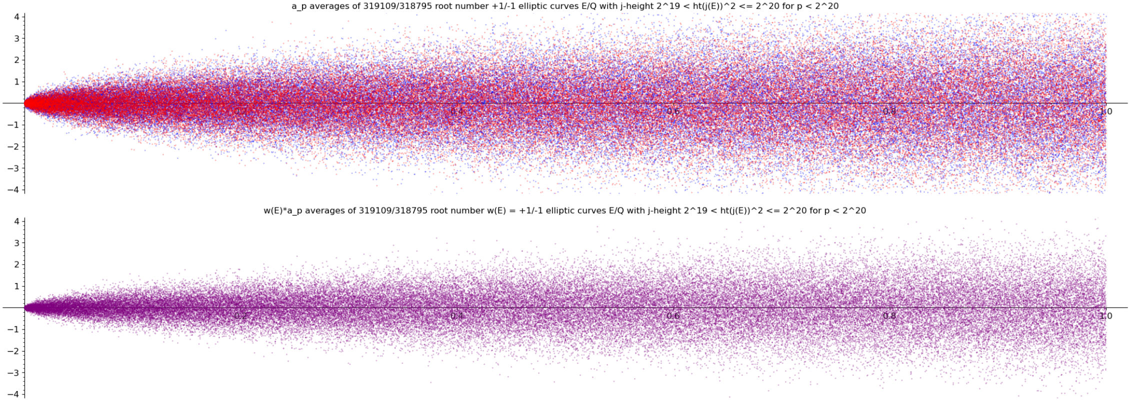
Elliptic curves with $\mathrm{ht}(E) := \max(4|A|^3, 27|B|^2)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{25}$.
The x-axis range is $[0, 2M]$. A blue/red (or purple) dot at $(p, \bar{a}_p)$ shows the average $\bar{a}_p$ of $a_p(E)$ (or $w_p(E)a_p(E)$) over even/odd rank (or all) $E/\mathbb{Q}$ with $\mathrm{ht}(E)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





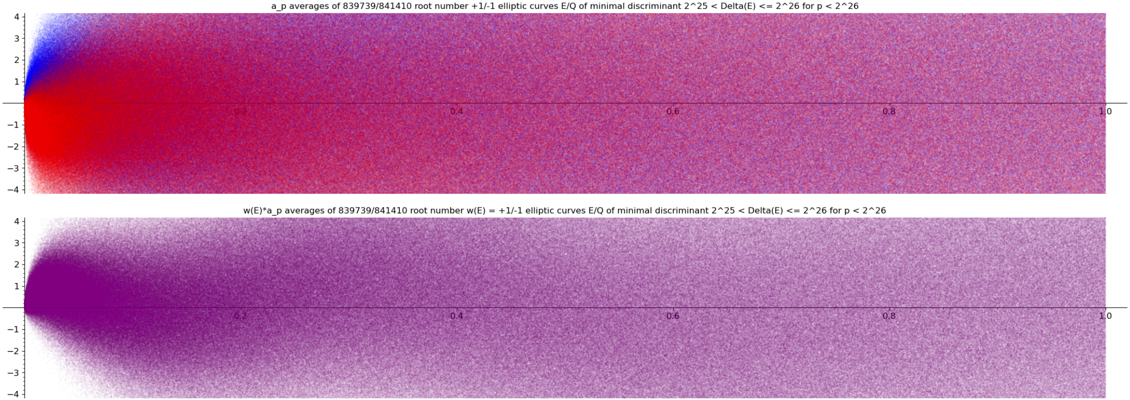
Ordering by j-invariant

Elliptic curves with $\mathrm{ht}(j(E))^2$ in $(M, 2M]$ for $M = 2^{10}, \ldots, 2^{19}$.
The x-axis range is $[0, 2M]$. A blue/red (or purple) dot at $(p, \bar{a}_p)$ shows the average $\bar{a}_p$ of $a_p(E)$ (or $w_p(E)a_p(E)$) over even/odd rank (or all) $E/\mathbb{Q}$ with $\mathrm{ht}(j(E)) \in (M, 2M]$.



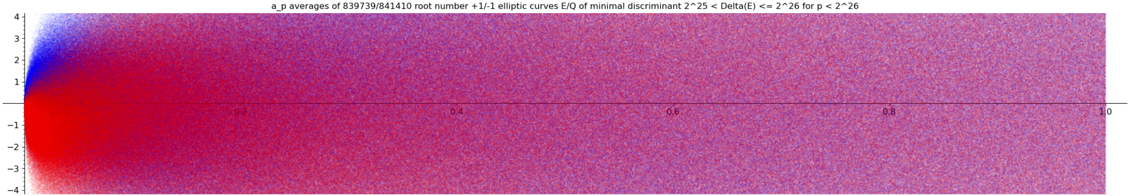
Ordering by minimal discriminant

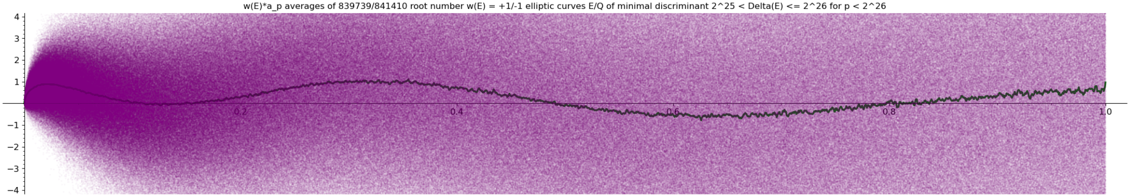
Elliptic curves with minimal discriminant $\Delta(E)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{25}$.
The x-axis range is $[0, 2M]$. A blue/red (or purple) dot at $(p, \bar{a}_p)$ shows the average $\bar{a}_p$ of $a_p(E)$ (or $w_p(E)a_p(E)$) over even/odd rank (or all) $E/\mathbb{Q}$ with $\Delta((E)) \in (M, 2M]$.



