Introduction to: 1- and 2-Level Densities for Families of Elliptic Curves: Evidence for the Underlying Group Symmetries

Steven J. Miller
Mathematics Department
Princeton University
Princeton, NJ 08544

May 2002

0.1 Note to the Reader

Below is the Introduction from my thesis, followed by bibliographical entries for all works referred to in the introduction. Several equations or theorems from my dissertation are referenced below; the links are not correct. For the correct equation and theorem numbers, see the actual thesis.

0.2 Summary of Thesis Results

0.2.1 Historical Background

In attempting to describe the energy levels of heavy nuclei ([Wig1], [Wig2], [Po], [BFFMPW]), researchers were confronted with daunting calculations for a many bodied system with extremely complicated interaction forces. Unable to explicitly calculate the energy eigenstates, physicists developed Random Matrix Theory to predict general properties of the system.

Let $\mathbf{H}$ represent the Hamiltonian of the system and ψ_E the energy eigenstate with energy E; hence $\mathbf{H}\psi_E = E\psi_E$. The hope was that the Hamiltonian of a many bodied nucleus (such as Uranium, with over 200 protons and neutrons) could be well modeled by a random matrix. Physical symmetries (for example, time reversal symmetry) would constrain the possible operators $\mathbf{H}$ (unitary, Hermitian, real-symmetric, etc.). Similar to ensembles from Statistical Mechanics, one assigns probability measures to matrices from various groups. By explicitly calculating properties associated to an individual matrix and integrating over the group, one can often use the group average to make good predictions about the expected behavior of statistics from a generic, randomly chosen element.

There are striking similarities to statistics associated to energy levels in physics and statistics associated to zeros of L-functions in Number Theory. The non-trivial zeros of an L-function correspond to the energy levels; instead of shooting high energy neutrons at the nucleus (to determine the energy levels), we instead hit the zeros with Schwartz test functions. In physics, we are only able to bombard our nucleus with neutrons whose energy level is restricted in some range; in Number Theory, with present analytic technology, this corresponds to only being able to evaluate sums of Schwartz test functions at the zeros when the functions have compact support in some fixed range.

The first L-function encountered is the Riemann-Zeta function (see, for example, [Da]):

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 - p^{-s}\right)^{-1}, \quad \mathrm{Re}(s) > 1. \tag{0.2.1}$$

While initially defined only for $\mathrm{Re}(s) > 1$, $\zeta(s)$ can be meromorphically continued to the entire complex plane, and satisfies a functional equation:

$$\xi(s) = \Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s) = \xi(1-s). \tag{0.2.2}$$

Due to the functional equation, it is enough to understand the behavior of $\zeta(s)$ for $\text{Re}(s) \geq \frac{1}{2}$. Because of the Gamma factor, $\zeta(s)$ trivially vanishes for s a negative even integer. The Riemann Hypothesis (RH) states all the (non-trivial) zeros have $\text{Re}(s) = \frac{1}{2}$. We call $0 \leq \text{Re}(s) \leq 1$ the critical strip, $\text{Re}(s) = \frac{1}{2}$ the critical line, and $s = \frac{1}{2}$ the critical point.

More generally, we may consider automorphic L-functions (see, for example, [Iw])

$$L(s,f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p L_p(p^{-s}, f)^{-1}, \quad \text{Re}(s) > s_0. \tag{0.2.3}$$

In this thesis we deal with elliptic curves (see [Kn] or [Si1]). Let E be the elliptic curve $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with discriminant Δ. For each prime p, consider the reduced curve E_p: $(a_i)_p = a_i \bmod p$. Let N_p be the number of incongruent solutions (x,y) to $E_p \bmod p$ (including the point at infinity), and define $a_p = p + 1 - N_p$. We form the L-function

$$L(s,E) \quad = \quad \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}. \tag{0.2.4}$$

By the Modularity Theorem for Elliptic Curves ([Wi], [TW], [BCDT]) $L(s,E)$ is analytic, has a functional equation (s into $2-s$), and is equal to $L(s,f)$ for a weight two, level N cuspidal newform, where N is the conductor of the elliptic curve. By sending $s \to s + \frac{1}{2}$, the functional equation is now s into $1-s$, and again the critical strip is $0 \leq \text{Re}(s) \leq 1$. The Generalized Riemann Hypothesis (GRH) asserts that all (non-trivial) zeros have $\text{Re}(s) = \frac{1}{2}$.

0.2.2 n-Level Correlations

In an impressive set of computations, starting with the $10^{20\text{th}}$ zero of $\zeta(s)$ (see, for example, [Od1], [Od]), Odlyzko studied the normalized spacings between adjacent zeros and found remarkable agreement with Random Matrix Theory. Specifically, consider the set of $N \times N$ random Hermitian matrices with entries chosen from the Gaussian distribution (the GUE). As $N \to \infty$, the limiting distribution of spacings between adjacent eigenvalues is indistinguishable from what Odlyzko observed!

Additionally, one can study the n-level correlations. Let $\{\alpha_j\}_{j=1}^N$ be an increasing sequence of numbers. In practice, we will take these to be either zeros of an L-function or eigenvalues of a matrix. For a compact box $B \subset \mathbb{R}^{n-1}$ we define the n-level correlation by

$$\frac{\#\Big\{(\alpha_{j_1} - \alpha_{j_2}, \dots, \alpha_{j_{n-1}} - \alpha_{j_n}) \in B, j_i \in \{1,\dots,N\}, j_i = j_k \text{ iff } i = k\Big\}}{N} \tag{0.2.5}$$

Instead of using a box, one can study a smoothed version with a test function on $\mathbb{R}^n$ (see [RS]). For test functions whose Fourier Transform has small support, Montgomery [Mon] proved the 2- and Hejhal [Hej] proved the 3-level correlations for the zeros of $\zeta(s)$ are the same as that of the GUE, and Rudnick-Sarnak [RS] proved the n-level correlations for all automorphic cuspidal L-functions are the same as the GUE.

