From the Manhattan Project to Elliptic Curves

Steven J Miller
Dept of Math/Stats, Williams College

sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu
http://www.williams.edu/Mathematics/sjmiller

SUMS: Brown University, March 18, 2017

Introduction

Goals

- Determine correct scale and statistics to study eigenvalues and zeros of L-functions.
- See similar behavior in different systems.
- Discuss the tools and techniques needed to prove the results.

Fundamental Problem: Spacing Between Events

General Formulation: Studying system, observe values at $t_1, t_2, t_3, \dots$.

Question: What rules govern the spacings between the t_i?

Fundamental Problem: Spacing Between Events

General Formulation: Studying system, observe values at $t_1, t_2, t_3, \dots$.

Question: What rules govern the spacings between the t_i?

Examples: Spacings between

- Energy Levels of Nuclei.
- Eigenvalues of Matrices.
- Zeros of L-functions.
- Summands in Zeckendorf Decompositions.
- Primes.
- $n^k \alpha \bmod 1$.

Fundamental Problem: Spacing Between Events

General Formulation: Studying system, observe values at $t_1, t_2, t_3, \dots$.

Question: What rules govern the spacings between the t_i?

Examples: Spacings between

- Energy Levels of Nuclei.
- Eigenvalues of Matrices.
- Zeros of *L*-functions.
- Summands in Zeckendorf Decompositions.
- Primes.
- $n^k\alpha \bmod 1$.

Sketch of proofs

In studying many statistics, often three key steps:

1. Determine correct scale for events.
2. Develop an explicit formula relating what we want to study to something we understand.
3. Use an averaging formula to analyze the quantities above.

It is not always trivial to figure out what is the correct statistic to study!

Classical Random Matrix Theory

With Olivia Beckwith, Leo Goldmakher, Chris Hammond, Steven Jackson, Cap Khoury, Murat Koloğlu, Gene Kopp, Victor Luo, Adam Massey, Eve Ninsuwan, Vincent Pham, Karen Shen, Jon Sinsheimer, Fred Strauch, Nicholas Triantafillou, Wentao Xiong

Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem intractable.

Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem intractable.

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

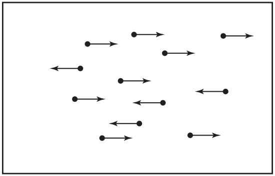
Get some info by shooting high-energy neutrons into nucleus, see what comes out.

Fundamental Equation:

$$H\psi_n = E_n\psi_n$$

H : matrix, entries depend on system
E_n : energy levels
ψ_n : energy eigenfunctions

Origins of Random Matrix Theory



- 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 (real Symmetric $A = A^T$, complex Hermitian $\overline{A}^T = A$).

Random Matrix Ensembles

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

Fix p, define

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

This means

$$\text{Prob}\left(A : a_{ij} \in [\alpha_{ij}, \beta_{ij}]\right) = \prod_{1 \le i \le j \le N} \int_{x_{ij}=\alpha_{ij}}^{\beta_{ij}} p(x_{ij}) dx_{ij}.$$

Want to understand eigenvalues of A.

Eigenvalue Distribution

$\delta(x - x_0)$ is a unit point mass at x_0:
$\int f(x)\delta(x - x_0)dx = f(x_0)$.

Eigenvalue Distribution

$\delta(x - x_0)$ is a unit point mass at x_0:
$\int f(x)\delta(x - x_0)dx = f(x_0)$.

To each A, attach a probability measure:

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

Eigenvalue Distribution

$\delta(x - x_0)$ is a unit point mass at x_0:
$\int f(x)\delta(x - x_0)dx = f(x_0)$.

To each A, attach a probability measure:

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

$$\int_a^b \mu_{A,N}(x)dx = \frac{\#\left\{\lambda_i : \frac{\lambda_i(A)}{2\sqrt{N}} \in [a,b]\right\}}{N}$$

Eigenvalue Distribution

$\delta(x - x_0)$ is a unit point mass at x_0:
$\int f(x)\delta(x - x_0)dx = f(x_0)$.

To each A, attach a probability measure:

$$\begin{aligned}
\mu_{A,N}(x) &= \frac{1}{N}\sum_{i=1}^{N}\delta\left(x - \frac{\lambda_i(A)}{2\sqrt{N}}\right) \\
\int_a^b \mu_{A,N}(x)dx &= \frac{\#\left\{\lambda_i : \frac{\lambda_i(A)}{2\sqrt{N}} \in [a,b]\right\}}{N} \\
\text{k}^{\text{th}}\text{ moment} &= \frac{\sum_{i=1}^{N}\lambda_i(A)^k}{2^k N^{\frac{k}{2}+1}} = \frac{\mathrm{Trace}(A^k)}{2^k N^{\frac{k}{2}+1}}.
\end{aligned}$$

Wigner's Semi-Circle Law

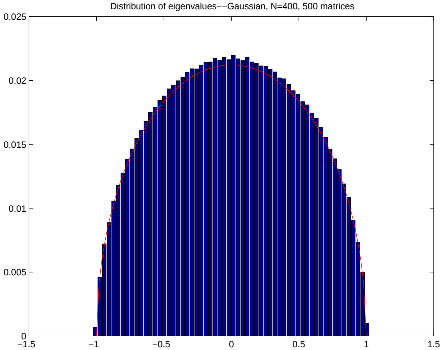
Wigner's Semi-Circle Law

$N \times N$ real symmetric matrices, entries i.i.d.r.v. from a fixed $p(x)$ with mean 0, variance 1, and other moments finite. Then for almost all A, as $N \to \infty$

$$\mu_{A,N}(x) \longrightarrow \begin{cases} \frac{2}{\pi}\sqrt{1-x^2} & \text{if } |x| \leq 1 \\ 0 & \text{otherwise.} \end{cases}$$

See Eugene Wigner's *The Unreasonable Effectiveness of Mathematics in the Natural Sciences* in Communications in Pure and Applied Mathematics, vol. 13, No. I (February 1960), online at `http://www.dartmouth.edu/~matc/MathDrama/reading/Wigner.html`.

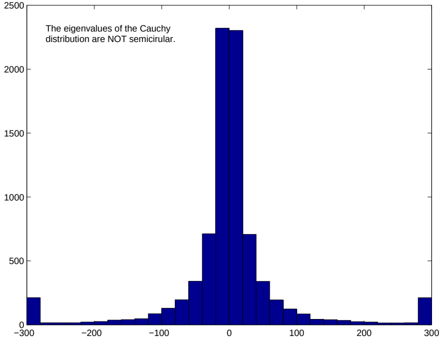
Numerical examples



500 Matrices: Gaussian 400×400

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

Numerical examples



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

I. Zakharevich, *A generalization of Wigner's law*, Comm. Math. Phys. **268** (2006), no. 2, 403–414. http://web.williams.edu/Mathematics/sjmiller/public_html/book/papers/innaz.pdf

SKETCH OF PROOF: Eigenvalue Trace Lemma

Want to understand the eigenvalues of A, but choose the matrix elements randomly and independently.

Eigenvalue Trace Lemma

Let A be an $N \times N$ matrix with eigenvalues $\lambda_i(A)$. Then

$$\mathrm{Trace}(A^k) \;=\; \sum_{n=1}^{N} \lambda_i(A)^k,$$

where

$$\mathrm{Trace}(A^k) \;=\; \sum_{i_1=1}^{N} \cdots \sum_{i_k=1}^{N} a_{i_1 i_2} a_{i_2 i_3} \cdots a_{i_N i_1}.$$

SKETCH OF PROOF: Correct Scale

$$\mathrm{Trace}(A^2) \;=\; \sum_{i=1}^{N} \lambda_i(A)^2.$$

By the Central Limit Theorem:

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

$$\sum_{i=1}^{N} \lambda_i(A)^2 \;\sim\; N^2$$

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

SKETCH OF PROOF: Averaging Formula

Recall k-th moment of $\mu_{A,N}(x)$ is $\mathrm{Trace}(A^k)/2^k N^{k/2+1}$.

Average k-th moment is

$$\int \cdots \int \frac{\mathrm{Trace}(A^k)}{2^k N^{k/2+1}} \prod_{i \leq j} p(a_{ij}) da_{ij}.$$

Proof by method of moments: Two steps

- Show average of k-th moments converge to moments of semi-circle as $N \to \infty$;
- Control variance (show it tends to zero as $N \to \infty$).

SKETCH OF PROOF: Averaging Formula for Second Moment

Substituting into expansion gives

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

Integration factors as

$$\int_{a_{ij}=-\infty}^{\infty}a_{ij}^2p(a_{ij})da_{ij}\quad\cdot\prod_{\substack{(k,l)\neq(i,j)\\k<l}}\int_{a_{kl}=-\infty}^{\infty}p(a_{kl})da_{kl}\;=\;1.$$

Higher moments involve more advanced combinatorics (Catalan numbers).

