From Nuclear Physics to Number Theory

How the Manhattan Project helped us understand primes

Steven J. Miller

Brown University

Colby College, March 8^{th}, 2005

http://www.math.brown.edu/$\sim$sjmiller

Acknowledgements

Random Matrices (with Peter Sarnak)

- Rebecca Lehman
- Yi-Kai Liu
- Chris Hammond
- Inna Zakharevich

Random Graphs (with Peter Sarnak, Yakov Sinai)

- Dustin Steinhauer
- Randy Qian
- Felice Kuan
- Leo Goldmakher

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 b/w Primes.
- Spacings b/w Energy Levels of Nuclei.
- Spacings b/w Eigenvalues of Matrices.
- Spacings b/w Zeros of Functions.

Goals of the Talk

- Determine correct scale to study spacings.

- See similar behavior in different systems.

- Discuss tools / techniques needed to prove the results.

PART I

NORMALIZED SPACINGS & BACKGROUND MATERIAL

Normalized Spacing

Example: Fractional Parts

For $\alpha \notin \mathbb{Q}$, set $x_n = n\alpha \bmod 1$.

Order $x_1, \dots, x_N$: $0 \ \leq \ y_1 \ \leq \ \cdots \ \leq \ y_N \leq \ 1$.

Normalized Spacing

Example: Fractional Parts

For $\alpha \notin \mathbb{Q}$, set $x_n = n\alpha \bmod 1$.

Order $x_1, \dots, x_N$: $0 \ \leq\ y_1 \ \leq\ \cdots \ \leq\ y_N \leq\ 1$.

Expect spacings between adjacent y's of size $\frac{1}{N}$.

Normalized Spacing

Example: Fractional Parts

For $\alpha \notin \mathbb{Q}$, set $x_n = n\alpha \bmod 1$.

Order $x_1, \dots, x_N$: $0 \ \leq \ y_1 \ \leq \ \cdots \ \leq \ y_N \leq \ 1$.

Expect spacings between adjacent y's of size $\frac{1}{N}$.

Should study $\frac{y_{n+1} - y_n}{1/N}$.

Normalized Spacing

Example: Primes

$$\pi(x) = \#\{p : p \text{ prime}, p \leq x\} \;\approx\; \frac{x}{\log x}$$

$$(\text{Ave Spacing b/w Primes at most } x) \;=\; \frac{x}{\pi(x)} \;\approx\; \log x.$$

Normalized Spacing

Example: Primes

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

$$(\text{Ave Spacing b/w Primes at most } x) \ =\ \frac{x}{\pi(x)} \ \approx\ \log x.$$

If $p_n, p_{n+1} \approx x$, study $\frac{p_{n+1} - p_n}{\log x}$.

Normalized Spacing

Example: Primes

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

$$(\text{Ave Spacing b/w Primes at most } x) = \frac{x}{\pi(x)} \approx \log x.$$

If $p_n, p_{n+1} \approx x$, study $\frac{p_{n+1}-p_n}{\log x}$.

One reason why twin primes are so hard: $\frac{2}{\log x} \to 0$.

Normalized Spacing

Example: Primes

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

$$(\text{Ave Spacing b/w Primes at most } x) = \frac{x}{\pi(x)} \approx \log x.$$

If $p_n, p_{n+1} \approx x$, study $\frac{p_{n+1}-p_n}{\log x}$.

One reason why twin primes are so hard: $\frac{2}{\log x} \to 0$.

Aside: Twin primes led to finding the pentium bug!

PART II

PROBABILITY AND LINEAR ALGEBRA REVIEW

Probability Review

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

$$\begin{aligned} p(x) &\geq 0 \\ \int_{-\infty}^{\infty} p(x)dx &= 1. \end{aligned}$$

Thus

$$\text{Prob}\left(x \in [a, b]\right) = \int_a^b p(x)dx.$$

Probability Review

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

$$\begin{aligned} p(x) &\geq 0 \\ \int_{-\infty}^{\infty} p(x)dx &= 1. \end{aligned}$$

Thus

$$\text{Prob}\,(x \in [a,b]) \;=\; \int_a^b p(x)dx.$$

Moments:

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

Good function uniquely determined by its Taylor Series, a good probability density is uniquely determined by its moments.

Probability Review (cont)

Important quantities:

1. Mean $\mu = \int xp(x)dx$.

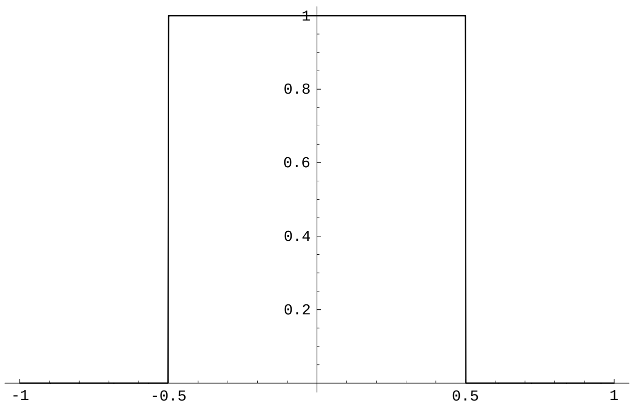
2. Variance $\sigma^2 = \int (x-\mu)^2 p(x)dx$.

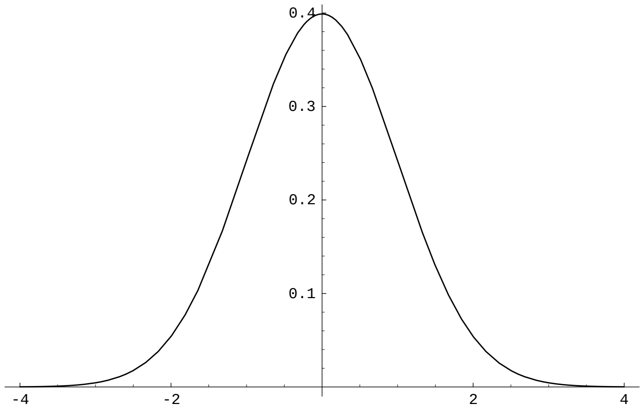
Probability Review (cont)

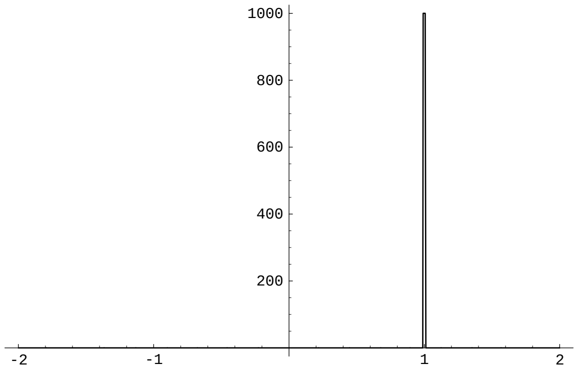
Important quantities:

1. Mean $\mu = \int xp(x)dx$.

2. Variance $\sigma^2 = \int (x-\mu)^2 p(x)dx$.







Uniform: $\mu = 0, \sigma^2 = \frac{1}{12}$

Gaussian: $\mu = 0, \sigma^2 = 1$

Delta Spike: $\mu = 1, \sigma^2 = 0$

$$p(x) = \begin{cases} 1 & \text{if } |x| \leq \frac{1}{2} \\ 0 & \text{otherwise} \end{cases}$$

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

$$\delta(x-1)$$

Linear Algebra Review

$$\begin{pmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{N1} & \cdots & a_{NN} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_N \end{pmatrix} = \begin{pmatrix} w_1 \\ \vdots \\ w_N \end{pmatrix}$$

In general, in $A\overrightarrow{v} = \overrightarrow{w}$, $\overrightarrow{w}$ will have different **magnitude** and **direction** than $\overrightarrow{v}$.

Linear Algebra Review

$$\begin{pmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{N1} & \cdots & a_{NN} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_N \end{pmatrix} = \begin{pmatrix} w_1 \\ \vdots \\ w_N \end{pmatrix}$$

In general, in $A\overrightarrow{v} = \overrightarrow{w}$, $\overrightarrow{w}$ will have different **magnitude** and **direction** than $\overrightarrow{v}$.

$\overrightarrow{v} \neq \overrightarrow{0}$ is an **eigenvector** with **eigenvalue** λ if

$$A\overrightarrow{v} = \lambda\overrightarrow{v}.$$

Linear Algebra Review

$$\begin{pmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{N1} & \cdots & a_{NN} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_N \end{pmatrix} = \begin{pmatrix} w_1 \\ \vdots \\ w_N \end{pmatrix}$$

In general, in $A\overrightarrow{v} = \overrightarrow{w}$, $\overrightarrow{w}$ will have different **magnitude** and **direction** than $\overrightarrow{v}$.

