

Murmurations: A computational perspective

Andrew V. Sutherland

Massachusetts Institute of Technology

December 1, 2023



Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation

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 $p|\Delta(E)$, 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 $\chi(p) = 0$ for $p|N(E)$ and $\chi(p) = 1$ otherwise and $N(E)|\Delta(E)$ is the **conductor**.

But in fact the a_p for $p \nmid \Delta(E)$ determine $L(E, s)$ (via strong multiplicity one), and also 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 $ST(E)$ ($= SU(2)$ if E does not have CM).
2. **Birch and Swinnerton-Dyer:**

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

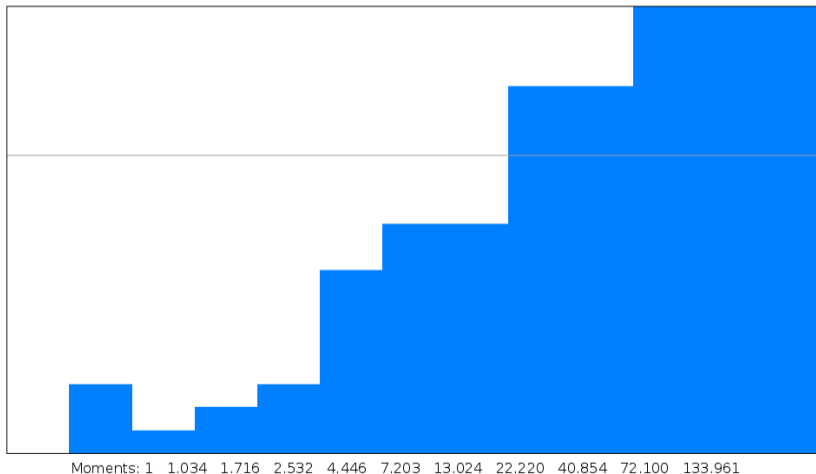
3. **Lang–Trotter:** For every nonzero $t \in \mathbb{Z}$ there is a real number $C_{E,t}$ for which

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

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

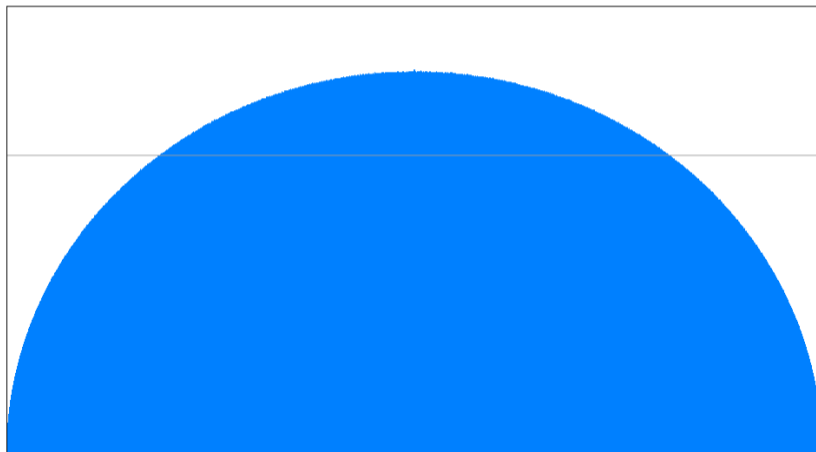
Example: Elkies' curve of rank ≥ 28 ($= 28$ under GRH).

a1 histogram of $y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429$ for $p \leq 2^{10}$
172 data points in 13 buckets, $z_1 = 0.023$, out of range data has area 0.250



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

a1 histogram of $y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429$ for $p \leq 2^{40}$
41203088796 data points in 202985 buckets



Moments: 1 0.000 1.000 0.000 2.000 0.000 5.000 0.001 14.000 0.003 42.000

How rank effects trace distributions

An early form of the BSD conjecture implies that

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

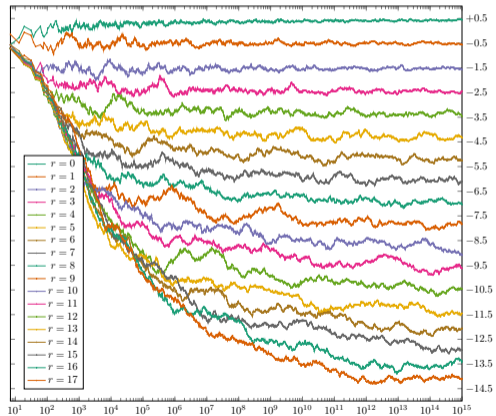
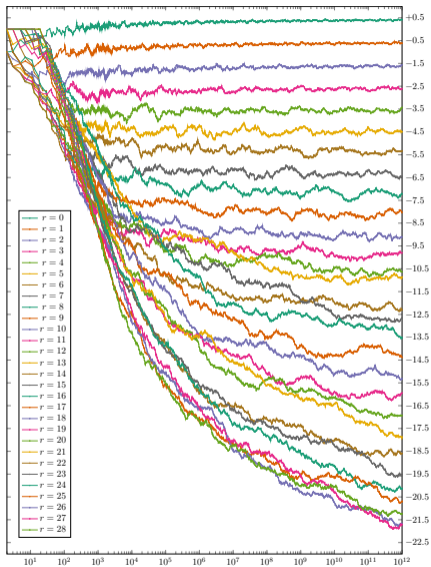
and sums of this form (Mestre-Nagao sums) are often used as a tool when searching for elliptic curves of large rank (which necessarily have large conductor N).^{1 2}

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.

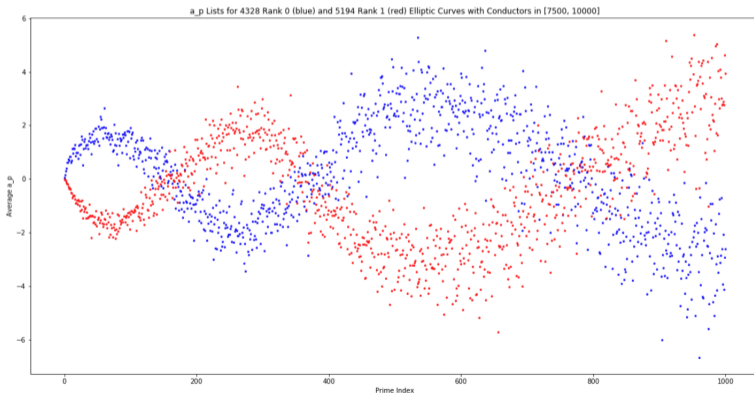
¹See [Sarnak's 2007 letter to Mazur](#).

