Murmurations: A computational perspective

And rew 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

$$L(E,s) \coloneqq \prod_{p} (1 - a_p p^{-s} + \chi(p) p^{1-2s})^{-1} = \sum_{n \ge 1} a_n n^{-s}$$

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 of ST(E) (= SU(2) if *E* does not have CM).
- 2. Birch and Swinnerton-Dyer:

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

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).

al histogram of y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429 for p <= 2^10 172 data points in 13 buckets, z1 = 0.023, out of range data has area 0.250



Moments: 1 1.034 1.716 2.532 4.446 7.203 13.024 22.220 40.854 72.100 133.961

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

al histogram of y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x + 34481611795030556467032985690390720374855944359319180361266008296291939448732243429 for p <= 2^40 41203088796 data points in 202985 buckets



How rank effects trace distributions

An early form of the BSD conjecture implies that

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

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).¹²

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 $M = 2^{11}, 2^{12}, \ldots, 2^{17}, 250000$. 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 $N_E \in (M, 2M]$.



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



Murmurations of elliptic curves over a_n (not just a_p)

Elliptic curve *L*-functions of conductor $N \in (M, 2M]$ for $M = 2^{11}, 2^{12}, \ldots, 2^{17}, 250000$. 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 $M = 2^{11}, 2^{12}, \ldots, 2^{17}, 250000$. 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 $N_F \in (M, 2M]$, using subintervals of size \sqrt{M} for p < 2M, with $M = 2^{17}$. -20 -30147455.b2, 163839.a1, 180222.be2, 196606.b1, 212990.11, 229374.a1, 245758.a1, 262143.d1

Murmurations depend critically on the conductor

Elliptic curves with ht(E) := max(4|A|³, 27B²) 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 $N_E \in (M, 2M]$.



Murmurations depend critically on the conductor

Elliptic curves with ht(*E*) := max(4|*A*|³, 27*B*²) in (*M*, 2*M*] for $M = 2^{16}, \ldots, 2^{25}$. The *x*-axis range is [0, 2*M*]. 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 631953/630995 root number w(E) = +1/-1 elliptic curves E/Q of naive height $2^{26} < h(E) <= 2^{27}$ for p < 2^{27}



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



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

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

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)*a p averages of 1691/1772 root number w(E) = +1/-1 weight 2 newforms for Gamma 0(N) of level 2^10 < N <= 2^11 and dimension g <= 1 for p < 2^11







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

-1 -2

-3



w(E)*a p/p^2 averages of 259/304 root number w(E) = +1/-1 weight 6 newforms for Gamma 0(N) of level 2^10 < N <= 2^11 and dimension g <= 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.



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

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

$$A := \prod_{\rho} \left(1 + \frac{p}{(\rho+1)^2(\rho-1)} \right), B := \prod_{\rho} \frac{p^4 - 2p^2 - p + 1}{(\rho^2 - 1)^2}, c(r) := \prod_{\rho \mid r} \left(1 + \frac{p^2}{p^4 - 2p^2 - \rho + 1} \right), D_k := \frac{12}{(k-1)\pi} \prod_{\rho} \frac{12}{(1 - \frac{1}{p^2 + \rho})}.$$
Theorem [Zubriling 2023] Let $\sum_{\rho \mid r} 2 \cdot (f) q^{\rho}$ denote a weight k newform for $\Gamma_{\sigma}(M)$ with

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 $(\sqrt{p}, \bar{a}_p \text{ or } \bar{m}_p)$ shows the average of a_p or $m_p := w(E)a_p(E)$ over even/odd or all E/\mathbb{Q} with $N_E \in (M, 2M]$.



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



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 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.

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



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 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.

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 USp(4). 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 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 10⁷ 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.

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 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 $B = \Box$.

- 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 $\operatorname{End}(E) = 0$, since disc 0 divides $a_p(E)^2 - 4p$. Let $\operatorname{Ell}_0(\mathbb{F}_p) := \{j(E) : E/\mathbb{F}_p \text{ has } \operatorname{End}(E) = 0\}$.

 $\operatorname{Gal}(\mathcal{K}_{\mathbb{O}}/\mathcal{K}) \simeq \operatorname{cl}(\mathbb{O})$ acts on $\operatorname{Ell}(\mathbb{O})$ via (horizontal) isogenies. If $[\mathfrak{l}] \in \operatorname{cl}(\mathbb{O})$ has norm ℓ and $j_1 \in \operatorname{Ell}_{\mathbb{O}}(\mathbb{F}_p)$ 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 $[\mathfrak{\bar{l}}]_{j_1}$ 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 cl(0) is a sequence of ideals l_1, \ldots, l_k such that every $[\mathfrak{a}] \in cl(0)$ may be written uniquely as

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

where $r_i = \min\{r : [l_i^r] \in \langle [l_1], \dots, [l_{i-1}] \rangle\}$ is $[l_i]$'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

$$arphi(X) = \gcd(\Phi_\ell(j_1',X),\Phi_{\ell'}(j_2,X)) \in \mathbb{F}_{p}[X]$$

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

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

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

where $g_k := g_k(b, c)$ is defined by $g_2 := 1$, $g_4 := b - c$, $g_{k+4} := (b - 2c)g_{k+2} - c^2g_k$. Assaf's recent paper gives formulas for tr $(T_n \circ W, S_k^{new}(N))$ via $tr(T_n \circ W, S_k(N))$. 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 tr($T_p \circ W$, $S_k^{\text{new}}(N)$) 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 some 5 million curves with conductor below 10^6 (98% of these are not in the LMFDB yet).

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



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



Thank you!





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