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

Michelle (Jiefei) Wu
Westminster School

September 8, 2019

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 $A_{k,\mathcal{E}(p)} := \sum_{t \mod p} a_{\mathcal{E}_t}(p)^k$ 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, and is related to one of the million-dollar Clay Millenium prizes - the Birch and Swinnerton-Dyer Conjecture - which states that eventually all curves E_t have rank at least r. 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 $A_{2,\mathcal{E}(p)} = p^2+O(p^{3/2})$, 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 0 is on average negative. This was verified for many families by Mackall, Miller, Rapti, and Winsor, and explains some of the disagreement between theory and computations 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). 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.

Keywords: Elliptic Curves, Legendre Symbol, Biases, Ranks.

Contents

1 Introduction

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 some basic geometry. The Pythagorean theorem states that if a, b, and c are the sides of a right triangle, then

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

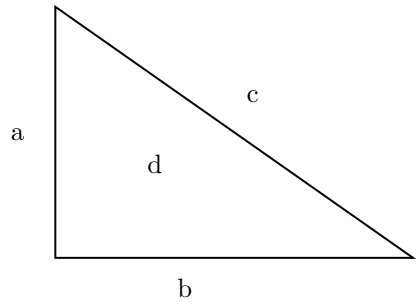

Figure 1: A right triangle with side length a, b and c and area d

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 $a^2+b^2=c^2$, which has three variables, we are going to study how to generate the rational points on a two-variable equation. Let $x=a/c$ and $y=b/c$, and we have a unit circle $x^2+y^2=1$.

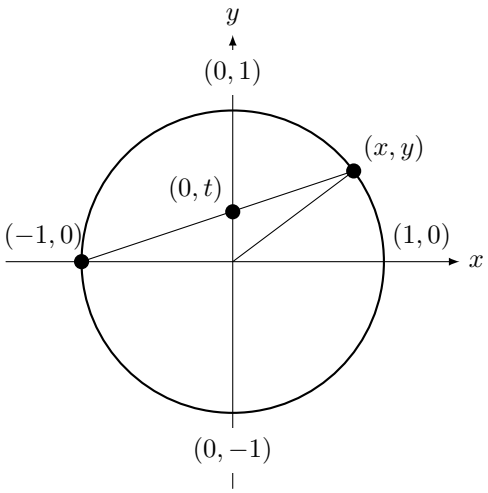

Figure 2: A rational parametrization of the circle $x^2+y^2=1$

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

$$y \quad = \quad t(1+x). \tag{1.3}$$

Hence, the other point of intersection is

$$1-x^2 \quad = \quad y^2=t^2(1+x)^2. \tag{1.4}$$

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

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

Using the above relation, we get

$$x = \frac{1-t^2}{1+t^2} \ , \ y = \frac{2t}{1+t^2}. \tag{1.6}$$

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).

Since we know what happens with exponent $n = 2$, we are now going to consider some higher degree equations.

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

$$y^2 = x^3 + ax + b \tag{1.7}$$

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*

$$A^n + B^n \ = \ C^n \tag{1.8}$$

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.

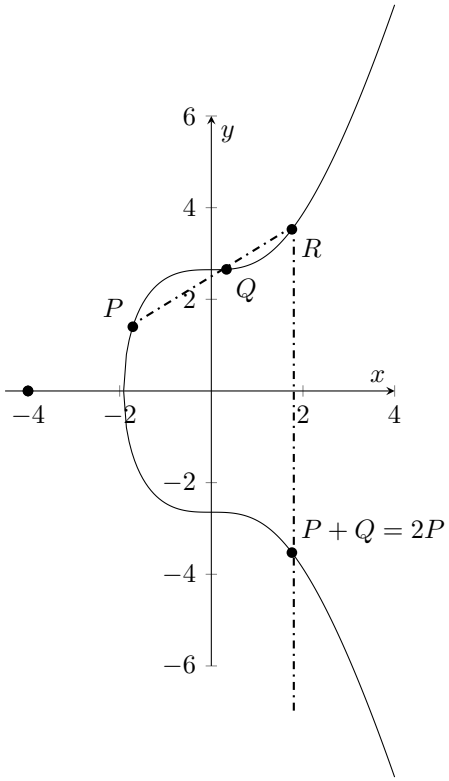

Figure 3: Demonstrating the addition law for the elliptic curve $E(\mathbb{Q})$: $y^2 = x^3 + 7$.

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:*

$$\begin{aligned}&(1) P + (Q + R) = (P + Q) + R, \;\; for\ all\ P, Q, R \in E.\\ &(2) P + Q = 2P, \;\; for\ all\ P, Q \in E.\end{aligned} \tag{1.9}$$

See Figure 3 for an illustration.

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*

$$a_E(p) \;:=\; p - |E(\mathbb{F}_p)|, \tag{1.10}$$

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

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 $a_{\mathcal{E}_t}(p)$:*

$$a_{\mathcal{E}_t}(p) \;:=\; p - |\mathcal{E}_t(\mathbb{F}_p)| \tag{1.11}$$

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

$$a_{\mathcal{E}_t}(p) \;=\; -\sum_{x \bmod p}\left(\frac{x^3+A(t)x+B(t)}{p}\right). \tag{1.12}$$

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*

$$|a_E(p)| \;\le\; 2\sqrt{p}. \tag{1.13}$$

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.

We can use the $a(p)$'s to define an L-function; this is a generalization of the Riemann Zeta Function, and it takes the local information of the number of solutions modulo p and creates a global object, from which we can deduce many properties of the elliptic curve.

Definition 6 (Elliptic Curve L-function)**.** *The Hasse-Weil L-function of E with coefficient $a_E(p)$ (1.12) is defined as*

$$L(E,s) \;=\; \prod_p \frac{1}{1-a_E(p)\cdot p^{-s}+p\cdot p^{-2s}}. \tag{1.14}$$

Though initially defined only when the real part of s is sufficiently large, it can be completed, through the introduction of several factors, to an entire function on the complex plane. With this normalization the completed L-function will have a functional equation relating values at s with those at $2-s$. The set $0 \le \mathrm{Re}(s)2$ is the critical strip, and $s=1$ is the central point.

This L-function leads us to the famous Birch and Swinnerton-Dyer conjecture, which we will talk about after we define rank.

Definition 7 (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:*

$$E(\mathbb{Q}) \;\cong\; \mathbb{Z}^r \times E(\mathbb{Q})_{\mathrm{tors}}. \tag{1.15}$$

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.

