Biases in Fourier Coefficients of Elliptic Curve L-functions.

Steven J. Miller (Williams College)
sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu
With Megumi Asada, Eva Fourakis, Andrew Kwon, Blake Mackall, Karl Winsor and Kevin Yang
http://web.williams.edu/Mathematics/sjmiller/public_html/

AMS Special Session on Analytic Number Theory and Automorphic Forms
Washington State University, April 23, 2017

Bias Conjecture for Elliptic Curves

Last Summer: 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* of the Fourier coefficients is

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

Tate's Conjecture

Tate's Conjecture for Elliptic Surfaces

Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E}, s)$ be the L-series attached to $H^2_{\text{ét}}(\mathcal{E}/\overline{\mathbb{Q}}, \mathbb{Q}_l)$. Then $L_2(\mathcal{E}, s)$ has a meromorphic continuation to $\mathbb{C}$ and satisfies

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

where $NS(\mathcal{E}/\mathbb{Q})$ is the $\mathbb{Q}$-rational part of the Néron-Severi group of $\mathcal{E}$. Further, $L_2(\mathcal{E}, s)$ does not vanish on the line $\mathrm{Re}(s) = 2$.

Tate's conjecture is known for rational surfaces: An elliptic surface $y^2 = x^3 + A(T)x + B(T)$ is rational iff one of the following is true:

- $0 < \max\{3\deg A, 2\deg B\} < 12$;
- $3\deg A = 2\deg B = 12$ and $\mathrm{ord}_{T=0} T^{12}\Delta(T^{-1}) = 0$.

Negative Bias in the First Moment

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

If Tate's Conjecture holds for $\mathcal{E}$ then

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

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

Bias Conjecture

Second Moment Asymptotic (Michel)

For families $\mathcal{E}$ with $j(T)$ non-constant, the second moment is

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

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

Bias Conjecture

Second Moment Asymptotic (Michel)

For families $\mathcal{E}$ with $j(T)$ non-constant, the second moment is

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

- 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**.

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.

Lower order terms and average rank

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

- $\phi(x) \geq 0$ gives upper bound average rank.
- Expect big-Oh term $\Omega(1/\log R)$.

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.

Methods for Obtaining Explicit Formulas

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

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

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

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

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

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 $\mathcal{E} : y^2 = x^3 + ax^2 + bx + cT + d$,

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

- 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 $\mathcal{E} : y^2 = x^3 + aT^2x + bT^2$,

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

- 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 Rank

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

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

- The average bias in the size p term is -2.
- The family has an usual 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
$\mathcal{E} : y^2 = x^3 + (T + a)x^2 + (bT + b^2 - ab + c)x - bc$,

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

- 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 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 congruence classes of p (i.e., values of Legendre symbols).

Numerical Investigations

Numerical Methods

- As complexity of coefficients increases, it is much harder to find an explicit formula.
- We can always just calculate the second moment from the explicit formula; if $\mathcal{E}\colon y^2 = f(x)$, we have

$$A_{2,\mathcal{E}}(p) \;=\; \sum_{t(p)} \left(\sum_{x(p)} \left(\frac{f(x)}{p} \right) \right)^2 .$$

- Takes an hour for the first 500 primes. Optimizations?

Numerical Methods

Consider the family $y^2 = f(x) = ax^3 + (bT + c)x^2 + (dT + e)x + f$. By similar arguments used to prove special cases,

$$A_{2,\mathcal{E}}(p) \ = \ p^2 - 2p + pC_0(p) - pC_1(p) - 1 + \#_1,$$

where

$$C_0(p) \ = \ \sum_{x(p)} \sum_{y(p):\ \beta(x,y)\equiv 0} \left(\frac{A(x)A(y)}{p}\right),$$

$$C_1(p) \ = \ \sum_{x(p):\ \beta(x,x)\equiv 0} \left(\frac{A(x)^2}{p}\right),$$

$$\#_1 \ = \ p \sum_{x(p)} \sum_{y(p):\ A(x)\equiv 0 \ and \ A(y)\equiv 0} \left(\frac{B(x)B(y)}{p}\right),$$

and β, A, and B are polynomials.

