Biases in First and Second Moments of the Fourier Coefficients in One- and Two-Parameter Families of Elliptic Curves

Jiefei(Michelle) Wu
Westminster School

February 13, 2020

Abstract

Let $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$ be a non-trivial one-parameter family of elliptic curves, and consider the k^{th} moments $pA_{k,\mathcal{E}(p)} := \sum_{t \bmod p} a_{\mathcal{E}_t}(p)^k$ of the Fourier coefficients $a_{\mathcal{E}_t}(p) := p + 1 - |\mathcal{E}_t(\mathbb{F}_p)|$. Rosen and Silverman proved that if $\mathcal{E}$ is a rational surface then there is a negative bias in the first moment $A_{1,\mathcal{E}(p)}$ (this is conjectured to hold for all elliptic surfaces); this bias is responsible for the rank of the elliptic surface. Michel investigated the second and higher moments; these are important as well and are related to the distribution of zeros of the L-function associated to the elliptic curve. He proved that $pA_{2,\mathcal{E}(p)} = p^2 + O(p^{3/2})$, with the lower order terms of size $p^{3/2}, p, p^{1/2}$ and 1 having important cohomological interpretations. In his Ph.D. thesis, Miller proposed that there is also a bias in the second moment, and the largest lower-order coefficient that does not average to zero is on average negative. This was proven for many families by Mackall, Miller, Rapti, and Winsor, and explains some of the disagreements between theory and computations for the small conductors for the distribution of ranks in families of elliptic curves; reconciling this disparity is one of the most important questions in the subject (it is still an open question, for example, if the rank can be arbitrarily large). If the bias conjecture holds, then it helps to explain for small conductors why numerically on average the rank is higher than expected, which helps us to understand one of the million dollar Clay Millenium prizes - the Birch and Swinnerton-Dyer Conjecture - which states that the geometric rank of a rational elliptic surface equals to its analytic rank. In this paper, we explore the first and second moments of some one- and two-parameter families of elliptic curves, looking to see if the biases persist and exploring the consequence these have on fundamental properties of elliptic curves. We observe that in all of the one- and two-parameter families we proved theoretically that the first term that does not average to zero in the second-moment expansion of the Fourier coefficients has a negative average. We found a potential counterexample to a stronger form of Miller's Conjecture based on the families studied to date, which is that the first term that does not average to zero is the p term and that has a negative average. While we are not able to prove it, the numerical data strongly suggests that the only term that does not average to zero is the constant term, which has a small negative bias of -1.

Keywords: Elliptic Curves, Legendre Symbol, Biases, Ranks, Birch and Swinnerton-Dyer Conjecture.

Contents

1 Introduction **4**
- 1.1 Basic Concepts of Elliptic Curves 4
- 1.2 Why Do We Care About the Biases? 10
- 1.3 The Bias Conjecture 16

2 Tools for Calculating Biases **17**

3 Biases in First and Second Moments in One-Parameter Families **20**
- 3.1 Construction of Rank 0 Families 20
  - 3.1.1 $y^2 = x^3 - x^2 - x + t$ 20
  - 3.1.2 $y^2 = x^3 - tx^2 + (x-1)t^2$ 22
- 3.2 Construction of Rank 1 Families 24
  - 3.2.1 $y^2 = x^3 + tx^2 + t^2$ 24
  - 3.2.2 $y^2 = x^3 + tx^2 + x + 1$ 28
  - 3.2.3 $y^2 = x^3 + tx^2 + tx + t^2$ 30
- 3.3 Construction of Rank 2 Families 34
  - 3.3.1 $y^2 = x^3 - x^2 + (x^2 - x)t + 1$ 34
  - 3.3.2 $y^2 = x^3 - x + t^4$ 36

4 Biases in First and Second Moments in Two-Parameter Families **37**
- 4.1 Construction of Rank 0 Families 38
  - 4.1.1 $y^2 = x^3 + tx + sx^2$ 38
  - 4.1.2 $y^2 = x^3 + t^2x + st^4$ 40
  - 4.1.3 $y^2 = x^3 + sx^2 - t^2x$ 43
- 4.2 Construction of Rank 1 Families 46
  - 4.2.1 $y^2 = x^3 + ts^2x^2 + (t^3 - t^2)x$ 46
  - 4.2.2 $y^2 = x^3 + t^2x^2 + (t^3 - t^2)sx$ 48
- 4.3 Construction of Rank 2 Families 50
  - 4.3.1 $y^2 = x^3 + t^2x^2 - (s^2 - s)t^2x$ 50
  - 4.3.2 $y^2 = x^3 - t^2x + t^3s^2 + t^4$ 53

5 Conclusion and Future Work **55**

6 Acknowledgements **57**

7 Declaration of Academic Integrity **57**

A Proof of Linear and Quadratic Legendre Sums **57**

B Proof of Rational Surfaces for One-Parameter Families **59**
B.1 Rank 0 One-Parameter Families 60
B.1.1 $y^2 = x^3 - x^2 - x - t$ 60
B.1.2 $y^2 = x^3 - tx^2 + (x - 1)t^2$ 60
B.2 Rank 1 One-Parameter Families 61
B.2.1 $y^2 = x^3 + tx^2 + t^2$ 61
B.2.2 $y^2 = x^3 + tx^2 + x + 1$ 61
B.2.3 $y^2 = x^3 + tx^2 + tx + t^2$ 62
B.3 Rank 2 One-Parameter Families 62
B.3.1 $y^2 = x^3 - x^2 + (x^2 - x)t + 1$ 62
B.3.2 $y^2 = x^3 - x + t^4$ 63

C Data Table For Rank 2 One-Parameter Families **64**
C.1 Second Moment of $x^3 - x^2 + (x^2 - x)t + 1$ 64
C.2 First Moment of $x^3 - x + t^4$ 65
C.3 Second Moment of $x^3 - x + t^4$ 66

D Mathematica Code For Computing the First and Second Moment **66**
D.1 First Moment Computation 66
D.2 Second Moment Computation 66
D.3 Statistics Display 67

E References **67**

1 Introduction

Elliptic curves generalize well-known concepts such as the Pythagorean triples and the rational points on the unit circle. They are also a key to Andrew Wiles' proof of the famous Fermat's Last Theorem. They have wide applications in cryptocurrency Bitcoin and cryptography.

In this section, we first define some basic concepts of elliptic curves; our main sources are [Mi4, MMRW, Rub, Si0, ST]. Next, we introduce previous findings on the bias conjecture. Then, we compute biases in the first and second moments of some one- and two- parameter families using methods from [Mi1] to see if the bias conjecture holds. In addition to looking at some new one-parameter families, this paper explores two-parameter families for the first time, since previous research papers focused only at one-parameter families or the family of all elliptic curves.

1.1 Basic Concepts of Elliptic Curves

We start with the Pythagorean Theorem. The Pythagorean theorem states that if a, b, and c are the sides of a right triangle, then

$$a^2 + b^2 = c^2. \tag{1.1}$$

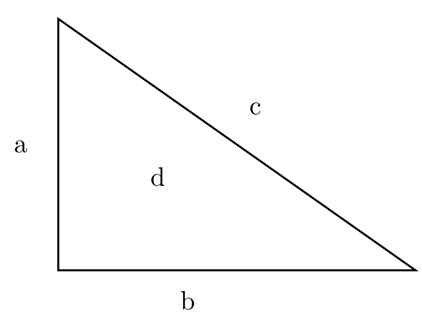


Figure 1: A right triangle with side length a, b and c and area d

Lemma 1.1 (Pythagorean Triples)**.** *Given any Pythagorean triple there exist m and n with $m > n > 0$ such that*

$$a = k \cdot (m^2 - n^2), \;\; b = k \cdot (2mn), \;\; c = k \cdot (m^2 + n^2), \tag{1.2}$$

where m, n and k are positive integers with $m > n$ and with m and n are coprime and not both odd, can generate all Pythagorean Triples.

After we finish studying how to generate the rational points on a quadratic equation $a^2+b^2=c^2$, we are going to study how to generate the rational points on a cubic equation.

Let $x=a/c$ and $y=b/c$, and we have a unit circle

$$x^2+y^2=1 \tag{1.3}$$

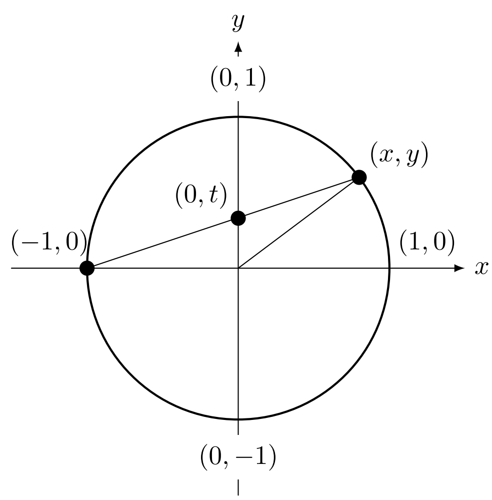


Figure 2: A rational parametrization of the circle $x^2+y^2=1$

We know one rational solution, $(-1,0)$. The line through (x,y) with slope t is given by the equation:

$$y \quad = \quad t(1+x). \tag{1.4}$$

Hence, the other point of intersection is

$$1-x^2 \quad = \quad y^2=t^2(1+x)^2. \tag{1.5}$$

Dividing each side by the root $x=-1$, we get

$$1-x \quad = \quad t^2(1+x). \tag{1.6}$$

Using the above relation, we get

$$x=\frac{1-t^2}{1+t^2}\ ,\ y=\frac{2t}{1+t^2}. \tag{1.7}$$

We can see that if x and y are rational numbers, then the slope $t = y/(1+x)$ will be a rational number too. Conversely, if t is a rational number, then x and y will be rational numbers too. Hence, by plugging random rational numbers numbers for t, we can generate all the rational numbers on the circle (except $x = -1$ in this case, because t is infinite).

Combining the area formula for a right triangle (1.1), equation of the unit circle (1.3) as well as the rational parametrization of the unit circle (1.6) together, we get

$$\begin{aligned} 1 &= \frac{1}{2}ab \\ &= \frac{1}{2}c^2xy \\ &= \frac{1}{2}c^2\left(\frac{1-t^2}{t^2+1}\right)\left(\frac{2t}{t^2+1}\right) \\ &= \frac{c^2}{(t^2+1)^2}(t-t^3). \end{aligned} \tag{1.8}$$

Dividing both sides by $c^2/(t^2+1)^2$, we get

$$(\frac{t^2+1}{c})^2 = t - t^3. \tag{1.9}$$

Let $Y = (t^2+1)/c$ and $X = -t$. We have

$$Y^2 = X^3 - X, \tag{1.10}$$

which is an equation of an elliptic curve.

Definition 1 (Elliptic Curve)**.** *A curve given by the equation*

$$y^2 = x^3 + ax + b \tag{1.11}$$

is an elliptic curve, where $a, b \in \mathbb{Q}$ and $4a^3 + 27b^2 \neq 0$ because we want to avoid degenerate cases. For example, we do not want $y^2 = x^2(x-1)$ to be an elliptic curve; when we send y to xy we get $y^2 = x - 1$, a parabola.

In this paper, we are going to study two kinds of families of elliptic curves: one-parameter and two-parameter. For the families we compute in this paper, we can do a change of variable to make the elliptic curves look like what we write in the introduction, but for convenience we often have an x^2 term.

Definition 2 (One-Parameter Family of Elliptic Curves)**.** *Let*

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

be a non-trivial one-parameter family, with $A(T), B(T) \in \mathbb{Q}[T]$*, which are polynomials of finite degree and rational coefficients.*

Definition 3 (Two-Parameter Family of Elliptic Curves)**.** *Let*

$$y^2 \ = \ x^3 + A(T,S)x + B(T,S)$$

be a non-trivial two-parameter family, with $A(T,S), B(T,S) \in \mathbb{Q}[T,S]$.

Elliptic curves have many applications. We have already seen one, where the answer of whether or not there is a rational right triangle with area d is related to the group of rational solutions of an associated curve. Another is the famous Fermat's Last Theorem.

Theorem 1.2 (Fermat's Last Theorem)**.** *For every integer* $n \geq 3$ *the equation*

$$A^n + B^n \ = \ C^n \tag{1.12}$$

has no solutions in non-zero integers A*,* B *and* C*.*

Building on the work of many others Wiles was able to prove the above by showing that if there existed a solution, it would lead to an elliptic curve with special properties, and then proving that no such curve exists.

Next, we are going to discuss some interesting properties of elliptic curves. For E the elliptic curve $y^2 = x^3 + ax + b$, the set of rational points is all pairs of rational numbers (x, y) such that $y^2 = x^3 + ax + b$. We denote this set by $E(\mathbb{Q})$. One of the major results of the subject is that we can define an addition law on the elements of $E(\mathbb{Q})$, which turns this set into a group. See Figure 3 for an illustration.

We do this as follows. Let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be two points in $E(\mathbb{Q})$, and consider the line connecting them (if $P = Q$ we take the tangent line to the curve at P). As the two points have rational coordinates, the slope of the line is rational, and using the point-slope form of the line we see that the line connecting them can be written as $y = mx + c$ for rational m and c. The line will intersect the elliptic curve in one more point. Substituting we find

$$(mx + c)^2 \ = \ x^3 + ax + b;$$

we already know two solutions to this ($x = x_1, x_2$). As a, b, m, c, x_1, x_2 are rational, the third root x_3 is also rational, and then so too is y_3; if we define $P+Q$ to be the reflection of this third point about the x-axis, namely $(x_3, -y_3)$, it turns out that $E(\mathbb{Q})$ is a group (the zero element is the "point at infinity").

Theorem 1.3 (Properties of Addition)**.** *The additional law on* $E(\mathbb{Q})$ *has the following properties:*

$$\begin{aligned} &(1) \quad P + (Q + R) = (P + Q) + R, \ \textit{for all } P, Q, R \in E. \\ &(2) \quad P + Q = Q + P, \ \textit{for all } P, Q \in E. \\ &(3) \quad P + P = 2P, \ \textit{for all } P \in E. \end{aligned}$$

See Figure 3 for an illustration.

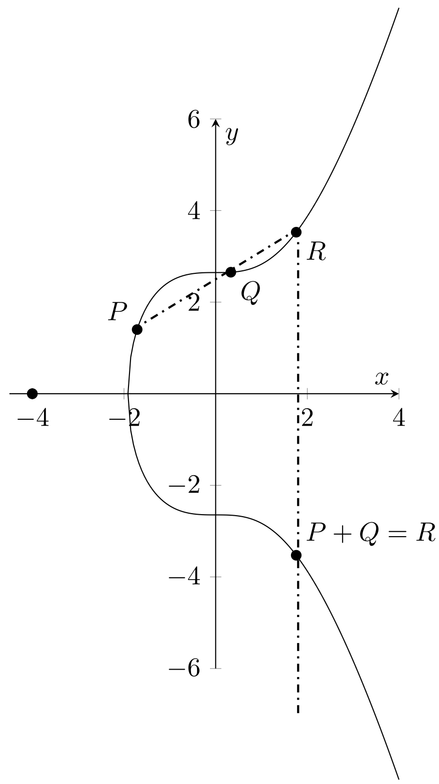


Figure 3: Demonstrating the addition law for the elliptic curve $E(\mathbb{Q})$: $y^2 = x^3 + 7$.

Theorem 1.4 (Group of Rational Points)**.** *Mordell's theorem states that a group of rational points is finitely generated on a non-singular cubic elliptic curve.*

Next, we are going to define one characteristic of elliptic curves that is relevant to our paper. Often one can gain an understanding of a global object by studying a local one. In particular, for a prime p we can look at how often we have pairs (x, y) satisfying $y^2 = x^3 + ax + b \bmod p$. As half the non-zero elements of $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \ldots, p-1\}$ are non-zero squares modulo p and the other half are not squares, it is reasonable to expect that for a randomly chosen x that half the time it will generate two solutions modulo p and half the time it will generate zero. Thus we expect the number of pairs to be of size p, and it is valuable to look at fluctuations about this expected number.

Definition 4 (Fourier Coefficients)**.** *For E an elliptic curve $y^2 = x^3 + ax + b$ and a prime p, we define the Fourier coefficients $a_E(p)$ by*

$$a_E(p) \ := \ p - |E(\mathbb{F}_p)|, \tag{1.13}$$

where $|E(\mathbb{F}_p)|$ is the number of solutions (x, y) to $y^2 = x^3 + ax + b \bmod p$ with $x, y \in \mathbb{F}_p$. These are used in constructing the associated L-function to the elliptic curve.

There is a very useful formula for $a_E(p)$ (sometimes if the curve E is clear we will write $a(p)$ or a_p). Recall the Legendre symbol $\left(\frac{a}{p}\right)$; it is zero if a is zero modulo p, it is 1 if a is a non-zero square modulo p, and -1 otherwise. Thus $1 + \left(\frac{x^3+ax+b}{p}\right)$ is the number of solutions modulo p for a fixed x. If we sum this over all x modulo p we obtain $|E(\mathbb{F}_p)|$, and thus

$$a_E(p) \ = \ -\sum_{x \bmod p} \left(\frac{x^3 + ax + b}{p}\right). \tag{1.14}$$

Definition 5 (Fourier Coefficients of A Specialized Curve)**.** *We specialize T to an integer t and obtain an elliptic curve $\mathcal{E}_t$ with coefficient $a_{\mathcal{E}_t}(p)$:*

$$a_{\mathcal{E}_t}(p) \ := \ p - |\mathcal{E}_t(\mathbb{F}_p)| \tag{1.15}$$

where $|\mathcal{E}_t(\mathbb{F}_p)|$ is the number of points over $\mathbb{F}_p$, the finite field. As before, we have

$$a_{\mathcal{E}_t}(p) \ = \ -\sum_{x \bmod p} \left(\frac{x^3 + A(t)x + B(t)}{p}\right). \tag{1.16}$$

Much is known about the $a(p)$'s. For our work we only need to know their size, though recent breakthroughs have determined much more about their distribution.

Theorem 1.5 (Hasse)**.** *In 1931, Hasse proved the Riemann Hypothesis for finite fields: if E is an elliptic curve and p a prime, then*

$$|a_E(p)| \ \le \ 2\sqrt{p}. \tag{1.17}$$

Hasse's theorem tells us that the fluctuations in the number of solutions from the expected value p are on the order of $\sqrt{p}$; this is very similar to square-root cancellation seen in many other problems in number theory.

Last but not least, we are going to define some other important characteristic of elliptic curves.

Definition 6 (Moment of a One-Parameter Family)**.** *Let $\mathcal{E}$ be a one parameter family of elliptic curves over $\mathbb{Q}(T)$, with $\mathcal{E}_t$ the specialized curves. For each positive integer r, we define the r^{th} moment of the traces of Frobenius by:*

$$A_{\mathcal{E},r(p)} \ := \ \frac{1}{p} \sum_{t \bmod p} a_{\mathcal{E}_t}(p)^r. \tag{1.18}$$

There is a natural extension to two-parameter families, where we sum over s and t modulo p.

Definition 7 (Big-Oh Notation)**.** *We say $f = O(g(x))$, read f is the big-Oh of g, if there exists an x_0 and a $B > 0$ such that for all $x \geq x_0$ we have $|f(x)| \leq Bg(x)$.*

Definition 8 (Rank)**.** *We can write the group of rational solutions of an elliptic curve E as an infinite lattice (r copies of $\mathbb{Z}$, where r is a non-negative integer) and a finite torsion part:*

$$E(\mathbb{Q}) \;\cong\; \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}. \tag{1.19}$$

The geometric rank is the number of copies of $\mathbb{Z}$, or the number of independent points of infinite order. The analytic rank is the order of vanishing of the associated L-function at the central point. We move on to discuss one well-known problem of elliptic curve L-functions: the Birch and Swinnerton-Dyer conjecture.

In the next section, we are going to talk about the connection between ranks and biases, which is tied to another unsolved Millennium Prize Problem, the Riemann Hypothesis.

