Lower Order Biases in Fourier Coefficients of Elliptic Curve and Cuspidal Newform families

Jared Lichtman, Steven Miller, Eric Winsor & Jianing Yang
jared.d.lichtman.18@dartmouth.edu, sjm1@williams.edu
rcwnsr@umich.edu, jyang@colby.edu
with Ryan Chen & Yujin H. Kim
Advisor: Steven J. Miller

Maine-Québec Number Theory Conference
Univ. o. Maine, October XIV, MMXVII

Elliptic Curves over $\mathbb{Q}$

Interested in elliptic curves over $\mathbb{Q}$

$$E/\mathbb{Q} : y^2 = x^3 + ax + b \cup \{\infty\}$$

where $a, b \in \mathbb{Q}$ and $4a^3 + 27b^2 \neq 0$, and their reduction mod p.

Definition (Good reduction)

An elliptic curve $E/\mathbb{Q} : y^2 = x^3 + ax + b$ has *good reduction* at a prime p if $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$.
The reduction $E(\mathbb{F}_p)$ is defined as $y^2 = x^3 + [a]x + [b]$, where $[a], [b]$ are the reductions of a and $b \pmod{p}$.

Hasse's Theorem

Recall

$$\begin{aligned} E(\mathbb{F}_p) &:= \{(x,y) : y^2 = x^3 + ax + b\} \\ \#E(\mathbb{F}_p) &= \sum_{x \in \mathbb{F}_p} \left(1 - \left(\frac{x^3+ax+b}{p}\right)\right) + 1 \\ &= p + 1 - \sum_{x \in \mathbb{F}_p} \left(\frac{x^3+ax+b}{p}\right). \end{aligned}$$

Define the *Frobenius trace* as $a_E(p) := p + 1 - \#E(\mathbb{F}_p)$, have Hasse bound $|a_E(p)| \leq 2\sqrt{p}$.

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

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

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 $\mathcal{E}$,

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

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, observe:

Bias Conjecture

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

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.

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

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

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

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.

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

Second Moments of Linear-coefficient Families

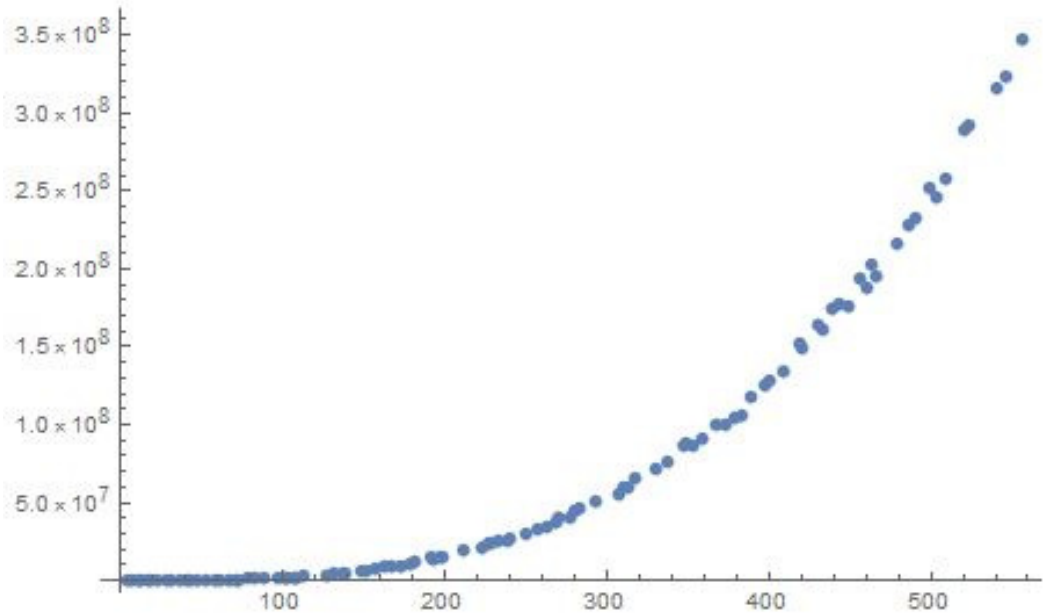
We computed explicit formulas for the second moments of some one-parameter families with linear coefficients in T:

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

Numerics for Higher Even Moments

Want to compute all higher moments; however, going beyond the second leads to intractable Legendre sums. Have some numerical results for higher moments.

For example, the 4^{th} moment of $y^2 \equiv x^3 + (t+1)x^2 + tx$:



Families with Constant $j(T)$

Constant $j(T)-$invariant families

Question: What happens in families with constant $j(T)-$?

