Numerical Investigation of Lower Order Biases in Moment Expansions of One-Parameter Families of Elliptic Curves

Timothy Cheek (timcheek@umich.edu)
Steven J. Miller (sjm1@williams.edu)

(joint with Pico Gilman, Kareem Jaber, Vismay Sharan, Marie-Hélène Tomé)

Murmurations in Arithmetic Geometry and Related Topics

November 11th, 2024

1 Intro to L-Functions

2 Bias Applications

3 Preliminaries

4 Computation of a_p

5 Computational Investigation

6 Normalized Second Moment

7 Algebraic Geometry

Introduction to L-Functions

Riemann Zeta Function

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

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

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

Functional Equation:

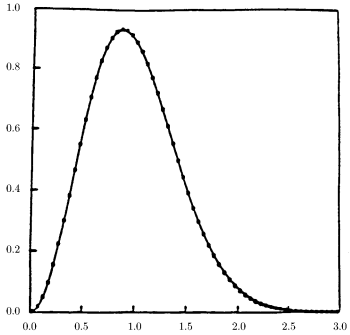
$$\Lambda(s,f) \;=\; \Lambda_\infty(s,f)L(s,f) \;=\; \Lambda(1-s,f).$$

Generalized Riemann Hypothesis (RH):

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

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

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).

Explicit Formula (Contour Integration)

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

Explicit Formula (Contour Integration)

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

Contour Integration:

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

Explicit Formula (Contour Integration)

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

Contour Integration (see Fourier Transform arising):

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

Knowledge of Zeros $\Leftrightarrow$ Knowledge of Coefficients.

Explicit Formula: Examples

Dirichlet L-functions: Let h 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 $\rho = \frac{1}{2} + i\gamma_\chi$; if the Generalized Riemann Hypothesis is true then $\gamma \in \mathbb{R}$. Then

$$\begin{aligned}\sum_\rho h\left(\gamma_\rho \frac{\log(m/\pi)}{2\pi}\right) &= \int_{-\infty}^{\infty} h(y)dy \\ -2\sum_p \frac{\log p}{\log(m/\pi)} \widehat{h}\left(\frac{\log p}{\log(m/\pi)}\right) \frac{\chi(p)}{p^{1/2}} & \\ -2\sum_p \frac{\log p}{\log(m/\pi)} \widehat{h}\left(2\frac{\log p}{\log(m/\pi)}\right) \frac{\chi^2(p)}{p} + O\Big(\frac{1}{\log m}\Big). &\end{aligned}$$

Explicit Formula: Examples

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

$$\begin{aligned}\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}}\sum_{\gamma_f}\phi\left(\frac{\log R}{2\pi}\gamma_f\right) &= \widehat{\phi}(0) + \frac{1}{2}\phi(0) - \frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}} P(f;\phi) \\ &\quad + O\left(\frac{\log\log R}{\log R}\right) \\ P(f;\phi) &= \sum_{p\nmid N}\lambda_f(p)\widehat{\phi}\left(\frac{\log p}{\log R}\right)\frac{2\log p}{\sqrt{p}\log R}.\end{aligned}$$

Measures of Spacings: n-Level Correlations

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

n-level correlation

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

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

Measures of Spacings: n-Level Correlations

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

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

$\diamond$ 2 and 3-correlations of $\zeta(s)$ (Montgomery, Hejhal).

$\diamond$ n-level correlations for all automorphic cupsidal L-functions (Rudnick-Sarnak).

$\diamond$ n-level correlations for the classical compact groups (Katz-Sarnak).

$\diamond$ Insensitive to any finite set of zeros.

Measures of Spacings: n-Level Density and Families

$\phi(x) := \prod_i \phi_i(x_i)$, ϕ_i even Schwartz functions whose Fourier Transforms are compactly supported.

n-level density

$$D_{n,f}(\phi) \quad = \quad \sum_{\substack{j_1,\dots,j_n \\ \text{distinct}}} \phi_1\left(L_f\gamma_f^{(j_1)}\right)\cdots\phi_n\left(L_f\gamma_f^{(j_n)}\right)$$

Measures of Spacings: n-Level Density and Families

$\phi(x) := \prod_i \phi_i(x_i)$, ϕ_i even Schwartz functions whose Fourier Transforms are compactly supported.

n-level density

$$D_{n,f}(\phi) \quad = \quad \sum_{\substack{j_1,\ldots,j_n \\ \text{distinct}}} \phi_1\left(L_f\gamma_f^{(j_1)}\right)\cdots\phi_n\left(L_f\gamma_f^{(j_n)}\right)$$

- ◇ Individual zeros contribute in limit.
- ◇ Most of contribution is from low zeros.
- ◇ Average over similar curves (family).

Measures of Spacings: n-Level Density and Families

$\phi(x) := \prod_i \phi_i(x_i)$, ϕ_i even Schwartz functions whose Fourier Transforms are compactly supported.

n-level density

$$D_{n,f}(\phi) \quad = \quad \sum_{\substack{j_1,\dots,j_n \\ \text{distinct}}} \phi_1\left(L_f\gamma_f^{(j_1)}\right)\cdots\phi_n\left(L_f\gamma_f^{(j_n)}\right)$$

- ◇ Individual zeros contribute in limit.
- ◇ Most of contribution is from low zeros.
- ◇ Average over similar curves (family).

Katz-Sarnak Conjecture

For a 'nice' family of L-functions, the n-level density depends only on a symmetry group attached to the family.

Normalization of Zeros

Local (hard, use C_f) vs Global (easier, use $\log C = |\mathcal{F}_N|^{-1} \sum_{f \in \mathcal{F}_N} \log C_f$). Hope: ϕ a good even test function with compact support, as $|\mathcal{F}| \to \infty$,

$$\begin{aligned} \frac{1}{|\mathcal{F}_N|} \sum_{f \in \mathcal{F}_N} D_{n,f}(\phi) &= \frac{1}{|\mathcal{F}_N|} \sum_{f \in \mathcal{F}_N} \sum_{\substack{j_1,\dots,j_n \\ j_i \neq \pm j_k}} \prod_i \phi_i \left(\frac{\log C_f}{2\pi} \gamma_E^{(j_i)} \right) \\ &\to \int \cdots \int \phi(x) W_{n,\mathcal{G}(\mathcal{F})}(x) dx. \end{aligned}$$

Katz-Sarnak Conjecture

As $C_f \to \infty$ the behavior of zeros near $1/2$ agrees with $N \to \infty$ limit of eigenvalues of a classical compact group.

1-Level Densities

The Fourier Transforms for the 1-level densities are

$$\begin{aligned}
\widehat{W_{1,\mathrm{SO(even)}}}(u) &= \delta_0(u) + \frac{1}{2}\eta(u) \\
\widehat{W_{1,\mathrm{SO}}}(u) &= \delta_0(u) + \frac{1}{2} \\
\widehat{W_{1,\mathrm{SO(odd)}}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) + 1 \\
\widehat{W_{1,Sp}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) \\
\widehat{W_{1,U}}(u) &= \delta_0(u)
\end{aligned}$$

where $\delta_0(u)$ is the Dirac Delta functional and

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

Correspondences

Similarities between L-Functions and Nuclei:

Zeros	$\longleftrightarrow$	Energy Levels
Schwartz test function	$\longrightarrow$	Neutron
Support of test function	$\longleftrightarrow$	Neutron Energy.

CLT Analogy

Similarities with Central Limit Theorem:
Nice distribution: normalize to mean 0, variance 1.

Higher moments only impact rate of convergence.

For us: first two moments of a_t's give main term.

Care about lower order terms in these / higher moments for rate of convergence.

Previous work looking for closed forms, today will discuss computations.

