NUMERICAL INVESTIGATION OF LOWER ORDER BIASES IN MOMENT EXPANSIONS OF ONE PARAMETER FAMILIES OF ELLIPTIC CURVES

TIMOTHY CHEEK, PICO GILMAN, KAREEM JABER, STEVEN J. MILLER, VISMAY SHARAN, AND MARIE-HÉLÈNE TOMÉ

Abstract. For a fixed elliptic curve E without complex multiplication, $a_p \coloneqq p+1-\#E(\mathbb{F}_p)$ is $O(\sqrt{p})$ and $a_p/2\sqrt{p}$ converges to a semicircular distribution. Michel proved that for a one-parameter family of elliptic curves $y^2 = x^3 + A(T)x + B(T)$ with $A(T), B(T) \in \mathbb{Z}[T]$ and non-constant j-invariant, the second moment of $a_p(t)$ is $p^2 + O(p^{3/2})$. The size and sign of the lower order terms has applications to the distribution of zeros near the central point of Hasse-Weil L-functions and the Birch and Swinnerton-Dyer conjecture. S. J. Miller conjectured that the highest order term of the lower order terms of the second moment that does not average to zero is on average negative. Previous work on the conjecture has been restricted to a small set of highly nongeneric families. We create a database and a framework to quickly and systematically investigate biases in the second moment of any one-parameter family. When looking at families which have so far been beyond current theory, we find several potential violations of the conjecture for $p \le 250,000$ and discuss new conjectures motivated by the data.

1. Introduction

We assume the reader is familiar with elliptic curves. For detailed references, see, for example, [Sil94; Sil09]. Let $\mathcal{E} \to \mathbb{P}^1$ be a non-split elliptic surface over $\mathbb{Q}$ with Weierstrass equation

$$\mathcal{E}\colon\ y^2 \ = \ x^3 + A(T)x + B(T) \tag{1.1}$$

with $4A(T)^3 + 27B(T)^2 \neq 0$. We can take $A(T), B(T) \in \mathbb{Z}[T]$ and its j-invariant is given by

$$j(T) \ \coloneqq \ 1728\frac{4A(T)^3}{4A(T)^3 + 27B(T)^2}. \tag{1.2}$$

If $0 \le \max\{3\deg(A(T)), 2\deg(B(T))\} < 12$, then $\mathcal{E}$ is a rational surface. In addition, almost all specializations $T = t \in \mathbb{Z}$ result in an elliptic curve E_t,

$$E_t \ \coloneqq \ y^2 \ = \ x^3 + A(t)x + B(t), \tag{1.3}$$

and we say the set of all such E_t forms a one-parameter family of elliptic curves of $\mathbb{Q}$. The rank of such a family is defined to be the minimum rank r that appears infinitely often among the curves E_t in the one-parameter family. The expected value of $\#E_t(\mathbb{F}_p)$ is $p+1$ and we write $a_t(p) \coloneqq p+1-\#E_t(\mathbb{F}_p)$ for the trace of Frobenius of E_t at p. By Hasse's theorem on elliptic curves [Has36] we have that $|a_t(p)| \le 2\sqrt{p}$.

The n-th moment of the Frobenius trace of a one parameter family is defined for each prime p as

$$\mathcal{A}_{n,\mathcal{E}}(p) \ \coloneqq \ \sum_{t=0}^{p-1} a_t(p)^n.$$

Note that we do not normalize by $1/p$, so this sum is always an integer. The moments of a one-parameter family encode arithmetic properties of the family. For example, Rosen and Silverman [RS98] proved a conjecture of Nagao [Nag97] relating the first moment to the rank of an elliptic

surface: if Tate's conjecture holds for the elliptic surface $\mathcal{E}$ (e.g., when $\mathcal{E}$ is a rational surface; see [Shi72]), then

$$\lim_{X\to\infty}\frac{1}{X}\sum_{p\le X}\frac{\mathcal{A}_{1,\mathcal{E}}(p)\log p}{p} \;=\; -\text{rank}\mathcal{E}(\mathbb{Q}(T)). \tag{1.4}$$

Therefore, the rank of such a surface is determined by its first moments, and is directly related to negative bias in the values of $a_t(p)$.

Motivated by the negative bias in the first moment and its arithmetic importance, it is natural to ask if biases also exist in higher moments and if these biases are also arithmetically significant. This is the impetus for our work: we build a large database of Frobenius traces for primes up to 250,000 so that we can then easily investigate any one-parameter family, by, for example, numerically computing higher moments and attempting to isolate their lower order biases. Given more computing power, the framework we establish can easily be used to generate a larger database, and investigate higher moments.

To make our investigations precise, we recall the following asymptotic second moment expansion.

Theorem 1.1 (Michel [Mic95])**.** *Let $\mathcal{E}$ be an elliptic surface with nonconstant j-invariant. Then the second moment is of the form*

$$\mathcal{A}_{2,\mathcal{E}}(p) \;=\; p^2+O\left(p^{3/2}\right), \tag{1.5}$$

with lower order terms of size $p^{3/2}$, p, $p^{1/2}$ and 1, respectively, where each has a cohomological interpretation.

In his Ph.D. thesis [Mil02], S. J. Miller computed a closed form expression for the second moment of several carefully chosen families. Based on these computations, and motivated by biases in the first moment expansion, Miller formulated the Bias Conjecture for the second moment: the largest lower order term in the second moment expansion which does not average to 0 is on average negative. As an application, negative biases in the second moment expansion are related to low-lying zeros and thus the average rank of $\mathcal{E}$ over $\mathbb{Q}(T)$, as this latter quantity can be bounded using the density of low-lying zeros. See [Bat+24; Mil05] for a detailed discussion to the excess rank problem.

Further results confirming the Bias Conjecture have been obtained in [Asa+23; KN21; KN22; Mac+16; Mil02; Mil04; Mil05]. For instance, see [Bat+24] for a table of families with closed form first and second moment expressions as obtained by [Asa+23; Mil02; Mil05]. The majority of these calculations rely on linear and quadratic Legendre symbol identites which we briefly touch on later; the takeaway is that these calculations are only tractable for lower degree $A(T), B(T)$, although this restriction often is still not enough. However, some results have also been obtained for specially chosen cubics and quartics. For example [Bat+24] recently proved that for primes $p\equiv 2 \bmod 3$, the family $\mathcal{E}: y^2=x^3+x+T^3$ has second moment p^2+p by making use of an automorphism to lower the degree of $B(T)$. For primes $p\equiv 1 \bmod 3$, however, they were not able to find a closed form expression and the data here appears random. Of note, the overall data appears generally slightly negative; we touch more on this later. Nonetheless, this demonstrates progress towards disproving the Bias Conjecture, as a positive density of primes have positive bias.

As such, by looking at families beyond the scope of Legendre symbol identities, we already begin to see interesting behavior. The salient point is that all of the families for which we have a closed form expression are specially chosen to be parameterized by low degree polynomials $A(T)$ and $B(T)$. Hence, we do not expect them to necessarily reflect the behavior of generic families. To this end, we computationally investigate one-parameter families defined by higher degree polynomials $A(T)$ and $B(T)$ where Legendre symbol calculations are intractable and to which the results of [KN21; KN22] on cubic pencils do not apply. Our numerical work seeks to evaluate whether we expect the

Bias Conjecture to hold by investigating a more generic swath of families. To isolate the lower order bias, we compute the following normalized second moment

$$\mathcal{B}_{2,\mathcal{E}}(p) \;=\; \frac{\mathcal{A}_{2,\mathcal{E}}(p) - p^2}{p^{3/2}} \tag{1.6}$$

and take a running average over primes p. Note that if the largest lower order term which does not average to 0 is of size p or $p^{1/2}$, then isolating lower order biases is difficult due to noise from the $p^{3/2}$ term drowning out fluctuations on the order of $p^{-1/2}$. Thus studying the Bias Conjecture numerically is a challenging problem. While our investigations turn up interesting families for further study, these techniques cannot prove or disprove the Bias Conjecture and are most useful for determining where to best allocate time and effort for further theoretical study and motivating the development of conjectures. Indeed, from a theoretical point of view, higher moments are signficantly more complicated to study, yet from a computational point of view, using our database one can compute them equally as easily. Hence, our work can be used to inform hypotheses about lower order biases in higher moment expansions.