The universality that Rudnick and Sarnak observed is somewhat surprising, but explainable as follows: the correlations are controlled by the second moments of the a_p's, and while there are many possible limiting distributions for the a_p's, they all have the same second moment.

Unfortunately, many different systems will have the same n-level correlations. Consider the classical compact groups: $U(N)$, $SU(N)$, $USp(2N)$, $SO(\text{even})$ and $SO(\text{odd})$. Fix a group, and choose a generic matrix element. Calculating the n-level correlations of its eigenvalues, integrating over the group, and taking the limit as $N \to \infty$, Katz and Sarnak prove the resulting answer is universal, independent of the particular group chosen. In particular, we cannot use the n-level correlations to distinguish GUE behavior, $U(N)$, from the other classical compact groups.

This brings up the intriguing possibility of investigating a statistic more sensitive to the underlying symmetry or structure than the n-level correlations. Following Iwaniec-Luo-Sarnak and Rubinstein, we introduce the concept of a family and n-level density for low lying zeros, and find a statistic which will depend on finer properties of the family.

0.2.3 Families and n-Level Density

Let $L(s, f)$ be the L-function associated to f. If we were to directly study the distribution of its zeros, there are two natural ways to proceed. First, we may take ever larger sets of zeros, normalize each by its average spacing, and then look at related statistics. Second, we may attempt to study the behavior of the low lying zeros (ie, those zeros near the critical point, $s = \frac{1}{2}$).

The first method leads to the n-level correlations, which are insensitive to the behavior of the low lying zeros. For example, fix a compact box $B \subset \mathbb{R}^{n-1}$ and a positive integer k. Consider the contributions to the n-level correlation from the first k zeros. Since the box is compact, provided the zeros tend to infinity, only finitely many will give us an n-tuple in the box if we force one of the zeros to be from the first k zeros. Letting N tend to infinity, we see there is no net contribution from these zeros. Note it is crucial that we take n distinct zeros in the definition of the n-level correlation. Thus, we may remove finitely many zeros without changing this statistic.

In many instances, the behavior of $L(f, \frac{1}{2})$ encodes critical information about the function. For example, for L-functions of elliptic curves, the order of vanishing of $L(s, E)$ at $s = \frac{1}{2}$ is conjecturally equal to the geometric rank of the Mordell-Weil group (Birch and Swinnerton-Dyer conjecture; known to be true when the function vanishes to at most first order: see [CW], [Ko]). The point $s = \frac{1}{2}$ is clearly special, as it is the center of the critical strip, and leads to the fascinating possibility that there could be a difference in spacing statistics for zeros near $\frac{1}{2}$ than zeros higher up; as we've remarked, if we look at large batches of zeros, this information will be drowned out. For example, if we force the Mordell-Weil group to be large, we expect many zeros exactly at $s = \frac{1}{2}$, and this might influence the behavior of the neighboring zeros. Hence we are led to study the distribution of the first few, or low lying, zeros.

By (often time consuming) computation, we can calculate the zeros of $L(f,s)$. Once found, we can try to interpret the results in terms of natural quantities associated to our function: how many zeros are there at $s = \frac{1}{2}$? How do the heights of the zeros above the critical point compare to the coefficients and special quantities of our function?

Similar to choosing an $N \times N$ matrix at random and calculating its eigenvalues, we only get one string of values. If, however, we can find a large number of functions similar to our original one, then we may calculate the zeros of each, and see how they vary from function to function.

This leads us to the concept of *family*. Roughly, a family will be a collection of geometric objects and their associated L-functions, where the geometric objects have similar properties. (In nuclear physics, this corresponds to amalgamating energy resonance data from different elements with similar invariants).

Iwaniec, Luo and Sarnak [ILS] considered (among others) all cuspidal newforms of a given level and weight. Rubinstein [Ru] considers twists by fundamental discriminants $D \in [N, 2N]$ of a fixed modular form.

In this thesis, we study the family of all elliptic curves and one-parameter families of elliptic curves. Thus, in our case the notion of family is the standard one from geometry: we have a collection of curves over a base, and the geometry is much clearer in our examples than in [ILS] and [Ru].

Explicitly, we will consider the family of all elliptic curves,

$$\mathcal{F} : y^2 = x^3 + ax + b,\ a \in [N^2, 2N^2],\ b \in [N^3, 2N^3], \tag{0.2.6}$$

and one-parameter families

$$\begin{aligned} \mathcal{F} : y^2 + a_1(t)xy + a_3(t)y &= x^3 + a_2(t)x^2 + a_4(t)x + a_6(t) \\ & \quad a_i(t) \in \mathbb{Z}[t],\ t \in [N, 2N]. \end{aligned} \tag{0.2.7}$$

Let $f(x)$ be an even Schwartz function whose Fourier Transform is supported in a neighborhood of the origin. We assume f is of the form $\prod_{i=1}^n f_i(x_i)$, although at the expense of more complicated notation we may drop this assumption.