Numerical Methods

- $C_o(p)$ ordinarily $O(p^2)$ to compute.
- Sum over zeros of $\beta(x, y) \mod p$
- Fixing an x, β is a quadratic in y. So, with the quadratic formula mod p, we know where to look for y to see if there is a zero.
- Now $O(p)$; runs from 6000^{th} to 7000^{th} prime in an hour.

Potential Counterexamples

Families of Rank as Large as 3

$\mathcal{E} : y^2 = x^3 + ax^2 + bT^2x + cT^2$ with $b, c \neq 0$:

$$\begin{aligned} A_{2,\mathcal{E}}(p) \;=\; & p^2 + p \sum_{P(x,y)\equiv 0} \left(\frac{(x^3+bx)(y^3+by)}{p} \right) \\ & + p \left[\sum_{x^3+bx\equiv 0} \left(\frac{ax^2+c}{p} \right) \right]^2 - p \sum_{P(x,x)\equiv 0} \left(\frac{x^3+bx}{p} \right)^2 \\ & - p \left(2 + \left(\frac{-b}{p} \right) \right) - \left[\sum_{x \bmod p} \left(\frac{x^3+bx}{p} \right) \right]^2 - 1 \end{aligned}$$

where $P(x,y) = bx^2y^2 + c(x^2+xy+y^2) + bc(x+y)$.

A Positive Size p Term?

$p\left[\sum_{x^3+bx\equiv 0}\left(\frac{ax^2+c}{p}\right)\right]^2$ can be $+9p$ on average!

- Terms such as $-p\sum_{P(x,x)\equiv 0}\left(\frac{x^3+bx}{p}\right)^2$, $-p\left(2+\left(\frac{-b}{p}\right)\right)$, and $-\left[\sum_{x \bmod p}\left(\frac{x^3+bx}{p}\right)\right]^2$ contribute negatively to the size p bias.

- The term $p\sum_{P(x,y)\equiv 0}\left(\frac{(x^3+bx)(y^3+by)}{p}\right)$ is of size $p^{3/2}$.

$$\begin{aligned} A_{2,\mathcal{E}}(p) \;=\; & p^2 + p\sum_{P(x,y)\equiv 0}\left(\frac{(x^3+bx)(y^3+by)}{p}\right) + p\left[\sum_{x^3+bx\equiv 0}\left(\frac{ax^2+c}{p}\right)\right]^2 \\ & - p\sum_{P(x,x)\equiv 0}\left(\frac{x^3+bx}{p}\right)^2 - p\left(2+\left(\frac{-b}{p}\right)\right) - \left[\sum_{x \bmod p}\left(\frac{x^3+bx}{p}\right)\right]^2 - 1 \end{aligned}$$

where $P(x,y) = bx^2y^2 + c(x^2+xy+y^2) + bc(x+y)$.

Analyzing the Size $p^{3/2}$ Term

We averaged $\sum_{P(x,y)\equiv 0}\left(\frac{(x^3+bx)(y^3+by)}{p}\right)$ over the first 10,000 primes for several rank 3 families of the form $\mathcal{E}: y^2 = x^3 + ax^2 + bT^2x + cT^2$.

Family	Average
$y^2 = x^3 + 2x^2 - 4T^2x + T^2$	-0.0238
$y^2 = x^3 - 3x^2 - T^2x + 4T^2$	-0.0357
$y^2 = x^3 + 4x^2 - 4T^2x + 9T^2$	-0.0332
$y^2 = x^3 + 5x^2 - 9T^2x + 4T^2$	-0.0413
$y^2 = x^3 - 5x^2 - T^2x + 9T^2$	-0.0330
$y^2 = x^3 + 7x^2 - 9T^2x + T^2$	-0.0311

The Right Object to Study

$c_{3/2}(p) := \sum_{P(x,y)\equiv 0}\left(\frac{(x^3+bx)(y^3+by)}{p}\right)$ is not a natural object to study (for us multiply by p).

An example distribution for $y^2 = x^3 + 2x^3 - 4T^2x + T^2$.

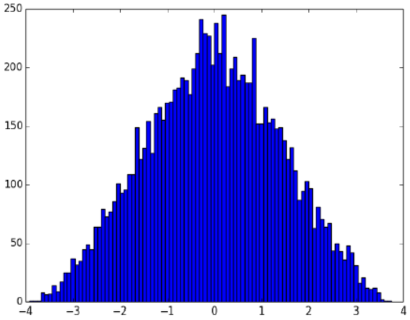

Figure: $c_{3/2}(p)$ over the first 10,000 primes.

