ALEX COWAN

RESEARCH STATEMENT

I do analytic number theory, computational number theory, and arithmetic statistics. Within these areas my interests are broad.

Section 1 presents [Cow24d] and [Cow25a]. I use analytic techniques to study the phenomenon of "murmurations" which has been of great interest ever since it was discovered empirically by data scientists three years ago. My work connects murmurations to the field of random matrix theory, the first time this connection has been made in the literature. In [Cow24d], I leverage existing results in random matrix theory to prove murmurations in many cases. In [Cow25a], I give more general constructions which explain several key properties of murmurations, and develop strong bounds in a couple auxiliary problems to prove murmurations "from scratch" in an important case.

Section 2 presents [Cow25c], technically challenging analytic work in which I use the spectral theory of automorphic forms to study the correlation between generalized divisor sums of integers a fixed distance apart. Such "shifted convolutions" are a cornerstone of modern analytic number theory with many applications. Existing general treatments of the problem all made simplifying assumptions which exclude the case I study. Determining the asymptotic value of this divisor sum correlation required an adaptation of a little-known theoretical technique, and the error term I obtain is unusually small. This work was the subject of a topics course I taught at Harvard; notes in the form of video lectures are available on my website and on YouTube.

Section 3 presents a selection of papers of mine in arithmetic statistics: [Cow24b] on the distribution of conductors of elliptic curves, [CM24, CFM24] on moduli spaces of genus 2 curves with prescribed real multiplication, and [Cow20] connecting statistics of points on elliptic curves and continued fractions.

Section 4 presents [Cow22a] on the design and implementation of an algorithm for generating a database of modular forms: complicated and mysterious objects of fundamental importance in number theory. The database I generate is 200 times larger than the one before it, and is available on the widely-used L-functions and Modular Forms Database (LMFDB) so as to be easily and readily accessible to number theorists broadly.

Contents

1. Murmurations 1
2. Spectral theory of automorphic forms and divisor sum correlations 4
3. Arithmetic statistics 5
4. A modular form database from supersingular isogeny graphs 8
References 10

1. Murmurations

A collaboration of data scientists [HLOP24] recently observed experimentally that the number of points on an elliptic curve mod p, when averaged over a set of elliptic curves of fixed rank and similar conductor, oscillates as p varies. (I.e., let a and b be integers, and consider the cardinality of the set of pairs $(x, y) \in (\mathbb{Z}/p)^2$ which solve the equation $E_{a,b} : y^2 = x^3 + ax + b$. When this cardinality is averaged over over $(a, b) \in \mathbb{Z}^2$ appropriately, the resulting function of p appears to oscillate and enjoy other peculiar characteristics. This is very surprising.)

These oscillations, called *murmurations*, hadn't been observed previously, and it's unclear what causes them. Manifestations of the phenomenon have since been observed empirically in many other settings [Sut22], but theoretical results remain elusive: prior to [Cow24d, Cow25a], only five cases [Zub23, Wan25, LOP25, BBLLD23, BLLD+24] had been established, with the latter three assuming GRH. These results use trace formulas, and the underlying mechanism remains mysterious.

In [Cow24d] I connect murmurations to distributions of low-lying zeros in families of L-functions and random matrix theory. This approach for studying murmurations hadn't appeared outside of my short note [Cow23], and leads to results in a wide variety of settings, notably including that of elliptic curves. Previously it was unclear how to predict anything at all about the nature of murmurations, even heuristically. Six examples are given in [Cow24d]: one unconditionally, two under GRH, and three under additional conjectures from random matrix theory.

Applying [Cow24d]'s method in the simple and computationally tractable case of a family $\mathcal{F}_\chi$ of even real primitive Dirichlet characters χ_d — for a given d the function χ_d evaluates to 1 for squares mod d, and -1 for non-squares — yields roughly

$$\frac{1}{\#\mathcal{F}_\chi}\sum_{d\in\mathcal{F}_\chi}\frac{1}{x^{\frac{1}{2}}}\sum_{\substack{p^k<x\\ k\text{ odd}}}\chi_d(p)\log p \approx \frac{1}{2\pi i}\int_{\frac{1}{2}+\varepsilon-iT}^{\frac{1}{2}+\varepsilon+iT}\frac{\pi^2}{6}\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}\frac{\zeta(2-2s)}{\zeta(3-2s)}\frac{1}{\#\mathcal{F}_\chi}\sum_{d\in\mathcal{F}_\chi}\left(\frac{\pi x}{d}\right)^{s-\frac{1}{2}}\frac{ds}{s}. \tag{1}$$

Figure 1.4 visualizes (1) in the case $\mathcal{F}_\chi := \{d : 95{,}000 < d < 105{,}000,\ d \text{ a fundamental discriminant}\}$. See [Cow24d, Thm. 1.2, Thm. 2.4] for more precise statements, including error terms and their provenance.

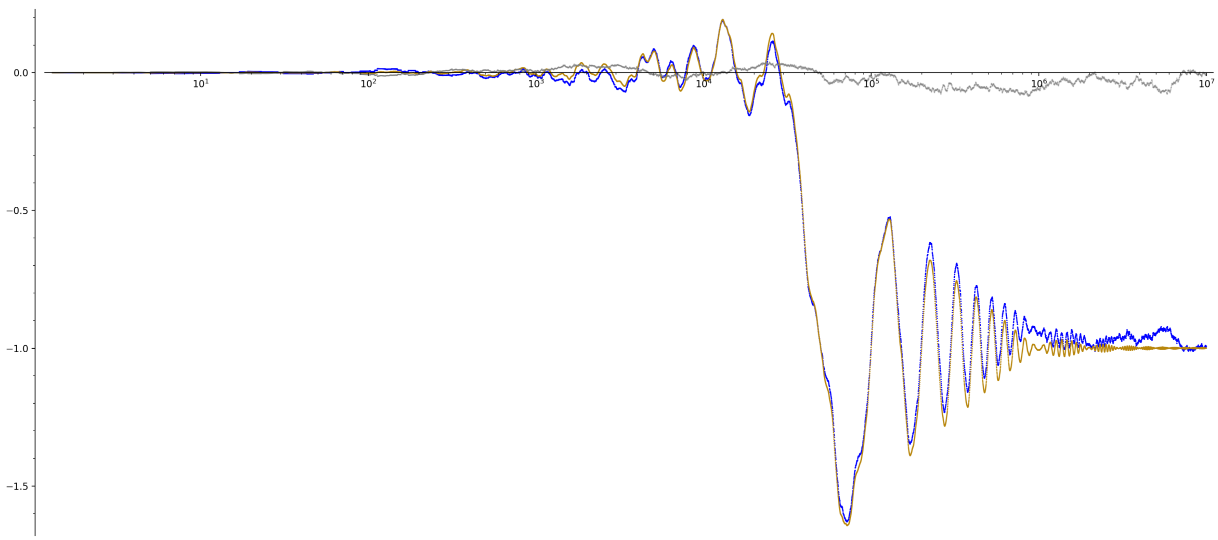

Figure 1.1. For $T = 900$ and $\varepsilon = 0.1$, the left and right hand sides of (1) in blue and gold respectively, as well as their difference in grey, as functions of x. The integral in (1) is approximated by Riemann sum evaluated at 180,000 equally-spaced points. In this example $\#\mathcal{F}_\chi = 3038$. My code is available at [Cow24c].

The behaviour of the quantity on the left hand side of (1) is surprisingly structured. Instead, one might have imagined that the values $\chi_d(p)$ would behave as if they were "randomly" $+1$ or -1 with equal probability. If this had been true, the left hand side of (1) would either converge to 0 or diverge almost surely, and certainly not possess the regular structure that's visible in figure 1.4.

Murmurations of elliptic curves were the initial catalyst for the study of the topic in general [HLOP24]. Prior to [Cow24d], there were no predictions at all for the precise way in which the average value of the number of points mod p oscillates, how many curves needed to be averaged for the oscillations to appear, the range in which oscillations were visible, etc.

