Second Moment Calculations for One-Parameter Families of Elliptic Curves

Pico Gilman (picogilman@gmail.com)
Marie-Hélène Tomé (mariehelene.tome@duke.edu)

(joint with Timothy Cheek, Kareem Jaber, Vismay Sharan)

Advisor: Steven J. Miller
SMALL REU at Williams College

2024 Young Mathematicians Conference

August 13th, 2024

1 Introduction

2 Computation of a_p

3 Computational Investigation

4 Normalized Second Moment

5 Algebraic Geometry

Elliptic Curves

An elliptic curve E is a genus 1 smooth projective curve with a distinguished point $\mathcal{O}_E$ (a "point at infinity").

Elliptic Curves

An elliptic curve E is a genus 1 smooth projective curve with a distinguished point $\mathcal{O}_E$ (a "point at infinity"). For K with $\mathrm{char}(K) \neq 2, 3$ and $A, B \in K$, an elliptic curve is defined by

$$E(K) \coloneqq \{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}_E\},$$

with discriminant $\Delta(E) \coloneqq -16(4A^3 + 27B^2) \neq 0$.

Elliptic Curves

An elliptic curve E is a genus 1 smooth projective curve with a distinguished point $\mathcal{O}_E$ (a "point at infinity"). For K with $\mathrm{char}(K) \neq 2, 3$ and $A, B \in K$, an elliptic curve is defined by

$$E(K) \coloneqq \{(x, y) \in K^2 : y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}_E\},$$

with discriminant $\Delta(E) \coloneqq -16(4A^3 + 27B^2) \neq 0$.

Theorem (Mordell-Weil 1922)

The set $E(\mathbb{Q})$ is a finitely generated abelian group whose identity element is $\mathcal{O}_E$:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tors}},$$

and we call r the rank of $E(\mathbb{Q})$.

Elliptic Curves mod p

From $E/\mathbb{Q}$ we obtain an infinite family of elliptic curves mod p, one for each $p \nmid \Delta(E)$:

- Reduction mod p is a group homomorphism $E(\mathbb{Q}) \longrightarrow E(\mathbb{F}_p)$;
- The expected number of solutions to $E_p := E(\mathbb{F}_p)$ is $p + 1$.

Elliptic Curves mod p

From $E/\mathbb{Q}$ we obtain an infinite family of elliptic curves mod p, one for each $p \nmid \Delta(E)$:

- Reduction mod p is a group homomorphism $E(\mathbb{Q}) \longrightarrow E(\mathbb{F}_p)$;
- The expected number of solutions to $E_p := E(\mathbb{F}_p)$ is $p+1$.

Theorem (Hasse 1933)

For $a_p := p + 1 - \#E(\mathbb{F}_p)$ we have that $|a_p| \leq 2\sqrt{p}$.

Hasse-Weil L-function

If $p \mid \Delta(E)$, let $\alpha_p \coloneqq 0, 1$, or -1 based on the type of singularity of E mod p.

Definition

The Hasse-Weil L-function of E is defined by

$$L(s, E) \coloneqq \prod_{p \mid \Delta(E)} \left(1 - \frac{\alpha_p}{p^s}\right)^{-1} \prod_{p \nmid \Delta(E)} \left(\frac{p^s + p^{1-s} - a_p}{p^s}\right)^{-1},$$

which converges uniformly and absolutely on compact subsets of $\{s \in \mathbb{C} : \mathrm{Re}(s) > 3/2\}$ and has an analytic continuation to all of $\mathbb{C}$.

The L-function $L(s, E)$ packages the information from the a_p's.

Birch and Swinerton-Dyer

Birch and Swinerton-Dyer 1950s: Computational experiments calculating

$$\pi_E(X) := \prod_{p \leq X, p \nmid \Delta(E)} \frac{\#E(\mathbb{F}_p)}{p} = \prod_{p \leq X, p \nmid \Delta(E)} \frac{p+1-a_p}{p}$$

led to the following conjecture.

Conjecture (Birch and Swinnerton-Dyer)

If $E/\mathbb{Q}$ has rank r, then there is some constant C such that $\pi_E(X) \sim C \log(X)^r$.

Birch and Swinerton-Dyer

Although the Euler product may not converge for $s = 1$, formally evaluating $L(s, E)$ at $s = 1$

$$L(1, E) \text{ “} = \text{”} \left(\prod_{p \mid \Delta(E)} \left(1 - \frac{\alpha_p}{p}\right) \prod_{p \nmid \Delta(E)} \frac{p + 1 - a_p}{p} \right)^{-1}.$$

Birch and Swinerton-Dyer

Although the Euler product may not converge for $s = 1$, formally evaluating $L(s, E)$ at $s = 1$

$$L(1, E) \text{ “} = \text{”} \left(\prod_{p|\Delta(E)} \left(1 - \frac{\alpha_p}{p}\right) \prod_{p\nmid\Delta(E)} \frac{p + 1 - a_p}{p} \right)^{-1}.$$

Idea: Larger $\#E(\mathbb{F}_p) = p + 1 - a_p$ on average, i.e., negative bias in the a_p's, should imply $L(s, E)$ tends to zero faster as $s \to 1$.

Birch and Swinerton-Dyer

Although the Euler product may not converge for $s = 1$, formally evaluating $L(s, E)$ at $s = 1$

$$L(1, E) \text{ “} = \text{”} \left(\prod_{p \mid \Delta(E)} \left(1 - \frac{\alpha_p}{p}\right) \prod_{p \nmid \Delta(E)} \frac{p + 1 - a_p}{p} \right)^{-1}.$$

Idea: Larger $\#E(\mathbb{F}_p) = p + 1 - a_p$ on average, i.e., negative bias in the a_p's, should imply $L(s, E)$ tends to zero faster as $s \to 1$.

