Abelian Varieties Over Finite Fields in the LMFDB

Taylor Dupuy

Joint w/ Kiran Kedlaya, David Roe, Christelle Vincent;
* Kiran Kedlaya, David Zureick-Brown;
** Edgar Costa, Stefano Marseglia, David Roe

LMFDB

⌂ → Abelian varieties → Fq

Feedback · Hide Menu

Isogeny classes of abelian varieties over finite fields

Introduction

Overview Random
Universe Knowledge

L-functions

Degree 1 Degree 2
Degree 3 Degree 4
ζ zeros

Modular forms

Classical Maass
Hilbert Bianchi

Varieties

Elliptic curves over $\mathbb{Q}$
Elliptic curves over $\mathbb{Q}(\alpha)$
Genus 2 curves over $\mathbb{Q}$
Higher genus families
Abelian varieties over $\mathbb{F}_q$

The database currently contains 2,945,722 isogeny classes of abelian varieties of dimension up to 6 over finite fields. You can browse further statistics or create your own.

Learn more about

Completeness of the data
Source of the data
Reliability of the data
Labeling convention

Browse

By dimension: 1 2 3 4 5 6

By base field cardinality: 2 3 4 5 7 8 9 16 17 19 23 25 27-211 223-1024

Some interesting isogeny classes or a random isogeny class

A table by dimension and base field.

Search

Advanced search options

Cardinality of the base field	81	e.g. 81 or 3-49	Primitive	
Characteristic of the base field	3	e.g. 3 or 2-5	Simple	
Dimension	2	e.g. 2	Geometrically simple	

The Database of Isogeny Classes of ~~Abelian Varieties~~ over finite fields

Weil Polynomials

Due to Honda-Tate

Weil Polynomials

Defn. A Weil q-number of weight w is some $\pi \in \bar{\mathbb{Q}}$ such that for every embedding $\psi: \mathbb{Q}(\pi) \hookrightarrow \mathbb{C}$

$$|\psi(\pi)|_\infty = q^{w/2}$$

Defn. A Weil Polyn of wt w is a polyn $P(T) \in \mathbb{Q}[T]$ all of whose roots are Weil q-numbers of weight w.

Defn. A Weil Polyn of wt w is a polyn $P(T) \in \mathbb{Q}[T]$ all of whose roots are Weil q-numbers of weight w.

Example: If $X/\mathbb{F}_q$ smooth projective, $\dim_{\mathbb{F}_q}(X) = n$, then

$$\det(T - Fr \mid H^i_\ell(X)) = P_i(T)$$

ℓ-adic cohomology: $\left[\varprojlim H^i(X_{\bar{\mathbb{F}}_q}, \mathbb{Z}/\ell^r)\right] \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$

$(\text{Zeros of } P_i(T)) \leftarrow$ Weil q-numbers of weight $i/2$

Theorem of Deligne.

Defn. A Weil Polyn of wt w is a polyn $P(T) \in \mathbb{Q}[T]$ all of whose roots are Weil q-numbers of weight w.

example: Abelian Varieties

$$H^i_\ell(A) = \underbrace{\Lambda^i H^1_\ell(A)}_{\text{ith wedge power}}$$

Knows about all other powers

example: Abelian Varieties

$$H^i_\ell(A) = \underbrace{\Lambda^i H^1_\ell(A)}_{\text{ith wedge power}}$$

$$P_A(T) = \det(T - Fr \mid H^1_\ell)$$
$$= (T-\alpha_1) \cdots (T-\alpha_{2g})$$

eigenvalues for $H^2_\ell(A)$:

$\alpha_i \alpha_j$

eigenvalues for $H^2_\ell(A)$:

$\alpha_i \alpha_j$

eigenvalues for $H^3_\ell(A)$:

$\alpha_i \alpha_j \alpha_k$

$\vdots$

eigenvalues for $H^3_\ell(A)$:

$$\alpha_i \alpha_j \alpha_k$$

Even More!!! (Honda-Tate)

Even More!!! (Honda-Tate)

Let A, B be two abelian varieties over $\mathbb{F}_q$.

- $A \sim B'$ for some $B' \leq B$ $\iff$ $P_A(T) \mid P_B(T)$
- If A simple

$$P_A(T) = h_A(T)^{e_A}$$

for some $e_A \in \mathbb{N}$.

- If A simple

$$P_A(T) = h_A(T)^{e_A}$$

for some $e_A \in \mathbb{N}$. irred

$$e_A = [\mathrm{End}^\circ(A/\mathbb{F}_q) : \text{center}]^{1/2}$$

- Every irreducible Weil q-polynomial occurs as some $h_A(T)$.

QUESTIONS

- How do we tabulate all of the weil polys?
- How many isogeny classes did we compute?
- What is this Ahmadi-Shparlinski conjecture you guys disproved?
- What are the arithmetic statistics for these Weil poly?
- How do we compute isomorphism classes?

- What are the arithmetic statistics for these Weil poly?

* Galois Groups
* Newton Polygons
* Point Counts / Zeta Fns
* Maximal Abelian Varieties (simple & nonsimple)
* Statistics for Endos
* Angle Ranks

* Newton Polygons

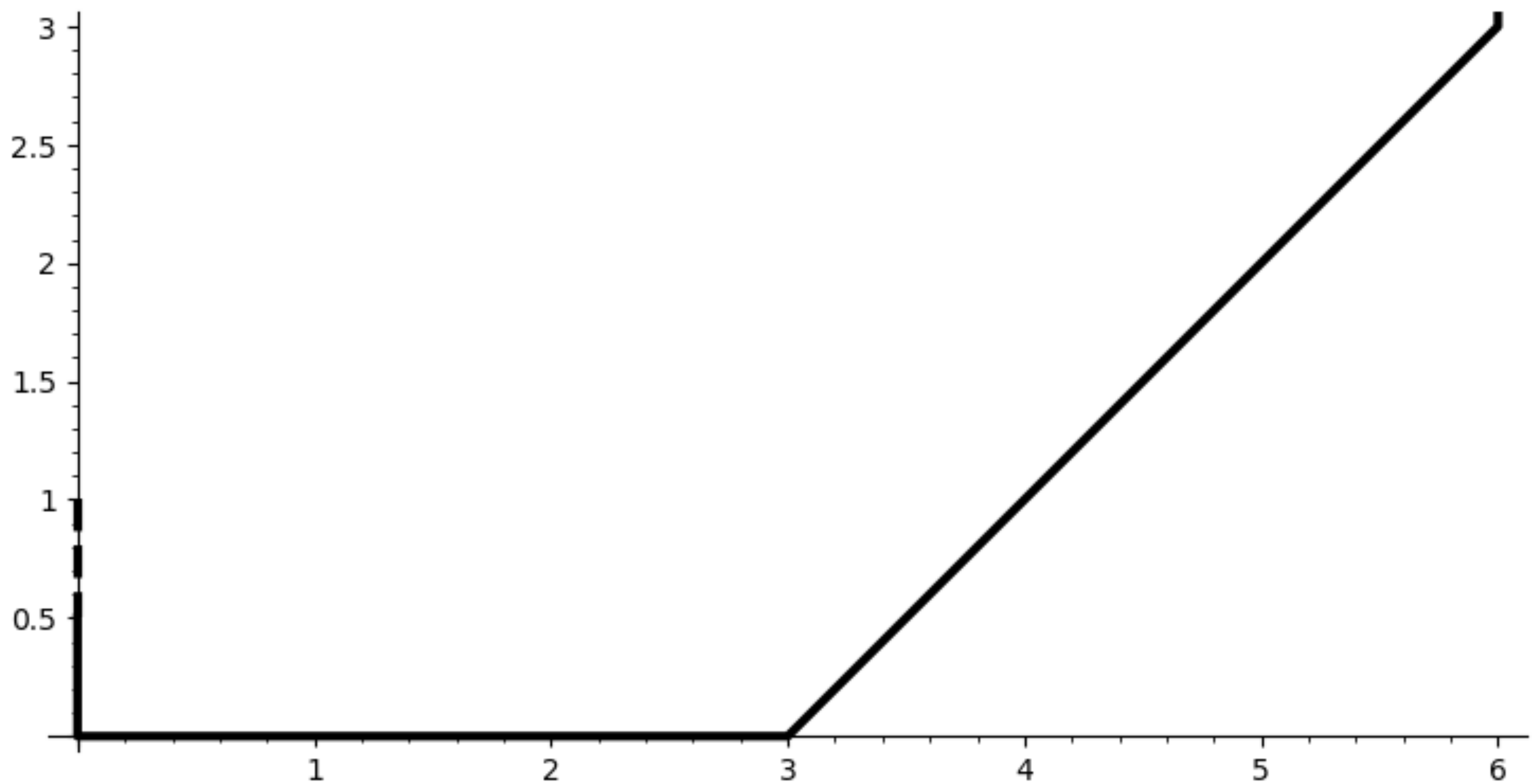
<u>Reminder</u>: Given $P_A(T) = \prod_{i=1}^{2g} (T - \alpha_i)$

$$\text{slopes} = \left\{ \frac{\mathrm{ord}_p(\alpha_i)}{\mathrm{ord}_p(q)} : i = 1, \ldots, 2g \right\}$$

$\mathrm{len}(s) = (\#$ of roots of slope $s_i)$

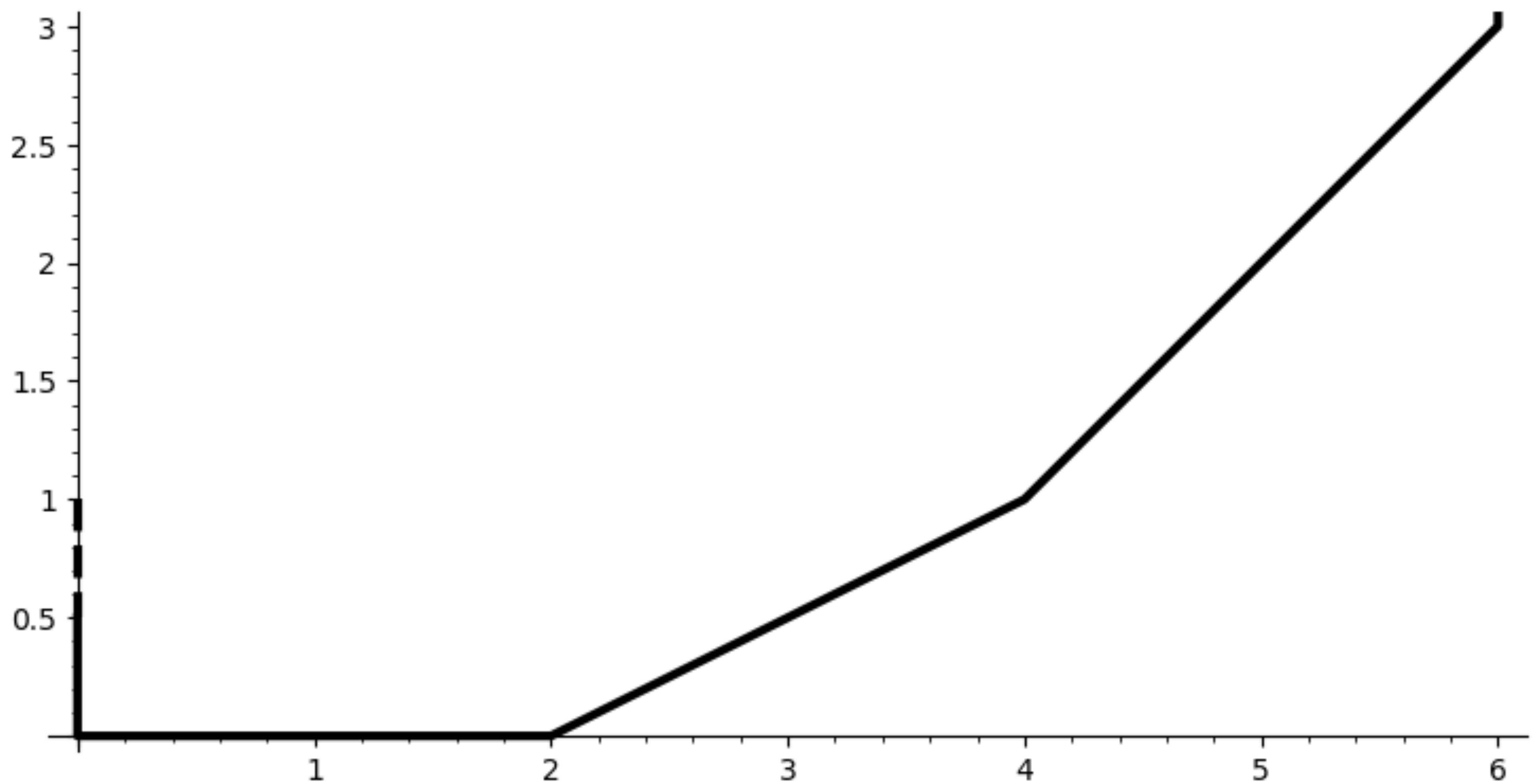
* Newton Polygons

Ordinary



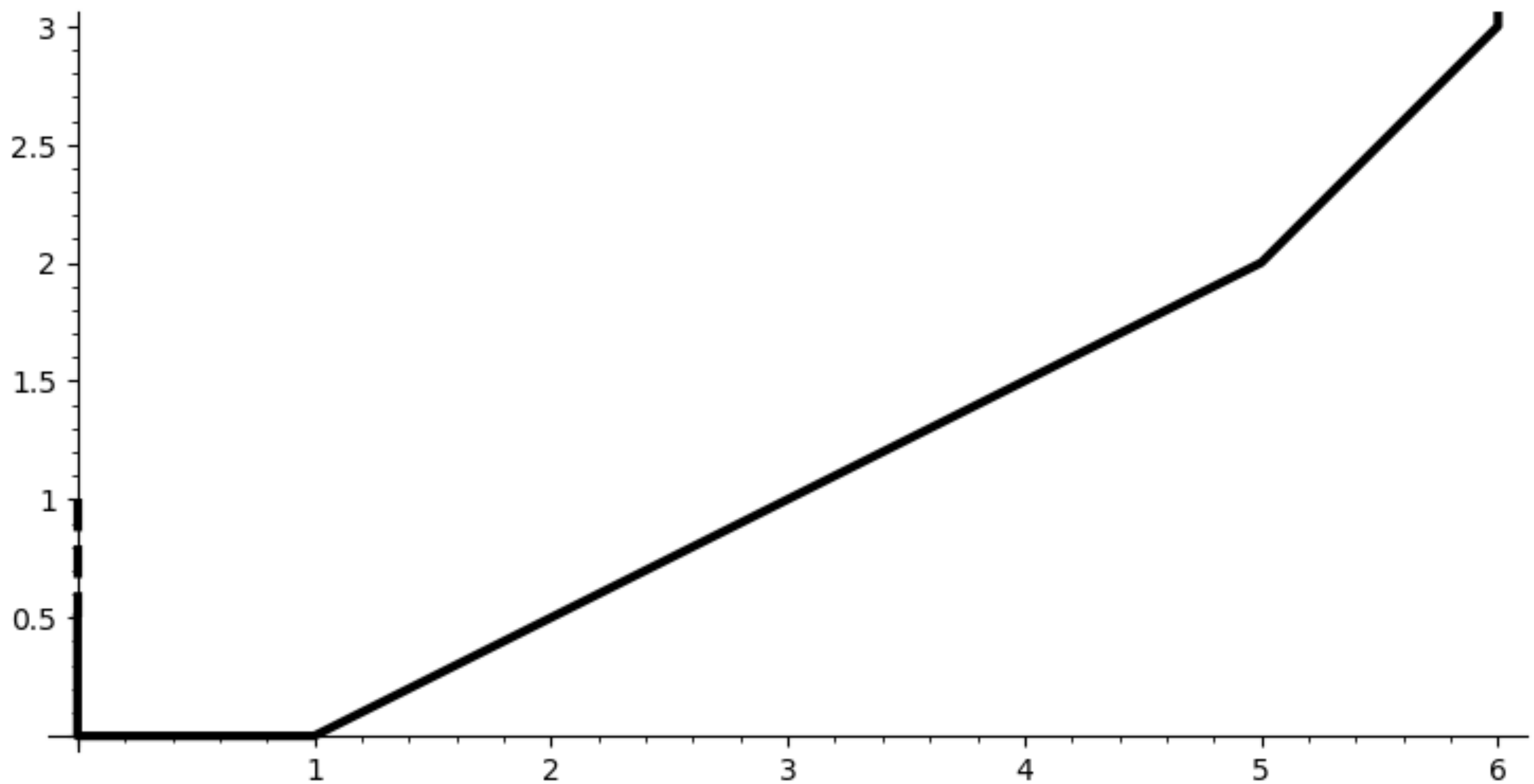
Newton Polygon with Slopes $[0, 0, 0, 1, 1, 1]$

