Computers in Undergraduate Education and Zeros of Elliptic Curves

Steven Miller*†

FoCM: Minneapolis, August 10^{th}, 2002

Abstract

For the last two years at Princeton, the Junior Research Seminar has involved students in numerically investigating hot conjectures. I will mention some of their results from Random Matrix Theory and Ramanujan Graphs.

Based on theory from the function field case, Katz and Sarnak predict every natural family of L-functions has an associated symmetry group controlling the distribution of zeros. Certain statistics (n-level correlations) are the same for all classical compact groups; others (n-level densities) differ. For families of elliptic curves, for small support and assuming standard conjectures, the 1- and 2-level densities agree with the appropriate classical compact group. I will sketch the proofs, and provide numerical evidence for the needed conjectures (as well as consequences of being able to prove these results for larger supports). These computations were done with last year's Junior Seminar.

1 Junior Research Seminar / Undergraduate Math Lab

Below is a list of problems investigated. To view the student reports and a more detailed write-up of the course, go to

http://www.math.princeton.edu/∼mathlab/index.html

Problems (2000 – 2001)

*E-mail: sjmiller@math.princeton.edu

†http://www.math.princeton.edu/∼sjmiller/math/talks/talks.html

1. Random Matrix Theory
2. Ramanujan Graphs
3. Hardy-Littlewood Varieties
4. Prime Spacings
5. Ranks of Elliptic Curves
6. $\{n^2\alpha\}$

Problems $(2001 - 2002)$: Elliptic Curves

1. Analytic / Geometric Ranks in Families
2. Points of Low Height in Families
3. Distribution of Signs in Families
4. First Zero above Critical Point
5. Sato-Tate
6. Cryptography

1.1 Random Matrix Theory

The results below are joint with Rebecca Lehman and Yi-Kai Liu.

Consider $N \times N$ symmetric matrices with entries i.i.d.r.v. chosen from a fixed probability distribution P.

GOE Conjecture: As $N \to \infty$, the probability density of the distance between two consecutive (normalized) eigenvalues approaches $\frac{\pi^2}{4}\frac{d^2\Psi}{dt^2}$ (the GOE distr). $\Psi(t)$ is (up to constants) the Fredholm determinant of the operator $f \to \int_{-t}^{t} K * f$, with kernel $K = \frac{1}{2\pi}\left(\frac{\sin(\xi-\eta)}{\xi-\eta} + \frac{\sin(\xi+\eta)}{\xi+\eta}\right)$.

This is only known if the entries are chosen from the Gaussian. The consecutive spacings are well approximated by Axe^{-Bx^2}.

Semi-Circle Law: Assume P has mean 0, variance 1, other moments finite, and let $\frac{\lambda_j}{2\sqrt{N}}$ be the normalized eigenvectors.

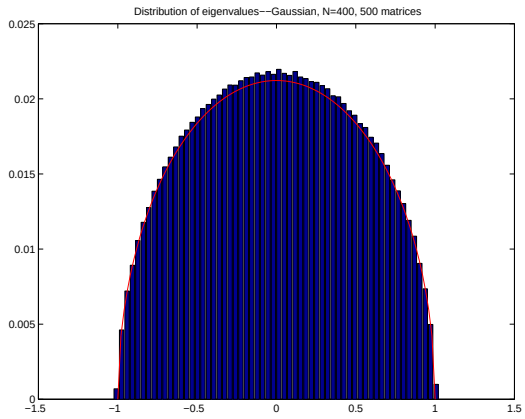
$$\begin{aligned} \text{If} \quad \mu_{A,N}(x) &= \frac{1}{N}\sum_{j=1}^{N}\delta\left(x - \frac{\lambda_j}{2\sqrt{N}}\right) \\ \text{Then} \quad \mu_{A,N}(x) &\to \frac{2}{\pi}\sqrt{1-x^2} \quad \text{with probability 1} \end{aligned}$$

The juniors investigated many probability distributions. In every case, they observed the normalized distances between the eigenvalues converging towards the GOE distribution as the size of the matrices increased.

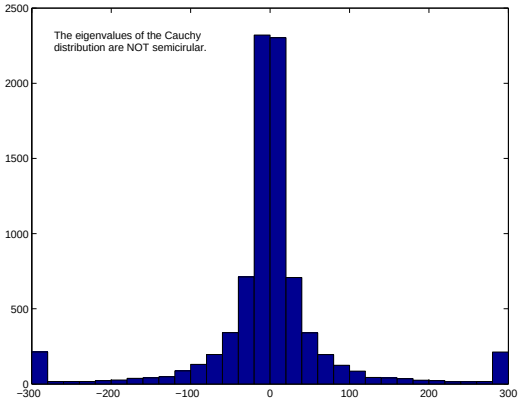
Probability distributions chosen include the uniform on $[-1, 1]$, the Cauchy (which has infinite variance and hence does not satisfy the conditions for the Semi-Circle Law), the discrete Poisson, sparse matrices (entries are $+1$ with probability p, -1 with probability p, and 0 with probability $1 - 2p$) and Gaussian band matrices.

1.1.1 Semi-Circle Law

Already at $N = 400$ we observe good agreement in the Semi-Circle Law for matrices with entries chosen from the Gaussian. Not surprising, the Cauchy Distribution (with infinite variance) does not satisfy the Semi-Circle Law. In particular, we observe with significant probability large eigenvalues. Later we observe, however, that the spacings between the central (ie, staying in the bulk of the spectrum) normalized eigenvalues arising from the Cauchy Distribution, as the size of the matrices increases, tend to the GOE.



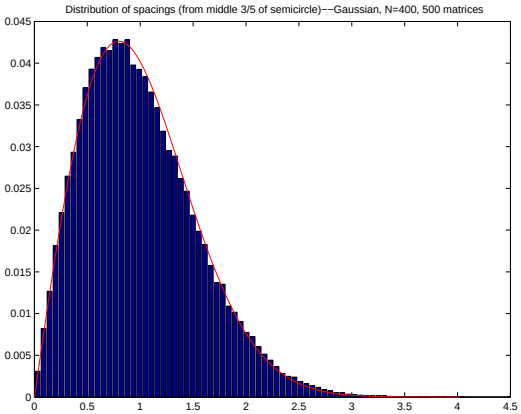
500 Matrices: Gaussian 400×400



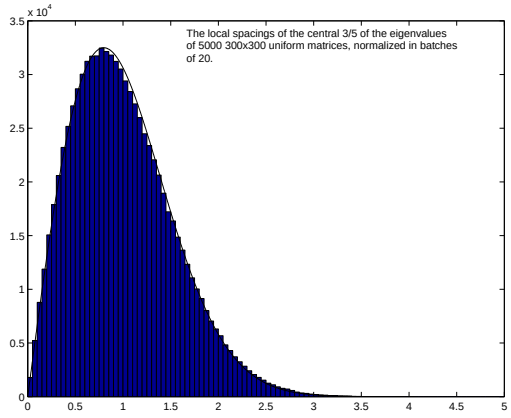
Cauchy: Not-Semicircular (Infinite Variance), $P(t) = \frac{1}{\pi(1+t^2)}$

