Lower-Order Biases in Elliptic Curve Fourier Coefficients

Karl Winsor
Joint with Blake Mackall, Steven J. Miller, Christina Rapti
krlwnsr@umich.edu

SMALL REU 2014, Williams College

29th Automorphic Forms Workshop,
Ann Arbor, Michigan
March 3, 2015

Table of Contents

Table of Contents

Elliptic Curves

An *elliptic curve* E over $\mathbb{Q}$ is the set of solutions $(x, y) \in \mathbb{Q}^2$ to an equation of the form

$$E : y^2 = x^3 + ax^2 + bx + c$$

with $a, b, c \in \mathbb{Z}$. For primes $p > 3$ the *elliptic curve Fourier coefficients* are

$$a_E(p) = p - \#\{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + ax^2 + bx + c\}.$$

Elliptic Curves

An *elliptic curve* E over $\mathbb{Q}$ is the set of solutions $(x, y) \in \mathbb{Q}^2$ to an equation of the form

$$E : y^2 = x^3 + ax^2 + bx + c$$

with $a, b, c \in \mathbb{Z}$. For primes $p > 3$ the *elliptic curve Fourier coefficients* are

$$a_E(p) = p - \#\{(x, y) \in \mathbb{F}_p^2 : y^2 = x^3 + ax^2 + bx + c\}.$$

The associated Dirichlet series

$$L(E, s) = \sum_{n=1}^{\infty} \frac{a_E(n)}{n^s}, \quad \Re(s) > \frac{3}{2}$$

can be analytically continued to an L-function on all of $\mathbb{C}$.

Families and Moments

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

$$\mathcal{E} : y^2 = x^3 + A[T]x^2 + B[T]x + C[T]$$

with $A[T], B[T], C[T] \in \mathbb{Z}[T]$.

Families and Moments

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

$$\mathcal{E} : y^2 = x^3 + A[T]x^2 + B[T]x + C[T]$$

with $A[T], B[T], C[T] \in \mathbb{Z}[T]$.

- Each specialization of T to an integer t gives an elliptic curve $\mathcal{E}(t)$ over $\mathbb{Q}$.

Families and Moments

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

$$\mathcal{E} : y^2 = x^3 + A[T]x^2 + B[T]x + C[T]$$

with $A[T], B[T], C[T] \in \mathbb{Z}[T]$.

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

$$A_{r,\mathcal{E}}(p) = \sum_{t=0}^{p-1} a_{\mathcal{E}(t)}(p)^r.$$

Table of Contents

Bias Conjecture

Second Moment Asymptotic [Michel]

For "nice" families $\mathcal{E}$, the second moment of the Fourier coefficients is equal to

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

Bias Conjecture

Second Moment Asymptotic [Michel]

For "nice" families $\mathcal{E}$, the second moment of the Fourier coefficients is equal to

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

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

Bias Conjecture

Second Moment Asymptotic [Michel]

For "nice" families $\mathcal{E}$, the second moment of the Fourier coefficients is equal to

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

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

In every family we have studied, we have observed:

Bias Conjecture

Second Moment Asymptotic [Michel]

For "nice" families $\mathcal{E}$, the second moment of the Fourier coefficients is equal to

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

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

In every family we have studied, we have observed:

Bias Conjecture

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

One Interpretation

Sato-Tate Law for Families without CM

For large primes p, the distribution of $\frac{a_{\mathcal{E}(t)}(p)}{\sqrt{p}}$, $t \in \{0, \dots, p-1\}$, approaches the semicircular density $F(x) = \frac{1}{2\pi} \int_{-2}^{x} \sqrt{4 - u^2} du$ on $[-2, 2]$.

- The Bias Conjecture can be interpreted as approaching the limiting second moment from below, as $p \to \infty$.

One Interpretation

Sato-Tate Law for Families without CM

For large primes p, the distribution of $\frac{a_{\mathcal{E}(t)}(p)}{\sqrt{p}}$, $t \in \{0, \ldots, p-1\}$, approaches the semicircular density $F(x) = \frac{1}{2\pi} \int_{-2}^{x} \sqrt{4 - u^2} du$ on $[-2, 2]$.

- The Bias Conjecture can be interpreted as approaching the limiting second moment from below, as $p \to \infty$.

