From Sato-Tate distributions to low-lying zeros (Des distributions de Sato-Tate aux zéros de bas hauteur)

Steven J Miller
Dept of Math/Stats, Williams College

sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu
http://www.williams.edu/Mathematics/sjmiller

Frobenius distributions of curves, CIRM, February 27, 2014

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

Measures of Spacings: *n*-Level Correlations

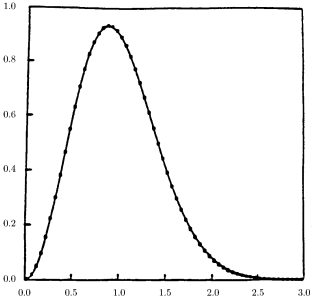
$\{\alpha_j\}$ increasing sequence of numbers, $B \subset \mathbb{R}^{n-1}$ a compact box. Define the *n*-level correlation by

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

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 Density and Families

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

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

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

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.

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

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

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

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

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

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 $\mathrm{ord}_{T=0} T^{12}\Delta(T^{-1}) = 0$.

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.

Comparing the RMT Models

Theorem: M– '04

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

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

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.

Identifying Family Symmetry and Lower Order Terms

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.

Some Number Theory Results

- Orthogonal: holomorphic cuspidal newforms: Iwaniec-Luo-Sarnak, Hughes-Miller, Ricotta-Royer, ... Elliptic curves: Miller, Young. Maass forms: Amersi, Alpoge, Iyer, Lazarev, Miller and Zhang.

- Symplectic: Quadratic Dirichlet characters: Rubinstein, Gao, Levinson-Miller, and Entin, Roddity-Gershon and Rudnick: n-level densities for twists $L(s, \chi_d)$ of the zeta-function.

- Unitary: Dirichlet characters: Fiorilli-Miller, Hughes-Rudnick. Cuspidal GL(3) Maass forms: Goldfeld-Kontorovich.

Main Tools

1. Control of conductors: Usually monotone, gives scale to study low-lying zeros.

2. Explicit Formula: Relates sums over zeros to sums over primes.

3. Trace Formulas: Orthogonality of characters in Fiorilli-Miller, Gao, Hughes-Rudnick, Levinson-Miller, Rubinstein. Petersson formula in Iwaniec, Luo and Sarnak, ... Kuznetsov in Amersi et al, Goldfeld-Kontorovich.

Applications of n-level density

One application: bounding the order of vanishing at the central point.

$\text{Average rank} \cdot \phi(0) \ \leq \ \int \phi(x) W_{G(\mathcal{F})}(x) dx$ if ϕ non-negative.

Can also use to bound the percentage that vanish to order r for any r.

Theorem (Miller, Hughes-Miller)

Using n-level arguments, for the family of cuspidal newforms of prime level $N \to \infty$ (split or not split by sign), for any r there is a c_r such that probability of at least r zeros at the central point is at most $c_n r^{-n}$.

Better results using 2-level than Iwaniec-Luo-Sarnak using the 1-level for $r \geq 5$.

Identifying the Symmetry Groups

- Often an analysis of the monodromy group in the function field case suggests the answer.
- Tools: Explicit Formula, Orthogonality of Characters / Petersson Formula.
- How to identify symmetry group in general? One possibility is by the signs of the functional equation:
- **Folklore Conjecture:** If all signs are even and no corresponding family with odd signs, Symplectic symmetry; otherwise SO(even). (False!)

Explicit Formula

- π: cuspidal automorphic representation on GL_n.
- $Q_\pi > 0$: analytic conductor of $L(s,\pi) = \sum \lambda_\pi(n)/n^s$.
- By GRH the non-trivial zeros are $\frac{1}{2} + i\gamma_{\pi,j}$.
- Satake params $\{\alpha_{\pi,i}(p)\}_{i=1}^n$; $\lambda_\pi(p^\nu) = \sum_{i=1}^n \alpha_{\pi,i}(p)^\nu$.
- $L(s,\pi) = \sum_n \frac{\lambda_\pi(n)}{n^s} = \prod_p \prod_{i=1}^n \left(1 - \alpha_{\pi,i}(p)p^{-s}\right)^{-1}$.