1.1.2 GOE Conjecture

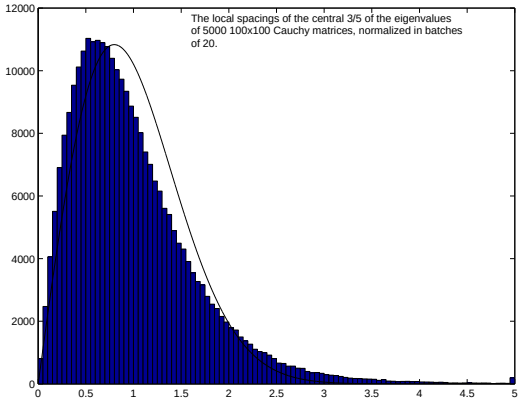
For comparison purposes, below is the distribution of spacings between normalized eigenvalues when the entries are chosen from the Gaussian distribution:



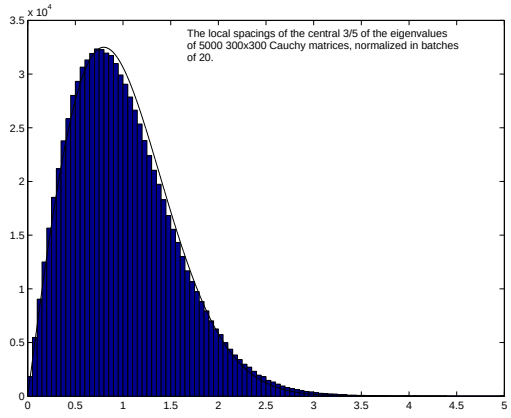
400 Gaussian Matrices, 400×400



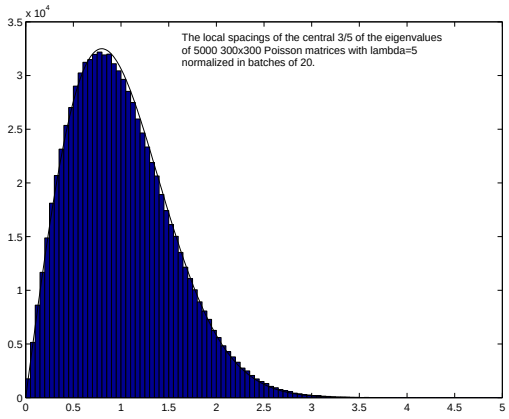
5000 Uniform on $[-1, 1]$ matrices: 300×300



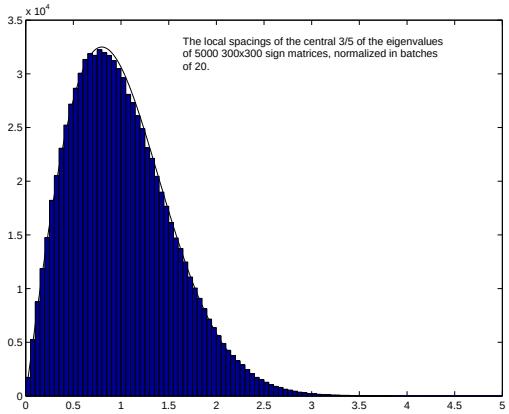
5000 Cauchy matrices: 100×100



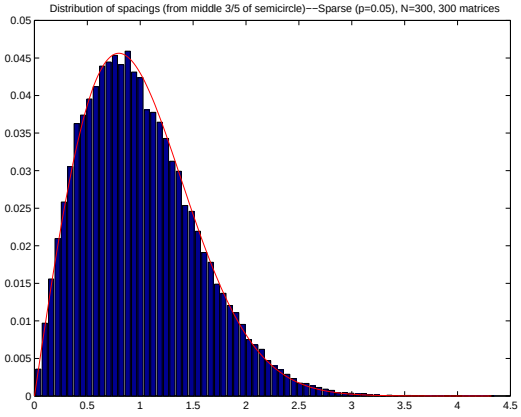
5000 Cauchy matrices: 300×300



5000 Poisson matrices, $P(n) = \frac{\lambda^n}{n!}e^{-\lambda}$, $\lambda = 5$, 300×300



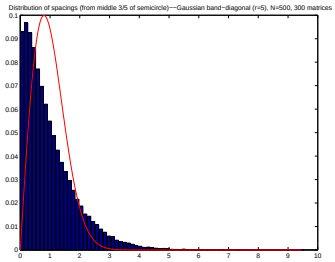
5000 Poisson matrices, $P(n) = \frac{\lambda^n}{n!}e^{-\lambda}$, $\lambda = 20$, 300×300



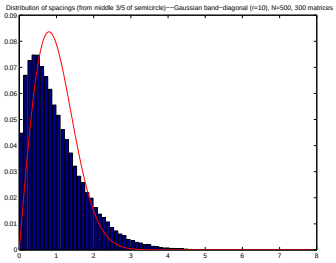
300 Sparse Matrices, $p = .05$ for $+1$, $p = .05$ for -1, $p = .90$ for 0, 300×300

1.1.3 Band Matrices

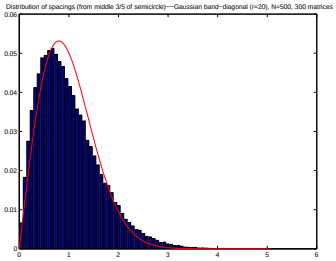
The juniors also investigated band matrices of width r (a matrix with non-zero entries along the first r diagonals above and below the main diagonal). The entries are chosen from the Gaussian distribution.



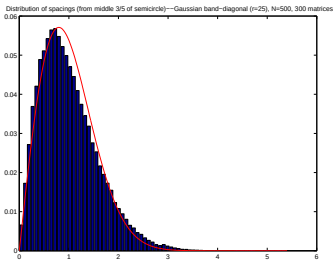
300 Band Matrices, 500×500, $r = 5$



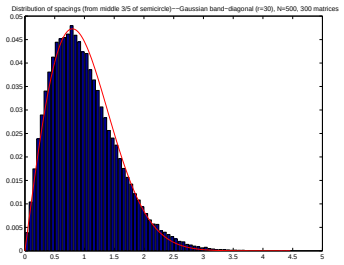
300 Band Matrices, 500×500, $r = 10$



300 Band Matrices, 500×500, $r = 20$



300 Band Matrices, 500×500, $r = 25$



300 Band Matrices, 500×500, $r = 30$

1.2 Ramanujan Graphs

The results below are joint with Peter Richter and Kevin Chang.

