Special Number Theory Seminar

From Random Matrix Theory to L-Functions

Steven J. Miller

Brown University

December 23, 2004

http://www.math.brown.edu/∼sjmiller/math/talks/talks.html

Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem Intractable.

Heavy nuclei like Uranium ($200+$ protons / neutrons) even worse!

Get some info by shooting high-energy neutrons into nucleus, see what comes out.

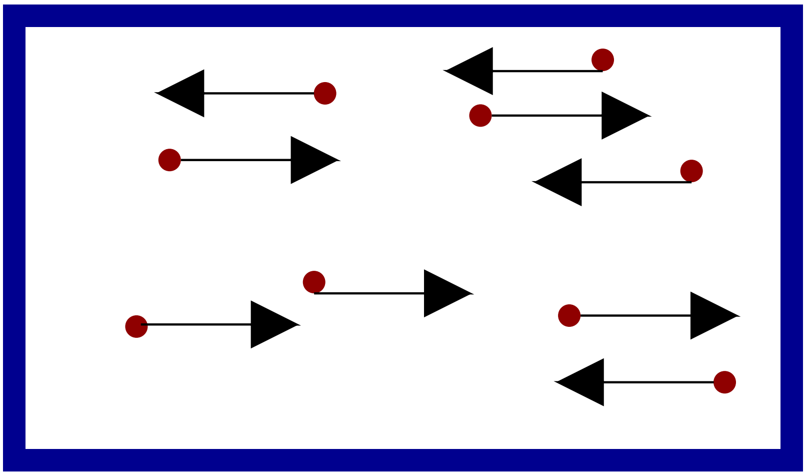
Fundamental Equation:

$$H\psi_n = E_n\psi_n$$

E_n are the energy levels

Approximate with finite matrix.

Origins (cont)



Statistical Mechanics: for each configuration, calculate quantity (say pressure).

Average over all configurations – most configurations close to system average.

Nuclear physics: choose matrix at random, calculate eigenvalues, average over matrices.

Look at: Real Symmetric, Complex Hermitian, Classical Compact Groups.

Random Matrix Ensembles

Real Symmetric Matrices:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1N} \\ a_{12} & a_{22} & a_{23} & \cdots & a_{2N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1N} & a_{2N} & a_{3N} & \cdots & a_N \end{pmatrix} = A^T$$

Let $p(x)$ be a probability density.

$$\begin{aligned} p(x) &\geq 0 \\ \int_{\mathbb{R}} p(x)dx &= 1. \end{aligned}$$

Often assume $p(x)$ has finite moments:

$$k^{th}\text{-moment} = \int_{\mathbb{R}} x^k p(x)dx.$$

Define

$$\text{Prob}(A) = \prod_{1 \leq i < j \leq N} p(a_{ij}).$$

Eigenvalue Distribution

Key to Averaging:

$$\text{Trace}(A^k) \;=\; \sum_{i=1}^{N} \lambda_i^k(A).$$

By the Central Limit Theorem:

$$\begin{aligned}
\text{Trace}(A^2) \;&=\; \sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}a_{ji} \\
&=\; \sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}^2 \\
&\sim\; N^2 \cdot 1 \\
\sum_{i=1}^{N} \lambda_i^2(A) \;&\sim\; N^2
\end{aligned}$$

Gives $N\text{Ave}(\lambda_i^2(A)) \;\sim\; N^2$ or $\lambda_i(A) \sim \sqrt{N}$.

Eigenvalue Distribution (cont)

$\delta(x - x_0)$ is a unit point mass at x_0.

To each A, attach a probability measure:

$$\mu_{A,N}(x) \;=\; \frac{1}{N}\sum_{i=1}^{N}\delta\left(x - \frac{\lambda_i(A)}{2\sqrt{N}}\right)$$

Obtain:

$$\begin{aligned} k^{th}\text{-moment} &= \int x^k \mu_{A,N}(x)dx \\ &= \frac{1}{N}\sum_{i=1}^{N}\frac{\lambda_i^k(A)}{(2\sqrt{N})^k} \\ &= \frac{\text{Trace}(A^k)}{2^k N^{\frac{k}{2}+1}} \end{aligned}$$

Semi-Circle Law

$N \times N$ real symmetric matrices, entries i.i.d.r.v. from fixed $p(x)$.

Semi-Circle Law: Assume p has mean 0, variance 1, other moments finite. Then

$$\mu_{A,N}(x) \ \longrightarrow\ \frac{2}{\pi}\sqrt{1-x^2} \ \text{ with probability } 1$$

Trace formula converts sums over eigenvalues to sums over entries of A.

Expected value of k^{th}-moment of $\mu_{A,N}(x)$ is

$$\int_{\mathbb{R}} \cdots \int_{\mathbb{R}} \frac{\text{Trace}(A^k)}{2^k N^{\frac{k}{2}+1}} \prod_{i<j} p(a_{ij}) da_{ij}$$

Proof: 2^{nd}-Moment

$$\text{Trace}(A^2) \;=\; \sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}a_{ji} \;=\; \sum_{i=1}^{N}\sum_{j=1}^{N} a_{ij}^2.$$

Substituting into expansion gives

$$\frac{1}{2^2N^2}\int_{\mathbb{R}}\cdots\int_{\mathbb{R}} \sum_{i,j=1}^{N} a_{ji}^2 \cdot p(a_{11})da_{11}\cdots p(a_{NN})da_{NN}$$

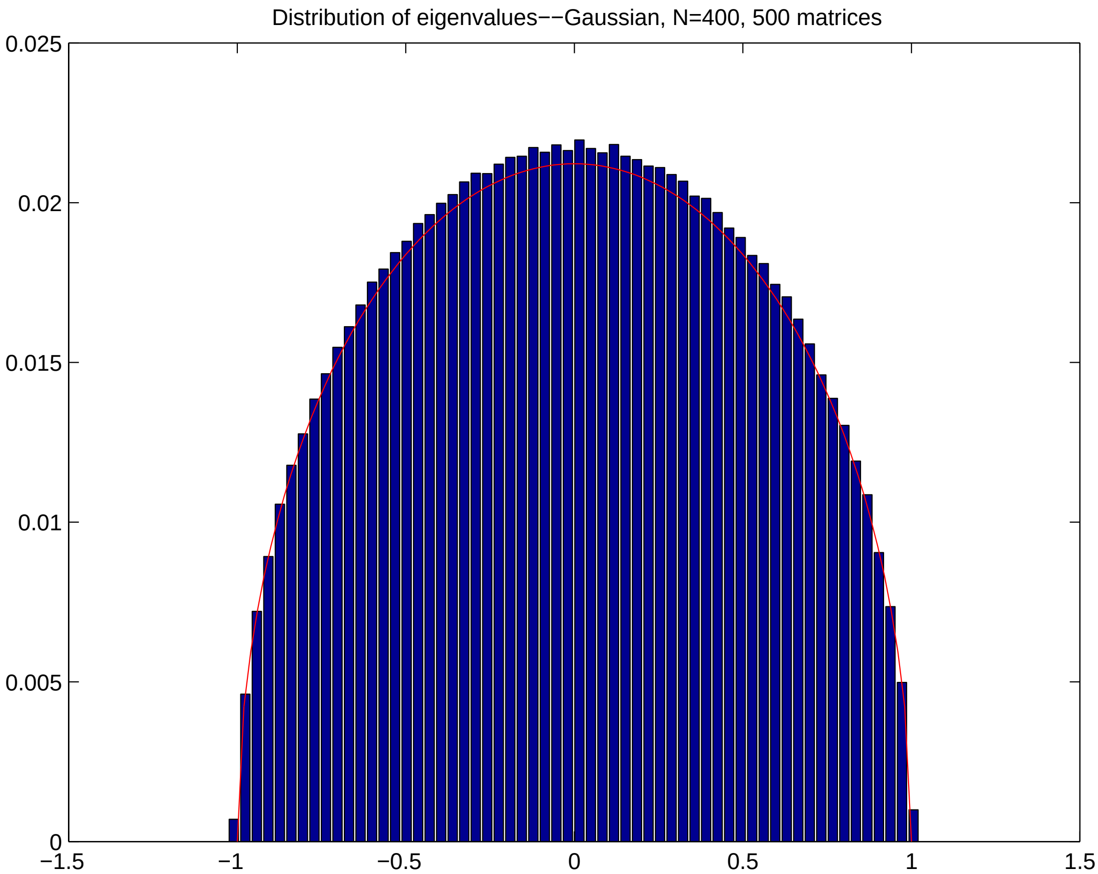
Integration factors as

$$\int_{a_{ij}\in\mathbb{R}} a_{ij}^2 p(a_{ij})da_{ij} \quad\cdot \prod_{\substack{(k,l)\neq(ij)\\ k<l}} \int_{a_{kl}\in\mathbb{R}} p(a_{kl})da_{kl} \;=\; 1.$$

Have N^2 summands, answer is $\frac{1}{4}$.

Key: Averaging Formula, Trace Lemma.

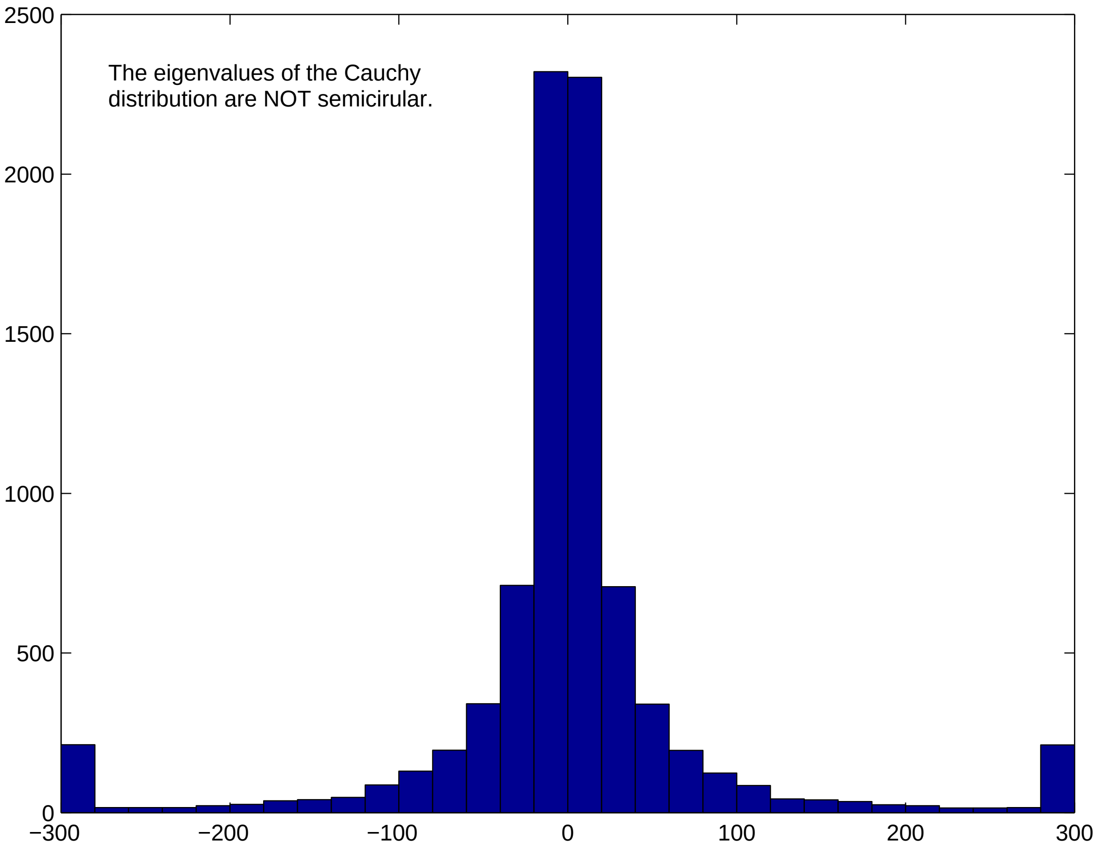
Random Matrix Theory: Semi-Circle Law



500 Matrices: Gaussian 400×400

$$p(x) = \frac{1}{\sqrt{2\pi}} e^{-x^2/2}$$

Random Matrix Theory:
Semi-Circle Law



Cauchy Distr: Not-Semicircular (Infinite Variance)

$$p(x) = \frac{1}{\pi(1+x^2)}$$

GOE Conjecture

GOE Conjecture: $N \times N$ Real Symmetric, entries iidrv. 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).