Ordering by minimal discriminant

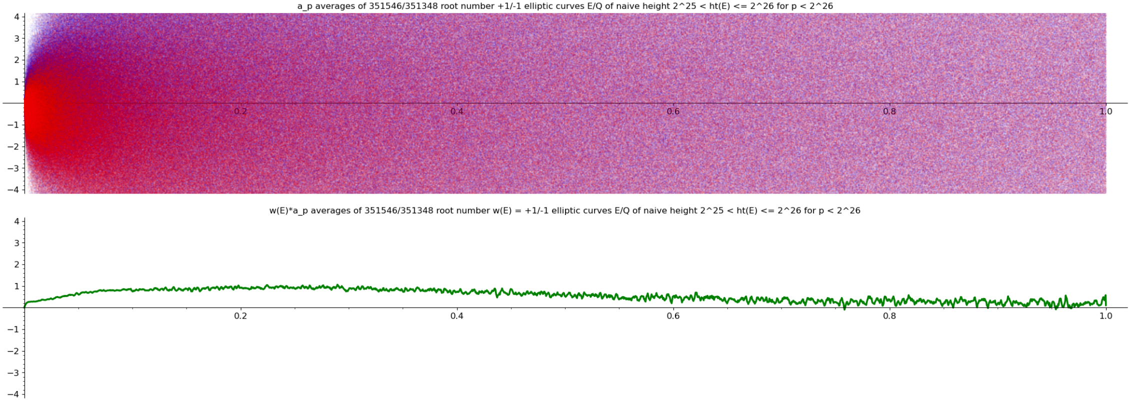
Elliptic curves with minimal discriminant $\Delta(E)$ in $(M, 2M]$ for $M = 2^{16}, \ldots, 2^{25}$.
The x-axis range is $[0, 2M]$. A blue/red (or purple) dot at $(p, \bar{a}_p)$ shows the average $\bar{a}_p$ of $a_p(E)$ (or $w_p(E)a_p(E)$) over even/odd rank (or all) $E/\mathbb{Q}$ with $\Delta((E)) \in (M, 2M]$.





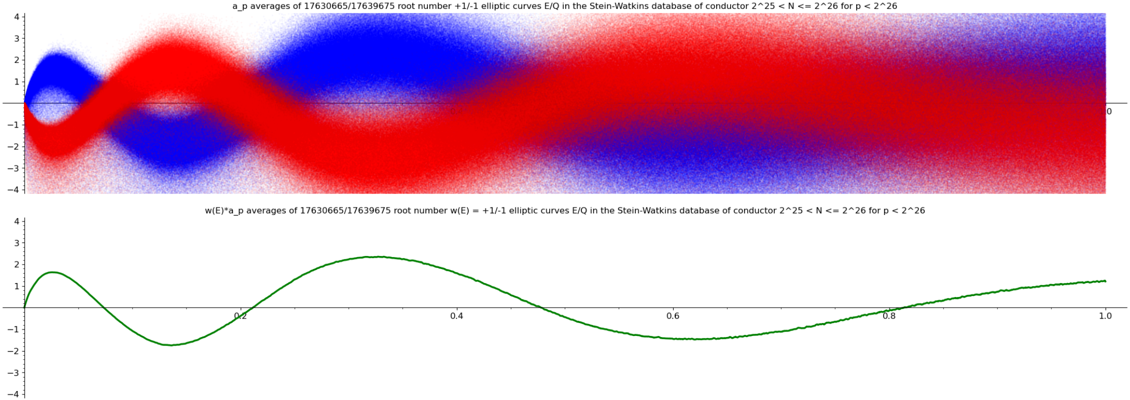
Ordering by naive height (redux)

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



Ordering by conductor in the Stein-Watkins database (SWDB)

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 $(p, \bar{a}_p)$ shows the average $\bar{a}_p$ of $a_p(E)$ (or $w_p(E)a_p(E)$) over even/odd rank (or all) $E/\mathbb{Q}$ with $N_E \in (M, 2M]$.



Arithmetic L-functions

An L-function is said to be analytic if it satisfies the properties that every good L-function should (analytic continuation, functional equation, Euler product, temperedness, central character); see Farmer–Pitale–Ryan–Schmidt 2018 for details.

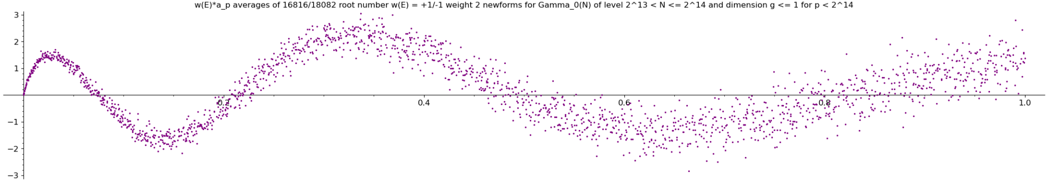
We that an analytic L-function $L(s) = \sum a_n n^{-s}$ is arithmetic if there is an integer w for which $a_n n^{w/2} \in \mathcal{O}_K$ for some number field K. The least such w is the motivic weight.