Let G_n be a family of k-regular graphs with n vertices, and let the adjacency matrix have eigenvalues λ_j.

1. $\lambda_0(G) = k$ for all $G \in G_n$
2. $\lambda_0(G) > \lambda_1(G)$ iff connected
3. $\liminf_{n\to\infty} \lambda_1(G_n) \geq 2\sqrt{k-1}$

We define the expander constant of a graph X with n vertices V as the largest constant $h(X)$ such that $|\partial A| \geq h(X)|A|$ for all subsets A of V with $\#A \leq \frac{n}{2}$. $|\partial A|$ is the boundary of A (the set of vertices v in $V - A$ with an edge from v to a vertex in A.

We have the following facts:

$$\frac{k-\lambda_1}{2} \;\leq\; h(X) \;\leq\; \sqrt{2k(k-\lambda_1)}.$$

For bipartite graphs:

$$\operatorname{diam}(X) \;\leq\; \frac{\log(2n)}{\log\left(\frac{k+\sqrt{k^2-\lambda_1^2}}{\lambda_1}\right)} \tag{1.1}$$

where $\operatorname{diam}(X)$ is the largest path between two vertices of X.

Graphs with small λ_1 have small diameters and high expander constants.

We say a k-regular graph is Ramanujan if $\lambda_1 \leq 2\sqrt{k-1}$. These give sparse graphs with small diameters and high connectivity, and are useful for network building. There are known constructions (using Number Theory) for $p^r + 1$, p prime.

The juniors generated large numbers of k-regular bipartite graphs and calculated λ_1 (the second largest eigenvalue).

1.2.1 Questions / Conjectures

Consider all 3-regular bipartite graphs with n vertices.

Question 1: As $n \to \infty$, what percent of the graphs are Ramanujan?

Question 2: As $n \to \infty$, does each graph have $\lambda_1 \to 2\sqrt{2}$?

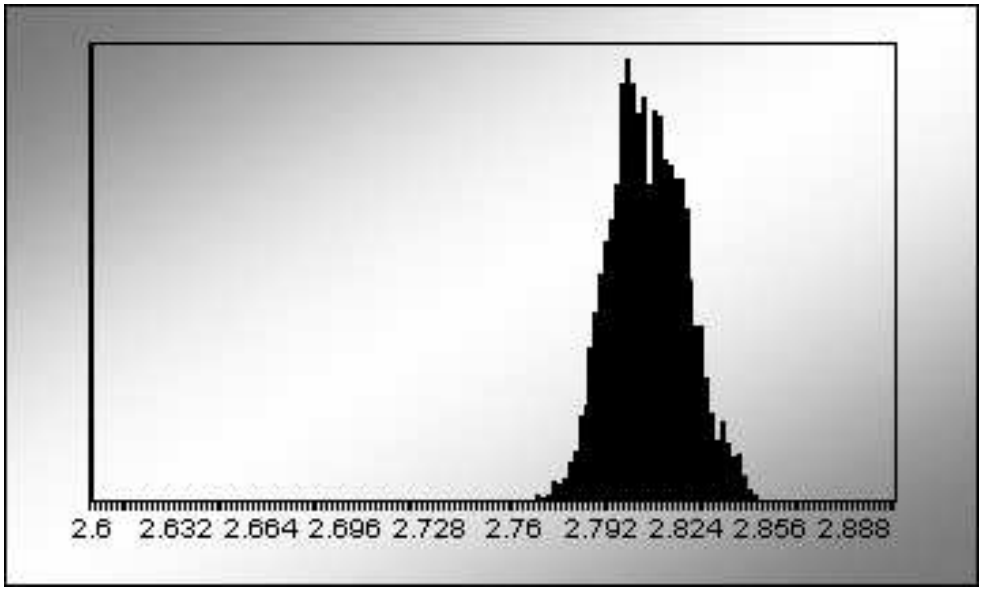
In other words, in the limit is a randomly chosen 3-regular bipartite graph Ramanujan? There are similar questions for n-regular bipartite graphs. Note 7 is smallest number with no known construction.

1.2.2 Results for $k = 3$

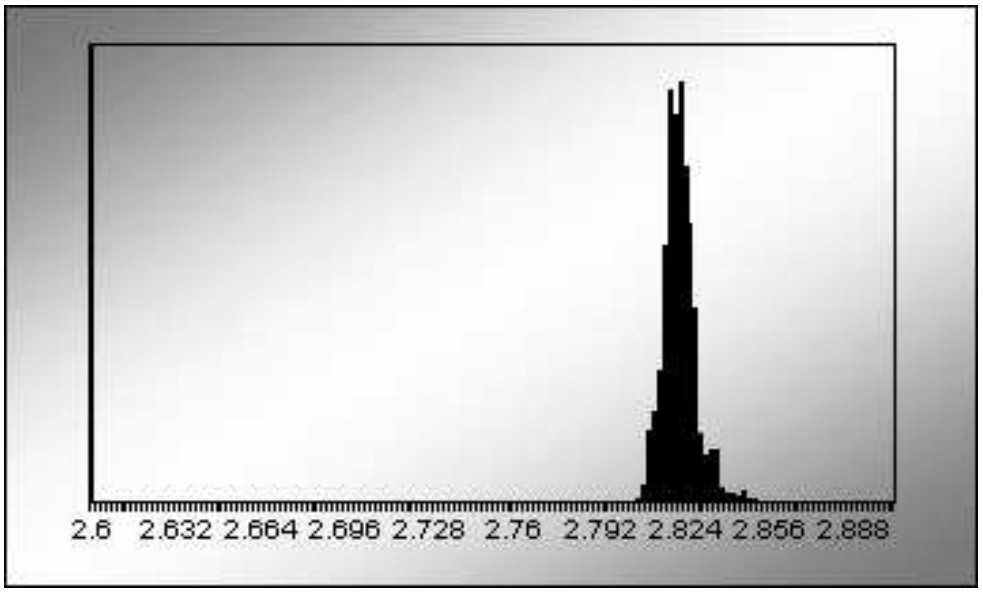
The juniors investigated 5000 randomly chosen 3-regular bipartite graphs for various numbers of vertices.

n	λ_1 mean	st dev	% Ram	λ_1 mean	st dev	% Ram
100	2.8076	0.042	76.14	2.777	0.031	95.28
200	2.8160	0.027	76.36	2.800	0.019	93.06
300	2.8187	0.020	77.38	2.808	0.014	92.84
400	2.8210	0.018	75.20	2.813	0.011	91.22
500	2.8216	0.014	76.62	2.815	0.009	91.40
600	2.8225	0.013	77.54	2.817	0.009	90.90
700	2.8226	0.012	78.46	2.818	0.008	91.00
800	2.8231	0.011	79.68	2.819	0.007	90.58
900	2.8233	0.011	80.34	2.820	0.007	91.06
1000	2.8235	0.009	79.86	2.820	0.006	91.12

First group allows double and triple bonds; second group simple (single bonds only). Note $2\sqrt{3-1} = 2\sqrt{2} = 2.828427$.