Let $\mathcal{F}_6(H)$ denote the family of elliptic curves

$$\mathcal{F}_6(H) := \{y^2 = x^3 + ax + b : 3 \nmid a,\ 2 \nmid b,\ |a| < H^{\frac{1}{3}},\ |b| < H^{\frac{1}{2}},\ p^4 \mid a \implies p^6 \nmid b\}. \tag{2}$$

Roughly speaking, $\mathcal{F}_6(H)$ consists of elliptic curves with height less than H and good or "pretty good" reduction at 2 and 3. For a given $E = E_{a,b} \in \mathcal{F}_6(H)$, let α_p and $\overline{\alpha}_p$ be the complex conjugates of norm 1 such that

$$\sqrt{p}(\alpha_p + \overline{\alpha}_p) := p - \#\{(x,y) \in (\mathbb{Z}/p)^2 : y^2 = x^3 + ax + b\}.$$

Theorem 1.2 (Murmurations of elliptic curves [Cow24d, Thm. 1.1])**.** *Let $\mathcal{F}_6(H)$ be the family* (2) *of elliptic curves ordered by height, let $\omega \in \{\pm 1\}$, and let $\mathcal{F}_6(H)^\omega := \{E \in \mathcal{F}_6(H) : \omega_E = \omega\}$. Assume that* [Cow24d, (7), (8)] *and the ratios conjecture* [DHP15, Conj. 3.7] *hold with $\mathcal{F}_6(H)$ replaced with $\mathcal{F}_6(H)^\omega$. For any H, y, T, ε such that $0 < \varepsilon < \frac{1}{2}$ and $(Hy)^{\frac{1}{2}+\varepsilon} \ll T < Hy$,*

$$\frac{1}{\#\mathcal{F}_6(H)^\omega} \sum_{E \in \mathcal{F}_6(H)^\omega} \frac{1}{\sqrt{Hy}} \sum_{\substack{p^k < Hy \\ p \nmid N_E}} \left(\alpha_p^k + \overline{\alpha}_p^k\right) \log p$$
$$= \frac{\omega}{2\pi i} \int_{\mathbb{R}} \int_{\frac{1}{2}+\varepsilon-iT}^{\frac{1}{2}+\varepsilon+iT} g(s) \Big(4\pi^2 \frac{y}{\lambda}\Big)^{s-\frac{1}{2}} \frac{ds}{s}\, F_N'(\lambda)\, d\lambda \,-\, 1 \,+\, O\Big((\log H)^{-\frac{5}{6}} + H^\varepsilon y^\varepsilon T^\varepsilon H^{-\frac{5}{12}+\varepsilon}\Big)$$

with

$$g(s) := \frac{\Gamma(\frac{3}{2}-s)}{\Gamma(\frac{1}{2}+s)} \zeta(2s) A(\tfrac{1}{2}-s, s-\tfrac{1}{2}),$$

where $A(\alpha, \gamma)$ is the product over primes defined in [Cow24d, Def. 3.2]*, and $F_N(\lambda)$ is the approximation defined in* [Cow24d, Def. 3.9] *to the cummulative distribution function of conductors among $E \in \mathcal{F}_6$.*

One of the most striking characteristics of murmurations is their "N/p-invariance", where N can be taken to be the analytic conductor of the arithmetic object's L-function. This scale-invariance can be seen in theorem 1.2, manifesting as the absence of any dependence on H in the (oscillation-producing) first term on the right hand side.

Determining F_N above, the distribution of the conductors of elliptic curves in $\mathcal{F}_6(H)$, is an interesting and difficult problem, and was the subject of the separate paper [Cow24b] motivated by theorem 1.2. The analogue of F_N for the family of all elliptic curves over $\mathbb{Q}$ is the function Φ from theorem 3.1 below. Both F_N and Φ are plotted in figure 3.3.

[Cow25a] further broadens the method of [Cow24d], and explains how to obtain murmurations from approximate functional equations, in many ways akin to passing from [CS07] to the more general [CFK+05]. Several universal characteristics about murmurations are explained, e.g. the source of the N/p-invariance, as well as the peculiar normalization in which the Dirichlet coefficients have size $\sqrt{p}$ in e.g. [Zub23, SS25].

[Cow25a] goes on to implement the generalized method to exhibit murmurations of quadratic twist families of GL_1 automorphic representations unconditionally. Let χ be a primitive Dirichlet character of conductor q and let t be a real number. Let $q_* := 4q$ if $2 \parallel q$ and $q_* := q$ otherwise. Fix $1 < D_0 < D$ and $\ell \in (\mathbb{Z}/q_*)^\times$, and set

$$\mathcal{F} := \big\{D_0 < d < D \,:\, d \text{ a fundamental discriminant},\ d = \ell \bmod q_*\big\}.$$

Let χ_d denote the Kronecker symbol $\left(\frac{d}{\cdot}\right)$. For any $d \in \mathcal{F}$, define

$$\omega_{\mathcal{F}} := i^{-\frac{1-\chi(-1)}{2}} \frac{\tau(\chi)}{\sqrt{q}} \left(\frac{qD}{\pi}\right)^{it} \chi_d(q)\chi(d),$$

where $\tau(\chi)$ is the Gauss sum. (The value of $\omega_{\mathcal{F}}$ is independent of the choice of $d \in \mathcal{F}$.)

Theorem 1.3 (Murmurations for quadratic twists of a GL_1 automorphic representation [Cow25a, Thm. 1.1])**.** *Let $\frac{5}{6} < \delta < 1$. In the range $(qD)^{1-\varepsilon} \ll x \ll (qD)^{1+\varepsilon}$, $D^{\delta-\varepsilon} \ll \#\mathcal{F} \ll D^{\delta+\varepsilon}$, $t \ll D^{1-\delta-\varepsilon}$,*

$$\frac{1}{\#\mathcal{F}} \sum_{d \in \mathcal{F}} \frac{1}{\sqrt{x}} \sum_{n<x} n^{it} \chi(n)\chi_d(n) = \frac{\omega_{\mathcal{F}}}{2\pi i} \int_{\frac{3}{4}-i\infty}^{\frac{3}{4}+i\infty} g(s) \left(\frac{\pi x}{qD}\right)^{s-\frac{1}{2}} \frac{ds}{s}$$
$$+ \operatorname*{Res}_{s=\frac{1}{2}+it} g(s) \,+\, O\big(q^{\frac{1}{6}} D^{\frac{1}{12}\rho} + q^{\frac{3}{4}} D^\rho + |t| D^{\delta-1}\big)(qD)^\varepsilon$$

with

$$g(s) := \frac{\Gamma\Big(\frac{1-s+it}{2} + \frac{1-\chi(-1)}{4}\Big)}{\Gamma\Big(\frac{s-it}{2} + \frac{1-\chi(-1)}{4}\Big)} \frac{L(2-2s+2it, \bar{\chi}^2)}{L^{(2)}(3-2s+2it, \bar{\chi}^2)} \prod_{p \nmid 2q} \left(1 - \frac{1}{(p+1)(1-\chi^2(p)p^{3-2s+2it})}\right)$$

and

$$\rho := -\frac{1}{14} + \frac{1}{8}\left(\delta - \frac{13}{14}\right) + \frac{7}{8}\left|\delta - \frac{13}{14}\right|.$$