In Terms of Elliptic Curve Coefficients

Compare it to the distribution of a sum of 2 elliptic curve coefficients.

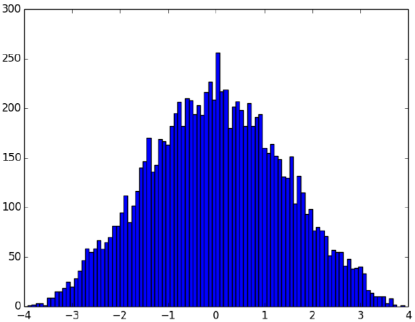

Figure: $-\sum_{x \mod p} \left(\frac{x^3+x+1}{p}\right) - \sum_{x \mod p} \left(\frac{x^3+x+2}{p}\right)$ over the first 10,000 primes.

More Error Distributions

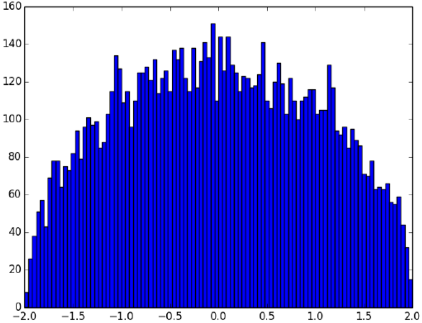

Figure: $c_{3/2}(p)$ for $y^2 = 4x^3 + 5x^2 + (4T - 2)x + 1$, first 10,000 primes.

More Error Distributions

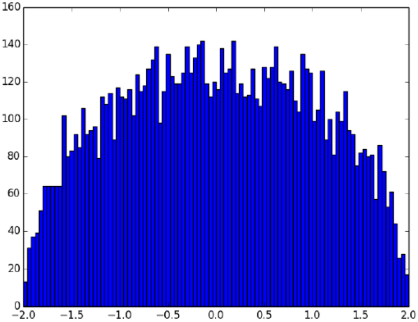

Figure: $-\sum_{x \bmod p} \left(\frac{x^3+x+1}{p}\right)$ distribution, first 10,000 primes.

More Error Distributions

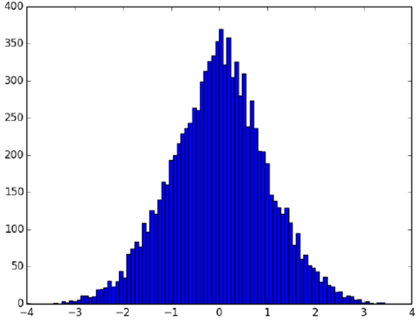

Figure: $c_{3/2}(p)$ over $y^2 = 4x^3 + (4T+1)x^2 + (-4T-18)x + 49$, first 10,000 primes.

More Error Distributions

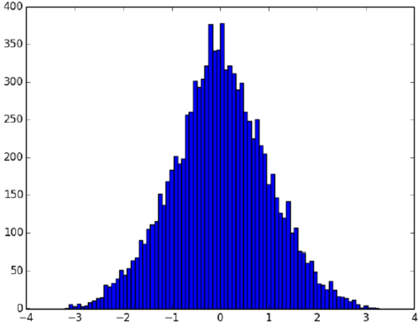

Figure: $-\sum_{x \bmod p} \left(\frac{x^5+x^3+x^2+x+1}{p}\right)$ distribution, first 10,000 primes.

Summary of $p^{3/2}$ Term Investigations

In the cases we've studied, the size $p^{3/2}$ terms

- appear to be governed by (hyper)elliptic curve coefficients;
- may be hiding negative contributions of size p;
- prevent us from numerically measuring average biases that arise in the size p terms.

Future Directions

Questions for Further Study

- Are the size $p^{3/2}$ terms governed by (hyper)elliptic curve coefficients? Or at least other L-function coefficients?
- Does the average bias always occur in the terms of size p?
- 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?

References

References

Biases:

- 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.

- *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.

- *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.

- *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.

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

Funded by NSF Grants DMS1265673, DMS1347804 and Williams College.

Thank you!