* Newton Polygons



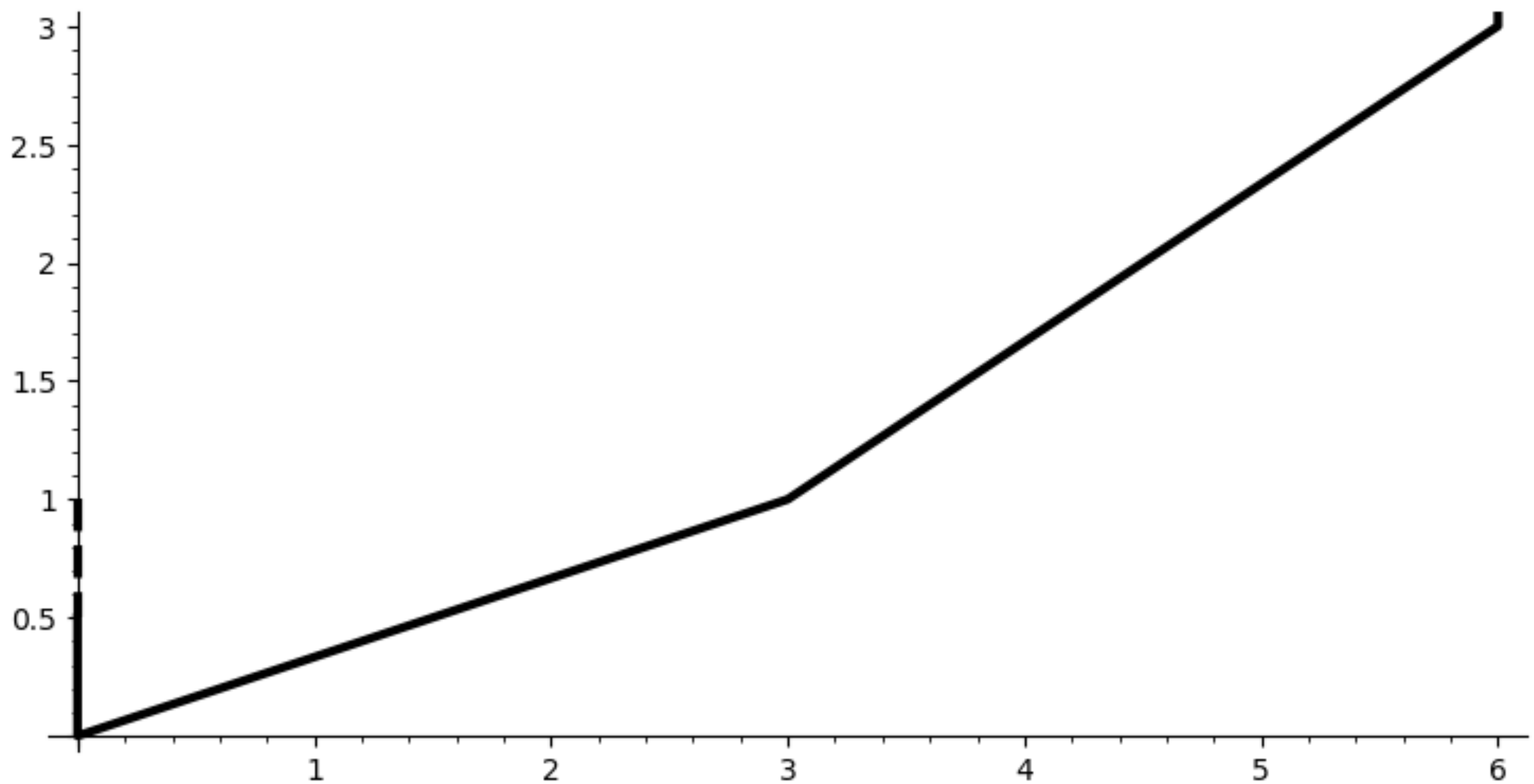
Newton Polygon with Slopes $[0, 0, 1/2, 1/2, 1, 1]$

* Newton Polygons



Newton Polygon with Slopes $[0, 1/2, 1/2, 1/2, 1/2, 1]$

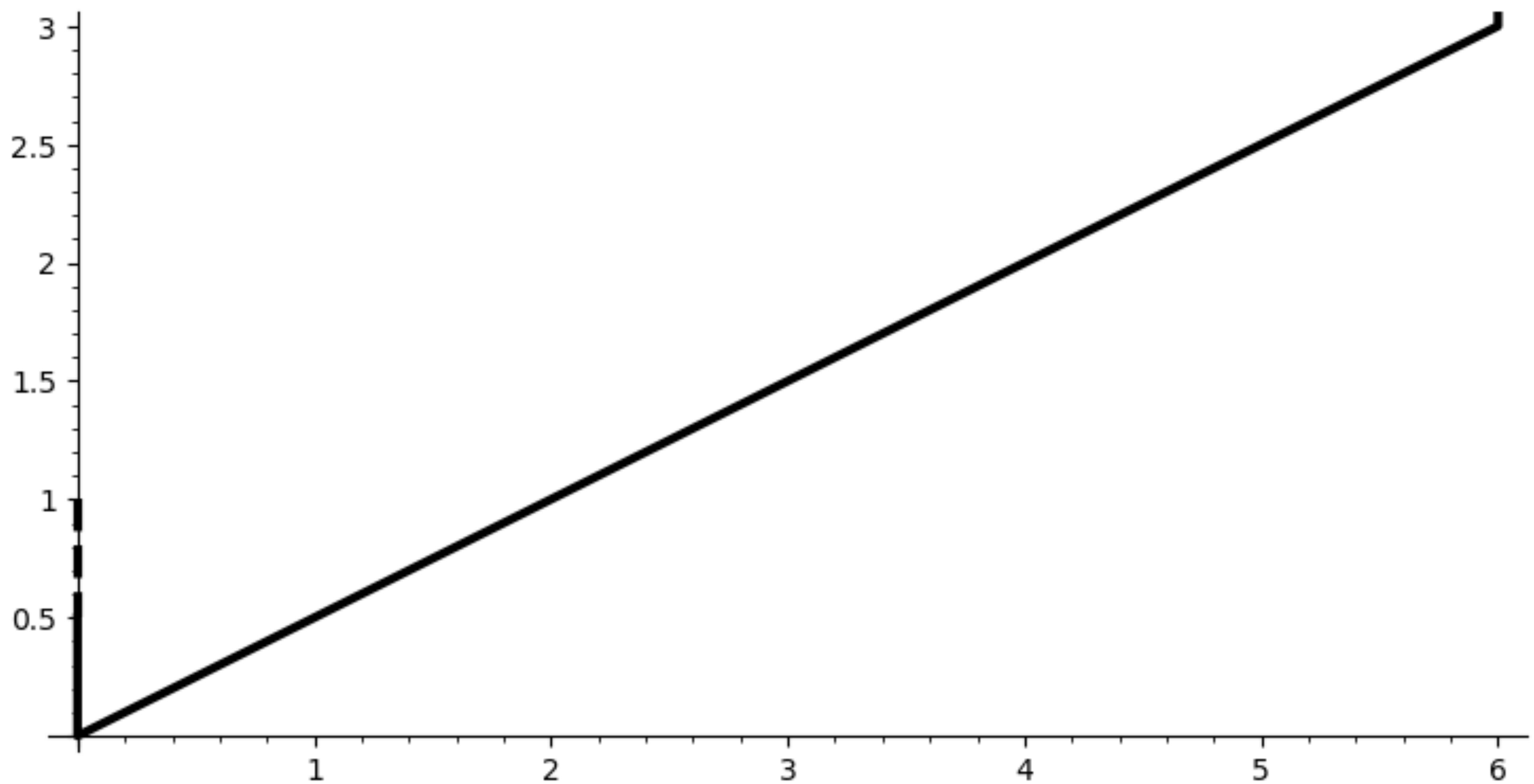
* Newton Polygons



Newton Polygon with Slopes $[1/3, 1/3, 1/3, 2/3, 2/3, 2/3]$

* Newton Polygons

Supersingular



Newton Polygon with Slopes $[1/2, 1/2, 1/2, 1/2, 1/2, 1/2]$

QUESTIONS

- How do we tabulate all of the Weil polys?
- How many isogeny classes did we compute?
- What is this Ahmadi-Shparlinski conjecture you guys disproved?
- What are the arithmetic statistics for these Weil poly?
- How do we compute isomorphism classes?

- How do we compute isomorphism classes?

- How do we compute isomorphism classes?

Theorem (Deligne 1969)

There is a functor

$$\mathrm{AV}^{\mathrm{ord}}_{\mathbb{F}_q} \xrightarrow{\mathrm{DM}} \{\text{Deligne Modules}\}$$

which is an equivalence of categories.

category of ordinary abelian varieties.

$\{$Deligne Modules$\}$

input: $A/\mathbb{F}_q$ ordinary abelian variety

<u>step 1</u>: $\tilde{A}/W(\mathbb{F}_q)$ canonical lift

<u>step 2</u>: $\tau : W(\mathbb{F}_q) \hookrightarrow \mathbb{C}$, $\tilde{A}_{\mathbb{C}}$

$\{$Deligne Modules$\}$

input: $A/\mathbb{F}_q$ ordinary abelian variet[y]

step 1: $\tilde{A}/W(\mathbb{F}_q)$ canonical lift

step 2: $\tau : W(\mathbb{F}_q) \hookrightarrow \mathbb{C}$, $\quad \tilde{A}_{\mathbb{C}}$

step 3:

$$DM(A) := H^1(\tilde{A}_{\mathbb{C}}(\mathbb{C}), \mathbb{Z})$$

singular cohomology

Fr $\qquad$ V $\qquad$ + axioms.

$$\boxed{DM(A) := H^1(\tilde{A}_{\mathbb{C}}(\mathbb{C}), \mathbb{Z})}$$

{Deligne Modules}

How to make this practical?

Theorem (Howe, Marseglia)

$$\left\{\begin{array}{c}\text{Deligne Modules for}\\ \text{fixed } P_A(T)\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{Fractional ideals}\\ \text{in } \mathbb{Q}(\pi_A)\end{array}\right\} / \sim$$

Theorem (Howe, Marseglia)

$$\left\{\begin{matrix}\text{Deligne Modules for}\\ \text{fixed } P_A(T)\end{matrix}\right\} \leftrightarrow \left\{\begin{matrix}\text{Fractional ideals}\\ \text{in } \mathbb{Q}(\pi_A)\end{matrix}\right\}\Big/\sim$$

Ideal Class Monoid

$$I \subseteq \mathbb{Q}(\pi)$$

$Fr = \pi$ $\qquad$ $V = q/\pi$

QUESTIONS

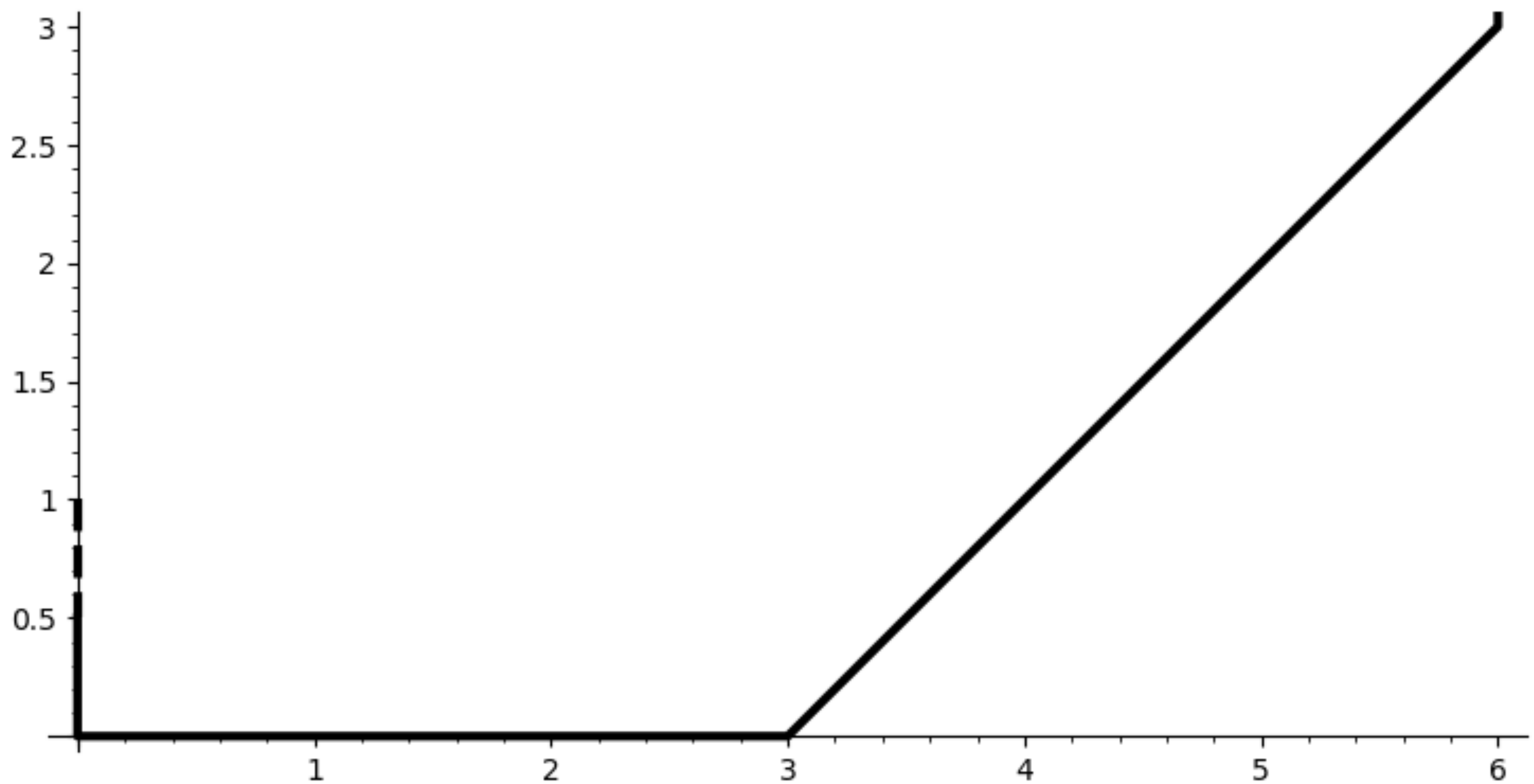
- How do we tabulate all of the Weil polys?
- How many isogeny classes did we compute?
- What is this Ahmadi-Shparlinski conjecture you guys disproved?
- What are the arithmetic statistics for these Weil poly?
- How do we compute isomorphism classes?

- What are the arithmetic statistics for these Weil Poly?