Conjecture 1.6 (Birch and Swinnerton-Dyer)**.** *Let E be a rational elliptic curve, and let $L(E,s)$ be its L-function. The order of vanishing of $L(E,s)$ at $s=1$ is equal to the rank of the group of rational points $E(\mathbb{Q})$:*

$$\operatorname*{ord}_{s=1} L(E,s) \;=\; \text{rank}E(\mathbb{Q}). \tag{1.16}$$

In other words, the Birch and Swinnerton-Dyer conjecture is that the notions of geometric and analytic rank are the same. Assuming the conjecture, we can estimate the distribution of zeros near the families of L-functions.

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

Definition 8 (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:*

$$A_{\mathcal{E},r(p)} \;=\; \frac{1}{p}\sum_{t \bmod p} a_{\mathcal{E}_t}(p)^r. \tag{1.17}$$

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

Definition 9 (Big-Oh notation)**.** *What it means by $f(x)=O(g(x))$ is that for all x sufficiently large there is some C such that the absolute value of $f(x)$ is less than or equal to $Cg(x)$: $|f(x)|\le Cg(x)$.*

1.2 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 show 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 1.7. *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*

$$A_{2,\mathcal{E}}(p) \;=\; p^2+O(p^{3/2}), \tag{1.18}$$

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

Theorem 1.8 (Birch theorem)**.** *For the family $\mathcal{F} : y^2 = x^3 + ax + b$ of all elliptic curves, the second moment of the Fourier coefficient equals to:*

$$A_{2,\mathcal{F}}(p) \;=\; \sum_{a,b \bmod p} a_{\mathcal{F}_{a,b}}(p) = p^3 - p^2. \tag{1.19}$$

We now state our main object of study; see [Bi, Mi1, Mi3, Mic].

Conjecture 1.9 (Bias Conjecture)**.** *B. Mackall, S. J. Miller, C. Rapti and K. Winsor conjecture that the largest lower term in the second moment expansion of a one-parameter family which does not average to 0 is on average negative.*

Unfortunately it is very hard to compute in closed form 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:

One-Parameter Family	Rank	$A_{1,\mathcal{F}(p)}$	$A_{2,\mathcal{F}(p)}$
$y^2 = x^3 - x^2 - x + t$	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	$p^2 - 2p - [\sum_{x(p)} \left(\frac{x^3+x^2}{p}\right)]^2 - \left(\frac{-3}{p}\right)p$
$y^2 = x^3 + tx^2 + x + 1$	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	$p^2 - 2p - 1$
$y^2 = x^3 - x^2 + (x^2 - x)t + 1$	2	-2p	$p^2 - 1$ (conjecture from observation)
$y^2 = x^3 - x + t^4$	2(conjecture)	-2p (conjecture)	$p^2 - p$ (conjecture from observation)

Two-Parameter Family	$A_{1,\mathcal{F}(p)}$	$A_{2,\mathcal{F}(p)}$
$y^2 = x^3 + tx + sx^2$	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	$p^3 - 2p^2 + p$
$y^2 = x^3 + t(x^2 - x) + s^2x^2$	-p	$p^3 - 2p^2 + 2p$
$y^2 = x^3 + ts^2x^2 + (t^3 - t^2)x$	-p	$p^3 - 3p^2 + p + 1$
$y^2 = x^3 + t^2x^2 + (t^3 - t^2)sx$	-p	$p^3 - 4p^2 + 5p$
$y^2 = x^3 + t^2x^2 - (s^2 - s)t^2x$	-2p	$p^3 - 3p^2 + 3p - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right)$
$y^2 = x^3 - t^2x + t^3s^2 + t^4$	-2p	$p^3 - 2p^2 + p - \left\lvert\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right\rvert p^2$

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 as well as Gauss Sum Expansion, which can be used to compute biases in elliptic curves. See more details from [RoSi, BEW, BAU].

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* $\mathbb{Q}(T)$*:*

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

Conjecture 2.2 (Tate's Conjecture for Elliptic Surfaces[MMRW])**.** *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 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 (Linear Legendre Sum)**.** *We have*

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

See Appendix A for a complete proof.

Lemma 2.5 (Quadratic Legendre Sum)**.** *Let a, b, c be positive integers. Assume $p > 2$ and $a \not\equiv 0 \mod p$, we have*

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

See Appendix A for a complete proof.

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.*

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

$$\left(\frac{x}{p}\right) \quad = \quad {G_p}^{-1} \sum_{c=1}^{p} \left(\frac{c}{p}\right) \boldsymbol{e}\left(\frac{cx}{p}\right) \tag{2.9}$$

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

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

Sadly, there are no nice closed form expressions for cuic and higher sums. This 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 prove in Appendix B that every rank 1 and 2 one-parameter families we compute are rational surfaces, so their first moment is equivalent to their rank. We do not check the families that have 0 as their first moment because by definition they are rational surfaces and their rank is 0.

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 $p > 3$,

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

According to linear Legendre sum (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 $y^2 = x^3 - x^2 - x + t$ is $p^2 - 2p - \left(\frac{-3}{p}\right)p$, which supports our bias conjecture.*

Proof.

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

Now, we compute the discriminant of the equation in t, denoted as δ, which we will 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 2.5), $\delta_2(x, y) = x^2 + xy - x + y^2 - y - 1 = y^2 + (x - 1)y + (x^2 - x - 1) \equiv 0$ 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 Lemma 2.5 again. The discriminant now equals to $4 - 4(-3)5$. 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

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

□

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.

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

□

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

Proof.

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

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

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

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 2.5, 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:

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

We use Lemma 2.5 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 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

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

□

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 $-p$, and the family's rank is 1.*

Proof.

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

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 $x^3+x^2=0 \mod p$. Hence, the total contribution is $2p-p=p$. □

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

Proof.

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

Its discriminant is:

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

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 both 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

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

Therefore

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

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 2.5, $\delta_2(x,y) = x^2+xy+x+y^2+y \equiv 0$ 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 solving $\delta_2(x,y)\equiv 0 \mod p$, 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: v Then, we use Lemma 2.5 again. The discriminant now equals to $4-4(-3)1$. 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 with $x^2+xy+x+y^2+y\equiv 0$ is $p-2-\left(\frac{-3}{p}\right)$; the number with $x-y\equiv 0$ is at most $p-2$. At most two pairs of (x,y) satisfy both $x^2+xy+x+y^2+y\equiv 0$ and $x=y$. These pairs satisfy $3x^2\equiv -2x$, and we do not have overcounting. Thus, the total number of pairs is

$$2p-2-\left(\frac{-3}{p}\right). \quad (3.23)$$

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

$$\left(\frac{(x^3+x^2)(y^3+y^2)}{p}\right) = \left(\frac{x(x^2+x)y(y^2+y)}{p}\right) = \left(\frac{x^2y^2(x+y+1)}{p}\right). \quad (3.24)$$