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



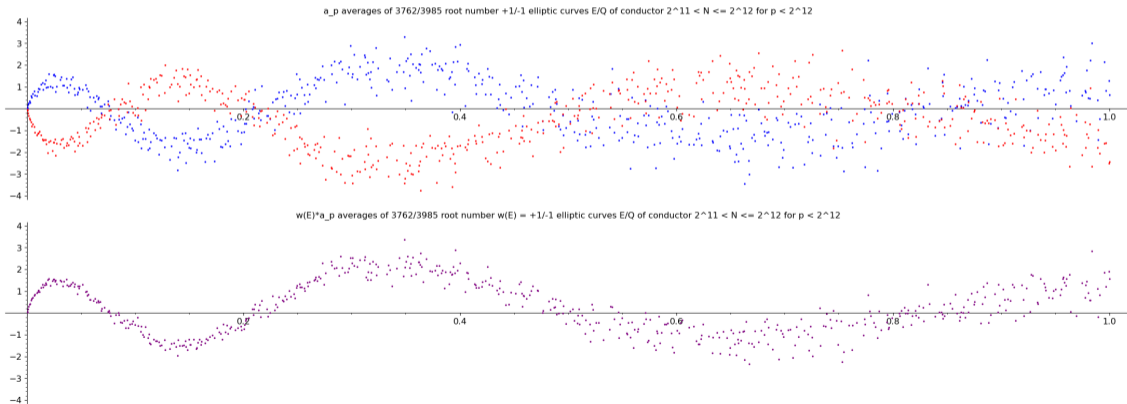
Murmurations of elliptic curves

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

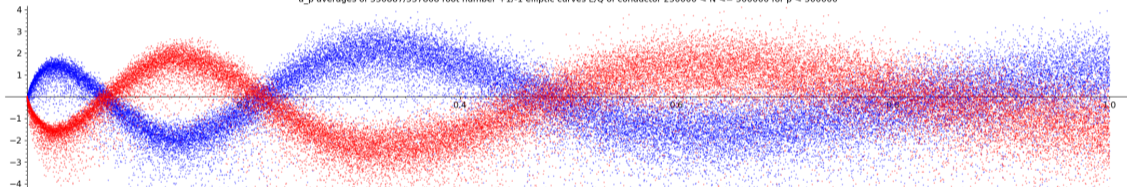
Elliptic curve L -functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \dots, 2^{17}, 250000$. The x -axis range is $[0, 2M]$. A blue/red or purple dot at $(p, \bar{a}_p$ or $\bar{m}_p)$ shows the average of a_p or $m_p := w(E)a_p(E)$ over even/odd or all E/\mathbb{Q} with $N_E \in (M, 2M]$.



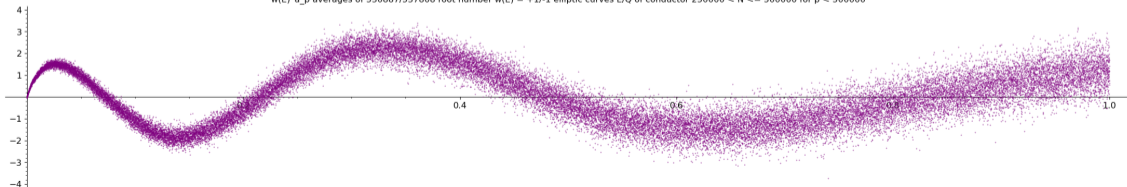
Murmurations of elliptic curves

Elliptic curve L -functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \dots, 2^{17}, 250000$. 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 $m_p := w(E)a_p(E)$ 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



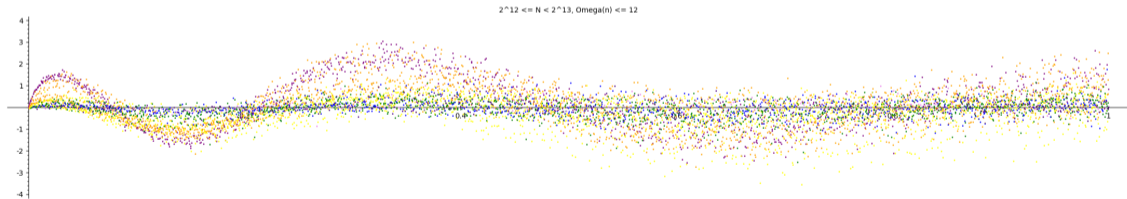
w(E)*a_p averages of 530887/537808 root number w(E) = +1/-1 elliptic curves E/Q of conductor 250000 < N <= 500000 for p < 500000



Murmurations of elliptic curves over a_n (not just a_p)

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 $[0, 2M]$. Dots at (n, \bar{m}_n) show the average of $m_n := w(E)a_n(E)$ over all E/\mathbb{Q} with $N_E \in (M, 2M]$.

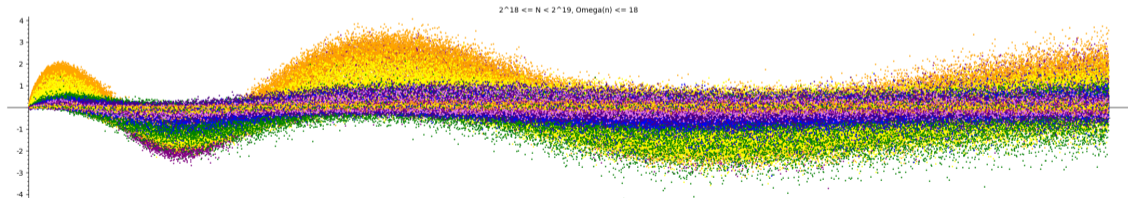
The color of the dot indicates the number of prime factors of n (with multiplicity).



Murmurations of elliptic curves over a_n (not just a_p)

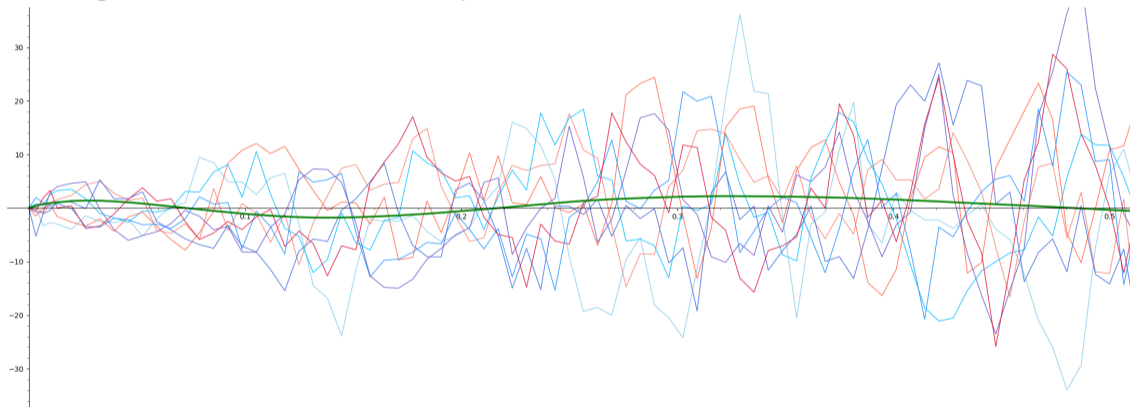
Elliptic curve L -functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \dots, 2^{17}, 250000$. The x -axis range is $[0, 2M]$. Dots at (n, \bar{m}_n) show the average of $m_n := w(E)a_n(E)$ over all E/\mathbb{Q} with $N_E \in (M, 2M]$.