* Galois Groups
* Newton Polygons
* Point Counts / Zeta Fns
* Maximal Abelian Varieties (simple & nonsimple)
* Statistics for Endos
* Angle Ranks

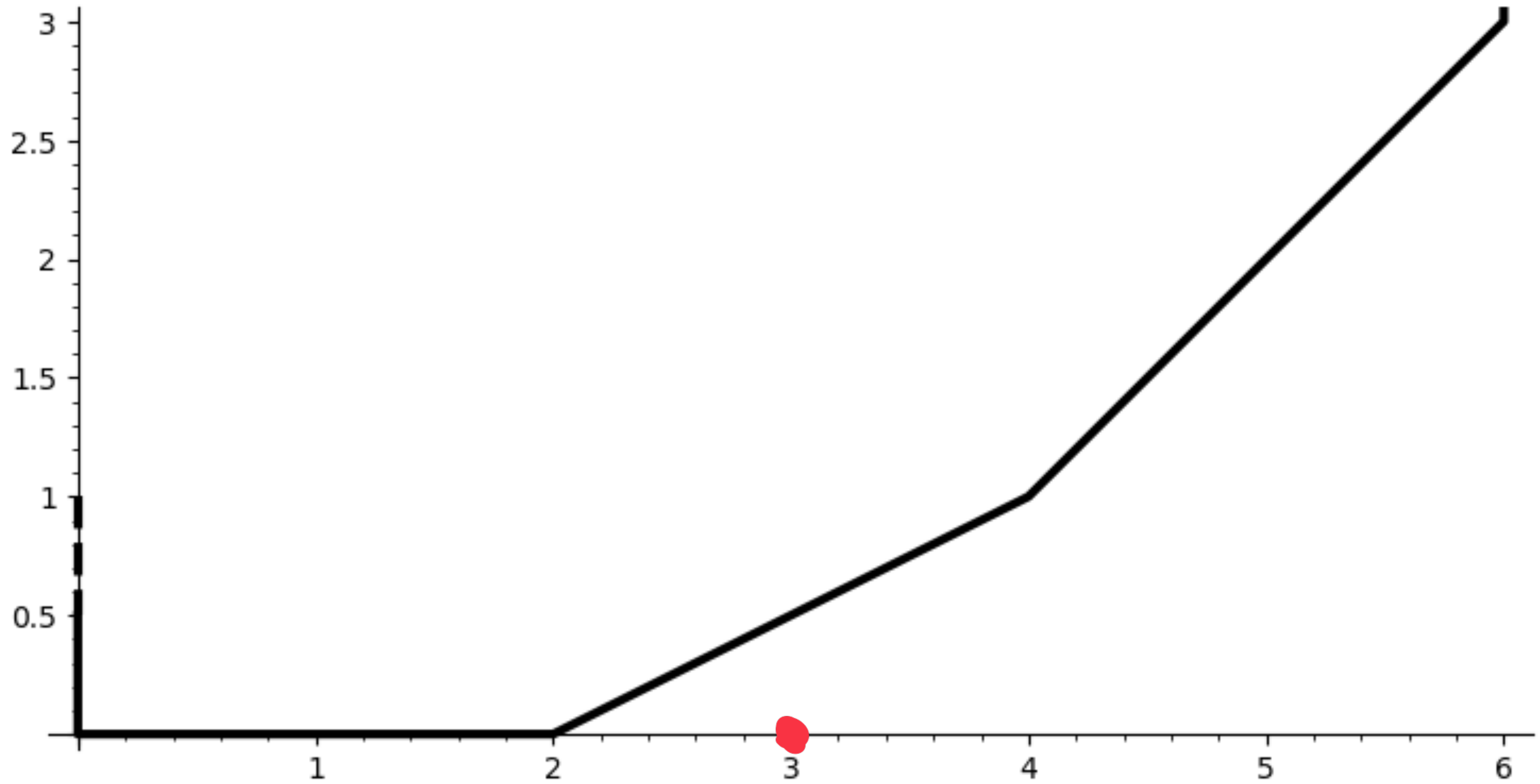
* Newton Polygons

Ordinary



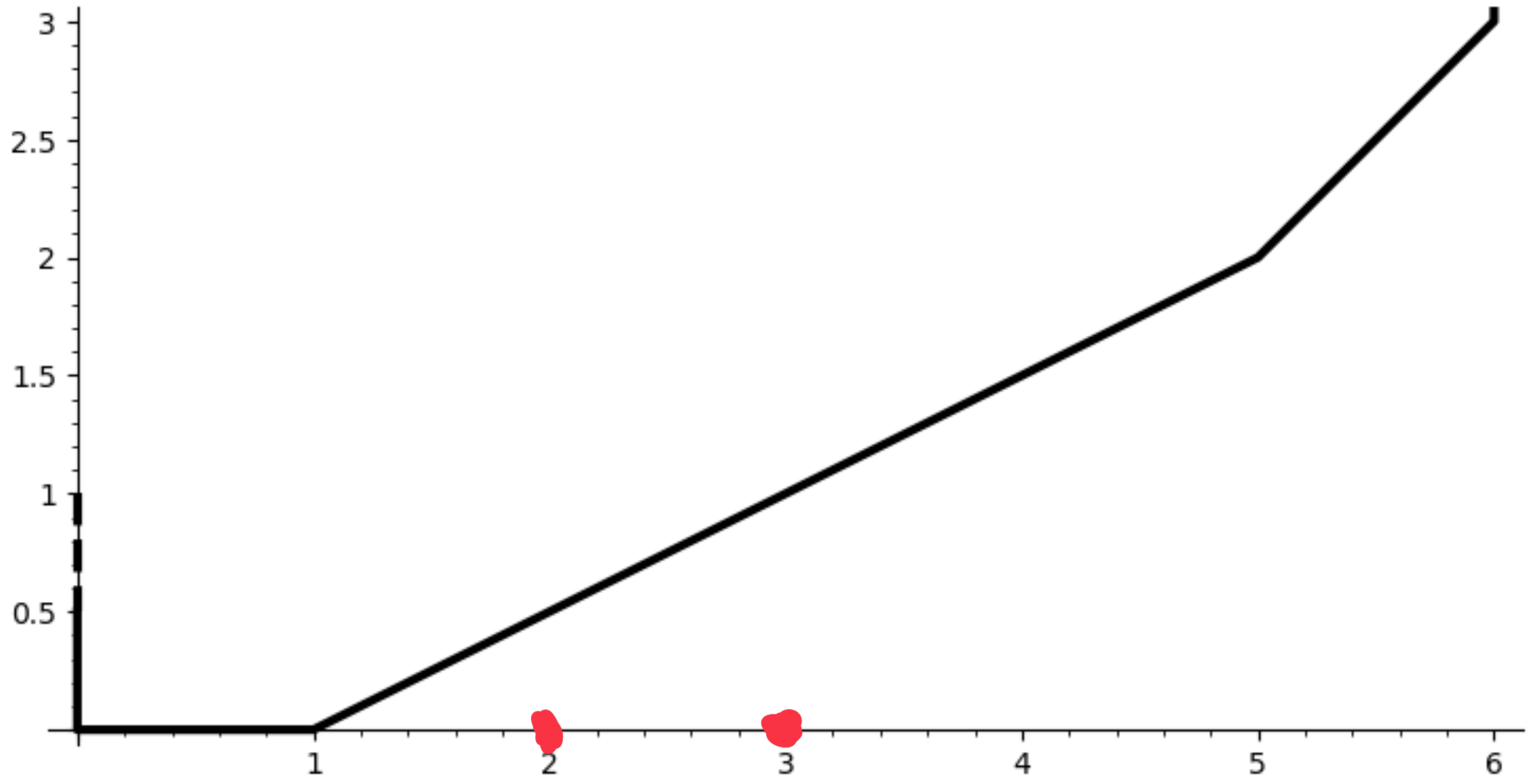
Newton Polygon with Slopes $[0, 0, 0, 1, 1, 1]$

* Newton Polygons



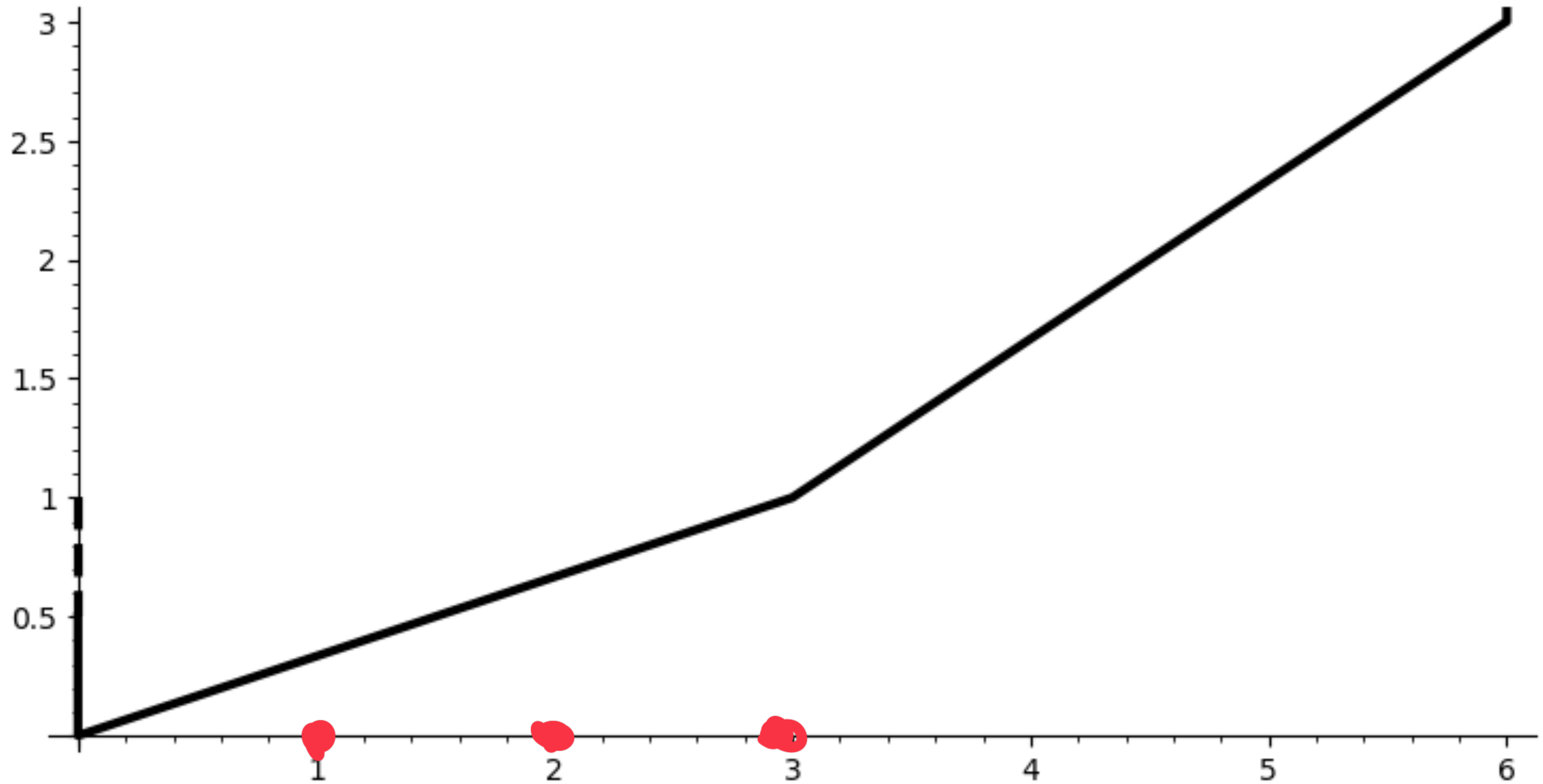
Newton Polygon with Slopes $[0, 0, 1/2, 1/2, 1, 1]$

* Newton Polygons



Newton Polygon with Slopes $[0, 1/2, 1/2, 1/2, 1/2, 1]$

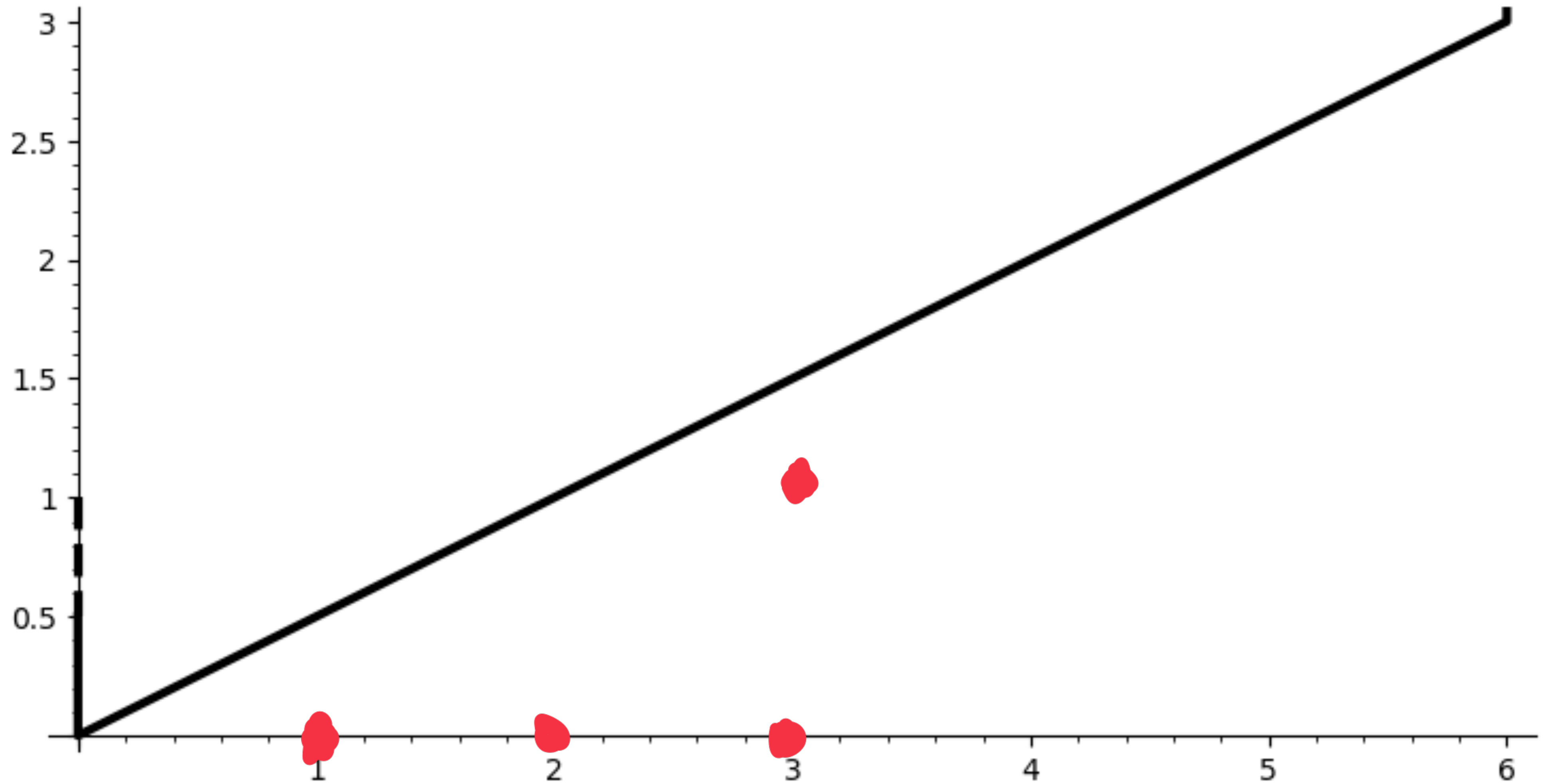
* Newton Polygons



Newton Polygon with Slopes $[1/3, 1/3, 1/3, 2/3, 2/3, 2/3]$

* Newton Polygons

Supersingular



Newton Polygon with Slopes $[1/2, 1/2, 1/2, 1/2, 1/2, 1/2]$

* Newton Polygons

What is the rule for Newton Polygon frequency?

Dimension	Slopes	$q=2$	$q=3$	$q=4$	$q=5$
4	$(0,0,0,0,1,1,1,1)$	453	5062	18178	87115
4	$\left(0,0,0,\frac{1}{2},\frac{1}{2},1,1,1\right)$	94	1048	6966	15698
4	$\left(0,0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1,1\right)$	43	381	1398	3108
4	$\left(0,\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},\frac{2}{3},\frac{2}{3},1\right)$	26	114	244	526
4	$\left(0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1\right)$	6	12	66	70
4	$\left(\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{1}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4},\frac{3}{4}\right)$	36	82	275	168
4	$\left(\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{1}{2},\frac{1}{2},\frac{2}{3},\frac{2}{3},\frac{2}{3}\right)$	2	2	20	16
4	$\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$	5	6	5	5

- What are the arithmetic statistics for these Weil Poly?