1.2 Why Do We Care About the Biases?

It is well known that the probability that a random integer up to x is prime is approximately $1/\log(x)$. However, the finer properties of the distribution of primes remains a mystery. The Riemann zeta function $\zeta(s)$ (see [Da] for more information), which connects integers to primes, can help us understand their distribution. We have for $\mathrm{Re}(s) > 1$

$$\zeta(s) \;:=\; \sum_{n=1}^{\infty} \frac{1}{n^s} \;=\; \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}; \tag{1.20}$$

the zeta function is defined as the sum over integers above, but its utility comes from the product expansion. The equivalence of these two expressions is due to the Fundamental Theorem of Arithmetic and the geometric series formula. Initially defined only for $\mathrm{Re}(s) > 1$, the zeta function can be analytically continued to the entire complex plane with a simple pole of residue 1 at $s = 1$. The line $\mathrm{Re}(s) = 1/2$ is the critical line, and $s = 1/2$ the central point.

While the deepest connections between the zeta function and the primes comes from applying results of complex analysis to the zeros of $\zeta(s)$, a lot can be deduced just by looking at the series expansion for real $s > 1$. We give two examples. First, when s goes to 1 from above the sum converges to the harmonic series, which diverges. Thus there must be infinitely many primes, as if there were only finitely many the sum would converge as $s \to 1$.

Another example is $\zeta(2)$. Euler showed that

$$\zeta(2) \;=\; \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \cdots \;=\; \frac{\pi^2}{6}, \tag{1.21}$$

which is irrational; however, if there were only finitely many primes then the product would be rational. Hence, there must be infinitely many primes.

As remarked above, while initially defined only for $\mathrm{Re}(s) > 1$, $\zeta(s)$ can be analytically continued to the entire complex plane, and satisfies a functional equation:

$$\xi(s) \ := \ \Gamma\left(\frac{s}{2}\right)\pi^{-\frac{s}{2}}\zeta(s) \ = \ \xi(1-s). \tag{1.22}$$

Riemann hypothesized that all the complex zeros of $\zeta(s)$ lie on the critical line $Re(s) = 1/2$. This conjecture remains one of the most difficult and important problems in mathematics. Its importance stems from the fact that by doing a contour integral of the logarithmic derivative of $\zeta(s)$ and shifting contours, one obtains the Explicit Formula, which relates a sum over zeros to a sum over prime.

Interestingly, the behavior of spacings between zeros of L-functions is similar to that of energy levels of heavy nuclei, and to eigenvalues of random matrix ensembles. In order to compare all these objects, it is useful to rescale so they have mean spacing one. Thus different objects are rescaled differently. As the average spacing between primes of size x is approximately $\log x$, we divide the gaps between primes by $\log x$ to obtain a sequence with mean spacing one. For zeros of $\zeta(s)$ high on the critical line $\mathrm{Re}(s) = 1/2$, the average spacing between zeros with imaginary part T is about $1/\log T$, so here we would multiply by $\log T$. Later we will study families of L-functions and their zeros near the central point, and will comment on the renormalization.

We now move on to discuss other L-functions, which generalize the Riemann zeta function. For the zeta function in the series expansion the coefficient of n^{-s} is always 1, and we have a product of degree one. For L-functions associated to elliptic curves, the coefficients at a prime p are related to counting the number of solutions modulo p, and we have a degree two product. There are unfortunately two ways to normalize the L-function, depending on whether or not we look at $a(p)$ or $a(p)/\sqrt{p}$. We use the former, and thus our L-function will have critical strip $0 < \mathrm{Re}(s) < 2$ and central point is $s = 1$; the latter gives a critical strip of $0 < \mathrm{Re}(s) < 1$ with central point $s = 1/2$.

Definition 9 (L-function)**.** *The Hasse-Weil L-function of an elliptic curve E : $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with coefficient $a_E(p)$ and discriminant Δ*

$$\Delta \ := \ -{b_2}^2 b_8 - 8{b_4}^3 - 27{b_6}^2 + 9b_2b_4b_6, \tag{1.23}$$

where $b_2 = {a_1}^2 + 4a_4$, $b_4 = 2a_4 + a_1a_3$ and $b_6 = {a_3}^2 + 4a_6$, is defined as

$$L(s,E) \quad := \quad \prod_{p|\Delta} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid\Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}}. \tag{1.24}$$

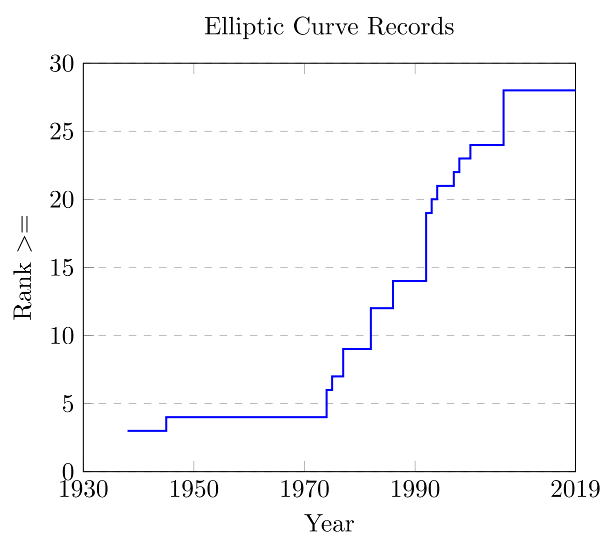
See [Kn].

Similar to the zeta function, these L-functions take local data and create a global object, from which much can be deduced. The most important of these inferences is the famous Birch and Swinnerton-Dyer conjecture.

Conjecture 1.6 (Birch and Swinnerton-Dyer Conjecture)**.** *The order of vanishing of $L(E, s)$ at the central point $s = 1$ is equal to the rank of the group of rational points $E(\mathbb{Q})$.*

In other words, Birch and Swinnerton-Dyer conjectured that the geometric rank of a rational elliptic curve equals to its analytic rank.

Unfortunately, it is not known what values of rank r are possible for rational elliptic curves. In 1938, Billing found an elliptic curve with rank 3. The largest known rank increased over the next few decades. The largest is due to Elkies in 2006, and is rank at least 28. Interestingly, there are not examples of elliptic curves for each rank smaller than 28 (see [Du] for a more comprehensive historical data on elliptic curve records):



Similar to using the Riemann Zeta function to understand the distribution of primes, we use the Explicit Formula ([KS]), which relates sums over primes of the Fourier coefficients $a_E(p)$ and $a_E^2(p)$ to sums of test functions over zeros, to deduce information about the zeros. Let us look at a one-parameter family $\mathcal{E} : y^2 = x^3 + A(t)x + B(t)$, with $t \in [N, 2N]$, and where ϕ is an even Schwartz-class function that decays rapidly (this means ϕ, and all of its derivatives, decay faster than $1/(1 + |x|)^A$ for any $A > 0$), $\log R$ is the average log conductor, and γ is the zeros of the L-function:

$$\frac{1}{N}\sum_{t=N}^{2N}\sum_{\gamma_t}\phi\left(\gamma_t\frac{\log R}{2\pi}\right) \;=\; \widehat{\phi}(0)+\phi(0)-\;\frac{2}{N}\sum_{t=N}^{2N}\sum_{p}\frac{\log p}{\log R}\frac{1}{p}\widehat{\phi}\left(\frac{\log p}{\log R}\right)a_t(p)$$
$$-\;\frac{2}{N}\sum_{t=N}^{2N}\sum_{p}\frac{\log p}{\log R}\frac{1}{p^2}\widehat{\phi}\left(\frac{2\log p}{\log R}\right)a_t(p)^2+O\left(\frac{\log\log R}{\log R}\right); \tag{1.25}$$

the result above comes from integrating the logarithmic derivative of the L-function against the Schwartz test function ϕ and then shifting contours.

Note that if the test function is non-negative, then dropping the contributions of ϕ at all the zeros that are not at the central point removes a non-negative amount from the left hand side. The right hand side then becomes an upper bound for the average rank of the elliptic curves in the family:

$$\frac{1}{N}\sum_{t=N}^{2N}\sum_{\gamma_t=0}\phi\,(0) \;\leq\; \widehat{\phi}(0)+\phi(0)-\;\frac{2}{N}\sum_{t=N}^{2N}\sum_{p}\frac{\log p}{\log R}\frac{1}{p}\widehat{\phi}\left(\frac{\log p}{\log R}\right)a_t(p)$$
$$-\;\frac{2}{N}\sum_{t=N}^{2N}\sum_{p}\frac{\log p}{\log R}\frac{1}{p^2}\widehat{\phi}\left(\frac{2\log p}{\log R}\right)a_t(p)^2+O\left(\frac{\log\log R}{\log R}\right), \tag{1.26}$$

which means that

$$\phi\,(0)*\text{AverageRank}(N) \;\leq\; \widehat{\phi}(0)+\phi(0)-\;\frac{2}{N}\sum_{t=N}^{2N}\sum_{p}\frac{\log p}{\log R}\frac{1}{p}\widehat{\phi}\left(\frac{\log p}{\log R}\right)a_t(p)$$
$$-\;\frac{2}{N}\sum_{t=N}^{2N}\sum_{p}\frac{\log p}{\log R}\frac{1}{p^2}\widehat{\phi}\left(\frac{2\log p}{\log R}\right)a_t(p)^2+O\left(\frac{\log\log R}{\log R}\right). \tag{1.27}$$

Thus when ϕ is non-negative, we obtain a bound for the average rank in the family by restricting the sum to be only over zeros at the central point. The error $O\left(\frac{\log\log R}{\log R}\right)$ comes from trivial estimation and ignores probable cancellation, and we expect $O\left(\frac{1}{\log R}\right)$ or smaller to be the correct magnitude. For most one-parameter families of elliptic curves we have $\log R \sim \log N^a$ for some integer a, where $t \in [N, 2N]$.

The main term of the first and second moments of the $a_t(p)$ give $\phi\,(0)*$ AverageRank(N) and $-\frac{1}{2}\phi(0)$; this is a standard application of the prime number theorem to evaluate the resulting sums; for details see the appendices on prime sums in [Mi1]. This is reminiscent of the Central Limit Theorem, where so long as some weak conditions are satisfied for independent, identically distributed random variables, their normalized sum converges to the standard normal. In that setting, if the moments are finite we can always adjust our distribution to have mean zero and variance one, and it is only these moments that enter the limiting analysis. The higher moments *do* have an impact, but it is only through the lower order terms, which control the *rate* of convergence.

We have a similar situation here. First, the higher moments of our Fourier coefficients contribute in the big-Oh terms $O\left(\frac{1}{\log R}\right)$. Second, the lower order terms in the first and second moments can contribute, but not to the main term in the expansions above. Explicitly, assume the second moment of $a_t(p)^2$ is $p^2 - m_{\mathcal{E}}p + O(1)$, $m_{\mathcal{E}} > 0$. We have already handled the contribution from p^2, and $-m_{\mathcal{E}}p$ contributes

$$\begin{aligned} S_2 \quad &\sim \quad \frac{-2}{N}\sum_p \frac{\log p}{\log R}\widehat{\phi}\left(2\frac{\log p}{\log R}\right)\frac{1}{p^2}\frac{N}{p}(-m_{\mathcal{E}}p) \\ &= \quad \frac{2m_{\mathcal{E}}}{\log R}\sum_p \widehat{\phi}\left(2\frac{\log p}{\log R}\right)\frac{\log p}{p^2}. \end{aligned} \tag{1.28}$$

We have a prime sum which converges between ϕ that decays, and this sum is bounded by $\sum_p \log p/p^2$. Thus, S_2 converges and there is a contribution of size $1/\log(R)$. This is the motivation behind why the Bias Conjecture, which S. J. Miller conjectured in his thesis [Mi1], matters, as a bias has an impact in our estimates on the rank and the behavior of zeros near the central point.

Conjecture 1.7 (Bias Conjecture for the Second Moment of Fourier Coefficients of Elliptic Curve L-Functions)**.** *Consider a family of elliptic curves. Then the largest lower term in the second moment expansion of a family which does not average to* 0 *is on average negative.*

If the Bias Conjecture holds, then when we estimate the rank of a family, there is always an extra term that slightly increases our upper bound for the average rank. This amount decreases as $\log R$ grows, and thus in the limit plays no role; however, it does lead to a small but noticeable contribution for small and modest sized conductors.

Another mystery is the distribution of zeroes on the critical strip. The average spacing at height t (i.e., imaginary part is t so points near $1 + it$) is about $1/\log(t)$. Thus, they are getting closer to each other, and one L-function gives us infinitely many zeros to study. Near the central point, however, we just have a few zeros. Since we can not do much with an individual elliptic curve, averaging over a family and the behavior near the central behavior, which is the n-level density, can be really helpful. If we want to deduce things about the zeros, we would want to calculate the 1-level density because ideally we would have 1 at the central point, and 0s everywhere else.

Definition 10 (1-Level Density)**.** *We assume that the Generalized Riemann Hypothesis holds for the L-functions $L(E, s)$ with zeros lying on the critical strip $1 + it$. Let us consider the family of all elliptic curves*

$$\mathcal{F} : y^2 = x^3 + ax + b,\ a \in [-N^2, N^2],\ b \in [-N^3, N^3], \tag{1.29}$$

and one-parameter families

$$\begin{aligned}\mathcal{F} : y^2 + a_1(t)xy + a_3(t)y &= x^3 + a_2(t)x^2 + a_4(t)x + a_6(t) \\ & \quad a_i(t) \in \mathbb{Z}[t],\ t \in [N, 2N], \end{aligned} \tag{1.30}$$

and two-parameter families

$$\begin{aligned}\mathcal{F} : y^2 + a_1(t,s)xy + a_3(t,s)y &= x^3 + a_2(t,s)x^2 + a_4(t,s)x + a_6(t,s) \\ & \quad a_i(t,s) \in \mathbb{Z}[t,s],\ t,s \in [N, 2N]. \end{aligned} \tag{1.31}$$

Let $f(x)$ be an even Schwartz function that is supported by the Fourier Transforms, γ_E the non-trivial zeros of the curve E, and N_E its conductor. We define the 1*-level density by*

$$D_{1,\mathcal{F}}(f) \ := \ \frac{1}{|\mathcal{F}|} \sum_{E \in \mathcal{F}} f_1\Big(\frac{\log N_E}{2\pi} \gamma_E^{(j_1)}\Big). \tag{1.32}$$

We use the Explicit Formula to convert the sum of our test function at scaled zeros in the definition of the one level density to a related sum over primes. For test functions ϕ suitably restricted (specifically, the support of their Fourier transform is small), we can evaluate the main term of the resulting prime sums and we can write these as integrals of our test function against fixed functions. Amazingly, similar results are seen when looking at energy levels of heavy nuclei, as well as in the distribution of eigenangles above 1 for the classical compact groups (Unitary, Symplectic, Orthogonal). This is one of many connections among number theory, physics and random matrix theory, and allows us to use the methods of one area to predict what the answer should be in another.

Using the Explicit Formula (1.5) to relate sums of a function ϕ against zeros of an L-function to sums of its Fourier Transform against primes, we evaluate not $\int f(x) W_{n,\mathcal{G}}(x) dx$ but $\int \widehat{f}(u) \widehat{W_{n,\mathcal{G}}}(u) du$. Denoting SO(even) (SO(odd)) by O^+ (O^-), the Fourier Transforms for the 1-level densities are

$$\begin{aligned}\widehat{W_{1,\mathrm{O}^+}}(u) &= \delta_0(u) + \frac{1}{2}\eta(u) \\ \widehat{W_{1,O}}(u) &= \delta_0(u) + \frac{1}{2} \\ \widehat{W_{1,\mathrm{O}^-}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) + 1 \\ \widehat{W_{1,Sp}}(u) &= \delta_0(u) - \frac{1}{2}\eta(u) \\ \widehat{W_{1,U}}(u) &= \delta_0(u), \end{aligned} \tag{1.33}$$

where $\eta(u)$ is 1, and 0 for $|u|$ less than 1, 1, and greater than 1, and δ_0 is the standard Dirac Delta functional. See [KS] and [Mi1].

1.3 The Bias Conjecture

Now we report on the results of our research. Much is known about the moments of the Fourier coefficients of elliptic curves. Work of Nagao, Rosen and Silverman shows that the first moment in families is related to the rank of the family over $\mathbb{Q}(T)$; specifically, a small negative bias results in rank; this was used by Arms, Lozano-Robledo and Miller [ALM] to construct one-parameter families of elliptic curves with moderate rank.

It is thus natural to ask if there is a bias in these sums in the second moments, and if so what are the consequences. One important one, due to Miller [Mi3], is that a negative bias here is related to some of the observed excess rank and repulsion of zeros of elliptic curve L-functions near the central point for finite conductors.

We start with a result from Michel on the main term of the second moments, and the size of the fluctuations, in one-parameter families.

Theorem 1.8. *For a one-parameter family $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$ with non-constant $j(T)$-invariant $j(T) = 1728\frac{4A(T)^3}{4A(T)^3+27B(T)^2}$, Michel has proven that in the second moment of the Fourier coefficients equals to*

$$pA_{2,\mathcal{E}}(p) \;=\; p^2 + O(p^{3/2}), \tag{1.34}$$

with the lower order terms of size $p^{3/2}, p, p^{1/2}$ and 1 having important cohomological interpretations.

Theorem 1.9 (Birch Theorem)**.** *For the family $\mathcal{E} : y^2 = x^3 + ax + b$ of all elliptic curves, the second moment of the Fourier coefficient equals to:*

$$pA_{2,\mathcal{F}}(p) \;=\; \sum_{a,b \bmod p} a_{\mathcal{F}_{a,b}}(p) = p^3 - p^2. \tag{1.35}$$

See [Bi, Mi1, Mi3, Mic].

Unfortunately it is very hard to compute in closed form of the Legendre sums arising from an ellitpic curve, though we will see later that we can compute linear and quadratic Legendre sums easily. Thus, in all our investigations below, we are forced to restrict our analysis to families where the resulting sums are tractable. There is therefore a danger that we are not looking at generic families.

Below is a summary of the new families we have successfully studied. In addition to several new one-parameter families, in this work two-parameter families are studied for the first time. For the two rank 2 one-parameter families we are unable to compute numerically, we demonstrate convincing results that for small primes the bias conjecture holds in them. We set $\delta_1(p)$ to be 1 if $p \equiv 1 \bmod 4$ and 0 otherwise, and $\delta_3(p)$ to be 1 if $p \equiv 3 \bmod 4$ and 0 otherwise:

One-Parameter Family	Rank	$pA_{1,\mathcal{F}(p)}$	$pA_{2,\mathcal{F}(p)}$
$y^2 = x^3 - x^2 - x + t$	0	0	$p^2 - 2p - \left(\frac{-3}{p}\right)p$
$y^2 = x^3 - tx^2 + (x-1)t^2$	0	0	$p^2 - 2p - [\sum_{x(p)} \left(\frac{x^3-x^2+x}{p}\right)]^2 - \left(\frac{-3}{p}\right)p$
$y^2 = x^3 + tx^2 + t^2$	1	-p	$p^2 - 2p - \left(\frac{-3}{p}\right)p - 1$
$y^2 = x^3 + tx^2 + x + 1$	1	-p	$p^2 - p - 1 + p\sum_{x(p)} \left(\frac{4x^3+x^2+2x+1}{p}\right)$
$y^2 = x^3 + tx^2 + tx + t^2$	1	-p	$p^2 - p - 1 - \delta_1(p)(2p)$
$y^2 = x^3 - x^2 + (x^2 - x)t + 1$	2	-2p	$p^2 - 1$ ("conjectured on average")
$y^2 = x^3 - x + t^4$	2("conjectured on average")	-2p ("conjectured on average")	$p^2 - p$ ("conjectured on average")

Table 1: The one-parameter families we proved theoretically all show that the largest lower order term that does not average to zero has a negative average. Unfortunately, we are not able to prove the second moment of $y^2 = x^3 - x^2 + (x^2 - x)t + 1$ as well as the first and second moment of $y^2 = x^3 - x + t^4$ theoretically. Due to the limited power of our computation software, we only generated data for the first 100 primes. Also, keep in mind that we did not observe the same form for every prime; we conjectured the average of its first or second moment. One family worth noting is $y^2 = x^3 - x^2 + (x^2 - x)t + 1$; it is a potential counterexample to a stronger form of Miller's Bias Conjecture based on the families studied to date, which is that in the second moment expansion the first term that does not average to zero is the p term and that has a negative average.