We define the n-level density by

$$D_{n,\mathcal{F}}(f) = \frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} \sum_{\substack{j_1, \dots, j_n \\ j_i \neq \pm j_k}} f_1\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j_1)}\Big) \cdots f_n\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j_n)}\Big), \tag{0.2.8}$$

where $\gamma_E^{(j_i)}$ runs through the non-trivial zeros of the curve E, and N_E is its conductor. We rescale the zeros by $\log N_E$ as this is the order of the number of zeros with imaginary part less than a large absolute constant. See [ILS].

We use the Explicit Formula (Theorem **??**) to relate sums of test functions over zeros to sums over primes of $a_E(p)$ and $a_E^2(p)$.

$$\sum_{\gamma_E^{(j)}} G\Big(\frac{\log N_E}{2\pi}\gamma_E^{(j)}\Big) = \widehat{G}(0) + G(0) - 2\sum_p \frac{\log p}{\log N_E}\frac{1}{p}\widehat{G}\Big(\frac{\log p}{\log N_E}\Big)a_E(p) \\ -2\sum_p \frac{\log p}{\log N_E}\frac{1}{p^2}\widehat{G}\Big(\frac{2\log p}{\log N_E}\Big)a_E^2(p) + O\big(\frac{\log\log N_E}{\log N_E}\big) \tag{0.2.9}$$

Simple combinatorics removes the $j_i = \pm j_k$ terms, and we obtain $D_{n,\mathcal{F}}(f)$. For $\widehat{F}$ of small support, for many families and $n \leq 2$, we show as $|\mathcal{F}| \to \infty$,

$$D_{n,\mathcal{F}}(f) \to \int \cdots \int f_1(x_1)\cdots f_n(x_n) W_{n,\mathcal{G}}(x_1, \cdots, x_n) dx_1 \cdots dx_n, \tag{0.2.10}$$

where $\mathcal{G} = \mathcal{G}(\mathcal{F})$ is the symmetry group associated to the family. For families of elliptic curves, geometric considerations ([KS1], [KS2]) lead one to expect orthogonal symmetries.

Which of the three orthogonal groups arises is controlled by the distribution of signs of the functional equation: we expect $\mathcal{G}$ to be SO(even) if every curve is even, SO(odd) if every curve is odd, and O if we have equidistribution in sign.

Katz and Sarnak [KS1] determined the $N \to \infty$ limits:

$\mathcal{G}$	$W_{n,\mathcal{G}}$
$U(N)$, $U_k(N)$	$\det\Big(K_0(x_j,x_k)\Big)_{1\leq j,k\leq n}$
$USp(N)$	$\det\Big(K_{-1}(x_j,x_k)\Big)_{1\leq j,k\leq n}$
SO(even)	$\det\Big(K_1(x_j,x_k)\Big)_{1\leq j,k\leq n}$
SO(odd)	$\det\Big(K_{-1}(x_j,x_k)\Big)_{1\leq j,k\leq n} + \sum_{\nu=1}^n \delta(x_\nu)\det\Big(K_{-1}(x_j,x_k)\Big)_{1\leq j,k\neq\nu\leq n}$

where

$$K_\epsilon(x,y) = \frac{\sin\Big(\pi(x-y)\Big)}{\pi(x-y)} + \epsilon\frac{\sin\Big(\pi(x+y)\Big)}{\pi(x+y)}. \tag{0.2.11}$$

0.2.4 Expression for $D_{1,\mathcal{F}}(f)$

Using the Explicit Formula to relate sums of a function f against zeros of an L-function to sums of its Fourier Transform against primes, we evaluate not $\int f(x)W_{n,\mathcal{G}}(x)dx$ but $\int \widehat{f}(y)\widehat{W_{n,\mathcal{G}}}(y)dy$. Denoting SO(even) (SO(odd)) by O^+ (O^-), the Fourier Transforms for the 1-level densities are

$$\begin{aligned}
\widehat{W_{1,O^+}}(u) &= \delta_0(u) + \frac{1}{2}\eta(u) \\
\widehat{W_{1,O}}(u) &= \delta_0(u) + \frac{1}{2} \\
\widehat{W_{1,O^-}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) + 1 \\
\widehat{W_{1,Sp}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) \\
\widehat{W_{1,U}}(u) &= \delta_0(u).
\end{aligned} \tag{0.2.12}$$

where $\eta(y)$ is 1, $\frac{1}{2}$, and 0 for $|y|$ less than 1, 1, and greater than 1, and δ_0 is the standard Dirac Delta functional. Note that the first three densities agree for $|y| < 1$ and split (ie, become distinguishable) for $|y| \geq 1$, but are all distinguishable from U for any support. Hence, unlike the n-level correlations over all zeros, the 1-level density is already sufficient to observe non-GUE and non-symplectic behavior.

It is very difficult to evaluate the relevant sums over zeros (which become sums over primes by the Explicit Formula) for test functions $\widehat{F}$ with large support. Brumer and Heath-Brown ([Br], [BHB5]) have done the family of all elliptic curves with support less than $\frac{2}{3}$; twists of a given curve have been done for support less than 1. Implicit in the work of Silverman [Si3] is an analysis of the 1-level density for many one-parameter families of elliptic curves, but with very small support.

Unfortunately, none of these are sufficient to determine which is the underlying symmetry group. Further, previous investigations have rescaled each curve's zeros by the average of the logarithms of the conductors. This simplifies the calculations; however, the normalization is no longer natural for each curve. In this thesis we perform both calculations (normalizing each curve's zeros by the correct local quantity $\log N_E$, and by the average log-conductor $\log M = \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} \log N_E$).

