FELLOWSHIP OF THE RING SEMINAR

(Sunda har i ened mente)

(Ash intya durbatuluk ash intya gimbatul. Ash intya thrakatuluk agh kala-ishi krimpatul)

Steven J. Miller

Brown University

Brandeis, April 1st, 2005

http://www.math.brown.edu/~sjmiller

Zeros Near the Central Point of Elliptic Curve L-Functions

Steven J. Miller
Brown University

Brandeis, April 1^{st}, 2005
http://www.math.brown.edu/∼sjmiller

Acknowledgments

Elliptic Curves (with Eduardo Dueñez)

- Adam O'Brien
- Aaron Lint

Fundamental Problem: Spacing Between Events

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

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

- 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.

- Understand zeros of Elliptic Curve L-functions near the central point.

PART I

RANDOM MATRIX THEORY

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.

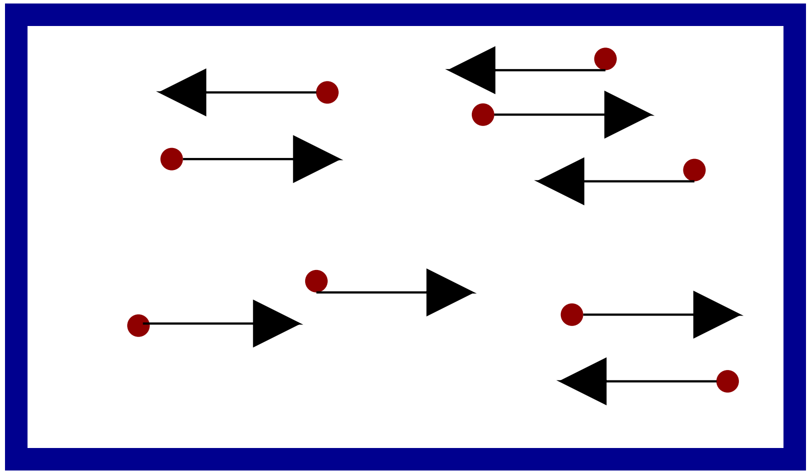
Fundamental Equation: $H\psi_n = E_n\psi_n$

H : matrix, entries depend on system

E_n : energy levels

ψ_n : energy eigenfunctions

Origins of Random Matrix Theory (continued)



Stat Mech: for each configuration, calculate quantity (say pressure).

Average over all configurations – most close to system average.

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

Look at: Real Symmetric ($A^T = A$), Complex Hermitian ($A^* = A$), Classical Compact groups (unitary, symplectic, orthogonal).

Random Matrix Ensembles

Real Symmetric Matrices:

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

Define

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

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

- 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

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

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

Eigenvalue Distribution

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

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 $\mathbb{R}$.

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

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

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

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

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

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

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

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

PART II

NUMBER THEORY

IDEA:

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

Riemann Zeta Function

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

Functional Equation:

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

Riemann Hypothesis:

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

Observation:

- Spacings between normalized zeros appear same as between normalized eigenvalues of Complex Hermitian matrices $(A^* = A)$.

Explicit Formula:
Analogue of the 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.

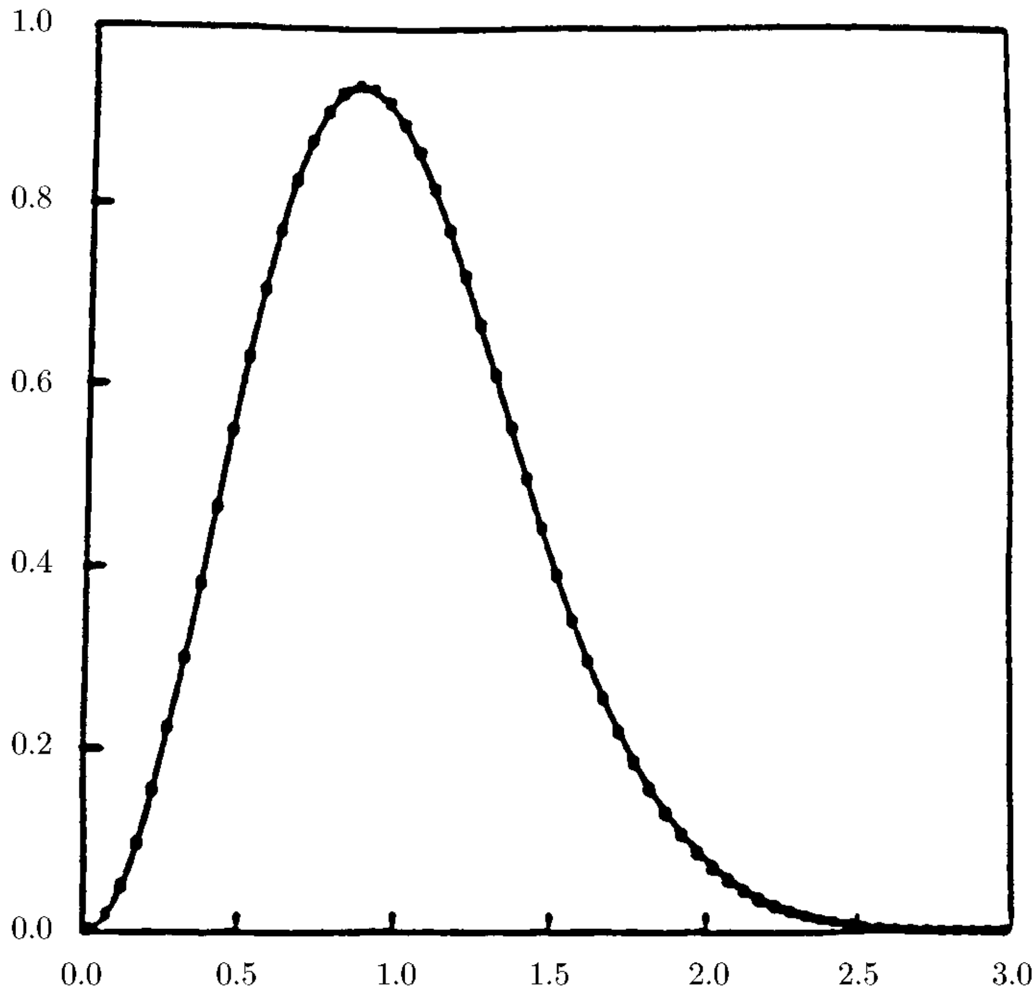
Normalized Zeros of Riemann Zeta Function
Zeros $\frac{1}{2} + i\gamma, \gamma \in \mathbb{R}$

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

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

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

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:**

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

- **Functional Equation:**

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

- **Riemann Hypothesis:**

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

- **Number of Zeros:**

$$\text{Number of zeros with } \gamma \sim T \text{ is like } T \log T$$
$$\text{Zeros near } s = \frac{1}{2} \text{ have } \gamma \sim \frac{1}{\log C}$$

Measures of Spacings: n-Level Correlations

$\{\alpha_j\}$ an increasing sequence of numbers, $B \subset \mathbb{R}^{n-1}$ a compact box. Define the n-level correlation by

