

LOWER-ORDER BIASES IN THE SECOND MOMENT OF DIRICHLET COEFFICIENTS IN FAMILIES OF L -FUNCTIONS

MEGUMI ASADA, RYAN C. CHEN, EVA FOURAKIS, YUJIN HONG KIM, ANDREW KWON, JARED DUKER
LICHTMAN, BLAKE MACKALL, STEVEN J. MILLER, ERIC WINSOR, KARL WINSOR, JIANING YANG,
AND KEVIN YANG

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 $A(T), B(T) \in \mathbb{Z}(T)$. Consider the k^{th} moments $A_{k,\mathcal{E}}(p) := \sum_{t \in \mathbb{F}_p} a_{\mathcal{E}_t}(p)^k$ of the Dirichlet coefficients $a_{\mathcal{E}_t}(p) := p + 1 - |\mathcal{E}_t(\mathbb{F}_p)|$. Rosen and Silverman proved Nagao's conjecture relating the first moment to the family's rank over $\mathbb{Q}(T)$, and Michel proved if $j(T)$ is not constant then the second moment equals $p^2 + O(p^{3/2})$. Cohomological arguments show the lower order terms are of sizes $p^{3/2}, p, p^{1/2}$ and 1. In every case we can analyze in closed form, the largest lower order term in the second moment expansion that doesn't average to zero is on average negative, though numerics suggest this may fail for families of moderate rank. We prove this Bias Conjecture for several large classes of families, including families with rank, complex multiplication, and constant $j(T)$ -invariant. We also study the analogous Bias Conjecture for families of Dirichlet characters, holomorphic forms on $\text{GL}(2)/\mathbb{Q}$, and their symmetric powers and Rankin-Selberg convolutions. We 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.

CONTENTS

1. Introduction	2
1.1. Bias in Families of L -Functions	3
1.2. Bias in Elliptic Curve Families	5
1.3. Outline	6
2. Linear one-parameter families of elliptic curves	8
3. Elliptic curve families of constant $j(T)$ -invariant	11
3.1. Counting Points Preliminaries	11
3.2. k^{th} Moments of the family $\mathcal{E}^r(T) : y^2 = x^3 - T^r Ax$	13
3.3. k^{th} Moments of the family $\mathcal{E}^r(T) : y^2 = x^3 + T^r B$	15
3.4. Computing the k^{th} moment for a family of any constant $j(T)$ -invariant	17
4. $\text{GL}(1)$ Families (Dirichlet Characters)	17
4.1. Preliminaries: Primes in Arithmetic Progression	17

Date: August 31, 2021.

2010 Mathematics Subject Classification. 60B10, 11B39, 11B05 (primary) 65Q30 (secondary).

Key words and phrases. Dirichlet characters, elliptic curves, cuspidal newforms, L -functions, lower order terms, excess rank.

This work was supported by NSF grants DMS 1347804, DMS1265673 and DMS1561945, Carnegie Mellon University, Princeton University, Williams College, the Eureka Program, the Finnerty Fund, and the Clare Boothe Luce Program of the Henry Luce Foundation. We thank the referee for numerous helpful comments, and Matija Kazalicki and Bartosz Naskrecki for sharing their preprints.

4.2. Characters of Prime Level	18
4.3. Characters of Prime Level and Prime Torsion	19
5. Holomorphic Newforms on $GL(2)/\mathbb{Q}$ and their Symmetric Lifts	20
5.1. Preliminaries	21
5.2. Proof of Theorem 5.1	22
6. Convolutions of Families	24
6.1. Proof of Theorem 6.1	26
6.2. Proof of Theorem 6.2	27
6.3. Proof of Theorem 6.3	29
7. Conclusion	30
Appendix A. Second Moments of Linear Elliptic Curve Families	30
A.1. Family $\mathcal{E}(T) : y^2 = (ax^2 + bx + c)(dx + e + T)$	30
A.2. Family $\mathcal{E}(T) : y^2 = x(ax^2 + bx + c + dTx)$	31
A.3. Family $\mathcal{E}(T) : y^2 = x(ax + b)(cx + d + Tx)$	32
Appendix B. Additional Elliptic Curve Families	33
Appendix C. Biases in Higher Moments	37
References	38

1. INTRODUCTION

The genesis of this paper are some computations on moments of the Dirichlet coefficients of the L -functions of elliptic curves by Miller in his thesis [Mi1, Mi2] and expanded in [Mi3]. The main purpose of that work was to verify the Katz-Sarnak Density Conjecture [KaSa1, KaSa2] for families of elliptic curves; in other words, that in the limit as the conductors tend to infinity the behavior of zeros near the central point in families of elliptic curve L -functions agree with the scaling limits of eigenvalues near 1 of orthogonal groups. In that and related work on numerous other families of L -functions (see [MMRT-BW] for an extensive discussion and survey of the literature and an expanded version of the argument below), the main term of number theory and random matrix theory agree; the lower order terms on the two sides, however, often differ, and it is in these lower order terms that the arithmetic of the family emerges. This is similar to the central limit theorem, which we expand on later.

In all families studied to date which can be computed in closed form a bias has been observed in these lower order terms; the purpose of this work is to describe these results, extensively investigate this phenomenon in other families, discuss the implications such a bias has in number theory, and hopefully motivate others to provide a theoretical understanding for this phenomenon (explicitly, as there is a cohomological interpretation of these elliptic curve moments, could such arguments give a proof for the bias?). Two of the most important applications are to the distribution of ranks in families, and lower order terms in the n -level densities; in particular, the presence of a negative bias leads to a slight increase in bounds on the average rank in families, as well as surfacing in lower order terms of the n -level densities of zeros of L -functions. The latter is particularly important, as the main term of these statistics agree with those from random matrix theory; the arithmetic of the family is absent in the main term but arises in the lower order terms, and breaks the universality of behavior. Thus we first describe the general framework (see [IK] for proofs and additional details), then describe the families studied and state our results.

1.1. Bias in Families of L -Functions. We quickly review some needed properties of L -functions; see for example [IK, RudSa]. Let π be a cuspidal automorphic representation on GL_n , and let $Q_\pi > 0$ be the analytic conductor of the associated L -function

$$L(s, \pi) = \sum_{m=1}^{\infty} \frac{\lambda_\pi(m)}{m^s}, \quad \frac{L'(s, \pi)}{L(s, \pi)} = - \sum_{m=1}^{\infty} \frac{\Lambda(m) a_\pi(m)}{m^s}, \quad (1.1)$$

where $\Lambda(m) = \log p$ if $m = p^k$ for a prime p , and 0 otherwise. Assuming the Generalized Riemann Hypothesis (GRH) the non-trivial zeros are of the form $1/2 + i\gamma_{\pi,j}$ with $\gamma_{\pi,j}$ real. Let $\{\alpha_{\pi,i}(p)\}_{i=1}^n$ be the Satake parameters of $L(s, \pi)$. We have the Euler product

$$L(s, \pi) = \sum_{m=1}^{\infty} \frac{\lambda_\pi(m)}{m^s} = \prod_p \prod_{i=1}^n (1 - \alpha_{\pi,i}(p) p^{-s})^{-1}, \quad (1.2)$$

and

$$a_\pi(p^\nu) = \sum_{i=1}^n \alpha_{\pi,i}(p)^\nu; \quad (1.3)$$

thus the $p^{\nu\text{th}}$ coefficient of $-L'(s, \pi)/L(s, \pi)$ is the ν^{th} moment of the Satake parameters (up to a factor of $\log p$). The explicit formula (see for example [ILS, RudSa]), applied to a given $L(s, \pi)$ and then averaged over a finite family \mathcal{F}_N , yields the 1-level density

$$\begin{aligned} D_{1, \mathcal{F}_N}(\phi) &:= \frac{1}{|\mathcal{F}_N|} \sum_{\pi \in \mathcal{F}_N} \sum_j \phi\left(\gamma_{\pi,j} \frac{\log Q_\pi}{2\pi}\right) \\ &= \widehat{\phi}(0) - 2 \frac{1}{|\mathcal{F}_N|} \sum_{\pi \in \mathcal{F}_N} \sum_p \sum_{\nu=1}^{\infty} \widehat{\phi}\left(\frac{\nu \log p}{\log Q_\pi}\right) \frac{a_\pi(p^\nu) \log p}{p^{\nu/2} \log Q_\pi} \\ &\quad + O\left(\frac{\log \log Q_\pi}{\log Q_\pi}\right), \end{aligned} \quad (1.4)$$

where ϕ is an even Schwarz test function with compactly supported Fourier transform $\widehat{\phi}$ and N is some parameter such that as N increases, the analytic conductors increase.¹ The Katz-Sarnak Density Conjecture states that as $N \rightarrow \infty$ the 1-level density converges to that of a classical compact group. This has been verified for many families for test functions whose Fourier transforms have suitably restricted support; see [MMRT-BW] for a list of many of these families, as well as a summary of the techniques used in the proofs.

In many situations, such as families of Dirichlet characters or cuspidal newforms of a given level and weight, the analytic conductors in our family are constant; thus $Q_\pi = Q_N$ say. For other families such as elliptic curves this fails, and one must either do sieving and additional work, or instead normalize by the average log-conductor; while this is satisfactory for the 1-level density it introduces problems for the general n -level density (see [Mi1, Mi2] for details and a resolution). Thus in calculating the 1-level density we can often push the sum over our family \mathcal{F}_N through the test function and reduce the analysis to averages of the moments of the Satake parameters. In all families studied to date we have sufficient decay in the $\lambda_\pi(p^\nu)$'s so that the sum over primes with

¹Note the 1-level density is well-defined even if GRH fails, though if there are zeros off the line then we lose the spectral interpretation of the zeros. If we adjust the rescaling of the zeros slightly we can remove the big-Oh error term, but its presence does not matter for calculating the main term, and is only important when we look at the 2 or higher level densities.

$\nu \geq 3$ converges; this is known for many families, and follows from the Ramanujan conjectures in general.² Thus determining the 1-level density, up to lower order terms, is equivalent to analyzing the $N \rightarrow \infty$ limits of

$$\begin{aligned} S_1(\mathcal{F}_N) &:= -2 \sum_p \hat{\phi} \left(\frac{\log p}{\log Q_N} \right) \frac{\log p}{\sqrt{p} \log Q_N} \left[\frac{1}{|\mathcal{F}_N|} \sum_{\pi \in \mathcal{F}_N} a_\pi(p) \right] \\ S_2(\mathcal{F}_N) &:= -2 \sum_p \hat{\phi} \left(2 \frac{\log p}{\log Q_N} \right) \frac{\log p}{p \log Q_N} \left[\frac{1}{|\mathcal{F}_N|} \sum_{\pi \in \mathcal{F}_N} a_\pi(p^2) \right]. \end{aligned} \quad (1.5)$$

As

$$a_\pi(p^\nu) = \alpha_{\pi,1}(p)^\nu + \cdots + \alpha_{\pi,n}(p)^\nu, \quad (1.6)$$

we see that only the first two moments of the Satake parameters enter the calculation. The sum over the remaining powers,

$$S_\nu(\mathcal{F}_N) := -2 \sum_{\nu=3}^{\infty} \sum_p \hat{\phi} \left(\nu \frac{\log p}{\log Q_N} \right) \frac{\log p}{p^{\nu/2} \log Q_N} \left[\frac{1}{|\mathcal{F}_N|} \sum_{\pi \in \mathcal{F}_N} a_\pi(p^\nu) \right], \quad (1.7)$$

is $O(1/\log Q_N)$ under the Ramanujan Conjectures. Thus the main term of the limiting behavior is controlled by the main terms of the first two moments of the Satake parameters (see Remark 1.1 for more on this); the higher moments (and the lower order terms in the first two moments) affect the rate of convergence to the random matrix theory limits. The goal of this work is to explore these lower order terms in a variety of families, and analyze the consequences for number theory.

As remarked above, the non-universality in the lower order terms is similar to that of the Central Limit Theorem. Given any nice density, one can renormalize it to have mean zero and variance one. The universality of the Central Limit Theorem is due to the fact that the higher moments of the density, which is where the shape emerges, only surface as lower order terms in the analysis, affecting only the *rate* of convergence to the Gaussian. The situation is thus very similar in families of L -functions, where both the third and higher moments of the Satake parameters, as well as lower order terms in the first and second moments, break universality and lead to lower order terms where arithmetic lives. These arguments show the importance of understanding the lower order terms, and is the motivation for this paper.

Remark 1.1. *We briefly comment on the first two moments, i.e., the sums in (1.5). For test functions with small support, $S_1(\mathcal{F}_N)$ contributes zero to the main term in all families investigated to date save for families of elliptic curves with rank r , where the main term of its contribution is $-r$ (if the support is large it can contribute; see [ILS] and the family of cuspidal newforms when the support exceeds $[-1, 1]$). Additionally, $S_2(\mathcal{F}_N)$ contributes $-c_{\mathcal{F}}\phi(0)/2$, and the family of L -functions has unitary, symplectic or orthogonal symmetry depending on whether or not the family symmetry constant $c_{\mathcal{F}}$ equals 0, 1 or -1. Further, in many cases it can be shown the symmetry of the Rankin-Selberg convolution of two families, $c_{\mathcal{F} \times \mathcal{G}}$, equals the product of the symmetries of the families. See [DuMi, SaShTe, ShTe] for more on determining the symmetry of a family, and [RudSa] for consequences of the second moment in universal behavior in another statistic, the n -level correlations.*

²The Satake parameters $|\alpha_{\pi,i}|$ are bounded by p^δ for some δ ; conjecturally $\delta = 0$. There has been significant progress towards these bounds with some $\delta < 1/2$; see [Kim, KimSa]. Any $\delta < 1/6$ implies the $\nu \geq 3$ terms do not contribute to the main term.

1.2. Bias in Elliptic Curve Families. As the initial impetus for this work came from families of elliptic curves, we start with a description of those results and then move to other families. Consider the elliptic surface \mathcal{E} given by $y^2 = x^3 + A(T)x + B(T)$ over $\mathbb{Q}(T)$ for $A(T), B(T) \in \mathbb{Z}[T]$; for almost all $t \in \mathbb{Z}$ the specialization \mathcal{E}_t obtained by setting $T = t$ is an elliptic curve. Let $a_{\mathcal{E}_t}(p)$ denote p minus the number of solutions to $y^2 \equiv x^3 + A(t)x + B(t) \pmod{p}$; this quantity is known as the p^{th} **Dirichlet coefficient** of \mathcal{E}_t , as such coefficients appear in the series expansion for the associated L -function. Set

$$A_{r,\mathcal{E}}(p) = \sum_{t \bmod p} a_{\mathcal{E}_t}^r(p), \quad (1.8)$$

so $A_{r,\mathcal{E}}(p)/p$ is the r^{th} moment.³ By work of Nagao, Rosen and Silverman [Na, RoSi] the first moment is related to the rank of the elliptic surface (it is a theorem if the surface is rational⁴, and conjectural in general):

$$\lim_{X \rightarrow \infty} \frac{1}{X} \sum_{p \leq X} -\frac{A_{1,\mathcal{E}}(p)}{p} \log p = \text{rank } \mathcal{E}(\mathbb{Q}(T)). \quad (1.9)$$

The main term of the second moment determines which classical compact group governs the behavior of zeros near the central point [DuMi, Mi2, ShTe], and by work of Michel [Mic] we have

$$A_{2,\mathcal{E}}(p) = p^2 + O(p^{3/2}) \quad (1.10)$$

if $j(T)$ is non-constant for the family.

The interesting observation in [Mi1, Mi3] is that, in every family of elliptic curves investigated, the largest lower order term in $A_{2,\mathcal{E}}(p)$ which did not average to zero had a negative average. While there were some families with a lower order term of size $p^{3/2}$ (and thus Michel's bound is sharp), in all those families such terms were on average zero. There were many families with a lower order term of size $-m_{\mathcal{E}}p$ for some $m_{\mathcal{E}} > 0$. While these terms are too small to influence the main term, they yield corrections of size the reciprocal of the logarithm of the conductors (which is the natural spacing between zeros near the central point); explicitly, they increase the 1-level density by

$$\frac{2m_{\mathcal{E}}}{\log Q} \sum_p \hat{\phi} \left(2 \frac{\log p}{\log Q} \right) \frac{\log p}{p^2}, \quad (1.11)$$

and thus break the universality of the main terms and lead to lower order terms depending on the arithmetic of the family.

For small conductors one consequence of the negative bias $-m_{\mathcal{E}}p$ is to increase the bounds for the average rank in families. While the amount of the increase is too small to explain the entirety of the observed excess rank phenomenon (see [DHKMS1, DHKMS2] for an explanation through the excised orthogonal ensemble), it *is* in the right direction and it is fascinating that the bias is always observed to be in the same direction. Of course, the families investigated are very special, as they are ones where the Legendre sum can be computed exactly so that the second moment can be fully determined, and thus may not be truly representative; see Appendix B for some families where we cannot compute the second moment in closed form but we do still observe the negative bias, and a discussion in Appendix C on some one-parameter families of moderate rank where there may

³We need to divide the p sum to have a moment, as we are averaging over p terms; some works include this division in the definition, others have it separate. We choose not to divide by p so that our sums are integer polynomials in p .

⁴An elliptic surface $y^2 = x^3 + A(T)x + B(T)$ is rational if and only if one of the following is true: (1) $0 < \max(\deg A, 2 \deg B) < 12$; (2) $3 \deg A = 2 \deg B = 12$ and $\text{ord}_{T=0} T^{12} \Delta(T^{-1}) = 0$.