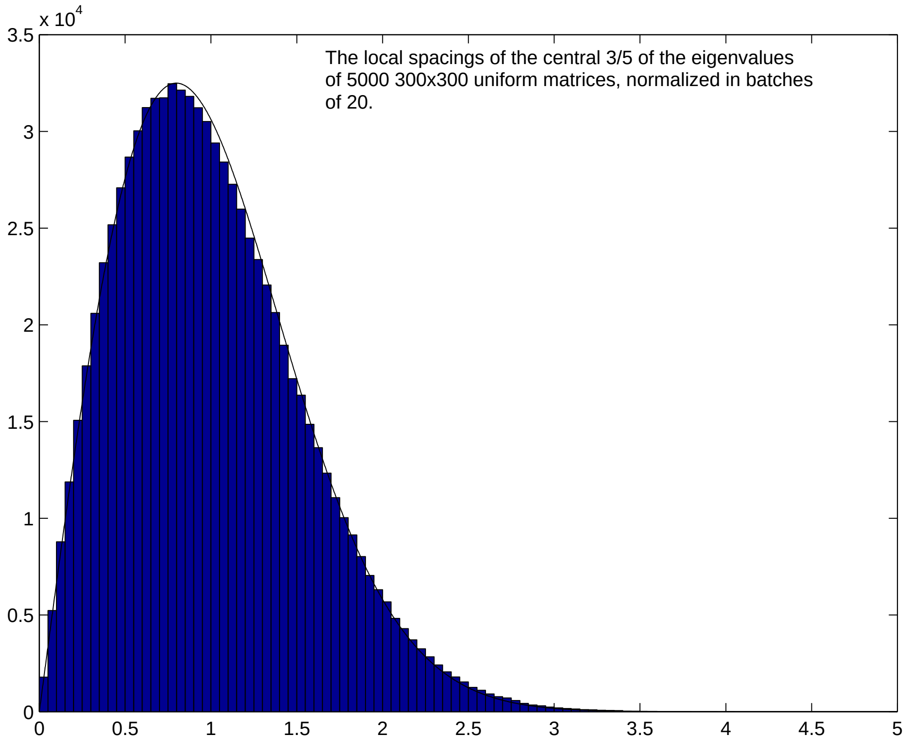
$\Psi(t)$ is (up to constants) the Fredholm determinant of the operator $f \longrightarrow \int_{-t}^{t} K * f$, kernel

$$K = \frac{1}{2\pi}\left(\frac{\sin(\xi - \eta)}{\xi - \eta} + \frac{\sin(\xi + \eta)}{\xi + \eta}\right)$$

Only known if entries chosen from Gaussian.

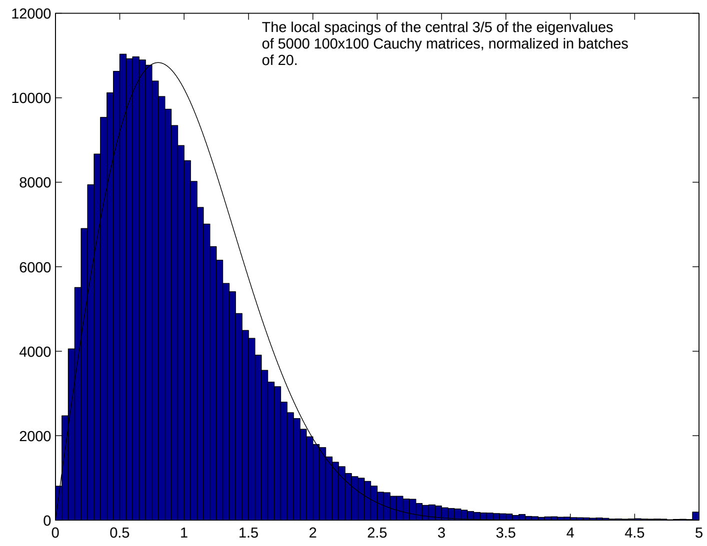
Consecutive spacings well approximated by Axe^{-Bx^2}.

Uniform Distribution: $p(x) = \frac{1}{2}$

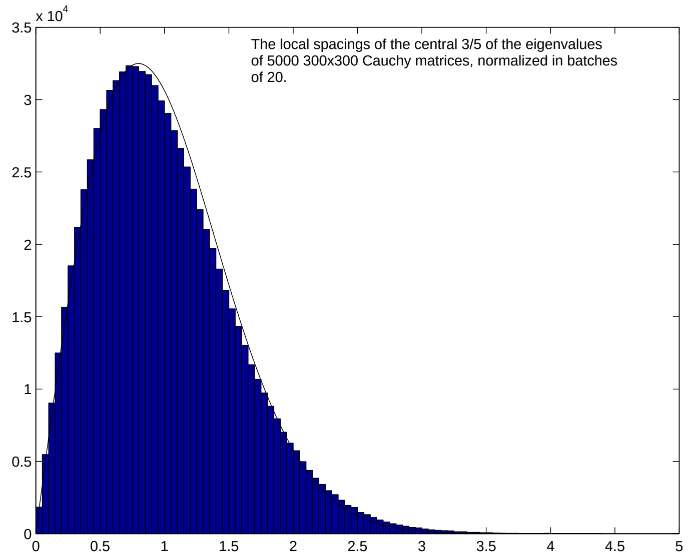


5000: 300×300 uniform on $[-1, 1]$

Cauchy Distribution: $p(x) = \frac{1}{\pi(1+x^2)}$

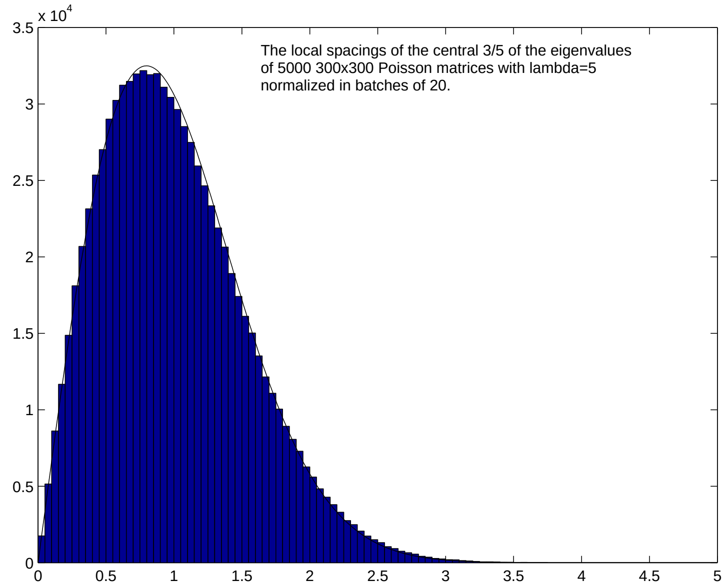


5000: 100×100 Cauchy

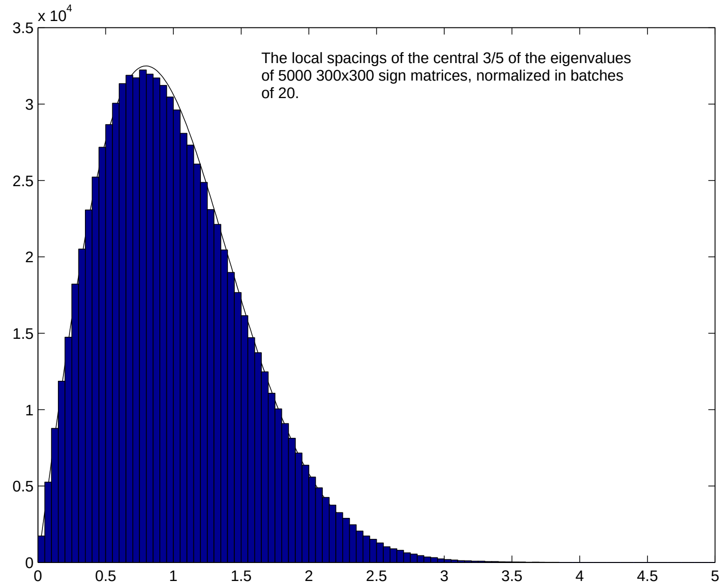


5000: 300×300 Cauchy

Poisson Distribution: $p(n) = \frac{\lambda^n}{n!} e^{-\lambda}$



5000: 300×300 Poisson, $\lambda = 5$



5000: 300×300 Poisson, $\lambda = 20$

Fat Thin Families

Need a family ***F A T*** enough to do averaging.

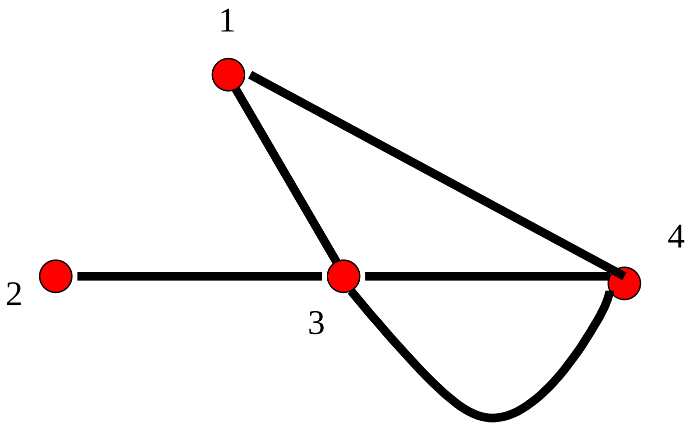
Need a family ***THIN*** enough so that everything isn't averaged out.

Real Symmetric Matrices have $\frac{N(N+1)}{2}$ independent entries.

Examples of thin sub-families:

- Band Matrices
- Random Graphs
- Special Matrices (Toeplitz)

Random Graphs



Degree of a vertex = number of edges leaving the vertex.

Adjacency matrix: a_{ij} = number edges from Vertex i to Vertex j.