Conjecture (Birch and Swinnerton-Dyer)

If $E/\mathbb{Q}$ has rank r, then

$$r \;=\; \mathrm{ord}_{s=1} L(s, E).$$

Connecting the two conjectures

Theorem (Goldfeld)

Suppose $\pi_E(X) \sim C\log(X)^r$. *Then* $r = \mathrm{ord}_{s=1}L(s,E)$ *and*

$$\lim_{s\to 1}\frac{L(s,E)}{(s-1)^r} = \frac{\sqrt{2}\mathrm{e}^{r\gamma}}{C}\prod_{p|\Delta(E)}(1-\alpha_p p^{-1})^{-1}.$$

In particular, if $r = 0$ *then*

$$L(1,E) = \sqrt{2}\left(\prod_{p|\Delta(E)}\left(1-\frac{\alpha_p}{p}\right)\prod_{p\nmid\Delta(E)}\frac{p+1-a_p}{p}\right)^{-1}.$$

One-parameter families

Let $\mathscr{E} \to \mathbb{P}^1$ be a non-split elliptic surface over $\mathbb{Q}$ with

$$\mathscr{E} : y^2 = x^3 + A(T)x + B(T),$$

where $A(T), B(T) \in \mathbb{Z}[T]$ and $4A(T)^3 + 27B(T)^2 \neq 0$. Almost all specializations $T = t \in \mathbb{Z}$ results in an elliptic curve E_t. This is a *one-parameter family* $\{E_t\}$ of elliptic curves over $\mathbb{Q}$.

- The *rank of a family* is the minimum rank r that appears infinitely often in E_t.

n-th Moments

Definition (n-th Moments of a 1-parameter Family of Elliptic Curves)

Let $a_t(p) \coloneqq p + 1 - \#E_t(\mathbb{F}_p)$. Then the n-th moment is given by

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

Note, we do not normalize by $1/p$.

Moments and the arithmetic properties of elliptic curves

Theorem (Nagao, Rosen-Silverman 1998)

Assuming Tate's conjecture holds for $\mathscr{E}$, we have that

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p\leq X} \mathscr{A}_{1,\mathscr{E}}(p) \frac{\log p}{p} \;=\; -\mathrm{rank}\mathscr{E}(\mathbb{Q}(T)).$$

Assuming Tate's conjecture (known for $\mathscr{E}$ if degrees of A, B sufficiently small):

- the rank is determined by the first moment;
- $\sum_{p\leq X} \log p \sim X$ so if $\mathscr{A}_{1,\mathscr{E}}(p) = -rp + O(1)$, then $\mathrm{rank}\mathscr{E}(\mathbb{Q}(T)) = r$;
- there is a negative bias in $a_t(p)$.

The Second Moment

The j-invariant of an elliptic surface $\mathscr{E}$ is

$$j(T) \;:=\; 1728\frac{4A(T)^3}{4A(T)^3+27B(T)^2}.$$

Second Moment Asymptotic (Michel, 1995)

For an elliptic surface $\mathscr{E}$ with $j(T)$ non-constant, we have

$$\mathscr{A}_{2,\mathscr{E}}(p) \;=\; p^2+O(p^{3/2}),$$

with lower order terms of size $p^{3/2}, p, p^{1/2}$, and 1.

Bias Conjecture

Question

Do lower order terms in the asymptotic second moment expansion also have a negative bias?

Bias Conjecture

Question

Do lower order terms in the asymptotic second moment expansion also have a negative bias?

Conjecture (S.J. Miller '02)

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

- *Excess rank problem*: disagreement between expected and observed average rank.
- Miller: negative bias in lower order terms increases bound for average rank obtained via 1-level density of zeros near central point.

Strong Bias Conjecture

Conjecture (Strong Bias Conjecture)

The largest lower term in the second moment expansion which does not average to 0 is negative for all but finitely many p.

Strong Bias Conjecture

Conjecture (Strong Bias Conjecture)

The largest lower term in the second moment expansion which does not average to 0 is negative for all but finitely many p.

- SMALL '23 disproved the strong bias conjecture with $x^3 + x + T^3$.
- For $p \equiv 2 \bmod 3$, there exists an automorphism $x^3 + x + T^3 \longmapsto x^3 + x + T$.
- The family $x^3 + x + T$ has second moment $p^2 + p$ for $p \equiv 2 \bmod 3$.

1 Introduction

2 Computation of a_p

3 Computational Investigation

4 Normalized Second Moment

5 Algebraic Geometry

Legendre Symbols

The Legendre symbol is

$$\left(\frac{a}{p}\right) := \begin{cases} 0 \text{ when } a = 0, \\ 1 \text{ when } a \neq 0 \text{ and square}, \\ -1 \text{ otherwise.} \end{cases}$$

Observation

When p is odd and for a given x, the number of solutions to $y^2 = x^3 + ax + b$ mod p is given by

$$1 + \left(\frac{x^3 + ax + b}{p}\right).$$

Legendre Symbols

Lemma

For p odd, then the elliptic curve given by $y^2 = x^3 + ax + b$ satisfies

$$a_p = -\sum_x \left(\frac{x^3 + ax + b}{p} \right).$$

Legendre Symbols

Lemma

For p odd, then the elliptic curve given by $y^2 = x^3 + ax + b$ satisfies

$$a_p = -\sum_x \left(\frac{x^3 + ax + b}{p} \right).$$

Consequently, we can calculate the second moment via

$$\mathscr{A}_{2,\mathscr{E}} = \sum_t \sum_{x,y} \left(\frac{x^3 + A(t)x + B(t)}{p} \right) \left(\frac{y^3 + A(t)y + B(t)}{p} \right).$$

In general, explicit formulas are difficult, however, it is possile in some special cases.