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	$p^3 - p^2 - \delta_3(p)(2p^2 - 2p)$
$y^2 = x^3 + ts^2x^2 + (t^3 - t^2)x$	$-p^2$	$p^3 - 3p^2 + 3p - 1 - \delta_3(p)(2p - 2)$
$y^2 = x^3 + t^2x^2 + (t^3 - t^2)sx$	$-p^2$	$p^3 - 3p^2 + 3p - \delta_3(p)(2p^2 - 4p)$
$y^2 = x^3 + t^2x^2 - (s^2 - s)t^2x$	$-2p^2$	$p^3 - 3p^2 + 2p + \delta_1(p)(p - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right))$
$y^2 = x^3 - t^2x + t^3s^2 + t^4$	$-2p^2$	$p^3 - 2p^2 + p - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right] p^2$

Table 2: The two-parameter families we proved theoretically all show a negative bias in the largest lower order term in the second-moment expansion.

In the next section we briefly review some standard tools and known results for computing sums of the Fourier coefficients in families. We then report on our new results in the next two sections, then end with some concluding remarks.

2 Tools for Calculating Biases

In this section, we explain why we can use rank as the first moment, and then introduce the linear and quadratic Legendre sums, the Jacobi symbol as well as the Gauss Sum Expansion, which can be used to compute biases in elliptic curves. See more details from [RoSi, BEW, BAU, Mi1].

Theorem 2.1 (Rosen-Silverman)**.** *For an elliptic surface(a one-parameter family), if Tate's conjecture holds, the first moment is related to the rank of the family over* $\mathbb{Q}(T)$*:*

$$\lim_{x\to\infty} \frac{1}{x} \sum_{p\le x} \frac{A_1, \mathcal{E}(p) \log p}{p} = rank\mathcal{E}(\mathbb{Q}(T)). \tag{2.1}$$

Conjecture 2.2 (Tate's Conjecture for Elliptic Surfaces[ST])**.** *Let $\mathcal{E}/\mathbb{Q}$ be an elliptic surface and $L_2(\mathcal{E}, s)$ be the L-series attached to ${H^2}_{et}(\mathcal{E}/\mathbb{Q}, \mathbb{Q}_l)$. Then $L_2(\mathcal{E}, s)$ has a meromorphic continuation to $\mathcal{C}$ and satisifies:*

$$-ord_{s=2} L_2(\mathcal{E}, s) = rankNS(\mathcal{E}/\mathbb{Q}), \tag{2.2}$$

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

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

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

Later in the paper, we find that most families are not in the Weierstrass form, or $y^2 = x^3 + A(T)x + B(T)$, so now we explain how to convert the families to Weierstrass Equations. We only need to do this to check to see if the one-parameter family is a rational surface, and hence the Rosen-Silverman theorem is applicable. For the computations it is often easier not to have them in Weierstrass form.

Theorem 2.3 (Convert to Weierstrass Equations)**.** *First, we transform $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ into*

$$E' : y^2 = x^3 + {a_2}'x^2 + {a_4}'x + {a_6}', \tag{2.3}$$

where the coefficients are given by

$${a_2}' = a_2 + \frac{1}{4}{a_1}^2,\ \ {a_4}' = a_4 + \frac{1}{2}a_1a_3 \text{ and } {a_6}' = a_6 + \frac{1}{4}{a_3}^2. \tag{2.4}$$

Then we transform E' into E'':

$$E'' : y^2 = x^3 + {a_4}''x + {a_6}'', \tag{2.5}$$

which

$${a_4}'' = {a_4}' - \frac{1}{3}{a_2'}^2 \text{ and } {a_6}'' = {a_6}' + \frac{2}{27}{a_2'}^3 - \frac{1}{3}{a_2}'{a_4}'. \tag{2.6}$$

All of the one-parameter families we compute are rational surfaces. See Appendix B for the complete proof. However, for two-parameter families, we cannot use the Rosen - Silverman theorem, and for us the ranks are conjectural. Checking their ranks is beyond the scope of this paper, but it can be done; see [WAZ] for more details. As our interest is in the biases of the second moments, we do not need to know these ranks for our purposes.

The key to our analysis in the families below are closed form expressions for linear and quadratic Legendre sums.

Lemma 2.4. *Let a, b, c be positive integers and $a \not\equiv 0 \bmod p$. Then*

$$\sum_{x \bmod p} \left(\frac{ax+b}{p}\right) = 0, \text{ if } p \nmid a, \tag{2.7}$$

and

$$\sum_{x \bmod p} \left(\frac{ax^2+bx+c}{p}\right) = \begin{cases} -\left(\frac{a}{p}\right), & \text{if } p \nmid b^2-4ac. \\ (p-1)\left(\frac{a}{p}\right), & \text{if } p \mid b^2-4ac. \end{cases} \tag{2.8}$$

See Appendix A for a complete proof.

By Dirichlet's theorem for primes in arithmetic progression, to first order as N tends to infinity there are the same number of primes congruent to 1 mod 4 as there are congruent to 3 mod 4. Thus, up to lower order terms tending to zero as N goes to infinity, the average behaves like:

Lemma 2.5 (Jacobi Symbol)**.**

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } n \equiv 1 \bmod 4. \\ -1, & \text{if } n \equiv 3 \bmod 4. \end{cases} \tag{2.9}$$

See [RoSi] for more details.

For some of our families, we need an alternative expansion for the Fourier coefficients:

Lemma 2.6 (Quadratic Formula mod p)**.** *For a quadratic $ax^2+bx+c \equiv 0$ mod p, $a \not\equiv 0$, there are two distinct roots if b^2-4ac equals to a non-zero square, one root if $b^2-4ac \equiv 0$, and zero root if b^2-4ac is not a square.*

See [Mi1] for more details.

Lemma 2.7 (Gauss Sum Expansion)**.** *We have the following expansion of $\left(\frac{x}{p}\right)$:*

$$\left(\frac{x}{p}\right) = G_p{}^{-1} \sum_{c=1}^{p} \left(\frac{c}{p}\right) \boldsymbol{e}\left(\frac{cx}{p}\right), \tag{2.10}$$

where $G_p = \sum_{a(p)} \left(\frac{a}{p}\right) \boldsymbol{e}\left(\frac{a}{p}\right)$, which equals to $\sqrt{p}$ for $p \equiv 1(4)$ and $i\sqrt{p}$ for $p \equiv 3(4)$. For the curve $y^2 = f_E(x)$, $a_E(p) = -\sum_{x(p)} \left(\frac{f_E(x)}{p}\right)$. We expand the x-sum by using Gauss sums, namely

$$a_E(p) = G_p{}^{-1} \sum_{x(p)} \sum_{c=1}^{p} \left(\frac{c}{p}\right) \boldsymbol{e}\left(\frac{cf_E(x)}{p}\right). \tag{2.11}$$

See [Mi1] for more details.

Sadly, there are no nice closed form expressions for cubic and higher sums, which is why elliptic curves are so hard to analyze as we need cubic sums for the coefficients. In this paper, we want to work with one- and two- parameter famillies that lead to linear or quadratic sums in the T- variable, or interchange the order of sums.

3 Biases in First and Second Moments in One-Parameter Families

We proved in Appendix B that every one-parameter family we computed are rational surfaces, so their first moment is equivalent to their rank.

3.1 Construction of Rank 0 Families

3.1.1 $y^2 = x^3 - x^2 - x + t$

Lemma 3.1. *The first moment of the one-parameter family $y^2 = x^3 - x^2 - x + t$ is 0. Since it is a rational surface, we can use the Rosen-Silverman theorem and the family's rank is 0.*

Proof. For $p > 3$,

$$\begin{aligned} -pA_{1,\mathcal{F}(p)} &= \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x^3 - x^2 - x + t}{p}\right) \\ &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{t + (x^3 - x^2 - x)}{p}\right) = 0. \end{aligned} \tag{3.1}$$

By the linear Legendre sum formula (Lemma 2.3), the t-sum is 0 if the equation is in the form of $at + b$. Therefore, $\sum_{t(p)}\sum_{x(p)}\left(\frac{x^3-x^2-x+t}{p}\right)$ equals to 0. □

Lemma 3.2. *The second moment of the one-parameter family $y^2 = x^3 - x^2 - x + t$ times p is $p^2 - 2p - \left(\frac{-3}{p}\right)p$, which supports our Bias Conjecture.*

Proof.

$$\begin{aligned} pA_{2,\mathcal{F}(p)} &= \sum_{t(p)} {a_t}^2(p) \\ &= \sum_{t(p)}\sum_{x,y(p)}\left(\frac{x^3 - x^2 - x + t}{p}\right)\left(\frac{y^3 - y^2 - y + t}{p}\right) \end{aligned} \tag{3.2}$$

Now, we compute the discriminant of the equation in t, denoted as δ, which we then evaluate the quadratic Legendre sums (Lemma 2.4) to compute the second moment:

$$\begin{aligned} a &= 1 \\ b &= (x^3 - x^2 - x) + (y^3 - y^2 - y) \\ c &= (x^3 - x^2 - x)(y^3 - y^2 - y) \\ \delta &= b^2 - 4ac = [(x^3 - x^2 - x) - (y^3 - y^2 - y)]^2. \end{aligned} \tag{3.3}$$

We see that $\delta(x, y)$ can be rewritten as

$$(x - y)(x^2 + xy - x + y^2 - y - 1). \tag{3.4}$$

We can see that $\delta(x, y) \equiv 0$ if $x = y$ and this happens p times. By the Quadratic Formula Mod p (Lemma 2.6), $\delta_2(x, y) = x^2 + xy - x + y^2 - y - 1 = y^2 + (x - 1)y + (x^2 - x - 1) \equiv 0$ when

$$y = \frac{-x + 1 \pm \sqrt{-3x^2 + 2x + 5}}{2}, \tag{3.5}$$

which reduces to find when $-3x^2 + 2x + 5$ is a square mod p. We get 2 distinct values of y if it is equivalent to a non-zero square, 1 value if it equals to 0, and no value if it does not equal to a square. When solving $\delta_2(x, y) \equiv 0 \mod p$, we need to make sure $y \notin (0)$. The number of solutions to $\delta_2(x, y) = x^2 + xy - x + y^2 - y - 1 \equiv 0(p)$ equals to:

$$\begin{aligned} \sum_{x=1}^{p-1} \left(1 + \left(\frac{-3x^2 + 2x + 5}{p}\right)\right) &= p - 1 + \sum_{x=1}^{p-1} \left(\frac{-3x^2 + 2x + 5}{p}\right) \\ &= p + \sum_{x(p)} \left(\frac{-3x^2 + 2x + 5}{p}\right). \end{aligned} \tag{3.6}$$

Then, we use Quadratic Formula Mod p (Lemma 2.6) again. The discriminant now equals to $4 - 4(-3)5 = 64$. For $p \geq 3$, p does not divide discriminant, so the sum is $p - \left(\frac{-3}{p}\right)$.

Then we check if there are any double-counting cases. If both factors are congruent to zero, we have $3x^2 - 2x - 1 \equiv 0$ when $x = 1, -3^{-1}$. Thus, the total number of pairs is

$$2p - 2 - \left(\frac{-3}{p}\right). \tag{3.7}$$

Therefore,

$$\begin{aligned} pA_{2,\mathcal{F}(p)} &= p\left[2p-2-\left(\frac{-3}{p}\right)\right]-p^2 \\ &= p^2-2p-\left(\frac{-3}{p}\right)p. \end{aligned} \tag{3.8}$$

□

3.1.2 $y^2 = x^3 - tx^2 + (x-1)t^2$

Lemma 3.3. *The first moment of the one-parameter family $y^2 = x^3 - tx^2 + (x-1)t^2$ is 0. Since it is a rational surface, we can use the Rosen-Silverman theorem and the family's rank is 0.*

Proof.

$$\begin{aligned} -pA_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} = \sum_{t(p)}\sum_{x(p)}\left(\frac{x^3-tx^2+(x-1)t^2}{p}\right) \\ &= \sum_{t(p)}\sum_{x(p)}\left(\frac{x^3-tx^2+xt^2-t^2}{p}\right) \\ &= \sum_{t=1}^{p-1}\sum_{x(p)}\left(\frac{t^3x^3-t^3x^2+t^3x-t^2}{p}\right) \\ &= \sum_{x(p)}\sum_{t=1}^{p-1}\left(\frac{t^2}{p}\right)\left(\frac{tx^3-tx^2+tx-1}{p}\right) \\ &= \sum_{x(p)}\sum_{t=0}^{p-1}\left(\frac{t(x^3-x^2+x)-1}{p}\right)-\sum_{x(p)}\left(\frac{-1}{p}\right) \\ &= \sum_{t(p)}\sum_{x=0}\left(\frac{-1}{p}\right)+\sum_{t(p)}\sum_{x(p);x\neq 0}\left(\frac{t(x^3-x^2+x)-1}{p}\right)-\sum_{x(p)}\left(\frac{-1}{p}\right) \\ &= -p+0+p \\ &= 0 \end{aligned} \tag{3.9}$$

□

Lemma 3.4. *The second moment of the one-parameter family $y^2 = x^3 - tx^2 + (x-1)t^2$ times p is $p^2 - 2p - \left(\frac{-3}{p}\right)p - 1$, which supports our Bias Conjecture.*

Proof.

$$\begin{aligned}
pA_{2,\mathcal{F}(p)} &= \sum_{t(p)} {a_t}^2(p) \\
&= \sum_{t(p)}\sum_{x(p)}\sum_{y(p)} \left(\frac{x^3-tx^2+xt^2-t^2}{p}\right)\left(\frac{y^3-ty^2+yt^2-t^2}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{x,y(p)} \left(\frac{t^3x^3-t^3x^2+t^3x-t^2}{p}\right)\left(\frac{t^3y^3-t^3y^2+t^3y-t^2}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{x,y(p)} \left(\frac{t^4}{p}\right)\left(\frac{t(x^3-x^2+x)-1}{p}\right)\left(\frac{t(y^3-y^2+y)-1}{p}\right) \\
&= \sum_{t=0}^{p-1}\sum_{x,y(p)} \left(\frac{t(x^3-x^2+x)-1}{p}\right)\left(\frac{t(y^3-y^2+y)-1}{p}\right) - \sum_{x,y(p)}\left(\frac{-1}{p}\right)\left(\frac{-1}{p}\right) \\
&= \sum_{t(p)}\sum_{x,y(p)} \left(\frac{t(x^3-x^2+x)-1}{p}\right)\left(\frac{t(y^3-y^2+y)-1}{p}\right) - p^2
\end{aligned} \tag{3.10}$$

We compute the discriminant of the equation in terms of t:

$$\begin{aligned}
a &= (x^3-x^2+x)(y^3-y^2+y) \\
b &= -[(x^3-x^2+x)+(y^3-y^2+y)] \\
c &= 1 \\
\delta &= b^2-4ac = [(x^3-x^2+x)-(y^3-y^2+y)]^2.
\end{aligned} \tag{3.11}$$

The only two ways that at least (x^3-x^2+x) or (y^3-y^2+y) vanishes are when $x=0$ and $y=0$. Hence, the total contribution is $2p$.

We can rewrite $\delta(x,y)$ as $(x-y)(x^2+xy-x+y^2-y+1)$. Like what we do for the previous several families, we see that $x=y\neq 0$ so the contribution from it is $p-1$.

Let $\delta_2(x,y)$ be $(x^2+xy-x+y^2-y+1)$. Using Lemma 2.6, we have:

$$\begin{aligned}
y &= \frac{-(x-1)\pm\sqrt{(x-1)^2-4(x^2-x+1)}}{2} \\
&= \frac{-(x-1)\pm\sqrt{-3x^2+2x-3}}{2}.
\end{aligned} \tag{3.12}$$

Hence, the number of solutions to $\delta_2(x,y)\equiv 0$ is:

$$\sum_{x=1}^{p-2}\left[1+\left(\frac{-3x^2+2x-3}{p}\right)\right] \quad = \quad p-2+\left(\frac{-3x^2+2x-3}{p}\right). \tag{3.13}$$

We use Lemma 2.6 again. The discriminant now is $2^2 - 4(-3)(-3)$. Hence, for $p > 5$, p does not divide the discriminant, and the sum is $-\left(\frac{-3}{p}\right)$.

Since we don't have double-counted solutions, the total number of pairs is

$$2p - 4 - \left(\frac{-3}{p}\right). \tag{3.14}$$

When $x = y \neq 0$, clearly $\left(\frac{(x^3-x^2+x)(y^3-y^2+y)}{p}\right) = 1$ and these terms each contribute 1.

Consider $x \neq y \neq 0$ and $x^2 + xy - x + y^2 - y + 1 \equiv 0$. Then $x^2 - x + 1 \equiv y(-y + 1 - x)$ and $y^2 - y + 1 \equiv x(-x + 1 - y)$ and

$$\left(\frac{(x^3 - x^2 + x)(y^3 - y^2 + y)}{p}\right) = \left(\frac{xy(-x + 1 - y)^2}{p}\right). \tag{3.15}$$

We can see that $x \neq y$, so all pairs have their Legendre factor $+1$. Therefore,

$$\begin{aligned} pA_{2,\mathcal{F}(p)} &= p\left(2p - 4 - \left(\frac{-3}{p}\right)\right) - \sum_{x,y(p)} \left(\frac{(x^3 - x^2 + x)(y^3 - y^2 + y)}{p}\right) + 2p - p^2 \\ &= p^2 - 2p - \left[\sum_{x(p)} \left(\frac{x^3 - x^2 + x}{p}\right)\right]^2 - \left(\frac{-3}{p}\right)p. \end{aligned} \tag{3.16}$$

□

Now we move on to construct some rank 1 families.

3.2 Construction of Rank 1 Families

3.2.1 $y^2 = x^3 + tx^2 + t^2$

Lemma 3.5. *The first moment of the one-parameter family $y^2 = x^3 + tx^2 + t^2$ is -1, and the family's rank is 1.*

Proof.

$$
\begin{aligned}
-pA_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} = \sum_{t(p)} \sum_{x(p)} \left(\frac{x^3+tx^2+t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x(p)} \left(\frac{t^3x^3+t^3x^2+t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x(p)} \left(\frac{t^2}{p}\right)\left(\frac{t(x^2+x^3)+1}{p}\right) \\
&= \sum_{t(p)} \sum_{x(p)} \left(\frac{t(x^2+x^3)+1}{p}\right) - \sum_{x(p)} \left(\frac{1}{p}\right) \\
&= \sum_{t(p)} \sum_{x(p)} \left(\frac{tx^3+tx^2+1}{p}\right) - \sum_{x(p)} \left(\frac{1}{p}\right) \\
&= \sum_{t(p)} \sum_{x=0,-1} \left(\frac{1}{p}\right) + \sum_{x\neq 0,-1} \sum_{t(p)} \left(\frac{t+1}{p}\right) - p \\
&= 2p + 0 - p \\
&= p
\end{aligned}
\tag{3.17}
$$

We apply the linear Legendre sums. Since $\left(\frac{t^2}{p}\right)$ yields 1, we can ignore it and separate $\left(\frac{t(x^3+x^2)+1}{p}\right)$ into two cases: when $t = 0$ and when $t \neq 0$. When $t = 0$, the sum is $\sum_{x(p)} \left(\frac{1}{p}\right) = p$ and we subtract it from the total sum. When $t \neq 0$, we have $2p$ when $x = 0, -1$ so that $x^3 + x^2 \equiv 0 \mod p$. Hence, the total contribution is $2p - p = p$. ∎

Lemma 3.6. *The second moment of the one-parameter family $y^2 = x^3+tx^2+t^2$ times p is $p^2 - 2p - \left(\frac{-3}{p}\right)p - 1$, which supports our Bias Conjecture.*

Proof.

$$\begin{aligned}
pA_{2,\mathcal{F}(p)} &= \sum_{t(p)} {a_t}^2(p) \\
&= \sum_{t(p)} \sum_{x,y(p)} \left(\frac{x^3+tx^2+t^2}{p}\right)\left(\frac{y^3+ty^2+t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x,y(p)} \left(\frac{x^3+tx^2+t^2}{p}\right)\left(\frac{y^3+ty^2+t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x,y(p)} \left(\frac{t^3x^3+t^3x^2+t^2}{p}\right)\left(\frac{t^3y^3+t^3y^2+t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x,y(p)} \left(\frac{t^4}{p}\right)\left(\frac{t(x^3+x^2)+1}{p}\right)\left(\frac{t(y^3+y^2)+1}{p}\right) \\
&= \sum_{t=0}^{p-1} \sum_{x,y(p)} \left(\frac{t^4}{p}\right)\left(\frac{t(x^3+x^2)+1}{p}\right)\left(\frac{t(y^3+y^2)+1}{p}\right) - \sum_{x,y(p)} \left(\frac{1}{p}\right) \\
&= \sum_{x,y(p)} \sum_{t=0}^{p-1} \left(\frac{t(x^3+x^2)+1}{p}\right)\left(\frac{t(y^3+y^2)+1}{p}\right) - p^2
\end{aligned} \tag{3.18}$$

Its discriminant is:

$$\begin{aligned}
a &= (x^3+x^2)(y^3+y^2) \\
b &= x^3+x^2+y^3+y^2 \\
c &= 1 \\
\delta &= b^2-4ac = ((x^3+x^2)-(y^3+y^2))^2.
\end{aligned} \tag{3.19}$$

First, we calculate the cases when at least (x^3+x^2) or (y^3+y^2) vanishes. When $x = 0, -1$, (x^3+x^2) equals to zero. Then, we have $\sum_t \left(\frac{t(y^3+y^2)+1}{p}\right)$, which is $2p$ from our $A_{1,\mathcal{F}(p)}$. Similarly, we have $2p$ for $\sum_t \left(\frac{t(x^3+x^2)+1}{p}\right)$. We overcount by $4p$ when both x^3+x^2 and y^3+y^2 are equivalent to 0. Therefore, the total sum of that at least (x^3+x^2) or (y^3+y^2) vanishes equals to $2p+2p-4p = 0$.