Family	$A_{1,\varepsilon}(p)$	$A_{2,\varepsilon}(p)$
$y^2 = x^3 + Sx + T$	0	$p^3 - p^2$
$y^2 = x^3 + 2^4(-3)^3(9T + 1)^2$	0	$\begin{cases} 2p^2 - 2p & p \equiv 2 \pmod{3} \\ 0 & p \equiv 1 \pmod{3} \end{cases}$
$y^2 = x^3 \pm 4(4T + 2)x$	0	$\begin{cases} 2p^2 - 2p & p \equiv 1 \pmod{4} \\ 0 & p \equiv 3 \pmod{4} \end{cases}$
$y^2 = x^3 + (T + 1)x^2 + Tx$	0	$p^2 - 2p - 1$
$y^2 = x^3 + x^2 + 2T + 1$	0	$p^2 - 2p - \left(\frac{-3}{p}\right)$
$y^2 = x^3 + Tx^2 + 1$	$-p$	$p^2 - n_{3,2,p}p - 1 + c_{3/2}(p)$
$y^2 = x^3 - T^2x + T^2$	$-2p$	$p^2 - p - c_1(p) - c_0p$
$y^2 = x^3 - T^2x + T^4$	$-2p$	$p^2 - p - c_1(p) - c_0p$
$y^2 = x^3 + Tx^2 - (T + 3)x + 1$	$-2\delta_{1;4}(p)p$	$p^2 - 4\delta_{1;6}(p)p - 1$

TABLE 1. First and second moments for elliptic curve families, with $n_{3,2,p}$ the number of cube roots of 2 modulo p , $c_0p = \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right]$, $c_1(p) = \left[\sum_{x \bmod p} \left(\frac{x^3 - x}{p}\right)\right]^2$, $c_{3/2}(p) = p \sum_{x(p)} \left(\frac{4x^3 + 1}{p}\right)$, and $\delta_{a;m}(p) = 1$ if $p \equiv a \pmod{m}$ and otherwise is 0. The subscript on $c_k(p)$ indicates the power of p .

be a positive bias. We present some of this evidence in Table 1 (the calculations for most of these families can be found in [Mi1, Mi3]; the new families can be handled using similar techniques).

1.3. Outline. In the present work we explore biases in the lower order terms of second moments in several different families of L -functions. A preliminary analysis of some elliptic curve families was reported in [MMRW]; we provide additional proofs for some of the families explored there as well as some new ones, and also investigate numerous other natural families (Dirichlet L -functions, cuspidal newforms, and their convolutions). In [HKLM] these investigations are extended to hyper-elliptic curves, and in Appendix B we report on some recent extensions to other one-parameter families of elliptic curves, as well as some two-parameter families.

One challenge is to make sure we are comparing similar items in each case. In particular, what normalization should we use for the sums? For example, consider one-parameter elliptic curve families over $\mathbb{Q}(T)$ with $T \in [N, 2N]$. For each p , p times the second moment is $\sum_{t(p)} a_{\varepsilon_t}(p)^2$ (we will have $\lfloor N/p \rfloor$ copies of this, and then an incomplete sum of at most p terms); by Michel's work the main term is of size p^2 if $j(T)$ is not constant, and we observe lower order terms not averaging to zero of size p . The sizes here are due to our normalizations, where the elliptic curve L -function has critical strip $1/2 < \operatorname{Re}(s) < 3/2$ and functional equation $s \rightarrow 2 - s$. To compare with other families of L -functions, where the critical strip is taken to be $0 < \operatorname{Re}(s) < 1$, we normalize and study $a_{\varepsilon_t}(p)/\sqrt{p}$; by Hasse's theorem each of these terms is at most 2 in absolute value.

Thus our complete sums over $t \bmod p$ have a main term of size p and the first term not averaging to zero is of size 1; however, we should also average over the family. For one-parameter families of elliptic curves we often look at $t \in [N, 2N]$ with $N \rightarrow \infty$; this gives us $\lfloor N/p \rfloor$ complete sums

of $t \bmod p$ and one incomplete sum of size at most p . Thus we have

$$\frac{1}{N} \sum_{t=N}^{2N} \frac{a_{\mathcal{E}_t}(p)^2}{p} = \frac{\lfloor N/p \rfloor}{N} \sum_{t \bmod p} \frac{a_{\mathcal{E}_t}(p)^2}{p} + \frac{1}{N} \sum_t^* \frac{a_{\mathcal{E}_t}(p)^2}{p}, \quad (1.12)$$

where the asterisk denotes an incomplete sum of at most $p - 1$ terms. Thus, as long as p is significantly less than N , the incomplete sum is negligible relative to the first term. We will sum over $p \leq X$ and divide by $\pi(X)$, the number of primes at most X , namely,

$$\frac{1}{\pi(X)} \sum_{p \leq X} \frac{1}{N} \sum_{t=N}^{2N} \frac{a_{\mathcal{E}_t}(p)^2}{p} = \frac{1 + o(1)}{\pi(X)} \sum_{p \leq X} \sum_{t \bmod p} \frac{a_{\mathcal{E}_t}(p)^2}{p^2}. \quad (1.13)$$

If the complete sum over $t \bmod p$ equals $p^2 - m_{\mathcal{E}}p$ then the p^2 factor yields the main term of 1 (recall we have $\lfloor N/p \rfloor$ complete sums) while the $m_{\mathcal{E}}$ yields the leading lower order term of size

$$- \frac{1}{\pi(X)} \sum_{p \leq X} \frac{m_{\mathcal{E}}}{p} = - \frac{m_{\mathcal{E}} \log \log X \log X}{X} (1 + o(1)), \quad (1.14)$$

where we used standard results for the size of $\pi(X)$ and the sum of the reciprocals of the primes up to X .

Remark 1.2. *It's important to put the size of the main and leading error term in perspective. With this averaging, the small bias leads to a contribution which is barely detectable, tending to zero rapidly as the range of primes averaged over grows. This is quite reasonable, as the relative size of the bias to the main term, at each prime, is of size $1/p$, and this leads to a slowly growing sum. Note this behavior is very different than what happens when we look at the contribution of these lower order terms in the n -level densities and the excess rank investigations (this means looking at the average rank for forms in our family with parameter up to some specified value, and letting that value tend to infinity). The difference is due to how we weigh the sums. For the n -level densities and the rank, we are not dividing by the number of primes and are weighting each term by $(\log p)/p$. Thus the main and leading lower order terms are of comparable magnitude; there is an enormous difference between comparing a sum of 1 versus $1/p$ and a sum of $1/p$ versus $1/p^2$.*

In §2 we verify the elliptic curve Bias Conjecture for several one parameter families over $\mathbb{Q}(T)$, and then extend to include higher moments for some families with constant $j(T)$ in §3; recent work by Kazalicki and Naskrecki [KN1, KN2] have proved the bias conjecture for several families under standard conjectures, though some recent work suggests that the bias conjecture might fail for families with moderate rank (see Appendix C). We turn to Dirichlet L -functions in §4, and see in Theorems 4.2 and 4.4 that under GSH the bias is sometimes positive and sometimes negative, similar to the behavior seen in investigating Chebyshev's bias. Using the Petersson formula we show in Theorem 5.1 that there can be a small positive bias for cuspidal newforms in §5, and then conclude in §6 by investigating how the bias behaves under convolution of families. Theorem 6.1 looks at two families of Dirichlet characters, Theorem 6.2 replaces one of those families with a family of r^{th} symmetric lifts of cuspidal newforms, and Theorem 6.3 studies two symmetric lift families. There is tremendous universality in the behavior of the zeros of families of L -functions; there are very few main terms that are seen for the n -level densities; however, by looking at the lower order terms we can distinguish the behavior in different families. It is here, in the lower order terms, that the arithmetic of the family lives, and the motivation of this paper is to determine,

or at least see and leave to others to investigate further, how the arithmetic affects the behavior of the zeros.

2. LINEAR ONE-PARAMETER FAMILIES OF ELLIPTIC CURVES

In this and the next section we amass more evidence for the Bias Conjecture by demonstrating negative bias in additional one-parameter families of elliptic curves. See [MMRW, Mi1, Mi3] for earlier calculations on the subject. The families studied are amenable to direct calculation; thus these are not generic families but ones chosen so that the resulting Legendre sums are tractable.

We collect several standard 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 but cubic and higher typically cannot (which is why it is so hard to work with elliptic curves, as these give rise to cubic Legendre sums). The idea behind all the constructions is to bypass the difficulty of dealing with these cubic and higher Legendre sums by looking at carefully chosen one-parameter families where we can execute the sum over t modulo p exactly *and* be left with sums of a special form that can be evaluated in closed form. We state below the result for linear and quadratic sums; see for example [BEW, Mi1] for the standard proof.

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

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

and, letting $\Delta = b^2 - 4ac$ (the discriminant in x of $ax^2 + bx + c$),

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

We first investigate families of the form $\mathcal{E}_t : y^2 = P(x)t + Q(x)$ where P and Q are fixed polynomials. For convenience, we suppose p is an odd prime. Recalling $a_{\mathcal{E}_t}(p) = -\sum_{x(p)} \left(\frac{P(x)t + Q(x)}{p} \right)$, we have

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

If $P(x)P(y)$ is not zero modulo p we have a quadratic in t , with discriminant

$$\Delta(x, y) := (P(x)Q(y) + Q(x)P(y))^2 - 4P(x)P(y)Q(x)Q(y) = (P(x)Q(y) - Q(x)P(y))^2; \quad (2.3)$$

note $\Delta(x, y) = 0$ if and only if $P(x)Q(y) - Q(x)P(y) = 0$. Applying Lemma 2.1 to the quadratic sum over t yields

$$\begin{aligned} A_{2,\mathcal{E}}(p) &= p \left[\sum_{P(x) \equiv 0} \left(\frac{Q(x)}{p} \right) \right]^2 + \sum_{x,y \bmod p} \left\{ \begin{array}{ll} -\left(\frac{P(x)P(y)}{p} \right) & \text{if } p \nmid \Delta(x, y) \\ (p-1) \left(\frac{P(x)P(y)}{p} \right) & \text{if } p \mid \Delta(x, y) \end{array} \right\} \\ &= p \left[\sum_{P(x) \equiv 0} \left(\frac{Q(x)}{p} \right) \right]^2 - \left[\sum_{x \bmod p} \left(\frac{P(x)}{p} \right) \right]^2 + p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right). \end{aligned} \quad (2.4)$$

We use this formula to compute $A_{2,\mathcal{E}}(p)$ for families whose sum over $\Delta(x, y) \equiv 0$ is tractable.

Proposition 2.2. *The one-parameter family*

$$\mathcal{E} : y^2 = (ax + b)(cx^2 + dx + e + T) \quad (2.5)$$

with $p > 3$ prime, $a, b, c, d, e \in \mathbb{Z}$ and $p \nmid a, c$ has vanishing first moment, hence rank zero, and second moment

$$A_{2,\mathcal{E}}(p) = \begin{cases} p^2 - \left(2 + \left(\frac{-1}{p} \right) \right) p & \text{if } p \nmid ad - 2bc \\ (p^2 - p) \left(1 + \left(\frac{-1}{p} \right) \right) & \text{if } p \mid ad - 2bc. \end{cases} \quad (2.6)$$

Proof. We write $\mathcal{E}_t : y^2 = P(x)t + Q(x)$ where $P(x) = ax + b$ and $Q(x) = (ax + b)(cx^2 + dx + e)$. The first moment is

$$\begin{aligned} A_{1,\mathcal{E}}(p) &= \sum_{t \bmod p} a_{\mathcal{E}_t}(p) \\ &= - \sum_{t \bmod p} \sum_{x \bmod p} \left(\frac{P(x)t + Q(x)}{p} \right) \\ &= - \sum_{x \bmod p} \left(\frac{ax + b}{p} \right) \sum_{t \bmod p} \left(\frac{t + (cx^2 + dx + e)}{p} \right) = 0 \end{aligned} \quad (2.7)$$

by Lemma 2.1 applied to the sum over $t \bmod p$. Hence \mathcal{E} has rank zero as it is a rational surface.

Write the family as $\mathcal{E}_t : y^2 = P(x)t + Q(x)$ for $P(x) = ax + b$ and $Q(x) = P(x)(cx^2 + dx + e)$. Then $P(x) \mid Q(x)$ and $\sum_{x(p)} \left(\frac{P(x)}{p} \right) = 0$ so by (2.4), we have

$$A_{2,\mathcal{E}}(p) = p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right). \quad (2.8)$$

Since

$$\begin{aligned} P(y)Q(x) - P(x)Q(y) &= (ax + b)(ay + b)[(cx^2 + dx + e) - (cy^2 + dy + e)] \\ &= (ax + b)(ay + b)(x - y)(cx + cy + d), \end{aligned} \quad (2.9)$$

we deduce $\Delta(x, y) \equiv 0$ if and only if $P(x) \equiv 0$, $P(y) \equiv 0$, $x \equiv y$, or $x + y \equiv -d/c$. Thus by inclusion-exclusion

$$\begin{aligned} \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) &= \sum_{x+y \equiv -d/c} \left(\frac{P(x)P(y)}{p} \right) + \sum_{x \equiv y} \left(\frac{P(x)P(y)}{p} \right) - \sum_{\substack{x+y \equiv -d/c \\ x \equiv y}} \left(\frac{P(x)P(y)}{p} \right) \\ &= \sum_{x \in (p)} \left(\frac{P(x)P(-x-d/c)}{p} \right) + (p-1) - \left(\frac{P(-d/2c)^2}{p} \right). \end{aligned} \quad (2.10)$$

We have $P(x)P(-x-d/c) = -a^2x^2 - a^2d/cx - abd/c + b^2$ so that

$$\sum_{x \in (p)} \left(\frac{P(x)P(-x-d/c)}{p} \right) = \left(\frac{-1}{p} \right) \cdot \begin{cases} -1 & \text{if } p \nmid ad - 2bc \\ p-1 & \text{if } p \mid ad - 2bc \end{cases} \quad (2.11)$$

since $P(x)P(-x-d/c)$ has discriminant $a^2(ad/c - 2b)^2$ and $p \nmid a, c$. Also note that

$$\left(\frac{P(-d/2c)}{p} \right)^2 = \left(\frac{-ad/2c + b}{p} \right)^2 = \begin{cases} 1 & \text{if } p \nmid ad - 2bc \\ 0 & \text{if } p \mid ad - 2bc. \end{cases} \quad (2.12)$$

Plugging into the above gives

$$\sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) = \begin{cases} -\left(\frac{-1}{p} \right) + (p-1) - 1 & \text{if } p \nmid ad - 2bc \\ (p-1) \left(\frac{-1}{p} \right) + (p-1) - 0 & \text{if } p \mid ad - 2bc \end{cases} \quad (2.13)$$

and thus

$$A_{2,\mathcal{E}}(p) = p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) = \begin{cases} p^2 - \left(2 + \left(\frac{-1}{p} \right) \right) p & \text{if } p \nmid ad - 2bc \\ (p^2 - p) \left(1 + \left(\frac{-1}{p} \right) \right) & \text{if } p \mid ad - 2bc. \end{cases} \quad (2.14)$$

□

If $ad - 2bc$ is not zero, then for all sufficiently large p we have $p \nmid ad - 2bc$, and thus by Dirichlet's theorem for primes in arithmetic progression the main term is p^2 and half the time the leading lower order term is $-3p$ and half the time it is $-p$.

We compute the first and second moments of three other one-parameter families. The proofs are similar to Proposition 2.2; see Appendix A for details.

Proposition 2.3. *The one-parameter family*

$$\mathcal{E} : y^2 = (ax^2 + bx + c)(dx + e + T) \quad (2.15)$$

with $p > 3$ prime, $a, b, c, d, e \in \mathbb{Z}$ and $p \nmid a, d$ has vanishing first moment, hence rank zero, and second moment given by

$$A_{2,\mathcal{E}}(p) = \begin{cases} p^2 - \left(1 + \left(\frac{b^2 - 4ac}{p} \right) \right) p - 1 & \text{if } p \nmid b^2 - 4ac \\ p - 1 & \text{if } p \mid b^2 - 4ac. \end{cases} \quad (2.16)$$

Proposition 2.4. *The one-parameter family*

$$\mathcal{E} : y^2 = x(ax^2 + bx + c + dTx) \quad (2.17)$$

with $p > 3$ prime, $a, b, c, d \in \mathbb{Z}$ and $p \nmid a, d$ has vanishing first moment, hence rank zero, and second moment given by

$$A_{2,\mathcal{E}}(p) = \begin{cases} p^2 - 2p - 1 & \text{if } p \nmid c \\ p - 1 & \text{if } p \mid c. \end{cases} \quad (2.18)$$

Proposition 2.5. *The one-parameteter family*

$$\mathcal{E} : y^2 = x(ax + b)(cx + d + Tx) \quad (2.19)$$

with $p > 3$ prime, $a, b, c, d \in \mathbb{Z}$ and $p \nmid a, d$ has vanishing first moment, hence rank zero, and second moment given by

$$A_{2,\mathcal{E}}(p) = \begin{cases} p^2 - 2p - 1 & \text{if } p \nmid b \\ p^2 - p & \text{if } p \mid b. \end{cases} \quad (2.20)$$

3. ELLIPTIC CURVE FAMILIES OF CONSTANT $j(T)$ -INVARIANT

So far, all of the families of elliptic curves that have been investigated for bias have had non-constant $j(T)$ -invariant (in T). This is motivated by a result of Michel [Mic], which states that for such families,

$$A_{2,\mathcal{E}}(p) = p^2 + O(p^{3/2}). \quad (3.1)$$

In this section, we study families of elliptic curves that have constant $j(T)$ -invariant and observe that, for these families, the Bias Conjecture does not seem to apply in a sensible way. Moreover, our methods allow us to compute moments of *arbitrary* degree. This is notable because, in general, it is extremely difficult to compute moments higher than second of elliptic curve families, due to the complexity of the Legendre sums.

In Section 3.2, we study the elliptic curve family $\mathcal{E}^r(T) : y^2 = x^3 - T^r Ax$, for any $r \in \mathbb{N}$ and $A \neq 0$. Such families have constant $j(T)$ -invariant equal to 1728. Our main result there is Theorem 3.5.

In Section 3.3, we study the elliptic curve family $\mathcal{E}^r(T) : y^2 = x^3 + T^r B$, for any $r \in \mathbb{N}$ and $B \neq 0$. Such families have constant $j(T)$ -invariant equal to 0. Our main result there is Theorem 3.7.

In Section 3.4, we compute the k^{th} moment of the elliptic curve family $\mathcal{E}(T) : y^2 = x^3 + T^2 Ax + T^3 B$, for any k . Note that such families have constant $j(T)$ -invariant given in terms of A and B . Our main result there is Theorem 3.9.

Since the moments of elliptic curve families are intimately related to the number of points on each elliptic curve within the family, we begin by detailing known results on counting points of elliptic curves of j -invariant 0 and 1728. For an elementary survey of results on counting points of elliptic curves of fixed j -invariant, see [BKNT].