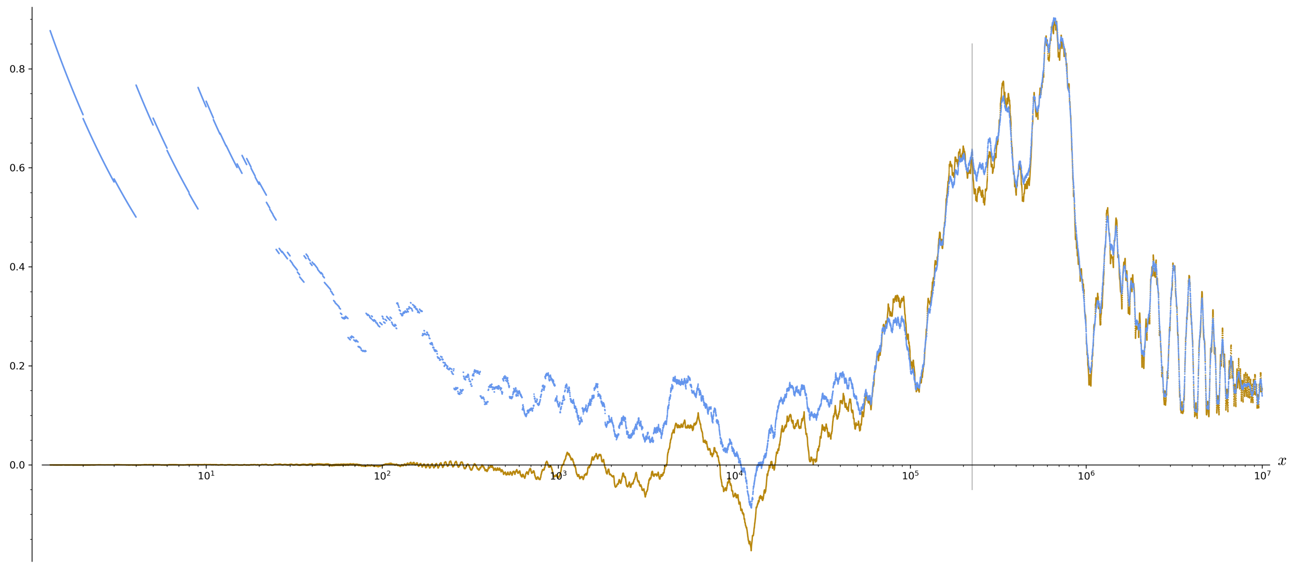

Figure 1.4. Real parts of the left (blue) and right (gold) hand sides of theorem 1.3 as functions of x, with $t = 2$, $\chi \bmod 7$ sending $3 \mapsto \frac{1+i\sqrt{3}}{2}$, and $\mathcal{F} = \{99{,}000 < d < 101{,}000 \,:\, d \text{ a fundamental discriminant},\ d = 1 \bmod 7\}$. The vertical grey line indicates the value of qD/π. The right hand side was estimated with a Riemann sum over $|\mathrm{Im}(s)| \leqslant 1{,}000$ sampled at 200,001 evenly spaced points, and the products over primes truncated at $p < 30{,}000$. In this example, $\#\mathcal{F} = 89$.

The proof of theorem 1.3 involves generalizing and sharpening results on statistics of quadratic characters of Jutila [Jut81] and Stankus [Sta83], and the use of a variation of the approximate functional equation which dynamically rebalances error terms to obtain a power savings.

As an intermediate result, the mean values of L-functions in families of quadratic twists (for fundamental discriminants of size $D > 0$ in a narrow slice of an arbitrary arithmetic progression) of GL_1 and GL_2 automorphic representations are determined roughly in the ranges $s \ll D^2$ and $s \ll D^{\frac{1}{2}}$ respectively. The previous best was the much smaller $s \ll D^{\frac{1}{4}}$ [VT81] for the trivial representation on GL_1 and all fundamental discriminants less than D.

2. Spectral theory of automorphic forms and divisor sum correlations

The classical *additive divisor problem* [Mot94] asks about the correlation between the number of divisors of n and the number of divisors of $n+1$ via the study of the sum $\sum_{n<X} \sigma_0(n)\sigma_0(n+1)$, where $\sigma_0(n) \coloneqq \sum_{d|n} 1$ is the number of divisors of the positive integer n. Many generalizations of the additive divisor problem are studied, both because they're inherently interesting and because they have important applications, e.g. to the growth of L-functions on vertical lines [Mic07]. One natural generalization comes from replacing $\sigma_0(n)$ in the classical additive divisor problem with

$$n^{-s}\sigma_{2s}(n,\chi) \coloneqq n^{-s} \sum_{d|n} \chi(d) d^{2s}.$$

The normalization above is natural in light of a functional equation $s \mapsto -s$. In [Cow25c] I prove the following theorem for "sufficiently generic" Dirichlet characters χ, ψ and complex numbers u, v.

Theorem 2.1 (Correlation of sum-of-divisors functions [Cow25c, Thm. 1.1])**.** *For any fixed shift $k \in \mathbb{Z}_{>0}$, the correlation (as n varies) between the shifted values $n^{-u}\sigma_{2u}(n,\chi)$ and $(n+k)^{-v}\sigma_{2v}(n+k,\psi)$ of generalized sum-of-divisors functions is given by*

$$\frac{1}{X}\sum_{n=1}^{X} \frac{\sigma_{2u}(n,\chi)\sigma_{2v}(n+k,\psi)}{n^u (n+k)^v} = c_+ X^{u+v} + c_- X^{-u-v} + O\Big(X^{|\mathrm{Re}(u)|+|\mathrm{Re}(v)|-\beta+\varepsilon}\Big)$$

as $X \to \infty$, with

$$c_+ := \frac{L(1+2u,\overline{\chi})L(1+2v,\overline{\psi})}{L(2+2u+2v,\overline{\chi\psi})}\frac{\sigma_{-1-2u-2v}(k,\overline{\chi\psi})}{1+u+v}\frac{\tau(\overline{\chi\psi})\chi\psi(k)}{\tau(\overline{\chi})\tau(\overline{\psi})}$$
$$c_- := \frac{L(1-2u,\chi)L(1-2v,\psi)}{L(2-2u-2v,\chi\psi)}\frac{\sigma_{-1+2u+2v}(k,\chi\psi)}{1-u-v}$$

and

$$\beta := \frac{1+2|\mathrm{Re}(u)|+2|\mathrm{Re}(v)|}{3+|\mathrm{Re}(u+v)|+|\mathrm{Re}(u-v)|}.$$

Theorem 2.1 is proved using spectral methods in automorphic forms. The sum on the left hand side is encoded in the Fourier coefficients of a function defined on a hyperbolic manifold. This function (a product of non-holomorphic Eisenstein series) is in turn expressed as a linear combination of eigenfunctions of the manifold's Laplacian. Then, with difficulty, the analytic properties of these eigenfunctions and the coefficients of this linear combination are understood sufficiently well to yield theorem 2.1. This overall approach is similar to the ones taken in e.g. [VT84, Jut96, DFI02, Mic04].

Previous work on shifted convolutions have always included extra simplifying assumptions imposed on χ, ψ, u, and v. Even very general treatments of these sorts of problems [MV10, Nel19, Wu19, HLN21] don't cover the case done by theorem 2.1. A key ingredient in [Cow25c] is the use of a generalized form of a lesser-known technique that's sometimes called "automorphic regularization" [Zag81, MV10]. This technique permits the spectral decomposition of automorphic functions which are not obviously square-integrable, enabling one to study a wider class of problems.

The error term in theorem 2.1 is unusually small compared to the main term for certain choices of u and v. Previous work had always observed a power savings of $\beta = \frac{1}{3}$, but loosening the restrictions on u and v allows the power savings to be larger than this: β can be as large as $\frac{8}{14} - \varepsilon$ for admissible χ, ψ, u, v. See [Cow25c, Thm. 1.1] for details.

Spectral methods in automorphic forms are a broadly useful toolkit. They're versatile in the types of problems they're ammenable to, and historically have yielded strong results [Iwa02]. In [Cow22b] I use spectral methods of automorphic forms study statistics of modular symbols, after interest was generated by Mazur and Rubin in [MR16, MR20]. Theorem 2.1 was the main subject of a topics course I designed and taught at Harvard. Notes in the form of video lectures are available on my website and on YouTube. I'm currently directing the research of two undergraduate students in this area.

