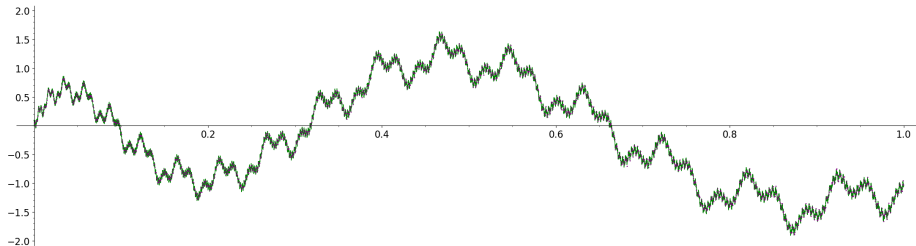


Murmurations for elliptic curves ordered by height

Andrew V. Sutherland

Massachusetts Institute of Technology

October 22, 2025



Joint work with Will Sawin (arXiv:[2504.12295](https://arxiv.org/abs/2504.12295)).

Elliptic curves and their L -functions

Let $E/\mathbb{Q}$ be an elliptic curve, say $E: y^2 = x^3 + Ax + B$ 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 $p \mid \Delta(E)$, 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 $\chi(p) = \begin{cases} 0 & p \mid N(E) \\ 1 & \text{otherwise} \end{cases}$ 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** $\varepsilon(E) = \pm 1$ which appear in the **functional equation**

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

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:**

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

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

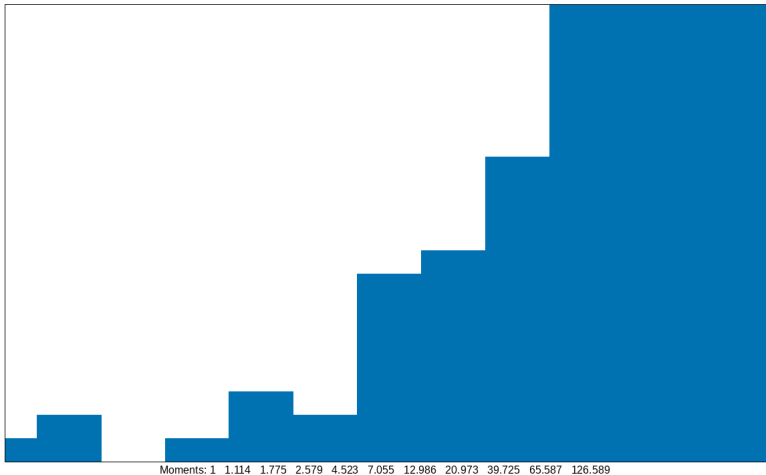
$$\#\{p \leq x : a_p(E) = t\} \sim C_{E,t} \frac{\sqrt{x}}{\log x}.$$

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

Example: Elkies–Klagsbrun curve of rank ≥ 29 .

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

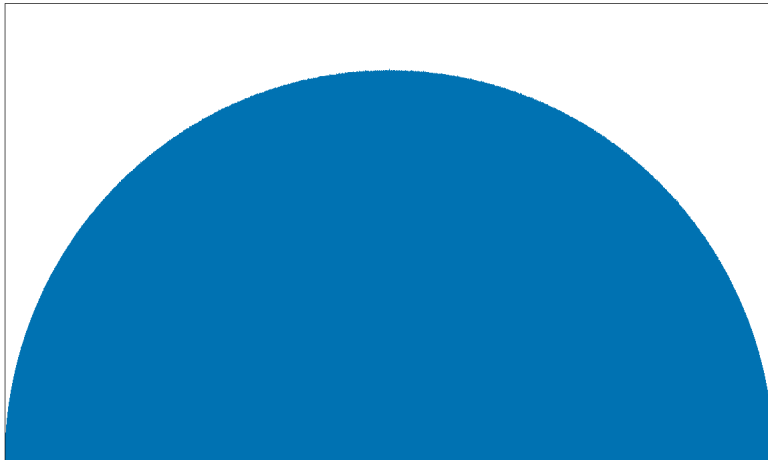
159 data points in 13 buckets, $z_1 = 0.025$, out of range data has area 0.252



Example: Elkies–Klagsbrun curve of rank ≥ 29 .

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

How rank affects trace distributions

An early form of the BSD conjecture implies that

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

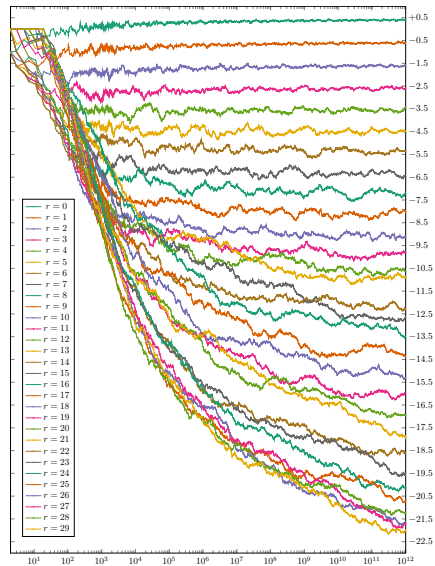
Sums of this form (Mestre–Nagao sums) are often used as a tool when searching for elliptic curves of large rank (which necessarily have large conductor N).^{1 2}

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.

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

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



Why are there still unsolved problems in number theory?

From Mazur's 2008 article *Finding meaning in error terms*:

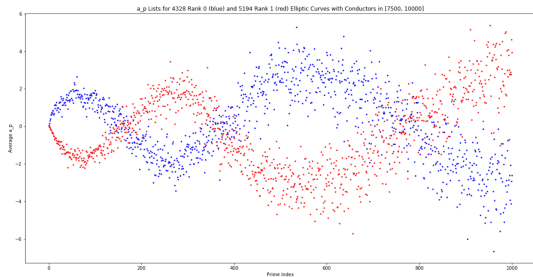
Eratosthenes, to take an example—and other ancient Greek mathematicians—might have imagined that all they needed were a few powerful insights and then everything about numbers would be as plain, say, as facts about triangles in the setting of Euclid's Elements of Geometry.

⋮

Sometimes, but not that often, in number theory we get a complete answer to a question we have posed, an answer that finishes the problem off. Often something else happens: we manage to find a fine, simple, good approximation to the data or phenomena that interests us—perhaps after some major effort—and then we discover that yet deeper questions lie hidden in the error term, i.e., in the measure of how badly our approximation misses its mark.

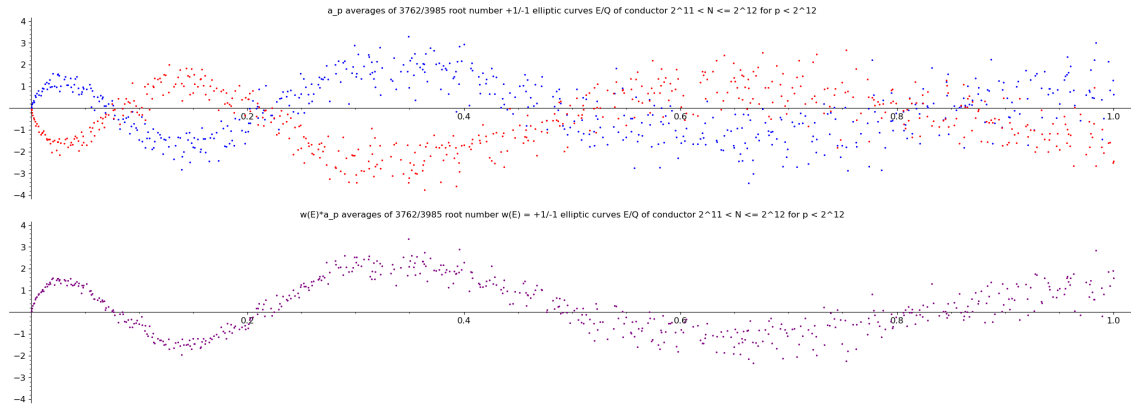
Murmurations of elliptic curves

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

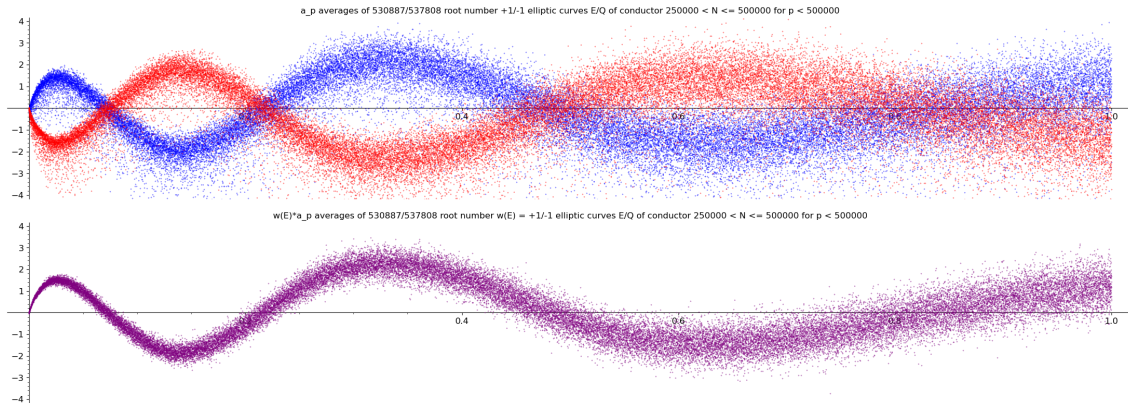
Elliptic curve L -functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \dots, 2^{17}, 250000$. The x -axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or $m_p := \varepsilon(E)a_p(E)$ over even/odd or all $E/\mathbb{Q}$ with $N(E) \in (M, 2M]$.³



³Letter to Sarnak, response from Sarnak.

