RESEARCH STATEMENT

ALEX COWAN

I do analytic number theory, computational number theory, and arithmetic statistics.

Section 1 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 generated is 200 times larger than the one before it, and is available on the widely-used L-functions and Modular Forms Database so as to be easily and readily accessible to number theorists broadly. My algorithm can be generalized to compute many other kinds of interesting arithmetic data.

Section 2 presents [Cow24b], wherein I use analytic techniques to study the phenomenon of "murmurations" which has been of great interest since its discovery two years ago. My work connects murmurations to the field of random matrix theory, the first time this connection has been made in the literature. To demonstrate how existing results for a specific problem in random matrix theory can be used to explain murmurations, I give proofs of murmurations, conditional on standard conjectures, for four cases.

Section 3 presents [Cow25], 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 last year at Harvard; notes in the form of video lectures are available on my website and on YouTube.

Section 4 presents a selection of papers of mine in arithmetic geometry, not primarily computational or analytic in nature, with statistical foci.

Contents

1. 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 called their *level*. The *q-expansion* of a newform is its Fourier expansion (guaranteed to have algebraic integer coefficients), and is in practice the most convenient way of describing it. For example, setting $q \coloneqq e^{2\pi i z}$, the first newform, which has level 11, is

$$f_{11}(z) = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 0q^8 - 2q^9 + \dots.$$

Modular forms are interesting in their own right, but 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. For example, the p^{th} Fourier coefficient of f_{11} above is equal to p minus the number of solutions mod p to the elliptic curve $y^2 + y = x^3 - x^2 - 10x - 20$. The connection between newforms of this type and arithmetic geometry is, in particular, the crux of the proof of Fermat's last theorem [DS05].

Let $S_2(N)$ be the complex vector space spanned by the weight 2 newforms of prime level N. Define the *degree* d of a newform of $S_2(N)$ to be the degree of the number field K_f its Fourier coefficients generate, or, equivalently, the size of its Galois orbit. For example, $S_2(11)$ is one-dimensional and f_{11} above has degree 1.

My work

In [Cow22a], I designed and implemented an algorithm that computed the q-expansions of all trivial nebentypus newforms with degree $d \leq 6$ 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 $d \geq 7$ (which is quite tricky!); these remaining newform orbits were then described with the help of [Ass24]. The algorithm computes q-expansions up to the Sturm bound [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 [LMF24] which, prior to uploading my data, contained all newforms with level $N \leq 10{,}000$ [BBB+21].

The data

The association between genus 1 modular abelian varieties — elliptic curves — and degree 1 modular forms is a theorem [Wil95, TW95, BCDT01]. The literature contains many conjectures and theorems 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 $d \geq 2$ 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 $d \geq 2$ is totally mysterious [Ser97, SZ24], whereas there are well established conjectures for the number of elliptic curves with bounded conductor [BM90, Wat08].

In light of this gap in understanding, databases of newforms of $S_2(N)$ are very helpful: the many examples they provide allow one to observe generalizations of phenomena which occur in the genus 1 case, and to then formulate heuristics and conjectures. Table 1.1 summarizes the dataset as a whole.

				(Old data)		(New data)			
Deg	Disc(K_f)	Gal($K_f/\mathbb{Q}$)	Total	$1 — 10^4$		$10^4 — 10^6$		$10^6 — 2 \cdot 10^6$	
				+	−	+	−	+	−
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 1.1. Number of prime level newforms by degree, discriminant, and Atkin–Lehner sign.

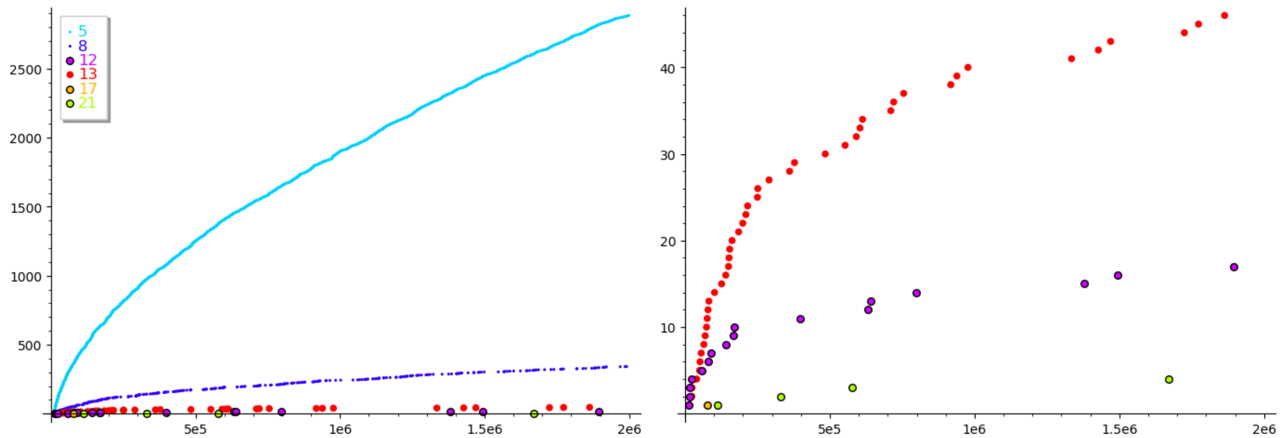

Figure 1.2. Counts of degree 2 forms by discriminant. The graph on the right excludes discriminants 5 and 8.