3. Arithmetic statistics

I have several papers [Cow20, BBC+20, Cow21, CM24, CFM24, Cow24b, Cow25b] falling under the broad umbrella of arithmetic statistics that are not primarily computational or analytic in nature. This section presents [Cow24b], [CM24, CFM24], and [Cow20].

Conductor distributions of elliptic curves

Elliptic curves are most naturally ordered by conductor but most easily ordered by height. Converting between these two orderings is an interesting and difficult problem. The well-known and widely believed Brumer–McGuinness–Watkins heuristics [BM90, Wat08] on this subject are in certain restricted cases supported empirically [BGR19]. Theoretical support of the Brumer–McGuinness–Watkins heuristics is challenging [CS23], and has only been done for families of elliptic curves that impose restrictions on the relationship between discriminant and conductor [SSW21].

Define

$$\mathcal{F}_{\mathbb{Q}}(H) := \{y^2 = x^3 + ax + b \,:\, |a| < H^{\frac{1}{3}},\, |b| < H^{\frac{1}{2}},\, p^4 \mid a \implies p^6 \nmid b\}.$$

Let

$$F_\Delta(\lambda) := \frac{1}{4}\int_{-1}^{1}\int_{-1}^{1}\begin{cases}1 & \text{if } -16(4\alpha^3+27\beta^2) < \lambda\\ 0 & \text{otherwise}\end{cases} d\alpha\, d\beta.$$

Let $\rho(p,n)$ denote the natural density of $(a,b)\in\mathbb{Z}^2$ such that $E: y^2=x^3+ax+b$'s discriminant to conductor ratio has p-part equal to the p-part of n, i.e., for any prime p and integer n,

$$\rho(p,n) := \lim_{H\to\infty}\frac{1}{4H^{\frac{5}{6}}}\#\left\{(a,b)\in\mathbb{Z}^2 \,:\, |a|^3,|b|^2<H,\ 4a^3+27b^2\neq 0,\ \gcd\left(\frac{\Delta_E}{N_E},p^\infty\right)=\gcd(n,p^\infty)\right\}.$$

The values of $\rho(p,n)$ are the simple rational functions of p and $\gcd(n,p^\infty)$ tabulated in [Cow24b, Table 1.5].

Theorem 3.1 below, which can be viewed as a precise and effective version of the heuristic argument from [BM90, Wat08], gives the distribution of the conductors in the height-ordered family $\mathcal{F}_\mathbb{Q}$ consisting of all elliptic curves over $\mathbb{Q}$ up to isomorphism.

Theorem 3.1 (Conductor distribution of elliptic curves [Cow24b, Thm. 1.7])**.** *For any $\lambda_1>\lambda_0>\frac{4464}{\log H}$, the proportion of elliptic curves $E\in\mathcal{F}_\mathbb{Q}(H)$ whose conductors N_E lie between $\lambda_0 H$ and $\lambda_1 H$ is*

$$\frac{\#\{E\in\mathcal{F}_\mathbb{Q}(H) \,:\, \lambda_0 H<N_E<\lambda_1 H\}}{\#\mathcal{F}_\mathbb{Q}(H)} = \Phi(\lambda_1)-\Phi(\lambda_0)+O((\log H)^{-1+\varepsilon})$$

with

$$\Phi(\lambda) := \frac{\zeta(10)}{\zeta(2)}\sum_{n=1}^{\infty}\left(F_\Delta(n\lambda)-F_\Delta(-n\lambda)\right)\prod_p\frac{\rho(p,n)}{1-p^{-2}}.$$

Theorem 3.1 has applications to the difficult problem of enumerating elliptic curves by conductor. It's expected that $\#\{E\in\mathcal{F}(H) \,:\, N_E<X\}\ll X^{\frac{5}{6}}$ as $H\to\infty$.

Theorem 3.2 (Counting by conductor [Cow24b, Thm. 1.9])**.**

$$X^{\frac{5}{6}} \ll \#\{E\in\mathcal{F}(H) \,:\, N_E<X\} \ll X^{\frac{5}{6}}\left(\frac{H}{X}\right)^{\frac{35}{54}}H^{\frac{7}{324}+\varepsilon}+H^{\frac{1}{2}}.$$

Theorem 3.2 is the strongest bound currently known for enumerating elliptic curves over $\mathbb{Q}$ with conductor at most X and height at most H when

$$\begin{aligned} & H^{\frac{217}{264}+\varepsilon}\approx H^{0.8220}\ll X\ll H^{\frac{53}{60}-\varepsilon}\approx H^{0.8833} \\ \iff\quad & X^{\frac{60}{53}+\varepsilon}\approx X^{1.1321}\ll H\ll X^{\frac{264}{217}-\varepsilon}\approx X^{1.2165}. \end{aligned}$$

If 264/217 is replaced by a larger number then the bound [DK00, Prop. 1] of Duke–Kowalski is better, and if 60/53 is replaced by a smaller number then bounding by $\#\mathcal{F}(H)$ is better.

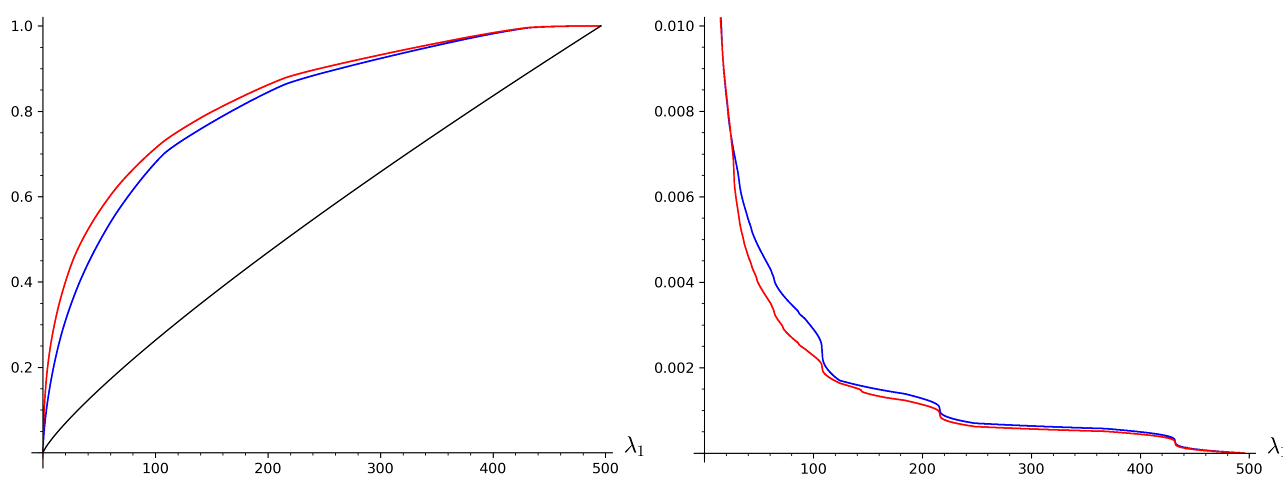

Figure 3.3.
Left: Main term on the right hand side of theorem 3.1 with $\lambda_0=0$ (red: $\mathcal{F}_\mathbb{Q}$, blue: $\mathcal{F}_6$), as well as the function $(\lambda_1/496)^{\frac{5}{6}}$ (black).
Right: Derivative with respect to λ_1 of the main term of theorem 3.1 (red: $\mathcal{F}_\mathbb{Q}$, blue: $\mathcal{F}_6$).
The identity [Cow24b, (27)] was used generate these plots. The code is available at [Cow24a].

The expression on the right hand side of theorem 3.1 may appear to be quite complicated. However it is simple to compute: for any $\lambda_1 > \lambda_0 > 0$ the sum over n is finite, because the summand is 0 whenever $n\lambda_0 > 496$, and the product over p is finite, because $\rho(p,n) = 1 - p^{-2}$ whenever $p \nmid 6n$.

Versions of theorems 3.1 and 3.2 for the family $\mathcal{F}_6$ from (2) are also given in [Cow24b], so as to be able to prove theorem 1.2 on murmurations of elliptic curves.