Murmurations of elliptic curves

Elliptic curve L -functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \dots, 2^{17}, 250000$. 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 $m_p := \varepsilon(E)a_p(E)$ over even/odd or all $E/\mathbb{Q}$ with $N(E) \in (M, 2M]$.³

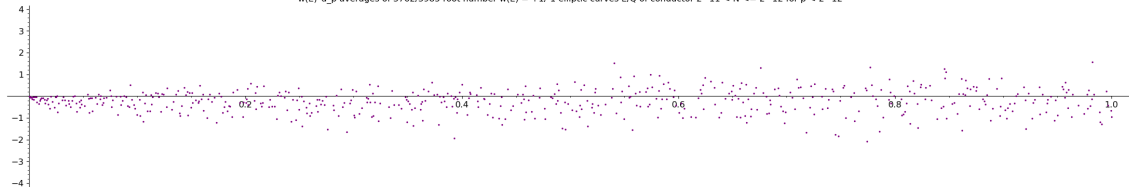


³Letter to Sarnak, response from Sarnak.

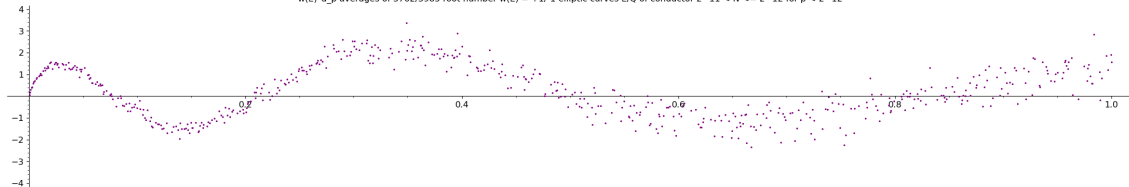
Bias cancellation

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

$w(E) \cdot a_p$ averages of 3762/3985 root number $w(E) = +1/-1$ elliptic curves $E/\mathbb{Q}$ of conductor $2^{11} < N \leq 2^{12}$ for $p < 2^{12}$



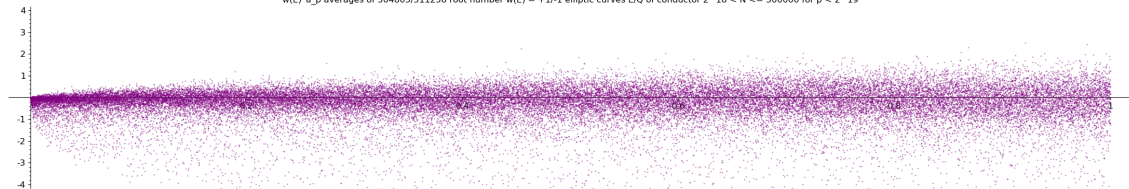
$w(E) \cdot a_p$ averages of 3762/3985 root number $w(E) = +1/-1$ elliptic curves $E/\mathbb{Q}$ of conductor $2^{11} < N \leq 2^{12}$ for $p < 2^{12}$



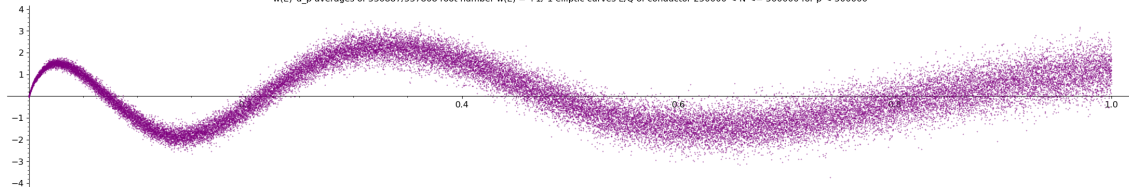
Bias cancellation

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

$w(E) \cdot a_p$ averages of 504805/511258 root number $w(E) = +1/-1$ elliptic curves E/Q of conductor $2^{18} < N \leq 500000$ for $p < 2^{19}$



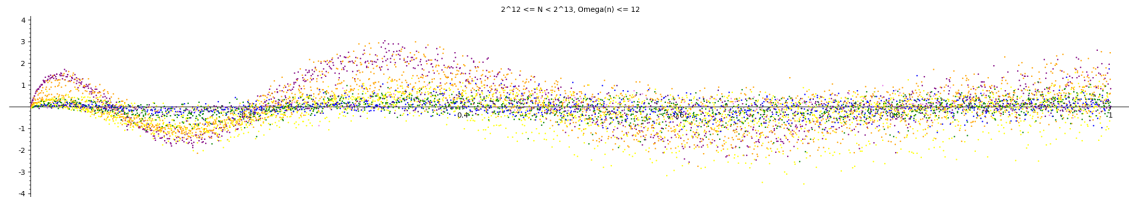
$w(E) \cdot a_p$ averages of 530887/537808 root number $w(E) = +1/-1$ elliptic curves E/Q of conductor $250000 < N \leq 500000$ for $p < 500000$



Murmurations of elliptic curves over a_n (not just a_p)

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

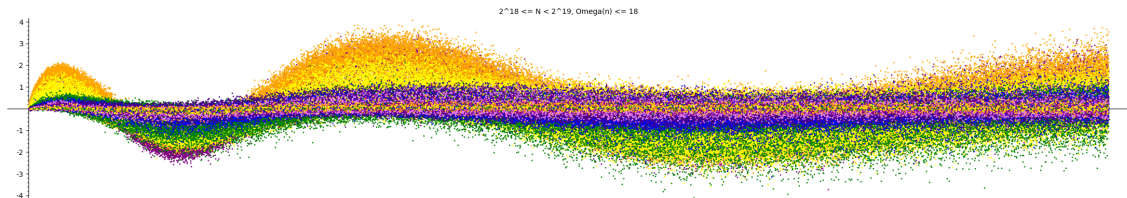
The color of the dot indicates the number of prime factors of n (with multiplicity).



Murmurations of elliptic curves over a_n (not just a_p)

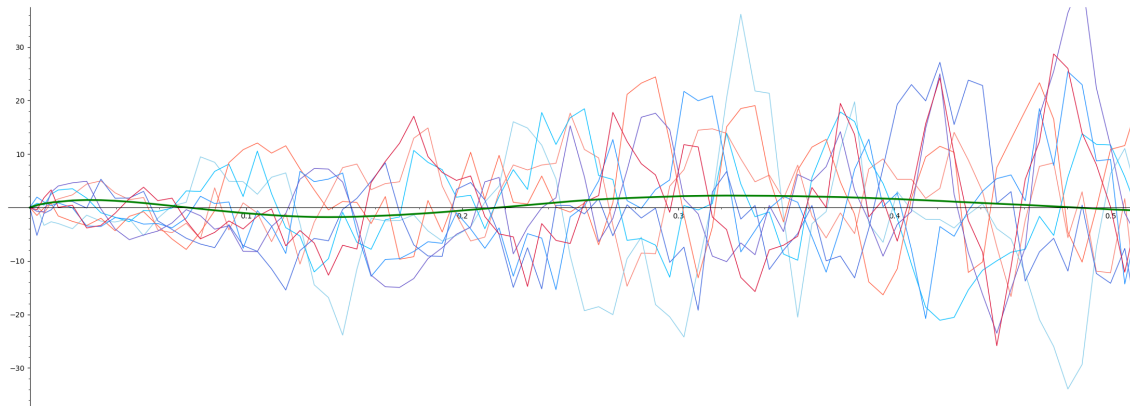
Elliptic curve L -functions of conductor $N \in (M, 2M]$ for $M = 2^{12}, \dots, 2^{17}, 250000$. The x -axis range is $[0, 2M]$. Dots at $(n, \bar{m}_n)$ show the average of $m_n := \varepsilon(E)a_n(E)$ over all $E/\mathbb{Q}$ with $N(E) \in (M, 2M]$.