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

Results on Zeros (Assuming GRH):

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

Interesting L-Functions

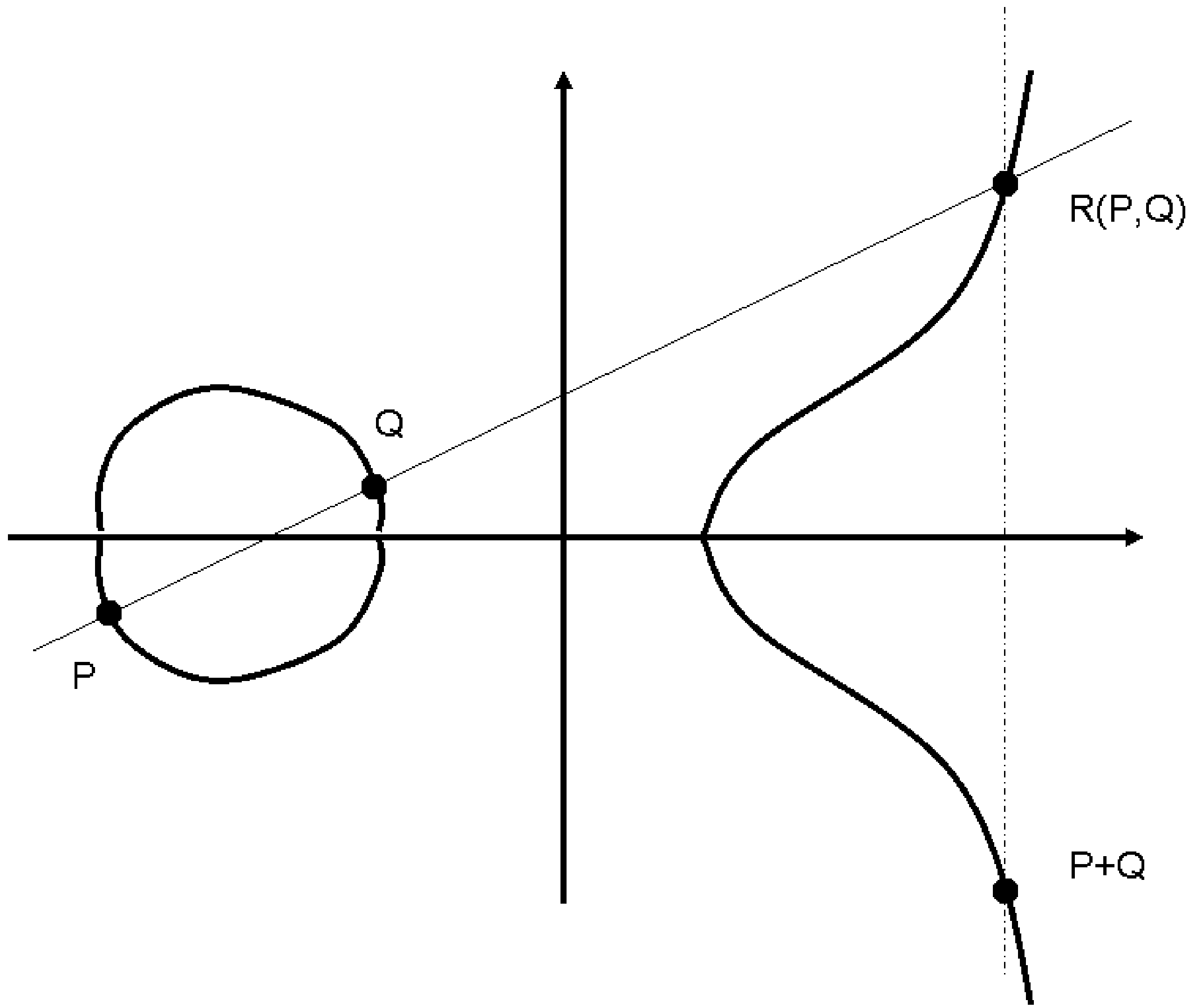
What makes an L-Function interesting?

- 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.

- 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.

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:

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

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

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

From Breuil, Conrad, Diamond, Taylor and Wiles:

$$\begin{aligned} \Lambda(E, s) &= (2\pi)^{-s} C_E^{s/2} \Gamma(s) L(E, s) \\ \Lambda(E, s) &= \epsilon_E \Lambda(E, 2 - s), \ \ \epsilon_E = \pm 1. \end{aligned}$$

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:

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

Have a FAMILY of L-Functions:

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

Families of Elliptic Curves

Mordell-Weil Theorem for Families:

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

- 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?

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.
  - Insensitive to finitely many zeros.

- **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, $N \to \infty$.
  - NT: pick many L-functions in a family, $C_t \to \infty$.

Random Matrix Ensembles

Real Symmetric, Complex Hermitian Matrices:

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

Classical Compact Groups:

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

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

Measures of Spacings: 1-Level Density and Families

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

$$D_{n,f}(\phi) \ = \ \sum_{\substack{j_1,\dots,j_n \\ j_i \neq \pm j_k}} \phi_1\left(\gamma_{j_1}\frac{\log C_f}{2\pi}\right) \cdots \phi_n\left(\gamma_{j_n}\frac{\log C_f}{2\pi}\right)$$

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

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

Normalization of Zeros

Local (hard) vs Global (easy). As $N \to \infty$:

$$\frac{1}{|\mathcal{F}_N|}\sum_{E_t\in\mathcal{F}_N} D_{n,E_t}(\phi) \;=\; \frac{1}{|\mathcal{F}_N|}\sum_{E_t\in\mathcal{F}_N}\sum_{\substack{j_1,\dots,j_n\\ j_i\neq\pm j_k}}\prod_i \phi_i\left(\gamma_{t,j_i}\frac{\log C_t}{2\pi}\right)$$

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

$$\to \int\cdots\int \widehat{\phi}(u)\widehat{W}_{n,\mathcal{G}(\mathcal{F})}(u)du.$$

Conj: Distribution of Low Zeros agrees with Orthogonal Densities.

Some Number Theory Results

- **Orthogonal:**

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

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

  Miller, Young: families of elliptic curves.

  Güloğlu: 1-level for $\{\text{Sym}^r f : f \in H_k(1)\}$, r odd.

- **Symplectic:**

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

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

  Güloğlu: 1-level for $\{\text{Sym}^r f : f \in H_k(1)\}$, r even.