Figure 3.3 plots the function Φ from theorem 3.1 and its derivative in red, as well as the analogous distributions for the family $\mathcal{F}_6$ in blue. The functions plotted are essentially the cumulative distribution functions (left) and histograms (right) of the multisets $\{N_E/H : E \in \mathcal{F}_{\mathbb{Q}}(H)\}$ and $\{N_E/H : E \in \mathcal{F}_6(H)\}$ as $H \to \infty$. These "histogram functions" are interesting: they're continuous but fail to be differentiable infinitely often.

Genus 2 curves with real multiplication

Genus 2 curves with real multiplication arose naturally in my research via their connection with the degree 2 newforms described in section 4. Elkies and Kumar [EK14] give a nice description of the moduli space of these curves, but it remained difficult to determine the fields of definition of the associated Weierstrass equations. For any one particular point in the moduli space this is straightforward thanks to a theorem of Mestre [Mes91], which says that the obstruction for the existence of a Weierstrass model over a field K can be expressed in terms of whether or not a specific conic with coefficients that are polynomials in the moduli has a K-rational point. However, this conic was too unwieldy to be useful for understanding the behaviour of genus 2 curves with real multiplication in aggregate.

In [CM24], Kimball Martin and I show that, in the case of real multiplication by discriminant 5, this Mestre conic which obstructs the existence of a Weierstrass model can be reduced to the very simple conic

$$x^2 - 5y^2 - (m^2 - 5n^2 - 5)z^2 = 0,$$

where m and n parameterize the rational moduli space given in [EK14].

In [CFM24], Sam Frengley, Kimball Martin, and I prove analogous statements for discriminants 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 44, 53, and 61. We also give generic families (in the sense of [CFM24, Remark 2.1]) in these cases; for $D \geqslant 12$ no such families were previously known. We prove some additional results, in particular that the Mestre obstruction vanishes for all discriminants which are $1 \bmod 8$. Our work involves a mix of theory and computation, and includes search algorithms for finding these sorts of reductions.

Real points on elliptic curves and continued fractions

An elliptic curve is a Diophantine equation of the form $E : y^2 = x^3 + ax + b$. The solutions, i.e. the points on a fixed elliptic curve, form an abelian group.

In [Cow20] I establish a correspondence between the statistics of the real or complex points on an elliptic curve and the statistics of continued fractions. Then, via the theory of continued fractions, I describe the statistical behaviour of points on elliptic curves from various perspectives, e.g. their distributions and their extreme values.

Theorem 3.4 (Lower bound for multiples of $P \in E(\mathbb{R})$ [Cow20, Thm. 1.1])**.** *Suppose that $E/\mathbb{C}$ has periods ω_1 and ω_2, chosen such that $\omega_1 \in \mathbb{R}_{>0}$ and $\operatorname{Im}(\omega_2) > 0$. Then for every point P of infinite order in the unbounded component of $E(\mathbb{R})$, there exist infinitely many n such that*

$$x(nP) > \frac{5}{\omega_1^2}n^2 + O(n^{-2}) \qquad \text{and} \qquad y(nP) > \frac{2 \cdot 5^{\frac{3}{2}}}{\omega_1^3}n^3 + O(n^{-1}).$$

If P is instead a point of infinite order on the bounded component of $E(\mathbb{R})$ (in the case where $E(\mathbb{R})$ has two connected components), then there exist infinitely many n such that

$$x(nP) > \frac{5}{4\omega_1^2}n^2 + O(n^{-2}) \qquad \text{and} \qquad y(nP) > \frac{5^{\frac{3}{2}}}{4\omega_1^3}n^3 + O(n^{-1}).$$

The implied constants depend only on E.

Theorem 3.5 (Distribution of multiples of $P \in E(\mathbb{R})$ [Cow20, Cor. 1.7])**.** *Fix $P_0 = (x_0, y_0) \in E(\mathbb{R})$ and $\varepsilon > 0$. For all $P \in E(\mathbb{R})$ of infinite order, the natural density of integers n for which $(x(nP) - x_0)^2 + (y(nP) - y_0)^2 < \varepsilon^2$ is*

$$\frac{1}{\omega_1\sqrt{y_0^2 + \left(6x_0^2 - \frac{g_2}{2}\right)^2}} \cdot 2\eta(\varepsilon + O(\varepsilon^2)),$$

where $\eta = 1$ if both P and P_0 are on the unbounded component of $E(\mathbb{R})$, $\eta = \frac{1}{2}$ if P is on the bounded component of $E(\mathbb{R})$, and $\eta = 0$ if P_0 is on the bounded component of $E(\mathbb{R})$ but P is not. The implied constant depends only on E and P_0.

Figure 3.6 illustrates theorems 3.4 and 3.5.

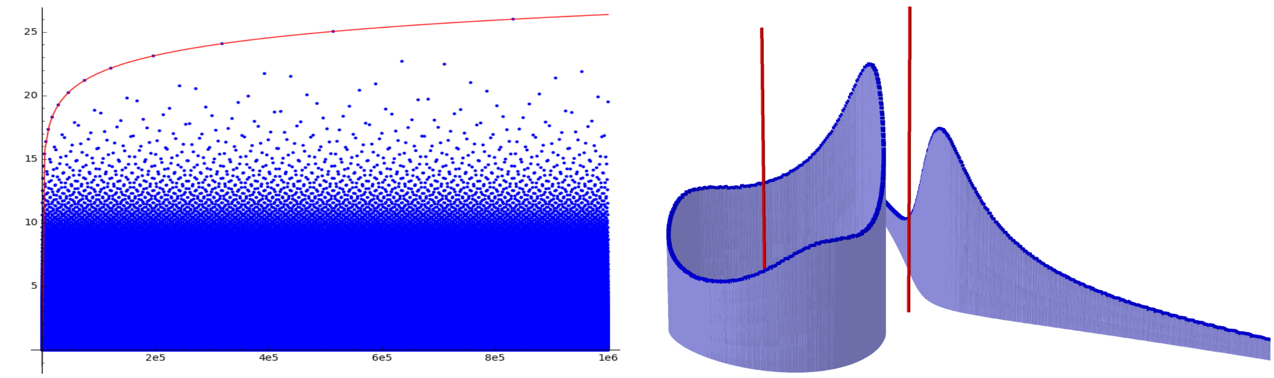

Figure 3.6.
Left: $\{\log(x(nP) + 2) : 1 < n < 10^6\}$ for $P \approx (-0.406, 0.966)$ on $E : y^2 = x^3 + 1$, with the lower bound of theorem 3.4 in red.
Right: Histogram of $\{nP : |n| < 5 \cdot 10^5, \, x(nP) < 1.89\}$ for $P = (0, 0)$ on E37a: $y^2 + y = x^3 - x$, with the poles $(x_0, y_0) = (\pm\sqrt{g_2/12}, 0)$ of the density function from theorem 3.5 shown in red.

[Cow20, §6] gives statistics for Bremner and Macleod's [BM14] equation

$$\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} = N$$

with N a given integer, to be solved for positive integers a, b, c. This equation is well-known for having surprisingly large solutions [ale16].

4. A modular form database from supersingular isogeny graphs

Background

Classical weight 2 *newforms* are complex functions with certain kinds of arithmetic symmetries. They are among the most important objects in number theory, and in many aspects remain quite mysterious.

Newforms can be ordered in a natural way according to a positive integer N called their *level*. Define the *degree* d of a newform to be the degree of the number field K_f generated by the coefficients of its Fourier series.

Modular forms are interesting in their own right, and also because standard "modularity conjectures" predict a correspondence between genus d factors of the "modular Jacobian" $J_0(N)$ — a fundamental object in arithmetic geometry — and weight 2 newforms of level N whose Fourier coefficients are algebraic integers of degree d.

