From Nuclear Physics to Number Theory

How the Manhattan Project Helps us Understand Primes and Elliptic Curves

Steven J. Miller

Brown University

University of Connecticut, March 24^{th}, 2005
http://www.math.brown.edu/$\sim$sjmiller

Acknowledgments

Random Matrices (with Peter Sarnak)

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

Elliptic Curves (with Eduardo Dueñez)

- Adam O'Brien
- Aaron Lint

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 Primes.
- Spacings between Energy Levels of Nuclei.
- Spacings between Eigenvalues of Matrices.
- Spacings between 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.

- Predictive power of Random Matrix Theory: suggests answers for questions in Number Theory.

PART I

NORMALIZED SPACINGS

Example: Fractional Parts

- For $\alpha \notin \mathbb{Q}$, set $x_n = n^2\alpha \bmod 1$.

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

Example: Fractional Parts

- For $\alpha \notin \mathbb{Q}$, set $x_n = n^2\alpha \bmod 1$.

- 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 $\frac{1}{N}$.

Example: Fractional Parts

- For $\alpha \notin \mathbb{Q}$, set $x_n = n^2\alpha \bmod 1$.

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

- Poissonian behavior for most α:
  behave like N numbers chosen uniformly in $[0, 1]$.

Example: Primes

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

Example: Primes

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

- Average spacing between primes at most x is $\frac{x}{\pi(x)} \ \sim \log x$.

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

Example: Primes

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

- Average spacing between primes at most x is $\frac{x}{\pi(x)} \sim \log x$.

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

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

Example: Primes

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

- Average spacing between primes at most x is $\frac{x}{\pi(x)} \sim \log x$.

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

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

  Aside: (Nicely 1994) Twin primes led to finding the Pentium bug!

$$\sum_{\substack{p \\ p,p+2 \text{ prime}}} \left(\frac{1}{p} + \frac{1}{p+2}\right) \approx 1.90216058.$$

Poisson Process: Spacings between Primes

Observation: See similar behavior in spacings between normalized fractional parts $n^2\alpha \bmod 1$ and normalized primes.

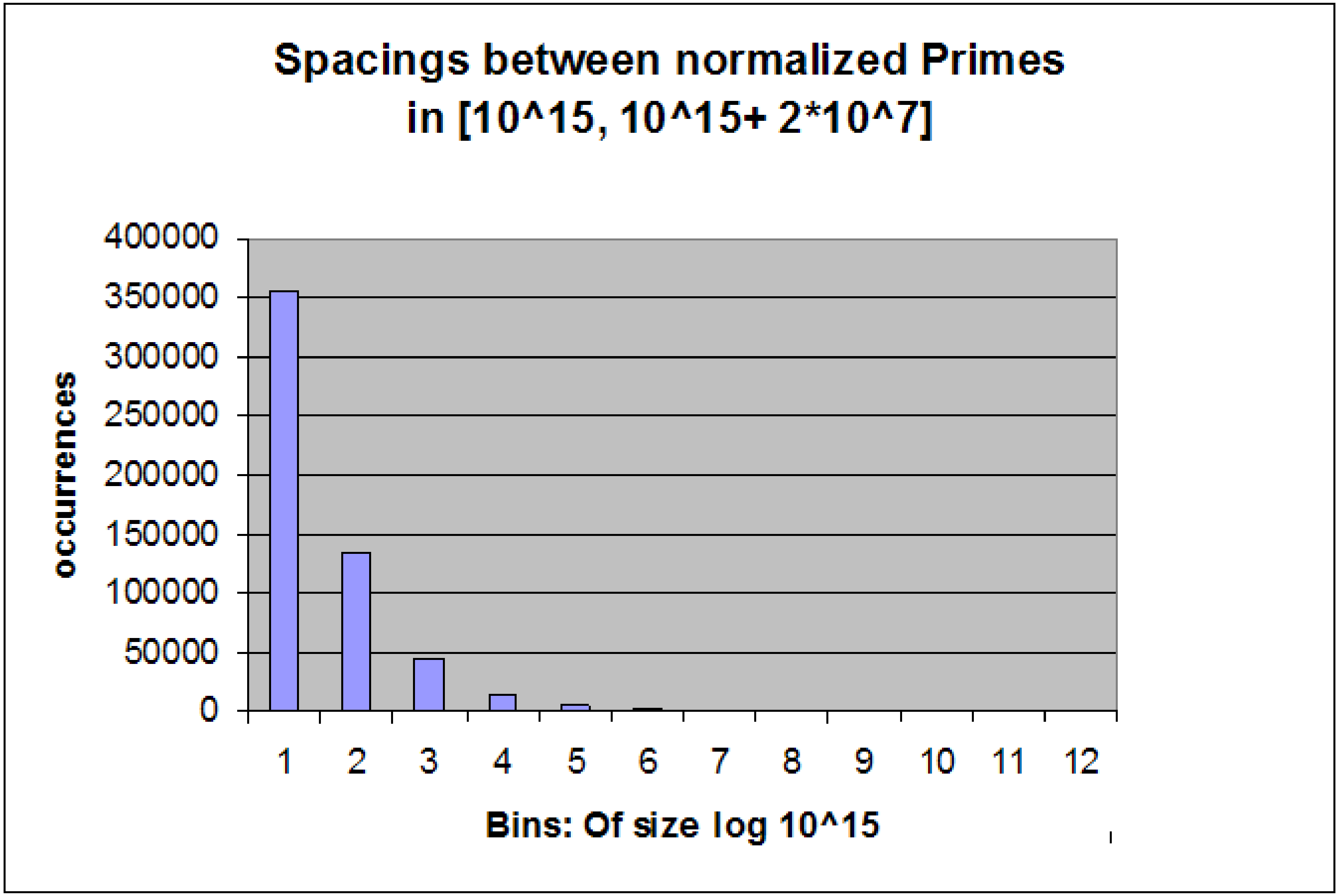
Poisson Process: Spacings between Primes

Observation: See similar behavior in spacings between normalized fractional parts $n^2\alpha \bmod 1$ and normalized primes.

Study spacings between normalized adjacent primes in $I = [10^{15}, 10^{15} + 2 \cdot 10^7]$.

Numerically observe and conjecture that as $|I| \to \infty$

$$\frac{\#\left\{p_i \in I : \frac{p_{i+1}}{\log p_{i+1}} - \frac{p_i}{\log p_i} \in [\alpha, \beta]\right\}}{\#\{p_i \in I\}} \longrightarrow \int_\alpha^\beta e^{-x} dx.$$


Spacings between normalized Primes
in [10^15, 10^15+ 2*10^7]
occurrences
400000
350000
300000
250000
200000
150000
100000
50000
0
1
2
3
4
5
6
7
8
9
10
11
12
Bins: Of size log 10^15

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!

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.

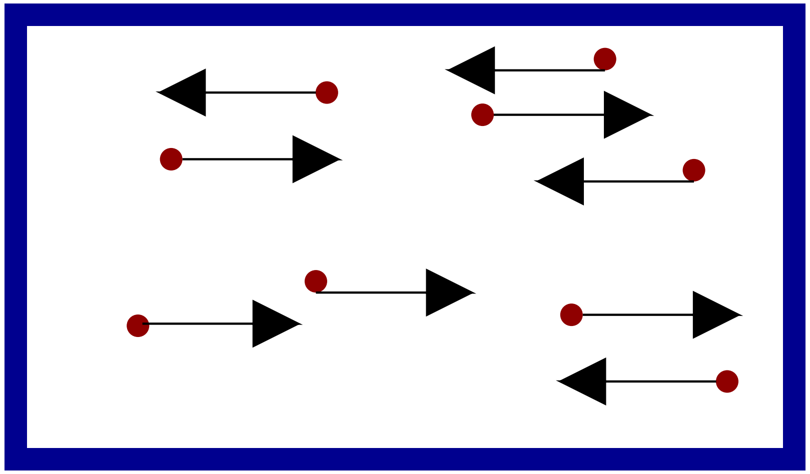
Heavy nuclei like Uranium ($200+$ protons / neutrons) even worse!

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

Fundamental Equation: $H\psi_n = E_n\psi_n$

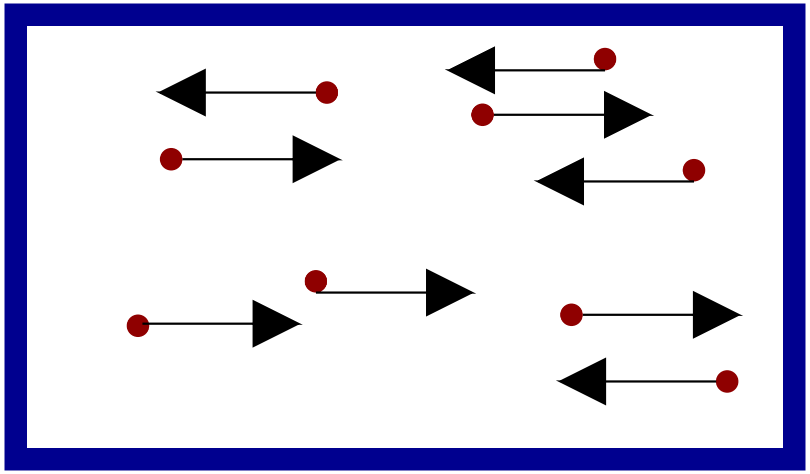
$$\begin{aligned} H &: \text{matrix, entries depend on system} \\ E_n &: \text{energy levels} \\ \psi_n &: \text{energy eigenfunctions} \end{aligned}$$

Origins of Random Matrix Theory (continued)



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

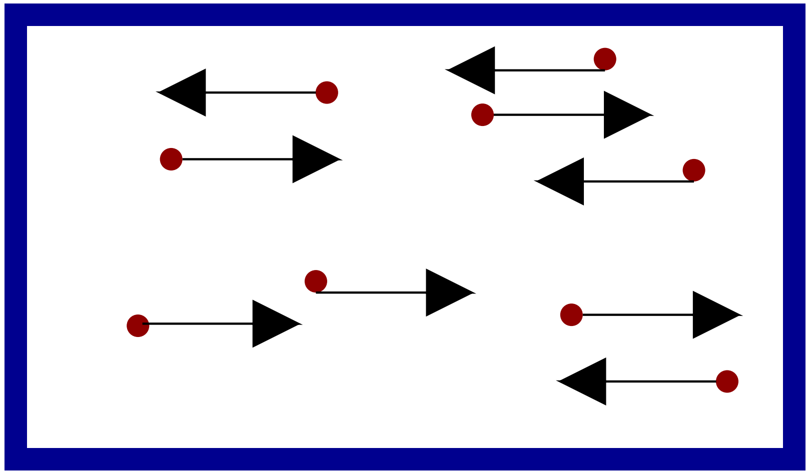
Origins of Random Matrix Theory (continued)



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

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

Origins of Random Matrix Theory (continued)

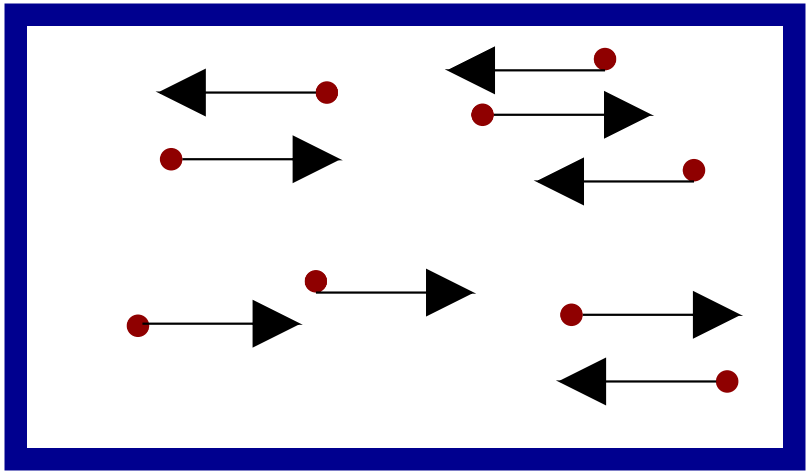


Statistical Mechanics: for each configuration, calculate quantity (say pressure).