3.1. Counting Points Preliminaries.

3.1.1. Elliptic Curves of j -invariant 0. Note that all elliptic curves with j -invariant 0 over a finite field take the form $y^2 = x^3 + B$. The following lemma shows that the order of an elliptic curve group over \mathbb{F}_p is determined by the sextic residue class of B .

Lemma 3.1 (Proposition 2.1, [BKNT]). *The elliptic curves $E_1 : y^2 = x^3 + B$ and $E_2 : y^2 = x^3 + t^6 B$, where $t, B \in \mathbb{F}_p^\times$, have the same number of points over \mathbb{F}_p .*

Suppose $p \equiv 1 \pmod{6}$ is a prime. We can partition \mathbb{F}_p^\times into six equivalence classes via the relation

$$k_1 \sim k_2, \iff \exists k \in \mathbb{F}_p^\times \text{ such that } k_1 k_2^{-1} = k^6,$$

for $k_1, k_2 \in \mathbb{F}_p^\times$. The second condition above states that $k_1 k_2^{-1}$ is a sixth power in \mathbb{F}_p^\times . These equivalence classes, which all have size $(p-1)/6$, will be referred to as *sextic residue classes*. For a prime $p \not\equiv 1 \pmod{6}$, we can still partition into sextic residue classes via the above equivalence relation, although there will not be six distinct equivalence classes.

From the above proposition, it follows that if $k_1, k_2 \in \mathbb{F}_p^\times$ are in the same sextic residue class, then the curves $E_1 : y^2 = x^3 + k_1$ and $E_2 : y^2 = x^3 + k_2$ have the same number of \mathbb{F}_p -points. Hence an elliptic curve $E : y^2 = x^3 + k$ (i.e., of j -invariant 0) takes on one of at most six different orders for the group of points $E(\mathbb{F}_p)$, where the number of distinct orders depends on the prime p . The above discussion of sextic residue classes implies that when $p \equiv 1 \pmod{6}$ (or equivalently, $p \equiv 1 \pmod{3}$), six distinct orders are realized, whereas when $p \equiv 2 \pmod{3}$, less than six distinct orders are realized. Below, we state in Theorem 3.2 a result of Gauss that gives these orders explicitly. Before doing so, it is convenient to introduce the notation $a_E(p)$, for an elliptic curve $E : y^2 = x^3 + ax + b$, defined to be

$$a_E(p) := p - \#\{(x, y) \in (\mathbb{Z}/p\mathbb{Z})^2 : y^2 \equiv x^3 + ax + b \pmod{p}\} = - \sum_{x \pmod{p}} \left(\frac{x^3 + ax + b}{p} \right). \quad (3.2)$$

Theorem 3.2 (Gauss, six orders for $j = 0$ curves). *Let E be the elliptic curve $y^2 = x^3 + B$ (i.e., a curve with j -invariant 0) with good reduction mod p .*

- (1) *If $p \equiv 2 \pmod{3}$, then $a_E(p) = 0$.*
- (2) *If $p \equiv 1 \pmod{3}$, write p uniquely as $p = a^2 + 3b^2$, where $a \equiv 2 \pmod{3}$ and $b > 0$. Then*

$$a_E(p) = \begin{cases} -2a & \text{for } B \text{ a sextic residue mod } p \\ 2a & \text{for } B \text{ a cubic, non-quadratic residue mod } p \\ a \pm 3b & \text{for } B \text{ a quadratic, non-cubic residue mod } p \\ -a \pm 3b & \text{for } B \text{ a non-quadratic, non-cubic residue mod } p. \end{cases} \quad (3.3)$$

We note that as B runs through the values of \mathbb{F}_p^\times , $a_E(p)$ is equal to each of $\{\pm 2a, \pm a \pm 3b\}$ with equal proportion, since the sextic residue classes equipartition \mathbb{F}_p^\times . The choices of signs in the expressions $a \pm 3b$ and $-a \pm 3b$ can be specified by an analog of the Legendre symbol for a fixed $\pi \in \mathbb{Z}[(1 + \sqrt{-3})/2]$ lying over p , which will be specified by the choice of a and b . See [IR, Theorem 18.3.4] for the statement and proof.

3.1.2. Elliptic Curves of j -invariant 1728. All elliptic curves with j -invariant 1728 are of the form $E : y^2 = x^3 - Ax$. Similar to the $j = 0$ case, the following lemma shows that the order of an elliptic curve group over \mathbb{F}_p is determined by the quartic residue class of A .

Lemma 3.3 (Proposition 3.1, [BKNT]). *For any $t \in \mathbb{F}_p^\times$, $E_1 : y^2 = x^3 - Ax$ and $E_2 : y^2 = x^3 - t^4 Ax$ have the same number of points over \mathbb{F}_p .*

The following theorem of Gauss gives the explicit dependence of $a_E(p)$ on the quartic residue class of A , for E an elliptic curve with j -invariant equal to 1728.

Theorem 3.4 (Gauss, four orders for $j = 1728$ curves). *Let $E : y^2 = x^3 - Ax$ (i.e., a $j = 1728$ curve) with good reduction mod p .*

- (1) If $p \equiv 3 \pmod{4}$, then $a_E(p) = 0$.
(2) If $p \equiv 1 \pmod{4}$, write p as $p = a^2 + b^2$, where b is even and $a + b \equiv 1 \pmod{4}$. Then

$$a_E(p) = \begin{cases} 2a & \text{for } A \text{ a quartic residue mod } p \\ -2a & \text{for } A \text{ a quadratic, non-quartic residue mod } p \\ \pm 2b & \text{for } A \text{ a non-quadratic residue mod } p. \end{cases} \quad (3.4)$$

For proofs, see [IR, Theorem 18.4.5] or [Wa]. Again, the sign in the expression $\pm 2b$ may be specified via a quartic residue symbol in the ring $\mathbb{Z}[i]$. We note that as A runs through the values of \mathbb{F}_p^\times , $a_E(p)$ is equal to each of the elements of the set $\{\pm 2a, \pm 2b\}$ with equal proportion—this is because the cosets of the image of the fourth-power map evenly partition \mathbb{F}_p^\times .

3.2. k^{th} Moments of the family $\mathcal{E}^r(T) : y^2 = x^3 - T^r Ax$. We now determine the k^{th} moment at p of the elliptic curve family $\mathcal{E}^r(T) : y^2 = x^3 - T^r Ax$ for any $k, r \in \mathbb{N}$ and $A \neq 0$. These families all have constant j -invariant $j(T) = 1728$. Note that it suffices to consider the equivalence class of $r \pmod{4}$, since $y^2 = x^3 - T^r Ax$ and $y^2 = x^3 - T^{r+4} Ax$ have the same number of \mathbb{F}_p points by Lemma 3.3. Thus, for $r \in \{0, 1, 2, 3\}$, we may define the quantity

$$A_{k, \mathcal{E}^{[r]_4}}(p) := A_{k, \mathcal{E}^{r'}}(p),$$

which gives the k^{th} moment at p for any $r' \in \mathbb{N}$ such that $r' \equiv r \pmod{4}$.

Our main result is the following.

Theorem 3.5. *For $r \in \mathbb{N}$ and $A \neq 0$, consider the elliptic curve family $\mathcal{E}^r(T) : y^2 = x^3 - T^r Ax$.*

- (1) *If $p \equiv 3 \pmod{4}$, then for all $k, r \in \mathbb{N}$, we have*

$$A_{k, \mathcal{E}^r}(p) = 0. \quad (3.5)$$

- (2) *For $p \equiv 1 \pmod{4}$, we have the following results:*

$$A_{k, \mathcal{E}^{[0]_4}}(p) = \begin{cases} (p-1)(2a)^k & \text{for } A \text{ a quartic residue mod } p \\ (p-1)(-2a)^k & \text{for } A \text{ a quadratic, non-quartic residue mod } p \\ (p-1)(\pm 2b)^k & \text{for } A \text{ a non-quadratic residue mod } p, \end{cases} \quad (3.6)$$

$$A_{k, \mathcal{E}^{[1]_4}}(p) = A_{k, \mathcal{E}^{[3]_4}}(p) = \begin{cases} (p-1)2^{k-1}(a^k + b^k) & \text{for } k \text{ even} \\ 0 & \text{for } k \text{ odd,} \end{cases} \quad (3.7)$$

and finally,

$$A_{k, \mathcal{E}^{[2]_4}}(p) = \begin{cases} (p-1)(2a)^k & \text{for } k \text{ even, } A \text{ a quadratic residue mod } p \\ (p-1)(2b)^k & \text{for } k \text{ even, } A \text{ a non-quadratic residue mod } p \\ 0 & \text{for } k \text{ odd,} \end{cases} \quad (3.8)$$

where a, b , and the plus/minuses in (3.6) are given by Theorem 3.4.

Remark 3.6. *We can trivially extend these results to any $\mathcal{E}(T) : y^2 = x^3 - (cT + d)^r Ax$, since $T \mapsto cT + d$ is a bijection of \mathbb{F}_p for $p \nmid c$.*

Proof of Theorem 3.5. If $p \equiv 3 \pmod{4}$, then by Theorem 3.4, every elliptic curve E with $j = 1728$ has $a_E(p) = 0$; thus, it follows trivially that $A_{k, \mathcal{E}^r} = 0$ for all $k, r \in \mathbb{N}$.

It remains to consider the $p \equiv 1 \pmod{4}$ case. For organizational clarity, we prove equation (3.6) in Section 3.2.1, equation (3.7) in Sections 3.2.2 and 3.2.3, and equation (3.8) in Section 3.2.4. \square

Per the above, we will always consider $p \equiv 1 \pmod{4}$ for the rest of the calculations in this subsection. It will often be convenient to define $a_p(x^3 + ax + b) := a_E(p)$, for $E : y^2 = x^3 + ax + b$ and $a_E(p)$ defined as in (3.2). Then, we can write

$$A_{k,\mathcal{E}^r}(p) = \sum_{T=1}^{p-1} a_p(x^3 - T^r Ax)^k = \sum_{T \in \mathbb{F}_p^\times} a_p(x^3 - T^r Ax)^k. \quad (3.9)$$

3.2.1. Proof of equation (3.6): $r \equiv 0 \pmod{4}$. In the $r \equiv 0 \pmod{4}$ case, we need only consider the constant family $\mathcal{E}^0(T) : y^2 = x^3 - Ax$. Then $A_{k,\mathcal{E}^0}(p) = (p-1)a_{\mathcal{E}}(p)^k$, and so equation (3.6) follows from Theorem 3.4.

3.2.2. Proof of equation (3.7): $r \equiv 1 \pmod{4}$. We examine $\mathcal{E}^1(T) : y^2 = x^3 - TAx$. Note that TA runs through the elements of \mathbb{F}_p^\times as T does, and since $(p-1)/4 \in \mathbb{Z}$, $a_p(x^3 - TAx)$ takes on each of the values given in Theorem 3.4 a total of $(p-1)/4$ times. Substituting into (3.9) gives

$$\begin{aligned} A_{k,\mathcal{E}^1}(p) &= \frac{p-1}{4} ((2a)^k + (-2a)^k + (2b)^k + (-2b)^k) \\ &= \begin{cases} (p-1)2^{k-1}(a^k + b^k) & \text{for } k \text{ even} \\ 0 & \text{for } k \text{ odd,} \end{cases} \end{aligned} \quad (3.10)$$

as desired.

3.2.3. Proof of equation (3.7): $r \equiv 3 \pmod{4}$. We now examine $\mathcal{E}^3(T) : y^2 = x^3 - T^3Ax$. Select a generator g of \mathbb{F}_p^\times . Since $A \neq 0$, we have $A \equiv g^m \pmod{p}$ for some unique $m \in \{1, \dots, p-1\}$. The reduction of the set $\{T^3A : 1 \leq T \leq p-1\}$ modulo p may then be written as $\{g^{3t+m} : 1 \leq t \leq p-1\}$.

By Theorem 3.4, we know $a_p(x^3 - T^3Ax)$ depends only on the “quartic coset” of T^3A modulo p ; in other words, there is a unique $i \in \{0, 1, 2, 3\}$ for which $T^3A \in g^i(\mathbb{F}_p^\times)^4$ and $a_p(x^3 - T^3Ax)$ depends only on i . Moreover, g^{3t+m} and $g^{3t'+m}$ lie in the same quartic coset if and only if $t \equiv t' \pmod{4}$. Since $p \equiv 1 \pmod{4}$, the congruence classes of t modulo 4 partition the set $\{t : 1 \leq t \leq p-1\}$ equally into four sets, each of size $(p-1)/4$. We conclude that the elements of the set $\{T^3A : 1 \leq T \leq p-1\}$ are uniformly distributed among all four quartic cosets. We may then compute as in the $r \equiv 1 \pmod{4}$ case to find that

$$A_{k,\mathcal{E}^3}(p) = A_{k,\mathcal{E}^1}(p). \quad (3.11)$$

This shows equation (3.7).

3.2.4. Proof of equation (3.8): $r \equiv 2 \pmod{4}$. We examine $\mathcal{E}^2(T) : y^2 = x^3 - T^2Ax$. If A is a quadratic residue, then T^2A is a quadratic residue for all $T \in \mathbb{F}_p^\times$. Moreover, writing $A \equiv a^2 \pmod{p}$, we have T^2A is a quartic residue whenever $\left(\frac{T}{p}\right) = \left(\frac{a}{p}\right)$, which occurs half of the time. Thus, from (3.9) and Theorem 3.4, we have

$$A_{k,\mathcal{E}^2}(p) = \frac{p-1}{2} ((2a)^k + (-2a)^k) = \begin{cases} (p-1)(2a)^k & \text{for } k \text{ even} \\ 0 & \text{for } k \text{ odd.} \end{cases} \quad (3.12)$$

On the other hand, if A is a quadratic non-residue, then T^2A is a quadratic non-residue for all $T \in \mathbb{F}_p^\times$, with half of these values in each non-quadratic coset of the image of the fourth-power map $\phi : x \mapsto x^4$ (fix a generator $g \in \mathbb{F}_p^\times$ —the non-quadratic cosets are $g\text{Im}(\phi)$ and $g^3\text{Im}(\phi)$); the

quadratic cosets are $\text{Im}(\phi)$ and $g^2\text{Im}(\phi)$). What this means is that a_p takes on each value in the “non-quadratic” case of Theorem 3.4 half of the time as T runs through \mathbb{F}_p^\times . Thus,

$$A_{k,\mathcal{E}^2}(p) = \frac{p-1}{2} ((2b)^k + (-2b)^k) = \begin{cases} (p-1)(2b)^k & \text{for } k \text{ even} \\ 0 & \text{for } k \text{ odd.} \end{cases} \quad (3.13)$$

Hence, we have shown equation (3.8). This concludes the proof of Theorem 3.5

3.3. k^{th} Moments of the family $\mathcal{E}^r(T) : y^2 = x^3 + T^r B$. We now analyze families of elliptic curves of the form $\mathcal{E}^r(T) : y^2 = x^3 + T^r B$, for all $r \in \mathbb{N}$. These families have constant j -invariant $j(T) = 0$. Similar to the $j = 1728$ case, note that it suffices to consider r modulo 6 by Lemma 3.1. Thus, for $r \in \{0, 1, \dots, 5\}$, we may consider the quantity $A_{k,\mathcal{E}^{[r]_6}}(p) := A_{k,\mathcal{E}^{r'}}(p)$, where $r' \equiv r \pmod{6}$. Following equation (3.9), we may write

$$A_{k,\mathcal{E}^{[r]_6}}(p) = A_{k,\mathcal{E}^r}(p) = \sum_{T=0}^{p-1} a_p(x^3 + T^r B)^k = \sum_{T \in \mathbb{F}_p^\times} a_p(x^3 + T^r B)^k. \quad (3.14)$$

Our main result is the following.

Theorem 3.7. *For $r \in \mathbb{N}$, consider the elliptic curve family $\mathcal{E}^r(T) : y^2 = x^3 + T^r B$. If $p \equiv 2 \pmod{3}$, then for all $k, r \in \mathbb{N}$,*

$$A_{k,\mathcal{E}^r}(p) = 0. \quad (3.15)$$

If $p \equiv 1 \pmod{3}$, we have the following results:

$$A_{k,\mathcal{E}^{[0]_6}}(p) = \begin{cases} (p-1)(-2a)^k & \text{for } B \text{ a sextic residue mod } p \\ (p-1)(2a)^k & \text{for } B \text{ a cubic, non-quadratic residue mod } p \\ (p-1)(a \pm 3b)^k & \text{for } B \text{ a quadratic, non-cubic residue mod } p \\ (p-1)(-a \pm 3b)^k & \text{for } B \text{ a non-quadratic, non-cubic residue mod } p, \end{cases} \quad (3.16)$$

$$A_{k,\mathcal{E}^{[1]_6}}(p) = A_{k,\mathcal{E}^{[5]_6}}(p) = \begin{cases} \frac{p-1}{3} ((2a)^k + (a-3b)^k + (a+3b)^k) & \text{for } k \text{ even} \\ 0 & \text{for } k \text{ odd,} \end{cases} \quad (3.17)$$

$$\begin{aligned} A_{k,\mathcal{E}^{[2]_6}}(p) &= A_{k,\mathcal{E}^{[4]_6}}(p) \\ &= \begin{cases} \frac{p-1}{3} ((-2a)^k + (a-3b)^k + (a+3b)^k) & \text{for } B \text{ a quadratic residue} \\ \frac{p-1}{3} ((2a)^k + (-a-3b)^k + (-a+3b)^k) & \text{otherwise} \end{cases} \end{aligned} \quad (3.18)$$

and finally,

$$A_{k,\mathcal{E}^{[3]_6}}(p) = \begin{cases} (p-1)(2a)^k & \text{for } B \text{ a cubic residue, } k \text{ is even} \\ 0 & \text{for } B \text{ a cubic residue, } k \text{ is odd} \\ \frac{p-1}{2} ((a \pm 3b)^k + (-a \mp 3b)^k) & \text{for } B \text{ a cubic non-residue,} \end{cases} \quad (3.19)$$

where a, b , and the plus/minuses in (3.16) and (3.19) are given by Theorem 3.2.