SKETCH OF PROOF: Averaging Formula for Higher Moments

Higher moments involve more advanced combinatorics (Catalan numbers).

$$\frac{1}{2^k N^{k/2+1}} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \sum_{i_1=1}^{N} \cdots \sum_{i_k=1}^{N} a_{i_1 i_2} \cdots a_{i_k i_1} \cdot \prod_{i \leq j} p(a_{ij}) da_{ij}.$$

Main contribution when the $a_{i_\ell i_{\ell+1}}$'s matched in pairs, not all matchings contribute equally (if did would get a Gaussian and not a semi-circle; this is seen in Real Symmetric Palindromic Toeplitz matrices).

Distribution of eigenvalues of real symmetric palindromic Toeplitz matrices and circulant matrices (with Adam Massey and John Sinsheimer), Journal of Theoretical Probability **20** (2007), no. 3, 637–662. http://arxiv.org/abs/math/0512146

GOE Conjecture

GOE Conjecture:

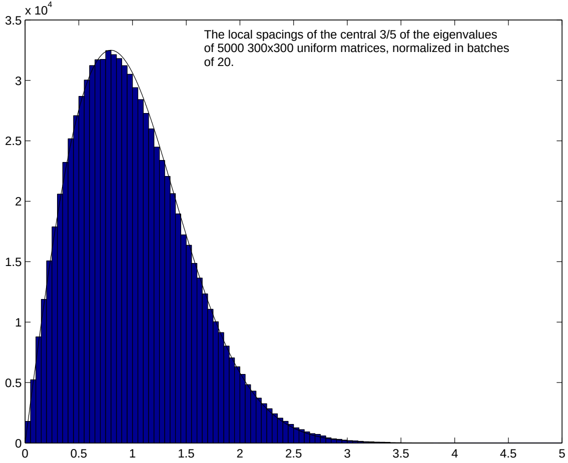
As $N \to \infty$, the probability density of the spacing b/w consecutive normalized eigenvalues approaches a limit independent of p.

Until recently only known if p is a Gaussian.

$$\text{GOE}(x) \approx \frac{\pi}{2} x e^{-\pi x^2/4}.$$

Numerical Experiment: Uniform Distribution

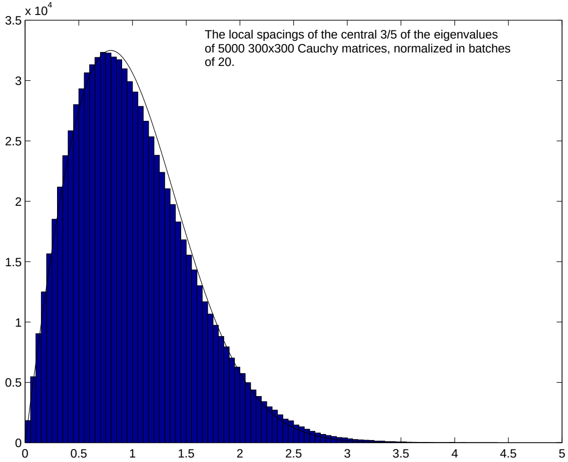
Let $p(x) = \frac{1}{2}$ for $|x| \leq 1$.



5000: 300×300 uniform on $[-1, 1]$

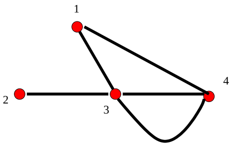
Cauchy Distribution

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



5000: 300×300 Cauchy

Random Graphs



Degree of a vertex $=$ number of edges leaving the vertex.
Adjacency matrix: a_{ij} $=$ number edges b/w Vertex i and Vertex j.

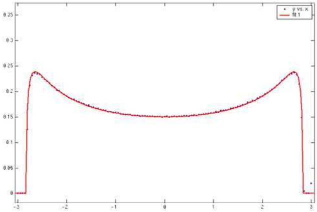
$$A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{pmatrix}$$

These are Real Symmetric Matrices.

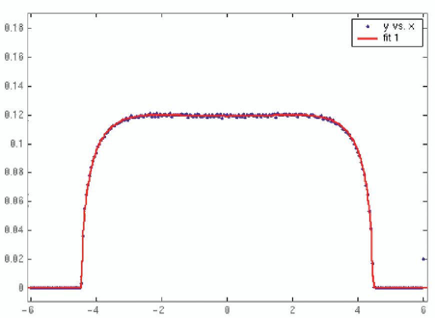
McKay's Law (Kesten Measure) with $d = 3$

Density of Eigenvalues for d-regular graphs

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



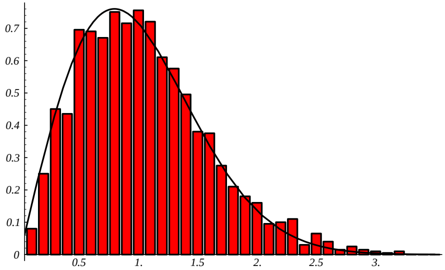
McKay's Law (Kesten Measure) with $d = 6$



Fat Thin: fat enough to average, thin enough to get something different than semi-circle (though as $d \to \infty$ recover semi-circle).

3-Regular Graph with 2000 Vertices: Comparison with the GOE

Spacings between eigenvalues of 3-regular graphs and the GOE:



Block Circulant Ensemble

With Murat Koloğlu, Gene Kopp, Fred Strauch and Wentao Xiong.

The Ensemble of m-Block Circulant Matrices

Symmetric matrices periodic with period m on wrapped diagonals, i.e., symmetric block circulant matrices.

8-by-8 real symmetric 2-block circulant matrix:

$$\left(\begin{array}{cc|cc|cc|cc} c_0 & c_1 & c_2 & c_3 & c_4 & d_3 & c_2 & d_1 \\ c_1 & d_0 & d_1 & d_2 & d_3 & d_4 & c_3 & d_2 \\ \hline c_2 & d_1 & c_0 & c_1 & c_2 & c_3 & c_4 & d_3 \\ c_3 & d_2 & c_1 & d_0 & d_1 & d_2 & d_3 & d_4 \\ \hline c_4 & d_3 & c_2 & d_1 & c_0 & c_1 & c_2 & c_3 \\ d_3 & d_4 & c_3 & d_2 & c_1 & d_0 & d_1 & d_2 \\ \hline c_2 & c_3 & c_4 & d_3 & c_2 & d_1 & c_0 & c_1 \\ d_1 & d_2 & d_3 & d_4 & c_3 & d_2 & c_1 & d_0 \end{array}\right).$$

Choose distinct entries i.i.d.r.v.

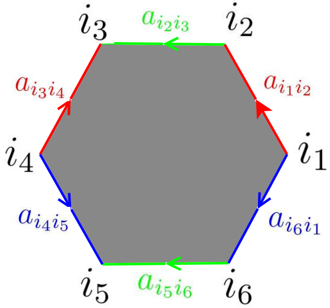
Oriented Matchings and Dualization

Compute moments of eigenvalue distribution (as m stays fixed and $N \to \infty$) using the combinatorics of pairings. Rewrite:

$$\begin{aligned} M_n(N) &= \frac{1}{N^{\frac{n}{2}+1}} \sum_{1 \le i_1, \dots, i_n \le N} \mathbb{E}(a_{i_1 i_2} a_{i_2 i_3} \cdots a_{i_n i_1}) \\ &= \frac{1}{N^{\frac{n}{2}+1}} \sum_{\sim} \eta(\sim) m_{d_1(\sim)} \cdots m_{d_l(\sim)}. \end{aligned}$$

where the sum is over oriented matchings on the edges $\{(1,2),(2,3),\dots,(n,1)\}$ of a regular n-gon.

Oriented Matchings and Dualization

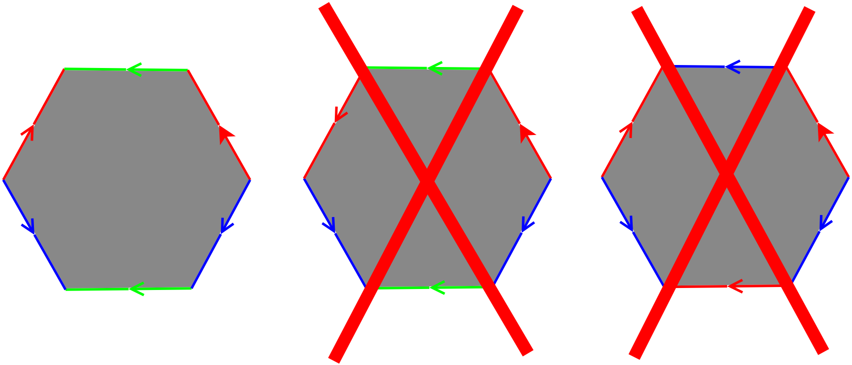


$$\left(\begin{array}{cc|cc|cc|cc}
c_0 & c_1 & c_2 & c_3 & c_4 & d_3 & c_2 & d_1 \\
c_1 & d_0 & d_1 & d_2 & d_3 & d_4 & c_3 & d_2 \\
\hline
c_2 & d_1 & c_0 & c_1 & c_2 & c_3 & c_4 & d_3 \\
c_3 & d_2 & c_1 & d_0 & d_1 & d_2 & d_3 & d_4 \\
\hline
c_4 & d_3 & c_2 & d_1 & c_0 & c_1 & c_2 & c_3 \\
d_3 & d_4 & c_3 & d_2 & c_1 & d_0 & d_1 & d_2 \\
\hline
c_2 & c_3 & c_4 & d_3 & c_2 & d_1 & c_0 & c_1 \\
d_1 & d_2 & d_3 & d_4 & c_3 & d_2 & c_1 & d_0
\end{array}\right)$$

Figure: An oriented matching in the expansion for $M_n(N) = M_6(8)$.

