From the Manhattan Project to Number Theory

Steven J Miller
Williams College

Steven.J.Miller@williams.edu
http://www.williams.edu/go/math/sjmiller

Wellesley College, February 2, 2010
Acknowledgements

- Much of this is joint and current work with Eduardo Dueñez, Duc Khiem Huynh, Jon Keating and Nina Snaith.

- Computer programs written with Adam O’Brien, Jon Hsu, Leo Goldmahker, Stephen Lu and Mike Rubinstein.
Outline

- Review elliptic curves and $L$-functions.
- Introduce relevant RMT ensembles.
- Reconcile theory and data.
Elliptic Curves and $L$-functions

Classical RMT

Results, Questions and Conjectures

Conclusions

Refs

Elliptic Curves and $L$-functions
Mordell-Weil Group

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

Addition of distinct points $P$ and $Q$  

Adding a point $P$ to itself  

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

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

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

Unique Factorization: \( n = p_1^{r_1} \cdots p_m^{r_m}. \)
Riemann Zeta Function

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

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

\[
\prod_{p} \left( 1 - \frac{1}{p^s} \right)^{-1} = \left[ 1 + \frac{1}{2^s} + \left( \frac{1}{2^s} \right)^2 + \cdots \right] \left[ 1 + \frac{1}{3^s} + \left( \frac{1}{3^s} \right)^2 + \cdots \right] = \sum_{n} \frac{1}{n^s}.
\]
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:
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:

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

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

**Functional Equation:**

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

**Riemann Hypothesis (RH):**

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

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

Functional Equation:

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

Generalized Riemann Hypothesis (GRH):

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

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

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

where

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

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

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

where

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

Birch and Swinnerton-Dyer Conjecture

Rank of group of rational solutions equals order of vanishing of $L(s, E)$ at $s = 1/2$. 
Classical Random Matrix Theory
Fundamental Problem: Spacing Between Events

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

**Question:** What rules govern the spacings between the $t_i$?

**Examples:**
- Spacings b/w Energy Levels of Nuclei.
- Spacings b/w Eigenvalues of Matrices.
- Spacings b/w Primes.
- Spacings b/w $n^k \alpha \mod 1$.
- Spacings b/w Zeros of $L$-functions.
In studying many statistics, often three key steps:

1. Determine correct scale for events.

2. Develop an explicit formula relating what we want to study to something we understand.

3. Use an averaging formula to analyze the quantities above.

It is not always trivial to figure out what is the correct statistic to study!
Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem Intractable.
Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem Intractable.

Heavy nuclei (Uranium: 200+ protons / neutrons) worse!
Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem Intractable.

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

Get some info by shooting high-energy neutrons into nucleus, see what comes out.
Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem Intractable.

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

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

Fundamental Equation:

\[ H\psi_n = E_n\psi_n \]

\( H \) : matrix, entries depend on system
\( E_n \) : energy levels
\( \psi_n \) : energy eigenfunctions
Origins (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 (real Symmetric $A = A^T$, complex Hermitian $\overline{A}^T = A$).
Random Matrix Ensembles

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

Fix \( p \), define

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

This means

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

\[ \delta(x - x_0) \] is a unit point mass at \( x_0 \):

\[ \int_{-\infty}^{\infty} f(x) \delta(x - x_0) \, dx = f(x_0). \]
Eigenvalue Distribution

\[ \delta(x - x_0) \text{ is a unit point mass at } x_0: \]
\[ \int_{-\infty}^{\infty} f(x) \delta(x - x_0) \, dx = f(x_0). \]

To each \( A \), attach a probability measure:

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

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

\[
\text{k}^{th} \text{ moment} = \frac{\sum_{i=1}^{N} \lambda_i(A)^k}{2^k N^{k/2 + 1}}.
\]
Want to understand the eigenvalues of $A$, but it is the matrix elements that are chosen randomly and independently.
Eigenvalue Trace Lemma

Want to understand the eigenvalues of $A$, but it is the matrix elements that are chosen randomly and independently.