$$\sum_j g\left(\gamma_{\pi,j}\frac{\log Q_\pi}{2\pi}\right) = \widehat{g}(0) - 2\sum_{p,\nu} \widehat{g}\left(\frac{\nu \log p}{\log Q_\pi}\right) \frac{\lambda_\pi(p^\nu)\log p}{p^{\nu/2}\log Q_\pi}$$

1-Level Density

Assuming conductors constant in family $\mathcal{F}$, have to study

$$\lambda_f(p^\nu) \;=\; \alpha_{f,1}(p)^\nu + \cdots + \alpha_{f,n}(p)^\nu$$

$$S_1(\mathcal{F}) \;=\; -2\sum_p \hat{g}\left(\frac{\log p}{\log R}\right)\frac{\log p}{\sqrt{p}\log R}\left[\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}}\lambda_f(p)\right]$$

$$S_2(\mathcal{F}) \;=\; -2\sum_p \hat{g}\left(2\frac{\log p}{\log R}\right)\frac{\log p}{p\log R}\left[\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}}\lambda_f(p^2)\right]$$

The corresponding classical compact group determined by

$$\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}}\lambda_f(p^2) \;=\; c_{\mathcal{F}} \;=\; \begin{cases} 0 & \text{Unitary} \\ 1 & \text{Symplectic} \\ -1 & \text{Orthogonal.} \end{cases}$$

Some Results: Rankin-Selberg Convolution of Families

Symmetry constant: $c_{\mathcal{L}} = 0$ (resp, 1 or -1) if family $\mathcal{L}$ has unitary (resp, symplectic or orthogonal) symmetry.

Rankin-Selberg convolution: Satake parameters for $\pi_{1,p} \times \pi_{2,p}$ are

$$\{\alpha_{\pi_1\times\pi_2,k}(p)\}_{k=1}^{nm} = \{\alpha_{\pi_1,i}(p)\cdot\alpha_{\pi_2,j}(p)\}_{\substack{1\le i\le n\\1\le j\le m}}.$$

Theorem (Dueñez-Miller)

If $\mathcal{F}$ and $\mathcal{G}$ are *nice* families of L-functions, then $c_{\mathcal{F}\times\mathcal{G}} = c_{\mathcal{F}} \cdot c_{\mathcal{G}}$.

Breaks analysis of compound families into simple ones.

Some Results: Rankin-Selberg Convolution of Families: Proofs

Symmetry constant: $c_{\mathcal{L}} = 0$ (resp, 1 or -1) if family $\mathcal{L}$ has unitary (resp, symplectic or orthogonal) symmetry.

Rankin-Selberg convolution: Moments of Satake parameters for $\pi_{1,p} \times \pi_{2,p}$ are

$$\sum_{k=1}^{nm} \alpha_{\pi_1 \times \pi_2, k}(p)^\nu \ = \ \sum_{i=1}^{n} \alpha_{\pi_1, i}(p)^\nu \sum_{j=1}^{m} \alpha_{\pi_2, j}(p)^\nu.$$

Theorem (Dueñez-Miller)

If $\mathcal{F}$ and $\mathcal{G}$ are *nice* families of *L*-functions, then $c_{\mathcal{F} \times \mathcal{G}} = c_{\mathcal{F}} \cdot c_{\mathcal{G}}$.

Breaks analysis of compound families into simple ones.

Takeaways

Very similar to Central Limit Theorem.

- Universal behavior: main term controlled by first two moments of Satake parameters, agrees with RMT.
- First moment zero save for families of elliptic curves.
- Higher moments control convergence and can depend on arithmetic of family.

Open Problem:

Develop a theory of lower order terms to split the universality and see the arithmetic.

Lower order terms

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/pdf/math/0506461v2.pdf.

Lower order terms in the 1-level density for families of holomorphic cuspidal newforms, Acta Arithmetica **137** (2009), 51–98.

http://arxiv.org/pdf/0704.0924.pdf.

Lower Order Terms

Convolve families of elliptic curves with ranks r_1 and r_2: see lower order term of size $r_1 r_2$ (over logarithms).

