Biases in Moments of the Dirichlet Coefficients in One-Parameter Families of Elliptic Curves

Steven J Miller (sjm1@williams.edu) – Williams College
President, Fibonacci Association
(Joint with SMALL REU groups, . . .)

Dartmouth, February 11, 2025

Overview

- Many problems have painfully slow convergence.
- Elliptic curves quantities converge like the log of the conductor; millions with conductors at most 10^{20} translates to less than 50.
- Improvements in computing power give larger data sets, and with machine learning techniques have found new behavior.
- Reporting on lower order terms in coefficients in families, describing an open conjecture where the “nice” term is hard to extract due to large, fluctuation terms, hoping to form collaborations....

Warning

Claim: 40% of all integers are prime and 20% start a twin prime pair!

Warning

Claim: 40% of all integers are prime and 20% start a twin prime pair!

“Proof”: If count up to 10 have 2, 3, 5 and 7 with 3 and 5 starting pairs.

Warning

Claim: 40% of all integers are prime and 20% start a twin prime pair!

“Proof”: If count up to 10 have 2, 3, 5 and 7 with 3 and 5 starting pairs.

If double the computation to 20 gain 11, 13, 17 and 19, with 11 and 17 starting pairs!

Random Matrix Ensembles with Split Limiting Behavior (with Paula Burkhardt, Peter Cohen, Jonathan Dewitt, Max Hlavacek, Carsten Sprunger, Yen Nhi Truong Vu, Roger Van Peski, and Kevin Yang, and an appendix joint with Manuel Fernandez and Nicholas Sieger), Random Matrices: Theory and Applications **7** (2018), no. 3, 1850006 (30 pages), DOI: 10.1142/S2010326318500065: https://arxiv.org/abs/1609.03120.

Applications of Moments of Dirichlet Coefficients in Elliptic Curve Families (with Zoe Batterman, Aditya Jambhale, Steven J. Miller, Akash L. Narayanan, Kishan Sharma, Andrew Yang, Chris Yao), to appear in the ICERM Conference Proceedings for the July 2023 Murmurations Workshop: https://arxiv.org/abs/2311.17215.

Classical Random Matrix Theory

Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem intractable.

Origins of Random Matrix Theory

Classical Mechanics: 3 Body Problem intractable.

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

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

Fundamental Equation:

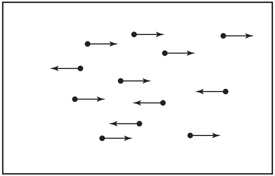
$$H\psi_n = E_n\psi_n$$

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.

Eigenvalue Distribution

$\delta(x - x_0)$ is a unit point mass at x_0:
$\int f(x)\delta(x - x_0)dx = f(x_0)$.

To each A, attach a probability measure:

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

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

$$\text{k}^{\text{th}} \text{ moment} = \frac{\sum_{i=1}^{N}\lambda_i(A)^k}{2^k N^{\frac{k}{2}+1}} = \frac{\text{Trace}(A^k)}{2^k N^{\frac{k}{2}+1}}.$$

Wigner's Semi-Circle Law

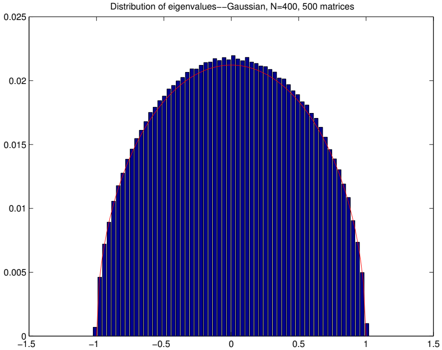
Wigner's Semi-Circle Law

$N \times N$ real symmetric matrices, entries i.i.d.r.v. from a fixed $p(x)$ with mean 0, variance 1, and other moments finite. Then for almost all A, as $N \to \infty$

$$\mu_{A,N}(x) \longrightarrow \begin{cases} \frac{2}{\pi}\sqrt{1-x^2} & \text{if } |x| \leq 1 \\ 0 & \text{otherwise.} \end{cases}$$

See Eugene Wigner's *The Unreasonable Effectiveness of Mathematics in the Natural Sciences* in Communications in Pure and Applied Mathematics, vol. 13, No. I (February 1960), online at http://www.dartmouth.edu/~matc/MathDrama/reading/Wigner.html.

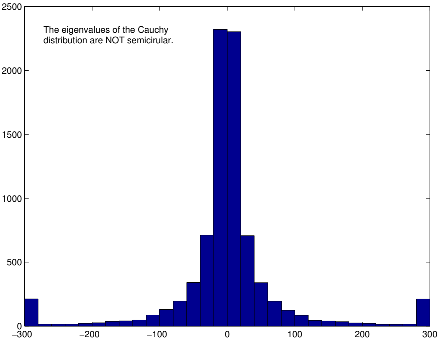
Numerical examples



500 Matrices: Gaussian 400×400

$$p(x) \;=\; \frac{1}{\sqrt{2\pi}}\, e^{-x^2/2}$$

Numerical examples



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

I. Zakharevich, *A generalization of Wigner's law*, Comm. Math. Phys. **268** (2006), no. 2, 403–414.

http://web.williams.edu/Mathematics/sjmiller/public_html/book/papers/innaz.pdf

SKETCH OF PROOF: Eigenvalue Trace Lemma

Want to understand the eigenvalues of A, but choose the matrix elements randomly and independently.

Eigenvalue Trace Lemma

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

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

where

$$\mathrm{Trace}(A^k) \;=\; \sum_{i_1=1}^{N} \cdots \sum_{i_k=1}^{N} a_{i_1 i_2} a_{i_2 i_3} \cdots a_{i_N i_1}.$$

SKETCH OF PROOF: Correct Scale

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

By the Central Limit Theorem:

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

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

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

SKETCH OF PROOF: Averaging Formula

Recall k-th moment of $\mu_{A,N}(x)$ is $\mathrm{Trace}(A^k)/2^k N^{k/2+1}$.

Average k-th moment is

$$\int \cdots \int \frac{\mathrm{Trace}(A^k)}{2^k N^{k/2+1}} \prod_{i \leq j} p(a_{ij}) da_{ij}.$$

Proof by method of moments: Two steps.

- Show average of k-th moments converge to moments of semi-circle as $N \to \infty$;
- Control variance (show it tends to zero as $N \to \infty$).

SKETCH OF PROOF: Averaging Formula for Second Moment

Substituting into expansion gives

$$\frac{1}{2^2 N^2} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \sum_{i=1}^{N} \sum_{j=1}^{N} a_{ij}^2 \cdot p(a_{11}) da_{11} \cdots p(a_{NN}) da_{NN}$$

Integration factors as

$$\int_{a_{ij}=-\infty}^{\infty} a_{ij}^2 p(a_{ij}) da_{ij} \quad \cdot \prod_{\substack{(k,\ell)\neq(i,j) \\ k<\ell}} \int_{a_{k\ell}=-\infty}^{\infty} p(a_{k\ell}) da_{k\ell} \;=\; 1.$$

Higher moments involve more advanced combinatorics (Catalan numbers).

SKETCH OF PROOF: Averaging Formula for Higher Moments

Higher moments involve more advanced combinatorics (Catalan numbers).

$$\frac{1}{2^k N^{k/2+1}} \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} \sum_{i_1=1}^{N} \cdots \sum_{i_k=1}^{N} a_{i_1 i_2} \cdots a_{i_k i_1} \cdot \prod_{i \le j} p(a_{ij}) da_{ij}.$$

Main contribution when the $a_{i_\ell i_{\ell+1}}$'s matched in pairs, not all matchings contribute equally (if did would get a Gaussian and not a semi-circle; this is seen in Real Symmetric Palindromic Toeplitz matrices).