* Galois Groups
* Newton Polygons
* Point Counts / Zeta Fns
* Maximal Abelian Varieties (simple & nonsimple)
* Statistics for Endos
* Angle Ranks

* Galois Groups

What is the rule for Galois Groups frequency?

Dimension	Group	$q = 2$	$q = 3$	$q = 4$	$q = 5$
3	6T1	4	2	6	
3	6T3	14	32	84	88
3	6T6	14	34	52	94
3	6T11	48	280	676	1850

* Galois Groups

	2	3	4	5	7	8	9	11
6T1	0.31636	0.11844	0.26715	$-\infty$	0.30254	0.23744	0.14698	0.25954
2T1	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$	0.079146	$-\infty$	$-\infty$
6T3	0.60225	0.59221	0.66064	0.58783	0.60854	0.54666	0.63575	0.57555
6T11	0.88343	0.96285	0.97157	0.98768	0.99256	0.99380	0.99424	0.99707
6T6	0.60225	0.60257	0.58913	0.59649	0.58877	0.60836	0.58708	0.59022

log(Number with given group)/log(Total)

- What are the arithmetic statistics for these Weil poly?

* Galois Groups
* Newton Polygons
* Point Counts / Zeta Fns
* Maximal Abelian Varieties (simple & nonsimple)
* Statistics for Endos
* Angle Ranks

* Galois Groups

g	Num of Groups	Num of Newton Poly
1	2	2
2	4	3
3	5	5
4	30	8
5	9	12
6	46	20

If random: possible = (5-1)*(5-1)*(5) = 80

* Galois Groups

Slopes	Group	Angle Rank	$q=2$	$q=3$	$q=4$	$q=5$
$(0,0,0,1,1,1)$	6T1	1	4		4	
$(0,0,0,1,1,1)$	6T3	1	4	10	12	28
$(0,0,0,1,1,1)$	6T3	3	2	6	10	42
$(0,0,0,1,1,1)$	6T6	3	14	32	48	82
$(0,0,0,1,1,1)$	6T11	3	32	218	502	1544
$\left(0,0,\frac{1}{2},\frac{1}{2},1,1\right)$	6T3	2	6	12	56	6
$\left(0,0,\frac{1}{2},\frac{1}{2},1,1\right)$	6T6	3			2	10
$\left(0,0,\frac{1}{2},\frac{1}{2},1,1\right)$	6T11	3	6	42	134	268
$\left(0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1\right)$	6T3	3			2	4
$\left(0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1\right)$	6T6	3			2	2
$\left(0,\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},1\right)$	6T11	3	4	16	26	30
$\left(\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},\frac{2}{3},\frac{2}{3}\right)$	6T3	1	2	4	4	8
$\left(\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},\frac{2}{3},\frac{2}{3}\right)$	6T6	3		2		
$\left(\frac{1}{3},\frac{1}{3},\frac{1}{3},\frac{2}{3},\frac{2}{3},\frac{2}{3}\right)$	6T11	3	6	4	14	8
$\left(\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2}\right)$	6T1	0		2	2	

Actual Possible = 15

- What are the arithmetic statistics for these Weil Poly?

* Galois Groups
* Newton Polygons
* Point Counts / Zeta Fns
* Maximal Abelian Varieties (simple & nonsimple)
* Statistics for Endos
* Angle Ranks

* Point Counts / Zeta Fns

Lang-Weil: For $X/\mathbb{F}_q$, smooth projective geom. irred. dimension d

$$\#X(\mathbb{F}_q) = q^d + O(q^{d-1/2}). \quad (\text{as } q \to \infty)$$

$$\Rightarrow \quad E_X = \frac{\#X(\mathbb{F}_q) - q^d}{q^{d-1/2}}$$

How Do The Errors Vary Over Isog classes?

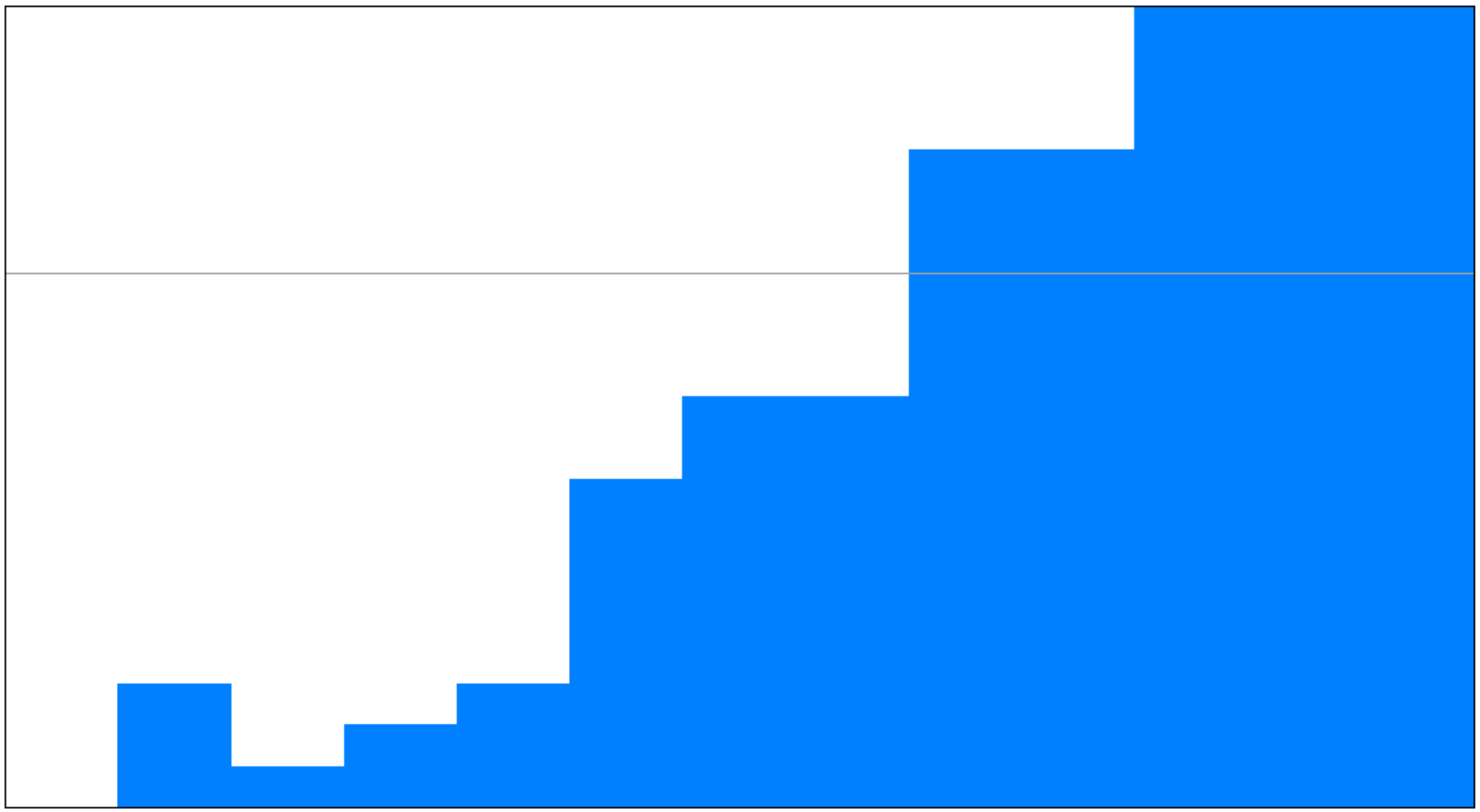
How Do The Errors Vary Over Isog classes?

$$E_X = \frac{\#X(\mathbb{F}_q) - q^d}{q^{d-1/2}}$$

set: $X = A$

Sutherland, g=1

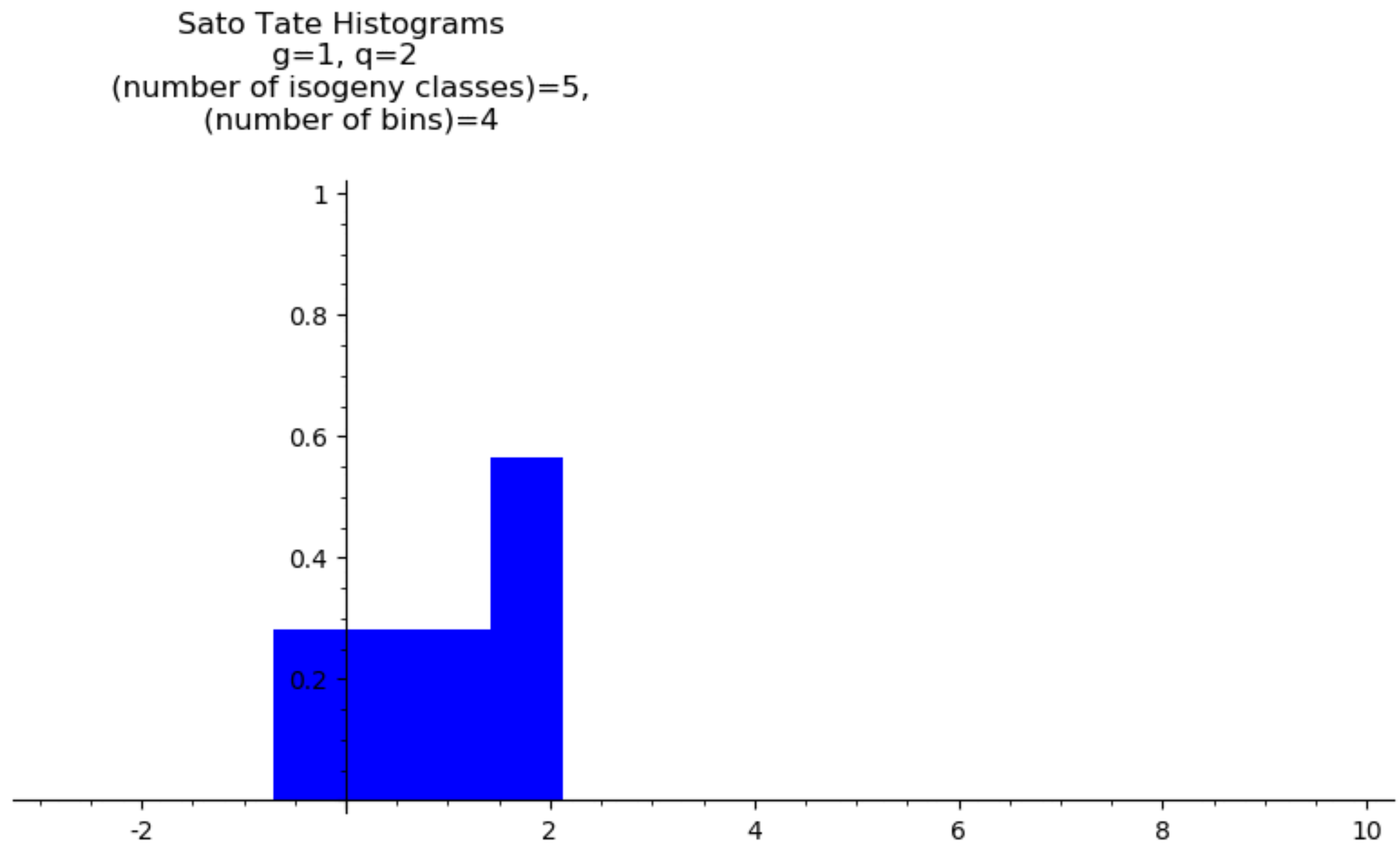
a1 histogram of y^2 + xy + y = x^3 - x^2 - 20067762415575526585033208209338542750930230312178956502x
+ 34481611795030556467032985690390720374855944359319180361266008296291939448732243429 for p <= 2^10
172 data points in 13 buckets, z1 = 0.023, out of range data has area 0.250



Moments: 1   1.034   1.716   2.532   4.446   7.203   13.024   22.220   40.854   72.100   133.961

How Do The Errors Vary Over Isog
classes?

Isog Classes, g=1

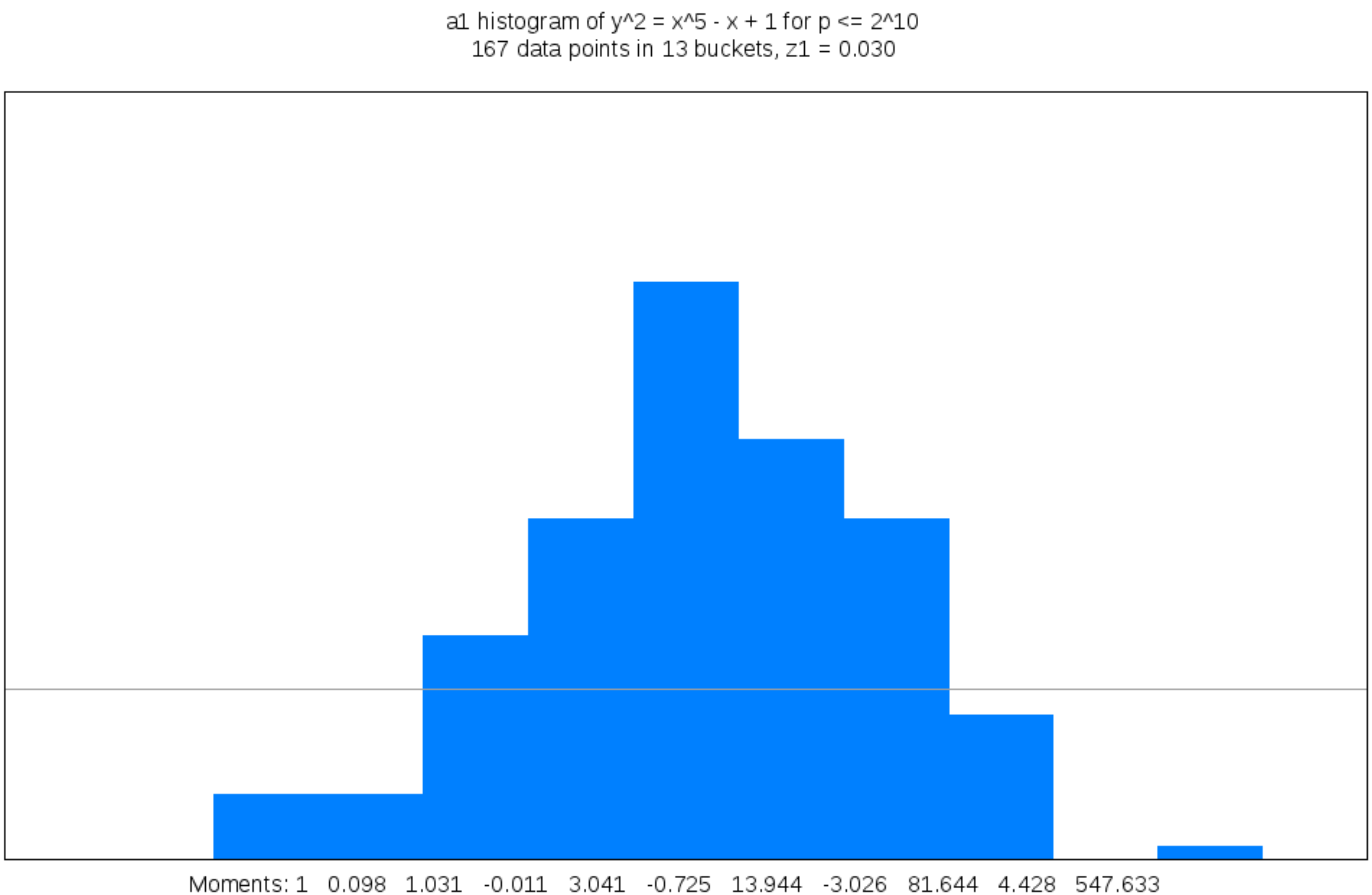


Moments: [0.707106781186548, 1.50000000000000, 2.47487373415292, 4.95000000000000, 9.72271824131503]