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



Murmurations are an aggregate phenomenon

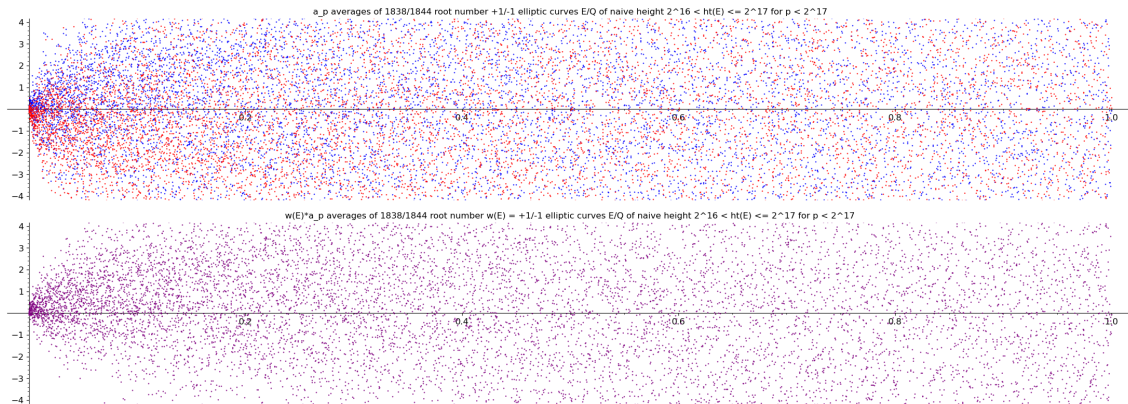
Moving average line plots of $\bar{m}_p$ for 8 individual and all $E/\mathbb{Q}$ with $N(E) \in (M, 2M]$, using subintervals of size $\sqrt{M}$ for $p \leq 2M$, with $M = 2^{17}$.



147455.b2, 163839.a1, 180222.be2, 196606.b1, 212990.11, 229374.a1, 245758.a1, 262143.d1

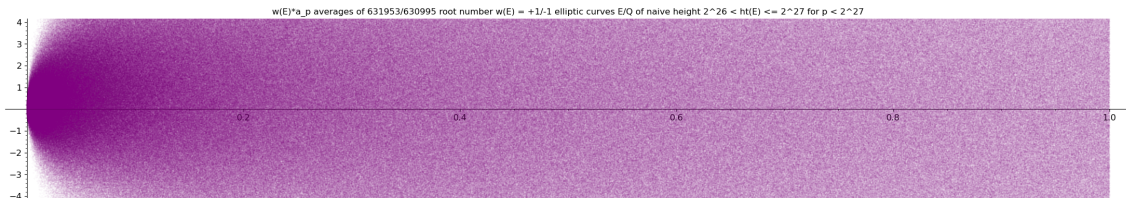
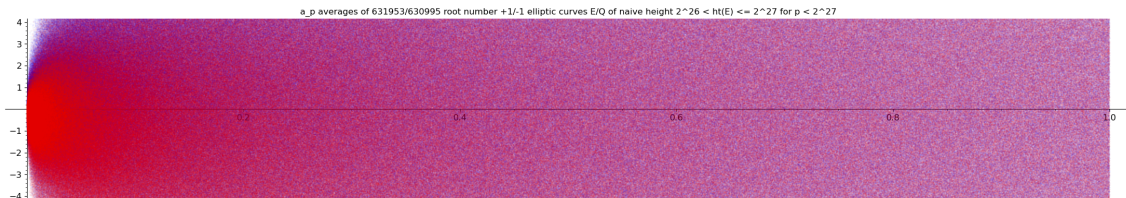
Ordering by (naive) height

Elliptic curves with $\text{ht}(E) := \max(4|A|^3, 27B^2)$ in $(M, 2M]$ for $M = 2^{16}, \dots, 2^{26}$. 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 (naive) height

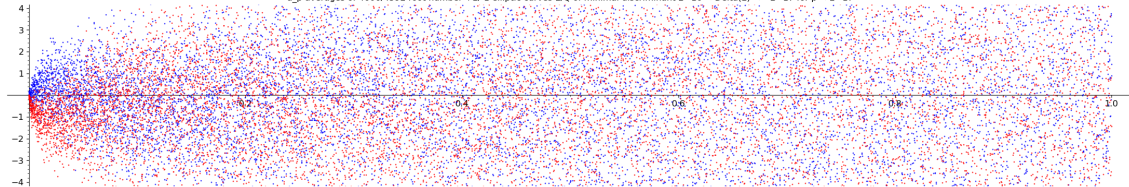
Elliptic curves with $\text{ht}(E) := \max(4|A|^3, 27B^2)$ in $(M, 2M]$ for $M = 2^{16}, \dots, 2^{26}$. The x-axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or m_p over even/odd or all $E/\mathbb{Q}$ with $N(E) \in (M, 2M]$.



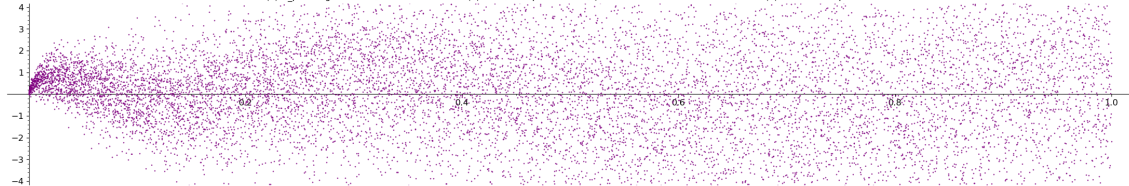
Ordering by absolute minimal discriminant

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

a_p averages of 4606/4592 root number +1/-1 elliptic curves $E/\mathbb{Q}$ of minimal discriminant $2^{16} < \Delta(E) \leq 2^{17}$ for $p < 2^{17}$



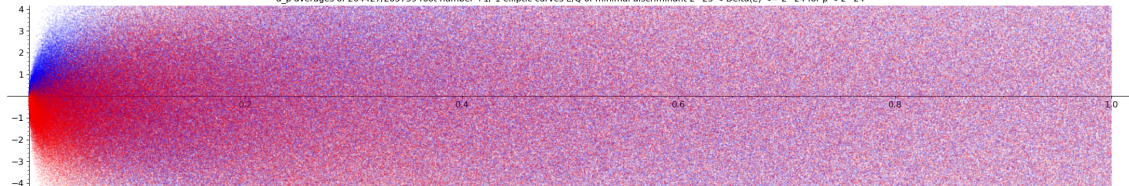
$w(E) \cdot a_p$ averages of 4606/4592 root number $w(E) = +1/-1$ elliptic curves $E/\mathbb{Q}$ of minimal discriminant $2^{16} < \Delta(E) \leq 2^{17}$ for $p < 2^{17}$



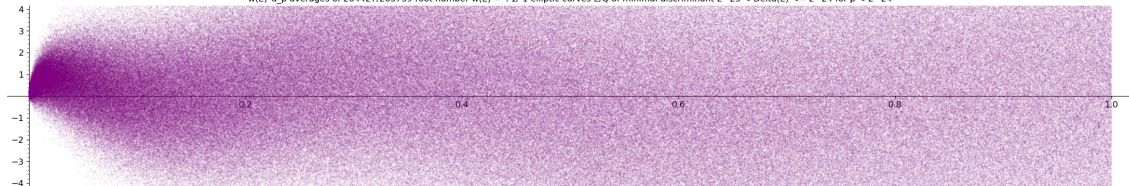
Ordering by absolute minimal discriminant

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

a_p averages of 264427/265739 root number +1/-1 elliptic curves $E/\mathbb{Q}$ of minimal discriminant $2^{23} < \Delta(E) \leq 2^{24}$ for $p < 2^{24}$



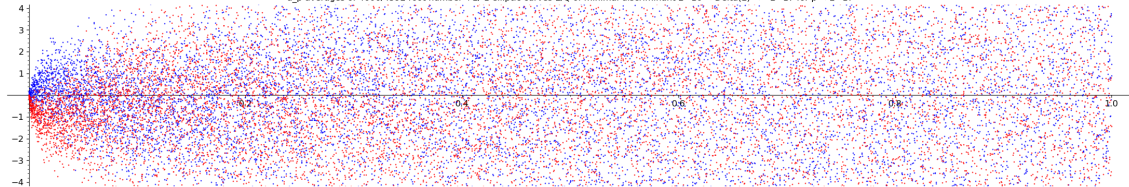
$w(E) \cdot a_p$ averages of 264427/265739 root number $w(E) = +1/-1$ elliptic curves $E/\mathbb{Q}$ of minimal discriminant $2^{23} < \Delta(E) \leq 2^{24}$ for $p < 2^{24}$



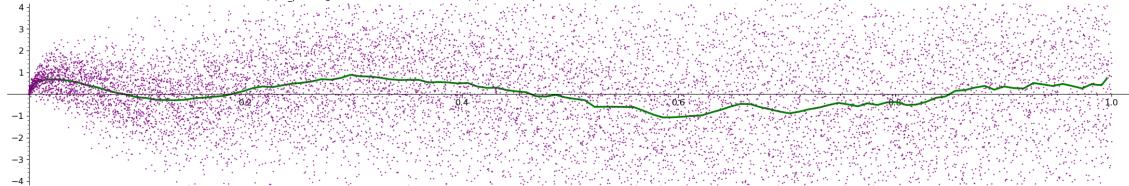
Ordering by absolute minimal discriminant