Checkerboard Ensemble

Checkerboard Matrices: $N \times N$ (k, w)-checkerboard ensemble

Matrices $M = (m_{ij}) = M^T$ with a_{ij} iidrv, mean 0, variance 1, finite higher moments, w fixed and

$$m_{ij} = \begin{cases} a_{ij} & \text{if } i \not\equiv j \bmod k \\ w & \text{if } i \equiv j \bmod k. \end{cases}$$

Example: $(3, w)$-checkerboard matrix:

$$\begin{pmatrix} w & a_{0,1} & a_{0,2} & w & a_{0,4} & \cdots & a_{0,N-1} \\ a_{1,0} & w & a_{1,2} & a_{1,3} & w & \cdots & a_{1,N-1} \\ a_{2,0} & a_{2,1} & w & a_{2,3} & a_{2,4} & \cdots & w \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{0,N-1} & a_{1,N-1} & w & a_{3,N-1} & a_{4,N-1} & \cdots & w \end{pmatrix}$$

Split Eigenvalue Distribution

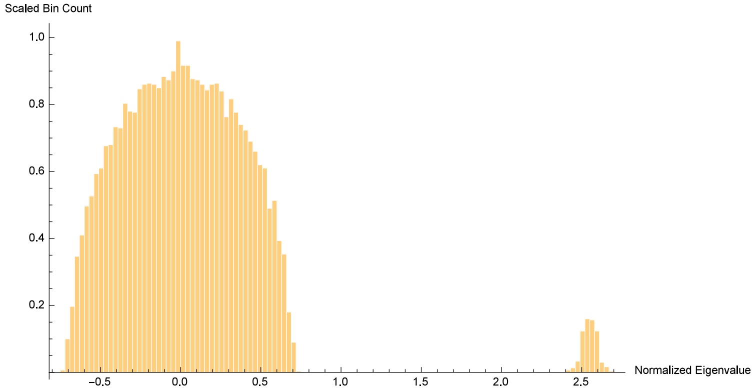


Figure: Histogram of normalized eigenvalues: 2-checkerboard 100×100 matrices, 100 trials.

Split Eigenvalue Distribution

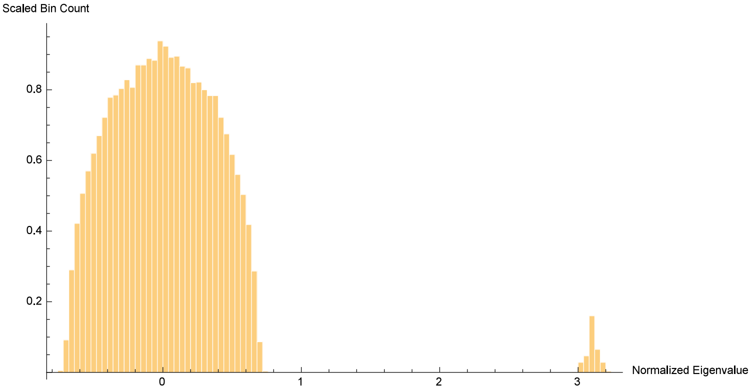


Figure: Histogram of normalized eigenvalues: 2-checkerboard 150×150 matrices, 100 trials.

Split Eigenvalue Distribution

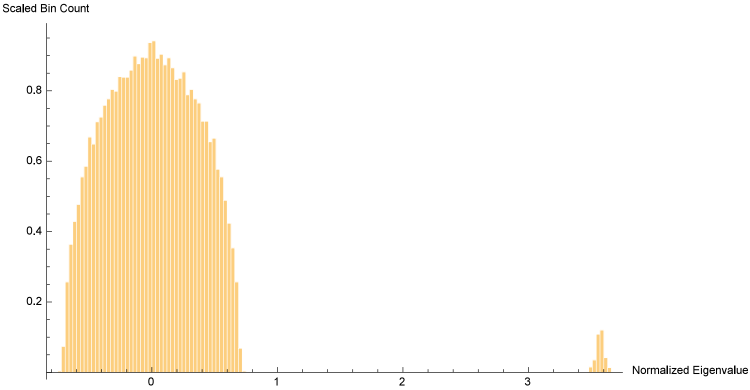


Figure: Histogram of normalized eigenvalues: 2-checkerboard 200×200 matrices, 100 trials.

Split Eigenvalue Distribution

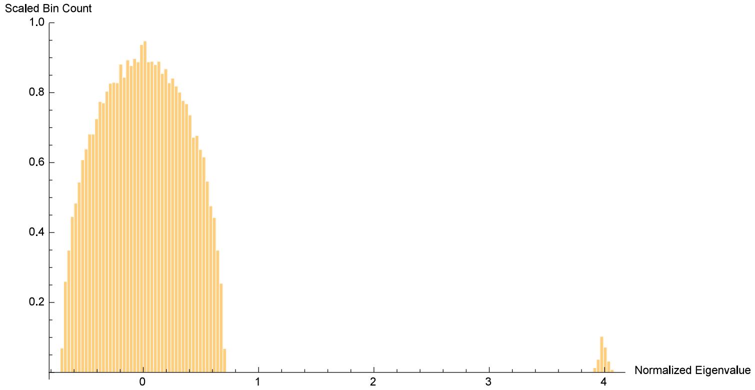


Figure: Histogram of normalized eigenvalues: 2-checkerboard 250×250 matrices, 100 trials.

Split Eigenvalue Distribution

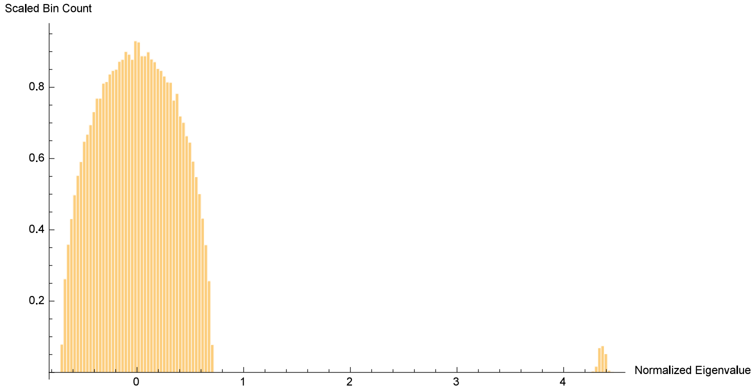


Figure: Histogram of normalized eigenvalues: 2-checkerboard 300×300 matrices, 100 trials.

Split Eigenvalue Distribution

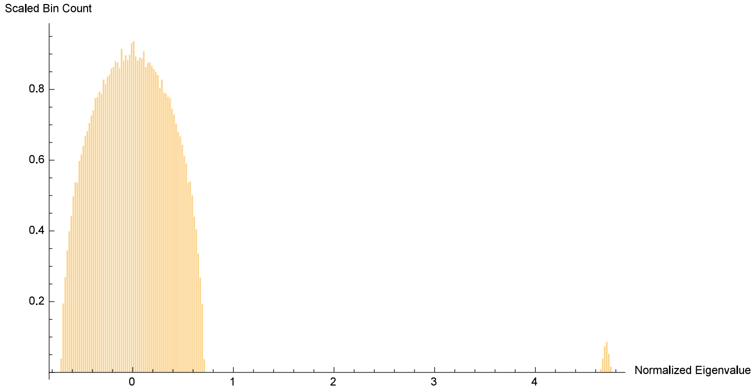


Figure: Histogram of normalized eigenvalues: 2-checkerboard 350×350 matrices, 100 trials.

The Weighting Function

Use weighting function $f_n(x) = x^{2n}(x-2)^{2n}$.

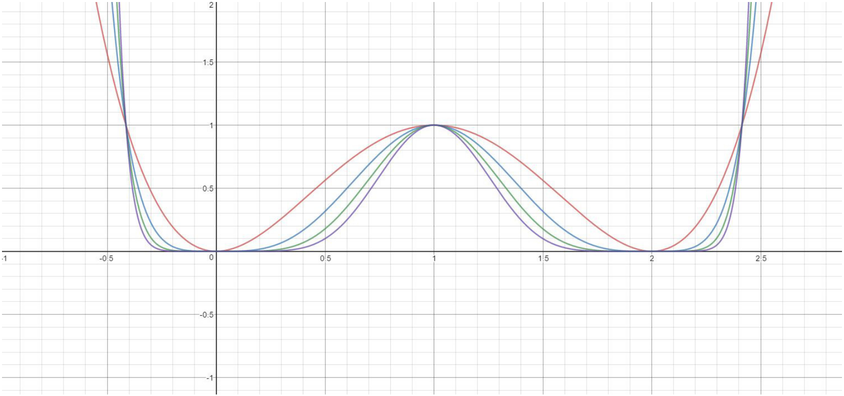


Figure: $f_n(x)$ plotted for $n \in \{1, 2, 3, 4\}$.