Then, assume $x, y \notin \{0, -1\}$. When $\delta(x,y) \equiv 0 \mod p$, we have

$$\delta(x,y) \quad = \quad (x-y)(x^2+xy+x+y^2+y). \tag{3.20}$$

Therefore,

$$pA_{2,\mathcal{F}(p)} = \sum_{x,y\neq 0,-1;\delta(x,y)\equiv 0} p\left(\frac{(x^3+x^2)(y^3+y^2)}{p}\right) - \sum_{x,y\neq 0,-1}\left(\frac{(x^3+x^2)(y^3+y^2)}{p}\right) - p^2. \quad (3.21)$$

We can see that $\delta(x,y)\equiv 0$ if $x=y$ and this happens p times. If $x=y$, then the second factor equals to $3x^2+2x$, which is congruent to zero at most twice.

By Lemma 2.6, $\delta_2(x,y) = x^2+xy+x+y^2+y\equiv 0$ when

$$y = \frac{-x-1\pm\sqrt{-3x^2-2x+1}}{2}, \quad (3.22)$$

which reduces to find when $-3x^2-2x+1$ is a square mod p. We get 2 distinct values of y if it is equivalent to a non-zero square, 1 value if it equals to 0, and no value if it does not equal to a square. When we solve $\delta_2(x,y)\equiv 0 \mod p$, we need to make sure $y\notin(0,-1)$. If $y=0$, then $x=-1$; if $y=-1$, then $x=0$. Therefore, we don't get an excluded y. Thus, the number of solutions to $\delta_2(x,y) = x^2+xy+x+y^2+y\equiv 0$ equals to:

$$\sum_{x=1}^{p-2}\left[1+\left(\frac{-3x^2-2x+1}{p}\right)\right] = p-2\left(\frac{-3x^2-2x+1}{p}\right). \quad (3.23)$$

Then, we use Lemma 2.6 again. The discriminant now equals to $4-4(-3)1=16$. For $p\geq 5$, p does not divide discriminant, so the sum is $-\left(\frac{-3}{p}\right)$.

For $x\neq 0,-1$, the number of solutions to $x^2+xy+x+y^2+y\equiv 0$ is $p-2-\left(\frac{-3}{p}\right)$; the number of solutions to $x-y\equiv 0$ is at most $p-2$. At most two pairs of (x,y) satisfy both $x^2+xy+x+y^2+y\equiv 0$ and $x=y$. There are no pairs that satisfy $3x^2\equiv -2x$, so we do not have over-counting. Thus, the total number of pairs is

$$2p-2-\left(\frac{-3}{p}\right). \quad (3.24)$$

When $\delta(x,y)\not\equiv 0$ and $x=y\neq 0,-1$, clearly $\left(\frac{(x^3+x^2)(y^3+y^2)}{p}\right)$ contributes 1.

Consider $x\neq y$ and $x^2+xy+x+y^2+y\equiv 0$ and $x,y\neq 0,-1$. Then, $y^2+y\equiv -x(x+y+1)$ and $x^2+x\equiv -y(y+x+1)$ and

$$\left(\frac{(x^3+x^2)(y^3+y^2)}{p}\right) = \left(\frac{x(x^2+x)y(y^2+y)}{p}\right) = \left(\frac{x^2y^2(x+y+1)}{p}\right). \quad (3.25)$$

As long as $x \neq -y-1$, the contribution is 1. If $x = -y-1$, then we will have $x^2 + x \equiv 0$. This implies $x = 0, -1$, which can not happen since $x, y \neq 0, -1$. Therefore, all pairs have their Legendre factor $+1$, and we need only count how many such pairs are there:

$$\begin{aligned} pA_{2,\mathcal{F}(p)} &= p\left[2p - 2 - \left(\frac{-3}{p}\right)\right] - \sum_{x,y\neq 0,-1}\left(\frac{(x^3+x^2)(y^3+y^2)}{p}\right) - p^2 \\ &= p^2 - 2p - \left(\frac{-3}{p}\right)p - 1. \end{aligned} \tag{3.26}$$

□

3.2.2 $y^2 = x^3 + tx^2 + x + 1$

Lemma 3.7. *The first moment of the one-parameter family $y^2 = x^3+tx^2+x+1$ is -1, and the family's rank is 1.*

Proof.

$$\begin{aligned} -pA_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} = \sum_{t(p)}\sum_{x(p)}\left(\frac{x^3+x^2(t+1)+x+1}{p}\right) \\ &= \sum_{x=1}^{p-1}\sum_{t(p)}\left(\frac{x^3+tx^2+x+1}{p}\right) + \sum_{t(p)}\left(\frac{1}{p}\right) \\ &= 0 + p \\ &= p \end{aligned} \tag{3.27}$$

□

Lemma 3.8. *The second moment of the one-parameter family $y^2 = x^3 + tx^2 + x + 1$ times p is $p^2 - p - 1 + p\sum_{x(p)}\left(\frac{4x^3+x^2+2x+1}{p}\right)$, which supports our Bias Conjecture.*

Proof. We compute the second moment using Gauss Sum Expansion (Lemma 2.7):

$$\begin{aligned} pA_{2,\mathcal{F}(p)} &= \sum_{t(p)} {a_t}^2(p) \\ &= \sum_{t(p)}\sum_{x(p)}\sum_{y(p)}\left(\frac{x^3+x+1+x^2t}{p}\right)\left(\frac{y^3+y+1+y^2t}{p}\right) \\ &= \sum_{x,y(p)}\sum_{c,d=1}^{p-1}\frac{1}{p}\left(\frac{cd}{p}\right)\mathbf{e}\left(\frac{c(x^3+x+1)-d(y^3+y+1)}{p}\right)\sum_{t(p)}\mathbf{e}\left(\frac{(cx^2-dy^2)t}{p}\right). \end{aligned} \tag{3.28}$$

Note that c and d are invertible mod p. If the numerator in the t-exponential is non-zero, the t-sum vanishes. If exactly one of x and y vanishes, the numerator is not congruent to zero mod p. Hence, either or neither are zero. If both are zero, the t-sum gives p, the c-sum gives G_p, the d-sum gives $(G_p)^{-1}$, for a total contribution of p.

Assume x and y are non-zero. Then $d = cx^2y^{-2}$ (otherwise the t-sum is zero). The t-sum yields p, and we have:

$$\begin{aligned}
pA_{2,\mathcal{F}(p)} &= \sum_{x,y=1}^{p-1}\sum_{c=1}^{p-1}\frac{1}{p}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x^3y^2+xy^2+y^2-x^2y^3-x^2y-x^2)}{p}\right)p+p \\
&= \sum_{x,y=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-xy-x-y)}{p}\right)+p \\
&= \sum_{x,y=1}^{p-1}\sum_{c=0}^{p-1}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-xy-x-y)}{p}\right)+p-\sum_{x,y=1}^{p-1}\left(\frac{x^2y^2}{p}\right) \\
&= \sum_{x,y=1}^{p-1}\sum_{c=0}^{p-1}\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-xy-x-y)}{p}\right)+p-(p-1)^2.
\end{aligned} \tag{3.29}$$

If $g(x,y) = (x-y)(x^2y^2-xy-x-y \equiv 0(p)$, then the c-sum is p, otherwise it is 0. We are left with counting how often $g(x,y) \equiv 0$ for x, y non-zero.

Clearly, whenever $x = y$, $g(x,y) \equiv 0(p)$. There are $p-1$ solutions for each non-zero x, so the total contribution is $p(p-1)$.

Consider $x^2y^2 - xy - x - y \equiv 0$ now. By the Quadratic Formula mod p,

$$\begin{aligned}
y &= \frac{(x+1)\pm\sqrt{(x+1)^2+4x^3}}{2x^2} \\
&= \frac{(x+1)\pm\sqrt{4x^3+x^2+2x+1}}{2x^2}.
\end{aligned} \tag{3.30}$$

If $4x^3+x^2+2x+1$ is a non-zero square, y has two distinct values. If it equals to 0, y has one value, and if it does not equal to a square, y does not have a value.

For a given non-zero x, the number of non-zero y for $4x^3+x^2+2x+1$ is $1+\left(\frac{4x^3+x^2+2x+1}{p}\right)$. Hence the number of non-zero pairs with $4x^3+x^2+2x+1$ is

$$\sum_{x\neq 0}\left(1+\left(\frac{4x^3+x^2+2x+1}{p}\right)\right) = p-1+\sum_{x=0}^{p}\left(\frac{4x^3+x^2+2x+1}{p}\right)-1. \tag{3.31}$$

Each of these pairs contributes p, so the total contribution is

$$p^2 + p \sum_x \left(\frac{4x^3 + x^2 + 2x + 1}{p} \right) - 2p. \tag{3.32}$$

We must be careful about double counting. If both $x - y \equiv 0$ and $x^2y^2 - xy - x - y \equiv 0$, then we find $x^3 \equiv x + 2$ $(x \neq 0)$, and we have one double-counted solution.

Therefore, the second moment times p equals to:

$$\begin{aligned} pA_{2,\mathcal{F}(p)} &= p^2 + p \left(\sum_{x(p)} \left(\frac{4x^3 + x^2 + 2x + 1}{p} \right) \right) - 2p - p + p(p-1) + p - (p-1)^2 \\ &= p^2 - p - 1 + p \sum_{x(p)} \left(\frac{4x^3 + x^2 + 2x + 1}{p} \right). \end{aligned} \tag{3.33}$$

Although we have a $p^{3/2}$ term in the second moment, by the Sato-Tate conjecture (which has been proven by Taylor, jointly with Clozel, Harris and Shepherd Barron, see [Clo]) this will have a mean of zero because it is p times the coefficients of an elliptic curve $\mathcal{E} : y^2 = 4x^3 + x^2 + 2x + 1$. Hence, the Bias Conjecture still holds. □

3.2.3 $y^2 = x^3 + tx^2 + tx + t^2$

Lemma 3.9. *The first moment of the one-parameter family $y^2 = x^3 + tx^2 + tx + t^2$ is -1, and the family's rank is 1.*

Proof.

$$
\begin{aligned}
-pA_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} = \sum_{t(p)} \sum_{x(p)} \left(\frac{x^3+tx^2+tx+t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x(p)} \left(\frac{x^3+tx^2+tx+t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x(p)} \left(\frac{t^3x^3+t^3x^2+t^2x+t^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x(p)} \left(\frac{t^2}{p}\right)\left(\frac{tx^3+tx^2+x+1}{p}\right) \\
&= \sum_{t=0}^{p-1} \sum_{x(p)} \left(\frac{t(x^3+x^2)+x+1}{p}\right) - \sum_{x(p)} \left(\frac{x+1}{p}\right) \\
&= \sum_{t(p)} \sum_{x=0,-1} \left(\frac{t(x^3+x^2)+x+1}{p}\right) + \sum_{t(p)} \sum_{x(p) x\neq 0,-1} \left(\frac{t(x^3+x^2)+x+1}{p}\right) - 0 \\
&= \sum_{t(p)} \sum_{x=-1} \left(\frac{0}{p}\right) + \sum_{t(p)} \sum_{x=0} \left(\frac{1}{p}\right) + \sum_{x(p) x\neq 0,-1} \sum_{t(p)} \left(\frac{t+x+1}{p}\right) \\
&= 0+p+0 = p
\end{aligned}
\tag{3.34}
$$

□

Lemma 3.10. *The second moment of the one-parameter family* $y^2 = x^3+tx^2+tx+t^2$ *times* p *is* p^2-3p-1 *if* p *is* 1 *mod* 4 *and* p^2-p-1 *if* p *is* 3 *mod* 4 *which supports our Bias Conjecture.*

Proof.

$$\begin{aligned}
pA_{2,\mathcal{F}(p)} &= \sum_{t(p)} {a_t}^2(p) \\
&= \sum_{t(p)} \sum_{x(p)} \sum_{y(p)} \left(\frac{tx^2+tx+t^2+x^3}{p}\right)\left(\frac{ty^2+ty+t^2+y^3}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x,y(p)} \left(\frac{t^3x^2+t^2x+t^2+t^3x^3}{p}\right)\left(\frac{t^3y^2+t^2y+t^2+t^3y^3}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{x,y(p)} \left(\frac{t^4}{p}\right)\left(\frac{t(x^3+x^2)+x+1}{p}\right)\left(\frac{t(y^3+y^2)+y+1}{p}\right) \\
&= \sum_{t=0}^{p-1} \sum_{x,y(p)} \left(\frac{t(x^3+x^2)+x+1}{p}\right)\left(\frac{t(y^3+y^2)+y+1}{p}\right) - \sum_{x,y(p)} \left(\frac{x+1}{p}\right)\left(\frac{y+1}{p}\right) \\
&= \sum_{t(p)} \sum_{x,y(p)} \left(\frac{t(x^3+x^2)+x+1}{p}\right)\left(\frac{t(y^3+y^2)+y+1}{p}\right) - 0 \\
&= \sum_{t(p)} \sum_{x,y(p)} \left(\frac{t(x^3+x^2)+x+1}{p}\right)\left(\frac{t(y^3+y^2)+y+1}{p}\right)
\end{aligned} \tag{3.35}$$

We have

$$\begin{aligned}
a &= (x^3+x^2)(y^3+y^2) \\
b &= (x^3+x^2)(y+1)+(y^3+y^2)(x+1) \\
c &= (x+1)(y+1) \\
\delta &= b^2-4ac = [(x^3+x^2)(y+1)-(y^3+y^2)(x+1)]^2.
\end{aligned} \tag{3.36}$$

The discriminant $\delta(x,y)$ can be rewritten as

$$\delta(x,y) \quad = \quad (x-y)(x+y)(x+1)(y+1). \tag{3.37}$$

The only way that makes $(x^3+x^2)(y+1)$ or $(y^3+y^2)(x+1)$ vanish is when x and y both equal to -1. Therefore,

$$\begin{aligned}
pA_{2,\mathcal{F}(p)} = &\sum_{x,y\neq 0,-1;\delta(x,y)\equiv 0} p\left(\frac{(x^3+x^2)(y+1)-(y^3+y^2)(x+1)}{p}\right) \\
&- \sum_{x,y\neq 0,-1} \left(\frac{(x^3+x^2)(y+1)-(y^3+y^2)(x+1)}{p}\right) - 1.
\end{aligned} \tag{3.38}$$

We can see that $\delta(x,y) \equiv 0$ if $x = y$ and this happens $p-2$ times. If $x = y$ then the second factor equals to $2x^3 + 3x^2 + 2x$, which is congruent to zero at most three times.

By the Quadratic Formula mod p (Lemma 2.6), $\delta_2(x,y) = x^2y + x^2 + xy^2 + 2xy + x + y^2 + y \equiv 0(p)$ when

$$\begin{aligned} y &= \frac{-(x^2+2x+1) \pm \sqrt{x^4 - 2x + 1}}{2(x+1)} \\ &= \frac{-(x^2+2x+1) \pm \sqrt{(x+1)^2(x-1)^2}}{2(x+1)}, \end{aligned} \tag{3.39}$$

which reduces to find when $(x+1)^2(x-1)^2$ is a square mod p. We get 2 distinct values of y if it is equivalent to a non-zero square, 1 value if it equals to 0, and no value if it does not equal to a square. We can see that $x^4 - 2x + 1$ is always a square unless $x = 1$ and $x = -1$. Since we already state that x can not equal to -1, so we only need to deal with $x = 1$. Thus, the number of solutions $\delta_2 \equiv 0(p)$ is $(p-2)$, and the total contribution is $p(p-2)$.

Therefore, on average p times the second moment equals to

$$\begin{aligned} pA_{2,\mathcal{F}(p)} &= p(p-2) - \sum_{x,y \neq 0,-1} \left(\frac{(x^3+x^2)(y+1) - (y^3+y^2)(x+1)}{p} \right) - 1 \\ &= p^2 - 2p - 1. \end{aligned} \tag{3.40}$$

Keep in mind that we have three kinds of primes: when $p = 2$ (this case is trivial in the computations we have in this paper), when $p \equiv 1 \bmod 4$ and when $p \equiv 3 \bmod 4$. When $x = y$ and $x = -y$, can both help the discriminant to vanish. If $x = y \neq 0$, then $\left(\frac{x}{p}\right)\left(\frac{y}{p}\right) = \left(\frac{x^2}{p}\right)$ and every prime always contributes p; if $p \equiv 1 \bmod 4$ and $x = -y \neq 0$, by the Jacobi Symbol (Lemma 2.5) $\left(\frac{x}{p}\right)\left(\frac{-y}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x^2}{p}\right) = \left(\frac{x^2}{p}\right)$ also contributes p. If $p \equiv 1 \bmod 4$ and $x = -y$, by the Jacobi Symbol there should be an extra contribution of p. However, since we already count the contribution from $x = -y$, we need to subtract p from the average second moment:

$$\begin{aligned} pA_{2,\mathcal{F}(p)} &= p^2 - 2p - 1 - p \\ &= p^2 - 3p - 1. \end{aligned} \tag{3.41}$$

If $p \equiv 3 \bmod 4$ and $x = -y$, by the Jacobi Symbol (Lemma 2.5) there should be an extra contribution of $-p$. However, since we already count the contribution from $x = -y$, we need to subtract $-p$ from the average second moment:

$$\begin{aligned} pA_{2,\mathcal{F}(p)} &= p^2 - 2p - 1 - (-p) \\ &= p^2 - p - 1. \end{aligned} \tag{3.42}$$

□

Now we move on to construct some rank 2 families.