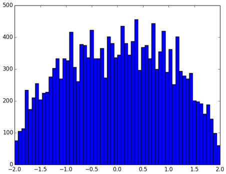


Figure: $a_{\mathcal{E}(t)}(p)$ for $y^2 = x^3 + Tx + 1$ at the 2014th prime

Implications for Excess Rank

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

Negative Bias in the First Moment

The First Moment $A_{1,\mathcal{E}}(p)$ and Family Rank [Rosen-Silverman]

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

Negative Bias in the First Moment

The First Moment $A_{1,\mathcal{E}}(p)$ and Family Rank [Rosen-Silverman]

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

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

Negative Bias in the First Moment

The First Moment $A_{1,\mathcal{E}}(p)$ and Family Rank [Rosen-Silverman]

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

- By the Prime Number Theorem, $A_{1,\mathcal{E}}(p) = -rp + O(1)$ implies $\mathrm{rank}(\mathcal{E}(\mathbb{Q}[T])) = r$.
- We can use this to study families of varying rank and understand the relationship between $A_{2,\mathcal{E}}(p)$ and $\mathrm{rank}(\mathcal{E}(\mathbb{Q}[T]))$.

Table of Contents

Methods for Obtaining Explicit Formulas

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

$$a_{\mathcal{E}(t)}(p) = -\sum_{x=0}^{p-1} \left(\frac{x^3 + A(t)x^2 + B(t)x + C(t)}{p} \right)$$

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

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a nonzero square in } \mathbb{F}_p \\ 0 & \text{if } x = 0 \text{ in } \mathbb{F}_p \\ -1 & \text{if } x \text{ is not a square in } \mathbb{F}_p \end{cases}$$

Lemmas on Legendre Symbols

Linear and Quadratic Legendre Sums

$$\sum_{x=0}^{p-1} \left(\frac{ax+b}{p}\right) = 0 \quad \text{if } p \nmid a$$

$$\sum_{x=0}^{p-1} \left(\frac{ax^2+bx+c}{p}\right) = \begin{cases} -\left(\frac{a}{p}\right) & \text{if } p \nmid b^2-4ac \\ (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2-4ac \end{cases}$$

Lemmas on Legendre Symbols

Linear and Quadratic Legendre Sums

$$\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)=0 \quad \text{if } p \nmid a$$

$$\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)=\begin{cases}-\left(\frac{a}{p}\right) & \text{if } p \nmid b^2-4ac \\ (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2-4ac\end{cases}$$

Average Values of Legendre Symbols

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

Rank 0 Families

Theorem [MMRW'14]: Rank 0 Families Obeying the Bias Conjecture

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

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

Rank 0 Families

Theorem [MMRW'14]: Rank 0 Families Obeying the Bias Conjecture

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

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

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

Families with Rank

Theorem [MMRW'14]: Families with Rank

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

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

Families with Rank

Theorem [MMRW'14]: Families with Rank

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

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

- These include families of rank 0, 1, and 2.

Families with Rank

Theorem [MMRW'14]: Families with Rank

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

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

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

Families with Complex Multiplication

Theorem [MMRW'14]: Families with Complex Multiplication

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

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

Families with Complex Multiplication

Theorem [MMRW'14]: Families with Complex Multiplication

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

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

- The average bias in the size p term is -1.

Families with Complex Multiplication

Theorem [MMRW'14]: Families with Complex Multiplication

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

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

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

Families with Unusual Distributions of Signs

Theorem [MMRW'14]: Families with Unusual Signs

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

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

Families with Unusual Distributions of Signs

Theorem [MMRW'14]: Families with Unusual Signs

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

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

- The average bias in the size p term is -2.

Families with Unusual Distributions of Signs

Theorem [MMRW'14]: Families with Unusual Signs

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

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

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

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

Theorem [MMRW'14]: Families with a Large Error

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

$$A_{2,\mathcal{E}}(p) = p^2 - 3p - 1 + p \sum_{x=0}^{p-1} \left(\frac{-cx(x+b)(bx-c)}{p} \right)$$

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

Theorem [MMRW'14]: Families with a Large Error

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

$$A_{2,\mathcal{E}}(p) = p^2 - 3p - 1 + p\sum_{x=0}^{p-1}\left(\frac{-cx(x+b)(bx-c)}{p}\right)$$

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

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

Theorem [MMRW'14]: Families with a Large Error

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

$$A_{2,\mathcal{E}}(p) = p^2 - 3p - 1 + p \sum_{x=0}^{p-1} \left(\frac{-cx(x+b)(bx-c)}{p} \right)$$

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

General Structure of the Lower Order Terms

The lower order terms in the second moment expansions appear to always...