The Weighting Function

Use weighting function $f_n(x) = x^{2n}(x-2)^{2n}$.

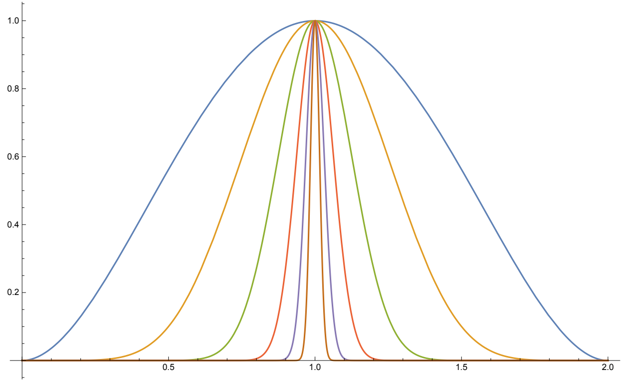


Figure: $f_n(x)$ plotted for $n = 4^m, m \in \{0, 1, \dots, 5\}$.

Spectral distribution of hollow GOE

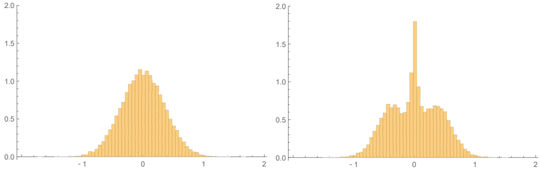


Figure: Hist. of eigenvals of 32000 (Left) 2×2 hollow GOE matrices, (Right) 3×3 hollow GOE matrices.

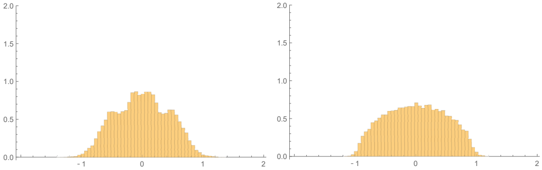


Figure: Hist. of eigenvals of 32000 (Left) 4×4 hollow GOE matrices, (Right) 16×16 hollow GOE matrices.

SMALL 2024 Results

Definition ((k, w)-Checkerboard)

Define $N \times N$ (k, w)-checkerboard matrices $M = (m_{ij})$ as follows:

$$m_{i,j} = \begin{cases} a_{i,j} & \text{if } i \not\equiv j \mod k \\ w & \text{if } i \equiv j \mod k \end{cases}$$

where $a_{ij} = a_{ji}$ with $a_{ij} \sim \mathcal{N}(0, 1)$ iid, and $w \in \mathbb{R}$. E.g., $(2, w)$-checkerboard matrices:

$$M = \begin{bmatrix} w & a_{0,1} & w & a_{0,1} & w & \cdots & a_{0,N-1} \\ a_{0,1} & w & a_{1,2} & w & a_{1,4} & \cdots & w \\ w & a_{1,2} & w & a_{2,3} & w & \cdots & a_{2,N-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{0,N-1} & w & a_{2,N-1} & w & a_{4,N-1} & \cdots & w \end{bmatrix}$$

Definition (Anticommutator of Checkerboard Matrices)

Draw A from $N \times N$ (k, w)-checkerboard matrices and B from $N \times N$ (j, v)-checkerboard matrices, consider $AB + BA$.

Distribution of Anticommutator of Checkerboard Matrices (Quantization)

Draw A from $N \times N$ (k, w)-checkerboard matrices and B from $N \times N$ (j, v)-checkerboard matrices. In addition to bulk of order N observe four blips of order $N^{3/2}$. Their respective centers are 0, $\pm\frac{1}{k}\sqrt{1-\frac{1}{j}}N^{\frac{3}{2}}$, and $\pm\frac{1}{j}\sqrt{1-\frac{1}{k}}N^{\frac{3}{2}}$.

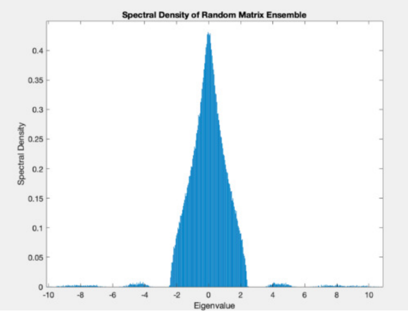


Figure: ESD of $AB + BA$

Moments of the Bulk: SMALL 2024

Odd moments of $AB + BA$ are 0, even moments follow the recurrence below.

Theorem

Moments of the Anti-Commutator of Checkerboard Matrices Let $f(0) = f(1) = 1$, $g(1) = 1$*, and*

$$f(k) = 2\sum_{j=1}^{k-1} g(j)f(k-j) + g(k)$$

$$g(k) = 2f(k-1) + \sum_{\substack{0 \le x_1, x_2 < k-1 \\ x_1 + x_2 < k-1}} (1 + \mathbf{1}_{x_1>0})(1 + \mathbf{1}_{x_2>0}) f(x_1) f(x_2) g(k-1-x_1-x_2).$$

Then the $2k^{\text{th}}$ *moment* M_{2k} *is* $2f(k)$.

Introduction to *L*-Functions

Riemann Zeta Function

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

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

$$\prod_p \left(1 - \frac{1}{p^s}\right)^{-1} = \left[1 + \frac{1}{2^s} + \left(\frac{1}{2^s}\right)^2 + \cdots\right] \left[1 + \frac{1}{3^s} + \left(\frac{1}{3^s}\right)^2 + \cdots\right] \cdots$$

$$= \sum_n \frac{1}{n^s}.$$

Riemann Zeta Function (cont)

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

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

Properties of $\zeta(s)$ and Primes:

- $\lim_{s \to 1^+} \zeta(s) = \infty$, $\pi(x) \to \infty$.
- $\zeta(2) = \frac{\pi^2}{6}$, $\pi(x) \to \infty$.

Riemann Zeta Function

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

Functional Equation:

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

Riemann Hypothesis (RH):

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

Observation: Spacings b/w zeros appear same as b/w eigenvalues of Complex Hermitian matrices $\overline{A}^T = A$.

General L-functions

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

Functional Equation:

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

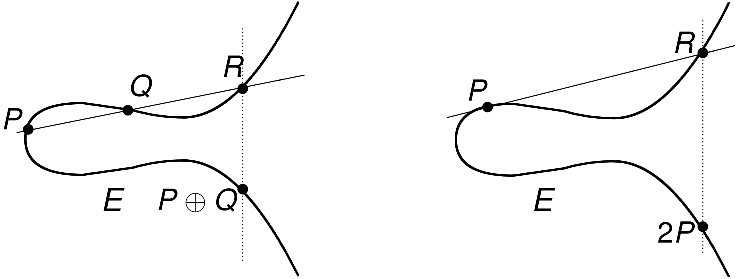
Generalized Riemann Hypothesis (RH):

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

Observation: Spacings b/w zeros appear same as b/w eigenvalues of Complex Hermitian matrices $\overline{A}^T = A$.

Elliptic Curves: Mordell-Weil Group

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



Addition of distinct points P and Q — Adding a point P to itself

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

Elliptic curve L-function

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

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

where

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

Elliptic curve L-function

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

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

where

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

Birch and Swinnerton-Dyer Conjecture

Rank of group of rational solutions equals order of vanishing of $L(s, E)$ at $s = 1/2$.

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: $h(D)$.

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)

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

Explicit Formula (Contour Integration)

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

Contour Integration:

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

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)

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

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

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

Contour Integration (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.