λ_1: 5000 simple 3-regular graphs, 300 vertices



λ_1: 5000 simple 3-regular graphs, 1000 vertices

1.2.3 Results: $k = 7$

The juniors investigated 5000 randomly chosen 7-regular bipartite graphs for various numbers of vertices.

n	λ_1 mean	st dev	% Ram	λ_1 mean	st dev	% Ram
100	4.791	0.113	83.74	4.530	0.100	99.90
200	4.833	0.069	82.68	4.709	0.063	99.70
300	4.849	0.053	83.54	4.767	0.048	99.42
400	4.858	0.043	82.90	4.796	0.040	98.92
500	4.865	0.036	82.92	4.815	0.035	98.77
600	4.869	0.032	83.20	4.828	0.031	98.26
700	4.871	0.028	84.02	4.836	0.028	98.20
800	4.874	0.027	83.18			
900	4.875	0.025	82.84			
1000	4.877	0.022	83.92			

First group allows multiple bonds; second group single bonds only. Note $2\sqrt{7-1} = 4.89898$.

1.2.4 Conclusions

From the data, we observe that as the number of vertices increase, λ_1's distribution is tightening around $2\sqrt{k-1}$ for $k = 3$ and 7. The percent of random graphs which are Ramanujan seems stable (with the percent depending on whether or not we allow multiple bonds), though no one wants to conjecture that it remains stable!

2 Zeros of Elliptic Curves: Evidence for a Spectral Interpretation

2.1 Introduction

General Formulation: Studying some system, one observes values at t_1, t_2, t_3, etc. What rules govern the spacings between events? (Often we need to normalize by average spacing).

Examples include spacings between primes and prime pairs, between energy levels of excited heavy nuclei, between eigenvalues of random matrices, and between zeros of L-functions.

Consider an elliptic curve $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in \mathbf{Q}$ and its L-function

$$L(s,E) = \prod_{p|\Delta} \left(1 - a_p p^{-s}\right)^{-1} \prod_{p \nmid \Delta} \left(1 - a_p p^{-s} + p^{1-2s}\right)^{-1}$$

By GRH: All non-trivial zeros are on the critical line. Hence it makes sense to talk about spacings between zeros.

The rational solutions form a group: $E(\mathbb{Q}) = \mathbb{Z}^r \bigoplus T$, T is the set of torsion points, r is the geometric rank.

The Birch and Swinnerton-Dyer Conjecture states the geometric rank equals the analytic rank (the order of vanishing of $L(s,E)$ at $s = \frac{1}{2}$).

We will study one parameter families of elliptic curves, where $a_i = a_i(t) \in \mathbb{Z}[t]$.

2.2 Random Matrix Theory

Consider the group of $N \times N$ matrices from one of the classical compact groups: unitary, symplectic, orthogonal.

One assigns probability measures to matrices from these 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 behaviour of statistics from a generic, randomly chosen element.

We expect that Random Matrix Theory can serve as a good guide for investigating properties of L-functions. See the talks by Rubinstein and Farmer for more details.

More generally, we can consider other spaces: GUE / GOE: Hermitian / Symmetric matrices with Gaussian probabilities for entries.

2.3 n-Level Correlations

Let $\{\alpha_j\}$ be an increasing sequence of numbers (zeros of an L-function, eigenvalues of a Hermitian matrix, ...) and $B \subset \mathbf{R}^{n-1}$ a compact box. Define the n-level correlation by

$$\lim_{N\to\infty} \frac{\#\left\{\left(\alpha_{j_1} - \alpha_{j_2}, \ldots, \alpha_{j_{n-1}} - \alpha_{j_n}\right) \in B, j_i \neq j_k\right\}}{N}$$

Instead of using a box, can use a smooth test function. See Rudnick and Sarnak.

Results:

1. Normalized spacings of $\zeta(s)$ starting at 10^{20} agree with the GUE distribution (Odlyzko).

2. Pair and triple correlations of $\zeta(s)$ agree with the GUE (Montgomery, Hejhal).

3. n-level correlations for all automorphic cupsidal L-functions agree with the GUE (Rudnick-Sarnak).

4. n-level correlations for the classical compact groups are all the same (and equal the GUE) (Katz-Sarnak).

5. the n-level correlations are insensitive to any finite set of zeros. (Fix a finite set of zeros: only finitely many other zeros give a tuple in the box).

2.4 n-Level Density and Families

Let $f(x) = \prod_i f_i(x_i)$, f_i even Schwartz functions whose Fourier Transforms are compactly supported.

$$D_{n,E}(f) \quad = \quad \sum_{\substack{j_1,\ldots,jn \\ distinct}} f_1\Big(L_E\gamma_E^{(j_1)}\Big)\cdots f_n\Big(L_E\gamma_E^{(j_n)}\Big)$$

Note

1. individual zeros contribute in limit

2. most of contribution is from low zeros

Similar to choosing an $N \times N$ matrix at random and calculating its eigenvalues, we only get one string of values if we study the n-level density attached to an L-function of an elliptic curve. If, however, we can find a large number of curves similar to our original one, then we may calculate the zeros of each, and see how they vary from curve to curve. Thus, we are led to the concept of a family of curves.

To any geometric family, Katz-Sarnak predict the n-level density depends only on a symmetry group attached to the family. For families of elliptic curves, they predict orthogonal symmetries, depending on the distrubution of signs of the functional equations. All even should be SO(even), all odd SO(odd), and equidistributed should be O.

2.5 Normalization of Zeros

How should we normalize the zeros of the curves in our family $\mathcal{F}$?

1. Local Data (hard): using some natural measure from the curve
2. Global Data (easy): using an average from the family

Hope: for f a good even test function with compact support, as $|\mathcal{F}| \to \infty$,

$$\begin{aligned}\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} D_{n,E}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_{\substack{j_1,\dots,j_n\\ j_i\neq\pm j_k}}\prod_i f_i\left(\frac{\log N_E}{2\pi}\gamma_E^{(j_i)}\right)\\ &\to \int\cdots\int f(x)W_{n,\mathcal{G}(\mathcal{F})}(x)dx\\ &= \int\cdots\int \widehat{f}(u)\widehat{W_{n,\mathcal{G}(\mathcal{F})}}(u)du,\end{aligned}$$

where the density $\widehat{W_{n,\mathcal{G}(\mathcal{F})}}(u)$ depends only on a symmetry group attached to the family. Note if we rescale each curve's zeros using local data (ie, if N_E depends on E), we must handle this variance in the sums.

2.6 1 and 2-Level Densities

Katz and Sarnak calculate the n-level densities for the classical compact groups. Unlike the correlations, the densities are different for different groups.