We expect our database to have many applications to computing other quantities related to the traces of Frobenius of a one-parameter family and can be used to attempt to formulate analogous Bias Conjectures for the higher moments $n \geq 3$. In Section 2, we discuss the techniques used to optimize computation and storage of the a_p values to generate a database storing data for a large number of primes. Then, in Section 3, we illustrate the utility of the database by performing an extensive family search for polynomials $A(T)$ and $B(T)$ of degree at most 5 and some of degree at most 10. We investigate whether these families have potential positive bias using two statistics, an unweighted running average of the normalized second moment and a log-weighted average of the normalized second moment. Our search found some candidates with potential positive bias for further investigation which we also detail in this section. We also numerically explored the distribution of the normalized second moment and we discuss our findings and a conjecture about the variance of these distributions which our numerical work generated in Section 4. Finally, in Section 6, we propose additional avenues for future work.

2. Creating a database of a_p values

There exists an explicit formula to compute $a_t(p)$ by calculating the number of solutions to E_t mod p using Legendre symbols. For $a \in \mathbb{F}_p$, the Legendre symbol is defined as

$$\left(\frac{a}{p}\right) \;=\; \begin{cases} 0 & a = 0, \\ 1 & a = n^2 \text{ for some } n, \\ -1 & \text{otherwise.} \end{cases} \tag{2.1}$$

Since $a_t(p) = p + 1 - \#E_t(\mathbb{F}_p)$, if $E_t : y^2 = x^3 + A(t)x + B(t)$, then for p odd we have that

$$-a_t(p) \;=\; \sum_{x=0}^{p-1} \left(\frac{x^3 + A(t)x + B(t)}{p}\right). \tag{2.2}$$

Hence the second moment can be computed as

$$\mathcal{A}_{2,\mathcal{E}}(p) \;=\; \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\sum_{w=0}^{p-1} \left(\frac{x^3 + A(t)x + B(t)}{p}\right)\left(\frac{w^3 + A(t)w + B(t)}{p}\right). \tag{2.3}$$

For the families for which Miller was able to obtain a closed form expression, switching the order of summation yielded a quadratic or linear Legendre sum which can be evaluated using the following lemma. Then, for the carefully chosen families he considered, the remaining sums were easy to evaluate.

Lemma 2.1 (Linear and Quadratic Legendre Sums)**.** *Let p be an odd prime. If $a \not\equiv 0 \bmod p$, then*

$$\sum_{t=0}^{p-1} \left(\frac{at+b}{p}\right) \;=\; 0, \tag{2.4}$$

and

$$\sum_{t=0}^{p-1} \left(\frac{at^2+bt+c}{p}\right) \;=\; \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p \mid (b^2-4ac), \\ -\left(\frac{a}{p}\right) & \text{otherwise.} \end{cases} \tag{2.5}$$

From (2.3), we compute a database of a_p for elliptic curves $E_{a,b} : y^3 = x^3 + ax + b$ for all values of $a, b \in \mathbb{F}_p$ for primes p up to some prime P. This requires both efficient algorithms to cut down computation time and efficient storage to minimize the amount of data that needs to be stored for each prime p. Naively, we need to compute p^2 values of a_p, however, in our database, we need only at most $4p + 6$ values: namely,

$$\#\text{ of } a_p \text{ stored} \;=\; \begin{cases} 4p & p \equiv 1 \bmod 4 \\ 2p & p \equiv 3 \bmod 4 \end{cases} + \begin{cases} 6 & p \equiv 1 \bmod 3 \\ 0 & p \equiv 0, 2 \bmod 3. \end{cases} \tag{2.6}$$

Using an additional optimization which we did not implement but which we detail below, one can reduce this to $2p + \theta(1)$ many a_p for all primes p. In building the database used in this paper, we take P to be the largest prime smaller than 250,000. However, our computation, storage, and look-up methods and can be extended to build a database for larger values of P and extract values of a_p for any $E_{a,b}$ corresponding to a pair of residues mod p for any prime $p \le P$ (up to limits in accurately storing large integers). The `C++` code for computing and storing the values of a_p for each p is available at [Che+24] and is contained in the file `quarticclasses.cpp`. Note that we store and compute $-a_p$ rather than a_p.

2.1. **Reduction to a smaller set of a_p's.** We take advantage of two automorphisms and Legendre symbol identities to reduce the number of a_p we need to compute and store. Since we are working over a field with characteristic zero, we write our elliptic curve with Weierstrass form $E : y^2 = x^3 + ax + b$ for some $a, b \in \mathbb{Q}$. By multiplying by an appropriate denominator, we take $a, b \in \mathbb{Z}$.

We reduce the number of a_p's necessary by working with only certain residue classes of a through a standard Weierstrass substitution. Specifically, for $\ell \in \mathbb{F}_p^\times$, we let $y = \ell^3 \tilde{y}$ and $x = \ell^2 \tilde{x}$ and we obtain

$$\ell^6 \tilde{y}^2 \;=\; \ell^6 \tilde{x}^3 + \ell^2 a \tilde{x} + b, \tag{2.7}$$

so that dividing by ℓ^6 we arrive at the elliptic curve $\tilde{E} : y^2 = x^3 + a\ell^{-4}x + b\ell^{-6}$. The elliptic curves E and $\tilde{E}$ are automorphic to one another and thus have the same number of solutions. Now, if we compute the a_p for each quartic (i.e., fourth power) residue class, we can now compute the a_p values for any elliptic curve over $\mathbb{F}_p$, i.e., it suffices to compute the values of a_p for one a in each quartic residue class. There are five quartic residue classes if $p \equiv 1 \bmod 4$ and three quartic residue classes if $p \equiv 3 \bmod 4$. In each case, one quartic residue class corresponds to $a = 0$. In the case $a = 0$, we further reduce the number of a_p that need to be computed and stored.

When $a = 0$ and $p \not\equiv 1 \bmod 3$, then $x \mapsto x^3$ is a bijection. Hence

$$\sum_{x=0}^{p-1} \left(\frac{x^3+b}{p}\right) \;=\; \sum_{x=0}^{p-1} \left(\frac{x+b}{p}\right) \;=\; 0. \tag{2.8}$$

When $a = 0$ and $p \equiv 1 \bmod 3$, it suffices to store one value of a_p for each sextic residue class of $b \bmod p$, of which there are six. Hence we have reduced to the following:

$$\#a_p \text{ we need to compute and store } = \begin{cases} 4p & \text{if } p \equiv 1 \bmod 4 \\ 2p & \text{if } p \equiv 3 \bmod 4 \end{cases} + \begin{cases} 6 & \text{if } p \equiv 1 \bmod 3 \\ 0 & \text{otherwise.} \end{cases}$$

The following is not implemented in our construction of the database but can be used to further reduce the number of a_p values that need to be computed and stored. Suppose -1 is a quadratic residue in $\mathbb{F}_p$ (i.e., $p \equiv 1 \bmod 4$) and let $i \in \mathbb{F}_p$ be such that $i^2 \equiv -1 \bmod p$. Then, make the substitutions $y = i\tilde{y}$ and $x = -\tilde{x}$ so that

$$\begin{aligned} y^2 &= x^3 + ax + b \\ (i\tilde{y})^2 &= -\tilde{x}^3 - a\tilde{x} + b \\ \tilde{y}^2 &= \tilde{x}^3 + a\tilde{x} - b. \end{aligned} \tag{2.9}$$

Thus, when $p \equiv 1 \bmod 4$, the curve $y^2 = x^3 + ax + b$ and the curve $y^2 = x^3 + ax - b$ are automorphic so it suffices to compute the values of a_p for $0 \leq b < p/2$. This means we now have that

$$\#a_p \text{ we need to compute and store } = \begin{cases} 2p+2 & \text{if } p \equiv 1 \bmod 4 \\ 2p & \text{if } p \equiv 3 \bmod 4 \end{cases} + \begin{cases} 6 & \text{if } p \equiv 1 \bmod 3 \\ 0 & \text{otherwise.} \end{cases}$$

