LOWER-ORDER BIASES IN ELLIPTIC CURVE FOURIER COEFFICIENTS IN FAMILIES

BLAKE MACKALL, STEVEN J. MILLER, CHRISTINA RAPTI, AND KARL WINSOR

ABSTRACT. Let $\mathcal{E} : y^2 = x^3+A(T)x+B(T)$ be a nontrivial one-parameter family of elliptic curves over $\mathbb{Q}(T)$, with $A(T), B(T) \in \mathbb{Z}(T)$, and consider the k^{th} moments $A_{k,\mathcal{E}}(p) := \sum_{t \bmod p} a_{\mathcal{E}_t}(p)^k$ of the Fourier coefficients $a_{\mathcal{E}_t}(p) := p + 1 - |\mathcal{E}_t(\mathbb{F}_p)|$. Rosen and Silverman proved a conjecture of Nagao relating the first moment $A_{1,\mathcal{E}}(p)$ to the rank of the family over $\mathbb{Q}(T)$, and Michel proved that the second moment is equal to $A_{2,\mathcal{E}}(p) = p^2 + O\left(p^{3/2}\right)$. Cohomological arguments show that the lower order terms are of sizes $p^{3/2}$, p, $p^{1/2}$, and 1. In every case we are able to analyze, the largest lower order term in the second moment expansion that does not average to zero is on average negative. We prove this "bias conjecture" for several large classes of families, including families with rank, complex multiplication, and unusual distributions of functional equation signs. We also identify all lower order terms in large classes of families, shedding light on the arithmetic objects controlling these terms. The negative bias in these lower order terms has implications toward the excess rank conjecture and the behavior of zeros near the central point of elliptic curve L-functions.

CONTENTS

Date: October 2, 2014.

2010 *Mathematics Subject Classification.* 11G05 (primary), 11G07, 11G40, 11M41 (secondary).

Key words and phrases. Elliptic curves, lower order terms, Sato-Tate law, Fourier coefficients, excess rank, 1-level density, Katz-Sarnak Density Conjecture.

This research was supported by NSF grants DMS1265673 and DMS1347804 and Williams College. Many of the computations were performed on computer clusters at the University of Michigan. This paper is a continuation (at the 2014 SMALL REU at Williams College) of a talk given by the second named author at the workshop on Frobenius distributions of curves at CIRM in February 2014; it is our pleasure to thank the participants there and several of our colleagues, especially , for many helpful conversations.

1. INTRODUCTION

We report on some recent theoretical and experimental results concerning lower order terms in the second moments of Fourier coefficients in families of elliptic curve L-functions, especially one-parameter families over $\mathbb{Q}(T)$. In every family studied we have found that the first lower order term which does not average to zero either has a provable negative average or behaves consistent with such a conclusion; in many cases we are able to derive an explicit formula for these values. We conjecture that this is a universal phenomenon, and all such families exhibit such a bias.

We first quickly review some needed results on elliptic curves and previous results in the field, and then summarize our findings. We end with some avenues of current and future research. The goal of this note is to clearly state our bias conjectures and provide complete calculations in several cases to support it; for additional results along these lines see the sequel paper [MMRW14].

1.1. Preliminaries and Previous Work.

We assume the reader is familiar with the basics of elliptic curves and L-functions; good references include [IK04, Kn92, Si86, ST92]. Given an elliptic curve E over $\mathbb{Q}$, we may write it as

$$y^2 \;=\; x^3 + ax + b, \tag{1.1}$$

with a and b integers. We set

$$a_E(p) \;=\; p - \#\{(x,y) \in \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} : y^2 \equiv x^3 + ax + b \bmod p\} \;=\; -\sum_{x \bmod p} \left(\frac{x^3+ax+b}{p}\right), \tag{1.2}$$

with $\left(\frac{n}{p}\right)$ the Legendre symbol (it is 1 if n is a non-zero square modulo p, 0 if n is zero modulo p, and -1 otherwise). By Hasse's theorem $|a_E(p)| \le 2\sqrt{p}$, and is the difference between how many solutions modulo p we expect on average, and how many we actually have. We call these the Fourier coefficients of the elliptic curve, and they are used in the series expansion for the associated L-function.

A common theme in many problems in number theory is to consider families of objects (for example, the proof of the infinitude of primes in arithmetic progression looks at a family of Dirichlet L-functions), and thus we consider families of elliptic curves. Most of our examples will be one-parameter families, where

$$\mathcal{E} : y^2 \;=\; x^3 + A(T)x + B(T), \quad A(T), B(T) \in \mathbb{Z}[T]. \tag{1.3}$$

For all but finitely many specializations of T to an integer t we obtain an elliptic curve E_t with coefficient $a_{E_t}(p)$ (though for brevity we often write $a_{\mathcal{E}_t}(p)$).

A lot is known about the distribution of the $a_E(p)$'s and the moments of the $a_{\mathcal{E}_t}(p)$'s, where we set

$$A_{r,\mathcal{E}}(p) \;:=\; \sum_{t \bmod p} a_{\mathcal{E}_t}(p)^r; \tag{1.4}$$

note we are not normalizing this sum by dividing by p (the number of elements in the family), and thus we expect it to be on the order of $p^{r/2+1}$.

First, if E is a fixed elliptic curve without complex multiplication then the normalized coefficients $a_E(p)/2\sqrt{p}$ converge to the Sato-Tate distribution;[1] see [B-LGHT11, CHT08, HS-BT10, T08]. Second, at least conjecturally the first moment $A_{1,\mathcal{E}}(p)$ is related to the rank of the elliptic

[1] If E has complex multiplication then writing $\cos\theta_{E,p} = a_E(p)/2\sqrt{p}$ one has the angles vanish for half the primes, and are equidistributed for the remaining.

surface $\mathcal{E}/\mathbb{Q}$. Specifically, Rosen and Silverman [RS98] prove a conjecture of Nagao, which says that if Tate's conjecture holds then

$$\lim_{X\to\infty} -\frac{1}{X}\sum_{p\le X}\frac{A_{1,\mathcal{E}}(p)\log p}{p} \;\to\; \text{rank}\,\mathcal{E}(\mathbb{Q}(T)); \tag{1.5}$$

Tate's conjecture is known for rational elliptic surfaces. Their result tells us that there is a negative bias in the coefficients $a_{\mathcal{E}_t}(p)$, and the larger the rank of the family the greater the average bias.