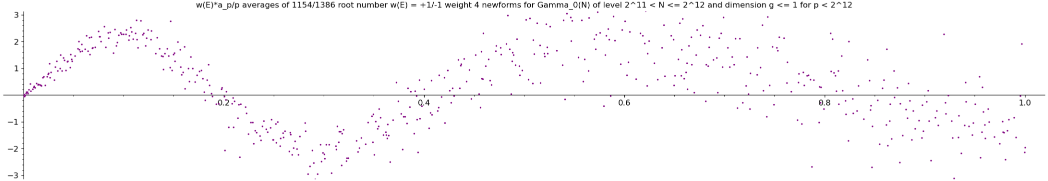
L-functions of abelian varieties have motivic weight $w = 1$.
L-functions of weight-k modular forms have motivic weight $w = k - 1$.

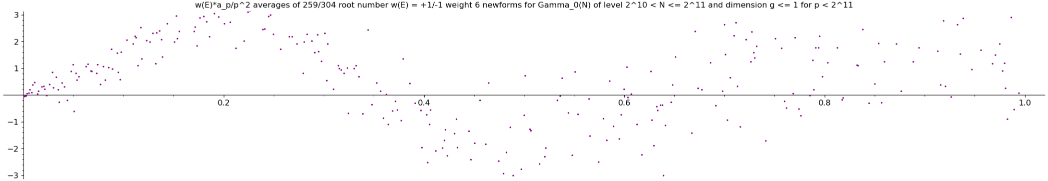
In what follows we consider families of arithmetic L-functions that are Galois closed, meaning that if we average Dirichlet coefficients a_p over L-functions of a given conductor we get integers. We also assume that analytic rank is Galois-invariant.

When averaging a_p's in motivic weight $w > 1$ we normalize via: $a_p \mapsto a_p / p^{(w-1)/2}$.

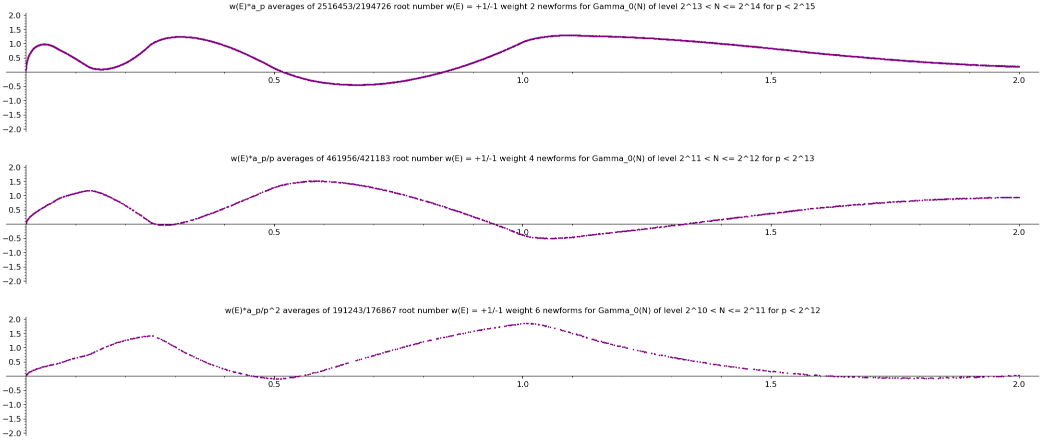
Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6$ with rational coefficients.



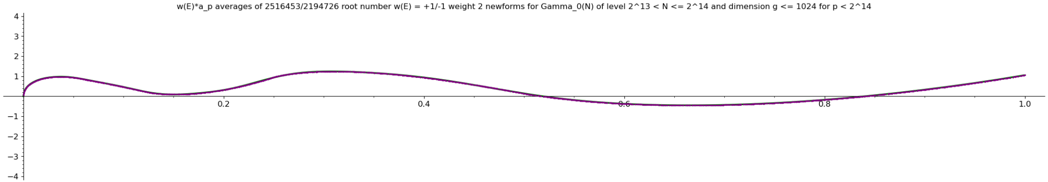


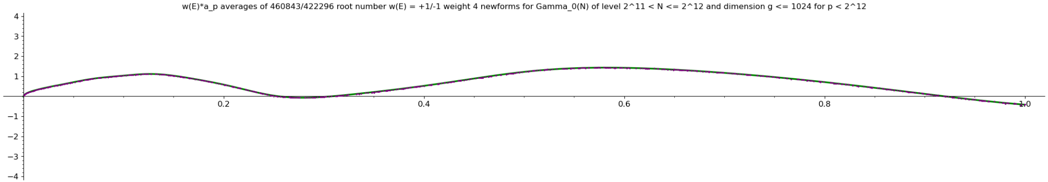


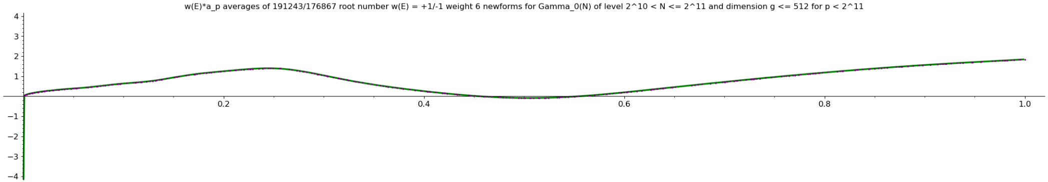
Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6$.



