1 Past work

1.1 Modular Symbols

Let \( f(z) \) be a cusp form of weight 2 and level \( N \), with Fourier coefficients \( a_n \). For simplicity, assume \( N \) is prime. For \( \gamma \in \Gamma_0(N) \), define the modular symbol

\[
\langle \gamma, f \rangle := 2\pi i \int_{\gamma \tau} f(w) \, dw
\]

for any \( \tau \) (the value of \( \langle \gamma, f \rangle \) is independent of the choice of \( \tau \)).

Modular symbols have been the subject of much research, both with a view towards their applications and for their own sake. They figure prominently in the very influential works of Merel [18] and Cremona [6], for example, because of their applications to elliptic curves, while Petridis and Risager [21] prove that modular symbols are normally distributed when ordered by \( |cz + d|^2 \) for any fixed \( z \in \mathcal{H} \), where \( c \) and \( d \) are the lower-left and lower-right entries of \( \gamma \) respectively, which is a very interesting result in its own right. Recently Mazur and Rubin in [17], inspired by the work of David, Fearnley, and Kisilevsky [7], make conjectures for the distribution of modular symbols ordered in ways which allow for applications to computing central values of \( L \)-functions of twisted elliptic curves. An average version of one of their conjectures was proven by Petridis and Risager in [23], and the full conjecture was proven by Diamantis, Hoffstein, Kiral, and Lee [8].

The main tool used to study the statistical properties of modular symbols is the Eisenstein series twisted by modular symbols \( E^*(z, s, \chi) \), introduced by Goldfeld in [12],

\[
E^*(z, s, \chi) := \sum_{\Gamma \subseteq \Gamma_0(N)} \chi(\gamma)\langle \gamma, f \rangle \text{Im}(\gamma z)^s
\]

where \( \chi \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) := \chi(d) \).

In my thesis, I give the Fourier expansion of \( E^*(z, s, \chi) \) in very explicit terms when \( N \) is prime and \( \chi \) is even and primitive of conductor \( N \). In particular, the constant term of \( E^*(z, s, \chi) \) in this case is found to be of a particularly simple form. It is notable that the techniques used fail completely when the conductor of \( \chi \) is not equal to \( N \), while generally the results in the literature require that the conductor of \( \chi \) be coprime to \( N \).

**Theorem 1** The constant term of the Fourier expansion for \( E^*(z, s, \chi) \) with primitive even \( \chi \) of conductor \( N \) is given by

\[
\int_0^1 E^*(x + iy, s, \chi) \, dx = \left( 2\tau(\bar{\chi})L_f(1, \chi)\pi^{\frac{1}{2}}N^{-2s} \frac{\Gamma(s - \frac{1}{2})L_f(2s)L(2 - 2s, \chi)}{\Gamma(s)L(2s, \chi)} - 2\tau(\chi)L_f(1, \chi)\pi^{\frac{1}{2}}N^{-2s} \frac{\Gamma(s - \frac{1}{2})L_f(2s)L(2 - 2s, \bar{\chi})}{\Gamma(s)L(2s, \bar{\chi})} \right) y^{1-s}.
\]
Then I also obtain applications to central values of Maass forms, and all error terms exactly in terms of zeroes of Dirichlet.

Inspecting the Fourier expansion, one can give the leading term of this identity exactly in terms of the eigenvalues

\[\gamma \cdot \gamma_1 \leq x\]

where \(\|\gamma\|_1 := |cz + d|^2\). Using the explicit form of the Fourier expansion of \(E^*(z, s, \chi)\) I can obtain analogous results when the sum on the left is twisted by \(\chi\):

**Theorem 3** For primitive even \(\chi\) of conductor \(N\),

\[\sum_{\gamma : \|\gamma\|_1 \leq x} \chi(\gamma) \langle \gamma, f \rangle \sim \sum_{s: \text{poles of } E^*(z, s, \chi)} \text{Res}_{w=s} E^*(z, w, \chi) \cdot x^s,\]

Inspecting the Fourier expansion, one can give the leading term of this identity exactly in terms of the eigenvalues of Maass forms, and all error terms exactly in terms of zeroes of Dirichlet \(L\)-functions.