The purpose of this work is to explore the second moments $A_{2,\mathcal{E}}(p)$. Our goal is to see if there is a similar bias here and, if so, what are the consequences. One important application is to the behavior of the low-lying zeros (the zeros of the associated L-functions near the central point). The Katz-Sarnak Density Conjectures [KS99a, KS99b] state that the behavior of these zeros, in the scaling limit as the conductors tends to infinity, agree with the scaling limit of eigenvalues near 1 of a corresponding classical compact group; see [ILS00, AAILMZ15] for a review of the theory of low-lying zeros in general, and the 1-level density statistic in particular. In previous work Miller and his colleagues (see [Mi05, Mi09]) interpreted lower order corrections to moments of these Fourier coefficients as controlling the rate of convergence of the low-lying zeros to the random matrix theory predictions. For example, in [Mi09] the first lower order correction term is isolated in the 1-level density of several GL_2 families of L-functions; it is always negative, and in [Mi05] it is related to the observed excess rank in families of elliptic curves with finite conductors[2].

1.2. **The Bias Conjecture.** An asymptotic result for the second moments of elliptic curve Fourier coefficients is given by Michel.

Theorem 1.1 (Michel [Mic95])**.** *For a one-parameter family $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$ with non-constant $j(T)$-invariant $j(T) = 1728\frac{4A(T)^3}{4A(T)^3+27B(T)^2}$, the second moment of the Fourier coefficients is given by*

$$A_{2,\mathcal{E}}(p) \;=\; p^2 + O(p^{3/2}). \tag{1.6}$$

The error term in Michel's theorem cannot be improved, as there are families where there is a lower order term of size $p^{3/2}$; see [Mi02, Mi05]

We have observed an interesting phenomenon in the lower order terms of the second moments of these Fourier coefficients. In every family we have studied, the following conjecture holds.

Conjecture 1.2 (Bias Conjecture)**.** *Let $\mathcal{E}$ be a one-parameter family of elliptic curves over $\mathbb{Q}(T)$. The largest lower order term in the second moment expansion of $A_{2,\mathcal{E}}$ that does not average to 0 is on average negative.*

The negative bias in the first moments of elliptic curve Fourier coefficients is related to their rank (see equation (1.5)). We will use this result to study families of varying rank to see if the bias we have observed in the second moments is also related to the family rank.

Instead of investigating one-parameter families we could examine two-parameter families. The larger cardinality of the family leads to significantly easier averaging, and the average second moment for the family of all elliptic curves was computed by Birch [Bi68].[3]

[2]Though the amount of excess rank it can explain is quite small.

[3]There were some typos in the manuscript; see [MM11] for corrected statements.

Theorem 1.3 (Birch)**.** *For the family $\mathcal{F} : y^2 = x^3 + ax + b$ ($a, b \in \mathbb{Z}$) of all elliptic curves, the second moment of the Fourier coefficients is equal to*

$$A_{2,\mathcal{F}} \;=\; \sum_{a,b \bmod p} a_{\mathcal{F}_{a,b}}(p) \;=\; p^3 - p^2. \tag{1.7}$$

We may thus view our Bias Conjecture as a refinement of Birch's result for one-parameter families. Below we report on some theoretical and experimental results supporting our conjecture. Unfortunately many of the families studied are special, either because we have carefully chosen the defining polynomials to ensure certain properties hold, or their degrees are small. However, while it is possible that these are painting a false impression of the true behavior, it is encouraging that to date all families studied support our conjecture.

2. Tools for Calculating Biases

We quickly gather several useful lemmas for calculating biases in elliptic curve families. Throughout this paper, $\left(\frac{\cdot}{p}\right)$ denotes a Legendre symbol, and $\sum_{x(p)}$ denotes a sum over all residue classes modulo p. Linear sums and quadratic sums of Legendre symbols can be easily evaluated (see for example [BEW98]).

Lemma 2.1. *Let a, b, c be positive integers, and assume $a \neq 0$. For $p \nmid a$,*

$$\sum_{x(p)} \left(\frac{ax+b}{p}\right) \;=\; 0 \tag{2.1}$$

and

$$\sum_{x(p)} \left(\frac{ax^2+bx+c}{p}\right) \;=\; \begin{cases} -\left(\frac{a}{p}\right) & \text{if } p \nmid b^2 - 4ac \\ (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid b^2 - 4ac. \end{cases} \tag{2.2}$$

We often use an averaging result for Legendre symbols.

Lemma 2.2. *Let $\pi(X)$ be the number of primes $p \leq X$, and fix $x \in \mathbb{Z}$. Then*

$$\lim_{X\to\infty} \frac{1}{\pi(X)} \sum_{p \leq X} \left(\frac{x}{p}\right) \;=\; \begin{cases} 1 & \text{if } x \in \mathbb{Z} \text{ is a non-zero square} \\ 0 & \text{otherwise.} \end{cases} \tag{2.3}$$

Proof. The proof is immediate from Dirichlet's theorem on primes in arithmetic progressions, as the number of residue classes modulo p that are non-zero squares equals the number that are not square. □

To compute the rank of the families we analyze, we use the following consequence of Rosen and Silverman's work. A key input is Tate's conjecture, alluded to earlier.

Conjecture 2.3 (Tate's Conjecture for Elliptic Surfaces [Ta65])**.** *Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E}, s)$ be the L-series attached to $H^2_{\mathrm{t}}(\mathcal{E}/\overline{\mathbb{Q}}, \mathbb{Q}_l)$. 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 if $\mathcal{E}$ is a rational surface. An elliptic surface $y^2 = x^3 + A(T)x + B(T)$ is rational iff one of the following is true: (1) $0 < \max\{3 \deg A, 2 \deg B\} < 12$; (2) $3 \deg A = 2 \deg B = 12$ and $\mathrm{ord}_{T=0} T^{12} \Delta(T^{-1}) = 0$. See pages 46–47 of [RS98] for more details.