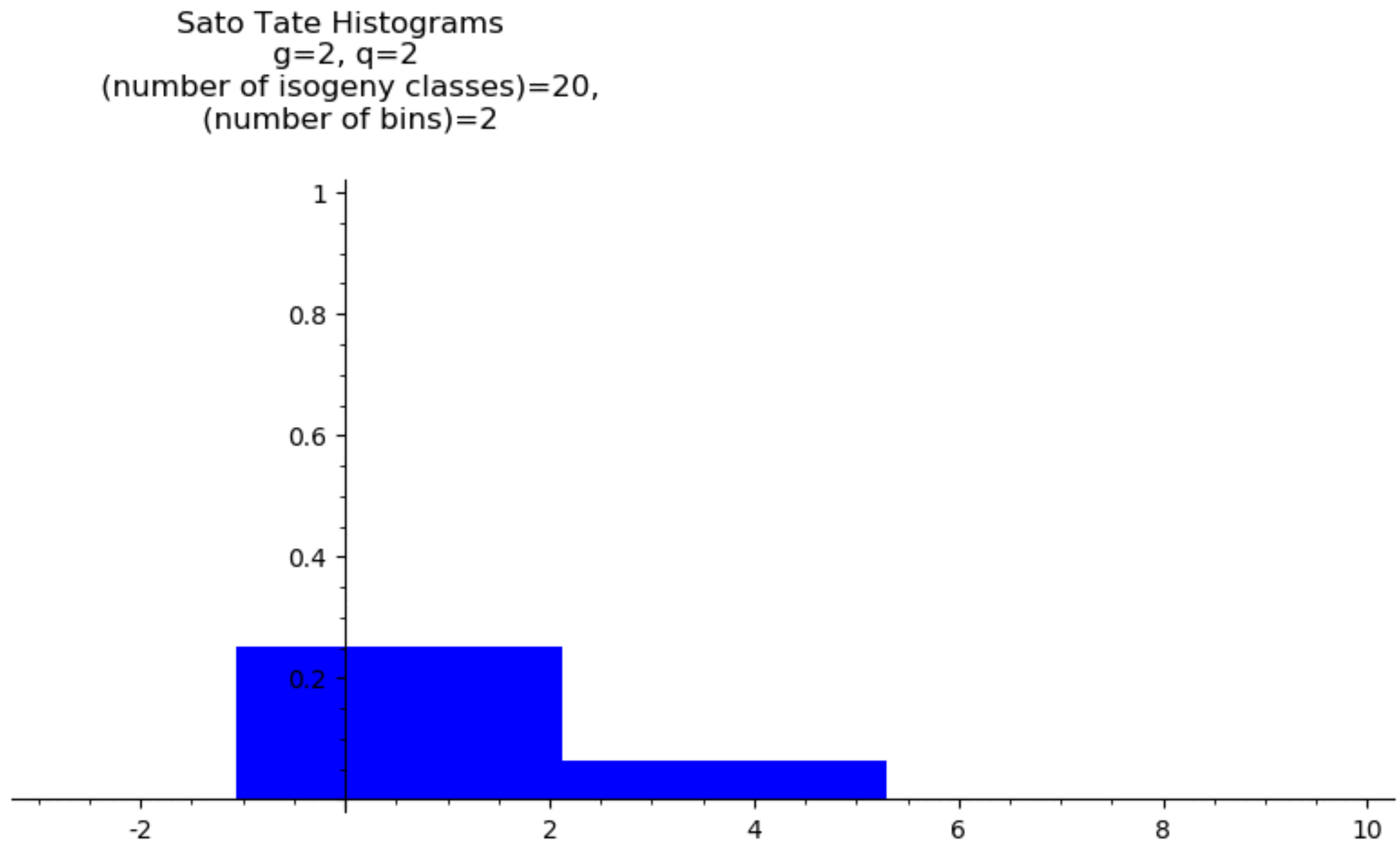
How Do The Errors Vary over Isog classes?

How Do The Errors Vary Over Isog classes?

Sutherland, g=2



Isog Classes, g=2



Moments: [0.689429111656884, 3.55625000000000, 12.2970288665723, 55.4851562500000, 259.317325107260]

How Do The Errors Vary over Isog classes?

How Do The Errors Vary Over Isog classes?

$$E_X = \frac{\#X(\mathbb{F}_q) - q^d}{q^{d-1/2}}$$

set: $X = C$

$$E_X = \frac{\#X(\mathbb{F}_q) - q^d}{q^{d-1/2}}$$

set: $X = A$

How Do The Errors Vary Over Isog classes?

$$E_X = \frac{\#X(\mathbb{F}_q) - q^d}{q^{d-1/2}}$$

set: $X = C$

$$E_X = \frac{\#X(\mathbb{F}_q) - q^d}{q^{d-1/2}}$$

set: $X = A$

$$E_X = \frac{\#X(\mathbb{F}_q) - q^d}{q^{d-1/2}}$$

set: $X = C$

$$E_X = \frac{\#X(\mathbb{F}_q) - q^d}{q^{d-1/2}}$$

set: $X = A$

Curves

Are we allowed to compare Drew's plots to our plots???

Abelian Varieties

How Do The Errors Vary Over Isog classes?

$X = C$ curve:

How Do The Errors Vary over Isog classes?

$$\#C(\mathbb{F}_q) = \mathrm{Tr}(\mathrm{Fr}\,|\,H^0) - \mathrm{Tr}(\mathrm{Fr}\,|\,H^1) + \mathrm{Tr}(\mathrm{Fr}\,|\,H^2)$$

$$= 1 - \mathrm{Tr}(\mathrm{Fr}\,|\,H^1) + q$$

$$\rightsquigarrow \boxed{E_C = \frac{1 - \mathrm{Tr}(\mathrm{Fr}\,|\,H^1) + q}{q}}$$

$X = A$ abelian variety:

$$\#A(\mathbb{F}_q) = \mathrm{Tr}(\mathrm{Fr}|H^0) - \mathrm{Tr}(\mathrm{Fr}|H^1) + \mathrm{Tr}(\mathrm{Fr}|H^2) - \cdots$$
$$- \mathrm{Tr}(\mathrm{Fr}|H^{2g-1}) + \mathrm{Tr}(\mathrm{Fr}|H^{2g})$$

$$\rightsquigarrow E_A = \frac{\#A(\mathbb{F}_q) - q^g}{q^{g-1/2}}$$

$$\#A(\mathbb{F}_q) = \underbrace{\mathrm{Tr}(\mathrm{Fr} \mid H^0) - \mathrm{Tr}(\mathrm{Fr} \mid H^1) + \mathrm{Tr}(\mathrm{Fr} \mid H^2) - \cdots}_{O(q^{g-1/2})}$$

$$\underbrace{\boxed{- \mathrm{Tr}(\mathrm{Fr} \mid H^{2g-1})}}_{\sum_i^{2g} \frac{\alpha_1 \alpha_2 \cdots \alpha_{2g}}{\alpha_i}} + \underbrace{\boxed{\mathrm{Tr}(\mathrm{Fr} \mid H^{2g})}}_{q^g}$$

(complex conj pairs)

$$E_A = \frac{\#A(\mathbb{F}_q) - q^g}{q^{g-1/2}}$$

How Do The Errors Vary Over Isog classes?

$$\sum_{i}^{2g} \frac{\alpha_1 \alpha_2 \cdots \alpha_{2g}}{\alpha_i} = g^g \sum_{i=1}^{2g} 1/\alpha_i$$

$$= g^g \sum_{i=1}^{2g} \overline{\alpha_i}/g$$

$$= g^{g-1} \sum_{i=1}^{2g} \alpha_i$$

How Do The Errors Vary over Isog classes?

$$\#A(\mathbb{F}_q) = \underbrace{Tr(Fr|H^0) - Tr(Fr|H^1) + Tr(Fr|H^2) - \cdots}_{O(q^{g-1/2})} \underbrace{\boxed{- Tr(Fr|H^{2g-1})}}_{\sum_{i=1}^{2g} \frac{\alpha_1 \alpha_2 \cdots \alpha_{2g}}{\alpha_i}} + \underbrace{\boxed{Tr(Fr|H^{2g})}}_{q^g}$$

(complex conj pairs)

$$E_A = \frac{\#A(\mathbb{F}_q) - q^g}{q^{g-1/2}}$$

How Do The Errors Vary Over Isog classes?

How Do The Errors Vary Over Isog classes?

$$E_A = \frac{\#A(\mathbb{F}_q) - q^g}{q^{g-1/2}}$$

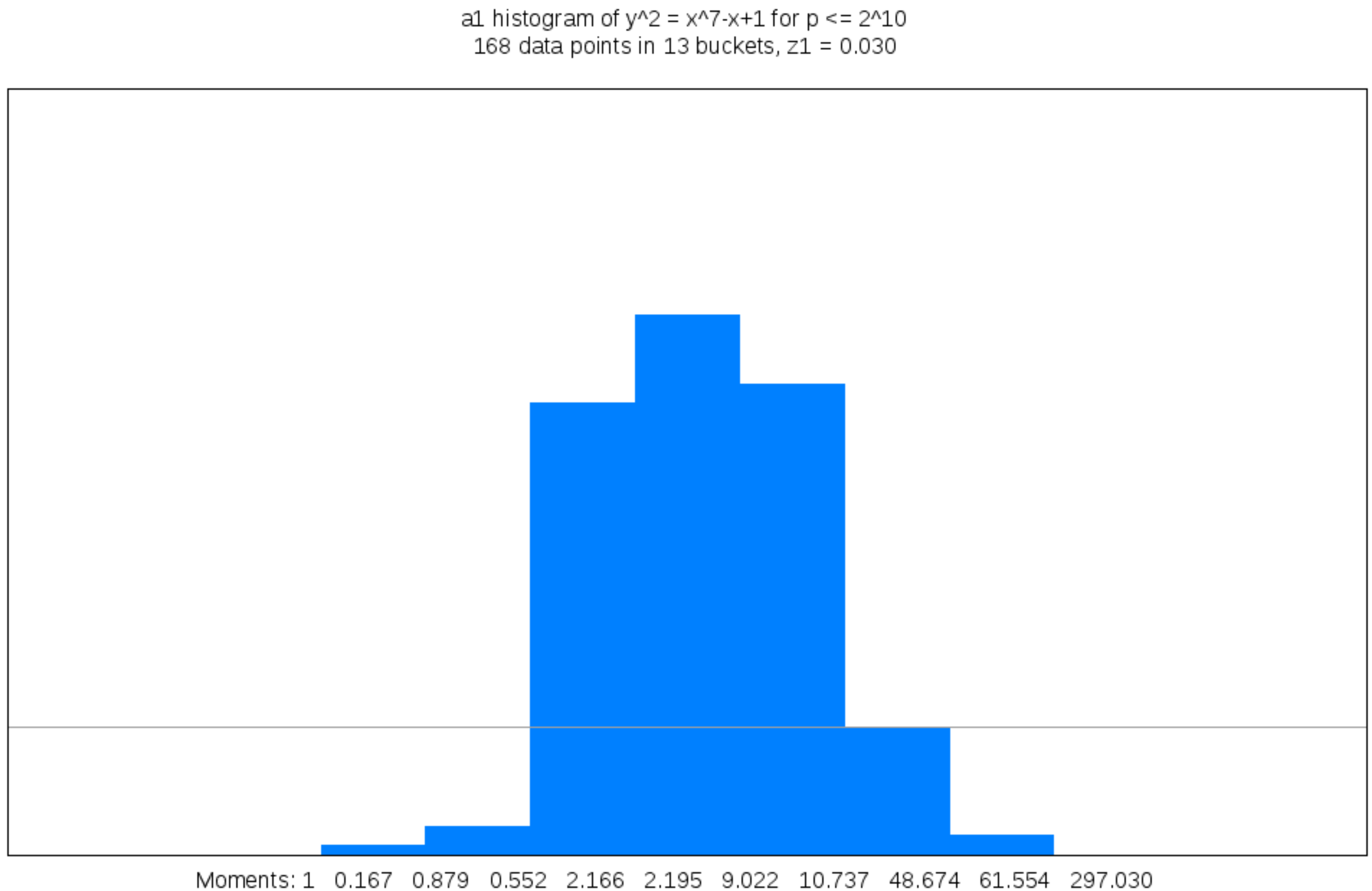
$$= \left(-\mathrm{Tr}(\mathrm{Fr} \mid H^{2g-1}) + O(q^{g-1})\right) / q^{g-1/2}$$