Remark 3.8. *Just as before, it is trivial to extend these results to any $\mathcal{E}(T) : y^2 = x^3 + (cT+d)^r B$.*

Proof of Theorem 3.7. If $p \equiv 2 \pmod{3}$, then by Theorem 3.2, every elliptic curve E with $j = 0$ has $a_E(p) = 0$; thus, it follows trivially that $A_{k,\mathcal{E}^r}(p) = 0$ for all $k, r \in \mathbb{N}$.

For the $p \equiv 1 \pmod{3}$ case, similar to the organization in Section 3.2, we prove equation (3.16) in Section 3.3.1, equation (3.17) in Section 3.3.2, equation (3.18) in Section 3.3.3, and equation (3.19) in Section 3.3.4. □

3.3.1. Proof of equation (3.16): $r \equiv 0 \pmod{6}$. In the $r \equiv 0 \pmod{6}$ case, we need only consider the constant family $\mathcal{E}^0(T) : y^2 = x^3 + B$. Then $A_{k,\mathcal{E}^0}(p) = (p-1)a_p(x^3 + B)^k$, and so Theorem 3.2 gives (3.16).

3.3.2. Proof of equation (3.17): $r \equiv 1, 5 \pmod{6}$. We examine $\mathcal{E}^1(T) : y^2 = x^3 + TB$. Since TB runs through all elements of \mathbb{F}_p^\times and since $\frac{p-1}{6} \in \mathbb{Z}$, equation (3.14) yields

$$\begin{aligned} A_{k,\mathcal{E}^1}(p) &= \frac{p-1}{6} \left((2a)^k + (-2a)^k + (a-3b)^k + (a+3b)^k + (-a+3b)^k + (-a-3b)^k \right) \\ &= \begin{cases} \frac{p-1}{3} \left((2a)^k + (a-3b)^k + (a+3b)^k \right) & \text{for } k \text{ even} \\ 0 & \text{for } k \text{ odd.} \end{cases} \end{aligned} \quad (3.20)$$

We note that the case $r \equiv 5 \pmod{6}$ reduces to that of $r \equiv 1 \pmod{6}$ via the isomorphism $T \mapsto T^{-1}$ on \mathbb{F}_p^\times . This shows (3.17).

3.3.3. Proof of equation (3.18): $r \equiv 2, 4 \pmod{6}$. We examine $\mathcal{E}^2(T) : y^2 = x^3 + T^2B$. Suppose B is a quadratic residue. Then T^2B is always a quadratic residue, runs through each of the quadratic residues of \mathbb{F}_p^\times twice, and is a sextic residue one-third of the time. To see this, fix a generator $g \in \mathbb{F}_p^\times$, denote the cosets of the image of the sixth power map by $\{[g^{6c}], [g^{6c+1}], [g^{6c+2}], [g^{6c+3}], [g^{6c+4}], [g^{6c+5}]\}$. Squaring gives $\{[g^{6c}], [g^{6c+2}], [g^{6c+4}]\}$, the three quadratic residue classes. Thus, from Theorem 3.2, we see that the values of a_p are split uniformly among $-2a$, $a-3b$, and $a+3b$. Indeed, $\frac{p-1}{3}$ is an integer, and so we have

$$A_{k,\mathcal{E}^2}(p) = \frac{p-1}{3} \left((-2a)^k + (a-3b)^k + (a+3b)^k \right) \quad (3.21)$$

for B a quadratic residue.

On the other hand, suppose B is a quadratic non-residue. Then T^2B is never a quadratic residue, while it is a cubic residue for one-third of the values of T . By the same argument as above, we have

$$A_{k,\mathcal{E}^2}(p) = \frac{p-1}{3} \left((2a)^k + (-a-3b)^k + (-a+3b)^k \right). \quad (3.22)$$

We note that the case $r \equiv 4 \pmod{6}$ reduces to that of $r \equiv 2 \pmod{6}$ via the isomorphism $T \mapsto T^{-1}$ on \mathbb{F}_p^\times . This shows equation (3.18).

3.3.4. Proof of equation (3.19): $r \equiv 3 \pmod{6}$. We examine $\mathcal{E}^3(T) : y^2 = x^3 + T^3B$. If B is a cubic residue, then T^3B is either a sextic or cubic residue, with each case occurring with equal proportion over the values of T . Thus,

$$A_{k,\mathcal{E}^3}(p) = \frac{p-1}{2} \left((-2a)^k + (2a)^k \right) = \begin{cases} (p-1)(2a)^k & k \text{ is even} \\ 0 & k \text{ is odd.} \end{cases} \quad (3.23)$$

On the other hand, if B is a cubic non-residue then

$$A_{k,\mathcal{E}^3}(p) = \frac{p-1}{2} \left((a \pm 3b)^k + (-a \mp 3b)^k \right), \quad (3.24)$$

where the plus/minus signs are determined by Theorem 3.2. This shows (3.19), thereby concluding the proof of Theorem 3.7.

3.4. Computing the k^{th} moment for a family of any constant $j(T)$ –invariant. For any constant $j(T)$, the k^{th} moment of the elliptic curve family $\mathcal{E}(T) : y^2 = x^3 + T^2Ax + T^3B$ can be computed for any k , where $j(T) = 1728 \cdot 4A^3/(4A^3 + 27B^2)$.

Theorem 3.9 ($j(T) \neq 0, 1728$). *Consider the elliptic curve family $\mathcal{E}(T) : y^2 = x^3 + T^2Ax + T^3B$. We have*

$$A_{k,\mathcal{E}(T)}(p) = \begin{cases} (p-1)a_{\mathcal{E}(1)}(p)^k & \text{for } k \text{ even} \\ 0 & \text{for } k \text{ odd.} \end{cases} \quad (3.25)$$

The proof follows from the following lemma, which is well-known.

Lemma 3.10. *Fix $d \in \mathbb{Z}$ such that $\left(\frac{d}{p}\right) = -1$, and consider the elliptic curves $E : y^2 = x^3 + Ax + B$ and $\tilde{E} : y^2 = x^3 + d^2Ax + d^3B$. Then*

$$a_{\tilde{E}}(p) = -a_E(p).$$

Proof of Lemma 3.10. Note that the curve

$$dy^2 = x^3 + Ax + B \quad (3.26)$$

has Weierstrass form $y^2 = x^3 + d^2Ax + d^3B$. It follows that the right hand side of (3.26) is a quadratic residue if and only if $x^3 + d^2Ax + d^3B$ is a non-residue. \square

Proof of Theorem 3.9. Note that when $T \neq 0$, half of the T are quadratic residues and the other half are quadratic non-residues. Since the Legendre symbol is multiplicative, it follows from Lemma 3.10 that for half of the curves E in the family, we have $a_E(p) = a_{\mathcal{E}(1)}(p)$, and for the other half, we have $a_E(p) = -a_{\mathcal{E}(1)}(p)$. This immediately yields the desired result. \square

4. GL(1) FAMILIES (DIRICHLET CHARACTERS)

We investigate two families. For the first, we study \mathcal{D}_q , the family of nontrivial Dirichlet characters of prime level q . For the second, we consider the sub-family of \mathcal{D}_q of characters χ with prime torsion ℓ (thus, χ^ℓ is the principal character). We take q and ℓ to be distinct odd primes such that $q \equiv 1 \pmod{\ell}$, and let $\mathcal{D}_{q,\ell} \subseteq \mathcal{D}_q$ be those ℓ -torsion characters; note it is not interesting to take $\ell = 2$, as the second moment summand would then be 1 at all primes p relatively prime to the level q .

4.1. Preliminaries: Primes in Arithmetic Progression. The bias in these families is related to the bias in primes in arithmetic progressions, specifically to the distribution of primes congruent to 1 or -1 modulo a fixed prime q . We record some useful facts, taken from [RubSa].

First, some notation. Let $\pi(X, q, a)$ denote the number of primes at most X which are congruent to a modulo q , and set

$$E(X, q, a) := (\varphi(q)\pi(X, q, a) - \pi(X)) \frac{\log X}{\sqrt{X}}. \quad (4.1)$$

By Dirichlet's theorem on primes in arithmetic progression we know that to first order, if a and q are relatively prime, that $\pi(X, q, a)$ and $\pi(X)/\varphi(q)$ are of the same size, and thus the difference $\varphi(q)\pi(X, q, a) - \pi(X)$ should be significantly smaller than X ; we expect it to be of size $\sqrt{X}/\log X$, hence the normalization factor. Set

$$c(q, a) = -1 + \sum_{b^2 \equiv a(q)} 1 \quad (4.2)$$

and

$$\psi(X, \chi) = \sum_{n < X} \Lambda(n) \chi(n) \quad (4.3)$$

with $\Lambda(n)$ the classical von-Mangoldt function. We have (see Lemma 2.1 in [RubSa]) that

$$E(X, q, a) = -c(q, a) + \sum_{\chi \neq \chi_0} \bar{\chi}(a) \frac{\psi(X, \chi)}{\sqrt{X}} + O\left(\frac{1}{\log X}\right). \quad (4.4)$$

Unfortunately it is difficult to evaluate the sum over characters, though we can express it as a sum over zeros of the associated L -functions and then attack its value by assuming the Generalized Riemann Hypothesis (GRH) and the Grand Simplicity Hypothesis (GSH, which states that the imaginary parts of the critical zeros of Dirichlet L -functions are linearly independent over the rationals).

4.2. Characters of Prime Level. The quantity below is defined to mirror the elliptic curve case (see (1.13)). We divide by the cardinality of the family \mathcal{D}_q , which is $\varphi(q) - 1 = q - 2$ (remember we are excluding the trivial character).

Definition 4.1. *The average second moment of the family \mathcal{D}_q is the sum*

$$M_2(\mathcal{D}_q, X) = \frac{1}{\pi(X)} \sum_{p \leq X} \frac{1}{q-2} \sum_{\chi \in \mathcal{D}_q} \chi^2(p). \quad (4.5)$$

Theorem 4.2. *Assuming GRH, the average second moment $M_2(\mathcal{D}_q, X)$ of the family \mathcal{D}_q converges to $\frac{1}{q-2}$ as $X \rightarrow \infty$. The lower order error term is $\frac{\sqrt{X}}{(q-2)\pi(X)\log X} (E(X, q, 1) + E(X, q, -1))$. Additionally assuming GSH and q sufficiently large, the error term as a function of X is sometimes positive and sometimes negative (and on a logarithmic scale each happens a positive percentage of the time).*

Proof. When evaluating the sum of Definition 4.1, we may assume $p \neq q$ as otherwise the character sum is trivially 0. By $\bar{\chi}$ we mean the inverse of $\chi \bmod q$, and p^{-1} is the inverse of p in \mathbb{F}_q^* . Rewriting (4.5) as

$$M_2(\mathcal{D}_q, X) = \frac{1}{\pi(X)} \sum_{p \leq X} \frac{1}{q-2} \sum_{\chi \in \mathcal{D}_q} \chi(p) \overline{\chi(p^{-1})}, \quad (4.6)$$

we deduce from the Schur orthogonality relations (for sums of Dirichlet characters) that

$$\sum_{\chi \in \mathcal{D}_q} \chi(p)^2 = -1 + \begin{cases} q-1 & \text{if } p \equiv \pm 1(q) \\ 0 & \text{if } p \not\equiv \pm 1(q). \end{cases} \quad (4.7)$$

Thus

$$\begin{aligned}
M_2(\mathcal{D}_q, X) &= \frac{1}{\pi(X)} \frac{1}{q-2} \left[\sum_{\substack{p \leq X \\ p \equiv \pm 1(q)}} (q-1) - \sum_{p \leq X} 1 \right] \\
&= \frac{1}{q-2} \frac{\varphi(q) (\pi(X, q, 1) + \pi(X, q, -1)) - \pi(X)}{\pi(X)} \\
&= \frac{1}{q-2} \frac{\pi(X) + (\varphi(q)\pi(X, q, 1) - \pi(X)) + (\varphi(q)\pi(X, q, -1) - \pi(X))}{\pi(X)} \\
&= \frac{1}{q-2} + \frac{\sqrt{X}}{(q-2)\pi(X) \log X} [E(X, q, 1) + E(X, q, -1)]. \tag{4.8}
\end{aligned}$$

Rubinstein and Sarnak [RubSa] prove that on a logarithmic scale, all possible orderings of the number of primes in distinct residue classes occur a positive percentage of the time. More precisely, if a_1, \dots, a_r are distinct residues relatively prime to q , set

$$P_{q; a_1, \dots, a_r} := \{X \in \mathbb{R} : \pi(X, q, a_1) > \pi(X, q, a_2) > \dots > \pi(X, q, a_r)\}. \tag{4.9}$$

The logarithmic density of a set P , denoted $\delta(P)$, exists (and is the common limit) if the following two limits exist and are equal:

$$\bar{\delta}(P) := \limsup_{X \rightarrow \infty} \frac{1}{\log X} \int_{t \in P \cap [2, X]} \frac{dt}{t}, \quad \underline{\delta}(P) := \liminf_{X \rightarrow \infty} \frac{1}{\log X} \int_{t \in P \cap [2, X]} \frac{dt}{t}. \tag{4.10}$$

Theorem 1.5 in [RubSa] states that for each $r \geq 2$, assuming GRH and GSH, we have

$$\max_{a_1, \dots, a_r(q)} \left| \delta(P_{q; a_1, \dots, a_r}) - \frac{1}{r!} \right| \rightarrow 0 \quad (\text{as } q \rightarrow \infty). \tag{4.11}$$

Thus for q sufficiently large, the secondary terms $E(X, q, \pm 1)$ in (4.8) are each greater than zero (i.e. positive bias) for a positive percentage of X on a logarithmic scale. Similarly $E(X, q, \pm 1) < 0$ (i.e. negative bias) for a positive percentage of X . \square

4.3. Characters of Prime Level and Prime Torsion. We now fix an odd prime ℓ and consider the family $\mathcal{D}_{q, \ell}$ of non-trivial characters of order ℓ with q prime and $q \equiv 1 \pmod{\ell}$, which implies via the structure theorem for finite abelian groups that the families $\mathcal{D}_{q, \ell}$ are nonempty.

Definition 4.3. *The average second moment of the family $\mathcal{D}_{q, \ell}$ is*

$$M_2(\mathcal{D}_{q, \ell}, X) = \frac{1}{\pi(X)} \sum_{p \leq X} \frac{1}{|\mathcal{D}_{q, \ell}|} \sum_{\chi \in \mathcal{D}_{q, \ell}} \chi^2(p). \tag{4.12}$$

In contrast to the previous family of all characters of level q , the restriction to characters with prime torsion ℓ gives us a family with zero main term.

Theorem 4.4. *Fix an odd prime ℓ . Then the family $\mathcal{D}_{q, \ell}$ has zero main term in its average second moment. Moreover, under GRH and GSH, the bias is positive and negative a positive percentage of the time.*

To prove Theorem 4.4, we recall some standard properties of the family $\mathcal{D}_{q, \ell}$ (cf. [IK]).

Lemma 4.5. *If ℓ is an odd prime and r is relatively prime to ℓ , then the map $\chi \mapsto \chi^r$ is an automorphism on $\mathcal{D}_{q, \ell}$.*

Lemma 4.6. *Let $\mathbb{F}_q^*(\ell) \subseteq \mathbb{F}_q^*$ be the ℓ^{th} power residues modulo q . Then $\#\mathbb{F}_q^*(\ell) = (q-1)/\ell$, which implies $\#\{a \in \mathbb{F}_q^* : a \notin \mathbb{F}_q^*(\ell)\} = (q-1)(\ell-1)/\ell$.*

Proof of Theorem 4.4. We must compute

$$M_2(\mathcal{D}_{q,\ell}, X) = \frac{1}{\pi(X)} \sum_{p \leq X} \frac{1}{|\mathcal{D}_{q,\ell}|} \sum_{\chi \in \mathcal{D}_{q,\ell}} \chi^2(p). \quad (4.13)$$

For $r \in \{1, \dots, \ell-1\}$, we know by Lemma 4.5 that the map $\chi \mapsto \chi^r$ is an automorphism of $\mathcal{D}_{q,\ell}$. This gives

$$\sum_{\chi \in \mathcal{D}_{q,\ell}} \chi(p)^2 = \sum_{\chi \in \mathcal{D}_{q,\ell}} \chi(p) = \frac{1}{\ell-1} \sum_{\chi \in \mathcal{D}_{q,\ell}} (\chi(p) + \chi^2(p) + \dots + \chi^{\ell-1}(p)). \quad (4.14)$$

For any $\chi \in \mathcal{D}_{q,\ell}$, we have that $p \notin \mathbb{F}_q^*(\ell)$ if and only if $\chi(p) \neq 1$. For such p we have

$$1 + \chi(p) + \chi^2(p) + \dots + \chi^{\ell-1}(p) = \frac{\chi^\ell(p) - 1}{\chi(p) - 1} = 0, \quad (4.15)$$

so we find that

$$\sum_{\chi \in \mathcal{D}_{q,\ell}} \chi(p)^2 = \frac{1}{\ell-1} \sum_{\chi \in \mathcal{D}_{q,\ell}} (-1) = -\frac{|\mathcal{D}_{q,\ell}|}{\ell-1} \quad (4.16)$$

if $p \notin \mathbb{F}_q^*(\ell)$.