Lemma 2.4. *If $\mathcal{E}$ is a one-parameter family with $A_{1,\mathcal{E}}(p) = -rp + O(1)$ and Tate's conjecture holds, then* $\mathrm{rank}(\mathcal{E}(\mathbb{Q}(T))) = r$.

Proof. This follows from the Prime Number Theorem applied to (1.5). □

Lemma 2.4 was used by Miller [Mi02] and Arms, Lozano-Robledo and Miller [AL-RM07] to construct one-parameter families of elliptic curves with moderate, prescribed rank. Interestingly, this method allows us to write down families of a given rank *without* computing the determinant of the height matrix associated to r points conjectured to be independent, though frequently one can extract the requisite number of candidate points for the height matrix from the calculations performed to determine $A_{1,\mathcal{E}}(p)$.

3. Proven Special Cases

3.1. **Preliminaries.** Most of our proven special cases are for families of the form

$$\mathcal{E} : y^2 \;=\; (aT+b)x^3 + (cT+d)x^2 + (eT+f)x + (gT+h), \tag{3.1}$$

that is, families where the T-polynomials are all linear. The technical advantage of studying these families is that the corresponding second moment expansions only involve quadratic polynomials in T, for which we can obtain clean explicit sum formulas. We begin by calculating the possible ranks of these families.

Lemma 3.1. *Consider a one-parameter family of elliptic curves of the form*

$$\mathcal{E} : y^2 \;=\; (aT+b)x^3 + (cT+d)x^2 + (eT+f)x + (gT+h), \tag{3.2}$$

where $a, \dots, h \in \mathbb{Z}$. The rank of this family is at most 3.

Proof. A simple change of variables converting $\mathcal{E}$ to Weierstrass form shows that it is a rational surface, and therefore we may use Lemma 2.4 to compute its rank. For primes $p > 3$, the first moment of the Fourier coefficients for this family is

$$\begin{aligned} A_{1,\mathcal{E}}(p) \;&=\; -\sum_{t(p)}\sum_{x(p)}\left(\frac{(at+b)x^3 + (ct+d)x^2 + (et+f)x + (gt+h)}{p}\right) \\ &=\; -\sum_{x(p)}\sum_{t(p)}\left(\frac{t(ax^3+cx^2+ex+g) + bx^3 + dx^2 + fx + h}{p}\right). \end{aligned} \tag{3.3}$$

By (2.1), the inner t-sum is 0 unless $ax^3 + cx^2 + ex + g \equiv 0$. We then have

$$A_{1,\mathcal{E}}(p) \;=\; -p \sum_{ax^3+cx^2+ex+g\equiv 0(p)} \left(\frac{bx^3+dx^2+fx+h}{p}\right) \;\geq\; -3p \tag{3.4}$$

since $ax^3 + cx^2 + ex + g$ has at most 3 roots in $\mathbb{F}_p$. By Lemma 2.4 we can now conclude the rank is at most 3. □

By choosing our coefficients so that $bx^3 + dx^2 + fx + h$ is a non-zero square in the integers when evaluated at the roots of $ax^3 + cx^2 + ex + g$, we can construct families of this form of ranks 0, 1, 2, and 3.

Next, we prove a structural lemma for the second moments of these families. The families of ranks 0, 1 and 2 studied by Fermigier [Fe96] are all included in this analysis (as are half of his families of rank 3 after a simple change of variables). As these families provided strong evidence

of excess rank, it is encouraging that these all satisfy our Bias Conjecture (and might even suggest a connection between our bias and excess rank).

Lemma 3.2. *Consider a one-parameter family of elliptic curves of the form*

$$\mathcal{E} : y^2 \;=\; (aT+b)x^3 + (cT+d)x^2 + (eT+f)x + (gT+h), \tag{3.5}$$

where $a, \dots, h \in \mathbb{Z}$. Let

$$P(x) \;:=\; ax^3 + cx^2 + ex + g, \quad Q(x) \;:=\; bx^3 + dx^2 + fx + h. \tag{3.6}$$

Then the second moment can be expanded as

$$A_{2,\mathcal{E}}(p) \;=\; p\left[\sum_{P(x)\equiv 0}\left(\frac{Q(x)}{p}\right)\right]^2 - \left[\sum_{x(p)}\left(\frac{P(x)}{p}\right)\right]^2 + p\sum_{\Delta(x,y)\equiv 0}\left(\frac{P(x)P(y)}{p}\right) \tag{3.7}$$

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

Proof. We can write the second moment as

$$\begin{aligned} A_{2,\mathcal{E}}(p) \;&=\; \sum_{t(p)}\left[\sum_{x(p)}\left(\frac{tP(x)+Q(x)}{p}\right)\right]^2 \\ &=\; \sum_{x(p)}\sum_{y(p)}\sum_{t(p)}\left(\frac{Q(x)Q(y) + t(P(x)Q(y)+P(y)Q(x)) + t^2P(x)P(y)}{p}\right). \end{aligned} \tag{3.8}$$

When $P(x), P(y) \neq 0$ we use (2.2) for quadratic Legendre sums, and when $P(x)$ or $P(y)$ are $\equiv 0$ we use (2.1) for linear Legendre sums. By inclusion-exclusion,

$$\begin{aligned} A_{2,\mathcal{E}}(p) \;=\; 2\sum_{P(x)\equiv 0}\sum_{y(p)}\sum_{t(p)}\left(\frac{Q(x)Q(y)+tP(y)Q(x)}{p}\right) - p\sum_{P(x)\equiv 0}\sum_{P(y)\equiv 0}\left(\frac{Q(x)Q(y)}{p}\right) \\ + \sum_{P(x)\neq 0}\sum_{P(y)\neq 0}\sum_{t(p)}\left(\frac{Q(x)Q(y) + t(P(x)Q(y)+P(y)Q(x)) + t^2P(x)P(y)}{p}\right) \end{aligned}$$