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

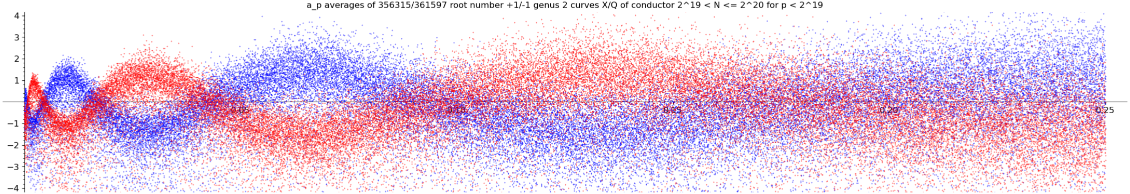


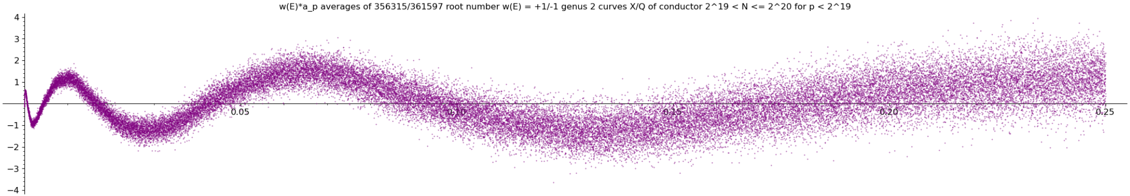




L-functions of genus 2 curves over $\mathbb{Q}$ with Sato-Tate group USp(4).

Recently constructed database of more than 5 million genus 2 curves $X/\mathbb{Q}$ of conductor at most 2^{20} includes 1,440,894 isogeny classes with ST group USp(4). Conductor in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{19}$ with x-axis range $[0, M]$.

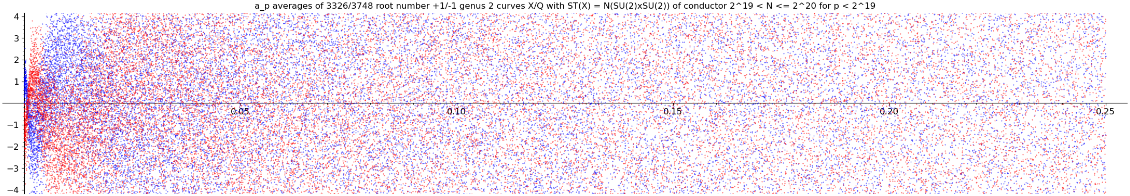


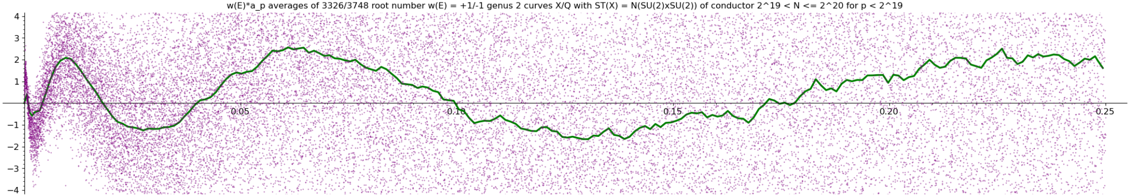


Coming soon to the LMFDB.

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

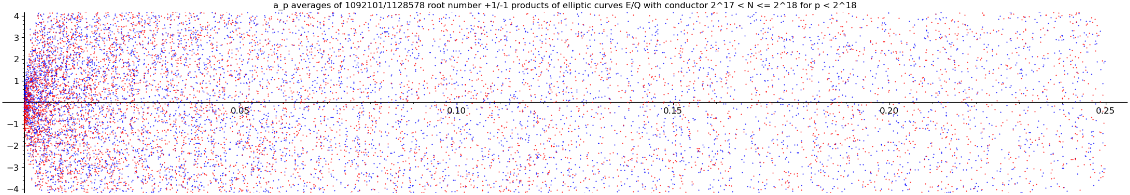
These are primitive L-functions arising from Hilbert or Bianchi modular forms.
Conductor in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{19}$ with x-axis range $[0, M]$.

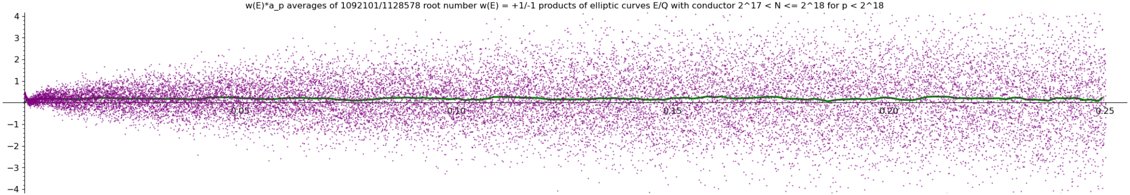




L-functions of products of $E/\mathbb{Q}$, Sato-Tate group $\mathrm{SU}(2) \times \mathrm{SU}(2)$.

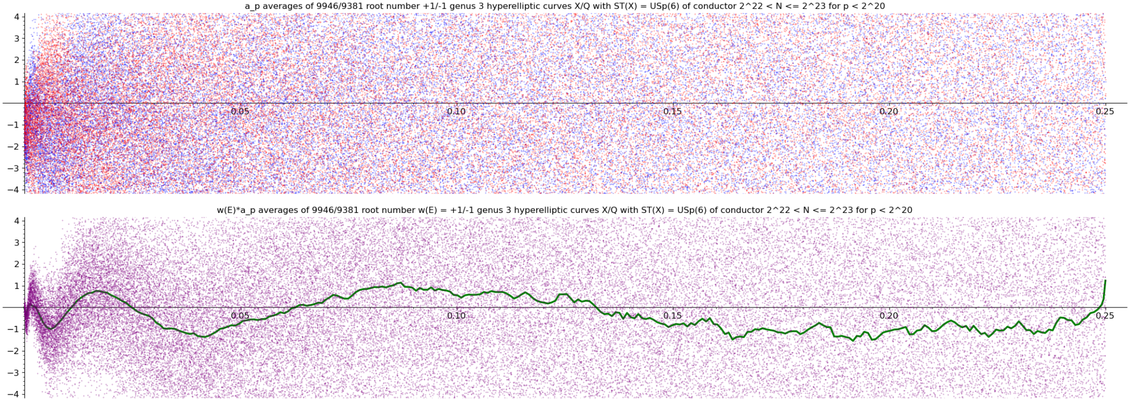
Conductor in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{17}$ with x-axis range $[0, M]$.