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

a_p averages of 4606/4592 root number $+1/-1$ elliptic curves $E/\mathbb{Q}$ of minimal discriminant $2^{16} < \Delta(E) \leq 2^{17}$ for $p < 2^{17}$



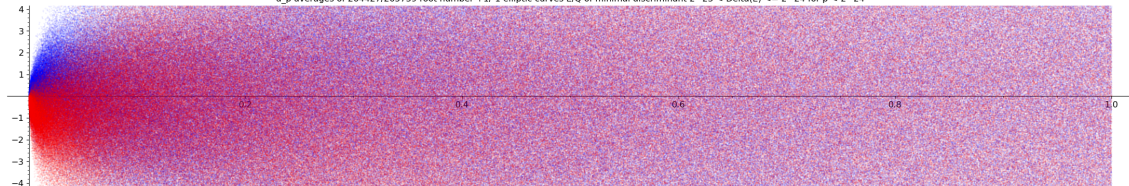
$w(E) \cdot a_p$ averages of 4606/4592 root number $w(E) = +1/-1$ elliptic curves $E/\mathbb{Q}$ of minimal discriminant $2^{16} < \Delta(E) \leq 2^{17}$ for $p < 2^{17}$



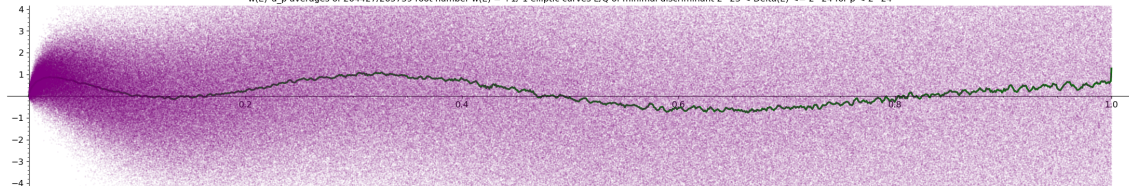
Ordering by absolute minimal discriminant

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

a_p averages of 264427/265739 root number +1/-1 elliptic curves $E/\mathbb{Q}$ of minimal discriminant $2^{23} < \Delta(E) \leq 2^{24}$ for $p < 2^{24}$

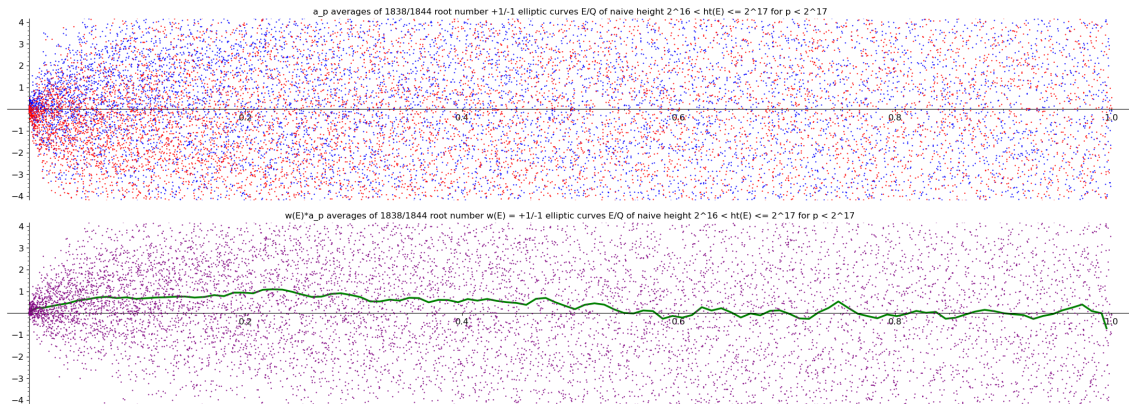


$w(E) \cdot a_p$ averages of 264427/265739 root number $w(E) = +1/-1$ elliptic curves $E/\mathbb{Q}$ of minimal discriminant $2^{23} < \Delta(E) \leq 2^{24}$ for $p < 2^{24}$



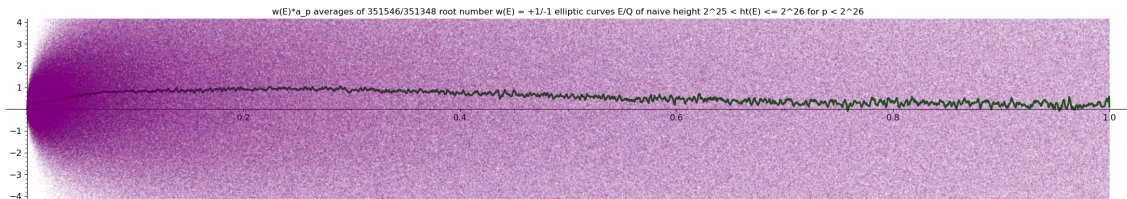
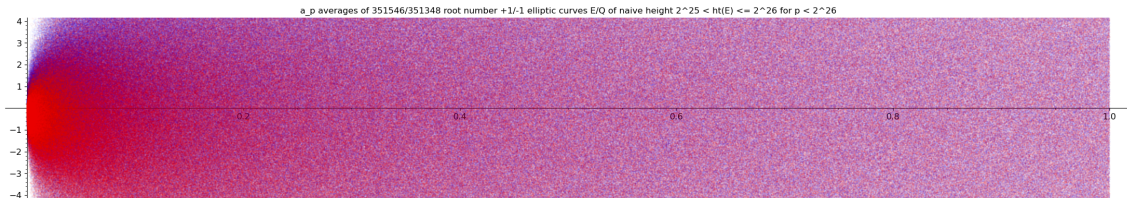
Ordering by height (redux)

Elliptic curves with $\text{ht}(E) := \max(4|A|^3, 27B^2)$ 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 $N(E) \in (M, 2M]$.



Ordering by height (redux)

Elliptic curves with $\text{ht}(E) := \max(4|A|^3, 27B^2)$ 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 $N(E) \in (M, 2M]$.



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 $x = 0, \frac{1}{n}, \frac{2}{n}, \dots, \frac{n-1}{n}$. For each L -function in our family we compute a_p for all primes $p \leq N$, and then for $x = 0, \frac{1}{n}, \dots, \frac{n-1}{n}$ we compute the average $\alpha_x(E)$ of $a_p(E)$ for

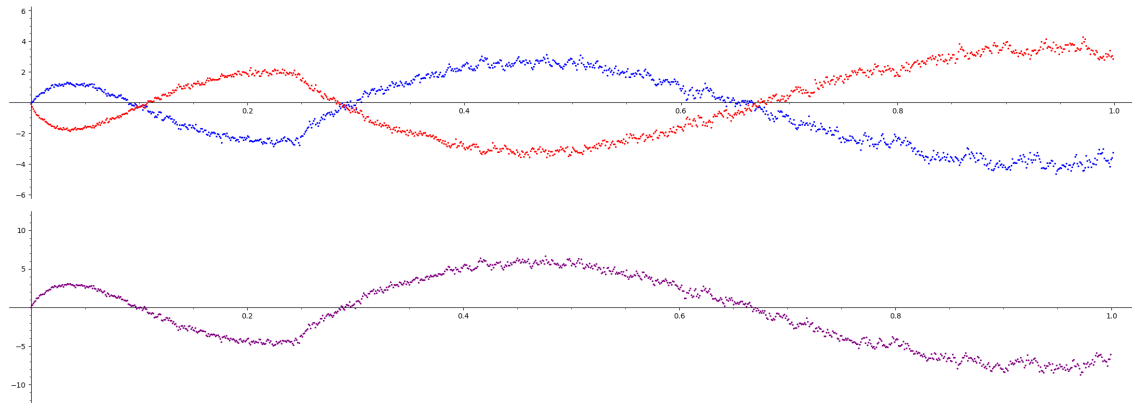
$$\frac{p}{N} \in \left(x, x + \frac{1}{n}\right],$$

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 $X \rightarrow \infty$.