I also obtain applications to central values of \(L\)-functions. Denote the constant term of \(E^*(z, s, \chi)\) by \(\phi^*_\chi(s)y^{1-s}\). Then

\[L_f(1, \chi) = \frac{\int_{(\sigma)} \phi^*_\chi(s)(N + \varepsilon)^{s} ds}{\tau(\chi) \int_{(\sigma)} 2\sqrt{\pi} \left(s - \frac{1}{2}\right)^{1/2} \frac{\Gamma(s) \left(N + \varepsilon\right)^{s} ds}{s}}\]

for every \(\varepsilon \in (0, N)\) and \(\sigma > 2\). Generalizing methods of Petridis used in [22], I prove that \(\phi^*_\chi(s) = -\phi^*_\chi(s)\), and with these relationships I deduce

**Theorem 4** Let \(N\) be prime and let \(f\) be a weight 2 cusp form on \(\Gamma_0(N)\). For primitive characters \(\chi \mod N\) and for all \(d,\)

\[\sum_{\chi: \deg(\chi) = d} \tau(\chi)L_f(1, \chi) = 0.\]

Note that this implies, for example, that \(L_f(1, \chi) = 0\) when \(\chi\) is the quadratic character mod \(N\). The vanishing in this case is known via the work of Schmidt [25], but the method used in his work relies on computing the
root number of the $L$-function, whereas my work proves the vanishing directly, making no reference at all to root numbers. If $f(z)$ corresponds to an elliptic curve $E/\mathbb{Q}$, then the Birch and Swinnerton-Dyer conjecture implies the existence of a point of infinite order on the elliptic curve which is the twist of $E$ by $\chi$. The approach taken in my thesis is purely analytic, and to my knowledge the only previous example of proving that an elliptic curve has positive analytic rank using purely complex analytic techniques is the Gross-Zagier formula [13].

1.2 Titchmarsh divisor problems for elliptic curves

R. Bell, C. Blakestad, A. Cojocaru, N. Jones, V. Matei, G. Smith, I. Vogt, and I investigate statistics of constants related to a version of the Titchmarsh divisor problem for elliptic curves in [3]. For an elliptic curve $E/\mathbb{Q}$ with good reduction at $p$, it is well known that $E(\mathbb{F}_p) \cong \mathbb{Z}/d_{1,p} \times \mathbb{Z}/d_{2,p}$ with $d_{1,p} | d_{2,p}$. One has the following conjectures:

Conjecture Let $E/\mathbb{Q}$ be an elliptic curve. Then as $x \to \infty$,

\[
\sum_{p<x} d_{1,p} \sim \text{li}(x) \cdot \sum_{m=1}^{\infty} \frac{\phi(m)}{[\mathbb{Q}(E[m]): \mathbb{Q}]}
\]

if $E$ does not have complex multiplication [15],\[
\sum_{p<x} d_{1,p} \sim x \cdot \text{Re} \frac{1}{s-1} \sum_{m=1}^{\infty} \frac{\phi(m)}{[\mathbb{Q}(E[m]): \mathbb{Q}]} m^{-s}
\]

if $E$ has complex multiplication [15],\[
\sum_{p<x} \tau(1, p) \sim \text{li}(x) \cdot \sum_{m=1}^{\infty} \frac{1}{[\mathbb{Q}(E[m]): \mathbb{Q}]}
\]

[1],\[
\sum_{p<x} d_{2,p} \sim \frac{1}{2} \text{li}(x^2) \cdot \sum_{m=1}^{\infty} \frac{(-1)^{\omega(m)} \phi(\text{rad } m)}{m[\mathbb{Q}(E[m]): \mathbb{Q}]}
\]


Let $C(A, B)$ be the set of $\mathbb{Q}$-isomorphism classes of elliptic curves $E : y^2 = x^3 + ax + b$ with $|a| < A$, $|b| < B$. We give explicit forms for the average values of the constants which appear on the right, proving