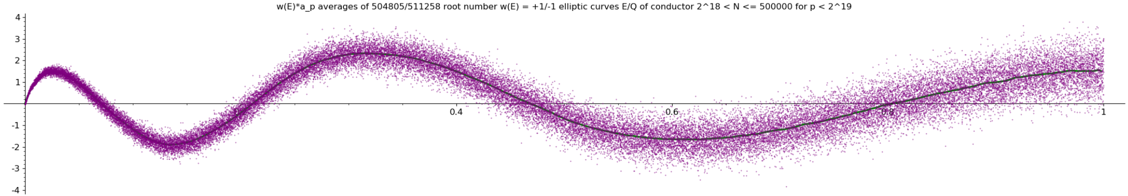
L-functions of genus 3 curves over $\mathbb{Q}$ with Sato-Tate group USp(6).

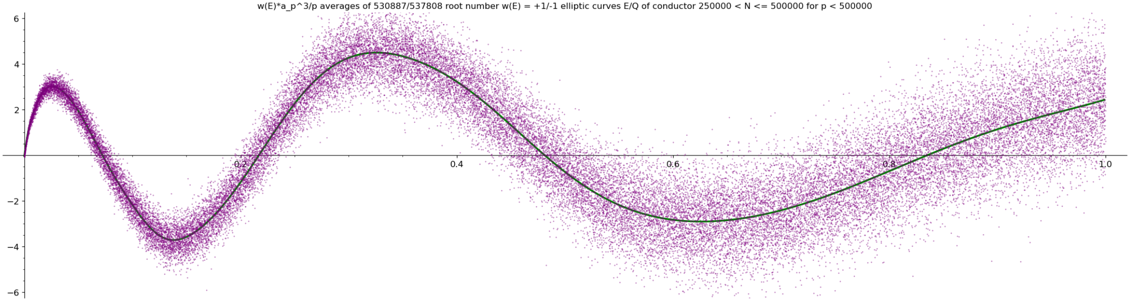
Recently constructed database of genus 3 curves $X/\mathbb{Q}$ of conductor at most 2^{20} includes 59,214 isogeny classes of hyperelliptic curves with ST group USp(6). Conductor in $(M, 2M]$ for $M = 2^{12}, \ldots, 2^{19}$ with x-axis range $[0, M]$.



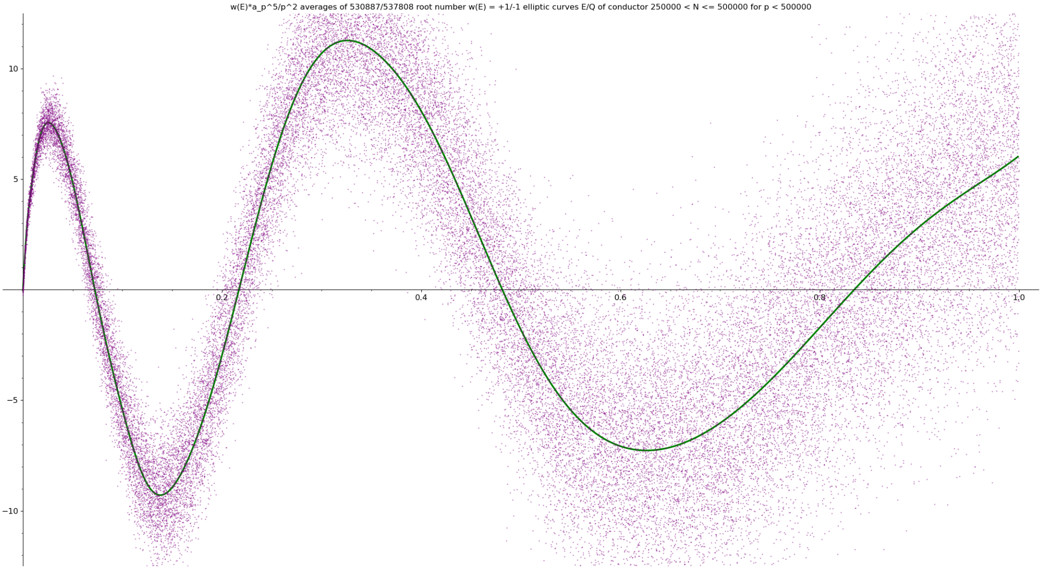
Coming soon to the LMFDB.

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





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



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

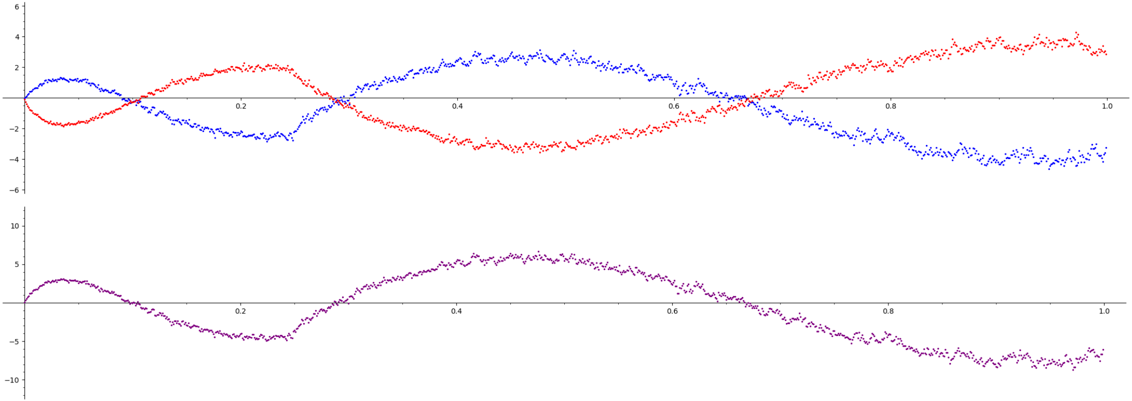
$$\frac{p}{N} \in \Big(x, x+\frac{1}{n}\Big],$$

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.