To retrieve the value of $a_t(p)$ corresponding to $E_t\colon\ y^2 = x^3 + A(t)x + B(t)$, we first find the quartic residue class of A. If $A \not\equiv 0 \bmod p$, then for $a = 1, 2, \ldots$, we compute $A(t)a^{-1} \bmod p$ and check whether it is a fourth power mod p. Once we have found some a with $A(t)a^{-1} \equiv \ell^4 \bmod p$, we compute the corresponding value of $B(t)$ as $B(t)\ell^{-6} \bmod p$ and retrieve the a_p value corresponding to (a, b) (i.e., the automorphic curve $y^2 = x^3 + ax + b = x^3 + A(t)\ell^{-4}x + B(t)\ell^{-6}$). Recall that if $p \not\equiv 1 \bmod 3$ and $A(t)$ is zero mod p, then $a_p = 0$ for all values of $B(t)$. Likewise, for all primes p, if $A(t)$ and $B(t)$ are both zero mod p then $a_p = 0$. If $p \equiv 1 \bmod 3$ and $B(t) \bmod p$ is nonzero, we find the sixth power residue class of $B(t)$ by computing $B(t)b^{-1} \bmod p$ for each value of b stored until this is a sixth power residue. Once we find b such that $B(t)b^{-1} \equiv \ell^6 \bmod p$, we retrieve the value of a_p for the curve $y^2 = x^3 + b$.

The only non-trivial arithmetic computation which is necessary is computing square roots of $x \bmod p$ (given that x is a square). When $p \equiv 3 \bmod 4$ we have

$$(x^{\frac{p+1}{4}})^2 = x^{\frac{p+1}{2}} = x^{\frac{p-1}{2}}x = x, \tag{2.10}$$

where $x^{\frac{p-1}{2}} = 1$, since x is a square. Unfortunately, when $p \equiv 1 \bmod 4$ we must apply a slightly more complicated idea: Cipolla's algorithm (see, for example, [Dic19] for the development of the algorithm). We first find some $a \in \mathbb{Z}$ such that $a^2 - x$ is not a square mod p. It is unknown if this can be done deterministically, however this can easily be done probabilistically extremely quickly. Since $a^2 - x$ is not a square, we conclude that

$$\mathbb{F}_{p^2} \cong \mathbb{F}_p(\sqrt{a^2 - x}). \tag{2.11}$$

Now, we have

$$\left(a + \sqrt{a^2 - x}\right)^p = a^p + \left(\sqrt{a^2 - x}\right)^p = a + \sqrt{a^2 - x}\,(a^2 - x)^{\frac{p-1}{2}} = a - \sqrt{a^2 - x}. \tag{2.12}$$

Thus, $(a + \sqrt{a^2 - x})^{p+1} = x$, and thus $((a + \sqrt{a^2 - x})^{\frac{p+1}{2}})^2 = x$. Notably, since x is a square in $\mathbb{F}_p$, we know that $(a + \sqrt{a^2 - x})^{\frac{p+1}{2}} \in \mathbb{F}_p$. We note that this algorithm can be computed efficiently by repeated squaring. An observant reader will note that when p is 3 mod 4, one can take $a = 0$ and this algorithm then reduces to the previous case.

3. Computationally Investigating the Bias Conjecture

While we expect our database to have many applications, we are initially motivated by calculating the second moment of one-parameter families of elliptic curves. Hence, we showcase how our database allows us to systematically computationally investigate the Bias Conjecture in one-parameter families for which obtaining a closed form of the second moment through Legendre symbols is intractable. The main, i.e., the most computationally expensive, inputs to calculating the second moment of a one-parameter family up to a value P is creating a database of all of the possible values of $a_t(p)$ for all $p \leq P$.

Since a one-parameter family is parameterized by $A(t)$ and $B(t)$, to compute the second moment, we need to look up $a_t(p)$, the a_p value for each curve $E_t : y^2 = x^3 + A(t)x + B(t)$ resulting from specializing $T = t$, i.e., for the pair $(a, b) = (A(t), B(t))$, and then sum over t as t ranges over all possible residues mod p. To isolate and study the bias in the lower order terms, we compute the normalized second moment $\mathcal{B}_{2,\mathcal{E}}(p) = (\mathcal{A}_{2,\mathcal{E}}(p) - p^2)/p^{3/2}$ for each prime p. We take P to be the largest prime smaller than $250,000$ and we compute the running average

$$\frac{1}{\pi(P) - 1} \sum_{2<p\leq P} \mathcal{B}_{2,\mathcal{E}}(p), \tag{3.1}$$

where $\pi(P)$ is the prime-counting function. We also introduce the log-weighted running average of the normalized second moment:

$$\frac{1}{N_w(P)} \sum_{2<p\leq P} \mathcal{B}_{2,\mathcal{E}}(p) \log p, \tag{3.2}$$

where $N_w(P) \coloneqq \sum_{2<p\leq P} \log p \sim P$. This is desirable since as can be seen in the graphs that follow, the running average for smaller primes is not representative of the long-term behavior.

Remark 3.1. *Since $N_w(P)$ and $\pi(P)$ both go to infinity, we can safely ignore any finite number of primes in the limit. Indeed, we may want to ignore the finite number of additional primes that divide the j-invariant, $A(T)$, or $B(T)$ or perhaps where some ramification occurs. Further study is required to deduce what is optimal.*

3.1. Potential positive bias families.

We conducted an exhaustive family search for a potential positive bias family by looking at one parameter families defined by all possible combinations of polynomials $A(T), B(T)$ of degree ≤ 5 with coefficients in $\{0, 1\}$. We computed the second moment for each of the resulting families for primes up to $1,000$ and noted those families whose running average of the normalized second moment was positive more than 95% of the time.[1] We then computed the second moment for those families which passed this initial filtering for primes up to $250,000$ and calculated the graphs of the running averages (see Figures 2, 3, 4, 5, 6, 7). As a point of comparison, we computed the second moment of the family $y^2 = x^3 + x + T^3$ for primes up to $250,000$ (see Figure 1). Although the running average appears to stabilize after $200,000$, looking at the oscillations in the running average up to $200,000$ it is clear that one should still be concerned whether going out to $250,000$ is far enough to see the long range behavior of the running average. Hence, while it would also be beneficial to compute the a_p values for a larger number of primes, this highlights the limitations of a computational approach. Our numerical investigations generate hypotheses and directions for future investigation but cannot prove or disprove the Bias Conjecture.

It is instructive to compare the graphs of the running averages of the families our family search found to the family $y^2 = x^3 + x + T^3$ for which [Bat+24] proved that for half of the primes, the second moment of this family has positive bias. While the graph of the running averages for

[1] Future work could focus on developing better measures of whether a family should be suspected of having positive bias and hence investigated further. For example, excluding primes $p \leq P_{\min}$.

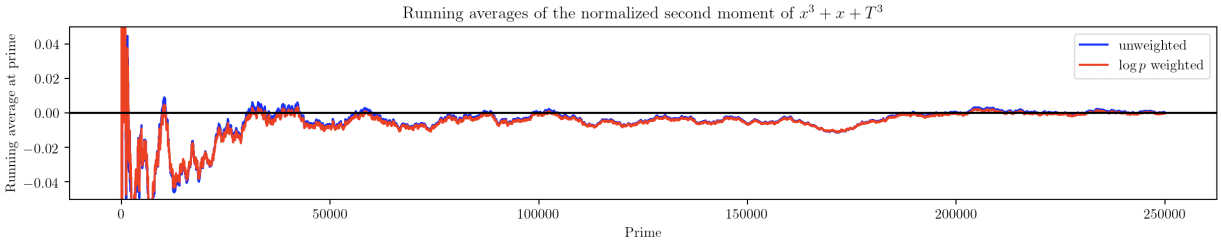

FIGURE 1. Running averages of the family investigated by [Bat+24].