Difficulty is isolating that from other errors (often of size $\log\log R/\log R$). Study weighted moments

$$\begin{aligned} A_{r,\mathcal{F}}(p) &:= \frac{1}{W_R(\mathcal{F})} \sum_{\substack{f\in\mathcal{F}\\ f\in S(p)}} w_R(f)\lambda_f(p)^r \\ A'_{r,\mathcal{F}}(p) &:= \frac{1}{W_R(\mathcal{F})} \sum_{\substack{f\in\mathcal{F}\\ f\notin S(p)}} w_R(f)\lambda_f(p)^r \\ S(p) &:= \{f\in\mathcal{F} : p \nmid N_f\}. \end{aligned}$$

Main difficulty in 1-level density is evaluating

$$S(\mathcal{F}) = -2\sum_p \sum_{m=1}^{\infty} \frac{1}{W_R(\mathcal{F})} \sum_{f\in\mathcal{F}} w_R(f) \frac{\alpha_f(p)^m + \beta_f(p)^m}{p^{m/2}} \frac{\log p}{\log R}\, \widehat{\phi}\left(m\frac{\log p}{\log R}\right).$$

Fourier Coefficient Expansion

$$\begin{aligned}
S(\mathcal{F}) &= -2\sum_p \sum_{m=1}^{\infty} \frac{A'_{m,\mathcal{F}}(p)}{p^{m/2}} \frac{\log p}{\log R}\, \widehat{\phi}\left(m\frac{\log p}{\log R}\right) \\
&\quad -2\widehat{\phi}(0)\sum_p \frac{2A_{0,\mathcal{F}}(p)\log p}{p(p+1)\log R} + 2\sum_p \frac{2A_{0,\mathcal{F}}(p)\log p}{p\log R}\, \widehat{\phi}\left(2\frac{\log p}{\log R}\right) \\
&\quad -2\sum_p \frac{A_{1,\mathcal{F}}(p)}{p^{1/2}}\frac{\log p}{\log R}\, \widehat{\phi}\left(\frac{\log p}{\log R}\right) + 2\widehat{\phi}(0)\frac{A_{1,\mathcal{F}}(p)(3p+1)}{p^{1/2}(p+1)^2}\frac{\log p}{\log R} \\
&\quad -2\sum_p \frac{A_{2,\mathcal{F}}(p)\log p}{p\log R}\, \widehat{\phi}\left(2\frac{\log p}{\log R}\right) + 2\widehat{\phi}(0)\sum_p \frac{A_{2,\mathcal{F}}(p)(4p^2+3p+1)\log p}{p(p+1)^3\log R} \\
&\quad -2\widehat{\phi}(0)\sum_p\sum_{r=3}^{\infty} \frac{A_{r,\mathcal{F}}(p)p^{r/2}(p-1)\log p}{(p+1)^{r+1}\log R} + O\left(\frac{1}{\log^3 R}\right) \\
&= S_{A'}(\mathcal{F}) + S_0(\mathcal{F}) + S_1(\mathcal{F}) + S_2(\mathcal{F}) + S_A(\mathcal{F}) + O\left(\frac{1}{\log^3 R}\right).
\end{aligned}$$

Letting $\widetilde{A}_{\mathcal{F}}(p) := \frac{1}{W_R(\mathcal{F})}\sum_{f\in S(p)} w_R(f)\frac{\lambda_f(p)^3}{p+1-\lambda_f(p)\sqrt{p}}$, by the geometric series formula we may replace $S_A(\mathcal{F})$ with $S_{\tilde{A}}(\mathcal{F})$, where

$$S_{\tilde{A}}(\mathcal{F}) = -2\widehat{\phi}(0)\sum_p \frac{\widetilde{A}_{\mathcal{F}}(p)p^{3/2}(p-1)\log p}{(p+1)^3\log R}.$$

Family Dependent Lower Order Terms: Miller ’09

$\mathcal{F}_{k,N}$ the family of even weight k and prime level N cuspidal newforms, or just the forms with even (or odd) functional equation.

Up to $O(\log^{-3} R)$, as $N \to \infty$ for test functions ϕ with $\text{supp}(\widehat{\phi}) \subset (-4/3, 4/3)$ the (non-conductor) lower order term is

$$-1.33258 \cdot 2\widehat{\phi}(0)/\log R.$$

Note the lower order corrections are independent of the distribution of the signs of the functional equations.

Family Dependent Lower Order Terms: Miller ’09

CM example, with or without forced torsion: $y^2 = x^3 + B(6T+1)^\kappa$ over $\mathbb{Q}(T)$, with $B \in \{1,2,3,6\}$ and $\kappa \in \{1,2\}$.