Then since

$$\begin{aligned} &2\sum_{P(x)\equiv 0}\sum_{y(p)}\sum_{t(p)}\left(\frac{Q(x)Q(y)+tP(y)Q(x)}{p}\right) \\ &=\; 2\sum_{P(x)\equiv 0}\left(\frac{Q(x)}{p}\right)\sum_{y(p)}\sum_{t(p)}\left(\frac{Q(y)+tP(y)}{p}\right) \\ &=\; 2p\sum_{P(x)\equiv 0}\sum_{P(y)\equiv 0}\left(\frac{Q(x)Q(y)}{p}\right), \end{aligned} \tag{3.9}$$

we can write

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

$$= \; p\left[\sum_{P(x)\equiv 0}\left(\frac{Q(x)}{p}\right)\right]^2 - \left[\sum_{x(p)}\left(\frac{P(x)}{p}\right)\right]^2 + p\sum_{\Delta(x,y)\equiv 0}\left(\frac{P(x)P(y)}{p}\right) \tag{3.10}$$

where

$$\Delta(x,y) \;=\; (P(x)Q(y) - P(y)Q(x))^2 \tag{3.11}$$

is the discriminant of the quadratic in t arising in (3.7). □

Lemma 3.2 removes any dependence of the second moment on sums over the t parameter. The leftmost term is a sum over at most 3 Legendre symbols, and the middle term is the square of a Legendre sum over a polynomial of at most degree 3, so averaging these terms over primes is tractable. The rightmost term is more complicated, and in general we are not able to explicitly analyze it. However, when the discriminant $\Delta(x,y)$ factors reasonably nicely, we can construct large classes of one-parameter families where all calculations can be explicitly done. Expanding out $P(x)$ and $Q(x)$, we find that

$$\Delta(x,y) \;=\; ((x-y)R(x,y))^2 \tag{3.12}$$

where

$$\begin{aligned} R(x,y) \;\;=\;\; & (ad-bc)x^2y^2 + (af-be)(x^2y+xy^2) + (ah-bg)(x^2+xy+y^2) \\ & + (cf-de)xy + (ch-dg)(x+y) + eh - fg. \end{aligned} \tag{3.13}$$

We can now prove a variety of special cases of the Bias Conjecture.

Lemma 3.3. *Fix integers b, d and f with $b \neq 0$, and a prime $p > 3$. The one-parameter family $\mathcal{E} : y^2 = bx^3 + dx^2 + fx + T$ has rank 0 over $\mathbb{Q}(T)$, and for $p \nmid b$ its second moment expansion is*

$$A_{2,\mathcal{E}}(p) \;=\; p^2 - p\left(1 - \left(\frac{-3}{p}\right) + \left(\frac{d^2-3bf}{p}\right)\right). \tag{3.14}$$

Proof. By Lemma 3.1, the first moment of the Fourier coefficients over this family is

$$A_{1,\mathcal{E}}(p) \;=\; 0. \tag{3.15}$$

As $\mathcal{E}$ is a rational surface, the rank of the family over $\mathbb{Q}(T)$ is 0. Using Lemma 3.2, the discriminant of the quadratic in t is

$$\Delta(x,y) \;=\; ((x-y)(b(x^2+xy+y^2)+d(x+y)+f))^2, \tag{3.16}$$

and thus the second moment can be expanded as

$$\begin{aligned} A_{2,\mathcal{E}}(p) \;&=\; -\left[\sum_{x(p)}\left(\frac{1}{p}\right)\right]^2 + p\sum_{\Delta(x,y)\equiv 0}\left(\frac{1}{p}\right) \\ &=\; -p^2 + p\sum_{x\equiv y(p)} 1 + p\sum_{x(p)}\sum_{y:by^2+(bx+d)y+(bx^2+dx+f)\equiv 0} 1 - p\sum_{3bx^2+2dx+f\equiv 0} 1. \end{aligned} \tag{3.17}$$

Note that the number of roots to a quadratic congruence $Ax^2+Bx+C \equiv 0(p)$ is equal to $1+\left(\frac{D}{p}\right)$, where $D = B^2 - 4AC$ is the discriminant of the quadratic. From this, we have

$$\begin{aligned} A_{2,\mathcal{E}}(p) &= p\sum_{x(p)}\left(1+\left(\frac{(bx+d)^2-4b(bx^2+dx+f)}{p}\right)\right) - p\left(1+\left(\frac{4d^2-12bf}{p}\right)\right) \\ &= p^2 - p\left(1+\left(\frac{d^2-3bf}{p}\right)\right) + p\sum_{x(p)}\left(\frac{-3b^2x^2-2bdx+d^2-4bf}{p}\right). \end{aligned} \tag{3.18}$$

By assumption, $p \nmid b$ and $p > 3$, so $p \nmid -3b^2$ and the rightmost sum is equal to $-\left(\frac{-3b^2}{p}\right) = \left(\frac{-3}{p}\right)$. Thus

$$A_{2,\mathcal{E}}(p) = p^2 - p\left(1-\left(\frac{-3}{p}\right)+\left(\frac{d^2-3bf}{p}\right)\right). \tag{3.19}$$

□

As an aside, the choice of family in Lemma 3.3 is just as general as the form $\mathcal{E} : y^2 = bx^3 + dx^2 + fx + gT + h$ for primes $p \nmid g$, since the maps $t \to t$ and $t \to gt + h$ are both bijections on the set of residue classes modulo p. We can go further and quantify the average bias in these families with the following definition.

Definition 3.4. *Let $C(p)$ denote the sum of the terms of order p in the expansion of the second moment $A_{2,\mathcal{E}}(p)$. The* average bias of size p *in the second moment is defined as*

$$\lim_{X\to\infty}\frac{1}{\pi(X)}\sum_{p\le X}\frac{C(p)}{p}, \tag{3.20}$$

when this limit exists.