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

Local averaging: elliptic curves ordered by conductor

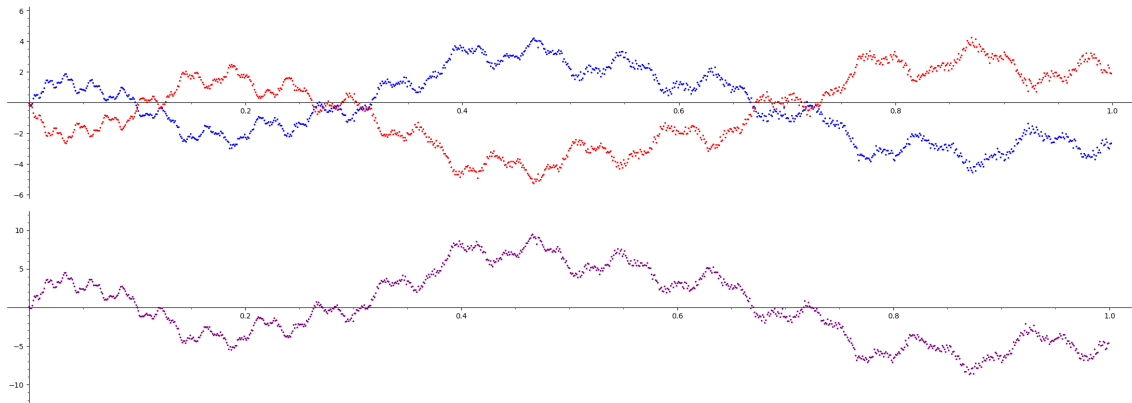
Elliptic curve L -functions of conductor $N \leq M$ for $M = 2^{12}, 2^{13}, \dots, 2^{17}, 2^{18}$. The x -axis range is $[0, 1]$. A blue/red (or purple) dot at $(x, \bar{\alpha}_x)$ shows the average $\bar{\alpha}_x$ of $\alpha_x(E)$ (or $\varepsilon(E)\alpha_x(E)$) over even/odd rank (or all) $E/\mathbb{Q}$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



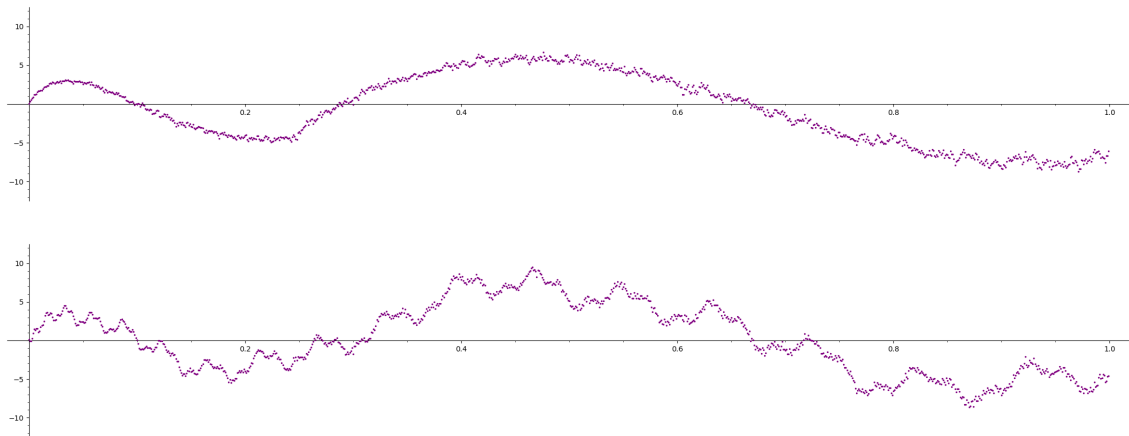
Local averaging: elliptic curves ordered by height

Elliptic curves with $\text{ht}(E) := \max(4|A|^3, 27B^2) \leq M$ for $M = 2^{18}, \dots, 2^{27}$.

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 $\varepsilon(E)\alpha_x(E)$) over even/odd rank (or all) $E/\mathbb{Q}$ with $\text{ht}(E) \leq M$.



Local averaging: elliptic curves ordered by conductor vs height



Arithmetic L -functions

We call an L -function **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 $L_{\text{an}}(s) = \sum a_n n^{-s}$ 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** $L(s) := L_{\text{an}}(s + \omega/2)$ has coefficients in $\mathcal{O}_K$ and satisfies

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

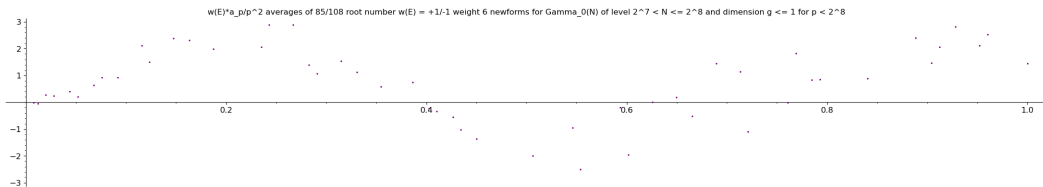
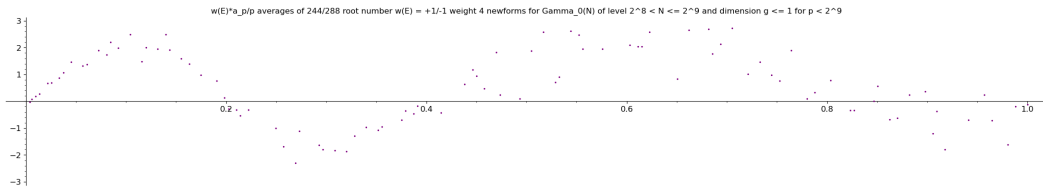
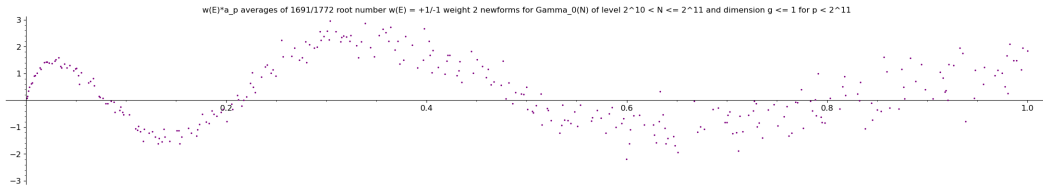
L -functions of abelian varieties have motivic weight $\omega = 1$.

L -functions of weight- k holomorphic cusp forms have motivic weight $\omega = k - 1$.

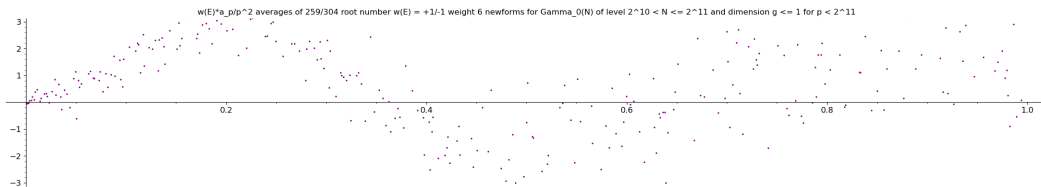
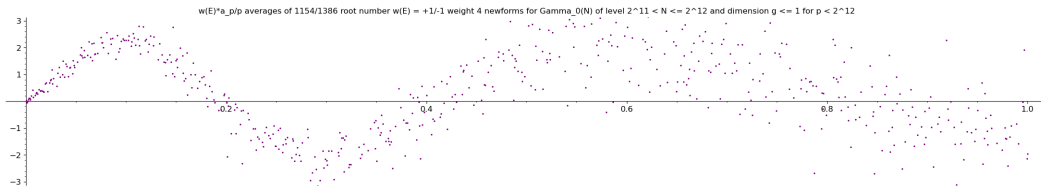
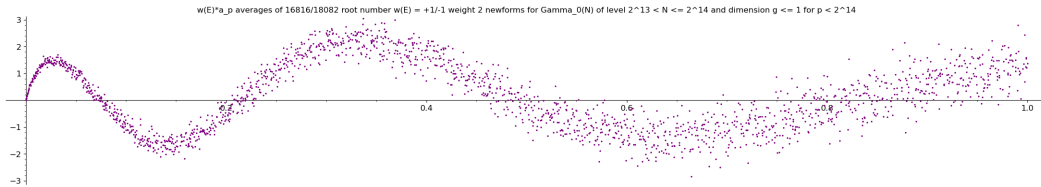
We consider **Galois-closed** families of **self-dual** arithmetically normalized L -functions. In any such family the values of a_p and m_p are integers and $w = \pm 1$.

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.

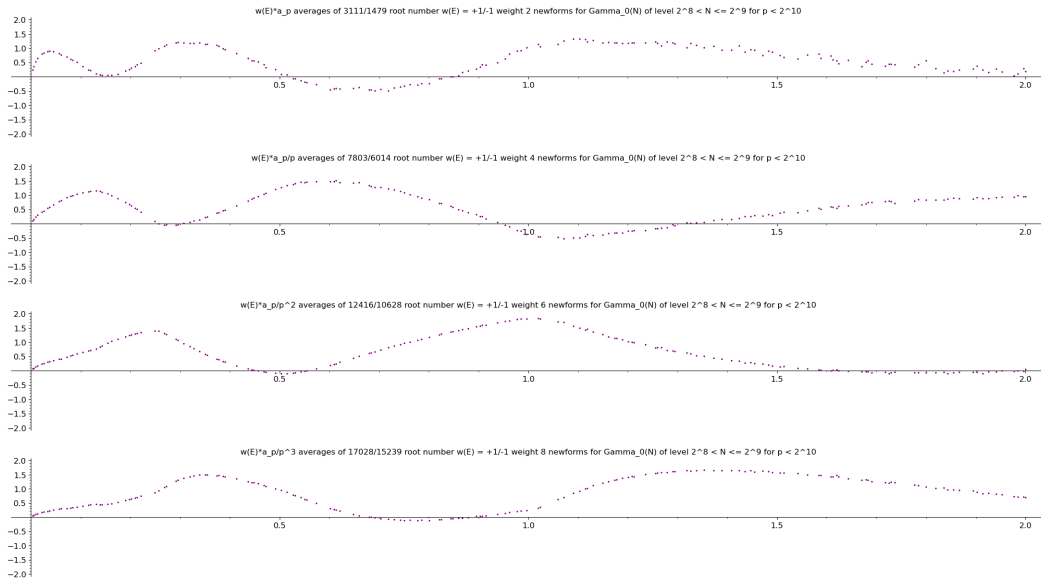
Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6$ with rational coefficients.



