Finite conductor models for zeros near the central point of elliptic curve L-functions

Steven J Miller (MC '96)
Dept of Math/Stats, Williams College

sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu
http://www.williams.edu/Mathematics/sjmiller
Joint with E. Dueñez, D. Huynh, J. P. Keating, N. C. Snaith

BC Number Theory / Algebraic Geometry Seminar
Boston College, April 30th, 2015

Introduction

Maass waveforms and low-lying zeros (with Levent Alpoge, Nadine Amersi, Geoffrey Iyer, Oleg Lazarev and Liyang Zhang), preprint 2014.

http://arxiv.org/pdf/1306.5886.pdf

Properties of zeros of L-functions

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

Distribution of zeros

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

Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem intractable.

Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem intractable.

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

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

Fundamental Equation:

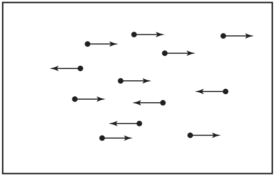
$$H\psi_n = E_n\psi_n$$

H : matrix, entries depend on system

E_n : energy levels

ψ_n : energy eigenfunctions

Origins of Random Matrix Theory



- Statistical Mechanics: for each configuration, calculate quantity (say pressure).
- Average over all configurations – most configurations close to system average.
- Nuclear physics: choose matrix at random, calculate eigenvalues, average over matrices (real Symmetric $A = A^T$, complex Hermitian $\overline{A}^T = A$).

Random Matrix Ensembles

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

Fix p, define

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

This means

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

Want to understand eigenvalues of A.

Measures of Spacings: *n*-Level Correlations

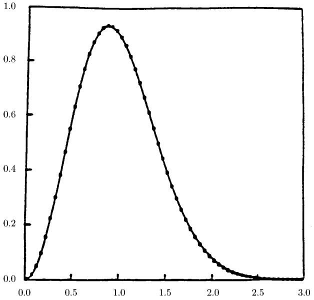
$\{\alpha_j\}$ increasing sequence of numbers, $B \subset \mathbb{R}^{n-1}$ a compact box. Define the *n*-level correlation by

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

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

Measures of Spacings: *n*-Level Correlations

1. Normalized spacings of $\zeta(s)$ starting at 10^{20}. (Odlyzko)



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

Measures of Spacings: *n*-Level Correlations

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

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

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

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

Measures of Spacings: *n*-Level Correlations

Let g_i be even Schwartz functions whose Fourier Transform is compactly supported, $L(s, f)$ an L-function with zeros $\frac{1}{2} + i\gamma_f$ and conductor Q_f:

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

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

Explicit Formula (Contour Integration)

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

Explicit Formula (Contour Integration)

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

Explicit Formula (Contour Integration)

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

$$= \frac{d}{ds}\sum_p \log\left(1-p^{-s}\right)$$

$$= \sum_p \frac{\log p \cdot p^{-s}}{1-p^{-s}} = \sum_p \frac{\log p}{p^s} + \mathrm{Good}(s).$$

Contour Integration:

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

Explicit Formula (Contour Integration)

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

$$= \frac{d}{ds}\sum_p \log\left(1-p^{-s}\right)$$

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

Contour Integration:

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

Explicit Formula (Contour Integration)

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

Contour Integration (see Fourier Transform arising):

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

Knowledge of zeros gives info on coefficients.

n-Level Density

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

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

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

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

Conjecture (Katz-Sarnak)

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

Testing Random Matrix Theory Predictions

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

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

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

Correspondences

Similarities between *L*-Functions and Nuclei:

$$\text{Zeros} \longleftrightarrow \text{Energy Levels}$$

$$\text{Schwartz test function} \longrightarrow \text{Neutron}$$

$$\text{Support of test function} \longleftrightarrow \text{Neutron Energy.}$$

Conjectures and Theorems for Families of Elliptic Curves

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

http://arxiv.org/pdf/math/0310159.

Tate's Conjecture

Tate's Conjecture for Elliptic Surfaces

Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E}, s)$ be the L-series attached to $H^2_{\text{ét}}(\mathcal{E}/\overline{\mathbb{Q}}, \mathbb{Q}_l)$. Then $L_2(\mathcal{E}, s)$ has a meromorphic continuation to $\mathbb{C}$ and satisfies

$$-\text{ord}_{s=2} L_2(\mathcal{E}, s) \; = \; \text{rank}\, NS(\mathcal{E}/\mathbb{Q}),$$

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 $\text{Re}(s) = 2$.

Conjectures: ABC, Square-Free

ABC Conjecture

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

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 $D(t)$ divisible by p^2 for some $p > \log N$ is $o(N)$.

Conjectures: Restricted Sign

Restricted Sign Conjecture (for the Family $\mathcal{F}$)

Consider a 1-parameter family $\mathcal{F}$ of elliptic curves. As $N \to \infty$, the signs of the curves E_t are equidistributed for $t \in [N, 2N]$.

Fails: constant $j(t)$ where all curves same sign.
Rizzo:

$$E_t : y^2 = x^3 + tx^2 - (t+3)x + 1, \ \ j(t) = 256(t^2 + 3t + 9),$$

for every $t \in \mathbb{Z}$, E_t has odd functional equation,

$$E_t : y^2 = x^3 + \frac{t}{4}x^2 - \frac{36t^2}{t - 1728}x - \frac{t^3}{t - 1728}, \ \ j(t) = t,$$

as t ranges over $\mathbb{Z}$ in the limit 50.1859% have even and 49.8141% have odd functional equation.

Conjectures: Polynomial Mobius

Polynomial Moebius

Let $f(t)$ be an irreducible polynomial such that no fixed square divides $f(t)$ for all t. Then $\sum_{t=N}^{2N} \mu(f(t)) = o(N)$.

Conjectures: Polynomial Mobius

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 Let $\mathcal{F}$ be a one-parameter family with coefficients integer polynomials in $t \in [N, 2N]$. If $j(t)$ 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.

Theorem: Preliminaries

Consider a one-parameter family

$$\mathcal{E}: y^2 + a_1(T)xy + a_3(T)y \ = \ x^3 + a_2(T)x^2 + a_4(T)x + a_6(T).$$

Let $a_t(p) = p + 1 - N_p$, where N_p is the number of solutions mod p (including ∞). Define

$$A_{\mathcal{E}}(p) \ := \ \frac{1}{p}\sum_{t(p)} a_t(p).$$

$A_{\mathcal{E}}(p)$ is bounded independent of p (Deligne).

Theorem: Preliminaries

Theorem

Rosen-Silverman (Conjecture of Nagao): For an elliptic surface (a one-parameter family), assume Tate's conjecture. Then

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p \le X} -A_{\mathcal{E}}(p) \log p \;=\; \operatorname{rank} \mathcal{E}(\mathbb{Q}(T)).$$

Tate's conjecture is known for rational surfaces: An elliptic surface $y^2 = x^3 + A(T)x + B(T)$ is rational iff one of the following is true:

- $0 < \max\{3\deg A, 2\deg B\} < 12$;
- $3\deg A = 2\deg B = 12$ and $\operatorname{ord}_{T=0} T^{12}\Delta(T^{-1}) = 0$.

Comparing the RMT Models

Theorem: M– '04

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

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

where

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

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

Data for Elliptic Curve Famillies
Dueñez, Huynh, Keating, Miller and Snaith

Investigations of zeros near the central point of elliptic curve L-functions, Experimental Mathematics **15** (2006), no. 3, 257–279.

http://arxiv.org/pdf/math/0508150.