1 Intro to L-Functions

2 Bias Applications

3 Preliminaries

4 Computation of a_p

5 Computational Investigation

6 Normalized Second Moment

7 Algebraic Geometry

Bias Applications

Lower order terms and average rank

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

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 non-negative, bound average rank by restricting the sum to be only over zeros at the central point.

Error $O\left(\frac{\log\log R}{\log R}\right)$ from trivial estimation, ignores probable cancellation; expect $O\left(\frac{1}{\log R}\right)$.

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 $-\frac{1}{2}\phi(0)$.

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

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

Have handled the contribution from p^2; $-m_{\mathscr{E}}p$ contributes

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

Thus there is a contribution of size $1/\log R$.

Lower order terms and average rank (cont)

Good choice of (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

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

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

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

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

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

$\sigma = 1$, $m_{\mathscr{E}} = 1$: 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 $r + \frac{1}{2} + .40$.

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

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

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

1 Intro to L-Functions

2 Bias Applications

3 Preliminaries

4 Computation of a_p

5 Computational Investigation

6 Normalized Second Moment

7 Algebraic Geometry

Elliptic Curves

An elliptic curve E is a genus 1 smooth projective curve with a distinguished point $\mathcal{O}_E$ (a "point at infinity").

Elliptic Curves

An elliptic curve E is a genus 1 smooth projective curve with a distinguished point $\mathcal{O}_E$ (a "point at infinity"). For K with $\mathrm{char}(K) \neq 2, 3$ and $A, B \in K$, an elliptic curve is defined by

$$E(K) \ := \ \{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}_E\},$$

with discriminant $\Delta(E) := -16(4A^3 + 27B^2) \neq 0$.

Elliptic Curves

An elliptic curve E is a genus 1 smooth projective curve with a distinguished point $\mathcal{O}_E$ (a "point at infinity"). For K with $\mathrm{char}(K) \neq 2, 3$ and $A, B \in K$, an elliptic curve is defined by

$$E(K) \coloneqq \{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}_E\},$$

with discriminant $\Delta(E) \coloneqq -16(4A^3 + 27B^2) \neq 0$.

Theorem (Mordell-Weil 1922)

The set $E(\mathbb{Q})$ is a finitely generated abelian group whose identity element is $\mathcal{O}_E$:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tors}},$$

and we call r the rank of $E(\mathbb{Q})$.

Elliptic Curves mod p

From $E/\mathbb{Q}$ we obtain an infinite family of elliptic curves mod p, one for each $p \nmid \Delta(E)$:

- Reduction mod p is a group homomorphism $E(\mathbb{Q}) \longrightarrow E(\mathbb{F}_p)$;
- The expected number of solutions to $E_p := E(\mathbb{F}_p)$ is $p + 1$.

Elliptic Curves mod p

From $E/\mathbb{Q}$ we obtain an infinite family of elliptic curves mod p, one for each $p \nmid \Delta(E)$:

- Reduction mod p is a group homomorphism $E(\mathbb{Q}) \longrightarrow E(\mathbb{F}_p)$;
- The expected number of solutions to $E_p := E(\mathbb{F}_p)$ is $p+1$.

Theorem (Hasse 1933)

For $a_p := p + 1 - \#E(\mathbb{F}_p)$ we have that $|a_p| \leq 2\sqrt{p}$.

Hasse-Weil L-function

If $p \mid \Delta(E)$, let $\alpha_p := 0, 1$, or -1 based on the type of singularity of E mod p.

Definition

The Hasse-Weil L-function of E is defined by

$$L(s,E) := \prod_{p|\Delta(E)} (1-\alpha_p p^{-s})^{-1} \prod_{p\nmid\Delta(E)} \left(1-a_p p^{-s}+p^{1-2s}\right)^{-1}.$$

The L-function $L(s,E)$ packages the information from the a_p's.

Birch and Swinerton-Dyer

1950s: Computational experiments calculating

$$\pi_E(X) \ := \prod_{p \le X, p \nmid \Delta(E)} \frac{\#E(\mathbb{F}_p)}{p} \ = \prod_{p \le X, p \nmid \Delta(E)} \frac{p+1-a_p}{p}$$

led to the following conjectures.

Conjecture (Birch and Swinnerton-Dyer)

If $E/\mathbb{Q}$ has rank r, then there is some constant C such that $\pi_E(X) \ \sim \ C \log(X)^r$.

Birch and Swinerton-Dyer

1950s: Computational experiments calculating

$$\pi_E(X) \ := \prod_{p \le X, p \nmid \Delta(E)} \frac{\#E(\mathbb{F}_p)}{p} \ = \prod_{p \le X, p \nmid \Delta(E)} \frac{p+1-a_p}{p}$$

led to the following conjectures.

Conjecture (Birch and Swinnerton-Dyer)

If $E/\mathbb{Q}$ has rank r, then there is some constant C such that $\pi_E(X) \ \sim \ C \log(X)^r$.

Conjecture (Birch and Swinnerton-Dyer)

If $E/\mathbb{Q}$ has rank r, then

$$r \ = \ \mathrm{ord}_{s=1} L(s, E).$$

Connecting the two conjectures

If we "formally" evaluate $L(s, E)$ at $s = 1$, then we get

$$L(1, E) \text{ “}=\text{”} \left(\prod_{p|\Delta(E)} \left(1 - \frac{\alpha_p}{p}\right) \prod_{p\nmid\Delta(E)} \frac{p + 1 - a_p}{p} \right)^{-1}.$$

Connecting the two conjectures

If we "formally" evaluate $L(s, E)$ at $s = 1$, then we get

$$L(1, E) \text{ “}=\text{”} \left(\prod_{p|\Delta(E)} \left(1 - \frac{\alpha_p}{p}\right) \prod_{p\nmid\Delta(E)} \frac{p + 1 - a_p}{p} \right)^{-1}.$$

Theorem (Goldfeld)

Suppose $\pi_E(X) \sim C \log(X)^r$. *Then* $r = \mathrm{ord}_{s=1} L(s, E)$ *and*

$$\lim_{s\to 1} \frac{L(s, E)}{(s-1)^r} = \frac{\sqrt{2}\mathrm{e}^{r\gamma}}{C} \prod_{p|\Delta(E)} (1 - \alpha_p p^{-1})^{-1}.$$

In particular, if $r = 0$, *then* $L(1, E) = \sqrt{2} \left(\prod_{p|\Delta(E)} \left(1 - \frac{\alpha_p}{p}\right) \prod_{p\nmid\Delta(E)} \frac{p+1-a_p}{p} \right)^{-1}$.

One-parameter families

Let $\mathscr{E} \to \mathbb{P}^1$ be a non-split elliptic surface over $\mathbb{Q}$ with

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

where $A(T), B(T) \in \mathbb{Z}[T]$ and $4A(T)^3 + 27B(T)^2 \neq 0$. Almost all specializations $T = t \in \mathbb{Z}$ results in an elliptic curve E_t. This is a *one-parameter family* $\{E_t\}$ of elliptic curves over $\mathbb{Q}$.

- The *rank of a family* is the minimum rank r that appears infinitely often in E_t.

n-th Moments

Definition (n-th Moments of a 1-parameter Family of Elliptic Curves)

Let $a_t(p) := p + 1 - \#E_t(\mathbb{F}_p)$. Then the n-th moment is given by

$$\mathscr{A}_{n,\mathscr{E}}(p) \ := \ \sum_{t=0}^{p-1} a_t(p)^n.$$

Note, we do not normalize by $1/p$.