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 1.1, Figure 1.2, 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 $K_f = \mathbb{Q}(\sqrt{5})$.

The algorithm

The main idea of the algorithm in [Cow22a] comes from Mestre's Méthode des Graphes [Mes86], in which he relates the q-expansion 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 space $S_2(N)$ 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 q-expansions.

In designing the algorithm, I extended Wiedemann's algorithm [Wie86] to compute characteristic polynomials, I implemented a method for computing the q-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 quite 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

The work presented in this section offers many tempting avenues for future research. Here are three that I'm currently pursuing.

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, or with applications to Hilbert modular forms, are possible; the algorithm is fundamentally one for quickly finding low-degree eigenvectors of sparse integer matrices, which many problems can be recast as.

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 and the surprising discoveries presented in this manuscript form a basis for continued future work.

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 in the database. The resulting data will be contributed to the LMFDB, supporting the LMFDB's interest in containing related arithmetic objects wherever possible.

2. Murmurations

A collaboration of data scientists [HLOP22] 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. 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]. The topic is currently of great interest [Chi24].

In [Cow24b] I connect murmurations to distributions of low-lying zeros in families of L-functions. These distributions are studied in the field of random matrix theory [ILS00, CS07], and I describe a process by which results in that field such as [Mil08, Mil09, HMM11, GJM+10, MP12, FM15, BBJ+24, DHP15, Čec24] can be adapted to explain murmurations of elliptic curves and other arithmetic objects.

Prior to [Cow24b], murmurations had been proven to exist in only three cases [Zub23, LOP23, BBLLD23], with the latter two assuming the generalized Riemann hypothesis (GRH). The connection between murmurations and L-function zeros was totally absent from the literature outside of my short note [Cow23].

To exemplify the underlying method, [Cow24b] proves murmurations in four cases: quadratic Dirichlet characters under GRH, holomorphic newforms of prescribed weight and sign under GRH, quadratic twists of elliptic curves under a "ratios conjecture", and elliptic curves ordered by height under a ratios conjecture and a root number equidistribution hypothesis.

Applying [Cow24b]'s method in the simple and computationally tractable case 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 2.1 visualizes (1) in the case $\mathcal{F}_\chi \coloneqq \{d : 95{,}000 < d < 105{,}000,\ d \text{ a fundamental discriminant}\}$. See [Cow24b, Thm. 1.2, Thm. 2.4] for more precise statements, including error terms and their provenance.

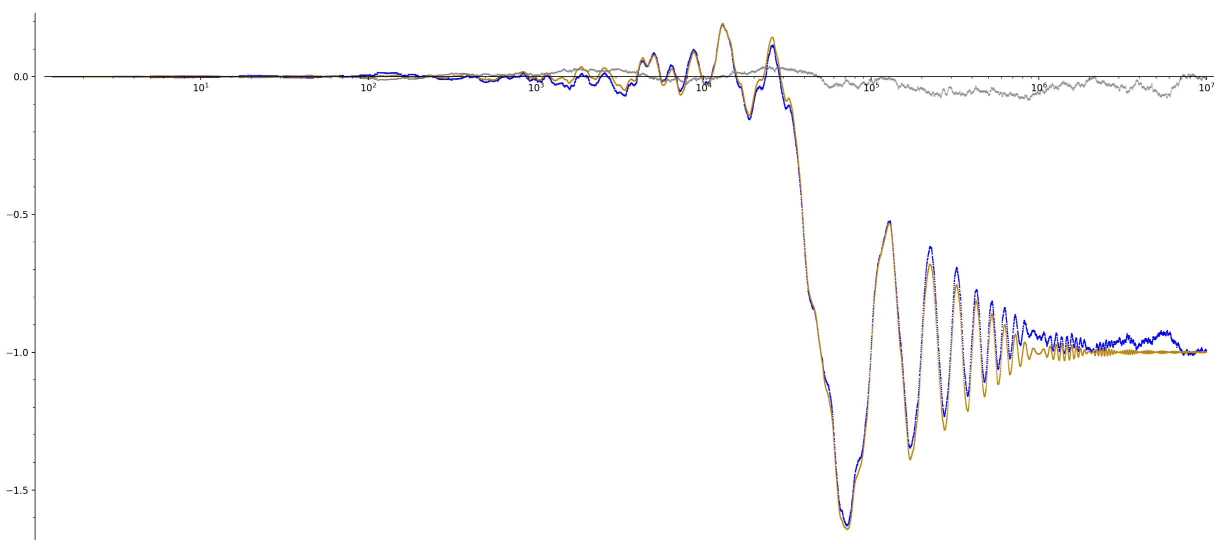

Figure 2.1. For $T = 900$ and $\varepsilon = 0.1$, the left and right hand sides of (1) in blue and gold respectively, as well as their difference in grey, as functions of X. The integral in (1) is approximated by Riemann sum evaluated at 180,000 equally-spaced points. In this example $\#\mathcal{F}_\chi = 3038$. My code is available at [Cow24d].