0.2.5 Expression for $D_{2,\mathcal{F}}(f)$

Theorem 0.2.1 (2-Level Densities for the Classical Compact Groups) *Let $c(\mathcal{G}) = 0$, $\frac{1}{2}$ or 1 for $\mathcal{G} = SO(even)$, O, and $SO(odd)$. For $\mathcal{G}$ one of these three groups we have*

$$\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 = \left[\widehat{f_1}(0) + \frac{1}{2}f_1(0)\right]\left[\widehat{f_2}(0) + \frac{1}{2}f_2(0)\right]$$

$$+ 2\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - 2\widehat{f_1 f_2}(0) - f_1(0)f_2(0) + \ c(\mathcal{G})f_1(0)f_2(0).$$

For $\mathcal{G} = U$ we have

$$\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,U}}(u)du_1du_2 \quad = \quad \widehat{f_1}(0)\widehat{f_2}(0) + \int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - \widehat{f_1 f_2}(0),$$

and for $\mathcal{G} = Sp$, we have

$$\begin{aligned}\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 \quad &= \quad \left[\widehat{f_1}(0) + \frac{1}{2}f_1(0)\right]\left[\widehat{f_2}(0) + \frac{1}{2}f_2(0)\right] \\ &+ 2\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - 2\widehat{f_1 f_2}(0) - f_1(0)f_2(0) \\ &- f_1(0)\widehat{f_2}(0) - \widehat{f_1}(0)f_2(0) + 2f_1(0)f_2(0).\end{aligned}$$

These densities are all distinguishable for functions with arbitrarily small support.

Assume the family has rank r over $\mathbb{Q}(t)$. By the Birch and Swinnerton-Dyer conjecture, Silverman's Specialization Theorem [Si2] implies $\exists t_0$ such that $\forall t \geq t_0$, the rank of E_t is at least r. We call these the *family zeros.*

As, in the limit, each curve's L-function has r zeros at the critical point, we isolate the contribution of these zeros from the 2-level density. After performing the necessary combinatorics, we are left with two pieces: the contribution from the family zeros, and the contribution from the remaining zeros.

The contribution to the 2-level density from the r family zeros is

$$r\widehat{f_1}(0)f_2(0) + rf_1(0)\widehat{f_2}(0) + (r^2 - r)f_1(0)f_2(0). \tag{0.2.13}$$

Let $D^{(r)}_{n,\mathcal{F}}(f)$ be the n-level density for the non-family zeros; ie, what is left after removing the trivial contributions from the r family zeros.

The utility of the 2-level density is that, even for functions with arbitrarily small support, the three likely candidate orthogonal symmetries *are* distinguishable, and in a very satisfying way. The three candidates differ by a factor which encodes the distribution of sign in the family, and all differ from the GUE's 2-level density.

While the 1-level density is sufficient to distinguish the various symmetry groups, it can only do so for large support (support at least 1). For some families, this is not a problem (see [ILS]); however, for elliptic curves, the polynomial growth of the conductor in a family makes even moderate support unreachable at present. This is why we concentrate on 2 and higher level densities.

0.2.6 Results

To calculate the 1-level density, we do not need to know any information about the sign of the functional equations. For the 2-level density, all we need is the percent of curves with even and odd functional equation. For the higher level densities, we need more than the percentage of odd / even; we need to know which curves are odd and which are even. For the family of all elliptic curves, or any family where we expect equidistribution in sign, this becomes a daunting challenge; however, the 2-level density *is* sufficient to distinguish the three groups.

Following Iwaniec-Luo-Sarnak [ILS] and Rubinstein [Ru], we calculated the 1- and 2-level densities for families of elliptic curves. The main result is Theorem **??**:

Rational Surfaces Density Theorem: *Consider a one-parameter family of elliptic curves of rank r over $\mathbb{Q}(t)$ that is a rational surface. Assume GRH, $j(t)$ non-constant, and the ABC conjecture if $\Delta(t)$ has an irreducible polynomial factor of degree at least 4. Let f_i be an even Schwartz function of small but non-zero support σ_i ($\sigma_1 < \min(\frac{1}{2}, \frac{2}{3m})$ for the 1-level density, $\sigma_1 + \sigma_2 < \frac{1}{3m}$ for the 2-level density), and $m = deg\ C(t)$. Assume the Birch and Swinnerton-Dyer conjecture for interpretation purposes. Possibly after passing to a subsequence,*

$$\begin{aligned} D_{1,\mathcal{F}}^{(r)}(f_1) &= \widehat{f_1}(0) + \frac{1}{2}f_1(0) \\ D_{2,\mathcal{F}}^{(r)}(f) &= \prod_{i=1}^{2}\left[\widehat{f_i}(0) + \frac{1}{2}f_i(0)\right] + 2\int_{-\infty}^{\infty}|u|\widehat{f_1}(u)\widehat{f_2}(u)du \\ &\quad -2\widehat{f_1 f_2}(0) - f_1(0)f_2(0) + (f_1f_2)(0)N(\mathcal{F},-1), \quad (0.2.14) \end{aligned}$$

where $N(\mathcal{F},-1)$ is the percent of curves with odd sign. The 1-level density of the non-family zeros, for small support, agrees with $SO(even)$, O, and $SO(odd)$. The 2-level density of the non-family zeros, for small support, agrees with $SO(even)$, O, and $SO(odd)$ depending on whether the signs are all even, equidistributed in the limit, or all odd. Thus, as our families have orthogonal symmetries, the densities of the non-family zeros agree with Katz and Sarnak's predictions, at least for small support.