Theorem 5 For any functions $A(x)$ and $B(x)$ such that $\lim_{x \to \infty} \frac{A(x)}{B(x)} = \infty$ and $\lim_{x \to \infty} \frac{\log A(x)}{\log B(x)} \in (0, \infty)$,

\[
\lim_{x \to \infty} \frac{1}{\#C(A, B}(x)) \sum_{E \in C(A, B}(x)) \left\{ \sum_{m=1}^{\infty} \frac{\phi(m)}{[\mathbb{Q}(E[m]): \mathbb{Q}]}, \text{ if } E \text{ does not have complex multiplication} \right\}
\]

\[
\sum_{m=1}^{\infty} \frac{\phi(m)}{[\mathbb{Q}(E[m]): \mathbb{Q}]} m^{-s}, \text{ if } E \text{ has complex multiplication}
\]

\[
= \sum_{m=1}^{\infty} \frac{\phi(m)}{\# \text{GL}_2(\mathbb{Z}/m)} = \prod_{\ell \text{ prime}} \left(1 + \frac{\ell^2}{(\ell^2 - 1)(\ell^4 - 1)} \right),
\]

\[
\lim_{x \to \infty} \frac{1}{\#C(A, B}(x)) \sum_{E \in C(A, B}(x)) \sum_{m=1}^{\infty} \frac{1}{[\mathbb{Q}(E[m]): \mathbb{Q}]} = \sum_{m=1}^{\infty} \frac{1}{\# \text{GL}_2(\mathbb{Z}/m)} = \prod_{\ell \text{ prime}} \left(1 + \frac{\ell^3}{(\ell - 1)(\ell^2 - 1)(\ell^4 - 1)} \right),
\]

\[
\lim_{x \to \infty} \frac{1}{\#C(A, B}(x)) \sum_{E \in C(A, B}(x)) \sum_{m=1}^{\infty} \frac{(-1)^{\omega(m)} \phi(\text{rad } m)}{m[\mathbb{Q}(E[m]): \mathbb{Q}]},
\]

\[
= \sum_{m=1}^{\infty} \frac{(-1)^{\omega(m)} \phi(\text{rad } m)}{m \cdot \# \text{GL}_2(\mathbb{Z}/m)} = \prod_{\ell \text{ prime}} \left(1 + \frac{\ell^3}{(\ell^2 - 1)(\ell^5 - 1)} \right).
\]
We also bound all higher moments of these quantities. Producing these statistics involves a mix of analytic and algebraic machinery, such as the open image theorems of Weil and Serre, with an effective version of the latter [30], [27], [14].

1.3 Computational number theory

I regularly use Sage in my work and I’ve participated in research projects using Mathematica, Magma, Python, C++, and C. I’ve implemented algorithms which successfully search for points on elliptic curves over cubic and quintic number fields, and algorithms which do computations with Fourier expansions of Eisenstein series of arbitrary level at arbitrary cusps. Both of these involved extremely technical methods and formulas, and required nontrivial speed optimizations, such as the use of cython, to run in reasonable timeframes.

2 Future work

2.1 Distributions of central values of $L$-functions

Mazur and Rubin in [17] ask questions related to the distribution of $L_f(1, \chi)$. In particular, they observe that certain associated distributions are distinctly non-normal. In my thesis I compute the average value of $L_f(1, \chi)$ as a first step in understanding the statistics of this quantity. In the future I plan to consider Eisenstein series twisted by higher powers of modular symbols, which allows one can obtain information about higher moments of the distribution of $L_f(1, \chi)$.

The statistics of Petridis and Risager from [21] can also be used for this, in the very special case where one chooses $z$ and $x$ in such a way to pick out sums of modular symbols for which the $L^2$ norm ordering and the ordering that appears in $L_f(1, \chi)$ coincide. For example, the integral

$$
\int E^*(iM, s, \chi)x^s \frac{ds}{s} = \sum_{c^2 M^2 + d^2 < xM} \chi(\gamma) \langle \gamma, f \rangle
$$

with $x = 4N^2M$ can be related to $L_f(1, \chi)$ as $M \to \infty$. Previously this approach was unavailable because the error term from [21] would then dwarf the main term, but with the explicit formulas for the Fourier expansion of $E^*(z, s, \chi)$ derived in my thesis this approach can now work.