3.3 Construction of Rank 2 Families

3.3.1 $y^2 = x^3 - x^2 + (x^2 - x)t + 1$

Lemma 3.11. *The first moment of the one-parameter family $y^2 = x^3 - x^2 + (x^2 - x)t + 1$ is -2, and the family's rank is 2.*

Proof.

$$\begin{aligned} -pA_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} = \sum_{t(p)}\sum_{x(p)} \left(\frac{x^3 - x^2 + (x^2 - x)t + 1}{p}\right) \\ &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1} \left(\frac{(x^2 - x)t + (x^3 - x^2 + 1)}{p}\right) \\ &= \sum_{x \neq 0,1}\sum_{t=0}^{p-1} \left(\frac{t + (x^3 - x^2 + 1)}{p}\right) + \sum_{t=0}^{p-1}\left[\left(\frac{1}{p}\right) + \left(\frac{1}{p}\right)\right] \\ &= 0 + 2p \\ &= 2p \end{aligned} \tag{3.43}$$

We apply linear Legendre sums to $\sum_{t=0}^{p-1}\left(\frac{(x^2-x)t+(x^3-x^2+1)}{p}\right)$. If $x = 0, 1$, we have two $\sum_{t(p)}\left(\frac{1}{p}\right)$, so the rank equals to 2. □

Conjecture 3.12. *We conjecture that the second moment of the one-parameter family $y^2 = x^3 - x^2 + (x^2 - x)t + 1$ times p is $p^2 - 1$ on average, which supports our Bias Conjecture.*

We are not able to prove the second moment of this family theoretically, so we observe numerically and generate the second moment form for the first 100 primes:

We can see that for the first 100 primes, every form has $p^2 - c_1 p - 1$ (see Appendix C.1 for the complete data table). The second moment c_1 is always less than $2\sqrt{p}$ in absolute value. This is important because otherwise, the count is not for an elliptic curve. What's more, c_1 seems to be even numbers and grow, but the sum of c_1s seems to average to zero. We conjecture that the form

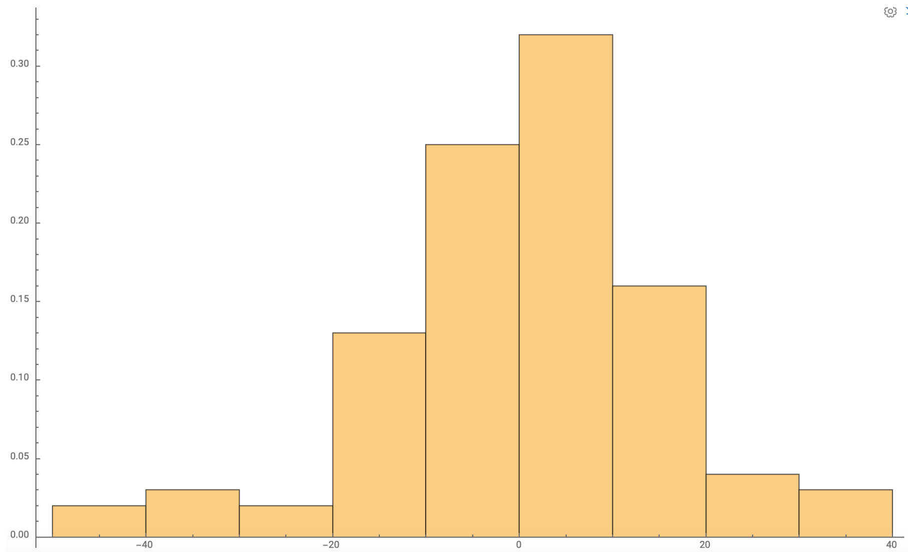


Figure 4: The distribution of the largest lower order term in the second moment expansion of $y^2 = x^3 - x^2 + (x^2 - x)t + 1$ for the first 100 primes.

of this one-parameter family is $p^2 - 1$ on average, but there might be terms of 1, $p^{1/2}$, p, or $p^{3/2}$. This family is a potential counterexample to a stronger form of Miller's Conjecture based on the families studied to date, which is that the first term that does not average to zero is the p term and that has a negative average.

3.3.2 $y^2 = x^3 - x + t^4$

Conjecture 3.13. *We conjecture that the first moment of the one-parameter family* $y^2 = x^3 - x + t^4$ *is* -2 *on average, and the family's rank is* 2 *on average.*

We are not able to prove the first moment of this family theoretically, so we observe numerically and generate the first moment form for the first 100 primes:

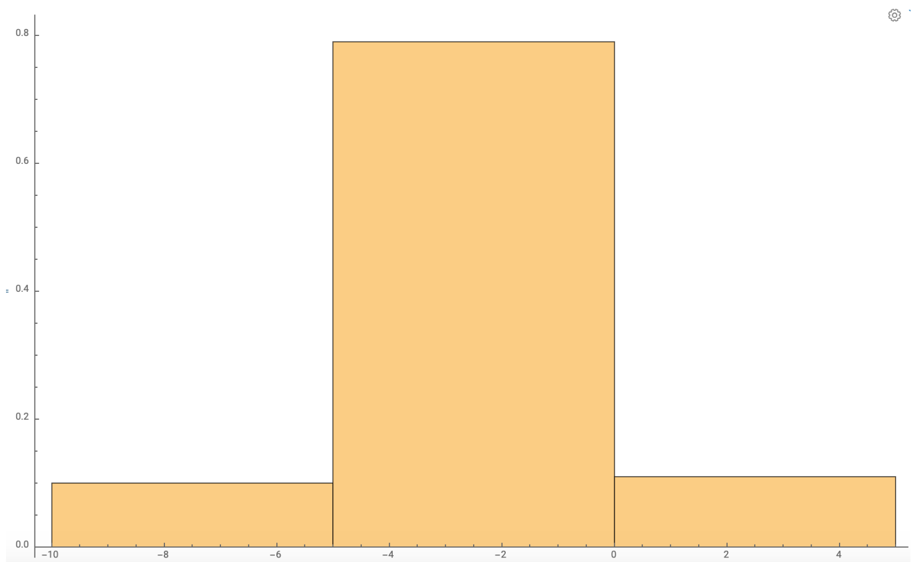


Figure 5: The distribution of the first moment of $y^2 = x^3 - x + t^4$ for the first 100 primes.

We can see that -2 appears frequently, but there are some 2 and -6 (see Appendix C.2 for the complete data table). We conjecture that the first moment is -2 on average and the rank of this family is 2 on average.

Conjecture 3.14. *We conjecture that the second moment of the one-parameter family $y^2 = x^3 - x + t^4$ times p is $p^2 - p$ on average, which supports our Bias Conjecture.*

We are not able to prove the second moment of this family theoretically, so we observe numerically and generate the second moment form for the first 100 primes:

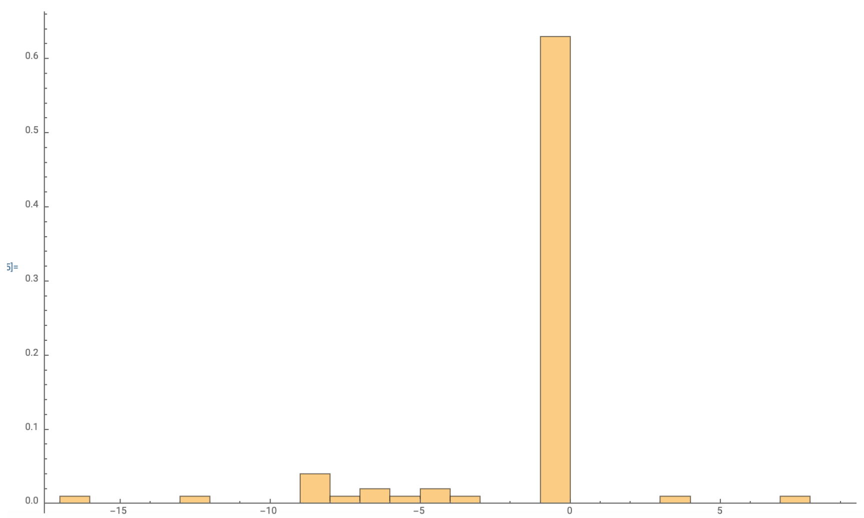


Figure 6: The distribution of the largest lower order term in the second moment expansion of $y^2 = x^3 - x + t^4$ for the first 100 primes.

We can see that for the first 100 primes, $p^2 - p$ appears most of the times (see Appendix C.3). We observe that primes that are 5 mod 8 do not have a constant term. Primes that are 3 mod 4 always have the form of $p^2 - p$ (although some 1 mod 4 primes have it too). However, we are not able to compute the exact second form times p. We conjecture the form times p to be $p^2 - p$ on average, but there might be terms of 1, $p^{1/2}$, p or $p^{3/2}$.

Now we turn to see if the Bias Conjecture holds in some two-parameter families.

4 Biases in First and Second Moments in Two-Parameter Families

In this section, we are going to compute the biases in first and second moments in two-parameter families. Keep in mind that for two-parameter families, Rosen - Silverman does not hold in them so the ranks are conjectural. Checking their ranks is beyond the scope of this paper. See [WAZ] for more details.

4.1 Construction of Rank 0 Families

4.1.1 $y^2 = x^3 + tx + sx^2$

Lemma 4.1. *The first moment of the two-parameter family $y^2 = x^3 + tx + sx^2$ is 0.*

Proof.

$$
\begin{aligned}
-p^2 A_{1,\mathcal{F}(p)} =& -\sum_{t(p)}\sum_{s(p)} a_{t,s}(p) = \sum_{t(p)}\sum_{x(p)}\sum_{s(p)} \left(\frac{x^3+tx+sx^2}{p}\right) \\
=& \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{s(p)} \left(\frac{t^3x^3+t^2x+st^2x^2}{p}\right) \\
=& \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{s(p)} \left(\frac{t^2}{p}\right)\left(\frac{tx^3+x+sx^2}{p}\right) \\
=& \sum_{t(p)}\sum_{x(p)}\sum_{s(p)} \left(\frac{tx^3+x+sx^2}{p}\right) - \sum_{x(p)}\sum_{s(p)} \left(\frac{x+sx^2}{p}\right) \\
=& \sum_{x(p)}\sum_{s(p)}\sum_{t(p)} \left(\frac{tx^3+sx^2+x}{p}\right) - 0 \\
=& \sum_{x(p)}\sum_{s(p)}\sum_{t=0} \left(\frac{sx^2+x}{p}\right) + \sum_{x(p)}\sum_{s(p)}\sum_{t(p);t\neq 0} \left(\frac{tx^3+x+sx^2}{p}\right) \\
&+ \sum_{x(p)}\sum_{t(p)}\sum_{s=0} \left(\frac{tx^3+x}{p}\right) + \sum_{x(p)}\sum_{t(p)}\sum_{s(p);s\neq 0} \left(\frac{tx^3+x+sx^2}{p}\right) - 0 \\
=& 0+0+0+0-0 \\
=& 0
\end{aligned}
\tag{4.1}
$$

□

Lemma 4.2. *The second moment of the two-parameter family $y^2 = x^3+tx+sx^2$ times p^2 is $p^3 - 2p^2 + p$, which supports our Bias Conjecture.*

Proof.

$$\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} a_{t,s}{}^2(p) \\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3+tx+sx^2}{p}\right)\left(\frac{y^3+ty+sy^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3+tx+sx^2}{p}\right)\left(\frac{y^3+ty+sy^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{t^3x^3+t^2x+st^2x^2}{p}\right)\left(\frac{t^3y^3+t^2y+st^2y^2}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{t^4}{p}\right)\left(\frac{tx^3+x+sx^2}{p}\right)\left(\frac{ty^3+y+sy^2}{p}\right) \\
&= \sum_{t=0}^{p-1} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{tx^3+x+sx^2}{p}\right)\left(\frac{ty^3+y+sy^2}{p}\right) - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x+sx^2}{p}\right)\left(\frac{y+sy^2}{p}\right) \\
&= \sum_{x,y(p)} \sum_{s(p)} \sum_{t(p)} \left(\frac{tx^3+x+sx^2}{p}\right)\left(\frac{ty^3+y+sy^2}{p}\right) - (p-1)
\end{aligned} \tag{4.2}$$

We compute the discriminant of the equation in terms of t and s:

$$\begin{aligned}
a &= x^3y^3 \\
b &= x^3(y+sy^2) + y^3(x+sx^2) \\
c &= (y+sy^2)(x+sx^2) \\
\delta &= b^2 - 4ac = [(x^3(y+sy^2) - y^3(x+sx^2)]^2 \\
&= [xy(x-y)(sxy+x+y)]^2.
\end{aligned} \tag{4.3}$$

We need to count the number of times x, y and s vanish. Let us consider $xy(x-y)$ first. When $x=0$, y can be any number except 0 because we have $x=y=0$ later when $x-y \equiv 0(p)$. We can also see that s vanishes, so the contribution from $x=0$ is $p-1$. Similarly, when $y=0$, its contribution is $p-1$. When $x=y\neq 0$, $x-y\equiv 0(p)$ and s does not vanish. We have a special case when $x=y=0$ and its contribution is 1. The total contribution from $x-y\equiv 0(p)$ is $p(p-1)+1$.

Then, we consider $sxy+x+y$. When $s\equiv 0(p)$, we are left with $x+y$. The contribution from $x+y\equiv 0(p)$ is $(p-1)^2$. When $s \not\equiv 0(p)$, the contribution from $s+x+y\equiv 0(p)$ is $(p-1)^3$. We need to be careful about double-counting. If $x=y$ and $sxy+x+y$ are both congruent to zero mod p, then we have $sx^2+2x\equiv 0(p)$. Every s has 1 corresponding x value, so we overcount by p^2.

Therefore, the second moment equals to:

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= (p-1)+(p-1)+(p-1)p+1+(p-1)^2+(p-1)^3-p^2-(p-1) \\ &= p^3-2p^2+p. \end{aligned} \tag{4.4}$$

□

4.1.2 $y^2 = x^3 + t^2x + st^4$

Lemma 4.3. *The first moment of the two-parameter family $y^2 = x^3 + t^2x + st^4$ is* 0.

Proof.

$$\begin{aligned} -p^2 A_{1,\mathcal{F}(p)} &= -\sum_{t(p)}\sum_{s(p)} a_{t,s}(p) = \sum_{t(p)}\sum_{x(p)}\sum_{s(p)} \left(\frac{x^3+t^2x+st^4}{p}\right) \\ &= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{s(p)} \left(\frac{t^3x^3+t^3x+st^4}{p}\right) \\ &= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{s(p)} \left(\frac{t^3}{p}\right)\left(\frac{x^3+x+st}{p}\right) \\ &= \sum_{x(p)}\sum_{s(p)}\sum_{t(p)} \left(\frac{t}{p}\right)\left(\frac{st+(x^3+x)}{p}\right) \\ &= \sum_{x(p)}\sum_{s(p)}\sum_{t(p)} \left(\frac{t}{p}\right)\left(\frac{t^{-1}st+(x^3+x)}{p}\right) \\ &= \sum_{x(p)}\sum_{s(p)}\sum_{t(p)} \left(\frac{t}{p}\right)\left(\frac{s+(x^3+x)}{p}\right). \end{aligned} \tag{4.5}$$

Since t is not zero, we send s to $t^{-1}s$, and look at the s sum, which equals to zero. □

Lemma 4.4. *The second moment times p^2 of the two-parameter family $y^2 = x^3+t^2x+st^4$ is $p^3-2p^2+p-2(p^2-p)\left(\frac{-3}{p}\right)$, which supports our Bias Conjecture.*

Proof. We have

$$\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} {a_{t,s}}^2(p)\\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3+t^2x+st^4}{p}\right)\left(\frac{y^3+t^2y+st^4}{p}\right)\\
&= \sum_{t=1}^{p-1} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{t^3x^3+t^3x+st^4}{p}\right)\left(\frac{t^3y^3+t^3y+st^4}{p}\right)\\
&= \sum_{t=1}^{p-1} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{t^6}{p}\right)\left(\frac{x^3+x+st}{p}\right)\left(\frac{y^3+y+st}{p}\right)\\
&= \sum_{t=0}^{p-1} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3+x+st}{p}\right)\left(\frac{y^3+y+st}{p}\right) - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3+x}{p}\right)\left(\frac{y^3+y}{p}\right)\\
&= \sum_{x,y(p)} \sum_{s(p)} \sum_{t(p)} \left(\frac{st+(x^3+x)}{p}\right)\left(\frac{st+(y^3+y)}{p}\right) - p\left[\sum_{x(p)} \left(\frac{x^3+x}{p}\right)\right]^2\\
&= \sum_{s=0} \sum_{t(p)} \left[\sum_{x(p)} \left(\frac{x^3+x}{p}\right)\right]^2 + \sum_{x,y(p)} \sum_{s\neq 0} \sum_{t(p)} \left(\frac{st+(x^3+x)}{p}\right)\left(\frac{st+(y^3+y)}{p}\right)\\
&- p\left[\sum_{x(p)} \left(\frac{x^3+x}{p}\right)\right]^2\\
&= \sum_{x,y(p)} \sum_{s\neq 0} \sum_{t(p)} \left(\frac{st+(x^3+x)}{p}\right)\left(\frac{st+(y^3+y)}{p}\right)\\
&= \sum_{x,y(p)} \sum_{s\neq 0} \sum_{t(p)} \left(\frac{ss^{-1}t+(x^3+x)}{p}\right)\left(\frac{ss^{-1}t+(y^3+y)}{p}\right)\\
&= \sum_{x,y(p)} \sum_{s\neq 0} \sum_{t(p)} \left(\frac{t+(x^3+x)}{p}\right)\left(\frac{t+(y^3+y)}{p}\right)\\
&= (p-1) \sum_{x,y(p)} \sum_{t(p)} \left(\frac{t+(x^3+x)}{p}\right)\left(\frac{t+(y^3+y)}{p}\right),
\end{aligned} \tag{4.6}$$

where in passing from the second to the third line we sent x and y modulo p to tx and ty, which is valid so long as t is not zero; to keep the sum over all t we need to subtract the $t = 0$ contribution. We can also see that when $s = 0$, since the t-sum is p and there is no t dependence, the contribution from $s = 0$ and $t = 0$ cancel out each other. Note that now as s is non-zero, we can send t to $s^{-1}t$, and we get a nice quadratic sum in t.

We use Lemma 2.4. The discriminant of our quadratic in t equals

$$\begin{aligned}
a &= 1 \\
b &= (x^3+x)+(y^3+y) \\
c &= (x^3+x)(y^3+y) \\
\delta(x,y) &= b^2-4ac = [(x^3+x)-(y^3+y)]^2 \\
&= [(x-y)(y^2+xy+(1+x^2))]^2,
\end{aligned} \tag{4.7}$$

and we are going to count the number of ways it vanishes. Therefore,

$$\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} = (p-1) & \left[\sum_{\substack{x,y \bmod p \\ \delta(x,y)\equiv 0(p)}} \sum_{t(p)} \left(\frac{t+(x^3+x)}{p}\right)\left(\frac{t+(y^3+y)}{p}\right) \right. \\
& \left. + \sum_{\substack{x,y \bmod p \\ \delta(x,y)\not\equiv 0(p)}} \sum_{t(p)} \left(\frac{t+(x^3+x)}{p}\right)\left(\frac{t+(y^3+y)}{p}\right) \right] \\
&= (p-1)\left[\sum_{\delta(x,y)\equiv 0(p)} (p-1) + \sum_{\delta(x,y)\not\equiv 0(p)} (-1) \right] \\
&= (p-1)\left[p \sum_{\delta(x,y)\equiv 0(p)} + p^2(-1) \right].
\end{aligned} \tag{4.8}$$

We have three cases for $\delta(x,y) \equiv 0(p)$:
Case 1: We need to count the number of solutions of $\delta_1(x,y) = x - y \equiv 0$, which happens p times when $x = y$.

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

$$y = \frac{-x \pm \sqrt{-3x^2-4}}{2}, \tag{4.9}$$

which reduced to finding when $-3x^2 - 4$ is a square. Thus, summing over x for $p > 2$ yields

$$\begin{aligned}
\sum_{x(p)} \left[1 + \left(\frac{-3x^2-4}{p}\right)\right] &= p + \sum_{x(p)} \left(\frac{-3x^2-4}{p}\right) \\
&= p - \left(\frac{-3}{p}\right),
\end{aligned} \tag{4.10}$$

which follows from Lemma 2.4. The discriminant now is $0^2 - 4 \cdot (-3) \cdot (-4)$. For $p \geq 5$, p does not divide the discriminant, hence this sum is $p - \left(\frac{-3}{p}\right)$.

Case 3: We need to be careful about double-counting. The double-counted pairs satisfy both $x = y$ and $y^2 + xy + (1 + x^2) \equiv 0(p)$, which means that they satisfy $3x^2 + 1 \equiv 0(p)$, or $-3x^2 \equiv 1$. 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 $\delta(x, y) \equiv 0(p)$ is:

$$\begin{aligned} \sum_{\delta_1(x,y)\equiv 0} + \sum_{\delta_2(x,y)\equiv 0} - \sum_{\delta_1(x,y)\equiv 0;\delta_2(x,y)\equiv 0} &= p + p - \left(\frac{-3}{p}\right) - 1 - \left(\frac{-3}{p}\right) \\ &= 2p - 1 - 2\left(\frac{-3}{p}\right). \end{aligned} \tag{4.11}$$

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

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= (p-1)\left[p\left(2p - 1 - 2\left(\frac{-3}{p}\right)\right) + p^2(-1)\right] \\ &= p(p-1)\left(p - 1 - 2\left(\frac{-3}{p}\right)\right) \\ &= p^3 - 2p^2 + p - 2(p^2 - p)\left(\frac{-3}{p}\right). \end{aligned} \tag{4.12}$$

□

4.1.3 $y^2 = x^3 + sx^2 - t^2x$

Lemma 4.5. *The first moment of the two-parameter family $y^2 = x^3 + sx^2 - t^2x$ is* 0.