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

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

Origins of Random Matrix Theory (continued)



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

Random Matrix Ensembles

Real Symmetric Matrices:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1N} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & a_{N3} & \cdots & a_{NN} \end{pmatrix} = A^T, \quad a_{ij} = a_{ji}, \ \lambda_i \in \mathbb{R}.$$

Random Matrix Ensembles

Real Symmetric Matrices:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1N} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2N} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & a_{N3} & \cdots & a_{NN} \end{pmatrix} = A^T, \quad a_{ij} = a_{ji},\ \lambda_i \in \mathbb{R}.$$

Define

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

Want to understand eigenvalues of randomly chosen A.

MAIN TOOL: Eigenvalue Trace Lemma

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

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

MAIN TOOL: Eigenvalue Trace Lemma

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

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

- Will give correct normalization for zeros;
- Allows us to pass from knowledge of matrix entries to knowledge of eigenvalues.

Correct Scale for Eigenvalues of Real Symmetric Matrices
Entries chosen from Mean 0, Variance 1 Density

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

Correct Scale for Eigenvalues of Real Symmetric Matrices
Entries chosen from Mean 0, Variance 1 Density

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

By the Central Limit Theorem:

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

Correct Scale for Eigenvalues of Real Symmetric Matrices
Entries chosen from Mean 0, Variance 1 Density

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

By the Central Limit Theorem:

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

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

Correct Scale for Eigenvalues of Real Symmetric Matrices Entries chosen from Mean 0, Variance 1 Density

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

By the Central Limit Theorem:

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

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

Gives NAverage$(\lambda_i(A)^2) \sim N^2$ or Average$(\lambda_i(A)) \sim \sqrt{N}$.

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.

For each $N \times N$ matrix 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.

For each $N \times N$ matrix 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,

$$\int_{\alpha}^{\beta} \mu_{A,N}(x)dx \;=\; \frac{\#\left\{\lambda_i : \frac{\lambda_i(A)}{2\sqrt{N}} \;\in\; [\alpha, \beta]\right\}}{N}.$$

Eigenvalue Distribution

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

For each $N \times N$ matrix 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,

$$\int_\alpha^\beta \mu_{A,N}(x)dx \;=\; \frac{\#\left\{\lambda_i : \frac{\lambda_i(A)}{2\sqrt{N}} \;\in\; [\alpha,\beta]\right\}}{N}.$$

$$k^{\text{th}} \text{ Moment of } \mu_{A,N} \;=\; \frac{1}{N}\sum_{i=1}^{N}\frac{\lambda_i(A)^k}{(2\sqrt{N})^k} \;=\; \frac{\text{Trace}(A^k)}{2^k N^{\frac{k}{2}+1}}.$$

Wigner's Semi-Circle Law

$N \times N$ real symmetric matrices, upper triangular entries independently chosen from a fixed probability density p on $\mathbb{R}$.

$$\int_\alpha^\beta \mu_{A,N}(x)dx \;=\; \frac{\#\left\{\lambda_i : \frac{\lambda_i(A)}{2\sqrt{N}} \;\in\; [\alpha,\beta]\right\}}{N}.$$

Wigner's Semi-Circle Law

$N \times N$ real symmetric matrices, upper triangular entries independently chosen from a fixed probability density p on $\mathbb{R}$.

$$\int_\alpha^\beta \mu_{A,N}(x)dx \;=\; \frac{\#\left\{\lambda_i : \frac{\lambda_i(A)}{2\sqrt{N}} \in [\alpha,\beta]\right\}}{N}.$$

THEOREM: Wigner's Semi-Circle Law: Assume p has mean 0, variance 1, other moments finite. As $N \to \infty$, almost all A have $\mu_{A,N}$ close to the Semi-Circle density

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

Wigner's Semi-Circle Law

$N \times N$ real symmetric matrices, upper triangular entries independently chosen from a fixed probability density p on $\mathbb{R}$.

$$\int_\alpha^\beta \mu_{A,N}(x)dx \;=\; \frac{\#\left\{\lambda_i : \frac{\lambda_i(A)}{2\sqrt{N}} \in [\alpha,\beta]\right\}}{N}.$$

THEOREM: Wigner's Semi-Circle Law: Assume p has mean 0, variance 1, other moments finite. Then as $N \to \infty$ almost all A have $\mu_{A,N}$ close to the Semi-Circle density

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

Technical: As $N \to \infty$ with probability one the Kolmogorov-Smirnov discrepency between $\mu_{A,N}$ and S tends to zero.

$$\mathrm{Disc}(\mu_{A,N}, S) \;=\; \sup_x \left| \int_{-\infty}^x \mu_{A,N}(t)dt - \int_{-\infty}^x S(t)dt \right|$$

Proof of Wigner's Semi-Circle Law

1. Eigenvalue Trace Lemma $\left(\text{Trace}(A^k) = \sum_i \lambda_i(A)^k\right)$ converts sums over eigenvalues to sums over entries of A.

2. Expected value of k^{th}-moment of $\mu_{A,N}(x)$ is
$$\int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \frac{\text{Trace}(A^k)}{2^k N^{\frac{k}{2}+1}} \prod_{i \le j} p(a_{ij}) da_{ij}.$$

3. Show the expected value of k^{th}-moment of $\mu_{A,N}(x)$ equals the k^{th}-moment of the Semi-Circle.

Random Matrix Theory: Semi-Circle Experiments

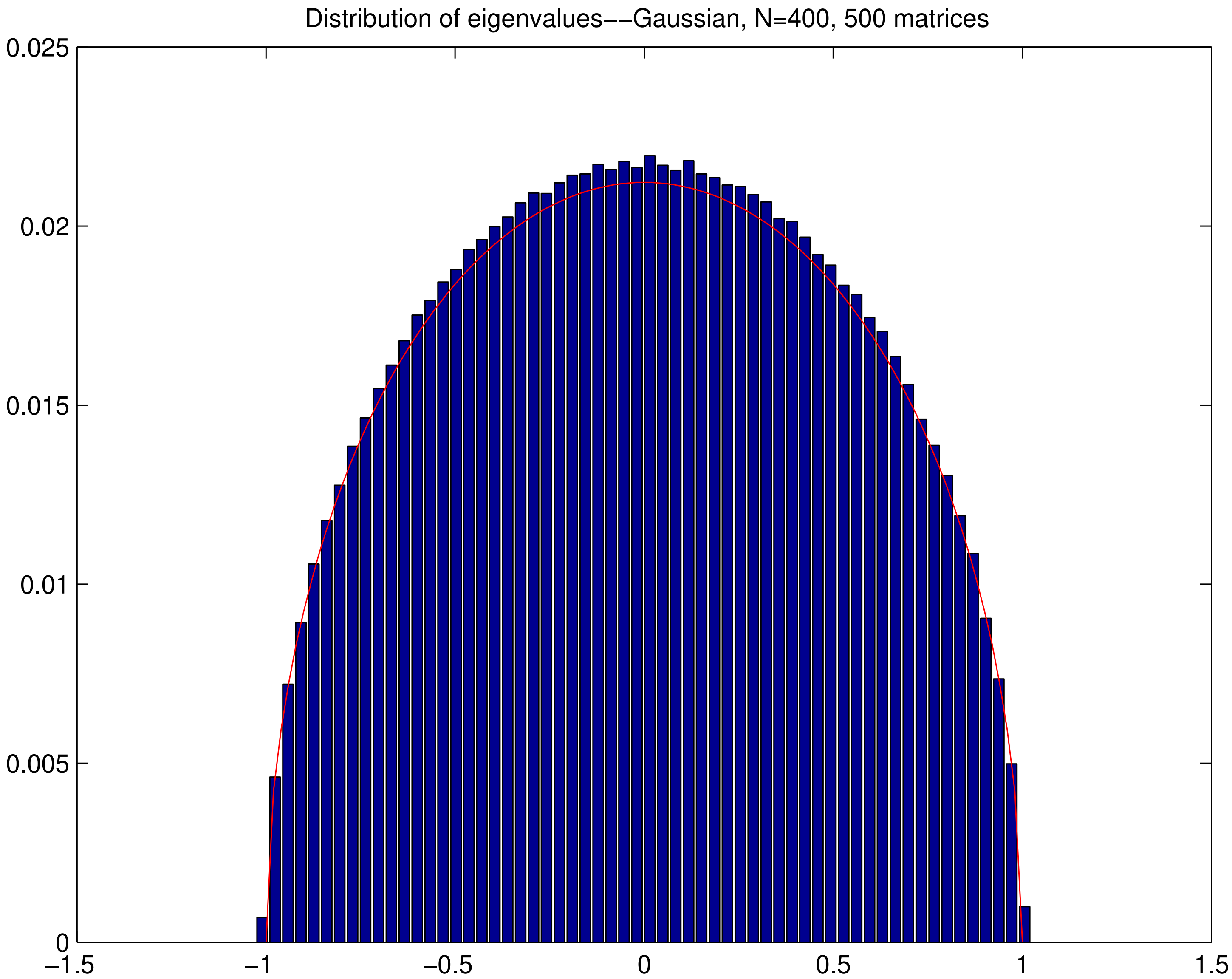
1. Choose a probability distribution p on $\mathbb{R}$.

2. Choose a large N (size of matrices).

3. Look at a large number of $N \times N$ real symmetric matrices, each matrix has its upper triangular entries independently chosen from p.

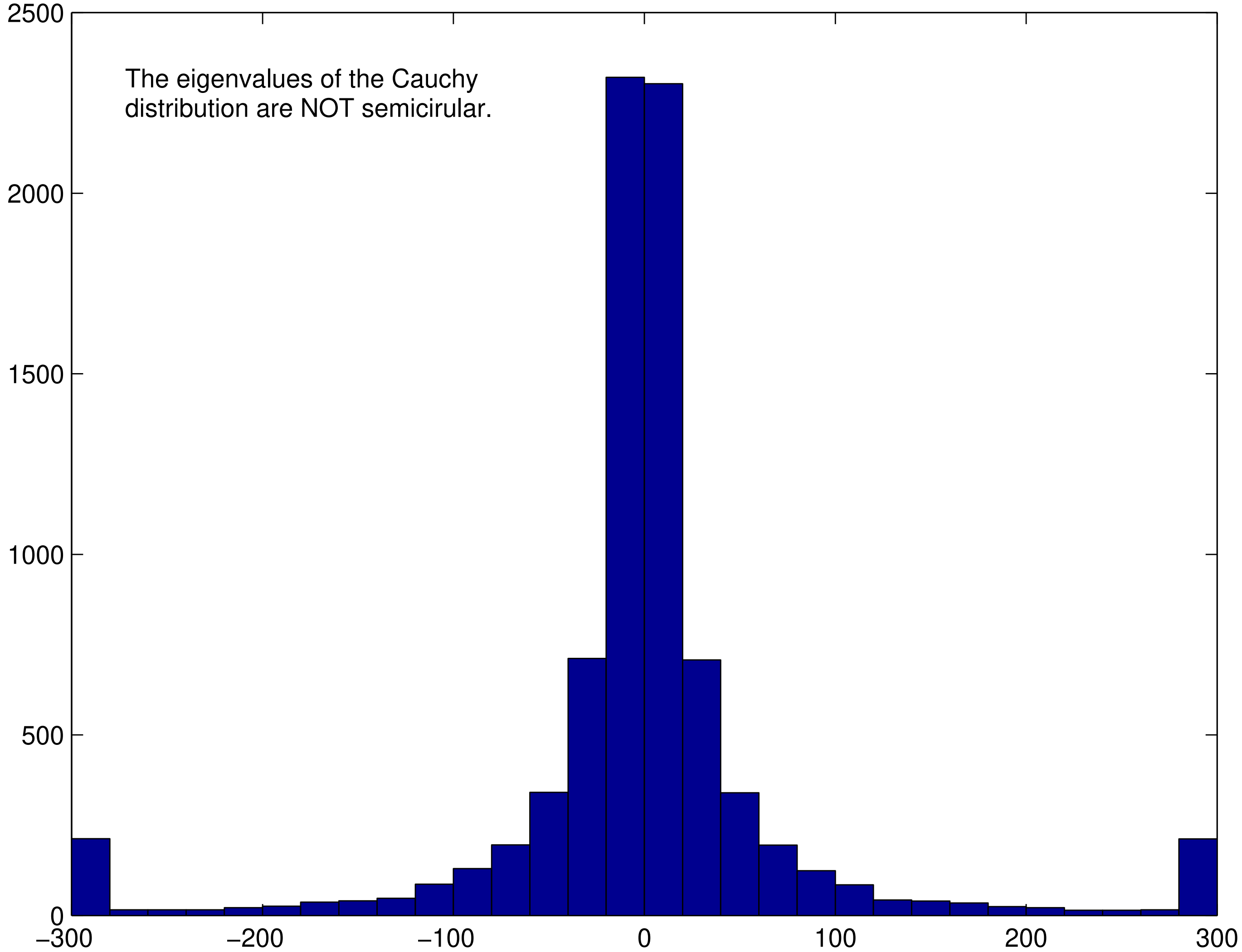
4. Calculate the normalized eigenvalues $\frac{\lambda_i(A)}{2\sqrt{N}}$, investigate their properties.