CM, sieve to $(6T+1)$ is $(6/\kappa)$-power free. If $\kappa = 1$ then all values of B the same, if $\kappa = 2$ the four values of B have different lower order corrections; in particular, if $B = 1$ then there is a forced torsion point of order three, $(0, 6T+1)$.

Up to errors of size $O(\log^{-3} R)$, the (non-conductor) lower order terms are approximately

$$\begin{aligned}
B = 1, \kappa = 1: &\qquad -2.124 \cdot 2\widehat{\phi}(0)/\log R,\\
B = 1, \kappa = 2: &\qquad -2.201 \cdot 2\widehat{\phi}(0)/\log R,\\
B = 2, \kappa = 2: &\qquad -2.347 \cdot 2\widehat{\phi}(0)/\log R\\
B = 3, \kappa = 2: &\qquad -1.921 \cdot 2\widehat{\phi}(0)/\log R\\
B = 6, \kappa = 2: &\qquad -2.042 \cdot 2\widehat{\phi}(0)/\log R.
\end{aligned}$$

Family Dependent Lower Order Terms: Miller ’09

CM example, with or without rank:
$y^2 = x^3 - B(36T+6)(36T+5)x$ over $\mathbb{Q}(T)$, with $B \in \{1,2\}$. If $B = 1$ the family has rank 1, while if $B = 2$ the family has rank 0.

Sieve to $(36T+6)(36T+5)$ is cube-free. Most important difference between these two families is the contribution from the $S_{\widetilde{\mathcal{A}}}(\mathcal{F})$ terms, where the $B = 1$ family is approximately $-.11 \cdot 2\widehat{\phi}(0)/\log R$, while the $B = 2$ family is approximately $.63 \cdot 2\widehat{\phi}(0)/\log R$.

This large difference is due to biases of size $-r$ in the Fourier coefficients $a_t(p)$ in a one-parameter family of rank r over $\mathbb{Q}(T)$.

Main term of the average moments of the p^{th} Fourier coefficients are given by the complex multiplication analogue of Sato-Tate in the limit, for each p there are lower order correction terms which depend on the rank.

Family Dependent Lower Order Terms: Miller '09

Non-CM Example: $y^2 = x^3 - 3x + 12T$ over $\mathbb{Q}(T)$. Up to $O(\log^{-3} R)$, the (non-conductor) lower order correction is approximately

$$-2.703 \cdot 2\widehat{\phi}(0)/\log R,$$

which is very different than the family of weight 2 cuspidal newforms of prime level N.

Explicit calculations

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

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	$\begin{cases} 2p^2-2p & p \equiv 1 \bmod 3 \\ 0 & p \equiv 3 \bmod 3 \end{cases}$
$y^2 = x^3 + (T+1)x^2 + Tx$	0	$p^2 - 2p - 1$
$y^2 = x^3 + x^2 + 2T + 1$	0	$p^2 - 2p - \left(\frac{-3}{p}\right)$
$y^2 = x^3 + Tx^2 + 1$	$-p$	$p^2 - n_{3,2,p}p - 1 + c_{\frac{3}{2}}(p)$
$y^2 = x^3 - T^2x + T^2$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 - T^2x + T^4$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$

Explicit calculations

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

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

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

$$\begin{aligned} \frac{1}{N}\sum_{t=N}^{2N} r_t\phi(0) &\leq \frac{\phi(0)}{\sigma} + \left(r+\frac{1}{2}\right)\phi(0) + \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2\log R}\right)\frac{m_{\mathcal{E}}}{\log R}\phi(0) \\ \text{Ave Rank}_{[N,2N]}(\mathcal{E}) &\leq \frac{1}{\sigma} + r + \frac{1}{2} + \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2\log R}\right)\frac{m_{\mathcal{E}}}{\log R}. \end{aligned}$$

$\sigma = 1$, $m_{\mathcal{E}} = 1$: 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!).

