1. Introduction

My research program centers on two main topics in the field of analytic number theory. The first is the subject of low-lying zeros of families of L-functions and their relationship to random matrix theory. The second is the subject of distribution properties of elliptic curves defined over $\mathbb{Q}$ when reduced modulo primes.

2. Low-lying zeros and 1-level densities

The main outstanding problem in the field of analytic number theory is the Generalized Riemann Hypothesis (GRH), which deals with the location of the nontrivial zeros of an L-function. In 1973, Montgomery [Mo] noticed that certain statistics of the zeros of the Riemann zeta function bear a striking similarity to statistics coming from random matrices in the group of $N \times N$ unitary matrices in the large N limit. In recent years, such similarities were also seen to be present for certain families of L-functions. However, it was predicted by Katz and Sarnak [KS2, KS3] that by looking at low-lying zeros of families of L-functions, one should expect different statistics, which correspond to statistics of eigenvalues coming from scaling limits of certain compact Lie groups, specifically one of $U(N), O(N), SO(2N+1), SO(2N)$ and $Sp(2N)$.

The 1-level density is a central statistic, which analyzes the low-lying zeros of members of a family. This statistic of L-function zeros has been studied extensively for various families of L-functions (see [ILS], [Mi2], [Y]) and remains a central object of research in the analytic theory of L-functions. It has the advantage of allowing one to isolate the symmetry type, while being quite versatile and tractable under certain restrictions on the involved test function. It should be noted that low-lying zeros of L-functions are of central importance in many number-theoretical problems, and their thorough understanding could lead to the solution of several long standing problems.

In [FPS2], Fiorilli, Södergren and I study the 1-level density of low-lying zeros of Dirichlet L-functions attached to real primitive characters of conductor at most X, previously considered by Özlük and Snyder [OS1], [OS2] and Katz and Sarnak [KS1], where they obtained an asymptotic expression for a test function with support in $(-1, 1)$. These low-lying zeros of Dirichlet L-functions are of particular interest since they have strong connections with important problems such as the size of class numbers of imaginary quadratic number fields and Chebyshev's bias for primes in arithmetic progressions.

For the family of quadratic Dirichlet L-functions, we extend this result under GRH to an asymptotic expansion of the 1-level density in descending powers of $\log X$, which is valid when the support of the Fourier transform of the corresponding even test function ϕ is contained in $(-2, 2)$. The new feature of our work is that we obtain a precise expression for both the main term and the lower order terms appearing when the supremum σ of the support of $\widehat{\phi}$ reaches 1. This investigation was motivated by the work of Rudnick [R] who studied the family of hyperelliptic curves of growing genus, which is an analogue of the family of quadratic Dirichlet L-functions in the function field setting. He obtained lower order terms which were unavailable in the number field setting and which did not come from a universal random matrix theory term. The new lower order term appearing when $\sigma = 1$ involves the

quantity $\widehat{\phi}(1)$, which is analogous to a lower order term previously obtained in the function field case.

The Ratios Conjecture of Conrey, Farmer and Zirnbauer [CFZ] has been shown by Conrey and Snaith [CS] to predict a precise expression for the 1-level density; this prediction was confirmed up to a power saving error term by Miller [Mi1] for a restricted class of test functions for the family of quadratic Dirichlet characters. However, it remains an open problem to show that the lower order terms predicted by the Ratios Conjecture agree with the number theoretic result for any family of L-functions for extended support. In a future work [FPS3] Fiorilli, Södergren and I plan to investigate how the Ratios Conjecture's prediction for the lower order terms for the family of quadratic Dirichlet characters compares with the new lower order term appearing when $\sigma = 1$ obtained in [FPS2].

In [FPS1], Fiorilli, Södergren and I have studied the low-lying zeros of L-functions attached to quadratic twists of a given elliptic curve E defined over $\mathbb{Q}$, previously considered in [HKS], [HMM]. We investigated the family of all quadratic twists coprime to the conductor of E. Building upon the techniques of Katz and Sarnak [KS1], we computed a very precise expression for the corresponding 1-level density. For test functions whose Fourier transforms have sufficiently restricted support, we obtained an unconditional result for the 1-level density up to an error term that is significantly sharper than the square-root error term predicted by the L-functions Ratios Conjecture. The key to obtaining an error term sharper than the Ratios Conjecture's prediction was to allow repetitions in our family by considering quadratic twists for all integers d coprime to the conductor rather than restricting to only square-free values.