Moments and the arithmetic properties of elliptic curves

Theorem (Nagao, Rosen-Silverman 1998)

Assuming Tate's conjecture holds for $\mathscr{E}$, we have that

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

Assuming Tate's conjecture (known for $\mathscr{E}$ if degrees of A, B sufficiently small):

- the rank is determined by the first moment;
- $\sum_{p\le X}\log p \sim X$ so if $\mathscr{A}_{1,\mathscr{E}}(p) = -rp + O(1)$, then $\mathrm{rank}\mathscr{E}(\mathbb{Q}(T)) = r$;
- there is a negative bias in $a_t(p)$.

The Second Moment

The j-invariant of an elliptic surface $\mathscr{E}$ is

$$j(T) \;:=\; 1728\frac{4A(T)^3}{4A(T)^3+27B(T)^2}.$$

Second Moment Asymptotic (Michel, 1995)

For an elliptic surface $\mathscr{E}$ with $j(T)$ non-constant, we have

$$\mathscr{A}_{2,\mathscr{E}}(p) \;=\; p^2+O(p^{3/2}),$$

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

Bias Conjecture

Question

Do lower order terms in the asymptotic second moment expansion also have a negative bias?

Bias Conjecture

Question

Do lower order terms in the asymptotic second moment expansion also have a negative bias?

Conjecture (S.J. Miller '02)

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

- *Excess rank problem*: disagreement between expected and observed average rank.
- Miller: negative bias in lower order terms increases bound for average rank obtained via 1-level density of zeros near central point.

Strong Bias Conjecture

Conjecture (Strong Bias Conjecture)

The largest lower term in the second moment expansion which does not average to 0 is negative for all but finitely many p.

Strong Bias Conjecture

Conjecture (Strong Bias Conjecture)

The largest lower term in the second moment expansion which does not average to 0 is negative for all but finitely many p.

- SMALL '23 disproved the strong bias conjecture with $x^3 + x + T^3$.
- For $p \equiv 2 \bmod 3$, there exists an automorphism $x^3 + x + T^3 \longmapsto x^3 + x + T$.
- The family $x^3 + x + T$ has second moment $p^2 + p$ for $p \equiv 2 \bmod 3$.

1 Intro to L-Functions

2 Bias Applications

3 Preliminaries

4 Computation of a_p

5 Computational Investigation

6 Normalized Second Moment

7 Algebraic Geometry

Legendre Symbols

The Legendre symbol is

$$\left(\frac{a}{p}\right) := \begin{cases} 0 \text{ when } a = 0, \\ 1 \text{ when } a \neq 0 \text{ and square}, \\ -1 \text{ otherwise.} \end{cases}$$

Observation

When p is odd and for a given x, the number of solutions to $y^2 = x^3 + ax + b$ mod p is given by

$$1 + \left(\frac{x^3 + ax + b}{p}\right).$$

Legendre Symbols

Lemma

For p odd, then the elliptic curve given by $y^2 = x^3 + ax + b$ satisfies

$$a_p = -\sum_x \left(\frac{x^3 + ax + b}{p}\right).$$

Legendre Symbols

Lemma

For p odd, then the elliptic curve given by $y^2 = x^3 + ax + b$ satisfies

$$a_p = -\sum_x \left(\frac{x^3 + ax + b}{p}\right).$$

Consequently, we can calculate the second moment via

$$\mathscr{A}_{2,\mathscr{E}} = \sum_t \sum_{x,y} \left(\frac{x^3 + A(t)x + B(t)}{p}\right)\left(\frac{y^3 + A(t)y + B(t)}{p}\right).$$

In general, explicit formulas are difficult, however, it is possile in some special cases.

Known Expansions

Essentially, the only know non-trivial second moment expansions are as follows:

Family	$A_{1,\mathscr{E}}(p)$	$A_{2,\mathscr{E}}(p)$
$y^2 = x^3 + 2^4(-3)^3(9T+1)^2$	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	$p^2 - 2p - 3$
$y^2 = x^3 + Tx^2 + 1$	$-p$	$p^2 - n_{3,2,p}p - 1 + c_{3/2}(p)$
$y^2 = x^3 - T^2x + T^2$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 - T^2x + T^4$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 + Tx^2 - (T+3)x + 1$	$-2c_{p,1;4}p$	$p^2 - 4c_{p,1;6}p - 1$

where $c_{p,a;m} = 1$ if $p \equiv a \bmod m$ and 0 otherwise; $n_{3,2,p}$ is the number of cubes root of 2 mod p; $c_\alpha(p)$ are certain Legendre sums multiplied by p.

Tractable Cases

Closed form expressions via Legendre sums are only tractable in special cases: explicit calculations made by reducing to lower degree polynomials $A(T), B(T)$, and using the identities for linear and quadratic Legendre sums

$$\sum_x \left(\frac{ax+b}{p}\right) = \mathbf{1}_{a=0} p \left(\frac{b}{p}\right)$$

and

$$\sum_x \left(\frac{ax^2+bx+c}{p}\right) = \left(\mathbf{1}_{b^2=4ac} ap - 1\right)\left(\frac{a}{p}\right).$$

Computational Investigation of the Bias Conjecture

- S.J. Miller formulated Bias Conjecture after drawing inspiration from proof of Nagao conjecture, computations for low-degree non-generic families.
- Small degree cases may be misleading: need to study families with higher degree polynomials $A(T), B(T)$ to observe generic families to test Bias Conjecture.
  - Analogously, would never conjecture on primes by just looking at first 10, 20 primes.

Contribution

- We compute a database of a_p for elliptic curves $E_{a,b} : y^2 = x^3 + ax + b$ for all values of $a, b \in \mathbb{F}_p$ for primes p up to $250,000$.

Contribution

- We compute a database of a_p for elliptic curves $E_{a,b} : y^2 = x^3 + ax + b$ for all values of $a, b \in \mathbb{F}_p$ for primes p up to $250,000$.
- This precomputation enables one to quickly study any family of choice (even large ones).
  - for one-parameter family $\mathscr{E}_t$, specialize $t = T$, reduce coeffictions $A(T), B(T)$ $\mathrm{mod} p$, and use our database as lookup table on $(A(T) \bmod p, B(T) \bmod p, p)$ to get corresponding a_p value.

Contribution

- We compute a database of a_p for elliptic curves $E_{a,b} : y^2 = x^3 + ax + b$ for all values of $a, b \in \mathbb{F}_p$ for primes p up to $250,000$.
- This precomputation enables one to quickly study any family of choice (even large ones).
  - for one-parameter family $\mathscr{E}_t$, specialize $t = T$, reduce coeffictions $A(T), B(T)$ $\mod p$, and use our database as lookup table on $(A(T) \bmod p, B(T) \bmod p, p)$ to get corresponding a_p value.
- Our inital experiments see interesting behavior, and we look for colleagues to try to convert observations to theorems.
  - e.g., study second moments of families with $A(T), B(T)$ of degree ≤ 5.

Constructing Lookup Table

- A priori, there are p^2-many moment calculations for each p (since there are p^2 elliptic curves over $\mathbb{F}_p$).

Constructing Lookup Table

- A priori, there are p^2-many moment calculations for each p (since there are p^2 elliptic curves over $\mathbb{F}_p$).
- Via automorphisms, to speed up pre-computation, we do better:

$$\#\text{ of } a_p \text{ stored} \;=\; \begin{cases} 4p & p \equiv 1 \bmod 4 \\ 2p & p \equiv 3 \bmod 4 \end{cases} + \begin{cases} 6 & p \equiv 1 \bmod 3 \\ 0 & p \equiv 0, 2 \bmod 3. \end{cases}$$

- We show how to reduce $4p$ appearing above to $2p + 2$.

Automorphisms

Consider the elliptic curve $\mathscr{E}: \ y^2 = x^3 + ax + b$. Letting $y = \ell^3 y'$ and $x = \ell^2 x'$ yields

$$\ell^6 y'^2 \ = \ \ell^6 x'^3 + \ell^2 a x' + b.$$

Dividing by ℓ^6, we conclude

$$\mathscr{E}: \ y'^2 \ = \ x'^3 + \frac{a}{\ell^4} x' + \frac{b}{\ell^6}.$$

Hence, these two curves are automorphic to each other and have the same number of $\mathbb{F}_p$ points.