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 $\mathbb{Q}(T)$:

$$\lim_{N\to\infty} \frac{1}{|\mathcal{F}_N|} \sum_{E_t \in \mathcal{F}_N} \sum_j \varphi\left(\frac{\log C_{E_t}}{2\pi} \gamma_{E_t,j}\right)$$

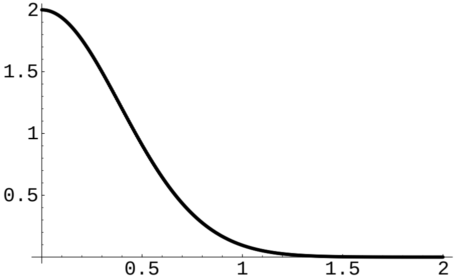
$$= \int \varphi(x)\rho_{\mathcal{G}}(x)dx + r\varphi(0)$$

where

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

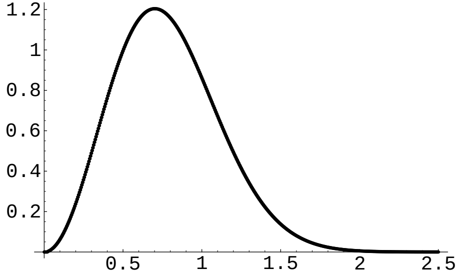
Supports Katz-Sarnak, B-SD, and Independent model in limit.

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

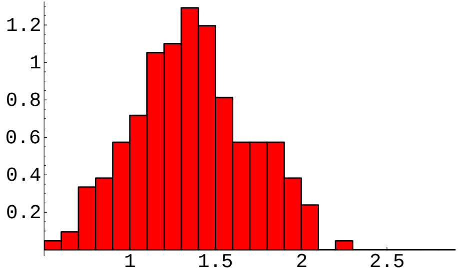


Figure 4a: 209 rank 0 curves from 14 rank 0 families, $\log(\mathrm{cond}) \in [3.26, 9.98]$, median $= 1.35$, mean $= 1.36$

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

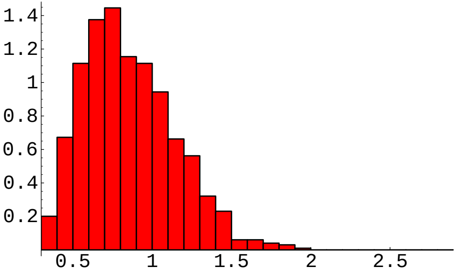


Figure 4b: 996 rank 0 curves from 14 rank 0 families, $\log(\mathrm{cond}) \in [15.00, 16.00]$, median $= .81$, mean $= .86$.

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

- All curves have $\log(\mathrm{cond}) \in [15, 16]$;
- $z_j =$ 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 $\log(\mathrm{cond}) \in [15, 16]$;
- 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 $\log(\text{cond}) \in [15, 16]$;
- $z_j =$ 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 $N_{\mathrm{effective}}$.
  - ⋄ Arithmetic info, predict with L-function Ratios Conj.
  - ⋄ Do the number theory computation.

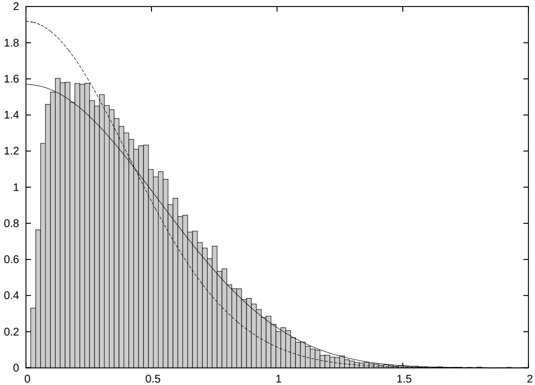
- Excised Orthogonal Ensembles.
  - ⋄ $L(1/2, E)$ discretized.
  - ⋄ Study matrices in $\mathrm{SO}(2N_{eff})$ with $|\Lambda_A(1)| \geq ce^N$.

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

Open Problem:

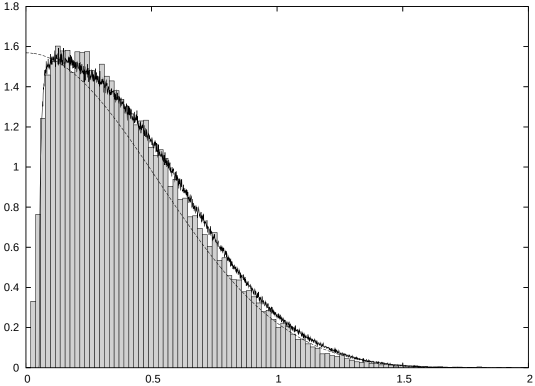
Generalize to other families (ongoing with Nathan Ryan).