Known Expansions

Essentially, the only know non-trivial second moment expansions are as follows:

Family	$A_{1,\mathscr{E}}(p)$	$A_{2,\mathscr{E}}(p)$
$y^2 = x^3 + 2^4(-3)^3(9T+1)^2$	0	$\begin{cases} 2p^2-2p & p \equiv 2 \bmod 3 \\ 0 & p \equiv 1 \bmod 3 \end{cases}$
$y^2 = x^3 \pm 4(4T+2)x$	0	$\begin{cases} 2p^2-2p & p \equiv 1 \bmod 4 \\ 0 & p \equiv 3 \bmod 4 \end{cases}$
$y^2 = x^3 + (T+1)x^2 + Tx$	0	$p^2 - 2p - 1$
$y^2 = x^3 + x^2 + 2T + 1$	0	$p^2 - 2p - 3$
$y^2 = x^3 + Tx^2 + 1$	$-p$	$p^2 - n_{3,2,p}p - 1 + c_{3/2}(p)$
$y^2 = x^3 - T^2x + T^2$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 - T^2x + T^4$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 + Tx^2 - (T+3)x + 1$	$-2c_{p,1;4}p$	$p^2 - 4c_{p,1;6}p - 1$

where $c_{p,a;m} = 1$ if $p \equiv a \bmod m$ and 0 otherwise; $n_{3,2,p}$ is the number of cubes root of 2 mod p; $c_\alpha(p)$ are certain Legendre sums multiplied by p.

Tractable Cases

Closed form expressions via Legendre sums are only tractable in special cases: explicit calculations made by reducing to lower degree polynomials $A(T), B(T)$, and using the identities for linear and quadratic Legendre sums

$$\sum_x \left(\frac{ax+b}{p}\right) = \mathbf{1}_{a=0} p \left(\frac{b}{p}\right)$$

and

$$\sum_x \left(\frac{ax^2+bx+c}{p}\right) = \left(\mathbf{1}_{b^2=4ac} ap - 1\right)\left(\frac{a}{p}\right).$$

Computational Investigation of the Bias Conjecture

- S.J. Miller formulated Bias Conjecture after drawing inspiration from proof of Nagao conjecture, computations for low-degree non-generic families.
- To test Bias Conjecture, need to study families with higher degree polynomials $A(T), B(T)$ to observe generic families.
- Computationally investigate families:
  - generate database of a_p values (primes up to $250,000$);
  - study second moments of families with $A(T), B(T)$ of degree ≤ 5.

Automorphisms

Consider the elliptic curve $\mathscr{E}\colon\ y^2 = x^3 + ax + b$. Letting $y = \ell^3 y'$ and $x = \ell^2 x'$ yields

$$\ell^6 y'^2 \ = \ \ell^6 x'^3 + \ell^2 a x' + b.$$

Dividing by ℓ^6, we conclude

$$\mathscr{E}\colon\ y'^2 \ = \ x'^3 + \frac{a}{\ell^4} x' + \frac{b}{\ell^6}.$$

Hence, these two curves are automorphic to each other and have the same number of $\mathbb{F}_p$ points.

Automorphisms

Consider the elliptic curve $\mathscr{E}\colon\ y^2 = x^3 + ax + b$. Letting $y = \ell^3 y'$ and $x = \ell^2 x'$ yields

$$\ell^6 y'^2 \ = \ \ell^6 x'^3 + \ell^2 a x' + b.$$

Dividing by ℓ^6, we conclude

$$\mathscr{E}\colon\ y'^2 \ = \ x'^3 + \frac{a}{\ell^4} x' + \frac{b}{\ell^6}.$$

Hence, these two curves are automorphic to each other and have the same number of $\mathbb{F}_p$ points. Thus, it suffices to compute the values of a_p for one a in each quartic residue class. For p odd,

$$\#\text{ of quartic residue classes} = \begin{cases} 5 & p \equiv 1 \pmod 4 \\ 3 & p \equiv 3 \pmod 4. \end{cases}$$

Automorphisms $(a = 0)$

Example

The curves $y^2 = x^3 + 8x + 3$ *and* $y^2 = x^3 + 2x + 9$ *are automorphic mod* 11 *with* $\ell = 3$.

Automorphisms $(a = 0)$

Example

The curves $y^2 = x^3 + 8x + 3$ *and* $y^2 = x^3 + 2x + 9$ *are automorphic mod* 11 *with* $\ell = 3$.

Example

The curves $y^2 = x^3 + 3$ *and* $y^2 = x^3 + 9$ *are automorphic mod* 11 *with* $\ell = 3$.

Automorphisms ($a = 0$)

Example

The curves $y^2 = x^3 + 8x + 3$ and $y^2 = x^3 + 2x + 9$ are automorphic mod 11 with $\ell = 3$.

Example

The curves $y^2 = x^3 + 3$ and $y^2 = x^3 + 9$ are automorphic mod 11 with $\ell = 3$.

This suggests that when $a = 0$, we only need to store 6 different a_p values, one for each sextic residue class of b. Hence,

$$\#\text{ of } a_p \text{ we need to store } = \begin{cases} 4p+6 & p \equiv 1 \pmod 4 \\ 2p+6 & p \equiv 3 \pmod 4. \end{cases}$$

Automorphisms $(a = 0)$ cont.