For example, in (3.14), $C(p) = -p\left(1-\left(\frac{-3}{p}\right)+\left(\frac{d^2-3bf}{p}\right)\right)$.

3.2. **Rank 0 Families.**

Theorem 3.5 (Proof of the Bias Conjecture for the Rank 0 Family from Lemma 3.3)**.** *Fix integers b, d and f with $b \neq 0$. The one-parameter family $\mathcal{E} : y^2 = bx^3 + dx^2 + fx + T$ satisfies the Bias Conjecture, with an explicitly computable bias (in terms of b, d and f), giving a lower order term on average of size $-\alpha p$ for some $\alpha = \alpha(b, d, f) \in [1, 2]$.*

Proof. The average bias in the families (see in Lemma 3.3) is

$$\lim_{X\to\infty}\frac{1}{\pi(X)}\sum_{p\le X}\left(-1+\left(\frac{-3}{p}\right)-\left(\frac{d^2-3bf}{p}\right)\right). \tag{3.21}$$

By Lemma 2.4, the limit in (3.21) is equal to -2 or -1, according to whether or not $d^2 - 3bf$ is a non-zero square in $\mathbb{Z}$ (note the term $\pi(X)^{-1}\sum_{p\le X}\left(\frac{-3}{p}\right)$ averages to zero). □

We thus have a large class of rank 0 families proven to obey the Bias Conjecture. The natural next step is to construct a class of families with positive rank satisfying the Bias Conjecture.

3.3. **Rank 0 and Rank 1 Families.**

Theorem 3.6 (Proof of the Bias Conjecture for some Rank 0 and Rank 1 Families)**.** *A one-parameter family $\mathcal{E} : y^2 = x^3 + Tx^2 + etx + e^3$ has rank 0 or 1 over $\mathbb{Q}(T)$ and second moment expansion*

$$A_{2,\mathcal{E}}(p) \;=\; p^2 - p\left(2 + \left(\frac{-1}{p}\right)\right) - 1 \tag{3.22}$$

for $p \nmid e$. In particular, these curves show an average bias of -2. When e is a square in the integers, these families are of rank 1. Otherwise, they are of rank 0.

Proof. Assume all of the same notation from Lemma 3.1, with $a = 0$, $b = 1$, $c = 1$, $d = 0$, e free, $f = 0$, $g = 0$, and $h = e^3$. By the same steps as in Lemma 3.3, we can write

$$A_{2,\mathcal{E}} \;=\; p\left[\sum_{x=0,-e}\left(\frac{x^3+e^3}{p}\right)\right]^2 - \left[\sum_{x(p)}\left(\frac{x^2+ex}{p}\right)\right]^2 + p\sum_{\Delta(x,y)}\left(\frac{(x^2+ex)(y^2+ey)}{p}\right) \tag{3.23}$$

where

$$\Delta(x,y) \;=\; (x-y)(x+e)(y+e)(e^2-xy). \tag{3.24}$$

Since $e \neq 0$, by the quadratic Legendre sum formula (Lemma 2.1) and inclusion-exclusion,

$$\begin{aligned}
A_{2,\mathcal{E}} \;&=\; p - 1 + p\sum_{\Delta(x,y)}\left(\frac{(x^2+ex)(y^2+ey)}{p}\right) \\
&=\; p - 1 + p\sum_{x(p)}\left(\frac{x^2+ex}{p}\right)^2 + \\
&\quad p\sum_{(x+e)(y+e)(e^2-xy)\equiv 0}\left(\frac{(x^2+ex)(y^2+ey)}{p}\right) - p\sum_{(x+e)^2(e^2-x^2)\equiv 0}\left(\frac{x^2+ex}{p}\right)^2 \\
&=\; p - 1 + p(p-2) + p\sum_{R(x,y)\equiv 0}\left(\frac{P(x)P(y)}{p}\right) - p\sum_{R(x,x)\equiv 0}\left(\frac{P(x)^2}{p}\right).
\end{aligned} \tag{3.25}$$

We begin our analysis with the last term. Since $R(x,x)$ (defined in (3.13)) factors as $(e+x)^3(e-x)$, $R(x,x)$ is only zero when $x = e$ or $x = -e$. Note that these are mutually exclusive for $p > 2$. When $x = e$ we get $-p\left(\frac{(e^2+e^2)^2}{p}\right) = -p\left(\frac{4e^4}{p}\right) = -p$, while for $x = -e$ we have $-p\left(\frac{(e^2-e^2)^2}{p}\right) = 0$. Thus we are left with

$$A_{2,\mathcal{E}}(p) \;=\; p^2 - 2p - 1 + p\sum_{R(x,y)\equiv 0}\left(\frac{P(x)P(y)}{p}\right). \tag{3.26}$$

This family is constructed so that $R(x,y)$ factors into $(e+x)(e+y)(e^2-xy)$. Thus, using inclusion-exclusion and letting $S(f(x),p)$ denote the set of solutions of $f(x) \equiv 0 \pmod p$, $S(R(x,y),p)$ can be expressed as

$$\begin{aligned}
&S(e+x,p) + S(e+y,p) - (S(e+x,p) \cap S(e+y,p)) \\
&+ S(e^2-xy,p) - (S(e^2-xy,p) \cap S(e+x,p)) - (S(e^2-xy,p) \cap S(e+y,p)) \\
&+ (S(e^2-xy,p) \cap S(e+x,p) \cap S(e+y,p)).
\end{aligned}$$