If $p = a^\ell$ for some $a \in \mathbb{F}_q^*$, then trivially $\sum_{\chi} \chi^2(p) = |\mathcal{D}_{q,\ell}|$ as each $\chi^2(p)$ equals 1. Thus

$$M_2(\mathcal{D}_{q,\ell}, X) = \frac{1}{\pi(X)} \left(\sum_{a \in \mathbb{F}_q^*(\ell)} \pi(X, q, a) - \frac{1}{\ell-1} \cdot \sum_{a \notin \mathbb{F}_q^*(\ell)} \pi(X, q, a) \right). \quad (4.17)$$

By Lemma 4.6 the number of terms in the sums over a are $(q-1)/\ell$ and $(q-1)(\ell-1)/\ell$ respectively; then by the Prime Number Theorem in arithmetic progressions the main terms cancel above. As before, assuming GRH and GSH, the bias is positive and negative a positive percentage of the time. \square

5. HOLOMORPHIC NEWFORMS ON $GL(2)/\mathbb{Q}$ AND THEIR SYMMETRIC LIFTS

For a fixed level q and even integer k , let $\mathcal{C}_{k,q}(\chi_0)$ denote the space of cusp forms of weight k , level q , and principal central character. We assume q is square-free throughout, and our main result will be concerned only with prime q (it should be possible to handle square-free q with more care). Note $\mathcal{C}_{k,q}(\chi_0)$ has a subspace which is an eigenspace for all p^{th} Hecke operators, $p \nmid q$, which is denoted by $H_{k,q}^*(\chi_0)$, and known as the space of cuspidal newforms of weight k , level q and principal central character. We study the L -functions associated to these objects and their symmetric lifts. We fix a square-free level q and consider the untwisted family

$$\mathcal{F}_{r,X,\delta,q} = \bigcup_{k < X^\delta} \text{Sym}^r [H_{k,q}^*(\chi_0)] \quad (5.1)$$

for $\delta > 0$; k **will always range over even integers in all sums below**, which we denote by a star in the summation. For $p \nmid q$, we define the p -local second moment of this family by

$$M_{2,p}(\mathcal{F}_{r,X,\delta,q}) = \frac{1}{\sum_{k < X^\delta}^* \dim H_{k,q}^*(\chi_0)} \sum_{k < X^\delta}^* \sum_{f \in H_{k,q}^*(\chi_0)} a_{\text{Sym}^r f}^2(p). \quad (5.2)$$

We fix a constant $\sigma > 0$ and sum over primes $p \leq X^\sigma$ that do not divide the level, and define the second moment of $\mathcal{F}_{r,X,\delta,q}$ by

$$M_{2,\sigma}(\mathcal{F}_{r,X,\delta,q}) = \frac{1}{\pi(X^\sigma)} \sum_{\substack{p \leq X^\sigma \\ p \neq q}} M_{2,p}(\mathcal{F}_{r,X,\delta,q}). \quad (5.3)$$

The parameter σ controls the number of primes p we sum over compared to the number of weights k we sum over in the p -local second moment. In particular, averaging over primes p allows us to exploit the dependence of the coefficients $a_{\text{Sym}^r f}^2(p)$ on the prime p ; this will extract the lower order terms determining the bias.

We now study the bias of

$$M_{2,\sigma}(\mathcal{F}_{r,X,\delta}) = \lim_{q \rightarrow \infty} M_{2,\sigma}(\mathcal{F}_{r,X,\delta,q}) \quad (5.4)$$

where the limit is taken over prime levels q . We prove the following bias result for the family $\mathcal{F}_{r,X,\delta}$.

Theorem 5.1. *We have*

$$M_{2,\sigma}(\mathcal{F}_{r,X,\delta}) = (1 + O(X^{-\delta})) \left(1 + \frac{\log \log X^\sigma}{\pi(X^\sigma)} + O\left(\frac{1}{\pi(X^\sigma)}\right) \right). \quad (5.5)$$

If we choose $\sigma < \delta$ then the main term of $M_{2,\sigma}(\mathcal{F}_{r,X,\delta})$ is 1 with leading lower order term

$$\frac{\log \log X^\sigma}{\pi(X^\sigma)}. \quad (5.6)$$

We say that these families have a main term of 1 and a small positive bias of $(\log \log X^\sigma)/\pi(X^\sigma)$ (which tends to 0 as $X \rightarrow \infty$), so long as $\delta > \sigma$.

We may also average over the level q ; as the calculations are similar in the interest of space we will not report on this case (in that situation, q is not square-free so we need to use some results from [BDDM]). So long as the error terms in counting the forms in the family are smaller than the leading error terms in the Petersson computations we will need, the rate at which we let the weights and levels grow with respect to the rate at which we average over primes does not change the sign of the bias in the family but does change the size of the bias.

Finally, we could also analyze higher moments. The situation is strikingly different here than in the case of elliptic curves, as the Petersson formula is still available, and thus for suitably restricted ranges the computations are handled analogously as above.

5.1. Preliminaries. We briefly review some needed facts; see [IK] for a detailed exposition. For an $f \in H_{k,q}^*(\chi_0)$, we consider the L -function attached to the r^{th} symmetric lift of f , whose local Euler factors are given by

$$L_p(\text{Sym}^r f, s) = \prod_{j=0}^r (1 - \alpha_p^{r-j} \beta_p^j p^{-s})^{-1} \quad (5.7)$$

where α_p, β_p are the two Satake parameters at p . Note if $r = 1$ we regain our original form f , and thus we can study families of cuspidal newforms and their symmetric lifts simultaneously. We have

$$\lambda_{\text{Sym}^r f}(p) = \lambda_f(p^r). \quad (5.8)$$

Before we proceed with computing anything, we recall that a *ramified* prime p is a prime that divides the level of the newform, and an *unramified* prime does not divide the level. Thus, by (5.8) and the theory of L -functions attached to holomorphic cusp forms f , we have for any distinct, unramified primes

$$\lambda_{\text{Sym}^r f}(p) \lambda_{\text{Sym}^r f}(q) = \lambda_{\text{Sym}^r f}(pq). \quad (5.9)$$

To compute the second-moment bias, we use the following standard fact.

Lemma 5.2. *For unramified primes p ,*

$$\lambda_{\text{Sym}^r f}^2(p) = \lambda_f^2(p^r) = \sum_{\ell=0}^r \lambda_f(p^{2\ell}). \quad (5.10)$$

Proof. Because $\alpha_p \beta_p = 1$ for p unramified, we have

$$\lambda_f^2(p^r) = (\alpha_p^r + \alpha_p^{r-2} + \cdots + \alpha_p^{-r})^2 = \sum_{\ell=1}^r (r - \ell + 1) (\alpha_p^{2\ell} + \alpha_p^{-2\ell}) + (r + 1). \quad (5.11)$$

Since $\lambda_f(p^m) = \alpha_p^m + \alpha_p^{m-2} + \cdots + \alpha_p^{-m}$, the far RHS of (5.11) agrees with the far RHS of (5.10). \square

The main tool is the Petersson formula; the version below is Proposition 2.13 in [ILS].

Proposition 5.3 (Proposition 2.13, [ILS]). *Let q be squarefree and $(n, q^2) \mid q$. Then*

$$\sum_{f \in H_{k,q}^*(\chi_0)} \lambda_f(n) = \begin{cases} \frac{k-1}{12} \frac{\varphi(q)}{\sqrt{n}} + O\left((n, q)^{-\frac{1}{2}} n^{\frac{1}{6}} k^{\frac{2}{3}} q^{\frac{2}{3}}\right) & n \text{ a square and } (n, q) = 1, \\ O\left((n, q)^{-\frac{1}{2}} n^{\frac{1}{6}} k^{\frac{2}{3}} q^{\frac{2}{3}}\right) & \text{otherwise.} \end{cases} \quad (5.12)$$

Lastly, we need asymptotics for even weight k of $\dim H_{k,q}^*(\chi_0)$ for q square-free. To do so, we appeal to the following.

Lemma 5.4 (Corollary 2.14, [ILS]). *For even weights $k \geq 2$ and q square-free,*

$$\dim H_{k,q}^*(\chi_0) = \frac{k-1}{12} \varphi(q) + O((kq)^{2/3}). \quad (5.13)$$

Note that in particular, the above corollary yields

$$\sum_{k < X^\delta}^* \dim H_{k,q}^*(\chi_0) = \frac{\varphi(q)}{48} X^{2\delta} + O(X^{5\delta/3} q^{2/3}). \quad (5.14)$$

5.2. Proof of Theorem 5.1. Let χ_0 denote the principal character. We fix a prime level q and consider the untwisted family $\mathcal{F}_{r,X,\delta,q}$ defined in (5.1), and for $\delta, \sigma > 0$ investigate the second moments $M_{2,p}(\mathcal{F}_{r,X,\delta,q})$ and $M_{2,\sigma}(\mathcal{F}_{r,X,\delta,q})$ defined in equations (5.2) and (5.3). The second moment of interest is the following limit of second moments:

$$M_{2,\sigma}(\mathcal{F}_{r,X,\delta}) = \lim_{q \rightarrow \infty} M_{2,\sigma}(\mathcal{F}_{r,X,\delta,q}). \quad (5.15)$$

Unfolding the RHS of (5.2), using (5.10) and Proposition 5.3, we have

$$\begin{aligned}
M_{2,\sigma}(\mathcal{F}_{r,X,\delta,q}) &= \frac{1}{\pi(X^\sigma)} \frac{1}{\sum_{k < X^\delta}^* \dim(H_{k,q}^*(\chi_0))} \sum_{\substack{p \leq X^\sigma \\ p \neq q}} \sum_{k < X^\delta}^* \sum_{f \in H_{k,q}^*(\chi_0)} \lambda_{\text{Sym}^r f}^2(p) \\
&= \frac{1}{\pi(X^\sigma)} \frac{1}{\sum_{k < X^\delta}^* \dim(H_{k,q}^*(\chi_0))} \sum_{\substack{p \leq X^\sigma \\ p \neq q}} \sum_{k < X^\delta}^* \sum_{\ell=0}^r \left(\frac{k-1}{12} \varphi(q) p^{-\ell} + O(p^{\ell/3} k^{2/3} q^{2/3}) \right).
\end{aligned} \tag{5.16}$$

We will now, as well as in later arguments, focus on leading terms and then handle lower order terms at the end. In (5.16) we first fix a prime and investigate the first k sum. Summing $\varphi(q)(k-1)/12$ over the even weight k , dividing by the number of such forms, and recalling $\varphi(q) = q-1$ for q prime, we have

$$\frac{X^{2\delta}/48 + O(X^\delta)}{X^{2\delta}/48 + O(X^{5\delta/3} q^{2/3}/\varphi(q))} = 1 + O(X^{-\delta} + X^{-\delta/3} q^{-1/3}); \tag{5.17}$$

the error from counting the number of forms is significantly smaller than the main lower order terms we'll find below.

We now average over the primes p . We have

$$\sum_{\substack{p \leq X^\sigma \\ p \neq q}} \sum_{\ell=0}^r p^{-\ell} = \sum_{p \leq X^\sigma} 1 + \sum_{p \leq X^\sigma} p^{-1} + \sum_{\ell=2}^r \sum_{p \leq X^\sigma} p^{-\ell} + O(1). \tag{5.18}$$

In particular, from the sum over primes p we extract the two leading terms that diverge as $X \rightarrow \infty$ and trivially bound the remaining $O(1)$ terms. The first term on the RHS of (5.18) is $\pi(X^\sigma)$. For the second term, we use the (see for example [Dav]):

$$\sum_{p \leq X} p^{-1} = \log \log X + O\left(1 + \frac{1}{\log X}\right). \tag{5.19}$$

Thus, taking into account the normalization factors, the main terms from the Peterrson formula are

$$(1 + O(X^{-\delta} + X^{-\delta/3} q^{-1/3})) \left(1 + \frac{\log \log X^\sigma}{\pi(X^\sigma)} + O\left(\frac{1}{\pi(X^\sigma)}\right) \right). \tag{5.20}$$

Now, accounting for the accumulation of error terms from the Peterrson formula, it suffices to show that, in the limit as $q \rightarrow \infty$,

$$\frac{1}{\pi(X^\sigma)} \frac{1}{\varphi(q) X^{2\delta}/48 + O(X^{5\delta/3} q^{2/3})} \sum_{\substack{p \leq X^\sigma \\ p \neq q}} \sum_{k < X^\delta}^* \sum_{\ell=0}^r O(p^{\ell/3} k^{2/3} q^{2/3}) \tag{5.21}$$

is negligible. However, we note that all the big-Oh terms have a factor of $q^{2/3}$, while the second fraction has a factor of $\varphi(q) = q-1$ for q prime. Thus since the big-Oh constants are absolute, in the limit $q \rightarrow \infty$, these error terms all vanish; we conclude that

$$M_{2,\sigma}(\mathcal{F}_{r,X,\delta}) = (1 + O(X^{-\delta})) \left(1 + \frac{\log \log X^\sigma}{\pi(X^\sigma)} + O\left(\frac{1}{\pi(X^\sigma)}\right) \right), \tag{5.22}$$

and so it is not hard to see that the leading error term $\frac{\log \log X^\sigma}{\pi(X^\sigma)}$ will remain as long as it is not smaller than $O(X^{-\delta})$. For this, it suffices to have $\delta > \sigma$, as claimed. \square

6. CONVOLUTIONS OF FAMILIES

In this section we explore the effect Rankin-Selberg convolution has on biases in second moments; we briefly summarize the framework (see [IK] for additional details). For an automorphic representation π on $\mathrm{GL}(n)$, we have the Satake parameters $\{\alpha_{\pi,i}(p)\}_{i=1}^n$ as the coefficients in the Euler product of the associated L -function

$$L(s, \pi) = \prod_p \prod_{i=1}^n (1 - \alpha_{\pi,i}(p)p^{-s})^{-1}. \quad (6.1)$$

The Rankin-Selberg method provides a way to combine families of L -functions. If the Satake parameters of the L -functions for π_1, π_2 are $\{\alpha_{\pi_1,i}(p)\}_{i=1}^n$ and $\{\alpha_{\pi_2,j}(p)\}_{j=1}^m$, then the pairwise products of the parameters determine the convolved family via

$$\{\alpha_{\pi_1 \times \pi_2, k}(p)\}_{k=1}^{nm} = \{\alpha_{\pi_1,i}(p) \cdot \alpha_{\pi_2,j}(p)\}_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}. \quad (6.2)$$

Occasionally the resulting L -function will not be primitive; for example, if $\pi_1 = \pi_2 = f$ is a cuspidal newform on $\mathrm{GL}(2)$, then $\zeta(s)$ divides the convolution L -function $L(s, f \times f)$, which then factors as $\zeta(s)L(s, \mathrm{sym}^2 f)$.

We study convolutions of families of Dirichlet L -functions as well as L -functions associated to cuspidal newforms and elliptic curves. The phenomena we find is that the second moment of the convolution is essentially the product of the moments of the constituent families. However, this does not necessarily enable us to detect a bias in the convolved family, especially if one of the biases is very small. We encounter this scenario in Theorem 6.2.

We describe the families we study. We first consider the convolution of two families of nontrivial Dirichlet characters, say $\mathcal{D}_{q_1}, \mathcal{D}_{q_2}$, where the levels q_1, q_2 are prime. Since the Satake parameters of these families are the Dirichlet characters, the Dirichlet coefficients of the convolution of these families, denoted by $\mathcal{D}_{q_1} \times \mathcal{D}_{q_2}$, are $\chi_1 \chi_2$, for $\chi_1 \in \mathcal{D}_{q_1}, \chi_2 \in \mathcal{D}_{q_2}$. We define the second moment of this family as

$$M_2(\mathcal{D}_{q_1} \times \mathcal{D}_{q_2}, X) = \frac{1}{\pi(X)} \sum_{p \leq X} \frac{1}{(q_1 - 2)(q_2 - 2)} \sum_{\substack{\chi_1 \in \mathcal{D}_{q_1} \\ \chi_2 \in \mathcal{D}_{q_2}}} \chi_1^2(p) \chi_2^2(p). \quad (6.3)$$

We prove the following bias result for this convolution (see (4.1) for the definition of $E(X, q, a)$).

Theorem 6.1. *Let $\mathcal{D}_{q_1}, \mathcal{D}_{q_2}$ be two families of nontrivial Dirichlet characters of distinct prime levels q_1, q_2 with $q_1 \not\equiv \pm 1 \pmod{q_2}, q_2 \not\equiv \pm 1 \pmod{q_1}$. Assuming the Generalized Riemann Hypothesis, the second moment of the convolved family $\mathcal{D}_{q_1} \times \mathcal{D}_{q_2}$ has main term $\frac{1}{(q_1-2)(q_2-2)}$ and lower order term*

$$\frac{1}{(q_1 - 2)(q_2 - 2)} \frac{\sqrt{X}}{\pi(X) \log X} (E_1(X, q_1, q_2) - E_2(X, q_1, q_2))$$

where

$$E_1(X, q_1, q_2) := E(X, q_1 q_2, 1) + E(X, q_1 q_2, -1) + E(X, q_1 q_2, r_3) + E(X, q_1 q_2, r_4), \quad (6.4)$$

with r_3, r_4 being the unique residues satisfying $r_3 \equiv 1 \pmod{q_1}, r_3 \equiv -1 \pmod{q_2}, r_4 \equiv -1 \pmod{q_1}, r_4 \equiv 1 \pmod{q_2}$, and

$$E_2(X, q_1, q_2) := E(X, q_1, 1) + E(X, q_1, -1) + E(X, q_2, 1) + E(X, q_2, -1). \quad (6.5)$$

Additionally assuming GSH, as $X \rightarrow \infty$ the bias is sometimes positive and sometimes negative depending on q_1, q_2 (and on a logarithmic scale each happens a positive percentage of the time).

In the convolution of families of Dirichlet L -functions and cuspidal newforms, as before we allow the level for the newforms to grow. We consider the family of nontrivial Dirichlet characters \mathcal{D}_{q_1} with prime level q_1 and the family

$$\mathcal{F}_{r,X,\delta,q_2} = \bigcup_{k < X^\delta} \text{Sym}^r [H_{k,q_2}^*(\chi_0)] \quad (6.6)$$

for prime level q_2 and $\delta > 0$. In taking the convolution $\mathcal{D}_{q_1} \times \mathcal{F}_{r,X,\delta,q_2}$ of these families, we find that the Dirichlet coefficients have the form $\chi(p)\lambda_{\text{Sym}^r f}(p)$ for $\chi \in \mathcal{D}_{q_1}, f \in H_{k,q_2}^*(\chi_0)$. For $\sigma > 0$, we define

$$\begin{aligned} M_{2,p}(\mathcal{D}_{q_1} \times \mathcal{F}_{r,X,\delta,q_2}) &= \frac{1}{q_1 - 2} \frac{1}{\sum_{k < X^\delta}^* \dim H_{k,q_2}^*(\chi_0)} \sum_{k < X^\delta}^* \sum_{\substack{\chi \in \mathcal{D}_{q_1} \\ f \in H_{k,q_2}^*(\chi_0)}} \chi^2(p) \lambda_{\text{Sym}^r f}^2(p) \\ M_{2,\sigma}(\mathcal{D}_{q_1} \times \mathcal{F}_{r,X,\delta}) &= \lim_{q_2 \rightarrow \infty} \frac{1}{\pi(X^\sigma)} \sum_{\substack{p \leq X^\sigma \\ p \neq q_2}} M_{2,p}(\mathcal{D}_{q_1} \times \mathcal{F}_{r,X,\delta,q_2}), \end{aligned} \quad (6.7)$$

where as before $*$ indicates that the sum is taken over even k . For this family, we prove the following bias result.