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

are there. Therefore

$$\begin{aligned} A_{2,\mathcal{F}(p)} &= p[2p-2-\left(\frac{-3}{p}\right)] - \sum_{x,y\neq 0,-1}\left(\frac{(x^3+x^2)(y^3+y^2)}{p}\right) - p^2 \\ &= p^2 - 2p - \left[\sum_{x(p)}\left(\frac{x^3+x^2}{p}\right)\right]^2 - \left(\frac{-3}{p}\right)p. \end{aligned} \tag{3.25}$$

□

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 $-p$, and the family's rank is 1.*

Proof.

$$\begin{aligned} -A_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} = \sum_{t(p)}\sum_{x(p)}\left(\frac{x^3+x^2(t+1)+x+1}{p}\right) \\ &= \sum_{x=1}^{p-1}\sum_{t(p)}\left(\frac{x^3+tx^2+x+1}{p}\right) + \sum_{t(p)}\left(\frac{1}{p}\right) \\ &= 0+p \\ &= p \end{aligned} \tag{3.26}$$

□

Lemma 3.8. *The second moment of the one-parameter family $y^2 = x^3+tx^2+x+1$ 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 2.6):

$$\begin{aligned} A_{2,\mathcal{F}(p)} &= \sum_{t(p)} {a_t}^2(p) \\ &= \sum_{t(p)}\sum_{x(p)}\sum_{y(p)}\left(\frac{x^3+x+1+x^2t}{p}\right)\left(\frac{y^3+y+1+y^2t}{p}\right) \\ &= \sum_{x,y(p)}\sum_{c,d=1}^{p-1}\frac{1}{p}\left(\frac{cd}{p}\right)\mathbf{e}\left(\frac{c(x^3+x+1)-d(y^3+y+1)}{p}\right)\sum_{t(p)}\mathbf{e}\left(\frac{(cx^2-dy^2)t}{p}\right). \end{aligned} \tag{3.27}$$

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:

$$\begin{aligned} A_{2,\mathcal{F}(p)} &= \sum_{x,y=1}^{p-1}\sum_{c=1}^{p-1}\frac{1}{p}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x^3y^2+xy^2+y^2-x^2y^3-x^2y-x^2)}{p}\right)p+p \\ &= \sum_{x,y=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-xy-x-y)}{p}\right)+p \\ &= \sum_{x,y=1}^{p-1}\sum_{c=0}^{p-1}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-xy-x-y)}{p}\right)+p-\sum_{x,y=1}^{p-1}\left(\frac{x^2y^2}{p}\right) \\ &= \sum_{x,y=1}^{p-1}\sum_{c=0}^{p-1}\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-xy-x-y)}{p}\right)+p-(p-1)^2. \end{aligned} \tag{3.28}$$

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

$$\begin{aligned} y &= \frac{(x+1) \pm \sqrt{(x+1)^2+4x^3}}{2x^2} \\ &= \frac{(x+1) \pm \sqrt{4x^3+x^2+2x+1}}{2x^2}. \end{aligned} \tag{3.29}$$

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

$$\sum_{x\neq 0}\left(1+\left(\frac{4x^3+x^2+2x+1}{p}\right)\right) = p-1+\sum_{x=0}^{p}\left(\frac{4x^3+x^2+2x+1}{p}\right)-1. \tag{3.30}$$

Each of these pairs contributes p, so the total contribution is $p^2+p\sum_x\left(\frac{4x^3+x^2+2x+1}{p}\right)-2p$.

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

$$\begin{aligned} A_{2,\mathcal{F}(p)} &= p^2 + p(\sum_{x(p)} \left(\frac{4x^3 + x^2 + 2x + 1}{p}\right)) - 2p - p + p(p-1) + p - (p-1)^2 \\ &= p^2 - p - 1 + p\sum_{x(p)} \left(\frac{4x^3 + x^2 + 2x + 1}{p}\right). \end{aligned} \tag{3.31}$$

□

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 $-p$, and the family's rank is 1.*

Proof.

$$\begin{aligned} -A_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} = \sum_{t(p)}\sum_{x(p)} \left(\frac{x^3 + tx^2 + tx + t^2}{p}\right) \\ &= \sum_{t=1}^{p-1}\sum_{x(p)} \left(\frac{x^3 + tx^2 + tx + t^2}{p}\right) \\ &= \sum_{t=1}^{p-1}\sum_{x(p)} \left(\frac{t^3x^3 + t^3x^2 + t^2x + t^2}{p}\right) \\ &= \sum_{t=1}^{p-1}\sum_{x(p)} \left(\frac{t^2}{p}\right)\left(\frac{tx^3 + tx^2 + x + 1}{p}\right) \\ &= \sum_{t=0}^{p-1}\sum_{x(p)} \left(\frac{t(x^3 + x^2) + x + 1}{p}\right) - \sum_{x(p)} \left(\frac{x+1}{p}\right) \\ &= \sum_{t(p)}\sum_{x=0,-1} \left(\frac{t(x^3 + x^2) + x + 1}{p}\right) + \sum_{t(p)}\sum_{x(p)x\neq 0,-1} \left(\frac{t(x^3 + x^2) + x + 1}{p}\right) - 0 \\ &= \sum_{t(p)}\sum_{x=-1} \left(\frac{0}{p}\right) + \sum_{t(p)}\sum_{x=0} \left(\frac{1}{p}\right) + \sum_{x(p)x\neq 0,-1}\sum_{t(p)} \left(\frac{t+x+1}{p}\right) \\ &= 0 + p + 0 = p \end{aligned} \tag{3.32}$$

□

Lemma 3.10. *The second moment of the one-parameter family $y^2 = x^3+tx^2+tx+t^2$ is p^2-2p-1, which supports our bias conjecture.*

Proof.

$$\begin{aligned}
A_{2,\mathcal{F}(p)} &= \sum_{t(p)} {a_t}^2(p) \\
&= \sum_{t(p)}\sum_{x(p)}\sum_{y(p)} \left(\frac{tx^2+tx+t^2+x^3}{p}\right)\left(\frac{ty^2+ty+t^2+y^3}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{x,y(p)} \left(\frac{t^3x^2+t^2x+t^2+t^3x^3}{p}\right)\left(\frac{t^3y^2+t^2y+t^2+t^3y^3}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{x,y(p)} \left(\frac{t^4}{p}\right)\left(\frac{t(x^3+x^2)+x+1}{p}\right)\left(\frac{t(y^3+y^2)+y+1}{p}\right) \\
&= \sum_{t=0}^{p-1}\sum_{x,y(p)} \left(\frac{t(x^3+x^2)+x+1}{p}\right)\left(\frac{t(y^3+y^2)+y+1}{p}\right) - \sum_{x,y(p)}\left(\frac{x+1}{p}\right)\left(\frac{y+1}{p}\right) \\
&= \sum_{t(p)}\sum_{x,y(p)} \left(\frac{t(x^3+x^2)+x+1}{p}\right)\left(\frac{t(y^3+y^2)+y+1}{p}\right) - 0 \\
&= \sum_{t(p)}\sum_{x,y(p)} \left(\frac{t(x^3+x^2)+x+1}{p}\right)\left(\frac{t(y^3+y^2)+y+1}{p}\right)
\end{aligned} \tag{3.33}$$