$\overrightarrow{v} \neq \overrightarrow{0}$ is an **eigenvector** with **eigenvalue** λ if

$$A\overrightarrow{v} \;=\; \lambda\overrightarrow{v}.$$

Note

$$A^2\overrightarrow{v} \;=\; A(A\overrightarrow{v}) \;=\; A(\lambda\overrightarrow{v}) \;=\; \lambda^2\overrightarrow{v}.$$

Linear Algebra Review (cont)

Say $\overrightarrow{v_i}$ eigenvectors with eigenvalues λ_i.

Assume

$$\overrightarrow{v} \; = \; c_1\overrightarrow{v_1} + \cdots + c_k\overrightarrow{v_k}.$$

Linear Algebra Review (cont)

Say $\overrightarrow{v_i}$ eigenvectors with eigenvalues λ_i.

Assume

$$\overrightarrow{v} \; = \; c_1\overrightarrow{v_1} + \cdots + c_k\overrightarrow{v_k}.$$

Then

$$A^m\overrightarrow{v} \; = \; A^m(c_1\overrightarrow{v_1} + \cdots + c_k\overrightarrow{v_k})$$

Linear Algebra Review (cont)

Say $\overrightarrow{v_i}$ eigenvectors with eigenvalues λ_i.

Assume

$$\overrightarrow{v} = c_1\overrightarrow{v_1} + \cdots + c_k\overrightarrow{v_k}.$$

Then

$$\begin{aligned} A^m\overrightarrow{v} &= A^m(c_1\overrightarrow{v_1} + \cdots + c_k\overrightarrow{v_k}) \\ &= A^m(c_1\overrightarrow{v_1}) + \cdots + A^m(c_k\overrightarrow{v_k}) \end{aligned}$$

Linear Algebra Review (cont)

Say $\overrightarrow{v_i}$ eigenvectors with eigenvalues λ_i.

Assume

$$\overrightarrow{v} = c_1\overrightarrow{v_1} + \cdots + c_k\overrightarrow{v_k}.$$

Then

$$\begin{aligned}
A^m\overrightarrow{v} &= A^m(c_1\overrightarrow{v_1} + \cdots + c_k\overrightarrow{v_k}) \\
&= A^m(c_1\overrightarrow{v_1}) + \cdots + A^m(c_k\overrightarrow{v_k}) \\
&= c_1A^m\overrightarrow{v_1} + \cdots + c_kA^m\overrightarrow{v_k}
\end{aligned}$$

Linear Algebra Review (cont)

Say $\overrightarrow{v_i}$ eigenvectors with eigenvalues λ_i.

Assume

$$\overrightarrow{v} = c_1\overrightarrow{v_1} + \cdots + c_k\overrightarrow{v_k}.$$

Then

$$\begin{aligned} A^m\overrightarrow{v} &= A^m(c_1\overrightarrow{v_1} + \cdots + c_k\overrightarrow{v_k}) \\ &= A^m(c_1\overrightarrow{v_1}) + \cdots + A^m(c_k\overrightarrow{v_k}) \\ &= c_1A^m\overrightarrow{v_1} + \cdots + c_kA^m\overrightarrow{v_k} \\ &= c_1\lambda_1^m\overrightarrow{v_1} + \cdots + c_k\lambda_k^m\overrightarrow{v_k}. \end{aligned}$$

PART II

RANDOM MATRIX THEORY

Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem Intractable.

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.

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:

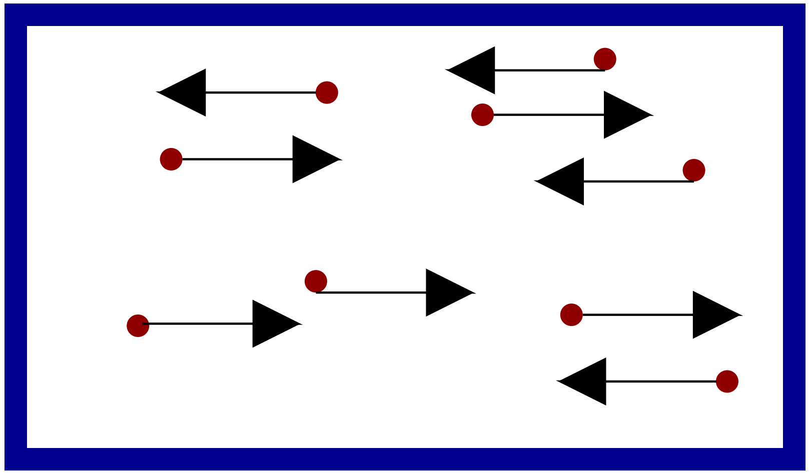
$$H\psi_n \;=\; E_n\psi_n$$

H : matrix, entries depend on system

E_n : are the energy levels

ψ_n : are the energy eigenfunctions

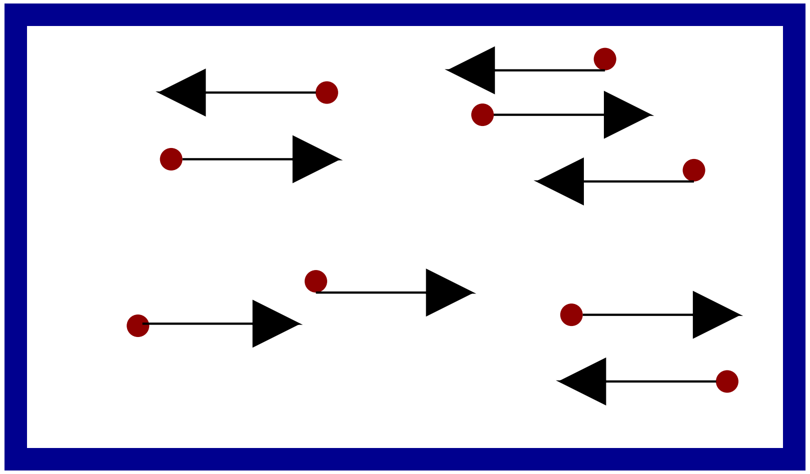
Origins (cont)



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

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

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 ($A = A^T$), Complex Hermitian ($\overline{A}^T = A$), Classical Compact groups.

Random Matrix Ensembles

Real Symmetric Matrices:

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

Random Matrix Ensembles

Real Symmetric Matrices:

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

Fix p, define

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

Random Matrix Ensembles

Real Symmetric Matrices:

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

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.

Eigenvalue Distribution

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

To each A, attach a probability measure:

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

Eigenvalue Distribution

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

To each A, attach a probability measure:

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

Equivalently

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

Semi-Circle Law

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

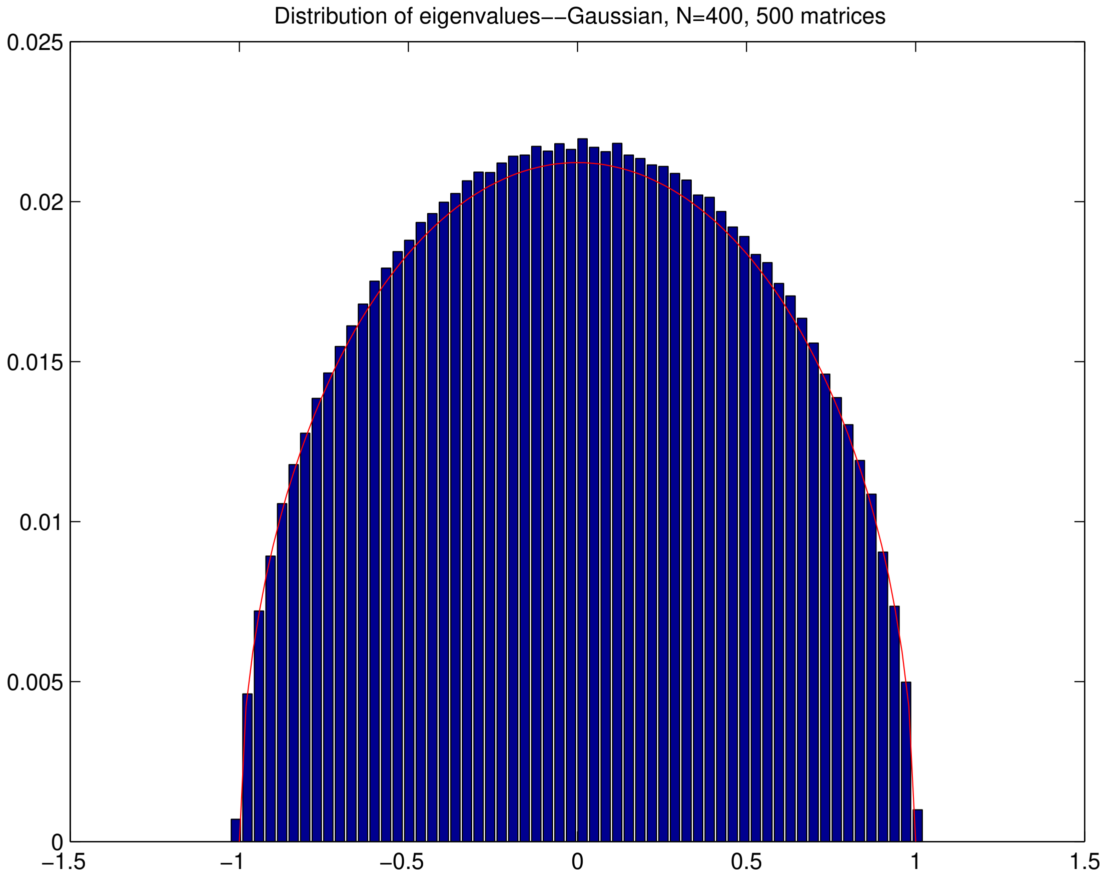
Semi-Circle Law

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

Semi-Circle Law: Assume p has mean 0, variance 1, other moments finite. Then for almost all A, as $N \to \infty$

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

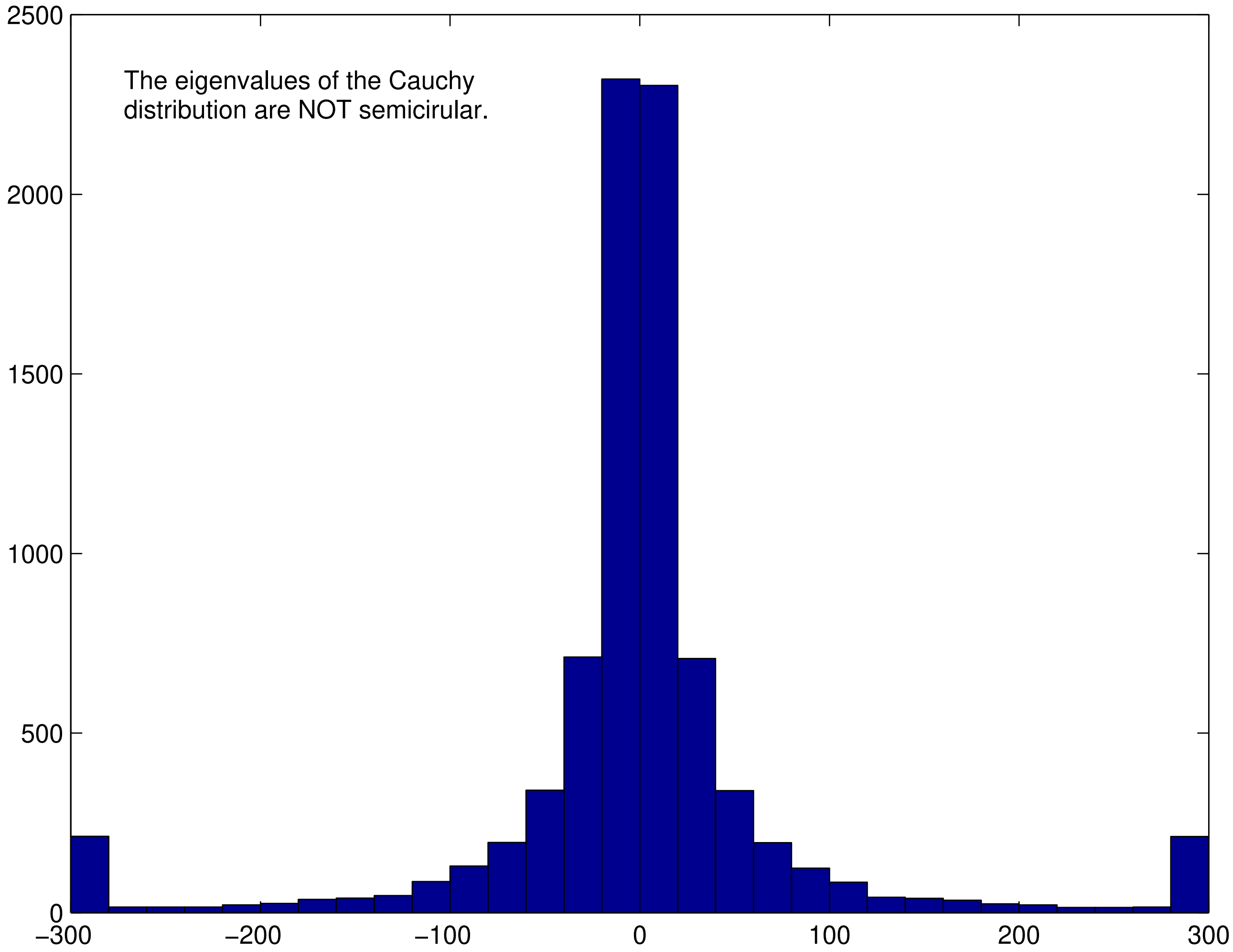
Random Matrix Theory: Semi-Circle Law



500 **Matrices: Gaussian** 400×400

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

Random Matrix Theory: Semi-Circle Law



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

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.

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.

Only known if p is a Gaussian.

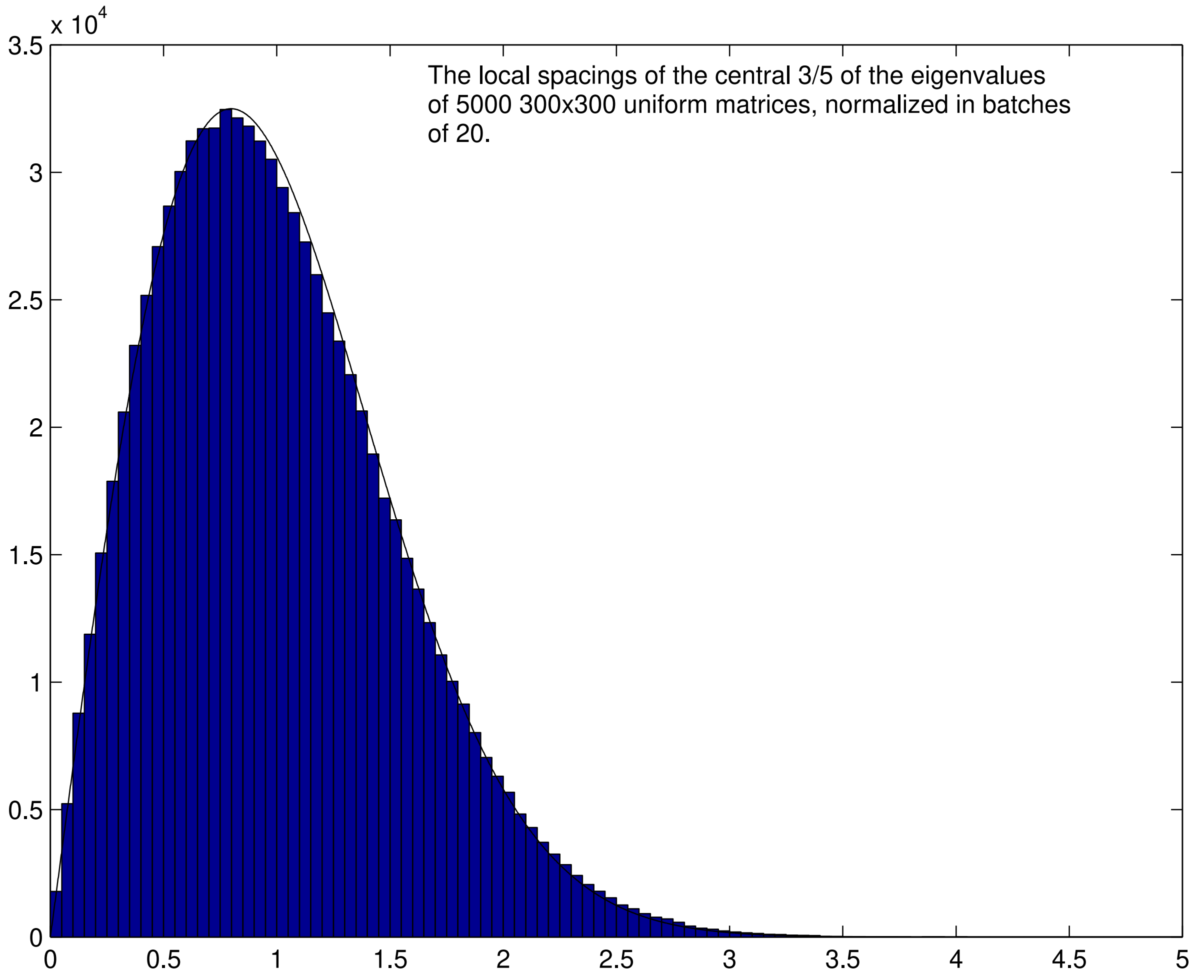
GOE Conjecture

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

Only known if p is a Gaussian.