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 Distribution: $p(x) = \frac{1}{\pi(1+x^2)}$, $x \in \mathbb{R}$

Infinite Variance

Gaussian Orthogonal Ensemble (GOE) Conjecture

Let $\mathrm{GOE}(x) \;\approx\; \frac{\pi}{2}\, x e^{-\frac{\pi}{4}x^2}$.

Gaussian Orthogonal Ensemble (GOE) Conjecture

Let $\mathrm{GOE}(x) \;\approx\; \frac{\pi}{2}\, xe^{-\frac{\pi}{4}x^2}$.

Let p be a probability distribution on $\mathbb{R}$ with mean zero, variance one and finite higher moments.

GOE Conjecture: As $N \to \infty$, for most A the probability density of the spacing between consecutive normalized eigenvalues converges to $\mathrm{GOE}(x)$:

$$\frac{\#\left\{i : \frac{\lambda_{i+1}(A)}{2\sqrt{N}} - \frac{\lambda_i(A)}{2\sqrt{N}} \in [\alpha, \beta]\right\}}{N} \longrightarrow \int_\alpha^\beta \mathrm{GOE}(x)dx.$$

Gaussian Orthogonal Ensemble (GOE) Conjecture

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

Let p be a probability distribution on $\mathbb{R}$ with mean zero, variance one and finite higher moments.

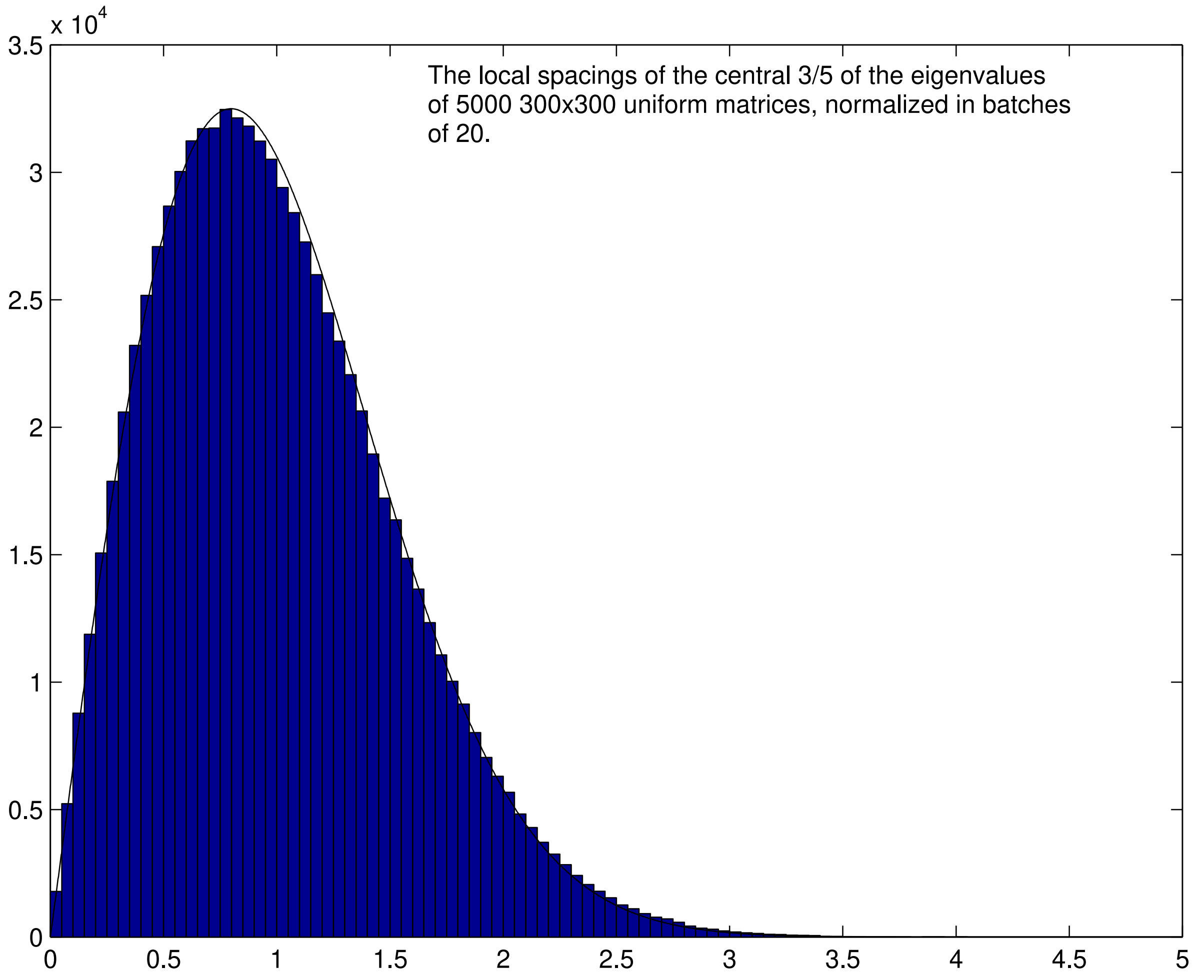
GOE Conjecture: As $N \to \infty$, for most A the probability density of the spacing between consecutive normalized eigenvalues converges to $\text{GOE}(x)$:

$$\frac{\#\left\{i : \frac{\lambda_{i+1}(A)}{2\sqrt{N}} - \frac{\lambda_i(A)}{2\sqrt{N}} \in [\alpha,\beta]\right\}}{N} \longrightarrow \int_\alpha^\beta \text{GOE}(x)dx.$$

Only proved for p a Gaussian with mean 0 and variance 1.

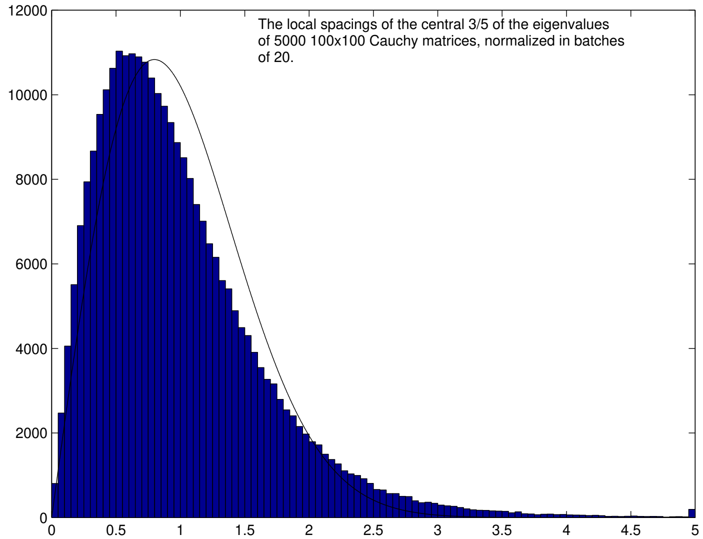
What about numerical data in other cases?

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

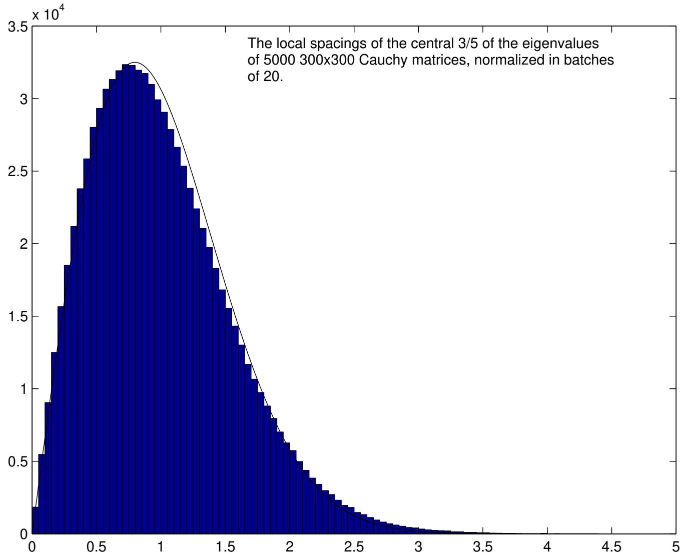


5000: 300×300 **uniform on** $[-1, 1]$

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



5000: 100×100 Cauchy



5000: 300×300 Cauchy

PART III

NUMBER THEORY

IDEA:

Zeros of Random Matrices Provide a Good Model for Zeros of Number Theoretic 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

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

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 (continued):

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

Properties of $\zeta(s)$ and Primes: Proofs that $\pi(x) \to \infty$.

Riemann Zeta Function (continued):

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

Properties of $\zeta(s)$ and Primes: Proofs that $\pi(x) \to \infty$.

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

Riemann Zeta Function (continued):

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

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

Properties of $\zeta(s)$ and Primes: Proofs that $\pi(x) \to \infty$.

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

- $\zeta(2) = \frac{\pi^2}{6}$.

Riemann Zeta Function (continued):

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

Properties of $\zeta(s)$ and Primes: Proofs that $\pi(x) \to \infty$.

- $\lim_{s \to 1^+} \zeta(s) = \infty$.
- $\zeta(2) = \frac{\pi^2}{6}$.
- $\zeta(1 + it) \neq 0$ for $t \in \mathbb{R}$ implies $\pi(x) \sim \frac{x}{\log x}$.

Riemann Zeta Function (continued):

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

Functional Equation:

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

Riemann Zeta Function (continued):

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

Functional Equation:

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

Riemann Hypothesis:

- All zeros have $\mathrm{Re}(s) = \frac{1}{2}$; can write zeros as $\frac{1}{2} + i\gamma, \gamma \in \mathbb{R}$.
- Number of zeros with $0 \leq \gamma \leq T$ is about $T \log T$.

Riemann Zeta Function (continued):

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

Functional Equation:

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

Riemann Hypothesis:

- All zeros have $\mathrm{Re}(s) = \frac{1}{2}$; can write zeros as $\frac{1}{2} + i\gamma, \gamma \in \mathbb{R}$.
- Number of zeros with $0 \le \gamma \le T$ is about $T \log T$.