- **Unitary:**

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

1-Level Densities

Fourier Transforms for 1-level densities:

$$\begin{aligned}
\widehat{W}_{1,\mathrm{SO(even)}}(u) &= \delta(u) + \tfrac{1}{2}\eta(u) \\
\widehat{W}_{1,\mathrm{SO}}(u) &= \delta(u) + \tfrac{1}{2} \\
\widehat{W}_{1,\mathrm{SO(odd)}}(u) &= \delta(u) - \tfrac{1}{2}\eta(u) + 1 \\
\\
\widehat{W}_{1,\mathrm{Sp}}(u) &= \delta(u) - \tfrac{1}{2}\eta(u) \\
\\
\widehat{W}_{1,\mathrm{U}}(u) &= \delta(u)
\end{aligned}$$

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

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

2-Level Densities

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

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

$$\begin{aligned} \int\int \widehat{\phi}_1(u_1)\widehat{\phi}_2(u_2)\widehat{W_{2,\mathcal{G}}}(u)du_1du_2 = & \left[\widehat{\phi}_1(0) + \frac{1}{2}\phi_1(0)\right]\left[\widehat{f}_2(0) + \frac{1}{2}\phi_2(0)\right] \\ & + 2\int |u|\widehat{\phi}_1(u)\widehat{\phi}_2(u)du \\ & -2\widehat{\phi_1\phi_2}(0) - \phi_1(0)\phi_2(0) \\ & + c(\mathcal{G})\phi_1(0)\phi_2(0). \end{aligned}$$

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

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

Interaction Model: $2r$ Eigenvalues at 1

Sub-ensemble of $\mathrm{SO}(2N)$ 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 $1 \le j,k \le N-r$.

Comparing the two Random Matrix Models

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:

$$\sum_{\gamma} \phi\left(\gamma \frac{\log C}{2\pi}\right).$$

Corrections of size

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

Motivation: Dirichlet Characters: m Prime

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

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

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

Can pass Character Sum through Test Function.

Elliptic Curves: Arithmetic Progression

One-parameter families:

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

We have

$$a_t(p) \;=\; -\sum_{x \bmod p} \left(\frac{x^3 + A(t)x + B(t)}{p}\right) \;=\; a_{t+mp}(p)$$

Can handle sums of $a_t(p)$ for t in arithmetic progression.

Comments on Previous Results

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

Elliptic curve E_t: discriminant $\Delta(t)$, conductor C_t is

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

1-Level Expansion

$$\begin{aligned}
D_{1,\mathcal{F}_N}(\phi) &= \frac{1}{|\mathcal{F}_N|}\sum_{E_t\in\mathcal{F}_N}\sum_j \phi\left(\gamma_{t,j}\frac{\log C_t}{2\pi}\right) \\
&= \frac{1}{|\mathcal{F}_N|}\sum_{E_t\in\mathcal{F}_N}\left[\widehat{\phi}(0)+\phi_i(0)\right] \\
&\quad - \frac{2}{|\mathcal{F}_N|}\sum_{E_t\in\mathcal{F}_N}\sum_p \frac{1}{p}\frac{\log p}{\log C_t}\widehat{\phi}\left(\frac{\log p}{\log C_t}\right) a_t(p) \\
&\quad - \frac{2}{|\mathcal{F}_N|}\sum_{E_t\in\mathcal{F}_N}\sum_p \frac{1}{p^2}\frac{\log p}{\log C_t}\widehat{\phi}\left(2\frac{\log p}{\log C_t}\right) a_t^2(p) + O\left(\frac{\log\log N}{\log N}\right)
\end{aligned}$$

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

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

2-Level Expansion

Need to evaluate terms like

$$\frac{1}{|\mathcal{F}_N|} \sum_{E_t \in \mathcal{F}_N} \prod_{i=1}^{2} \frac{1}{p_i^{r_i}} \, g_i\left(\frac{\log p_i}{\log C_t}\right) a_t^{r_i}(p_i).$$

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

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

Input

For many families

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

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

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

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

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

DEFINITIONS

$$D_{n,\mathcal{F}_N}(\phi) = \frac{1}{|\mathcal{F}_N|} \sum_{E_t \in \mathcal{F}_N} \sum_{\substack{j_1,\dots,j_n \\ j_i \neq \pm j_k}} \prod_i \phi_i \left(\gamma_{t,j_i} \frac{\log C_t}{2\pi} \right)$$

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

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

ASSUMPTIONS

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

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

Pass to positive percent sub-seq where conductors polynomial of degree m.
ϕ_i even Schwartz, support σ_i:

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

MAIN RESULT

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

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

where

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

1 and 2-level densities confirm Katz-Sarnak, Birch and Swinnderton-Dyer predictions for small support.

- Agree with Independent Model, note universality;
- Dependence on $\mathcal{F}$ through lower order correction terms.

Examples

Constant-Sign Families:

- $y^2 = x^3 + 2^4(-3)^3(9t+1)^2$,
  $9t+1$ Square-Free: all even.

- $y^2 = x^3 \pm 4(4t+2)x$,
  $4t+2$ Square-Free: $+$ all odd, $-$ all even.

- $y^2 = x^3 + tx^2 - (t+3)x + 1$,
  t^2+3t+9 Square-Free: all odd.

First two rank 0 over $\mathbb{Q}(T)$, third is rank 1.

Without 2-Level Density, couldn't say *which* orthogonal group.

Examples (cont)

Rational Surface of Rank 6 over $\mathbb{Q}(T)$:

$$\begin{aligned} y^2 &= x^3 + (2at - B)x^2 + (2bt - C)(t^2 + 2t - A + 1)x \\ &\quad + (2ct - D)(t^2 + 2t - A + 1)^2 \end{aligned}$$

$$\begin{aligned} A &= 8,916,100,448,256,000,000 \\ B &= -811,365,140,824,616,222,208 \\ C &= 26,497,490,347,321,493,520,384 \\ D &= -343,107,594,345,448,813,363,200 \\ a &= 16,660,111,104 \\ b &= -1,603,174,809,600 \\ c &= 2,149,908,480,000 \end{aligned}$$

Need GRH, Sq-Free Sieve to handle sieving.

Sketch of Proof

1. Sieving (Arithmetic Progressions)

2. Partial Summation (Complete Sums)

3. Controlling Conductors (Monotone).

Sieving

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

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

Handle first by progressions.

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

Sieving (cont)

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

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

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

If $(d, p_1p_2) = 1$, go through complete set of residue classes $\frac{N/d^2}{p_1p_2}$ times.

Partial Summation

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

Applying Partial Summation

$$
\begin{aligned}
S(d,i,r,p) &= \sum_{t'=0}^{[N/d^2]} \widetilde{a}^{r}_{d,i,p}(t') G_{d,i,p}(t') \\
&= \left(\frac{[N/d^2]}{p} A_{r,\mathcal{F}}(p) + O\left(p^R\right) \right) G_{d,i,p}([N/d^2]) \\
&\quad - \sum_{u=0}^{[N/d^2]-1} \left(\frac{u}{p} A_{r,\mathcal{F}}(p) + O\left(p^R\right) \right) \left(G_{d,i,p}(u) - G_{d,i,p}(u+1) \right)
\end{aligned}
$$

Difficult Piece: Fourth Sum I

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

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

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

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

Fourth Sum: II

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

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

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

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

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

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

Handling the Conductors: I

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

$$\begin{aligned}
C(t) &= \prod_{p|\Delta(t)} p^{f_p(t)} \\
D_1(t) &= \text{primitive irred poly factors } \Delta(t) \text{ and } c_4(t) \text{ share} \\
D_2(t) &= \text{remaining primitive irred poly factors of } \Delta(t) \\
D(t) &= D_1(t)D_2(t)
\end{aligned}$$

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

Handling the Conductors: II

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

Let P be the product of the bad primes.