When $p \not\equiv 1 \pmod 3$, $x \mapsto x^3$ is an bijection. Hence

$$\sum_x \left(\frac{x^3 + b}{p}\right) = \sum_x \left(\frac{x + b}{p}\right) = 0.$$

Therefore, we can compute and store fewer a_p:

$$\#\text{ of } a_p \text{ we need to store } = \begin{cases} 4p & p \equiv 1 \pmod 4 \\ 2p & p \equiv 3 \pmod 4 \end{cases} + \begin{cases} 6 & p \equiv 1 \pmod 3 \\ 0 & p \equiv 0, 2 \pmod 3). \end{cases}$$

Automorphisms $(\sqrt{-1})$

Suppose there is some $i \in \mathbb{F}_p$ such that $i^2 = -1$. Then, put $y = iy'$ and $x = -x$, and thus

$$\begin{aligned} y^2 &= x^3 + ax + b \\ (iy')^2 &= -x^3 - ax + b \\ y'^2 &= x^3 + ax - b. \end{aligned}$$

Automorphisms $(\sqrt{-1})$

Suppose there is some $i \in \mathbb{F}_p$ such that $i^2 = -1$. Then, put $y = iy'$ and $x = -x$, and thus

$$\begin{aligned} y^2 &= x^3 + ax + b \\ (iy')^2 &= -x^3 - ax + b \\ y'^2 &= x^3 + ax - b. \end{aligned}$$

Hence, we need to compute a_p for $0 \leq b < p/2$. Thus

$$\#\text{ of } a_p \text{ we need to store } = \begin{cases} 2p+2 & p \equiv 1 \pmod 4 \\ 2p & p \equiv 3 \pmod 4 \end{cases} + \begin{cases} 6 & p \equiv 1 \pmod 3 \\ 0 & p \equiv 0, 2 \pmod 3). \end{cases}$$

N.b. this slide has not been implemented due to our code already being sufficiently fast.

1 Introduction

2 Computation of a_p

3 Computational Investigation

4 Normalized Second Moment

5 Algebraic Geometry

Normalized Second Moment

- By Michel's theorem, there are $\alpha(p), \beta(p)$ both $O(1)$ such that

$$\mathscr{A}_{2,\mathscr{E}}(p) \;=\; p^2 + \alpha(p)p^{3/2} + \beta(p)p + O(p^{1/2}).$$

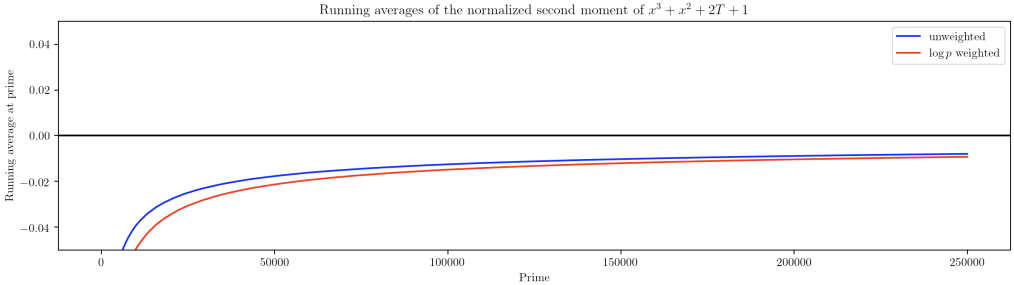
- We compute the *normalized second moment* of $\mathscr{A}_{2,\mathscr{E}}(p)$, which we define to be

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

and graph its running average and $\log p$-weighted running average to find potential positive bias families to investigate further with algebraic geometry.

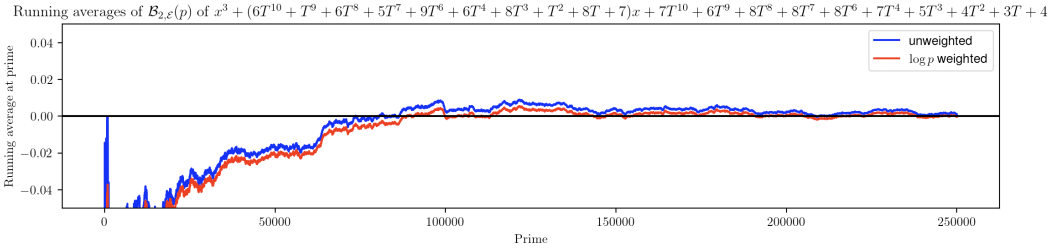
A Family with Known Negative Bias

For $\mathscr{E} : y^2 = x^3 + x^2 + 2T + 1$, we know that $\mathscr{A}_{2,\mathscr{E}}(p) = p^2 - 2p - 3$ has negative bias.

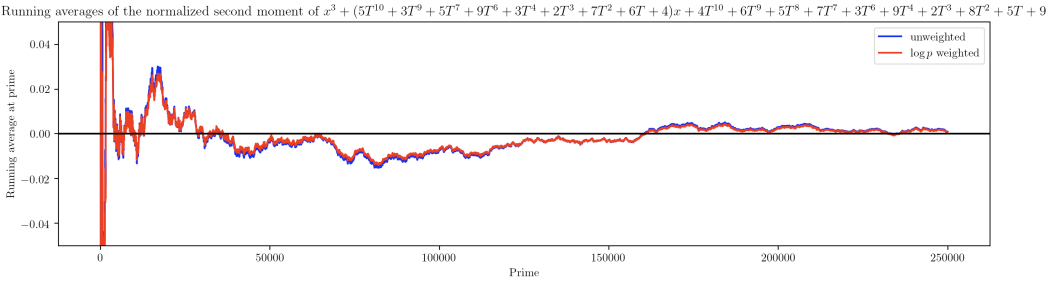


SMALL '24 Generic Random Family 1

We sampled coefficients iid from $\{0, 1, \ldots, 9\}$ and obtained the following families.