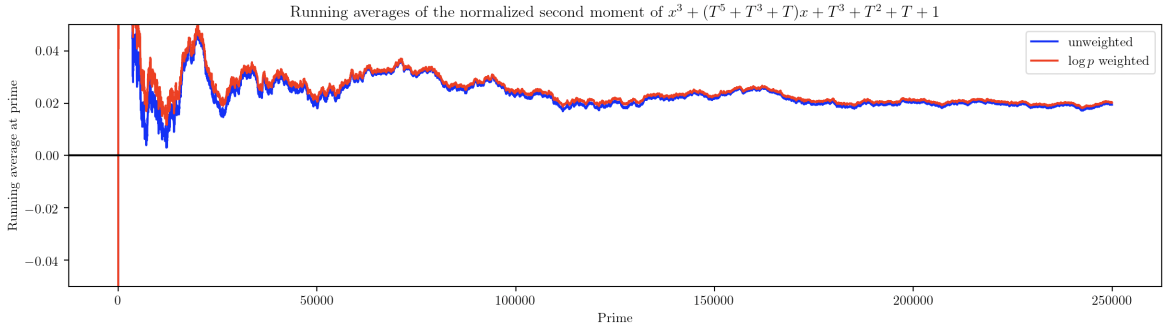

FIGURE 2. Running averages of $y^2 = x^3 + (T^5 + T^3 + T)x + T^3 + T^2 + T + 1$.

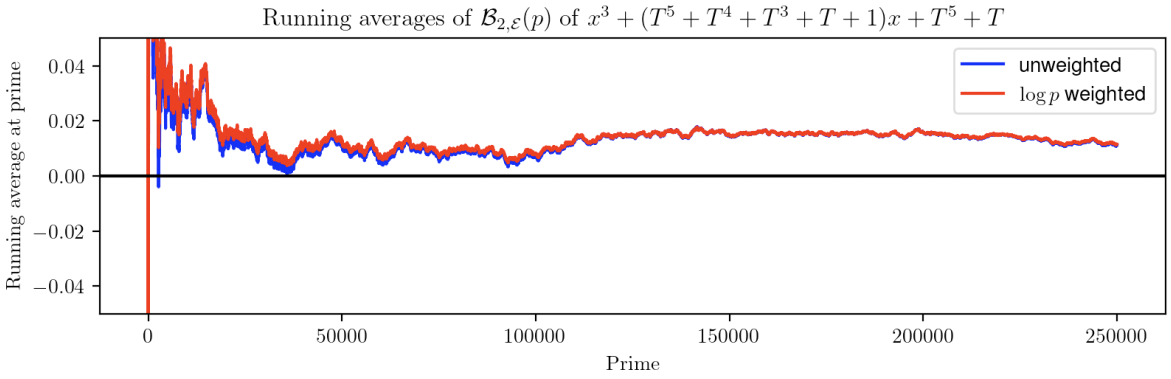

FIGURE 3. Running averages of $y^2 = x^3 + (T^5 + T^4 + T^3 + T + 1)x + T^5 + T$.

$y^2 = x^3 + x + T^3$ is negative most of the time but seems to tend to zero at 250,000, the graphs in Figures 2, 3, 4, 5, 6, 7 remain positive up to 250,000 and seem to stabilize for primes beyond 100,000. Therefore, with the above caveats in mind, we have reason to suspect these families may have positive bias.

Remark 3.2. *When splitting up these familes based on the primes residue class mod* 12*, we often see extremely different behavior in the resulting* 4 *residue classes. Specifically, if* p *is such that* $A(T)$ *and* $B(T)$ *split completely, the bias tends to be significantly higher. Because our polynomials' coefficients are either* 0 *or* 1*, being* 1 mod 12 *tends to result in splitting.*

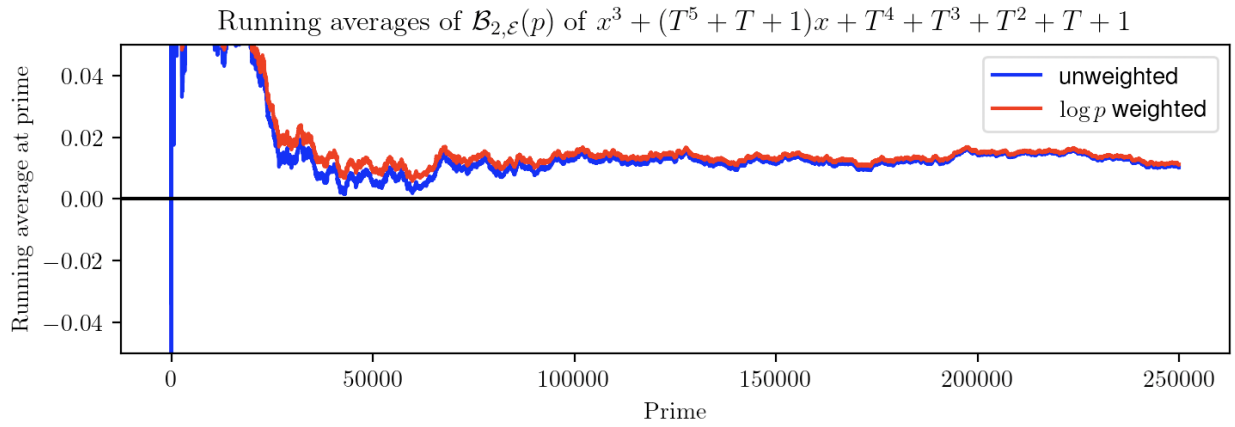

FIGURE 4. Running averages of $y^2 = x^3 + (T^5 + T + 1)x + T^4 + T^3 + T^2 + T + 1$.

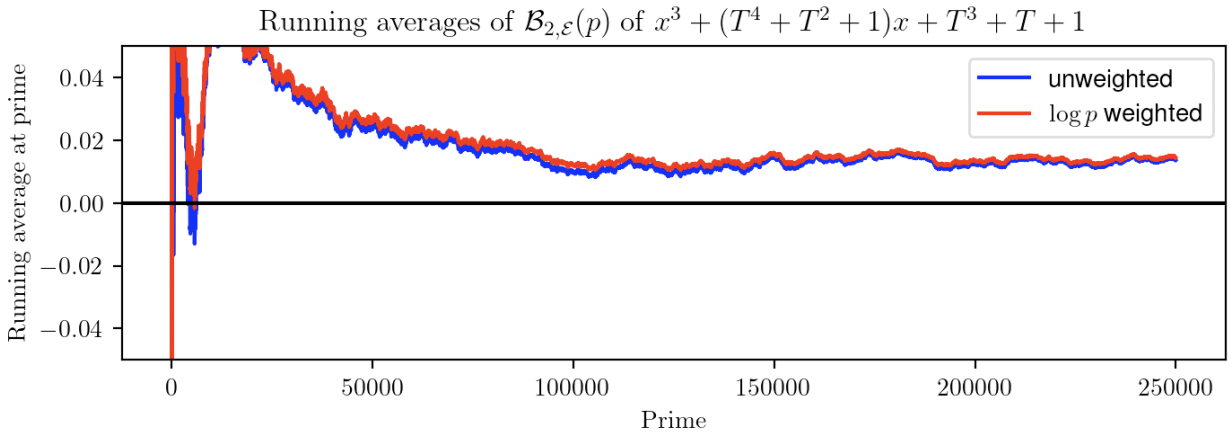

FIGURE 5. Running averages of $y^2 = (T^4 + T^2 + 1)x + T^3 + T + 1$.