- $\mathcal{E}(T) : y^2 = x^3 + A(T)x$ has $j(T) = 1728, \forall T \in \mathbb{Z}$.
- $\mathcal{E}(T) : y^2 = x^3 + B(T)$ has $j(T) = 0$.

For these families we can compute any moment.

Computation is *fast* when $j(T)$ is constant.

$j = 0$ Curves

Consider $\mathcal{E} : y^2 = x^3 + B$ over $\mathbb{F}_p$.

If $p \equiv 2 \pmod 3$, then $a_E(p) = 0$.

Gauss' Six-Order Theorem

If $p \equiv 1 \pmod 3$, can write $p = a^2 + 3b^2$, $a \equiv 2 \pmod 3$, $b > 0$, and

$$a_E(p) = \begin{cases} -2a & B \text{ is a sextic residue in } \mathbb{F}_p \\ 2a & B \text{ cubic, non-sextic residue} \\ a \pm 3b & B \text{ quadratic, non-sextic} \\ -a \pm 3b & B \text{ non-quadratic, non-cubic.} \end{cases}$$

Moments of One-Parameter $j = 0$ Families

For $r \geq 0$, compute k^{th} moment of $\mathcal{E}_T : y^2 = x^3 - AT^r$.

Have $A_k(p) = 0$ when $p \equiv 3(4)$, and moments determined only by $r \pmod 6$:

$$r \equiv 1, 5(6) \ : A_k(p) = \begin{cases} 0 & k \text{ is odd} \\ \frac{p-1}{3}\left((2a)^k + (a-3b)^k + (a+3b)^k\right) & k \text{ is even} \end{cases}$$

$$r \equiv 2, 4(6) \ : A_k(p) = \begin{cases} \frac{p-1}{3}\left((-2a)^k + (a-3b)^k + (a+3b)^k\right) & A \text{ quadratic residue} \\ \frac{p-1}{3}\left((2a)^k + (-a-3b)^k + (-a+3b)^k\right) & A \text{ quadratic nonresidue} \end{cases}$$

$$r \equiv 3 \ : A_k(p) = \begin{cases} \frac{p-1}{2}\left((-2a)^k + (2a)^k\right) & A \text{ cubic residue} \\ \frac{p-1}{2}\left((a \pm 3b)^k + (-a \mp 3b)^k\right) & A \text{ cubic nonresidue.} \end{cases}$$

$j = 1728$ Curves

Consider $\mathcal{E} : y^2 = x^3 - Ax$ over $\mathbb{F}_p$.

If $p \equiv 3 \pmod 4$, then $a_E(p) = 0$.

Gauss' Four-Order Theorem

If $p \equiv 1 \pmod 4$, then write $p = a^2 + b^2$, where b is even and $a + b \equiv 1 \pmod 4$. We have:

$$a_E(p) = \begin{cases} 2a & A \text{ is a quartic residue} \\ -2a & A \text{ quadratic, non-quartic residue} \\ \pm 2b & A \text{ not a quadratic residue.} \end{cases}$$

Moments of One-Parameter $j = 1728$ Families

For $r \geq 0$, consider $\mathcal{E}(T) : y^2 = x^3 - AT^r x$. When $p \equiv 3 \pmod 4$, all moments are 0. Have

$$r \equiv 1, 3(4) \ : A_k(p) = \begin{cases} 0 & k \text{ is odd} \\ (p-1)2^{k-1}(a^k + b^k) & k \text{ is even} \end{cases}$$

$$r \equiv 2(4) \ : A_k(p) = \begin{cases} 0 & k \text{ is odd} \\ (p-1)(2a)^k & A \text{ quadratic residue}, k \text{ is even} \\ (p-1)(2b)^k & A \text{ quadratic nonresidue}, k \text{ is even} \end{cases}$$

For $r \equiv 0(4)$, we get similar but more elaborate results.

Bias in L-functions of Cuspidal Newforms

Cuspidal Newforms

Definition (Holomorphic Form of Weight k, level N)

A holomorphic function $f(z) : \mathbb{H} \to \mathbb{C}$, of moderate growth, for which

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \text{ where}$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \right\}.$$

Modular forms are *periodic* and have a Fourier expansion, if constant term equals 0 called a **cusp form**. A cuspidal **newform** of level N is a cusp form that cannot be reduced to a cusp form of level M, where $M \mid N$.

Averaging over Weights

Let $\mathcal{F}_{X,\delta,N}$ be the family of cuspidal newforms of weights smaller than some positive X^δ of a square-free level N.