Automorphisms

Consider the elliptic curve $\mathscr{E}: \ y^2 = x^3 + ax + b$. Letting $y = \ell^3 y'$ and $x = \ell^2 x'$ yields

$$\ell^6 y'^2 \ = \ \ell^6 x'^3 + \ell^2 a x' + b.$$

Dividing by ℓ^6, we conclude

$$\mathscr{E}: \ y'^2 \ = \ x'^3 + \frac{a}{\ell^4} x' + \frac{b}{\ell^6}.$$

Hence, these two curves are automorphic to each other and have the same number of $\mathbb{F}_p$ points. Thus, it suffices to compute the values of a_p for one a in each quartic residue class. For p odd,

$$\#\text{ of quartic residue classes} = \begin{cases} 5 & p \equiv 1 \pmod 4 \\ 3 & p \equiv 3 \pmod 4. \end{cases}$$

Automorphisms $(a = 0)$

Example

The curves $y^2 = x^3 + 8x + 3$ *and* $y^2 = x^3 + 2x + 9$ *are automorphic mod* 11 *with* $\ell = 3$.

Example

The curves $y^2 = x^3 + 3$ *and* $y^2 = x^3 + 9$ *are automorphic mod* 11 *with* $\ell = 3$.

Automorphisms $(a = 0)$

Example

The curves $y^2 = x^3 + 8x + 3$ and $y^2 = x^3 + 2x + 9$ are automorphic mod 11 with $\ell = 3$.

Example

The curves $y^2 = x^3 + 3$ and $y^2 = x^3 + 9$ are automorphic mod 11 with $\ell = 3$.

This suggests that when $a = 0$, we only need to store 6 different a_p values, one for each sextic residue class of b. Hence,

$$\#\text{ of } a_p \text{ we need to store } = \begin{cases} 4p + 6 & p \equiv 1 \pmod 4 \\ 2p + 6 & p \equiv 3 \pmod 4. \end{cases}$$

Automorphisms $(a = 0)$ cont.

When $p \not\equiv 1 \pmod 3$, $x \mapsto x^3$ is an bijection. Hence

$$\sum_x \left(\frac{x^3+b}{p}\right) = \sum_x \left(\frac{x+b}{p}\right) = 0.$$

Therefore, we can compute and store fewer a_p:

$$\#\text{ of } a_p \text{ we need to store } = \begin{cases} 4p & p \equiv 1 \pmod 4 \\ 2p & p \equiv 3 \pmod 4 \end{cases} + \begin{cases} 6 & p \equiv 1 \pmod 3 \\ 0 & p \equiv 0, 2 \pmod 3). \end{cases}$$

Automorphisms $(\sqrt{-1})$

Suppose there is some $i \in \mathbb{F}_p$ such that $i^2 = -1$. Then, put $y = iy'$ and $x = -x$, and thus

$$\begin{aligned} y^2 &= x^3 + ax + b \\ (iy')^2 &= -x^3 - ax + b \\ y'^2 &= x^3 + ax - b. \end{aligned}$$

Automorphisms $(\sqrt{-1})$

Suppose there is some $i \in \mathbb{F}_p$ such that $i^2 = -1$. Then, put $y = iy'$ and $x = -x$, and thus

$$\begin{aligned} y^2 &= x^3 + ax + b \\ (iy')^2 &= -x^3 - ax + b \\ y'^2 &= x^3 + ax - b. \end{aligned}$$

Hence, we need to compute a_p for $0 \le b < p/2$. Thus

$$\#\text{ of } a_p \text{ we need to store } = \begin{cases} 2p+2 & p \equiv 1 \pmod 4 \\ 2p & p \equiv 3 \pmod 4 \end{cases} + \begin{cases} 6 & p \equiv 1 \pmod 3 \\ 0 & p \equiv 0, 2 \pmod 3). \end{cases}$$

N.b. this slide has not been implemented due to our code already being sufficiently fast.

Constructing Lookup Table, con.

- Upshot: we store values of a_p for each residue class corresponding to congruence relation of $p \bmod 12$.

Constructing Lookup Table, con.

- Upshot: we store values of a_p for each residue class corresponding to congruence relation of $p \bmod 12$.
- To find $a_T(p)$ corresponding to E_t: $y^2 = x^3 + A(T)x + B(T)$ (for $A(T) \neq 0 \bmod p$):

Constructing Lookup Table, con.

- Upshot: we store values of a_p for each residue class corresponding to congruence relation of $p \bmod 12$.
- To find $a_T(p)$ corresponding to E_t: $y^2 = x^3 + A(T)x + B(T)$ (for $A(T) \neq 0 \bmod p$):
  - for $a = 1, 2, \ldots,$ we compute $A(T)a^{-1} \bmod p$ and check whether it is a fourth power mod p.

Constructing Lookup Table, con.

- Upshot: we store values of a_p for each residue class corresponding to congruence relation of $p \bmod 12$.
- To find $a_T(p)$ corresponding to E_t: $y^2 = x^3 + A(T)x + B(T)$ (for $A(T) \neq 0 \bmod p$):
  - for $a = 1, 2, \ldots,$ we compute $A(T)a^{-1} \bmod p$ and check whether it is a fourth power mod p.
  - Once we have found some a with $A(T)a^{-1} \equiv \ell^4 \bmod p$, we compute the corresponding value of $B(T)$ as $B(T)\ell^{-6} \bmod p$.

Constructing Lookup Table, con.

- Upshot: we store values of a_p for each residue class corresponding to congruence relation of $p \bmod 12$.
- To find $a_T(p)$ corresponding to E_t: $y^2 = x^3 + A(T)x + B(T)$ (for $A(T) \neq 0 \bmod p$):
  - for $a = 1, 2, \ldots,$ we compute $A(T)a^{-1} \bmod p$ and check whether it is a fourth power mod p.
  - Once we have found some a with $A(T)a^{-1} \equiv \ell^4 \bmod p$, we compute the corresponding value of $B(T)$ as $B(T)\ell^{-6} \bmod p$.
  - retrieve the a_p value corresponding to (a, b) (i.e., the automorphic curve $y^2 = x^3 + ax + b = x^3 + A(T)\ell^{-4}x + B(T)\ell^{-6}$).

Constructing Lookup Table, con.

- To find $a_T(p)$ corresponding to E_t: $y^2 = x^3 + A(T)x + B(T)$ (for $A(T) = 0 \bmod p$):

Constructing Lookup Table, con.

- To find $a_T(p)$ corresponding to E_t: $y^2 = x^3 + A(T)x + B(T)$ (for $A(T) = 0 \bmod p$):
  - $a_p = 0$ if $p \not\equiv 1 \bmod 3$ or $B(T) = 0 \bmod p$.

Constructing Lookup Table, con.

- To find $a_T(p)$ corresponding to E_t: $y^2 = x^3 + A(T)x + B(T)$ (for $A(T) = 0 \bmod p$):
  - $a_p = 0$ if $p \not\equiv 1 \bmod 3$ or $B(T) = 0 \bmod p$.
  - Otherwise, we find sixth power residue class of $B(T)$ by computing $B(T)b^{-1} \bmod p$ for each value of b stored until this is sixth power residue.

Constructing Lookup Table, con.