Theorem 6.2. *Let \mathcal{D}_{q_1} be the family of nontrivial Dirichlet characters of prime level q_1 and let $\mathcal{F}_{r,X,\delta,q_2}$ be the family of the r^{th} symmetric lifts of cuspidal newforms with even weight $k < X^\delta$ and prime level q_2 . Assuming GRH and $\delta > \sigma$, the second moment of the convolved family $\mathcal{D}_{q_1} \times \mathcal{F}_{r,X,\delta,q_2}$ as $q_2 \rightarrow \infty$ has main term $\frac{1}{q_1 - 2}$ and lower order terms*

$$\frac{1}{(q_1 - 2)\pi(X^\sigma)} \left(\frac{\sqrt{X^\sigma}}{\log X^\sigma} (E(X^\sigma, q_1, 1) + E(X^\sigma, q_1, -1)) + \log \log X^\sigma \right) + O_{q_1,r}(1/\pi(X^\sigma)), \quad (6.8)$$

where the subscripts denote that the implied constant depends on q_1, r .

Unfortunately, with the second moment expressed in the above form, we do not know how to say anything precise about the sign or size of the leading lower order term.

We may also convolve families of cuspidal newforms with each other, allowing the levels to grow. We consider families of cuspidal newforms

$$\mathcal{F}_{r_1,X,\delta_1,q_1} = \bigcup_{k_1 < X^{\delta_1}} \text{Sym}^{r_1} [H_{k_1,q_1}^*(\chi_0)], \quad \mathcal{F}_{r_2,X,\delta_2,q_2} = \bigcup_{k_2 < X^{\delta_2}} \text{Sym}^{r_2} [H_{k_2,q_2}^*(\chi_0)], \quad (6.9)$$

where the family $\mathcal{F}_{r_1,X,\delta_1,q_1} \times \mathcal{F}_{r_2,X,\delta_2,q_2}$ has Dirichlet coefficients given by $\lambda_{\text{Sym}^{r_1} f_1}(p)\lambda_{\text{Sym}^{r_2} f_2}(p)$ for $f_1 \in H_{k_1,q_1}^*(\chi_0), f_2 \in H_{k_2,q_2}^*(\chi_0)$. We take the p -local second moment of the convolved family,

$M_{2,p}(\mathcal{F}_{r_1,X,\delta_1,q_1} \times \mathcal{F}_{r_2,X,\delta_2,q_2})$ to be

$$\left(\sum_{k_1 < X^{\delta_1}}^* \dim H_{k_1,q_1}^*(\chi_0) \sum_{k_2 < X^{\delta_2}}^* \dim H_{k_2,q_2}^*(\chi_0) \right)^{-1} \sum_{k_1 < X^{\delta_1}} \sum_{k_2 < X^{\delta_2}} \sum_{\substack{f_1 \in H_{k_1,q_1}^*(\chi_0) \\ f_2 \in H_{k_2,q_2}^*(\chi_0)}} \lambda_{\text{Sym}^{r_1} f_1}^2(p) \lambda_{\text{Sym}^{r_2} f_2}^2(p), \quad (6.10)$$

and

$$M_{2,\sigma}(\mathcal{F}_{r_1,X,\delta_1} \times \mathcal{F}_{r_2,X,\delta_2}) = \lim_{q_1, q_2 \rightarrow \infty} \frac{1}{\pi(X^\sigma)} \sum_{\substack{p \leq X^\sigma \\ p \neq q_1, q_2}} M_{2,p}(\mathcal{F}_{r_1,X,\delta_1,q_1} \times \mathcal{F}_{r_2,X,\delta_2,q_2}). \quad (6.11)$$

For this convolution, we derive the following bias result.

Theorem 6.3. *Let $\mathcal{F}_{r_1,X,\delta_1,q_1}, \mathcal{F}_{r_2,X,\delta_2,q_2}$ be families of r_1^{th} and r_2^{th} symmetric lifts of cuspidal newforms with even weights $k_1 < X^{\delta_1}, k_2 < X^{\delta_2}$ and square-free distinct levels q_1, q_2 . Assuming that $\sigma < \min(\delta_1, \delta_2)$, we have*

$$M_{2,\sigma}(\mathcal{F}_{r_1,X,\delta_1} \times \mathcal{F}_{r_2,X,\delta_2}) = 1 + \frac{2 \log \log X^\sigma}{\pi(X^\sigma)} + O(X^{-\sigma} \log X^\sigma), \quad (6.12)$$

which has positive bias.

6.1. Proof of Theorem 6.1. We ignore the normalization factors for now, as they are easily incorporated later. The quantity of primary interest is

$$\sum_{p \leq X} \sum_{\substack{\chi_1 \in \mathcal{D}_{q_1} \\ \chi_2 \in \mathcal{D}_{q_2}}} \chi_1^2(p) \chi_2^2(p) = \sum_{p \leq X} \left(\sum_{\chi_1 \in \mathcal{D}_{q_1}} \chi_1^2(p) \right) \left(\sum_{\chi_2 \in \mathcal{D}_{q_2}} \chi_2^2(p) \right), \quad (6.13)$$

which orthogonality relations from (4.7) allow us to rewrite as

$$\sum_{\substack{p \leq X \\ p \equiv \pm 1(q_1) \\ p \equiv \pm 1(q_2)}} (q_1 - 1)(q_2 - 1) - \sum_{\substack{p \leq X \\ p \equiv \pm 1(q_1)}} (q_1 - 1) - \sum_{\substack{p \leq X \\ p \equiv \pm 1(q_2)}} (q_2 - 1) + \sum_{p \leq X} 1. \quad (6.14)$$

Now, the definition of $E(X, q, a)$, given in (4.1), allows us to simplify this further as

$$\pi(X) + \frac{\sqrt{X}}{\log X} (E_1(X, q_1, q_2) - E_2(X, q_1, q_2)) \quad (6.15)$$

with E_1, E_2 as defined in the statement of Theorem 6.1. Now, given $q_2 \not\equiv 1 \pmod{q_1}$,

$$\begin{aligned}
E(X, q_1, 1) &= \frac{1}{q_2 - 1} (\varphi(q_1 q_2) \pi(X, q_1, 1) - (q_2 - 1) \pi(X)) \frac{\log X}{\sqrt{X}} \\
&= \frac{1}{q_2 - 1} \left(\varphi(q_1 q_2) \left(\sum_{\substack{0 \leq k < q_2 \\ k q_1 \not\equiv -1 \pmod{q_2}}} \pi(X, q_1 q_2, 1 + k q_1) \right) - (q_2 - 1) \pi(X) \right) \frac{\log X}{\sqrt{X}} \\
&= \frac{1}{q_2 - 1} \sum_{\substack{0 \leq k < q_2 \\ k q_1 \not\equiv -1 \pmod{q_2}}} E(X, q_1 q_2, 1 + k q_1), \tag{6.16}
\end{aligned}$$

where we ignore the value of k that satisfies $k q_1 \equiv -1 \pmod{q_2}$ since in that case $\pi(X, q_1 q_2, 1 + k q_1)$ counts primes that are necessarily divisible by q_2 , since if $q_2 \mid 1 + k q_1$ then $p \equiv 1 + k q_1 \pmod{q_1 q_2}$ means that $q_2 \mid p$, and so $p = q_2$. However, we assumed that q_2 is not congruent to 1 $\pmod{q_1}$, and so there are no primes counted by $\pi(X, q_1 q_2, 1 + k q_1)$ in this case.

We can compare $E(X, q_1, 1)$ and $E(X, q_1 q_2, 1)$. The former is an average of values, one of which is precisely $E(X, q_1 q_2, 1)$; analogous calculations can be done to compare $E(X, q_1, -1)$ and $E(X, q_1 q_2, -1)$ and the other two pairs of terms. Writing everything over the denominator $q_2 - 1$, it becomes clear that if the four residue classes (modulo $q_1 q_2$) with the most primes correspond to the terms in E_1 , then the bias is positive; on the other hand, those residue classes can be those with the fewest primes, yielding a negative bias. \square

6.2. Proof of Theorem 6.2. We separate the calculation into several steps, starting with $M_{2,p}(\mathcal{D}_{q_1} \times \mathcal{F}_{r,X,\delta,q_2})$. Note that in

$$\begin{aligned}
&M_{2,p}(\mathcal{D}_{q_1} \times \mathcal{F}_{r,X,\delta,q_2}) \\
&= \frac{1}{q_1 - 2} \frac{1}{\sum_{k < X^\delta}^* \dim H_{k,q_2}^*(\chi_0)} \sum_{k < X^\delta}^* \left(\sum_{\chi \in \mathcal{D}_{q_1}} \chi^2(p) \right) \left(\sum_{f \in H_{k,q_2}^*(\chi_0)} \lambda_{\text{Sym}^r f}^2(p) \right) \tag{6.17}
\end{aligned}$$

the sum $\sum_{\chi \in \mathcal{D}_{q_1}} \chi^2(p)$ has no dependence on k . Applying the Petersson formula in Proposition 5.3 (since we assume $p \neq q_2$) and expanding, we find

$$\begin{aligned}
\sum_{k < X^\delta}^* \sum_{f \in H_{k,q_2}^*(\chi_0)} \lambda_{\text{Sym}^r f}^2(p) &= \sum_{k < X^\delta}^* \sum_{f \in H_{k,q_2}^*(\chi_0)} \sum_{\ell=0}^r \lambda_f(p^{2\ell}) \\
&= \varphi(q_2) \sum_{k < X^\delta}^* \sum_{\ell=0}^r \left[\frac{k-1}{12} p^{-\ell} + O(p^{\frac{\ell}{3}} k^{\frac{2}{3}} q_2^{\frac{2}{3}} / \varphi(q_2)) \right]. \tag{6.18}
\end{aligned}$$

Gathering the error terms, we can write this as

$$\varphi(q_2) \left(\sum_{k < X^\delta}^* \frac{k-1}{12} \right) \left(\sum_{\ell=0}^r p^{-\ell} \right) + O\left(r p^{\frac{r}{3}} X^{\frac{5\delta}{3}} q_2^{\frac{2}{3}} \right). \tag{6.19}$$

To normalize by $\sum_{k < X^\delta}^* \dim H_{k,q_2}^*(\chi_0)$, we recall our earlier calculation which showed the ratio of the sum $\varphi(q_2)(k-1)/12$ over even weight $k < X^\delta$ to the sum $\sum_{k < X^\delta}^* \dim H_{k,q_2}^*(\chi_0)$ is

$$\frac{X^{2\delta}/48 + O(X^\delta)}{X^{2\delta}/48 + O(X^{5\delta/3}q_2^{2/3}/\varphi(q_2))} = 1 + O\left(X^{-\delta} + X^{-\delta/3}q_2^{-1/3}\right). \quad (6.20)$$

Thus, we have that $M_{2,p}(\mathcal{D}_{q_1} \times \mathcal{F}_{r,X,\delta,q_2})$ is

$$\frac{1}{q_1 - 2} \left(\sum_{\chi \in \mathcal{D}_{q_1}} \chi^2(p) \right) \left[\left(\sum_{\ell=0}^r p^{-\ell} \right) \left(1 + O\left(X^{-\delta} + X^{-\frac{\delta}{3}}q_2^{-\frac{1}{3}}\right) \right) + O\left(\frac{rp^{\frac{r}{3}}X^{-\frac{\delta}{3}}q_2^{\frac{2}{3}}}{\varphi(q_2)}\right) \right], \quad (6.21)$$

where we also divide the error term by $\varphi(q_2)X^{2\delta}$. Now, summing over primes, we consider the sum of one of the error terms

$$\sum_{\substack{p \leq X^\sigma \\ p \neq q_2}} \left(\sum_{\chi \in \mathcal{D}_{q_1}} \chi^2(p) \right) O(rp^{\frac{r}{3}}X^{-\frac{\delta}{3}}q_2^{\frac{2}{3}}/\varphi(q_2)) = O\left(\phi(q_1)rX^{\frac{(r+3)\sigma-\delta}{3}}q_2^{-\frac{1}{3}}\right), \quad (6.22)$$

where we again use the fact that $\varphi(q_2) = q_2 - 1$ for q_2 prime. The main terms are given by

$$\frac{1}{q_1 - 2} (1 + O(X^{-\delta} + X^{-\delta/3}q_2^{-1/3})) \sum_{\substack{p \leq X^\sigma \\ p \neq q_2}} \left(\sum_{\chi \in \mathcal{D}_{q_1}} \chi^2(p) \right) \left(\sum_{\ell=0}^r p^{-\ell} \right), \quad (6.23)$$

and splitting the sum over ℓ we write the nested sums as

$$\sum_{\substack{p \leq X^\sigma \\ p \equiv \pm 1(q_1) \\ p \neq q_2}} (q_1 - 1) - \sum_{\substack{p \leq X^\sigma \\ p \neq q_2}} 1 + \sum_{\substack{p \leq X^\sigma \\ p \neq q_2}} \left(\sum_{\chi \in \mathcal{D}_{q_1}} \chi^2(p) \right) \left(\sum_{\ell=1}^r p^{-\ell} \right). \quad (6.24)$$

The restriction $p \neq q_2$ changes the above sums by at most a constant, and q_1 is fixed, so we can rewrite the above in terms of $E(X^\sigma, q_1, 1)$ and $E(X^\sigma, q_1, -1)$ as in the case of Dirichlet L -functions:

$$\begin{aligned} \pi(X^\sigma) + \frac{\sqrt{X^\sigma}}{\log X^\sigma} (E(X^\sigma, q_1, 1) + E(X^\sigma, q_1, -1)) + (q_1 - 1) \sum_{\substack{p \leq X^\sigma \\ p \equiv \pm 1(q_1)}} \frac{1}{p} - \sum_{p \leq X^\sigma} \frac{1}{p} + O(r + q_1 + q_1 r) \\ = \pi(X^\sigma) + \frac{\sqrt{X^\sigma}}{\log X^\sigma} (E(X^\sigma, q_1, 1) + E(X^\sigma, q_1, -1)) + \log \log X^\sigma + O_{q_1,r}(1), \end{aligned} \quad (6.25)$$

where we use the well-known corollary of the Prime Number Theorem for arithmetic progressions,

$$\sum_{\substack{p \leq X^\sigma \\ p \equiv a \pmod{q_1}}} \frac{1}{p} = \frac{\log \log X^\sigma}{\varphi(q_1)} + O(\phi(q_1)). \quad (6.26)$$

Thus, the second moment $M_{2,\sigma}(\mathcal{D}_{q_1} \times \mathcal{F}_{r,X,\delta})$ is

$$\begin{aligned} \lim_{q_2 \rightarrow \infty} \frac{1}{q_1 - 2} \frac{(1 + O(X^{-\delta} + X^{-\delta/3} q_2^{-1/3}))}{\pi(X^\sigma)} \left(\pi(X^\sigma) + \frac{\sqrt{X^\sigma}}{\log X^\sigma} (E(X^\sigma, q_1, 1) + E(X^\sigma, q_1, -1)) \right. \\ \left. + \log \log X^\sigma + O_{q_1,r}(1) + O\left(\phi(q_1) r X^{\frac{(r+3)\sigma-\delta}{3}} q_2^{-\frac{1}{3}}\right) \right). \end{aligned} \quad (6.27)$$

The main term is $1/(q_1 - 2)$, and as $q_2 \rightarrow \infty$ we find that $O(X^{-\delta} + X^{-\delta/3} q_2^{-1/3})$ goes to $O(X^{-\delta})$ and $O(\phi(q_1) r X^{\frac{(r+3)\sigma-\delta}{3}} q_2^{-1/3})$ vanishes since the implied constants are absolute. We are left with

$$\begin{aligned} \frac{1 + O(X^{-\delta})}{(q_1 - 2)\pi(X^\sigma)} \left(\pi(X^\sigma) + \frac{\sqrt{X^\sigma}}{\log X^\sigma} (E(X^\sigma, q_1, 1) + E(X^\sigma, q_1, -1)) + \log \log X^\sigma + O_{q_1,r}(1) \right) \\ = \frac{1}{q_1 - 2} + \frac{1}{(q_1 - 2)\pi(X^\sigma)} \left(\frac{\sqrt{X^\sigma}}{\log X^\sigma} (E(X^\sigma, q_1, 1) + E(X^\sigma, q_1, -1)) + \log \log X^\sigma \right) \\ + O_{q_1,r}(X^{-\delta} + \pi(X^\sigma)^{-1}). \end{aligned} \quad (6.28)$$

To conclude, we note that since $\delta > \sigma$, the error term $O_{q_1,r}(X^{-\delta} + \pi(X^\sigma)^{-1})$ can be consolidated as $O_{q_1,r}(1/\pi(X^\sigma))$. \square

6.3. Proof of Theorem 6.3. In the p -local second moment $M_{2,p}(\mathcal{F}_{r_1,X,\delta_1,q_1} \times \mathcal{F}_{r_2,X,\delta_2,q_2})$, the entire expression factors as

$$\prod_{i=1}^2 \left(\frac{1}{\sum_{k_i < X^{\delta_i}}^* \dim H_{k_i,q_i}^*(\chi_0)} \sum_{k_i < X^{\delta_i}}^* \sum_{f_i \in H_{k_i,q_i}^*(\chi_0)} \lambda_{\text{Sym}^{r_i} f_i}^2(p) \right), \quad (6.29)$$

and applying the Petersson formula yields, that the above is equal to

$$\prod_{i=1}^2 \left(\frac{\varphi(q_i)}{\sum_{k_i < X^{\delta_i}}^* \dim H_{k_i,q_i}^*(\chi_0)} \sum_{k_i < X^{\delta_i}}^* \frac{k_i - 1}{12} \sum_{\ell_i=0}^{r_i} [p^{-\ell_i} + O(p^{\frac{\ell_i}{3}} k_i^{-\frac{1}{3}} q_i^{\frac{2}{3}} / \varphi(q_i))] \right). \quad (6.30)$$

Continuing the calculations analogously to the proof of Theorem 5.1, we find that it suffices to calculate the leading terms of

$$\frac{1 + O(X^{-\delta_1} + X^{-\delta_2})}{\pi(X^\sigma)} \sum_{\substack{p \leq X^\sigma \\ p \neq q_1, q_2}} \left(\sum_{\ell_1=0}^{r_1} p^{-\ell_1} \right) \left(\sum_{\ell_2=0}^{r_2} p^{-\ell_2} \right). \quad (6.31)$$

We claim those are

$$\frac{1 + O(X^{-\delta_1} + X^{-\delta_2})}{\pi(X^\sigma)} \left(\sum_{\substack{p \leq X^\sigma \\ p \neq q_1, q_2}} 1 + \frac{2}{p} \right) = (1 + O(X^{-\delta_1} + X^{-\delta_2})) \left(1 + \frac{2 \log \log X^\sigma}{\pi(X^\sigma)} + O\left(\frac{1}{\pi(X^\sigma)}\right) \right). \quad (6.32)$$

It is trivial to bound the other terms from

$$\sum_{\substack{p \leq X^\sigma \\ p \neq q_1, q_2}} \left(\sum_{\ell_1=0}^{r_1} p^{-\ell_1} \right) \left(\sum_{\ell_2=0}^{r_2} p^{-\ell_2} \right) \quad (6.33)$$

other than the term $\sum_{p \leq X^\sigma} (1 + \frac{2}{p})$ by $O(1)$, and so we conclude that as long as $\sigma < \min(\delta_1, \delta_2)$, the leading error term will be $\frac{2 \log \log X^\sigma}{\pi(X^\sigma)}$, yielding the claimed bias. \square

7. CONCLUSION

The motivation of this paper is to understand how the finer arithmetic of families of L -functions affect the distribution of the zeros near the central point. The Katz-Sarnak Density Conjecture [KaSa1, KaSa2] has been verified for many families for suitably restricted test functions, but these results only concern the main term. Similar to the work of Rudnick and Sarnak [RudSa], who showed that the universality in the n -level correlations comes from the universality in the main term of moments of the Satake parameters, the main term of the moments of the Satake parameters also leads to the small number of observed main terms for the n -level densities (specifically, unitary, symplectic and orthogonal behavior). Differences in families are not seen in the main terms in these statistics; however, we can observe differences in behavior arising from lower order terms in these moments.