Explicit Formula: Example

Dirichlet L-functions: Let ϕ be an even Schwartz function and $L(s,\chi) = \sum_n \chi(n)/n^s$ a Dirichlet L-function from a non-trivial character χ with conductor m and zeros $\rho = \frac{1}{2} + i\gamma_\chi$. Then

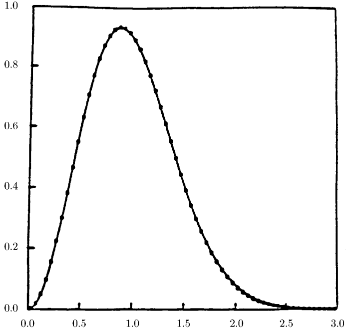
$$\sum_\rho \phi\left(\gamma_\chi \frac{\log(m/\pi)}{2\pi}\right) = \int_{-\infty}^{\infty} \phi(y)dy$$

$$-2\sum_p \frac{\log p}{\log(m/\pi)} \widehat{\phi}\left(\frac{\log p}{\log(m/\pi)}\right) \frac{\chi(p)}{p^{1/2}}$$

$$-2\sum_p \frac{\log p}{\log(m/\pi)} \widehat{\phi}\left(2\frac{\log p}{\log(m/\pi)}\right) \frac{\chi^2(p)}{p} + O\left(\frac{1}{\log m}\right).$$

Katz-Sarnak
Density Conjectures

Zeros of $\zeta(s)$ vs GUE



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

Measures of Spacings: n-Level Correlations

$\{\alpha_j\}$ increasing sequence, box $B \subset \mathbf{R}^{n-1}$.

n-level correlation

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

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

Measures of Spacings: *n*-Level Correlations

$\{\alpha_j\}$ increasing sequence, box $B \subset \mathbf{R}^{n-1}$.

1. Normalized spacings of $\zeta(s)$ starting at 10^{20} (Odlyzko).
2. 2 and 3-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 $\frac{1}{2} + i\gamma_f$ and conductor Q_f:

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

- 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

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

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.

r^{th} centered moments of low-lying zeroes

Apart from one technical obstruction, we obtain support $\sigma = \frac{4}{2r - \mathbb{1}_{2\nmid r}}$, generalizing Baluyot-Chandee-Li '23 $r = 1, \sigma = 4$ result.

Theorem (Cheek, Gilman, Jaber, Miller, Tomé '24

Assume GRH and let Φ_i be even Schwartz functions with $\hat{\Phi}_i$ compactly supported in $(-\sigma, \sigma)$ for $\sigma \leq \min\left\{\frac{3}{2(n-1)}, \frac{4}{2n - \mathbb{1}_{2\nmid n}}\right\}$. Then

$$\lim_{Q\to\infty} \frac{1}{N(Q)} \sum_{q} \Psi\left(\frac{q}{Q}\right) \sum_{f \in \mathcal{H}_k(q)}^{h} \prod_{i=1}^{r} \left(D(f; \Phi_i) - \langle D(f; \Phi_i) \rangle_* \right).$$

agrees with RMT results and predictions for orthogonal symmetry.

1-Level Densities

Let $\mathcal{G}$ be one of the classical compact groups: Unitary, Symplectic, Orthogonal (or SO(even), SO(odd)).
If $\mathrm{supp}(\widehat{g}) \subset (-1, 1)$, 1-level density of $\mathcal{G}$ is

$$\widehat{g}(0) \quad - \quad c_{\mathcal{G}} \, \frac{g(0)}{2},$$

where

$$c_{\mathcal{G}} \;=\; \begin{cases} 0 & \mathcal{G} \text{ is Unitary} \\ 1 & \mathcal{G} \text{ is Symplectic} \\ -1 & \mathcal{G} \text{ is Orthogonal.} \end{cases}$$

Identifying the Symmetry Groups

- Often suggested by monodromy group in the function field.
- Tools: Explicit Formula, Summation 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!)

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

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: $\{\alpha_{\pi,i}(p)\}_{i=1}^n$; $\lambda_\pi(p^\nu) = \sum_{i=1}^n \alpha_{\pi,i}(p)^\nu$.
- $L(s,\pi) = \sum_n \frac{\lambda_\pi(n)}{n^s} = \prod_p \prod_{i=1}^n \left(1 - \alpha_{\pi,i}(p)p^{-s}\right)^{-1}$.

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

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

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.

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

1-Level Density

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

$$\nu^{\text{th}} \text{ moment} : \lambda_f(p^\nu) \ = \ \alpha_{f,1}(p)^\nu + \cdots + \alpha_{f,n}(p)^\nu$$

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

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

The corresponding classical compact group determined by

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

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.

Lower Order Terms

S. J. Miller, *Lower order terms in the 1-level density for families of holomorphic cuspidal newforms*, Acta Arithmetica **137** (2009), 51–98. https://arxiv.org/abs/0704.0924

$$S(p) \;=\; \{f \in \mathcal{F} : p \nmid N_f\}. \tag{1.11}$$

Thus for $f \notin S(p)$, $\alpha_f(p)^m + \beta_f(p)^m = \lambda_f(p)^m$. Let

$$A_{r,\mathcal{F}}(p) \;=\; \frac{1}{W_R(\mathcal{F})} \sum_{\substack{f\in\mathcal{F} \\ f\in S(p)}} w_R(f)\lambda_f(p)^r, \quad A'_{r,\mathcal{F}}(p) \;=\; \frac{1}{W_R(\mathcal{F})} \sum_{\substack{f\in\mathcal{F} \\ f\notin S(p)}} w_R(f)\lambda_f(p)^r; \tag{1.12}$$

we use the convention that $0^0 = 1$; *thus* $A_{0,\mathcal{F}}(p)$ *equals the cardinality of* $S(p)$.

Lower Order Terms

Theorem 1.1 (Expansion for $S(\mathcal{F})$ in terms of moments of $\lambda_f(p)$). *Let* $\log R$ *be the average log-conductor of a finite family of L-functions* $\mathcal{F}$*, and let* $S(\mathcal{F})$ *be as in* (1.10)*. We have*

$$\begin{aligned}
S(\mathcal{F}) \;=\; & -2\sum_p \sum_{m=1}^{\infty} \frac{A'_{m,\mathcal{F}}(p)}{p^{m/2}} \frac{\log p}{\log R}\, \widehat{\phi}\left(m\frac{\log p}{\log R}\right) \\
& -2\widehat{\phi}(0) \sum_p \frac{2A_{0,\mathcal{F}}(p)\log p}{p(p+1)\log R} + 2\sum_p \frac{2A_{0,\mathcal{F}}(p)\log p}{p\log R}\, \widehat{\phi}\left(2\frac{\log p}{\log R}\right) \\
& -2\sum_p \frac{A_{1,\mathcal{F}}(p)}{p^{1/2}} \frac{\log p}{\log R}\, \widehat{\phi}\left(\frac{\log p}{\log R}\right) + 2\widehat{\phi}(0)\frac{A_{1,\mathcal{F}}(p)(3p+1)}{p^{1/2}(p+1)^2}\frac{\log p}{\log R} \\
& -2\sum_p \frac{A_{2,\mathcal{F}}(p)\log p}{p\log R}\, \widehat{\phi}\left(2\frac{\log p}{\log R}\right) + 2\widehat{\phi}(0)\sum_p \frac{A_{2,\mathcal{F}}(p)(4p^2+3p+1)\log p}{p(p+1)^3\log R} \\
& -2\widehat{\phi}(0)\sum_p \sum_{r=3}^{\infty} \frac{A_{r,\mathcal{F}}(p)p^{r/2}(p-1)\log p}{(p+1)^{r+1}\log R} + O\left(\frac{1}{\log^3 R}\right) \\
=\; & S_{A'}(\mathcal{F}) + S_0(\mathcal{F}) + S_1(\mathcal{F}) + S_2(\mathcal{F}) + S_A(\mathcal{F}) + O\left(\frac{1}{\log^3 R}\right).
\end{aligned} \tag{1.13}$$

If we let

$$\widetilde{A}_{\mathcal{F}}(p) \;=\; \frac{1}{W_R(\mathcal{F})} \sum_{f\in S(p)} w_R(f) \frac{\lambda_f(p)^3}{p+1-\lambda_f(p)\sqrt{p}}, \tag{1.14}$$

then by the geometric series formula we may replace $S_A(\mathcal{F})$ *with* $S_{\widetilde{A}}(\mathcal{F})$*, where*

$$S_{\widetilde{A}}(\mathcal{F}) \;=\; -2\widehat{\phi}(0)\sum_p \frac{\widetilde{A}_{\mathcal{F}}(p)p^{3/2}(p-1)\log p}{(p+1)^3\log R}. \tag{1.15}$$

Correspondences

Similarities between L-Functions and Nuclei:

$$\begin{array}{rcl} \text{Zeros} & \longleftrightarrow & \text{Energy Levels} \\ \text{Schwartz test function} & \longrightarrow & \text{Neutron} \\ \text{Support of test function} & \longleftrightarrow & \text{Neutron Energy.} \end{array}$$

Bias Conjecture

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* (note not normalizing by $1/p$) is

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

where $a_{\mathcal{E}(t)}(p) = p + 1 - \#\mathcal{E}_t(\mathbb{F}_p)$ is the Frobenius trace of $\mathcal{E}(t)$.