Murmurations of elliptic curves were the initial catalyst for the study of the topic in general [HLOP22]. Prior to [Cow24b], there were no predictions at all for the precise way in which the average value of the number of points mod p oscillated, how many curves needed to be averaged for the oscillations to appear, the range in which oscillations were visible, etc.

Stating Theorem 2.2, about murmurations for elliptic curves ordered by height, requires some notation. Let $\mathcal{F}(H)$ denote the family of elliptic curves

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

Roughly speaking, $\mathcal{F}(H)$ consists of elliptic curves with height less than H and good or "pretty good" reduction at 2 and 3. The quantities α_p and $\overline{\alpha}_p$ featuring in Theorem 2.2 are 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 2.2. *Let $\mathcal{F}(H)$ be the family of elliptic curves ordered by height from* [Cow24b, Def. 3.1]*, $\omega \in \{\pm 1\}$, and $\mathcal{F}(H)^\omega \coloneqq \{E \in \mathcal{F}(H) \,:\, \omega_E = \omega\}$. Assume that loc. cit. (7), (8), and the ratios conjecture* [DHP15, Conj. 3.7] *hold with $\mathcal{F}(H)$ replaced with $\mathcal{F}(H)^\omega$. For any H, y, T, ε such that $0 < \varepsilon < \frac{1}{2}$ and $(Hy)^{\frac{1}{2}+\varepsilon} \ll T < Hy$,*

$$\begin{aligned}
&\frac{1}{\#\mathcal{F}(H)^\omega} \sum_{E \in \mathcal{F}(H)^\omega} \frac{1}{\sqrt{Hy}} \sum_{\substack{p^k < Hy \\ p \nmid N_E}} \left(\alpha_p^k + \overline{\alpha}_p^k\right) \log p \\
&\qquad = \frac{\omega}{2\pi i} \int_{\mathbb{R}} \int_{\frac{1}{2}+\varepsilon-iT}^{\frac{1}{2}+\varepsilon+iT} \frac{\Gamma(\frac{3}{2}-s)}{\Gamma(\frac{1}{2}+s)} \zeta(2s) A(\tfrac{1}{2}-s, s-\tfrac{1}{2}) \left(4\pi^2 \frac{y}{\lambda}\right)^{s-\frac{1}{2}} \frac{ds}{s} F_N'(\lambda)\, d\lambda \\
&\qquad\quad - \frac{1}{\sqrt{Hy}} \sum_{p^k < \sqrt{Hy}} \log p + O\Big(H^\varepsilon y^\varepsilon T^\varepsilon \mathcal{R}(H) \#\mathcal{F}(H)^{-1} + (\log H)^{-\frac{5}{6}}\Big),
\end{aligned}$$

where $A(\alpha,\gamma)$, F_N, and $\mathcal{R}(H)$ are defined in loc. cit. Def. 3.2, Def. 3.9, and Thm. 3.4.

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 2.2, 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 $\mathcal{F}(H)$, is an interesting and difficult problem, and was the subject of the separate paper [Cow24a] motivated by Theorem 2.2. I present that paper in Section 4.

The random matrix theory side of the link laid out in [Cow24b] is better understood than the murmurations side; some random matrix theory papers describe a "recipe" [CS07]. Though [Cow24b] could be used to prove murmurations in many more cases, my view is that the most natural next step in my work on murmurations is to translate what's known by random matrix theorists into an understanding of the phenomenon of murmurations as a whole — a similar "recipe".

3. 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 [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 [Cow25], I show, with some restrictions on the Dirichlet characters χ, ψ and the complex numbers u, v, that

Theorem 3.1.

$$\begin{aligned}
\sum_{n=1}^{X} \frac{\sigma_{2u}(n,\chi)\sigma_{2v}(n-k,\psi)}{n^{u+v}} &= \frac{L(1-2u,\chi)L(1-2v,\psi)}{L(2-2u-2v,\chi\psi)} \sigma_{-1+2u+2v}(k,\chi\psi) \frac{X^{1-u-v}}{1-u-v} \\
&\quad + \frac{L(1+2u,\overline{\chi})L(1+2v,\overline{\psi})}{L(2+2u+2v,\overline{\chi\psi})} \sigma_{-1-2u-2v}(k,\overline{\chi\psi}) \frac{X^{1+u+v}}{1+u+v} \frac{\tau(\overline{\chi\psi})\chi\psi(k)}{\tau(\overline{\chi})\tau(\overline{\psi})} \\
&\quad + O\Big(X^{1+|\Re(u)|+|\Re(v)|-\frac{1+2|\Re(u)|+2|\Re(v)|}{3+|\Re(u+v)|+|\Re(u-v)|}+\varepsilon}\Big)
\end{aligned}$$

as $X \to \infty$.