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

http://arxiv.org/pdf/1005.1298.

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

http://arxiv.org/pdf/1107.4426.

Comparing the RMT Models

Theorem: M– ’04

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

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

where

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

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

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

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

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

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

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

Problem: small data sets, sub-families, convergence rate log(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 $\sum_{p \le x} 1/p \sim \log\log x$.

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).

$$\begin{aligned} \text{Rank } r &= 28.60\% & \text{Rank } r+1 &= 47.56\% \\ \text{Rank } r+2 &= 20.97\% & \text{Rank } r+3 &= 2.79\% \\ \text{Rank } r+4 &= .08\% \end{aligned}$$

Data on excess rank (cont)

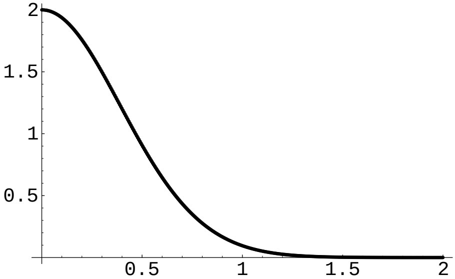
$$y^2 = x^3 + 16Tx + 32$$

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

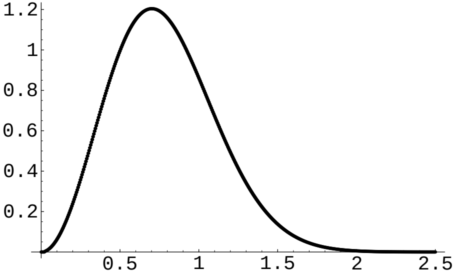
Final conductors $\sim 10^{11}$, small on log scale.

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



1st normalized evalue above 1: SO(even)

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



1st normalized evalue above 1: SO(odd)

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

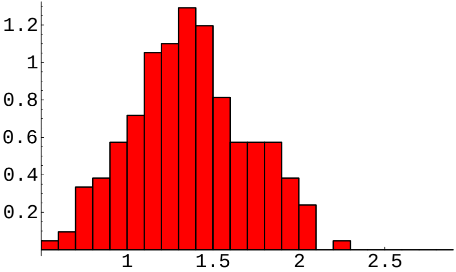


Figure 4a: 209 rank 0 curves from 14 rank 0 families, $\log(\mathrm{cond}) \in [3.26, 9.98]$, median $= 1.35$, mean $= 1.36$

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

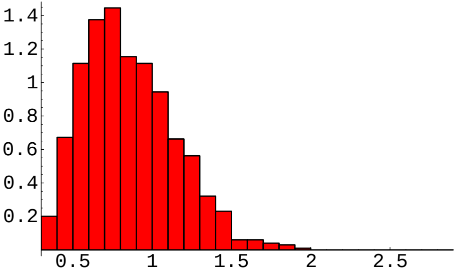


Figure 4b: 996 rank 0 curves from 14 rank 0 families, $\log(\text{cond}) \in [15.00, 16.00]$, median $= .81$, mean $= .86$.

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

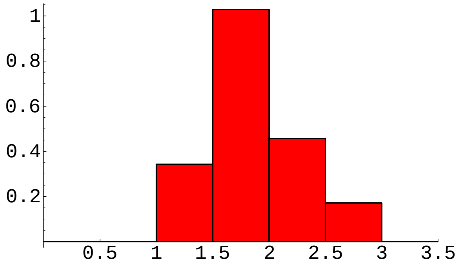


Figure 5*a*: 35 curves, $\log(\text{cond}) \in [7.8, 16.1]$, $\widetilde{\mu} = 1.85$, $\mu = 1.92$, $\sigma_\mu = .41$

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

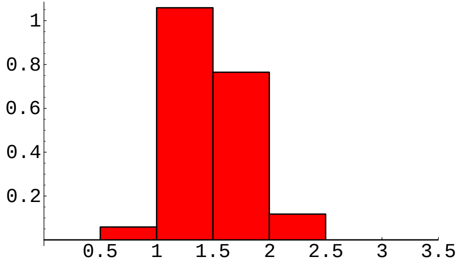


Figure 5*b*: 34 curves, $\log(\text{cond}) \in [16.2, 23.3]$, $\widetilde{\mu} = 1.37$, $\mu = 1.47$, $\sigma_\mu = .34$

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

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

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

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

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

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

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

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

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

Summary of Data

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

New Model for Finite Conductors

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

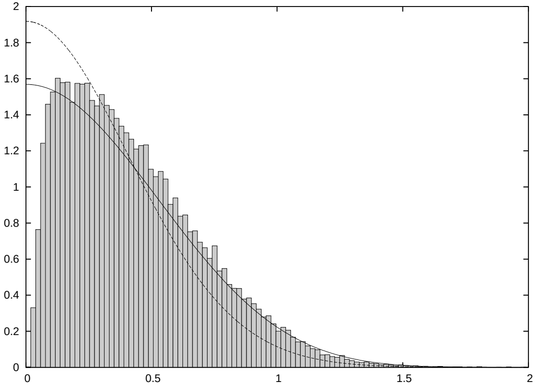
- Excised Orthogonal Ensembles.
  - ◇ $L(1/2, E)$ discretized.
  - ◇ Study matrices in $\mathrm{SO}(2N_{eff})$ with $|\Lambda_A(1)| \geq ce^N$.

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

Open Problem:

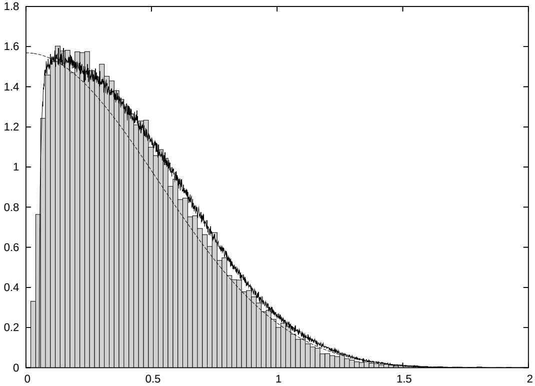
Generalize to other families (Owen Barrett, Nathan Ryan, ...).

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



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

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



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

Ratio's Conjecture

History

- Farmer (1993): Considered

$$\int_0^T \frac{\zeta(s+\alpha)\zeta(1-s+\beta)}{\zeta(s+\gamma)\zeta(1-s+\delta)}\, dt,$$

conjectured (for appropriate values)

$$T\frac{(\alpha+\delta)(\beta+\gamma)}{(\alpha+\beta)(\gamma+\delta)} - T^{1-\alpha-\beta}\frac{(\delta-\beta)(\gamma-\alpha)}{(\alpha+\beta)(\gamma+\delta)}.$$

History

- Farmer (1993): Considered

$$\int_0^T \frac{\zeta(s+\alpha)\zeta(1-s+\beta)}{\zeta(s+\gamma)\zeta(1-s+\delta)}\, dt,$$

conjectured (for appropriate values)

$$T\frac{(\alpha+\delta)(\beta+\gamma)}{(\alpha+\beta)(\gamma+\delta)} - T^{1-\alpha-\beta}\frac{(\delta-\beta)(\gamma-\alpha)}{(\alpha+\beta)(\gamma+\delta)}.$$

- Conrey-Farmer-Zirnbauer (2007): conjecture formulas for averages of products of L-functions over families:

$$R_{\mathcal{F}} = \sum_{f\in\mathcal{F}} \omega_f \frac{L\left(\frac{1}{2}+\alpha, f\right)}{L\left(\frac{1}{2}+\gamma, f\right)}.$$

Uses of the Ratios Conjecture

- Applications:
  ◇ n-level correlations and densities;
  ◇ mollifiers;
  ◇ moments;
  ◇ vanishing at the central point;

- Advantages:
  ◇ RMT models often add arithmetic ad hoc;
  ◇ predicts lower order terms, often to square-root level.