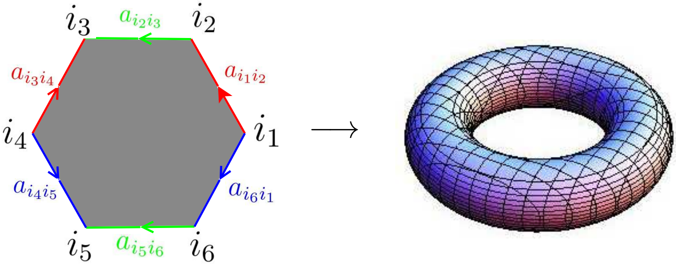
Contributing Terms

As $N \to \infty$, the only terms that contribute to this sum are those in which the entries are matched in pairs and with opposite orientation.



Only Topology Matters

Think of pairings as topological identifications; the contributing ones give rise to orientable surfaces.



Contribution from such a pairing is m^{-2g}, where g is the genus (number of holes) of the surface. Proof: combinatorial argument involving Euler characteristic.

Computing the Even Moments

Theorem: Even Moment Formula

$$M_{2k} = \sum_{g=0}^{\lfloor k/2 \rfloor} \varepsilon_g(k) m^{-2g} + O_k\left(\frac{1}{N}\right),$$

with $\varepsilon_g(k)$ the number of pairings of the edges of a $(2k)$-gon giving rise to a genus g surface.

J. Harer and D. Zagier (1986) gave generating functions for the $\varepsilon_g(k)$.

Harer and Zagier

$$\sum_{g=0}^{\lfloor k/2 \rfloor} \varepsilon_g(k) r^{k+1-2g} \;=\; (2k-1)!!\, c(k,r)$$

where

$$1 + 2\sum_{k=0}^{\infty} c(k,r) x^{k+1} \;=\; \left(\frac{1+x}{1-x}\right)^r.$$

Thus, we write

$$M_{2k} \;=\; m^{-(k+1)} (2k-1)!!\, c(k,m).$$

Results

A multiplicative convolution and Cauchy's residue formula yield

Theorem: Koloğlu, Kopp and Miller

Limiting spectral density $f_m(x)$ of the real symmetric m-block circulant ensemble is

$$f_m(x) = \frac{e^{-\frac{mx^2}{2}}}{\sqrt{2\pi m}} \sum_{r=0}^{m} \frac{1}{(2r)!} \sum_{s=0}^{m-r} \binom{m}{r+s+1} \frac{(2r+2s)!}{(r+s)!s!} \left(-\frac{1}{2}\right)^s (mx^2)^r.$$

As $m \to \infty$, $f_m(x)$ approaches the semicircle distribution.

Results (continued)

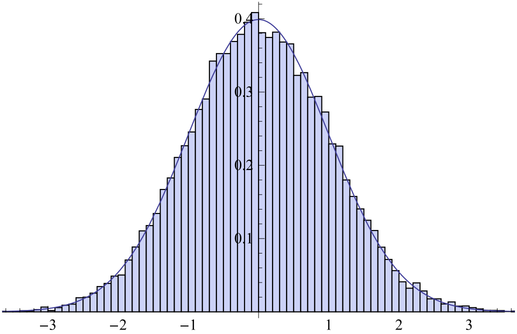


Figure: Plot for f_1 and histogram of eigenvalues of 100 circulant matrices of size 400×400.

Results (continued)

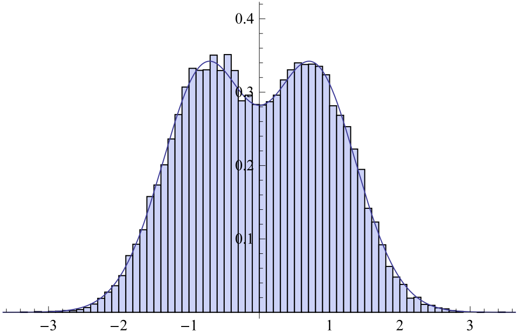


Figure: Plot for f_2 and histogram of eigenvalues of 100 2-block circulant matrices of size 400×400.

Results (continued)

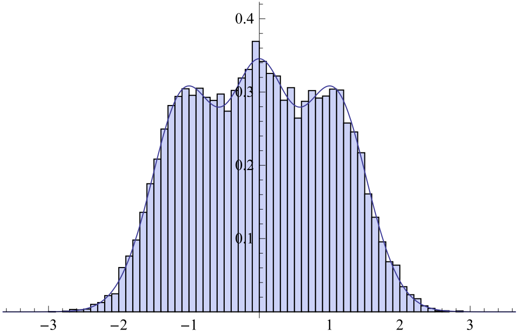


Figure: Plot for f_3 and histogram of eigenvalues of 100 3-block circulant matrices of size 402×402.

Results (continued)

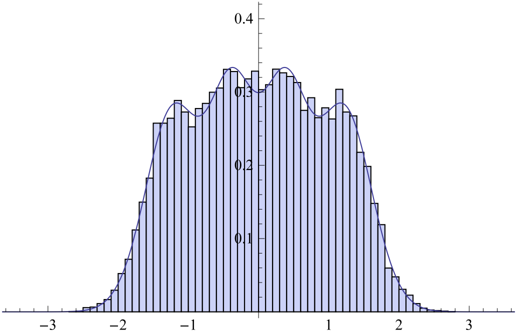


Figure: Plot for f_4 and histogram of eigenvalues of 100 4-block circulant matrices of size 400×400.

Results (continued)

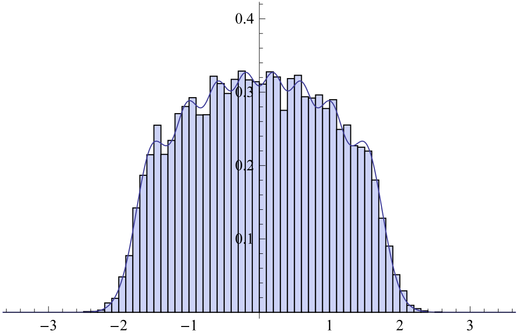


Figure: Plot for f_8 and histogram of eigenvalues of 100 8-block circulant matrices of size 400×400.

Results (continued)

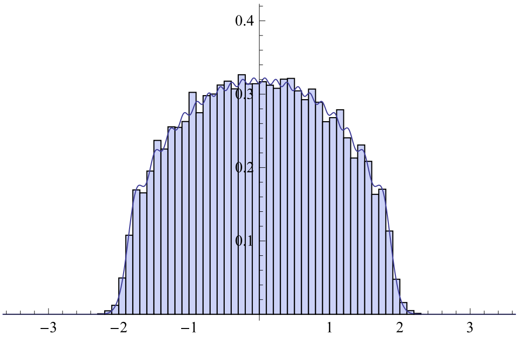


Figure: Plot for f_{20} and histogram of eigenvalues of 100 20-block circulant matrices of size 400×400.

Results (continued)

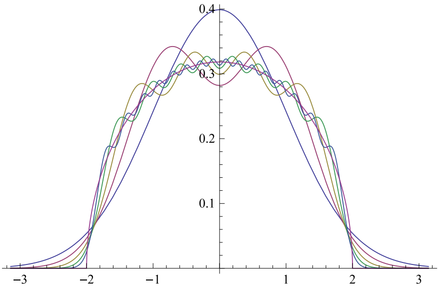


Figure: Plot of convergence to the semi-circle.