General Structure of the Lower Order Terms

The lower order terms in the second moment expansions appear to always...

- have no size $p^{3/2}$ term or a size $p^{3/2}$ term that is on average 0;

General Structure of the Lower Order Terms

The lower order terms in the second moment expansions appear to always...

- have no size $p^{3/2}$ term or a size $p^{3/2}$ term that is on average 0;
- exhibit their negative bias in the size p term;

General Structure of the Lower Order Terms

The lower order terms in the second moment expansions appear to always...

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

Table of Contents

Largest Error Term

In general, determining the lower order terms of $A_{2,\mathcal{E}}$ is intractable.

Largest Error Term

In general, determining the lower order terms of $A_{2,\mathcal{E}}$ is intractable.

- Possible approach: numerically measure the average value of the lower-order terms by averaging

$$\frac{A_{2,\mathcal{E}}(p) - p^2}{p^{3/2}} \quad \text{or} \quad \frac{A_{2,\mathcal{E}}(p) - p^2}{p}$$

over large ranges of primes.

Largest Error Term

In general, determining the lower order terms of $A_{2,\mathcal{E}}$ is intractable.

- Possible approach: numerically measure the average value of the lower-order terms by averaging

$$\frac{A_{2,\mathcal{E}}(p) - p^2}{p^{3/2}} \quad \text{or} \quad \frac{A_{2,\mathcal{E}}(p) - p^2}{p}$$

  over large ranges of primes.
- Problem: the $p^{3/2}$ normalization averages to 0; the p normalization does not appear to converge.

Higher Genus Sato-Tate

- We believe that when Michel's estimate is sharp, the size $p^{3/2}$ term is given by Fourier coefficients of some L-function.

Higher Genus Sato-Tate

- We believe that when Michel's estimate is sharp, the size $p^{3/2}$ term is given by Fourier coefficients of some L-function.
- A generalized Sato-Tate conjecture due to Sutherland predicts the limiting distributions of hyperelliptic curve coefficients.

Higher Genus Sato-Tate

- We believe that when Michel's estimate is sharp, the size $p^{3/2}$ term is given by Fourier coefficients of some L-function.
- A generalized Sato-Tate conjecture due to Sutherland predicts the limiting distributions of hyperelliptic curve coefficients.
- We can compute an approximate distribution for $\frac{A_{2,\mathcal{E}}(p)-p^2}{p^{3/2}}$ and compare it with the Fourier coefficient distribution of some hyperelliptic curve.

Distribution of Error Terms: Example 1

Denote $c_{3/2}(p) = \frac{A_{2,\mathcal{E}}(p) - p^2}{p^{3/2}}$. Consider the family

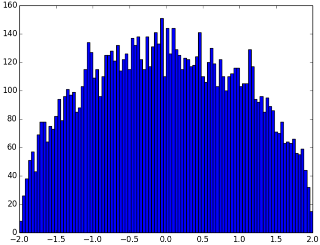
$$\mathcal{E} : y^2 = 4x^3 + 5x^2 + (4T - 2)x + 1$$

Distribution of Error Terms: Example 1

Denote $c_{3/2}(p) = \frac{A_{2,\mathcal{E}}(p) - p^2}{p^{3/2}}$. Consider the family

$$\mathcal{E} : y^2 = 4x^3 + 5x^2 + (4T - 2)x + 1$$

Figure: Distribution of $c_{3/2}(p)$ over the first 10000 primes



Approx. moments: 1, 0, 1, 0, 2, 0, 5, 0, 14, ...
Hyperelliptic curve: $y^2 = x^3 + x + 1$

Distribution of Error Terms: Example 2

Denote $c_{3/2}(p) = \frac{A_{2,\mathcal{E}}(p) - p^2}{p^{3/2}}$. Consider the family