This is proved by purely analytic techniques: an automorphic function which encodes the sum on the left is constructed and then expressed as a combination of eigenfunctions of the Laplacian on a hyperbolic manifold. The analysis that's done to establish Theorem 3.1 generalizes the key steps of many well-known results, e.g. [VT84, Jut96, DFI02, Mic04]. This analysis is quite involved, and in previous work there had always been extra simplifying assumptions imposed on χ, ψ, u, and v. Even the very general treatments of these sorts of problems [MV10, Nel19, Wu19, HLN21] don't cover the case done in Theorem 3.1.

A key ingredient in [Cow25] 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 3.1 is unusually small compared to the main term for certain admissible choices of u and v. Previous work had always observed a power savings of $\frac{1}{3}$, but loosening the restrictions on u and v allows the power savings to be larger than this, both in an absolute and a relative sense. The error term is obtained using the best technique currently known, the "spectral large sieve", and the additional power saving is a natural consequence of some of the generalizations made in Theorem 3.1 relative to previous work.

In general, 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, MR19]. As part of the topics course I taught last fall I gave a version of Theorem 3.1 involving holomorphic Eisenstein series, also requiring automorphic regularization, which seems to have not yet appeared in the literature.

4. Arithmetic geometry

I have several papers [Cow20, BBC+20, Cow21, CM22, CFM24, Cow24a] falling under the broad umbrella of arithmetic geometry that are not primarily computational or analytic in nature. This section presents [Cow20], [CM22, CFM24], and [Cow24a].

Real points on elliptic curves and continued fractions

An elliptic curve is a Diophantine equation of the form $E : y^2 = x^3 + ax + b$. These equations and their solutions are very important in modern number theory. 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. Figure 4.1 illustrates two examples.

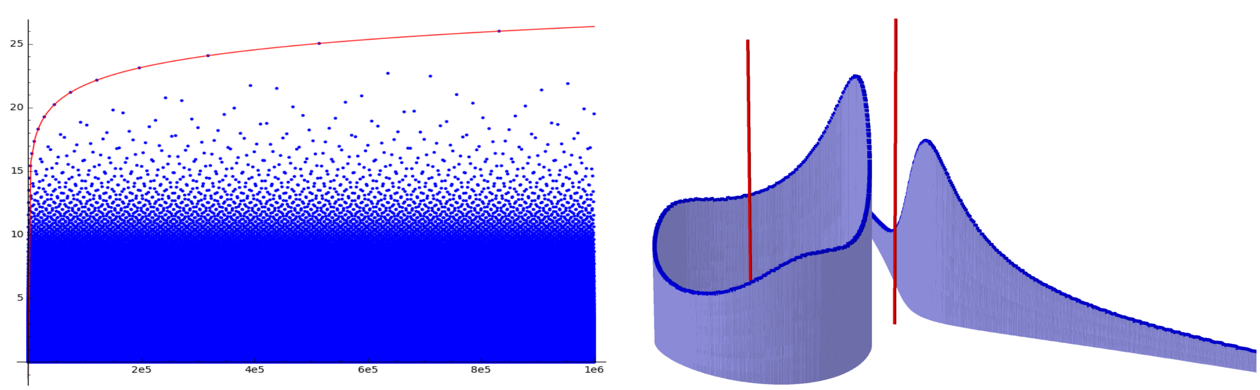

Figure 4.1. How large multiples of a fixed point get (left), and the distribution of those multiples (right).

The plot on the left of Figure 4.1 shows points $(n, \log(x(nP)+2))$ for $P \approx (-0.406, 0.966)$ on $E : y^2 = x^3+1$, i.e. it captures how large the multiples of a fixed point P get. The red curve is the lower(!) bound of [Cow20, Thm. 1.1]:

$$x(nP) > \frac{5}{\omega_1^2}n^2 + O(n^{-2})$$

for infinitely many n, where ω_1 is the positive real period of E.

The plot on the right of Figure 4.1 shows $\{nP : -5 \cdot 10^5 < n < 5 \cdot 10^5,\ x(nP) < 1.89\}$ for $P = (0, 8)$ on E37a: $y^2 = 4x^3 - 64x + 64$, i.e. the distribution of the multiples of a fixed point P. This distribution is given explicitly in [Cow20, Cor. 1.7]; in this case it is

$$\frac{1}{\omega_1 \sqrt{y^2 + (6x^2 - 32)^2}}.$$

The poles of this density function are shown in red.

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 1. 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 [CM22], 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 $D \geq 12$ 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 algorithms for finding these sorts of reductions.

Conductor distributions

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].

[Cow24a] gives the distribution of the conductors of elliptic curves in the large height-ordered family $\mathcal{F}(H)$ considered in [You10, DHP15]. Describing this distribution is closely connected to, and in many ways a refined version of, the problem discussed in the previous paragraph. The elliptic curves my results apply to are restricted only in their reduction at 2 and 3, and only so that this result can be used to prove Theorem 2.2; in the near future I anticipate updating the results below with variations applying to all elliptic curves, with no restrictions (more precisely, all globally minimal short Weierstrass equations over $\mathbb{Q}$).

Theorem 4.2 below can be viewed as a precise and effective version of the Brumer–McGuinness–Watkins heuristic. Presenting it requires the introduction of some notation. Define $\mathcal{F}(H)$ as in (2), i.e.