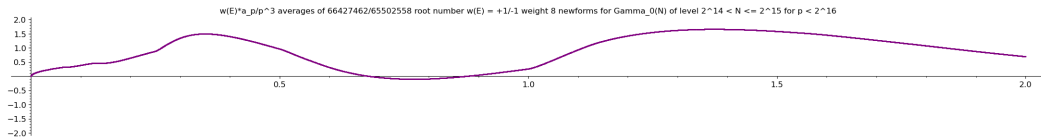
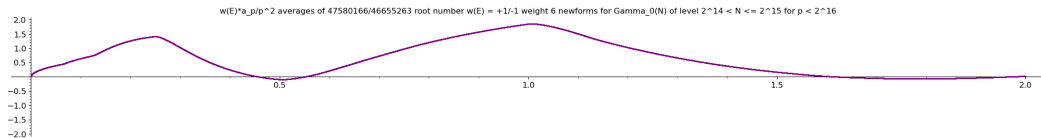
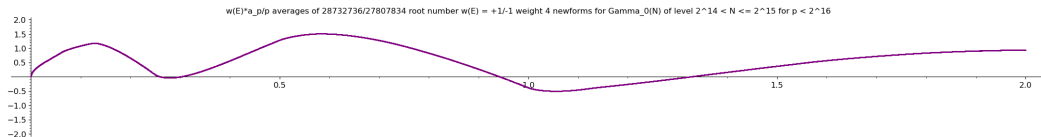
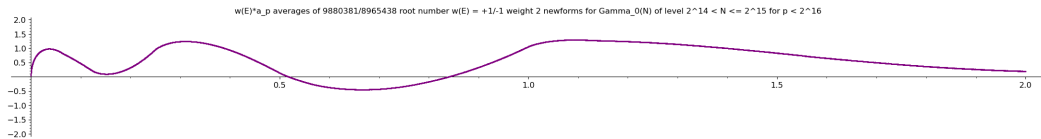
Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6$ with rational coefficients.



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

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

$$M_k(y) := D_k \left(Ay - (-1)^{k/2} B \sum_{1 \leq r \leq 2y} c(r) \sqrt{4y^2 - r^2} U_{k-2}\left(\frac{r}{2y}\right) - \pi y^2 \delta_{k=2} \right),$$

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

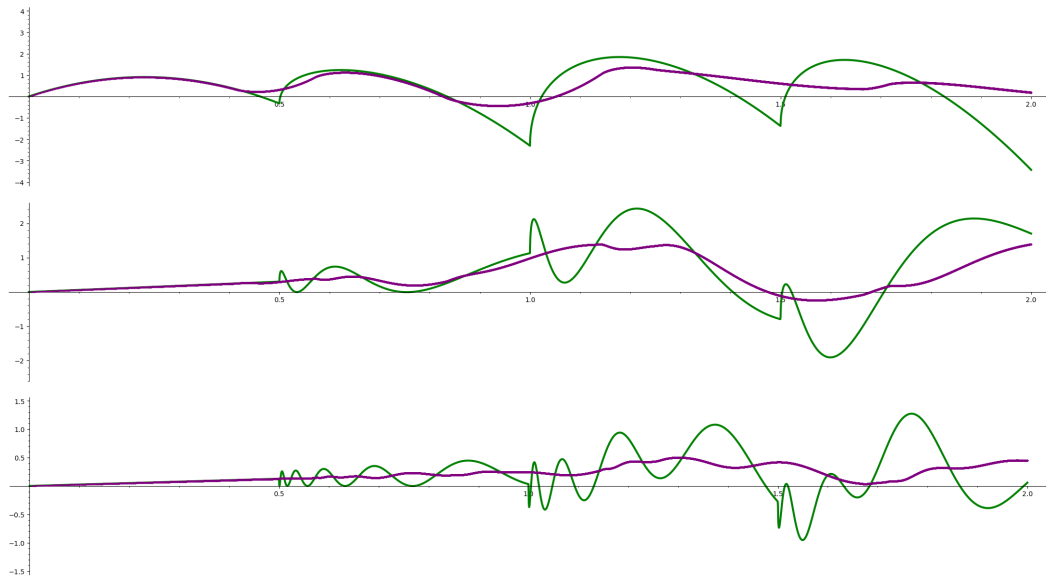
Theorem [Zubrilina 2023]. Let $\sum a_n(f)q^n$ denote a weight- k newform for $\Gamma_0(N)$ with root number $w(f)$. Let $X, Y, P \rightarrow \infty$ with P prime, $Y \sim X^{1-\delta}$, $P \ll X^{1+\delta_1}$, $\delta, \delta_1 > 0$ and $2\delta_1 < \delta < 1$, and put $y := \sqrt{P/X}$. Then for every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

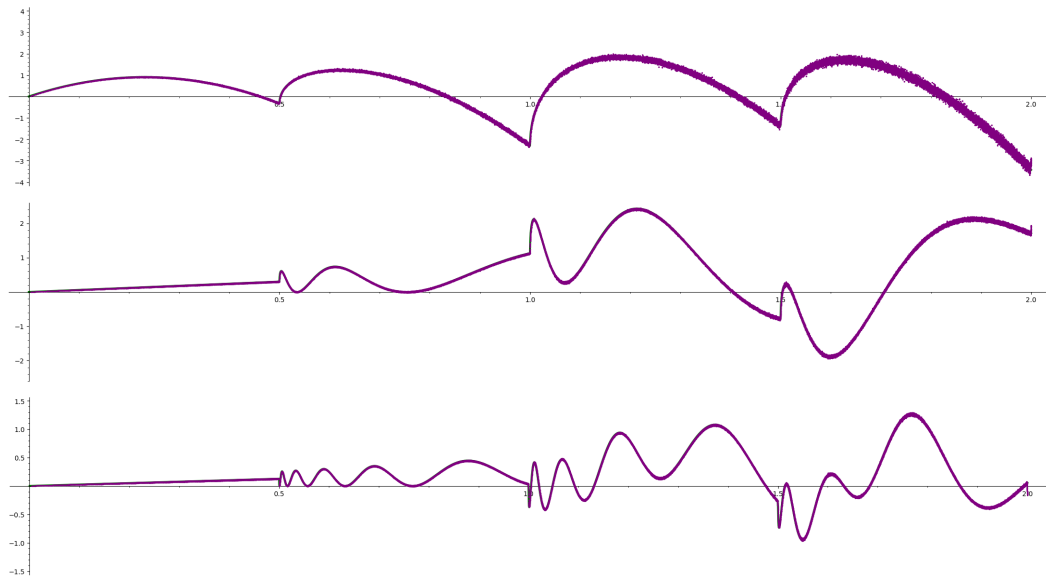
Zubrilina's theorem for $k = 2, 14, 32$

([click here for other \$k\$](#))



Zubrilina's theorem for $k = 2, 14, 32$

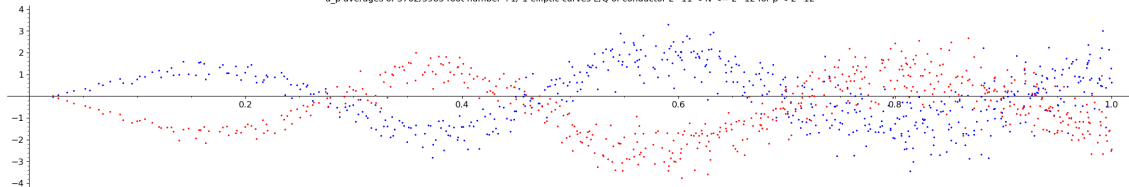
([click here for other \$k\$](#))



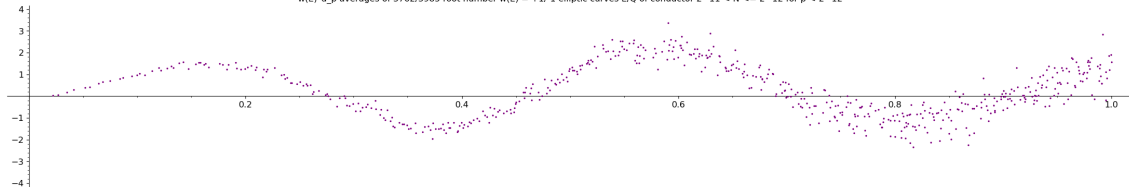
Murmurations of elliptic curves with square root normalization

Elliptic curve L -functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \dots, 2^{17}, 250000$. 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 $m_p := \varepsilon(E)a_p(E)$ over even/odd or all $E/\mathbb{Q}$ with $N(E) \in (M, 2M]$.