Observation:

- Spacings between normalized zeros appear same as between normalized eigenvalues of Complex Hermitian matrices $(\overline{A}^T = A)$.

Normalized Zeros of Riemann Zeta Function
Zeros $\frac{1}{2} + i\gamma, \gamma \in \mathbb{R}$

Know $\#\{\gamma : 0 \leq \gamma \leq T\}$ is about $T \log T$.

Normalized Zeros of Riemann Zeta Function
Zeros $\frac{1}{2} + i\gamma, \gamma \in \mathbb{R}$

Know $\#\{\gamma : 0 \leq \gamma \leq T\}$ is about $T \log T$.

Average spacing of zeros with $\gamma \sim T$ is $\frac{T}{T \log T} = \frac{1}{\log T}$.

Contrast with primes: Average spacing of primes $p \sim x$ is $\frac{x}{x/\log x} = \log x$.

Normalized Zeros of Riemann Zeta Function
Zeros $\frac{1}{2} + i\gamma, \gamma \in \mathbb{R}$

Know $\#\{\gamma : 0 \le \gamma \le T\}$ is about $T \log T$.

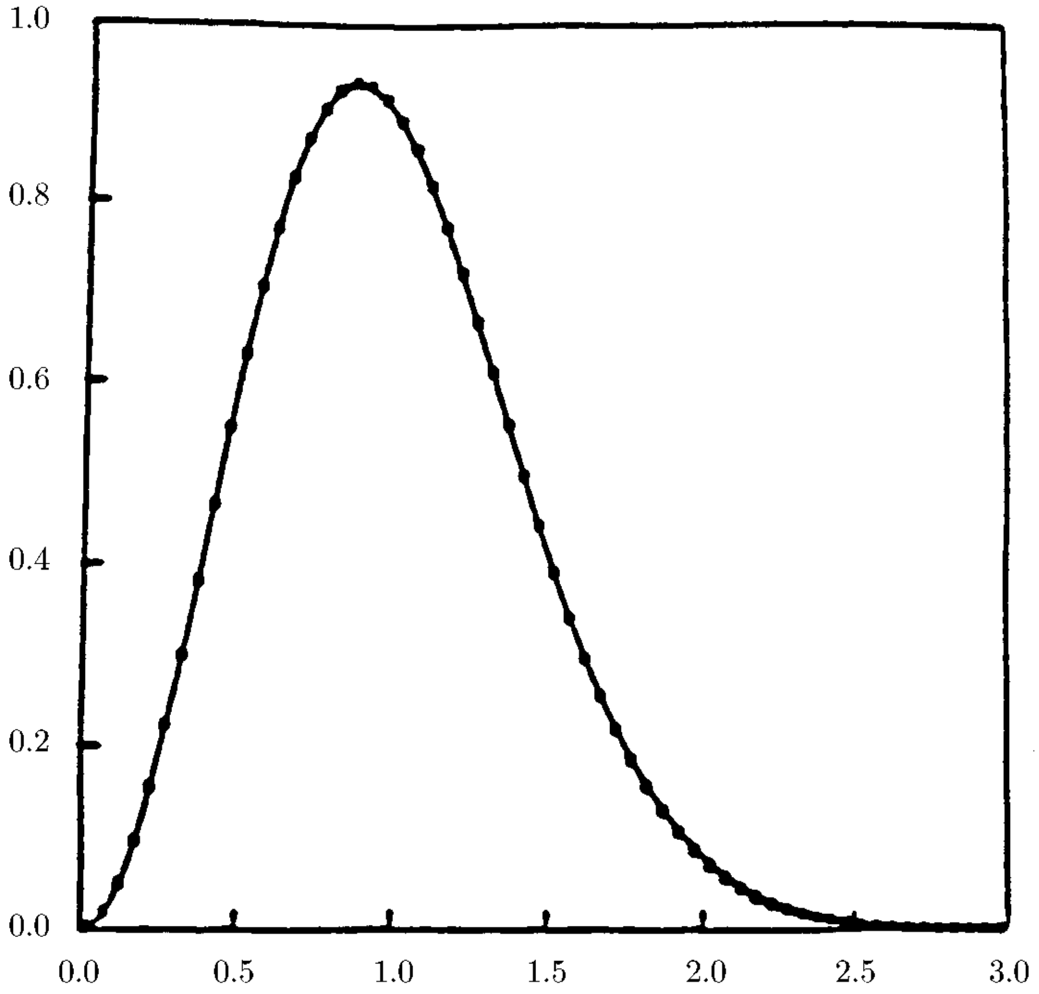
Average spacing of zeros with $\gamma \sim T$ is $\frac{T}{T \log T} = \frac{1}{\log T}$.

Contrast with primes: Average spacing of primes $p \sim x$ is $\frac{x}{x/\log x} = \log x$.

Normalized zeros: study $\gamma_{n+1} \log \gamma_{n+1} - \gamma_n \log \gamma_n$.

Contrast with primes, where we studied $\frac{p_{n+1}}{\log p_{n+1}} - \frac{p_n}{\log p_n}$.

Zeros of $\zeta(s)$ vs. GUE(x):



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

General L-Functions

- **Euler Product:**

$$L(s) \ := \ \sum_{n=1}^{\infty} \frac{a_n}{n^s} \ = \ \prod_p \frac{1}{L_p(p^{-s})}, \quad \mathrm{Re}(s) \gg 0, \ L_p(x) = \text{polynomial}.$$

General L-Functions

- **Euler Product:**

$$L(s) \;:=\; \sum_{n=1}^{\infty} \frac{a_n}{n^s} \;=\; \prod_p \frac{1}{L_p(p^{-s})}, \quad \mathrm{Re}(s) \gg 0, \; L_p(x) = \text{polynomial}.$$

- **Functional Equation:**

$$\begin{aligned} \Lambda(s) \;&:=\; (\Gamma - \text{Factors}) \cdot L(s) \\ \Lambda(s) \;&=\; \frac{\varepsilon(s)}{C^s}\overline{\Lambda(1-\overline{s})}, \; C > 0 \text{ is the Conductor} \end{aligned}$$

General L-Functions

- **Euler Product:**

$$L(s) \ := \ \sum_{n=1}^{\infty} \frac{a_n}{n^s} \ = \ \prod_p \frac{1}{L_p(p^{-s})}, \quad \text{Re}(s) \gg 0, \ L_p(x) = \text{polynomial.}$$

- **Functional Equation:**

$$\begin{aligned} \Lambda(s) \ &:= \ (\Gamma - \text{Factors}) \cdot L(s) \\ \Lambda(s) \ &= \ \frac{\varepsilon(s)}{C^s}\overline{\Lambda(1-\overline{s})}, \ C > 0 \text{ is called the Conductor} \end{aligned}$$

- **Riemann Hypothesis:**
All zeros have $\text{Re}(s) = \frac{1}{2}$; can write zeros as $\frac{1}{2} + i\gamma, \gamma \in \mathbb{R}$.

General L-Functions

- **Euler Product:**

$$L(s) \ := \ \sum_{n=1}^{\infty} \frac{a_n}{n^s} \ = \ \prod_p \frac{1}{L_p(p^{-s})}, \quad \mathrm{Re}(s) \gg 0,\ L_p(x) = \text{polynomial}.$$

- **Functional Equation:**

$$\begin{aligned} \Lambda(s) \ &:= \ (\Gamma - \text{Factors}) \cdot L(s) \\ \Lambda(s) \ &= \ \frac{\varepsilon(s)}{C^s} \overline{\Lambda(1-\overline{s})},\ C > 0 \text{ is called the Conductor} \end{aligned}$$

- **Riemann Hypothesis:**
  All zeros have $\mathrm{Re}(s) = \frac{1}{2}$; can write zeros as $\frac{1}{2} + i\gamma, \gamma \in \mathbb{R}$.

- **Number of Zeros:**

$$\text{Number of zeros with } \gamma \sim T \text{ is like } T \log T$$

$$\text{Zeros near } s = \frac{1}{2} \text{ have } \gamma \sim \frac{1}{\log C}$$

(Heuristic): Knowledge of Zeros

$P(x)$ 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 of $P(x)$.

Explicit Formula / Contour Integration: Analogue of Eigenvalue Trace Lemma

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

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 the L-function coefficients.

Interesting L-Functions

What makes an L-Function interesting?

Interesting L-Functions

What makes an L-Function interesting?

- Coefficients a_n of arithmetic significance.
- Look for L-Functions with multiple zeros:
  - Conjectured that all zeros are simple except for deep reasons;
  - Do multiple zeros attract or repel nearby zeros?

Interesting L-Functions

What makes an L-Function interesting?

- Coefficients a_n of arithmetic significance.
- Look for L-Functions with multiple zeros:
    - Conjectured that all zeros are simple except for deep reasons;
    - Do multiple zeros attract or repel nearby zeros?

Will see L-Functions of Elliptic Curves are interesting.

Interesting L-Functions

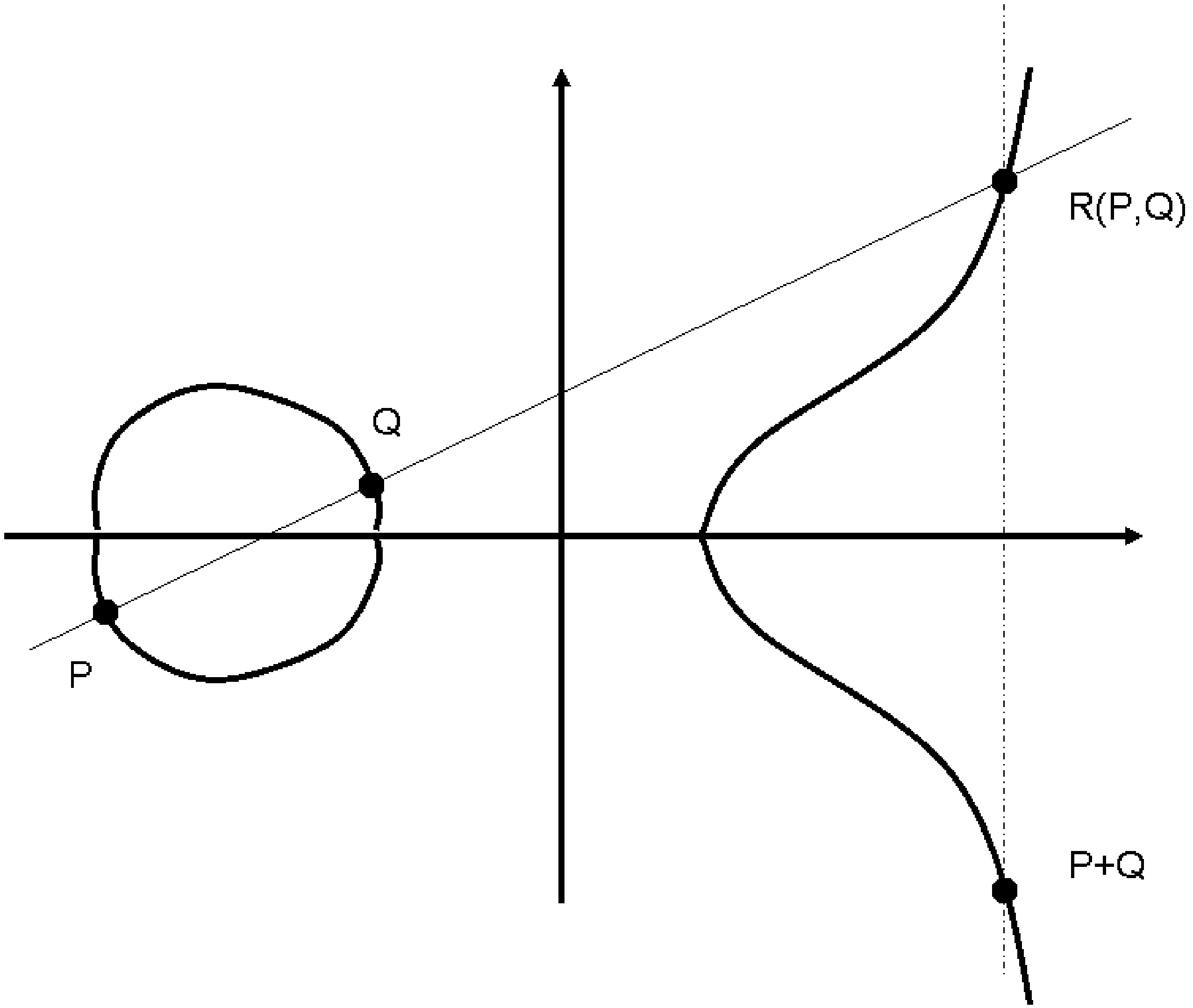
What makes an L-Function interesting?