In [DHP], David, Huynh and I have used the Ratios Conjecture approach of Conrey, Farmer and Zirnbauer [CFZ] to obtain closed formulas for the 1-level density for two families of L-functions attached to elliptic curves. The first family is the family of all elliptic curves with nonzero discriminant. This family was studied previously by Young [Y] for test functions with Fourier transforms of small support. However, assuming the Ratios Conjecture, in addition to a closed formula for the 1-level density, we also obtained an explicit expression for the lower order terms.

The second family is a one-parameter family of curves with rank 1 which was previously studied by Washington [W] and Miller [Mi2]. For this family assuming the Ratios Conjecture we have shown that the 1-level density is the sum of the Dirac distribution and the even orthogonal distribution. This is a new phenomenon for a family of odd rank. This occurs since there is always a trivial zero at the central point, $\Re(s) = 1/2$. This accounts for the Dirac distribution. This affects the remaining part of the 1-level density which contributes the even orthogonal distribution. We remark that this family was studied in the past for test functions with Fourier transforms of small support [Mi2], but since the Fourier transforms of the even orthogonal and odd orthogonal distributions are indistinguishable for small support, it was not possible to identify the distribution with those techniques.

3. Reductions of elliptic curves over finite fields

My second field of study is reductions of elliptic curves defined over $\mathbb{Q}$ modulo primes. There are many interesting open conjectures in this field, but my main focus has been on amicable pairs and aliquot cycles, first considered by Silverman and Stange [SS]. For an elliptic curve $E/\mathbb{Q}$ we define the set $(p_1, \dots, p_L)$ of distinct primes to be an *aliquot cycle* of length L of E if each p_i is a prime of good reduction for E and

$$\#E_{p_1}(\mathbb{F}_{p_1}) = p_2, \dots, \#E_{p_{L-1}}(\mathbb{F}_{p_{L-1}}) = p_L, \#E_{p_L}(\mathbb{F}_{p_L}) = p_1,$$

where $\#E_{p_i}(\mathbb{F}_{p_i})$ is the number of points on the reduced elliptic curve E_{p_i} over the finite field $\mathbb{F}_{p_i}$. In the case $L = 2$ the set is called an *amicable pair*.

Fix an elliptic curve $E/\mathbb{Q}$ and let $\pi_{E,L}(X)$ denote the function that counts the number aliquot cycles with $p_1 \leq X$. Silverman and Stange [SS] first gave heuristic arguments to support a conjecture about the behaviour of this function. This was later refined by Jones [J] following a heuristic argument similar to that of Lang and Trotter [LT] for elliptic curves without complex multiplication. We state the refined conjecture below.

Conjecture 3.1 (Jones). *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and let $L \geq 2$ be a positive integer. Then there is a non-negative real constant $C_{E,L} \geq 0$ such that, as $X \to \infty$, we have that*

$$\pi_{E,L}(X) \sim C_{E,L} \int_2^X \frac{1}{2\sqrt{t}(\log t)^L} dt.$$

Moreover, Jones gave an explicit expression for the constant $C_{E,L}$ in terms of invariants of the elliptic curve.

We consider the function $\pi_{E,L}(X)$ on average over a family of elliptic curves. There is a rich history in the literature of considering distribution questions about elliptic curves on average over a family of curves in the work of Fouvry and Murty [FM], David and Pappalardi [DP], Banks and Shparlinski [BS] and Balog, Cojocaru and David [BCD]. Let a and b be integers and let $E_{a,b}$ be the elliptic curve given by the Weierstrass equation

$$E_{a,b} : y^2 = x^3 + ax + b,$$

with discriminant $\Delta(E_{a,b}) \neq 0$. For $A, B > 0$ we consider the two parameter family of elliptic curves as

$$\mathcal{C} := \mathcal{C}(A, B) = \{E_{a,b} : |a| \leq A, |b| \leq B, \Delta(E_{a,b}) \neq 0\}. \tag{3.1}$$

Building on the techniques of [BCD] and [CDKS], I have shown in [P1] the following unconditional upper bound for the average number of aliquot cycles.