We have

$$\begin{aligned}
a &= (x^3+x^2)(y^3+y^2) \\
b &= (x^3+x^2)(y+1)+(y^3+y^2)(x+1) \\
c &= (x+1)(y+1) \\
\delta &= [(x^3+x^2)(y+1)-(y^3+y^2)(x+1)]^2.
\end{aligned} \tag{3.34}$$

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

$$\delta(x,y) = (x-y)(x+y)(x+1)(y+1). \tag{3.35}$$

Therefore

$$\begin{aligned}
A_{2,\mathcal{F}(p)} = &\sum_{x,y\neq 0,-1;\delta(x,y)\equiv 0} p\left(\frac{(x^3+x^2)(y+1)-(y^3+y^2)(x+1)}{p}\right) \\
&- \sum_{x,y\neq 0,-1}\left(\frac{(x^3+x^2)(y+1)-(y^3+y^2)(x+1)}{p}\right)+5p.
\end{aligned} \tag{3.36}$$

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 1.5), $\delta_2(x,y) = x^2y + x^2 + xy^2 + 2xy + x + y^2 + y \equiv 0(p)$ when

$$\begin{aligned} y &= \frac{-(x^2+2x+1) \pm \sqrt{x^4 - 2x + 1}}{2(x+1)} \\ &= \frac{-(x^2+2x+1) \pm \sqrt{(x+1)^2(x-1)^2}}{2(x+1)}. \end{aligned} \tag{3.37}$$

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

$$\begin{aligned} A_{2,\mathcal{F}(p)} &= p(p-2) - 1 \\ &= p^2 - 2p - 1. \end{aligned} \tag{3.38}$$

□

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 $-2p$, and the family's rank is 2.*

Proof.

$$\begin{aligned} -A_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} = \sum_{t(p)} \sum_{x(p)} \left(\frac{x^3 - x^2 + (x^2 - x)t + 1}{p} \right) \\ &= \sum_{x=0}^{p-1} \sum_{t=0}^{p-1} \left(\frac{(x^2 - x)t + (x^3 - x^2 + 1)}{p} \right) \\ &= \sum_{x \neq 0,1} \sum_{t=0}^{p-1} \left(\frac{t + (x^3 - x^2 + 1)}{p} \right) - \sum_{t=0}^{p-1} \left[\left(\frac{1}{p} \right) + \left(\frac{1}{p} \right) \right] \\ &= 0 - 2p \\ &= -2p \end{aligned} \tag{3.39}$$

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 $y^2=x^3-x^2+(x^2-x)t+1$ is p^2-1, which supports our bias conjecture.*

Proof. We are not able to compute the second moment of this family, so we observe numerically and generate a possible equation for primes from 3 to 349:

p	$A_{2,\mathcal{F}(p)}$	Form	p	$A_{2,\mathcal{F}(p)}$	Form	p	$A_{2,\mathcal{F}(p)}$	Form
3	14	p^2+2p-1	113	11864	p^2-8p-1	271	70730	$p^2-10p-1$
5	34	p^2+2p-1	127	16636	p^2+4p-1	277	80052	$p^2+12p-1$
7	62	p^2+2p-1	131	21090	$p^2+30p-1$	281	78960	p^2-1
11	120	p^2-1	137	18768	p^2-1	283	79522	p^2-2p-1
13	246	p^2+6p-1	139	19598	p^2+2p-1	293	95810	$p^2+34p-1$
17	322	p^2+2p-1	149	20412	$p^2-12p-1$	307	96090	p^2+6p-1
19	322	p^2-2p-1	151	24612	$p^2+12p-1$	311	84902	$p^2-38p-1$
23	436	p^2-4p-1	157	24334	p^2-2p-1	313	102350	$p^2+14p-1$
29	840	p^2-1	163	29176	$p^2+16p-1$	317	96684	$p^2-12p-1$
31	898	p^2-2p-1	167	28222	p^2+2p-1	331	106912	p^2-8p-1
37	1368	p^2-1	173	29582	p^2-2p-1	337	102784	$p^2-32p-1$
41	1598	p^2-2p-1	179	31324	p^2-4p-1	347	125960	$p^2+16p-1$
43	1848	p^2-1	181	33846	p^2+6p-1	349	129478	$p^2+22p-1$
47	2114	p^2-2p-1	191	32660	$p^2-20p-1$			
53	2596	p^2-4p-1	193	35704	p^2-8p-1			
59	2890	$p^2-10p-1$	197	36444	$p^2-12p-1$			
61	3354	p^2-6p-1	199	38406	p^2-6p-1			
67	5292	$p^2+12p-1$	211	47052	$p^2+12p-1$			
71	5324	p^2+4p-1	223	54634	$p^2+22p-1$			
73	5766	p^2+6p-1	227	56522	$p^2+22p-1$			
79	6556	p^2+4p-1	229	50150	$p^2-10p-1$			
83	6058	$p^2-10p-1$	233	58016	$p^2+16p-1$			
89	9166	$p^2+14p-1$	239	59988	$p^2+12p-1$			
97	8826	p^2-6p-1	241	54706	$p^2-14p-1$			
101	10402	p^2+2p-1	251	65510	$p^2+10p-1$			
103	10814	p^2+2p-1	257	70674	$p^2+18p-1$			
107	9308	$p^2-20p-1$	263	63908	$p^2-20p-1$			
109	12752	p^2+8p-1	269	67518	$p^2-18p-1$			

We can see that for primes within 349, every form has p^2-c_1p-1. 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 of this one-parameter family is p^2-1, but there might be terms of 1, $p^{1/2}$, p, or $p^{3/2}$. □

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 $-2p$, and the family's rank is 2.*