The Limiting Spectral Measure for Ensembles of Symmetric Block Circulant Matrices (with Murat Koloğlu, Gene S. Kopp, Frederick W. Strauch and Wentao Xiong), Journal of Theoretical Probability **26** (2013), no. 4, 1020–1060. http://arxiv.org/abs/1008.4812

Bonus: Checkerboard: Definition

Definition

The $N \times N$ (k, w)-checkerboard ensemble is the ensemble of matrices $M = (m_{ij})$ given by

$$m_{ij} = \begin{cases} a_{ij} & \text{if } i \not\equiv j \bmod k \\ w & \text{if } i \equiv j \bmod k \end{cases}$$

where the $a_{ij} = a_{ji}$ are iid with mean 0, variance 1, and finite higher moments, and w is constant.

Bonus: Checkerboard: Example

A $(3, w)$-checkerboard matrix is of the form

$$\begin{pmatrix} w & a_{0,1} & a_{0,2} & w & a_{0,4} & \cdots & a_{0,N-1} \\ a_{1,0} & w & a_{1,2} & a_{1,3} & w & \cdots & a_{1,N-1} \\ a_{2,0} & a_{2,1} & w & a_{2,3} & a_{2,4} & \cdots & w \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{0,N-1} & a_{1,N-1} & w & a_{3,N-1} & a_{4,N-1} & \cdots & w \end{pmatrix}$$

Bonus: Checkerboard: Split Behavior

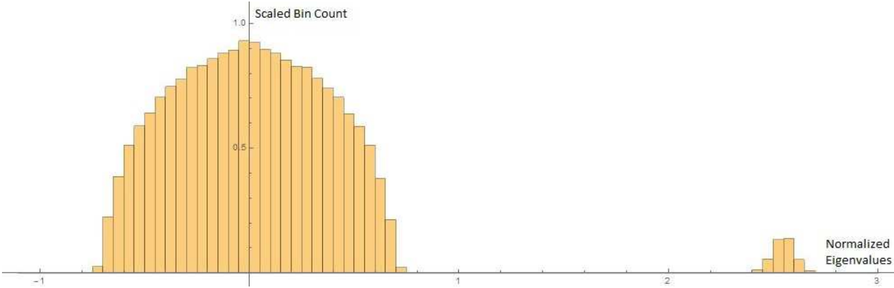


Figure: Histogram of normalized eigenvalues for 500 100×100 2-checkerboard matrices.

Introduction to L-Functions

Riemann Zeta Function

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

Riemann Zeta Function

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

Unique Factorization: $n = p_1^{r_1} \cdots p_m^{r_m}$.

Riemann Zeta Function

$$\zeta(s) \;=\; \sum_{n=1}^{\infty} \frac{1}{n^s} \;=\; \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \mathrm{Re}(s) > 1.$$

Unique Factorization: $n = p_1^{r_1} \cdots p_m^{r_m}$.

$$\begin{aligned} \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \;&=\; \left[1 + \frac{1}{2^s} + \left(\frac{1}{2^s}\right)^2 + \cdots\right]\left[1 + \frac{1}{3^s} + \left(\frac{1}{3^s}\right)^2 + \cdots\right]\cdots \\ &=\; \sum_n \frac{1}{n^s}. \end{aligned}$$

Riemann Zeta Function (cont)

$$\zeta(s) = \sum_n \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \mathrm{Re}(s) > 1$$
$$\pi(x) = \#\{p : p \text{ is prime}, p \le x\}$$

Properties of $\zeta(s)$ and Primes:

Riemann Zeta Function (cont)

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

$$\pi(x) = \#\{p : p \text{ is prime}, p \leq x\}$$

Properties of $\zeta(s)$ and Primes:

- $\lim_{s\to 1^+} \zeta(s) = \infty$, $\pi(x) \to \infty$.

Riemann Zeta Function (cont)

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

$$\pi(x) = \#\{p : p \text{ is prime}, p \le x\}$$

Properties of $\zeta(s)$ and Primes:

- $\lim_{s \to 1^+} \zeta(s) = \infty$, $\pi(x) \to \infty$.
- $\zeta(2) = \frac{\pi^2}{6}$, $\pi(x) \to \infty$.

Riemann Zeta Function

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

Functional Equation:

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

Riemann Hypothesis (RH):

All non-trivial zeros have $\mathrm{Re}(s) = \frac{1}{2}$; can write zeros as $\frac{1}{2} + i\gamma$.

Observation: Spacings b/w zeros appear same as b/w eigenvalues of Complex Hermitian matrices $\overline{A}^T = A$.

General L-functions

$$L(s,f) = \sum_{n=1}^{\infty} \frac{a_f(n)}{n^s} = \prod_{p \text{ prime}} L_p(s,f)^{-1}, \quad \mathrm{Re}(s) > 1.$$

Functional Equation:

$$\Lambda(s,f) = \Lambda_\infty(s,f) L(s,f) = \Lambda(1-s,f).$$

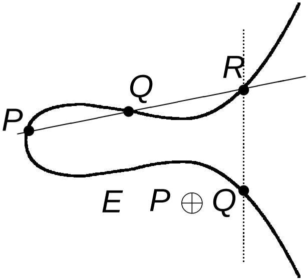
Generalized Riemann Hypothesis (RH):

All non-trivial zeros have $\mathrm{Re}(s) = \frac{1}{2}$; can write zeros as $\frac{1}{2} + i\gamma$.

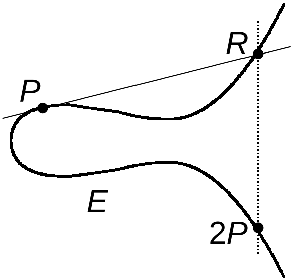
Observation: Spacings b/w zeros appear same as b/w eigenvalues of Complex Hermitian matrices $\overline{A}^T = A$.

Elliptic Curves: Mordell-Weil Group

Elliptic curve $y^2 = x^3 + ax + b$ with rational solutions $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ and connecting line $y = mx + b$.



Addition of distinct points P and Q



Adding a point P to itself

$$E(\mathbb{Q}) \approx E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$$

Elliptic curve L-function

$E: y^2 = x^3 + ax + b$, associate L-function

$$L(s,E) \ = \ \sum_{n=1}^{\infty} \frac{a_E(n)}{n^s} \ = \ \prod_{p \text{ prime}} L_E(p^{-s}),$$

where

$$a_E(p) = p - \#\{(x,y) \in (\mathbb{Z}/p\mathbb{Z})^2 : y^2 \equiv x^3 + ax + b \bmod p\}.$$

Elliptic curve L-function

$E: y^2 = x^3 + ax + b$, associate L-function

$$L(s, E) = \sum_{n=1}^{\infty} \frac{a_E(n)}{n^s} = \prod_{p \text{ prime}} L_E(p^{-s}),$$

where

$$a_E(p) = p - \#\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 : y^2 \equiv x^3 + ax + b \bmod p\}.$$

Birch and Swinnerton-Dyer Conjecture

Rank of group of rational solutions equals order of vanishing of $L(s, E)$ at $s = 1/2$.

Properties of zeros of L-functions

- infinitude of primes, primes in arithmetic progression.
- Chebyshev's bias: $\pi_{3,4}(x) \geq \pi_{1,4}(x)$ 'most' of the time.
- Birch and Swinnerton-Dyer conjecture.
- Goldfeld, Gross-Zagier: bound for $h(D)$ from L-functions with many central point zeros.
- Even better estimates for $h(D)$ if a positive percentage of zeros of $\zeta(s)$ are at most $1/2 - \epsilon$ of the average spacing to the next zero.

Distribution of zeros

- $\zeta(s) \neq 0$ for $\mathfrak{Re}(s) = 1$: $\pi(x)$, $\pi_{a,q}(x)$.
- GRH: error terms.
- GSH: Chebyshev's bias.
- Analytic rank, adjacent spacings: $h(D)$.

Explicit Formula (Contour Integration)

$$-\frac{\zeta'(s)}{\zeta(s)} \;=\; -\frac{d}{ds}\log\zeta(s) = -\frac{d}{ds}\log\prod_p\left(1-p^{-s}\right)^{-1}$$

Explicit Formula (Contour Integration)

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

Explicit Formula (Contour Integration)

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

Contour Integration:

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

Explicit Formula (Contour Integration)

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

Contour Integration:

$$
\int -\frac{\zeta'(s)}{\zeta(s)}\,\phi(s)ds \quad \text{vs} \quad \sum_p \log p \int \phi(s)p^{-s}ds.
$$

Explicit Formula (Contour Integration)

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

Contour Integration (see Fourier Transform arising):

$$
\int -\frac{\zeta'(s)}{\zeta(s)}\phi(s)ds \quad \text{vs} \quad \sum_p \log p \int \phi(s) e^{-\sigma\log p} e^{-it\log p} ds.
$$

Knowledge of zeros gives info on coefficients.