Theorem 3.2. *Let $\epsilon > 0$, let $E/\mathbb{Q}$ be an elliptic curve and let $\mathcal{C}$ be the family of elliptic curves in* (3.1) *with*

$$A, B > X^{\epsilon} \quad \text{and} \quad X^{\frac{3L}{2}}(\log X)^6 < AB < e^{X^{\frac{1}{6}-\epsilon}}.$$

Then as $X \to \infty$ we have that

$$\frac{1}{|\mathcal{C}|} \sum_{E \in \mathcal{C}} \pi_{E,L}(X) \ll_L \frac{\sqrt{X}}{(\log X)^L},$$

where the implied constant depends on L only.

Remark 3.3. (i) Note that the condition $AB < e^{X^{\frac{1}{6}-\epsilon}}$ is not a limiting constraint since we are mainly interested in averages for small values of A and B.

In [P2], Theorem 3.2 was significantly improved, in the case of amicable pairs when $L = 2$, from an unconditional upper bound on average to an unconditional asymptotic result on average. More precisely, by building on the work of [Kou], [DS1] and [CDKS] I have obtained the following result.

Theorem 3.4. *Let $\epsilon > 0$, let $E/\mathbb{Q}$ be an elliptic curve and let $\mathcal{C}$ be the family of elliptic curves in* (3.1) *with*

$$A, B > X^{\epsilon} \quad \text{and} \quad X^3(\log X)^6 < AB < e^{X^{\frac{1}{6}-\epsilon}}.$$

Then we have that

$$\frac{1}{|\mathcal{C}|}\sum_{E\in\mathcal{C}}\pi_{E,2}(X) = C_2\frac{\sqrt{X}}{(\log X)^2} + O\left(\frac{\sqrt{X}}{(\log X)^{2+\epsilon}}\right),$$

where

$$C_2 := \frac{8}{3\pi^2}\prod_{\ell}\left(1 - \frac{(2\ell^4+3\ell^3)(\ell-2)-(\ell-1)(\ell^4-2\ell^3-4\ell^2+1)}{(\ell-1)(\ell^2-1)^3}\right).$$

The average number of aliquot cycles, and in particular amicable pairs, has been independently considered by David, Koukoulopolous and Smith [DKS, Theorem 1.6] using different techniques building upon a theorem of Gekeler [G, Theorem 5.5]. They also obtain an asymptotic result on average, but they express their average constant as a product over primes ℓ of the limit as $k \to \infty$ of matrix counts in $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})^L$ with certain conditions on the traces and determinants. However, the constant C_2 is not an obvious consequence of this limit in the case $L = 2$ and in a future work I plan to show agreement between these two constants.

Finally, for an elliptic curve $E/\mathbb{Q}$, David and Smith [DS1], [DS2] considered the function $M_E(N)$ that counts the number of primes p such that $\#E_p(\mathbb{F}_p) = N$, for a fixed integer N. They obtained an asymptotic average result for the function $M_E(N)$ over the family of elliptic curves $\mathcal{C}$ in (3.1) with $A, B > N^{\frac{1}{2}+\epsilon}$ and $AB > N^{\frac{3}{2}+\epsilon}$ for some $\epsilon > 0$ conditional on the Barban-Davenport-Halberstam Conjecture (cf. [DS1, Conjecture 2]). This result was improved in [P3], following the techniques of [Kow] and [P1] to hold for much smaller bounds on the size of A and B, namely, for

$$e^{N^{\epsilon}} \gg A, B > N^{\epsilon} \quad \text{and} \quad AB > N^{\frac{3}{2}}(\log N)^{6+2\gamma}\log\log N,$$

for some $\epsilon > 0$.