Proof. We are not able to compute the first moment of this family numerically, so we generate a table of forms for small primes:

p	$A_{2,\mathcal{F}(p)}$	Form	p	$A_{2,\mathcal{F}(p)}$	Form	p	$A_{2,\mathcal{F}(p)}$	Form
3	6	$2p$	113	678	$6p$	271	542	$2p$
5	10	$2p$	127	254	$2p$	277	554	$2p$
7	14	$2p$	131	262	$2p$	281	-562	$-2p$
11	22	$2p$	137	822	$6p$	283	566	$2p$
13	26	$2p$	139	278	$2p$	293	586	$2p$
17	-34	$-2p$	149	298	$2p$	307	614	$2p$
19	38	$2p$	151	302	$2p$	311	622	$2p$
23	46	$2p$	157	314	$2p$	313	1878	$6p$
29	58	$2p$	163	326	$2p$	317	634	$2p$
31	62	$2p$	167	334	$2p$	331	662	$2p$
37	74	$2p$	173	346	$2p$	337	2022	$6p$
41	246	$6p$	179	358	$2p$	347	694	$2p$
43	86	$2p$	181	362	$2p$	349	698	$2p$
47	94	$2p$	191	382	$2p$			
53	106	$2p$	193	-386	$-2p$			
59	118	$2p$	197	394	$2p$			
61	122	$2p$	199	398	$2p$			
67	134	$2p$	211	422	$2p$			
71	142	$2p$	223	446	$2p$			
73	-146	$-2p$	227	454	$2p$			
79	158	$2p$	229	458	$2p$			
83	166	$2p$	233	-466	$-2p$			
89	-178	$-2p$	239	478	$2p$			
97	-194	$-2p$	241	-482	$-2p$			
101	202	$2p$	251	502	$2p$			
103	206	$2p$	257	1542	$6p$			
107	214	$2p$	263	526	$2p$			
109	218	$2p$	269	538	$2p$			

We can see that $2p$ appears frequently in the table above, but there are some $-2p$ and $6p$. We conjecture that they will average to $2p$ eventually and the rank of this family is 2. □

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

Proof. We are not able to compute the second moment of this family numerically, so we generate a table of the forms for small primes:

p	$A_{2,\mathcal{F}(p)}$	Form	p	$A_{2,\mathcal{F}(p)}$	Form	p	$A_{2,\mathcal{F}(p)}$	Form
3	18	p^2+3p	113	12092	$p^2-5p-112$	271	73170	p^2-p
5	20	p^2-p	127	16002	p^2-p	277	76452	p^2-p
7	42	p^2-p	131	17030	p^2-p	281	76828	$p^2-7p-166$
11	110	p^2-p	137	17924	$p^2-6p-23$	283	79806	p^2-p
13	156	p^2-p	139	19182	p^2-p	293	83212	p^2-9p
17	132	p^2-9p-4	149	22052	p^2-p	307	93492	p^2-p
19	342	p^2-p	151	22650	p^2-p	311	96410	p^2-p
23	506	p^2-p	157	24492	p^2-p	313	111460	$p^2+43p+32$
29	812	p^2-p	163	26406	p^2-p	317	90028	p^2-33p
31	930	p^2-p	167	27722	p^2-p	331	109230	p^2-p
37	740	p^2-17p	173	33907	p^2+23p	337	118380	$p^2+14p+93$
41	2596	$p^2+22p+13$	179	31862	p^2-p	347	120062	p^2-p
43	1806	p^2-p	181	32580	p^2-p	349	143788	p^2+63p
47	2162	p^2-p	191	36290	p^2-p			
53	3180	p^2+7p	193	35716	$p^2-7p-182$			
59	3422	p^2-p	197	37036	p^2-9p			
61	3660	p^2-p	199	39402	p^2-p			
67	4422	p^2-p	211	44310	p^2-9p			
71	4970	p^2-p	223	49506	p^2-p			
73	3612	$p^2-23p-38$	227	51302	p^2-p			
79	6162	p^2-p	229	52212	p^2-p			
83	6806	p^2-p	233	49516	$p^2-20p-113$			
89	7548	$p^2-4p-17$	239	56882	p^2-p			
97	7332	$p^2-21p-40$	241	49044	$p^2-37p-120$			
101	7676	p^2-25p	251	62750	p^2-p			
103	10506	p^2-p	257	59212	$p^2-26p-155$			
107	11342	p^2-p	263	68906	p^2-p			
109	11772	p^2-p	269	80700	p^2+31p			

We can see that for primes within 349, p^2-p appears frequently in the table above. 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 form. We conjecture the form to be p^2-p, but there might be terms of 1, $p^{1/2}$, p or $p^{3/2}$. □

Now we turn to prove the Bias Conjecture 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.

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

□

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

Proof.

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

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

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

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:

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

□

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

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

Proof.

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

By quadratic Legendre sum (lemma 2.5), the t-sum is $p-1$ if $p \mid (x^3+x)$ and -1 otherwise. When $x=0$, the contribution is $p-1$ and otherwise it is -1. Hence, the total contribution from t is $1(p-1)+(p-1)(-1)=0$. □

Lemma 4.4. *The second moment of the two-parameter family $y^2 = x^3+t^2x+st^4$ is $(p-1)(p-1)\left(p-1-2\left(\frac{-3}{p}\right)\right)$, which supports our bias conjecture.*

Proof.

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

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

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

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 $(p-1)^2$.

If s is not congruent to zero mod p, we need to calculate when $(x-y)(y^2+xy+(1+x^2))$ is congruent to zero mod p. The solutions of the first factor are $x = y$; for fixed x, the discriminant of the second factor is $x^2 - 4(1+x^2) = -3x^2 - 4$. Thus, summing over x for $p > 2$ yields $p - 1 - 2\left(\frac{-3}{p}\right)$. We double-count by $3x^2+1 \equiv 0(p)$, so the contribution from this case is $(p-1)(p-1)\left(p-1-2\left(\frac{-3}{p}\right)\right)$.