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

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

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

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

Get integers such that if $D(\tau)$ is sq-free then $C(\tau) = c_{\text{bad}} \frac{D_1^2(\tau)}{c_1} \frac{D_2(\tau)}{c_2}$.

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 from Independent Model.
- Application: Bounding average rank in a family (use positive test function).

PART III

NUMERICAL DATA: THEORY vs. EXPERIMENT

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 $r(\mathcal{E}) + 1$.

For many families, observe

Percent with rank $r(\mathcal{E}) = 32\%$	Percent with rank $r(\mathcal{E}) + 1 = 48\%$
Percent with rank $r(\mathcal{E}) + 2 = 18\%$	Percent with rank $r(\mathcal{E}) + 3 = 2\%$

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 $\sum_{p \le x} \frac{1}{p} \sim \log\log x$.

Data on Excess Rank

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

Family: $a_1 : 0$ to 10, rest -10 to 10.
14 Hours, 2,139,291 curves (2,971 singular, 248,478 distinct).

Percent with rank $r = 28.60\%$

Percent with rank $r + 1 = 47.56\%$

Percent with rank $r + 2 = 20.97\%$

Percent with rank $r + 3 = 2.79\%$

Percent with rank $r + 4 = .08\%$

Data on Excess Rank

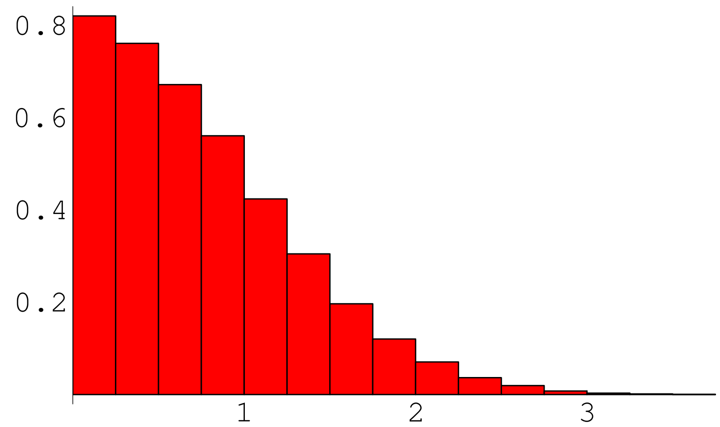
$$y^2 \; = \; x^3 + 16Tx + 32$$

Each data set runs over 2000 consecutive t-values.

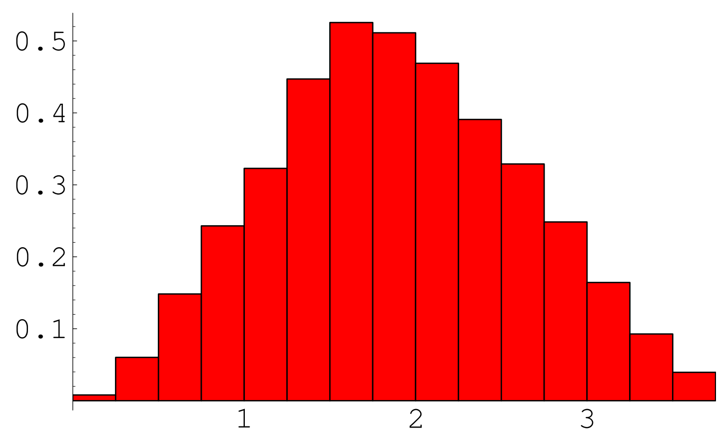
t-Start	Rk 0	Rk 1	Rk 2	Rk 3	Time (hrs)
-1000	39.4	47.8	12.3	0.6	<1
1000	38.4	47.3	13.6	0.6	<1
4000	37.4	47.8	13.7	1.1	1
8000	37.3	48.8	12.9	1.0	2.5
24000	35.1	50.1	13.9	0.8	6.8
50000	36.7	48.3	13.8	1.2	51.8

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

Theoretical Distribution of First Normalized Zero



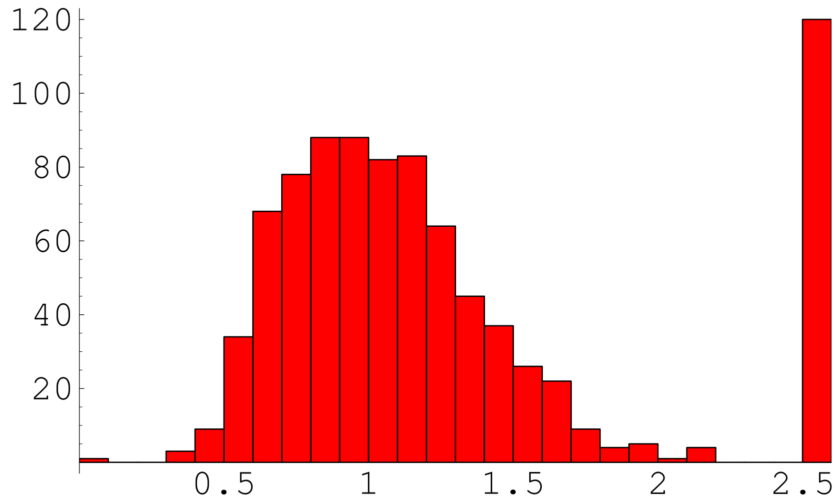
First normalized eigenvalue: 230,400 from SO(6) with Haar Measure



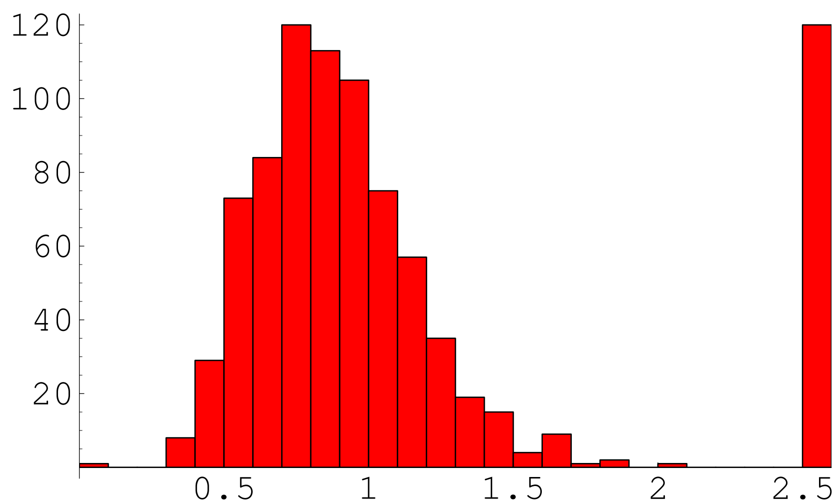
First normalized eigenvalue: 322,560 from SO(7) with Haar Measure

Rank 0 Curves: 1st Normalized Zero

(Far left and right bins just for formatting)