The association between genus 1 modular abelian varieties — elliptic curves — and degree 1 modular forms is an important theorem [Wil95, TW95, BCDT01, DS05]. The literature contains many conjectures and results about the distributions of related invariants [PPVW19, BKL+15, BS15, HS17, Poo18, LR21, SSW21, Gol82, WDE+15, etc.]. However, in many situations it is poorly understood what the correct generalizations for $d \geqslant 2$ should be, and merely formulating conjectures which are plausible is of great interest. Even the basic question asking how many such objects exist with prescribed degree $d \geqslant 2$ is totally mysterious [Ser97, SZ24], whereas there are well established conjectures for the number of elliptic curves with bounded conductor [BM90, Wat08].

My work

In [Cow22a], I designed and implemented an algorithm that computed the Fourier expansions of all trivial nebentypus newforms with degree $d \leqslant 6$ and prime level $N < 2{,}000{,}000$. Moreover, for $4{,}752 < N < 1{,}000{,}000$, the algorithm verified that there are exactly two newform orbits per level with $d \geqslant 7$ (which is quite tricky); these remaining newform orbits were then described with the help of Eran Assaf [Ass24]. The algorithm computes the first N Fourier coefficients [Stu87] in time $O(N^{2+\varepsilon})$ and space $O(N^{1+\varepsilon})$, improving on the $O(N^{3+\varepsilon})$ runtime of previous methods [BBB+21].

The database generated by [Cow22a] builds on many existing databases, like the Antwerp tables [BK75], Cremona's database of elliptic curves [CMF+24, Cre97], and the LMFDB [LMF] which, prior to uploading my data, contained all newforms with level $N \leqslant 10{,}000$ [BBB+21].

Table 4.1 summarizes the dataset as a whole. You can click here to see the data on the LMFDB.

				(Old data)		(New data)			
Deg	Disc(K_f)	Gal$(K_f/\mathbb{Q})$	Total	$1 — 10^4$ +	$1 — 10^4$ −	$10^4 — 10^6$ +	$10^4 — 10^6$ −	$10^6 — 2 \cdot 10^6$ +	$10^6 — 2 \cdot 10^6$ −
1	1	C_1	15578	140	189	4364	4479	3206	3200
2	5	C_2	3044	93	65	938	962	508	478
	8	C_2	379	18	19	115	127	54	46
	13	C_2	59	4	9	21	19	1	5
	12	C_2	18		1	8	6	1	2
	21	C_2	5		1	1	2		1
	17	C_2	1			1			
3	49	C_3	154	19	15	40	50	20	10
	229	S_3	29	6	2	13	7		1
	148	S_3	18	7	5	3	3		
	81	C_3	16	2	1	2	11		
	257	S_3	16	3	6	4	2		1
	169	C_3	11	1	1	2	4	1	2
	321	S_3	3		2		1		
4	725	D_4	22	10	6	2	3		1
	1957	S_4	6	2	2	1	1		
	2777	S_4	5	2	1		2		
	8768	D_4	1			1			
5	70601	S_5	3	2			1		
	11^4	C_5	1				1		
6	13^5	C_6	1				1		

Table 4.1. Number of prime level newforms by degree, discriminant, and Atkin–Lehner sign.

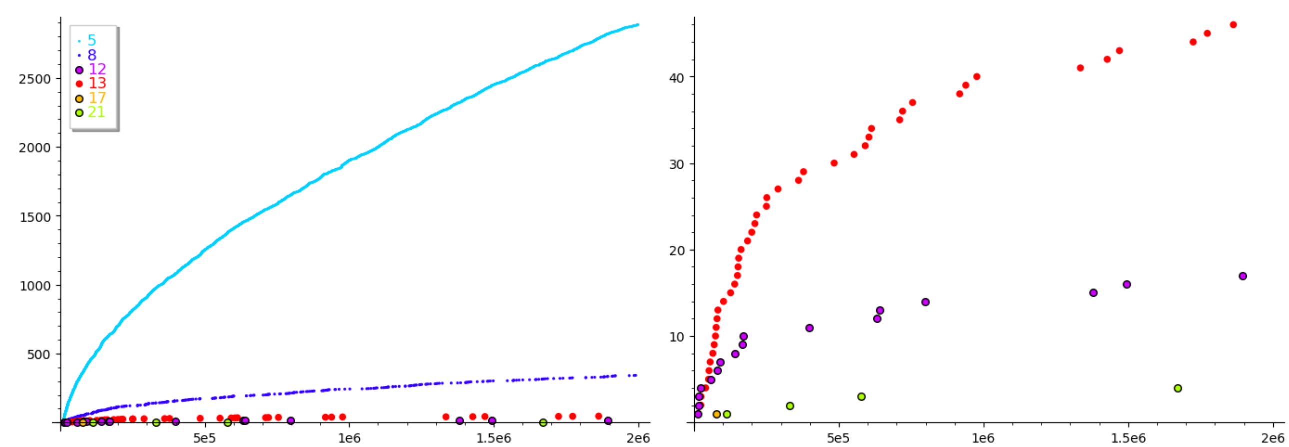

Figure 4.2. Number of degree 2 forms with prescribed discriminant and prime level between 10^4 and X, as a function of X. The graph on the right excludes discriminants 5 and 8.

In [CM23], Kimball Martin and I investigate this new modular form data. As one of many examples of how the dataset enables a better understanding of newforms, table 4.1, figure 4.2, and heuristics based on the geometry of associated moduli spaces [EK14] lead us to conjecture that 100% of degree 2 newforms f of prime level have $K_f = \mathbb{Q}(\sqrt{5})$. Conjectures based on my data are also formulated by [DO25] and [DS25].

The algorithm

The main idea of the algorithm in [Cow22a] comes from Mestre's Méthode des Graphes [Mes86], in which he relates the Fourier expansions of weight 2 newforms of prime level to "supersingular isogeny graphs". These graphs have recently been of independent interest because of their applications in cryptography [CLG09, JDF11, EHL+18, ACNL+23, CD23, etc.].

The relationship [Mes86] presents between supersingular isogeny graphs and weight 2 newforms depends on a trace formula: the action of the Hecke operator T_ℓ on the complex vector space $S_2(N)$ of weight 2 newforms of level N can be represented as the adjacency matrix of the supersingular ℓ-isogeny graph. My algorithm finds simultaneous eigenvectors of these matrices, and then uses a formula from Mestre's work to compute the associated Fourier expansions.

In designing the algorithm, I extended Wiedemann's algorithm [Wie86] to compute characteristic polynomials, I implemented a method for computing the Fourier expansion of the modular j function over finite fields which is much faster than existing implementations, I designed a method to find all the low degree eigenvectors of Hecke operators over $\mathbb{Z}$ using only knowledge of their characteristic polynomials over finite fields, and I designed a method to check that, besides the aforementioned low degree factors, the Hecke modules were irreducible, again only using knowledge of the Hecke operators over finite fields. This last part, checking irreducibility, is challenging. For example, it involved the design and implementation of a technical quadratic time algorithm for a manifestation of the subset-sum problem, which is NP-complete in general.

Extensions

Constructions similar to [Mes86] exist in many other settings. I have already computed datasets of modular forms with level of the form $2p$, $3p$, or $4p$, and I have implemented a variation which computes q-expansions to shallow depths for squarefree levels. Many other generalizations, e.g. using modular symbols [Cre97, Boo24], or with applications to Hilbert modular forms [HTV25], are possible; the algorithm is fundamentally one for quickly finding low-degree eigenvectors of sparse integer matrices, which many problems can be recast as.

In work in progress with Noam Elkies, we generate, from the q-expansions in the database defined over $\mathbb{Q}(\sqrt{5})$, Weierstrass models of the associated genus 2 curves with real multiplication by discriminant 5. We develop a variety of theoretical and computational techniques to do this for every form of this sort in the database.

An explicitly statistical and probabilistic investigation of the database, joint with Kimball Martin, is in preparation [CM]. A working manuscript and slides are available on my personal webpage. Both the novel statistical methodology, rooted in information theory, and the surprising discoveries presented in this manuscript form a basis for future work. In [Cow25b], I use these statistical methods, along with a new bound on the left tail of the uniform multinomial's relative entropy (a.k.a. Kulback–Leibler divergence), to discover an unusual phenomenon regarding the equidistribution of primes in arithmetic progressions.