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



Murmurations are an aggregate phenomenon

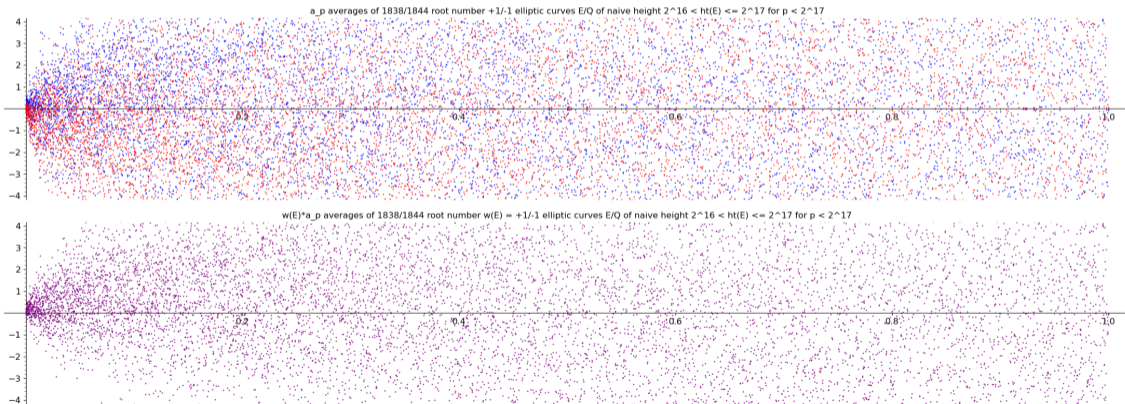
Moving average line plots of \bar{m}_p for 8 individual and all E/\mathbb{Q} with $N_E \in (M, 2M]$, using subintervals of size \sqrt{M} for $p \leq 2M$, with $M = 2^{17}$.



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

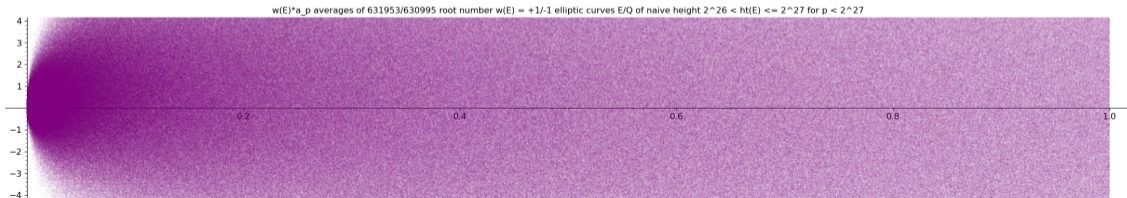
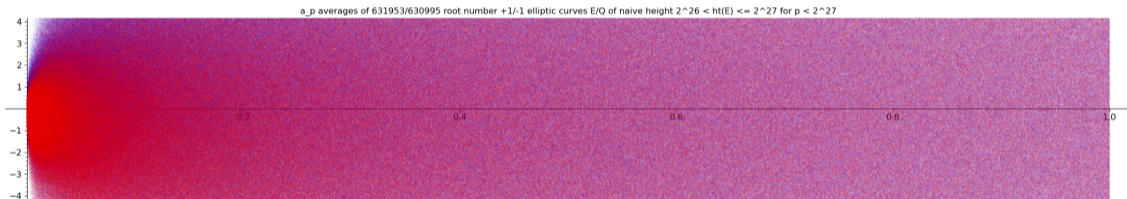
Murmurations depend critically on the conductor

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



Murmurations depend critically on the conductor

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

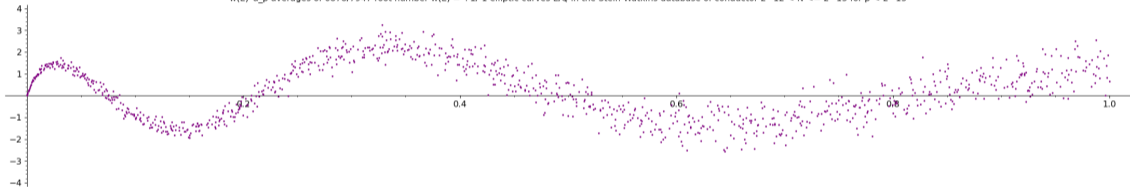


Murmurations scale

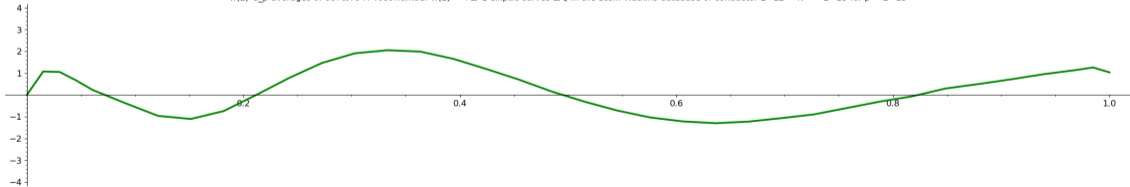
Elliptic curves in the SWDB of conductor $N \in (M, 2M]$ for $M = 2^{12}, \dots, 2^{25}$.

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

$w(E) \cdot a_p$ averages of 6878/7947 root number $w(E) = +1/-1$ elliptic curves E/\mathbb{Q} in the Stein-Watkins database of conductor $2^{12} < N \leq 2^{13}$ for $p < 2^{13}$



$w(E) \cdot a_p$ averages of 6878/7947 root number $w(E) = +1/-1$ elliptic curves E/\mathbb{Q} in the Stein-Watkins database of conductor $2^{12} < N \leq 2^{13}$ for $p < 2^{13}$

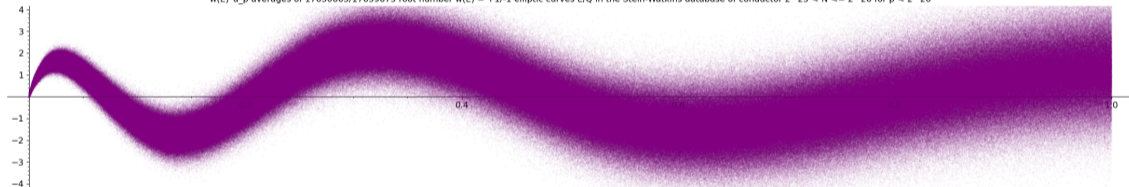


Murmurations scale

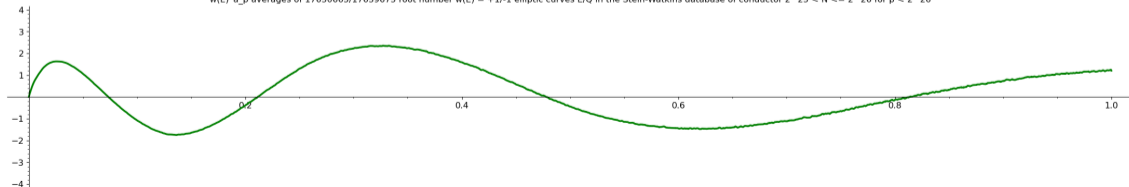
Elliptic curves in the SWDB of conductor $N \in (M, 2M]$ for $M = 2^{12}, \dots, 2^{25}$.