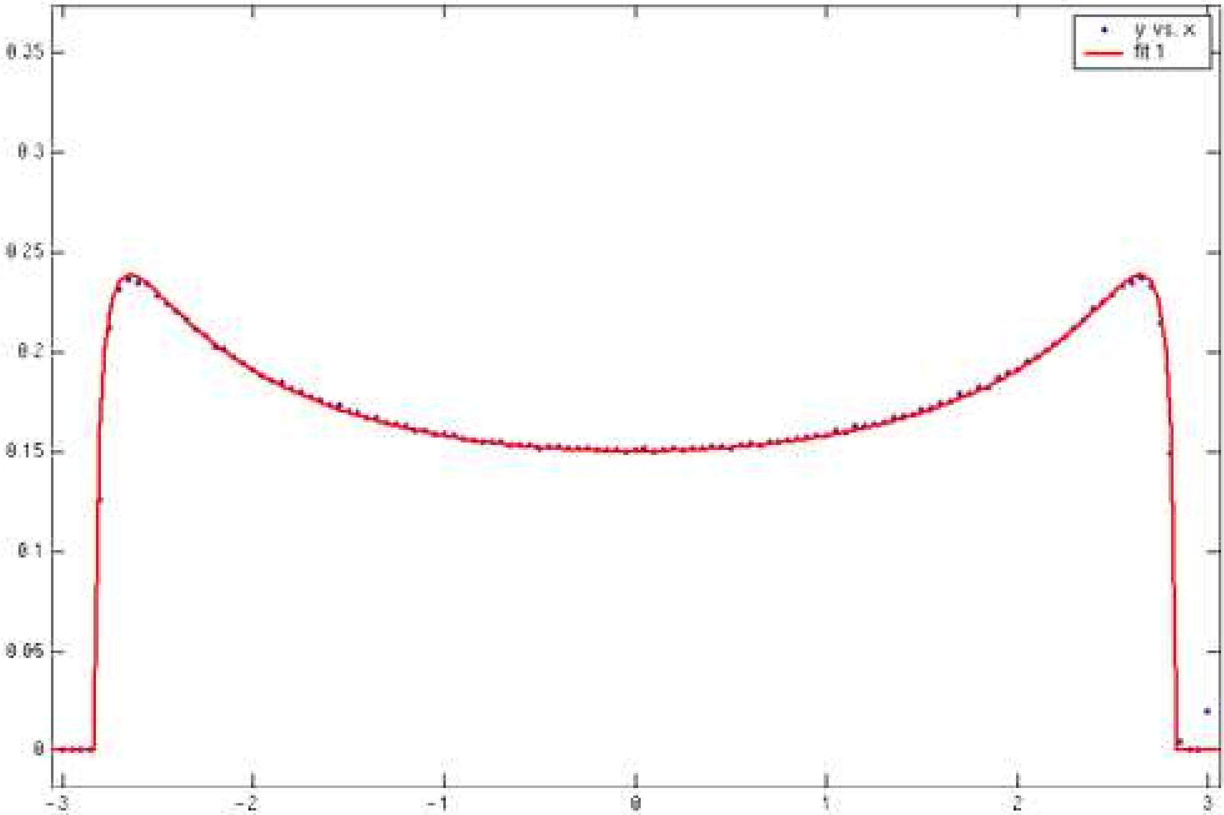
$$A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{pmatrix}$$

These are Real Symmetric Matrices.

McKay's Law (Kesten Measure)

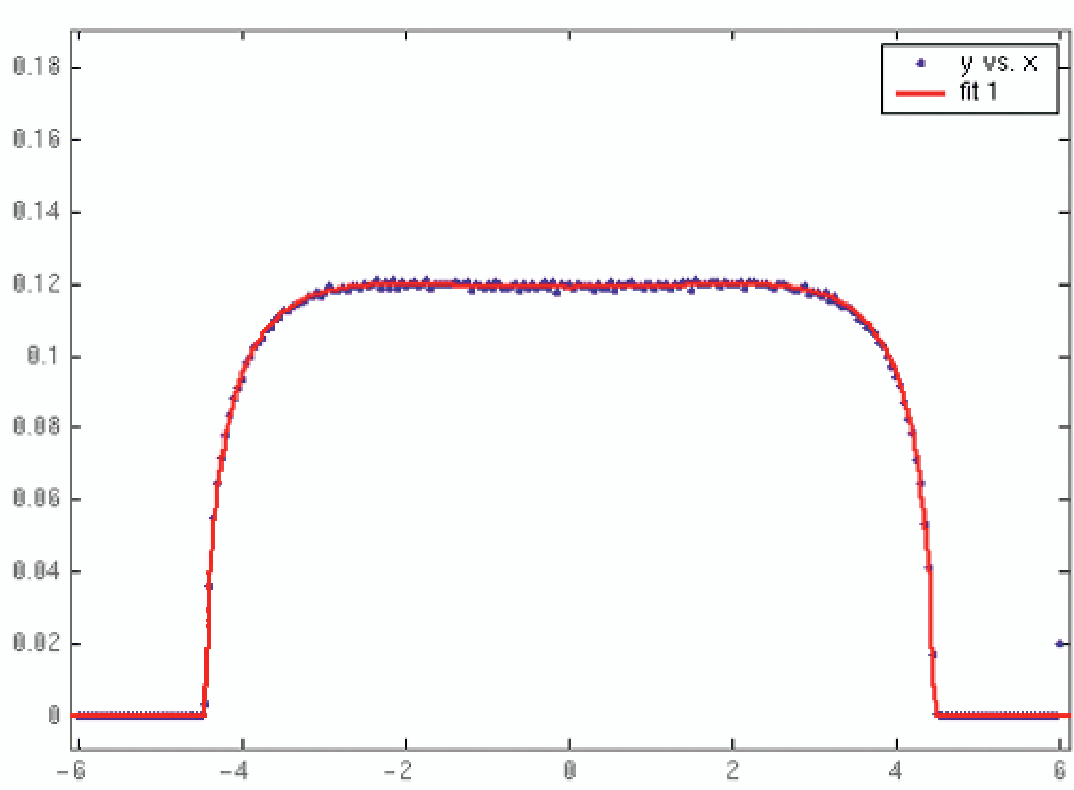
Density of States for d-regular graphs

$$f(x) \;=\; \begin{cases} \frac{d}{2\pi(d^2-x^2)}\sqrt{4(d-1)-x^2} & |x| \le 2\sqrt{d-1} \\ 0 & \text{otherwise} \end{cases}$$



$$d \;=\; 3.$$

McKay's Law (Kesten Measure)

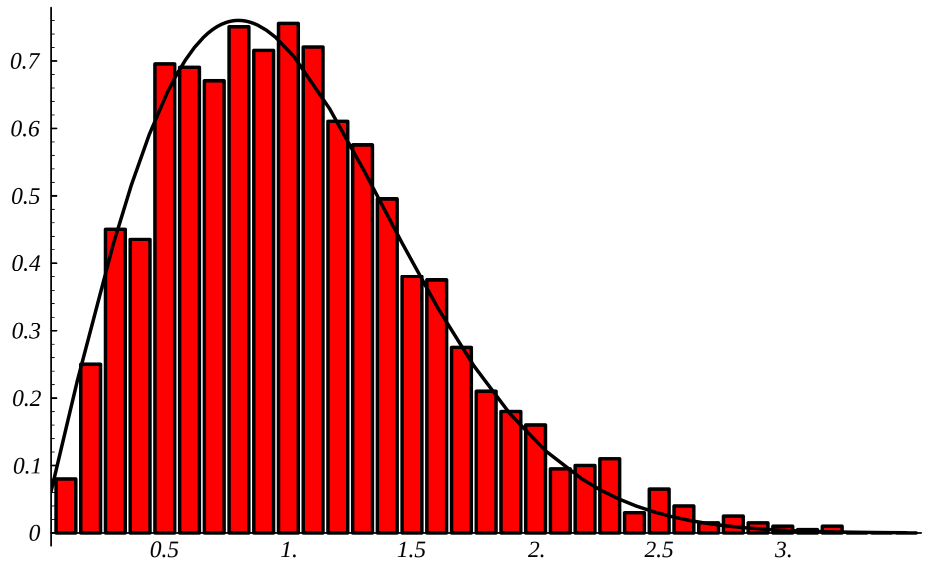


$$d = 6.$$

Idea of proof: Trace lemma, combinatorics and counting.

Fat Thin: fat enough to average, thin enough to get something different than Semi-circle.

d-Regular and GOE



3-Regular, 2000 Vertices

Graph courtesy of D. Jakobson, S. D. Miller, Z. Rudnick, R. Rivin

Riemann Zeta Function: $\zeta(s)$

Riemann Zeta-Function:

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

Functional Equation:

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

Riemann Hypothesis: All non-trivial zeros have $\mathrm{Re}(s) = \frac{1}{2}$; ie, on the critical line.

Spacings between zeros same as spacings between eigenvalues of Complex Hermitian matrices.

Contour Integration

$$
\begin{aligned}
-\frac{\zeta'(s)}{\zeta(s)} &= -\frac{\mathrm{d}}{\mathrm{d}s}\log\zeta(s) \\
&= \frac{\mathrm{d}}{\mathrm{d}s}\sum_p \log\left(1-p^{-s}\right) \\
&= \sum_p \frac{\log p \ \cdot \ p^{-s}}{1-p^{-s}} \\
&= \sum_p \frac{\log p}{p^s} + \text{Good}(s).
\end{aligned}
$$

Contour Integration:

$$
\int -\frac{\zeta'(s)}{\zeta(s)}\frac{x^s}{s}ds \quad \text{vs} \quad \sum_p \log p \int \left(\frac{x}{p}\right)^s \frac{ds}{s}
$$

$$
x - \sum_{\substack{\rho \\ \zeta(\rho)=0}} \frac{x^\rho}{\rho} \quad \text{vs} \quad \sum_{p\le x}\log p.
$$

L-Functions

L-functions: Re$(s) > s_0$:

$$L(s,f) = \sum_{n=1}^{\infty} \frac{a_n(f)}{n^s} = \prod_p L_p(p^{-s}, f)^{-1}.$$

Functional equation: $s \longleftrightarrow 1-s$.

GRH: All L-functions (after normalization) have their non-trivial zeros on the critical line.

Measures of Spacings: n-Level Correlations

$\{\alpha_j\}$ be an increasing sequence of numbers, $B \subset \mathbf{R}^{n-1}$ 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.

Results:

1. Normalized spacings of $\zeta(s)$ starting at 10^{20} (Odlyzko)
2. Pair and triple correlations of $\zeta(s)$ (Montgomery, Hejhal)
3. n-level correlations for all automorphic cupsidal L-functions (Rudnick-Sarnak)
4. n-level correlations for the classical compact groups (Katz-Sarnak)
5. insensitive to any finite set of zeros

Measures of Spacings: n-Level Density and Families

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

$$D_{n,f}(\phi) \;=\; \sum_{\substack{j_1,\dots,j_n \\ distinct}} \phi_1\left(L_f\gamma_f^{(j_1)}\right)\cdots\phi_n\left(L_f\gamma_f^{(j_n)}\right)$$

1. individual zeros contribute in limit
2. most of contribution is from low zeros
3. average over similar curves (family)

To any geometric family, Katz-Sarnak predict the n-level density depends only on a symmetry group attached to the family.

Correspondences

Similarities b/w Nuclear Physics and L-Functions

Zeros $\longleftrightarrow$ Energy Levels

Support $\longleftrightarrow$ Neutron Energy

Conjecture: Zeros near central point in a family of L-functions behave like eigenvalues near 1 of a classical compact group (Unitary, Symplectic, Orthogonal).

$$\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}} D_{n,f}(\phi) \;=\; \frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}}\sum_{\substack{j_1,\dots,j_n\\ j_i\neq\pm j_k}}\prod_i \phi_i\left(\frac{\log N_f}{2\pi}\gamma_f^{(j_i)}\right)$$

$$\to \int\cdots\int \phi(x)W_{n,\mathcal{G}(\mathcal{F})}(x)dx$$

$$= \int\cdots\int \widehat{\phi}(u)\widehat{W_{n,\mathcal{G}(\mathcal{F})}}(u)du.$$

Some Number Theory Results

- Orthogonal:

  Iwaniec-Luo-Sarnak: 1-level density for $H_k^{\pm}(N)$, N square-free;

  Hughes-Miller: n-level density for $H_k^{\pm}(N)$, N square-free;

  Dueñez-Miller: 1, 2-level $\{\phi \times \text{sym}^2 f : f \in H_k(1)\}$, ϕ even Maass;

  Miller: 1, 2-level for one-parameter families of elliptic curves.