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,

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

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

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

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

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

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

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

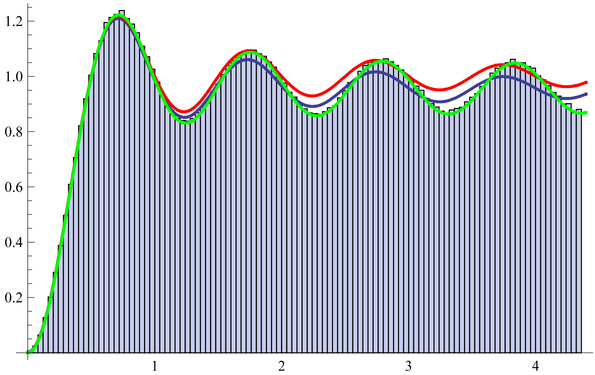
$$+\frac{1}{L}\int_{-\infty}^{\infty} g(\tau)\left(-\frac{\zeta'}{\zeta}\left(1+\frac{2\pi i\tau}{L}\right)+\frac{L_E'}{L_E}\left(\mathrm{sym}^2,1+\frac{2\pi i\tau}{L}\right)-\sum_{\ell=1}^{\infty}\frac{(M^\ell-1)\log M}{M^{\left(2+\frac{2i\pi\tau}{L}\right)\ell}}\right)d\tau$$

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

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

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

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).

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

◇ Green: all lower order terms.

Excised Orthogonal Ensembles

Excised Orthogonal Ensemble: Preliminaries

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

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

w ith $e^{\pm i\theta_1}, \dots, e^{\pm i\theta_N}$ 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

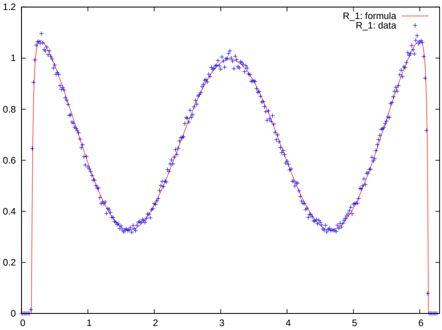


Figure: One-level density of excized $SO(2N), N = 2$ with cut-off $|\Lambda_A(1, N)| \geq 0.1$. The red curve uses our formula. The blue crosses give the empirical one-level density of 200,000 numerically generated matrices.

Theory vs Experiment

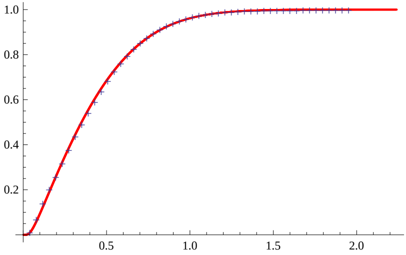


Figure: Cumulative probability density of the first eigenvalue from 3×10^6 numerically generated matrices $A \in SO(2N_{\rm std})$ with $|\Lambda_A(1, N_{\rm std})| \geq 2.188 \times \exp(-N_{\rm std}/2)$ and $N_{\rm std} = 12$ red dots compared with the first zero of even quadratic twists $L_{E_{11}}(s, \chi_d)$ 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.

Constructing Families with Moderate Rank

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/pdf/math/0406579.pdf.

Mordell-Weil and Legendre Expansions

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 $x^2 \equiv a \bmod p$.

1-Level Expansion

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

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

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

Input

For many families

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

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):

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

Rank 6 Family

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.

Constructing Rank 6 Family

Idea: can explicitly evaluate linear and quadratic Legendre sums.

Use: a and b are not both zero mod p and $p > 2$, then for $t \in \mathbb{Z}$

$$\sum_{t=0}^{p-1} \left(\frac{at^2+bt+c}{p}\right) = \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p|(b^2-4ac) \\ -\left(\frac{a}{p}\right) & \text{otherwise.} \end{cases}$$

Thus if $p|(b^2-4ac)$, the summands are $\left(\frac{a(t-t')^2}{p}\right) = \left(\frac{a}{p}\right)$, and the t-sum is large.

Constructing Rank 6 Family

$$\begin{aligned} y^2 = f(x,T) &= x^3T^2 + 2g(x)T - h(x) \\ g(x) &= x^3 + ax^2 + bx + c, \ c \neq 0 \\ h(x) &= (A-1)x^3 + Bx^2 + Cx + D \\ D_T(x) &= g(x)^2 + x^3h(x). \end{aligned}$$

Note that $D_T(x)$ is one-fourth of the discriminant of the quadratic (in T) polynomial $f(x,T)$.