Negative Bias in the First Moment

First moment related to the rank of the elliptic curve family.

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

Given technical assumptions (Tate's conjecture) related to L-functions associated with $\mathcal{E}$,

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

Bias Conjecture

The $j(T)$-*invariant* is $j(T) = 1728\frac{4A(T)^3}{4A(T)^3+27B(T)^2}$.

Second Moment Asymptotic (Michel)

For families with $j(T)$ non-constant, the second moment is

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

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

Bias Conjecture

The $j(T)$-*invariant* is $j(T) = 1728\frac{4A(T)^3}{4A(T)^3+27B(T)^2}$.

Second Moment Asymptotic (Michel)

For families with $j(T)$ non-constant, the second moment is

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

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

In every family studied before July 2023, observe:

Bias Conjecture

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

Comments

Relation with Excess Rank

- Lower order negative bias increases the bound for average rank in families through statistics of zero densities near the central point.
- Unfortunately only a *small* amount, not enough to explain observed excess rank.

Results to date

- Very special families, Legendre sums computable, not generic.
- Confirmed for additional families by M. Kazalicki and B. Naskrecki.

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.

Methods for Obtaining Explicit Formulas

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

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

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol $\bmod p$ 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 6 Family

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

$$\begin{aligned} y^2 &= x^3 + (2aT - B)x^2 + (2bT - C)(T^2 + 2T - A + 1)x \\ &\quad +(2cT - D)(T^2 + 2T - A + 1)^2 \end{aligned}$$

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

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

1-Parameter Families

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.

Tools: 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.

Simple Second Moment: Not Generic Family!

Family: $y^2 = x^2(x+1) + x(x+1)t$.

$$A_{1,\mathcal{E}}(p) \ = \ \sum_{t(p)} a_t(p) \ = \ -\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x^2(x+1)+x(x+1)t}{p}\right).$$

If x equals 0 or -1, then the t-sum is zero.

Otherwise $t \to x^{-1}(x-1)^{-1}t$ and get zero from the t-sum.

Hence $A_{1,\mathcal{E}}(p)$ vanishes.

Simple Second Moment: Not Generic Family!

Family: $y^2 = x^2(x+1) + x(x+1)t$.

$$A_{2,\mathcal{F}}(p) = \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x^2(x+1)+x(x+1)t}{p}\right)\left(\frac{y^2(y+1)+y(y+1)t}{p}\right)$$

$$= \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{x(x+1)y(y+1)}{p}\right)\left(\frac{t+x}{p}\right)\left(\frac{t+y}{p}\right)$$

$$= \sum_{x=1}^{p-2}\sum_{y=1}^{p-2}\left(\frac{x(x+1)y(y+1)}{p}\right)\sum_{t=0}^{p-1}\left(\frac{(t+x)(t+y)}{p}\right).$$

The t-sum is $p-1$ if $x=y$ and -1 otherwise.

Simple Second Moment: Not Generic Family!

Family: $y^2 = x^2(x+1) + x(x+1)t$.

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= \sum_{x=1}^{p-2}\left(\frac{x^2(x+1)^2}{p}\right)p - \sum_{x=1}^{p-2}\sum_{y=1}^{p-2}\left(\frac{x(x+1)y(y+1)}{p}\right) \\ &= (p-2)p - \left(\sum_{x=0}^{p-1}\left(\frac{x(x+1)}{p}\right)\right)^2 \\ &= p^2 - 2p - (-1)^2 = p^2 - 2p - 1, \end{aligned}$$

thus $A_{2,\mathcal{E}}(p) = p^2 - 2p - 1$.

More Involved Second Moment: $y^2 = x^3 + tx^2 + 1$

$$
\begin{aligned}
A_{1,\mathcal{F}}(p) &= -\sum_{t(p)}\sum_{x(p)}\left(\frac{x^3+1+tx^2}{p}\right)\\
&= -\sum_{t(p)}\left(\frac{1}{p}\right) - \sum_{x=1}^{p-1}\sum_{t(p)}\left(\frac{x^3+1+tx^2}{p}\right)\\
&= -p - \sum_{x=1}^{p-1}\sum_{t(p)}\left(\frac{x^3+1+t}{p}\right) \;=\; -p.
\end{aligned}
$$

so family has rank 1.

For completeness will paste second moment calculation from my thesis.

More Involved Second Moment: $y^2 = x^3 + tx^2 + 1$

https://web.williams.edu/Mathematics/sjmiller/public_html/math/thesis/SJMthesis_Rev2005.pdf

We use the Gauss sum expansion (Equation 2.4) to calculate $A_{2,\mathcal{F}}(p)$.

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= \sum_{t(p)} \sum_{x(p)} \sum_{y(p)} \left(\frac{x^3+1+x^2t}{p}\right)\left(\frac{y^3+1+y^2t}{p}\right) \\ &= \sum_{x,y(p)} \sum_{c,d=1}^{p-1} \frac{1}{p}\left(\frac{cd}{p}\right)\mathbf{e}\left(\frac{c(x^3+1)-d(y^3+1)}{p}\right)\sum_{t(p)}\mathbf{e}\left(\frac{(cx^2-dy^2)t}{p}\right). \end{aligned} \tag{13.7}$$

Note c and d are invertible mod p. If the numerator in the t-exponential is non-zero, the t-sum vanishes. If exactly one of x and y vanishes, the numerator is not congruent to zero mod p. Hence either or neither are zero. If both are zero, the t-sum gives p, the c-sum gives G_p, the d-sum gives $\overline{G}_p$, for a total contribution of p.

More Involved Second Moment: $y^2 = x^3 + tx^2 + 1$

Assume x and y are non-zero. Then $d = c(x^2y^{-2})$ (otherwise the t-sum is zero). The t-sum yields p, and we have

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= \sum_{x,y=1}^{p-1}\sum_{c=1}^{p-1}\frac{1}{p}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x^3y^2+y^2-x^2y^3-x^2)}{p}\right)p+p \\ &= \sum_{x,y=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-(x+y))}{p}\right)+p \\ &= \sum_{x,y=1}^{p-1}\sum_{c=0}^{p-1}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-(x+y))}{p}\right)+p-\sum_{x,y=1}^{p-1}\left(\frac{x^2y^2}{p}\right) \\ &= \sum_{x,y=1}^{p-1}\sum_{c=0}^{p-1}\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-(x+y))}{p}\right)+p-(p-1)^2. \end{aligned} \tag{13.8}$$

If $g(x,y) = (x-y)(x^2y^2-(x+y)) \equiv 0(p)$ then the c-sum is p, otherwise it is 0. We are left with counting how often $g(x,y) \equiv 0$ for x, y non-zero.

A few words must be said about why we cooked up this family. If, instead of x^2t we had xt, we would have found the condition $d = c(x/y)$. As we have $\left(\frac{cd}{p}\right)$ this would lead to $\left(\frac{c^2}{p}\right)\left(\frac{xy}{p}\right)$ times a similar c-exponential. It would not be sufficient to find how often a similar $g(x,y)$ vanished; we would need to know at which x and y (or, slightly weaker, the value of $\left(\frac{xy}{p}\right)$).

Clearly, whenever $x = y$, $g(x,y) \equiv 0$; therefore there are $p-1$ solutions from this term. For x non-zero, each such pair contributes p, for a total contribution of $(p-1)p$.

More Involved Second Moment: $y^2 = x^3 + tx^2 + 1$

Consider now $x^2y^2 \equiv x+y$, which we may rewrite as a quadratic: $x^2y^2 - y - x \equiv 0$. By Lemma C.3 (the Quadratic Formula mod p), if the discriminant $1+4x^3$ is a square mod p there are roots; if it is not a square mod p there are no roots. The roots would be

$$y \equiv \frac{1 \pm \sqrt{1+4x^3}}{2x^2}, \tag{13.9}$$

where the square-root and divisions are operations mod p. If $1+4x^3$ is a non-zero square, there will be two distinct choices for y. If $1+4x^3 \equiv 0$, there is one choice for y, and if $1+4x^3$ is not a square mod p, there are no y such that $x^2y^2 \equiv x+y$.