- To find $a_T(p)$ corresponding to E_t: $y^2 = x^3 + A(T)x + B(T)$ (for $A(T) = 0 \bmod p$):
  - $a_p = 0$ if $p \not\equiv 1 \bmod 3$ or $B(T) = 0 \bmod p$.
  - Otherwise, we find sixth power residue class of $B(T)$ by computing $B(T)b^{-1} \bmod p$ for each value of b stored until this is sixth power residue.
  - For such b such that $B(T)b^{-1} \equiv \ell^6 \bmod p$, we retrive a_p value for curve $y^2 = x^3 + b$.

Computing Square Roots

- Only non-trivial arithmetic computation is computing square roots of $x \bmod p$ (assuming x is a square):

Computing Square Roots

- Only non-trivial arithmetic computation is computing square roots of $x \bmod p$ (assuming x is a square):
  - $p \equiv 3 \bmod 4$: $(x^{\frac{p+1}{4}})^2 = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}} x = x.$

Computing Square Roots

- Only non-trivial arithmetic computation is computing square roots of $x \bmod p$ (assuming x is a square):
  - $p \equiv 3 \bmod 4$: $(x^{\frac{p+1}{4}})^2 = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}} x = x$.
  - $p \equiv 1 \bmod 4$: use Cipolla's algorithm:

Computing Square Roots

- Only non-trivial arithmetic computation is computing square roots of $x \bmod p$ (assuming x is a square):
  - $p \equiv 3 \bmod 4$: $(x^{\frac{p+1}{4}})^2 = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}} x = x$.
  - $p \equiv 1 \bmod 4$: use Cipolla's algorithm:
    - Use trial and error to find $a \in \mathbb{F}_p$ such that $a^2 - x$ is not square (expected number of trials is about 2); no deterministic algorithm known.

Computing Square Roots

- Only non-trivial arithmetic computation is computing square roots of $x \bmod p$ (assuming x is a square):
  - $p \equiv 3 \bmod 4$: $(x^{\frac{p+1}{4}})^2 = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}} x = x$.
  - $p \equiv 1 \bmod 4$: use Cipolla's algorithm:
    - Use trial and error to find $a \in \mathbb{F}_p$ such that $a^2 - x$ is not square (expected number of trials is about 2); no deterministic algorithm known.
    - Then $((a + \sqrt{a^2 - x})^{\frac{p+1}{2}})^2 = x \in \mathbb{F}_p(\sqrt{a^2 - x}) \cong \mathbb{F}_{p^2}$, but $(a + \sqrt{a^2 - x})^{\frac{p+1}{2}} \in \mathbb{F}_p$ since x is a square in $\mathbb{F}_p$.

1 Intro to L-Functions

2 Bias Applications

3 Preliminaries

4 Computation of a_p

5 Computational Investigation

6 Normalized Second Moment

7 Algebraic Geometry

Normalized Second Moment

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

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

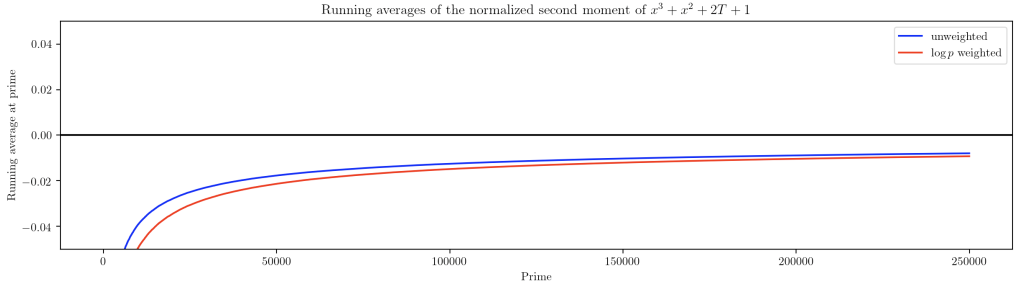
- We compute the *normalized second moment* of $\mathscr{A}_{2,\mathscr{E}}(p)$, which we define to be

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

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

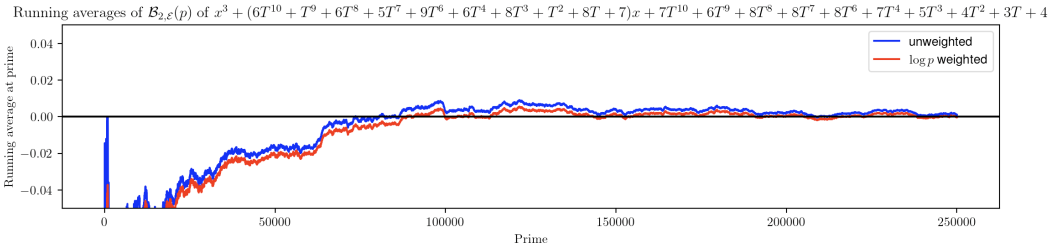
A Family with Known Negative Bias

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

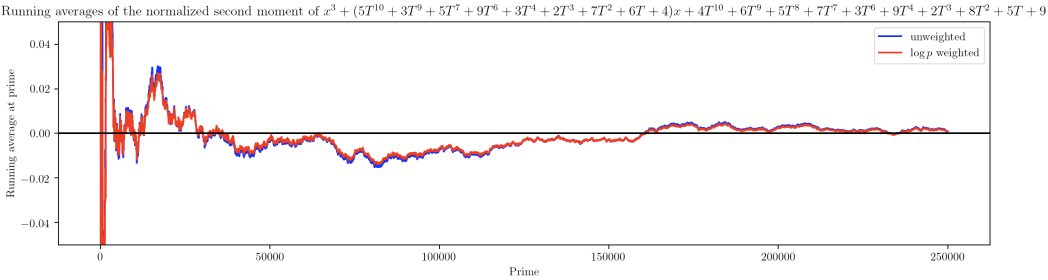


SMALL '24 Generic Random Family 1

We sampled coefficients iid from $\{0, 1, \ldots, 9\}$ and obtained the following families.