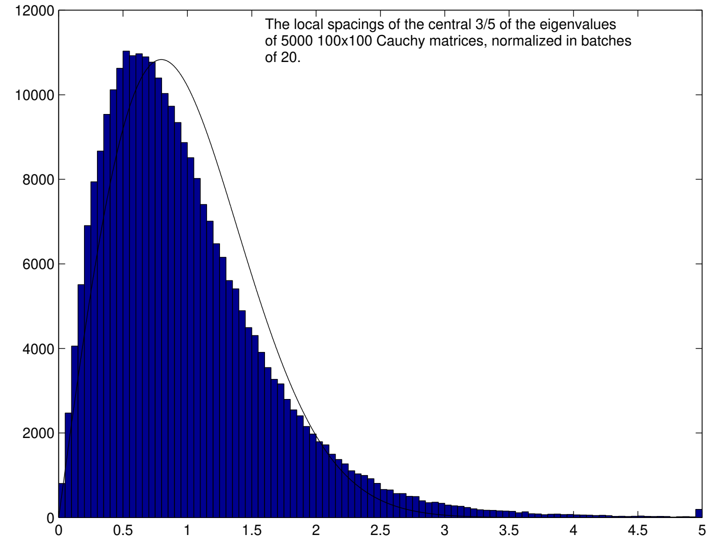
$$\text{GOE}(x) \ \approx \ Axe^{-Bx^2}.$$

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

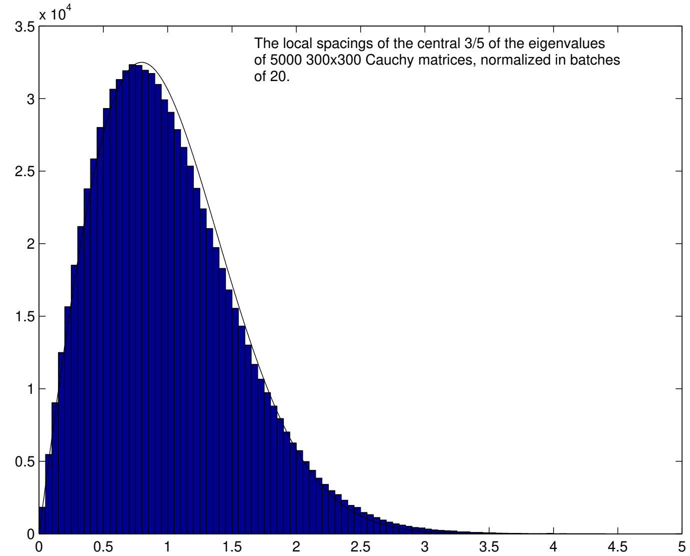


5000: 300×300 uniform on $[-1, 1]$

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



5000: 100×100 Cauchy



5000: 300×300 Cauchy

Fat Thin Families

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

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.

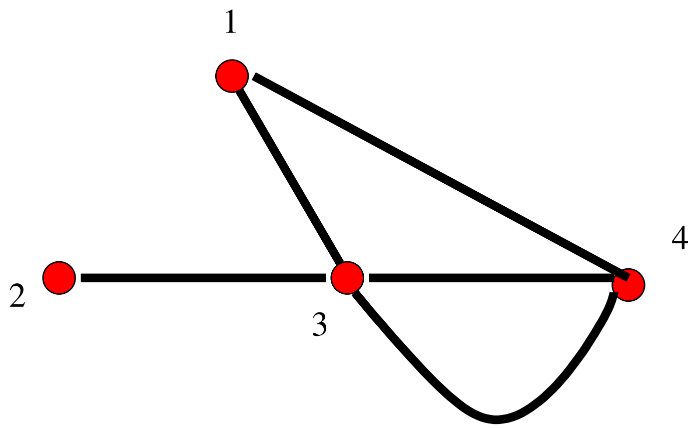
Fat Thin Families

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

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

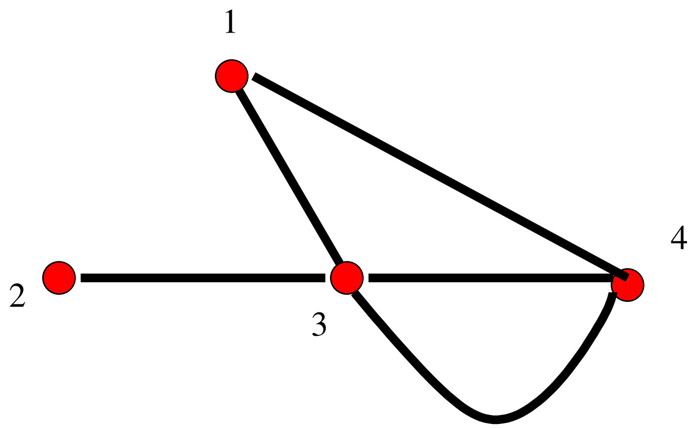
Real Symmetric Matrices have $\frac{N(N+1)}{2}$ independent entries.

Random Graphs



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

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.

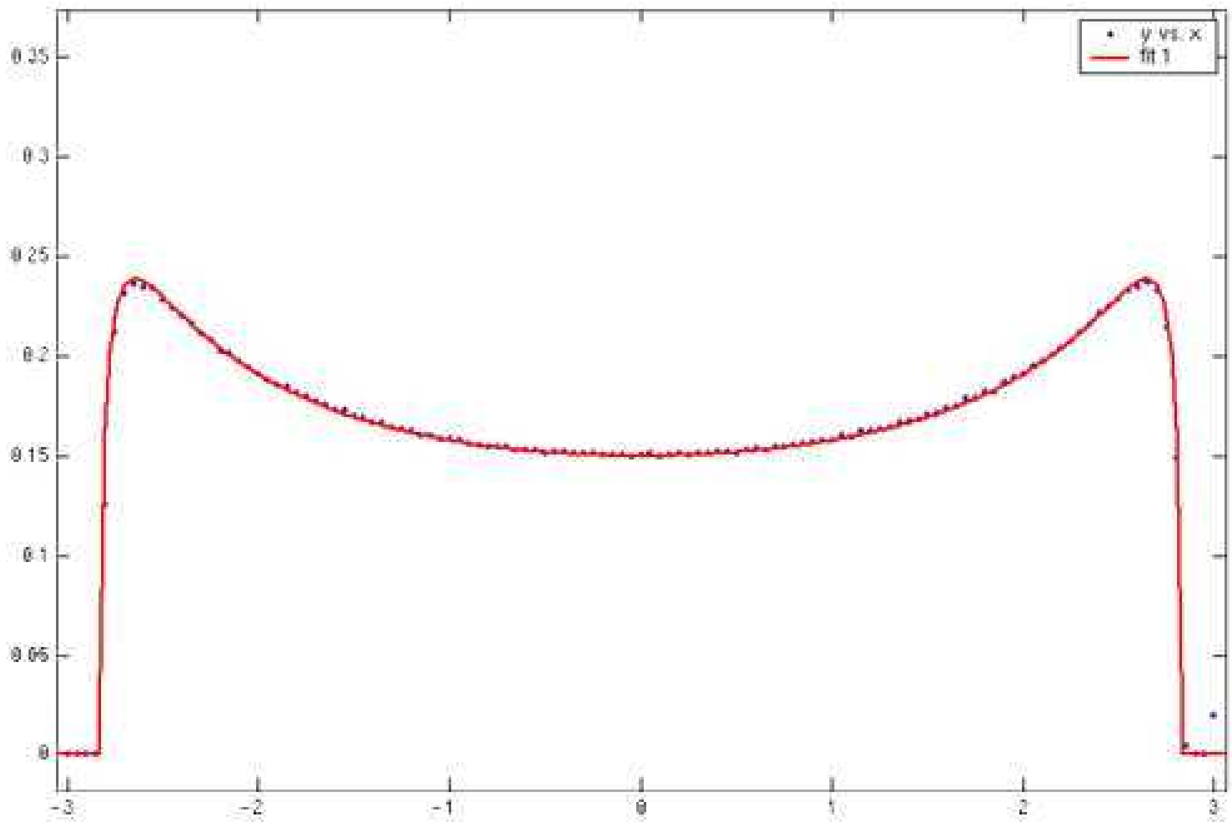
$$A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{pmatrix}$$

These are Real Symmetric Matrices.