**Eigenvalue Trace Lemma**

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

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

where

$$\text{Trace}(A^k) = \sum_{i_1=1}^{N} \cdots \sum_{i_k=1}^{N} a_{i_1i_2} a_{i_2i_3} \cdots a_{i_Ni_1}.$$
Results, Questions
and Conjectures
Zeros of $\zeta(s)$ vs GUE

70 million spacings b/w adjacent zeros of $\zeta(s)$, starting at the $10^{20}$th zero (from Odlyzko) versus RMT prediction.
1-Level Density

$L$-function $L(s, f)$: by RH non-trivial zeros $\frac{1}{2} + i\gamma_{f,j}$.

$C_f$: analytic conductor.

$\varphi(x)$: compactly supported even Schwartz function.

$$D_{1,f}(\varphi) = \sum_j \varphi \left( \frac{\log C_f}{2\pi} \gamma_{f,j} \right)$$
1-Level Density

$L$-function $L(s, f)$: by RH non-trivial zeros $\frac{1}{2} + i\gamma_{f,j}$.

$C_f$: analytic conductor.

$\varphi(x)$: compactly supported even Schwartz function.

$$D_{1,f}(\varphi) = \sum_j \varphi \left( \frac{\log C_f}{2\pi} \gamma_{f,j} \right)$$

- individual zeros contribute in limit
- most of contribution is from low zeros
1-Level Density

$L$-function $L(s, f)$: by RH non-trivial zeros $\frac{1}{2} + i\gamma_{f,j}$.

$C_f$: analytic conductor.

$\varphi(x)$: compactly supported even Schwartz function.

\[
D_{1,f}(\varphi) = \sum_j \varphi \left( \frac{\log C_f}{2\pi} \gamma_{f,j} \right)
\]

- individual zeros contribute in limit
- most of contribution is from low zeros

Katz-Sarnak Conjecture:

\[
D_{1,\mathcal{F}}(\varphi) = \lim_{N \to \infty} \frac{1}{|\mathcal{F}_N|} \sum_{f \in \mathcal{F}_N} D_{1,f}(\varphi) = \int \varphi(x) \rho_{G(\mathcal{F})}(x) dx.
\]
Comparing the RMT Models

**Theorem: M– ’04**

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

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

where

\[
G = \begin{cases} 
  \text{SO} & \text{if half odd} \\
  \text{SO(even)} & \text{if all even} \\
  \text{SO(odd)} & \text{if all odd}
\end{cases}
\]

Confirm Katz-Sarnak, B-SD predictions for small support.

Supports Independent and not Interaction model in the limit.
Sketch of Proof

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

- **Averaging Formulas**: Orthogonality of characters, Petersson formula.

- **Control of conductors**: Monotone.
Explicit Formula (Contour Integration)

\[- \frac{\zeta'(s)}{\zeta(s)} = - \frac{d}{ds} \log \zeta(s) = - \frac{d}{ds} \log \prod_p (1 - p^{-s})^{-1}\]
Explicit Formula (Contour Integration)

\[-\frac{\zeta'(s)}{\zeta(s)} = -\frac{d}{ds} \log \zeta(s) = -\frac{d}{ds} \log \prod_p (1 - p^{-s})^{-1}\]

\[= \frac{d}{ds} \sum_p \log (1 - p^{-s})\]

\[= \sum_p \frac{\log p \cdot p^{-s}}{1 - p^{-s}} = \sum_p \frac{\log p}{p^s} + \text{Good}(s).\]
Explicit Formula (Contour Integration)

\[-\frac{\zeta'(s)}{\zeta(s)} = -\frac{d}{ds} \log \zeta(s) = -\frac{d}{ds} \log \prod_p (1 - p^{-s})^{-1}\]

\[= \frac{d}{ds} \sum_p \log (1 - p^{-s})\]

\[= \sum_p \frac{\log p \cdot p^{-s}}{1 - p^{-s}} = \sum_p \frac{\log p}{p^s} + \text{Good}(s).\]