- Coefficients a_n of arithmetic significance.
- Look for L-Functions with multiple zeros:
  - Conjectured that all zeros are simple except for deep reasons;
  - Do multiple zeros attract or repel nearby zeros?

Will see L-Functions of Elliptic Curves are interesting.

- Many have multiple zeros at $s = \frac{1}{2}$.
- Can investigate if these zeros attract or repel.

Elliptic Curves: E**:** $y^2 = x^3 + Ax + B$



Elliptic Curves: Group of Rational Solutions $E(\mathbb{Q})$

Studying E: $y^2 = x^3 + Ax + B$

Mordell-Weil Theorem: Rational solutions: $E(\mathbb{Q}) = \mathbb{Z}^r \bigoplus$ Finite Group.

Elliptic Curves: Group of Rational Solutions $E(\mathbb{Q})$

Studying E: $y^2 = x^3 + Ax + B$

Mordell-Weil Theorem: Rational solutions: $E(\mathbb{Q}) = \mathbb{Z}^r \bigoplus$ Finite Group.

Question: how does r depend on E?

Elliptic Curves: Group of Rational Solutions $E(\mathbb{Q})$

Studying E: $y^2 = x^3 + Ax + B$

Mordell-Weil Theorem: Rational solutions: $E(\mathbb{Q}) = \mathbb{Z}^r \bigoplus$ Finite Group.

Question: how does r depend on E?

Attach an L-Function to E: As $\zeta(s)$ gives us information on primes, expect L-Function gives us information on E.

Elliptic Curves: Group of Rational Solutions $E(\mathbb{Q})$

Studying E: $y^2 = x^3 + Ax + B$

Mordell-Weil Theorem: Rational solutions: $E(\mathbb{Q}) = \mathbb{Z}^r \bigoplus$ Finite Group.

Question: how does r depend on E?

Attach an L-Function to E: As $\zeta(s)$ gives us information on primes, expect L-Function gives us information on E.

Review: Legendre Symbol: $\left(\frac{0}{p}\right) = 0$ and

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } x^2 \equiv a \bmod p \text{ has two solutions} \\ -1 & \text{if } x^2 \equiv a \bmod p \text{ has no solutions.} \end{cases}$$

Note $1 + \left(\frac{a}{p}\right)$ is the number of solutions to $x^2 \equiv a \bmod p$.

L-Function of an Elliptic Curve $E : y^2 = x^3 + Ax + B$

Let N_p be the number of solutions mod p:

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

L-Function of an Elliptic Curve $E : y^2 = x^3 + Ax + B$

Let N_p be the number of solutions mod p:

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

Local data: $a_p = p - N_p$. Use to build the L-function:

$$L(E, s) \;:=\; \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

L-Function of an Elliptic Curve $E : y^2 = x^3 + Ax + B$

Let N_p be the number of solutions mod p:

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

Local data: $a_p = p - N_p$. Use to build the L-function:

$$L(E, s) := \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Local to Global: $\{a_p\}_{p \text{ prime}} \longleftrightarrow E(\mathbb{Q}) = \mathbb{Z}^r \bigoplus$ Finite Group.

L-Function of an Elliptic Curve $E: y^2 = x^3 + Ax + B$

Let N_p be the number of solutions mod p:

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

Local data: $a_p = p - N_p$. Use to build the L-function:

$$L(E, s) \ := \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Local to Global: $\{a_p\}_{p \text{ prime}} \longleftrightarrow E(\mathbb{Q}) = \mathbb{Z}^r \bigoplus$ Finite Group.

Birch and Swinnerton-Dyer Conjecture: Geometric rank r equals number of zeros of $L(E, s)$ at $s = \frac{1}{2}$. **Possibility of repulsion / attraction from zeros at $s = \frac{1}{2}$!**

Families of Elliptic Curves:

$$\mathcal{E} : y^2 \ = \ x^3 + A(T)x + B(T), \quad A(T), B(T) \in \mathbb{Z}[T].$$

Families of Elliptic Curves:

$$\mathcal{E} : y^2 \;=\; x^3 + A(T)x + B(T), \;\; A(T), B(T) \in \mathbb{Z}[T].$$

Have a FAMILY of L-Functions:

- $t \in \mathbb{Z}$ gives an elliptic curve E_t with conductor C_t.
- $t \in \mathbb{Z}$ gives a family of L-functions $L(E_t, s)$.
- C_t is typically growing polynomially in t.

Families of Elliptic Curves:

$$\mathcal{E} : y^2 \ = \ x^3 + A(T)x + B(T), \quad A(T), B(T) \in \mathbb{Z}[T].$$

Have a FAMILY of L-Functions:

- $t \in \mathbb{Z}$ gives an elliptic curve E_t with conductor C_t.
- $t \in \mathbb{Z}$ gives a family of L-functions $L(E_t, s)$.
- C_t is typically growing polynomially in t.

Similar to RMT where we had many $N \times N$ matrices

- Do E_t from the same family have similar properties?
- $N \to \infty$ becomes $C_t \to \infty$.

Families of Elliptic Curves

Mordell-Weil Theorem for Families:

$$\mathcal{E} : y^2 \ = \ x^3 + A(T)x + B(T), \quad A(T), B(T) \in \mathbb{Z}[T].$$

Families of Elliptic Curves

Mordell-Weil Theorem for Families:

$$\mathcal{E} : y^2 \ = \ x^3 + A(T)x + B(T), \quad A(T), B(T) \in \mathbb{Z}[T].$$

- Group of Rational Function Solutions:

  $P(T) = (x(T), y(T))$.

  $\mathcal{E}(\mathbb{Q}(T)) = \mathbb{Z}^{r(\mathcal{E})} \bigoplus$ Finite Group.

Families of Elliptic Curves

Mordell-Weil Theorem for Families:

$$\mathcal{E} : y^2 \ = \ x^3 + A(T)x + B(T), \quad A(T), B(T) \in \mathbb{Z}[T].$$

- Group of Rational Function Solutions:

  $P(T) = (x(T), y(T))$.

  $\mathcal{E}(\mathbb{Q}(T)) = \mathbb{Z}^{r(\mathcal{E})} \bigoplus$ Finite Group.

- Specialization Theorem: For all $t \in \mathbb{Z}$ sufficiently large: $r(E_t) \geq r(\mathcal{E})$.

Families of Elliptic Curves

Mordell-Weil Theorem for Families:

$$\mathcal{E} : y^2 \ = \ x^3 + A(T)x + B(T), \quad A(T), B(T) \in \mathbb{Z}[T].$$

- Group of Rational Function Solutions:

  $P(T) = (x(T), y(T))$.

  $\mathcal{E}(\mathbb{Q}(T)) = \mathbb{Z}^{r(\mathcal{E})} \bigoplus$ Finite Group.

- Specialization Theorem: For all $t \in \mathbb{Z}$ sufficiently large: $r(E_t) \geq r(\mathcal{E})$.

Questions:

- How does $r(E_t)$ vary in the family?
- How do the zeros of $L(s, E_t)$ vary in the family?

Example of a Family of Elliptic Curves

Consider $\mathcal{E} : y^2 \ = \ x^3 - T^2x + T^4$.

- **Can find some rational solutions by inspection:**
  - $P_1(T) = (T, T^2)$
  - $P_2(T) = (T^2, T^3)$

Example of a Family of Elliptic Curves

Consider $\mathcal{E} : y^2 \;=\; x^3 - T^2x + T^4$.

- **Can find some rational solutions by inspection:**
  - $P_1(T) = (T, T^2)$
  - $P_2(T) = (T^2, T^3)$
  - These points generate infinite part of $\mathcal{E}(\mathbb{Q}(T))$.
  - This means the rank of $\mathcal{E}(\mathbb{Q}(T))$ is 2.

Example of a Family of Elliptic Curves

Consider $\mathcal{E} : y^2 \ = \ x^3 - T^2x + T^4$.

- **Can find some rational solutions by inspection:**
  - $P_1(T) = (T, T^2)$
  - $P_2(T) = (T^2, T^3)$
  - These points generate infinite part of $\mathcal{E}(\mathbb{Q}(T))$.
  - This means the rank of $\mathcal{E}(\mathbb{Q}(T))$ is 2.

- **What is $r(E_t)$ for $t \in \mathbb{Z}$**

Example of a Family of Elliptic Curves

Consider $\mathcal{E} : y^2 \ = \ x^3 - T^2x + T^4$.

- **Can find some rational solutions by inspection:**
  - $P_1(T) = (T, T^2)$
  - $P_2(T) = (T^2, T^3)$
  - These points generate infinite part of $\mathcal{E}(\mathbb{Q}(T))$.
  - This means the rank of $\mathcal{E}(\mathbb{Q}(T))$ is 2.

- **What is $r(E_t)$ for $t \in \mathbb{Z}$**
  - $r(E_1) = 1$. Not surprising as $P_1(1) = P_2(1)$!

Example of a Family of Elliptic Curves

Consider $\mathcal{E} : y^2 \ = \ x^3 - T^2 x + T^4$.

- **Can find some rational solutions by inspection:**
  - $P_1(T) = (T, T^2)$
  - $P_2(T) = (T^2, T^3)$
  - These points generate infinite part of $\mathcal{E}(\mathbb{Q}(T))$.
  - This means the rank of $\mathcal{E}(\mathbb{Q}(T))$ is 2.

- **What is $r(E_t)$ for $t \in \mathbb{Z}$**
  - $r(E_1) = 1$. Not surprising as $P_1(1) = P_2(1)$!
  - $r(E_2) = 2$.

Example of a Family of Elliptic Curves

Consider $\mathcal{E} : y^2 \; = \; x^3 - T^2x + T^4$.

- **Can find some rational solutions by inspection:**
  - $P_1(T) = (T, T^2)$
  - $P_2(T) = (T^2, T^3)$
  - These points generate infinite part of $\mathcal{E}(\mathbb{Q}(T))$.
  - This means the rank of $\mathcal{E}(\mathbb{Q}(T))$ is 2.

- **What is $r(E_t)$ for $t \in \mathbb{Z}$**
  - $r(E_1) = 1$. Not surprising as $P_1(1) = P_2(1)$!
  - $r(E_2) = 2$.
  - $r(E_{42}) = 4$!

L-Functions and Random Matrix Theory

- Spacings between normalized zeros of all "nice" L-functions look like spacings between normalized eigenvalues of complex Hermitian matrices.

L-Functions and Random Matrix Theory

- Spacings between normalized zeros of all "nice" L-functions look like spacings between normalized eigenvalues of complex Hermitian matrices.
  - (GUE Model) Limit as $N \to \infty$ of $N \times N$ complex Hermitian matrices with upper triangular entries independently chosen from the standard normal.
  - Zeros with $\gamma \sim T$ well-modelled by $N \times N$ matrices with $N \sim \log T$.