References

[ACNL+23] Sarah Arpin, Catalina Camacho-Navarro, Kristin Lauter, Joelle Lim, Kristina Nelson, Travis Scholl, and Jana Sotáková, *Adventures in supersingularland*, Exp. Math. **32** (2023), no. 2, 241–268.

[ale16] alex alexeq, *Estimating the size of solutions of a diophantine equation*, `https://mathoverflow.net/questions/227713/estimating-the-size-of-solutions-of-a-diophantine-equation`, 2016.

[Ass24] Eran Assaf, *A note on the trace formula*, arXiv 2311.03523, 2024.

[BBB+21] Alex J. Best, Jonathan Bober, Andrew R. Booker, Edgar Costa, John E. Cremona, Maarten Derickx, Min Lee, David Lowry-Duda, David Roe, Andrew V. Sutherland, and John Voight, *Computing classical modular forms*, Arithmetic geometry, number theory, and computation, Simons Symp., Springer, Cham, [2021] ©2021, pp. 131–213.

[BBC+20] Renee Bell, Clifford Blakestad, Alina Carmen Cojocaru, Alexander Cowan, Nathan Jones, Vlad Matei, Geoffrey Smith, and Isabel Vogt, *Constants in Titchmarsh divisor problems for elliptic curves*, Res. Number Theory **6** (2020), no. 1, Paper No. 1, 24.

[BBLLD23] Jonathan Bober, Andrew R. Booker, Min Lee, and David Lowry-Duda, *Murmurations of modular forms in the weight aspect*, arXiv 2310.07746, 2023.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[BGR19] Michael A. Bennett, Adela Gherga, and Andrew Rechnitzer, *Computing elliptic curves over* $\mathbb{Q}$, Math. Comp. **88** (2019), no. 317, 1341–1390.

[BK75] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Lecture Notes in Mathematics, Vol. 476, Springer-Verlag, Berlin-New York, 1975.

[BKL+15] Manjul Bhargava, Daniel M. Kane, Hendrik W. Lenstra, Jr., Bjorn Poonen, and Eric Rains, *Modeling the distribution of ranks, Selmer groups, and Shafarevich-Tate groups of elliptic curves*, Camb. J. Math. **3** (2015), no. 3, 275–321.

[BLLD+24] Andrew R. Booker, Min Lee, David Lowry-Duda, Andrei Seymour-Howell, and Nina Zubrilina, *Murmurations of Maass forms*, arXiv 2409.00765, 2024.

[BM90] Armand Brumer and Oisín McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 375–382.

[BM14] Andrew Bremner and Allan Macleod, *An unusual cubic representation problem*, Ann. Math. Inform. **43** (2014), 29–41.

[Boo24] Krit Boonsiriseth, *Performance engineering of modular symbols*, https://hdl.handle.net/1721.1/156828, 2024.

[BS15] Manjul Bhargava and Arul Shankar, *Binary quartic forms having bounded invariants, and the boundedness of the average rank of elliptic curves*, Ann. of Math. (2) **181** (2015), no. 1, 191–242.

[CD23] Wouter Castryck and Thomas Decru, *An efficient key recovery attack on SIDH*, Advances in cryptology—EUROCRYPT 2023. Part V, Lecture Notes in Comput. Sci., vol. 14008, Springer, Cham, [2023] ©2023, pp. 423–447.

[CFK+05] J. B. Conrey, D. W. Farmer, J. P. Keating, M. O. Rubinstein, and N. C. Snaith, *Integral moments of L-functions*, Proc. London Math. Soc. (3) **91** (2005), no. 1, 33–104.

[CFM24] Alex Cowan, Sam Frengley, and Kimball Martin, *Generic models for genus 2 curves with real multiplication*, arXiv 2403.03191, 2024.

[CLG09] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren, *Cryptographic hash functions from expander graphs*, J. Cryptology **22** (2009), no. 1, 93–113.

[CM] Alex Cowan and Kimball Martin, *Statistics of modular forms with small rationality fields*, In preparation.

[CM23] ———, *Counting modular forms by rationality field*, arXiv 2301.10357, 2023.

[CM24] ———, *Moduli for rational genus 2 curves with real multiplication for discriminant 5*, J. Théor. Nombres Bordeaux **36** (2024), no. 2, 493–525.

[CMF+24] John Cremona, Marcus Mo, Isuru Fernando, Fernando Perez, François Bissey, William Stein, Dima Pasechnik, E. M. Bray, qed777, Giovanni Mascellani, Antonio Rojas, abergeron, Jerry James, Keno Fischer, and Moritz Firsching, *JohnCremona/eclib: 20240408*, https://doi.org/10.5281/zenodo.10950409, April 2024.

[Cow20] Alex Cowan, *The distribution of multiples of real points on an elliptic curve*, J. Number Theory **211** (2020), 530–544.

[Cow21] ———, *Conjecture: 100% of elliptic surfaces over $\mathbb{Q}$ have rank zero*, Arithmetic geometry, number theory, and computation, Simons Symp., Springer, Cham, [2021] ©2021, pp. 335–342.

[Cow22a] ———, *Computing newforms using supersingular isogeny graphs*, Res. Number Theory **8** (2022), no. 4, Paper No. 96.

[Cow22b] ———, *Non-random behavior in sums of modular symbols*, Int. J. Number Theory **18** (2022), no. 4, 879–903.

[Cow23] ———, *Murmurations and explicit formulas*, arXiv 2306.10425, 2023.

[Cow24a] ———, *Conductor distribution code*, https://github.com/thealexcowan/conductordistribution, 2024.

[Cow24b] ———, *Conductor distributions of elliptic curves*, arXiv 2408.09745, 2024.

[Cow24c] ———, *Kronecker symbol murmurations code*, https://github.com/thealexcowan/murmurations, 2024.

[Cow24d] ———, *Murmurations and ratios conjectures*, arXiv 2408.12723, 2024.

[Cow25a] ———, *On the mean value of GL_1 and GL_2 L-functions, with applications to murmurations*, arXiv 2504.09944, 2025.

[Cow25b] ———, *The relative entropy of primes in arithmetic progressions is really small*, arXiv 2504.20691, 2025.

[Cow25c] ———, *A twisted additive divisor problem*, Journal of Number Theory **266** (2025), 1–32.

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[CS07] J. B. Conrey and N. C. Snaith, *Applications of the L-functions ratios conjectures*, Proc. Lond. Math. Soc. (3) **94** (2007), no. 3, 594–646.

[CS23] John E. Cremona and Mohammad Sadek, *Local and global densities for Weierstrass models of elliptic curves*, Math. Res. Lett. **30** (2023), no. 2, 413–461.

[DFI02] W. Duke, J. B. Friedlander, and H. Iwaniec, *The subconvexity problem for Artin L-functions*, Invent. Math. **149** (2002), no. 3, 489–577.

[DHP15] Chantal David, Duc Khiem Huynh, and James Parks, *One-level density of families of elliptic curves and the Ratios Conjecture*, Res. Number Theory **1** (2015), Paper No. 6, 37.

[DK00] W. Duke and E. Kowalski, *A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations*, Invent. Math. **139** (2000), no. 1, 1–39, With an appendix by Dinakar Ramakrishnan.

[DO25] Maarten Derickx and Petar Orlić, *Morphisms on the modular curve $X_0(p)$ and degree 6 points*, arXiv 2506.21166, 2025.

[DS05] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Graduate Texts in Mathematics, vol. 228, Springer-Verlag, New York, 2005.

[DS25] Maarten Derickx and Michael Stoll, *Prime order torsion on elliptic curves over number fields. Part I: Asymptotics*, arXiv 2505.14109, 2025.