Inputs for 1-level density

- Approximate Functional Equation:

$$L(s,f) = \sum_{m\le x} \frac{a_m}{m^s} + \epsilon \mathbb{X}_L(s) \sum_{n\le y} \frac{a_n}{n^{1-s}};$$

◇ ϵ sign of the functional equation,
◇ $\mathbb{X}_L(s)$ ratio of Γ-factors from functional equation.

Inputs for 1-level density

- Approximate Functional Equation:

$$L(s,f) = \sum_{m \le x} \frac{a_m}{m^s} + \epsilon \mathbb{X}_L(s) \sum_{n \le y} \frac{a_n}{n^{1-s}};$$

◇ ϵ sign of the functional equation,
◇ $\mathbb{X}_L(s)$ ratio of Γ-factors from functional equation.

- Explicit Formula: g Schwartz test function,

$$\sum_{f \in \mathcal{F}} \omega_f \sum_{\gamma} g\left(\gamma \frac{\log N_f}{2\pi}\right) = \frac{1}{2\pi i} \int_{(c)} - \int_{(1-c)} R'_{\mathcal{F}}(\cdots) g(\cdots)$$

◇ $R'_{\mathcal{F}}(r) = \frac{\partial}{\partial \alpha} R_{\mathcal{F}}(\alpha,\gamma)\Big|_{\alpha=\gamma=r}$.

Procedure (Recipe)

- Use approximate functional equation to expand numerator.

Procedure (Recipe)

- Use approximate functional equation to expand numerator.
- Expand denominator by generalized Mobius function: cusp form

$$\frac{1}{L(s,f)} = \sum_h \frac{\mu_f(h)}{h^s},$$

where $\mu_f(h)$ is the multiplicative function equaling 1 for $h = 1$, $-\lambda_f(p)$ if $n = p$, $\chi_0(p)$ if $h = p^2$ and 0 otherwise.

Procedure (Recipe)

- Use approximate functional equation to expand numerator.
- Expand denominator by generalized Mobius function: cusp form
$$\frac{1}{L(s,f)} = \sum_h \frac{\mu_f(h)}{h^s},$$
where $\mu_f(h)$ is the multiplicative function equaling 1 for $h = 1$, $-\lambda_f(p)$ if $n = p$, $\chi_0(p)$ if $h = p^2$ and 0 otherwise.
- Execute the sum over $\mathcal{F}$, keeping only main (diagonal) terms.

Procedure (Recipe)

- Use approximate functional equation to expand numerator.
- Expand denominator by generalized Mobius function: cusp form

$$\frac{1}{L(s,f)} = \sum_h \frac{\mu_f(h)}{h^s},$$

where $\mu_f(h)$ is the multiplicative function equaling 1 for $h = 1$, $-\lambda_f(p)$ if $n = p$, $\chi_0(p)$ if $h = p^2$ and 0 otherwise.
- Execute the sum over $\mathcal{F}$, keeping only main (diagonal) terms.
- Extend the m and n sums to infinity (complete the products).

Procedure (Recipe)

- Use approximate functional equation to expand numerator.
- Expand denominator by generalized Mobius function: cusp form
$$\frac{1}{L(s,f)} = \sum_h \frac{\mu_f(h)}{h^s},$$
where $\mu_f(h)$ is the multiplicative function equaling 1 for $h = 1$, $-\lambda_f(p)$ if $n = p$, $\chi_0(p)$ if $h = p^2$ and 0 otherwise.
- Execute the sum over $\mathcal{F}$, keeping only main (diagonal) terms.
- Extend the m and n sums to infinity (complete the products).
- Differentiate with respect to the parameters.

Procedure ('Illegal Steps')

- Use approximate functional equation to expand numerator.
- Expand denominator by generalized Mobius function: cusp form

$$\frac{1}{L(s,f)} = \sum_h \frac{\mu_f(h)}{h^s},$$

where $\mu_f(h)$ is the multiplicative function equaling 1 for $h = 1$, $-\lambda_f(p)$ if $n = p$, $\chi_0(p)$ if $h = p^2$ and 0 otherwise.
- Execute the sum over $\mathcal{F}$, keeping only main (diagonal) terms.
- Extend the m and n sums to infinity (complete the products).
- Differentiate with respect to the parameters.

1-Level Prediction from Ratio's Conjecture

$$\begin{aligned} & A_E(\alpha,\gamma) \\ = \quad & Y_E^{-1}(\alpha,\gamma) \times \prod_{p|M}\left(\sum_{m=0}^{\infty}\left(\frac{\lambda(p^m)\omega_E^m}{p^{m(1/2+\alpha)}} - \frac{\lambda(p)}{p^{1/2+\gamma}}\frac{\lambda(p^m)\omega_E^{m+1}}{p^{m(1/2+\alpha)}}\right)\right) \times \\ & \prod_{p\nmid M}\left(1+\frac{p}{p+1}\left(\sum_{m=1}^{\infty}\frac{\lambda(p^{2m})}{p^{m(1+2\alpha)}} - \frac{\lambda(p)}{p^{1+\alpha+\gamma}}\sum_{m=0}^{\infty}\frac{\lambda(p^{2m+1})}{p^{m(1+2\alpha)}} \right.\right. \\ & \left.\left. + \frac{1}{p^{1+2\gamma}}\sum_{m=0}^{\infty}\frac{\lambda(p^{2m})}{p^{m(1+2\alpha)}}\right)\right) \end{aligned}$$

where

$$Y_E(\alpha,\gamma) = \frac{\zeta(1+2\gamma)L_E(\mathrm{sym}^2,1+2\alpha)}{\zeta(1+\alpha+\gamma)L_E(\mathrm{sym}^2,1+\alpha+\gamma)}.$$

Huynh, Morrison and Miller confirmed Ratios' prediction, which is

1-Level Prediction from Ratio's Conjecture

$$\frac{1}{X^*}\sum_{d\in\mathcal{F}(X)}\sum_{\gamma_d} g\left(\frac{\gamma_d L}{\pi}\right)$$

$$= \frac{1}{2LX^*}\int_{-\infty}^{\infty} g(\tau)\sum_{d\in\mathcal{F}(X)}\left[2\log\left(\frac{\sqrt{M}|d|}{2\pi}\right)+\frac{\Gamma'}{\Gamma}\left(1+\frac{i\pi\tau}{L}\right)+\frac{\Gamma'}{\Gamma}\left(1-\frac{i\pi\tau}{L}\right)\right]d\tau$$