In this paper we look at several families. The most interesting are the one-parameter elliptic curves, where a negative bias is always seen in the second moments. This has implications for the distribution of zeros; in particular, it leads to a small correction term which helps explain some of the observed “excess rank” in families with small conductors. We hope that this will encourage further work studying whether similar negative biases exist in general for other families. If the negative biases persist, it is natural to wonder if there is a deeper explanation for this phenomenon.

APPENDIX A. SECOND MOMENTS OF LINEAR ELLIPTIC CURVE FAMILIES

A.1. Family $\mathcal{E}(T) : y^2 = (ax^2 + bx + c)(dx + e + T)$.

Proposition A.1. *The one-parameter family*

$$\mathcal{E}(T) : y^2 = (ax^2 + bx + c)(dx + e + T) \quad (\text{A.1})$$

with $p > 3$ prime, $a, b, c, d, e \in \mathbb{Z}$ and $p \nmid a, d$ has vanishing first moment, hence rank zero, and second moment given by

$$A_{2,\mathcal{E}}(p) = \begin{cases} p^2 - \left(1 + \left(\frac{b^2 - 4ac}{p}\right)\right) p - 1 & \text{if } p \nmid b^2 - 4ac \\ p - 1 & \text{if } p \mid b^2 - 4ac. \end{cases} \quad (\text{A.2})$$

Proof. We have $P(x) = ax^2 + bx + c$ and $Q(x) = P(x)(dx + e)$. Substituting into (2.4),

$$\begin{aligned}
A_{2,\mathcal{E}}(p) &= p \left[\sum_{P(x) \equiv 0} \left(\frac{Q(x)}{p} \right) \right]^2 - \left[\sum_{x \equiv y} \left(\frac{P(x)}{p} \right) \right]^2 + p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) \\
&= p \cdot 0 - \left[\left(\frac{a}{p} \right) \cdot \begin{cases} -1 & \text{if } p \nmid b^2 - 4ac \\ p-1 & \text{if } p \mid b^2 - 4ac \end{cases} \right]^2 + p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) \\
&= \begin{cases} -1 & \text{if } p \nmid b^2 - 4ac \\ -(p-1)^2 & \text{if } p \mid b^2 - 4ac \end{cases} + p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) \tag{A.3}
\end{aligned}$$

since $p \nmid a$. Note that $\Delta(x, y) = (P(y)Q(x) - P(x)Q(y))^2 \equiv 0$ if and only if $P(x) \equiv 0, P(y) \equiv 0$, or $x \equiv y$, since

$$\begin{aligned}
P(y)Q(x) - P(x)Q(y) &= (ax^2 + bx + c)(ay^2 + by + c)[(dx + e) - (dy + e)] \\
&= P(x)P(y)d(x - y). \tag{A.4}
\end{aligned}$$

Thus the sum over $\Delta(x, y) \equiv 0$ becomes

$$\begin{aligned}
\sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) &= \sum_{x \equiv y} \left(\frac{P(x)P(y)}{p} \right) = \sum_{x \equiv y} \left(\frac{P(x)}{p} \right)^2 \\
&= p - \#\{\alpha : P(\alpha) \equiv 0 \pmod{p}\}. \tag{A.5}
\end{aligned}$$

Then since $\#\{\alpha : P(\alpha) \equiv 0 \pmod{p}\} = 1 + \left(\frac{b^2 - 4ac}{p} \right)$, we have

$$\begin{aligned}
A_{2,\mathcal{E}}(p) &= \begin{cases} -1 & \text{if } p \nmid b^2 - 4ac \\ -(p-1)^2 & \text{if } p \mid b^2 - 4ac \end{cases} + p \left(p - \left(1 + \left(\frac{b^2 - 4ac}{p} \right) \right) \right) \\
&= \begin{cases} p^2 - \left(1 + \left(\frac{b^2 - 4ac}{p} \right) \right) p - 1 & \text{if } p \nmid b^2 - 4ac \\ p - 1 & \text{if } p \mid b^2 - 4ac \end{cases} \tag{A.6}
\end{aligned}$$

as claimed. \square

A.2. Family $\mathcal{E}(T) : y^2 = x(ax^2 + bx + c + dTx)$.

Proposition A.2. *The family*

$$\mathcal{E}(T) : y^2 = x(ax^2 + bx + c + dTx) \tag{A.7}$$

with $p > 3$ prime, $a, b, c, d \in \mathbb{Z}$ and $p \nmid a, d$ has vanishing first moment, hence rank zero, and second moment given by

$$A_{2,\mathcal{E}}(p) = \begin{cases} p^2 - 2p - 1 & \text{if } p \nmid c \\ p - 1 & \text{if } p \mid c. \end{cases} \tag{A.8}$$

Proof. We have $P(x) = dx^2$ and $Q(x) = x(ax^2 + bx + c)$. Substituting into (2.4),

$$\begin{aligned}
A_{2,\mathcal{E}}(p) &= p \left[\sum_{P(x) \equiv 0} \left(\frac{Q(x)}{p} \right) \right]^2 - \left[\sum_{x \equiv 0} \left(\frac{P(x)}{p} \right) \right]^2 + p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) \\
&= p \cdot 0 - (p-1)^2 + p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right). \tag{A.9}
\end{aligned}$$

Note that $\Delta(x, y) \equiv 0$ if and only if $x \equiv 0$, $y \equiv 0$, $x \equiv y$, or $axy \equiv c$ since

$$\begin{aligned}
P(y)Q(x) - P(x)Q(y) &= dxy[ay(ax^2 + bx + c) - x(ay^2 + by + c)] \\
&= dxy(x - y)(axy - c). \tag{A.10}
\end{aligned}$$

But $P(x)P(y) \equiv 0$ when $xy \equiv 0$, so by inclusion-exclusion we have

$$\begin{aligned}
\sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) &= \left(\sum_{x \equiv y \not\equiv 0} + \sum_{\substack{axy \equiv c \\ x, y \not\equiv 0}} - \sum_{\substack{ax^2 \equiv c \\ x \not\equiv 0 \text{ and } x \equiv y}} \right) \left(\frac{P(x)P(y)}{p} \right) \\
&= \sum_{x \not\equiv 0} \left(\left(\frac{P(x)}{p} \right)^2 + \left(\frac{P(x)P(c/ax)}{p} \right) \right) - 2 \left(\frac{d(c/a)^2}{p} \right)^2 \\
&= \sum_{x \not\equiv 0} \left(\left(\frac{dx^2}{p} \right)^2 + \left(\frac{(cd/a)^2}{p} \right) \right) - 2 \left(\frac{c^2}{p} \right) = \sum_{x \not\equiv 0} \left(1 + \left(\frac{c^2}{p} \right) \right) - 2 \left(\frac{c^2}{p} \right) \\
&= (p-1) \left(1 + \left(\frac{c^2}{p} \right) \right) - 2 \left(\frac{c^2}{p} \right) \tag{A.11}
\end{aligned}$$

by the assumption $p \nmid a, d$. Hence we obtain

$$A_{2,\mathcal{E}}(p) = -p^2 + 2p - 1 + p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) = (p^2 - 3p) \left(\frac{c^2}{p} \right) + p - 1. \tag{A.12}$$

This gives the result. \square

A.3. Family $\mathcal{E}(T) : y^2 = x(ax + b)(cx + d + Tx)$.

Proposition A.3. *The one-parameter family*

$$\mathcal{E}(T) : y^2 = x(ax + b)(cx + d + Tx) \tag{A.13}$$

with $p > 3$ prime, $a, b, c, d \in \mathbb{Z}$ and $p \nmid a, d$ has vanishing first moment, hence rank zero, and second moment given by

$$A_{2,\mathcal{E}}(p) = \begin{cases} p^2 - 2p - 1 & \text{if } p \nmid b \\ p^2 - p & \text{if } p \mid b. \end{cases} \tag{A.14}$$

Proof. We have $P(x) = x^2(ax + b)$ and $Q(x) = x(ax + b)(cx + d)$. Noting that $P(x) \equiv 0$ implies $Q(x) \equiv 0$, and $\sum_{x \equiv 0} \left(\frac{P(x)}{p} \right) = \sum_{x \not\equiv 0} \left(\frac{ax+b}{p} \right) = -\left(\frac{b}{p} \right)$ by Lemma 2.1. Then substituting into

(2.4), we have

$$\begin{aligned}
A_{2,\mathcal{E}}(p) &= p \left[\sum_{P(x) \equiv 0} \left(\frac{Q(x)}{p} \right) \right]^2 - \left[\sum_{x \equiv 0} \left(\frac{P(x)}{p} \right) \right]^2 + p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) \\
&= p \cdot 0 - \left(\frac{b}{p} \right)^2 + p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right). \tag{A.15}
\end{aligned}$$

Note that $\Delta(x, y) \equiv 0$ if and only if $x \equiv 0, y \equiv 0, ax \equiv -b, ay \equiv -b$, or $x \equiv y$ since

$$\begin{aligned}
P(y)Q(x) - P(x)Q(y) &= xy(ax + b)(ay + b)(y(cx + d) - x(cy + d)) \\
&= xy(ax + b)(ay + b)d(y - x). \tag{A.16}
\end{aligned}$$

All cases except $x \equiv y$ imply $P(x)P(y) \equiv 0$, so

$$\begin{aligned}
\sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) &= \sum_{x \equiv y} \left(\frac{P(x)P(y)}{p} \right) = \sum_{x \equiv 0} \left(\frac{P(x)}{p} \right)^2 = \sum_{x \not\equiv 0} \left(\frac{ax + b}{p} \right)^2 \\
&= \sum_{x \equiv 0} \left(\frac{ax + b}{p} \right)^2 - \left(\frac{b}{p} \right)^2 = p - 1 - \left(\frac{b^2}{p} \right), \tag{A.17}
\end{aligned}$$

recalling $p \nmid a$. Hence plugging back in, we obtain

$$A_{2,\mathcal{E}}(p) = p \sum_{\Delta(x,y) \equiv 0} \left(\frac{P(x)P(y)}{p} \right) - \left(\frac{b^2}{p} \right) = (p^2 - p) - (p + 1) \left(\frac{b^2}{p} \right). \tag{A.18}$$

This gives the result. \square

APPENDIX B. ADDITIONAL ELLIPTIC CURVE FAMILIES

Miller and Wu [Wu] investigated additional one-parameter, and some two-parameter, families of elliptic curves. We briefly summarize a representative sample of their results. While in Table 2 most of the families were carefully chosen so that the corresponding Legendre sums could be evaluated exactly, the last two were deliberately chosen differently in order to provide a better test of the Bias Conjecture. Note the normalization in [Wu] includes dividing the first and second moments by p to be a true average, and we set $\delta_1(p)$ to be 1 if $p \equiv 1 \pmod{4}$ and 0 otherwise in both tables below.

One-Parameter Family	Rank	$pA_{1,\mathcal{F}}(p)$	$pA_{2,\mathcal{F}}(p)$
$y^2 = x^3 - x^2 - x + t$	0	0	$p^2 - 2p - \left(\frac{-3}{p}\right)p$
$y^2 = x^3 + tx^2 + t^2$	1	-p	$p^2 - 2p - \left(\frac{-3}{p}\right)p - 1$
$y^2 = x^3 + tx^2 + tx + t^2$	1	-p	$p^2 - p - 1 - \delta_1(p)(2p)$

TABLE 2. First and second moments of some families from [Wu].

These families provide additional support for the Bias Conjecture. It is worth remembering that these families were all carefully chosen so that the resulting sums could be computed exactly; as this is not the case in general, it is quite likely that the behavior here is not representative.

As a further test, two-parameter families were studied. Unfortunately the Rosen-Silverman theorem is not available to determine the rank, and we just record the values of the first moments as for our purposes we do not need to compute the ranks (though see [Waz] for results on ranks). We report the results from [Wu] in Table 3, with $\delta_1(p)$ as before (it is 1 if $p \equiv 1 \pmod{4}$ and 0 otherwise) and $\delta_3(p) = 1$ if $p \equiv 3 \pmod{4}$ and 0 otherwise.

Two-Parameter Family	$p^2 A_{1,\mathcal{F}}(p)$	$p^2 A_{2,\mathcal{F}}(p)$
$y^2 = x^3 + tx + sx^2$	0	$p^3 - 2p^2 + p$
$y^2 = x^3 + t^2x + st^4$	0	$p^3 - 2p^2 + p - 2(p^2 - p)\left(\frac{-3}{p}\right)$
$y^2 = x^3 + sx^2 - t^2x$	0	$p^3 - p^2 - \delta_1(p)(2p^2 - 2p)$
$y^2 = x^3 + t^2x^2 + (t^3 - t^2)sx$	$-p^2$	$p^3 - 3p^2 + 3p - \delta_1(p)(2p^2 - 4p)$
$y^2 = x^3 + t^2x^2 - (s^2 - s)t^2x$	$-2p^2$	$p^3 - 3p^2 + 2p + \delta_1(p) \left(2p - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 - (s^2 - s)x}{p} \right) \left(\frac{y^3 - (s^2 - s)y}{p} \right) \right)$

TABLE 3. First and second moments from some two-parameter families from [Wu].

We thus again see a negative bias in the largest lower order term in the second-moment expansion. This should be understood in the sense of a normalized average over primes p , e.g. as in the introduction and elsewhere in the paper. For example, consider the family $y^2 = x^3 - t^2x + t^3s^2 + t^4$ appearing in the last row of Table 3. The largest lower order term of the second moment $p^2 A_{2,\mathcal{F}}(p)$ is on average negative in the sense that

$$\lim_{X \rightarrow \infty} \frac{1}{\pi(X)} \sum_{p \leq X} \frac{p^2 A_{2,\mathcal{F}}(p) - p^3}{p^2} = -2 < 0.$$

To make this calculation, compute that for $p \geq 5$ we have

$$\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right) = \begin{cases} 2 & \text{if } p \equiv 1 \pmod{12} \\ 0 & \text{if } p \equiv 7, 11 \pmod{12} \\ -2 & \text{if } p \equiv 5 \pmod{12} \end{cases}$$

and moreover note that p equidistributes among the congruence classes 1, 5, 7, 11 modulo 12 as $X \rightarrow \infty$. When $p \equiv 5 \pmod{12}$ we have $p^2 A_{2,\mathcal{F}}(p) = p^3 + p$ and the largest lower order term $+p$ is positive. However, such terms do not contribute after dividing by p^2 and averaging over p . Instead, the lower order terms of size p^2 coming from the cases $p \equiv 1, 7, 11 \pmod{12}$ dictate the average. A similar interpretation should be applied to the conclusion of Lemma B.2 below.

We now give the details for a representative calculation, that of the family $y^2 = x^3 + t^2x + st^4$. Note that we must adjust our definitions of $A_{r,\mathcal{F}}$ and divide by p^2 and not p , as we have sums over t and s modulo p .

Lemma B.1. *For $p \geq 5$, the first moment of the two-parameter family $y^2 = x^3 + t^2x + st^4$ is 0.*

Proof. The claim follows from straightforward algebra; briefly we note there is no contribution from $t = 0$, and then we can send s to $t^{-1}s \pmod{p}$, and the resulting s sum is complete and thus

zero. Explicitly,

$$\begin{aligned}
-p^2 A_{1, \mathcal{F}(p)} &= - \sum_{t(p)} \sum_{s(p)} a_{t,s}(p) = \sum_{t(p)} \sum_{x(p)} \sum_{s(p)} \left(\frac{x^3 + t^2 x + st^4}{p} \right) \\
&= \sum_{t=1}^{p-1} \sum_{x(p)} \sum_{s(p)} \left(\frac{t^3 x^3 + t^3 x + st^4}{p} \right) \\
&= \sum_{t=1}^{p-1} \sum_{x(p)} \sum_{s(p)} \left(\frac{t^3}{p} \right) \left(\frac{x^3 + x + st}{p} \right) \\
&= \sum_{x(p)} \sum_{s(p)} \sum_{t=1}^{p-1} \left(\frac{t}{p} \right) \left(\frac{st + (x^3 + x)}{p} \right) \\
&= \sum_{x(p)} \sum_{s(p)} \sum_{t=1}^{p-1} \left(\frac{t}{p} \right) \left(\frac{t^{-1} st + (x^3 + x)}{p} \right) \\
&= \sum_{x(p)} \sum_{s(p)} \sum_{t=1}^{p-1} \left(\frac{t}{p} \right) \left(\frac{s + (x^3 + x)}{p} \right). \tag{B.1}
\end{aligned}$$

□

Lemma B.2. For $p \geq 5$ the second moment times p^2 of the two-parameter family $y^2 = x^3 + t^2 x + st^4$ is $p^3 - 2p^2 + p - 2(p^2 - p)\left(\frac{-3}{p}\right)$, which supports the Bias Conjecture.