We study several families of constant sign, and show the density is as expected. Thus, for these constant sign families, the 2-level density reflects the predicted symmetry, which is invisible through the 1-level density because of support considerations.

Similar to the universality Rudnick and Sarnak [RS] found in studying n-level correlations of L-functions, our universality follows from the sums of $a_t^2(p)$ in our families (the second moments). For non-constant $j(t)$, this follows from a Sato-Tate law proved by P. Michel [Mi] (Theorem **??**); however, for many of our families show this by direct calculation. While Michel's result is sufficient to prove the observed universality (modulo the distribution of signs), his evaluation of the second moment for the family has a large error term, which is not surprising as his result holds for all families. For many families, we are able to explicitly determine the lower order corrections to the second moment. While these terms (in the limit) do not contribute to the n-level density, for many families considered there is a positive contribution of size $\frac{1}{\log N}$ to the densities.

0.2.7 Outline of the Proof of Theorem ??

Using standard methods as well as a new construction, we construct families of elliptic curves of rank r over $\mathbb{Q}(t)$. For a prime p and a curve $E_t \in \mathcal{E}$, let

$$\begin{aligned} a_t(p) &= \sum_{x=0}^{p-1} \left(\frac{f_{E_t}(x)}{p} \right) = O(\sqrt{p}) \\ A_{\mathcal{E}}(p) &= \frac{1}{p} \sum_{t=0}^{p-1} a_{E_t}(p) = O(1). \end{aligned} \tag{0.2.15}$$

The first statement is just Hasse's Theorem; the second follows from Deligne [De]. Silverman and Rosen [RSi] prove

Theorem 0.2.2 (Silverman-Rosen) *For an elliptic surface (a one-parameter family), assume Tate's conjecture. Then*

$$\lim_{X \to \infty} \sum_{p \leq X} -A_{\mathcal{E}}(p) \log p = \text{rank } \mathcal{E}(\mathbb{Q}(t)) \tag{0.2.16}$$

Most of our examples are rational surfaces, where Tate's conjecture is known. Let

$$A_{r,\mathcal{F}}(p) = \sum_{t(p)} a_t^r(p). \tag{0.2.17}$$

Note $A_{1,\mathcal{F}}(p) = pA_{\mathcal{E}}(p)$. Knowledge of $A_{1,\mathcal{F}}(p)$ and $A_{2,\mathcal{F}}(p)$ is all we need to determine $D_{2,\mathcal{F}}(f)$ for surfaces where Tate's conjecture is known (modulo, of course, GRH, the distribution of sign of the functional equations, and being able to get a good handle on how the conductors vary with t. The last is the difficult part of the proof).

For any one parameter family, if $p_1, \dots, p_n$ are distinct primes,

$$\sum_{t(p_1 \cdots p_n)} a_{t_1}^{r_1}(p_1) \cdots a_{t_n}^{r_n}(p_n) = A_{r_1,\mathcal{F}}(p_1) \cdots A_{r_n,\mathcal{F}}(p_n). \tag{0.2.18}$$

We substitute the above into the Explicit Formula. There is no contribution if any of the r_i's is greater than 2. If Tate's conjecture is true, we can interpret sums of $A_{1,\mathcal{F}}(p)$ in terms of the rank over $\mathbb{Q}(t)$. See Lemma **??**.

We are left with determining $A_{2,\mathcal{F}}(p)$, performing the necessary combinatorial arguments, handling the conductors, and determining the distribution of signs. By clever choice and delicate character sums, we can often evaluate $A_{2,\mathcal{F}}(p)$ directly without recourse to higher theorems, although Michel's result (Theorem **??**) is often, though not always, applicable.

Equation 0.2.18 can be generalized to apply to the family of all elliptic curves; unfortunately, the method of proof used is very specific to elliptic curves, and crucially uses the fact that $a_{t+mp}(p) = a_t(p)$.

To handle the conductors, we show that by passing to a subsequence, and then sieving an auxiliary polynomial to being square-free (see Theorem **??**), the conductors are given by a monotone integer polynomial. As the construction works for any family with deg $\Delta(t) \leq 12$, modulo the distribution of signs, we are able to prove the 1- and 2-level densities for a sub-family of any rational one-parameter family.

The main difficulty in the proof is the t-dependence in the conductors. It required very delicate arguments to handle it. For comparison purposes, we give a simple proof of the corresponding results for the rescaled densities.

In their investigations of 1-level densities for weight k cuspidal newforms of level N, Iwaniec, Luo and Sarnak evaluate $\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}} a_f(m)a_f(n)$ by application of the Petersson Formula; for us, Equation 0.2.18 is our best analogue (for small support) to the Petersson Formula.

0.2.8 Applications

To date, there are two main applications of investigating higher level densities ($n > 1$). First, it provides evidence that the underlying group symmetries really are SO(even), O and SO(odd), and which group depends only on the distribution of signs. For supports reachable by present methods, the 1-level density is unable to distinguish the three candidates; the 2-level density can, and does not necessitate knowing *which* curves in a family are odd; all that is needed is the percent. Of course, for most families it is only conjectured that there is equidistribution in sign. Nevertheless, there are a few special constant-sign families which provide the first examples of a family of elliptic curves where we can definitively say which of the three candidates works; moreover, the expected candidate is the observed one.

Second, we obtain improved estimates of the percent of curves with high rank above the family rank. Unfortunately, the arguments are not useful for rank slightly above the family rank, and are therefore useless (unless we can greatly increase the support) in putting to rest the 'Excess Rank' question.