McKay's Law

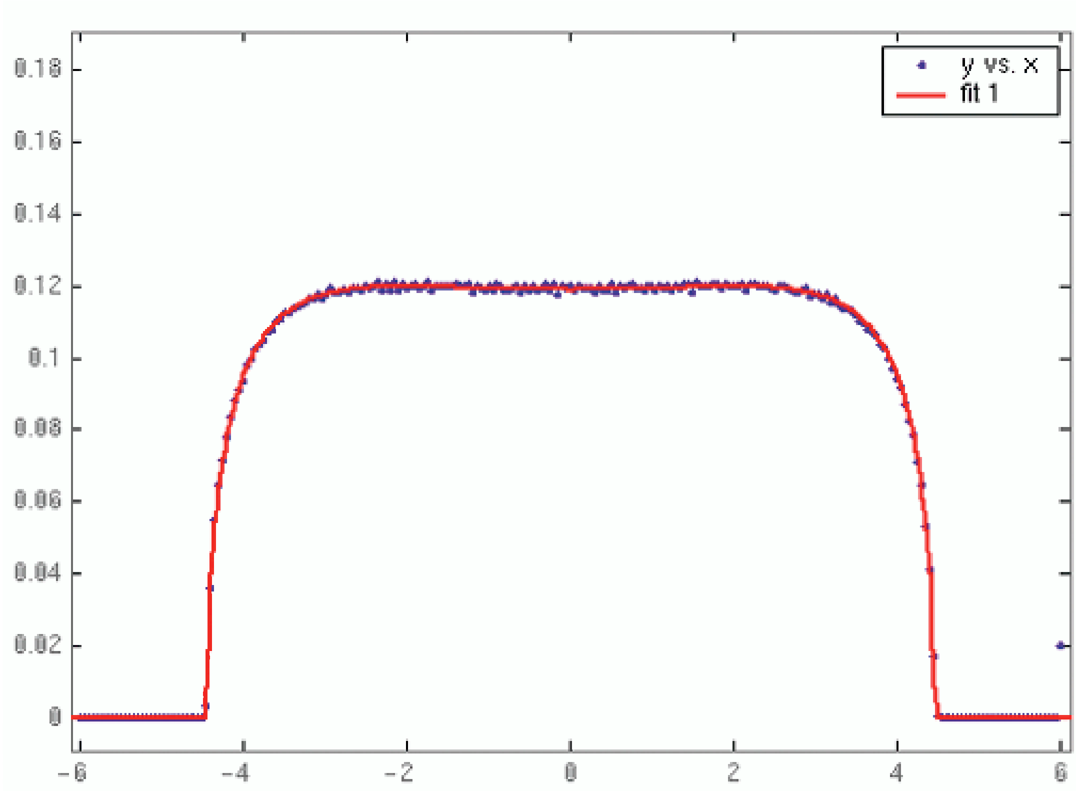
Density of Eigenvalues for d-regular graphs

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



$$d = 3.$$

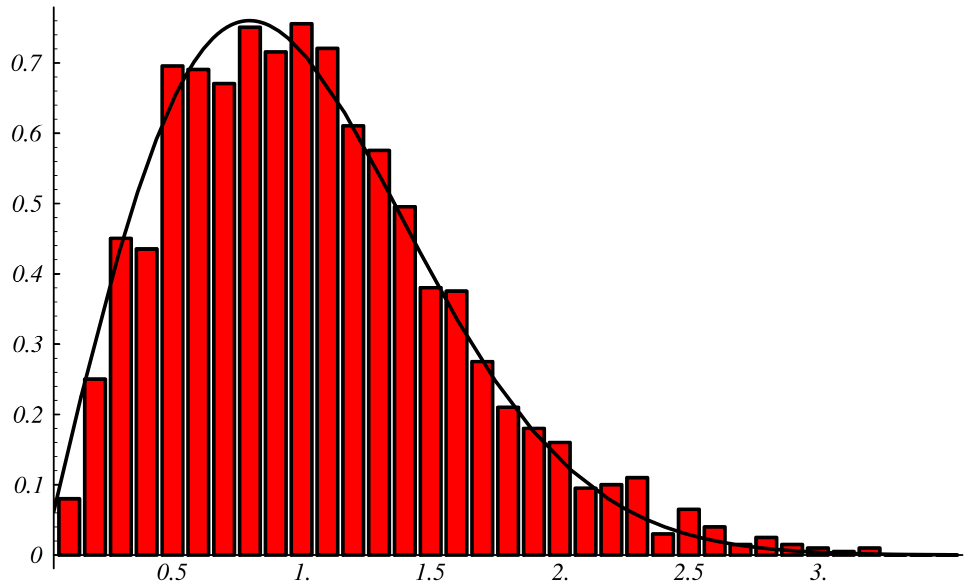
McKay's Law



$$d = 6.$$

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

3-Regular, 2000 Vertices and GOE



PART III

NUMBER THEORY

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

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

Geometric Series (and Extending Functions): If $|u| < 1$,

$$\sum_{k=0}^{\infty} u^k = 1 + u + u^2 + u^3 + \cdots = \frac{1}{1-u}$$

Riemann Zeta Function

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

Geometric Series (and Extending Functions): If $|u| < 1$,

$$\sum_{k=0}^{\infty} u^k = 1 + u + u^2 + u^3 + \cdots = \frac{1}{1-u}$$

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

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \left[1 + \frac{1}{2^s} + \left(\frac{1}{2^s}\right)^2 + \cdots\right] \left[1 + \frac{1}{3^s} + \left(\frac{1}{3^s}\right)^2 + \cdots\right] \cdots$$

$$= \sum_n \frac{1}{n^s}.$$

Riemann Zeta Function (cont):

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

Riemann Zeta Function (cont):

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

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

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

Riemann Zeta Function (cont):

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

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

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

Riemann Zeta Function (cont):

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

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

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

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

Riemann Zeta Function (cont):

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

Functional Equation:

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

Riemann Zeta Function (cont):

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

Functional Equation:

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

Riemann Hypothesis:

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

Riemann Zeta Function (cont):

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

Functional Equation:

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

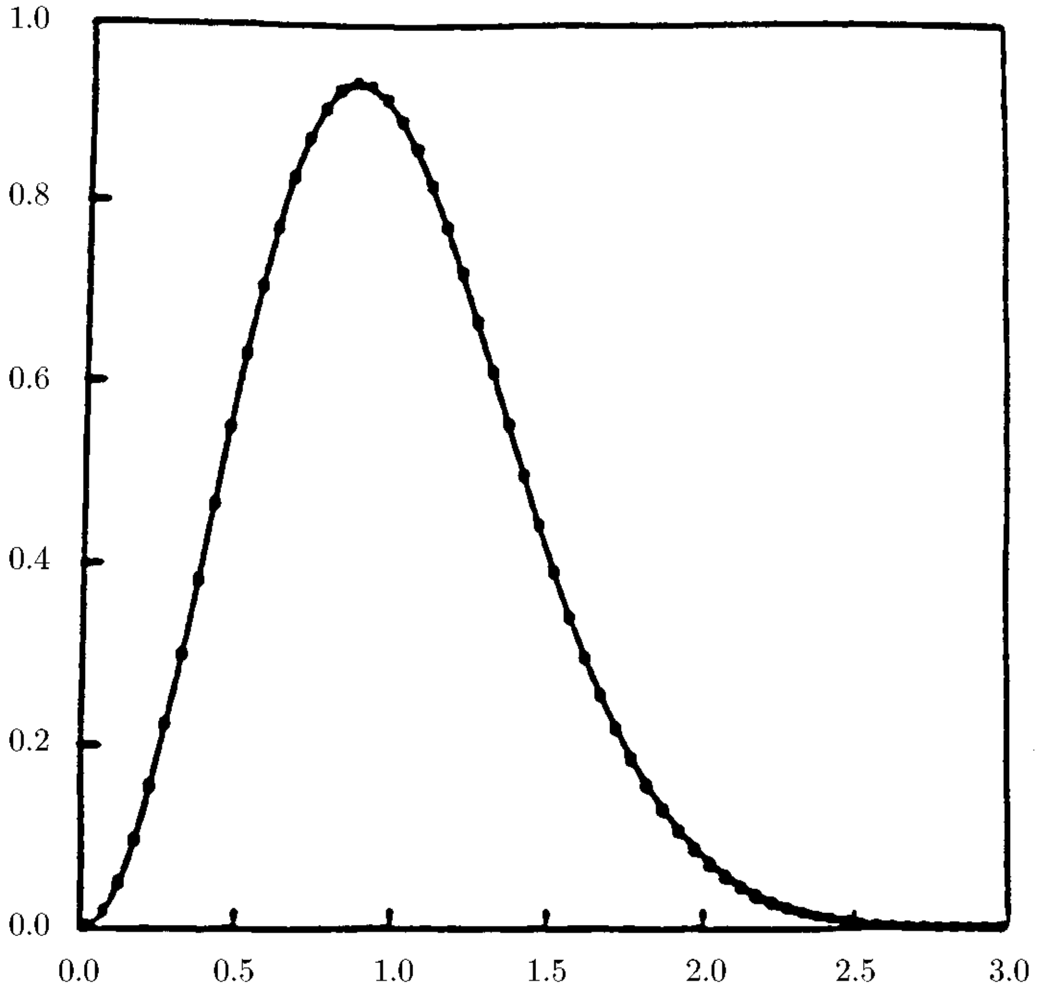
Riemann Hypothesis:

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

Observation:

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

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)

Families of L-Functions

More generally, we may consider an L-function

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

Families of L-Functions

More generally, we may consider an L-function

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

Examples:

- Dirichlet Characters: $a_n(f) \;=\; \chi_f(n)$.
- Elliptic Curves: $y^2 \;=\; x^3 + A_f x + B_f$, $a_p(f)$ is related to number of solns mod p.

General Riemann Hypothesis: All L-functions (after normalization) have their zeros on the critical line.

PART IV

SKETCH OF PROOFS

SKETCH OF PROOF: Eigenvalue Trace Lemma

$$\text{Trace}(A) \;=\; a_{11} + a_{22} + \cdots + a_{NN}.$$

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

Allows us to pass from knowledge of matrix entries to knowledge of eigenvalues.

SKETCH OF PROOF: Correct Scale

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

SKETCH OF PROOF: Correct Scale

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

By the Central Limit Theorem:

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

SKETCH OF PROOF: Correct Scale

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

By the Central Limit Theorem:

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

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

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: Eigenvalue Distribution

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

SKETCH OF PROOF: Eigenvalue Distribution

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

To each A, attach a probability measure:

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

SKETCH OF PROOF: Eigenvalue Distribution

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

To each A, attach a probability measure:

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

Equivalently

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

SKETCH OF PROOF: Eigenvalue Distribution

$\delta(x - x_0)$ 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:

$$k^{th}\text{-moment} \;=\; \int_{-\infty}^{\infty} x^k \mu_{A,N}(x)dx \;=\; \frac{1}{N}\sum_{i=1}^{N}\frac{\lambda_i(A)^k}{(2\sqrt{N})^k} \;=\; \frac{\text{Trace}(A^k)}{2^k N^{\frac{k}{2}+1}}$$

SKETCH OF PROOF: Semi-Circle Law

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

Semi-Circle Law: Assume p has mean 0, variance 1, other moments finite. Then for almost all A, as $N \to \infty$

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

SKETCH OF PROOF: Semi-Circle Law

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

Semi-Circle Law: Assume p has mean 0, variance 1, other moments finite. Then for almost all A, as $N \to \infty$

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

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

SKETCH OF PROOF: Semi-Circle Law

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

Semi-Circle Law: Assume p has mean 0, variance 1, other moments finite. Then for almost all A, as $N \to \infty$

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

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

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

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

SKETCH OF PROOF: 2^{nd}-Moment

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

SKETCH OF 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

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

SKETCH OF PROOF: 2^{nd}-Moment

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

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

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

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

SKETCH OF PROOF: Zero Knowledge (Heuristic)

$P(x)$ polynomial, zeros $r_1, \ldots, r_n$. Then

$$\begin{aligned} P(x) &= (x-r_1)(x-r_2)\cdots(x-r_n) \\ &= x^n + a_{n-1}(r_1,\ldots,r_n)x^{n-1} + \cdots + a_0(r_1,\ldots,r_n) \end{aligned}$$

where

$$\begin{aligned} a_{n-1}(r_1,\ldots,r_n) &= -(r_1+\cdots+r_n) \\ &\vdots \\ a_0(r_1,\ldots,r_n) &= r_1 r_2 \cdots r_n. \end{aligned}$$

Knowledge of zeros gives info on coefficients.

Explicit Formula: (Contour Integration)

$$-\frac{\zeta'(s)}{\zeta(s)} \quad = \quad -\frac{\mathrm{d}}{\mathrm{d}s}\log\zeta(s)$$

Explicit Formula: (Contour Integration)

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

Explicit Formula: (Contour Integration)

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

Contour Integration:

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

Knowledge of zeros gives info on coefficients.

PART V

CONCLUSIONS

Correspondences

Similarities b/w Nuclei and Primes:

$$\text{Energy Levels} \longleftrightarrow \text{Zeros of } \zeta(s)$$

Correspondences

Similarities b/w Nuclei and Primes:

$$\text{Energy Levels} \longleftrightarrow \text{Zeros of } \zeta(s)$$

$$\text{Neutron Energy} \longleftrightarrow \text{Summation Formulas}$$

Correspondences

Similarities b/w Nuclei and Primes:

Energy Levels	$\longleftrightarrow$	Zeros of $\zeta(s)$
Neutron Energy	$\longleftrightarrow$	Summation Formulas
Different Elements: U, Pu, ...	$\longleftrightarrow$	Different L-Functions

Summary

- Similar behavior in different systems.

Summary

- Similar behavior in different systems.

- Find correct scale.

Summary

- Similar behavior in different systems.

- Find correct scale.

- Average over similar elements.

Summary

- Similar behavior in different systems.
- Find correct scale.
- Average over similar elements.
- Need a Trace Lemma.

Summary

- Similar behavior in different systems.

- Find correct scale.

- Average over similar elements.

- Need a Trace Lemma.

- Thin subsets can exhibit very different behavior.

Open Problems (RMT)

Real Symmetric Band Matrices

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

Real Symmetric Toeplitz Matrices

$$\begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{N-1} \\ b_1 & b_0 & b_1 & \cdots & b_{N-2} \\ b_2 & b_1 & b_0 & \cdots & b_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{N-1} & b_{N-2} & b_{N-3} & \cdots & b_0 \end{pmatrix}$$

Dependence on p, Rates of Convergence, Non-independent entries

Open Problems (NT)

Primes in Congruence Classes:

Improving support for Dirichlet L-fns related to size of $\pi_{m,1}(x) - \frac{\pi(x)}{\phi(m)}$.

Identifying Classical Compact Group:

In function field know what the corresponding RMT group is; little known for GL_n L-fns.

Montgomery-Odlyzko Law:

Numerical observation that zeros of L-fns at height T behave like eigenvalues of $N \times N$ matrices with $N = \log \frac{T}{2\pi}$.

Finite Height / Finite Family Size:

Know correct model for high zeros ($N = \log \frac{T}{2\pi}$); what is the correct model for zeros near the central point as conductor tends to infinity?

APPENDIX I: 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

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

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.

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

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):

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

Note can pass Character Sum through Test Function.

Character Sums

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

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

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

First Sum

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

No contribution if $\sigma < 2$.

Second Sum

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

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

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

$$\begin{aligned}
&\ll \frac{1}{m-2}\sum_p^{m^{\sigma/2}} p^{-1} + \frac{2m-2}{m-2}\sum_{p\equiv\pm1(m)}^{m^{\sigma/2}} p^{-1} \\
&\ll \frac{1}{m-2}\sum_k^{m^{\sigma/2}} k^{-1} + \sum_{\substack{k\equiv1(m)\\k\geq m+1}}^{m^{\sigma/2}} k^{-1} + \sum_{\substack{k\equiv-1(m)\\k\geq m-1}}^{m^{\sigma/2}} k^{-1} \\
&\ll \frac{\log(m^{\sigma/2})}{m-2} + \frac{1}{m}\sum_k^{m^{\sigma/2}} k^{-1} + \frac{1}{m}\sum_k^{m^{\sigma/2}} k^{-1} + O\left(\frac{1}{m}\right) \\
&\ll \frac{\log m}{m} + \frac{\log m}{m} + \frac{\log m}{m}.
\end{aligned}$$

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

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

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

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 $(k_1, k_2, \ldots, k_s)$ 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

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

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 $m/M_2 \le 3^r$, $s = 0$ 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:

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

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

Second Sum Bounds:

Handle similarly as before. Say

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

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

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

APPENDIX II:
Elliptic Curve L-Functions

Excess Rank

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

For many families, observe

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

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):