- Symplectic:

  Rubinstein: n-level densities for $L(s, \chi_d)$;

  Dueñez-Miller: 1-level for $\{\phi \times f : f \in H_k(1)\}$, ϕ even Maass.

- Unitary:

  Miller, Hughes-Rudnick: Families of Primitive Dirichlet Characters.

Main Tools

- Explicit Formula: Relates sums over zeros to sums over primes.

- Averaging Formulas: Petersson formula in ILS, Orthogonality of characters in Rubinstein, Hughes-Rudnick, Miller.

- Control of conductors: Monotone.

1-Level Densities

The Fourier Transforms for the 1-level densities are

$$\begin{aligned}
\widehat{W_{1,\text{SO(even)}}}(u) &= \delta_0(u) + \frac{1}{2}\eta(u) \\
\widehat{W_{1,\text{SO}}}(u) &= \delta_0(u) + \frac{1}{2} \\
\widehat{W_{1,\text{SO(odd)}}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) + 1
\end{aligned}$$

$$\widehat{W_{1,\text{Symplectic}}}(u) = \delta_0(u) - \frac{1}{2}\eta(u)$$

$$\widehat{W_{1,\text{Unitary}}}(u) = \delta_0(u)$$

where $\delta_0(u)$ is the Dirac Delta functional and

$$\eta(u) = \begin{cases} 1 & \text{if } |u| < 1 \\ \frac{1}{2} & \text{if } |u| = 1 \\ 0 & \text{if } |u| > 1 \end{cases}$$

Dirichlet Characters:
m Prime

$(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic of order $m-1$ with generator g.

Let $\zeta_{m-1} = e^{2\pi i/(m-1)}$.

Principal character χ_0:

$$\chi_0(k) = \begin{cases} 1 & (k,m) = 1 \\ 0 & (k,m) > 1. \end{cases}$$

The $m-2$ primitive characters are determined (by multiplicativity) by action on g.

As each $\chi : (\mathbb{Z}/m\mathbb{Z})^* \to \mathbb{C}^*$, for each χ there exists an l such that $\chi(g) = \zeta_{m-1}^l$. Thus

$$\chi_l(k) \;=\; \begin{cases} \zeta_{m-1}^{la} & k \equiv g^a(m) \\ 0 & (k,m) > 0 \end{cases}$$

Dirichlet L-Functions

Let χ be a primitive character mod m. Let

$$c(m,\chi) = \sum_{k=0}^{m-1} \chi(k) e^{2\pi i k/m}.$$

$c(m,\chi)$ is a Gauss sum of modulus $\sqrt{m}$.

$$\begin{aligned} L(s,\chi) &= \prod_p (1-\chi(p)p^{-s})^{-1} \\ \Lambda(s,\chi) &= \pi^{-\frac{1}{2}(s+\epsilon)} \Gamma\left(\frac{s+\epsilon}{2}\right) m^{\frac{1}{2}(s+\epsilon)} L(s,\chi), \end{aligned}$$

where

$$\begin{aligned} \epsilon &= \begin{cases} 0 & \text{if } \chi(-1) = 1 \\ 1 & \text{if } \chi(-1) = -1 \end{cases} \\ \Lambda(s,\chi) &= (-i)^{\epsilon} \frac{c(m,\chi)}{\sqrt{m}} \Lambda(1-s,\bar{\chi}). \end{aligned}$$

Explicit Formula

Let ϕ be an even Schwartz function with compact support $(-\sigma, \sigma)$.

Let χ be a non-trivial primitive Dirichlet character of conductor m.

$$\sum \phi\left(\gamma \frac{\log(\frac{m}{\pi})}{2\pi}\right)$$

$$= \int_{-\infty}^{\infty} \phi(y) dy$$

$$- \sum_p \frac{\log p}{\log(m/\pi)} \widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right) [\chi(p) + \bar{\chi}(p)] p^{-\frac{1}{2}}$$

$$- \sum_p \frac{\log p}{\log(m/\pi)} \widehat{\phi}\left(2\frac{\log p}{\log(m/\pi)}\right) [\chi^2(p) + \bar{\chi}^2(p)] p^{-1}$$

$$+ O\left(\frac{1}{\log m}\right).$$

Expansion

$\{\chi_0\} \cup \{\chi_l\}_{1 \le l \le m-2}$ are all the characters mod m.

Consider the family of primitive characters mod a prime m ($m-2$ characters):

$$\begin{aligned}
&\int_{-\infty}^{\infty} \phi(y)dy \\
-&\ \frac{1}{m-2}\sum_{\chi\neq\chi_0}\sum_p \frac{\log p}{\log(m/\pi)}\widehat{\phi}\Big(\frac{\log p}{\log(m/\pi)}\Big)[\chi(p)+\bar{\chi}(p)]p^{-\frac{1}{2}} \\
-&\ \frac{1}{m-2}\sum_{\chi\neq\chi_0}\sum_p \frac{\log p}{\log(m/\pi)}\widehat{\phi}\Big(2\frac{\log p}{\log(m/\pi)}\Big)[\chi^2(p)+\bar{\chi}^2(p)]p^{-1} \\
+&\ O\Big(\frac{1}{\log m}\Big).
\end{aligned}$$

Note can pass Character Sum through Test Function.

Character Sums

$$\sum_{\chi} \chi(k) = \begin{cases} m-1 & k \equiv 1(m) \\ 0 & \text{otherwise} \end{cases}$$

For any prime $p \neq m$

$$\sum_{\chi \neq \chi_0} \chi(p) \;=\; \begin{cases} m-1-1 & p \equiv 1(m) \\ -1 & \text{otherwise} \end{cases}$$

Substitute into

$$\frac{1}{m-2} \sum_{\chi \neq \chi_0} \sum_{p} \frac{\log p}{\log(m/\pi)} \widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right) [\chi(p) + \bar{\chi}(p)] p^{-\frac{1}{2}}$$

First Sum

$$\begin{aligned}
&\frac{-2}{m-2}\sum_{p}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\Big(\frac{\log p}{\log(m/\pi)}\Big)p^{-\frac{1}{2}}\\
&+\ 2\frac{m-1}{m-2}\sum_{p\equiv 1(m)}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\Big(\frac{\log p}{\log(m/\pi)}\Big)p^{-\frac{1}{2}}\\
&\ll\ \frac{1}{m}\sum_{p}^{m^\sigma}p^{-\frac{1}{2}}\ +\ \sum_{p\equiv 1(m)}^{m^\sigma}p^{-\frac{1}{2}}\\
&\ll\ \frac{1}{m}\sum_{k}^{m^\sigma}k^{-\frac{1}{2}}\ +\ \sum_{\substack{k\equiv 1(m)\\ k\geq m+1}}^{m^\sigma}k^{-\frac{1}{2}}\\
&\ll\ \frac{1}{m}\sum_{k}^{m^\sigma}k^{-\frac{1}{2}}\ +\ \frac{1}{m}\sum_{k}^{m^\sigma}k^{-\frac{1}{2}}\\
&\ll\ \frac{1}{m}m^{\sigma/2}.
\end{aligned}$$

No contribution if $\sigma < 2$.

Second Sum

$$\frac{1}{m-2}\sum_{\chi\neq\chi_0}\sum_{p}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\left(2\frac{\log p}{\log(m/\pi)}\right)\frac{\chi^2(p)+\bar{\chi}^2(p)}{p}.$$

$$\sum_{\chi\neq\chi_0}[\chi^2(p)+\bar{\chi}^2(p)] \;=\; \begin{cases} 2(m-2) & p\equiv\pm1(m) \\ -2 & p\not\equiv\pm1(m)\end{cases}$$

Up to $O\left(\frac{1}{\log m}\right)$ we find that

$$\ll \frac{1}{m-2}\sum_{p}^{m^{\sigma/2}} p^{-1} + \frac{2m-2}{m-2}\sum_{p\equiv\pm1(m)}^{m^{\sigma/2}} p^{-1}$$

$$\ll \frac{1}{m-2}\sum_{k}^{m^{\sigma/2}} k^{-1} + \sum_{\substack{k\equiv1(m)\\ k\geq m+1}}^{m^{\sigma/2}} k^{-1} + \sum_{\substack{k\equiv-1(m)\\ k\geq m-1}}^{m^{\sigma/2}} k^{-1}$$

$$\ll \frac{\log(m^{\sigma/2})}{m-2} + \frac{1}{m}\sum_{k}^{m^{\sigma/2}} k^{-1} + \frac{1}{m}\sum_{k}^{m^{\sigma/2}} k^{-1} + O\left(\frac{1}{m}\right)$$

$$\ll \frac{\log m}{m} + \frac{\log m}{m} + \frac{\log m}{m}.$$

Results

Theorem [Hughes-Rudnick 2002]
$\mathcal{F}_N$ all primitive characters with prime conductor N.

If supp$(\widehat{\phi}) \subset (-2, 2)$, as $N \to \infty$ agrees with Unitary.

Theorem [Miller 2002]
$\mathcal{F}_N$ all primitive characters with conductor odd square-free integer in $[N, 2N]$.

If supp$(\widehat{\phi}) <\subset (-2, 2)$, as $N \to \infty$ agrees with Unitary.

Elliptic Curves

$$E : y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6, \ \ a_i \in \mathbb{Q}$$

Often can write $E : y^2 = x^3 + Ax + B$.

Let N_p be the number of solns mod p:

$$N_p = \sum_{x(p)} \left[1 + \left(\frac{x^3 + Ax + B}{p}\right)\right] = p+\sum_{x(p)} \left(\frac{x^3 + Ax + B}{p}\right)$$

Local data: $a_E(p) = p - N_p$.

More generally, let $a_i = a_i(T) \in \mathbb{Z}[T]$.

Elliptic Curves (cont)

$$L(E,s) \;=\; \sum_{n=1}^{\infty} \frac{a_E(n)}{n^s} \;=\; \prod_p L_p(E,s).$$

By GRH: All zeros on the critical line.

Rational solutions: $E(\mathbb{Q}) = \mathbb{Z}^r \bigoplus T$.

Birch and Swinnerton-Dyer Conjecture:
Geometric rank r equals analytic rank (order of vanishing at central point).

Elliptic Curves

Conductors grow rapidly.

Results for small support, where Orthogonal densities indistinguishable.