Hence, we have

$$\begin{aligned}
A_{2,\mathcal{F}(p)} &= (p-1)^2 + (p-1)(p-1)\left(p-1-2\left(\frac{-3}{p}\right)\right) \\
&= p^3 - 2p^2 + p - 2(p^2-p)\left(\frac{-3}{p}\right).
\end{aligned} \tag{4.8}$$

□

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.

$$
\begin{aligned}
-A_{1,\mathcal{F}(p)} =& -\sum_{t(p)} a_{t(p)} \sum_{s(p)} a_{s(p)} = \sum_{t(p)} \sum_{x(p)} \sum_{s(p)} \left(\frac{x^3 + sx^2 - t^2x}{p} \right) \\
=& \sum_{t=1}^{p-1} \sum_{x(p)} \sum_{s(p)} \left(\frac{t^3x^3 + t^2sx^2 - t^3x}{p} \right) \\
=& \sum_{t=1}^{p-1} \sum_{x(p)} \sum_{s(p)} \left(\frac{t^2}{p} \right) \left(\frac{t(x^3 - x) + sx^2}{p} \right) \\
=& \sum_{t=0}^{p-1} \sum_{x(p)} \sum_{s(p)} \left(\frac{t(x^3 - x) + sx^2}{p} \right) - \sum_{x(p)} \sum_{s(p)} \left(\frac{sx^2}{p} \right) \\
=& \sum_{t(p)} \sum_{x(p)} \sum_{s(p)} \left(\frac{t(x^3 - x) + sx^2}{p} \right) - 0 \qquad (4.9) \\
=& \sum_{t(p)} \sum_{s(p)} \sum_{x=-1,0,1;x(p)} \left(\frac{t(x^3 - x) + sx^2}{p} \right) \\
&+ \sum_{t(p)} \sum_{s(p)} \sum_{x\neq-1,0,1;x(p)} \left(\frac{t(x^3 - x) + sx^2}{p} \right) - 0 \\
=& \sum_{s(p)} \left(\frac{0}{p} \right) + \sum_{s(p)} \left(\frac{-s}{p} \right) + \sum_{s(p)} \left(\frac{s}{p} \right) + \sum_{t(p)} \sum_{s(p)} \sum_{x\neq-1,0,1;x(p)} \left(\frac{t(x^3 - x) + sx^2}{p} \right) - 0 \\
=& 0 + 0 + 0 + 0 - 0 \\
=& 0
\end{aligned}
$$

□

Lemma 4.6. *The second moment of the two-parameter family $y^2 = x^3 + sx^2 - t^2x$ is $p^3 - 2p^2 + p$, which supports our bias conjecture.*

Proof.

$$\begin{aligned}
A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} {a_{t,s}}^2(p) \\
&= \sum_{t(p)}\sum_{s(p)}\sum_{x,y(p)} \left(\frac{x^3+sx^2-t^2x}{p}\right)\left(\frac{y^3+sy^2-t^2y}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{s(p)}\sum_{x,y(p)} \left(\frac{t^3x^3+t^2sx^2-t^3x}{p}\right)\left(\frac{t^3y^3+t^2sy^2-t^3y}{p}\right) \\
&= \sum_{t=1}^{p-1}\sum_{s(p)}\sum_{x,y(p)} \left(\frac{t^4}{p}\right)\left(\frac{t(x^3-x)+sx^2}{p}\right)\left(\frac{t(y^3-y)+sy^2}{p}\right) \\
&= \sum_{t=0}^{p-1}\sum_{s(p)}\sum_{x,y(p)} \left(\frac{t(x^3-x)+sx^2}{p}\right)\left(\frac{t(y^3-y)+sy^2}{p}\right) - \sum_{x,y(p)}\sum_{s(p)} \left(\frac{sx^2}{p}\right)\left(\frac{sy^2}{p}\right) \\
&= \sum_{x,y(p)}\sum_{s(p)}\sum_{t(p)} \left(\frac{t(x^3-x)+sx^2}{p}\right)\left(\frac{t(y^3-y)+sy^2}{p}\right) - (p-1)^3
\end{aligned} \tag{4.10}$$

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

$$\begin{aligned}
a &= (x^3-x)(y^3-y) \\
b &= (x^3-x)sy^2+(y^3-y)sx^2 \\
c &= s^2x^2y^2 \\
\delta &= [(x^3-x)sy^2-(y^3-y)sx^2]^2 \\
&= [sxy(x-y)(xy+1)]^2.
\end{aligned} \tag{4.11}$$

Similar to **4.1.2**, 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, we have

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

□

4.2 Construction of Rank 1 Families

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

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

Proof.

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

□

Lemma 4.8. *The second moment of the two-parameter family $y^2 = x^3 + sx^2 - t^2x$ is $p^3 - 2p^2 + 2p$.*

Proof.

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

As usual, we compute the discriminant of the equation in terms of t and s:

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

We first consider the contribution from $xy(x-y)$. The solutions to $x \equiv 0(p)$ and $y \equiv 0(p)$ happen $p-1$ times when $x=0$ or $y=0$. For $x-y \equiv 0(p)$, we have two cases. When $x=y=0$, s disappears and its contribution is 1. When $x=y\neq 0$, s does not disappear and $x-y \equiv 0(p)$ happens $p-1$ times when $x=y$. The contribution from those three cases is $p-1+p-1+p(p-1)+1=p^2+p-1$.

Then we consider when s^2 is congruent to zero mod p. The contribution from $x-y-1 \equiv 0(p)$ is $(p-1)^2$.

When s^2 is not congruent to zero mod p, which happens $(p-1)$ times, $s^2xy-x-y-1$ must be congruent to zero mod p. It can be rewritten as $(s^2x-1)y-(x+1)$, and its discriminant equals to $(s^2x-1)^2=s^4x^2-2s^2x+1$. By Lemma 2.5, summing over x for $p>2$ yields $\sum_{s=1}^{p-1}[1+\left(\frac{s^4}{p}\right)]=p-1$. Hence, the contribution from this case is $(p-1)(p-1)(p-1)=(p-1)^3$.

We must be careful about double-counting. When $s^2x^2-2x-1 \equiv 0$ and $x \neq 0$, each s has a corresponding x-value, so we double count by $p(p-1)$.

Thus,

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

□

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

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

Proof.

$$\begin{aligned}
-A_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} \sum_{s(p)} a_{s(p)} \\
&= \sum_{t(p)} \sum_{x(p)} \sum_{s(p)} \left(\frac{x^3 + ts^2x^2 + (t^3 - t^2)x}{p} \right) \\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x=1} \left(\frac{t^3x^3 + t^3s^2x^2 + t^4x - t^3x}{p} \right) \\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x=1} \left(\frac{t^3}{p} \right) \left(\frac{x^3 + s^2x^2 + tx - x}{p} \right) \\
&= \sum_{x(p)} \sum_{s(p)} \sum_{t(p)} \left(\frac{t}{p} \right) \left(\frac{tx + (x^3 + s^2x^2 - x)}{p} \right)
\end{aligned} \tag{4.17}$$

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 $1[2(p-1)+(p-2)(-1)]+(p-1)[1(p-1)+(p-1)(-1)] = p$. □

Lemma 4.10. *The second moment of the two-parameter family $y^2 = x^3 + ts^2x^2 + (t^3 - t^2)x$ is $p^3 - 3p^2 + p + 1$, which supports our bias conjecture.*

Proof.