[EHL$^+$18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit, *Supersingular isogeny graphs and endomorphism rings: reductions and solutions*, Advances in cryptology—EUROCRYPT 2018. Part III, Lecture Notes in Comput. Sci., vol. 10822, Springer, Cham, 2018, pp. 329–368.

[EK14] Noam Elkies and Abhinav Kumar, *K3 surfaces and equations for Hilbert modular surfaces*, Algebra Number Theory **8** (2014), no. 10, 2297–2411.

[Gol82] Dorian Goldfeld, *Sur les produits partiels eulériens attachés aux courbes elliptiques*, C. R. Acad. Sci. Paris Sér. I Math. **294** (1982), no. 14, 471–474.

[HLN21] Jeff Hoffstein, Min Lee, and Maria Nastasescu, *First moments of Rankin-Selberg convolutions of automorphic forms on* $\mathrm{GL}(2)$, Res. Number Theory **7** (2021), no. 4, Paper No. 60, 44.

[HLOP24] Yang-Hui He, Kyu-Hwan Lee, Thomas Oliver, and Alexey Pozdnyakov, *Murmurations of elliptic curves*, Experimental Mathematics (2024), 1–13.

[HS17] Robert Harron and Andrew Snowden, *Counting elliptic curves with prescribed torsion*, J. Reine Angew. Math. **729** (2017), 151–170.

[HTV25] Jeffery Hein, Gonzalo Tornaria, and John Voight, *Computing hilbert modular forms as orthogonal modular forms*, arXiv 2506.21981, 2025.

[Iwa02] Henryk Iwaniec, *Spectral methods of automorphic forms*, second ed., Graduate Studies in Mathematics, vol. 53, American Mathematical Society, Providence, RI; Revista Matemática Iberoamericana, Madrid, 2002.

[JDF11] David Jao and Luca De Feo, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies*, Post-quantum cryptography, Lecture Notes in Comput. Sci., vol. 7071, Springer, Heidelberg, 2011, pp. 19–34.

[Jut81] M. Jutila, *On the mean value of* $L(\frac{1}{2}, \chi)$ *for real characters*, Analysis **1** (1981), no. 2, 149–161.

[Jut96] Matti Jutila, *The additive divisor problem and its analogs for Fourier coefficients of cusp forms. I*, Math. Z. **223** (1996), no. 3, 435–461.

[LMF] The LMFDB Collaboration, *The L-functions and modular forms database*, http://www.lmfdb.org.

[LOP25] Kyu-Hwan Lee, Thomas Oliver, and Alexey Pozdnyakov, *Murmurations of Dirichlet characters*, Int. Math. Res. Not. IMRN (2025), no. 1, Paper No. rnae277, 28.

[LR21] Álvaro Lozano-Robledo, *A probabilistic model for the distribution of ranks of elliptic curves over* $\mathbb{Q}$, J. Number Theory **221** (2021), 270–338.

[Mes86] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), Nagoya Univ., Nagoya, 1986, pp. 217–242.

[Mes91] Jean-François Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, Effective methods in algebraic geometry (Castiglioncello, 1990), Progr. Math., vol. 94, Birkhäuser Boston, Boston, MA, 1991, pp. 313–334.

[Mic04] P. Michel, *The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points*, Ann. of Math. (2) **160** (2004), no. 1, 185–236.

[Mic07] Philippe Michel, *Analytic number theory and families of automorphic L-functions*, Automorphic forms and applications, IAS/Park City Math. Ser., vol. 12, Amer. Math. Soc., Providence, RI, 2007, pp. 181–295.

[Mot94] Yōichi Motohashi, *The binary additive divisor problem*, Ann. Sci. École Norm. Sup. (4) **27** (1994), no. 5, 529–572.

[MR16] Barry Mazur and Karl Rubin, *The statistical behavior of modular symbols and arithmetic conjectures*, http://www.math.harvard.edu/~mazur/papers/heuristics.Toronto.12.pdf, 2016.

[MR20] Barry Mazur and Karl Rubin, *Arithmetic conjectures suggested by the statistical behavior of modular symbols*, arXiv 1910.12798, 2020.

[MV10] Philippe Michel and Akshay Venkatesh, *The subconvexity problem for* GL_2, Publ. Math. Inst. Hautes Études Sci. (2010), no. 111, 171–271.

[Nel19] Paul D. Nelson, *Eisenstein series and the cubic moment for* PGL_2, 2019, arXiv 1911.06310.

[Poo18] Bjorn Poonen, *Heuristics for the arithmetic of elliptic curves*, Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. II. Invited lectures, World Sci. Publ., Hackensack, NJ, 2018, pp. 399–414.

[PPVW19] Jennifer Park, Bjorn Poonen, John Voight, and Melanie Matchett Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) **21** (2019), no. 9, 2859–2903.

[Ser97] Jean-Pierre Serre, *Répartition asymptotique des valeurs propres de l'opérateur de Hecke* T_p, J. Amer. Math. Soc. **10** (1997), no. 1, 75–102.

[SS25] Will Sawin and Andrew V. Sutherland, *Murmurations for elliptic curves ordered by height*, arXiv 2504.12295, 2025.

[SSW21] Ananth N. Shankar, Arul Shankar, and Xiaoheng Wang, *Large families of elliptic curves ordered by conductor*, Compos. Math. **157** (2021), no. 7, 1538–1583.

[Sta83] E. Stankus, *The mean value of* $L(1/2, \chi_d)$ *for* $d \equiv l \pmod{D}$, Litovsk. Mat. Sb. **23** (1983), no. 2, 169–177.

[Stu87] Jacob Sturm, *On the congruence of modular forms*, Number theory (New York, 1984–1985), Lecture Notes in Math., vol. 1240, Springer, Berlin, 1987, pp. 275–280.

[Sut22] Andrew Sutherland, *Letter to Michael Rubinstein and Peter Sarnak*, `https://math.mit.edu/~drew/RubinsteinSarnakLetter.pdf`, 2022.

[SZ24] Peter Sarnak and Nina Zubrilina, *Convergence to the Plancherel measure of Hecke eigenvalues*, Acta Arithmetica **214** (2024), 191–213 (English (US)), Publisher Copyright: © Instytut Matematyczny PAN, 2024.

[TW95] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.

[VT81] A. I. Vinogradov and L. A. Takhtadzhyan, *Analogues of the Vinogradov-Gauss formula on the critical line*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **109** (1981), 41–82, 180–181, 182–183, Differential geometry, Lie groups and mechanics, IV.

[VT84] ———, *The zeta function of the additive divisor problem and spectral expansion of the automorphic Laplacian*, vol. 134, 1984, Automorphic functions and number theory, II, pp. 84–116.

[Wan25] Zeyu Wang, *Murmurations of Hecke L-functions of imaginary quadratic fields*, arXiv 2503.17967, 2025.

[Wat08] Mark Watkins, *Some heuristics about elliptic curves*, Experiment. Math. **17** (2008), no. 1, 105–125.

[WDE+15] Mark Watkins, Stephen Donnelly, Noam D. Elkies, Tom Fisher, Andrew Granville, and Nicholas F. Rogers, *Ranks of quadratic twists of elliptic curves*, Numéro consacré au trimestre "Méthodes arithmétiques et applications", automne 2013, Publ. Math. Besançon Algèbre Théorie Nr., vol. 2014/2, Presses Univ. Franche-Comté, Besançon, 2015, pp. 63–98.

[Wie86] Douglas H. Wiedemann, *Solving sparse linear equations over finite fields*, IEEE Trans. Inform. Theory **32** (1986), no. 1, 54–62.

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[Wu19] Han Wu, *Deducing Selberg trace formula via Rankin-Selberg method for* GL_2, Trans. Amer. Math. Soc. **372** (2019), no. 12, 8507–8551.

[Zag81] Don Zagier, *The Rankin-Selberg method for automorphic functions which are not of rapid decay*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 415–437 (1982).

[Zub23] Nina Zubrilina, *Murmurations*, arXiv 2310.07681, 2023.