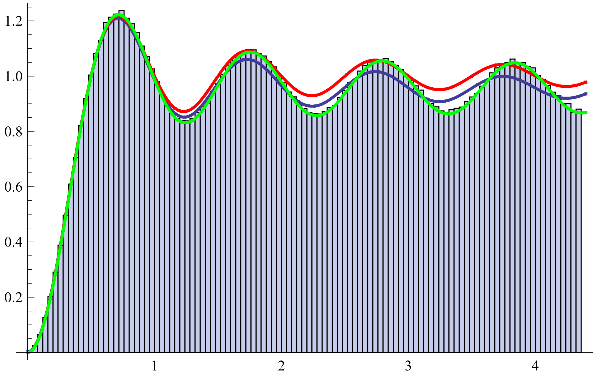
$$+\frac{1}{L}\int_{-\infty}^{\infty} g(\tau)\left(-\frac{\zeta'}{\zeta}\left(1+\frac{2\pi i\tau}{L}\right)+\frac{L_E'}{L_E}\left(\mathrm{sym}^2,1+\frac{2\pi i\tau}{L}\right)-\sum_{\ell=1}^{\infty}\frac{(M^\ell-1)\log M}{M^{\left(2+\frac{2i\pi\tau}{L}\right)\ell}}\right)d\tau$$

$$-\frac{1}{L}\sum_{k=0}^{\infty}\int_{-\infty}^{\infty} g(\tau)\frac{\log M}{M^{(k+1)(1+\frac{\pi i\tau}{L})}}d\tau+\frac{1}{L}\int_{-\infty}^{\infty} g(\tau)\sum_{p\nmid M}\frac{\log p}{(p+1)}\sum_{k=0}^{\infty}\frac{\lambda(p^{2k+2})-\lambda(p^{2k})}{p^{(k+1)(1+\frac{2\pi i\tau}{L})}}d\tau$$

$$-\frac{1}{LX^*}\int_{-\infty}^{\infty} g(\tau)\sum_{d\in\mathcal{F}(X)}\left[\left(\frac{\sqrt{M}|d|}{2\pi}\right)^{-2i\pi\tau/L}\frac{\Gamma(1-\frac{i\pi\tau}{L})}{\Gamma(1+\frac{i\pi\tau}{L})}\frac{\zeta(1+\frac{2i\pi\tau}{L})L_E(\mathrm{sym}^2,1-\frac{2i\pi\tau}{L})}{L_E(\mathrm{sym}^2,1)}\right.$$

$$\left.\times A_E\left(-\frac{i\pi\tau}{L},\frac{i\pi\tau}{L}\right)\right]d\tau+O(X^{-1/2+\varepsilon});$$

Numerics (J. Stopple): 1,003,083 negative fundamental discriminants $-d \in [10^{12}, 10^{12} + 3.3 \cdot 10^6]$



Histogram of normalized zeros ($\gamma \leq 1$, about 4 million).

$\diamond$ Red: main term. $\diamond$ Blue: includes $O(1/\log X)$ terms.

$\diamond$ Green: all lower order terms.

Excised Orthogonal Ensembles

Excised Orthogonal Ensemble: Preliminaries

Characteristic polynomial of $A \in \mathrm{SO}(2N)$ is

$$\Lambda_A(e^{i\theta}, N) := \det(I - Ae^{-i\theta}) = \prod_{k=1}^{N}(1 - e^{i(\theta_k - \theta)})(1 - e^{i(-\theta_k - \theta)}),$$

with $e^{\pm i\theta_1}, \dots, e^{\pm i\theta_N}$ the eigenvalues of A.

Motivated by the arithmetical size constraint on the central values of the L-functions, consider Excised Orthogonal Ensemble $T_{\mathcal{X}}$: $A \in \mathrm{SO}(2N)$ with $|\Lambda_A(1, N)| \geq \exp(\mathcal{X})$.

One-Level Densities

One-level density $R_1^{G(N)}$ for a (circular) ensemble $G(N)$:

$$R_1^{G(N)}(\theta) = N \int \dots \int P(\theta, \theta_2, \dots, \theta_N) d\theta_2 \dots d\theta_N,$$

where $P(\theta, \theta_2, \dots, \theta_N)$ is the joint probability density function of eigenphases.

One-Level Densities

One-level density $R_1^{G(N)}$ for a (circular) ensemble $G(N)$:

$$R_1^{G(N)}(\theta) = N \int \dots \int P(\theta, \theta_2, \dots, \theta_N) d\theta_2 \dots d\theta_N,$$

where $P(\theta, \theta_2, \dots, \theta_N)$ is the joint probability density function of eigenphases.
The one-level density excised orthogonal ensemble:

$$R_1^{T_{\mathcal{X}}}(\theta_1) := C_{\mathcal{X}} \cdot N \int_0^{\pi} \cdots \int_0^{\pi} H(\log|\Lambda_A(1,N)| - \mathcal{X}) \times \\ \times \prod_{j<k} (\cos\theta_j - \cos\theta_k)^2 d\theta_2 \cdots d\theta_N,$$

Here $H(x)$ denotes the Heaviside function

$$H(x) = \begin{cases} 1 \text{ for } x > 0 \\ 0 \text{ for } x < 0, \end{cases}$$

and $C_{\mathcal{X}}$ is a normalization constant

One-Level Densities

One-level density $R_1^{G(N)}$ for a (circular) ensemble $G(N)$:

$$R_1^{G(N)}(\theta) = N \int \dots \int P(\theta, \theta_2, \dots, \theta_N) d\theta_2 \dots d\theta_N,$$

where $P(\theta, \theta_2, \dots, \theta_N)$ is the joint probability density function of eigenphases.
The one-level density excised orthogonal ensemble:

$$R_1^{T_{\mathcal{X}}}(\theta_1) = \frac{C_{\mathcal{X}}}{2\pi i} \int_{c-i\infty}^{c+i\infty} 2^{Nr} \frac{\exp(-r\mathcal{X})}{r} R_1^{J_N}(\theta_1; r-1/2, -1/2) dr$$

where $C_{\mathcal{X}}$ is a normalization constant and

$$R_1^{J_N}(\theta_1; r-1/2, -1/2) = N \int_0^\pi \cdots \int_0^\pi \prod_{j=1}^N w^{(r-1/2,-1/2)}(\cos\theta_j) \times \prod_{j<k} (\cos\theta_j - \cos\theta_k)^2 d\theta_2 \cdots d\theta_N$$

is the one-level density for the Jacobi ensemble J_N with weight function

$$w^{(\alpha,\beta)}(\cos\theta) = (1-\cos\theta)^{\alpha+1/2}(1+\cos\theta)^{\beta+1/2}, \qquad \alpha = r - 1/2 \text{ and } \beta = -1/2.$$

Results

- With $C_{\mathcal{X}}$ normalization constant and $P(N, r, \theta)$ defined in terms of Jacobi polynomials,

$$R_1^{T_{\mathcal{X}}}(\theta) = \frac{C_{\mathcal{X}}}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{\exp(-r\mathcal{X})}{r} 2^{N^2+2Nr-N} \times \\ \times \prod_{j=0}^{N-1} \frac{\Gamma(2+j)\Gamma(1/2+j)\Gamma(r+1/2+j)}{\Gamma(r+N+j)} \times \\ \times (1-\cos\theta)^r \frac{2^{1-r}}{2N+r-1} \frac{\Gamma(N+1)\Gamma(N+r)}{\Gamma(N+r-1/2)\Gamma(N-1/2)} P(N, r, \theta)\, dr.$$

- Residue calculus implies $R_1^{T_{\mathcal{X}}}(\theta) = 0$ for $d(\theta, \mathcal{X}) < 0$ and

$$R_1^{T_{\mathcal{X}}}(\theta) = R_1^{\mathrm{SO}(2N)}(\theta) + C_{\mathcal{X}} \sum_{k=0}^{\infty} b_k \exp((k+1/2)\mathcal{X}) \quad \text{for } d(\theta, \mathcal{X}) \geq 0,$$

where $d(\theta, \mathcal{X}) := (2N-1)\log 2 + \log(1-\cos\theta) - \mathcal{X}$ and b_k are coefficients arising from the residues. As $\mathcal{X} \to -\infty$, θ fixed, $R_1^{T_{\mathcal{X}}}(\theta) \to R_1^{\mathrm{SO}(2N)}(\theta)$.