Study 1 and 2-Level Densities.

$$D_{n,E}(\phi) = \sum_{\substack{j_1,\dots,j_n \\ \text{distinct}}} \phi_1\left(L_E\gamma_E^{(j_1)}\right)\cdots\phi_n\left(L_E\gamma_E^{(j_n)}\right)$$

$$D_{n,\mathcal{F}}(\phi) = \frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} D_{n,E}(\phi).$$

2-Level Densities

$$c(\mathcal{G}) = \begin{cases} 0 & \text{if } \mathcal{G} = \text{SO(even)} \\ \frac{1}{2} & \text{if } \mathcal{G} = \text{O} \\ 1 & \text{if } \mathcal{G} = \text{SO(odd)} \end{cases}$$

For $\mathcal{G} = \text{SO(even)}$, O or SO(odd):

$$\begin{aligned} & \int\int \widehat{\phi_1}(u_1)\widehat{\phi_2}(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 \\ = & \left[\widehat{\phi_1}(0) + \frac{1}{2}\phi_1(0)\right]\left[\widehat{f_2}(0) + \frac{1}{2}\phi_2(0)\right] \\ & + 2\int |u|\widehat{\phi_1}(u)\widehat{\phi_2}(u)du \\ & -2\widehat{\phi_1\phi_2}(0) - \phi_1(0)\phi_2(0) \\ & + c(\mathcal{G})\phi_1(0)\phi_2(0). \end{aligned}$$

Comments on Previous Results

- explicit formula relating zeros and Fourier coeffs;
- averaging formulas for the family;
- conductors easy to control (constant, monotone)

Elliptic curve E_t: discriminant $\Delta(t)$, conductor $N_{E_t} = C(t)$ is

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

Conj: Distribution of Low Zeros agrees with Orthogonal Densities.

1-Level Expansion

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

Want to move $\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}}$, leads us to study

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

2-Level Expansion

Need to evaluate terms like

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

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

$$\sum_{t \bmod p_1\cdots p_n} a_t^{r_1}(p_1)\cdots a_t^{r_n}(p_n) \;=\; A_{r_1,\mathcal{F}}(p_1)\cdots A_{r_n,\mathcal{F}}(p_n).$$

Input

For many families

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

Rational Elliptic Surfaces (Rosen and Silverman): If rank r over $\mathbb{Q}(T)$:

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

Surfaces with $j(T)$ non-constant (Michel):

$$A_{2,\mathcal{F}}(p) = p^2 + O\left(p^{3/2}\right).$$

DEFINITIONS

$$D_{n,\mathcal{F}}(\phi) = \frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} \sum_{\substack{j_1,\dots,j_n \\ j_i \neq \pm j_k}} \prod_i \phi_i \left(\frac{\log N_E}{2\pi} \gamma_E^{(j_i)} \right)$$

$D_{n,\mathcal{F}}^{(r)}(\phi)$: n-level density with contribution of r zeros at central point removed.

$\mathcal{F}_N$: Rational one-parameter family, $t \in [N, 2N]$, conductors monotone.

ASSUMPTIONS

1-parameter family of Ell Curves, rank r over $\mathbb{Q}(T)$, rational surface.

Assume

- GRH;
- $j(T)$ non-constant;
- Sq-Free Sieve if $\Delta(T)$ has irr poly factor of deg ≥ 4.

Pass to positive percent sub-seq where conductors polynomial of degree m.

ϕ_i even Schwartz, support $(-\sigma_i, \sigma_i)$:

- $\sigma_1 < \min\left(\frac{1}{2}, \frac{2}{3m}\right)$ for 1-level
- $\sigma_1 + \sigma_2 < \frac{1}{3m}$ for 2-level.

MAIN RESULT

Theorem (M–): Under previous conditions, as $N \to \infty$, $n = 1, 2$:

$$D^{(r)}_{n,\mathcal{F}_N}(\phi) \longrightarrow \int \phi(x) W_{\mathcal{G}}(x) dx,$$

where

$$\mathcal{G} = \begin{cases} \text{O} & \text{if half odd} \\ \text{SO(even)} & \text{if all even} \\ \text{SO(odd)} & \text{if all odd} \end{cases}$$

1 and 2-level densities confirm Katz-Sarnak, B-SD predictions for small support.

Excess Rank

One-parameter family, rank r over $\mathbb{Q}(T)$, RMT $\Longrightarrow$ 50% rank r, r+1.

For many families, observe

Percent with rank r	= 32%
Percent with rank r+1	= 48%
Percent with rank r+2	= 18%
Percent with rank r+3	= 2%

Problem: small data sets, sub-families, convergence rate $\log(\text{conductor})$?

Data on Excess Rank

$$y^2 + a_1xy + a_3y \ = \ x^3 + a_2x^2 + a_4x + a6$$

Family: $a_1 : 0$ to 10, rest -10 to 10.

Percent with rank 0 = 28.60%
Percent with rank 1 = 47.56%
Percent with rank 2 = 20.97%
Percent with rank 3 = 2.79%
Percent with rank 4 = .08%

14 Hours, 2,139,291 curves
(2,971 singular, 248,478 distinct).

Data on Excess Rank

$$y^2 + y = x^3 + Tx$$

Each data set 2000 curves from start.

t-Start	Rk 0	Rk 1	Rk 2	Rk 3	Time (hrs)
-1000	39.4	47.8	12.3	0.6	<1
1000	38.4	47.3	13.6	0.6	<1
4000	37.4	47.8	13.7	1.1	1
8000	37.3	48.8	12.9	1.0	2.5
24000	35.1	50.1	13.9	0.8	6.8
50000	36.7	48.3	13.8	1.2	51.8

Last set has conductors of size 10^{11}, but on logarithmic scale still small.

Excess Rank Calculations
Families with $y^2 = f_t(x)$; $D(t)$ SqFree

Family	t Range	Num t	r	r	$r+1$	$r+2$	$r+3$
$+4(4t+2)$	$[2, 2002]$	1622	0		95.44		4.56
$-4(4t+2)$	$[2, 2002]$	1622	0	70.53		29.35	
$9t+1$	$[2, 247]$	169	0	71.01		28.99	
t^2+9t+1	$[2, 272]$	169	1	71.60		27.81	
$t(t-1)$	$[2, 2002]$	643	0	40.44	48.68	10.26	0.62
$(6t+1)x^2$	$[2, 101]$	93	1	34.41	47.31	17.20	1.08
$(6t+1)x$	$[2, 77]$	66	2	30.30	50.00	16.67	3.03

1. $x^3 + 4(4t+2)x$, $4t+2$ Sq-Free, odd.
2. $x^3 - 4(4t+2)x$, $4t+2$ Sq-Free, even.
3. $x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ Sq-Free, even.
4. $x^3 + tx^2 - (t+3)x + 1$, t^2+3t+9 Sq-Free, odd.
5. $x^3 + (t+1)x^2 + tx$, $t(t-1)$ Sq-Free, rank 0.
6. $x^3 + (6t+1)x^2 + 1$, $4(6t+1)^3 + 27$ Sq-Free, rank 1.
7. $x^3 - (6t+1)^2x + (6t+1)^2$, $(6t+1)[4(6t+1)^2 - 27]$ Sq-Free, rank 2.

Excess Rank Calculations
Families with $y^2 = f_t(x)$; All $D(t)$

Family	t Range	Num t	r	r	$r+1$	$r+2$	$r+3$
$+4(4t+2)$	$[2, 2002]$	2001	0	6.45	85.76	3.95	3.85
$-4(4t+2)$	$[2, 2002]$	2001	0	63.52	9.90	25.99	.50
$9t+1$	$[2, 247]$	247	0	55.28	23.98	20.73	
t^2+9t+1	$[2, 272]$	271	1	73.80		25.83	
$t(t-1)$	$[2, 2002]$	2001	0	42.03	48.43	9.25	0.30
$(6t+1)x^2$	$[2, 101]$	100	1	32.00	50.00	17.00	1.00
$(6t+1)x$	$[2, 77]$	76	2	32.89	50.00	14.47	2.63

1. $x^3 + 4(4t+2)x$, $4t+2$ Sq-Free, odd.
2. $x^3 - 4(4t+2)x$, $4t+2$ Sq-Free, even.
3. $x^3 + 2^4(-3)^3(9t+1)^2$, $9t+1$ Sq-Free, even.
4. $x^3 + tx^2 - (t+3)x + 1$, t^2+3t+9 Sq-Free, odd.
5. $x^3 + (t+1)x^2 + tx$, $t(t-1)$ Sq-Free, rank 0.
6. $x^3 + (6t+1)x^2 + 1$, $4(6t+1)^3 + 27$ Sq-Free, rank 1.
7. $x^3 - (6t+1)^2x + (6t+1)^2$, $(6t+1)[4(6t+1)^2 - 27]$ Sq-Free, rank 2.

Orthogonal Random Matrix Model

RMT: $2N$ eigenvalues, in pairs $e^{\pm i\theta_j}$, probability measure on $[0,\pi]^N$:

$$d\epsilon_0(\theta) \propto \prod_{j<k} (\cos\theta_k - \cos\theta_j)^2 \prod_j d\theta_j$$

Model: forced zeros independent (suggested by Function Field analogue)

$$\mathcal{A}_{2N,2r} = \left\{ \begin{pmatrix} g & \\ & I_{2r} \end{pmatrix} : g \in SO(2N-2r) \right\}$$

Orthogonal Random Matrix Models

RMT: $2N$ eigenvalues, in pairs $e^{\pm i\theta_j}$, probability measure on $[0,\pi]^N$:

$$d\epsilon_0(\theta) \propto \prod_{j<k}(\cos\theta_k - \cos\theta_j)^2 \prod_j d\theta_j$$

Interaction Model: NOT SUGGESTED BY FUNCTION FIELD

Sub-ensemble of $SO(2N)$ with the last $2n$ of the $2N$ eigenvalues equal $+1$:

$$d\varepsilon_{2n}(\theta) \propto \prod_{j<k}(\cos\theta_k - \cos\theta_j)^2 \prod_j (1-\cos\theta_j)^{2n} \prod_j d\theta_j,$$

with $1 \leq j,k \leq N-n$.

Independent Model: SUGGESTED BY FUNCTION FIELD

$$\mathcal{A}_{2N,2n} = \left\{ \begin{pmatrix} g & \\ & I_{2n} \end{pmatrix} : g \in SO(2N-2n) \right\}$$

Random Matrix Models and One-Level Densities

Fourier transform of 1-level density:

$$\hat{\rho}_0(u) = \delta(u) + \frac{1}{2}\eta(u).$$

Fourier transform of 1-level density (Rank 2, Independent):

$$\hat{\rho}_{2,\text{Ind}}(u) = \left[\delta(u) + \frac{1}{2}\eta(u) + 2\right].$$

Fourier transform of 1-level density (Rank 2, Interaction):

$$\hat{\rho}_{2,\text{Int}}(u) = \left[\delta(u) + \frac{1}{2}\eta(u) + 2\right] + 2(|u| - 1)\eta(u).$$

Testing RMT Model

For small support, 1-level densities for Elliptic Curves agree with $\rho_{r,\text{Indep}}$.

Curve E, conductor N_E, expect first zero $\frac{1}{2} + i\gamma_E^{(1)}$ with $\gamma_E^{(1)} \approx \frac{1}{\log N_E}$.