$$= q^{-1/2} \sum_{i=1}^{2g} \alpha_i + O(q^{-1/2})$$

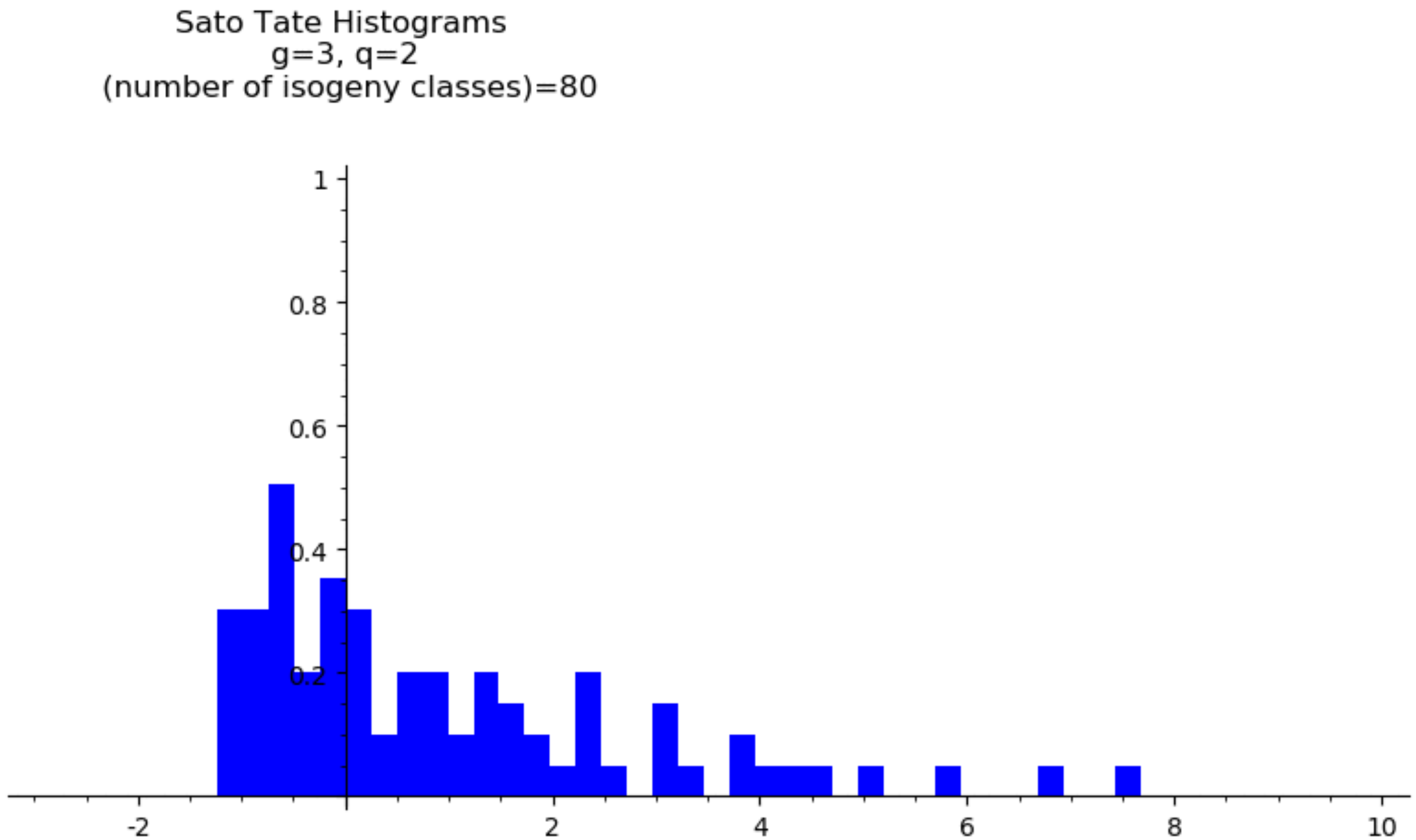
$$= E_C + O(q^{-1/2})$$

Drew's Plots are $\underline{\underline{OK}}$

Sutherland g=3

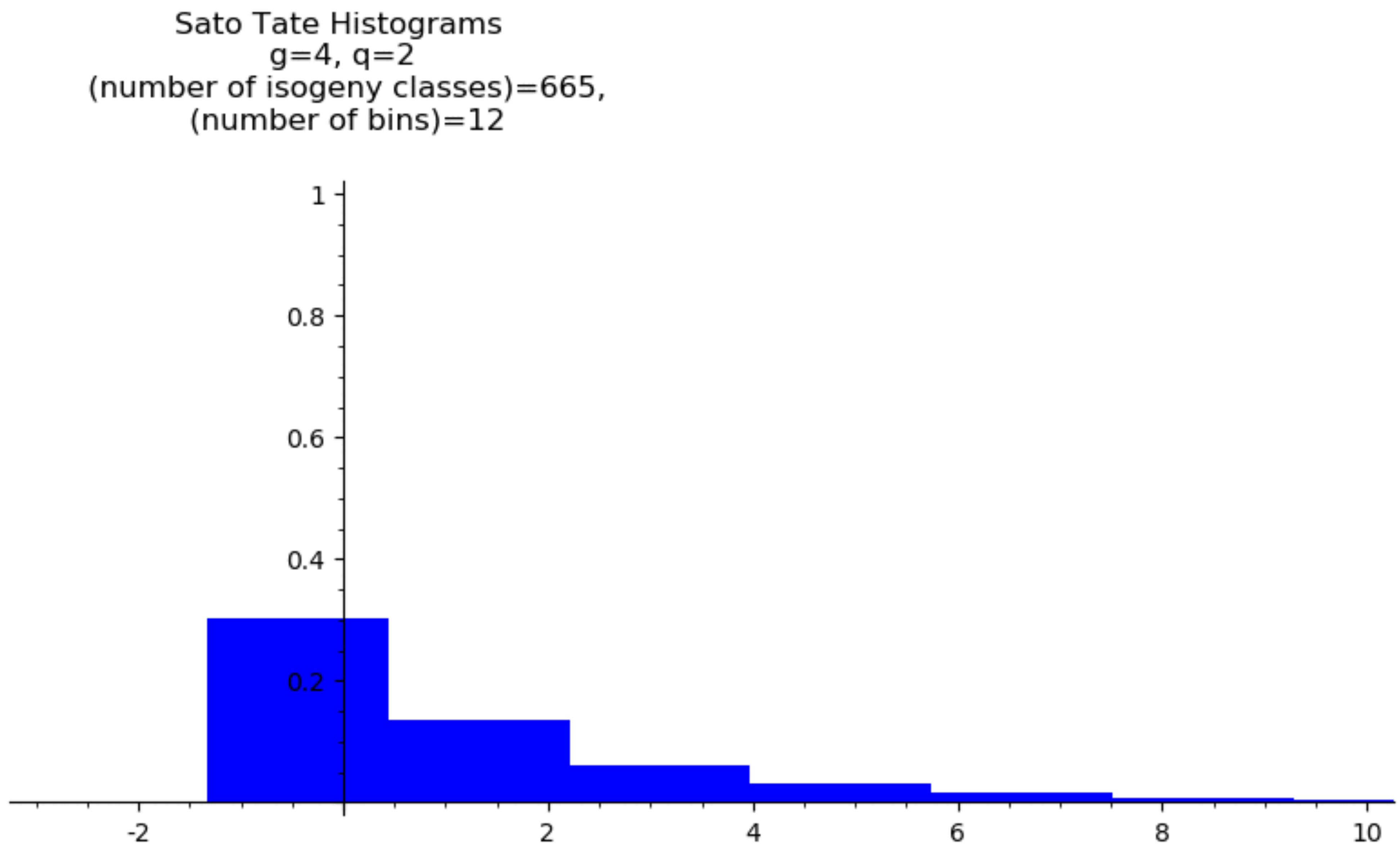


Isog Classes, g=3



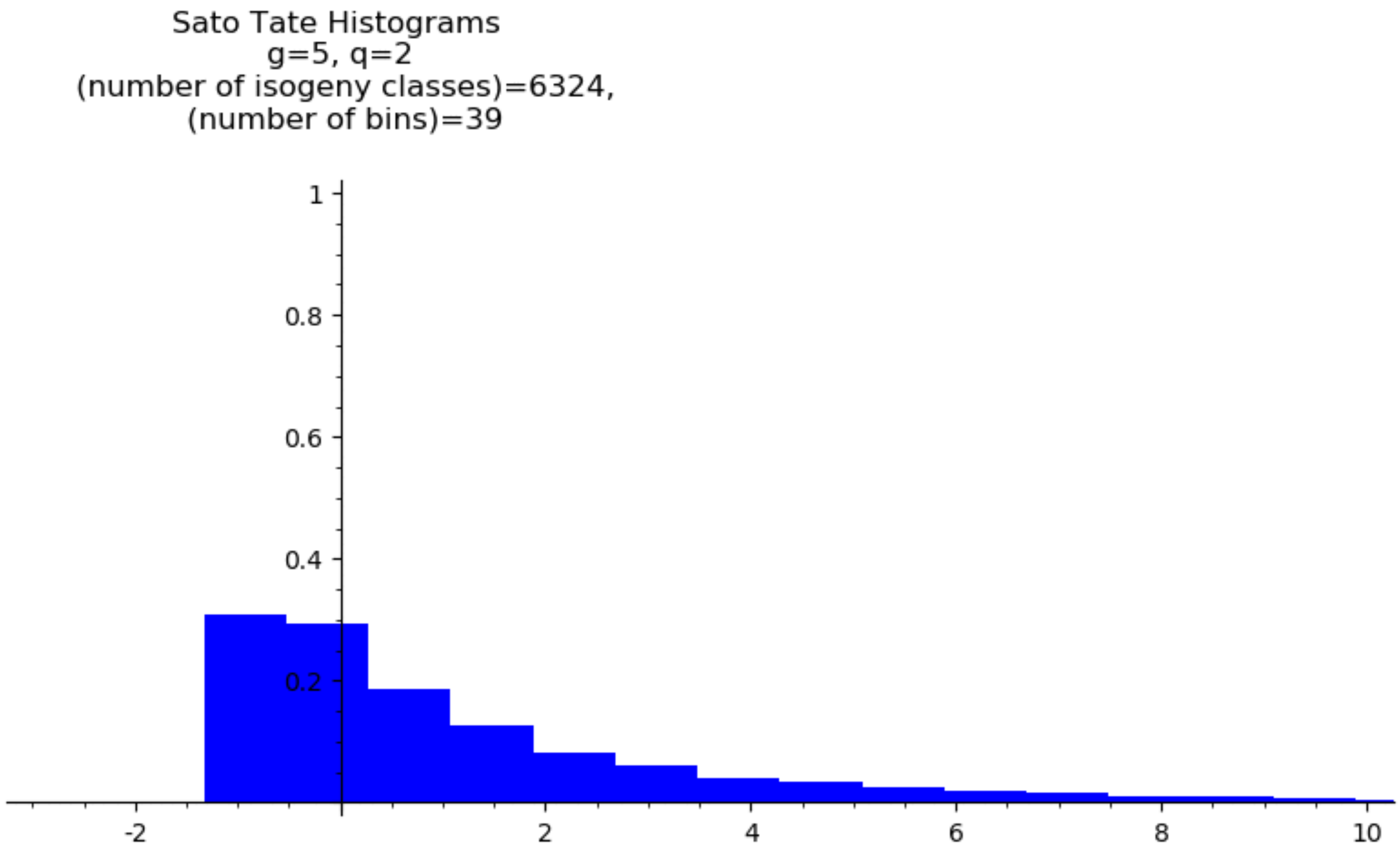
Moments: [1.07833784130949, 6.15234375000000, 38.0919251665952, 309.739672851563, 2860.44597199945]

Isog Classes, g=4



Moments: [1.10359165492329, 7.93043937969925, 68.3729049710662, 822.778373087259, 11831.8423819417]

Isog Classes, g=5



Moments: [1.36721008148421, 10.7234382412239, 110.639910824874, 1580.18394625843, 27431.1587237160]

QUESTIONS

- How do we tabulate all of the Weil polys?
- How many isogeny classes did we compute?
- What is this Ahmadi-Shparlinski conjecture you guys disproved?
- What are the arithmetic statistics for these Weil poly?

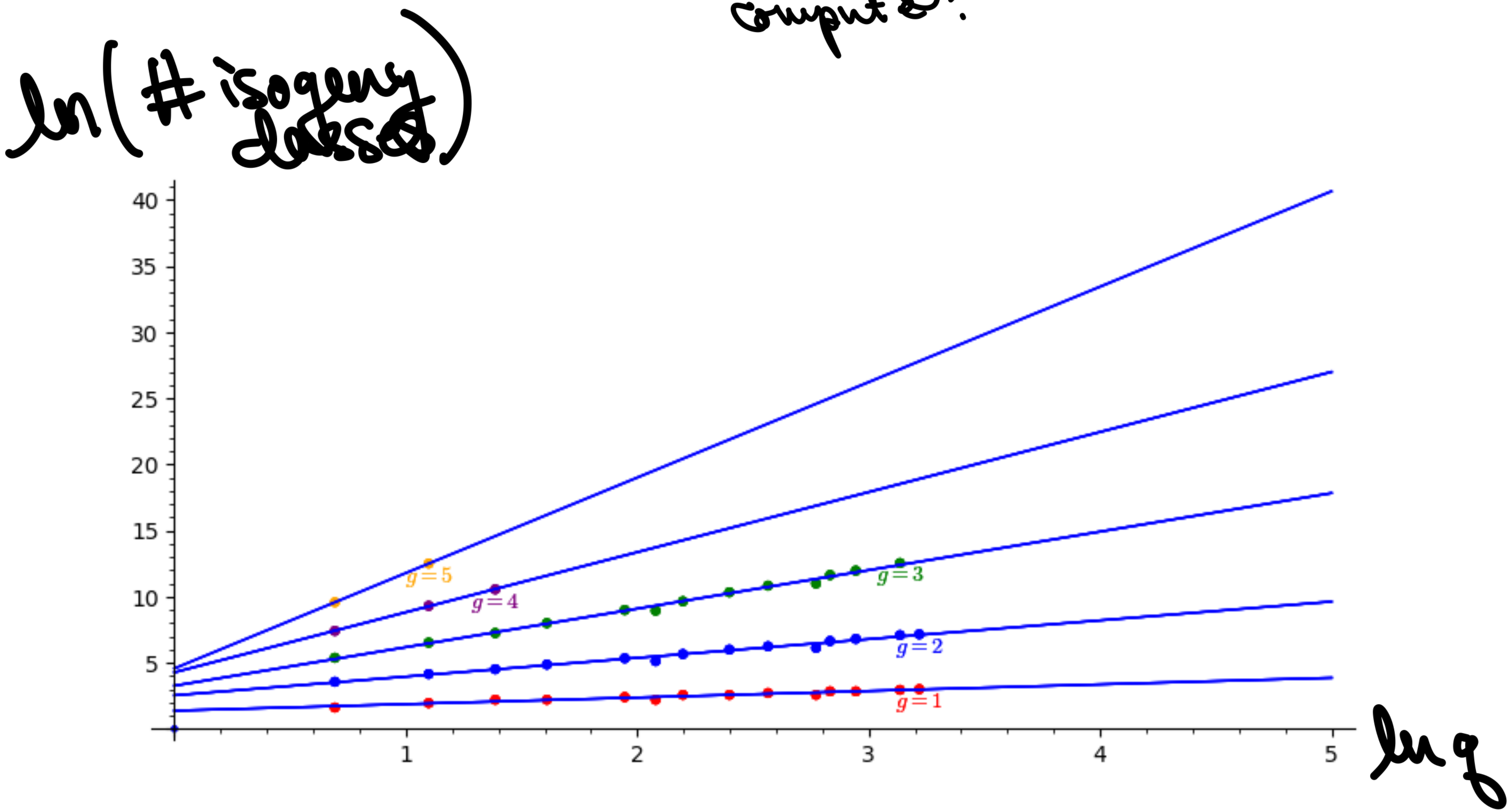
- How many isogeny classes did we compute?

$$N(g,q) = \#\{\text{Isog classes, dim} = g, /\mathbb{F}_q\}$$

- How many isogeny classes did we compute?

g	max q	num isog classes
1	503	6184
2	223	1253897
3	27	1055307
4	7	183607
5	4	281790
6	3	164937

- How many isogeny classes did we compute?



- How many isogeny classes did we compute?

$$N(g,q) = \#\{\text{Isog classes, dim} = g, /\mathbb{F}_q\}$$

Theorem (DiPippo–Howe)

$$N(g,q) \approx \left(\frac{2^g}{g!} \prod_{i=1}^{g} \left(\frac{2i}{2i-1}\right)^{g+1-i} \right) q^{g(g+1)/4}$$

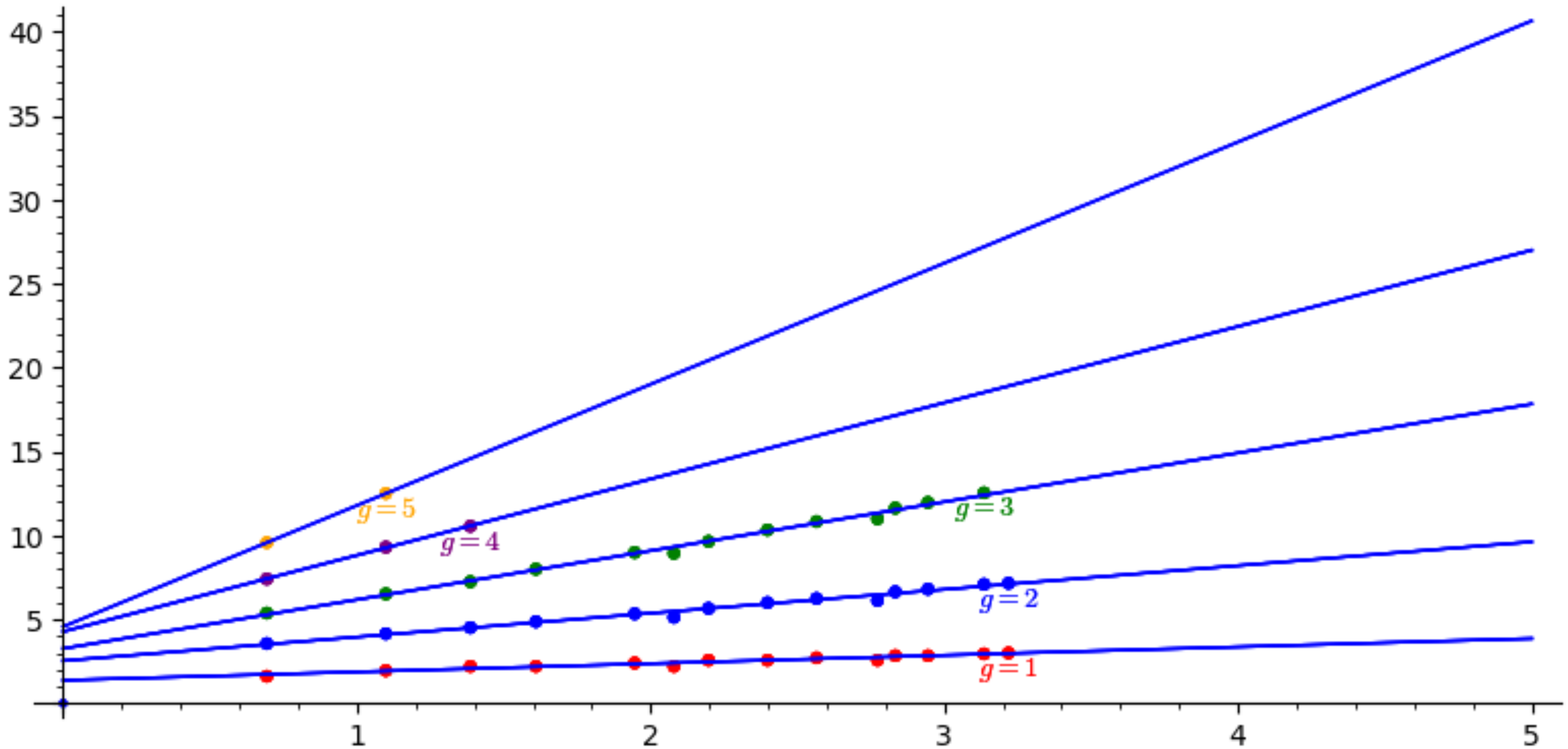
- How many isogeny classes did we compute?