Proof.

$$
\begin{aligned}
-p^2 A_{1,\mathcal{F}(p)} &= -\sum_{t(p)}\sum_{s(p)} a_{t,s}(p) = \sum_{t(p)}\sum_{x(p)}\sum_{s(p)} \left(\frac{x^3+sx^2-t^2x}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{s(p)} \left(\frac{t^3x^3+t^2sx^2-t^3x}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{x(p)}\sum_{s(p)} \left(\frac{t^2}{p}\right)\left(\frac{t(x^3-x)+sx^2}{p}\right) \\
&= \sum_{t=0}^{p-1}\sum_{x(p)}\sum_{s(p)} \left(\frac{t(x^3-x)+sx^2}{p}\right) - \sum_{x(p)}\sum_{s(p)}\left(\frac{sx^2}{p}\right) \\
&= \sum_{t(p)}\sum_{x(p)}\sum_{s(p)} \left(\frac{t(x^3-x)+sx^2}{p}\right) - 0 \qquad (4.13) \\
&= \sum_{t(p)}\sum_{s(p)}\sum_{x=-1,0,1;x(p)} \left(\frac{t(x^3-x)+sx^2}{p}\right) \\
&+ \sum_{t(p)}\sum_{s(p)}\sum_{x\neq-1,0,1;x(p)} \left(\frac{t(x^3-x)+sx^2}{p}\right) - 0 \\
&= \sum_{s(p)}\left(\frac{0}{p}\right) + \sum_{s(p)}\left(\frac{-s}{p}\right) + \sum_{s(p)}\left(\frac{s}{p}\right) + \sum_{t(p)}\sum_{s(p)}\sum_{x\neq-1,0,1;x(p)} \left(\frac{t(x^3-x)+sx^2}{p}\right) - 0 \\
&= 0+0+0+0-0 \\
&= 0
\end{aligned}
$$

$\square$

Lemma 4.6. *The second moment of the two-parameter family* $y^2 = x^3 + sx^2 - t^2x$ *times* p^2 *is* $p^3 - p^2$ *if* $p \equiv 1 \bmod 4$ *and* $p^3 - 3p^2 + 2p$ *if* $p \equiv 3 \bmod 4$*, which supports our Bias Conjecture.*

Proof.

$$\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} {a_{t,s}}^2(p) \\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3+sx^2-t^2x}{p}\right)\left(\frac{y^3+sy^2-t^2y}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{t^3x^3+t^2sx^2-t^3x}{p}\right)\left(\frac{t^3y^3+t^2sy^2-t^3y}{p}\right) \\
&= \sum_{t=1}^{p-1} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{t^4}{p}\right)\left(\frac{t(x^3-x)+sx^2}{p}\right)\left(\frac{t(y^3-y)+sy^2}{p}\right) \\
&= \sum_{t=0}^{p-1} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{t(x^3-x)+sx^2}{p}\right)\left(\frac{t(y^3-y)+sy^2}{p}\right) - \sum_{x,y(p)} \sum_{s(p)} \left(\frac{sx^2}{p}\right)\left(\frac{sy^2}{p}\right) \\
&= \sum_{x,y(p)} \sum_{s(p)} \sum_{t(p)} \left(\frac{t(x^3-x)+sx^2}{p}\right)\left(\frac{t(y^3-y)+sy^2}{p}\right) - (p-1)^3
\end{aligned} \tag{4.14}$$

We compute the discriminant of the equation in terms of t and s:

$$\begin{aligned}
a &= (x^3-x)(y^3-y) \\
b &= (x^3-x)sy^2 + (y^3-y)sx^2 \\
c &= s^2x^2y^2 \\
\delta &= b^2 - 4ac = [(x^3-x)sy^2 - (y^3-y)sx^2]^2 \\
&= [sxy(x-y)(xy+1)]^2.
\end{aligned} \tag{4.15}$$

When s is congruent to zero mod p, $xy(x-y)(xy+1)$ does not have to be congruent to zero mod p. For our convenience, we only count the number of times when $x \neq 0$, $y = 0$ and $x = 0$, $y \neq 0$. The contribution is $(p-1)^2$.

When s is not congruent to zero mod p, $xy(x-y)(xy+1)$ has to be congruent to zero mod p. The contribution from $xy(x-y)$ is $(p-1)(p-1)$, as $x \neq 0$, $y \neq 0$ and $x \neq y$. Then we have $xy+1 \equiv 0(p)$, so the contribution is also $(p-1)(p-1)$. Hence, its total contribution is $(p-1)(p-1)(2p-2)$.

Therefore, on average p^2 times the second moment equals to

$$\begin{aligned}
pA_{2,\mathcal{F}(p)} &= (p-1)^2 + (p-1)(p-1)(2p-2) - (p-1)^3 \\
&= p^3 - 2p^2 + p.
\end{aligned} \tag{4.16}$$

When $x = 7 \neq 0$ and $p \equiv 1 \bmod 4$, by the Jacobi Symbol (Lemma 2.5)

$\left(\frac{x}{p}\right)\left(\frac{-y}{p}\right) = \left(\frac{x^2}{p}\right)$ contributes p. Hence, we have

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= p^3 - 2p^2 + p + p(p-1) \\ &= p^3 - p^2. \end{aligned} \tag{4.17}$$

When $x = y \neq 0$ and $p \equiv 3 \bmod 4$, by the Jacobi Symbol (Lemma 2.5) $\left(\frac{x}{p}\right)\left(\frac{-y}{p}\right) = -\left(\frac{x^2}{p}\right)$ contributes $-p$. Hence, we have

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= p^3 - 2p^2 + p - p(p-1) \\ &= p^3 - 3p^2 + 2p. \end{aligned} \tag{4.18}$$

□

4.2 Construction of Rank 1 Families

4.2.1 $y^2 = x^3 + ts^2x^2 + (t^3 - t^2)x$

Lemma 4.7. *The first moment of the two-parameter family $y^2 = x^3 + ts^2x^2 + (t^3 - t^2)x$ is -1.*

Proof.

$$\begin{aligned} -p^2 A_{1,\mathcal{F}(p)} &= -\sum_{t(p)}\sum_{s(p)} a_{t,s}(p) \\ &= \sum_{t(p)}\sum_{x(p)}\sum_{s(p)} \left(\frac{x^3 + ts^2x^2 + (t^3 - t^2)x}{p}\right) \\ &= \sum_{t(p)}\sum_{s(p)}\sum_{x=1} \left(\frac{t^3x^3 + t^3s^2x^2 + t^4x - t^3x}{p}\right) \\ &= \sum_{t(p)}\sum_{s(p)}\sum_{x=1} \left(\frac{t^3}{p}\right)\left(\frac{x^3 + s^2x^2 + tx - x}{p}\right) \\ &= \sum_{x(p)}\sum_{s(p)}\sum_{t(p)} \left(\frac{t}{p}\right)\left(\frac{tx + (x^3 + s^2x^2 - x)}{p}\right) \end{aligned} \tag{4.19}$$

The t-sum is $p-1$ if $p \mid (x^3 + s^2x^2 - x)$ and -1 otherwise. When s is congruent to zero mod p, $x = \pm 1$ contributes $p-1$, and other times everything else contributes -1. When s is not congruent to zero mod p, which happens $p-1$ times, $x = 0$ contributes $p-1$ and other times everything else contributes -1. Thus, the total contribution is $p[2(p-1) + (p-2)(-1)] + (p-1)[1(p-1) + (p-1)(-1)] = p^2$. □

Lemma 4.8. *The second moment of the two-parameter family $y^2 = x^3 + ts^2x^2 + (t^3 - t^2)x$ times p^2 is $p^3 - 3p^2 + 3p - 1$ when $p \equiv 1 \bmod 4$ and $p^3 - 3p^2 + p + 1$ when $p \equiv 3 \bmod 4$, which supports our Bias Conjecture.*

Proof.

$$\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} {a_{t,s}}^2(p) \\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 + ts^2x^2 + (t^3 - t^2)x}{p}\right)\left(\frac{y^3 + ts^2y^2 + (t^3 - t^2)y}{p}\right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t=1}^{p-1} \left(\frac{t^3x^3 + t^3s^2x^2 + t^4x - t^3x}{p}\right)\left(\frac{t^3y^3 + t^3s^2y^2 + t^4y - t^3y}{p}\right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t=1}^{p-1} \left(\frac{t^6}{p}\right)\left(\frac{tx + x^3 + s^2x^2 - x}{p}\right)\left(\frac{ty + y^3 + s^2y^2 - y}{p}\right) \qquad (4.20) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t(p)} \left(\frac{tx + x^3 + s^2x^2 - x}{p}\right)\left(\frac{ty + y^3 + s^2y^2 - y}{p}\right) \\
&\quad - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 + s^2x^2 - x}{p}\right)\left(\frac{y^3 + s^2y^2 - y}{p}\right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t(p)} \left(\frac{tx + x^3 + s^2x^2 - x}{p}\right)\left(\frac{ty + y^3 + s^2y^2 - y}{p}\right) - (p^2 - 1)
\end{aligned}$$

$$\begin{aligned}
a &= xy \\
b &= x(y^3 + s^2y^2 - y) + y(x^3 + s^2x^2 - x) \\
c &= (x^3 + s^2x^2 - x)(y^3 + s^2y^2 - y) \\
\delta &= b^2 - 4ac = [x(y^3 + s^2y^2 - y) - y(x^3 + s^2x^2 - x)]^2 \\
&= [xy(y - x)(s^2 + x + y)]^2
\end{aligned} \qquad (4.21)$$

When $x = 0$, y can be any number except 0 because we have $x = y$ later (and there's case when $x = y = 0$. For the same reason, when $y = 0$, x can be any number except 0. For $x = y$, there are p values. In all of these three cases, s can be any value except 0 (we have a special case later) so the total contribution is $(p-1)[(p-1) + (p-1) + p]$.

When s is congruent to zero mod p, which happens once, $x = -y \neq 0$ happens $p - 1$ times, so its contribution is $p - 1$.

When s is not congruent to zero mod p, which happens $p - 1$ times, the contribution from $s^2 + x + y \equiv 0(p)$ is $(p-1)(p-2)^2$.

We must be careful about double-counting. When $y - x$ and $s^2 + x + y$ are both congruent to zero mod p $(s, x, y \neq 0)$, we have $s^2 + 2x \equiv 0(p)$. Each s has a corresponding x, so the contribution from this case is $(p - 1)$.

Hence, on average the second moment times p^2 equals to

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= 3(p-1)[(p-1)+(p-1)+p]+(p-1)+(p-1)(p-2)^2-(p-1)-(p^2-1) \\ &= p^3-3p^2+2p. \end{aligned} \tag{4.22}$$

If $p \equiv 1 \bmod 4$ and when $x=-y$, by the Jacobi Symbol (Lemma 2.5) $\left(\frac{x}{p}\right)\left(\frac{-y}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{x^2}{p}\right) = \left(\frac{x^2}{p}\right)$ contributes an extra $p-1$ (as s must equal to 0 and $x, y \neq 0$):

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= p^3-3p^2+2p+p-1 \\ &= p^3-3p^2+3p-1. \end{aligned} \tag{4.23}$$

If $p \equiv 3 \bmod 4$ and when $x=-y$, by the Jacobi Symbol (Lemma 2.5) $\left(\frac{-1}{p}\right)\left(\frac{x^2}{p}\right) = -\left(\frac{x^2}{p}\right)$ contributes an extra $-(p-1)$ (as s must equal to 0 and $x, y \neq 0$):

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= p^3-3p^2+2p-(p-1) \\ &= p^3-3p^2+p+1. \end{aligned} \tag{4.24}$$

□

4.2.2 $y^2 = x^3 + t^2x^2 + (t^3 - t^2)sx$

Lemma 4.9. *The first moment of the two-parameter family $y^2 = x^3 + t^2x^2 + (t^3 - t^2)sx$ is -1.*

Proof.

$$\begin{aligned} -p^2 A_{1,\mathcal{F}(p)} &= -\sum_{t(p)}\sum_{s(p)} a_{t,s}(p) \\ &= \sum_{t(p)}\sum_{x(p)}\sum_{s(p)} \left(\frac{x^3+t^2x^2+(t^3-t^2)sx}{p}\right) \\ &= \sum_{t(p)}\sum_{s(p)}\sum_{x=1} \left(\frac{t^3x^3+t^4x^2+t^4sx-t^3sx}{p}\right) \\ &= \sum_{t(p)}\sum_{s(p)}\sum_{x=1} \left(\frac{t^3}{p}\right)\left(\frac{x^3+tx^2+tsx-sx}{p}\right) \\ &= \sum_{x(p)}\sum_{s(p)}\sum_{t(p)} \left(\frac{t}{p}\right)\left(\frac{t(x^2+sx)+(x^3-sx)}{p}\right) \end{aligned} \tag{4.25}$$

The t-sum is $p-1$ if $p \mid (x^3 - sx)$ and -1 otherwise. When s is congruent to zero mod p and $x = 0$, s vanishes so every s contributes p. When s is not congruent to zero mod p, which happens $p-1$ times, $x^2 = s \neq 0$ contributes $p-1$ and other times everything else contributes -1. Thus, the total contribution is $p^2 + p(p-1)[1(p-1) + (p-1)(-1)] = p^2$. $\square$

Lemma 4.10. *The second moment of the two-parameter family* $y^2 = x^3 + t^2x^2 + (t^3 - t^2)sx$ *times* p^2 *is* $p^3 - 3p^2 + 3p$ *if* $p \equiv 1 \bmod 4$ *and* $p^3 - 5p^2 + 7p$ *if* $p \equiv 3 \bmod 4$*, which supports our Bias Conjecture.*

Proof.

$$\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} {a_{t,s}}^2(p) \\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 + t^2x^2 + (t^3 - t^2)sx}{p}\right)\left(\frac{y^3 + t^2y^2 + (t^3 - t^2)sy}{p}\right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t=1}^{p-1} \left(\frac{t^3x^3 + t^4x^2 + t^4sx - t^3sx}{p}\right)\left(\frac{t^3y^3 + t^4y^2 + t^4sy - t^3sy}{p}\right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t=1}^{p-1} \left(\frac{t^6}{p}\right)\left(\frac{t(x^2 + sx) + (x^3 - sx)}{p}\right)\left(\frac{t(y^2 + sy) + (y^3 - sy)}{p}\right) \\
&\quad - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 - sx}{p}\right)\left(\frac{y^3 - sy}{p}\right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t(p)} \left(\frac{t(x^2 + sx) + (x^3 - sx)}{p}\right)\left(\frac{t(y^2 + sy) + (y^3 - sy)}{p}\right) \\
&\quad - p(p-1)
\end{aligned} \tag{4.26}$$

The discriminant of the equation equals to

$$\begin{aligned}
a &= (x^2 + sx)(y^2 + sy) \\
b &= (x^2 + sx)(y^3 - sy) + (y^2 + sy)(x^3 - sx) \\
c &= (x^3 - sx)(y^3 - sy) \\
\delta &= b^2 - 4ac = [(x^2 + sx)(y^3 - sy) - (y^2 + sy)(x^3 - sx)]^2 \\
&= [xy(x - y)(s(x + y + 1) + xy)]^2.
\end{aligned} \tag{4.27}$$

We have two special cases when xy is congruent to zero mod p. When $x = 0$ and $y = 1$ or $y = 0$ and $x = 1$, s vanishes. The contribution from other $xy(x-y)$ cases is $p(p-2) + p(p-2) + p^2 = 3p^2 - 4p$. Hence, the total contribution is $3p^2 - 4p + 2$.

When s is congruent to zero mod p, $xy = 0$. Since x and y can not equal to zero, there is no contribution from this case.

When s is not congruent to zero mod p, the contribution is $(p-1)^3(x \neq 0$ and $y \neq 0)$. We must be careful about double-counting. We are aware that if xy and $s(x+y+1)+xy$ are both congruent to zero, we double-count by $2p(p-2)$ solutions (s can be any value, but $x \neq 0, 1$ and $y \neq 0, 1$). If $x-y$ and $s(x+y+1)+xy$ are both congruent to zero, we get $s(2x+1)+x^2 \equiv 0(p)$. We double-count by $(p-1)p+1$ solutions as when $x \neq 0$, the contribution is always p except when $x=1$, the contribution is 1.

Thus, on average the second moment of this family times p^2 equals to

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= 3p^2 - 4p + 2 + 0 + (p-1)^3 - 2p(p-2) - (p-1)p - 1 - p(p-1) \\ &= p^3 - 4p^2 + 5p. \end{aligned} \tag{4.28}$$

If $p \equiv 1 \bmod 4$ and $x = -y$, by the Jacobi Symbol (Lemma 2.5) there is an extra contribution of $(p-1)^2+1$ from $s - y^2 \equiv 0(p)$:

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= p^3 - 4p^2 + 5p + (p-1)^2 + 1 \\ &= p^3 - 3p^2 + 3p. \end{aligned} \tag{4.29}$$

If $p \equiv 3 \bmod 4$ and $x = -y$, by the Jacobi Symbol (Lemma 2.5) there is an extra contribution of $-[(p-1)^2+1]$ from $s - y^2 \equiv 0(p)$:

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= p^3 - 4p^2 + 5p - [(p-1)^2 + 1] \\ &= p^3 - 5p^2 + 7p. \end{aligned} \tag{4.30}$$

$\square$

4.3 Construction of Rank 2 Families

4.3.1 $y^2 = x^3 + t^2x^2 - (s^2 - s)t^2x$

Lemma 4.11. *The first moment of the two-parameter family $y^2 = x^3 + t^2x^2 - (s^2 - s)t^2x$ is -2.*

Proof.

$$\begin{aligned}
-p^2 A_{1,\mathcal{F}(p)} &= -\sum_{t(p)}\sum_{s(p)} a_{t,s}(p) \\
&= \sum_{t(p)}\sum_{x(p)}\sum_{s(p)} \left(\frac{x^3+t^2x^2-(s^2-s)t^2x}{p}\right) \\
&= \sum_{t(p)}\sum_{s(p)}\sum_{x=1} \left(\frac{t^3x^3+t^4x^2-(s^2-s)t^3x}{p}\right) \\
&= \sum_{t(p)}\sum_{s(p)}\sum_{x=1} \left(\frac{t^3}{p}\right)\left(\frac{x^3+tx^2-(s^2-s)x}{p}\right) \\
&= \sum_{x(p)}\sum_{s(p)}\sum_{t(p)} \left(\frac{t}{p}\right)\left(\frac{tx^2+(x^3-(s^2-s)x)}{p}\right)
\end{aligned} \tag{4.31}$$

The t-sum is $p-1$ if $p \mid (x^3-(s^2-s)x)$ and -1 otherwise. When s^2-s is congruent to zero mod p - which happens twice - and $x=0$, s vanishes so x contributes p. When s is not congruent to zero mod p, every x contributes $p-1$ ($x \neq 0$). Thus, the total contribution is $p^2+p[2(p-1)+(p-2)(-1)] = 2p^2$. $\square$

Lemma 4.12. *The second moment of the two-parameter family $y^2 = x^3+t^2x^2-(s^2-s)t^2x$ times p^2 is $p^3-3p^2+3p-\sum_{s(p)}\sum_{x,y(p)}\left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right)$ if $p \equiv 1 \bmod 4$ and p^3-3p^2+2p if $p \equiv 3 \bmod 4$, which supports our Bias Conjecture.*

Proof.

$$
\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} {a_{t,s}}^2(p)\\
&= \sum_{t(p)}\sum_{s(p)}\sum_{x,y(p)} \left(\frac{x^3+t^2x^2-(s^2-s)t^2x}{p}\right)\left(\frac{y^3+t^2y^2-(s^2-s)t^2y}{p}\right)\\
&= \sum_{s(p)}\sum_{x,y(p)}\sum_{t=1}^{p-1} \left(\frac{t^3x^3+t^4x^2-(s^2-s)t^3x}{p}\right)\left(\frac{t^3y^3+t^4y^2-(s^2-s)t^3y}{p}\right)\\
&= \sum_{s(p)}\sum_{x,y(p)}\sum_{t=1}^{p-1} \left(\frac{t^6}{p}\right)\left(\frac{tx^2+(x^3-(s^2-s)x)}{p}\right)\left(\frac{ty^2+(y^3-(s^2-s)y)}{p}\right) \qquad (4.32)\\
&\quad - \sum_{s(p)}\sum_{x,y(p)} \left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right)\\
&= \sum_{s(p)}\sum_{x,y(p)}\sum_{t(p)} \left(\frac{tx^2+(x^3-(s^2-s)x)}{p}\right)\left(\frac{ty^2+(y^3-(s^2-s)y)}{p}\right) -\\
&\quad - \sum_{s(p)}\sum_{x,y(p)} \left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right)
\end{aligned}
$$

$$
\begin{aligned}
a &= x^2y^2\\
b &= (y^3-(s^2-s)y)x^2+(x^3-(s^2-s)x)y^2\\
c &= (y^3-(s^2-s)y)(x^3-(s^2-s)x)\\
\delta &= b^2-4ac = [(y^3-(s^2-s)y)x^2-(x^3-(s^2-s)x)y^2]^2\\
&= [xy(x-y)(-s^2+s-xy)]^2
\end{aligned}
\qquad (4.33)
$$

The contribution from $xy(x-y)$ is $p(p-1)+p(p-1)+p^2 = 3p^2-2p$.