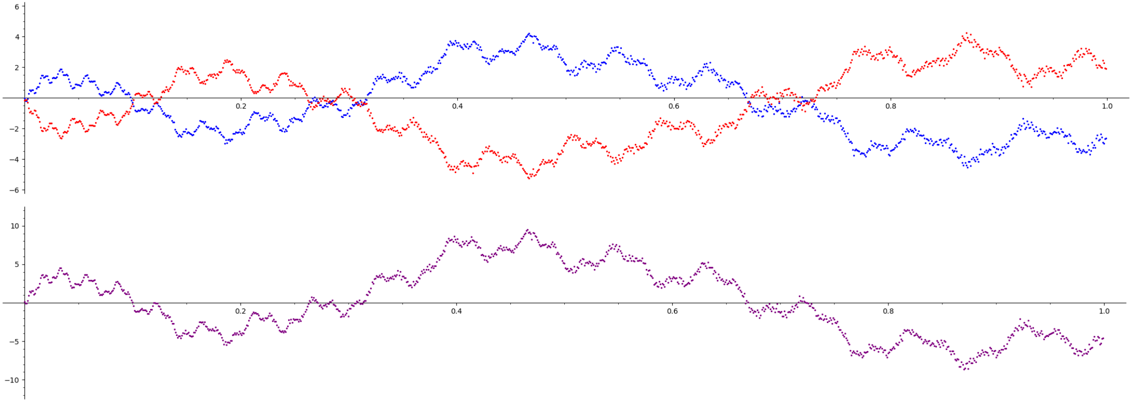
Local averaging: elliptic curves ordered by conductor

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 $N_E \leq M$.

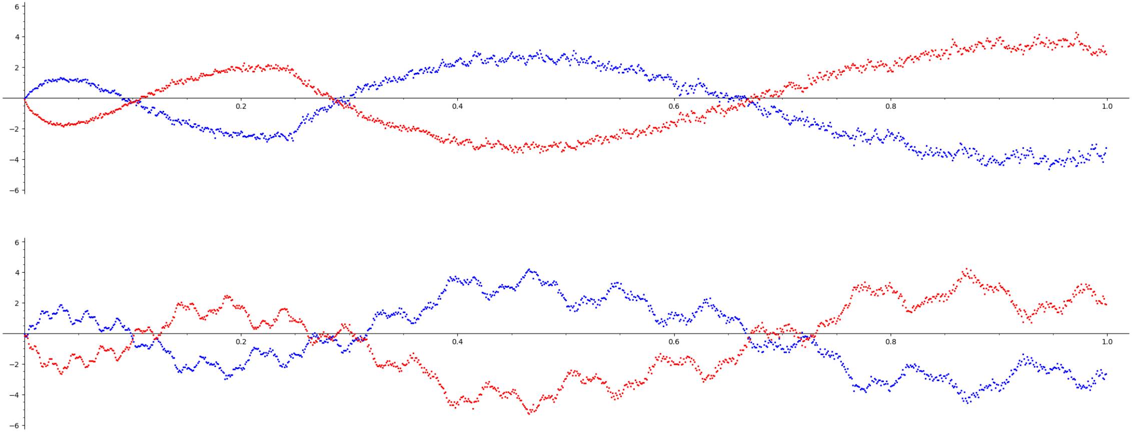


Local averaging: elliptic curves ordered by naive height

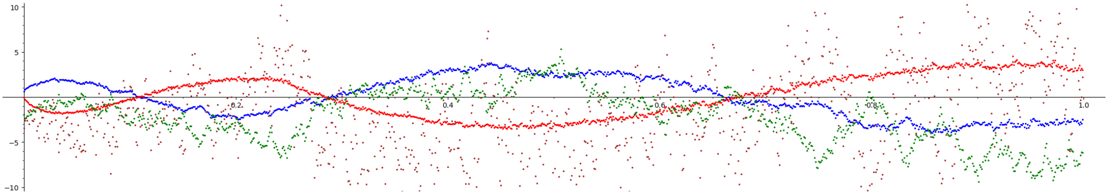
Elliptic curves with $\mathrm{ht}(E) := \max(4|A|^3, 27|B|^2) \le M$ for $M = 2^{18}, \ldots, 2^{27}$.
The x-axis range is $[0, 1]$. A blue/red (or purple) dot at $(x, \bar{\alpha}_x)$ shows the average $\bar{\alpha}_x$ of $\alpha_x(E)$ (or $w_p(E)\alpha_x(E)$) over even/odd rank (or all) $E/\mathbb{Q}$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