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

and 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 $\rho = \rho(p, m)$ be the function defined case by case in [Cow24a, Def. 3.3]; the values of ρ are simple rational functions of p depending only on the p-part of m, and satisfy $\rho(p, m) \asymp (p \cdot \gcd(p^\infty, m))^{-1}$ when $p \mid m$.

Theorem 4.2. *For any* $\lambda_1 > \lambda_0 > \frac{4464}{\log H}$,

$$\frac{\#\{E \in \mathcal{F}(H) \,:\, \lambda_0 < \frac{N_E}{H} < \lambda_1\}}{\#\mathcal{F}(H)} = \frac{\zeta^{(6)}(10)}{\zeta^{(6)}(2)} \sum_{m=1}^{\infty} \big(F_\Delta(m\lambda_1) - F_\Delta(m\lambda_0) + F_\Delta(-m\lambda_0) - F_\Delta(-m\lambda_1)\big) \cdot \rho(2,m)\rho(3,m) \prod_{\substack{p \geq 5 \\ p \mid m}} \frac{\rho(p,m)}{1-p^{-2}} + O((\log H)^{-1+\varepsilon}).$$

The expression on the right hand side of Theorem 4.2 may appear to be quite complicated. However, it is simple to compute: for any given λ_0 and λ_1 the sum over m is finite, because the summand is 0 for $m\lambda_0 > 496$. Figure 4.3 and Figure 4.4 plot the main term of Theorem 4.2 and its derivative. These are essentially the cumulative distribution function and histogram/distribution of $\{N_E/H \,:\, E \in \mathcal{F}(H)\}$.

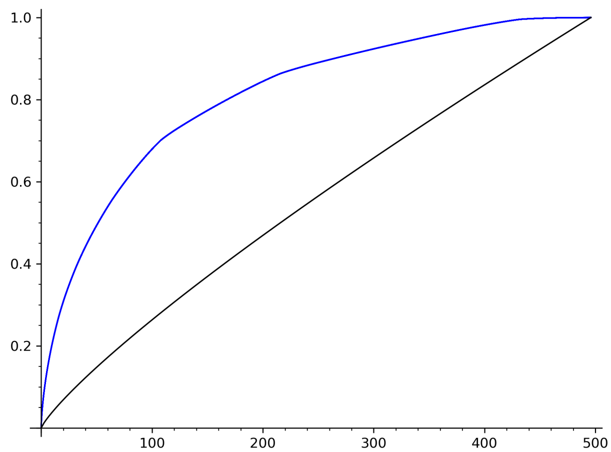

Figure 4.3. Main term on the right hand side of Theorem 4.2 with $\lambda_0 = 0$, as a function of λ_1 (blue), and the function $(\lambda_1/496)^{\frac{5}{6}}$ (black).

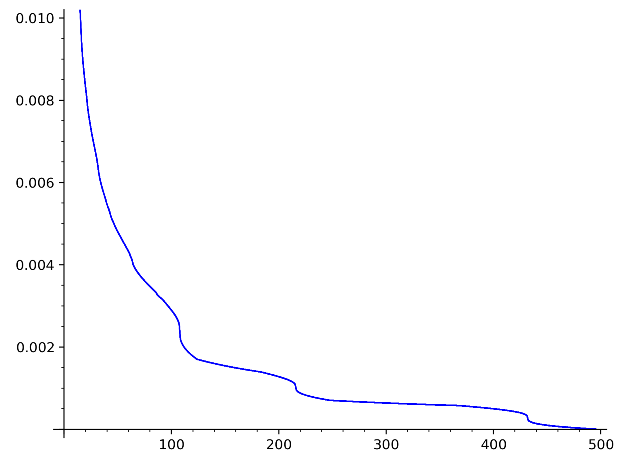

Figure 4.4. Derivative with respect to λ_1 of the main term of Theorem 4.2, computed numerically with $\Delta\lambda_1 = 0.496$ [Cow24c].

Theorem 4.2 gives no information about the region $N_E \leq \frac{4464H}{\log H}$, where the conductor is much smaller than the height bound. Theorem 4.5 and Theorem 4.6 describe the distribution there, complementing Theorem 4.2.

Theorem 4.5. *For any* $\lambda > \frac{4464}{\log H}$,

$$\lambda^{\frac{5}{6}} \ll \frac{\#\{E \in \mathcal{F}(H) \,:\, N_E < \lambda H\}}{\#\mathcal{F}(H)} \ll \lambda^{\frac{5}{6}}.$$

Theorem 4.6.

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

Analyzing the distribution of small conductors in $\mathcal{F}(H)$ is connected to the problem of estimating the number of elliptic curves with bounded conductor, i.e. $\#\{E \in \mathcal{F}(H) \,:\, N_E < X\}$ as $H \to \infty$ with X fixed. Based on [Wat08, §4] it is commonly believed that $\#\{E \in \mathcal{F}(\infty) \,:\, N_E < X\} \sim cX^{\frac{5}{6}}$ for some explicit $c > 0$ [SSW21, §1]. The best known general result of this sort is [DK00, Prop. 1] by Duke and Kowalski, which says that the number of elliptic curves with conductor less than X is $\ll X^{1+\varepsilon}$.