4. Short term goals

One of the most important problems in the area of reductions of elliptic curves over $\mathbb{Q}$ modulo primes p is the Lang-Trotter Conjecture [LT]. Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication and fix an integer t. The Lang-Trotter Conjecture predicts an asymptotic expression for the number of primes less than x with fixed trace of the Frobenius automorphism $a_p(E) = t$, with an explicit conjectural constant. By applying the celebrated

open image theorem of Serre [Se] the explicit constant can be expressed as a product of a non-negative rational number depending on E and t and a nonzero universal constant depending only on t. In [AP], Akbary and I consider the analogous Lang-Trotter Conjecture for two non-isogenous elliptic curves E_1 and E_2. That is, we fix integers t_1 and t_2 and consider the function

$$\pi_{E_1,E_2,t_1,t_2}(x) := \#\{p \leq x : a_p(E_1) = t_1 \text{ and } a_p(E_2) = t_2\}.$$

This leads to the following analogous Lang-Trotter conjecture for two elliptic curves.

Conjecture 4.1. *(**Lang-Trotter**) Let E_1 and E_2 be two elliptic curves defined over $\mathbb{Q}$ without complex multiplication and that are not $\overline{\mathbb{Q}}$-isogenous. Fix integers t_1 and t_2. Then we have as $x \to \infty$ that*

$$\pi_{E_1,E_2,t_1,t_2}(x) \sim c_{E_1,E_2,t_1,t_2} \log\log x.$$

As in the single variable case we may apply the open image theorem for two elliptic curves of Serre [Se, Théorème 6, p.324] to write the conjectural constant c_{E_1,E_2,t_1,t_2} as a product of a non-negative rational number depending on E_1, E_2, t_1 and t_2 and a nonzero universal constant c_{t_1,t_2} depending only on t_1 and t_2. We obtain an explicit expression for c_{t_1,t_2} when $t_1 = \pm t_2$ and we give a conjecture for the explicit universal constant in the case where $t_1 \neq t_2$. Finally by applying a general theorem of David, Koukoulopoulos and Smith [DKS, Theorem 4.2] we also prove Conjecture 4.1 on average.

References

[AP] A. Akbary and J. Parks, On the Lang-Trotter Conjecture for two elliptic curves. In preparation.

[BCD] A. Balog, A. Cojocaru, and C. David, Average twin prime conjecture for elliptic curves. *American Journal of Mathematics*, **133** no. 5, (2011) 1179–1229.

[BS] W. Banks and I. Shparlinski, Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height. *Israel J. Math.* **173** (2009), 253–277.

[CDKS] V. Chandee, C. David, D. Koukoulopoulos, and E. Smith, The frequency of elliptic curves over prime finite fields. *Canad. J. Math.* **68** (2016), no. 4, 72–761.

[CFZ] B. Conrey, D. Farmer and M. Zirnbauer, Autocorrelation of ratios of L-functions, *Commun. Number Theory Phys.* **2** (2008), no. 3, 593–636.

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

[DHP] C. David, D. Huynh, and J. Parks, One-level density of families of elliptic curves and the ratios conjectures. *Res. Number Theory* **1** (2015), 1:6.

[DKS] C. David, D. Koukoulopoulos and E. Smith, Sums of Euler products and statistics of elliptic curves *Math. Ann.*, to appear.

[DP] C. David and F. Pappalardi, Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices* 1999, no. 4, 165–183.

[DS1] C. David and E. Smith, Elliptic curves with a given number of points over finite fields. *Compos. Math.* **149** (2013), no. 2, 175–203.

[DS2] C. David and E. Smith, Corrigendum to: Elliptic curves with a given number of points over finite fields. *Compos. Math.*, **150** (2014), no. 8, 1347–1348.

[FM] E. Fouvry and M. R. Murty, On the distribution of supersingular primes. *Canad. J. Math.* **48** (1996), no. 1, 81–104.

[FPS1] D. Fiorilli, J. Parks, and A. Södergren, Low-lying zeros of elliptic curve L-functions: Beyond the ratios conjecture. *Math. Proc. Cambridge Philos. Soc.* **160** (2016), no. 2, 315–351.

[FPS2] D. Fiorilli, J. Parks, and A. Södergren, Low-lying zeros of quadratic Dirichlet L-functions. *Compos. Math.*, to appear.

[FPS3] D. Fiorilli, J. Parks, and A. Södergren, On the transition in the 1-level density of low-lying zeros of quadratic Dirichlet L-functions. In preparation.