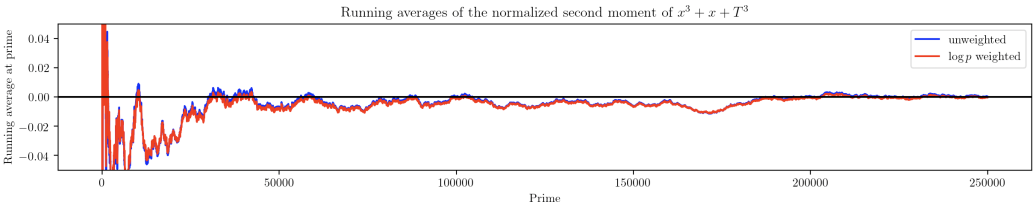


SMALL '24 Generic Random Family 2



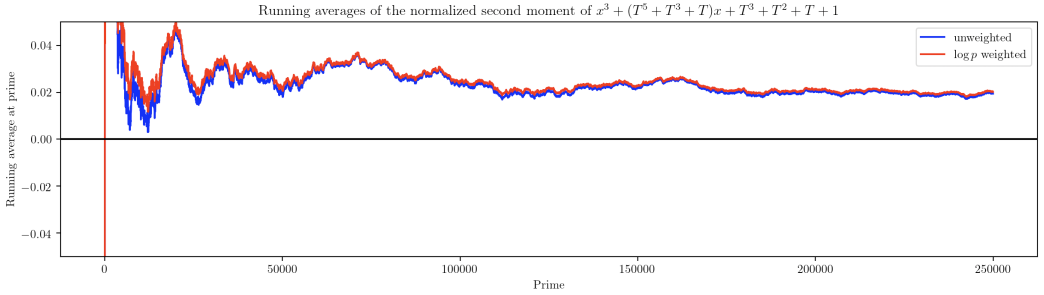
SMALL '23 Family

Recall that the SMALL '23 family $\mathscr{E} : y^2 = x^3 + x + T^3$ has positive bias for all primes $p \equiv 2 \bmod 3$, unknown bias for rest.



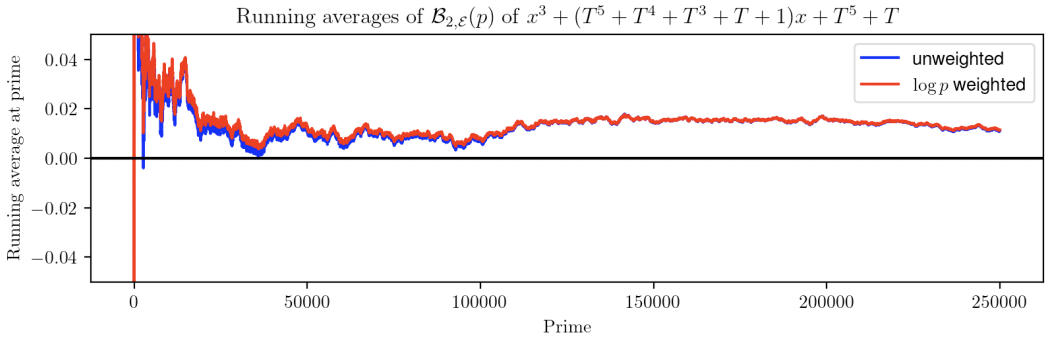
SMALL '24 Potential Positive Bias Family 1: $x^3 + (T^5 + T^3 + T)x + T^3 + T^2 + T + 1$

$$A(T) = T(T^2 - T + 1), \quad B(T) = (T+1)(T^2+1)$$



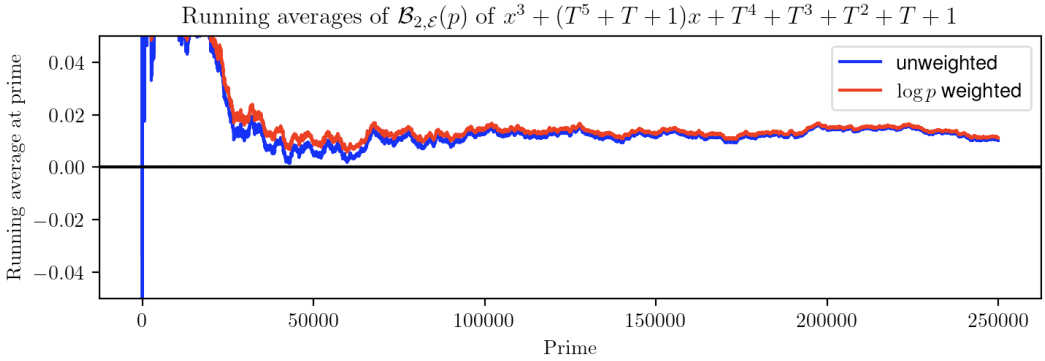
SMALL '24 Potential Positive Bias Family 2: $x^3 + (T^5 + T^4 + T^3 + T + 1)x + T^5 + T$