Numerical check

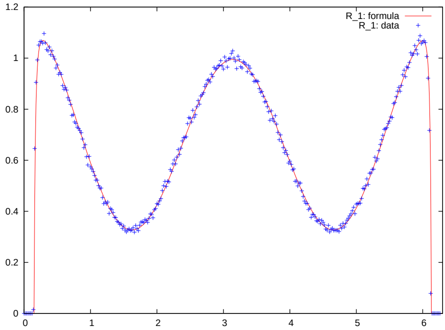


Figure: One-level density of excized $SO(2N), N = 2$ with cut-off $|\Lambda_A(1, N)| \geq 0.1$. The red curve uses our formula. The blue crosses give the empirical one-level density of 200,000 numerically generated matrices.

Theory vs Experiment

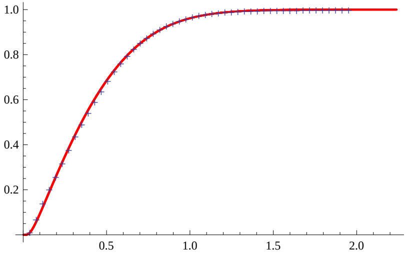


Figure: Cumulative probability density of the first eigenvalue from 3×10^6 numerically generated matrices $A \in SO(2N_{\rm std})$ with $|\Lambda_A(1, N_{\rm std})| \geq 2.188 \times \exp(-N_{\rm std}/2)$ and $N_{\rm std} = 12$ red dots compared with the first zero of even quadratic twists $L_{E_{11}}(s, \chi_d)$ with prime fundamental discriminants $0 < d \leq 400{,}000$ blue crosses. The random matrix data is scaled so that the means of the two distributions agree.

Open Questions and References

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

- Generalize excised ensembles for higher weight GL_2 families where expect different discretizations.
- Obtain better estimates on vanishing at the central point by finding optimal test functions for the second and higher moment expansions.
- Further explore *L*-function Ratios Conjecture to predict lower order terms in families, compute these terms on number theory side.

Publications: Random Matrix Theory

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

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

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

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

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

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

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

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

Publications: L-Functions

1. *The low lying zeros of a* $GL(4)$ *and a* $GL(6)$ *family of L-functions* (with Eduardo Dueñez), Compositio Mathematica **142** (2006), no. 6, 1403–1425. http://arxiv.org/abs/math/0506462
2. *Low lying zeros of L–functions with orthogonal symmetry* (with Christopher Hughes), Duke Mathematical Journal **136** (2007), no. 1, 115–172. http://arxiv.org/abs/math/0507450
3. *Lower order terms in the 1-level density for families of holomorphic cuspidal newforms*, Acta Arithmetica **137** (2009), 51–98. http://arxiv.org/abs/0704.0924
4. *The effect of convolving families of L-functions on the underlying group symmetries* (with Eduardo Dueñez), Proceedings of the London Mathematical Society, 2009; doi: 10.1112/plms/pdp018. http://arxiv.org/pdf/math/0607688.pdf
5. *Low-lying zeros of number field L-functions* (with Ryan Peckner), Journal of Number Theory **132** (2012), 2866–2891. http://arxiv.org/abs/1003.5336
6. *The low-lying zeros of level 1 Maass forms* (with Levent Alpoge), preprint 2013. http://arxiv.org/abs/1301.5702
7. *The n-level density of zeros of quadratic Dirichlet L-functions* (with Jake Levinson), submitted September 2012 to Acta Arithmetica. http://arxiv.org/abs/1208.0930
8. *Moment Formulas for Ensembles of Classical Compact Groups* (with Geoffrey Iyer and Nicholas Triantafillou), preprint 2013.

Publications: Elliptic Curves

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

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

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

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

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

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

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

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

9. *Moments of the rank of elliptic curves* (with Siman Wong), Canad. J. of Math. **64** (2012), no. 1, 151–182. http://web.williams.edu/Mathematics/sjmiller/public_html/math/papers/mwMomentsRanksEC81

Publications: L-Function Ratio Conjecture

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

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

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

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

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

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

Thank you!

Bias Conjecture for Moments of Fourier Coefficients of Elliptic Curve L-functions

Joint with students Blake Mackall (Williams), Christina Rapti (Bard) and Karl Winsor (Michigan)

Emails: Blake.R.Mackall@williams.edu, cr9060@bard.edu and krlwnsr@umich.edu.

Families and Moments

A *one-parameter family* of elliptic curves is given by

$$\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$$

where $A(T), B(T)$ are polynomials in $\mathbb{Z}[T]$.

- Each specialization of T to an integer t gives an elliptic curve $\mathcal{E}(t)$ over $\mathbb{Q}$.
- The r^{th} *moment* of the Fourier coefficients is

$$A_{r,\mathcal{E}}(p) = \sum_{t \bmod p} a_{\mathcal{E}(t)}(p)^r.$$

Tate's Conjecture

Tate's Conjecture for Elliptic Surfaces

Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E}, s)$ be the L-series attached to $H^2_{\text{ét}}(\mathcal{E}/\overline{\mathbb{Q}}, \mathbb{Q}_l)$. Then $L_2(\mathcal{E}, s)$ has a meromorphic continuation to $\mathbb{C}$ and satisfies

$$-\mathrm{ord}_{s=2} L_2(\mathcal{E}, s) \;=\; \mathrm{rank}\, NS(\mathcal{E}/\mathbb{Q}),$$

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 $\mathrm{Re}(s) = 2$.

Tate's conjecture is known for rational surfaces: An elliptic surface $y^2 = x^3 + A(T)x + B(T)$ is rational iff one of the following is true:

- $0 < \max\{3\deg A, 2\deg B\} < 12$;
- $3\deg A = 2\deg B = 12$ and $\mathrm{ord}_{T=0} T^{12}\Delta(T^{-1}) = 0$.

Negative Bias in the First Moment

$A_{1,\mathcal{E}}(p)$ and Family Rank (Rosen-Silverman)

If Tate's Conjecture holds for $\mathcal{E}$ then

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p\le X} \frac{A_{1,\mathcal{E}}(p)\log p}{p} \ = \ -\mathrm{rank}(\mathcal{E}/\mathbb{Q}).$$

- By the Prime Number Theorem, $A_{1,\mathcal{E}}(p) = -rp + O(1)$ implies $\mathrm{rank}(\mathcal{E}/\mathbb{Q}) = r$.

Bias Conjecture

Second Moment Asymptotic (Michel)

For families $\mathcal{E}$ with $j(T)$ non-constant, the second moment is

$$A_{2,\mathcal{E}}(p) \;=\; p^2 + O(p^{3/2}).$$

- The lower order terms are of sizes $p^{3/2}$, p, $p^{1/2}$, and 1.

Bias Conjecture

Second Moment Asymptotic (Michel)

For families $\mathcal{E}$ with $j(T)$ non-constant, the second moment is

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

- The lower order terms are of sizes $p^{3/2}$, p, $p^{1/2}$, and 1.

In every family we have studied, we have observed:

Bias Conjecture

The largest lower term in the second moment expansion which does not average to 0 is on average **negative**.