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

$w(E)*a_p$ averages of 17630665/17639675 root number $w(E) = +1/-1$ elliptic curves E/\mathbb{Q} in the Stein-Watkins database of conductor $2^{25} < N \leq 2^{26}$ for $p < 2^{26}$



$w(E)*a_p$ averages of 17630665/17639675 root number $w(E) = +1/-1$ elliptic curves E/\mathbb{Q} in the Stein-Watkins database of conductor $2^{25} < N \leq 2^{26}$ for $p < 2^{26}$



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 $L_{\text{an}}(s) = \sum a_n n^{-s}$ 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 $\omega = 1$.

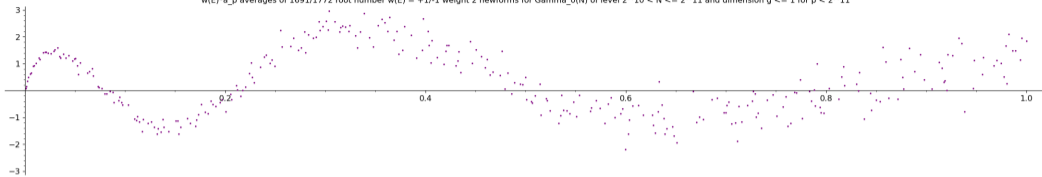
L -functions of weight- k holomorphic cuspforms have motivic weight $\omega = k - 1$.

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 $w = \pm 1$.

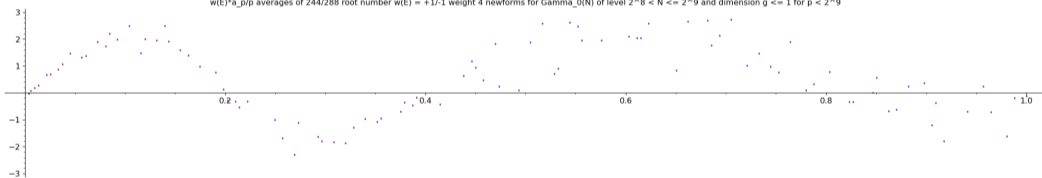
When averaging a_p 's in motivic weight $\omega > 1$ we **normalize** them via $a_p \mapsto a_p / p^{(\omega-1)/2}$. This ensures that we always have $|a_p| = O(\sqrt{p})$, as with elliptic curves.

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

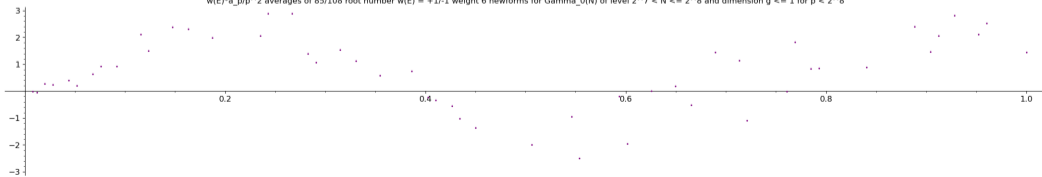
$w(E) \cdot a_p$ averages of 1691/1772 root number $w(E) = +1/-1$ weight 2 newforms for $\Gamma_0(N)$ of level $2^{10} < N \leq 2^{11}$ and dimension $g \leq 1$ for $p < 2^{11}$



$w(E) \cdot a_{p/p}$ averages of 244/288 root number $w(E) = +1/-1$ weight 4 newforms for $\Gamma_0(N)$ of level $2^8 < N \leq 2^9$ and dimension $g \leq 1$ for $p < 2^9$

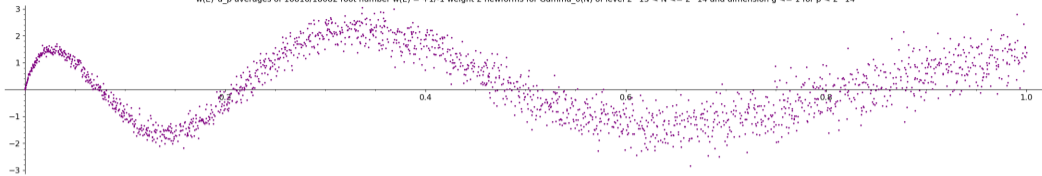


$w(E) \cdot a_{p/p^2}$ averages of 85/108 root number $w(E) = +1/-1$ weight 6 newforms for $\Gamma_0(N)$ of level $2^7 < N \leq 2^8$ and dimension $g \leq 1$ for $p < 2^8$

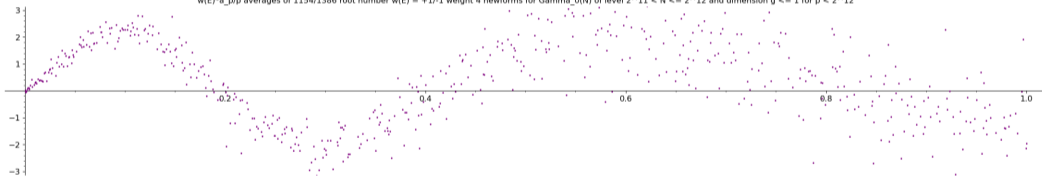


Newforms for $\Gamma_0(N)$ of weight $k = 2, 4, 6$ with rational coefficients.

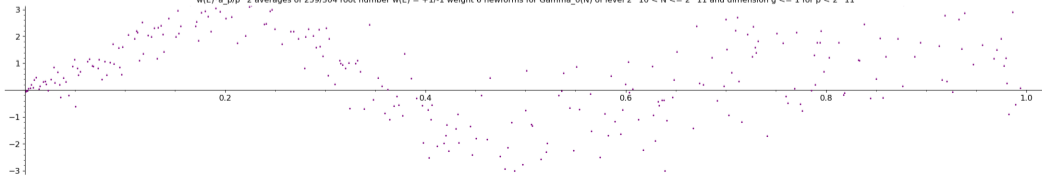
$w(E)^*a_p$ averages of 16816/18082 root number $w(E) = +1/-1$ weight 2 newforms for $\Gamma_0(N)$ of level $2^{13} < N \leq 2^{14}$ and dimension $g \leq 1$ for $p < 2^{14}$