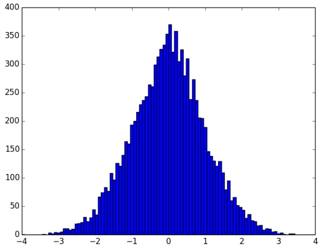
$$\mathcal{E} : y^2 = 4x^3 + (4T + 1)x^2 + (-4T - 18)x + 49$$

Distribution of Error Terms: Example 2

Denote $c_{3/2}(p) = \frac{A_{2,\mathcal{E}}(p) - p^2}{p^{3/2}}$. Consider the family

$$\mathcal{E} : y^2 = 4x^3 + (4T+1)x^2 + (-4T-18)x + 49$$

Figure: Distribution of $c_{3/2}(p)$ over the first 10000 primes



Approx. moments: 1, 0, 1, 0, 3, 0, 14, 0, 84, ...
Hyperelliptic curve: $y^2 = x^5 - x + 1$

Distribution of Error Terms: Example 3

Denote $c_{3/2}(p) = \frac{A_{2,\mathcal{E}}(p) - p^2}{p^{3/2}}$. Consider the family

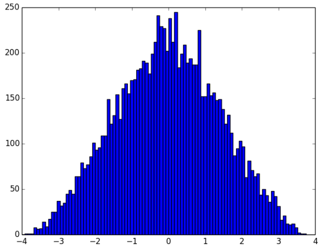
$$\mathcal{E} : y^2 = x^3 + 2x^3 - 4T^2x + T^2$$

Distribution of Error Terms: Example 3

Denote $c_{3/2}(p) = \frac{A_{2,\mathcal{E}}(p) - p^2}{p^{3/2}}$. Consider the family

$$\mathcal{E} : y^2 = x^3 + 2x^3 - 4T^2x + T^2$$

Figure: Distribution of $c_{3/2}(p)$ over the first 10000 primes



Approx. moments: 1, 0, 2, 0, 6, 0, 10, 0, 70, ...
Hyperelliptic curve: $y^2 = x^6 + x^2 + 1$

Summary of Error Term Investigations

- Larger error terms that average to 0 prevent us from numerically measuring average biases that arise in the size p terms.

Summary of Error Term Investigations

- Larger error terms that average to 0 prevent us from numerically measuring average biases that arise in the size p terms.
- In every case we studied, the size $p^{3/2}$ error term appeared to be governed by (hyper)elliptic curve coefficients.

Summary of Error Term Investigations

- Larger error terms that average to 0 prevent us from numerically measuring average biases that arise in the size p terms.
- In every case we studied, the size $p^{3/2}$ error term appeared to be governed by (hyper)elliptic curve coefficients.
- We do not have a general way of identifying the hyperelliptic curve coefficient associated to the error term of a given family.

Table of Contents

Questions for Further Study

- Does the Bias Conjecture hold similarly for all higher even moments?

Questions for Further Study

- Does the Bias Conjecture hold similarly for all higher even moments?
- What other (families of) objects obey the Bias Conjecture? Kloosterman sums? Cusp forms of a given weight and level? Higher genus curves?

Questions for Further Study

- Does the Bias Conjecture hold similarly for all higher even moments?
- What other (families of) objects obey the Bias Conjecture? Kloosterman sums? Cusp forms of a given weight and level? Higher genus curves?
- How does the second moment bias relate to other properties of the family?

Acknowledgments

We would like to thank

- Professor Miller and Dr Caroline Turnage-Butterbaugh
- SMALL REU 2014
- Williams College
- University of Michigan Computing Resources
- NSF Grant DMS-1347804 and NSF Grant DMS-1265673 .

Bibliography

- P. Michel, Average rank of families of elliptic curves and Sato-Tate laws, Monatshefte fur Mathematik, vol. 120, num. 2, p. 127-136, 1995.
- S. Fermigier. Etude experimentale du rang de familles de courbes elliptiques sur **Q**. Experimental Mathematics 5 (1996), no. 2, 119–130.
- S. Miller, 1 and 2 Level Density Functions for Families of Elliptic Curves: Evidence for the Underlying Group Symmetries, Compositio Mathematica 140 (2004), no.4, 952-992.