Briefly, assume equidistribution of sign. Then $D_{1,\mathcal{F}}(f) = \widehat{f_1}(0) + \frac{1}{2}f_1(0) + rf_1(0)$. To estimate the percent with rank at least $r+R$, P_R, we get $Rf(0)P_R \leq \widehat{f_1}(0) + \frac{1}{2}f_1(0)$, $R > 1$. Note the family rank r has been cancelled from both sides.

By using the 2-level density, however, we get *squares* of the rank on the left hand side. (Sometimes it's better to use, not the 2-level density, but a close cousin where we don't require the sums to be over distinct zeros). The advantage is we get a cross term rR. The disadvantage is our support is smaller. Assume we can calculate the 1-level density for functions of support $< \sigma$. Let $f(x_1, x_2) = \prod_i f_i(x_i)$, $\text{supp}(f_i) = \sigma_i$. While we expect to be able to calculate $D_{2,\mathcal{F}}(f)$ for $\sigma_1 + \sigma_2 \leq \sigma$, our method of proof yields the weaker $\sigma_1 + \sigma_2 \leq \frac{\sigma}{2}$; however, once R is large, the 2-level density yields better results.

Third, some of the families have interesting potential lower order density terms. A detailed analysis of the correction to the second moment of the $a_t(p)$'s (and $a_E(p)$ for the family of all elliptic curves) sheds some light on the Excess Rank phenomenon observed by Fermigier and others. Consider a family of elliptic curves $\mathcal{E}$ of rank r over $\mathbb{Q}(t)$. By Silverman's Specialization Theorem [Si2], for t sufficiently large, the rank of E_t over $\mathbb{Q}$ is at least r. If we assume equidistribution of sign, we might expect half the curves to have rank r and half rank $r+1$. For many families (though all with constant $A_{\mathcal{E}}(p)$), Fermigier [Fe2] observed approximately 32% had rank r, 18% rank $r+2$, and 48% rank $r+1$, 2% rank $r+3$. The Excess Rank question is: will the 18% persist for large values of N?

The correction term to the second moment, as remarked before, results in a potential contribution to the 1-level density. We can only say potential as the error terms propagating through our proofs are of size $\frac{\log \log N}{\log N}$! A significantly more delicate analysis is needed; however, assuming reasonable cancellation, these corrections do indicate the possibility of lower order terms in the densities.

In estimating the number of curves of a given rank, this leads to slightly higher theoretical bounds for small N, though of course, in the limit, the bounds converge to what we get by ignoring the corrections. The existence of these lower order corrections opens up the exciting possibility of detecting fine structure distinguishing families of elliptic curves which, at first glance, seem to have the same underlying group symmetry.

0.2.9 Notation

We follow standard notation. All elliptic curves are over $\mathbb{Q}$. We consider one-parameter families $E_t : y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x + a_4(t) + a_6(t)$, $a_i(t)$ is an integer polynomial.

By ([TW], [Wi] and [BCDT]), all elliptic curves are modular. Hence we may freely use $L(s, E)$ and its functional equation.

Definition 0.2.3 (n-Level Density) *$D_{n,\mathcal{F}}(f)$ is the n-level density of the family $\mathcal{F}$ with test function $f(x) = \prod_i f_i(x)$. Each curve's zeros are rescaled by the logarithm of its conductor. In the explicit formula we sum over all n-tuples $(j_1, \dots, j_n)$ with $j_i \neq \pm j_k$.*

A related quantity often encountered is

Definition 0.2.4 *$D^*_{n,\mathcal{F}}(f)$ is the n-level density without the combinatorics; ie, the sums are over all n-tuples of zeros.*

Rescaling each curves' zeros by the logarithm of its conductor gives the correct local scaling; it is, however, significantly harder to handle these sums. We often study a related quantity:

Definition 0.2.5 (Modified n-Level Density) *$D'_{n,\mathcal{F}}(f)$ differs from the n-level density by rescaling each curve's zeros by the average log-conductor, $\log M = \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} \log N_E$, instead of by $\log N_E$.*

Finally (under certain assumptions), our families often have r family zeros at the critical point. Removing the contributions from these zeros yields

Definition 0.2.6 *$D^{(r)}_{n,\mathcal{F}}(f)$ is the n-level density with the contribution from r critical point zeros removed.*

0.2.10 Assumptions

We assume the following at various points in the thesis:

Generalized Riemann Hypothesis (for Elliptic Curves) *Let $L(s,E)$ be the (normalized) L-function of the elliptic curve E. Then the non-trivial zeros of $L(s,E)$ satisfy $Re(s) = \frac{1}{2}$.*

Occasionally we assume the Riemann Hypothesis for the Riemann Zeta-function and Dirichlet L-functions.

Birch and Swinnerton-Dyer Conjecture [BSD1], [BSD2] *Let E be an elliptic curve of geometric rank r over $\mathbb{Q}$ (the Mordell-Weil group is $\mathbb{Z}^r \oplus T$, T is the subset of torsion points). Then the analytic rank (the order of vanishing of the L-function at the critical point) is also r.*

We assume the above only for interpretation purposes.