$$A(T) = (T+1)^2(T^2 - T + 1), \quad B(T) = T(T^4 + 1)$$



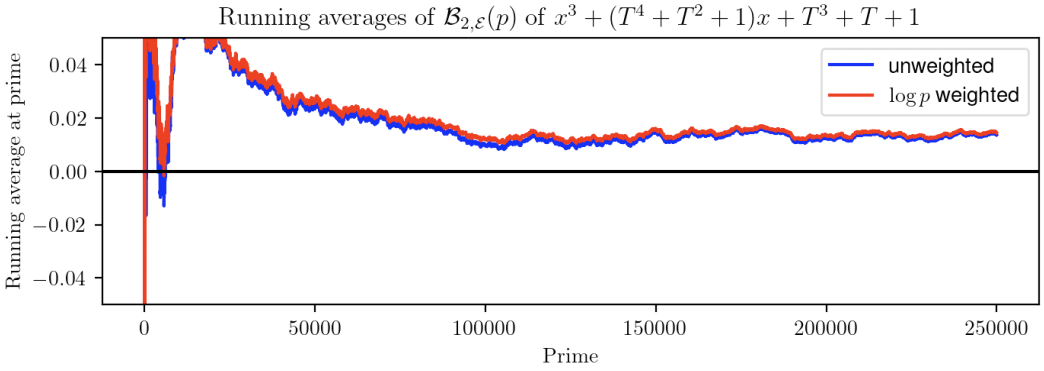
SMALL '24 Potential Positive Bias Family 3: $x^3 + (T^5 + T + 1)x + T^4 + T^3 + T^2 + T + 1$

$$A(T) = (T^2 + T + 1)(T^3 + T^2 - 1), \quad B(T) = (T + 1)(T^2 + 1)$$

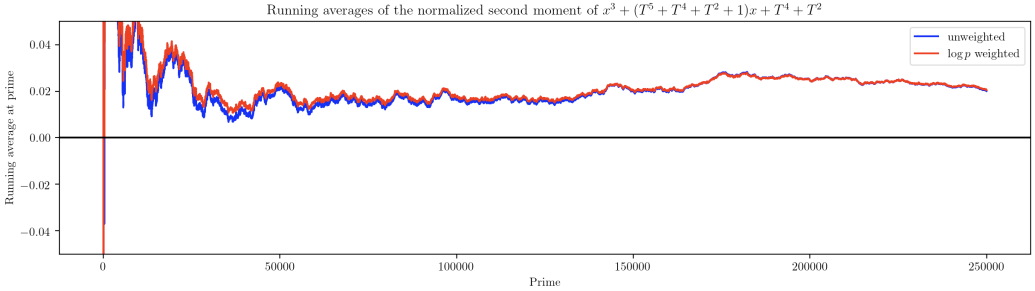


SMALL '24 Potential Positive Bias Family 4: $x^3 + (T^4 + T^2 + 1)x + T^3 + T + 1$

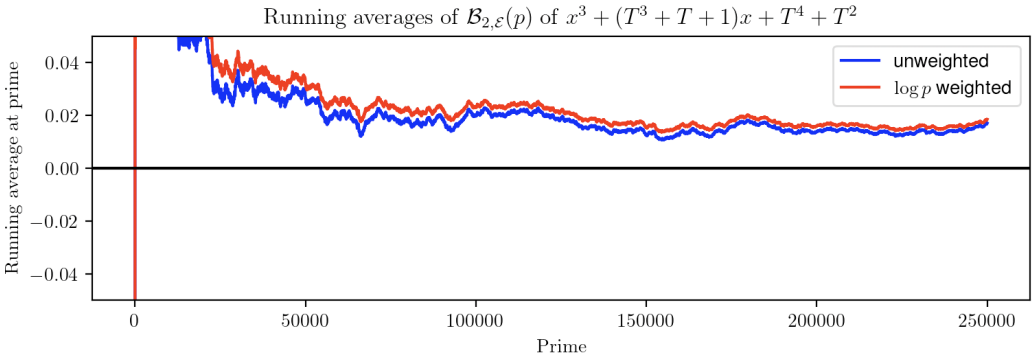
$$A(T) = (T^2 - T + 1)(T^2 + T + 1)$$



SMALL '24 Potential Positive Bias Family 5: $x^3 + (T^5 + T^4 + T^2 + 1)x + T^4 + T^2$

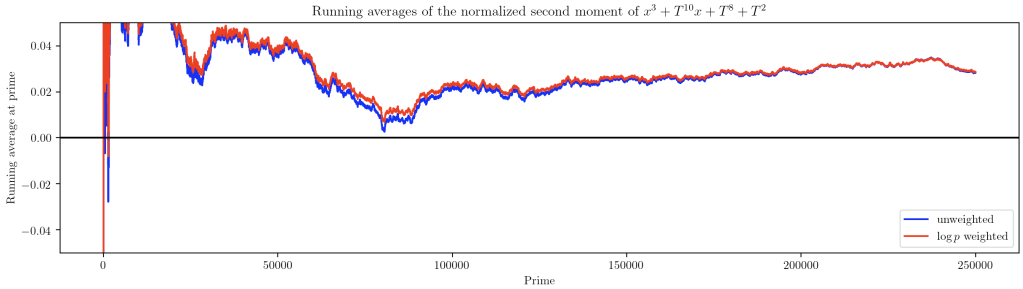


SMALL '24 Potential Positive Bias Family 6: $x^3 + (T^3 + T + 1)x + T^4 + T^2$



SMALL '24 Potential Positive Bias Family 7: $x^3 + T^{10}x + T^8 + T^2$

$$B(T) = T^2(T^4 - T^2 + 1)(T^2 + 1)$$



Assuming there is zero bias, this is a 4.5σ deviation. This happens ~ 3.4 in one million times.

1 Introduction

2 Computation of a_p

3 Computational Investigation

4 Normalized Second Moment

5 Algebraic Geometry

Motivation

Theorem (Sato-Tate, Taylor et al. 2006 and 2008)

Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication, then $a_p/\sqrt{p}$ converges to a semicircular distribution.