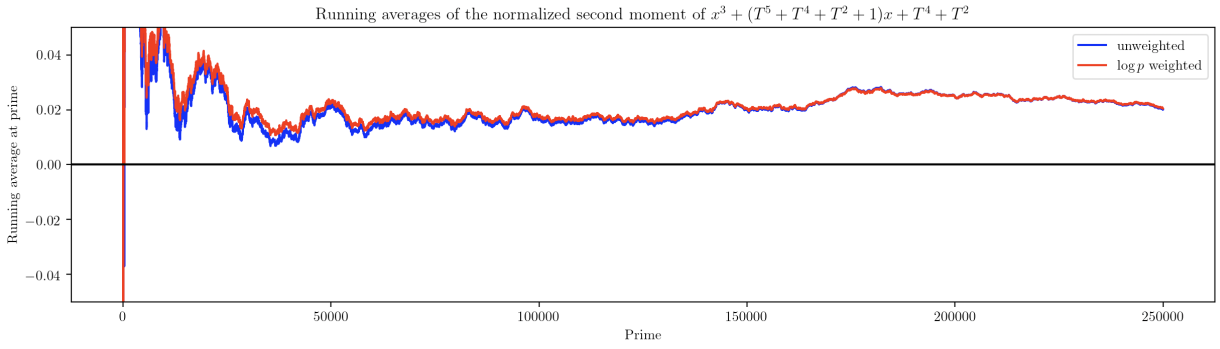

FIGURE 6. Running averages of $y^2 = x^3 + (T^5 + T^4 + T^2 + 1)x + T^4 + T^2$.

Remark 3.3. *One may worry that positive graphs of the running averages the families we have chosen out of* 2^{10} *families explored are the result of random fluctuations rather than underlying*

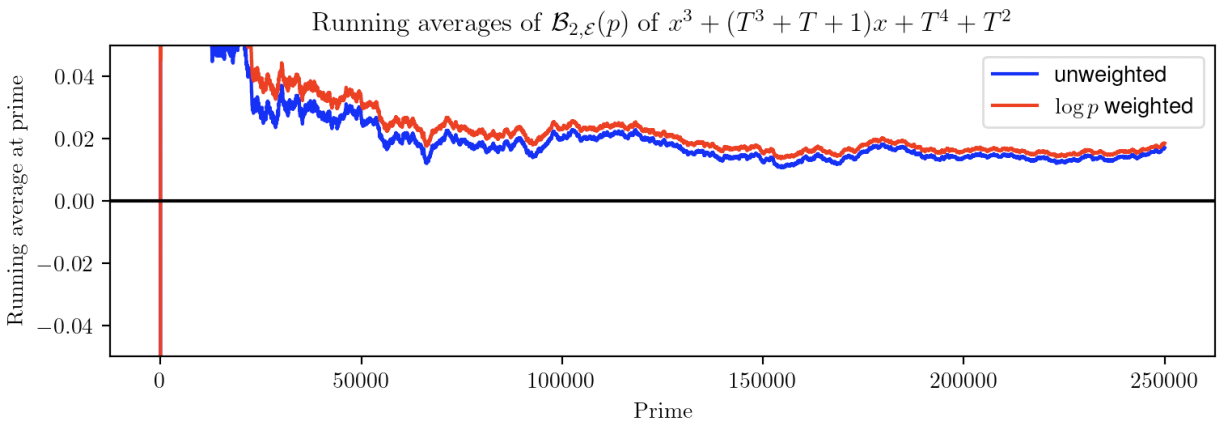

FIGURE 7. Running averages of $y^2 = x^3 + (T^3 + T + 1)x + T^4 + T^2$.

structure in the one-parameter family which may yield positive bias in the lower order terms of the second moment. However, when factoring $A(T)$ and $B(T)$ which appear in the above families, $A(T)$ is either irreducible or has a factor of $T^2 - T + 1$, $T^2 + T + 1$, or $T^2 + 1$ and the same is true for $B(T)$. This leads us to suspect that the positive graphs of these families are due to more than just the random chance.

When looking at polynomials of degree at most 10, we found the family $y^2 = x^3 + T^{10}x + T^8 + T^2$, which is our most promising candidate for having positive bias (see Figure 8). At the largest prime smaller than 250,000, the running average of the normalized second moment for this family is approximately 0.0287 and the log-weighted running average is approximately 0.0283, or a 4.2 σ deviation. Note that the polynomial $B(T)$ has a factor of $T^2 + 1$.

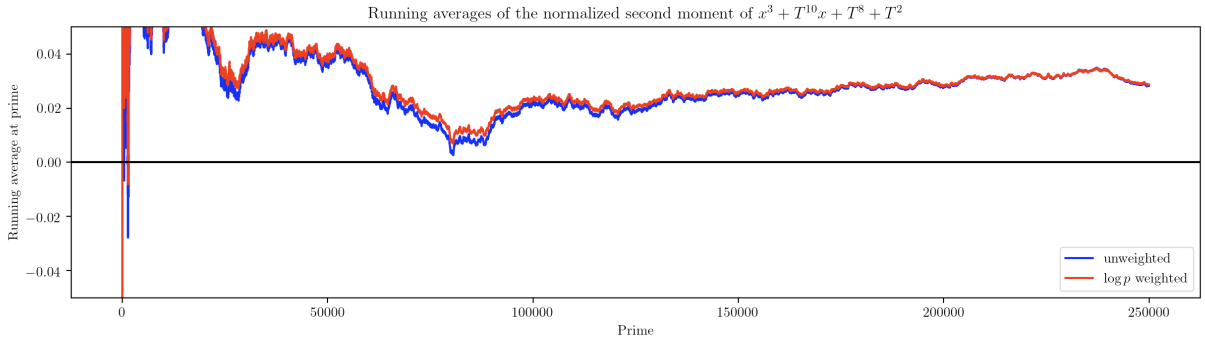

FIGURE 8. Running averages of $y^2 = x^3 + T^{10}x + T^8 + T^2$

4. Distribution of the Normalized Second Moment $\mathcal{B}_{2,\mathcal{E}}(p)$

Motivated by the Sato-Tate Conjecture, we study the distribution of the normalized second moment of a one-parameter family. It is natural to ask what determines the variance of the distribution of the normalized second moment of a one-parameter family. Based on our numerical computations, we formulate the following conjecture.

Conjecture 4.1. *The variance of the distribution of $\mathcal{B}_{2,\mathcal{E}}(p)$ always converges to a positive integer.*

Indeed there seems to be a deeper connection between the polynomials $A(T)$ and $B(T)$ and the conjectured integer the variance converges too. Indeed, the one parameter family given by $y^2 = x^3 + A(T^n)x + B(T^n)$ seems to be an integral multiple of $y^2 = x^3 + A(T)x + B(T)$ based on the prime factorization of n, A and B.

The following figures have binned the data between the maximum and the minimum over all primes less than $250,000$ and then split into 100 equal sized buckets.

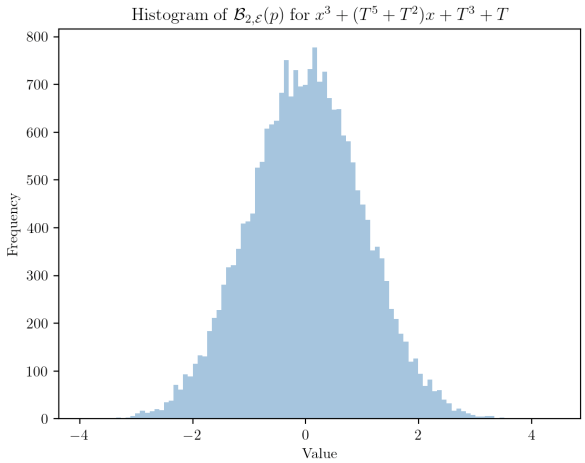

FIGURE 9. A Family with variance 1.015

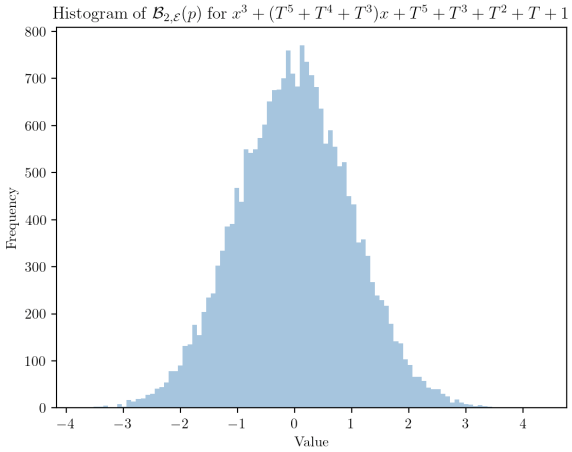

FIGURE 10. A Family with variance 1.005.