First, a note about our previous conditions. Neither x nor y is allowed to be zero. If $y = 0$ then $x^2y^2 = x + y$ reduces to $x = 0$ (similarly if $x = 0$). Hence we do not need to worry about our

More Involved Second Moment: $y^2 = x^3 + tx^2 + 1$

solutions violating x, y non-zero.

From the above, we've seen that for a given non-zero x, the number of non-zero y with $x^2y^2 \equiv x + y$ is $1 + \left(\frac{4x^3+1}{p}\right)$. Hence the number of non-zero pairs with $x^2y^2 \equiv x + y$ is

$$\sum_{x\neq 0}\left(1+\left(\frac{4x^3+1}{p}\right)\right) = p - 1 + \sum_{x=0}^{p}\left(\frac{4x^3+1}{p}\right) - 1. \quad (13.10)$$

Each of these pairs contributes p. Thus, these pairs contribute $p^2 - 2p + p\sum_x \left(\frac{4x^3+1}{p}\right)$.

We must be careful about double counting. If both $x - y \equiv 0$ and $x^2y^2 \equiv x + y$, then we find $x^4 \equiv 2x$. As $x \neq 0$, we obtain $x^3 \equiv 2$. If 2 has a cube root mod p, we have double counted three solutions; if it does not, we have counted correctly. Let $h_{3,p}(2)$ denote the number of cube roots of 2 modulo p.

Thus

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= p^2 - 2p + p\sum_{x(p)}\left(\frac{4x^3+1}{p}\right) + p(p-1) - ph_{3,p}(2) + p - (p-1)^2 \\ &= p^2 - ph_{3,p}(2) - 1 + p\sum_{x(p)}\left(\frac{4x^3+1}{p}\right) = p^2 + O(p^{\frac{3}{2}}). \quad (13.11) \end{aligned}$$

Lemma (SMALL '14)

Consider a one-parameter family of elliptic curves of the form

$$\mathcal{E} : y^2 \ = \ P(x)T + Q(x),$$

where $P(x), Q(x) \in \mathbb{Z}[x]$ have degrees at most 3. Then the second moment can be expanded as

$$A_{2,\mathcal{E}}(p) = p\left[\sum_{P(x)\equiv 0}\left(\frac{Q(x)}{p}\right)\right]^2 - \left[\sum_{x(p)}\left(\frac{P(x)}{p}\right)\right]^2 + p\sum_{\Delta(x,y)\equiv 0}\left(\frac{P(x)P(y)}{p}\right)$$

where $\Delta(x,y) = (P(x)Q(y) - P(y)Q(x))^2$.

Kazalicki and Naskrecki proved Bias Conjecture for these families.

Second Moments of Linear-coefficient Families

We computed explicit formulas for the second moments of some one-parameter families with linear coefficients in T:

Family	$A_{2,\mathcal{E}}(p)$
$y^2 = (ax+b)(cx^2+dx+e+T)$	$\begin{cases} p^2 - p\left(2 + \left(\frac{-1}{p}\right)\right) & \text{if } p \nmid ad-2bc \\ (p^2-p)\left(1+\left(\frac{-1}{p}\right)\right) & \text{if } p \mid ad-2bc \end{cases}$
$y^2 = (ax^2+bx+c)(dx+e+T)$	$\begin{cases} p^2 - p\left(1 + \left(\frac{b^2-4ac}{p}\right)\right) - 1 & \text{if } p \nmid b^2-4ac \\ p-1 & \text{if } p \mid b^2-4ac \end{cases}$

Possible Positive Bias: $y^2 = x^3 + x + T^3$

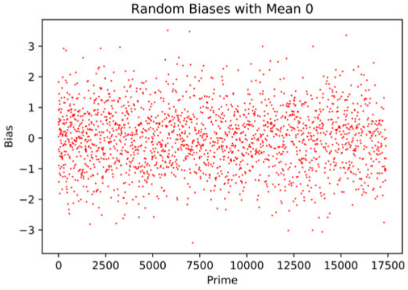
Want to compute higher moments; beyond the second are intractable Legendre sums.

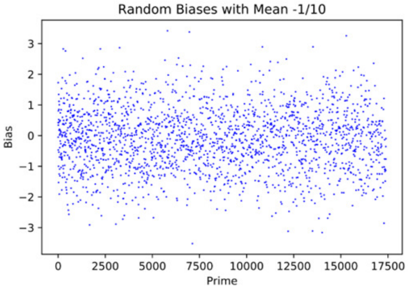
SMALL '23 REU: family with potential positive bias: $y^2 = x^3 + x + T^3$:

Zoe Batterman, Aditya Jambhale, Steven J. Miller, Akash Narayanan, Kishan Sharma, Andrew Yang and Chris Yao: *Applications of Moments of Dirichlet Coefficients in Elliptic Curve Families*, to appear in the ICERM Conference Proceedings for the July 2023 Murmurations Workshop: https://arxiv.org/abs/2311.17215.

Random Experiment

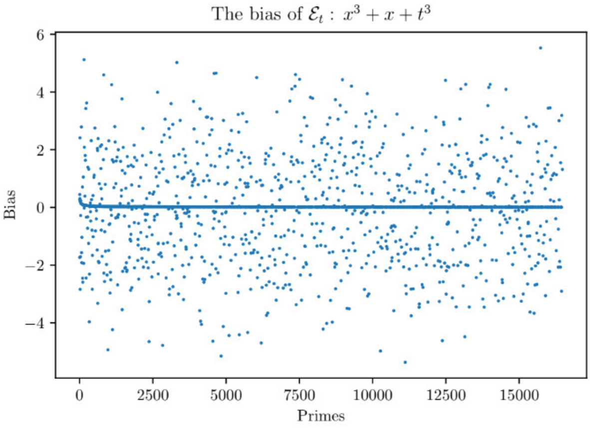
If your experiment needs statistics, you ought to have done a better experiment. – Ernest Rutherford





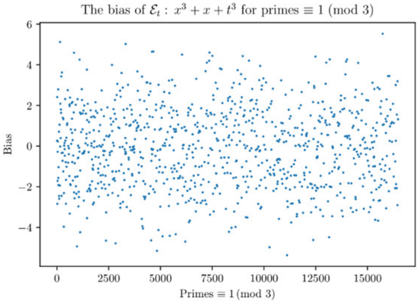
Second Moment: Positive Bias for $y^2 = x^3 + x + T^3$?

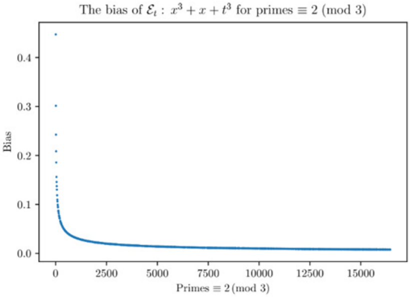
Study $(A_{2,\mathcal{E}}(p) - p^2)/p^{3/2}$.



Second Moment: Positive Bias for $y^2 = x^3 + x + T^3$?

Study $(A_{2,\mathcal{E}}(p) - p^2)/p^{3/2}$.





$\mathcal{E}: y^2 = x^3 + x + T^3$: Positive Bias for $p \equiv 2 \bmod 3$

For primes congruent to 2 modulo 3, the second moment of $\mathcal{E}$ is given by

$$\mathcal{A}_{2,\mathcal{E}}(p) \ = \ p^2 + p.$$

Sketch of proof: For $p \equiv 2 \bmod 3$ we have $t^3 \to t$ is an isomorphism.

After algebra, resulting sums are quadratic.

Fortunately can determine when discriminant vanishes and count. $\square$

No discernable pattern for $p \equiv 1 \bmod 3$

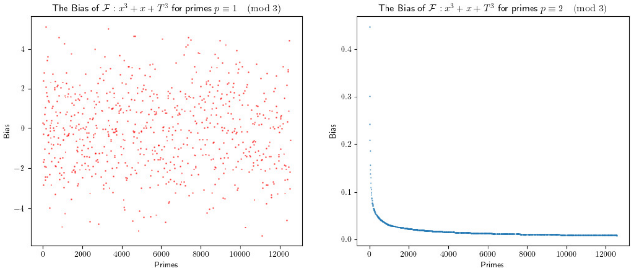


Figure 1: Left: A plot of the bias in the second moment for primes congruent to 1 mod 3. Right: The same plot but for primes congruent to 2 mod 3.