Explicit Formula: Example

Dirichlet *L*-functions: Let ϕ be an even Schwartz function and $L(s, \chi) = \sum_n \chi(n)/n^s$ a Dirichlet *L*-function from a non-trivial character χ with conductor m and zeros $\rho = \frac{1}{2} + i\gamma_\chi$. Then

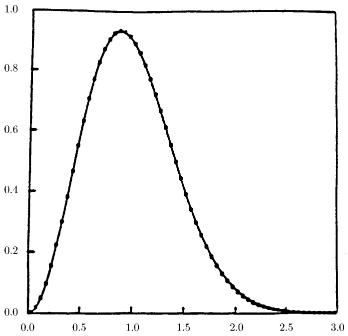
$$\sum_\rho \phi\left(\gamma_\chi \frac{\log(m/\pi)}{2\pi}\right) = \int_{-\infty}^{\infty} \phi(y)dy$$

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

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

Katz-Sarnak
Density Conjectures

Zeros of $\zeta(s)$ vs GUE



70 million spacings b/w adjacent zeros of $\zeta(s)$, starting at the $10^{20\text{th}}$ zero (from Odlyzko).

Measures of Spacings: n-Level Correlations

$\{\alpha_j\}$ increasing sequence, box $B \subset \mathbf{R}^{n-1}$.

n-level correlation

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

(Instead of using a box, can use a smooth test function.)

Measures of Spacings: n-Level Correlations

$\{\alpha_j\}$ increasing sequence, box $B \subset \mathbf{R}^{n-1}$.

1. Normalized spacings of $\zeta(s)$ starting at 10^{20} (Odlyzko).
2. 2 and 3-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 g_i be even Schwartz functions whose Fourier Transform is compactly supported, $L(s,f)$ an L-function with zeros $\frac{1}{2}+\mathrm{i}\gamma_f$ and conductor Q_f:

$$D_{n,f}(g) = \sum_{\substack{j_1,\dots,j_n \\ j_i \neq \pm j_k}} g_1\left(\gamma_{f,j_1}\frac{\log Q_f}{2\pi}\right)\cdots g_n\left(\gamma_{f,j_n}\frac{\log Q_f}{2\pi}\right)$$

- Properties of n-level density:
  - ⋄ Individual zeros contribute in limit
  - ⋄ Most of contribution is from low zeros
  - ⋄ Average over similar L-functions (family)

n-Level Density

n-level density: $\mathcal{F} = \cup \mathcal{F}_N$ a family of L-functions ordered by conductors, g_k an even Schwartz function: $D_{n,\mathcal{F}}(g) =$

$$\lim_{N\to\infty} \frac{1}{|\mathcal{F}_N|} \sum_{f\in\mathcal{F}_N} \sum_{\substack{j_1,\dots,j_n \\ j_i \neq \pm j_k}} g_1\left(\frac{\log Q_f}{2\pi}\gamma_{j_1;f}\right)\cdots g_n\left(\frac{\log Q_f}{2\pi}\gamma_{j_n;f}\right)$$

As $N \to \infty$, n-level density converges to

$$\int g(\vec{x})\rho_{n,\mathcal{G}(\mathcal{F})}(\vec{x})d\vec{x} \quad = \quad \int \widehat{g}(\vec{u})\widehat{\rho}_{n,\mathcal{G}(\mathcal{F})}(\vec{u})d\vec{u}.$$

Conjecture (Katz-Sarnak)

(In the limit) Scaled distribution of zeros near central point agrees with scaled distribution of eigenvalues near 1 of a classical compact group.

1-Level Densities

Let $\mathcal{G}$ be one of the classical compact groups: Unitary, Symplectic, Orthogonal (or SO(even), SO(odd)).
If $\mathrm{supp}(\widehat{g}) \subset (-1, 1)$, 1-level density of $\mathcal{G}$ is

$$\widehat{g}(0) \ - \ c_{\mathcal{G}} \frac{g(0)}{2},$$

where

$$c_{\mathcal{G}} \ = \ \begin{cases} 0 & \mathcal{G} \text{ is Unitary} \\ 1 & \mathcal{G} \text{ is Symplectic} \\ -1 & \mathcal{G} \text{ is Orthogonal.} \end{cases}$$

Identifying the Symmetry Groups

- Often suggested by monodromy group in the function field.
- Tools: Explicit Formula, Summation Formula.
- How to identify symmetry group in general? One possibility is by the signs of the functional equation: **Folklore Conjecture:** If all signs are even and no corresponding family with odd signs, Symplectic symmetry; otherwise SO(even). (False!)

The low lying zeros of a $GL(4)$ *and a* $GL(6)$ *family of L-functions* (with Eduardo Dueñez), Compositio Mathematica **142** (2006), no. 6, 1403–1425.
http://arxiv.org/abs/math/0506462

Explicit Formula

- π: cuspidal automorphic representation on GL_n.
- $Q_\pi > 0$: analytic conductor of $L(s, \pi) = \sum \lambda_\pi(n)/n^s$.
- By GRH the non-trivial zeros are $\frac{1}{2} + i\gamma_{\pi,j}$.
- Satake params: $\{\alpha_{\pi,i}(p)\}_{i=1}^n$; $\lambda_\pi(p^\nu) = \sum_{i=1}^n \alpha_{\pi,i}(p)^\nu$.
- $L(s, \pi) = \sum_n \frac{\lambda_\pi(n)}{n^s} = \prod_p \prod_{i=1}^n (1 - \alpha_{\pi,i}(p)p^{-s})^{-1}$.

$$\sum_j g\left(\gamma_{\pi,j}\frac{\log Q_\pi}{2\pi}\right) = \widehat{g}(0) - 2\sum_{p,\nu} \widehat{g}\left(\frac{\nu \log p}{\log Q_\pi}\right) \frac{\lambda_\pi(p^\nu)\log p}{p^{\nu/2}\log Q_\pi}$$

Some Results: Rankin-Selberg Convolution of Families

Symmetry constant: $c_{\mathcal{L}} = 0$ (resp, 1 or -1) if family $\mathcal{L}$ has unitary (resp, symplectic or orthogonal) symmetry.

Rankin-Selberg convolution: Satake parameters for $\pi_{1,p} \times \pi_{2,p}$ are $\{\alpha_{\pi_1 \times \pi_2}(k)\}_{k=1}^{nm} = \{\alpha_{\pi_1}(i) \cdot \alpha_{\pi_2}(j)\}_{\substack{1 \le i \le n \\ 1 \le j \le m}}$.

Theorem (Dueñez-Miller)

If $\mathcal{F}$ and $\mathcal{G}$ are *nice* families of L-functions, then $c_{\mathcal{F} \times \mathcal{G}} = c_{\mathcal{F}} \cdot c_{\mathcal{G}}$.

Breaks analysis of compound families into simple ones.

The effect of convolving families of L-functions on the underlying group symmetries (with Eduardo Dueñez), Proceedings of the London Mathematical Society, 2009; doi: 10.1112/plms/pdp018. http://arxiv.org/pdf/math/0607688.pdf

1-Level Density

Assuming conductors constant in family $\mathcal{F}$, have to study

$$\begin{aligned}
\nu^{\text{th}}\ \text{moment}: \lambda_f(p^\nu) &= \alpha_{f,1}(p)^\nu + \cdots + \alpha_{f,n}(p)^\nu \\
S_1(\mathcal{F}) &= -2\sum_p \hat{g}\left(\frac{\log p}{\log R}\right)\frac{\log p}{\sqrt{p}\log R}\left[\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}}\lambda_f(p)\right] \\
S_2(\mathcal{F}) &= -2\sum_p \hat{g}\left(2\frac{\log p}{\log R}\right)\frac{\log p}{p\log R}\left[\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}}\lambda_f(p^2)\right]
\end{aligned}$$

The corresponding classical compact group determined by

$$\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}}\lambda_f(p^2) = c_{\mathcal{F}} = \begin{cases} 0 & \text{Unitary} \\ 1 & \text{Symplectic} \\ -1 & \text{Orthogonal.} \end{cases}$$

Takeaways

Very similar to Central Limit Theorem.

- Universal behavior: main term controlled by first two moments of Satake parameters, agrees with RMT.
- First moment zero save for families of elliptic curves.
- Higher moments control convergence and can depend on arithmetic of family.

Correspondences

Similarities between *L*-Functions and Nuclei:

Zeros	$\longleftrightarrow$	Energy Levels
Schwartz test function	$\longrightarrow$	Neutron
Support of test function	$\longleftrightarrow$	Neutron Energy.