Our elliptic curve $\mathcal{E}$ is not written in standard form, as the coefficient of x^3 is T^2. This is harmless. As $y^2 = f(x,T)$, for the fiber at $T = t$ we have

$$a_t(p) = -\sum_{x(p)} \left(\frac{f(x,t)}{p}\right) = -\sum_{x(p)} \left(\frac{x^3t^2 + 2g(x)t - h(x)}{p}\right).$$

Constructing Rank 6 Family

We study $-pA_{\mathcal{E}}(p) = \sum_{x=0}^{p-1} \sum_{t=0}^{p-1} \left(\frac{f(x,t)}{p}\right)$.
When $x \equiv 0$ the t-sum vanishes if $c \not\equiv 0$, as it is just $\sum_{t=0}^{p-1} \left(\frac{2ct-D}{p}\right)$.

Assume now $x \not\equiv 0$. By the lemma on Quadratic Legendre Sums

$$\sum_{t=0}^{p-1} \left(\frac{x^3t^2 + 2g(x)t - h(x)}{p}\right) = \begin{cases} (p-1)\left(\frac{x^3}{p}\right) & \text{if } p \mid D_t(x) \\ -\left(\frac{x^3}{p}\right) & \text{otherwise.} \end{cases}$$

Goal:find coefficients a, b, c, A, B, C, D so that $D_t(x)$ has six distinct, non-zero roots that are squares.

Constructing Rank 6 Family

Assume we can find such coefficients. Then

$$
\begin{aligned}
-pA_{\mathcal{E}}(p) &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) = \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{x^3t^2+2g(x)t-h(x)}{p}\right) \\
&= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) + \sum_{x:D_t(x)\equiv 0}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) \\
&\quad + \sum_{x:xD_t(x)\not\equiv 0}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) \\
&= 0 + 6(p-1) - \sum_{x:xD_t(x)\not\equiv 0}\left(\frac{x^3}{p}\right) = 6p.
\end{aligned}
$$

Constructing Rank 6 Family

We must find $a, \dots, D$ such that $D_t(x)$ has six distinct, non-zero roots ρ_i^2:

$$\begin{aligned} D_t(x) &= g(x)^2 + x^3 h(x) \\ &= Ax^6 + (B + 2a)x^5 + (C + a^2 + 2b)x^4 \\ &\quad + (D + 2ab + 2c)x^3 \\ &\quad + (2ac + b^2)x^2 + (2bc)x + c^2 \\ &= A(x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0) \\ &= A(x - \rho_1^2)(x - \rho_2^2)(x - \rho_3^2)(x - \rho_4^2)(x - \rho_5^2)(x - \rho_6^2). \end{aligned}$$

Constructing Rank 6 Family

Because of the freedom to choose B, C, D there is no problem matching coefficients for the x^5, x^4, x^3 terms. We must simultaneously solve in integers

$$\begin{aligned} 2ac + b^2 &= R_2 A \\ 2bc &= R_1 A \\ c^2 &= R_0 A. \end{aligned}$$

For simplicity, take $A = 64R_0^3$. Then

$$\begin{aligned} c^2 &= 64R_0^4 & \longrightarrow\quad c &= 8R_0^2 \\ 2bc &= 64R_0^3 R_1 & \longrightarrow\quad b &= 4R_0 R_1 \\ 2ac + b^2 &= 64R_0^3 R_2 & \longrightarrow\quad a &= 4R_0 R_2 - R_1^2. \end{aligned}$$

Constructing Rank 6 Family

For an explicit example, take $r_i = \rho_i^2 = i^2$. For these choices of roots,

$$R_0 = 518400, \; R_1 = -773136, \; R_2 = 296296.$$

Solving for *a* through *D* yields

$$\begin{aligned}
A &= 64R_0^3 &= 8916100448256000000\\
c &= 8R_0^2 &= 2149908480000\\
b &= 4R_0R_1 &= -1603174809600\\
a &= 4R_0R_2 - R_1^2 &= 16660111104\\
B &= R_5A - 2a &= -811365140824616222208\\
C &= R_4A - a^2 - 2b &= 26497490347321493520384\\
D &= R_3A - 2ab - 2c &= -343107594345448813363200
\end{aligned}$$