a_p averages of 3762/3985 root number $+1/-1$ elliptic curves $E/\mathbb{Q}$ of conductor $2^{11} < N \leq 2^{12}$ for $p < 2^{12}$



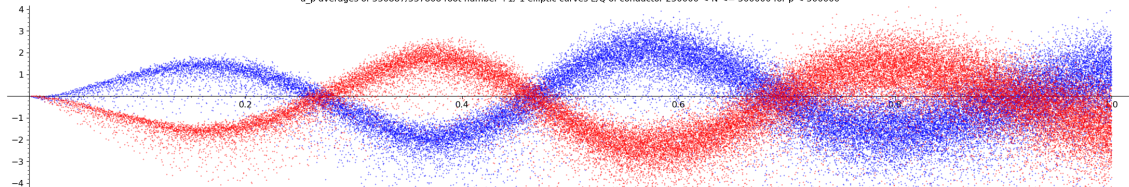
$w(E)a_p$ averages of 3762/3985 root number $w(E) = +1/-1$ elliptic curves $E/\mathbb{Q}$ of conductor $2^{11} < N \leq 2^{12}$ for $p < 2^{12}$



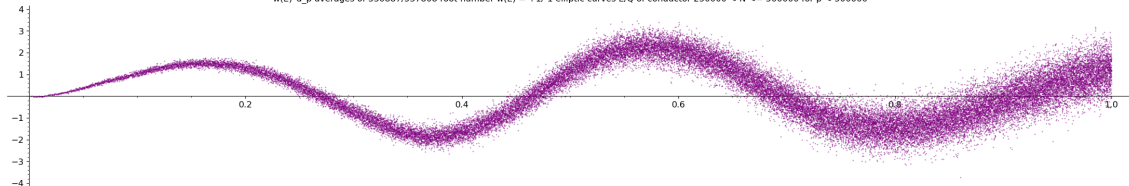
Murmurations of elliptic curves with square root normalization

Elliptic curve L -functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \dots, 2^{17}, 250000$. 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 $m_p := \varepsilon(E)a_p(E)$ over even/odd or all $E/\mathbb{Q}$ with $N(E) \in (M, 2M]$.

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



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



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 $W: \mathbb{R}_{>0} \rightarrow \mathbb{R}$ with compact support, the limit

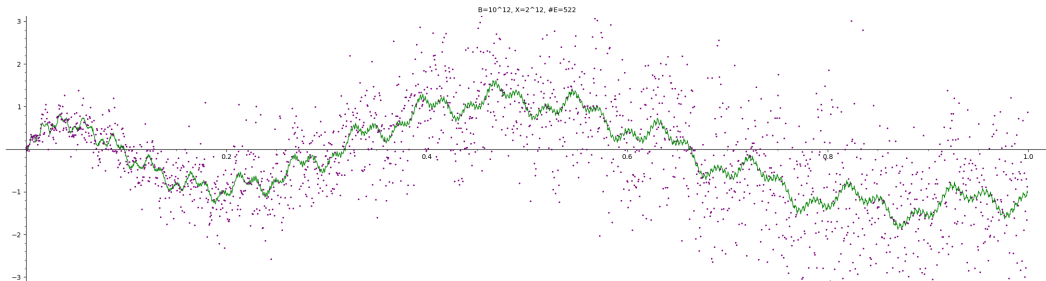
$$\lim_{X \rightarrow \infty} \frac{1}{\#\mathcal{E}(X)} \sum_{E \in \mathcal{E}(X)} \frac{1}{N(E)} \sum_{n \geq 1} W\left(\frac{n}{N(E)}\right) \varepsilon(E) a_n(E)$$

exists and is equal to

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

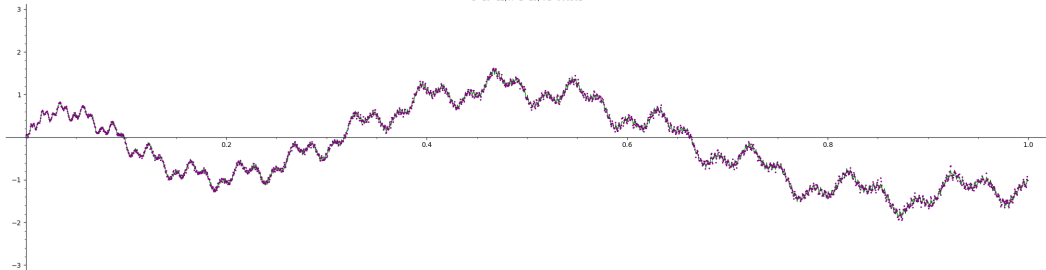
with $\ell_{2,\nu} = \frac{t_2(\nu+2)}{1023}$, $\ell_{3,\nu} = \dots$, $\ell_{p,\nu} = \frac{p^9 - p^8}{p^{10} - 1} t_p(\nu + 2)$, where $t_p(k) = \text{tr}(T_p)$ on $S_k(1)$.

A murmuration theorem for elliptic curves



A murmuration theorem for elliptic curves

$B=10^{12}$, $X=2^{25}$, $\#E=906302$



The Voronoi summation formula

Lemma (Kowalski-Michel-VanderKam 2002,
Blomer-Fouvry-Kowalski-Michel-Milićević-Sawin 2023, Sawin-S 2025)

Let $E/\mathbb{Q}$ be an elliptic curve. Fix $a, q \in \mathbb{Z}_{>0}$ with $\gcd(aN(E), q) = 1$, and let $\overline{aN(E)}$ be the inverse of $aN(E) \bmod q$. For any smooth $W: \mathbb{R}_{>0} \rightarrow \mathbb{R}$ with compact support we have

$$\begin{aligned} & \frac{\varepsilon(E)}{N(E)} \sum_{n=1}^{\infty} a_n(E) \sqrt{\frac{n}{N(E)}} W\left(\frac{n}{N(E)}\right) e^{2\pi i a n / q} \\ &= \frac{1}{q} \sum_{n=1}^{\infty} \frac{a_n(E)}{\sqrt{n}} e^{2\pi i \overline{aN(E)} n / q} \int_0^{\infty} 2\pi \sqrt{u} W(u) J_1\left(4\pi \frac{\sqrt{un}}{q}\right) du. \end{aligned}$$

Proof strategy

The Voronoi summation formula can be shown to imply

$$\frac{1}{N(E)} \sum_{n=1}^{\infty} W\left(\frac{n}{N(E)}\right) \varepsilon(E) a_n(E) = \sum_{n=1}^{\infty} \frac{a_n(E)}{\sqrt{n}} \int_0^{\infty} 2\pi\sqrt{u} W(u) J_1(4\pi\sqrt{un}) du. \quad (2)$$

Noting that $a_n(E) = \prod_{p|n} a_{p^{v_p(n)}}(E_{A,B})$ and each $a_{p^{v_p(n)}}(E_{A,B})$ is a p -adically continuous function of A, B , one can show

$$\lim_{X \rightarrow \infty} \mathbb{E}_{\{E \in \mathcal{E}(X)\}} [a_n(E)] = \int_{\prod_p \mathbb{Z}_p^2 \setminus (p^4 \mathbb{Z}_p \times p^6 \mathbb{Z}_p)} \prod_{p|n} a_{p^{v_p(n)}}(E) = \prod_{p|n} \ell_{p, v_p(n)}, \quad (3)$$

Taking limits on both sides of (2), proving absolute convergence, moving the limit on the RHS inside the sum, and applying (3) yields the theorem.

Refinements

Conjecture (Sawin-S 2025)

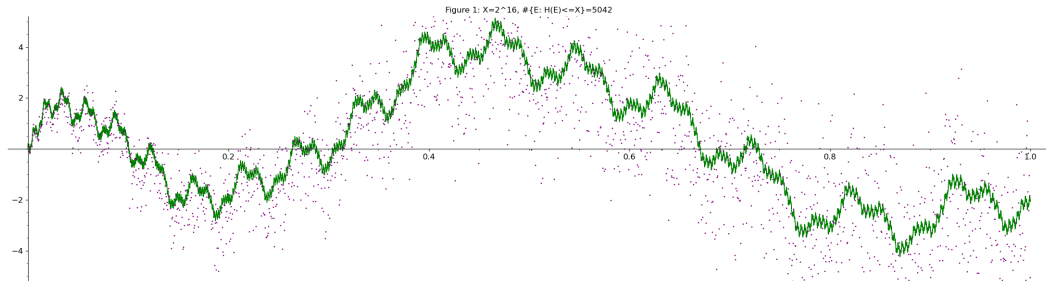
For all real numbers $0 < C_1 < C_2$ we have

$$\lim_{X \rightarrow \infty} \mathbb{E}_{\{E \in \mathcal{E}(X)\}} \left[\frac{\log(N(E)^{\frac{C_1+C_2}{2}})}{N(E)} \sum_{\substack{p \in (C_1 N(E), C_2 N(E)] \\ p \text{ prime}}} \varepsilon(E) a_p(E) \right]$$