Tate's Conjecture for Elliptic Surfaces [Ta] *Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E},s)$ be the L-series attached to $H^2_{\acute{e}t}(\mathcal{E}/\overline{\mathbb{Q}},\mathbb{Q}_l)$. Then $L_2(\mathcal{E},s)$ has a meromorphic continuation to $\boldsymbol{C}$ and satisfies $-ord_{s=2}L_2(\mathcal{E},s) = rankNS(\mathcal{E}/\mathbb{Q})$, where $NS(\mathcal{E}/\mathbb{Q})$ is the $\mathbb{Q}$-rational part of the Néron-Severi group of $\mathcal{E}$. Further, $L_2(\mathcal{E},s)$ does not vanish on the line $Re(s) = 2$.*

Most of the one-parameter families we investigate are rational surfaces, where Tate's conjecture is known. See, for example, [RSi].

ABC Conjecture *Fix $\epsilon > 0$. For coprime positive integers a, b and c with $c = a + b$ and $N(a,b,c) = \prod_{p|abc} p$, $c \ll_\epsilon N(a,b,c)^{1+\epsilon}$.*

The full strength of ABC is never needed in the arguments below; rather, we need a consequence of ABC, the Square-Free Sieve (see [Gr]):

Square-Free Sieve Conjecture *Fix an irreducible polynomial $f(t)$ of degree at least 4. As $N \to \infty$, the number of $t \in [N, 2N]$ with $D(t)$ divisible by p^2 for some $p > \log N$ is $o(N)$.*

For irreducible polynomials of degree at most 3, the above is known, complete with a better error than $o(N)$. See [Ho], chapter 4.

We use the Square-Free Sieve for the following: let $D(t)$ be the product of the irreducible polynomial factors of $\Delta(t)$. If no square divides $D(t)$ for all t, for $D(t)$ square-free we can often compute the conductors $C(t)$ exactly, obtaining $C(t)$ is an integral polynomial. By inclusion / exclusion, we can handle the sieving by factors $d < \log N$; we need the Square-Free Sieve to bound the number of $t \in [N, 2N]$ with $D(t)$ divisibly by p^2 for some $p > \log N$. (If $\forall t$, a square B divides $D(t)$, instead of sieving to $D(t)$ square-free we sieve to $D(t)$ square-free save for primes $p|B$, where the power of $p|D(t)$ is independent of t). We call such t (or $D(t)$) good.

The Sign Conjecture for Elliptic Curves states, in the limit, half of all curves have even functional equation and half have odd. Of course, this may depend on the method of parametrization. We often only need a restricted version, namely

Restricted Sign Conjecture (for the Family $\mathcal{F}$) *Consider a 1-parameter family $\mathcal{F}$ of elliptic curves. As $N \to \infty$, the signs of the curves E_t are equidistributed for $t \in [N, 2N]$.*

The Restricted Sign conjecture sometimes fails. First, there are families with constant $j(t)$ where all curves have the same sign. Rizzo [Ri] shows that for the family

$$E_t : y^2 = x^3 + tx^2 - (t+3)x + 1, \quad j(t) = 256(t^2 + 3t + 9), \tag{0.2.19}$$

for every $t \in \mathbb{Z}$, E_t has odd functional equation. This example is due to Washington [Wa]. Further, Rizzo proves for the family

$$E_t : y^2 = x^3 + \frac{t}{4}x^2 - \frac{36t^2}{t-1728}x - \frac{t^3}{t-1728}, \quad j(t) = t, \tag{0.2.20}$$

as t ranges over $\mathbb{Z}$, in the limit 50.1859% have even functional equation and 49.8141% have odd functional equation.

Failure of the Restricted Sign conjecture by all curves in a family having the same sign is easily manageable; in fact, it is only in such cases that we are able to explicitly determine all n-level densities. Failure such as Rizzo's second example, with a split other than $100\% - 0\%$ or $50\% - 50\%$, leads to a non-equal mixing of $SO(\text{even})$ and $SO(\text{odd})$.

Helfgott [Hel] has recently related the Restricted Sign conjecture to the Square-Free Sieve conjecture and standard conjectures on sums of Moebius:

Polynomial Moebius *Let $f(t)$ be an irreducible polynomial such that no fixed square divides $f(t)$ for all t. Then $\sum_{t=N}^{2N} \mu(f(t)) = o(N)$.*

The Polynomial Moebius conjecture is known for linear $f(t)$.

Helfgott shows ABC and Polynomial Moebius imply the Restricted Sign conjecture for many families. More precisely, let $M(t)$ be the product of irreducible polynomials dividing $\Delta(t)$ and not $c_4(t)$.

Theorem 0.2.7 (Equidistribution of Sign in a Family) *Let $\mathcal{F}$ be a one-parameter family with coefficients integer polynomials in $t \in [N, 2N]$. If $j(t)$ and $M(t)$ are non-constant, then the signs of E_t, $t \in [N, 2N]$, are equidistributed as $N \to \infty$. Further, if we restrict to good t, $t \in [N, 2N]$ such that $D(t)$ is good (usually square-free), the signs are still equidistributed in the limit.*

In Appendix **??** we numerically investigate the conjectured equidistribution of sign for a representative family with $j(t)$ and $M(t)$ non-constant. It is a pleasure to thank Atul Pokharel for providing the graphs.

0.2.11 Organization of the Thesis

We first enumerate several useful results for calculating the 1- and 2-level densities. We calculate these densities for the classical compact groups, and a useful expansion for the densities for families of elliptic curves. We prove our result on sub-families of rational one-parameter elliptic surfaces.

Next, we calculate the densities for several families of elliptic curves of constant sign, followed by many examples where the signs vary.

We then use the 2-level density to obtain improved bounds on the percent of elliptic curves with high rank above the rank of the family over $\mathbb{Q}(t)$.