Proof. We see there is no contribution from $t = 0$, we then send x and y to tx and ty modulo p pull out a t^6 from the Legendre sums, and then send s to $t^{-1}s \bmod p$ to simplify further:

$$\begin{aligned}
p^2 A_{2, \mathcal{F}(p)} &= \sum_{t, s(p)} a_{t,s}^2(p) = \sum_{t(p)} \sum_{s(p)} \sum_{x, y(p)} \left(\frac{x^3 + t^2 x + st^4}{p} \right) \left(\frac{y^3 + t^2 y + st^4}{p} \right) \\
&= \sum_{t=1}^{p-1} \sum_{s(p)} \sum_{x, y(p)} \left(\frac{t^3 x^3 + t^3 x + st^4}{p} \right) \left(\frac{t^3 y^3 + t^3 y + st^4}{p} \right) \\
&= \sum_{t=1}^{p-1} \sum_{s(p)} \sum_{x, y(p)} \left(\frac{t^6}{p} \right) \left(\frac{x^3 + x + st}{p} \right) \left(\frac{y^3 + y + st}{p} \right) \\
&= \sum_{t=1}^{p-1} \sum_{s(p)} \sum_{x, y(p)} \left(\frac{s + (x^3 + x)}{p} \right) \left(\frac{s + (y^3 + y)}{p} \right) \\
&= (p-1) \sum_{x, y(p)} \sum_{s(p)} \left(\frac{s + (x^3 + x)}{p} \right) \left(\frac{s + (y^3 + y)}{p} \right). \tag{B.2}
\end{aligned}$$

To evaluate this sum, consider the quadratic polynomial in s given by $(s + (x^3 + x))(s + (y^3 + y))$, and write $\delta(x, y)$ for the discriminant of this quadratic. The second part of Lemma 2.1 gives

$$\sum_{s(p)} \left(\frac{s + (x^3 + x)}{p} \right) \left(\frac{s + (y^3 + y)}{p} \right) = \begin{cases} -1 & \text{if } p \nmid \delta(x, y) \\ (p-1) & \text{if } p \mid \delta(x, y). \end{cases}$$

This gives

$$p^2 A_{2, \mathcal{F}(p)} = (p-1) \left[p \left(\sum_{\substack{x, y \bmod p \\ \delta(x, y) \equiv 0(p)}} 1 \right) - p^2 \right]. \quad (\text{B.3})$$

We have thus reduced the problem to determining how often p divides

$$\delta(x, y) = [(x - y)(y^2 + xy + (1 + x^2))]^2. \quad (\text{B.4})$$

Set $\delta_1(x, y) = x - y$ and $\delta_2(x, y) = y^2 + xy + (1 + x^2)$, so that $\delta(x, y) = \delta_1(x, y)^2 \delta_2(x, y)^2$. For each δ_i , we count the number of pairs (x, y) such that $\delta_i(x, y)$ is zero modulo p , and then subtract the doubly counted pairs where both factors vanish modulo p .

Case 1: We have $\delta_1(x, y) = x - y \equiv 0 \pmod{p}$ when $x = y$; thus there are p such pairs.

Case 2: We need to count the number of solutions of $\delta_2(x, y) = y^2 + xy + (1 + x^2) \equiv 0 \pmod{p}$. By the Quadratic Formula modulo p , we have

$$y = \frac{-x \pm \sqrt{-3x^2 - 4}}{2},$$

and thus there are two solutions if $-3x^2 - 4$ is a non-zero square, one solution if it is zero modulo p , and otherwise no solutions.⁵ Thus, summing over x yields the number of pairs is

$$\sum_{x(p)} \left[1 + \left(\frac{-3x^2 - 4}{p} \right) \right] = p + \sum_{x(p)} \left(\frac{-3x^2 - 4}{p} \right) = p - \left(\frac{-3}{p} \right), \quad (\text{B.5})$$

where we used Lemma 2.1 to evaluate the quadratic sum (the discriminant is -48 , which is invertible modulo p as we assumed $p \geq 5$).

Case 3: The double-counted pairs satisfy both $x = y$ and $y^2 + xy + (1 + x^2) \equiv 0 \pmod{p}$, which means that they satisfy $3x^2 + 1 \equiv 0 \pmod{p}$, or $-3x^2 \equiv 1 \pmod{p}$. Thus, there is a double-counted solution if and only if $\left(\frac{-3}{p} \right) = 1$, and the number of double-counted pairs is $1 + \left(\frac{-3}{p} \right)$.

Therefore, the total number of pairs for $\delta(x, y) \equiv 0 \pmod{p}$ is

$$p + \left[p - \left(\frac{-3}{p} \right) \right] - \left[1 + \left(\frac{-3}{p} \right) \right] = 2p - 1 - 2 \left(\frac{-3}{p} \right). \quad (\text{B.6})$$

⁵This is why we assumed $p > 2$, so 2 is invertible modulo p .

Hence, the second moment times p^2 of the family equals

$$\begin{aligned} p^2 A_{2, \mathcal{F}(p)} &= (p-1) \left[p \left(2p-1 - 2 \left(\frac{-3}{p} \right) \right) - p^2 \right] \\ &= p^3 - 2p^2 + p - 2(p^2 - p) \left(\frac{-3}{p} \right). \end{aligned} \tag{B.7}$$

□

APPENDIX C. BIASES IN HIGHER MOMENTS

By Steven J. Miller and Yan Weng

We end with some additional results and directions for future research.

Miller and Weng recently pushed these investigations in two new directions; below we briefly summarize their findings, and refer the reader to [MWe, MWeWu] for details. First, they studied a large number of families of elliptic curves where it was not clear if there was a closed form polynomial expansion for the second moment (previous families to date were chosen because the resulting sums could be done in closed form, and thus these may not be indicative of the behavior of a generic family). By looking at the values for primes in different congruence classes, they were able to conjecture formulas for second moments and in some cases prove them, but for a typical family they found that the formula cannot be a polynomial in $p \bmod 2^a 3^b 5^c$ (unless a, b or c are quite large!). This is not surprising, as there are a few families where the second moments can be explicitly computed and are not polynomials.

Next, they looked at families with moderate rank to see if the bias is still present; all the families that can be analyzed in closed form have small rank and polynomials in the defining equations of low degree. While such families are computationally difficult to deal with for many quantities (for example, the analytic conductors grow very rapidly, making it hard to compute more than a few low-lying zeros), the bias calculations are not significantly harder than what has been done before. The reason is that the Legendre sums only involve the polynomials modulo the prime, and thus the large coefficients are immediately reduced. The difficulty is that in these families it seems that the $p^{3/2}$ term is frequently present, making it hard to see a bias in terms of size p . The data is not inconsistent with a *positive* bias for these higher rank families, indicating further study is warranted.

Their final experiment was to examine if there is a bias in the higher moments. Using the theory of modular forms, one can write down formulas involving averages of powers of the Satake parameters, but unfortunately these cannot be evaluated in closed form. Computationally, it is very difficult to see numerical biases for these moments as the conjecture states that the first lower order term that does not average to zero has a negative average; if there is a larger lower order term that does average to zero, it will drown out this bias and make it impossible to detect numerically.

Below is a summary of their main results.

- All the rank 0 and rank 1 families studied have data consistent with a negative bias in their second moment sums. However, for higher rank families (rank at least 4) the data suggests that there is instead a positive bias.
- For the fourth moment, we also believe that the rank 0 and rank 1 families have negative biases. We see this in some families; in others we see the presence of terms of size $p^{5/2}$

whose behavior is consistent with their averaging to zero, but its presence makes it impossible to detect the lower order terms. Interestingly, again for higher rank families (rank at least 4) the data is consistent with a positive bias.

- The sixth moment results are similar to the fourth moment. The results are consistent with either a negative bias, or a leading term (now of size $p^{7/2}$) averaging to zero for lower rank families. Our data also suggests that higher rank families have positive biases.
- For the odd moments, the coefficients of the leading term vary with the primes. Our data suggests that the average value of the main term for the $(2k+1)^{\text{st}}$ moment is $-C_{k+1}rp^{k+1}$, where $C_n = \frac{1}{n+1}\binom{2n}{n}$ is the n^{th} Catalan number.

REFERENCES

- [ALM] S. Arns, S. J. Miller and A. Lozano-Robledo, *Constructing elliptic curves over $\mathbb{Q}(T)$ with moderate rank*, Journal of Number Theory **123** (2007), no. 2, 388–402.
- [BKNT] J. C. Bahr, Y. H. Kim, E. Neyman, and G. K. Taylor, *On Orders of Elliptic Curves over Finite Fields*, Rose-Hulman Undergraduate Mathematics Journal **19** (2019), Iss. 1, Article 2.
- [BBDDM] O. Barrett, P. Burkhardt, J. DeWitt, R. Dorward and S. J. Miller, *One-Level density for holomorphic cusp forms of arbitrary level*, to appear in Research in Number Theory. <https://arxiv.org/pdf/1604.03224>.
- [BEW] 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.
- [CHT] L. Clozel, M. Harris and R. Taylor, *Automorphy for some ℓ -adic lifts of automorphic mod ℓ Galois representations*, Publications Mathématiques de L’IHÉS **108** (2008), no. 1, 1–181.
- [Co] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics **138**, Springer-Verlag, Berlin-New York (1996).
- [Con] J. B. Conrey, *L-Functions and random matrices*. Pages 331–352 in *Mathematics unlimited — 2001 and Beyond*, Springer-Verlag, Berlin, 2001.
- [CFKRS] B. Conrey, D. Farmer, P. Keating, M. Rubinstein and N. Snaith, *Integral moments of L-functions*, Proc. London Math. Soc. (3) **91** (2005), no. 1, 33–104.
- [CFZ1] J. B. Conrey, D. W. Farmer and M. R. Zirnbauer, *Autocorrelation of ratios of L-functions*, Commun. Number Theory Phys. **2** (2008), no. 3, 593–636.
- [CFZ2] J. B. Conrey, D. W. Farmer and M. R. Zirnbauer, *Howe pairs, supersymmetry, and ratios of random characteristic polynomials for the classical compact groups*, preprint, <http://arxiv.org/abs/math-ph/0511024>.
- [ConSn] J. B. Conrey and N. C. Snaith, *Applications of the L-functions Ratios Conjecture*, Proc. Lon. Math. Soc. **93** (2007), no 3, 594–646.
- [Dav] H. Davenport and H. L. Montgomery, *Multiplicative Number Theory*, Springer-Verlag, New York, 1980.
- [De] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.
- [DHKMS1] E. Dueñez, D. K. Huynh, J. C. Keating, S. J. Miller and N. Snaith, *The lowest eigenvalue of Jacobi Random Matrix Ensembles and Painlevé VI*, Journal of Physics A: Mathematical and Theoretical **43** (2010) 405204 (27pp).
- [DHKMS2] E. Dueñez, D. K. Huynh, J. C. Keating, S. J. Miller and N. Snaith, *Models for zeros at the central point in families of elliptic curves*, J. Phys. A: Math. Theor. **45** (2012) 115207 (32pp).
- [DuMi] E. Dueñez and S. J. Miller, *The effect of convolving families of L-functions on the underlying group symmetries*, Proceedings of the London Mathematical Society, 2009; doi: 10.1112/plms/pdp018.
- [HKLM] T. Hammonds, S. Kim, B. Logsdon and S. J. Miller, *Rank and Bias in Families of Hyperelliptic Curves via Nagao’s Conjecture*, preprint. <https://arxiv.org/abs/1906.09407>.
- [HW] G. H. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 5th edition, Oxford Science Publications, Clarendon Press, Oxford, 1995.

- [He1] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, I*, Math. Z. **1** (1918), 357–376.
- [He2] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, II*, Math. Z. **6** (1920), 11–51.
- [HM] C. Hughes and S. J. Miller, *Low lying zeros of L -functions with orthogonal symmetry*, Duke Mathematical Journal **136** (2007), no. 1, 115–172.
- [IR] K. Ireland, and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1990.
- [IK] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, AMS Colloquium Publications, Vol. 53, AMS, Providence, RI, 2004.
- [ILS] 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.
- [KaSa1] N. Katz and P. Sarnak, *Random Matrices, Frobenius Eigenvalues and Monodromy*, AMS Colloquium Publications **45**, AMS, Providence, 1999.
- [KaSa2] N. Katz and P. Sarnak, *Zeros of zeta functions and symmetries*, Bull. AMS **36**, 1999, 1 – 26.
- [KN1] M. Kazalicki and B. Naskrecki, *Second moments and the bias conjecture for the family of cubic pencils* (2020), preprint, <https://arxiv.org/pdf/2012.11306>.
- [KN2] M. Kazalicki and B. Naskrecki, *Diophantine triples and $K3$ surfaces* (2021), preprint, <https://arxiv.org/pdf/2101.11705>.
- [Kim] H. Kim, *Functoriality for the exterior square of GL_2 and the symmetric fourth of GL_2* , Jour. AMS **16** (2003), no. 1, 139–183.
- [KimSa] H. Kim and P. Sarnak, *Appendix: Refined estimates towards the Ramanujan and Selberg conjectures*, Appendix to [Kim].
- [MMRT-BW] B. Mackall, S. J. Miller, C. Rapti, C. Turnage-Butterbaugh and K. Winsor, *Some Results in the Theory of Low-lying Zeros* (with an appendix with Megumi Asada, Eva Fourakis, Kevin Yang), in Families of automorphic forms and the trace formula (editors), Simons Symposia series, Springer-Verlag.
- [MMRW] B. Mackall, S. J. Miller, C. Rapti and K. Winsor, *Lower-Order Biases in Elliptic Curve Dirichlet Coefficients in Families*, to appear in the Conference Proceedings of the Workshop on Frobenius distributions of curves at CIRM in February 2014.
- [Mic] P. Michel, *Rang moyen de famille de courbes elliptiques et lois de Sato-Tate*, Monatshefte für Mathematik **120** (1995), 127–136.
- [Mi1] S. J. Miller, *1- and 2-level densities for families of elliptic curves: evidence for the underlying group symmetries*, Princeton University, PhD thesis (2002). http://web.williams.edu/Mathematics/sjmiller/public_html/math/thesis/SJMthesis_Rev2005.pdf.
- [Mi2] 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.
- [Mi3] 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.
- [MWe] S. J. Miller and Y. Weng, *Biases in Moments of Dirichlet Coefficients of Elliptic Curve Families* (2021), <http://arxiv.org/abs/2102.02702>.
- [MWeWu] S. J. Miller, Y. Weng and J. Wu, *Biases in Moments of the Dirichlet Coefficients in One- and Two-Parameter Families of Elliptic Curves* (2021), preprint.
- [Na] K. Nagao, *$\mathbb{Q}(t)$ -rank of elliptic curves and certain limit coming from the local points*, Manuscr. Math. **92** (1997), 13–32.
- [Ri] O. Rizzo, *Average root numbers for a non-constant family of elliptic curves*, Compositio Mathematica **136** (2003), 1–23.
- [RoSi] M. Rosen and J. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133** (1998), 43–67.
- [RubSa] M. Rubinstein and P. Sarnak, *Chebyshev’s bias*, Experiment. Math. **3** (1994), no. 3, 173–197.
- [RudSa] Z. Rudnick and P. Sarnak, *Zeros of principal L -functions and random matrix theory*, Duke Math. J. **81**, 1996, 269–322.
- [SaShTe] P. Sarnak, S. W. Shin and N. Templier, *Families of L -functions and their symmetry*, in Families of automorphic forms and the trace formula (editors), Simons Symposia series, Springer-Verlag.

- [ShTe] S. W. Shin and N. Templier, *Sato-Tate theorem for families and low-lying zeros of automorphic L -functions* (with appendices by Robert Kottwitz [A] and by Raf Cluckers, Julia Gordon, and Immanuel Halupczok [B]), *Inventiones mathematicae* **203** (2016), no. 1, 1–177.
- [Wa] L. C. Washington, *Elliptic curves: Number Theory and Cryptography*, CRC Press, 2008.
- [Waz] R. Wazir, *Arithmetic on elliptic threefolds*, *Composito Mathematica* **140** (2004), 567–580.
- [Wu] J. Wu, *Biases in First and Second Moments of the Dirichlet Coefficients in One- and Two-Parameter Families of Elliptic Curves* (student research project advised by S. J. Miller), https://web.williams.edu/Mathematics/sjmillier/public_html/math/papers/WuBiasesinEllipticCurvesPaperFinal81.pdf.

Email address: maa2@williams.edu

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

Email address: rcchen@mit.edu

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, CAMBRIDGE, MA 02142

Email address: erfl@williams.edu

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

Email address: yujin.kim@cims.nyu.edu

COURANT INSTITUTE OF MATHEMATICAL SCIENCES, NEW YORK UNIVERSITY, NEW YORK, NY 10012

Email address: akwon@andrew.cmu.edu

DEPARTMENT OF MATHEMATICS, CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PA 15213

Email address: jared.d.lichtman@gmail.com

DEPARTMENT OF MATHEMATICS, DARTMOUTH COLLEGE, HANOVER, NH 03755

Email address: bmackall60@gmail.com

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

Email address: sjm1@williams.edu

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

Email address: rcwnsr@umich.edu

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

Email address: krlwnsr@umich.edu

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

Email address: jyang@colby.edu

DEPARTMENT OF MATHEMATICS, COLBY COLLEGE, WATERTOWN, ME 04901

Email address: kyang95@stanford.edu

DEPARTMENT OF MATHEMATICS, HARVARD UNIVERSITY, CAMBRIDGE, MA 02138