Averaging over primes less than X^σ, define the r^{th} moment of the family $\mathcal{F}_{X,\delta,N}$ as:

$$M_{r,\sigma}(\mathcal{F}_{X,\delta,N}) = \frac{1}{\pi(X^\sigma)} \sum_{p<X^\sigma} \frac{1}{\sum_{k<X^\delta} |H_k^*(N)|} \sum_{k<X^\delta} \sum_{f\in H_k^*(N)} \lambda_f^r(p).$$

Averaging over Weights

Let $\mathcal{F}_{X,\delta,N}$ be the family of cuspidal newforms of weights smaller than some positive X^δ of a square-free level N.

Averaging over primes less than X^σ, define the r^{th} moment of the family $\mathcal{F}_{X,\delta,N}$ as:

$$M_{r,\sigma}(\mathcal{F}_{X,\delta,N}) = \frac{1}{\pi(X^\sigma)} \sum_{p<X^\sigma} \frac{1}{\sum_{k<X^\delta} |H_k^*(N)|} \sum_{k<X^\delta} \sum_{f\in H_k^*(N)} \lambda_f^r(p).$$

Study the asymptotic behavior of the moments as $N \to \infty$:

$$M_{r,\sigma}(\mathcal{F}_{X,\delta}) = \lim_{N\to\infty} M_{r,\sigma}(\mathcal{F}_{X,\delta,N}).$$

Averaging over Weights

Theorem (SMALL '17)

Let $\mathcal{F}_{X,\delta,N}$ be the family of cuspidal newforms of weights $k \leq X^{\delta}$ of a square-free level N, and $M_{r,\sigma}(\mathcal{F}_{X,\delta})$ the limiting r^{th} moment of the family as the level $N \to \infty$. Then

$$M_{r,\sigma}(\mathcal{F}_{X,\delta}) = \begin{cases} C_{r/2} + C_{r/2-1}\frac{\log\log X^{\sigma}}{\pi(X^{\sigma})} & \text{even r} \\ \quad + O\left(\frac{1}{X^{2\delta}} + \frac{1}{\pi(X^{\sigma})}\right) & \\ 0 & \text{odd } r, \end{cases}$$

where $C_n = \frac{1}{n+1}\binom{2n}{n}$ is the n^{th} Catalan number.

Bias for cuspidal newforms is a positive integer, instead of the negative bias in elliptic curve families.

An Important Tool: Petersson Trace Formula

Petersson Trace Formula

For any $n, m \geq 1$, we have

$$\frac{\Gamma(k-1)}{(4\pi p)^{k-1}} \sum_{f \in H^*_{k,N}(\chi_0)} |\lambda_f(p)|^2 = \delta(p,p) + 2\pi i^{-k} \sum_{c \equiv 0(N)} \frac{S_c(p,p)}{c} J_{k-1}\left(\frac{4\pi p}{c}\right)$$

where $\lambda_f(n)$ is the n-th Hecke eigenvalue of f,
$\delta(m,n)$ is Kronecker's delta,
$S_c(m,n)$ is the classical Kloosterman sum, and
$J_{k-1}(t)$ is the k-Bessel function.

An Important Tool: Petersson Trace Formula

[ILS] gives the following bound for the Petersson Trace Formula:

$$\sum_{f \in H_k^*(N)} \lambda_f(n) = \begin{cases} \delta_{n,\square} \frac{k-1}{12} \frac{\varphi(N)}{\sqrt{n}} & n^{\frac{9}{7}} \leq k^{\frac{16}{21}} N^{\frac{6}{7}} \\ 0 & \text{else} \end{cases} + O\left((n,N)^{-\frac{1}{2}} n^{\frac{1}{6}} k^{\frac{2}{3}} N^{\frac{2}{3}}\right)$$

where level N and n are square-free, $(n, N^2) \mid N$, and $\varphi(n)$ denotes the Euler totient function.

We also find the following relation that allows us to compute higher moments of cuspidal newform families.

$$\lambda_f(p)^r = \sum_{0 \leq l \leq r/2} C(r-l, l) \lambda_f(p^{r-2l})$$

where $C(n,k) = \binom{n+k}{k} - \binom{n+k}{k-1}$ are numbers in the Catalan's Triangle.

Questions for Further Study

- Does the Bias Conjecture hold for elliptic families with constant j-invariant?
- Are there cuspidal newform families with negative biases in their moments?
- Does the average bias always occur in the terms of size p or 1?
- How is the Bias Conjecture formulated for all higher even moments? Can they be modeled by polynomials?
- What other families obey the Bias Conjecture? Kloosterman sums? Higher genus curves?

References

- 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.

- S.J. Miller, S. Wong, *Moments of the rank of elliptic curves*, Canad. J. of Math. **64** (2012), no. 1, 151–182. http://web.williams.edu/Mathematics/sjmiller/public_html/math/papers/mwMomentsRanksEC812final.pdf

Thank you!

Questions?

Work supported by NSF Grants DMS1561945 and DMS1659037, Dartmouth College, Princeton University and Williams College.