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

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

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

Testing RMT Model

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

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

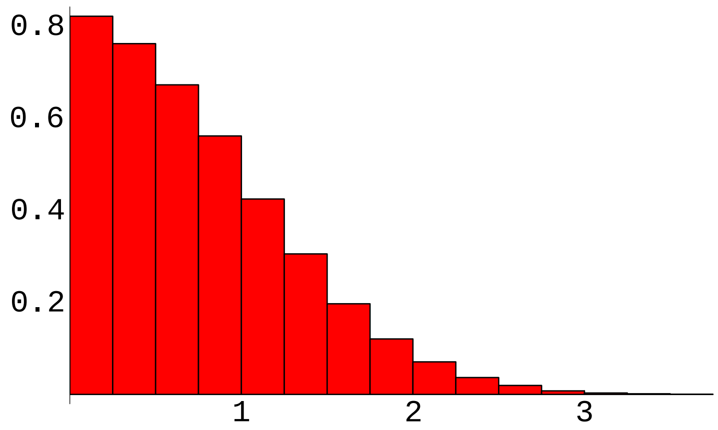
If r zeros at central point, if repulsion of zeros is of size $\frac{c_r}{\log N_E}$, might detect in 1-level density:

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

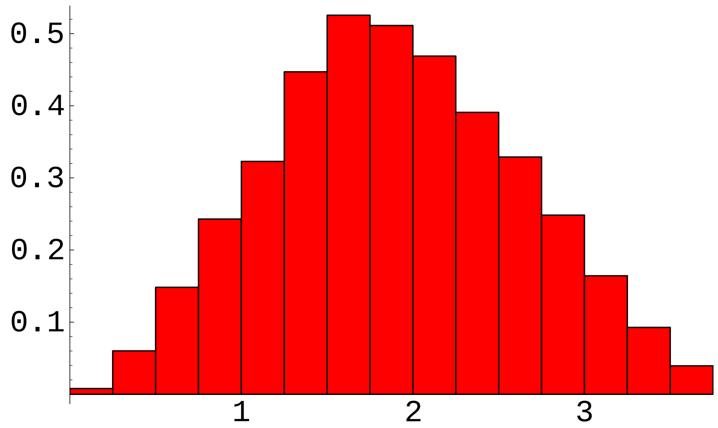
Corrections of size

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

Theoretical Distribution of First Normalized Zero



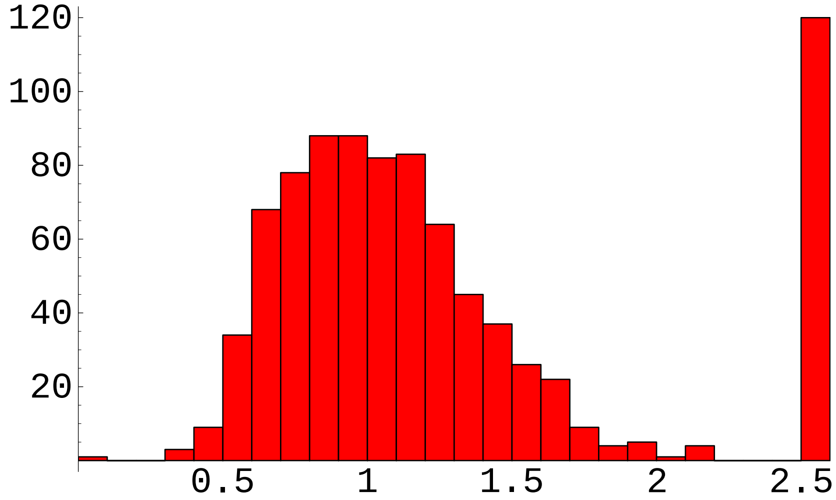
First normalized eigenvalue: 230,400 from SO(6) with Haar Measure



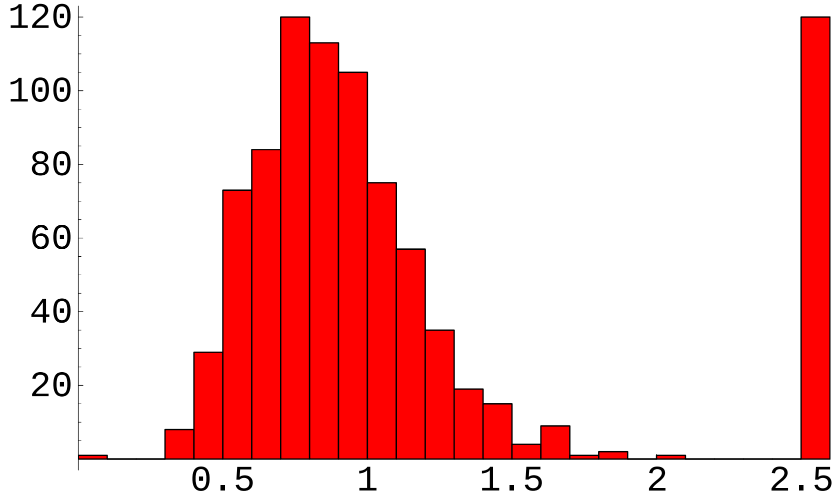
First normalized eigenvalue: 322,560 from SO(7) with Haar Measure

Rank 0 Curves: 1st Normalized Zero

(Far left and right bins just for formatting)