		Ordinary		Arbitrary	
g	q	Predicted	Actual	Predicted	Actual
3	25	284444	284740	355556	332166
4	5	104025	105600	130032	132839
5	3	170796	171180	256194	267465
6	2	72362	74122	144724	164937

Table 1: Predicted versus actual values for the number of isogeny classes of ordinary/arbitrary abelian varieties of dimension g over $\mathbb{F}_q$.

• How many isogeny classes did we compute?

ln(# isogeny classes)



ln q

- How many isogeny classes did we compute?

	a		b	
g	Predicted	Actual	Predicted	Actual
1	0.5	0.4971	1.3863	1.3717
2	1.5	1.4178	2.3671	2.5302
3	3	2.9135	3.1248	3.2598
4	5	4.5452	3.7283	4.2707
5	7.5	7.2188	4.2141	4.5660

Table 1: Predicted versus actual (least squares) values for the equation $\log N(g,q) = a\log(q) + b$.

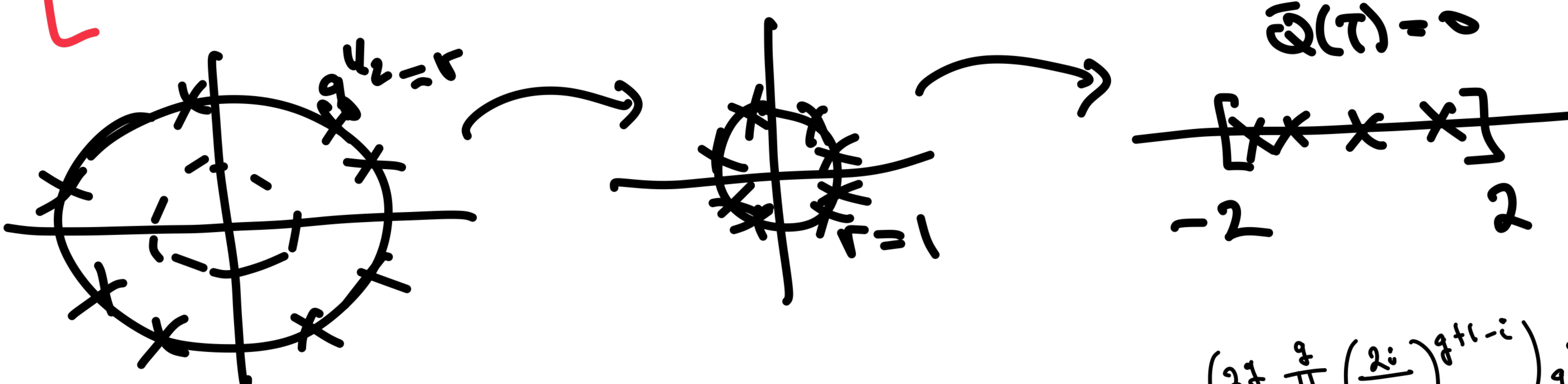
Step 1: Reduce to Root Unitary

- How many isogeny classes did we compute?

$$P(T) \rightsquigarrow \bar{P}(T) := P(q^{1/2}T)$$

Step 2: Reduce to Real Root Case

$$\bar{P}(T) = T^g \bar{Q}(T + 1/T) \rightsquigarrow \bar{Q}(T)$$



$$N(g,q) \approx \left(\frac{2^g}{g!}\prod_{i=1}^{g}\left(\frac{2i}{2i-1}\right)^{g+1-i}\right) q^{g(g+1)/4}$$

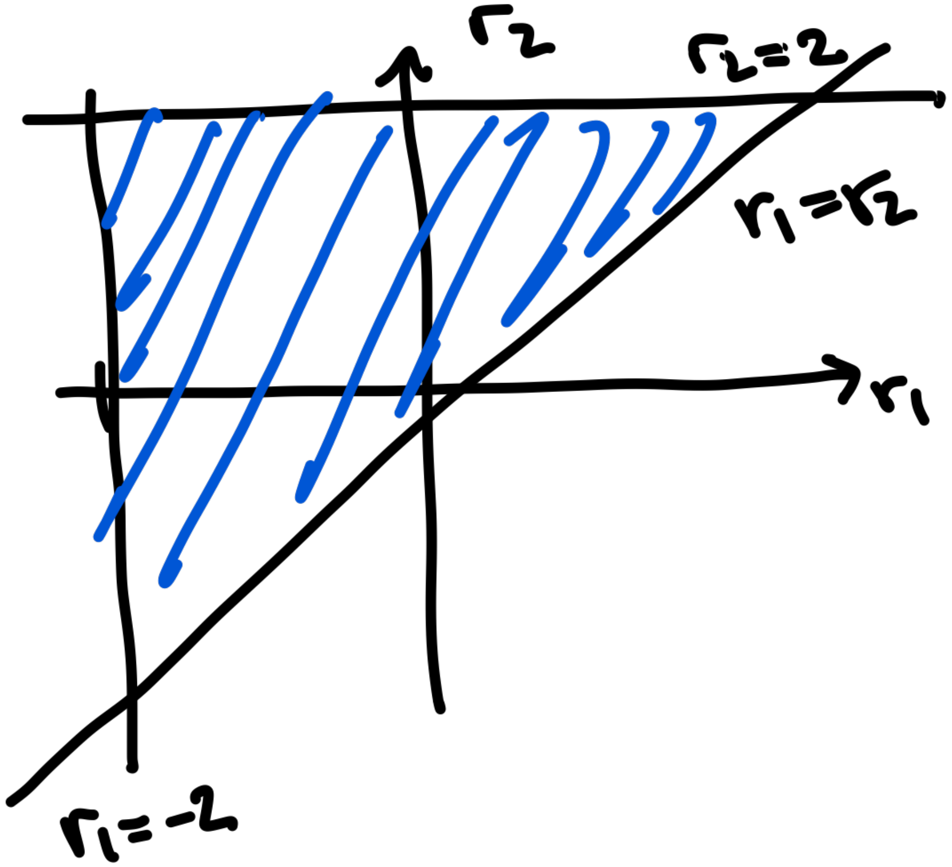
- How many isogeny classes did we compute?

$$N(g,q) \approx \left(\frac{2^g}{g!} \prod_{i=1}^{g} \left(\frac{2i}{2i-1} \right)^{g+1-i} \right) q^{g(g+1)/4}$$

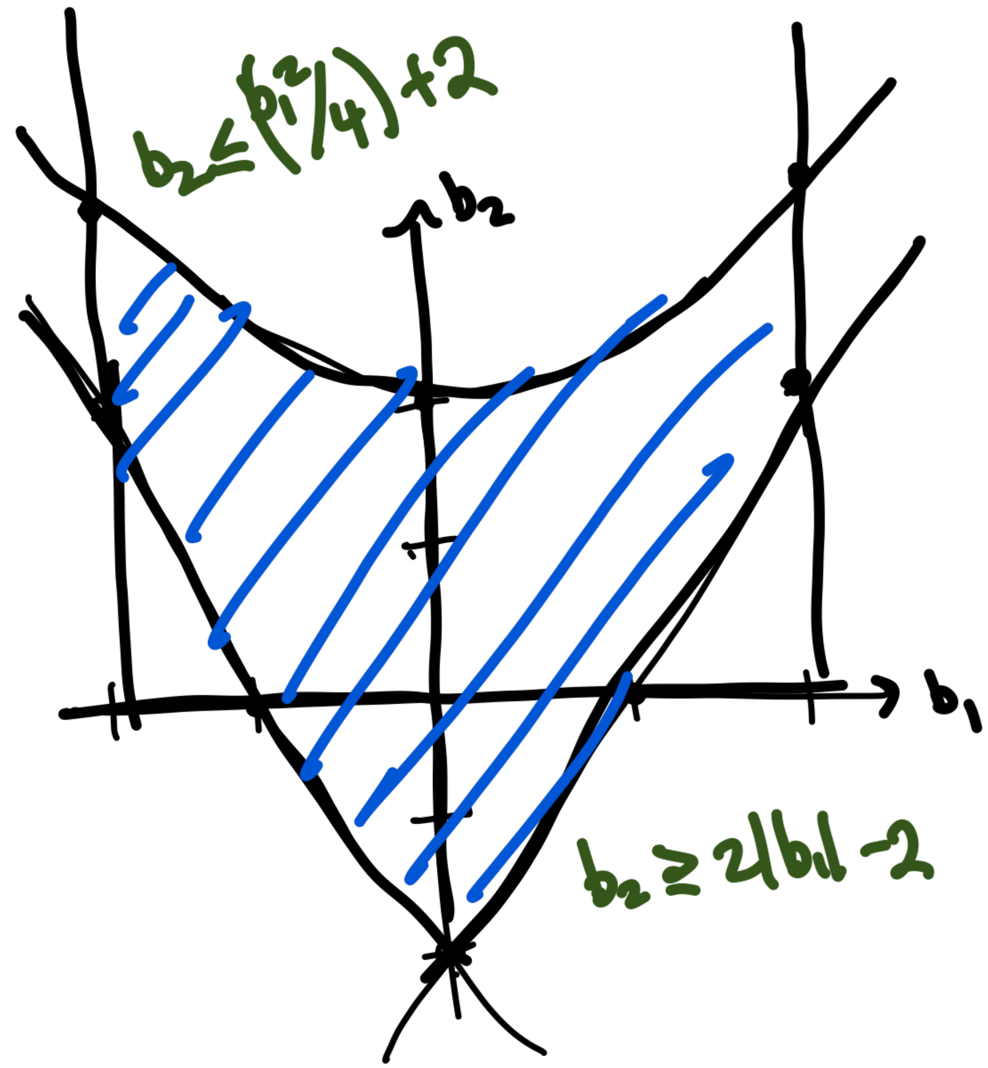
Approximate By Volume.

$$V_n = \{(a_1,\dots,a_g)\in\mathbb{R}^g \mid T^g + a_1T^{g-1}+\dots+a_g \text{ has roots in } [-2,2]\}$$

$$I_n = \{(r_1,\dots,r_g) : -2\le r_1\le \dots \le r_g \le 2\}$$

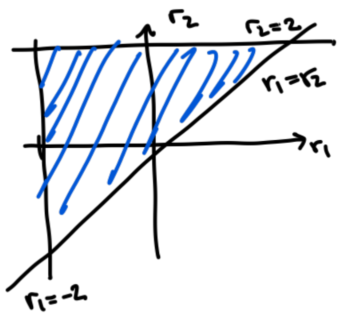


$\xrightarrow{\varphi}$

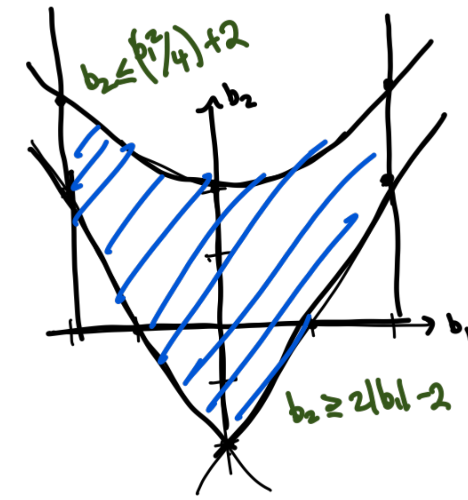


$$(r_1,r_2) \overset{\varphi}{\longmapsto} (b_1,b_2) = (-r_1-r_2,\ r_1r_2+2)$$

$$N(g,q) \approx \left(\frac{2^g}{g!}\prod_{i=1}^{g}\left(\frac{2i}{2i-1}\right)^{g+1-i}\right) q^{g(g+1)/4}$$



roots $\longmapsto$ poly with those roots



$\longleftrightarrow$ root unitary poly with those roots as traces

$\longleftrightarrow$ explicit expression only keeping track of half of coord.

$$N(g,q) \approx \left(\frac{2^g}{g!} \prod_{i=1}^{g} \left(\frac{2i}{2i-1}\right)^{g+1-i} \right) q^{g(g+1)/4}$$

$$\mathrm{vol}(V_g) = \int_{\varphi(I_n)} db_1 \cdots db_g$$

$$= \int_{I_n} |\det \varphi'| \, dr_1 \cdots dr_g$$

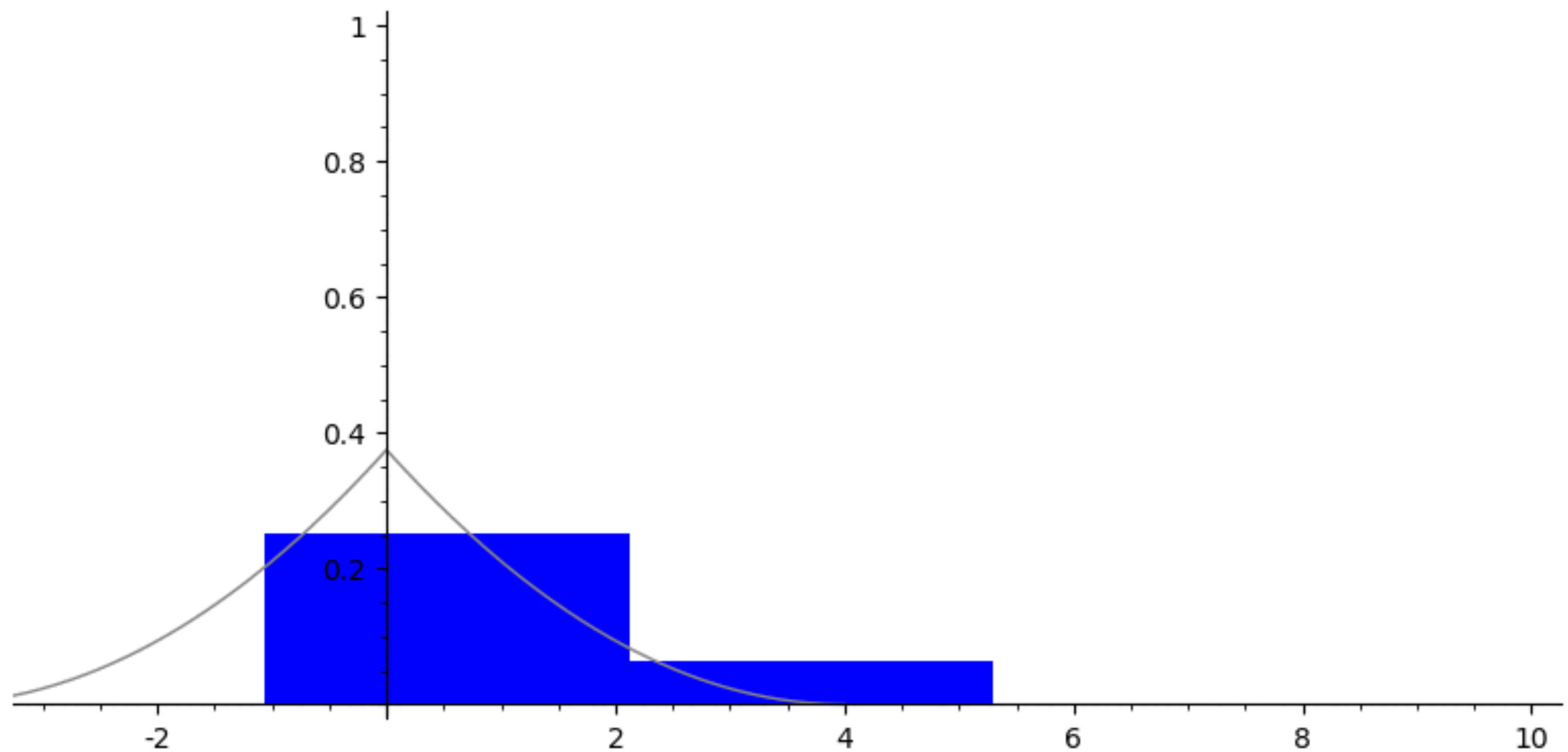
Vandermonde-like matrix

$$= \frac{1}{g!} \int_{I_n} \mathrm{Van}(r_1, \ldots, r_g) \, dr_1 \cdots dr_g$$

$$= \left(\frac{2g}{g!} \prod_{i=1}^{g} \left(\frac{2i}{2i-1} \right)^{g+1-i} \right) g^{g(g+1)/4}$$