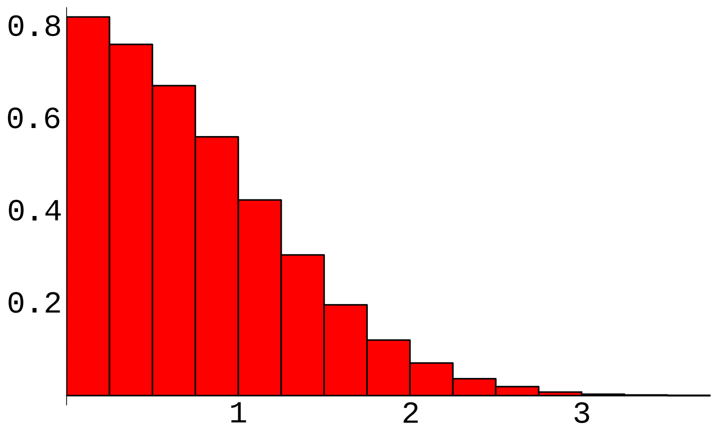
If r zeros at central point, if repulsion of zeros is of size $\frac{c_r}{\log N_E}$, might detect in 1-level density:

$$\frac{1}{|\mathcal{F}_N|} \sum_{E \in \mathcal{F}_N} \sum_j \phi\left(\frac{\gamma_E^{(j)} \log N_E}{2\pi}\right).$$

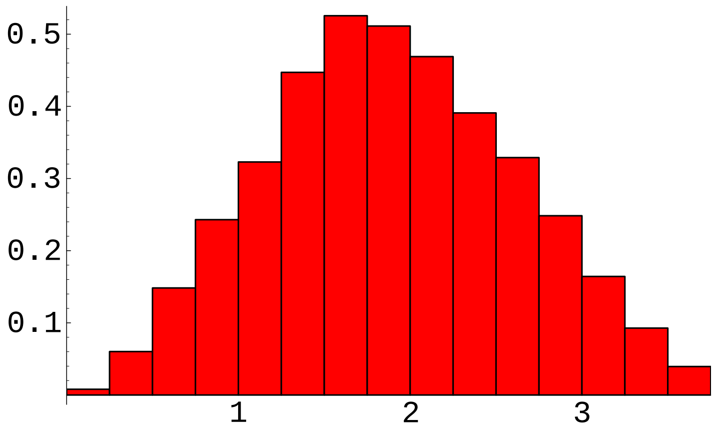
Corrections of size

$$\phi\left(x_0 + c_r\right) - \phi(x_0) \ \approx \ \phi'\left(x(x_0, c_r)\right) \cdot c_r.$$

Theoretical Distribution of First Normalized Zero



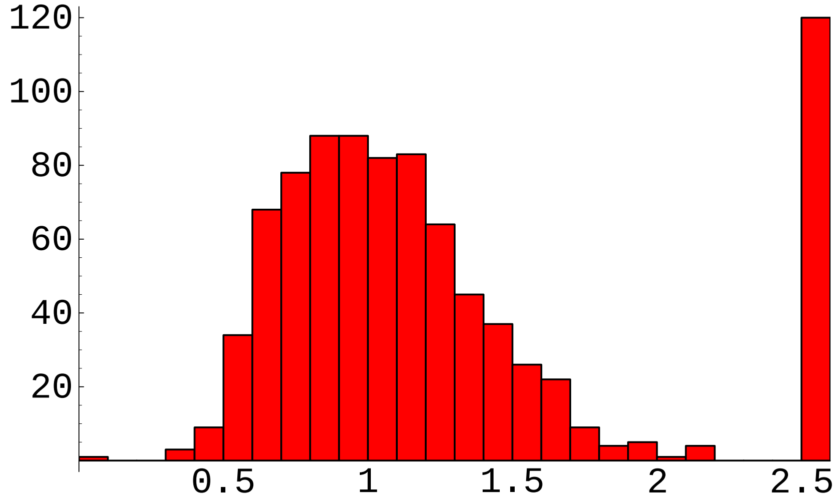
First normalized eigenvalue: 230,400 from SO(6) with Haar Measure



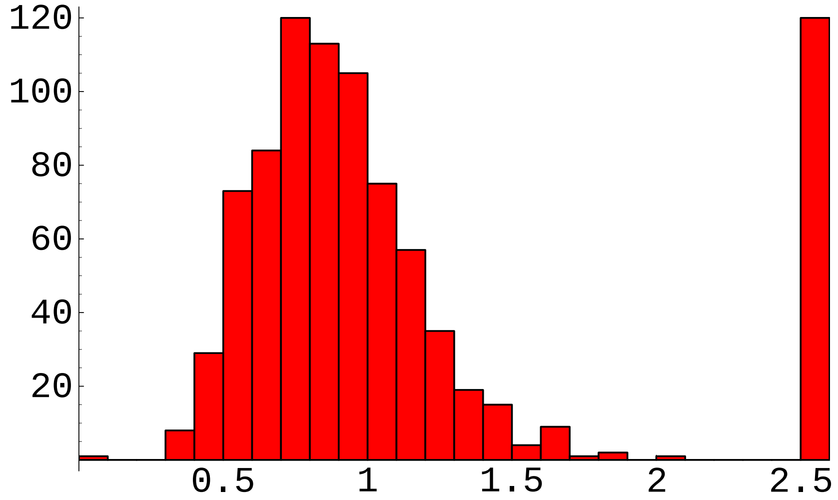
First normalized eigenvalue: 322,560 from SO(7) with Haar Measure

Rank 0 Curves: 1st Normalized Zero

(Far left and right bins just for formatting)

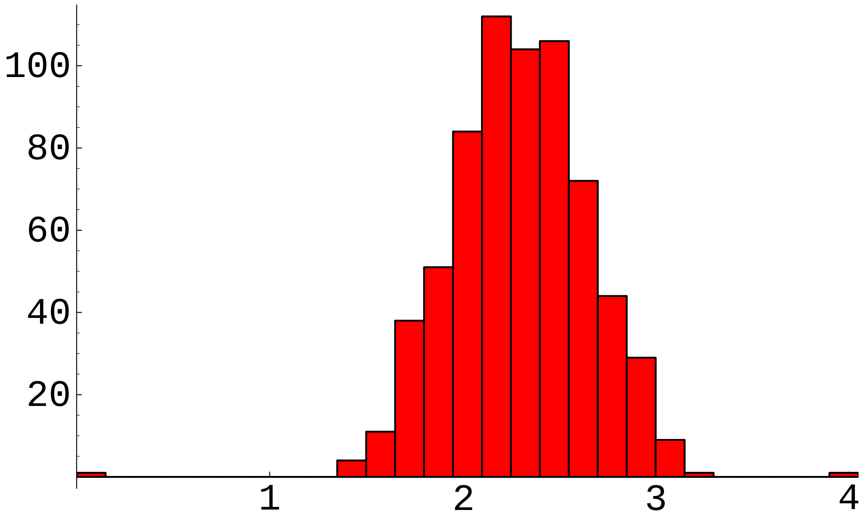


750 curves, $\log(\text{cond}) \in [3.2, 12.6]$; mean $= 1.04$

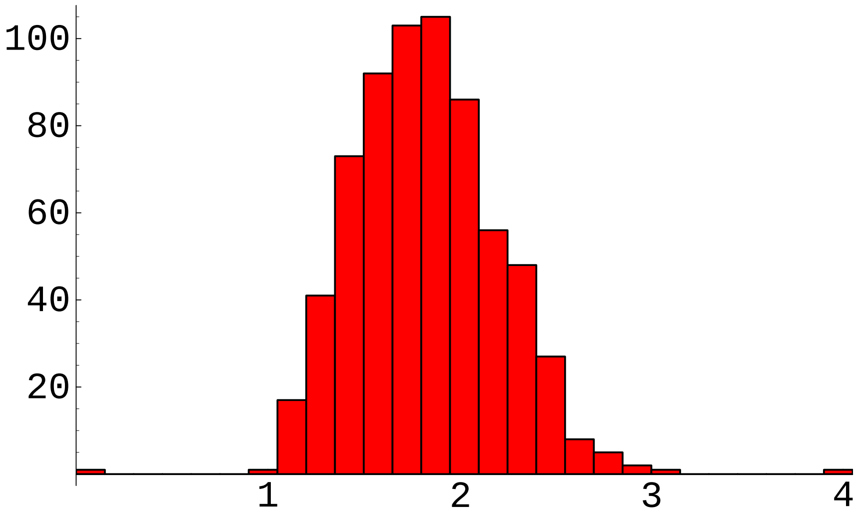


750curves, $\log(\text{cond}) \in [12.6, 14.9]$; mean $= .88$

Rank 2 Curves: 1st Normalized Zero

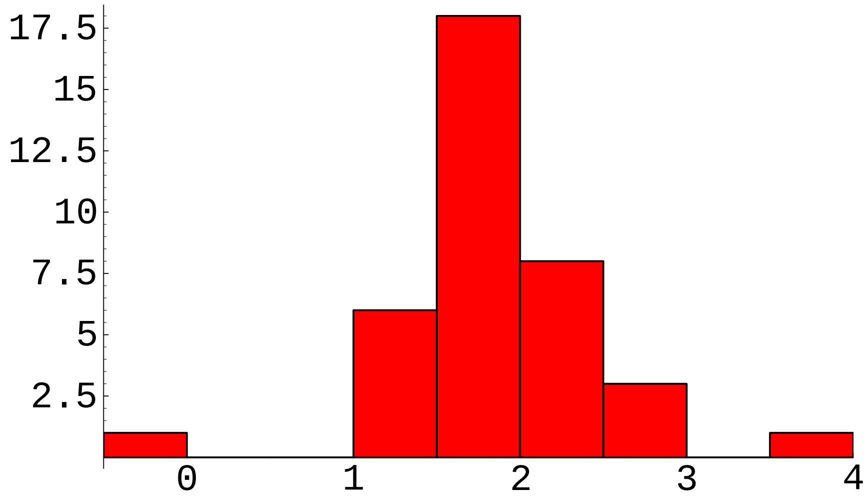


665 **curves**, $\log($**cond**$) \in [10, 10.3125]$; **mean** $= 2.30$

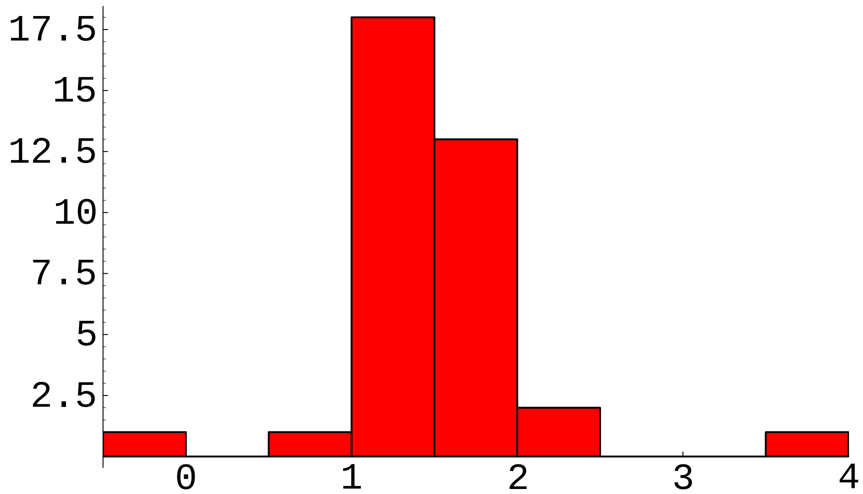


665 **curves**, $\log($**cond**$) \in [16, 16.5]$; **mean** $= 1.82$

Rank 2 Curves: $[0, 0, 0, -t^2, t^2]$ 1st Normalized Zero



35 curves, $\log(\text{cond}) \in [7.8, 16.1]$; mean $= 2.24$



34 curves, $\log(\text{cond}) \in [16.2, 23.3]$; mean $= 2.00$

Summary

- Similar behavior in different systems.
- Find correct scale.
- Average over similar elements.
- Need an Explicit Formula.
- Different statistics tell different stories.
- Evidence for B-SD, RMT interpretation of zeros
- Need more data.