Preliminary Evidence and Patterns

Let $n_{3,2,p}$ equal the number of cube roots of 2 modulo p, and set
$c_0(p) = \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right] p$, $c_1(p) = \left[\sum_{x \bmod p} \left(\frac{x^3-x}{p}\right)\right]^2$, $c_{3/2}(p) = p \sum_{x(p)} \left(\frac{4x^3+1}{p}\right)$.

Family	$A_{1,\mathcal{E}}(p)$	$A_{2,\mathcal{E}}(p)$
$y^2 = x^3 + Sx + T$	0	$p^3 - p^2$
$y^2 = x^3 + 2^4(-3)^3(9T+1)^2$	0	$\begin{cases} 2p^2-2p & p\equiv 2 \bmod 3 \\ 0 & p \equiv 1 \bmod 3 \end{cases}$
$y^2 = x^3 \pm 4(4T+2)x$	0	$\begin{cases} 2p^2-2p & p\equiv 1 \bmod 4 \\ 0 & p \equiv 3 \bmod 4 \end{cases}$
$y^2 = x^3 + (T+1)x^2 + Tx$	0	$p^2 - 2p - 1$
$y^2 = x^3 + x^2 + 2T + 1$	0	$p^2 - 2p - \left(\frac{-3}{p}\right)$
$y^2 = x^3 + Tx^2 + 1$	$-p$	$p^2 - n_{3,2,p}p - 1 + c_{3/2}(p)$
$y^2 = x^3 - T^2x + T^2$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 - T^2x + T^4$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 + Tx^2 - (T+3)x + 1$	$-2c_{p,1;4}p$	$p^2 - 4c_{p,1;6}p - 1$

where $c_{p,a;m} = 1$ if $p \equiv a \bmod m$ and otherwise is 0.

Preliminary Evidence and Patterns

The first family is the family of all elliptic curves; it is a two parameter family and we expect the main term of its second moment to be p^3.

Note that except for our family $y^2 = x^3 + Tx^2 + 1$, all the families $\mathcal{E}$ have $A_{2,\mathcal{E}}(p) = p^2 - h(p)p + O(1)$, where $h(p)$ is non-negative. Further, many of the families have $h(p) = m_{\mathcal{E}} > 0$.

Note $c_1(p)$ is the square of the coefficients from an elliptic curve with complex multiplication. It is non-negative and of size p for $p \not\equiv 3 \bmod 4$, and zero for $p \equiv 1 \bmod 4$ (send $x \mapsto -x \bmod p$ and note $\left(\frac{-1}{p}\right) = -1$).

It is somewhat remarkable that all these families have a correction to the main term in Michel's theorem in the same direction, and we analyze the consequence this has on the average rank. For our family which has a $p^{3/2}$ term, note that on average this term is zero and the p term is negative.

Lower order terms and average rank

$$\frac{1}{N}\sum_{t=N}^{2N}\sum_{\gamma_t}\phi\left(\gamma_t\frac{\log R}{2\pi}\right) = \widehat{\phi}(0)+\phi(0)-\frac{2}{N}\sum_{t=N}^{2N}\sum_{p}\frac{\log p}{\log R}\frac{1}{p}\widehat{\phi}\left(\frac{\log p}{\log R}\right)a_t(p)$$
$$-\frac{2}{N}\sum_{t=N}^{2N}\sum_{p}\frac{\log p}{\log R}\frac{1}{p^2}\widehat{\phi}\left(\frac{2\log p}{\log R}\right)a_t(p)^2+O\left(\frac{\log\log R}{\log R}\right).$$

If ϕ is non-negative, we obtain a bound for the average rank in the family by restricting the sum to be only over zeros at the central point. The error $O\left(\frac{\log\log R}{\log R}\right)$ comes from trivial estimation and ignores probable cancellation, and we expect $O\left(\frac{1}{\log R}\right)$ or smaller to be the correct magnitude. For most families $\log R \sim \log N^a$ for some integer a.

Lower order terms and average rank (cont)

The main term of the first and second moments of the $a_t(p)$ give $r\phi(0)$ and $-\frac{1}{2}\phi(0)$.

Assume the second moment of $a_t(p)^2$ is $p^2 - m_{\mathcal{E}}p + O(1)$, $m_{\mathcal{E}} > 0$.

We have already handled the contribution from p^2, and $-m_{\mathcal{E}}p$ contributes

$$\begin{aligned} S_2 &\sim \frac{-2}{N}\sum_p \frac{\log p}{\log R}\widehat{\phi}\left(2\frac{\log p}{\log R}\right)\frac{1}{p^2}\frac{N}{p}(-m_{\mathcal{E}}p) \\ &= \frac{2m_{\mathcal{E}}}{\log R}\sum_p \widehat{\phi}\left(2\frac{\log p}{\log R}\right)\frac{\log p}{p^2}. \end{aligned}$$

Thus there is a contribution of size $\frac{1}{\log R}$.

Lower order terms and average rank (cont)

A good choice of test functions (see Appendix A of [ILS]) is the Fourier pair

$$\phi(x) \ = \ \frac{\sin^2(2\pi\frac{\sigma}{2}x)}{(2\pi x)^2}, \quad \widehat{\phi}(u) \ = \ \begin{cases} \frac{\sigma-|u|}{4} & \text{if } |u| \le \sigma \\ 0 & \text{otherwise.} \end{cases}$$

Note $\phi(0) = \frac{\sigma^2}{4}$, $\widehat{\phi}(0) = \frac{\sigma}{4} = \frac{\phi(0)}{\sigma}$, and evaluating the prime sum gives

$$S_2 \quad \sim \quad \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2 \log R}\right) \frac{m_{\mathcal{E}}}{\log R} \, \phi(0).$$

Lower order terms and average rank (cont)

Let r_t denote the number of zeros of E_t at the central point (i.e., the analytic rank). Then up to our $O\left(\frac{\log\log R}{\log R}\right)$ errors (which we think should be smaller), we have

$$\frac{1}{N}\sum_{t=N}^{2N} r_t\phi(0) \leq \frac{\phi(0)}{\sigma} + \left(r+\frac{1}{2}\right)\phi(0) + \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2\log R}\right)\frac{m_{\mathcal{E}}}{\log R}\phi(0)$$

$$\text{Ave Rank}_{[N,2N]}(\mathcal{E}) \leq \frac{1}{\sigma} + r + \frac{1}{2} + \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2\log R}\right)\frac{m_{\mathcal{E}}}{\log R}.$$

$\sigma = 1$, $m_{\mathcal{E}} = 1$: for conductors of size 10^{12}, the average rank is bounded by $1 + r + \frac{1}{2} + .03 = r + \frac{1}{2} + 1.03$. This is significantly higher than Fermigier's observed $r + \frac{1}{2} + .40$.

$\sigma = 2$: lower order correction contributes .02 for conductors of size 10^{12}, the average rank bounded by $\frac{1}{2} + r + \frac{1}{2} + .02 = r + \frac{1}{2} + .52$. Now in the ballpark of Fermigier's bound (already there without the potential correction term!).

Interpretation: Approaching semicircle 2nd moment from below

Sato-Tate Law for Families without CM

For large primes p, the distribution of $a_{\mathcal{E}(t)}(p)/\sqrt{p}$, $t \in \{0, 1, \dots, p-1\}$, approaches a semicircle on $[-2, 2]$.