Elliptic Curves: First Zero Above Central Point

Eduardo Dueñez, Duc Khim Huynh, Jon P. Keating and Nina Snaith

Theoretical results: $y^2 = x^3 + A(T)x + B(T)$

Theorem: M– '04

For small support, one-param family of rank r over $\mathbb{Q}(T)$:

$$\lim_{N\to\infty} \frac{1}{|\mathcal{F}_N|} \sum_{E_t \in \mathcal{F}_N} \sum_j \varphi\left(\frac{\log C_{E_t}}{2\pi}\gamma_{E_t,j}\right) = \int \varphi(x)\rho_{\mathcal{G}}(x)dx + r\varphi(0)$$

$$\text{where} \quad \mathcal{G} = \begin{cases} \mathrm{SO(odd)} & \text{if half odd} \\ \mathrm{SO(even)} & \text{if all even} \\ \text{weighted average} & \text{otherwise.} \end{cases}$$

Supports Katz-Sarnak, B-SD, and Independent model in limit.

Independent Model:

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

Interesting Families

Let $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$ be a one-parameter family of elliptic curves of rank r over $\mathbb{Q}(T)$.
Natural sub-families:

- Curves of rank r.
- Curves of rank $r + 2$.

Interesting Families

Let $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$ be a one-parameter family of elliptic curves of rank r over $\mathbb{Q}(T)$.
Natural sub-families:

- Curves of rank r.
- Curves of rank $r + 2$.

Question: Does the sub-family of rank $r + 2$ curves in a rank r family behave like the sub-family of rank $r + 2$ curves in a rank $r + 2$ family?

Equivalently, does it matter how one conditions on a curve being rank $r + 2$?

Testing Random Matrix Theory Predictions

Know the right model for large conductors, searching for the correct model for finite conductors.

In the limit must recover the independent model, and want to explain data on:

1. **Excess Rank:** Rank r one-parameter family over $\mathbb{Q}(T)$: observed percentages with rank $\geq r+2$.
2. **First (Normalized) Zero above Central Point:** Influence of zeros at the central point on the distribution of zeros near the central point.

Excess Rank

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

For many families, observe

$$\begin{array}{lcr} \text{Percent with rank r} & \approx & 32\% \\ \text{Percent with rank r+1} & \approx & 48\% \\ \text{Percent with rank r+2} & \approx & 18\% \\ \text{Percent with rank r+3} & \approx & 2\% \end{array}$$

Problem: small data sets, sub-families, convergence rate log(conductor).

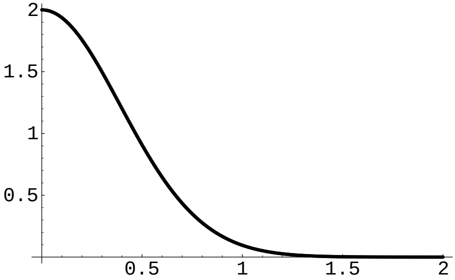
Data on Excess Rank

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

Each set is 2000 curves, last has conductors of size 10^{17}, (small on logarithmic scale).

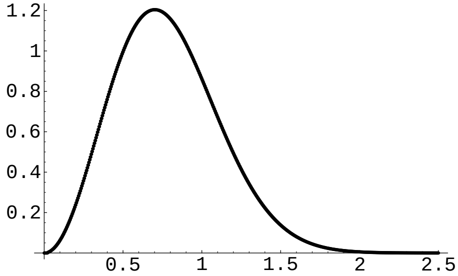
t-Start	Rk 0	Rk 1	Rk 2	Rk 3	Time (hrs)
-1000	39.4	47.8	12.3	0.6	<1
1000	38.4	47.3	13.6	0.6	<1
4000	37.4	47.8	13.7	1.1	1
8000	37.3	48.8	12.9	1.0	2.5
24000	35.1	50.1	13.9	0.8	6.8
50000	36.7	48.3	13.8	1.2	51.8

RMT: Theoretical Results ($N \to \infty$)



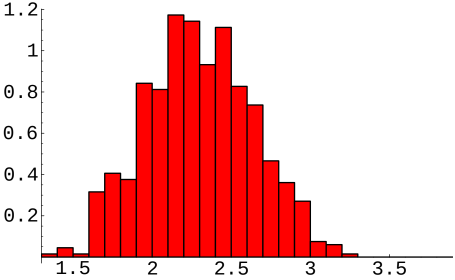
1st normalized evalue above 1: SO(even)

RMT: Theoretical Results ($N \to \infty$)



1st normalized evalue above 1: SO(odd)

Rank 2 Curves: 1st Norm. Zero above the Central Point

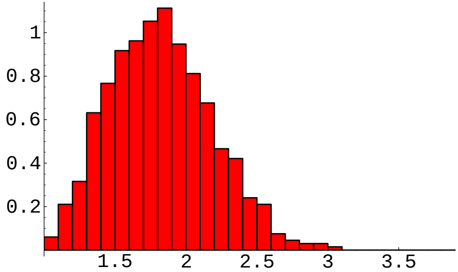


665 rank 2 curves from

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

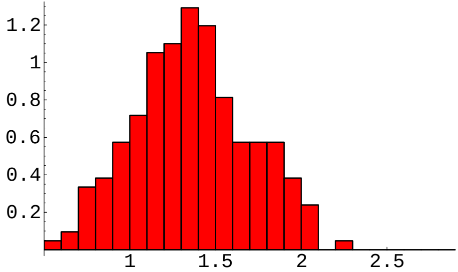
$\log(\mathrm{cond}) \in [10, 10.3125]$, median $= 2.29$, mean $= 2.30$

Rank 2 Curves: 1st Norm. Zero above the Central Point



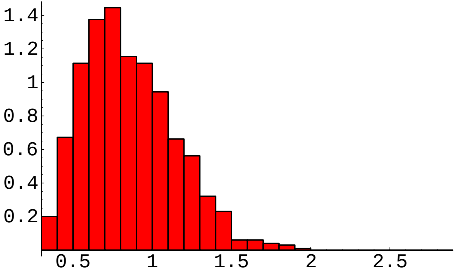
665 rank 2 curves from
$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.
$\log(\mathrm{cond}) \in [16, 16.5]$, median $= 1.81$, mean $= 1.82$

Rank 0 Curves: 1st Norm Zero: 14 One-Param of Rank 0



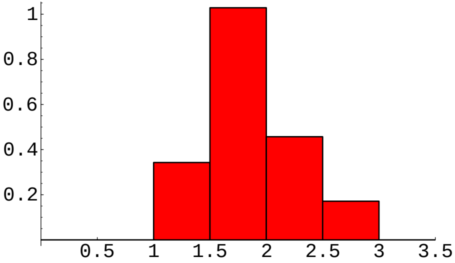
209 rank 0 curves from 14 rank 0 families, $\log(\text{cond}) \in [3.26, 9.98]$, median $= 1.35$, mean $= 1.36$

Rank 0 Curves: 1st Norm Zero: 14 One-Param of Rank 0



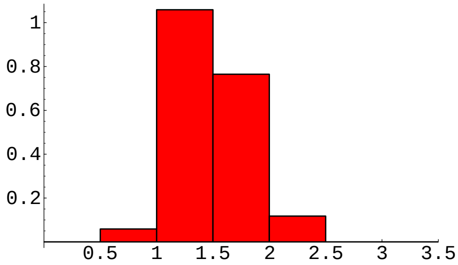
996 rank 0 curves from 14 rank 0 families,
$\log(\mathrm{cond}) \in [15.00, 16.00]$, median $=$ .81, mean $=$ .86.

Rank 2 Curves from $y^2 = x^3 - T^2x + T^2$ (Rank 2 over $\mathbb{Q}(T)$) 1st Normalized Zero above Central Point



35 curves, $\log(\text{cond}) \in [7.8, 16.1]$, $\widetilde{\mu} = 1.85$, $\mu = 1.92$, $\sigma_\mu = .41$

Rank 2 Curves from $y^2 = x^3 - T^2x + T^2$ (Rank 2 over $\mathbb{Q}(T)$)
1st Normalized Zero above Central Point



34 curves, $\log(\text{cond}) \in [16.2, 23.3]$, $\widetilde{\mu} = 1.37$, $\mu = 1.47$, $\sigma_\mu = .34$

Summary of Data

- The repulsion of the low-lying zeros increased with increasing rank, and was present even for rank 0 curves.
- As the conductors increased, the repulsion decreased.
- Statistical tests failed to reject the hypothesis that, on average, the first three zeros were all repelled equally (i.e., shifted by the same amount).

Spacings b/w Norm Zeros: Rank 0 One-Param Families over $\mathbb{Q}(T)$

- All curves have $\log(\text{cond}) \in [15, 16]$;
- $z_j =$ imaginary part of j^{th} normalized zero above the central point;
- 863 rank 0 curves from the 14 one-param families of rank 0 over $\mathbb{Q}(T)$;
- 701 rank 2 curves from the 21 one-param families of rank 0 over $\mathbb{Q}(T)$.