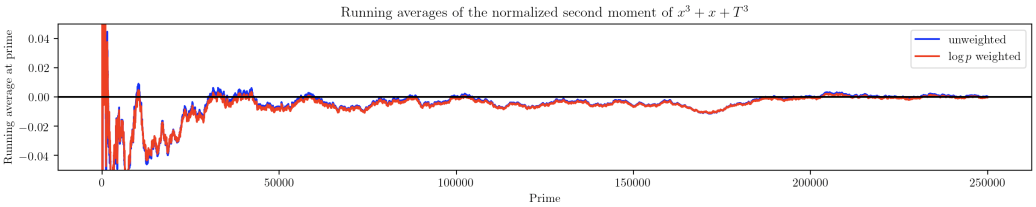


SMALL '24 Generic Random Family 2



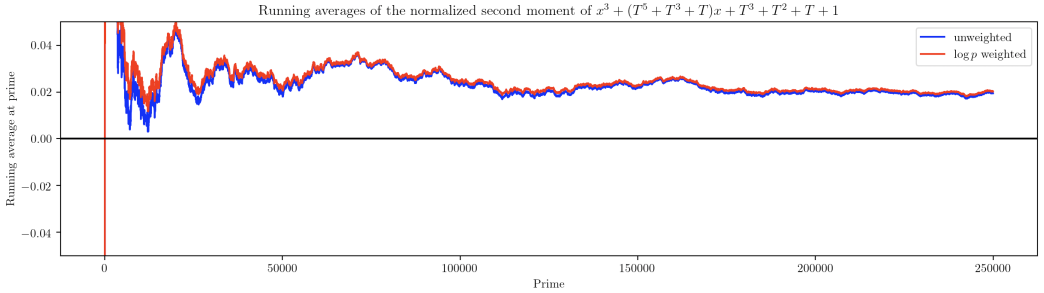
SMALL '23 Family

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



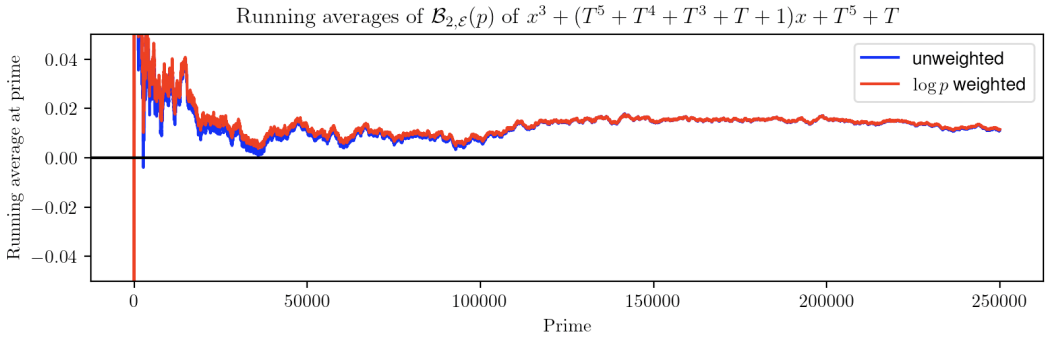
SMALL '24 Potential Positive Bias Family 1: $x^3 + (T^5 + T^3 + T)x + T^3 + T^2 + T + 1$

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



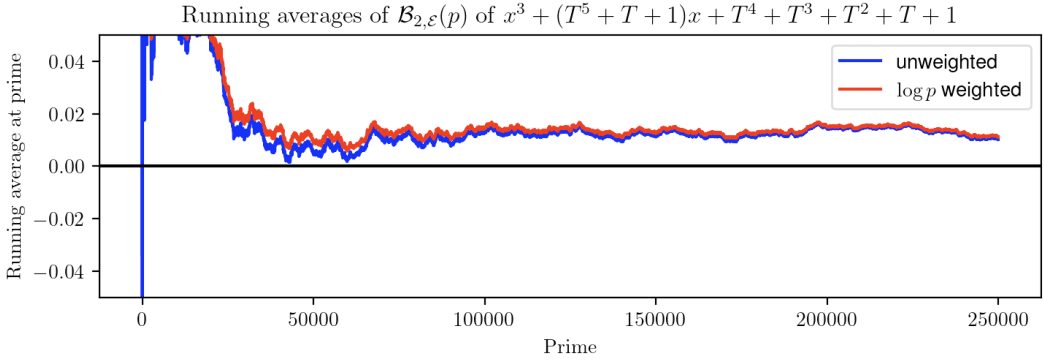
SMALL '24 Potential Positive Bias Family 2: $x^3 + (T^5 + T^4 + T^3 + T + 1)x + T^5 + T$

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



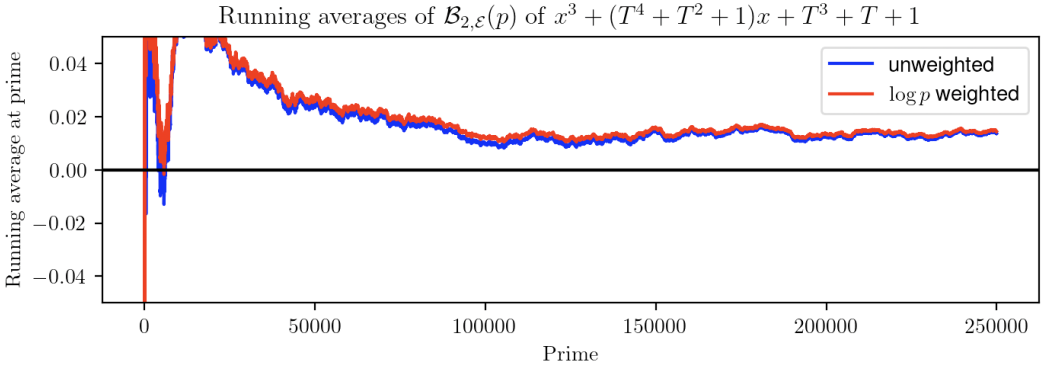
SMALL '24 Potential Positive Bias Family 3: $x^3 + (T^5 + T + 1)x + T^4 + T^3 + T^2 + T + 1$

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

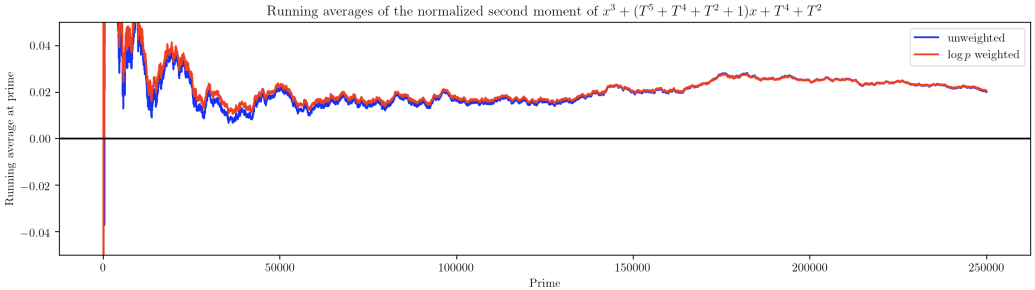


SMALL '24 Potential Positive Bias Family 4: $x^3 + (T^4 + T^2 + 1)x + T^3 + T + 1$

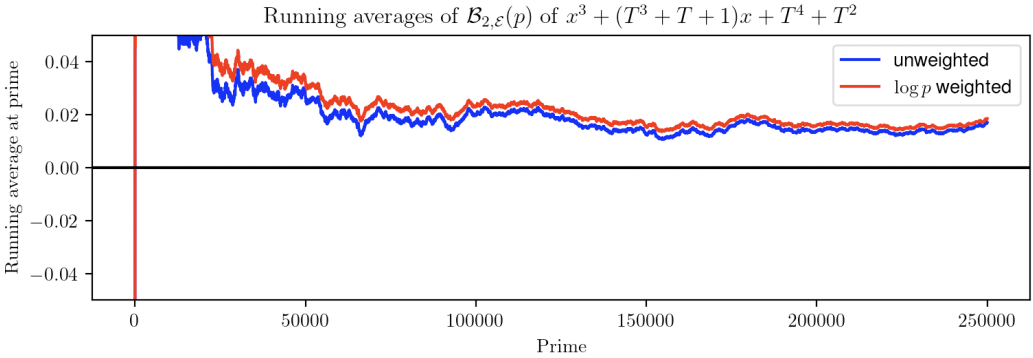
$$A(T) = (T^2 - T + 1)(T^2 + T + 1)$$



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

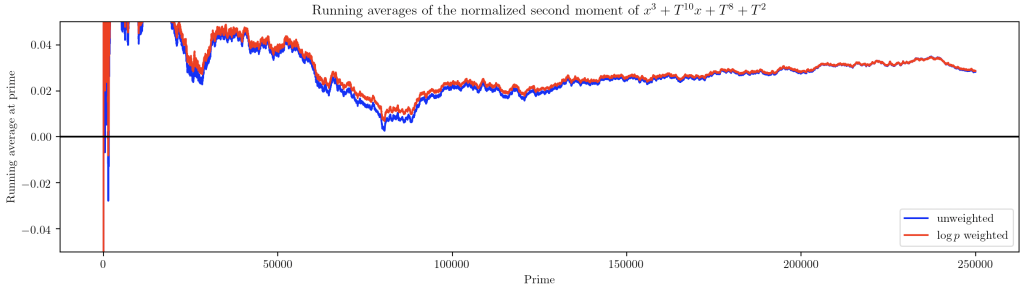


SMALL '24 Potential Positive Bias Family 6: $x^3 + (T^3 + T + 1)x + T^4 + T^2$



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 ~ 3.4 in one million times.