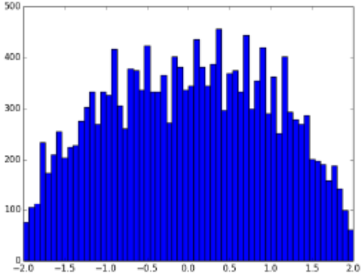


Figure: $a_{\mathcal{E}(t)}(p)$ for $y^2 = x^3 + Tx + 1$ at the 2014th prime.

Implications for Excess Rank

- Katz-Sarnak's one-level density statistic is used to measure the average rank of curves over a family.
- More curves with rank than expected have been observed, though this excess average rank vanishes in the limit.
- Lower-order biases in the moments of families explain a small fraction of this excess rank phenomenon.

Theoretical Evidence

Methods for Obtaining Explicit Formulas

For a family $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$, we can write

$$a_{\mathcal{E}(t)}(p) = -\sum_{x \mod p} \left(\frac{x^3 + A(t)x + B(t)}{p}\right)$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol mod$p$ given by

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a non-zero square modulo } p \\ 0 & \text{if } x \equiv 0 \bmod p \\ -1 & \text{otherwise.} \end{cases}$$

Lemmas on Legendre Symbols

Linear and Quadratic Legendre Sums

$$\sum_{x \bmod p} \left(\frac{ax+b}{p}\right) = 0 \quad \text{if } p \nmid a$$

$$\sum_{x \bmod p} \left(\frac{ax^2+bx+c}{p}\right) = \begin{cases} -\left(\frac{a}{p}\right) & \text{if } p \nmid b^2-4ac \\ (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2-4ac \end{cases}$$

Lemmas on Legendre Symbols

Linear and Quadratic Legendre Sums

$$\sum_{x \bmod p} \left(\frac{ax+b}{p}\right) = 0 \quad \text{if } p \nmid a$$

$$\sum_{x \bmod p} \left(\frac{ax^2+bx+c}{p}\right) = \begin{cases} -\left(\frac{a}{p}\right) & \text{if } p \nmid b^2-4ac \\ (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2-4ac \end{cases}$$

Average Values of Legendre Symbols

The value of $\left(\frac{x}{p}\right)$ for $x \in \mathbb{Z}$, when averaged over all primes p, is 1 if x is a non-zero square, and 0 otherwise.

Rank 0 Families

Theorem (MMRW'14): Rank 0 Families Obeying the Bias Conjecture

For families of the form $\mathcal{E} : y^2 = x^3 + ax^2 + bx + cT + d$,

$$A_{2,\mathcal{E}}(p) \;=\; p^2 - p\left(1 + \left(\frac{-3}{p}\right) + \left(\frac{a^2 - 3b}{p}\right)\right).$$

- The average bias in the size p term is -2 or -1, according to whether $a^2 - 3b \in \mathbb{Z}$ is a non-zero square.

Families with Rank

Theorem (MMRW'14): Families with Rank

For families of the form $\mathcal{E} : y^2 = x^3 + aT^2x + bT^2$,

$$A_{2,\mathcal{E}}(p) = p^2 - p\left(1 + \left(\frac{-3}{p}\right) + \left(\frac{-3a}{p}\right)\right) - \left(\sum_{x(p)} \left(\frac{x^3 + ax}{p}\right)\right)^2.$$

- These include families of rank 0, 1, and 2.
- The average bias in the size p terms is -3 or -2, according to whether $-3a \in \mathbb{Z}$ is a non-zero square.

Families with Complex Multiplication

Theorem (MMRW'14): Families with Complex Multiplication

For families of the form $\mathcal{E} : y^2 = x^3 + (aT + b)x$,

$$A_{2,\mathcal{E}}(p) \;=\; (p^2 - p)\left(1 + \left(\frac{-1}{p}\right)\right).$$

- The average bias in the size p term is -1.
- The size p^2 term is not constant, but is on average p^2, and an analogous Bias Conjecture holds.

Families with Unusual Distributions of Signs

Theorem (MMRW'14): Families with Unusual Signs

For the family $\mathcal{E} : y^2 = x^3 + Tx^2 - (T+3)x + 1$,

$$A_{2,\mathcal{E}}(p) \;=\; p^2 - p\left(2 + 2\left(\frac{-3}{p}\right)\right) - 1.$$

- The average bias in the size p term is -2.
- The family has an usual distribution of signs in the functional equations of the corresponding L-functions.

The Size $p^{3/2}$ Term

Theorem (MMRW'14): Families with a Large Error

For families of the form
$\mathcal{E} : y^2 = x^3 + (T+a)x^2 + (bT + b^2 - ab + c)x - bc,$

$$A_{2,\mathcal{E}}(p) \;=\; p^2 - 3p - 1 + p \sum_{x \bmod p} \left(\frac{-cx(x+b)(bx-c)}{p} \right)$$

- The size $p^{3/2}$ term is given by an elliptic curve coefficient and is thus on average 0.
- The average bias in the size p term is -3.

General Structure of the Lower Order Terms

The lower order terms appear to always

- have no size $p^{3/2}$ term or a size $p^{3/2}$ term that is on average 0;
- exhibit their negative bias in the size p term;
- be determined by polynomials in p, elliptic curve coefficients, and congruence classes of p (i.e., values of Legendre symbols).

Numerical Investigations

Numerical Methods

- As complexity of coefficients increases, it is much harder to find an explicit formula.
- We can always just calculate the second moment from the explicit formula; if $\mathcal{E}$: $y^2 = f(x)$, we have

$$A_{2,\mathcal{E}}(p) = \sum_{t(p)} \left(\sum_{x(p)} \left(\frac{f(x)}{p} \right) \right)^2.$$

- Takes an hour for the first 500 primes. Optimizations?

Numerical Methods

Consider the family $y^2 = f(x) = ax^3 + (bT + c)x^2 + (dT + e)x + f$. By similar arguments used to prove special cases,

$$A_{2,\mathcal{E}}(p) \;=\; p^2 - 2p + pC_0(p) - pC_1(p) - 1 + \#_1,$$

where

$$C_0(p) \;=\; \sum_{x(p)} \sum_{y(p):\ \beta(x,y)\equiv 0} \left(\frac{A(x)A(y)}{p}\right),$$

$$C_1(p) \;=\; \sum_{x(p):\ \beta(x,x)\equiv 0} \left(\frac{A(x)^2}{p}\right),$$

$$\#_1 \;=\; p\sum_{x(p)} \sum_{y(p):\ A(x)\equiv 0 \text{ and } A(y)\equiv 0} \left(\frac{B(x)B(y)}{p}\right),$$

and β, A, and B are polynomials.

Numerical Methods

- $C_o(p)$ ordinarily $O(p^2)$ to compute.
- Sum over zeros of $\beta(x,y) \mod p$
- Fixing an x, β is a quadratic in y. So, with the quadratic formula mod p, we know where to look for y to see if there is a zero.
- Now $O(p)$; runs from 6000^{th} to 7000^{th} prime in an hour.

Potential Counterexamples

Families of Rank as Large as 3

$\mathcal{E}: y^2 = x^3 + ax^2 + bT^2x + cT^2$ with $b, c \neq 0$:

$$A_{2,\mathcal{E}}(p) = p^2 + p \sum_{P(x,y)\equiv 0} \left(\frac{(x^3+bx)(y^3+by)}{p}\right) + p\left[\sum_{x^3+bx\equiv 0}\left(\frac{ax^2+c}{p}\right)\right]^2 - p\sum_{P(x,x)\equiv 0}\left(\frac{x^3+bx}{p}\right)^2 - p\left(2+\left(\frac{-b}{p}\right)\right) - \left[\sum_{x \bmod p}\left(\frac{x^3+bx}{p}\right)\right]^2 - 1$$

where $P(x,y) = bx^2y^2 + c(x^2+xy+y^2) + bc(x+y)$.