In this context, Theorem 4.5 and Theorem 4.6 can be viewed as upper bounds on the number of elliptic curves with bounded conductor when one is allowed to take the height of said curves to be large but not arbitrarily large. The aforementioned result of Duke–Kowalski alone implies neither Theorem 4.5, nor Theorem 4.6 in the case $X \gg H^{\frac{217}{264}+\varepsilon} > H^{0.8219}$.

The proofs of Theorem 4.2, Theorem 4.5, and Theorem 4.6 are technical but largely elementary. The key ingredient is [Cow24a, Lemma 4.2], which intertwines "Archimedean" and "non-Archimedean" restrictions on the elliptic curves in $\mathcal{F}(H)$ in an effective way. There is some similarity with elements of [BM90, Wat08, SSW21, CS23]. See [Cow24a, §2] for a more thorough overview.

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(2):241–268, 2023. 1

[Ass24] Eran Assaf. A note on the trace formula, 2024. arXiv 2311.03523. 1

[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. In *Arithmetic geometry, number theory, and computation*, Simons Symp., pages 131–213. Springer, Cham, [2021] ©2021. 1

[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(1):Paper No. 1, 24, 2020. arXiv 1706.03422. 4

[BBJ+24] Owen Barrett, Zoë X. Batterman, Aditya Jambhale, Steven J. Miller, Akash L. Narayanan, Kishan Sharma, and Chris Yao. A random matrix model for a family of cusp forms, 2024. arXiv 2407.14526. 2

[BBLLD23] Jonathan Bober, Andrew R. Booker, Min Lee, and David Lowry-Duda. Murmurations of modular forms in the weight aspect, 2023. arXiv 2310.07746. 2

[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(4):843–939, 2001. 1

[BGR19] Michael A. Bennett, Adela Gherga, and Andrew Rechnitzer. Computing elliptic curves over $\mathbb{Q}$. *Math. Comp.*, 88(317):1341–1390, 2019. 4

[BK75] B. J. Birch and W. Kuyk, editors. *Modular functions of one variable. IV.* Lecture Notes in Mathematics, Vol. 476. Springer-Verlag, Berlin-New York, 1975. 1

[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(3):275–321, 2015. 1

[BM90] Armand Brumer and Oisín McGuinness. The behavior of the Mordell-Weil group of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 23(2):375–382, 1990. 1, 4, 4

[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(1):191–242, 2015. 1

[CD23] Wouter Castryck and Thomas Decru. An efficient key recovery attack on SIDH. In *Advances in cryptology—EUROCRYPT 2023. Part V*, volume 14008 of *Lecture Notes in Comput. Sci.*, pages 423–447. Springer, Cham, [2023] ©2023. 1

[Čec24] Martin Čech. The ratios conjecture for real Dirichlet characters and multiple Dirichlet series. *Trans. Amer. Math. Soc.*, 377(5):3487–3528, 2024. 2

[CFM24] Alex Cowan, Sam Frengley, and Kimball Martin. Generic models for genus 2 curves with real multiplication, 2024. arXiv 2403.03191. 4, 4

[Chi24] Lyndie Chiou. Elliptic curve 'murmurations' found with ai take flight. `https://www.quantamagazine.org/elliptic-curve-murmurations-found-with-ai-take-flight-20240305/`, 2024. 2

[CLG09] Denis X. Charles, Kristin E. Lauter, and Eyal Z. Goren. Cryptographic hash functions from expander graphs. *J. Cryptology*, 22(1):93–113, 2009. 1

[CM] Alex Cowan and Kimball Martin. Statistics of modular forms with small rationality fields. In preparation. 1

[CM22] Alex Cowan and Kimball Martin. Moduli for rational genus 2 curves with real multiplication for discriminant 5, 2022. To appear, arXiv 2206.05752. 4, 4

[CM23] Alex Cowan and Kimball Martin. Counting modular forms by rationality field, 2023. arXiv 2301.10357. 1

[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, April 2024. https://doi.org/10.5281/zenodo.10950409. 1

[Cow20] Alex Cowan. The distribution of multiples of real points on an elliptic curve. *J. Number Theory*, 211:530–544, 2020. arXiv 1901.10656. 4, 4, 4

[Cow21] Alex Cowan. Conjecture: 100% of elliptic surfaces over $\mathbb{Q}$ have rank zero. In *Arithmetic geometry, number theory, and computation*, Simons Symp., pages 335–342. Springer, Cham, [2021] ©2021. arXiv 2009.08622. 4

[Cow22a] Alex Cowan. Computing newforms using supersingular isogeny graphs. *Res. Number Theory*, 8(4):Paper No. 96, 2022. arXiv 2010.10745. (document), 1, 1

[Cow22b] Alex Cowan. Non-random behavior in sums of modular symbols. *Int. J. Number Theory*, 18(4):879–903, 2022. arXiv 1905.10743. 3

[Cow23] Alex Cowan. Murmurations and explicit formulas, 2023. arXiv 2306.10425. 2