The Fourier Transforms for the 1-level densities are

$$\widehat{W_{1,O^+}}(u) = \delta_0(u) + \frac{1}{2}\eta(u)$$

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

where $\delta_0(u)$ is the Dirac Delta functional and $\eta(u)$ is 1, $\frac{1}{2}$, and 0 for $|u|$ less than 1, 1, and greater than 1. Note the three orthogonal densities are indistinguishable for supports less than 1, though they are distinguishable from the Unitary and Symplectic densities.

We give the effect of the Fourier Transform of the densities on test functions supported in $\sigma_1 + \sigma_2 < 1$, where σ_i is the support of f_i.

Let $c(\mathcal{G}) = 0$, $\frac{1}{2}$ or 1 for $\mathcal{G} = SO(\text{even})$, O, and $SO(\text{odd})$. For $\mathcal{G}$ one of these three orthogonal groups we have

$$\begin{aligned}
\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 &= \left[\widehat{f_1}(0) + \frac{1}{2}f_1(0)\right]\left[\widehat{f_2}(0) + \frac{1}{2}f_2(0)\right] \\
&\quad + 2\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - 2\widehat{f_1f_2}(0) \\
&\quad -f_1(0)f_2(0) \\
&\quad + c(\mathcal{G})f_1(0)f_2(0).
\end{aligned}$$

For $\mathcal{G} = U$ (Unitary) we have

$$\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,U}}(u)du_1du_2 = \widehat{f_1}(0)\widehat{f_2}(0) + \int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - \widehat{f_1f_2}(0),$$

and for $\mathcal{G} = Sp$ (Symplectic) we have

$$\begin{aligned}
\int\int \widehat{f_1}(u_1)\widehat{f_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 &= \left[\widehat{f_1}(0) + \frac{1}{2}f_1(0)\right]\left[\widehat{f_2}(0) + \frac{1}{2}f_2(0)\right] \\
&\quad + 2\int |u|\widehat{f_1}(u)\widehat{f_2}(u)du - 2\widehat{f_1f_2}(0) \\
&\quad - f_1(0)f_2(0) \\
&\quad -f_1(0)\widehat{f_2}(0) - \widehat{f_1}(0)f_2(0) + 2f_1(0)f_2(0).
\end{aligned}$$

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

For the orthogonal groups, the densities (in this range) depend only on the distribution of the signs of the functional equations.

2.7 Previous Results

All proofs begin with the Explicit Formula, which relates sums of test functions over zeros to sums over primes of $a_E(p)$ and $a_E^2(p)$. N_E is the conductor of E.

$$\begin{aligned}\sum_{\gamma_E^{(j)}} G\left(\frac{\log N_E}{2\pi}\gamma_E^{(j)}\right) &= \widehat{G}(0) + G(0) \\ &\quad - 2\sum_p \frac{\log p}{\log N_E}\frac{1}{p}\widehat{G}\left(\frac{\log p}{\log N_E}\right)a_E(p) \\ &\quad - 2\sum_p \frac{\log p}{\log N_E}\frac{1}{p^2}\widehat{G}\left(\frac{2\log p}{\log N_E}\right)a_E^2(p) \\ &\quad + O\left(\frac{\log\log N_E}{\log N_E}\right).\end{aligned}$$

Modified Explicit Formula:

$$\begin{aligned}\sum_{\gamma_E^{(j)}} G\left(\frac{\log X}{2\pi}\gamma_E^{(j)}\right) &= \frac{\log N_E}{\log X}\widehat{G}(0) + G(0) \\ &\quad - 2\sum_p \frac{\log p}{\log X}\frac{1}{p}\widehat{G}\left(\frac{\log p}{\log X}\right)a_E(p) \\ &\quad - 2\sum_p \frac{\log p}{\log X}\frac{1}{p^2}\widehat{G}\left(\frac{2\log p}{\log X}\right)a_E^2(p) \\ &\quad + O\left(\frac{\log\log X}{\log X}\right).\end{aligned}$$

The goal is to pass the summation on the curves past the test functions to the arithmetic data $a_E(p)$. This is significantly easier if we use global

data to rescale each curve's zeros. Previous investigations have rescaled each curve's zeros by the average of the logarithms of the conductors. This greatly simplifies the calculations; however, the normalization is no longer natural for each curve, as each curve can sit in infinitely many families, each with a different average spacing. By using local normalizations for each curve's zeros, the n-level density for a family becomes the average of the n-level densities for each curve.

We comment on two previous works:

1. Orthogonal: Iwaniec-Luo-Sarnak: 1-level density for holomorphic even weight k cuspidal newforms of square-free level N (SO(even) and SO(odd) if split by sign)

2. Symplectic: Rubinstein: n-level densities for twists $L(s, \chi_d)$ of the zeta-function.

The main tools in these proofs are:

1. Averaging Formulas (Petersson formula in ILS, Orthogonality of characters in Rubinstein).

2. Constancy of conductors.

For families of Elliptic Curves, the conductors are given by

$$C(t) \ = \ \prod_{p|\Delta(t)} p^{f_p(t)}$$

Thus, two curves close in a family could have wildly different factorizations, leading to very different conductors. By sieving to a positive percent subsequence, we will restrict to curves where the conductors are well controlled.

2.8 1- and 2-Level Expansion

We will give most of the details for the proof of the 1-level density, and confine ourselves to sketching what is needed for the higher level densities.

$$\begin{aligned} D_{1,\mathcal{F}}(f) &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_j f\left(\frac{\log N_E}{2\pi}\gamma_E^{(j)}\right) \\ &= \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\widehat{f}(0)+f_i(0) \\ &\quad -\frac{2}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_p\frac{\log p}{\log N_E}\frac{1}{p}\widehat{f}\left(\frac{\log p}{\log N_E}\right)a_E(p) \\ &\quad -\frac{2}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\sum_p\frac{\log p}{\log N_E}\frac{1}{p^2}\widehat{f}\left(2\frac{\log p}{\log N_E}\right)a_E^2(p) \\ &\quad +O\left(\frac{\log\log N_E}{\log N_E}\right) \end{aligned}$$

We want to move $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}$ past the test functions to the arithmetic data $a_E(p)$. This leads us to study

$$A_{r,\mathcal{F}}(p) = \sum_{t(p)} a_t^r(p), \quad r=1 \text{ or } 2.$$

For the 2-Level Expansion, we need to evaluate terms like

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}\prod_{i=1}^{2}\frac{1}{p_i^{r_i}}g_i\left(\frac{\log p_i}{\log N_E}\right)a_E^{r_i}(p_i).$$

Lemma: *Analogue of Petersson / Orthogonality: If $p_1,\dots,p_n$ are distinct primes*, then

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

The above is what allows us to calculate the 2-level densities (for small support).