L-Functions and Random Matrix Theory

- Spacings between normalized zeros of all "nice" L-functions look like spacings between normalized eigenvalues of complex Hermitian matrices.
  - (GUE Model) Limit as $N \to \infty$ of $N \times N$ complex Hermitian matrices with upper triangular entries independently chosen from the standard normal.
  - Zeros with $\gamma \sim T$ well-modelled by $N \times N$ matrices with $N \sim \log T$.

- For a while, seemed this was the only set of matrices relevant to number theory.

L-Functions and Random Matrix Theory

- GUE Model cannot be enough for all of Number Theory:

L-Functions and Random Matrix Theory

- GUE Model cannot be enough for all of Number Theory:
  - Appears to be good for describing behavior of zeros far from $s = \frac{1}{2}$.
  - Insensitive to finitely many zeros.

L-Functions and Random Matrix Theory

- GUE Model cannot be enough for all of Number Theory:
  - Appears to be good for describing behavior of zeros far from $s = \frac{1}{2}$.
  - Insensitive to finitely many zeros.

- Often zeros near $s = \frac{1}{2}$ are interesting:

L-Functions and Random Matrix Theory

- GUE Model cannot be enough for all of Number Theory:
  - Appears to be good for describing behavior of zeros far from $s = \frac{1}{2}$.
  - Insensitive to finitely many zeros.

- Often zeros near $s = \frac{1}{2}$ are interesting:
  - Different types of L-functions have different behavior of zeros near $s = \frac{1}{2}$.
  - Possibility of multiple zeros at $s = \frac{1}{2}$ and attraction or repulsion.
  - Need a theory for these low zeros.

Measures of Spacings:
1-Level Density and Families

Let ϕ be an even Schwartz function whose Fourier Transform is compactly supported. Let $L(s)$ be an L-function with zeros $\frac{1}{2} + i\gamma$ ($\gamma \in \mathbb{R}$) and conductor C.

Measures of Spacings: 1-Level Density and Families

Let ϕ be an even Schwartz function whose Fourier Transform is compactly supported. Let $L(s)$ be an L-function with zeros $\frac{1}{2}+i\gamma$ ($\gamma \in \mathbb{R}$) and conductor C. Define the 1-level density by

$$\sum_n \phi\left(\gamma_n \log C\right)$$

Measures of Spacings: 1-Level Density and Families

Let ϕ be an even Schwartz function whose Fourier Transform is compactly supported. Let $L(s)$ be an L-function with zeros $\frac{1}{2} + i\gamma$ $(\gamma \in \mathbb{R})$ and conductor C. Define the 1-level density by

$$\sum_n \phi\left(\gamma_n \log C\right)$$

- Individual zeros γ_n contribute in limit
- Most of contribution is from low zeros
- Average over similar L-functions (family)

Measures of Spacings: 1-Level Density and Families

Let ϕ be an even Schwartz function whose Fourier Transform is compactly supported. Let $L(s)$ be an L-function with zeros $\frac{1}{2} + i\gamma$ ($\gamma \in \mathbb{R}$) and conductor C. Define the 1-level density by

$$\sum_n \phi\left(\gamma_n \log C\right)$$

- Individual zeros γ_n contribute in limit
- Most of contribution is from low zeros
- Average over similar L-functions (family)

To any geometric family, Katz-Sarnak predict the 1-level density depends only on a symmetry group (a classical compact group) attached to the family.

Random Matrix Ensembles and Number Theory

- **Zeros far away from $s = \frac{1}{2}$ well-modelled by GUE.**

Random Matrix Ensembles and Number Theory

- **Zeros far away from $s = \frac{1}{2}$ well-modelled by GUE.**
  - Choose one L-Function, look at high zeros.
  - One L-function has enough freedom to average.

Random Matrix Ensembles and Number Theory

- **Zeros far away from $s = \frac{1}{2}$ well-modelled by GUE.**
    - Choose one L-Function, look at high zeros.
    - One L-function has enough freedom to average.

- **Story different for zeros near $s = \frac{1}{2}$.**

Random Matrix Ensembles and Number Theory

- **Zeros far away from $s = \frac{1}{2}$ well-modelled by GUE.**
  - Choose one L-Function, look at high zeros.
  - One L-function has enough freedom to average.

- **Story different for zeros near $s = \frac{1}{2}$.**
  - One L-function no longer suffices for averaging.
  - Look at many similar L-functions.
  - Hope L-functions' zeros near $s = \frac{1}{2}$ behave similarly.

Random Matrix Ensembles and Number Theory

- **Zeros far away from $s = \frac{1}{2}$ well-modelled by GUE.**
  - Choose one L-Function, look at high zeros.
  - One L-function has enough freedom to average.

- **Story different for zeros near $s = \frac{1}{2}$.**
  - One L-function no longer suffices for averaging.
  - Look at many similar L-functions.
  - Hope L-functions' zeros near $s = \frac{1}{2}$ behave similarly.

- **Analogy with Random Matrix Theory:**

Random Matrix Ensembles and Number Theory

- **Zeros far away from $s = \frac{1}{2}$ well-modelled by GUE.**
  - Choose one L-Function, look at high zeros.
  - One L-function has enough freedom to average.

- **Story different for zeros near $s = \frac{1}{2}$.**
  - One L-function no longer suffices for averaging.
  - Look at many similar L-functions.
  - Hope L-functions' zeros near $s = \frac{1}{2}$ behave similarly.

- **Analogy with Random Matrix Theory:**
  - RMT: pick many $N \times N$ matrices at random, average, study limit as $N \to \infty$.
  - NT: pick many L-functions in a family with conductors about the same size, average, study what happens as conductors go to infinity.

Random Matrix Ensembles

Real Symmetric, Complex Hermitian Matrices:

1. $\lambda \in \mathbb{R}$.
2. Randomness: upper triangular entries independently chosen from p; freedom to choose p.

Random Matrix Ensembles

Real Symmetric, Complex Hermitian Matrices:

1. $\lambda \in \mathbb{R}$.
2. Randomness: upper triangular entries independently chosen from p; freedom to choose p.

Classical Compact Groups:

1. $\lambda = e^{i\theta}$, $\theta \in (-\pi, \pi] \subset \mathbb{R}$.
2. Randomness: Haar measure; canonical choice.
3. Subgroups: Orthogonal Matrices ($Q^T Q = I$):

$$\begin{array}{rl} \text{SO(even)} : e^{i\theta} : & \cdots \leq -\theta_2 \leq -\theta_1 \leq \quad 0 \quad \leq \theta_1 \leq \theta_2 \leq \cdots \\ \text{SO(odd)} : e^{i\theta} : & \cdots \leq -\theta_2 \leq -\theta_1 \leq \theta_0 = 0 \leq \theta_1 \leq \theta_2 \leq \cdots \end{array}$$

Theorems for Families of Elliptic Curves
Family $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$, specialized curves E_t

If family $\mathcal{E}$ has rank $r(\mathcal{E})$: As conductors go to infinity:

- Results suggest E_t has at least $r(\mathcal{E})$ zeros at $s = \frac{1}{2}$;
- Behavior of remaining zeros near $s = \frac{1}{2}$ agree with eigenvalues near 1 of orthogonal groups.

Theorems for Families of Elliptic Curves

Family $\mathcal{E}: y^2 = x^3 + A(T)x + B(T)$, specialized curves E_t

If family $\mathcal{E}$ has rank $r(\mathcal{E})$: As conductors go to infinity:

- Results suggest E_t has at least $r(\mathcal{E})$ zeros at $s = \frac{1}{2}$;
- Behavior of remaining zeros near $s = \frac{1}{2}$ agree with eigenvalues near 1 of orthogonal groups.

Method of Proof

- Explicit Formula: *(Analogue of Eigenvalue Trace Lemma)*
  - Relates Sums over Zeros to Sums over Primes.
  - Gives correct scale.
- Summation Formulas: *(Analogue of Integrating Matrix Entries)*
  - Sums of Legendre Symbols.
  - Like Central Limit Theorem, just first two moments matter: $\sum_{t \bmod p} a_{p,t}$ and $\sum_{t \bmod p} a_{p,t}^2$.

Predictions from Random Matrix Theory
Family $\mathcal{E}$ of Elliptic Curves with rank $r(\mathcal{E})$

Families of Elliptic Curves well-modelled by Orthogonal Groups: zeros near $s = \frac{1}{2}$ look like eigenvalues near 1.

Predictions from Random Matrix Theory
Family $\mathcal{E}$ of Elliptic Curves with rank $r(\mathcal{E})$

Families of Elliptic Curves well-modelled by Orthogonal Groups: zeros near $s = \frac{1}{2}$ look like eigenvalues near 1.

As conductor C_t goes to infinity, expect half the elliptic curves E_t to have rank $r(\mathcal{E})$, half to have rank $r(\mathcal{E}) + 1$.

Predictions from Random Matrix Theory
Family $\mathcal{E}$ of Elliptic Curves with rank $r(\mathcal{E})$

Families of Elliptic Curves well-modelled by Orthogonal Groups: zeros near $s = \frac{1}{2}$ look like eigenvalues near 1.

As conductor C_t goes to infinity, expect half the elliptic curves E_t to have rank $r(\mathcal{E})$, half to have rank $r(\mathcal{E}) + 1$.

As conductor C_t goes to infinity, for each E_t expect the $r(\mathcal{E})$ family zeros to be independent of the other zeros of E_t near $s = \frac{1}{2}$.

Predictions from Random Matrix Theory
Family $\mathcal{E}$ of Elliptic Curves with rank $r(\mathcal{E})$

Families of Elliptic Curves well-modelled by Orthogonal Groups: zeros near $s = \frac{1}{2}$ look like eigenvalues near 1.

As conductor C_t goes to infinity, expect half the elliptic curves E_t to have rank $r(\mathcal{E})$, half to have rank $r(\mathcal{E}) + 1$.

As conductor C_t goes to infinity, for each E_t expect the $r(\mathcal{E})$ family zeros to be independent of the other zeros of E_t near $s = \frac{1}{2}$.

In particular, the distribution of the first zero above $s = \frac{1}{2}$ should be independent of $r(\mathcal{E})$.

Excess Rank

One-parameter family, rank $r(\mathcal{E})$ over $\mathbb{Q}(T)$.

For each $t \in \mathbb{Z}$, consider curves E_t.

RMT $\Longrightarrow$ 50% rank $r(\mathcal{E})$, 50% rank $r(\mathcal{E}) + 1$.

Excess Rank

One-parameter family, rank $r(\mathcal{E})$ over $\mathbb{Q}(T)$.

For each $t \in \mathbb{Z}$, consider curves E_t.

RMT $\Longrightarrow$ 50% rank $r(\mathcal{E})$, 50% rank $r(\mathcal{E}) + 1$.

For many families, observe

$$\begin{array}{llll} \text{Percent with rank } r(\mathcal{E}) & = 32\% & \text{Percent with rank } r(\mathcal{E})+1 & = 48\% \\ \text{Percent with rank } r(\mathcal{E})+2 & = 18\% & \text{Percent with rank } r(\mathcal{E})+3 & = 2\% \end{array}$$

Excess Rank

One-parameter family, rank $r(\mathcal{E})$ over $\mathbb{Q}(T)$.
For each $t \in \mathbb{Z}$, consider curves E_t.
RMT $\Longrightarrow$ 50% rank $r(\mathcal{E})$, 50% rank $r(\mathcal{E}) + 1$.

For many families, observe

$$\begin{array}{lclcl} \text{Percent with rank } r(\mathcal{E}) & = & 32\% & \text{Percent with rank } r(\mathcal{E})+1 & = & 48\% \\ \text{Percent with rank } r(\mathcal{E})+2 & = & 18\% & \text{Percent with rank } r(\mathcal{E})+3 & = & 2\% \end{array}$$

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

Interval	Primes	Twin Primes Pairs
$[1, 10]$	$2, 3, 5, 7$ (40%)	$(3, 5), (5, 7)$ (20%)
$[11, 20]$	$11, 13, 17, 19$ (40%)	$(11, 13), (17, 19)$ (20%)

Small data can be misleading! Remember $\sum_{n \leq N} \frac{1}{n} \sim \log N$.