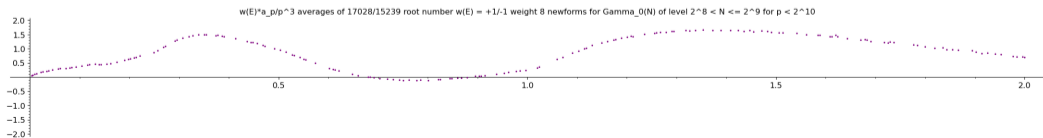
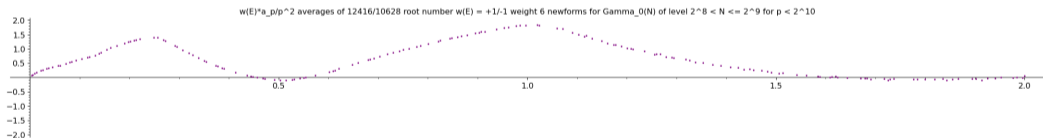
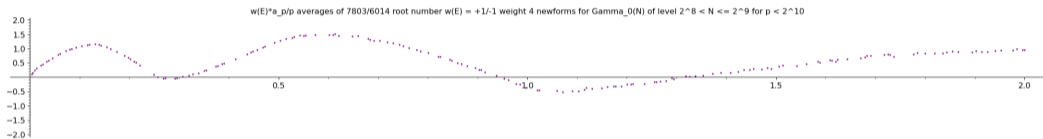
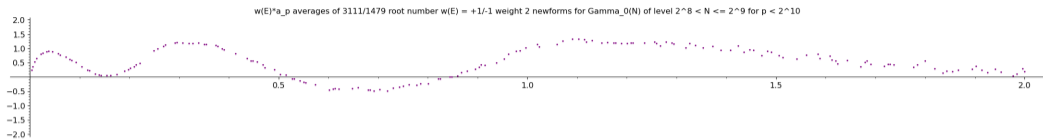
$w(E)^*a_p$ averages of 1154/1386 root number $w(E) = +1/-1$ weight 4 newforms for $\Gamma_0(N)$ of level $2^{11} < N \leq 2^{12}$ and dimension $g \leq 1$ for $p < 2^{12}$



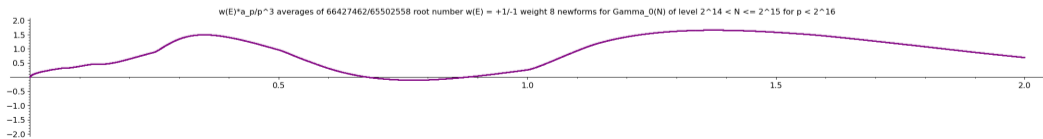
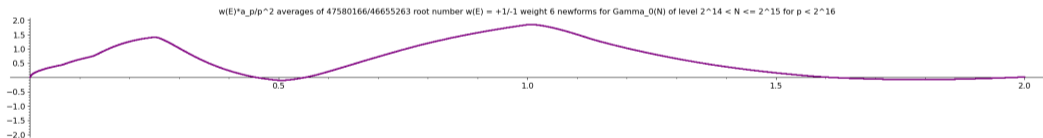
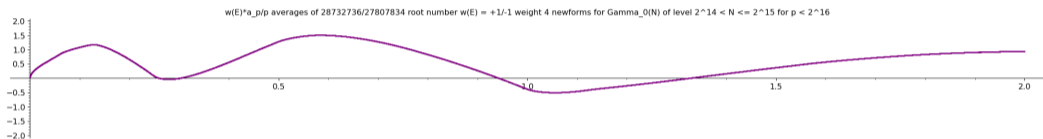
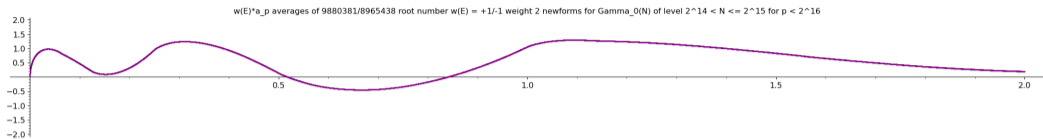
$w(E)^*a_p$ averages of 259/304 root number $w(E) = +1/-1$ weight 6 newforms for $\Gamma_0(N)$ of level $2^{10} < N \leq 2^{11}$ and dimension $g \leq 1$ for $p < 2^{11}$



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



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



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

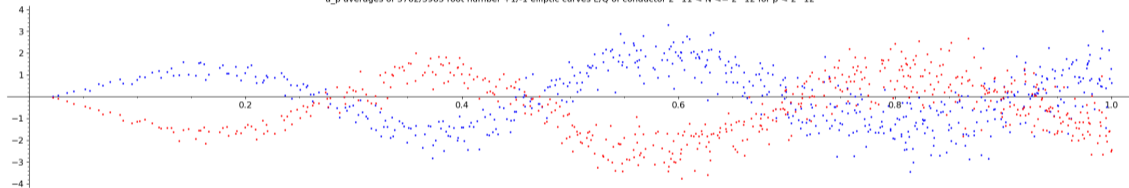
$$\frac{\sum_{N \in [X, X+Y]}^{\square\text{-free}} \sum_f w(f) a_P(f) P^{(1-k/2)}}{\sum_{N \in [X, X+Y]}^{\square\text{-free}} \sum_f 1} = M_k(y) + O_\varepsilon(X^{-\delta'+\varepsilon} + P^{-1})$$

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

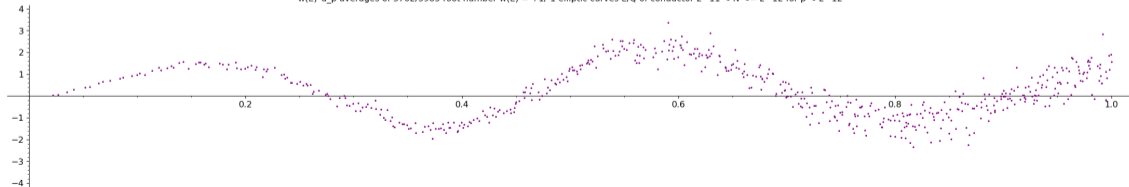
Murmurations of elliptic curves with squareroot normalization

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 $m_p := w(E)a_p(E)$ 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 $p < 2^{12}$



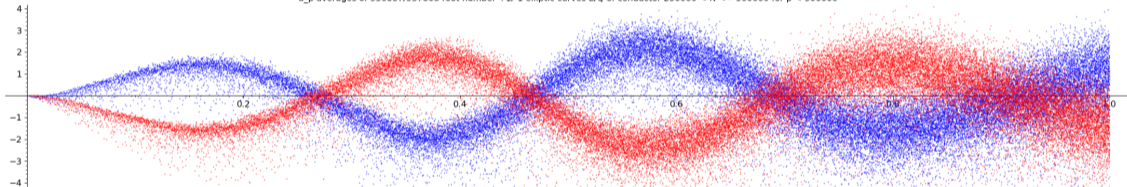
$w(E)a_p$ averages of 3762/3985 root number $w(E) = +1/-1$ elliptic curves E/\mathbb{Q} of conductor $2^{11} < N \leq 2^{12}$ for $p < 2^{12}$



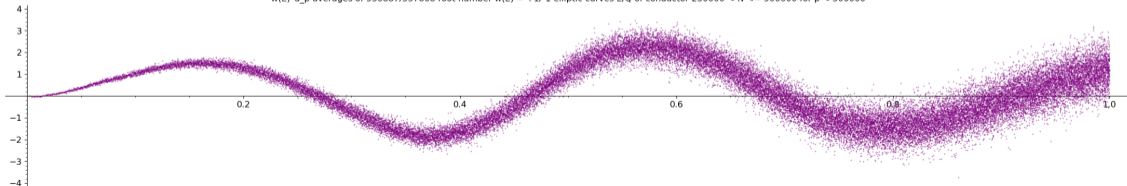
Murmurations of elliptic curves with squareroot normalization