Larger negative bias for $p \equiv 1 \bmod 3$

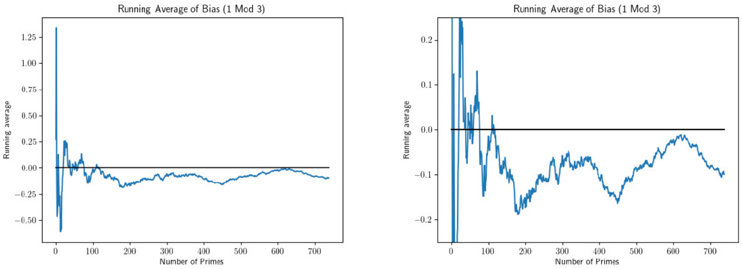


Figure 6: Left: Running average of the bias for $\mathcal{F} : y^2 = x^3 + x + T^3$ for $p \equiv 1 \bmod 3$. Right: A zoomed-in version of the previous plot.

Running Averages

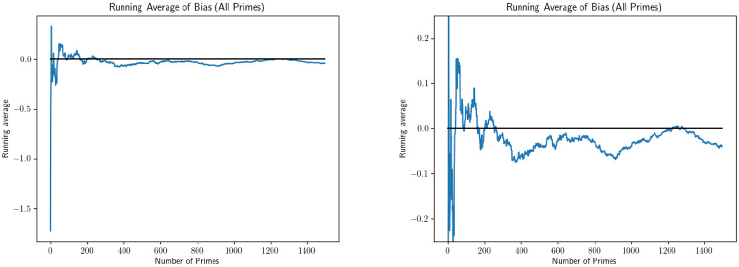


Figure 5: Left: Running average of the bias for $\mathcal{F} : y^2 = x^3 + x + T^3$. Right: A zoomed-in version of the previous plot.

Questions

- Does a negative bias for $p \equiv 1 \bmod 3$ overwhelm positive bias for $p \equiv 2 \bmod 3$?
- Is there a formula for $A_{2,\mathcal{E}}(p)$ for $p \equiv 1 \bmod 3$?
- What happens for “generic” family – these are special as can do (at least some of) the Legendre sums.

SMALL 2024: Computational Exploration

Approach: For $A, B \pmod{p}$, store $\sum_{x \pmod{p}} \left(\frac{x^3+Ax+B}{p}\right)$ in a file, then call this data when needed to quickly compute running averages of second moments of any family.

Issue: This is slow on its own.

- The automorphisms $x \to c^2x$, $y \to c^3x$ and $x \to -x$ allow us to only store As that are representitives of quartic residue classes, and Bs up to $\frac{p}{2}$
- Efficient square root computation with Cipolla's algorithm
- Parallelization of code

Next steps: Use data to find interesting families that are "sufficiently" nice and study them with algebraic geometry techniques.

Bias Explorations

- By Michel's theorem, there are $\alpha(p), \beta(p)$ both $O(1)$ such that

$$\mathcal{A}_{2,\mathcal{E}}(p) \;=\; p^2 + \alpha(p)p^{3/2} + \beta(p)p + O(p^{1/2}).$$

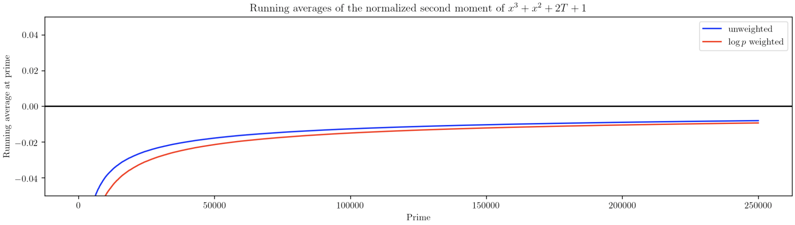
- We compute the *normalized second moment* of $\mathcal{A}_{2,\mathcal{E}}(p)$, which we define to be

$$\mathcal{B}_{2,\mathcal{E}}(p) \;:=\; \frac{\mathcal{A}_{2,\mathcal{E}}(p) - p^2}{p^{3/2}}$$

and graph its running average and $\log p$-weighted running average to find potential positive bias families to investigate further with algebraic geometry.

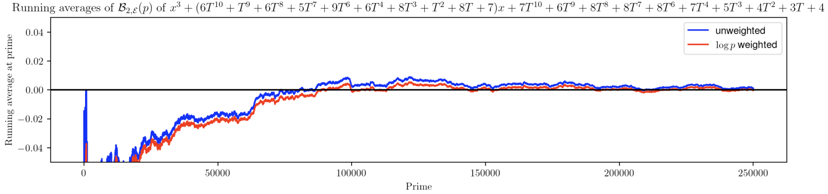
Bias Explorations

A Family with Known Negative Bias For $\mathcal{E} : y^2 = x^3 + x^2 + 2T + 1$, we know that $\mathcal{A}_{2,\mathcal{E}}(p) = p^2 - 2p - 3$ has negative bias.



Bias Explorations

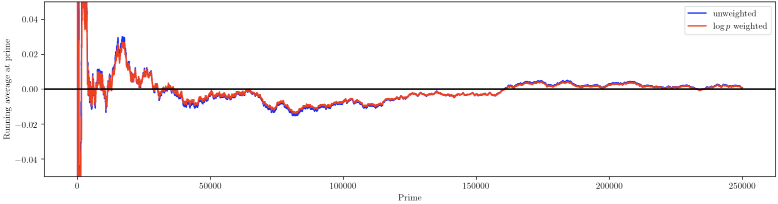
SMALL '24 Generic Random Family 1:
We sampled coefficients iid from $\{0, 1, \dots, 9\}$ and obtained the following families.



Bias Explorations

SMALL ’24 Generic Random Family 2

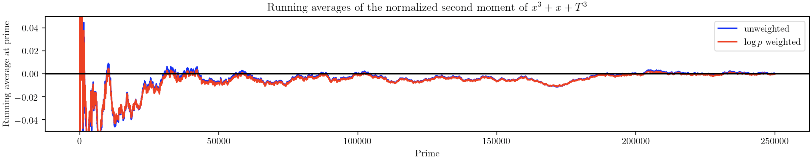
Running averages of the normalized second moment of $x^3 + (5T^{10} + 3T^9 + 5T^7 + 9T^6 + 3T^4 + 2T^3 + 7T^2 + 6T + 4)x + 4T^{10} + 6T^9 + 5T^8 + 7T^7 + 3T^6 + 9T^4 + 2T^3 + 8T^2 + 5T + 9$



Bias Explorations

SMALL '23 Family

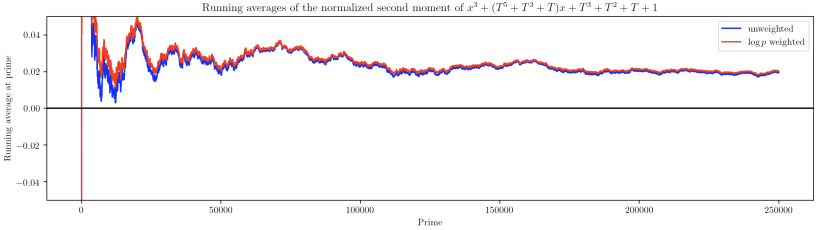
Recall that the SMALL '23 family $\mathcal{E} : y^2 = x^3 + x + T^3$ has positive bias for all primes $p \equiv 2 \bmod 3$, unknown bias for rest.