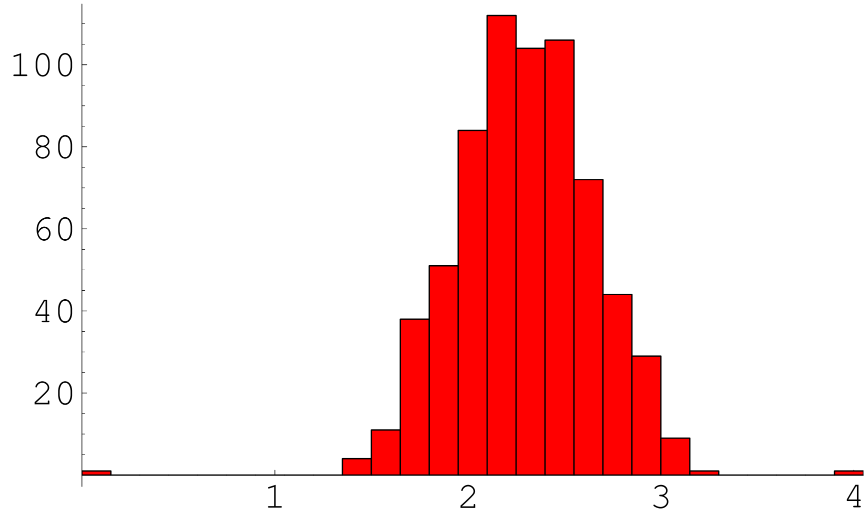


750 **curves**, $\log(\textbf{cond}) \in [3.2, 12.6]$; **mean** $= 1.04$

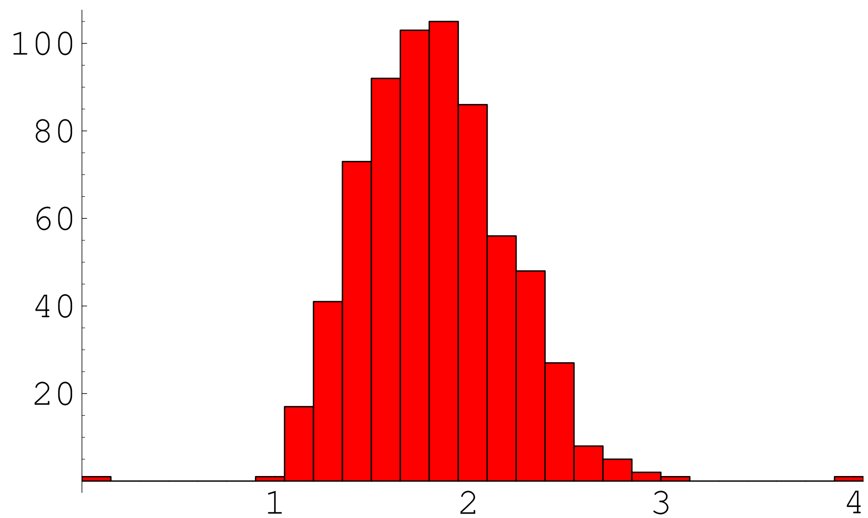


750 **curves**, $\log(\textbf{cond}) \in [12.6, 14.9]$; **mean** $= .88$

Rank 2 Curves: 1st Normalized Zero

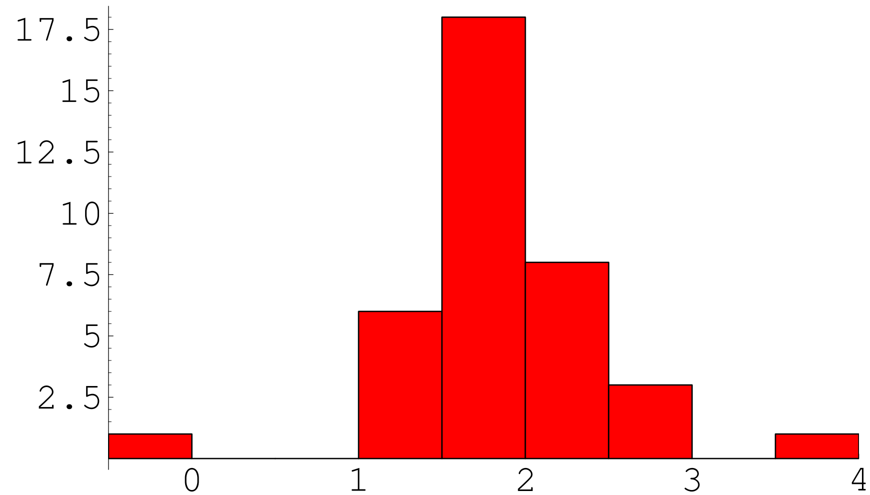


665 **curves**, $\log(\textbf{cond}) \in [10, 10.3125]$; **mean** $= 2.30$

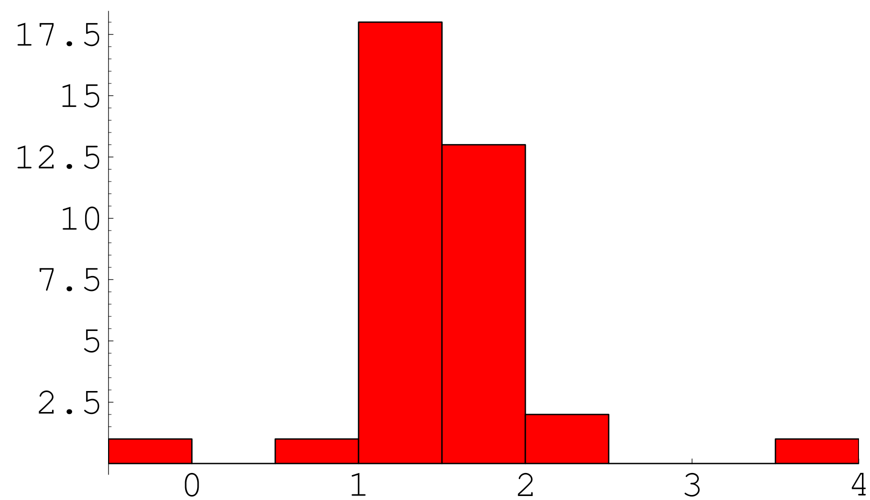


665 **curves**, $\log(\textbf{cond}) \in [16, 16.5]$; **mean** $= 1.82$

Rank 2 Curves: $y^2 = x^3 - T^2x + T^2$: 1st Normalized Zero



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



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

PART VI

CONCLUSIONS

Correspondences

Similarities between Heavy 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

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)?