1 Intro to L-Functions

2 Bias Applications

3 Preliminaries

4 Computation of a_p

5 Computational Investigation

6 Normalized Second Moment

7 Algebraic Geometry

Motivation

Theorem (Sato-Tate, Taylor et al. 2006 and 2008)

Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication, then $a_p/2\sqrt{p}$ converges to a semicircular distribution.

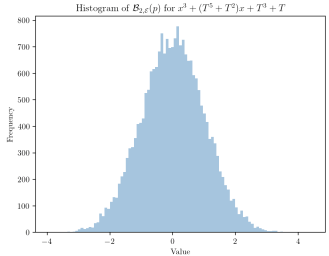
Motivation

Theorem (Sato-Tate, Taylor et al. 2006 and 2008)

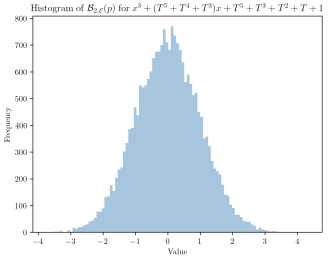
Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication, then $a_p/2\sqrt{p}$ converges to a semicircular distribution.

This motivates the exploration of the distribution of the normalized second moment.

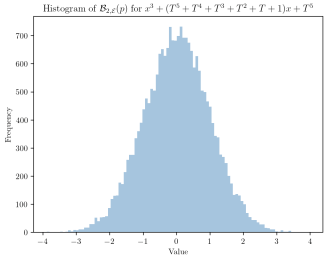
Distribution of the normalized second moment



Variance = 1.0151610262691482



Variance = 1.0046817588446215



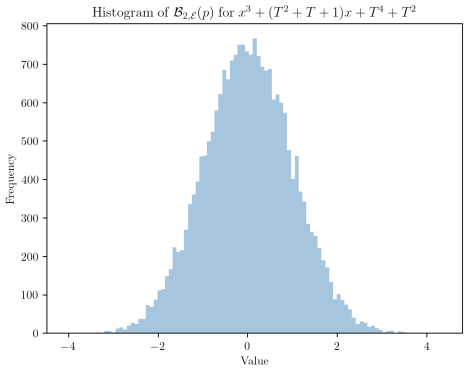
Variance = 0.9891139950619033

Conjecture

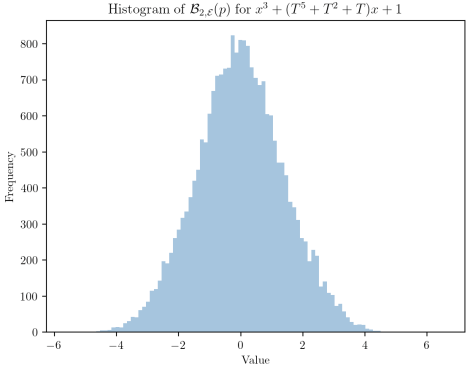
The variance of normalized second moments of a one-parameter family converges to an integer.

Question

What distribution does $\mathscr{B}_{2,\mathscr{E}}(p)$ converge to and what determines the variance?

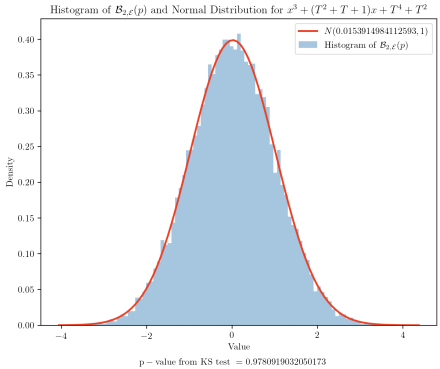


Variance = 0.9941929897237586

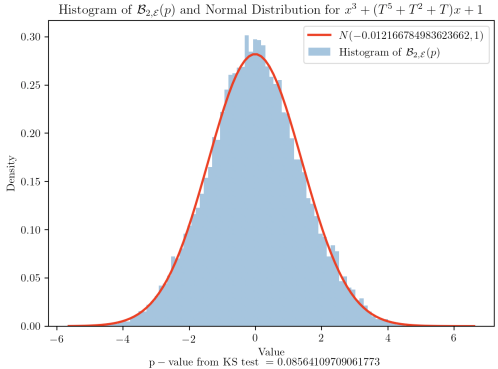


Variance = 1.9905981294487558

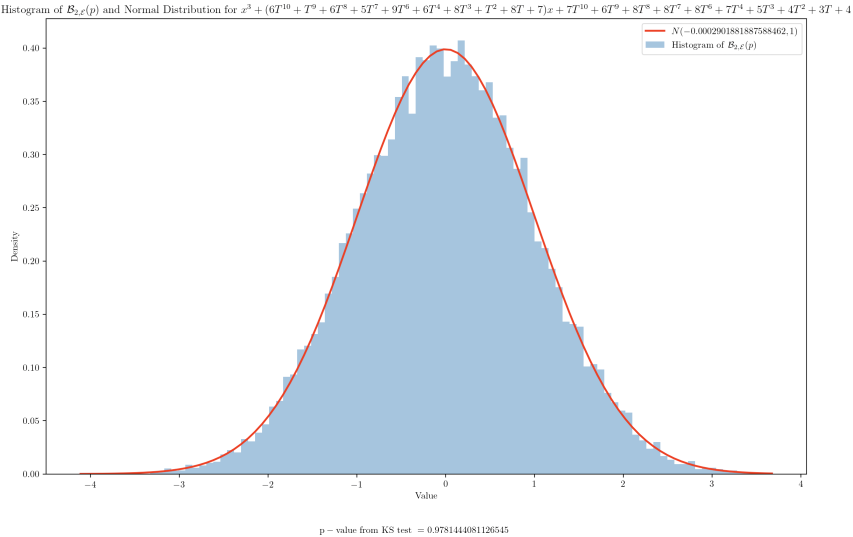
An Open Problem: Gaussian-like Behavior

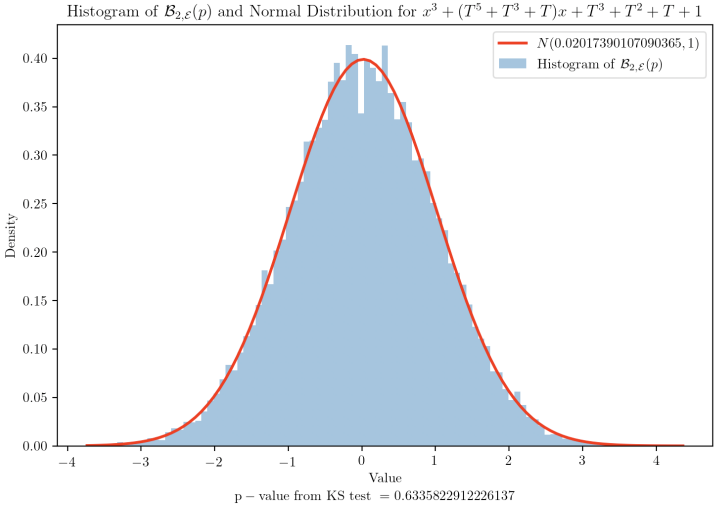


Variance = 0.9941929897237586



Variance = 1.9905981294487558


Histogram of $\mathcal{B}_{2,\mathcal{E}}(p)$ and Normal Distribution for $x^3+(6T^{10}+T^9+6T^8+5T^7+9T^6+6T^4+8T^3+T^2+8T+7)x+7T^{10}+6T^9+8T^8+8T^7+8T^6+7T^4+5T^3+4T^2+3T+4$
$N(-0.00029018818875884 62,1)$
Histogram of $\mathcal{B}_{2,\mathcal{E}}(p)$
Density
Value
p − value from KS test = 0.9781444081126545