For many families

1. $A_{1,\mathcal{F}}(p) = -rp \ + \ O(1)$
2. $A_{2,\mathcal{F}}(p) = p^2 \ + \ O(p^{3/2})$

Actually, we only need $A_{1,\mathcal{F}}(p) = -rp \ + \ O(1)$ on average. For any surface satisfying Tate's Conjecture, Silverman and Rosen prove

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p\le X} -A_{\mathcal{E}}(p) \log p = r,$$

which is sufficient for our proofs. Any rational elliptic surface satisfies Tate's Conjecture, which is why we have restricted ourselves to such surfaces. Recall an elliptic surface $y^2 = x^3 + A(t)x + B(t)$ is rational iff one of the following is true: (1) $0 < \max\{3\text{deg}A, 2\text{deg}B\} < 12$; (2) $3\text{deg}A = 2\text{deg}B = 12$ and $\text{ord}_{t=0}t^{12}\Delta(t^{-1}) = 0$.

For surfaces with $j(t)$ non-constant, Michel proves $A_{2,\mathcal{F}}(p) = p^2 + O\Big(p^{3/2}\Big)$.

2.9 New Results

To calculate the 1-level density, we do not need 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 to know which curves are even and which are odd. 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. We calculate the 1- and 2-level densities for families of elliptic curves.

We first fix notation. Let $D(t)$ be the product of the irreducible polynomial factors of $\Delta(t)$. Let $C(t)$ be the conductor of the curve E_t. Let B be the largest square which divides $D(t)$ for all t. Pass to a subsequence $ct + t_0$, and call $t \in [N, 2N]$ good if $D(ct + t_0)$ is square-free, except for primes $p|B$, where the power of such $p|D(t)$ is independent of t. Then

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 or Square-Free Sieve conjecture if $\Delta(t)$ has an irreducible polynomial factor of degree at least 4.*

Possibly after passing to a subsequence, for t good, $C(t)$ is a polynomial of degree m. 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).*

The 1*-level density agrees with the orthogonal densities plus a term which equals the contributions from* r *zeros at the critical point. The* 2*-level density agrees with* $SO(even)$*,* O*, and* $SO(odd)$ *depending on whether the signs are all even, equidistributed in the limit, or all odd, plus a term which equals the contribution from* r *zeros at the critical point. Thus, for small support, the densities of the zeros agree with Katz and Sarnak's predictions. Further, the densities confirm that the curves behave as if they have* r *zeros at the critical point, as predicted by the B-SD conjecture.*

Similar to the universality Rudnick and Sarnak found in studying n-level correlations, 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 Michel.

Helfgott shows the Square-Free Sieve and Polynomial Moebius Conjectures imply the Restricted Sign Conjecture for many one-parameter families of elliptic curves. More precisely, let $M(t)$ be the product of the irreducible polynomials dividing $\Delta(t)$ and not $c_4(t)$.

Theorem: 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.*

We give some examples. Consider the following Constant-Sign Families:

1. $y^2 = x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ Sq-Free: all even.
2. $y^2 = x^3 \pm 4(4t+2)x$, $4t+2$ Sq-Free: $+$ yields all odd, $-$ yields all even.
3. $y^2 = x^3 + tx^2 - (t+3)x + 1$, t^2+3t+9 Sq-Free: all odd.

The first two have rank 0 over $\mathbf{Q}(t)$; the third has rank 1. We only assume GRH for first two; B-SD is used to interpret the third. Because we can calculate the signs, the 2-level density allows us to distinguish the candidate orthogonal symmetries. Thus, *this is the first example where we can say we are observing SO(even) but not SO(odd) symmetry (and vice-versa), conditional only on GRH.*

As an example, consider the following family of Rank 6 over $\mathbf{Q}(t)$:

$$\begin{aligned} y^2 &= x^3 + (2at - B)x^2 + (2bt - C)(t^2 + 2t - A + 1)x \\ &\quad + (2ct - D)(t^2 + 2t - A + 1)^2 \end{aligned}$$

$$\begin{aligned} A &= 8916100448256000000 \\ B &= -811365140824616222208 \\ C &= 26497490347321493520384 \\ D &= -343107594345448813363200 \\ a &= 16660111104 \\ b &= -1603174809600 \\ c &= 2149908480000 \end{aligned} \tag{2.2}$$

Modulo reasonable conjectures, its 1 and 2-level densities agree with Katz and Sarnak's predictions. In non-Weierstrass form, this curve can be written as quadratic in t.

2.10 Sieving

Let $S(t)$ be some quantity associated to our family of elliptic curves.

$$\begin{aligned} \sum_{\substack{t=N \\ D(t) \\ sqfree}}^{2N} S(t) &= \sum_{d=1}^{N^{k/2}} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2) \\ t\in[N,2N]}} S(t) \\ &= \sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2) \\ t\in[N,2N]}} S(t) + \sum_{d\geq \log^l N}^{N^{k/2}} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2) \\ t\in[N,2N]}} S(t). \end{aligned}$$

We handle first piece by progressions. Note we can only evaluate sums of $a_t(p)$ for t in arithmetic progressions.

We handle second piece by Cauchy-Schwartz: The number of t in the second sum (by ABC or SqFree Sieve Conj) is $o(N)$. We can show $\sum_{t=N}^{2N} S^2(t) = O(N)$. Then

$$\begin{aligned}\sum_{t\in\mathcal{T}} S(t) &\ll \left(\sum_{t\in\mathcal{T}} S^2(t)\right)^{\frac{1}{2}} \cdot \left(\sum_{t\in\mathcal{T}} 1\right)^{\frac{1}{2}} \\ &\ll \left(\sum_{t\in[N,2N]} S^2(t)\right)^{\frac{1}{2}} \cdot o\Big(\sqrt{N}\Big).\end{aligned}$$

Notation: $\widetilde{a}_{d,i,p}(t') = a_{t(d,i,t')}(p)$, $G_{d,i,P}(u)$ is related to the test functions, d and i from progressions.

Applying Partial Summation

$$\begin{aligned}S(d,i,r,p) &= \sum_{t'=0}^{[N/d^2]} \widetilde{a}^r_{d,i,p}(t') G_{d,i,p}(t') \\ &= \left(\frac{[N/d^2]}{p} A_{r,\mathcal{F}}(p) + O\Big(p^R\Big)\right) G_{d,i,p}([N/d^2]) \\ &\quad - \sum_{u=0}^{[N/d^2]-1} \left(\frac{u}{p} A_{r,\mathcal{F}}(p) + O\Big(p^R\Big)\right) \\ &\qquad \cdot \Big(G_{d,i,p}(u) - G_{d,i,p}(u+1)\Big)\end{aligned}$$

$O(p^R)$ is the error from using Hasse to bound the partial sums: $p^R = p^{1+\frac{r}{2}}$. Three of the four pieces can be easily handled.