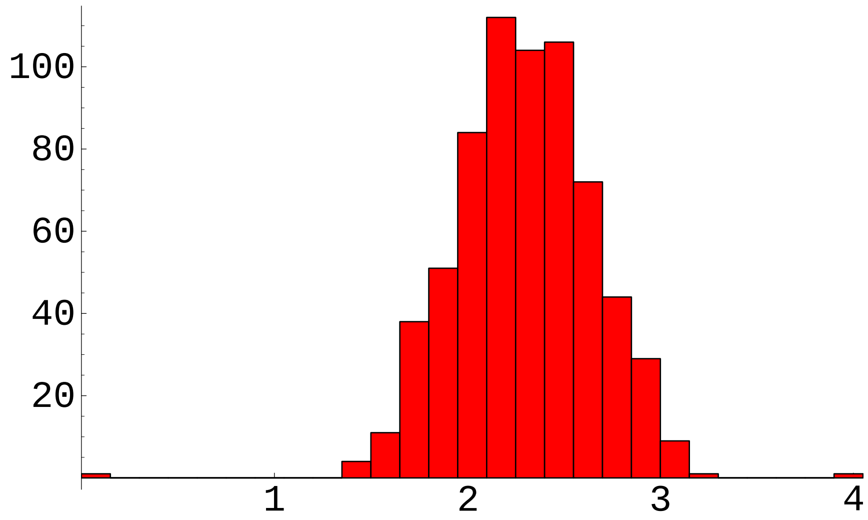


750 curves, $\log(\text{cond}) \in [3.2, 12.6]$; mean $= 1.04$

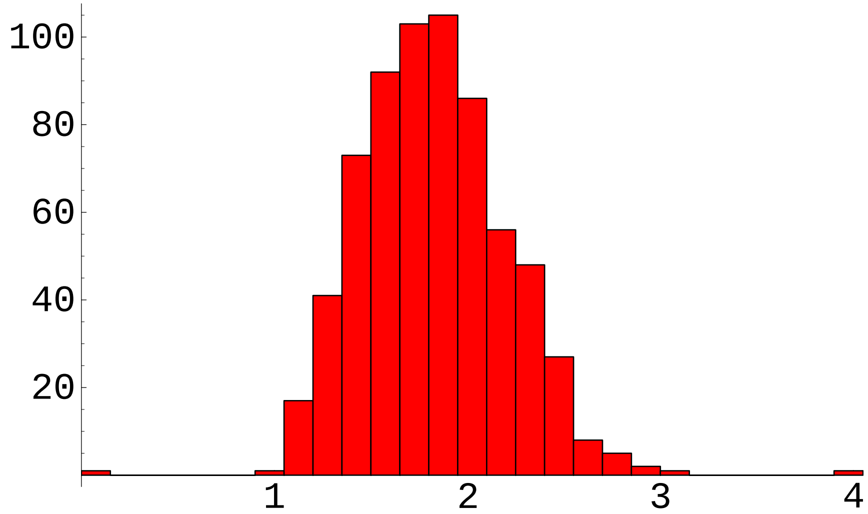


750 curves, $\log(\text{cond}) \in [12.6, 14.9]$; mean $= .88$

Rank 2 Curves: 1st Normalized Zero

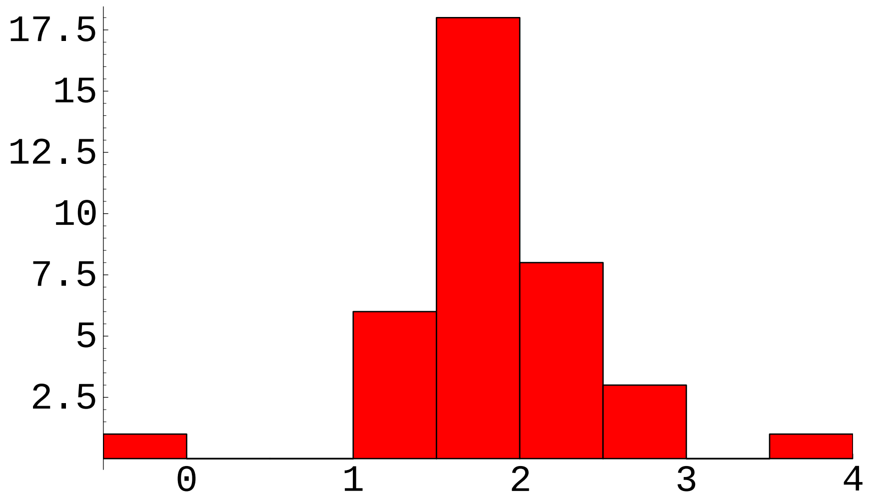


665 curves, $\log(\text{cond}) \in [10, 10.3125]$; mean $= 2.30$

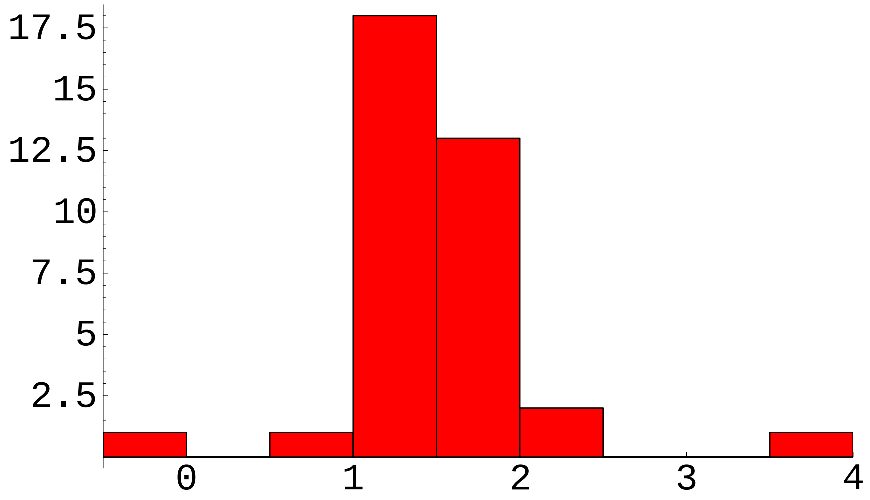


665 curves, $\log(\text{cond}) \in [16, 16.5]$; mean $= 1.82$

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 $= 2.00$

APPENDIX III:
Bibliography

Bibliography

[Bai] Z. Bai, *Methodologies in spectral analysis of large-dimensional random matrices, a review*, Statist. Sinica **9** (1999), no. 3, 611-677.

[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, $79-108$.

[Bol] B. Bollobás, *Random Graphs*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 2001.

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: 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, $375-382$.

[BDJ] W. Bryc, A. Dembo, T. Jiang, *Spectral Measure of Large Randm Hankel, Markov and Toeplitz Matrices*, preprint.

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

[Con] J. B. Conrey, *L-functions and Random Matrices*.

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

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

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

[DM] E. Dueñez and S. J. Miller, *The Low-Lying Zeros of a GL_6 Family*, preprint.

[Dy1] F. Dyson, *Statistical theory of the energy levels of complex systems: I, II, III*,. J. Mathematical Phys., **3**, 1962,140Ű156, 157-165, 166-175.

[Dy2] F. Dyson, *The threefold way. Algebraic structure of symmetry groups and ensembles in quantum mechanics*, J. Mathematical Phys., **3**, 1962, 1199Ű1215.

[Ed] H. M. Edwards, *Riemann's Zeta Function*, Academic Press, Inc., 1974.

[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.

[FSV] P. J. Forrester, N. C. Snaith and J. J. M. Verbaarschot, *Developments in Random Matrix Theory*.

[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.

[GV] D. A. Goldston and R. C. Vaughan, *On the Montgomery-Hooley asymptotic formula*, Sieve methods, exponential sums and their applications in number theory (ed. G. R. H. Greaves, G. Harman and M. N. Huxley, Cambridge University Press, 1996), 117-142.

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

[HM] C. Hammond and S. J. Miller, *Eigenvalue spacing distribution for the ensemble of real symmetric Toeplitz matrices*, to appear in the Journal of Theoretical Probability.

[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.

[HuMi] C. Hughes and S. J. Miller, *Low-lying zeros of L–functions with orthogonal symmetry*, preprint.

[HuRu1] C. Hughes and Z. Rudnick, *Mock Gaussian behaviour for linear statistics of classical compact groups*, J. Phys. A **36**, (2003) 2919–2932.

[HuRu2] C. Hughes and Z. Rudnick, *Linear Statistics of Low-Lying Zeros of L-functions*, Quart. J. Math. Oxford **54**, (2003), 309–333.

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

[JMRR] D. Jakobson, S. D. Miller, I. Rivin and Z. Rudnick, *Eigenvalue spacings for regular graphs*, Emerging applications of number theory (Minneapolis, MN, 1996), $317-327$.

[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, $1-26$.

[KeSn] J. P. Keating and N. C. Snaith, *Random matrices and L-functions*,

[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, $847-862$.

[McK] B. McKay, *The expected eigenvalue distribution of a large regular graph*, Linear Algebra Appl. 40 (1981), $203-216$.

[Meh1] M. Mehta, *On the statistical properties of level spacings in nuclear spectra*, Nucl. Phys. 18, 1960, 395-.

[Meh2] M. Mehta, *Random Matrices, 2nd edition*, Academic Press Inc., Boston, 1991.

[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.brown.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 **104**, (2004), 952–992.

[Mil3] S. J. Miller, 1-*Level Density for Square-Free Dirichlet Characters*, preprint.

[Mon1] H. Montgomery, *Prime's in arithmetic progression*, Michigan Math. J. 17 (1970), 33-39.

[Mon2] H. Montgomery, *The pair correlation of zeros of the zeta function*, Analytic Number Theory, Proc. Sympos. Pure Math. **24**, Amer. Math. Soc., Providence, 1973, $181 - 193$.

[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, $13 - 32$.

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

[Od2] A. Odlyzko, *The* 10^{22}-*nd zero of the Riemann zeta function*, Proc. Conference on Dynamical, Spectral and Arithmetic Zeta-Functions, M. van Frankenhuysen and M. L. Lapidus, eds., Amer. Math. Soc., Contemporary Math. series, 2001, http://www.research.att.com/∼amo/doc/zeta.html

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

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

[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, $43 - 67$.

[Ru1] 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.

[Rub2] M. Rubinstein, *Low-lying zeros of* L-*functions and random matrix theory*, Duke Math. J. **109** (2001), no. 1, 147–181.

[RubSa] M. Rubinstein and P. Sarnak, *Chebyshev's bias*, Experiment. Math. 3 (1994), no. 3, 173-197.

[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, $227-236$.

[Sosh] A. Soshnikov, *Central limit theorem for local linear statistics in classical compact groups and related combinatorial identities*, Ann. Probab. **28** (2000), 1353–1370.

[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, $553-572$.

[TrWi] C. Tracy and H. Widom, *Correlation functions, cluster functions, and spacing distributions for random matrices*, J. Statist. Phys., **92** (5-6), 1998, 809Ű835.

[Va] R. C. Vaughan, *On a variance associated with the distribution of primes in arithmetic progression*, Proc. London Math. Soc. (3) **82** (2001), 533-553.

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

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

[Wig2] E. Wigner, *Characteristic vectors of bordered matrices with infinite dimensions*, Ann. of Math. **2**, 62, 1955, 548Ű564.

[Wig3] E. Wigner, *Statistical Properties of real symmetric matrices*, Canadian Mathematical Congress Proceedings, University of Toronto Press, Toronto, 1957, 174-184.

[Wig4] E. Wigner, *Characteristic vectors of bordered matrices with infinite dimensions. II*, Ann. of Math. **2**, 65, 1957, 203Ű207.

[Wig5] E. Wigner, *On the distribution of the roots of certain symmetric matrices. Ann. of Math*, **2**, 67, 1958, 325Ű327.

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

[Wom] N. C. Wormald, *Models of random regular graphs*.

[Za] I. Zakharevich, *A Generalization of Wigner's Law*, preprint.