To evaluate the double sum in (3.26), we can evaluate it over each of these x, y regions with the appropriate sign. As $P(-e) = 0$, we can omit the summation over all regions where $x = -e$ or $y = -e$ (and this includes regions with $x = -e$ or $y = -e$ as part of an intersection). The only region we are left with is $S(e^2 - xy, p)$. The sum over this region can be expressed as

$$\begin{aligned} \sum_{x(p),x\neq 0,y=e^2x^{-1}} \left(\frac{P(x)P(y)}{p}\right) &= \sum_{x(p),x\neq 0} \left(\frac{(x^2+ex)(e^4x^{-2}+e^3x^{-1})}{p}\right) \\ = \sum_{x(p),x\neq 0} \left(\frac{(x^2+ex)(e^2+ex)}{p}\right) &= \sum_{x(p),x\neq 0} \left(\frac{ex(x+e)^2}{p}\right) = \sum_{x(p)} \left(\frac{ex(x+e)^2}{p}\right). \end{aligned} \tag{3.27}$$

As $\left(\frac{(x+e)^2}{p}\right) = 1$ unless $x = -e$ in which case it is 0, we can rewrite the last sum in (3.27) as

$$\sum_{x(p)} \left(\frac{ex}{p}\right) - \left(\frac{-e^2}{p}\right) = -\left(\frac{-e^2}{p}\right) = -\left(\frac{-1}{p}\right). \tag{3.28}$$

Thus the contribution from this sum is $-p\left(\frac{-1}{p}\right)$, and the second moment formula is

$$A_{2,\mathcal{E}}(p) = p^2 - 2p - 1 - p\left(\frac{-1}{p}\right), \tag{3.29}$$

and this formula matches the one proposed. □

3.4. **Complex Multiplication Families.** We now turn to proving the Bias Conjecture for several families with complex multiplication. Note these families have constant $j(T)$-invariant of 0, so Theorem 1.1 by Michel does not apply. In particular, we will see that the term of size p^2 is not constant, but is on average p^2 (in a sense that can be made precise). Once we separate all of the size p^2 terms from the lower order terms, we find that a similar Bias Conjecture holds.

Theorem 3.7 (Proof of the Bias Conjecture for some CM-families)**.** *Fix an integer $b \neq 0$. For the CM-families of the form $\mathcal{E} : y^2 = bx^3 + T$ and $p \nmid b$,* $\mathrm{rank}(\mathcal{E}(\mathbb{Q}(T)) = 0$ *and*

$$A_{2,\mathcal{E}}(p) = \left(p^2 - p\right)\left(1 + \left(\frac{-3}{p}\right)\right). \tag{3.30}$$

As $\left(\frac{-3}{p}\right)$ averages to zero, these families have an average bias of -1.

Proof. For a family $\mathcal{E} : y^2 = bx^3 + T$, by Lemma 3.1, $A_{1,\mathcal{E}}(p) = 0$ and the family rank is 0. For $p \nmid b$, by Lemma 3.2 and inclusion-exclusion, the second moment is

$$\begin{aligned} A_{2,\mathcal{E}}(p) &= -p^2 + p \sum_{(x-y)(x^2+xy+y^2)\equiv 0} 1 \\ &= -p^2 + p\sum_{x(p)} 1 + p\sum_{x(p)} \sum_{y:x^2+xy+y^2\equiv 0} 1 - p\sum_{3x^2\equiv 0} 1 \end{aligned} \tag{3.31}$$

Since the discriminant of x^2+xy+y^2 as a quadratic in y is $-3x^2$, by the quadratic formula modulo p, the number of solutions to the congruence $x^2+xy+y^2 \equiv 0$ is $1+\left(\frac{-3x^2}{p}\right)$. Then

$$\begin{aligned} A_{2,\mathcal{E}}(p) &= p\sum_{x(p)}\left(1+\left(\frac{-3x^2}{p}\right)\right)-p \\ &= p\left(p+(p-1)\left(\frac{-3}{p}\right)\right)-p \\ &= \left(p^2-p\right)\left(1+\left(\frac{-3}{p}\right)\right) \end{aligned} \tag{3.32}$$

□

4. Numerical Investigations

4.1. **Measuring Average Bias.** In general, analyzing the double sum

$$A_{2,\mathcal{E}}(p) = \sum_{t(p)}\left[\sum_{x(p)}\left(\frac{x^3+A(t)x+B(t)}{p}\right)\right]^2 \tag{4.1}$$

explicitly is extremely difficult, especially for one-parameter families involving higher degree polynomials. We would like to analyze more complicated families numerically. Unfortunately, this is not always feasible.

Consider the following heuristic. Recall that Michel's result bounds the error in the second moment expansion by $O(p^{3/2})$. Miller [Mi05] showed that this bound is sharp, and our numerical explorations suggest that in some sense, an arbitrarily chosen family with high-degree polynomials almost always has an error term of size $p^{3/2}$. Central limit theorem intuition would predict, if the $p^{3/2}$ term averages to 0, that this average converges to 0 at a rate of about $1/\sqrt{p}$. However, this risks oscillations that conceal the size p biases for arbitrarily large primes. Thus our numerics must seek an understanding of the size $p^{3/2}$ error term that will allow us to isolate the contribution from the order p terms.

4.2. **Distributions of the Error Terms.** In the absence of a reliable method to numerically measure negative bias occurring in the size p, we want to better understand the larger error terms of size $p^{3/2}$. From our experiments, it appears that most one-parameter families have size $p^{3/2}$ error terms. Only especially nice families have second moments equal to $p^2+O(p)$.

Consider a family of the form $\mathcal{E}: y^2=(aT+b)x^3+(cT+d)x^2+(eT+f)x+(gT+h)$, and consider the term

$$\sum_{\Delta(x,y)\equiv 0}\left(\frac{P(x)P(y)}{p}\right) \tag{4.2}$$

in the notation of Lemma 3.2. Recall that

$$\Delta(x,y) = ((x-y)(R(x,y))^2 \tag{4.3}$$

with $R(x,y)$ as in (3.13). After applying inclusion-exclusion to isolate out the term

$$Y(p) = \sum_{R(x,y)\equiv 0}\left(\frac{P(x)P(y)}{p}\right), \tag{4.4}$$

all other terms including the original terms in Lemma 3.2 are of sizes p^2, p, or 1, and are tractable. Also, these terms have a simple structure, given by polynomials in p, Legendre symbols, or elliptic curve coefficients. As it is written, there is no clear arithmetic object associated to the term in (4.4). However, we believe that this term is concealing a Fourier coefficient of some L-function, in particular a hyperelliptic curve coefficient; some evidence for this belief can be found in [Mi05], where such a term is identified, as well as other families studied in [MMRW14]. Our goal is to provide evidence for this idea.