A Positive Size p Term?

$p\left[\sum_{x^3+bx\equiv 0}\left(\frac{ax^2+c}{p}\right)\right]^2$ can be $+9p$ on average!

- Terms such as $-p\sum_{P(x,x)\equiv 0}\left(\frac{x^3+bx}{p}\right)^2$, $-p\left(2+\left(\frac{-b}{p}\right)\right)$, and $-\left[\sum_{x \bmod p}\left(\frac{x^3+bx}{p}\right)\right]^2$ contribute negatively to the size p bias.
- The term $p\sum_{P(x,y)\equiv 0}\left(\frac{(x^3+bx)(y^3+by)}{p}\right)$ is of size $p^{3/2}$.

$$\begin{aligned} A_{2,\mathcal{E}}(p) \ =\ & p^2 + p\sum_{P(x,y)\equiv 0}\left(\frac{(x^3+bx)(y^3+by)}{p}\right) + p\left[\sum_{x^3+bx\equiv 0}\left(\frac{ax^2+c}{p}\right)\right]^2 \\ & - p\sum_{P(x,x)\equiv 0}\left(\frac{x^3+bx}{p}\right)^2 - p\left(2+\left(\frac{-b}{p}\right)\right) - \left[\sum_{x \bmod p}\left(\frac{x^3+bx}{p}\right)\right]^2 - 1 \end{aligned}$$

where $P(x,y) = bx^2y^2 + c(x^2+xy+y^2) + bc(x+y)$.

Analyzing the Size $p^{3/2}$ Term

We averaged $\sum_{P(x,y)\equiv 0}\left(\frac{(x^3+bx)(y^3+by)}{p}\right)$ over the first 10,000 primes for several rank 3 families of the form $\mathcal{E}: y^2 = x^3 + ax^2 + bT^2x + cT^2$.

Family	Average
$y^2 = x^3 + 2x^2 - 4T^2x + T^2$	-0.0238
$y^2 = x^3 - 3x^2 - T^2x + 4T^2$	-0.0357
$y^2 = x^3 + 4x^2 - 4T^2x + 9T^2$	-0.0332
$y^2 = x^3 + 5x^2 - 9T^2x + 4T^2$	-0.0413
$y^2 = x^3 - 5x^2 - T^2x + 9T^2$	-0.0330
$y^2 = x^3 + 7x^2 - 9T^2x + T^2$	-0.0311

The Right Object to Study

$c_{3/2}(p) := \sum_{P(x,y)\equiv 0} \left(\frac{(x^3+bx)(y^3+by)}{p}\right)$ is not a natural object to study (for us multiply by p).

An example distribution for $y^2 = x^3 + 2x^3 - 4T^2x + T^2$.

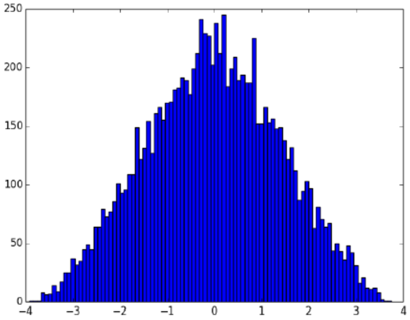


Figure: $c_{3/2}(p)$ over the first 10,000 primes.

In Terms of Elliptic Curve Coefficients

Compare it to the distribution of a sum of 2 elliptic curve coefficients.

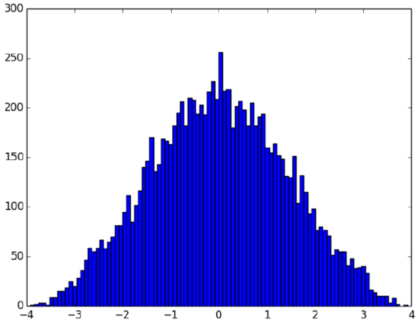


Figure: $-\sum_{x \bmod p} \left(\frac{x^3+x+1}{p}\right) - \sum_{x \bmod p} \left(\frac{x^3+x+2}{p}\right)$ over the first 10,000 primes.

More Error Distributions

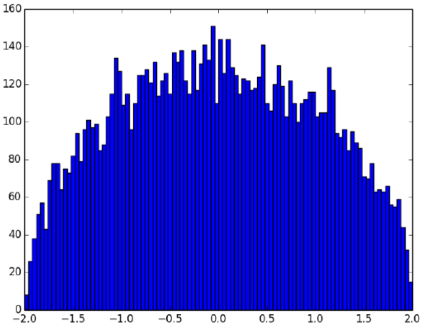


Figure: $c_{3/2}(p)$ for $y^2 = 4x^3 + 5x^2 + (4T - 2)x + 1$, first 10,000 primes.

More Error Distributions

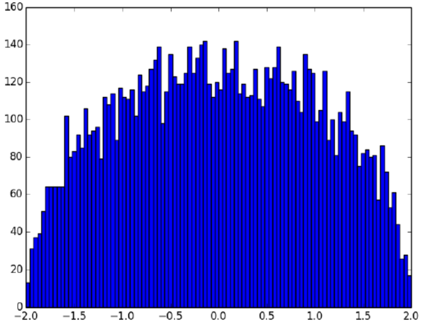


Figure: $-\sum_{x \bmod p} \left(\frac{x^3+x+1}{p}\right)$ distribution, first 10,000 primes.

More Error Distributions

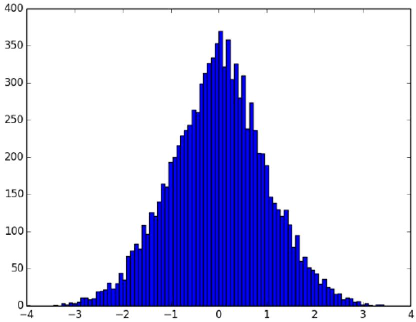


Figure: $c_{3/2}(p)$ over $y^2 = 4x^3 + (4T+1)x^2 + (-4T-18)x + 49$, first 10,000 primes.

More Error Distributions

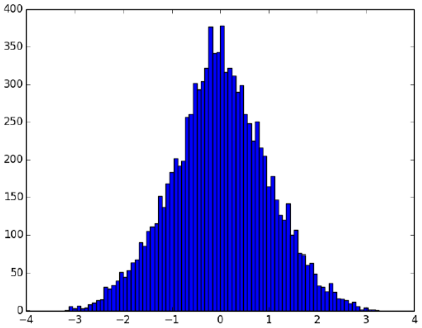


Figure: $-\sum_{x \bmod p} \left(\frac{x^5+x^3+x^2+x+1}{p}\right)$ distribution, first 10,000 primes.

Summary of $p^{3/2}$ Term Investigations

In the cases we've studied, the size $p^{3/2}$ terms

- appear to be governed by (hyper)elliptic curve coefficients;
- may be hiding negative contributions of size p;
- prevent us from numerically measuring average biases that arise in the size p terms.

Future Directions

Questions for Further Study

- Are the size $p^{3/2}$ terms governed by (hyper)elliptic curve coefficients? Or at least other L-function coefficients?
- Does the average bias always occur in the terms of size p?
- Does the Bias Conjecture hold similarly for all higher even moments?
- What other (families of) objects obey the Bias Conjecture? Kloosterman sums? Cusp forms of a given weight and level? Higher genus curves?