We sketch the method used to handle the difficult piece.

$$\frac{1}{N}\sum_p \frac{1}{p^r} \sum_{d,i} \sum_{u=0}^{[N/d^2]-1} O(p^{1+\frac{r}{2}}) \cdot \Big(G_{d,i,p}(u) - G_{d,i,p}(u+1)\Big)$$

Taylor Expansion is not enough when $r = 1$. We gain a $\frac{1}{\log N}$ from the G difference. The p-sum (p goes to a power of N) is N to a positive power.

Summing over u gives $\frac{N}{d^2}$, the N here cancelling with the $\frac{1}{N}$ which come from the cardinality of the family. We are left with a small power of N over $\log N$. Thus, a more delicate analysis is required.

The main problem with the above argument was Taylor only gained us a $\frac{1}{\log N}$, but we had $\frac{N}{d^2}$ terms. We use Bounded Variation, which requires the conductors are be monotone.

$$\begin{aligned} & \sum_{u=0}^{[N/d^2]-1} \left| G_{d,i,p}(u) - G_{d,i,p}(u+1) \right| \\ = & \sum_{u=0}^{[N/d^2]-1} \left| g\left(\frac{\log p}{\log C(t_i(d)+ud^2)}\right) - g\left(\frac{\log p}{\log C(t_i(d)+(u+1)d^2)}\right) \right| \end{aligned}$$

If the conductors are monotone, the above becomes an exercise in bounded variation for the Schwartz function g. Note this bound is independent of $\frac{N}{d^2}$ (the number of subdivisions). If g is supported in $(-\sigma, \sigma)$, the above is $O(\sigma \cdot ||g'||_\infty)$. (We do not need the full strength of bounded variation: we can use the Mean Value Theorem to bound each term by the sup-norm of g' times the length of that subinterval.

Thus, we need to sieve as we do for two reasons. We can only evaluate sums of elliptic curve quantities in arithmetic progressions, and we need the conductors to be monotone to bound certain sums. By sieving to subsequences, for an auxiliary polynomial (see next subsection) square-free, the conductors are given by a monotone polynomial. We then extend this to be the conductor for all t (by inclusion / exclusion, the other t do not contribute, so we can have any auxiliary definition there). This has the advantage of allowing us to differentiate the conductors in the Taylor Expansion, which is useful for bounding some of the error terms.

2.11 Handling the Conductors

$$\begin{aligned} C(t) &= \prod_{p|\Delta(t)} p^{f_p(t)} \\ D_1(t) &= \text{primitive irred. poly. factors } \Delta(t) \text{ and } c_4(t) \text{ share} \\ D_2(t) &= \text{remaining primitive irred. poly. factors of } \Delta(t) \\ D(t) &= D_1(t)D_2(t) \end{aligned}$$

For $D(t)$ square-free, $C(t)$ is like $D_1^2(t)D_2(t)$ except for a finite set of bad primes.

Let P be the product of the bad primes.

By Tate's Algorithm, we can determine $f_p(t)$, which depends on the coefficients $a_i(t)$ mod powers of p.

Apply Tate's Algorithm to E_{t_1} to determine $f_p(t_1)$ for the bad primes. For m large, $f_p(\tau) = f_p(P^m t + t_1) = f_p(t_1)$ for $p|P$.

For m enormous, for bad primes, the order of p dividing $D(P^m t + t_1)$ is independent of t. So we can find integers such that $C(\tau) = c_{bad}\frac{D_1^2(\tau)}{c_1}\frac{D_2(\tau)}{c_2}$, $D(\tau)$ square-free.

2.12 Application: Bounding Excess Rank

Consider a one-parameter family with rank r over $\mathbb{Q}(t)$. The 1-level density is

$$D_{1,\mathcal{F}}(f_1) = \widehat{f_1}(0) + \frac{1}{2}f_1(0) + rf_1(0).$$

To estimate the percent with rank at least $r + R$, P_R, we get

$$Rf_1(0)P_R \leq \widehat{f_1}(0) + \frac{1}{2}f_1(0),\ R > 1.$$

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. The advantage is we get a cross term rR. The disadvantage is our support is smaller. Once R is large, the 2-level density yields better results.

For notational convenience, by even (odd) we mean a curve whose rank r_E satisfies $r_E - r$ is even (odd); ie, even (odd) rank above the rank of the family.

Let P_0 be the probability that an even curve has rank at least $r + 2a_0$, and P_1 the probability that an odd curve has rank at least $r + 1 + 2b_0$.

For convenience, we assume half the curves have even and half have odd sign, though at the expense of not splitting into even and odd bounds this can be removed.

The 1-level density gives the following bounds:

$$\begin{aligned} P_0 &\leq \frac{1}{a_0\sigma} \\ P_1 &\leq \frac{1}{b_0\sigma} \end{aligned} \tag{2.3}$$

We obtain the following bounds from the 2-level density. While we expect we may take the supports to be half the support from the 1-level density, for most families we can only prove that we may take the supports one-quarter that of the one level density.

$$\begin{aligned} P_0 &\leq \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24} + \frac{r+\frac{1}{2}}{\sigma_2}}{a_0(a_0+r)} \\ P_1 &\leq \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24} + \frac{r+\frac{1}{2}}{\sigma_2}}{b_0(b_0+r+1)}. \end{aligned} \tag{2.4}$$

$$\begin{aligned} P_0 &\leq \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24} + \frac{r}{\sigma_2} - \frac{1}{6\sigma_2}}{a_0(a_0+r-1)} \\ P_1 &\leq \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24} + \frac{r}{\sigma_2} - \frac{1}{6\sigma_2}}{b_0(b_0+r)}, \end{aligned} \tag{2.5}$$

where $a_0 \neq 1$ if $r = 0$.

$$\begin{aligned} P_0 &\leq \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24}}{a_0^2} + \frac{1}{2a_0}\frac{1}{a_0\sigma_2} \\ P_1 &\leq \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24}}{b_0 + b_0^2} + \frac{1}{2(1+b_0)}\frac{1}{b_0\sigma_2} \end{aligned} \tag{2.6}$$

Note, for $r = 0$, this is the same as our first attempt.

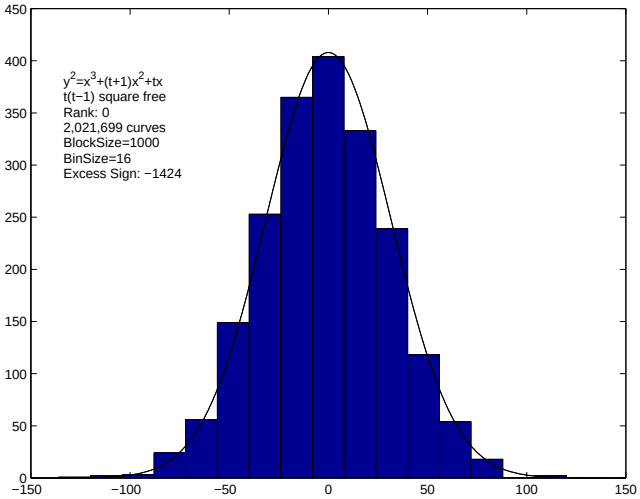
The three bounds are obtained by using different approximations. The key feature is that the bounds are proportional to $\frac{1}{a_0^2}$ instead of $\frac{1}{b_0}$.