Appendix

Below are some additional details / topics of interest.

Appendix One: Dirichlet Characters

Below is a sketch of the calculation for square-free conductors (and not just prime conductors).

Dirichlet Characters: m Square-free

Fix an r and let $m_1, \dots, m_r$ be distinct odd primes.

$$\begin{aligned} m &= m_1 m_2 \cdots m_r \\ M_1 &= (m_1-1)(m_2-1)\cdots(m_r-1) = \phi(m) \\ M_2 &= (m_1-2)(m_2-2)\cdots(m_r-2). \end{aligned}$$

M_2 is the number of primitive characters mod m, each of conductor m.

A general primitive character mod m is given by $\chi(u) = \chi_{l_1}(u)\chi_{l_2}(u)\cdots\chi_{l_r}(u)$.

Let $\mathcal{F} = \{\chi : \chi = \chi_{l_1}\chi_{l_2}\cdots\chi_{l_r}\}$.

$$\frac{1}{M_2}\sum_p \frac{\log p}{\log(m/\pi)}\widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right)p^{-\frac{1}{2}}\sum_{\chi\in\mathcal{F}}[\chi(p)+\bar{\chi}(p)]$$

$$\frac{1}{M_2}\sum_p \frac{\log p}{\log(m/\pi)}\widehat{\phi}\left(2\frac{\log p}{\log(m/\pi)}\right)p^{-1}\sum_{\chi\in\mathcal{F}}[\chi^2(p)+\bar{\chi}^2(p)]$$

Characters Sums:

$$\sum_{l_i=1}^{m_i-2} \chi_{l_i}(p) = \begin{cases} m_i - 1 - 1 & p \equiv 1(m_i) \\ -1 & \text{otherwise} \end{cases}$$

Define

$$\delta_{m_i}(p, 1) = \begin{cases} 1 & p \equiv 1(m_i) \\ 0 & \text{otherwise} \end{cases}$$

Then

$$\begin{aligned} \sum_{\chi \in \mathcal{F}} \chi(p) &= \sum_{l_1=1}^{m_1-2} \cdots \sum_{l_r=1}^{m_r-2} \chi_{l_1}(p) \cdots \chi_{l_r}(p) \\ &= \prod_{i=1}^{r} \sum_{l_i=1}^{m_i-2} \chi_{l_i}(p) \\ &= \prod_{i=1}^{r} \Bigg(-1 + (m_i - 1)\delta_{m_i}(p, 1) \Bigg). \end{aligned}$$

Expansion Preliminaries:

$k(s)$ is an s-tuple $(k_1, k_2, \ldots, k_s)$ with $k_1 < k_2 < \cdots < k_s$.

This is just a subset of $(1, 2, \ldots, r)$, 2^r possible choices for $k(s)$.

$$\delta_{k(s)}(p,1) = \prod_{i=1}^{s} \delta_{m_{k_i}}(p,1).$$

If $s = 0$ we define $\delta_{k(0)}(p,1) = 1 \; \forall p$.

Then

$$\begin{aligned} & \prod_{i=1}^{r} \Big(-1 + (m_i - 1)\delta_{m_i}(p,1) \Big) \\ = \; & \sum_{s=0}^{r} \sum_{k(s)} (-1)^{r-s} \delta_{k(s)}(p,1) \prod_{i=1}^{s} (m_{k_i} - 1) \end{aligned}$$

First Sum:

$$\ll \sum_{p}^{m^\sigma} p^{-\frac{1}{2}} \frac{1}{M_2} \Big(1 + \sum_{s=1}^{r} \sum_{k(s)} \delta_{k(s)}(p,1) \prod_{i=1}^{s} (m_{k_i} - 1) \Big).$$

As $m/M_2 \le 3^r$, $s = 0$ sum contributes

$$S_{1,0} = \frac{1}{M_2} \sum_{p}^{m^\sigma} p^{-\frac{1}{2}} \ll 3^r m^{\frac{1}{2}\sigma - 1},$$

hence negligible for $\sigma < 2$. Now we study

$$\begin{aligned} S_{1,k(s)} &= \frac{1}{M_2} \prod_{i=1}^{s} (m_{k_i} - 1) \sum_{p}^{m^\sigma} p^{-\frac{1}{2}} \delta_{k(s)}(p,1) \\ &\ll \frac{1}{M_2} \prod_{i=1}^{s} (m_{k_i} - 1) \sum_{n \equiv 1 (m_{k(s)})}^{m^\sigma} n^{-\frac{1}{2}} \\ &\ll \frac{1}{M_2} \prod_{i=1}^{s} (m_{k_i} - 1) \frac{1}{\prod_{i=1}^{s} (m_{k_i})} \sum_{n}^{m^\sigma} n^{-\frac{1}{2}} \\ &\ll 3^r m^{\frac{1}{2}\sigma - 1}. \end{aligned}$$

First Sum (cont):

There are 2^r choices, yielding

$$S_1 \ll 6^r m^{\frac{1}{2}\sigma - 1},$$

which is negligible as m goes to infinity for fixed r if $\sigma < 2$.

Cannot let r go to infinity.

If m is the product of the first r primes,

$$\begin{aligned} \log m &= \sum_{k=1}^{r} \log p_k \\ &= \sum_{p \le r} \log p \approx r \end{aligned}$$

Therefore

$$6^r \approx m^{\log 6} \approx m^{1.79}.$$

Second Sum Expansions:

$$\sum_{l_i=1}^{m_i-2} \chi_{l_i}^2(p) \;=\; \begin{cases} m_i - 1 - 1 & p \equiv \pm 1 (m_i) \\ -1 & \text{otherwise} \end{cases}$$

$$\begin{aligned} & \sum_{\chi \in \mathcal{F}} \chi^2(p) \\ = & \sum_{l_1=1}^{m_1-2} \cdots \sum_{l_r=1}^{m_r-2} \chi_{l_1}^2(p) \cdots \chi_{l_r}^2(p) \\ = & \prod_{i=1}^{r} \sum_{l_i=1}^{m_i-2} \chi_{l_i}^2(p) \\ = & \prod_{i=1}^{r} \Big(-1 + (m_i - 1)\delta_{m_i}(p, 1) + (m_i - 1)\delta_{m_i}(p, -1) \Big) \end{aligned}$$

Second Sum Bounds:

Handle similarly as before. Say

$$\begin{aligned} p &\equiv \quad 1 \text{ mod } m_{k_1}, \dots, m_{k_a} \\ p &\equiv -1 \text{ mod } m_{k_{a+1}}, \dots, m_{k_b} \end{aligned}$$

How small can p be?

$+1$ congruences imply $p \geq m_{k_1} \cdots m_{k_a} + 1$.

-1 congruences imply $p \geq m_{k_{a+1}} \cdots m_{k_b} - 1$.

Since the product of these two lower bounds is greater than $\prod_{i=1}^{b}(m_{k_i} - 1)$, at least one must be greater than $\left(\prod_{i=1}^{b}(m_{k_i} - 1)\right)^{\frac{1}{2}}$.

There are 3^r pairs, yielding

$$\text{Second Sum} = \sum_{s=0}^{r} \sum_{k(s)} \sum_{j(s)} S_{2,k(s),j(s)} \ll 9^r m^{-\frac{1}{2}}.$$

Summary:

Agrees with Unitary for $\sigma < 2$.

We proved:

Lemma:

- m square-free odd integer with $r = r(m)$ factors;
- $m = \prod_{i=1}^{r} m_i$;
- $M_2 = \prod_{i=1}^{r}(m_i - 2)$.

Consider the family $\mathcal{F}_m$ of primitive characters mod m. Then

$$\begin{aligned} \text{First Sum} &\ll \frac{1}{M_2} 2^r m^{\frac{1}{2}\sigma} \\ \text{Second Sum} &\ll \frac{1}{M_2} 3^r m^{\frac{1}{2}}. \end{aligned}$$

Dirichlet Characters: $m \in [N, 2N]$ Square-free

$\mathcal{F}_N$ all primitive characters with conductor odd square-free integer in $[N, 2N]$.

At least $N/\log^2 N$ primes in the interval.

At least $N \cdot \frac{N}{\log^2 N} = N^2 \log^{-2} N$ primitive characters:

$$M \;\geq\; N^2 \log^{-2} N \quad \Rightarrow \quad \frac{1}{M} \;\leq\; \frac{\log^2 N}{N^2}.$$

Bounds

$$S_{1,m} \ll \frac{1}{M} 2^{r(m)} m^{\frac{1}{2}\sigma}$$
$$S_{2,m} \ll \frac{1}{M} 3^{r(m)} m^{\frac{1}{2}}.$$

$2^{r(m)} = \tau(m)$, the number of divisors of m, and $3^{r(m)} \leq \tau^2(m)$.

While it is possible to prove

$$\sum_{n \leq x} \tau^l(n) \ll x(\log x)^{2^l - 1}$$

the crude bound

$$\tau(n) \leq c(\epsilon) n^{\epsilon}$$

yields the same region of convergence.

First Sum Bound

$$\begin{aligned}
S_1 &= \sum_{\substack{m=N \\ m \ squarefree}}^{2N} S_{1,m} \\
&\ll \sum_{m=N}^{2N} \frac{1}{M} 2^{r(m)} m^{\frac{1}{2}\sigma} \\
&\ll \frac{1}{M} N^{\frac{1}{2}\sigma} \sum_{m=N}^{2N} \tau(m) \\
&\ll \frac{1}{M} N^{\frac{1}{2}\sigma} c(\epsilon) N^{1+\epsilon} \\
&\ll \frac{\log^2 N}{N^2} N^{\frac{1}{2}\sigma} c(\epsilon) N^{1+\epsilon} \\
&\ll c(\epsilon) N^{\frac{1}{2}\sigma+\epsilon-1} \log^2 N.
\end{aligned}$$

No contribution if $\sigma < 2$.

Second sum handled similarly.

Appendix Two: Sketch of Proof for Elliptic Curve Families

We give a quick sketch of the main ingredients. The greatest difficulty is the oscillatory behavior of the conductors. Localizing them to $\log N^r + O(1)$ is too crude – the $O(1)$ factor is enough to ruin the results.

Sieving

$$\sum_{\substack{t=N \\ D(t)\text{sqfree}}}^{2N} S(t) = \sum_{d=1}^{N^{k/2}} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2) \\ t\in[N,2N]}} S(t)$$

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

Handle first by progressions.

Handle second by Cauchy-Schwartz:
The number of t in the second sum (by Sq-Free Sieve Conj) is $o(N)$:

Sieving (cont)

$$\sum_{d=1}^{\log^l N} \mu(d) \sum_{\substack{D(t)\equiv 0(d^2) \\ t\in[N,2N]}} S(t)$$

$t_i(d)$ roots of $D(t) \equiv 0 \bmod d^2$.

$t_i(d), t_i(d) + d^2, \ldots, t_i(d) + \left[\frac{N}{d^2}\right] d^2$.

If $(d, p_1 p_2) = 1$, go through complete set of residue classes $\frac{N/d^2}{p_1 p_2}$ times.