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 $m_p := w(E)a_p(E)$ 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



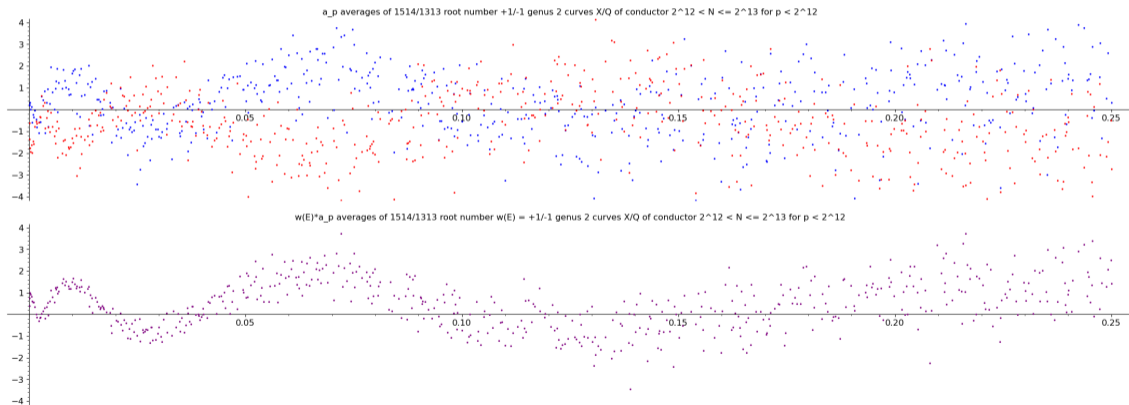
w(E)*a_p averages of 530887/537808 root number w(E) = +1/-1 elliptic curves E/Q of conductor 250000 < N <= 500000 for p < 500000



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

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 Sato-Tate group $\mathrm{USp}(4)$.

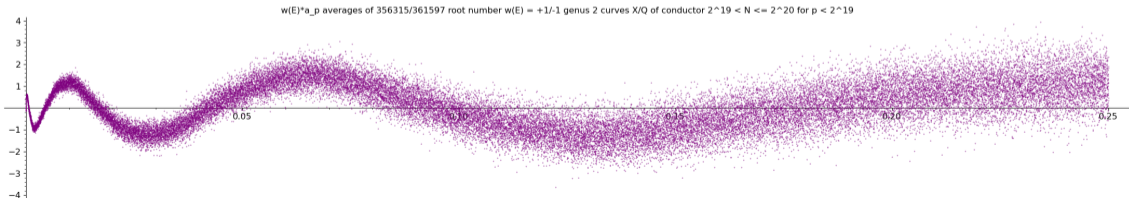
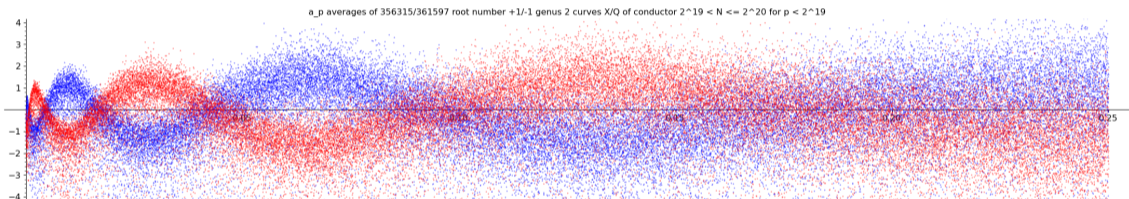
Conductor of $L(X, s)$ in $(M, 2M]$ for $M = 2^{12}, \dots, 2^{19}$ with x -axis range $[0, M/2]$.



Coming soon to the [LMFDB](#).

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

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 Sato-Tate group $\mathrm{USp}(4)$.
Conductor of $L(X, s)$ in $(M, 2M]$ for $M = 2^{12}, \dots, 2^{19}$ with x-axis range $[0, M/2]$.

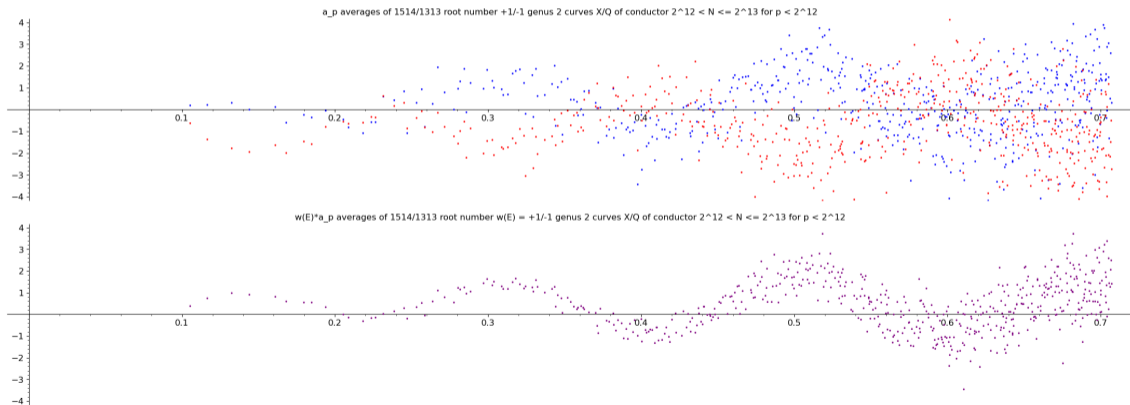


Coming soon to the [LMFDB](#).

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

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 Sato-Tate group $\mathrm{USp}(4)$.

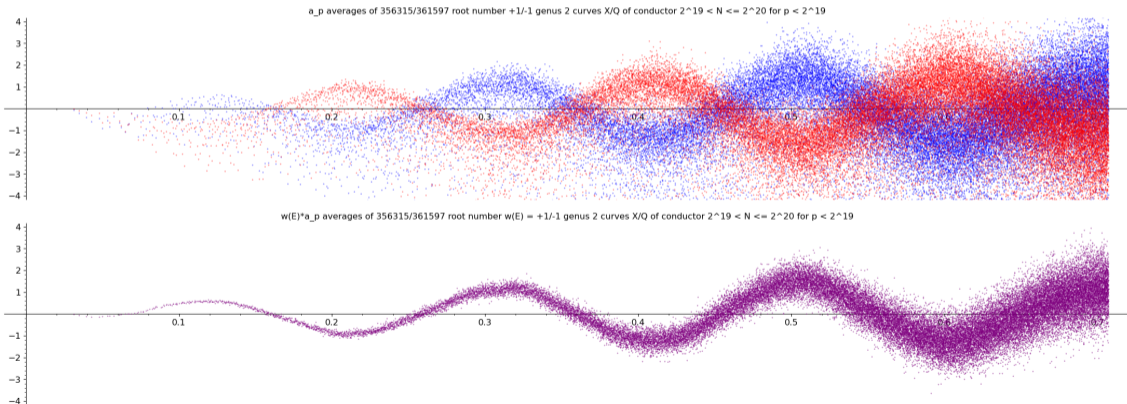
Conductor of $L(X, s)$ in $(M, 2M]$ for $M = 2^{12}, \dots, 2^{19}$ with x -axis range $[0, M/2]$.