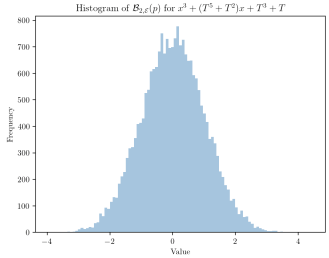
Motivation

Theorem (Sato-Tate, Taylor et al. 2006 and 2008)

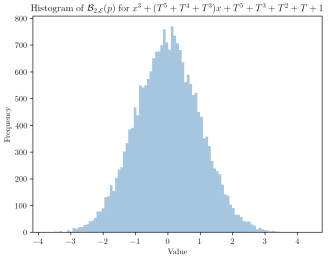
Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication, then $a_p/\sqrt{p}$ converges to a semicircular distribution.

This motivates the exploration of the distribution of the normalized second moment.

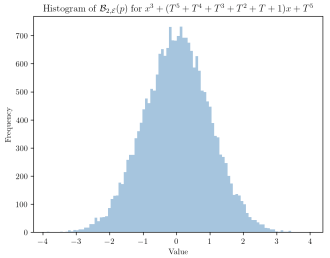
Distribution of the normalized second moment



Variance = 1.0151610262691482



Variance = 1.0046817588446215



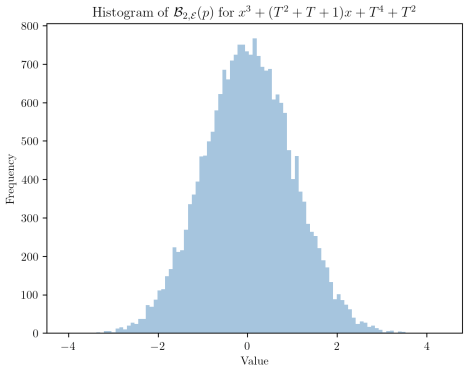
Variance = 0.9891139950619033

Conjecture

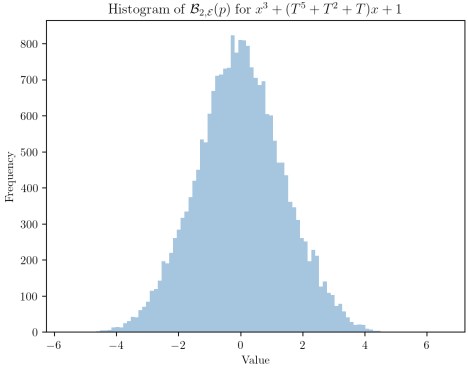
The variance of normalized second moments of a one-parameter family converges to an integer.

Question

What distribution does $\mathscr{B}_{2,\mathscr{E}}(p)$ converge to and what determines the variance?