When $s = 0$ or $s = -1$, $-s^2+s$ is congruent to zero mod p. We need $xy \equiv 0(p)$. However, there is no contribution, since $x \neq 0$ and $y \neq 0$.

When $-s^2+s$ is not congruent to zero mod p, we need $-s^2+s-xy \equiv 0(p)$. The contribution from this case is $(p-2)(p-1)^2$.

Last but not least, we calculate the double-counting cases. When xy and $-s^2+s-xy$ are both congruent to zero mod p, the contribution is 2. When $x-y$ and $-s^2+s-xy$ are both congruent to zero mod p, we have $-s^2+s-x^2 \equiv 0(p)$ and the contribution is $2p^2-2$ $(s \neq 0,1)$.

Thus, on average the second moment of this family times p^2 equals to:

$$\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} &= 3p^2 - 2p + 0 + (p-2)(p-1)^2 - (2p^2-2) \\
&- \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right) \\
&= p^3 - 3p^2 + 3p - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right).
\end{aligned} \tag{4.34}$$

Keep in mind that although we have an extra term in the second moment above, the term will contribute positive values, making the negative bias larger. Hence, the Bias Conjecture still holds.

If $p \equiv 1 \bmod 4$, there is an extra contribution of p as s can be any value:

$$\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} &= p^3 - 3p^2 + 3p - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right) + p \\
&= p^3 - 3p^2 + 4p - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right).
\end{aligned} \tag{4.35}$$

If $p \equiv 3 \bmod 4$, $\sum_{s(p)} \sum_{x(p)} \left(\frac{x^3-(s^2-s)x}{p}\right) = \sum_{s(p)} \sum_{x(p)} \left(\frac{x}{p}\right)\left(\frac{x^2-s^2+s}{p}\right) = 0$ because the two distinct solutions to $1+4x^2 \equiv 0 \bmod p$ are both non-squares modulo p. In addition, there is an extra contribution of $-p$ as s can be any value:

$$\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} &= p^3 - 3p^2 + 3p - 0 - p \\
&= p^3 - 3p^2 + 2p.
\end{aligned} \tag{4.36}$$

□

4.3.2 $y^2 = x^3 - t^2x + t^3s^2 + t^4$

Lemma 4.13. *The first moment of the two-parameter family $y^2 = x^3 - t^2x + t^3s^2 + t^4$ is -2.*

Proof.

$$\begin{aligned}
-p^2 A_{1,\mathcal{F}(p)} &= -\sum_{t(p)}\sum_{s(p)} a_{t,s}(p) \\
&= \sum_{t(p)}\sum_{x(p)}\sum_{s(p)} \left(\frac{x^3 - t^2x + t^3s^2 + t^4}{p}\right) \\
&= \sum_{t(p)}\sum_{s(p)}\sum_{x=1} \left(\frac{t^3x^3 - t^3x + t^3s^2 + t^4}{p}\right) \\
&= \sum_{t(p)}\sum_{s(p)}\sum_{x=1} \left(\frac{t^3}{p}\right)\left(\frac{x^3 - x + s^2 + t}{p}\right) \\
&= \sum_{x(p)}\sum_{s(p)}\sum_{t(p)} \left(\frac{t}{p}\right)\left(\frac{t + (x^3 - x + s^2)}{p}\right)
\end{aligned} \tag{4.37}$$

The t-sum is $p-1$ if $p \mid x^3 - x + s^2$ and -1 otherwise. When $s^2 = 0$, each of $x = -1, 0, 1$ contributes $p-1$ and everything else contributes -1. When $s^2 \neq 0$, one x value contributes $p-1$ and everything else contributes -1. Thus, the total contribution is $p[3(p-1)+(p-3)(-1)]+(p-1)[1(p-1)+(p-1)(-1)] = 2p^2$. $\square$

Lemma 4.14. *The second moment of the two-parameter family* $y^2 = x^3 - t^2x + t^3s^2 + t^4$ *times* p^2 *is* $p^3 - 2p^2 + p - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right] p^2$*, which supports our Bias Conjecture.*

Proof.

$$\begin{aligned}
p^2 A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} a_{t,s}{}^2(p) \\
&= \sum_{t(p)}\sum_{s(p)}\sum_{x,y(p)} \left(\frac{x^3 - t^2x + t^3s^2 + t^4}{p}\right)\left(\frac{y^3 - t^2y + t^3s^2 + t^4}{p}\right) \\
&= \sum_{s(p)}\sum_{x,y(p)}\sum_{t=1}^{p-1} \left(\frac{t^3x^3 - t^3x + t^3s^2 + t^4}{p}\right)\left(\frac{t^3y^3 - t^3y + t^3s^2 + t^4}{p}\right) \\
&= \sum_{s(p)}\sum_{x,y(p)}\sum_{t=1}^{p-1} \left(\frac{t^6}{p}\right)\left(\frac{t + (x^3 - x + s^2)}{p}\right)\left(\frac{t + (y^3 - y + s^2)}{p}\right) \\
&\quad - \sum_{s(p)}\sum_{x,y(p)} \left(\frac{x^3 - x + s^2}{p}\right)\left(\frac{y^3 - y + s^2}{p}\right) \\
&= \sum_{s(p)}\sum_{x,y(p)}\sum_{t(p)} \left(\frac{t + (x^3 - x + s^2)}{p}\right)\left(\frac{t + (y^3 - y + s^2)}{p}\right) - p(p-1)
\end{aligned} \tag{4.38}$$

$$\begin{aligned} a &= 1 \\ b &= (x^3 - x + s^2) + (y^3 - y + s^2) \\ c &= (x^3 - x + s^2)(y^3 - y + s^2) \\ \delta &= b^2 - 4ac = [(x^3 - x + s^2) - (y^3 - y + s^2)]^2 \\ &= [(x-y)(x^2 + xy + y^2 - 1)]^2 \end{aligned} \tag{4.39}$$

We see that s disappears, so every s has the same contribution. The solutions to the first factor are $x = y$, which happens p times. For fixed$x$, the discriminant of the second factor can be rewritten as $\frac{-x \pm \sqrt{4-3x^2}}{2}$, and the sum is $\sum_{x=1}^{p-1}[1 + \left(\frac{4-3x^2}{p}\right)] = p - 1 - \left(\frac{-3}{p}\right)$. We must be careful about double-counting. When both factors are congruent to zero mod p, some pairs satisify $3x^2 \equiv 1$. If $\left(\frac{3}{p}\right) = 1$ we have double-counted two solutions; if it is -1, there was no double counting. Hence, the contribution is $p^2(p - 1 - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right]$.

Thus,

$$\begin{aligned} p^2 A_{2,\mathcal{F}(p)} &= p^2(p - 1 - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right] - p(p-1) \\ &= p^3 - 2p^2 + p - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right] p^2. \end{aligned} \tag{4.40}$$

□

5 Conclusion and Future Work

We have shown in every one- and two-parameter family we are able to prove theoretically the largest lower order term that does not average to zero has a negative average. For the families we are unable to prove theoretically, we conjecture that these terms of their second moments on average are negative from the data we get. However, because of our limitation to generate data, we are not sure if the form contains terms of size $p^{3/2}$ because they dwarf the smaller order p terms and make them hard to see. We can investigate on finding a more efficient way to generate data. In particular, there are families with terms of size $p^{3/2}$ that average to zero, and are followed by terms of size p with a negative average.

While we have concentrated on the second moments of the Fourier coefficients in elliptic curves, there are a lot of other fields we can explore. For example, we can explore higher ranks (> 2), higher moments (> 2) as well as other families, and see if similar biases exist. The difficulty is that the resulting sums cannot be handled by existing techniques; in general we cannot even compute $a(p)$ for a given elliptic curve, as we cannot do cubic Legendre sums.

Another area we want to focus on in the future is getting to know the two-parameter families better. What are the implications of the negative bias of the two-parameter families? How do they behave differently from one-parameter families or other families and why?

We have two tables below: the first table records the rank, the first moment times p and the second moment times p of every one-parameter family we prove theoretically or generate data for the first 100 primes in this paper; the second table records the rank, the first moment times p^2 and the second moment times p^2 of every two-parameter family we prove theoretically. We set $\delta_1(p)$ to be 1 if $p \equiv 1 \bmod 4$ and 0 otherwise, and $\delta_3(p)$ to be 1 if $p \equiv 3 \bmod 4$ and 0 otherwise.

One-Parameter Family	Rank	$pA_{1,\mathcal{F}(p)}$	$pA_{2,\mathcal{F}(p)}$
$y^2 = x^3 - x^2 - x + t$	0	0	$p^2 - 2p - \left(\frac{-3}{p}\right)p$
$y^2 = x^3 - tx^2 + (x-1)t^2$	0	0	$p^2 - 2p - [\sum_{x(p)} \left(\frac{x^3-x^2+x}{p}\right)]^2 - \left(\frac{-3}{p}\right)p$
$y^2 = x^3 + tx^2 + t^2$	1	-p	$p^2 - 2p - \left(\frac{-3}{p}\right)p - 1$
$y^2 = x^3 + tx^2 + x + 1$	1	-p	$p^2 - p - 1 + p\sum_{x(p)} \left(\frac{4x^3+x^2+2x+1}{p}\right)$
$y^2 = x^3 + tx^2 + tx + t^2$	1	-p	$p^2 - p - 1 - \delta_1(p)(2p)$
$y^2 = x^3 - x^2 + (x^2 - x)t + 1$	2	-2p	$p^2 - 1$ (“conjectured on average”)
$y^2 = x^3 - x + t^4$	2(“conjectured on average”)	-2p (“conjectured on average”)	$p^2 - p$ (“conjectured on average”)

Table 3: The one-parameter families we proved theoretically all show that the largest lower order term that does not average to zero has a negative average. Unfortunately, we are not able to prove the second moment of $y^2 = x^3 - x^2 + (x^2 - x)t + 1$ as well as the first and second moment of $y^2 = x^3 - x + t^4$ theoretically. Due to the limited power of our computation software, we only generated data for the first 100 primes. Also, keep in mind that we did not observe the same form for every prime; we conjectured the average of its first or second moment. One family worth noting is $y^2 = x^3 - x^2 + (x^2 - x)t + 1$; it is a potential counterexample to a stronger form of Miller's Bias Conjecture based on the families studied to date, which is that in the second moment expansion the first term that does not average to zero is the p term and that has a negative average.

Two-Parameter Family	$p^2A_{1,\mathcal{F}(p)}$	$p^2A_{2,\mathcal{F}(p)}$
$y^2 = x^3 + tx + sx^2$	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	$p^3 - p^2 - \delta_3(p)(2p^2 - 2p)$
$y^2 = x^3 + ts^2x^2 + (t^3 - t^2)x$	$-p^2$	$p^3 - 3p^2 + 3p - 1 - \delta_3(p)(2p - 2)$
$y^2 = x^3 + t^2x^2 + (t^3 - t^2)sx$	$-p^2$	$p^3 - 3p^2 + 3p - \delta_3(p)(2p^2 - 4p)$
$y^2 = x^3 + t^2x^2 - (s^2 - s)t^2x$	$-2p^2$	$p^3 - 3p^2 + 2p + \delta_1(p)(p - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right))$
$y^2 = x^3 - t^2x + t^3s^2 + t^4$	$-2p^2$	$p^3 - 2p^2 + p - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right] p^2$

Table 4: The two-parameter families we proved theoretically all show a negative bias in the largest lower order term in the second-moment expansion.

6 Acknowledgements

First of all, I want to thank my mentor, Professor S. J. Miller, for his patience and dedication throughout the research process. Elliptic Curve is an intricate and exciting topic; without his guidance, I would not be able to familiarize with it quickly and explore its new realms.

I am also deeply grateful to my family, friends, and teachers for their unwavering support. They are willing to listen to my doubts, frustrations, and happiness and help me balance this project with other aspects of my life.

Pursuing this project has made me realized the fun behind the amount of work that is being put into research as a mathematician. I hope that one day, I will be able to spread the beauty of mathematics and help others.

7 Declaration of Academic Integrity

I solemnly declare that the paper I submitted is under the guidance of my mentor. As far as I am concerned, except the citations and references listed, this paper does not contain others' works. If not true, I will assume all responsibilities.

A Proof of Linear and Quadratic Legendre Sums

Lemma A.1 (Linear Legendre Sum)**.**

$$\sum_{x \bmod p} \left(\frac{ax+b}{p}\right) = 0 \ if \ p \nmid a. \tag{A.1}$$

Proof. Since $p \nmid a$, there are exactly $\frac{p-1}{2}$ quadratic residues, $\frac{p-1}{2}$ quadratic nonresidues, and 1 number that is divisible by p in a system of residues modulo p. Hence, linear legendre sum equals to

$$\sum_{x \bmod p} \left(\frac{ax+b}{p}\right) = (\frac{p-1}{2}) \times 1 + \frac{p-1}{2} \times -1 + 1 \times 0 = 0. \tag{A.2}$$

□

Lemma A.2 (Quadratic Legendre Sum)**.** *Let a, b, c be positive integers. Assume $p > 2$ and $a \not\equiv 0 \mod p$, we have:*

$$\sum_{x \bmod p} \left(\frac{ax^2+bx+c}{p}\right) = \begin{cases} -\left(\frac{a}{p}\right), & if\ p \nmid b^2-4ac. \\ (p-1)\left(\frac{a}{p}\right), & if\ p \mid b^2-4ac. \end{cases} \tag{A.3}$$

Proof.

$$\begin{aligned}
\sum_{x \bmod p} \left(\frac{ax^2+bx+c}{p}\right) &= \left(\frac{a^{-1}}{p}\right) \sum_{x \bmod p} \left(\frac{a^2x^2+bax+ac}{p}\right) \\
&= \left(\frac{a}{p}\right) \sum_{x \bmod p} \left(\frac{x^2+bx+ac}{p}\right) \\
&= \left(\frac{a}{p}\right) \sum_{x \bmod p} \left(\frac{x^2+bx+4^{-1}b^2+ac-4^{-1}b^2}{p}\right) \\
&= \left(\frac{a}{p}\right) \sum_{x \bmod p} \left(\frac{(x+2^{-1}b)^2-4^{-1}(b^2-4ac)}{p}\right) \\
&= \sum_{x \bmod p} \left(\frac{a}{p}\right) \left(\frac{x^2-D}{p}\right)
\end{aligned} \tag{A.4}$$

We have three cases in total:
Case 1: If D is zero mod p, then the sum equals to:

$$\sum_{x=0}^{p-1} \left(\frac{x^2}{p}\right) = p-1. \tag{A.5}$$

Case 2: If D is a non-zero square mod p, then

$$\sum_{x=0}^{p-1} \left(\frac{x^2-D}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x+d}{p}\right)\left(\frac{x-d}{p}\right) = -1. \tag{A.6}$$

where $d^2 = D$. Shift x by d, and then replace x with $(2d)x$, we have:

$$\begin{aligned}
S(d) &= \sum_{x=0}^{p-1} \left(\frac{x+2d}{p}\right)\left(\frac{x}{p}\right) \\
&= \sum_{x=0}^{p-1} \left(\frac{2dx+2d}{p}\right)\left(\frac{2dx}{p}\right) \\
&= \left(\frac{2d}{p}\right)^2 \sum_{x=0}^{p-1} \left(\frac{x+1}{p}\right)\left(\frac{x}{p}\right) \\
&= S(1).
\end{aligned} \tag{A.7}$$

Note that $\sum_{d=0}^{p-1} S(d)$ equals to 0, so $\sum_{d \bmod p} S(d)$ equals to 0. We can also see that if d is not 0, then $S(d) = S(1)$ because $\left(\frac{2d}{p}\right)^2$ equals to 1, and if we move $2d$ by 1, the two equations are equivalent to each other. If d equals to 0, $S(0) = p-1$ because $\left(\frac{x+d}{p}\right)\left(\frac{x}{p}\right)$ now becomes $\left(\frac{x}{p}\right)^2$. Hence,

$$\begin{aligned} \sum_{d \bmod p} S(d) &= S(0) + \sum_{d=1}^{p-1} S(1) \\ &= (p-1) + (p-1)S(1). \end{aligned} \tag{A.8}$$

Thus, $S(1) = -1$.

Case 3: When D is not a square, we use the multiplicative property of Legendre sums (i.e when p is a prime, $(0, 1, 2, ..., p-1)$ is the same as $(1, g, g^2, ..., g^{p-1})$ for some generator g) to compute the sum. We can rewrite D as g^{2k+1} because anything of the form g^{2k} is a perfect square mod p, and of the form g^{2k+1} is not. We can also rewrite x as $g^k x$ because summing over x mod p is the same as summing over $g^k x$ mod p. Therefore, we have

$$\sum_{x \bmod p} \left(\frac{g^{2k}x^2 - g^{2k+1}}{p}\right) = \sum_{x \bmod p} \left(\frac{g^{2k}}{p}\right)\left(\frac{x^2 - g}{p}\right) = \sum_{x \bmod p} \left(\frac{x^2 - g}{p}\right). \tag{A.9}$$

Thus, $S(g^{2k+1}) = S(g)$ for all k, which means contribution for $\left(\frac{x^2-g}{p}\right)$ is the same.

Define the set of non-zero squares as $\mathcal{S}$ and the set of non-squares as $\mathcal{N}$. This shows that for all non-squares, the contribution is the same and it is the sum of $\left(\frac{x^2-g}{p}\right)$. Since $\sum_{D=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x^2-D}{p}\right) = 0$, the quadratic Legendre sum $S(g)$ when D is not a square equals to:

$$\begin{aligned} \sum_{D=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x^2-D}{p}\right) &= \sum_{x=0}^{p-1}\left(\frac{x^2}{p}\right) + \sum_{D\in\mathcal{S}}\sum_{x=0}^{p-1}\left(\frac{x^2-D}{p}\right) + \sum_{g\in\mathcal{N}}\sum_{x=0}^{p-1}\left(\frac{x^2-g}{p}\right) \\ &= (p-1) + \frac{p-1}{2}(-1) + \frac{p-1}{2}S(g). \end{aligned} \tag{A.10}$$

Hence, $S(g) = -1$.

□

B Proof of Rational Surfaces for One-Parameter Families

In this section, we will prove that the one-parameter families we computed are rational surfaces using **Theorem 2.3**, or else the first moment does not equal to their rank.