Histogram of $\mathcal{B}_{2,\mathcal{E}}(p)$ and Normal Distribution for $x^3 + (T^5 + T^3 + T)x + T^3 + T^2 + T + 1$
$N(0.02017390107090365, 1)$
Histogram of $\mathcal{B}_{2,\mathcal{E}}(p)$
Density
0.00
0.05
0.10
0.15
0.20
0.25
0.30
0.35
0.40
−4
−3
−2
−1
0
1
2
3
4
Value
p − value from KS test = 0.6335822912226137

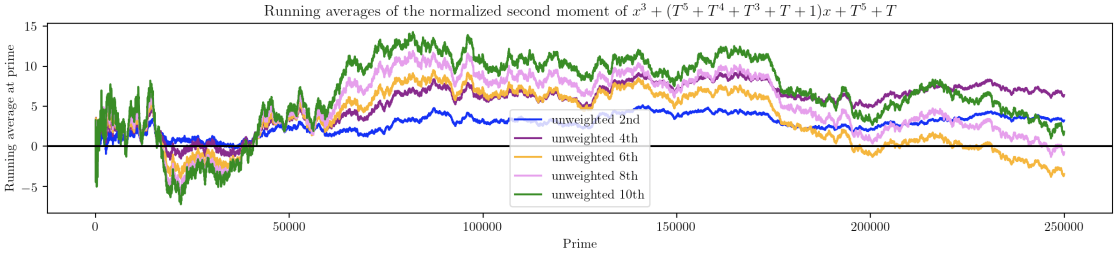
Higher moments

It turns out that

$$\mathscr{A}_{2n,\mathscr{E}}(p) \;=\; C_n p^{n+1} + O(p^{n+1/2}),$$

where C_n denotes the nth Catalan number. If we normalize $\mathscr{A}_{2n,\mathscr{E}}$ via

$$\mathscr{B}_{2n,\mathscr{E}}(p) \;=\; \frac{\mathscr{A}_{2n,\mathscr{E}}(p)}{C_n p^{n+1/2}} - \sqrt{p},$$



We can similarly study the histogram of $\mathscr{B}_{2n,\mathscr{E}}(p)$ values for $n = 2, 3, 4, 5$

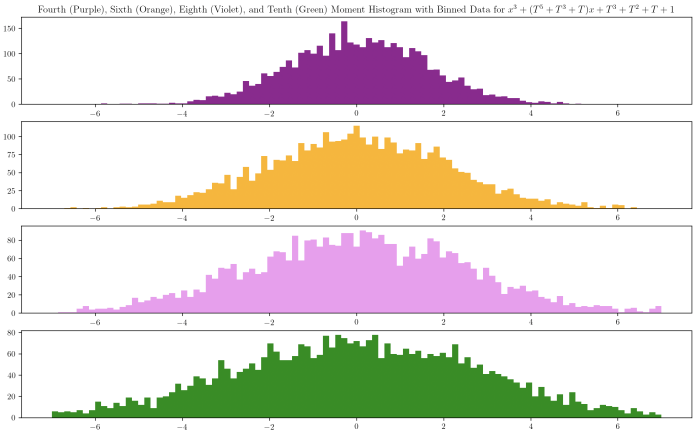


Figure 1: Normalized centered moments split into 100 buckets from -7 to 7

Similarly, we can ask if the variance of these higher moments converges to an integer. The numerical evidence suggests that this is false for moments $2n > 2$.
However, if we define a slightly different normalization for $\mathscr{A}_{2n,\mathscr{E}}$

$$\mathscr{B}'_{2n,\mathscr{E}}(p) \;=\; \frac{\mathscr{A}_{2n,\mathscr{E}}(p)}{p^{n+1/2}} - C_n\sqrt{p},$$

then this effectively multiplies all our normalized values of C_n, and thus multiplies the variance of C_n^2. Here, for $p \leq 250,000$ single data points can change the variance by .1 or more, and thus we do not have enough data to conjecture or reject that the variance converges to an integer.

1 Intro to L-Functions

2 Bias Applications

3 Preliminaries

4 Computation of a_p

5 Computational Investigation

6 Normalized Second Moment

7 Algebraic Geometry

Threefolds

We relate the bias in the second moment to point counting on a threefold. For a given one parameter family $y^2 = x^3 + A(T)x + B(T)$, consider the surface

$$y_i^2 z_i = x_i^3 + A(T)x_i z_i^2 + B(T)z_i^3, \qquad \text{for } i = 1, 2.$$

Threefolds

We relate the bias in the second moment to point counting on a threefold. For a given one parameter family $y^2 = x^3 + A(T)x + B(T)$, consider the surface

$$y_i^2 z_i = x_i^3 + A(T)x_i z_i^2 + B(T)z_i^3, \quad \text{for } i = 1, 2.$$

To make these calculations possible, we need to be in weighted projective space. If $\deg A \leq 4$ and $\deg B \leq 6$, we let $A(T, U)$ and $B(T, U)$ be the homogenizations of $A(T)$ and $B(T)$ to degree 4 and 6 we consider the threefold

$$V : y_i^2 z_i = x_i^3 + A(T, U)x_i z_i^2 + B(T, U)z_i^3, \quad \text{for } i = 1, 2.$$

Rational Threefold

In general, V is extremely complicated, e.g., a Calabi-Yau manifold:

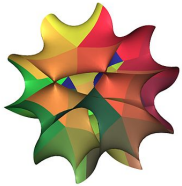


Figure from Andrew J. Hanson's "A construction for computer visualization of certain complex curves," Notices of the Amer. Math. Soc. 41 (9): 1156-1163, (November/December 1994)

- However, if for $p > 7$, we can control our elliptic surface mod p, then V becomes rational.
- In some sense this means our singularities are controllable.
- From there one can use known techniques to count points on V mod p.

Acknowledgements

We are grateful to Professor Steven J. Miller for suggesting this problem and for his mentorship. We would also like to thank Adam Logan for many helpful conversations.

This research was supported by the National Science Foundation, under grant DMS2241623, Duke University, Princeton University, the University of Michigan, and Williams College.

References

[1] Z. Batterman, A. Jambhale, S.J. Miller, A. L. Narayanan, K. Sharma, C. Yao, *Applications of Moments of Dirichlet Coefficients in Elliptic Curve Families*, ICERM Conference Proceedings for the July 2023 Murmurations Workshop.

[2] T. Cheek, P. Gilman, K. Jaber, V. Sharan, and M. Tomé. Elliptic Curve Coding. GitHub repository. 2024. https://github.com/KareemSaysHi/SMALL2024-Elliptic-Curve-Coding.

[3] Andrew J. Hanson, "A construction for computer visualization of certain complex curves," Notices of the Amer. Math. Soc. 41 (9): 1156-1163, (November/December 1994).

[4] P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Mont. Math. 120 (1995) 127-136.

[5] S. J. Miller, *One- and two-level densities for families of elliptic curves: evidence for the underlying group symmetries*. Princeton University, PhD thesis, 2002.

[6] 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.

[7] S. J. Miller, *Variation in the number of points on elliptic curves and applications to excess rank*, C. R. Math. Acad. Sci. Soc. R. Can., 27 (2005) no. 4, 111–120.

[8] S. J. Miller, *Investigations of zeros near the central point of elliptic curve L-functions*, Exp. Math. 15 (2006), no. 3, 257–279.

[9] K. Nagao, $\mathbb{Q}(T)$*-rank of elliptic curves and certain limit coming from local points*, Manuscr. Math. 92 (1997) 13-32.

[10] M. Rosen and J. H. Silverman, *On the rank of an elliptic surface*, Invent. Math. 133 (1998), 43-67.

[11] K. Rubin and A. Silverberg. *Ranks of Elliptic Curves*, Bull. AMS 39 (2002), 455-474.