2.13 Distribution of Signs

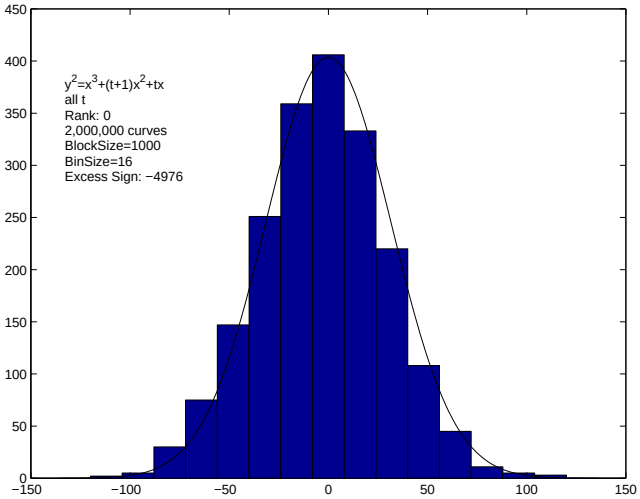
For N curves, the excess of positive to negative signs in intervals of 1000 was computed, for a total of $\frac{N}{1000}$ blocks. If the signs are randomly distributed, one would expect a histogram bin plot to reveal a Gaussian structure, with mean 0 and standard deviation $\sqrt{1000}$. Note this is a far stronger assumption than equidistribution of sign.

Atul Pokharel (one of the juniors last year) tested this for a variety of one-parameter families, both for all t and for t such that $D(t)$ was square-free.

Consider the family $y^2 = x^3 + (t+1)x^2 + tx$.

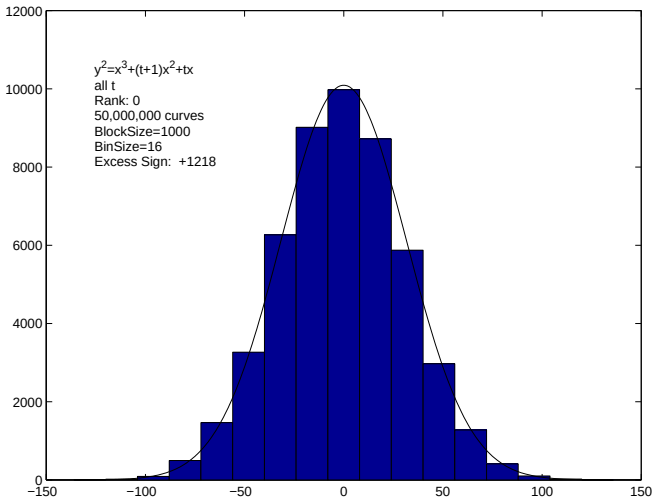


Histogram plot:$D(t)$ sq-free, first $2 \cdot 10^6$ such t.



Histogram plot: All $t \in [2, 2 \cdot 10^6]$.

Distribution of signs: $y^2 = x^3 + (t+1)x^2 + tx$



Histogram plot: All $t \in [2, 5 \cdot 10^7]$

The observed behaviour agrees with the predicted behaviour. Note as the number of curves increase (comparing the plot of $5 \cdot 10^7$ points to $2 \cdot 10^6$ points), the fit to the Gaussian improves. A more delicate analysis of the data is currently underway.

2.14 Summary and Future Work

For one-parameter families of elliptic curves (more generally, for families where Tate's conjecture is known), the 1 and 2-level densities for test functions of small support agree with the Katz-Sarnak predictions. For some families (including some interesting families of constant sign), only GRH is assumed. In general, the Square-Free Sieve is required for the 1-level densities, and a bit more (sums of the moebius function evaluated at polynomials – need this to obtain the distribution of signs in a family) for the 2-level densities.

The greatest difficulty is the variation of the conductors. As the elliptic curve quantities can only be evaluated in progressions, we do an inclusion / exclusion with progressions. By appropriate sieving, the conductors are given by a monotone polynomial, which is crucial for bounding error terms.

The 2-level density, besides lending support to Katz and Sarnak's predictions, also yield better bounds for the percent of curves of high rank above the family rank.

Finally, in many of the families investigated (see [Mil]), potential lower order correction terms were observed in the n-level densities. Unfortunately, these terms are of size $\frac{1}{\log N}$, while the errors are of size $\frac{\log\log N}{\log N}$.

Recall Michel proved for non-constant $j(t)$ that

$$A_{2,\mathcal{F}}(p) = \sum_{t(p)} a_t(p)^2 = p^2 + O(p^{\frac{3}{2}}). \tag{2.7}$$

The main term of $A_{2,\mathcal{F}}(p)$ will contribute in the limit, while the error term will not.

For a great many families, we can do better than Michel's $O(p^{\frac{3}{2}})$ bound for the error term, although we can construct families where the error is as large as $p^{\frac{3}{2}}$. Many families (including the family of all elliptic curves) investigated have a correction of size $-m_{\mathcal{F}}p + O(1)$, where $m_{\mathcal{F}} > 0$ depends on the family and is different for different families. This results in contribution to the 1-level density of size $\frac{1}{\log N}$.

This opens up the exciting possibility of seeing an expansion of the n-level density in $\frac{1}{\log N}$, and while all one-parameter families of rank r have the same main term, they could have distinguishable lower order terms. A more careful bounding of the error terms is currently being pursued.

References

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

[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.

[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, $1 - 26$.

[Meh] M. Mehta, *Random Matrices,* $2nd$ *edition*, Academic Press Inc., Boston, 1991.

[Mes] J. Mestre, *Formules explicites et minorations de conducteurs de varits algbriques*, Compositio Mathematica **58**, 1986, $209 - 232$.

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

[Mil] S. J. Miller, 1- *and* 2-*Level Densities for Families of Elliptic Curves: Evidence for the Underlying Group Symmetries*, P.H.D. Thesis, Princeton University, 2002, http://www.math.princeton.edu/∼sjmiller/thesis/thesis.ps.

[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, $273 - 308$.

[Od2] 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

[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, $269 - 322$.

[Sar] P. Sarnak, *Some applications of modular forms*, Cambridge Tracts in Mathematics, 99, Cambridge University Press, Cambridge, 1990.

[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, $227 - 236$.