Contour Integration:

\[\int - \frac{\zeta'(s)}{\zeta(s)} \phi(s) ds \quad \text{vs} \quad \sum_p \log p \int \phi(s) p^{-s} ds.\]
Explicit Formula (Contour Integration)

\[-\frac{\zeta'(s)}{\zeta(s)} = -\frac{d}{ds} \log \zeta(s) = -\frac{d}{ds} \log \prod_p (1 - p^{-s})^{-1}\]

\[= \frac{d}{ds} \sum_p \log (1 - p^{-s})\]

\[= \sum_p \log p \cdot \frac{p^{-s}}{1 - p^{-s}} = \sum_p \frac{\log p}{p^s} + \text{Good}(s).\]

Contour Integration (see Fourier Transform arising):

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

Knowledge of zeros gives info on coefficients.
Explicit Formula: Examples

Cuspidal Newforms: Let $\mathcal{F}$ be a family of cuspidal newforms (say weight $k$, prime level $N$ and possibly split by sign) $L(s, f) = \sum_n \lambda_f(n)/n^s$. Then

$$\frac{1}{|\mathcal{F}|} \sum_{f \in \mathcal{F}} \sum_{\gamma_f} \phi \left( \frac{\log R}{2\pi} \gamma_f \right) = \hat{\phi}(0) + \frac{1}{2} \phi(0) - \frac{1}{|\mathcal{F}|} \sum_{f \in \mathcal{F}} P(f; \phi)$$

$$+ O \left( \frac{\log \log R}{\log R} \right)$$

$$P(f; \phi) = \sum_{p \mid N} \lambda_f(p) \hat{\phi} \left( \frac{\log p}{\log R} \right) \frac{2 \log p}{\sqrt{p} \log R}.$$
RMT: Theoretical Results ($N \to \infty$)

Figure 1a: 1st norm. evalue above 1: SO(even)
Figure 1b: 1st norm. evalue above 1: SO(odd)
Rank 0 Curves: 1st Normalized Zero above Central Point

Figure 2a: 750 rank 0 curves from

\[ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \]

\[ \log(\text{cond}) \in [3.2, 12.6], \text{ median} = 1.00 \text{ mean} = 1.04, \sigma_\mu = .32 \]
Rank 0 Curves: 1st Normalized Zero above Central Point

Figure 2b: 750 rank 0 curves from

\[ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \]

\[ \log(\text{cond}) \in [12.6, 14.9], \text{ median} = .85, \text{ mean} = .88, \sigma_\mu = .27 \]
Modeling lowest zero of $L_{E_{11}}(s, \chi_d)$ with $0 < d < 400,000$

Lowest zero for $L_{E_{11}}(s, \chi_d)$ (bar chart), lowest eigenvalue of SO(2N) with $N_{\text{eff}}$ (solid), standard $N_0$ (dashed).
Modeling lowest zero of $L_{E_{11}}(s, \chi_d)$ with $0 < d < 400,000$

Lowest zero for $L_{E_{11}}(s, \chi_d)$ (bar chart), lowest eigenvalue of SO(2N) with $N_0 = 12$ (solid) with discretisation and with standard $N_0 = 12.26$ (dashed) without discretisation.
Modeling lowest zero of $L_{E_{11}}(s, \chi_d)$ with $0 < d < 400,000$

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

- $L$-functions encode arithmetic.

- Understand behavior as conductors tend to infinity.

- New random matrix model (incorporates arithmetic and discretization).

- **Similarities between $L$-Functions and Nuclei:**

  Zeros $\leftrightarrow$ Energy Levels

  Schwartz test function $\longrightarrow$ Neutron

  Support of test function $\longleftrightarrow$ Neutron Energy.
References

Caveat: this bibliography is only meant to be a first reference.


Elliptic Curves and $L$-functions

Classical RMT

Results, Questions and Conjectures

Conclusions

Refs


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


N. Snaith, *Derivatives of random matrix characteristic polynomials with applications to elliptic curves*, preprint.