Coming soon to the [LMFDB](#).

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

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 Sato-Tate group $\mathrm{USp}(4)$.
Conductor of $L(X, s)$ in $(M, 2M]$ for $M = 2^{12}, \dots, 2^{19}$ with x-axis range $[0, M/2]$.



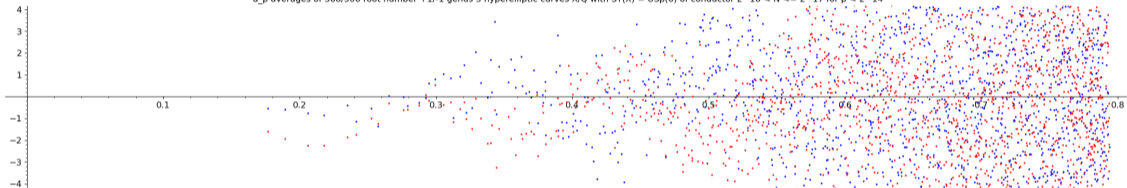
Coming soon to the [LMFDB](#).

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

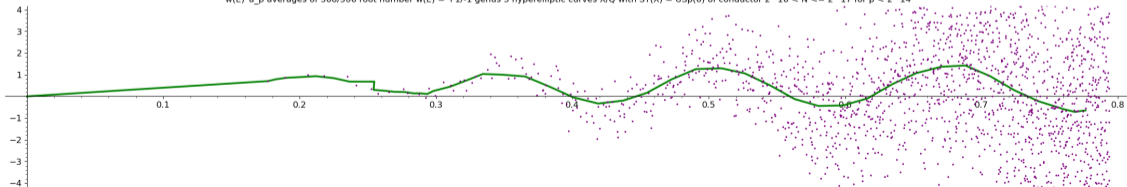
Recently constructed database of genus 3 curves X/\mathbb{Q} of conductor at most 10^7 includes 59,214 isogeny classes of hyperelliptic curves with ST group $\mathrm{USp}(6)$.

Conductor of $L(X, s)$ in $(M, 2M]$ for $M = 2^{16}, \dots, 2^{22}$ with x -axis range $[0, M/2]$.

a_p averages of 368/506 root number $+1/-1$ genus 3 hyperelliptic curves X/\mathbb{Q} with $\mathrm{ST}(X) = \mathrm{USp}(6)$ of conductor $2^{16} < N \leq 2^{17}$ for $p < 2^{14}$



$w(E)a_p$ averages of 368/506 root number $w(E) = +1/-1$ genus 3 hyperelliptic curves X/\mathbb{Q} with $\mathrm{ST}(X) = \mathrm{USp}(6)$ of conductor $2^{16} < N \leq 2^{17}$ for $p < 2^{14}$



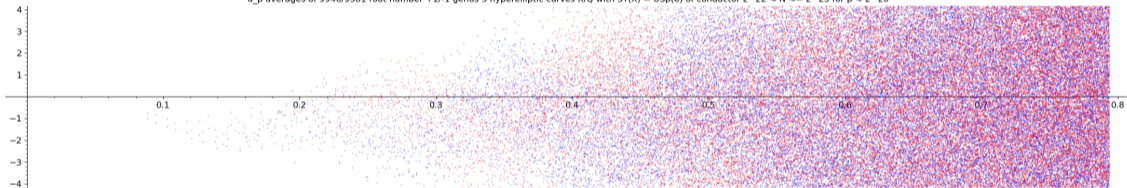
Coming soon to the [LMFDB](#).

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

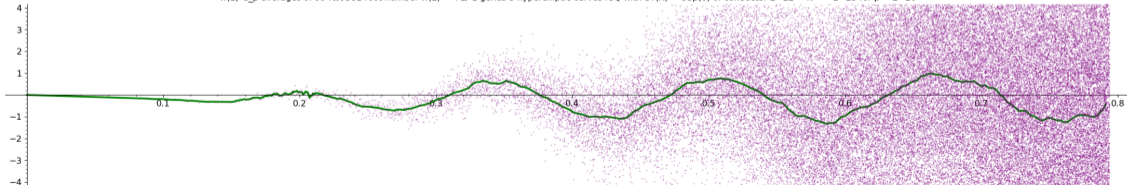
Recently constructed database of genus 3 curves X/\mathbb{Q} of conductor at most 10^7 includes 59,214 isogeny classes of hyperelliptic curves with ST group $\mathrm{USp}(6)$.

Conductor of $L(X, s)$ in $(M, 2M]$ for $M = 2^{16}, \dots, 2^{22}$ with x-axis range $[0, M/2]$.

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



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 $2^{22} < N \leq 2^{23}$ for $p < 2^{20}$



Coming soon to the [LMFDB](#).

Computing trace averages of many E/\mathbb{Q}

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

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

Complexity estimates ignore $\log \log p$ factors.

Realizing the CM torsor via isogenies

Having computed $a_p(E)$ for one E/\mathbb{F}_p , we can (typically) easily compute $\text{End}(E) = \mathcal{O}$, since $\text{disc } \mathcal{O}$ divides $a_p(E)^2 - 4p$. Let $\text{Ell}_{\mathcal{O}}(\mathbb{F}_p) := \{j(E) : E/\mathbb{F}_p \text{ has } \text{End}(E) = \mathcal{O}\}$.

$\text{Gal}(K_{\mathcal{O}}/K) \simeq \text{cl}(\mathcal{O})$ acts on $\text{Ell}(\mathcal{O})$ via (horizontal) isogenies.

If $[\mathfrak{l}] \in \text{cl}(\mathcal{O})$ has norm ℓ and $j_1 \in \text{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ then

$$\Phi_{\ell}(j_1, [\mathfrak{l}]j_1) = 0,$$

where $\Phi_{\ell}(X, Y)$ is the classical modular polynomial. Typically $[\mathfrak{l}]j_1$ and $[\bar{\mathfrak{l}}]j_1$ are the only roots of $\Phi_{\ell}(j_1, X)$ in \mathbb{F}_p , and we can choose them to ensure this.

A **polycyclic presentation** for $\text{cl}(\mathcal{O})$ is a sequence of ideals $\mathfrak{l}_1, \dots, \mathfrak{l}_k$ such that every $[\mathfrak{a}] \in \text{cl}(\mathcal{O})$ may be written uniquely as

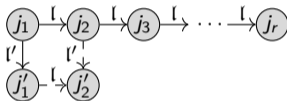
$$[\mathfrak{a}] = [\mathfrak{l}_1^{e_1}] \cdots [\mathfrak{l}_k^{e_k}] \quad (0 \leq e_i < r_i),$$

where $r_i = \min\{r : [\mathfrak{l}_i^r] \in \langle [\mathfrak{l}_1], \dots, [\mathfrak{l}_{i-1}] \rangle\}$ is $[\mathfrak{l}_i]$'s **relative order**.