Data on Excess Rank

$$y^2 = x^3 + 16Tx + 32$$

Each data set runs over 2000 consecutive t-values.

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.

SO(even) Random Matrix Models

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

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

SO(even) Random Matrix Models

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

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

Independent Model: $2r$ Eigenvalues at 1

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

SO(even) Random Matrix Models

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

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

Independent Model: $2r$ Eigenvalues at 1

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

Interaction Model: $2r$ Eigenvalues at 1

Sub-ensemble of SO$(2N)$ with $2r$ eigenvalues forced to be $+1$:

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

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

Comparing the two Random Matrix Models

For small support, 1-level densities for Elliptic Curves agree with Independent Model.

Comparing the two Random Matrix Models

For small support, 1-level densities for Elliptic Curves agree with Independent Model.

Elliptic Curve E, conductor C, expect first zero above $s = \frac{1}{2}$ to be $\frac{1}{2} + i\gamma$ with $\gamma \sim \frac{1}{\log C}$.

Comparing the two Random Matrix Models

For small support, 1-level densities for Elliptic Curves agree with Independent Model.

Elliptic Curve E, conductor C, expect first zero above $s = \frac{1}{2}$ to be $\frac{1}{2} + i\gamma$ with $\gamma \sim \frac{1}{\log C}$.

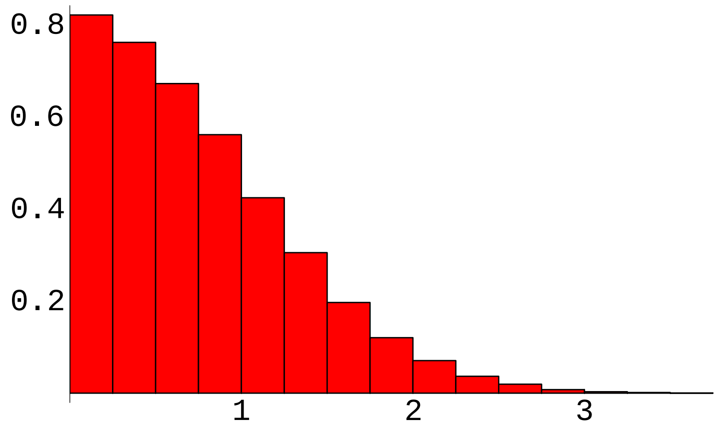
If r zeros at central point, if repulsion of zeros is of size $\frac{c_r}{\log C}$, would detect in zeros near central point:

$$\sum_n \phi\left(\gamma_n \log C\right).$$

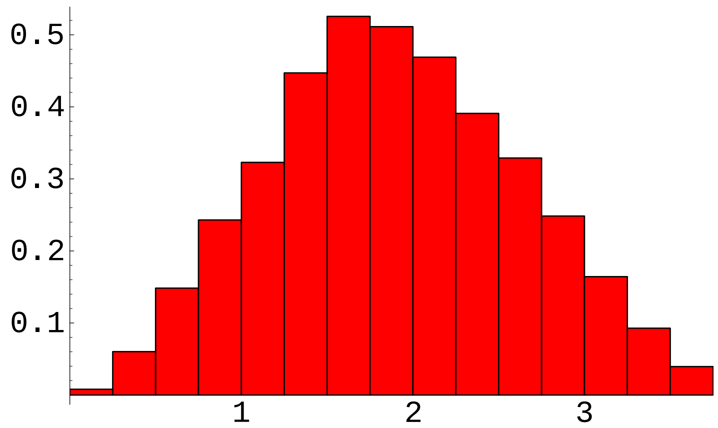
Corrections of size

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

Theoretical Distribution of First Normalized Zero



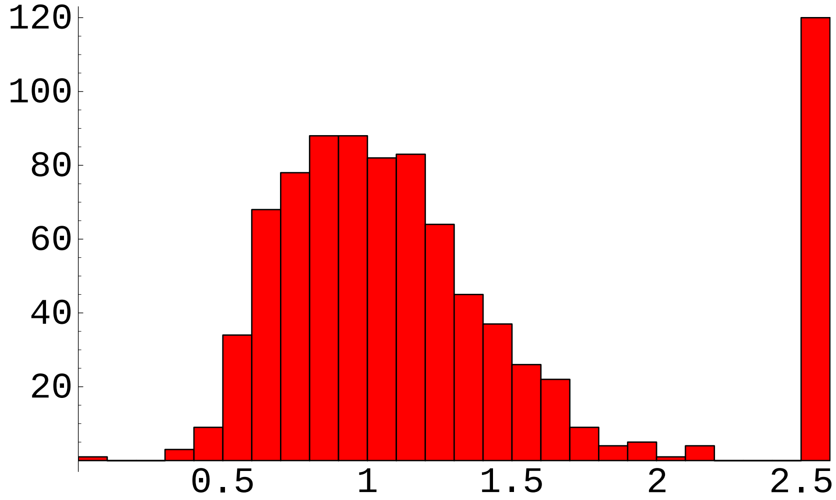
First normalized eigenvalue: 230,400 from SO(6) with Haar Measure



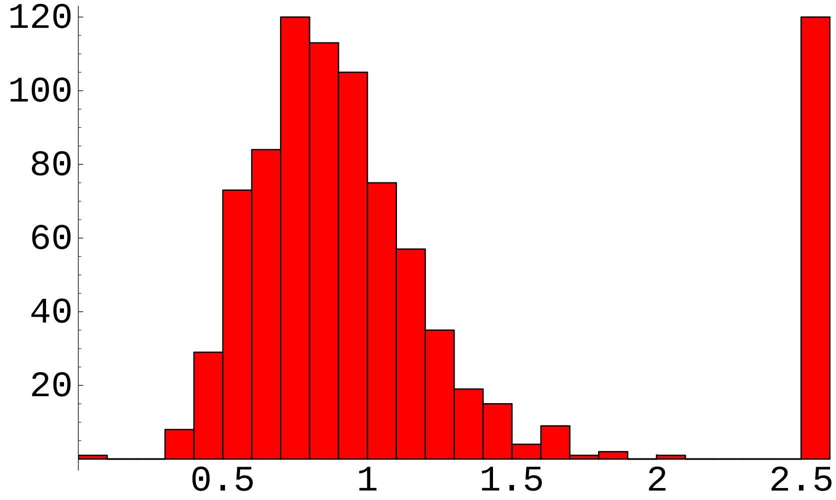
First normalized eigenvalue: 322,560 from SO(7) with Haar Measure

Rank 0 Curves: 1st Normalized Zero

(Far left and right bins just for formatting)

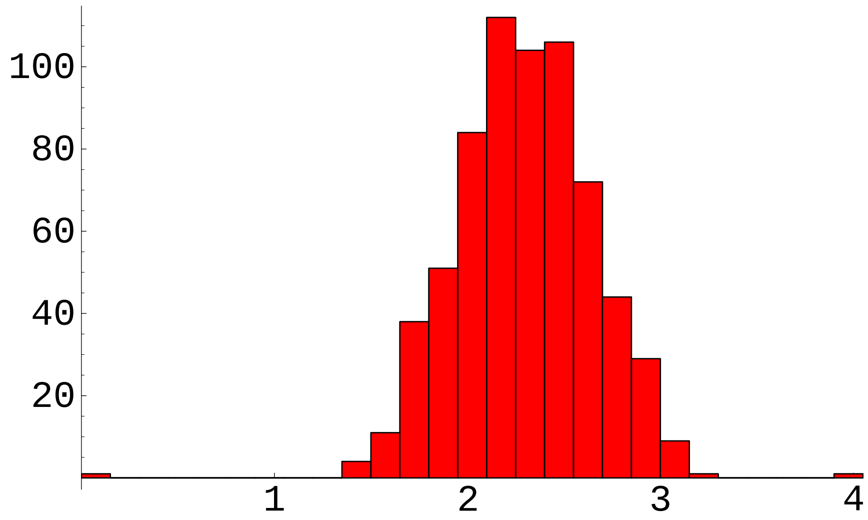


750 curves, $\log(\text{cond}) \in [3.2, 12.6]$; mean $= 1.04$

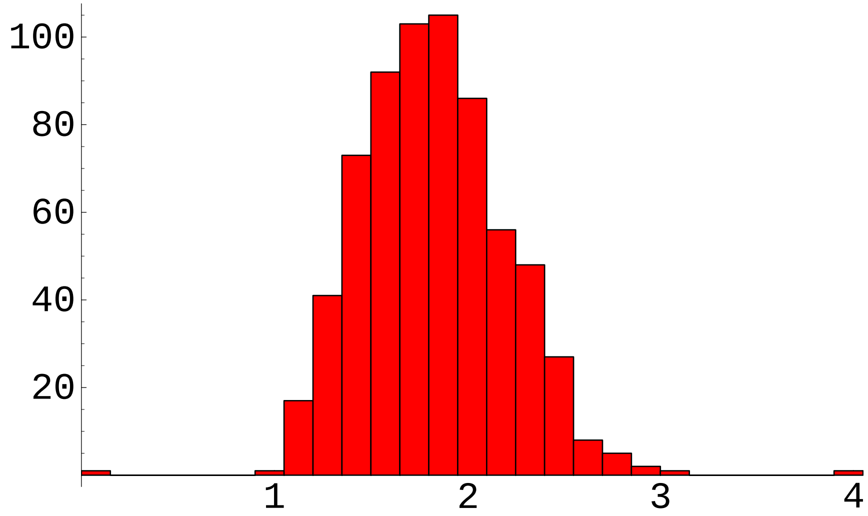


750 curves, $\log(\text{cond}) \in [12.6, 14.9]$; mean $= .88$

Rank 2 Curves: 1st Normalized Zero

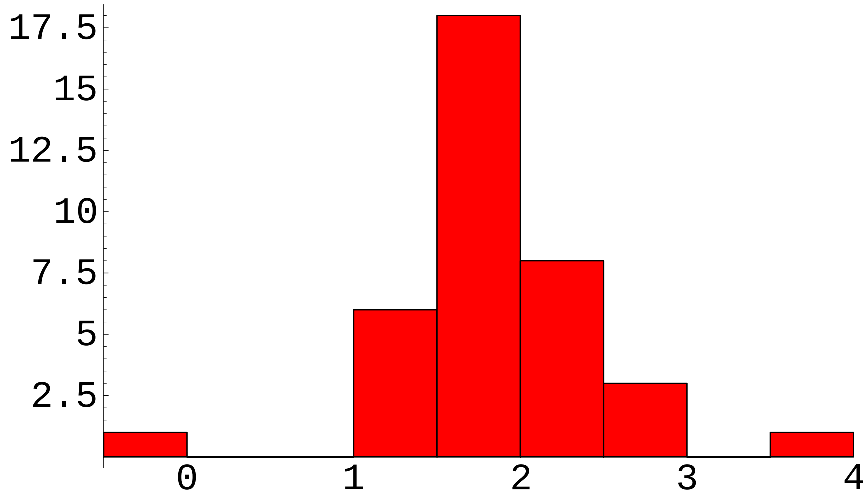


665 curves, $\log(\text{cond}) \in [10, 10.3125]$; mean $= 2.30$

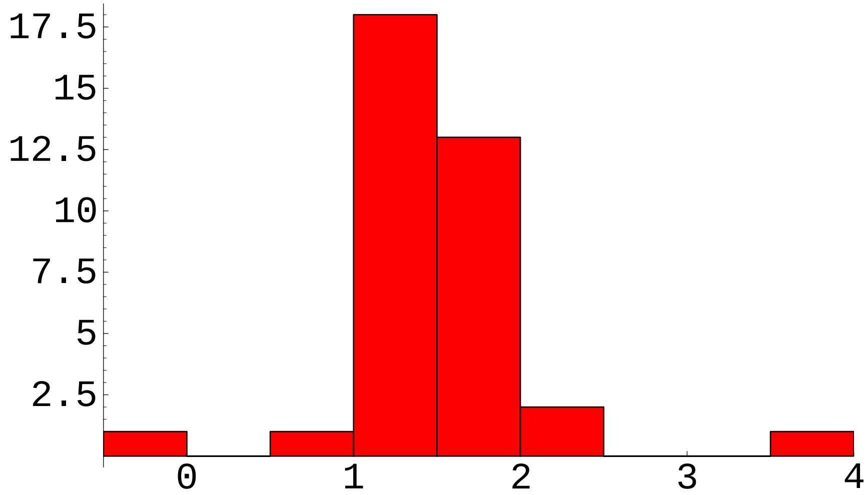


665 curves, $\log(\text{cond}) \in [16, 16.5]$; mean $= 1.82$

Rank 2 Curves: $y^2 = x^3 - T^2x + T^2$: 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 $= 2.00$

PART VI

CONCLUSIONS

Correspondences

Similarities between Nuclei and Primes:

Energy Levels	$\longleftrightarrow$	Zeros of L-Functions
Neutron Energy	$\longleftrightarrow$	Support of Test Functions
Different Elements: U, Pu, ...	$\longleftrightarrow$	Different L-Functions

Summary

- Find correct scale to compare different systems.