	863 Rank 0 Curves	**701 Rank 2 Curves**	**t-Statistic**
Median $z_2 - z_1$	1.28	1.30	
Mean $z_2 - z_1$	1.30	1.34	-1.60
StDev $z_2 - z_1$	0.49	0.51	
Median $z_3 - z_2$	1.22	1.19	
Mean $z_3 - z_2$	1.24	1.22	0.80
StDev $z_3 - z_2$	0.52	0.47	
Median $z_3 - z_1$	2.54	2.56	
Mean $z_3 - z_1$	2.55	2.56	-0.38
StDev $z_3 - z_1$	0.52	0.52	

Spacings b/w Norm Zeros: Rank 2 one-param families over $\mathbb{Q}(T)$

- All curves have $\log(\text{cond}) \in [15, 16]$;
- z_j = imaginary part of the j^{th} norm zero above the central point;
- 64 rank 2 curves from the 21 one-param families of rank 2 over $\mathbb{Q}(T)$;
- 23 rank 4 curves from the 21 one-param families of rank 2 over $\mathbb{Q}(T)$.

	64 Rank 2 Curves	23 Rank 4 Curves	t-Statistic
Median $z_2 - z_1$	1.26	1.27	
Mean $z_2 - z_1$	1.36	1.29	0.59
StDev $z_2 - z_1$	0.50	0.42	
Median $z_3 - z_2$	1.22	1.08	
Mean $z_3 - z_2$	1.29	1.14	1.35
StDev $z_3 - z_2$	0.49	0.35	
Median $z_3 - z_1$	2.66	2.46	
Mean $z_3 - z_1$	2.65	2.43	2.05
StDev $z_3 - z_1$	0.44	0.42	

Rank 2 Curves from Rank 0 & Rank 2 Families over $\mathbb{Q}(T)$

- All curves have $\log(\mathrm{cond}) \in [15, 16]$;
- z_j = imaginary part of the j^{th} norm zero above the central point;
- 701 rank 2 curves from the 21 one-param families of rank 0 over $\mathbb{Q}(T)$;
- 64 rank 2 curves from the 21 one-param families of rank 2 over $\mathbb{Q}(T)$.

	701 Rank 2 Curves	**64 Rank 2 Curves**	**t-Statistic**
Median $z_2 - z_1$	1.30	1.26	
Mean $z_2 - z_1$	1.34	1.36	0.69
StDev $z_2 - z_1$	0.51	0.50	
Median $z_3 - z_2$	1.19	1.22	
Mean $z_3 - z_2$	1.22	1.29	1.39
StDev $z_3 - z_2$	0.47	0.49	
Median $z_3 - z_1$	2.56	2.66	
Mean $z_3 - z_1$	2.56	2.65	1.93
StDev $z_3 - z_1$	0.52	0.44	

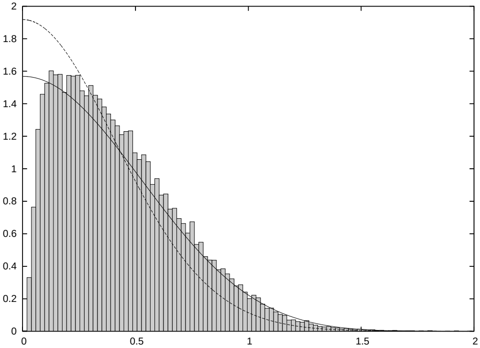
New Model for Finite Conductors

- Replace conductor N with $N_{\text{effective}}$.
  - ⋄ Arithmetic info, predict with L-function Ratios Conj.
  - ⋄ Do the number theory computation.

- Excised Orthogonal Ensembles.
  - ⋄ $L(1/2, E)$ discretized.
  - ⋄ Char. polys $\Lambda_A(\theta) = \det(I - e^{i\theta}A^{-1})$ model $L(1/2 + it, E)$.
  - ⋄ Study matrices in $\mathrm{SO}(2N_{\mathit{eff}})$ with $|\Lambda_A(0)| \geq ce^N$.

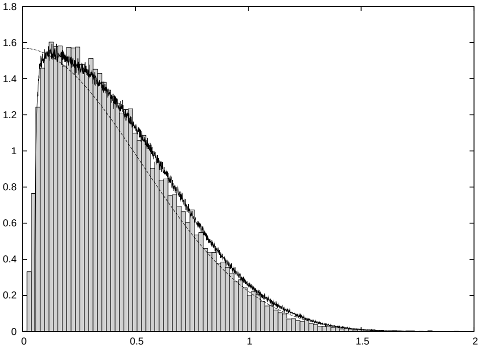
- Painlevé VI differential equation solver.
  - ⋄ Use explicit formulas for densities of Jacobi ensembles.
  - ⋄ Key input: Selberg-Aomoto integral for initial conditions.

Modeling lowest zero of $L_{E_{11}}(s, \chi_d)$ with $0 < d < 400,000$



Lowest zero for $L_{E_{11}}(s, \chi_d)$ (bar chart), lowest eigenvalue of SO(2N) with N_{eff} (solid), standard N_0 (dashed).

Modeling lowest zero of $L_{E_{11}}(s, \chi_d)$ with $0 < d < 400,000$



Lowest zero for $L_{E_{11}}(s, \chi_d)$ (bar chart); lowest eigenvalue of SO(2N): N_{eff} = 2 (solid) with discretisation, and $N_{\text{eff}} = 2.32$ (dashed) without discretisation.

The lowest eigenvalue of Jacobi Random Matrix Ensembles and Painlevé VI, (with E. Dueñez, D. K. Huynh, J. Keating and N. Snaith), Journal of Physics A: Mathematical and Theoretical **43** (2010) 405204 (27pp). http://arxiv.org/pdf/1005.1298

Models for zeros at the central point in families of elliptic curves (with E. Dueñez, D. K. Huynh, J. Keating and N. Snaith), J. Phys. A: Math. Theor. **45** (2012) 115207 (32pp). http://arxiv.org/pdf/1107.4426

Open Questions and References

Open Questions: Low-lying zeros of *L*-functions

- Generalize excised ensembles for higher weight GL_2 families where expect different discretizations.

- Obtain better estimates on vanishing at the central point by finding optimal test functions for the second and higher moment expansions.

- Further explore *L*-function Ratios Conjecture to predict lower order terms in families, compute these terms on number theory side.

See Dueñez-Huynh-Keating-Miller-Snaith, Miller, and the Ratios papers.

Publications: Random Matrix Theory

1. *Distribution of eigenvalues for the ensemble of real symmetric Toeplitz matrices* (with Christopher Hammond), Journal of Theoretical Probability **18** (2005), no. 3, 537–566. http://arxiv.org/abs/math/0312215

2. *Distribution of eigenvalues of real symmetric palindromic Toeplitz matrices and circulant matrices* (with Adam Massey and John Sinsheimer), Journal of Theoretical Probability **20** (2007), no. 3, 637–662. http://arxiv.org/abs/math/0512146

3. *The distribution of the second largest eigenvalue in families of random regular graphs* (with Tim Novikoff and Anthony Sabelli), Experimental Mathematics **17** (2008), no. 2, 231–244. http://arxiv.org/abs/math/0611649

4. *Nuclei, Primes and the Random Matrix Connection* (with Frank W. K. Firk), Symmetry **1** (2009), 64–105; doi:10.3390/sym1010064. http://arxiv.org/abs/0909.4914

5. *Distribution of eigenvalues for highly palindromic real symmetric Toeplitz matrices* (with Steven Jackson and Thuy Pham), Journal of Theoretical Probability **25** (2012), 464–495. http://arxiv.org/abs/1003.2010

6. *The Limiting Spectral Measure for Ensembles of Symmetric Block Circulant Matrices* (with Murat Koloğlu, Gene S. Kopp, Frederick W. Strauch and Wentao Xiong), Journal of Theoretical Probability **26** (2013), no. 4, 1020–1060. http://arxiv.org/abs/1008.4812

7. *Distribution of eigenvalues of weighted, structured matrix ensembles* (with Olivia Beckwith, Karen Shen), submitted December 2011 to the Journal of Theoretical Probability, revised September 2012. http://arxiv.org/abs/1112.3719 .

8. *The expected eigenvalue distribution of large, weighted d-regular graphs* (with Leo Goldmahker, Cap Khoury and Kesinee Ninsuwan), preprint.