APPENDICES

Appendix I: Standard Conjectures

Generalized Riemann Hypothesis (for Elliptic Curves) *Let $L(s, E)$ be the (normalized) L-function of the elliptic curve E. Then the non-trivial zeros of $L(s, E)$ satisfy Re$(s) = \frac{1}{2}$.*

Birch and Swinnerton-Dyer Conjecture [BSD1], [BSD2] *Let E be an elliptic curve of geometric rank r over $\mathbb{Q}$ (the Mordell-Weil group is $\mathbb{Z}^r \oplus T$, T is the subset of torsion points). Then the analytic rank (the order of vanishing of the L-function at the central point) is also r.*

Tate's Conjecture for Elliptic Surfaces [Ta] *Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E}, s)$ be the L-series attached to $H^2_{ét}(\mathcal{E}/\overline{\mathbb{Q}}, \mathbb{Q}_l)$. Then $L_2(\mathcal{E}, s)$ has a meromorphic continuation to **C** and satisfies $-ord_{s=2}L_2(\mathcal{E}, s) =$ rank $NS(\mathcal{E}/\mathbb{Q})$, where $NS(\mathcal{E}/\mathbb{Q})$ is the $\mathbb{Q}$-rational part of the Néron-Severi group of $\mathcal{E}$. Further, $L_2(\mathcal{E}, s)$ does not vanish on the line Re$(s) = 2$.*

Most of the 1-param families we investigate are rational surfaces, where Tate's conjecture is known. See [RSi].

Appendix II: Equidistribution of Signs

ABC Conjecture *Fix $\epsilon > 0$. For co-prime positive integers a, b and c with $c = a + b$ and $N(a,b,c) = \prod_{p|abc} p$, $c \ll_\epsilon N(a,b,c)^{1+\epsilon}$.*

The full strength of ABC is never needed; rather, we need a consequence of ABC, the Square-Free Sieve (see [Gr]):

Square-Free Sieve Conjecture *Fix an irreducible polynomial $f(t)$ of degree at least 4. As $N \to \infty$, the number of $t \in [N, 2N]$ with $f(t)$ divisible by p^2 for some $p > \log N$ is $o(N)$.*

For irreducible polynomials of degree at most 3, the above is known, complete with a better error than $o(N)$ ([Ho], chapter 4).

Restricted Sign Conjecture (for the Family $\mathcal{F}$) *Consider a one-parameter family $\mathcal{F}$ of elliptic curves. As $N \to \infty$, the signs of the curves E_t are equidistributed for $t \in [N, 2N]$.*

The Restricted Sign conjecture often fails. First, there are families with constant $j(E_t)$ where all curves have the same sign. Helfgott [He] has recently related the Restricted Sign conjecture to the Square-Free Sieve conjecture and standard conjectures on sums of Moebius:

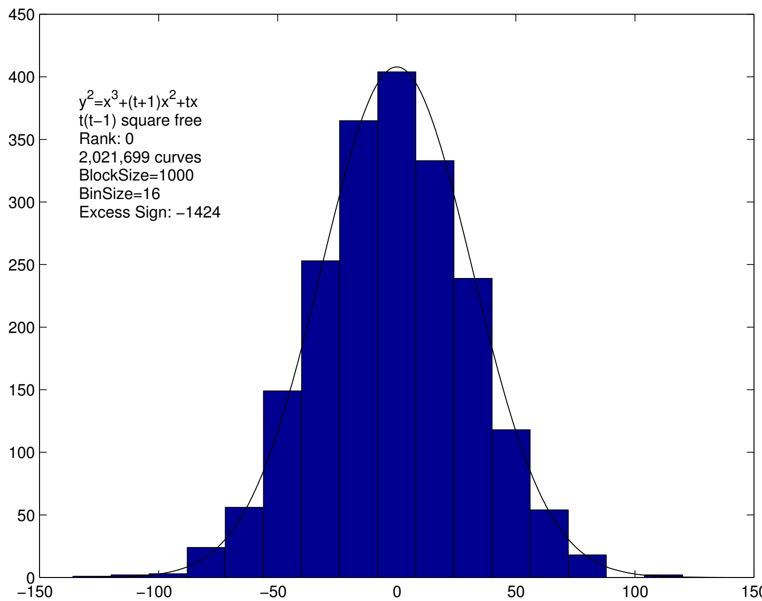
Polynomial Moebius *Let $f(t)$ be a non-constant polynomial such that no fixed square divides $f(t)$ for all t. Then $\sum_{t=N}^{2N} \mu(f(t)) = o(N)$.*

The Polynomial Moebius conjecture is known for linear $f(t)$.

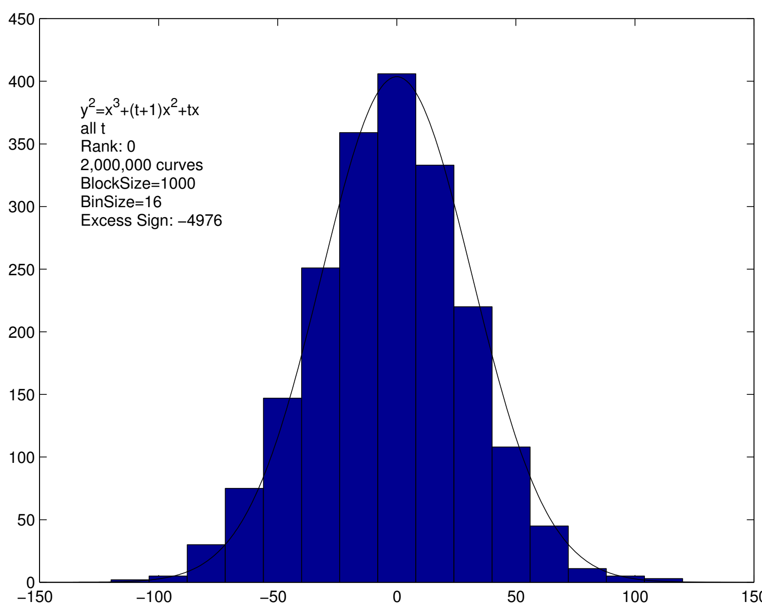
Helfgott shows the Square-Free Sieve and Polynomial Moebius imply the Restricted Sign conjecture for many families. More precisely, let $M(t)$ be the product of the irreducible polynomials dividing $\Delta(t)$ and not $c_4(t)$.

Theorem: Equidistribution of Sign in a Family [He]: *Let $\mathcal{F}$ be a one-parameter family with $a_i(t) \in \mathbb{Z}[t]$. If $j(E_t)$ and $M(t)$ are non-constant, then the signs of E_t, $t \in [N, 2N]$, are equidistributed as $N \to \infty$. Further, if we restrict to good t, $t \in [N, 2N]$ such that $D(t)$ is good (usually square-free), the signs are still equidistributed in the limit.*