We examine families of ranks from 0 to 3 from [Fe96], compute an approximation to the distribution of the error terms, and compare the distribution to those found in [KS14] based on a generalized Sato-Tate conjecture. We also examine some CM-families and some irrational families.

All of the rank 0 and rank 1 families studied in [Fe96] are equivalent, via a coordinate change for primes $p > 3$, to a family of the form

$$\mathcal{E} : y^2 \ = \ bx^3 + dx^2 + (eT + f)x + h. \tag{4.5}$$

These families contain the exact same curves as the corresponding families

$$\mathcal{E} : y^2 \ = \ bx^3 + dx^2 + Tx + h. \tag{4.6}$$

We assume $p \nmid b, d, h$. In these cases, the term in Equation 4.4 is equal to

$$Y(p) \ = \ \sum_{b(x^2+xy+y^2)+d(x+y)-h\equiv 0(p)} \left(\frac{xy}{p}\right). \tag{4.7}$$

For the sake of computational efficiency, we can convert this sum into a sum only over x by noting that we are summing over the roots of a quadratic in y. We have

$$Y(p) \ = \ \sum_{by^2+(bx+d)y+(bx^2+dx-h)\equiv 0(p)} \left(\frac{xy}{p}\right) \tag{4.8}$$

and the discriminant of the quadratic in y is

$$D(x) \ = \ (bx+d)^2 - 4b(bx^2+dx-h) \ = \ -3b^2x^2 - 2bdx + d^2 + 4bh, \tag{4.9}$$

so by the quadratic formula modulo p

$$Y(p) \ = \ \sum_{\left(\frac{D(x)}{p}\right)\in\{0,1\}} \left(\frac{x(2b)^{-1}\left(-bx - d \pm D(x)^{1/2}\right)}{p}\right), \tag{4.10}$$

where $\pm$ indicates an inner sum of two Legendre symbols when $\left(\frac{D(x)}{p}\right) = 1$ and one Legendre symbol when $\left(\frac{D(x)}{p}\right) = 0$. In the cases we analyze, it appears that $Y(p) = O(p^{1/2})$ and that this bound is sharp.

In Figure 4.2 we compute $C(p)$ over the first 10,000 primes and report the first 8 moments of the error distribution in the number of points on the curves (i.e., on the $a_{\mathcal{E}_t}(p)$'s). These numerics suggest that the errors are converging to a semicircular distribution. This is not inconsistent with the error term being governed by a non-CM elliptic curve (possibly weighted by a Legendre symbol). We find similar agreement when we look at rank 0 families of this form. We end by looking at the distribution of the normalized $a_{\mathcal{E}_t}(p)$'s for a specific one-parameter family in Figure 4.2.

b	d	f	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8
4	-7	4	-0.015	1.013	-0.017	2.044	-0.0089	5.149	0.066	14.515
4	5	1	-.007	0.990	0.004	1.975	0.044	4.938	0.215	13.834
4	1	1	0.007	0.993	0.024	1.980	0.085	4.943	0.300	13.804
4	1	4	0.008	0.997	0.013	1.981	0.035	4.937	0.118	13.795
4	1	9	0.006	0.993	0.013	1.970	0.016	4.892	-0.007	13.635
4	4	1	0.006	0.986	0.024	1.963	0.067	4.914	0.193	13.824
4	5	4	0.006	1.016	0.037	2.038	0.130	5.096	0.435	14.282
4	4	9	-0.007	1.016	-0.016	2.051	-0.045	5.175	-0.123	14.594
4	5	9	0.006	0.991	0.001	1.973	-0.029	4.927	-0.159	13.792

FIGURE 1. Moments of rank 1 family error distributions. The odd moments of the normalized semi-circular distribution are all zero, while the even moments (starting with the second) are 1, 2, 5 and 14.

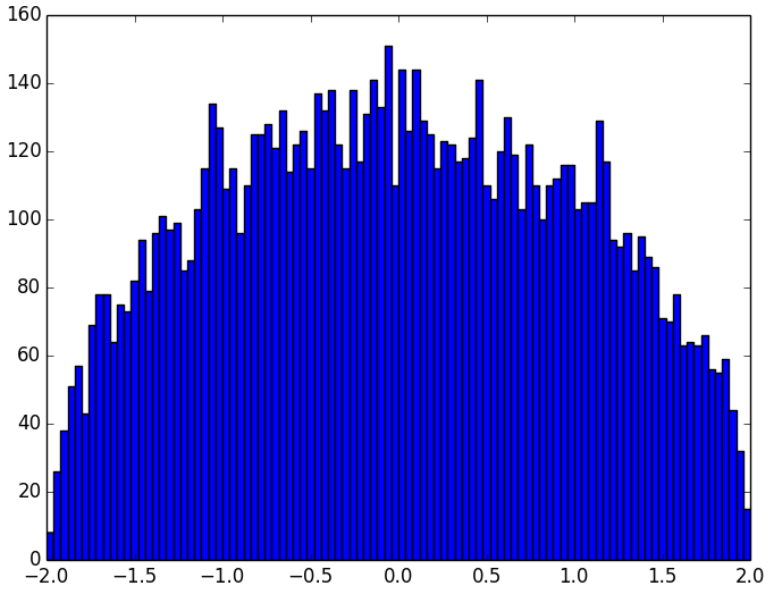

FIGURE 2. Error Distribution of the $a_{\mathcal{E}_t}(p)$'s for the family $y^2 = 4x^3+5x^2+Tx+1$ for the first 10,000 primes.

5. CONCLUSION AND FUTURE WORK

We have found strong support, both numerical and theoretical, for the bias conjecture for one-parameter families with coefficients low degree polynomials; additional examples may be found in [MMRW14].