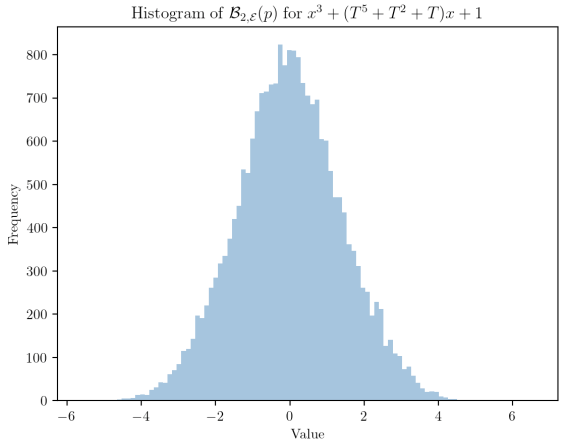

FIGURE 11. A family with variance 1.991.

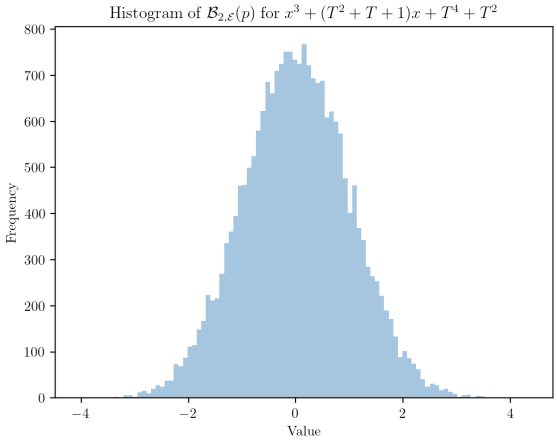

FIGURE 12. A family with variance 0.994.

Our generic case seems to be variance converging to 1 (see Figures 9, 10, and 12). In this generic case, the distribution of $\mathcal{B}_{2,\mathcal{E}}(p)$ seems to exhibit Gaussian-like behavior. We found one family $\mathcal{E} : y^2 = x^3 + (T^5 + T^2 + 1)x + 1$ whose variance seems to be converging to 2 (see Figure 11).

Additionally, when restricting the data to ignore the first $10,000$ primes, we net a family with the similar variance and distribution. Indeed, the only difference seems to be that the data is slightly more random, which is expected given that there are fewer data points.

Thus, a natural next question is what distribution the normalized second moment of a one-parameter family converges to in our seemingly generic case of variance 1 Gaussian-like behavior

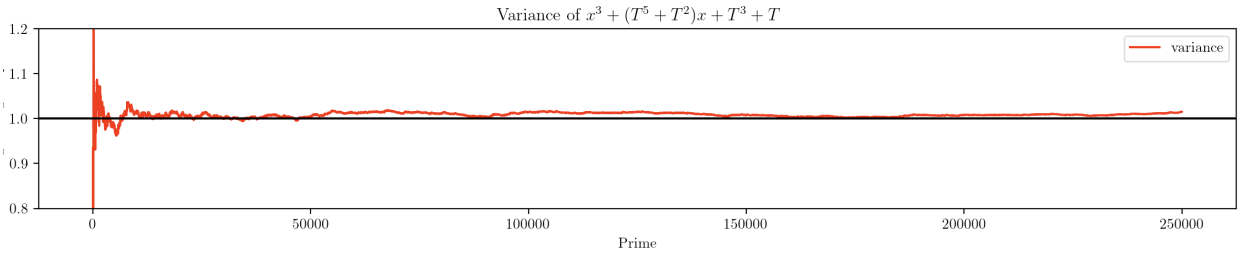

FIGURE 13. The graph of the variance of a family over primes $\leq p$.

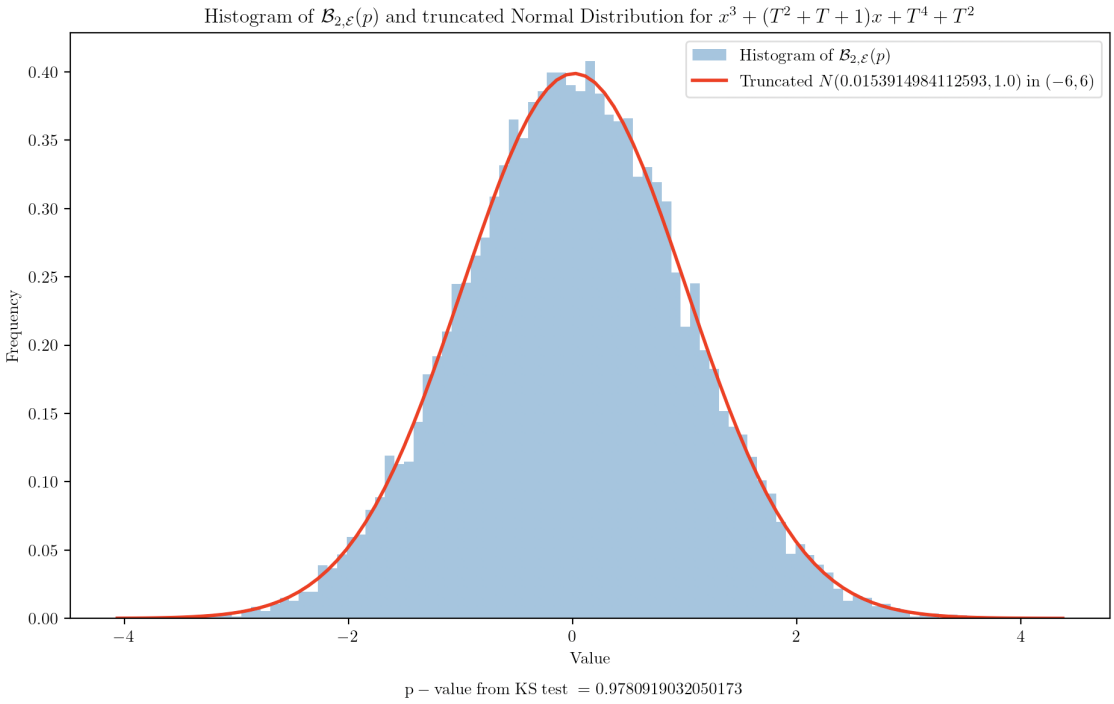

FIGURE 14. Fitting a truncated normal to the variance 1 family in Figure 12

and what is our generic case, i.e., what restrictions can we impose on our one-parameter family to ensure we are in the generic case?

These distributions look like normal distributions, however they cannot be as they must be bounded due to Theorem 1.1. This led us to investigate whether a truncated normal distribution with the same mean and variance as the family was a good fit to the data. When comparing the fit of a truncated normal distribution for a generic family to the variance 2 family, the truncated normal is a better fit for the variance 1 family while for the variance 2 family, there is too much mass around zero (see Figures 14 and 15).

Our numerics motivate the study of the distribution of the second moment of a one-parameter family. Further, the database allows for efficient computation of higher moments of one-parameter families.

5. Higher moments

Calculating higher moments is difficult because it measures a more subtle distribution of a_p values. However, numerically calculating higher moments is no different than the second moment.

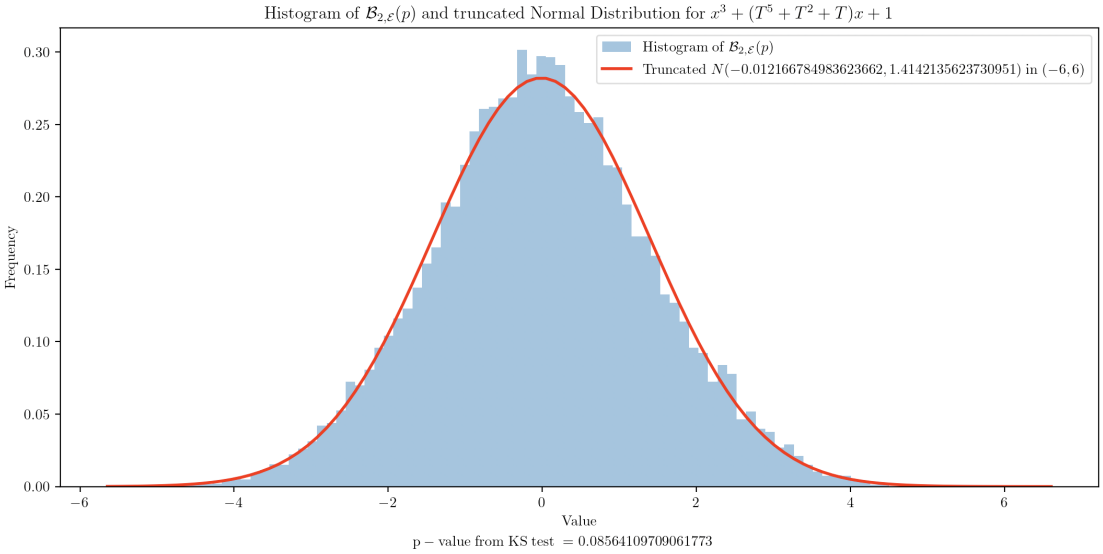

FIGURE 15. Fitting a truncated normal to the variance 2 family.