B.1 Rank 0 One-Parameter Families

B.1.1 $y^2 = x^3 - x^2 - x - t$

Lemma B.1. *One-parameter family $y^2 = x^3 - x^2 - x - t$ is a rational surface.*

Proof. We first convert the family to its Weierstrass form and we have

$$\begin{aligned} a'2 &= -1, \\ a'4 &= -1, \\ a'6 &= -t, \\ a''4 &= -1 - \frac{1}{3}(-1)^2 = -\frac{4}{3}, \\ a''6 &= -t + \frac{2}{27}(-1)^3 - \frac{1}{3} \cdot (-1) \cdot (-1) = -t - \frac{11}{27}. \end{aligned} \tag{B.1}$$

Hence, we get

$$y^2 = x^3 - \frac{4}{3}x - t - \frac{11}{27}. \tag{B.2}$$

Recall that Tate's conjecture is known for rational surfaces: an elliptic curve $y^2 = x^3 + A(T)x + B(T)$ is rational if $0 < \max(3\deg A, 2\deg B) < 12$ is true. In this family, $0 < \max(3\deg A = 0, 2\deg B = 2) = 2 < 12$, so the family is a rational surface. □

B.1.2 $y^2 = x^3 - tx^2 + (x-1)t^2$

Lemma B.2. *One-parameter family $y^2 = x^3 - tx^2 + (x-1)t^2$ is a rational surface.*

Proof. We first convert the family to its Weierstrass form and we have

$$\begin{aligned} a'2 &= -t, \\ a'4 &= t^2, \\ a'6 &= -t^2, \\ a''4 &= t^2 - \frac{1}{3}(-t)^2 = \frac{2}{3}t^2, \\ a''6 &= -t^2 + \frac{2}{27}(-t)^3 - \frac{1}{3} \cdot (-t) \cdot (t^2) = -t^2 + \frac{7}{27}t^3. \end{aligned} \tag{B.3}$$

Hence, we get

$$y^2 = x^3 + \frac{2}{3}t^2x - t^2 + \frac{7}{27}t^3. \tag{B.4}$$

Recall that Tate's conjecture is known for rational surfaces: an elliptic curve $y^2 = x^3 + A(T)x + B(T)$ is rational if $0 < \max(3\deg A, 2\deg B) < 12$ is true. In this family, $0 < \max(3\deg A = 6, 2\deg B = 6) = 6 < 12$, so this family is a rational surface. □

B.2 Rank 1 One-Parameter Families

B.2.1 $y^2 = x^3 + tx^2 + t^2$

Lemma B.3. *One-parameter family $y^2 = x^3 + tx^2 + t^2$ is a rational surface.*

Proof. We first convert the family to its Weierstrass form and we have

$$\begin{aligned} a'2 &= t, \\ a'4 &= 0, \\ a'6 &= t^2, \\ a''4 &= 0 - \frac{1}{3}t^2 = -\frac{1}{3}t^2, \\ a''6 &= t^2 + \frac{2}{27}t^3 - \frac{1}{3} \cdot 0 \cdot t = t^2 + \frac{2}{27}t^3. \end{aligned} \tag{B.5}$$

Hence, we get

$$y^2 = x^3 - \frac{1}{3}t^2 x + t^2 + \frac{2}{27}t^3. \tag{B.6}$$

Recall that Tate's conjecture is known for rational surfaces: an elliptic curve $y^2 = x^3 + A(T)x + B(T)$ is rational if $0 < \max(3\deg A, 2\deg B) < 12$ is true. In this family, $0 < \max(3\deg A = 6, 2\deg B = 6) = 6 < 12$, so this family is a rational surface. □

B.2.2 $y^2 = x^3 + tx^2 + x + 1$

Lemma B.4. *One-parameter family $y^2 = x^3 + tx^2 + x + 1$ is a rational surface.*

Proof. We first convert the family to its Weierstrass form and we have

$$\begin{aligned} a'2 &= t \\ a'4 &= 1 \\ a'6 &= 1 \\ a''4 &= 1 - \frac{1}{3}t^2 \\ a''6 &= 1 + \frac{2}{27}t^3 - \frac{1}{3} \cdot 1 \cdot t = 1 + \frac{2}{27}t^3 - \frac{1}{3}t. \end{aligned} \tag{B.7}$$

Hence, we get

$$y^2 = x^3 + (1 - \frac{1}{3}t^2)x + 1 + \frac{2}{27}t^3 - \frac{1}{3}t. \tag{B.8}$$

In this family, $0 < \max(3\deg A = 6, 2\deg B = 6) = 6 < 12$, so this family is a rational surface. □

B.2.3 $y^2 = x^3 + tx^2 + tx + t^2$

Lemma B.5. *One-parameter family $y^2 = x^3+tx^2+tx+t^2$ is a rational surface.*

Proof. We first convert the family to its Weierstrass form using and we have:

$$\begin{aligned} a'2 &= t \\ a'4 &= t \\ a'6 &= t^2 \\ a''4 &= t - \frac{1}{3}t^2 = \frac{2}{3}t^2 \\ a''6 &= t^4 + \frac{2}{27}t^3 - \frac{1}{3}\cdot t \cdot t = t^4 + \frac{2}{27}t^3 - \frac{1}{3}t^2. \end{aligned} \tag{B.9}$$

Hence, we get

$$y^2 = x^3 + \frac{2}{3}t^2x + t^4 + \frac{2}{27}t^3 - \frac{1}{3}t^2. \tag{B.10}$$

In this family, $0 < \max(3\deg A = 6, 2\deg B = 8) = 8 < 12$, so this family is a rational surface.

$\square$

B.3 Rank 2 One-Parameter Families

B.3.1 $y^2 = x^3 - x^2 + (x^2 - x)t + 1$

Lemma B.6. *One-parameter family $y^2 = x^3 - x^2 + (x^2 - x)t + 1$ is a rational surface.*

Proof. We first convert the family to its Weierstrass form and we have:

$$\begin{aligned} a'2 &= t - 1 \\ a'4 &= -t \\ a'6 &= 1 \\ a''4 &= -t - \frac{1}{3}(-1)^2 = -t - \frac{1}{3} \\ a''6 &= 1 + \frac{2}{27}(t-1)^3 - \frac{1}{3}\cdot(t-1)\cdot(-t) = 1 + \frac{2}{27}(t-1)^3 + \frac{1}{3}(t^2 - t). \end{aligned} \tag{B.11}$$

Hence, we get

$$y^2 = x^3 - (-t - \frac{1}{3})x + t^2 + 1 + \frac{2}{27}(t-1)^3 + \frac{1}{3}(t^2 - t). \tag{B.12}$$

In this family, $0 < \max(3\deg A = 3, 2\deg B = 6) = 6 < 12$, so the family is a rational surface. $\square$

B.3.2 $y^2 = x^3 - x + t^4$

Lemma B.7. *One-parameter family $y^2 = x^3 - x + t^4$ is a rational surface.*

Proof. This family is already in its Weierstrass form. In this family, $0 < \max(3\deg A = 0, 2\deg B = 8) = 8 < 12$, so this family is a rational surface. $\square$

C Data Table For Rank 2 One-Parameter Families

C.1 Second Moment of $x^3 - x^2 + (x^2 - x)t + 1$

p	$pA_{2,\mathcal{F}(p)}$	Form	p	$pA_{2,\mathcal{F}(p)}$	Form	p	$pA_{2,\mathcal{F}(p)}$	Form	p	$pA_{2,\mathcal{F}(p)}$	Form
3	14	p^2+2p-1	113	11864	p^2-8p-1	271	70730	$p^2-10p-1$	443	194476	p^2-4p-1
5	34	p^2+2p-1	127	16636	p^2+4p-1	277	80052	$p^2+12p-1$	449	205192	p^2+8p-1
7	62	p^2+2p-1	131	21090	$p^2+30p-1$	281	78960	p^2-1	457	216160	$p^2+16p-1$
11	120	p^2-1	137	18768	p^2-1	283	79522	p^2-2p-1	461	211598	p^2-2p-1
13	246	p^2+6p-1	139	19598	p^2+2p-1	293	95810	$p^2+34p-1$	463	219924	$p^2+12p-1$
17	322	p^2+2p-1	149	20412	$p^2-12p-1$	307	96090	p^2+6p-1	467	209682	$p^2-18p-1$
19	322	p^2-2p-1	151	24612	$p^2+12p-1$	311	84902	$p^2-38p-1$	479	232314	p^2+6p-1
23	436	p^2-4p-1	157	24334	p^2-2p-1	313	102350	$p^2+14p-1$	487	231324	$p^2-12p-1$
29	840	p^2-1	163	29176	$p^2+16p-1$	317	96684	$p^2-12p-1$	491	243044	p^2+4p-1
31	898	p^2-2p-1	167	28222	p^2+2p-1	331	106912	p^2-8p-1	499	227044	$p^2-44p-1$
37	1368	p^2-1	173	29582	p^2-2p-1	337	102784	$p^2-32p-1$	503	254014	p^2+2p-1
41	1598	p^2-2p-1	179	31324	p^2-4p-1	347	125960	$p^2+16p-1$	509	262134	p^2+6p-1
43	1848	p^2-1	181	33846	p^2+6p-1	349	129478	$p^2+22p-1$	521	266230	$p^2-10p-1$
47	2114	p^2-2p-1	191	32660	$p^2-20p-1$	353	116842	$p^2-22p-1$	523	280850	$p^2+14p-1$
53	2596	p^2-4p-1	193	35704	p^2-8p-1	359	113084	$p^2-44p-1$	541	312156	$p^2+36p-1$
59	2890	$p^2-10p-1$	197	36444	$p^2-12p-1$	367	125146	$p^2-26p-1$	547	303584	p^2+8p-1
61	3354	p^2-6p-1	199	38406	p^2-6p-1	373	134652	$p^2-12p-1$			
67	5292	$p^2+12p-1$	211	47052	$p^2+12p-1$	379	149704	$p^2+16p-1$			
71	5324	p^2+4p-1	223	54634	$p^2+22p-1$	383	148906	p^2+6p-1			
73	5766	p^2+6p-1	227	56522	$p^2+22p-1$	389	138872	$p^2-32p-1$			
79	6556	p^2+4p-1	229	50150	$p^2-10p-1$	397	159990	p^2+6p-1			
83	6058	$p^2-10p-1$	233	58016	$p^2+16p-1$	401	160800	p^2-1			
89	9166	$p^2+14p-1$	239	59988	$p^2+12p-1$	409	163190	$p^2-10p-1$			
97	8826	p^2-6p-1	241	54706	$p^2-14p-1$	419	169694	$p^2-14p-1$			
101	10402	p^2+2p-1	251	65510	$p^2+10p-1$	421	189028	$p^2+28p-1$			
103	10814	p^2+2p-1	257	70674	$p^2+18p-1$	431	180588	$p^2-12p-1$			
107	9308	$p^2-20p-1$	263	63908	$p^2-20p-1$	433	184890	p^2-6p-1			
109	12752	p^2+8p-1	269	67518	$p^2-18p-1$	439	193598	p^2+2p-1			

C.2 First Moment of $x^3 - x + t^4$

p	$pA_{1,\mathcal{F}(p)}$	Form	p	$pA_{1,\mathcal{F}(p)}$	Form	p	$pA_{1,\mathcal{F}(p)}$	Form	p	$pA_{1,\mathcal{F}(p)}$	Form
3	-6	$-2p$	113	-678	$-6p$	271	-542	$-2p$	443	-886	$-2p$
5	-10	$-2p$	127	-254	$-2p$	277	-554	$-2p$	449	898	$2p$
7	-14	$-2p$	131	-262	$-2p$	281	562	$2p$	457	-2742	$-6p$
11	-22	$-2p$	137	-822	$-6p$	283	-566	$-2p$	461	-922	$-2p$
13	-26	$-2p$	139	-278	$-2p$	293	-586	$-2p$	463	-926	$-2p$
17	34	$2p$	149	-298	$-2p$	307	-614	$-2p$	467	-934	$-2p$
19	-38	$-2p$	151	-302	$-2p$	311	-622	$-2p$	479	-958	$-2p$
23	-46	$-2p$	157	-314	$-2p$	313	-1878	$-6p$	487	-974	$-2p$
29	-58	$-2p$	163	-326	$-2p$	317	-634	$-2p$	491	-982	$-2p$
31	-62	$-2p$	167	-334	$-2p$	331	-662	$-2p$	499	-998	$-2p$
37	-74	$-2p$	173	-346	$-2p$	337	-2022	$-6p$	503	-1006	$-2p$
41	-246	$-6p$	179	-358	$-2p$	347	-694	$-2p$	509	-1018	$-2p$
43	-86	$-2p$	181	-362	$-2p$	349	-698	$-2p$	521	-3126	$-6p$
47	-94	$-2p$	191	-382	$-2p$	353	-2118	$-6p$	523	-1046	$-2p$
53	-106	$-2p$	193	386	$2p$	359	-718	$-2p$	541	-1082	$-2p$
59	-118	$-2p$	197	-394	$-2p$	367	-734	$-2p$	547	-1094	$-2p$
61	-122	$-2p$	199	-398	$-2p$	373	-746	$-2p$			
67	-134	$-2p$	211	-422	$-2p$	379	-758	$-2p$			
71	-142	$-2p$	223	-446	$-2p$	383	-766	$-2p$			
73	146	$2p$	227	-454	$-2p$	389	-778	$-2p$			
79	-158	$-2p$	229	-458	$-2p$	397	-794	$-2p$			
83	-166	$-2p$	233	466	$2p$	401	802	$2p$			
89	178	$2p$	239	-478	$-2p$	409	-2454	$-6p$			
97	194	$2p$	241	482	$2p$	419	-838	$-2p$			
101	-202	$-2p$	251	-502	$-2p$	421	-842	$-2p$			
103	-206	$-2p$	257	-1542	$-6p$	431	-862	$-2p$			
107	-214	$-2p$	263	-526	$-2p$	433	866	$2p$			
109	-218	$-2p$	269	-538	$-2p$	439	-878	$-2p$			

C.3 Second Moment of $x^3 - x + t^4$

p	$pA_{2,\mathcal{F}(p)}$	Form	p	$pA_{2,\mathcal{F}(p)}$	Form	p	$pA_{2,\mathcal{F}(p)}$	Form	p	$pA_{2,\mathcal{F}(p)}$	Form
3	18	p^2+3p	113	12092	$p^2-5p-112$	271	73170	p^2-p	443	195806	p^2-p
5	20	p^2-p	127	16002	p^2-p	277	76452	p^2-p	449	250068	$p^2+108p-25$
7	42	p^2-p	131	17030	p^2-p	281	76828	$p^2-7p-166$	457	202932	$p^2-13p+24$
11	110	p^2-p	137	17924	$p^2-6p-23$	283	79806	p^2-p	461	200996	p^2-25p
13	156	p^2-p	139	19182	p^2-p	293	83212	p^2-9p	463	213906	p^2-p
17	132	p^2-9p-4	149	22052	p^2-p	307	93492	p^2-p	467	217622	p^2-p
19	342	p^2-p	151	22650	p^2-p	311	96410	p^2-p	479	228962	p^2-p
23	506	p^2-p	157	24492	p^2-p	313	111460	$p^2+43p+32$	487	236682	p^2-p
29	812	p^2-p	163	26406	p^2-p	317	90028	p^2-33p	491	240590	p^2-p
31	930	p^2-p	167	27722	p^2-p	331	109230	p^2-p	499	248502	p^2-p
37	740	p^2-17p	173	33907	p^2+23p	337	118380	$p^2+14p+93$	503	252506	p^2-p
41	2596	$p^2+22p+13$	179	31862	p^2-p	347	120062	p^2-p	509	283004	p^2+47p
43	1806	p^2-p	181	32580	p^2-p	349	143788	p^2+63p	521	288212	$p^2+32p+99$
47	2162	p^2-p	191	36290	p^2-p	353	122764	$p^2-5p-80$	523	273006	p^2-p
53	3180	p^2+7p	193	35716	$p^2-7p-182$	359	128522	p^2-p	541	292140	p^2-p
59	3422	p^2-p	197	37036	p^2-9p	367	134322	p^2-p	547	298662	p^2-p
61	3660	p^2-p	199	39402	p^2-p	373	120852	p^2-49p			
67	4422	p^2-p	211	44310	p^2-9p	379	143262	p^2-p			
71	4970	p^2-p	223	49506	p^2-p	383	146306	p^2-p			
73	3612	$p^2-23p-38$	227	51302	p^2-p	389	157156	p^2+15p			
79	6162	p^2-p	229	52212	p^2-p	397	169916	p^2+31p			
83	6806	p^2-p	233	49516	$p^2-20p-113$	401	173732	$p^2+32p+99$			
89	7548	$p^2-4p-17$	239	56882	p^2-p	409	163908	$p^2-8p-101$			
97	7332	$p^2-21p-40$	241	49044	$p^2-37p-120$	419	175142	p^2-p			
101	7676	p^2-25p	251	62750	p^2-p	421	176820	p^2-p			
103	10506	p^2-p	257	59212	$p^2-26p-155$	431	185330	p^2-p			
107	11342	p^2-p	263	68906	p^2-p	433	223268	$p^2+82p-273$			
109	11772	p^2-p	269	80700	p^2+31p	439	192282	p^2-p			

D Mathematica Code For Computing the First and Second Moment

D.1 First Moment Computation

```
p = 13; Sum[Sum[JacobiSymbol[(x^3-x+t^4), p],{x, 0, p-1}],{t,0,p-1}]
```

D.2 Second Moment Computation

```
h[u_, v_] := v^3 - v^2 + (v^2 - v) u + 1;
f[p_] := Sum[
   Sum[Sum[JacobiSymbol[h[t, x] h[t, y], p], {x, 0, p - 1}], {y, 0,
     p - 1}], {t, 0, p - 1}];
g[p_] := 1.0 (f[p] - p^2)/p;
secondmomentrange[nstart_, nend_] :=
  Module[{}, For[n = nstart, n <= nend, n++, {prime = Prime[n];
      Print["We are looking at the prime ", prime];
      Print["The second moment term Sum_{t,x,y mod p} a_t(p)^2 is ",
       f[prime]];
      Print["The second moment minus p^2 then divided by p is ",
       g[prime]];
      Print[" "]'}];];
```

D.3 Statistics Display

```
data = {}
Mean[data] 1.0
StandardDeviation[data] 1.0
Histogram[data, Automatic, "Probability"]
```

E References

References

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

[BAU] L. Bauer, *Weierstrass equations: Seminar on elliptic curves and the Weil conjectures*, to appear in the 4th talk in the seminar on elliptic curves and the Weil conjectures supervised by Prof. Dr. Moritz Kerz in the summer term at the University of Regensburg (2016), http://www.mathematik.uni-regensburg.de/kerz/ss16/ausarb/bauer.pdf.

[BEW] B. Berndt, R. Evans, and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, Vol. 21, 1998.

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

[Clo] L. Clozel, *The Sato-Tate Conjecture*, IP Current Developments in Mathematics, 2006.

[Da] H. Davenport, *Multiplicative Number Theory, 2nd edition*, Graduate Texts in Mathematics **74**, Springer-Verlag, New York, 1980, revised by H. Montgomery.

[Du] A. Dujella, *History of elliptic curves rank records*, https://web.math.pmf.unizg.hr/~duje/tors/rankhist.html.

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

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

[MMRW] B. Mackall, S. J. Miller, C. Rapti and K. Winsor, *Lower-Order Biases in Elliptic Curve Fourier 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 fur 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.

[Mi4] S. J. Miller and R. Takloo-Bighash, *An Invitation to Modern Number Theory*, Princeton University Press (2006).

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

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

[Rub] K. Rubin, *Right triangles and elliptic curves*, to appear in Ross Reunion in July 2007. https://www.math.uci.edu/~krubin/lectures/rossweb.pdf.

[Si0] J. Silverman, *An Introduction to the Theory of Elliptic Curves*, to appear in the Summer School on *Computational Number Theory and Applications to Cryptography* at University of Wyoming in July 2006. https://www.math.brown.edu/~jhs/Presentations/WyomingEllipticCurve.pdf.

[Si1] J. Silverman, *Heights and the specialization map for families of abelian varieties*, J. Reine Angew. Math. **342** (1983), 197–211.

[Si2] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, Berlin-New York (1986).

[ST] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, New York, 1992.

[Su] A. Sutherland, *Point Counting*, https://ocw.mit.edu/courses/mathematics/18-783-elliptic-curves-spring-2015/lecture-notes/MIT18_783S15_lec8.pdf.

[WAZ] R. Wazir, *Arithmetic on elliptic threefolds*, Composito Mathematica **140** (2004), 567-580.