- Similar behavior in different systems.

- Need a Trace Lemma.

- Average over similar elements.

- Need more data.

Open Problems in Number Theory

Identifying Classical Compact Group:

Given a reasonable family of L-functions, determine the corresponding symmetry group.

Montgomery-Odlyzko Law:

Show that zeros of L-functions at height $T \to \infty$ behave like eigenvalues of $N \times N$ matrices with $N \sim \log \frac{T}{2\pi}$.

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 we move through the family (ordered by conductor)?

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 in $(-\sigma, \sigma)$.

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 $m/M_2 \leq 3^r$, $s = 0$ 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 $\sigma < 2$. 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 (continued):

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:
Random Graphs

Random Graphs (with Peter Sarnak, Yakov Sinai)

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

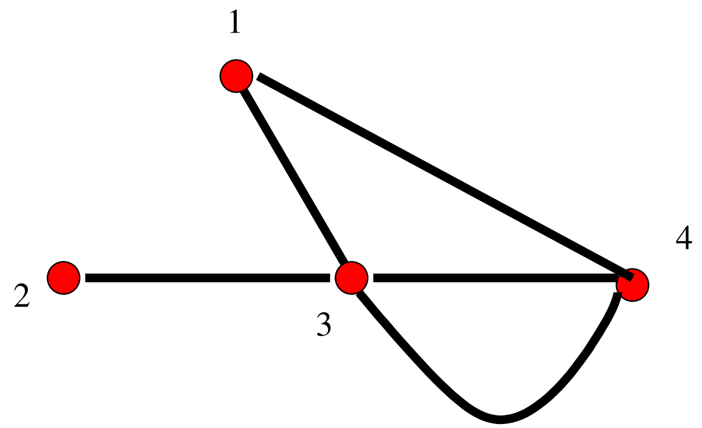
Fat Thin Families

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.

Adjacency matrix: a_{ij} = number edges between Vertex i and Vertex j.

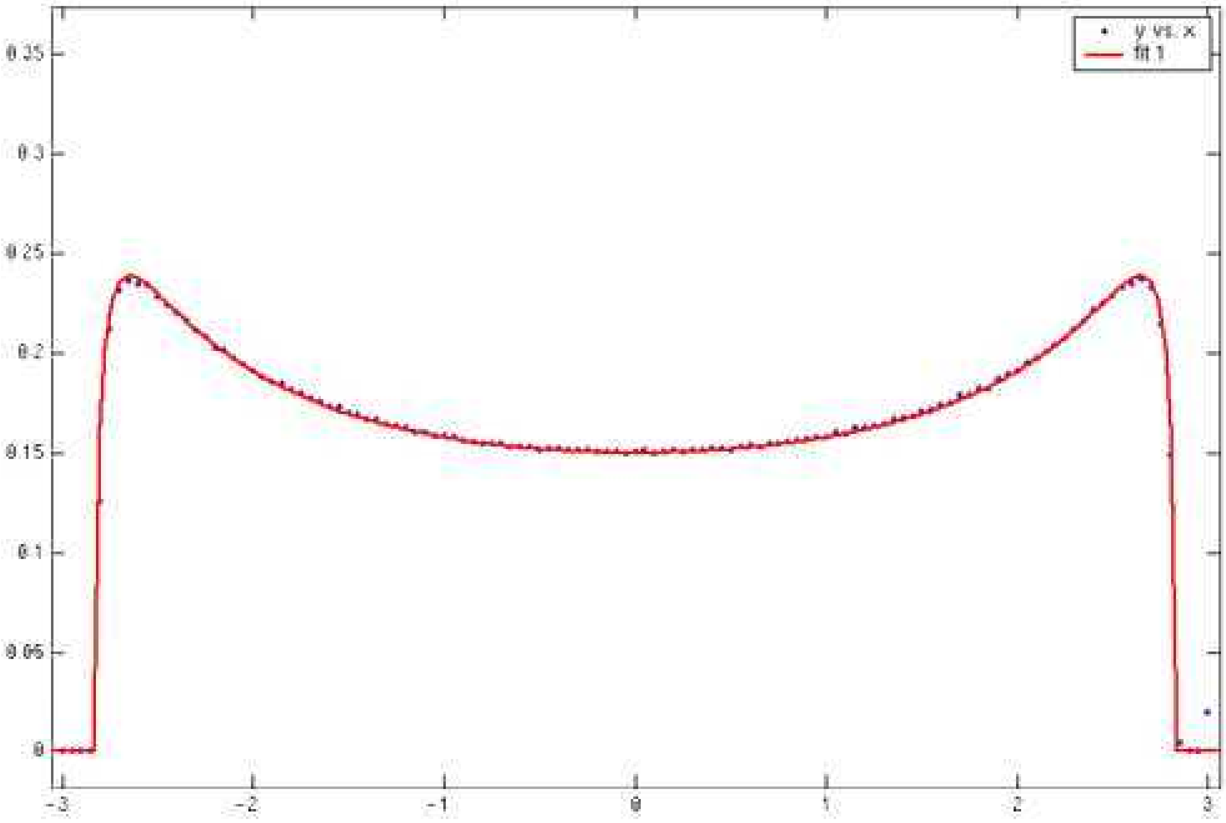
$$A = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 2 \\ 1 & 0 & 2 & 0 \end{pmatrix}$$

These are Real Symmetric Matrices.

McKay's Law

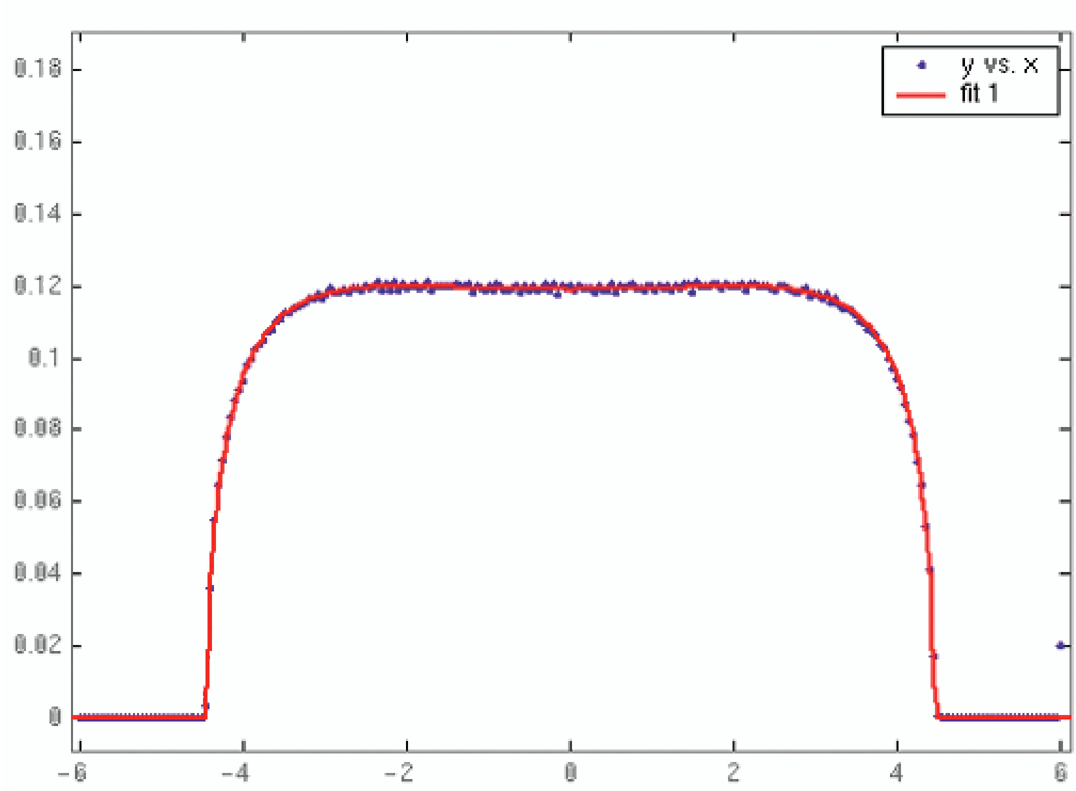
Density of Eigenvalues for d-regular graphs

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



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

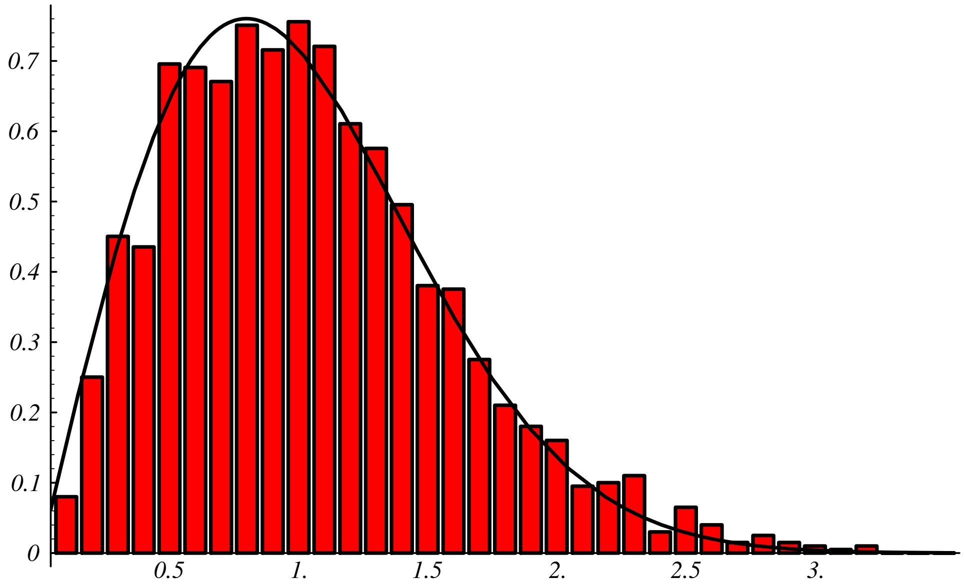
McKay's Law



$$d = 6.$$

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

3-Regular, 2000 Vertices and GOE



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*, Mathematics unlimited - 2001 and beyond, 331-352, Springer, Berlin, 2001.

[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/$\sim$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.