$$\begin{aligned}
A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} {a_{t,s}}^2(p) \\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 + ts^2x^2 + (t^3 - t^2)x}{p} \right) \left(\frac{y^3 + ts^2y^2 + (t^3 - t^2)y}{p} \right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t=1}^{p-1} \left(\frac{t^3x^3 + t^3s^2x^2 + t^4x - t^3x}{p} \right) \left(\frac{t^3y^3 + t^3s^2y^2 + t^4y - t^3y}{p} \right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t=1}^{p-1} \left(\frac{t^6}{p} \right) \left(\frac{tx + x^3 + s^2x^2 - x}{p} \right) \left(\frac{ty + y^3 + s^2y^2 - y}{p} \right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t(p)} \left(\frac{tx + x^3 + s^2x^2 - x}{p} \right) \left(\frac{ty + y^3 + s^2y^2 - y}{p} \right) \\
&\quad - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 + s^2x^2 - x}{p} \right) \left(\frac{y^3 + s^2y^2 - y}{p} \right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t(p)} \left(\frac{tx + x^3 + s^2x^2 - x}{p} \right) \left(\frac{ty + y^3 + s^2y^2 - y}{p} \right) - (p^2 - 1)
\end{aligned} \tag{4.18}$$

$$\begin{aligned} a &= xy \\ b &= x(y^3+s^2y^2-y)+y(x^3+s^2x^2-x) \\ c &= (x^3+s^2x^2-x)(y^3+s^2y^2-y) \\ \delta &= [x(y^3+s^2y^2-y)-y(x^3+s^2x^2-x)]^2 \\ &= [xy(y-x)(s^2+x+y)]^2 \end{aligned} \tag{4.19}$$

The contribution from $xy(y-x)$ is $p(p-1)+p(p-1)+p^2 = 3p^2-2p$. 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 so the total contribution is $p[(p-1)+(p-1)+p] = 3p^2-2p$.

When s is congruent to zero mod p, $x+y \equiv 0(p)$ and $x=-y \neq 0$ happens $p-1$ times, so its contribution is $(p-1)^2$.

When s is not congruent to zero mod p, the contribution from $s^2+x+y \equiv 0(p)$ is $(p-1)^3$.

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

Hence, we have

$$\begin{aligned} A_{2,\mathcal{F}(p)} &= 3p^2-2p+(p-1)^2+(p-1)^3-p^2-2p(p-1)-(p^2-1) \\ &= p^3-3p^2+p+1. \end{aligned} \tag{4.20}$$

□

4.2.3 $y^2 = x^3+t^2x^2+(t^3-t^2)sx$

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

Proof.

$$\begin{aligned} -A_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} \sum_{s(p)} a_{s(p)} \\ &= \sum_{t(p)} \sum_{x(p)} \sum_{s(p)} \left(\frac{x^3 + t^2x^2 + (t^3 - t^2)sx}{p} \right) \\ &= \sum_{t(p)} \sum_{s(p)} \sum_{x=1} \left(\frac{t^3x^3 + t^4x^2 + t^4sx - t^3sx}{p} \right) \\ &= \sum_{t(p)} \sum_{s(p)} \sum_{x=1} \left(\frac{t^3}{p} \right) \left(\frac{x^3 + tx^2 + tsx - sx}{p} \right) \\ &= \sum_{x(p)} \sum_{s(p)} \sum_{t(p)} \left(\frac{t}{p} \right) \left(\frac{t(x^2 + sx) + (x^3 - sx)}{p} \right) \end{aligned} \tag{4.21}$$

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 $p + (p-1)[1(p-1) + (p-1)(-1)] = p$. □

Lemma 4.12. *The second moment of the two-parameter family $y^2 = x^3 + t^2x^2 + (t^3 - t^2)sx$ is $p^3 - 4p^2 + 5p$, which supports our bias conjecture.*

Proof.

$$\begin{aligned} A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} {a_{t,s}}^2(p) \\ &= \sum_{t(p)} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 + t^2x^2 + (t^3 - t^2)sx}{p} \right) \left(\frac{y^3 + t^2y^2 + (t^3 - t^2)sy}{p} \right) \\ &= \sum_{s(p)} \sum_{x,y(p)} \sum_{t=1}^{p-1} \left(\frac{t^3x^3 + t^4x^2 + t^4sx - t^3sx}{p} \right) \left(\frac{t^3y^3 + t^4y^2 + t^4sy - t^3sy}{p} \right) \\ &= \sum_{s(p)} \sum_{x,y(p)} \sum_{t=1}^{p-1} \left(\frac{t^6}{p} \right) \left(\frac{t(x^2 + sx) + (x^3 - sx)}{p} \right) \left(\frac{t(y^2 + sy) + (y^3 - sy)}{p} \right) \\ &\quad - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 - sx}{p} \right) \left(\frac{y^3 - sy}{p} \right) \\ &= \sum_{s(p)} \sum_{x,y(p)} \sum_{t(p)} \left(\frac{t(x^2 + sx) + (x^3 - sx)}{p} \right) \left(\frac{t(y^2 + sy) + (y^3 - sy)}{p} \right) \\ &\quad - p(p-1) \end{aligned} \tag{4.22}$$

The discriminant of the equation equals to

$$\begin{aligned} a &= (x^2+sx)(y^2+sy) \\ b &= (x^2+sx)(y^3-sy)+(y^2+sy)(x^3-sx) \\ c &= (x^3-sx)(y^3-sy) \\ \delta &= [(x^2+sx)(y^3-sy)-(y^2+sy)(x^3-sx)]^2 \\ &= [xy(x-y)(s(x+y+1)+xy)]^2. \end{aligned} \tag{4.23}$$

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,

$$\begin{aligned} A_{2,\mathcal{F}(p)} &= 3p^2-4p+2+0+(p-1)^3-2p(p-2)-(p-1)p-1-p(p-1) \\ &= p^3-4p^2+5p. \end{aligned} \tag{4.24}$$

□

4.3 Construction of Rank 2 Families

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

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

Proof.

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

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 $p + [2(p-1) + (p-2)(-1)] = 2p$. □

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

Proof.

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

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

Similar to **4.2.2**, the contribution from $xy(x-y)$ is $3p^2-2p$.