Constructing Rank 6 Family

We convert $y^2 = f(x,t)$ to $y^2 = F(x,T)$, which is in Weierstrass normal form. We send $y \to \frac{y}{T^2+2T-A+1}$, $x \to \frac{x}{T^2+2T-A+1}$, and then multiply both sides by $(T^2+2T-A+1)^2$. For future reference, we note that

$$\begin{aligned} T^2+2T-A+1 &= (T+1-\sqrt{A})(T+1+\sqrt{A}) \\ &= (T-t_1)(T-t_2) \\ &= (T-2985983999)(T+2985984001). \end{aligned}$$

We have

$$\begin{aligned} f(x,T) &= T^2x^3+(2x^3+2ax^2+2bx+2c)T-(A-1)x^3-Bx^2-Cx-D \\ &= (T^2+2T-A+1)x^3+(2aT-B)x^2+(2bT-C)x+(2cT-D) \\ F(x,T) &= x^3+(2aT-B)x^2+(2bT-C)(T^2+2T-A+1)x \\ &\quad +(2cT-D)(T^2+2T-A+1)^2. \end{aligned}$$

Constructing Rank 6 Family

We now study the $-pA_{\mathcal{E}}(p)$ arising from $y^2 = F(x, T)$. It is enough to show this is $6p + O(1)$ for all p greater than some p_0. Note that t_1, t_2 are the unique roots of $t^2 + 2t - A + 1 \equiv 0 \bmod p$. We find

$$-pA_{\mathcal{E}}(p) = \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right) = \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right).$$

For $t \neq t_1, t_2$, send $x \longrightarrow (t^2 + 2t - A + 1)x$. As $(t^2 + 2t - A + 1) \not\equiv 0$, $\left(\frac{(t^2+2t-A+1)^2}{p}\right) = 1$. Simple algebra yields

$$\begin{aligned} -pA_{\mathcal{E}}(p) &= 6p + O(1) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + O(1) \\ &= 6p + O(1) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{(2at-B)x^2 + (2bt-C)x + (2ct-D)}{p}\right). \end{aligned}$$

Constructing Rank 6 Family

The last sum above is negligible (i.e., is $O(1)$) if

$$D(t) \;=\; (2bt - C)^2 - 4(2at - B)(2ct - D) \not\equiv 0(p).$$

Calculating yields

$$\begin{aligned} D(t_1) &= 429124348024383656112309214358020990540185 6 \\ &= 2^{32} \cdot 3^{25} \cdot 7^5 \cdot 11^2 \cdot 13 \cdot 19 \cdot 29 \cdot 31 \cdot 47 \cdot 67 \cdot 83 \cdot 97 \cdot 103 \\ D(t_2) &= 4291243816662452751895093255391719515488256 \\ &= 2^{33} \cdot 3^{12} \cdot 7 \cdot 11 \cdot 13 \cdot 41 \cdot 173 \cdot 17389 \cdot 805873 \cdot 9447850813. \end{aligned}$$

Constructing Rank 6 Family

Hence, except for finitely many primes (coming from factors of $D(t_i)$, $a, \dots, D$, t_1 and t_2), $-A_{\mathcal{E}}(p) = 6p + O(1)$ as desired.

We have shown: There exist integers a, b, c, A, B, C, D so that the curve $\mathcal{E} : y^2 = x^3T^2 + 2g(x)T - h(x)$ over $\mathbb{Q}(T)$, with $g(x) = x^3 + ax^2 + bx + c$ and $h(x) = (A-1)x^3 + Bx^2 + Cx + D$, has rank 6 over $\mathbb{Q}(T)$. In particular, with the choices of a through D above, $\mathcal{E}$ is a rational elliptic surface and has Weierstrass form

$$y^2 = x^3 + (2aT - B)x^2 + (2bT - C)(T^2 + 2T - A + 1)x + (2cT - D)(T^2 + 2T - A + 1)^2$$

Constructing Rank 6 Family

We show $\mathcal{E}$ is a rational elliptic surface by translating $x \mapsto x - (2aT - B)/3$, which yields $y^2 = x^3 + A(T)x + B(T)$ with $\deg(A) = 3, \deg(B) = 5$.

Therefore the Rosen-Silverman theorem is applicable, and because we can compute $A_{\mathcal{E}}(p)$, we know the rank is exactly 6 (and we never need to calculate height matrices). $\square$

Thank you!