Indeed, one can calculate the second through tenth moments all at once nearly as quickly as just the second moment.

To highlight some applications of our database, we calculate higher moments of a one-parameter family. Without the closed form for a_p values we computed above, this method would not be possible. By Theorem 1 of [Bir68],

$$\mathcal{A}_{2n,\mathcal{E}}(p) \;=\; C_n p^{n+1} + O\left(p^{n+1/2}\right) \tag{5.1}$$

where $C_n = \frac{(2n)!}{n!(n+1)!}$ denotes the nth Catalan number. Like before, we investigate

$$\mathcal{B}_{2n,\mathcal{E}}(p) \;:=\; \frac{(\mathcal{A}_{2n,\mathcal{E}}(p)/C_n) - p^{n+1}}{p^{n+1/2}}. \tag{5.2}$$

The (unweighted) running averages $\mathcal{B}_{2n,\mathcal{E}}$ for a generic family are shown below.

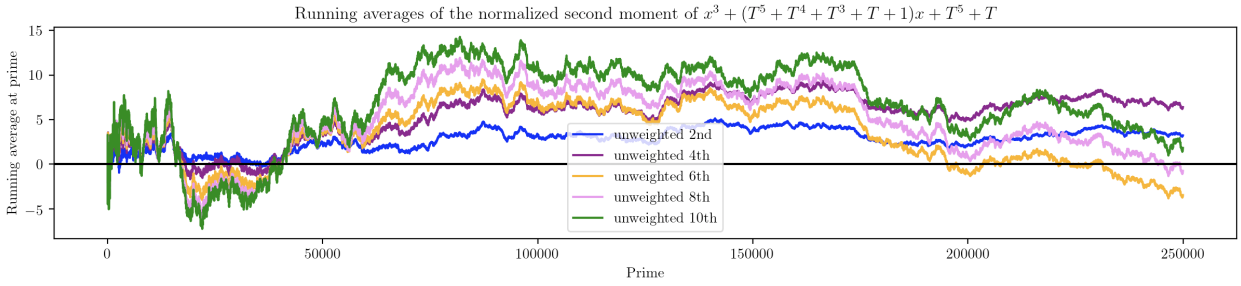

FIGURE 16. Normalized 2nd through 10th moments

We recall from above that in the second moment case, our variance converges to an integer, and the data is very similar to a normal distribution. We consider how these properties change for higher moments. Initially, the distribution of $\mathcal{B}_{4,\mathcal{E}}$ and $\mathcal{B}_{6,\mathcal{E}}$ look like normal distributions. There are a couple of notable differences.

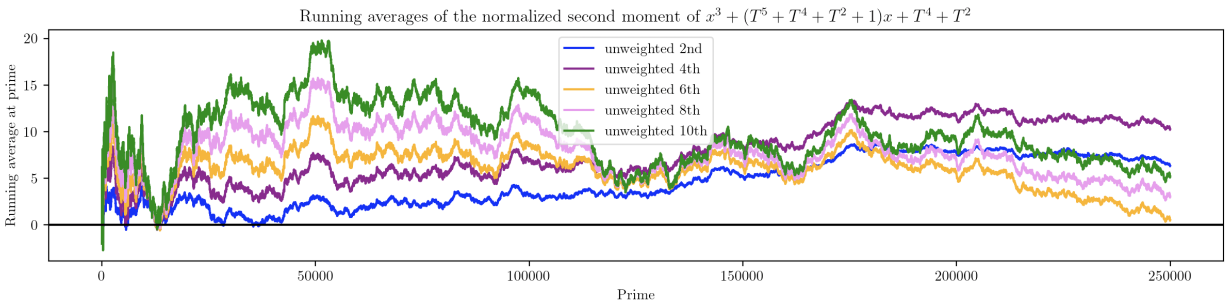

FIGURE 17. Normalized 2nd through 10th moments

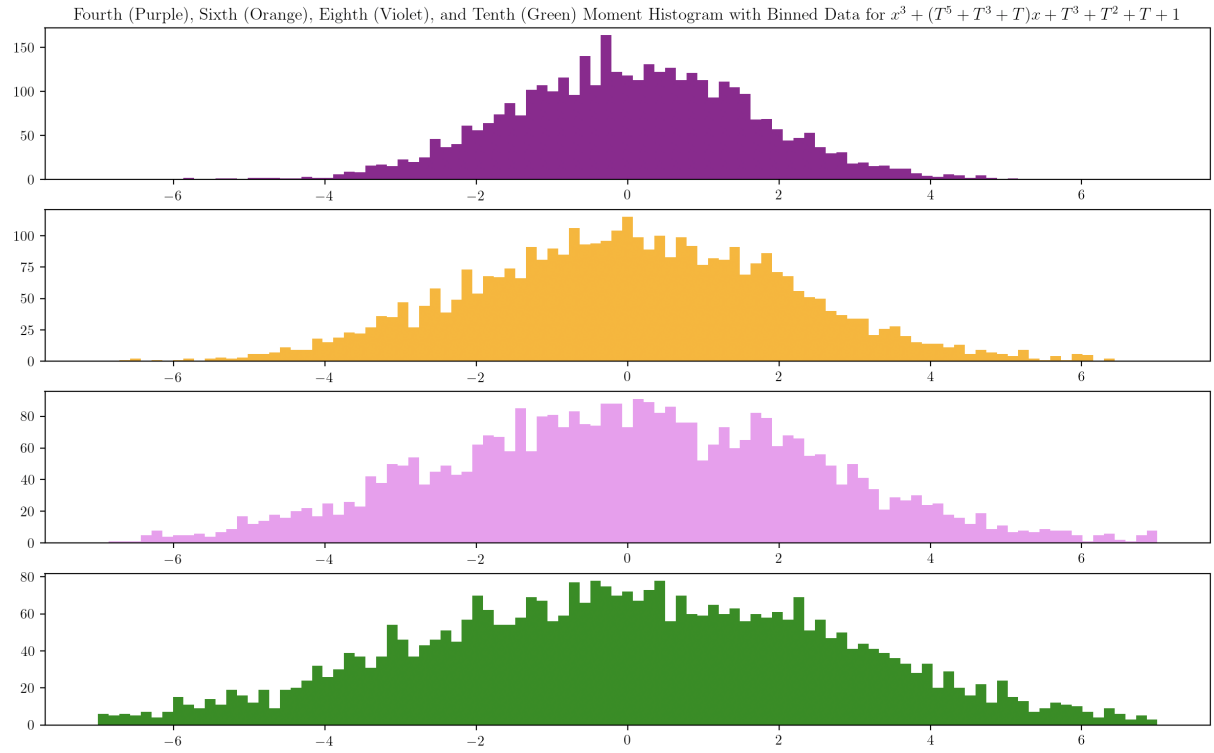

FIGURE 18. Normalized 4th through 10th moments, split into 100 buckets from -7 to 7

First, the distribution of $\mathcal{B}_{2n,\mathcal{E}}$ values seem to be spreading out as n increases. This is equivalent to the variances increasing, and indeed the data seem to support this. One potential reason is that a small bias in a_p values will result in higher deviations from the expectation in higher moments.