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,

$$\begin{aligned} A_{2,\mathcal{F}(p)} &= 3p^2-2p+0+(p-2)(p-1)^2-(2p^2-2) \\ &\quad -\sum_{s(p)}\sum_{x,y(p)}\left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right) \\ &= p^3-3p^2+3p-\sum_{s(p)}\sum_{x,y(p)}\left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right). \end{aligned} \tag{4.28}$$

□

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

Lemma 4.15. *The first moment of the two-parameter family $y^2=x^3-t^2x+t^3s^2+t^4$ is $-2p$.*

Proof.

$$\begin{aligned}
-A_{1,\mathcal{F}(p)} &= -\sum_{t(p)} a_{t(p)} \sum_{s(p)} a_{s(p)} \\
&= \sum_{t(p)} \sum_{x(p)} \sum_{s(p)} \left(\frac{x^3 - t^2 x + t^3 s^2 + t^4}{p} \right) \\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x=1} \left(\frac{t^3 x^3 - t^3 x + t^3 s^2 + t^4}{p} \right) \\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x=1} \left(\frac{t^3}{p} \right) \left(\frac{x^3 - x + s^2 + t}{p} \right) \\
&= \sum_{x(p)} \sum_{s(p)} \sum_{t(p)} \left(\frac{t}{p} \right) \left(\frac{t + (x^3 - x + s^2)}{p} \right)
\end{aligned} \tag{4.29}$$

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 $1[3(p-1)+(p-3)(-1)]+(p-1)[1(p-1)+(p-1)(-1)] = 2p$. □

Lemma 4.16. *The second moment of the two-parameter family $y^2 = x^3 - t^2 x + t^3 s^2 + t^4$ 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.

$$\begin{aligned}
A_{2,\mathcal{F}(p)} &= \sum_{t,s(p)} {a_{t,s}}^2(p) \\
&= \sum_{t(p)} \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 - t^2 x + t^3 s^2 + t^4}{p} \right) \left(\frac{y^3 - t^2 y + t^3 s^2 + t^4}{p} \right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t=1}^{p-1} \left(\frac{t^3 x^3 - t^3 x + t^3 s^2 + t^4}{p} \right) \left(\frac{t^3 y^3 - t^3 y + t^3 s^2 + t^4}{p} \right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t=1}^{p-1} \left(\frac{t^6}{p} \right) \left(\frac{t + (x^3 - x + s^2)}{p} \right) \left(\frac{t + (y^3 - y + s^2)}{p} \right) \\
&\quad - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3 - x + s^2}{p} \right) \left(\frac{y^3 - y + s^2}{p} \right) \\
&= \sum_{s(p)} \sum_{x,y(p)} \sum_{t(p)} \left(\frac{t + (x^3 - x + s^2)}{p} \right) \left(\frac{t + (y^3 - y + s^2)}{p} \right) - p(p-1)
\end{aligned} \tag{4.30}$$

$$\begin{aligned} a &= 1 \\ b &= (x^3 - x + s^2) + (y^3 - y + s^2) \\ c &= (x^3 - x + s^2)(y^3 - y + s^2) \\ \delta &= [(x^3 - x + s^2) - (y^3 - y + s^2)]^2 \\ &= [(x-y)(x^2 + xy + y^2 - 1)]^2 \end{aligned} \tag{4.31}$$

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,

$$\begin{aligned} A_{2,\mathcal{F}(p)} &= p^2(p - 1 - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right] - p(p-1) \\ &= p^3 - 2p^2 + p - \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right] p^2. \end{aligned} \tag{4.32}$$

□

5 Conclusion and Future Work

We have shown in all of the one- and two-parameter families we computed that the largest lower order term in the second-moment of the Fourier coefficients has a negative average. For the families we cannot compute numerically, we conjecture that these terms of their second moments 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 $p^{3/2}$ and $p^{1/2}$ 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.

Below are the two tables which record biases in every one- and two- parameter families we compute or conjecture in this paper:

One-Parameter Family	Rank	$A_{1,\mathcal{F}(p)}$	$A_{2,\mathcal{F}(p)}$
$y^2 = x^3 - x^2 - x + t$	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	$p^2 - 2p - [\sum_{x(p)} \left(\frac{x^3+x^2}{p}\right)]^2 - \left(\frac{-3}{p}\right)p$
$y^2 = x^3 + tx^2 + x + 1$	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	$p^2 - 2p - 1$
$y^2 = x^3 - x^2 + (x^2 - x)t + 1$	2	-2p	$p^2 - 1$ (conjecture from observation)
$y^2 = x^3 - x + t^4$	2(conjecture)	-2p (conjecture)	$p^2 - p$ (conjecture from observation)

Two-Parameter Family	$A_{1,\mathcal{F}(p)}$	$A_{2,\mathcal{F}(p)}$
$y^2 = x^3 + tx + sx^2$	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	$p^3 - 2p^2 + p$
$y^2 = x^3 + t(x^2 - x) + s^2x^2$	-p	$p^3 - 2p^2 + 2p$
$y^2 = x^3 + ts^2x^2 + (t^3 - t^2)x$	-p	$p^3 - 3p^2 + p + 1$
$y^2 = x^3 + t^2x^2 + (t^3 - t^2)sx$	-p	$p^3 - 4p^2 + 5p$
$y^2 = x^3 + t^2x^2 - (s^2 - s)t^2x$	-2p	$p^3 - 3p^2 + 3p - \sum_{s(p)} \sum_{x,y(p)} \left(\frac{x^3-(s^2-s)x}{p}\right)\left(\frac{y^3-(s^2-s)y}{p}\right)$
$y^2 = x^3 - t^2x + t^3s^2 + t^4$	-2p	$p^3 - 2p^2 + p - \left\lfloor \left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right) \right\rfloor p^2$

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^kx because summing over x mod p is the same as summing over g^kx 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 $\sum_{D=0}^{p-1}\sum_{x=0}^{p-1}(\frac{x^2-D}{p}) = 0$, 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 the one-parameter families that we compute are rational surfaces using **Theorem 2.3**, or else the first moment does not equal to the rank. Keep in mind that we will not prove rank 0 one-parameter families. This is because the first moment of a one-parameter family is 0, then according to Rosen-Silverman, it is a rational surface.

B.1 Rank 1 One-Parameter Families

B.1.1 $y^2 = x^3 + tx^2 + t^2$

Lemma B.1. *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

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

Hence, we get

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

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

B.1.2 $y^2 = x^3 + tx^2 + x + 1$

Lemma B.2. *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

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

Hence, we get

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

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

B.1.3 $y^2 = x^3 + tx^2 + tx + t^2$

Lemma B.3. *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:

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

Hence, we get

$$y^2 = x^3 + \frac{2}{3}t^2x + t^4 + \frac{3}{27}t^3 - \frac{1}{3}t^2. \tag{B.6}$$

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

□

B.2 Rank 2 One-Parameter Families

B.2.1 $y^2 = x^3 - x^2 + (x^2 - x)t + 1$

Lemma B.4. *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:

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

Hence, we get

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

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

B.2.2 $y^2 = x^3 - x + t^4$

Lemma B.5. *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 the family is a rational surface. □

C 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.

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

[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.