Publications: L-Functions

1. *The low lying zeros of a* $GL(4)$ *and a* $GL(6)$ *family of L-functions* (with Eduardo Dueñez), Compositio Mathematica **142** (2006), no. 6, 1403–1425. http://arxiv.org/abs/math/0506462

2. *Low lying zeros of L–functions with orthogonal symmetry* (with Christopher Hughes), Duke Mathematical Journal **136** (2007), no. 1, 115–172. http://arxiv.org/abs/math/0507450

3. *Lower order terms in the 1-level density for families of holomorphic cuspidal newforms*, Acta Arithmetica **137** (2009), 51–98. http://arxiv.org/abs/0704.0924

4. *The effect of convolving families of L-functions on the underlying group symmetries* (with Eduardo Dueñez), Proceedings of the London Mathematical Society, 2009; doi: 10.1112/plms/pdp018. http://arxiv.org/pdf/math/0607688.pdf

5. *Low-lying zeros of number field L-functions* (with Ryan Peckner), Journal of Number Theory **132** (2012), 2866–2891. http://arxiv.org/abs/1003.5336

6. *The low-lying zeros of level 1 Maass forms* (with Levent Alpoge), preprint 2013. http://arxiv.org/abs/1301.5702

7. *The n-level density of zeros of quadratic Dirichlet L-functions* (with Jake Levinson), submitted September 2012 to Acta Arithmetica. http://arxiv.org/abs/1208.0930

8. *Moment Formulas for Ensembles of Classical Compact Groups* (with Geoffrey Iyer and Nicholas Triantafillou), preprint 2013.

Publications: Elliptic Curves

1. 1- *and* 2-*level densities for families of elliptic curves: evidence for the underlying group symmetries*, Compositio Mathematica **140** (2004), 952–992. http://arxiv.org/pdf/math/0310159

2. *Variation in the number of points on elliptic curves and applications to excess rank*, C. R. Math. Rep. Acad. Sci. Canada **27** (2005), no. 4, 111–120. http://arxiv.org/abs/math/0506461

3. *Investigations of zeros near the central point of elliptic curve L-functions*, Experimental Mathematics **15** (2006), no. 3, 257–279. http://arxiv.org/pdf/math/0508150

4. *Constructing one-parameter families of elliptic curves over $\mathbb{Q}(T)$ with moderate rank* (with Scott Arms and Álvaro Lozano-Robledo), Journal of Number Theory **123** (2007), no. 2, 388–402. http://arxiv.org/abs/math/0406579

5. *Towards an 'average' version of the Birch and Swinnerton-Dyer Conjecture* (with John Goes), Journal of Number Theory **130** (2010), no. 10, 2341–2358. http://arxiv.org/abs/0911.2871

6. *The lowest eigenvalue of Jacobi Random Matrix Ensembles and Painlevé VI*, (with Eduardo Dueñez, Duc Khiem Huynh, Jon Keating and Nina Snaith), Journal of Physics A: Mathematical and Theoretical **43** (2010) 405204 (27pp). http://arxiv.org/pdf/1005.1298

7. *Models for zeros at the central point in families of elliptic curves* (with Eduardo Dueñez, Duc Khiem Huynh, Jon Keating and Nina Snaith), J. Phys. A: Math. Theor. **45** (2012) 115207 (32pp). http://arxiv.org/pdf/1107.4426

8. *Effective equidistribution and the Sato-Tate law for families of elliptic curves* (with M. Ram Murty), Journal of Number Theory **131** (2011), no. 1, 25–44. http://arxiv.org/abs/1004.2753

9. *Moments of the rank of elliptic curves* (with Siman Wong), Canad. J. of Math. **64** (2012), no. 1, 151–182. http://web.williams.edu/Mathematics/sjmiller/public_html/math/papers/mwMomentsRanksEC812final.pdf

Publications: L-Function Ratio Conjecture

1. *A symplectic test of the L-Functions Ratios Conjecture*, Int Math Res Notices (2008) Vol. 2008, article ID rnm146, 36 pages, doi:10.1093/imrn/rnm146. http://arxiv.org/abs/0704.0927

2. *An orthogonal test of the L-Functions Ratios Conjecture*, Proceedings of the London Mathematical Society 2009, doi:10.1112/plms/pdp009. http://arxiv.org/abs/0805.4208

3. *A unitary test of the L-functions Ratios Conjecture* (with John Goes, Steven Jackson, David Montague, Kesinee Ninsuwan, Ryan Peckner and Thuy Pham), Journal of Number Theory **130** (2010), no. 10, 2238–2258. http://arxiv.org/abs/0909.4916

4. *An Orthogonal Test of the L-functions Ratios Conjecture, II* (with David Montague), Acta Arith. **146** (2011), 53–90. http://arxiv.org/abs/0911.1830

5. *An elliptic curve family test of the Ratios Conjecture* (with Duc Khiem Huynh and Ralph Morrison), Journal of Number Theory **131** (2011), 1117–1147. http://arxiv.org/abs/1011.3298

6. *Surpassing the Ratios Conjecture in the 1-level density of Dirichlet L-functions* (with Daniel Fiorilli). submitted September 2012 to Proceedings of the London Mathematical Society. http://arxiv.org/abs/1111.3896

Example:
Dirichlet L-functions

Dirichlet Characters (m prime)

$(\mathbb{Z}/m\mathbb{Z})^*$ is cyclic of order $m-1$ with generator g. Let $\zeta_{m-1} = e^{2\pi i/(m-1)}$. The principal character χ_0 is given by

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

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 $\chi(g) = \zeta_{m-1}^{l}$. Hence for each $l, 1 \le l \le m-2$ we have

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

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

$$\epsilon = \begin{cases} 0 & \text{if } \chi(-1) = 1 \\ 1 & \text{if } \chi(-1) = -1 \end{cases}$$

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.

$$\begin{aligned}
&\sum \phi\left(\gamma \frac{\log(\frac{m}{\pi})}{2\pi}\right) \\
= \quad & \int_{-\infty}^{\infty} \phi(y)dy \\
&- \sum_p \frac{\log p}{\log(m/\pi)} \widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right)[\chi(p) + \bar{\chi}(p)]p^{-\frac{1}{2}} \\
&- \sum_p \frac{\log p}{\log(m/\pi)} \widehat{\phi}\left(2\frac{\log p}{\log(m/\pi)}\right)[\chi^2(p) + \bar{\chi}^2(p)]p^{-1} \\
&+ O\left(\frac{1}{\log m}\right).
\end{aligned}$$

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):

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

Note can pass Character Sum through Test Function.

Character Sums

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

Character Sums

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

For any prime $p \neq m$

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

Character Sums

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

For any prime $p \neq m$

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

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: no contribution if $\sigma < 2$

$$\frac{-2}{m-2}\sum_{p}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right)p^{-\frac{1}{2}}$$

$$+\quad 2\frac{m-1}{m-2}\sum_{p\equiv 1(m)}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right)p^{-\frac{1}{2}}$$

First Sum: no contribution if $\sigma < 2$

$$\frac{-2}{m-2}\sum_{p}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right)p^{-\frac{1}{2}}$$

$$+\quad 2\frac{m-1}{m-2}\sum_{p\equiv 1(m)}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right)p^{-\frac{1}{2}}$$

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

First Sum: no contribution if $\sigma < 2$

$$\frac{-2}{m-2}\sum_{p}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\Big(\frac{\log p}{\log(m/\pi)}\Big)p^{-\frac{1}{2}}$$

$$+\quad 2\frac{m-1}{m-2}\sum_{p\equiv 1(m)}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\Big(\frac{\log p}{\log(m/\pi)}\Big)p^{-\frac{1}{2}}$$

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

First Sum: no contribution if $\sigma < 2$

$$\frac{-2}{m-2}\sum_{p}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right)p^{-\frac{1}{2}}$$

$$+\quad 2\frac{m-1}{m-2}\sum_{p\equiv 1(m)}^{m^\sigma}\frac{\log p}{\log(m/\pi)}\widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right)p^{-\frac{1}{2}}$$

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

$$\ll\quad \frac{1}{m}\sum_{k}^{m^\sigma}k^{-\frac{1}{2}}+\frac{1}{m}\sum_{k}^{m^\sigma}k^{-\frac{1}{2}}\ll\frac{1}{m}m^{\sigma/2}.$$

Second Sum

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

$$\sum_{\chi\neq\chi_0}[\chi^2(p)+\bar{\chi}^2(p)] = \begin{cases} 2(m-2) & p\equiv\pm 1(m) \\ -2 & p\not\equiv\pm 1(m)\end{cases}$$

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

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

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

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

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

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

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

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

Expansion Preliminaries

$k(s)$ is an s-tuple $(k_1, k_2, \dots, k_s)$ with $k_1 < k_2 < \cdots < k_s$.
This is just a subset of $(1, 2, \dots, r)$, 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

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

As $m/M_2 \leq 3^r$, $s=0$ 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 $\sigma < 2$.

First Sum

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

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

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 and Bounds

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

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

Second Sum Expansions and Bounds

Handle similarly as before. Say

$$\begin{aligned} p &\equiv 1 \bmod m_{k_1}, \dots, m_{k_a} \\ p &\equiv -1 \bmod m_{k_a+1}, \dots, m_{k_b} \end{aligned}$$

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 $\sigma < 2$ for square-free $m \in [N, 2N]$ from:

Theorem

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

Then family $\mathcal{F}_m$ of primitive characters mod m has

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