[Cow24a] Alex Cowan. Conductor distributions of elliptic curves, 2024. arXiv 2408.09745. 2, 4, 4, 4

[Cow24b] Alex Cowan. Murmurations and ratios conjectures, 2024. arXiv 2408.12723. (document), 2, 2, 2, 2.2, 2

[Cow24c] Alex Cowan. Conductor distribution code. `https://github.com/thealexcowan/conductordistribution`, July 2024. 4.4

[Cow24d] Alex Cowan. Kronecker symbol murmurations code. `https://github.com/thealexcowan/murmurations`, July 2024. 2.1

[Cow25] Alex Cowan. A twisted additive divisor problem. *Journal of Number Theory*, 266:1–32, 2025. arXiv 2304.12572. (document), 3, 3

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, second edition, 1997. 1

[CS07] J. B. Conrey and N. C. Snaith. Applications of the L-functions ratios conjectures. *Proc. Lond. Math. Soc. (3)*, 94(3):594–646, 2007. 2, 2

[CS23] John E. Cremona and Mohammad Sadek. Local and global densities for Weierstrass models of elliptic curves. *Math. Res. Lett.*, 30(2):413–461, 2023. 4, 4

[DFI02] W. Duke, J. B. Friedlander, and H. Iwaniec. The subconvexity problem for Artin L-functions. *Invent. Math.*, 149(3):489–577, 2002. 3

[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:Paper No. 6, 37, 2015. 2, 2.2, 4

[DK00] W. Duke and E. Kowalski. A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations. *Invent. Math.*, 139(1):1–39, 2000. With an appendix by Dinakar Ramakrishnan. 4

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. 1

[EHL+18] Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Advances in cryptology—EUROCRYPT 2018. Part III*, volume 10822 of *Lecture Notes in Comput. Sci.*, pages 329–368. Springer, Cham, 2018. 1

[EK14] Noam Elkies and Abhinav Kumar. K3 surfaces and equations for Hilbert modular surfaces. *Algebra Number Theory*, 8(10):2297–2411, 2014. 1, 4

[FM15] Daniel Fiorilli and Steven J. Miller. Surpassing the ratios conjecture in the 1-level density of Dirichlet L-functions. *Algebra Number Theory*, 9(1):13–52, 2015. 2

[GJM+10] John Goes, Steven Jackson, Steven J. Miller, David Montague, Kesinee Ninsuwan, Ryan Peckner, and Thuy Pham. A unitary test of the ratios conjecture. *J. Number Theory*, 130(10):2238–2258, 2010. 2

[Gol82] Dorian Goldfeld. Sur les produits partiels eulériens attachés aux courbes elliptiques. *C. R. Acad. Sci. Paris Sér. I Math.*, 294(14):471–474, 1982. 1

[HLN21] Jeff Hoffstein, Min Lee, and Maria Nastasescu. First moments of Rankin-Selberg convolutions of automorphic forms on GL(2). *Res. Number Theory*, 7(4):Paper No. 60, 44, 2021. 3

[HLOP22] Yang-Hui He, Kyu-Hwan Lee, Thomas Oliver, and Alexey Pozdnyakov. Murmurations of elliptic curves, 2022. arXiv 2204.10140. 2, 2

[HMM11] Duc Khiem Huynh, Steven J. Miller, and Ralph Morrison. An elliptic curve test of the L-functions ratios conjecture. *J. Number Theory*, 131(6):1117–1147, 2011. 2

[HS17] Robert Harron and Andrew Snowden. Counting elliptic curves with prescribed torsion. *J. Reine Angew. Math.*, 729:151–170, 2017. 1

[ILS00] Henryk Iwaniec, Wenzhi Luo, and Peter Sarnak. Low lying zeros of families of L-functions. *Inst. Hautes Études Sci. Publ. Math.*, (91):55–131 (2001), 2000. 2

[Iwa02] Henryk Iwaniec. *Spectral methods of automorphic forms*, volume 53 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI; Revista Matemática Iberoamericana, Madrid, second edition, 2002. 3

[JDF11] David Jao and Luca De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-quantum cryptography*, volume 7071 of *Lecture Notes in Comput. Sci.*, pages 19–34. Springer, Heidelberg, 2011. 1

[Jut96] Matti Jutila. The additive divisor problem and its analogs for Fourier coefficients of cusp forms. I. *Math. Z.*, 223(3):435–461, 1996. 3

[LMF24] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2024. [Online; accessed 20 September 2024]. 1

[LOP23] Kyu-Hwan Lee, Thomas Oliver, and Alexey Pozdnyakov. Murmurations of Dirichlet characters, 2023. arXiv 2307.00256. 2

[LR21] Álvaro Lozano-Robledo. A probabilistic model for the distribution of ranks of elliptic curves over $\mathbb{Q}$. *J. Number Theory*, 221:270–338, 2021. 1

[Mes86] J.-F. Mestre. La méthode des graphes. Exemples et applications. In *Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986)*, pages 217–242. Nagoya Univ., Nagoya, 1986. 1, 1