Distribution of Signs: $y^2 = x^3 + (T+1)x^2 + Tx$

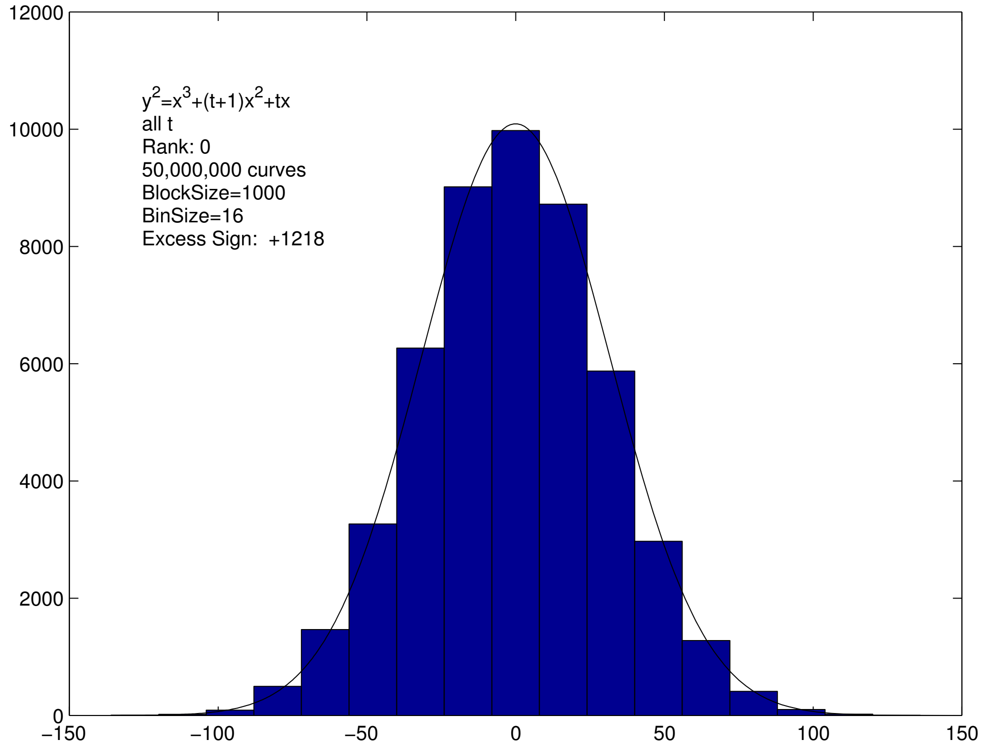


Histogram plot: $D(t)$ sq-free, first $2 \cdot 10^6$ such t.



Histogram plot: All $t \in [2, 2 \cdot 10^6]$.

Distribution of signs: $y^2 = x^3 + (T+1)x^2 + Tx$



Histogram plot: All $t \in [2, 5 \cdot 10^7]$

The observed behavior agrees with the predicted behavior. Note as the number of curves increase (comparing the plot of $5 \cdot 10^7$ points to $2 \cdot 10^6$ points), the fit to the Gaussian improves.

Graphs by Atul Pokharel

Appendix III: Numerically Approximating Ranks: Preliminaries

Cusp form f, level N, weight 2:

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

Define

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

Get

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

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

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

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

Differentiate k times with respect to s:

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

At $s = 1$,

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

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

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

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

Integrating by parts

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

We obtain

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

where

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

Expansion of $G_r(x)$

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

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

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

For $r = 0$,

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

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

Appendix IV: Bounding Excess Rank

$$D_{1,\mathcal{F}}(\phi_1) = \widehat{\phi}_1(0) + \frac{1}{2}\phi_1(0) + r\phi_1(0).$$

To estimate the percent with rank at least $r + R$, P_R, we get

$$R\phi_1(0)P_R \leq \widehat{\phi}_1(0) + \frac{1}{2}\phi_1(0), \; R > 1.$$

Note the family rank r has been cancelled from both sides.

The 2-level density gives ***squares*** of the rank on the left, get a cross term rR.

The disadvantage is our support is smaller.

Once R is large, the 2-level density yields better results. We now give more details.

n-Level Density and Excess Rank Bounds

For $n = 1$ and 2, consider the test functions

$$\begin{aligned}\widehat{f}_i(u) &= \frac{1}{2}\left(\frac{1}{2}\sigma_n - \frac{1}{2}|u|\right), \ |u| \leq \sigma \\ f_i(x) &= \frac{\sin^2(2\pi\frac{1}{2}\sigma_n x)}{(2\pi x)^2}.\end{aligned}$$

Expect $\sigma_2 = \frac{\sigma_1}{2}$; only able to prove for $\sigma_2 = \frac{\sigma_1}{4}$.

Note $f_i(0) = \frac{\sigma_n^2}{4}$, $\widehat{f}_i(0) = f_i(0)\frac{1}{\sigma_n}$.

Assume B-SD, Equidistribution of Sign

Notation

Family with rank r, $D_{1,\mathcal{F}}(f) = \widehat{f}(0) + \frac{1}{2}f(0) + rf(0)$.

By even (odd) we mean a curve whose rank r_E has $r_E - r$ even (odd).

P_0: probability even curve has rank $\geq r + 2a_0$.

P_1: probability odd curve has rank $\geq r + 1 + 2b_0$.

$$D_{1,\mathcal{F}}(f) = \frac{1}{|\mathcal{F}_N|} \sum_{E \in \mathcal{F}} \sum_{\gamma_E} f\left(\frac{\log N_E}{2\pi}\gamma_E\right),$$

γ_E is the imaginary part of the zeros.

Average Rank: 1-Level Bounds

$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} r_E f(0) \ \leq\ \widehat{f_1}(0) + \frac{1}{2}f_1(0) + r f_1(0)$$
$$\frac{1}{|\mathcal{F}|}\sum_{E\in\mathcal{F}} r_E \ \leq\ \frac{1}{\sigma_1} + \frac{1}{2} + r.$$

- All Curves: $r = 0$, $\sigma = \frac{4}{7}$, giving 2.25 (Brumer, Heath-Brown: [Br], [BHB3], [BHB5])
- 1-Parameter Families: $\left(\deg(N(t)) + r + \frac{1}{2}\right)\cdot(1 + o(1))$ (Silverman [Si3]).

Hope 1-Level Density true for $\sigma \to \infty$.

Would yield average rank is $r + \frac{1}{2}$.

Excess Rank: 1-Level Bounds

Assume half even, half odd.

Even curves: $1 - P_0$ have rank $\leq r + 2a_0 - 2$; replace ranks with r. P_0 have rank $\geq r + 2a_0$; replace with $r + 2a_0$.

Odd curves: $1 - P_1$ contributing $r + 1$. P_1 contributing $r + 1 + 2b_0$.

$$\begin{aligned}
\frac{1}{\sigma_1} + \frac{1}{2} + r &\geq \frac{1}{2}\Big[(1 - P_0)r + P_0(r + 2a_0)\Big] \\
&\quad + \frac{1}{2}\Big[(1 - P_1)(r + 1) + P_1(r + 1 + 2b_0)\Big] \\
\frac{1}{\sigma_1} &\geq a_0 P_0 + b_0 P_1.
\end{aligned}$$

1-Level Density Bounds for Excess Rank

$$\begin{aligned}
P_0 &\leq \frac{1}{a_0\sigma_1} \\
P_1 &\leq \frac{1}{b_0\sigma_1} \\
\text{Prob}\{\text{rank} \geq r + 2a_0\} &\leq \frac{1}{a_0\sigma_1}.
\end{aligned}$$

2-Level Bounds:

$$\begin{aligned} D_{2,\mathcal{F}}(f) &= D^*_{2,\mathcal{F}}(f) - 2D_{1,\mathcal{F}}(f_1 f_2) + f_1(0) f_2(0) N(\mathcal{F}, -1) \\ D^*_{2,\mathcal{F}}(f) &= \prod_{i=1}^{2} \left[\widehat{f_i}(0) + \frac{1}{2} f_i(0) \right] + 2 \int |u| \widehat{f_1}(u) \widehat{f_2}(u) du \\ &\quad + r \widehat{f_1}(0) f_2(0) + r f_1(0) \widehat{f_2}(0) + (r^2 + r) f_1(0) f_2(0) \\ D_{1,\mathcal{F}}(f) &= \widehat{f}(0) + \frac{1}{2} f(0) + r f(0). \end{aligned}$$