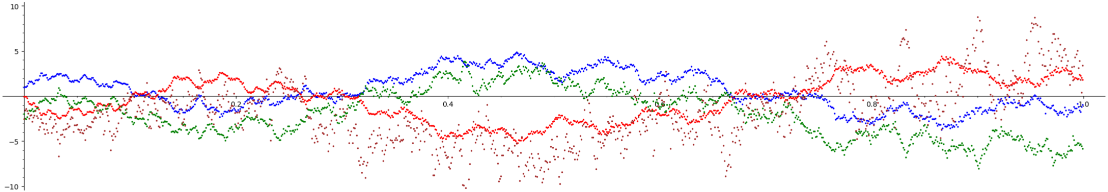


Local averaging: elliptic curves ordered by conductor vs height

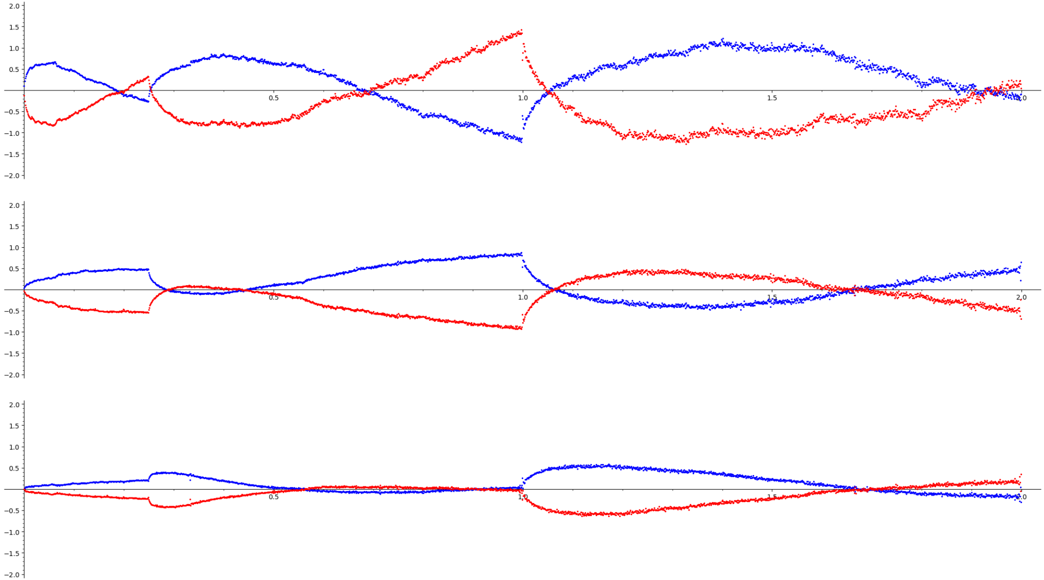


Local averaging: elliptic curves ordered by conductor vs height (rank)

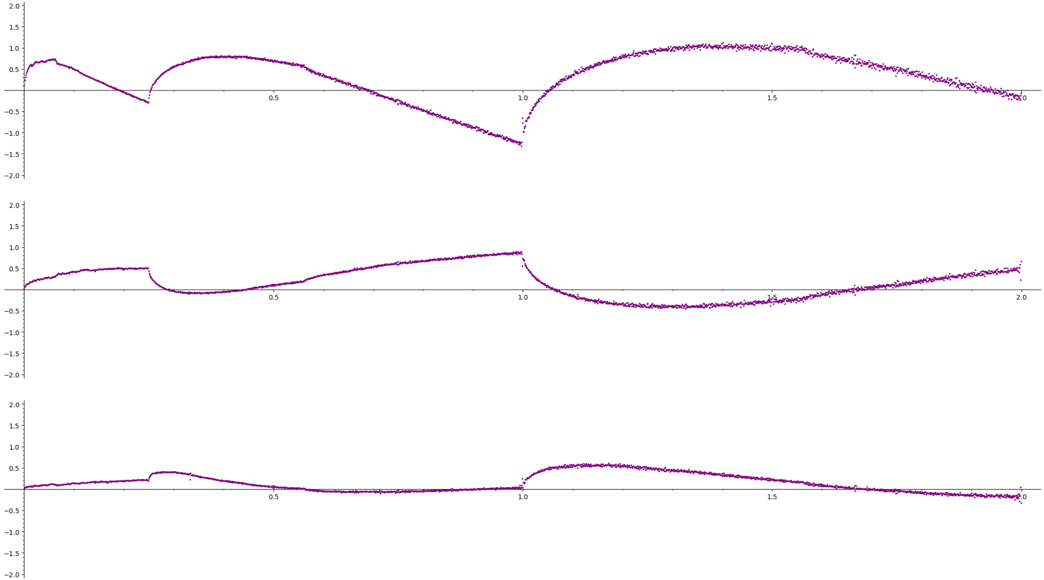




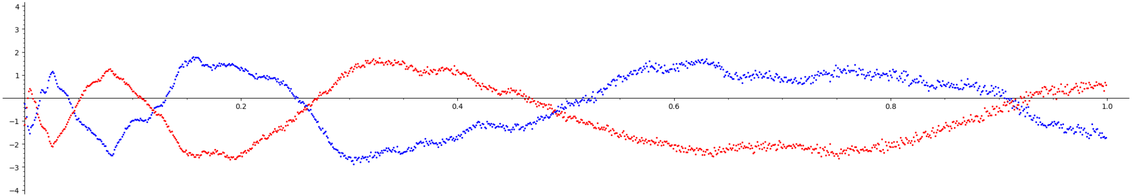
Local averaging: newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6$