Using GCDs

We can replace most root-finding steps with GCDs.

Suppose we have computed a cycle of ℓ -isogenies. After computing a single ℓ' -isogeny, we can compute the next cycle of ℓ -isogenies using GCDs.



Provided $4\ell^2\ell'^2 < |D|$, the monic polynomial

$$\varphi(X) = \gcd(\Phi_\ell(j'_1, X), \Phi_{\ell'}(j_2, X)) \in \mathbb{F}_p[X]$$

will have degree 1 and we can compute $j'_2 = -\varphi(0)$ as its unique root.

Even when our polycyclic presentation with one generator, we can choose an auxiliary prime ℓ' so $[\ell'] = [\ell]^n$ and use GCDs to a single line of j -invariants after n steps.

Computing murmurations using the trace formula

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

By massaging a **theorem of Popa**, one finds that

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

$$h^*(D, N) := \sum_{\substack{u|N \\ u^2|D}} \mu(u) H'\left(\frac{D}{u^2}\right), \quad s_k(N, n) := \frac{\varphi(N)}{N^{k/2}} \sum_{\substack{uv=Nn \\ N|(u+v)}} \min(u, v)^{k-1}, \quad \sigma_N(n) := \sum_{\substack{m|n \\ m \perp N}} \frac{n}{m},$$

where $g_k := g_k(b, c)$ is defined by $g_2 := 1$, $g_4 := b - c$, $g_{k+4} := (b - 2c)g_{k+2} - c^2 g_k$.

Assaf's recent paper gives formulas for $\text{tr}(T_n \circ W, S_k^{\text{new}}(N))$ via $\text{tr}(T_n \circ W, S_k(N))$.

Key point: For $n = O(N)$ the sum contains $O(1)$ terms!

Computing murmurations using the trace formula

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

$$h^*(D, N) = \sum_{u|N, u^2|D} \mu(u) H'(\frac{D}{u^2}) = \sum_{u|\frac{c}{w}} \mu(u) H'(\frac{D}{u^2}) = \varphi_1^{D/w^2}(w) h'(\frac{D}{w^2}),$$

where $\varphi_1^D(n)$ is the multiplicative function defined on prime powers as

$$\varphi_1^D(p^e) = 1 + \frac{p^e - 1}{p - 1} \left(p - \left(\frac{D}{p} \right) \right).$$

The class numbers for $|D| \leq 2^{40}$ 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 $\text{tr}(T_p \circ W, S_k^{\text{new}}(N))$ for $2^{18} \leq N < 2^{19}$ and $p \leq 2^{19}$ 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.

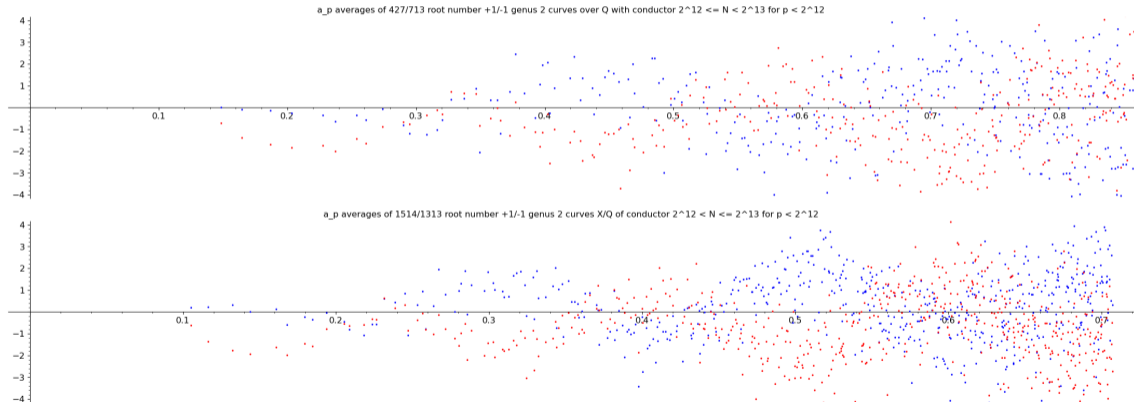
The algorithms described in [BSSVY 2016] and [S 2018] enumerate curves by discriminant, but curves with very large discriminants can have very small conductors.

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 some 5 million curves with conductor below 10^6 (98% of these are not in the LMFDB yet).

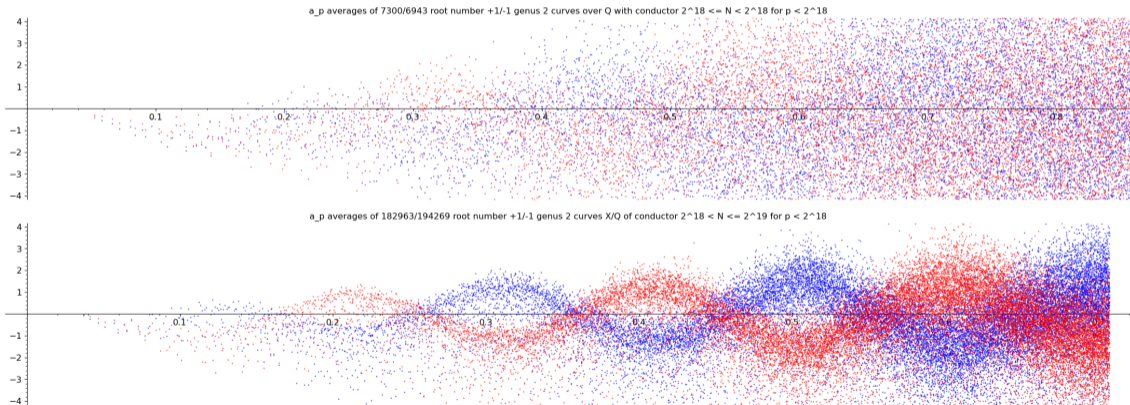
L -functions of genus 2 curves over \mathbb{Q} with Sato-Tate group $USp(4)$.

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

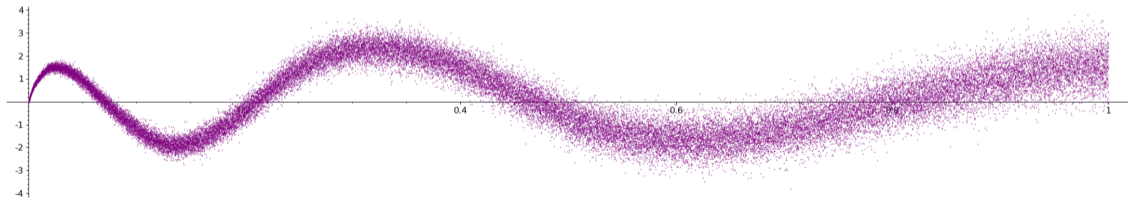


L -functions of genus 2 curves over \mathbb{Q} with Sato-Tate group $USp(4)$.

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



Thank you!



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