[Mes91] Jean-François Mestre. Construction de courbes de genre 2 à partir de leurs modules. In *Effective methods in algebraic geometry (Castiglioncello, 1990)*, volume 94 of *Progr. Math.*, pages 313–334. Birkhäuser Boston, Boston, MA, 1991. 4

[Mic04] P. Michel. The subconvexity problem for Rankin-Selberg L-functions and equidistribution of Heegner points. *Ann. of Math. (2)*, 160(1):185–236, 2004. 3

[Mic07] Philippe Michel. Analytic number theory and families of automorphic L-functions. In *Automorphic forms and applications*, volume 12 of *IAS/Park City Math. Ser.*, pages 181–295. Amer. Math. Soc., Providence, RI, 2007. 3

[Mil08] Steven J. Miller. A symplectic test of the L-functions ratios conjecture. *Int. Math. Res. Not. IMRN*, (3):Art. ID rnm146, 36, 2008. 2

[Mil09] Steven J. Miller. An orthogonal test of the L-functions ratios conjecture. *Proc. Lond. Math. Soc. (3)*, 99(2):484–520, 2009. 2

[Mot94] Yōichi Motohashi. The binary additive divisor problem. *Ann. Sci. École Norm. Sup. (4)*, 27(5):529–572, 1994. 3

[MP12] Steven J. Miller and Ryan Peckner. Low-lying zeros of number field L-functions. *J. Number Theory*, 132(12):2866–2891, 2012. 2

[MR16] Barry Mazur and Karl Rubin. The statistical behavior of modular symbols and arithmetic conjectures. 2016. 3

[MR19] Barry Mazur and Karl Rubin. Arithmetic conjectures suggested by the statistical behavior of modular symbols, 2019. 3

[MV10] Philippe Michel and Akshay Venkatesh. The subconvexity problem for GL_2. *Publ. Math. Inst. Hautes Études Sci.*, (111):171–271, 2010. 3

[Nel19] Paul D. Nelson. Eisenstein series and the cubic moment for PGL_2, 2019. arXiv 1911.06310. 3

[Poo18] Bjorn Poonen. Heuristics for the arithmetic of elliptic curves. In *Proceedings of the International Congress of Mathematicians—Rio de Janeiro 2018. Vol. II. Invited lectures*, pages 399–414. World Sci. Publ., Hackensack, NJ, 2018. 1

[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(9):2859–2903, 2019. 1

[Ser97] Jean-Pierre Serre. Répartition asymptotique des valeurs propres de l'opérateur de Hecke T_p. *J. Amer. Math. Soc.*, 10(1):75–102, 1997. 1

[SSW21] Ananth N. Shankar, Arul Shankar, and Xiaoheng Wang. Large families of elliptic curves ordered by conductor. *Compos. Math.*, 157(7):1538–1583, 2021. 1, 4, 4

[Stu87] Jacob Sturm. On the congruence of modular forms. In *Number theory (New York, 1984–1985)*, volume 1240 of *Lecture Notes in Math.*, pages 275–280. Springer, Berlin, 1987. 1

[Sut22] Andrew Sutherland. Letter to Michael Rubinstein and Peter Sarnak. https://math.mit.edu/~drew/RubinsteinSarnakLetter.pdf, 2022. 2

[SZ24] Peter Sarnak and Nina Zubrilina. Convergence to the Plancherel measure of Hecke eigenvalues. *Acta Arithmetica*, 214:191–213, 2024. Publisher Copyright: © Instytut Matematyczny PAN, 2024. 1

[TW95] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995. 1

[VT84] A. I. Vinogradov and L. A. Takhtadzhyan. The zeta function of the additive divisor problem and spectral expansion of the automorphic Laplacian. volume 134, pages 84–116. 1984. Automorphic functions and number theory, II. 3

[Wat08] Mark Watkins. Some heuristics about elliptic curves. *Experiment. Math.*, 17(1):105–125, 2008. 1, 4, 4

[WDE+15] Mark Watkins, Stephen Donnelly, Noam D. Elkies, Tom Fisher, Andrew Granville, and Nicholas F. Rogers. Ranks of quadratic twists of elliptic curves. In *Numéro consacré au trimestre "Méthodes arithmétiques et applications", automne 2013*, volume 2014/2 of *Publ. Math. Besançon Algèbre Théorie Nr.*, pages 63–98. Presses Univ. Franche-Comté, Besançon, 2015. 1

[Wie86] Douglas H. Wiedemann. Solving sparse linear equations over finite fields. *IEEE Trans. Inform. Theory*, 32(1):54–62, 1986. 1

[Wil95] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995. 1

[Wu19] Han Wu. Deducing Selberg trace formula via Rankin-Selberg method for GL_2. *Trans. Amer. Math. Soc.*, 372(12):8507–8551, 2019. 3

[You10] Matthew P. Young. Moments of the critical values of families of elliptic curves, with applications. *Canad. J. Math.*, 62(5):1155–1181, 2010. 4

[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(3):415–437 (1982), 1981. 3

[Zub23] Nina Zubrilina. Murmurations, 2023. arXiv 2310.07681. 2

Email address: alex.cowan@uwaterloo.ca