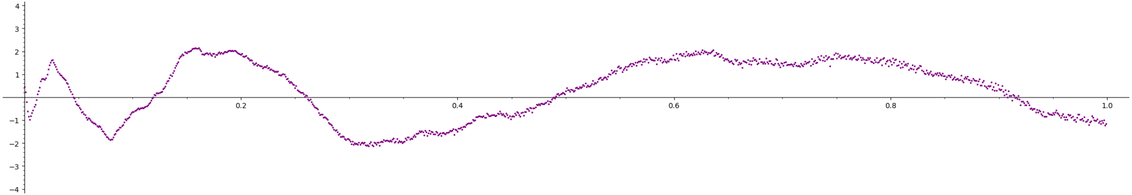


Local averaging: newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6$

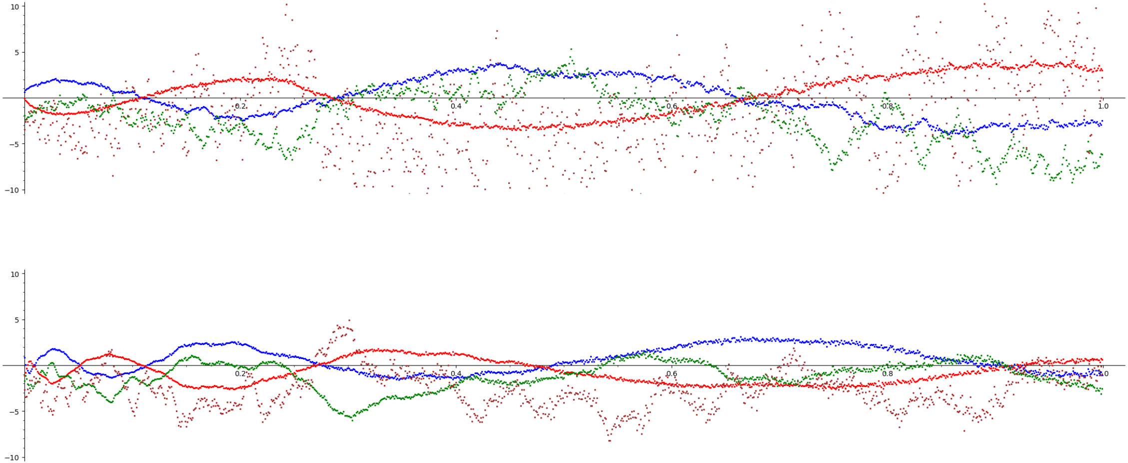


Local averaging: genus 2 USp(4) L-functions

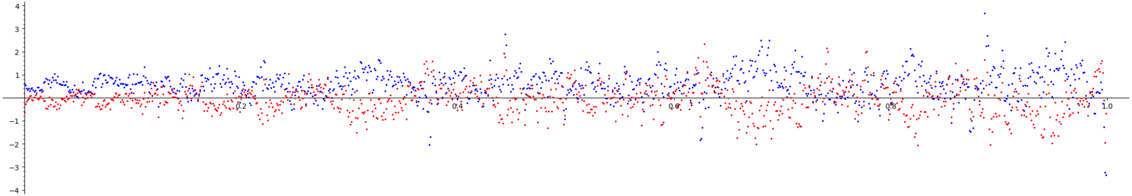


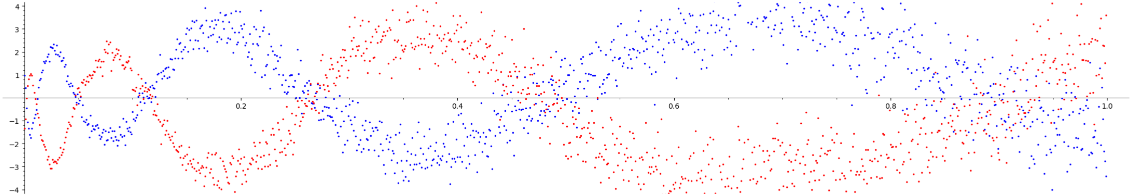


Local averaging: SU(2) and USp(4) L-functions (rank)



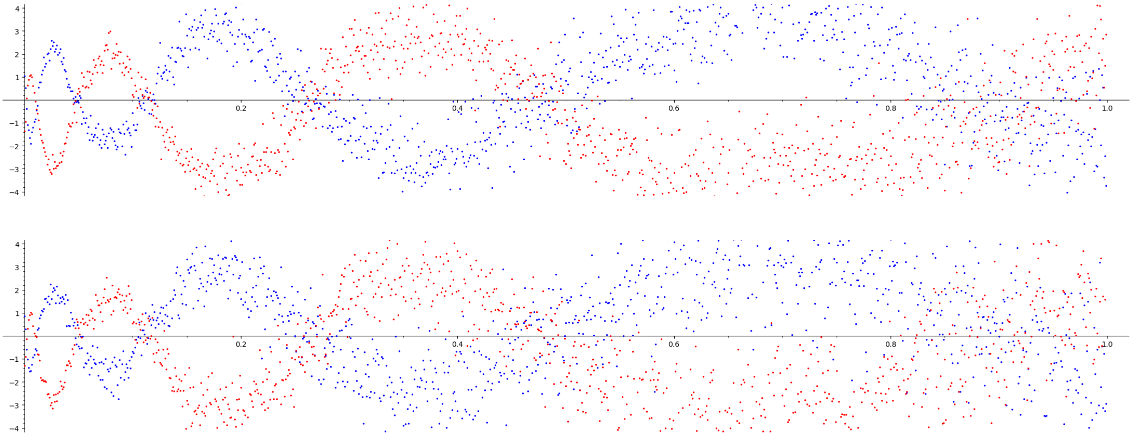
Local averaging: genus 2 SU(2) × SU(2) and N(SU(2) × SU(2)) L-functions





Local averaging: genus 2 $N(\mathrm{SU}(2) \times \mathrm{SU}(2))$ L-functions

Abelian surfaces with Sato-Tate group $N(\mathrm{SU}(2) \times \mathrm{SU}(2))$ have L-functions that correspond to a Hilbert or Bianchi modular form.



Local averaging: twists of `11a1`

Local averaging also allows us to consider thinner families of L-functions.

For example, consider the L-functions of quadratic twists of a fixed elliptic curve $E/\mathbb{Q}$. The conductor grows like X^2 and the naive height grows like X^6.