Bias Explorations

SMALL ’24 Potential Positive Bias Family 1:
$x^3 + (T^5 + T^3 + T)x + T^3 + T^2 + T + 1$

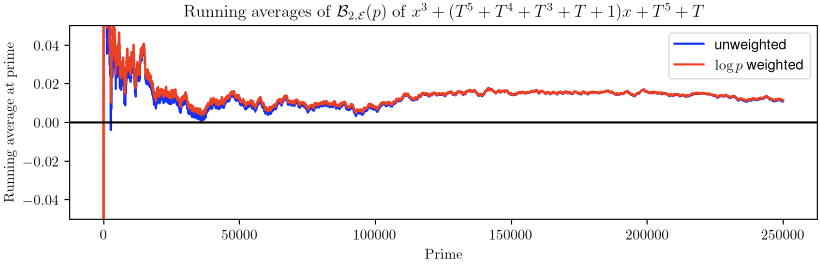
$$A(T) = T(T^2 - T + 1), \quad B(T) = (T+1)(T^2+1)$$



Bias Explorations

SMALL '24 Potential Positive Bias Family 2:
$x^3 + (T^5 + T^4 + T^3 + T + 1)x + T^5 + T$

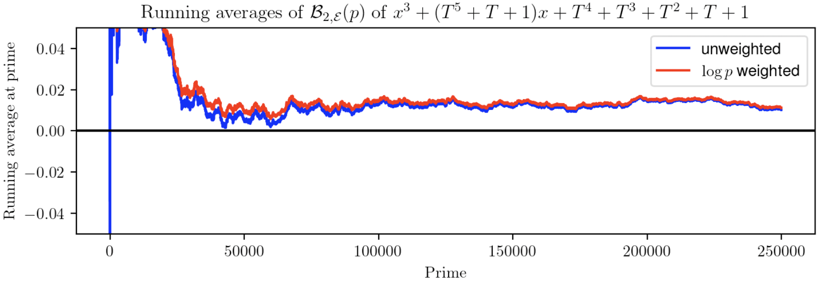
$$A(T) \;=\; (T+1)^2(T^2 - T + 1), \quad B(T) \;=\; T(T^4+1)$$



Bias Explorations

SMALL '24 Potential Positive Bias Family 3:
$x^3 + (T^5 + T + 1)x + T^4 + T^3 + T^2 + T + 1$

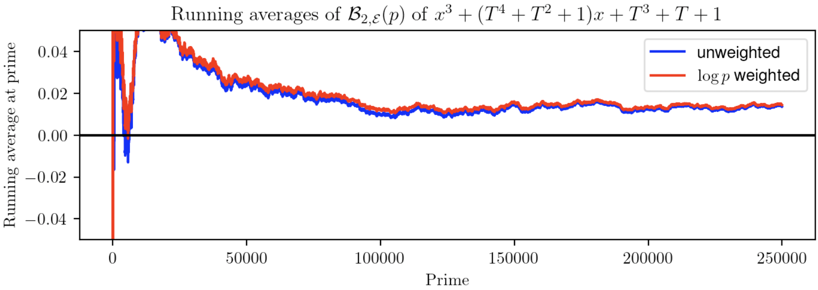
$$A(T) \;=\; (T^2 + T + 1)(T^3 + T^2 - 1), \quad B(T) \;=\; (T + 1)(T^2 + 1$$



Bias Explorations

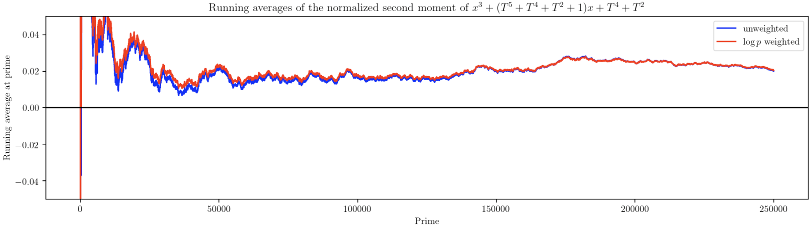
SMALL '24 Potential Positive Bias Family 4:
$x^3 + (T^4 + T^2 + 1)x + T^3 + T + 1$

$$A(T) = (T^2 - T + 1)(T^2 + T + 1)$$



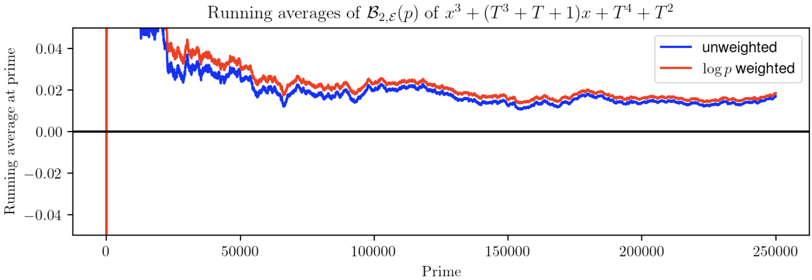
Bias Explorations

SMALL '24 Potential Positive Bias Family 5:
$x^3 + (T^5 + T^4 + T^2 + 1)x + T^4 + T^2$



Bias Explorations

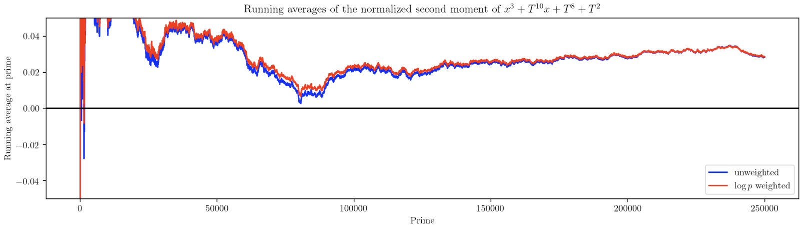
SMALL '24 Potential Positive Bias Family 6:
$x^3 + (T^3 + T + 1)x + T^4 + T^2$



Bias Explorations

SMALL '24 Potential Positive Bias Family 7: $x^3 + T^{10}x + T^8 + T^2$

$$B(T) = T^2(T^4 - T^2 + 1)(T^2 + 1)$$



Assuming there is zero bias, this is a 4.5σ deviation. This happens $\sim$ 3.4 in one million times.

References

Additional References

- M. Kazalicki and B. Naskrecki, *Diophantine triples and K3 surfaces*, Journal of Number Theory **236** (2022), 41–70, https://arxiv.org/pdf/2101.11705.

- M. Kazalicki and B. Naskrecki, *Second moments and the Bias Conjecture for the family of cubic pencils*, preprint, https://arxiv.org/pdf/2012.11306.pdf.

- B. Mackall, S.J. Miller, C. Rapti, K. Winsor, *Lower-Order Biases in Elliptic Curve Fourier Coefficients in Families*, Frobenius Distributions: Lang-Trotter and Sato-Tate Conjectures (David Kohel and Igor Shparlinski, editors), Contemporary Mathematics 663, AMS, Providence, RI 2016. https://web.williams.edu/Mathematics/sjmiller/public_html/math/papers/BiasCIRM30.pdf

- S.J. Miller, 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.

- S.J. Miller, *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.

- S.J. Miller, *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.

- S.J. Miller, *Lower order terms in the 1-level density for families of holomorphic cuspidal newforms*, Acta Arithmetica **137** (2009), 51–98. http://arxiv.org/pdf/0704.0924v4.

Thank you!

Work supported by NSF Grants DMS1561945, DMS1659037, and DMS2241623, the Churchill Program, the Dr. Herchel Smith Fellowship, Dartmouth College, Princeton University and Williams College and the Williams-Exeter Programme.

Appendices:
Bias and Average Rank
Constructing Rank 6 Family

Biases in Lower Order Terms

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.

Biases in Lower Order Terms

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 $1/\log R$.

Lower order terms and average rank (cont)

A good choice of test functions (see Appendix A of Iwaniec-Luo-Sarnak (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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\begin{aligned}
D(t_1) &= 4291243480243836561123092143580209905401856 \\
&= 2^{32} \cdot 3^{25} \cdot 7^5 \cdot 11^2 \cdot 13 \cdot 19 \cdot 29 \cdot 31 \cdot 47 \cdot 67 \cdot 83 \cdot 97 \cdot 103 \\
D(t_2) &= 4291243816662452751895093255391719515488256 \\
&= 2^{33} \cdot 3^{12} \cdot 7 \cdot 11 \cdot 13 \cdot 41 \cdot 173 \cdot 17389 \cdot 805873 \cdot 9447850813.
\end{aligned}$$

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

$$\begin{aligned} y^2 &= x^3 + (2aT - B)x^2 + (2bT - C)(T^2 + 2T - A + 1)x \\ &\quad + (2cT - D)(T^2 + 2T - A + 1)^2 \end{aligned}$$

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 $\deg(A) = 3, \deg(B) = 5$.

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