[G] E. Gekeler, Frobenius distributions of elliptic curves over finite prime fields. *Int. Math. Res. Not.*, 2003, no. 37, 1999–2018.

[HKS] D. Huynh, J. Keating, and N. Snaith, Lower order terms for the one-level density of elliptic curve L-functions. *J. Number Theory* **129** (2009), no. 12, 2883–2902.

[HMM] D. Huynh, S. Miller, and R. Morrison, An elliptic curve test of the L-functions ratios conjecture. *J. Number Theory* **131** (2011), no. 6, 1117–1147.

[ILS] H. Iwaniec, W. Luo, and P. Sarnak, Low lying zeros of families of L-functions. *Inst. Hautes Études Sci. Publ. Math.* No. 91 (2000), 55–131 (2001).

[J] N. Jones, Elliptic aliquot cycles of fixed length. *Pacific J. Math.* **263** (2013), no. 2, 353–371.

[KS1] N. M. Katz and P. Sarnak, Zeros of zeta functions, their spacings and their spectral nature, preprint, 1997.

[KS2] N. M. Katz, P. Sarnak, Zeroes of zeta functions and symmetry, Bull. Amer. Math. Soc. (N.S.) **36** (1999), no. 1, 1–26.

[KS3] N. M. Katz, P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, American Mathematical Society Colloquium Publications **45**, American Mathematical Society, Providence, RI, 1999.

[Kou] D. Koukoulopoulos, Primes in short arithmetic progressions. *Int. J. Number Theory*, **11** (2015), no. 5, 1499–1521.

[Kow] E. Kowalski, Analytic problems for elliptic curves. *J. Ramanujan Math. Soc.*, **21** (2006) no. 1, 19–114.

[LT] S. Lang and H. Trotter, *Frobenius distributions in GL_2-extensions: Distribution of Frobenius automorphismsin GL_2-extensions of the rational numbers.* Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976.

[Mi1] S. J. Miller, A symplectic test of the L-functions ratios conjecture, Int. Math. Res. Not. IMRN 2008, no. 3, Art. ID rnm146, 36 pp.

[Mi2] S.J. Miller, One- and two-level densities for rational families of elliptic curves: evidence for the underlying group symmetries, *Compos. Math.* **140** (2004), no. 4, 952–992.

[Mo] H. Montgomery, The pair correlation of zeros of the zeta function. *Analytic number theory (Proc. Sympos. Pure Math., Vol. XXIV, St. Louis Univ., St. Louis, Mo., 1972)*, pp. 181–193. Amer. Math. Soc., Providence, R.I., 1973.

[OS1] A. E. Özlük, C. Snyder, Small zeros of quadratic L-functions, Bull. Austral. Math. Soc. **47** (1993), no. 2, 307–319.

[OS2] A. E. Özlük, C. Snyder, On the distribution of the nontrivial zeros of quadratic L-functions close to the real axis, Acta Arith. **91** (1999), no. 3, 209–228.

[P1] J. Parks, Amicable pairs and aliquot cycles on average. *Int. J. Number Theory* **11** (2015), no. 6, 1751–1790.

[P2] J. Parks, An asymptotic for the average number of amicable pairs with an appendix by Sumit Giri. preprint, arxiv:1410.5888.

[P3] J. Parks, A remark on elliptic curves with a given number of points over finite fields. *SCHOLAR–a scientific celebration highlighting open lines of arithmetic research*, 165–179, Contemp. Math., 655, *Amer. Math. Soc., Providence, RI*, 2015.

[R] Z. Rudnick, Traces of high powers of the Frobenius class in the hyperelliptic ensemble, Acta Arith. **143** (2010), no. 1, 81–99.

[Se] J-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* 15 (1972), 259–331.

[SS] J. Silverman and K. Stange, Amicable pairs and aliquot cycles for elliptic curves. *Exp. Math.*, **20** (2011), no. 3, 329–357.

[W] L. Washington, Class numbers of the simplest cubic fields. *Math. Comp.* **48** (1987), no. 177, 371–384.

[Y] M. Young, Low-lying zeros of families of elliptic curves. *J. Amer. Math. Soc.* **19** (2006), no. 1, 205–250.