We show for many one-parameter rational elliptic surfaces there is a strong possibility that there is a lower order correction term to the densities. As the term is of size $\frac{1}{\log N}$; to show it really is present requires a significantly more detailed analysis of all previous error terms.

Finally, we sketch the complications that arise in studying the 3- and higher level densities in non-constant sign families, and provide numerous appendices for calculations used in the thesis.

Bibliography

[BSD1] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. I*, J. reine angew. Math. **212**, 1963, 7 − 25.

[BSD2] B. Birch and H. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. reine angew. Math. **218**, 1965, 79 − 108.

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over **Q**: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14**, no. 4, 2001, 843 − 939.

[BFFMPW] T. Brody, J. Flores, J. French, P. Mello, A. Pandey, S. Wong, *Random-matrix physics: spectrum and strength fluctuations*, Rev. Mod. Phys. vol. **53**, no. 3, July 1981, 385 − 479.

[Br] A. Brumer, *The average rank of elliptic curves I*, Invent. Math. **109**, 1992, 445 − 472.

[BHB5] A. Brumer and R. Heath-Brown, *The average rank of elliptic curves V*, preprint.

[CW] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnterton-Dyer*, Invent. Math. **39**, 1977, 43 − 67.

[Da] H. Davenport, *Multiplicative Number Theory,* 2*nd edition*, Graduate Texts in Mathematics **74**, Springer-Verlag, New York, 1980, revised by H. Montgomery.

[De] P. Deligne, *La conjecture de Weil. II* Inst. Hautes Études Sci. Publ. Math. **52**, 1980, 137 − 252.

[Di] F. Diamond, *On deformation rings and Hecke rings*, Ann. Math. **144**, 1996, 137 − 166.

[Fe2] S. Fermigier, *Étude expérimentale du rang de familles de courbes elliptiques sur* $\mathbb{Q}$, Exper. Math. **5**, 1996, 119 − 130.

[Gr] Granville, *ABC Allows Us to Count Squarefrees*, International Mathematics Research Notices **19**, 1998, 991 − 1009.

[Hej] D. Hejhal, *On the triple correlation of zeros of the zeta function*, Internat. Math. Res. Notices 1994, no. 7, 294 – 302.

[Hel] H. Helfgott, *Average root numbers in families of elliptic curves and the average of the Moebius function on integers represented by a polynomial*, preprint.

[Ho] C. Hooley, *Applications of Sieve Methods to the Theory of Numbers*, Cambridge University Press, Cambridge, 1976.

[Iw] H. Iwaniec, *Topics in Classical Automorphic Forms*, American Mathematical Society, Graduate Studies in Mathematics, vol. **17**, Providence, 1997.

[ILS] H. Iwaniec, W. Luo and P. Sarnak, *Low lying zeros of families of L-functions*, Inst. Hautes Études Sci. Publ. Math. **91**, 2000, 55 – 131.

[KS1] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications **45**, AMS, Providence, 1999.

[KS2] N. Katz and P. Sarnak, *Zeros of zeta functions and symmetries*, Bull. AMS **36**, 1999, 1 – 26.

[Kn] A. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, 1992.

[Ko] V. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990), Math. Soc. Japan, Tokyo, 1991, 429 – 436.

[Mi] P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Monat. Math. **120**, 1995, 127 – 136.

[Mon] H. Montgomery, *The pair correlation of zeros of the zeta function*, Analytic Number Theory, Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence, 1973, 181 – 193.

[Od1] A. Odlyzko, *On the distribution of spacings between zeros of the zeta function*, Math. Comp. **48**, 1987, no. 177, 273 – 308.

[Od] A. Odlyzko, *The* 10^{22}*-nd zero of the Riemann zeta function*, Proc. Conference on Dynamical, Spectral and Arithmetic Zeta-Functions, M. van Frankenhuysen and M. L. Lapidus, eds., Amer. Math. Soc., Contemporary Math. series, 2001, http://www.research.att.com/∼amo/doc/zeta.html

[Po] C. Porter (editor), Statistical Theories of Spectra: Fluctuations, Academic Press, 1965.

[Ri] Rizzo, *Average root numbers for a non-constant family of elliptic curves*, preprint.

[RSi] M. Rosen and J. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133**, 1998, 43 – 67.

[Ru] M. Rubinstein, *Evidence for a spectral interpretation of the zeros of L-functions*, P.H.D. Thesis, Princeton University, 1998, http://www.ma.utexas.edu/users/miker/thesis/thesis.html.

[RS] Z. Rudnick and P. Sarnak, *Zeros of principal L-functions and random matrix theory*, Duke Journal of Math. **81**, 1996, 269 – 322.

[Si1] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, Berlin - New York, 1986.

[Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, Berlin - New York, 1994.

[Si3] J. Silverman, *The average rank of an algebraic family of elliptic curves*, J. reine angew. Math. **504**, 1998, 227 – 236.

[Ta] J. Tate, *Algebraic cycles and the pole of zeta functions*, Arithmetical Algebraic Geometry, Harper and Row, New York, 1965, 93 – 110.

[TW] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. Math. **141**, 1995, 553 – 572.

[Wa] L. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48**, number 177, 1987, 371 – 384.

[Wig1] E. Wigner, *On the statistical distribution of the widths and spacings of nuclear resonance levels*, Proc. Cambridge Philo. Soc. **47**, 1951, 790 – 798.

[Wig2] E. Wigner, *Statistical Properties of real symmetric matrices*, Canadian Mathematical Congress Proceedings, University of Toronto Press, Toronto, 1957, 174 – 184.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math **141**, 1995, 443 – 551.