Partial Summation

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

Applying Partial Summation

$$S(d,i,r,p) = \sum_{t'=0}^{[N/d^2]} \widetilde{a}^r_{d,i,p}(t') G_{d,i,p}(t')$$

$$= \left(\frac{[N/d^2]}{p} A_{r,\mathcal{F}}(p) + O\left(p^R\right) \right) G_{d,i,p}([N/d^2])$$

$$- \sum_{u=0}^{[N/d^2]-1} \left(\frac{u}{p} A_{r,\mathcal{F}}(p) + O\left(p^R\right) \right) \left(G_{d,i,p}(u) - G_{d,i,p}(u+1) \right)$$

Difficult Piece: Fourth Sum I

$$\sum_{u=0}^{[N/d^2]-1} O(P^R)\Big(G_{d,i,P}(u) - G_{d,i,P}(u+1)\Big)$$

Taylor $G_{d,i,P}(u) - G_{d,i,P}(u+1)$ gives $P^R \frac{N}{d^2} \frac{1}{P^r \log N}$.

$\frac{1}{|\mathcal{F}|}\sum_{i,d}$ gives $O(\frac{P^R}{P^r \log N})$.

Problem is in summing over the primes, as we no longer have $\frac{1}{|\mathcal{F}|}$.

Fourth Sum: II

If exactly one of the r_j's is non-zero, then

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

If conductors monotone, for fixed i, d and p, small independent of N (bounded variation).

If two of the r_j's are non-zero:

$$\begin{aligned} |a_1a_2 - b_1b_2| &= |a_1a_2 - b_1a_2 + b_1a_2 - b_1b_2| \\ &\le |a_1a_2 - b_1a_2| + |b_1a_2 - b_1b_2| \\ &= |a_2| \cdot |a_1 - b_1| + |b_1| \cdot |a_2 - b_2| \end{aligned}$$

Handling the Conductors: I

$$
\begin{aligned}
y^2 + a_1(t)xy + a_3(t)y &= x^3 + a_2(t)x^2 + a_4(t)x + a_6(t) \\
C(t) &= \prod_{p|\Delta(t)} p^{f_p(t)} \\
D_1(t) &= \text{primitive irred poly factors } \Delta(t), c_4(t) \text{ share} \\
D_2(t) &= \text{remaining primitive irred poly factors of } \Delta(t) \\
D(t) &= D_1(t)D_2(t)
\end{aligned}
$$

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

Handling the Conductors: II

$$y^2+a_1(t)xy+a_3(t)y \;=\; x^3+a_2(t)x^2+a_4(t)x+a_6(t)$$

Let P be the product of the bad primes.

Tate's Algorithm gives $f_p(t)$, depend only on $a_i(t)$ mod powers of p.

Apply Tate's Algorithm to E_{t_1}. Get $f_p(t_1)$ for $p|P$. For m large, $p|P$,

$$f_p(\tau) = f_p(P^m t + t_1) = f_p(t_1),$$

and order of p dividing $D(P^m t + t_1)$ is independent of t.

Get integers st $C(\tau) = c_{bad}\frac{D_1^2(\tau)}{c_1}\frac{D_2(\tau)}{c_2}$, $D(\tau)$ sq-free.

Appendix III:
Numerically Approximating Ranks

We give a quick sketch of how to compute values of L-functions at the central point. If the conductor is of size N_E, approximately $\sqrt{N_E} \log N_E$ Fourier coefficients $a_E(p)$ are needed.

Numerically Approximating Ranks: Preliminaries

Cusp form f, level N, weight 2:

$$\begin{aligned} f(-1/Nz) &= -\epsilon N z^2 f(z) \\ f(i/y\sqrt{N}) &= \epsilon y^2 f(iy/\sqrt{N}). \end{aligned}$$

Define

$$\begin{aligned} L(f,s) &= (2\pi)^s \Gamma(s)^{-1} \int_0^{i\infty} (-iz)^s f(z) \frac{dz}{z} \\ \Lambda(f,s) &= (2\pi)^{-s} N^{s/2} \Gamma(s) L(f,s) = \int_0^{\infty} f(iy/\sqrt{N}) y^{s-1} dy. \end{aligned}$$

Get

$$\Lambda(f,s) = \epsilon \Lambda(f, 2-s), \quad \epsilon = \pm 1.$$

To each E corresponds an f, write $\int_0^{\infty} = \int_0^1 + \int_1^{\infty}$ and use transformations.

Algorithm for $L^r(s, E)$: I

$$\begin{aligned}\Lambda(E,s) &= \int_0^\infty f(iy/\sqrt{N})y^{s-1}dy \\ &= \int_0^1 f(iy/\sqrt{N})y^{s-1}dy + \int_1^\infty f(iy/\sqrt{N})y^{s-1}dy \\ &= \int_1^\infty f(iy/\sqrt{N})(y^{s-1} + \epsilon y^{1-s})dy.\end{aligned}$$

Differentiate k times with respect to s:

$$\Lambda^{(k)}(E,s) = \int_1^\infty f(iy/\sqrt{N})(\log y)^k(y^{s-1} + \epsilon(-1)^k y^{1-s})dy.$$

At $s = 1$,

$$\Lambda^{(k)}(E,1) = (1 + \epsilon(-1)^k)\int_1^\infty f(iy/\sqrt{N})(\log\ y)^k dy.$$

Trivially zero for half of k; let r be analytic rank.

Algorithm for $L^r(s, E)$: II

$$\Lambda^{(r)}(E,1) = 2\int_1^\infty f(iy/\sqrt{N})(\log\ y)^r dy$$
$$= 2\sum_{n=1}^\infty a_n \int_1^\infty e^{-2\pi ny/\sqrt{N}}(\log\ y)^r dy.$$

Integrating by parts

$$\Lambda^{(r)}(E,1) = \frac{\sqrt{N}}{\pi}\sum_{n=1}^\infty \frac{a_n}{n}\int_1^\infty e^{-2\pi ny/\sqrt{N}}(\log\ y)^{r-1}\frac{dy}{y}.$$

We obtain

$$L^{(r)}(E,1) = 2r!\sum_{n=1}^\infty \frac{a_n}{n} G_r\left(\frac{2\pi n}{\sqrt{N}}\right),$$

where

$$G_r(x) = \frac{1}{(r-1)!}\int_1^\infty e^{-xy}(\log y)^{r-1}\frac{dy}{y}.$$

Expansion of $G_r(x)$

$$G_r(x) = P_r\left(\log\frac{1}{x}\right) + \sum_{n=1}^{\infty} \frac{(-1)^{n-r}}{n^r \cdot n!} x^n$$

$P_r(t)$ is a polynomial of degree r, $P_r(t) = Q_r(t - \gamma)$.

$$\begin{aligned}
Q_1(t) &= t; \\
Q_2(t) &= \frac{1}{2}t^2 + \frac{\pi^2}{12}; \\
Q_3(t) &= \frac{1}{6}t^3 + \frac{\pi^2}{12}t - \frac{\zeta(3)}{3}; \\
Q_4(t) &= \frac{1}{24}t^4 + \frac{\pi^2}{24}t^2 - \frac{\zeta(3)}{3}t + \frac{\pi^4}{160}; \\
Q_5(t) &= \frac{1}{120}t^5 + \frac{\pi^2}{72}t^3 - \frac{\zeta(3)}{6}t^2 + \frac{\pi^4}{160}t - \frac{\zeta(5)}{5} - \frac{\zeta(3)\pi^2}{36}.
\end{aligned}$$

For $r = 0$,

$$\Lambda(E,1) = \frac{\sqrt{N}}{\pi} \sum_{n=1}^{\infty} \frac{a_n}{n}\, e^{-2\pi n y/\sqrt{N}}.$$

Need about $\sqrt{N}$ or $\sqrt{N}\log N$ terms.

Bibliography

[BEW] B. Berndt, R. Evans and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. **21**, Wiley-Interscience Publications, John Wiley & Sons, Inc., New York, 1998.

[Bi] B. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43**, 1968, $57 - 60$.

[BS] B. Birch and N. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology **5**, 1966, $295 - 299$.

[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* $\mathbf{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14**, no. 4, 2001, $843 - 939$.

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

[BHB3] A. Brumer and R. Heath-Brown, *The average rank of elliptic curves III*, preprint.

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

[BM] A. Brumer and O. McGuinness, *The behaviour of the Mordell-Weil group of elliptic curves*, Bull. AMS **23**, 1991, $375 - 382$.

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

[Cr] Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

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

[Fe1] S. Fermigier, *Zéros des fonctions* L *de courbes elliptiques*, Exper. Math. **1**, 1992, $167 - 173$.

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

[FP] E. Fouvrey and J. Pomykala, *Rang des courbes elliptiques et sommes d'exponentelles*, Monat. Math. **116**, 1993, $111-125$.

[GM] F. Gouvéa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4**, 1991, $45-65$.

[Go] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory (Proc. Conf. in Carbondale, 1979), Lecture Notes in Math. **751**, Springer-Verlag, 1979, $108-118$.

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

[Hej] D. Hejhal, *On the Triple Correlation of the Zeroes of the Zeta Function*, IMRN, 293-302, (1994).

[He] H. Helfgott, *On the distribution of root numbers in families of elliptic curves*, preprint.

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

[HuRu] C. Hughes and Z. Rudnick, *Mock Gaussian behaviour for linear statistics of classical compact groups*, J. Phys. A **36**, (2003) 2919–2932.

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

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

[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, $1-26$.

[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, $429-436$.

[Mai] L. Mai, *The analytic rank of a family of elliptic curves*, Canadian Journal of Mathematics **45**, 1993, $847-862$.

[Mes1] J. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Mathematica **58**, 1986, $209-232$.

[Mes2] J. Mestre, *Courbes elliptiques de rang $\geq$ 11 sur $\boldsymbol{Q}(t)$*, C. R. Acad. Sci. Paris, ser. 1, **313**, 1991, $139 - 142$.

[Mes3] J. Mestre, *Courbes elliptiques de rang $\geq$ 12 sur $\boldsymbol{Q}(t)$*, C. R. Acad. Sci. Paris, ser. 1, **313**, 1991, $171 - 174$.

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

[Mil1] 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.pdf.

[Mil2] S. J. Miller, 1- *and* 2-*Level Densities for Families of Elliptic Curves: Evidence for the Underlying Group Symmetries*, Compositio Mathematica, Volume 140, 4, 952-992.

[Mil3] S. J. Miller, *Density functions for families of Dirichlet characters*, preprint.

[Mor] Mordell, *Diophantine Equations*, Academic Press, New York, 1969.

[Na1] K. Nagao, *On the rank of elliptic curve $y^2 = x^3 - kx$*, Kobe J. Math. **11**, 1994, $205 - 210$.

[Na2] K. Nagao, *Construction of high-rank elliptic curves*, Kobe J. Math. **11**, 1994, $211 - 219$.

[Na3] K. Nagao, $\mathbb{Q}(t)$-*rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. **92**, 1997, $13 - 32$.

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

[Ro] D. Rohrlich, *Variation of the root number in families of elliptic curves*, Compos. Math. **87**, 1993, $119 - 151$.

[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, $269 - 322$.

[Sh] T. Shioda, *Construction of elliptic curves with high-rank via the invariants of the Weyl groups*, J. Math. Soc. Japan **43**, 1991, $673 - 719$.

[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, $227 - 236$.

[St1] N. Stephens, *A corollary to a conjecture of Birch and Swinnerton-Dyer*, J. London Math. Soc. **43**, 1968, $146 - 148$.

[St2] N. Stephens, *The diophantine equation $X^3 + Y^3 = DZ^3$ and the conjectures of Birch and Swinnerton-Dyer*, J. reine angew. Math. **231**, 1968, $16 - 162$.

[ST] C. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, Journal of the American Mathematical Society **40**, number 4, 1995.

[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, $371 - 384$.

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