2.2 New versions of Lang-Trotter statistics

The following theorem of Serre [26] is an important ingredient in the proof of the Sato-Tate conjecture (expository: [10], [28]):

Theorem (Serre) Let $G$ be a compact group and let $X$ be the set of conjugacy classes of $G$. Let $(x_p)$ be a sequence in $X$ indexed by the rational primes. If, for every nontrivial irreducible representation $\rho : G \to \text{GL}_d(\mathbb{C})$, the function

$$
L(\rho, s) := \prod_p \det(1 - \rho(x_p)p^{-s})^{-1}
$$

is holomorphic on Re($s$) $\geq 1$ and nonzero at $s = 1$, then the sequence $(x_p)$ is equidistributed according to the Haar measure on $G$, and conversely.

If one applies this theorem to the case where $G = \text{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ for arbitrary $\ell$ and $x_p = \text{Frob}_p$, then
the conclusion of the theorem would imply the Lang-Trotter conjecture ([16], § 3). In all but a small and well understood set of cases, we have $G = GL_2(\mathbb{F}_q)$, and in this case the representations $\rho$ are well known [9]. Moreover, $Frob_p$, being defined only up to conjugacy, can be taken to be its rational canonical form (also known as the Frobenius normal form):

$$Frob_p = \begin{pmatrix} 0 & -p \\ 1 & a_p \end{pmatrix} \text{ or } \begin{pmatrix} \sqrt{p} & 0 \\ 0 & \sqrt{p} \end{pmatrix}$$

depending on whether or not the minimal polynomial of $Frob_p$ is of degree 2 or 1. By examining the image of these matrices under the complex representations of $GL_2(\mathbb{F}_q)$ one obtains results somewhat analogous to vertical Lang-Trotter theorems, in the sense that they exist as different perspectives on the classical Lang Trotter conjecture. Moreover, this approach highlights similarities between the Lang-Trotter and Sato-Tate conjectures which are infrequently highlighted explicitly in the literature, and suggests the adelic perspective of considering $Frob_p$ as an element of the maximal compact of $GSp_{2g}(\mathbb{A}_Q)$ for an abelian variety of dimension $g$ and considering the complex representations of this group. This unifies both conjectures in a way which is novel as far as I’m aware.

2.3 Counting elliptic curves by conductor

It is an open problem to determine the number of elliptic curves over $\mathbb{Q}$ of conductor up to $X$. The best existing conjecture is due to Watkins in [29], who predicts a leading term of $cX^{5/6}$ for explicit $c$, using a heuristic based on a heuristic of Brumer and McGuinness [5] for counting elliptic curves by discriminant. In future work I plan to obtain unconditional results that justify the connection between the heuristics of Watkins and Brumer-McGuinness using the recent work of Sadek [24], in which he counts the number of elliptic curves with given Kodaira type at a prime $p$. This produces a connection between elliptic curves ordered by height, by discriminant, and by conductor. In much of arithmetic statistics there is a tension in which of these quantities one uses to order elliptic curves. Ordering by height lends itself to the easiest calculations, while ordering by conductor tends to give more natural results. At the moment there are few ways to relate one ordering to another, so improved results in this area would be very useful.

Another avenue towards counting elliptic curves is via the algorithms of Cremona [6], which compute the number of elliptic curves of conductor $N$ by examining the action of the Hecke operators on a space of modular symbols, ultimately leading to explicit matrix computations which can be carried out by computer, as Cremona does when he generates his databases of elliptic curves. This lends itself to an approach via random matrix theory. Using random matrices to predict elliptic curve statistics is well established, and the main obstacle towards unconditional results is showing that the matrices coming from elliptic curves are indeed equidistributed in the group of matrices being considered. For example, the popular and insightful heuristics of Park, Poonen, Voight, and Wood [20] and those of Bhargava, Kane, Lenstra, Hendrik, Poonen, and Rains [4] for the distribution of ranks of elliptic curves hinge on viewing objects such as Selmer groups and Shafarevich-Tate groups as coming from random matrices, and while it would be very surprising if these groups did not obey the induced statistics, a proof of such facts seems to be far out of reach at the moment. In the case of Cremona’s algorithms, one has a concrete source of the matrices which can be used to overcome this difficulty. Moreover, this problem is clearly very amenable to computational investigation, which will allow for a refinement of the conjecture of Watkins. Such improvements would be helpful for deriving statistics from databases of elliptic curves. Balakrishnan, Ho, Kaplan, Spicer, Stein, and Weigandt in [2] explain that it is hard to generate exhaustive tables of elliptic curves when ordered by conductor because one is uncertain of how many curves they will contain.

References