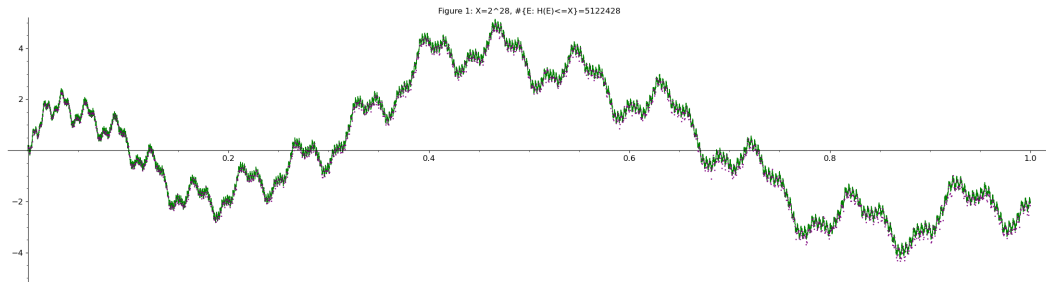
$$= \int_{C_1}^{C_2} 2\pi\sqrt{u} \sum_{\substack{q \in \mathbb{N} \\ \text{squarefree}}} \sum_{m \in \mathbb{N}} \frac{\mu(\gcd(m, q))}{qm\varphi\left(\frac{q}{\gcd(m, q)}\right)} J_1\left(4\pi\frac{\sqrt{um}}{q}\right) \prod_{p|q} \hat{\ell}_{p, 2\nu_p(m)} \prod_{p|m, p \nmid q} \ell_{p, 2\nu_p(m)} du.$$

where $\hat{\ell}_{p,0} = \frac{1-p^{-1}}{1-p^{-10}}$, $\hat{\ell}_{p,2} = \frac{-p-p^{-1}+p^{-2}+p^{-8}}{(1-p^{-10})(p-1)}$, $\hat{\ell}_{p,\nu} = -\frac{p^{-1}+p^{-2}}{1-p^{-10}}(p+1+t_p(\nu+2))$ for primes $p > 3$, and more complicated (but completely explicit) formulas for $p = 2, 3$.

Refinements (testing the conjecture)



Refinements (testing the conjecture)



Refinements

Theorem (Sawin-S 2025)

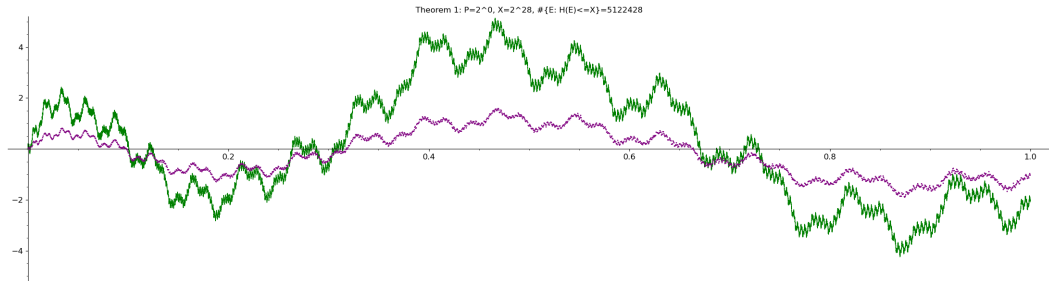
Let W be a smooth, compactly-supported function on $(0, \infty)$. The limit

$$\lim_{P \rightarrow \infty} \lim_{X \rightarrow \infty} \mathbb{E}_{\{E \in \mathcal{E}(X)\}} \left[\frac{\prod_{p \leq P} (1 - 1/p)^{-1}}{N(E)} \sum_{\substack{n \in \mathbb{N} \\ p \nmid n \text{ for } p \leq P}} W\left(\frac{n}{N(E)}\right) \varepsilon(E) a_n(E) \right]$$

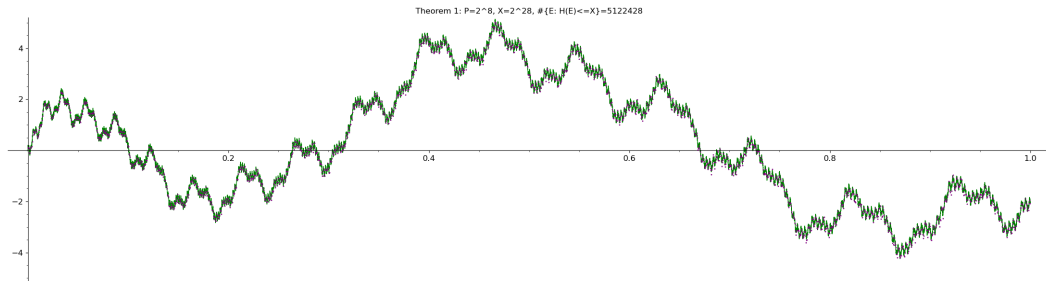
exists and is equal to

$$\int_0^\infty W(u) \sqrt{u} \left(2\pi \sum_{\substack{q \in \mathbb{N} \\ \text{squarefree}}} \sum_{m \in \mathbb{N}} \frac{\mu(\gcd(m, q))}{qm \varphi\left(\frac{q}{\gcd(m, q)}\right)} J_1\left(4\pi \frac{\sqrt{u}m}{q}\right) \prod_{p|q} \hat{\ell}_{p, 2v_p(m)} \prod_{p|m, p \nmid q} \ell_{p, 2v_p(m)} \right) du.$$

Refinements (illustrating the theorem)



Refinements (illustrating the theorem)



Ordering by (prime) conductor

Let $\mathcal{P}(X)$ be the set of isomorphism classes of $E/\mathbb{Q}$ of prime conductor $N(E) \leq X$.

Conjecture (Sawin-S 2025)

For all real $0 < C_1 < C_2$ we have

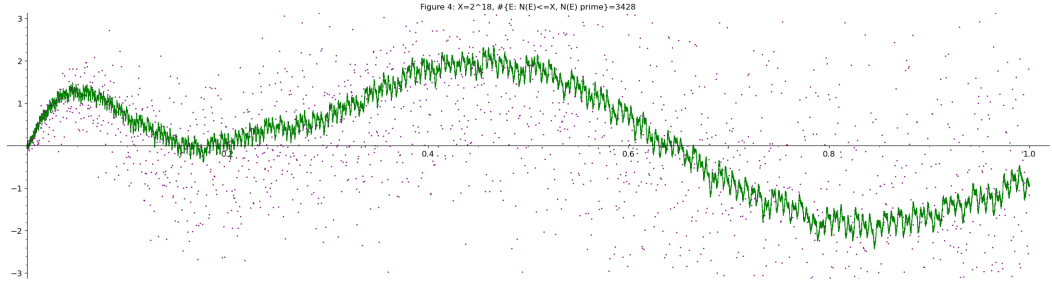
$$\lim_{X \rightarrow \infty} \mathbb{E}_{\{E \in \mathcal{P}(X)\}} \left[\frac{\log\left(N(E)^{\frac{C_1+C_2}{2}}\right)}{N(E)} \sum_{p \in (C_1 N(E), C_2 N(E)]} \varepsilon(E) a_p(E) \right]$$

exists and is equal to

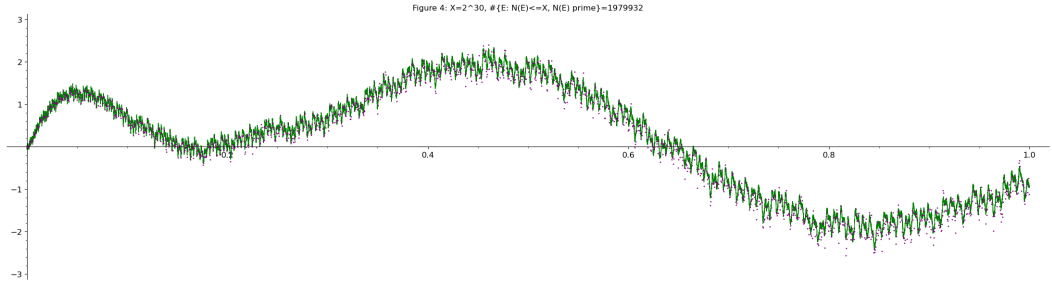
$$\int_{C_1}^{C_2} 2\pi\sqrt{u} \sum_{\substack{q \in \mathbb{N} \\ \text{squarefree}}} \sum_{m=1}^{\infty} \frac{\mu(\gcd(m, q))}{qm\varphi\left(\frac{q}{\gcd(m, q)}\right)} J_1\left(4\pi \frac{\sqrt{u}m}{q}\right) \prod_{p|m} \ell'_{p, 2\nu_p(m)} du.$$

with $\ell'_{p, \nu} = -p^{-1}(1 + t_p(\nu + 2))$, where $t_p(k) = \text{tr}(T_p)$ on $S_k(1)$.

Ordering by (prime) conductor (testing the conjecture)



Ordering by (prime) conductor (testing the conjecture)



Thank you!



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