Second, the variances no longer seem to be an integer. Perhaps this is because the correct way to normalize the $\mathcal{A}_{2n,\mathcal{E}}$ values is by

$$\mathcal{B}'_{2n,\mathcal{E}}(p) \;:=\; \frac{\mathcal{A}_{2n,\mathcal{E}}(p) - C_n p^{n+1}}{p^{n+1/2}}. \tag{5.3}$$

However, under this normalization, we do not have enough data to conclude that $\mathcal{B}'$ values either converge or do not converge to an integer.

Remark 5.1. *The difference between these two normalizations is that the second one multiplies the variance by* $(C_n)^2$.

Third, as n increases, the distribution seems to stray further and further away from a smooth distribution. This suggests that convergence occurs at a slower rate for higher moments.

Finally, the higher moments do not seem to have a generic behavior of positive or negative bias: some families seem to have positive bias while others seem to have negative bias. Further investigation is warranted to understand how the polynomials $A(T)$ and $B(T)$ determine the value to which the higher moments converge.

6. Future work

To compute moments up to a fixed number X, we first need to compute approximately $2X^2/\log X$ many a_p values, and then do a comparable amount of work to compute moments.

However, computing a_p values using the naive algorithm described above requires $O(p)$ computations. This algorithm's advantage is that due to summing over all of $\mathbb{F}_p$ in some cases we can extract cancellation. However, if one simply wishes to compute a_p values, one can employ Schoof's algorithm. See, for instance, [Dew98] for a discussion of this algorithm which allows for computation of a_p in $O(\log^6(p))$ times (assuming arithmetic operations are $O(1)$). Indeed, taking our $p = 3, 5, 7, 11, 13$ one can compute a_p values for primes less than $14,000,000$, which is approximately 50 times as many primes as we computed.

Computing significantly more a_p values should provide computation evidence for Conjecture 4.1, allow for further testing of the bias conjecture, and probing higher moments, potentially even over certain residue classes mod p. One can consider certain classes of primes, for instance, those which split, split completely, ramify etc. over a certain number field, to investigate how $A(T)$ and $B(T)$ may influence the behavior of the higher moments.

For potentially easier things to study, how does the variance, second moment, and distribution of second moments of $y^2 = x^3 + A(T^n)x + B(T^n)$ relate to $y^2 = x^3 + A(T)x + B(T)$? Additionally, what happens for primes where $A(T)$ and $B(T)$ both factor completely? Or perhaps, what happens when both $A(T)$ and $B(T)$ are irreducible. These questions dicussing behavior in these restricted environments provide fertile ground for explorations. We note that we have been splitting our data into 100 buckets. One can explore how a different number of buckets changes how good the p-values from the KS test nets, and use this to work towards determining the distribution.

Other potential areas of study include exploring higher moments, using techniques from algebraic geometry to study a threefold that holds second (or higher) moment information, finding the distribution that the second moment converges to, proving Conjecture 4.1, proving Remark 3.2, and determining the integer that the second moment converges to based on the polynomials $A(T)$ and $B(T)$.

Acknowledgements

This research was completed at the Williams College SMALL REU Program and was supported by Williams College and the National Science Foundation (grant DMS2241623). The authors are grateful for the support of Duke University, Princeton University, and the University of Michigan. The authors would like to thank Adam Logan for helpful discussions.

References

[Asa+23] M. Asada, R. C. Chen, E. Fourakis, Y. H. Kim, A. Kwon, D. J. Lichtman, B. Mackall, S. J. Miller, E. Winsor, K. Winsor, J. Yang, and K. Yang. "Lower-order biases in the second moment of Dirichlet coefficients in families of L-functions". In: *Exp. Math.* 32.3 (2023), pp. 431–456. DOI: 10.1080/10586458.2021.1980453.

[Bat+24] Z. Batterman, A. Jambhale, S. J. Miller, A. L. Narayanan, K. Sharma, A. Yang, and C. Yao. *Applications of Moments of Dirichlet Coefficients in Elliptic Curve Families*. To appear in the ICERM Conference Proceedings for the July 2023 Murmurations Workshop. 2024. arXiv: 2311.17215 [math.NT].

[Bir68] B. J. Birch. "How the Number of Points of An Elliptic Curve Over a Fixed Prime Field Varies". In: *Journal of the London Mathematical Society* s1-43.1 (1968), pp. 57–60. DOI: https://doi.org/10.1112/jlms/s1-43.1.57.

[Che+24] T. Cheek, P. Gilman, K. Jaber, V. Sharan, and M. Tomé. *Elliptic Curve Coding*. GitHub repository. 2024. URL: https://github.com/KareemSaysHi/SMALL2024-Elliptic-Curve-Coding.

[Dew98] L. Dewaghe. "Remarks on the Schoof-Elkies-Atkin algorithm". In: *Math. Comp. 67* (1998), pp. 1247–1252.

[Dic19] L. E. Dickson. *History of the Theory of Numbers*. Carnegie Institution of Washington, 1919, p. 218.

[Has36] H. Hasse. "Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung." In: *Journal für die reine und angewandte Mathematik* 1936.175 (1936), pp. 193–208. DOI: doi:10.1515/crll.1936.175.193.

[KN21] M. Kazalicki and B. Naskrecki. *Second moments and the bias conjecture for the family of cubic pencils*. 2021. arXiv: 2012.11306 [math.NT].

[KN22] M. Kazalicki and B. Naskrecki. "Diophantine triples and K3 surfaces". In: *J. Number Theory* 236 (2022), pp. 41–70. ISSN: 0022-314X. DOI: 10.1016/j.jnt.2021.07.009.

[Mac+16] B. Mackall, S. J. Miller, C. Repti, and K. Winsor. "Lower-order biases in elliptic curve Fourier coefficients in families, in: Frobenius distributions: Lang-Trotter and Sato-Tate conjectures". In: *Contemp. Math., Amer. math. Soc.* 663 (2016), pp. 223–238.

[Mic95] P. Michel. "Rang moyen de famille de courbes elliptiques et lois de Sato-Tate". In: *Monatshefte für Mathematik* 120 (1995), pp. 127–136. DOI: 10.1007/BF01585913.

[Mil02] S. J. Miller. "1- and 2-level densities for families of elliptic curves: evidence for the underlying group symmetries". PhD thesis. Princeton University, 2002.

[Mil04] S. J. Miller. "1- and 2-level densities for families of elliptic curves: evidence for the underlying group symmetries". In: *Compositio Mathematica* 140 (2004), pp. 952–992.

[Mil05] S. J. Miller. "Variation in the number of points on elliptic curves and applications to excess rank". In: *C. R. Math. Acad. Sci. Soc. R. Can.* 27.4 (2005), pp. 111–120.

[Nag97] K. Nagao. "$\mathbb{Q}(T)$-rank of elliptic curves and certain limit coming from the local points". In: *Manuscripta Math* 92 (1997), pp. 13–32. DOI: doi:10.1007/BF02678178.

[RS98] M. Rosen and J. Silverman. "On The Rank Of An Elliptic Surface". In: *Inventiones Mathematicae* 133 (May 1998), pp. 43–67. DOI: 10.1007/s002220050238.

[Shi72] T. Shioda. "On elliptic modular surfaces". In: *Journal of the Mathematical Society of Japan* 24.1 (1972), pp. 20–59. DOI: 10.2969/jmsj/02410020. URL: https://doi.org/10.2969/jmsj/02410020.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves (Graduate Texts in Mathematics)*. Springer-Verlag New York, Incorporated, 2009.

[Sil94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves (Graduate Texts in Mathematics)*. Springer, 1994.

Department of Mathematics, University of Michigan
Email address: timcheek@umich.edu

Department of Mathematics, University of California Santa Barbara
Email address: picogilman@gmail.com

Department of Mathematics, Princeton University
Email address: kj5388@princeton.edu

Department of Mathematics, Williams College
Email address: sjm1@williams.edu

Department of Mathematics, Yale University
Email address: vismay.sharan@yale.edu

Department of Mathematics, Duke University
Email address: mariehelene.tome@duke.edu