$D^*_{2,\mathcal{F}}(f)$ is over all zeros. Gives

$$\begin{aligned} \frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} r_E^2 &\le \frac{1}{\sigma_2^2} + \frac{1}{\sigma_2} + \frac{1}{4} + \frac{1}{3} + \frac{2r}{\sigma_2} + r^2 + r \\ &= \frac{1}{\sigma_2^2} + \frac{2r+1}{\sigma_2} + \frac{1}{12} + r^2 + r + \frac{1}{2}. \end{aligned}$$

Excess Rank: 2-Level Bounds: I

Similar proof yields

Theorem: First 2-Level Density Bounds

$$P_0 \ \le \ \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24} + \frac{r+\frac{1}{2}}{\sigma_2}}{a_0(a_0+r)}$$

$$P_1 \ \le \ \frac{\frac{1}{2\sigma_2^2} + \frac{1}{24} + \frac{r+\frac{1}{2}}{\sigma_2}}{b_0(b_0+r+1)}.$$

For $\sigma_2 = \frac{\sigma_1}{4}$, $r = 0$, $a_1 = 1$: ***worse*** than 1-level density.

For fixed $\sigma_2 = \frac{\sigma_1}{4}$ and r, as we increase a_0 we eventually do get a better bound.

Proportional to $\frac{1}{(a_0\sigma_1)^2}$ instead of $\frac{1}{a_0\sigma_1}$.

Excess Rank: 2-Level Bounds: II

Use $D_{2,\mathcal{F}}(f)$ instead of $D^*_{2,\mathcal{F}}(f)$.

$r_E \;=\;$ number of zeros of curve E. Sum over $j_1 \neq j_2$.

r_E even, get $r_E(r_E-2)$ (each zero matched with r_E-2 others).

r_E odd: $(r_E-1)(r_E-2)+(r_E-1) = r_E(r_E-2)+1$.

Theorem: Second 2-Level Density Bounds

$$\begin{aligned} P_0 &\leq \frac{\frac{1}{2\sigma_2^2}+\frac{1}{24}+\frac{r}{\sigma_2}-\frac{1}{6\sigma_2}}{a_0(a_0+r-1)} \\ P_1 &\leq \frac{\frac{1}{2\sigma_2^2}+\frac{1}{24}+\frac{r}{\sigma_2}-\frac{1}{6\sigma_2}}{b_0(b_0+r)}, \end{aligned}$$

where $a_0 \neq 1$ if $r=0$.

$\sigma_2 = \frac{\sigma_1}{4}$ and $r=0$, better for $a_0 > \frac{\sigma_1^2+8\sigma_1+192}{24\sigma_1}$.
$r=1$, better for $a_0 > \frac{\sigma_1^2+80\sigma_1+192}{24\sigma_1}$.

Decay is proportional to $\frac{1}{(a_0\sigma_1)^2}$.
Note the numerator is never negative; at least $\frac{1}{18}$.

Excess Rank: 2-Level Bounds: IIIa

$$r_E \;=\; r + z_E.$$

$\sum_{j_1}\sum_{j_2} f_1(L\gamma_{E_{j_1}})f_2(L\gamma_{E_{j_2}})$. Let j_1 be one of the r family zeros, varying j_2 gives $f_1(0)D_{1,E}(f_2)$. Interchanging j_1 and j_2 we get a contribution of $D_{1,E}(f_1)f_2(0)$ for each of the r family.

Only double counting when j_1 and j_2 are both a family zero. Subtract off $r^2 f_1(0)f_2(0)$. For the other z_E zeros: already taken into account contribution from j_1 one of the z_E zeros and j_2 one of the r family zeros (and vice-versa).

Thus, for a given curve, a lower bound of the contribution from all pairs (j_1, j_2) is

$$r f_1(0)D_{1,E}(f_2) + rD_{1,E}(f_1)f_2(0) - r^2 f_1(0)f_2(0) + z_E^2.$$

Excess Rank: 2-Level Bounds: IIIb

Summing over all $E \in \mathcal{F}$ and simplifying gives

$$\frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} z_E^2 \ \leq \ \frac{1}{\sigma_2^2} + \frac{1}{\sigma_2} + \frac{1}{12} + \frac{1}{2}.$$

Similar calculation gives

Theorem: Third 2-Level Density Bounds

$$P_0 \ \leq \ \frac{\frac{1}{2\sigma_2^2} + \frac{1}{2\sigma_2} + \frac{1}{24}}{a_0^2}$$

$$P_1 \ \leq \ \frac{\frac{1}{2\sigma_2^2} + \frac{1}{2\sigma_2} + \frac{1}{24}}{b_0 + b_0^2}$$

$\sigma_2 = \frac{\sigma_1}{4}$: beats 1-level for $a_0 > \frac{\sigma_1^2 + 48\sigma_1 + 192}{24\sigma_1}$.
$r \neq 0$: beats first 2-level once $a_0 > \frac{\sigma_1^2 + 48\sigma_1 + 192}{96\sigma_1}$.

$r \geq 1$: beats second 2-level once $a_0 > \frac{3(r-1)}{3r-2} \frac{\sigma_1^2 + 48\sigma_1 + 192}{96\sigma_1}$.

Heath-Brown & Brumer

Family of all elliptic curves $E_{a,b}$:

$$\mathcal{F}_T \;=\; \{y^2 = x^3 + ax + b; |a| \le T^{\frac{1}{3}}, |b| \le T^{\frac{1}{2}}.$$

From 1-Level Expansion, get

$$r(E_{a,b}) \;\le\; 2 + \frac{\log T}{\log X} - 2\sum_{p \le X} a_P(E_{a,b}) h\left(\frac{\log p}{\log X}\right) + O\left(\frac{1}{\log X}\right).$$

If $r(E_{a,b}) \ge r \ge 3 + 2\frac{\log T}{\log X}$, then $|U(E_{a,b}, X)| \ge \frac{\log T}{2}$.

Led to

$$\#\{E_{a,b} \in \mathcal{F}_T : r(E_{a,b}) \ge r\} \cdot \left(\frac{\log T}{2}\right)^{2k} \;\le\; \sum_{E_{a,b} \in \mathcal{F}} |U(E_{a,b}, X)|^{2k}.$$

Find $X = T^{\frac{1}{10k}}$, $k = \left[\frac{r-3}{20}\right]$. Yields

$$\begin{aligned} \text{Prob}\,(\text{rank}(E_{a,b}) \ge r) &\ll (11r)^{-\frac{r}{20}} \\ \text{rank}(E_{a,b}) &\le 17\frac{\log T}{\log\log T}. \end{aligned}$$

APPENDIX V:
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 **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/∼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/$\sim$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.