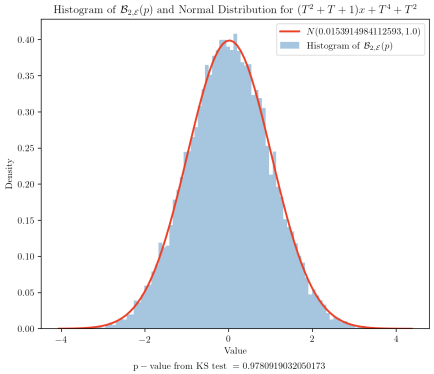


Variance = 0.9941929897237586

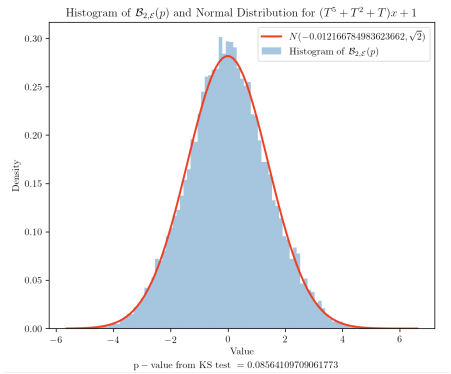


Variance = 1.9905981294487558

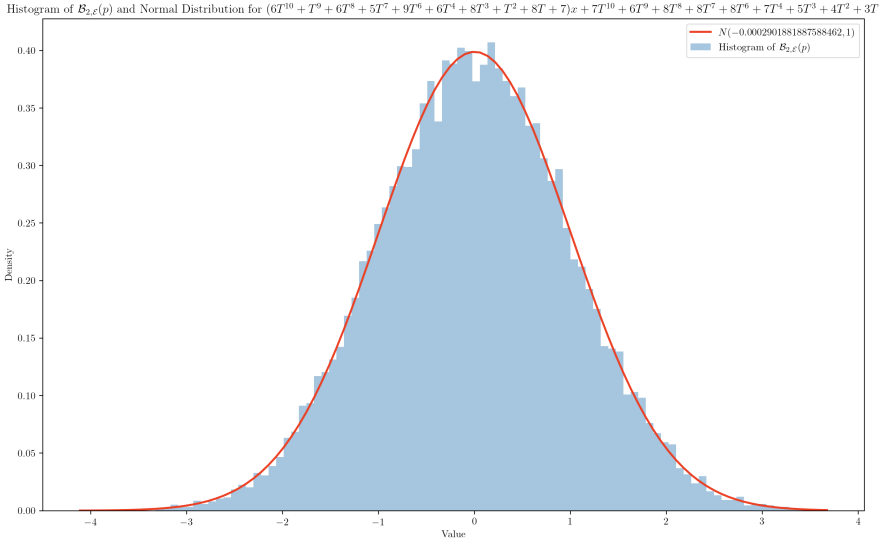
An Open Problem: Gaussian-like Behavior

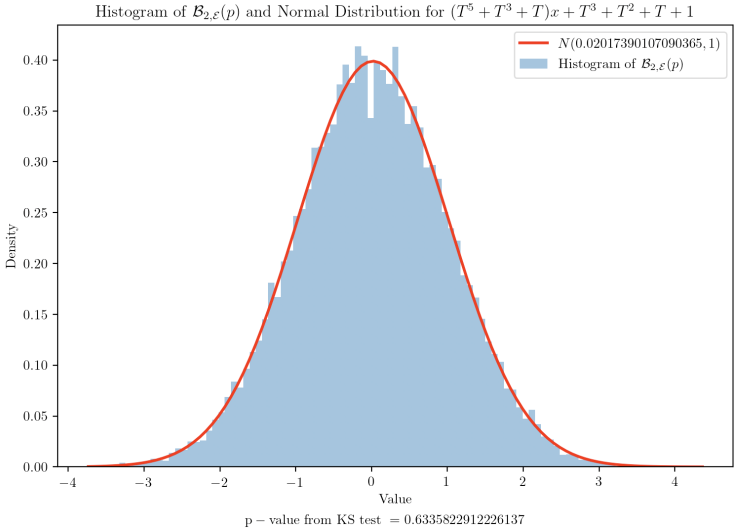


Variance = 0.9941929897237586



Variance = 1.9905981294487558


Histogram of $\mathcal{B}_{2,\mathcal{E}}(p)$ and Normal Distribution for $(6T^{10}+T^9+6T^8+5T^7+9T^6+6T^4+8T^3+T^2+8T+7)x+7T^{10}+6T^9+8T^8+8T^7+8T^6+7T^4+5T^3+4T^2+3T+4$
$N(-0.00029018818875884 62, 1)$
Histogram of $\mathcal{B}_{2,\mathcal{E}}(p)$
Density
Value
0.00
0.05
0.10
0.15
0.20
0.25
0.30
0.35
0.40
−4
−3
−2
−1
0
1
2
3
4


Histogram of $\mathcal{B}_{2,\mathcal{E}}(p)$ and Normal Distribution for $(T^5+T^3+T)x+T^3+T^2+T+1$
$N(0.02017390107090365, 1)$
Histogram of $\mathcal{B}_{2,\mathcal{E}}(p)$
Density
Value
p − value from KS test = 0.6335822912226137

1 Introduction

2 Computation of a_p

3 Computational Investigation

4 Normalized Second Moment

5 Algebraic Geometry

Threefolds

We relate the bias in the second moment to point counting on a threefold. For a given one parameter family $y^2 = x^3 + A(T)x + B(T)$, consider the surface

$$y_i^2 z_i = x_i^3 + A(T)x_i z_i^2 + B(T)z_i^3, \qquad \text{for } i = 1, 2.$$

Threefolds

We relate the bias in the second moment to point counting on a threefold. For a given one parameter family $y^2 = x^3 + A(T)x + B(T)$, consider the surface

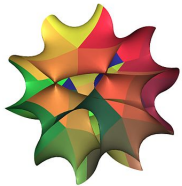
$$y_i^2 z_i = x_i^3 + A(T)x_i z_i^2 + B(T)z_i^3, \quad \text{for } i = 1, 2.$$

To make these calculations possible, we need to be in weighted projective space. If $\deg A \leq 4$ and $\deg B \leq 6$, we let $A(T, U)$ and $B(T, U)$ be the homogenizations of $A(T)$ and $B(T)$ to degree 4 and 6 we consider the threefold

$$V : y_i^2 z_i = x_i^3 + A(T, U)x_i z_i^2 + B(T, U)z_i^3, \quad \text{for } i = 1, 2.$$

Rational Threefold

In general, V is extremely complicated, e.g., a Calabi-Yau manifold:



- However, if for $p > 7$, we can control our elliptic surface mod p, then V becomes rational.
- In some sense this means our singularities are controllable.
- From there one can use known techniques to count points on V mod p.

Acknowledgements

We are grateful to Professor Steven J. Miller for suggesting this problem and for his mentorship. We would also like to thank Adam Logan for many helpful conversations.

This research was supported by the National Science Foundation, under grant DMS2241623, Duke University, Princeton University, the University of Michigan, and Williams College.

References

[1] Z. Batterman, A. Jambhale, S.J. Miller, A. L. Narayanan, K. Sharma, C. Yao, *Applications of Moments of Dirichlet Coefficients in Elliptic Curve Families*, ICERM Conference Proceedings for the July 2023 Murmurations Workshop.

[2] T. Cheek, P. Gilman, K. Jaber, and M. Tomé. Elliptic Curve Coding. GitHub repository. 2024. https://github.com/KareemSaysHi/SMALL2024-Elliptic-Curve-Coding.

[3] Andrew J. Hanson, "A construction for computer visualization of certain complex curves," Notices of the Amer. Math. Soc. 41 (9): 1156-1163, (November/December 1994).

[4] P. Michel, *Rang moyen de familles de courbes elliptiques et lois de Sato-Tate*, Mont. Math. 120 (1995) 127-136.

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

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

[7] S. J. Miller, *Variation in the number of points on elliptic curves and applications to excess rank*, C. R. Math. Acad. Sci. Soc. R. Can., 27 (2005) no. 4, 111–120.

[8] S. J. Miller, *Investigations of zeros near the central point of elliptic curve L-functions*, Exp. Math. 15 (2006), no. 3, 257–279.

[9] K. Nagao, $\mathbb{Q}(T)$*-rank of elliptic curves and certain limit coming from local points*, Manuscr. Math. 92 (1997) 13-32.

[10] M. Rosen and J. H. Silverman, *On the rank of an elliptic surface*, Invent. Math. 133 (1998), 43-67.

[11] K. Rubin and A. Silverberg. *Ranks of Elliptic Curves*, Bull. AMS 39 (2002), 455-474.