While we have concentrated on the second moments of the Fourier coefficients in families of elliptic curve L-functions, there are many other related systems and questions to study. We can also investigate higher moments as well as other families of L-functions, and see if similar biases exist. If so, such biases can again have consequences for the distribution of low-lying zeros.

Another natural question is to better understand the nature of the bias. Specifically, what can be said about the possible values of these terms? To date, in every family where we can write down a closed form expression for the bias it has always been a combination of polynomials in p and coefficients of elliptic curve L-functions (though we allow ourselves to have different expressions depending on the congruence property of the prime). Does this persist both for other families of elliptic curves, and for the other generalizations mentioned earlier? We are currently investigating these and other related questions in [MMRW14].

REFERENCES

[AAILMZ15] L. Alpoge, N. Amersi, G. Iyer, O. Lazarev, S. J. Miller and L. Zhang, *Maass waveforms and low-lying zeros*, to appear in "Analytic Number Theory: In honor of Helmut Maier's 60th birthday," Springer-Verlag.

[AL-RM07] S. Arms, Á. Lozano-Robledo and S. J. Miller, *Constructing one-parameter families of elliptic curves over $\mathbb{Q}(T)$ with moderate rank*, Journal of Number Theory **123** (2007), no. 2, 388–402.

[B-LGHT11] T. Barnet-Lamb, D. Geraghty, M. Harris and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy II*, P.R.I.M.S. **47** (2011), 29–98.

[BEW98] B. Berndt, R. Evans, and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol. 21, Wiley-Interscience Publications, John Wiley & Sons, New York, 1998.

[Bi68] B. J. Birch, *How the number of points of an elliptic curve over a fixed prime field varies*, J. London Math. Soc. **43** (1968), 57–60.

[CHT08] L. CLozel, M. Harris and R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l representations*, Pub. Math. IHES **108** (2008), 1–181.

[Fe96] S. Fermigier, *Etude experimentale du rang de familles de courbes elliptiques sur*, Experimental Mathematics **5** (1996), no. 2, 119–130.

[HS-BT10] M. Harris, N. Shepherd-Barron and R. Taylor, *A family of Calabi-Yau varieties and potential automorphy*, Annals of Math. 171 (2010), 779-813.

[IK04] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, AMS Colloquium Publications, Vol. 53, AMS, Providence, RI, 2004.

[ILS00] H. Iwaniec, W. Luo, and P. Sarnak, *Low lying zeros of families of L-functions*, Inst. Hautes Études Sci. Publ. Math. **91** (2000), 55–131.

[KS99a] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications, Vol. 45, AMS, Providence, RI, 1999.

[KS99b] N. Katz and P. Sarnak, *Zeros of zeta functions and symmetries*, Bull. AMS **36** (1999), 1–26.

[KS14] K. S. Kedlaya, A. V. Sutherland, *Hyperelliptic curves, L-polynomials, and random matrices*, in Arithmetic, Geometry, Cryptography, and Coding Theory: International Conference, November 5-9, 2007, CIRM, Marseilles, France. Gilles Lachaud, Christophe Ritzenthaler, Michael A. Tsfasman, editors. 2009. (Contemporary Mathematics ; v.487)

[Kn92] A. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, NJ, 1992.

[MMRW14] B. Mackall, S. J. Miller, C. Rapti and K. Winsor, *Lower-Order Biases Moments of Fourier Coefficients in Families of Elliptic Curve L-Functions*, preprint 2014.

[Ma07] B. Mazur, *Finding meaning in error terms*, Bull. Amer. Math. Soc. **45** (2008), 185–228.

[Mic95] P. Michel, *Rang moyen de famille de courbes elliptiques et lois de Sato-Tate*, Monatshefte fur Mathematik **120** (1995), 127–136.

[Mi02] S. J. Miller, *1- and 2-level densities for families of elliptic curves: evidence for the underlying group symmetries*, PhD thesis, 2002, Princeton University.

[Mi04] S. J. Miller, *1- and 2-level densities for families of elliptic curves: evidence for the underlying group symmetries*, Compositio Mathematica **140** (2004), no. 4, 952–992.

[Mi05] 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.

[Mi09] S. J. Miller, *Lower order terms in the 1-level density for families of holomorphic cuspidal newforms*, Acta Arithmetica **137** (2009), 51–98.
[MM11] S. J. Miller, M. R. Murty, *Effective equidistribution and the Sato-Tate law for families of elliptic curves*, Journal of Number Theory **131** (2011), no. 1, 25–44.
[Na97] K. Nagao, $\mathbb{Q}(t)$*-rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. 92, 1997, 13–32.
[Ri03] O. Rizzo, *Average root numbers for a non-constant family of elliptic curves*, Compositio Mathematica 136: 1-23, 2003.
[RS98] M. Rosen and J. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133** (1998), 43–67.
[Si86] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag, Berlin - New York, 1986.
[ST92] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.
[Ta65] J. Tate, *Algebraic cycles and the pole of zeta functions*, Arithmetical Algebraic Geometry, Harper and Row, New York, 1965, 93–110.
[T08] R. Taylor, *Automorphy for some l-adic lifts of automorphic mod l Galois representations. II*, Publ. Math. Inst. Hautes Études Sci. **108**, 183–239.
[Wa87] L. Washington, *Class numbers of the simplest cubic fields*, Math. Comp. **48** (1987), no. 177, 371–384.
[XY13] P. Xi and Y. Yi, *A note on the moments of Kloosterman sums*, Proceedings of the American Mathematical Society **141** (2013), 1233–1240.

E-mail address: brm1@williams.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267

E-mail address: sjm1@williams.edu

DEPARTMENT OF MATHEMATICS AND STATISTICS, WILLIAMS COLLEGE, WILLIAMSTOWN, MA 01267

E-mail address: cr9060@bard.edu

DEPARTMENT OF MATHEMATICS, BARD COLLEGE, ANNANDALE-ON-HUDSON, NY 12504

E-mail address: krlwnsr@umich.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109