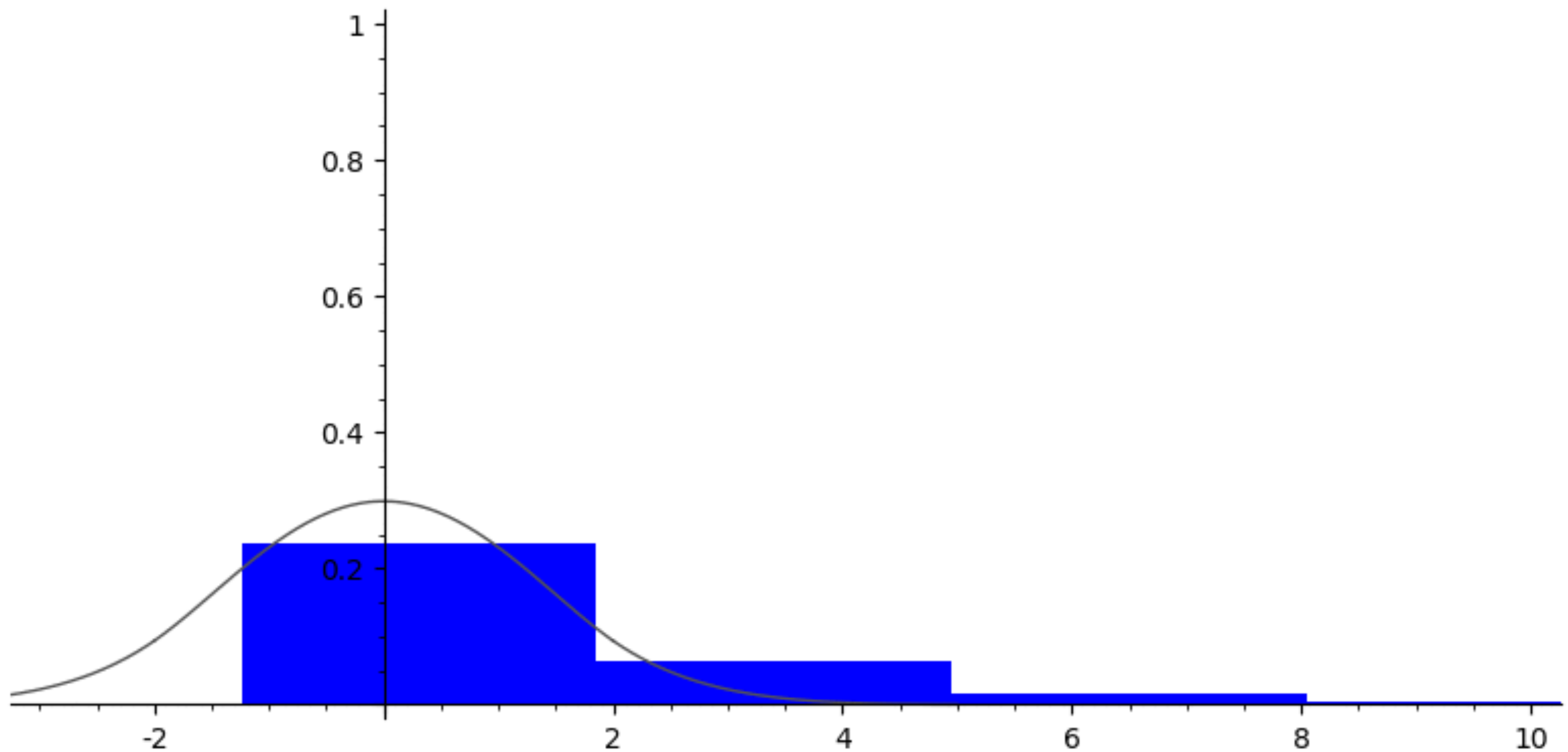
Not-o-Tate Distributions
come from "slicing"

Sato Tate Histograms
g=2, q=2
(number of isogeny classes)=20,
(number of bins)=2



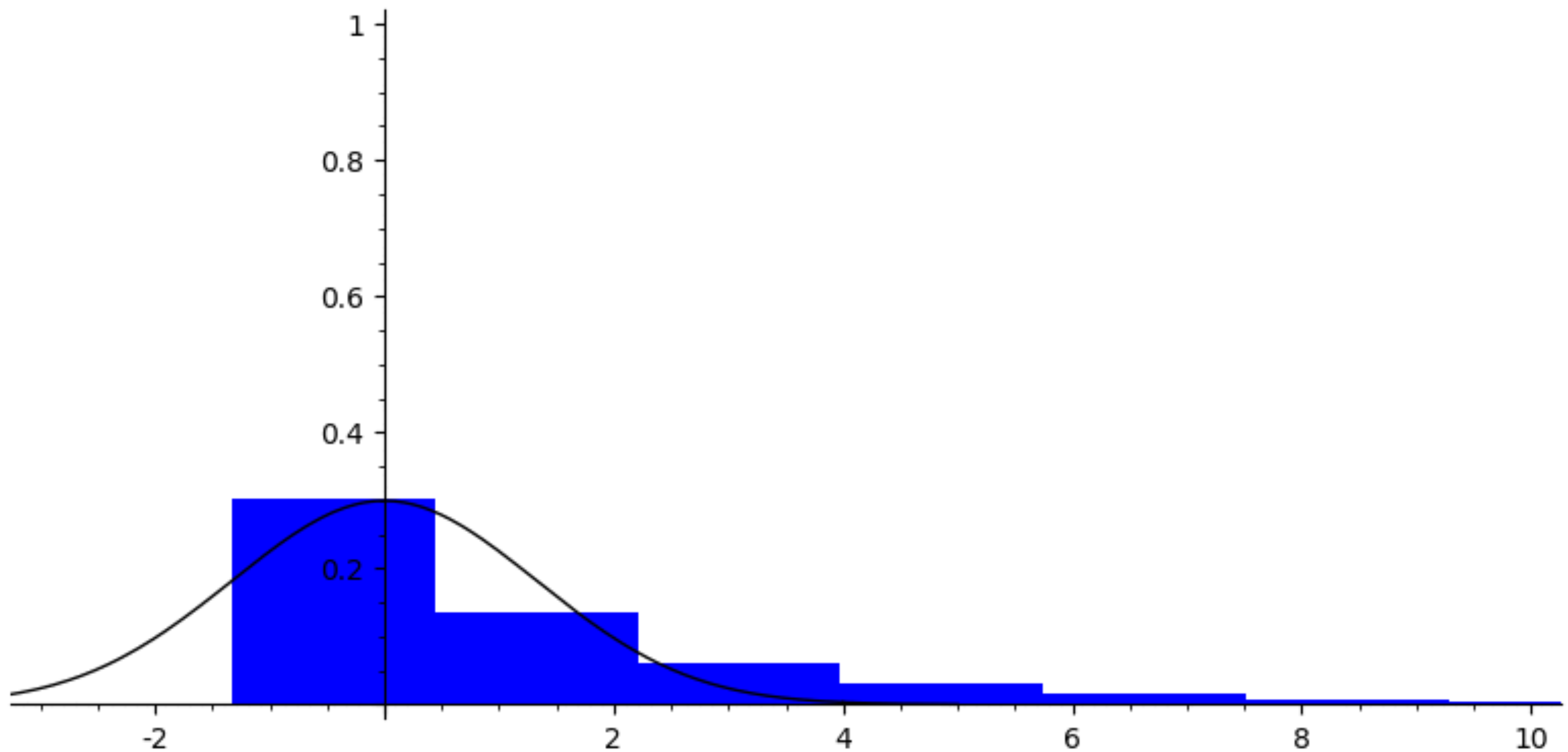
Moments: [0.689429111656884, 3.55625000000000, 12.2970288665723, 55.4851562500000, 259.317325107260]

Sato Tate Histograms
g=3, q=2
(number of isogeny classes)=80,
(number of bins)=4



Moments: [1.07833784130949, 6.15234375000000, 38.0919251665952, 309.739672851563, 2860.44597199945]

Sato Tate Histograms
g=4, q=2
(number of isogeny classes)=665,
(number of bins)=12



Moments: [1.10359165492329, 7.93043937969925, 68.3729049710662, 822.778373087259, 11831.8423819417]

Formulas for Not-o-Tate

$$g = 1 : \begin{cases} \frac{1}{4} & |x| \leq 2 \\ 0 & |x| > 2 \end{cases}$$

$$g = 2 : \begin{cases} \frac{3}{2^7}(4 - |x|)^2 & (|x| \leq 4) \\ 0 & (|x| > 4) \end{cases}$$

$$g = 3 : \begin{cases} \frac{3}{2^{13}}(15|x|^4 - 200|x|^2 + 816) & (|x| \leq 2) \\ \frac{3}{2^{15}}(6 - |x|)^5 & (2 < |x| \leq 6) \\ 0 & (|x| > 6) \end{cases}$$

$$g = 4 : \begin{cases} \frac{5(-|x|^9 - 72|x|^8 - 2304|x|^7 + 64512|x|^6 - 516096|x|^5 + 1548288|x|^4 - 7077888|x|^2 + 24117248)}{2^{30}} & |x| \leq 4 \\ \frac{5}{2^{30}}(8 - |x|)^9 & (4 < |x| \leq 8) \\ 0 & (|x| > 8). \end{cases}$$

g	2nd	4th	6th	8th	10th	12th	14th
3	1.7142	8.6857	71.7575	796.1318	10750.4655	166954.5839	2.8786×10^6
4	1.7777	9.4199	82.5201	1001.4566	15384.2906	282674.8553	5.9748×10^6
5	1.8181	9.8834	89.1908	1121.6573	18035.9973	351973.2932	8.0435×10^6
6	1.8461	10.2041	93.7929	1203.9623	19814.7906	397315.2698	9.3803×10^6

Table 1: Even moments for the Sato-Ain't distributions for $g = 3, 4, 5, 6$.

QUESTIONS

- How do we tabulate all of the Weil polys?
- How many isogeny classes did we compute?
- What is this Ahmadi-Shparlinski conjecture you guys disproved?
- What are the arithmetic statistics for these Weil poly?

- What is this Ahmadi-Shparlinski conjecture you guys disproved?

$$\delta = \dim_{\mathbb{Q}}\left(\operatorname{span}_{\mathbb{Q}}\left\{\frac{\operatorname{Arg}(\alpha_i)}{2\pi} ; 1 \le i \le N\right\} \vee \{1\}\right) - 1$$

Angle Rank

Principal branch

$$\delta = \dim_{\mathbb{Q}}\left(\operatorname{span}_{\mathbb{Q}}\left\{\frac{\operatorname{Arg}(\alpha_i)}{2\pi} ; 1 \le i \le N\right\} \vee \{1\}\right) - 1$$

Basics:

- $\overline{\alpha_i} = q/\alpha_i$, also root $\Rightarrow \delta(A) \le \frac{2g}{2} = g$
- A supersingular $\left(\Longleftrightarrow \frac{\operatorname{ord}(\alpha_i)}{\operatorname{ord}(q)} = \frac{1}{2} \text{ for all } i\right)$

  $\Longleftrightarrow \alpha_i = q^{1/2} \zeta$

  root of 1

- $\delta(A_{\mathbb{F}_q}) = \delta(A_{\mathbb{F}_{q^r}})$

  invariant under base change.

$$\delta(A_{\mathbb{F}_q}) = \delta(A_{\mathbb{F}_{q^r}})$$

<u>proof</u>;

$$P_A(T) = (T-\alpha_1)(T-\alpha_2)\cdots(T-\alpha_{2g})$$

$$P_{A_{\mathbb{F}_{q^r}}}(T) = (T-\alpha_1^r)(T-\alpha_2^r)\cdots(T-\alpha_{2g}^r)$$

$$\delta = \dim_{\mathbb{Q}}\left(\operatorname{span}_{\mathbb{Q}}\left\{\frac{\operatorname{Arg}(\alpha_i)}{2\pi}\,;\, 1 \le i \le N\right\} \vee \{1\}\right) - 1$$

<u>Basics:</u>

- $\overline{\alpha_i} = q/\alpha_i$, also root $\Longrightarrow \delta(A) \le \frac{2g}{2} = g$
- A supersingular $\left(\Longleftrightarrow \frac{\operatorname{ord}(\alpha_i)}{\operatorname{ord}(q)} = \frac{1}{2} \text{ for all } i \right)$

  $\Longleftrightarrow \alpha_i = q^{1/2}\zeta$

  root of 1

- $\delta(A_{\mathbb{F}_q}) = \delta(A_{\mathbb{F}_{q^r}})$

  invariant under base change.

$$\delta = \dim_{\mathbb{Q}}\left(\mathrm{span}_{\mathbb{Q}} \left\{ \frac{\mathrm{Arg}(\alpha_i)}{2\pi} \; ; \; 1 \le i \le N \right\} \cup \{1\} \right) - 1$$

Conjecture (Ahmadi–Shparlinski)

$A = \mathrm{Jac}\, X / \mathbb{F}_q$ ordinary geometrically simple $\Longrightarrow$ $\delta(A) = g$

False

Conjecture (Ahmadi-Shparlinski)

False

Conjecture (Ahmadi-Shparlinski)

$C/\mathbb{F}_3$ hyperelliptic, $g=4$

$$y^2 = x^9 + x^8 + x^7 + 2x^5 + x$$

4.3.ab_e_ae_ac

$$L(C/\mathbb{F}_3, T) = 1 - T + 2T^2 - 4T^3 - 2T^4 - 12T^5 + 18T^6 - 27T^7 + 81T^8$$

$$P(T) = (T-\alpha_1)(T-\alpha_2)(T-\alpha_3)(T-\alpha_4)(T-\alpha_5)(T-\alpha_6) \cdot (T-\alpha_7)(T-\alpha_8)$$

$$P(T) = (T-\alpha_1)(T-\alpha_2)(T-\alpha_3)(T-\alpha_4)(T-\alpha_5)(T-\alpha_6)$$
$$\cdot (T-\alpha_7)(T-\alpha_8)$$

$$\frac{\alpha_1}{\alpha_2 \alpha_3 \alpha_4} = \frac{-1}{3}$$

non-conj roots.

4.3. ab_e_ae_ac

THANK YOU!

Primitive Element Polynomial For Splitting Field

$$
\begin{aligned}
x^{48} &- 12\,x^{47} + 126\,x^{46} - 1136\,x^{45} + 10623\,x^{44} - 80788\,x^{43} + 572972\,x^{42} - 3794180\,x^{41} \\
&+ 25110359\,x^{40} - 150754924\,x^{39} + 864296430\,x^{38} - 4608220388\,x^{37} + 24630124727\,x^{36} \\
&- 120357179236\,x^{35} + 544218581694\,x^{34} - 1976498403408\,x^{33} + 6175583306542\,x^{32} \\
&- 11748946994864\,x^{31} - 25953303296718\,x^{30} + 658025272943440\,x^{29} - 4918263858685364\,x^{28} \\
&+ 27257734674932420\,x^{27} - 118028134817669378\,x^{26} + 474022673382364964\,x^{25} \\
&- 1432580743005391943\,x^{24} + 3158573611513583112\,x^{23} + 2911135044988486 44\,x^{22} \\
&- 2894885178838514033 2\,x^{21} + 250066543986644814756\,x^{20} - 1032538101324173545784\,x^{19} \\
&+ 4433828273954846081182\,x^{18} - 13741075467595938086308\,x^{17} + 58230819876836241546592\,x^{16} \\
&- 149204830396162560632528\,x^{15} + 367825526639876473987746\,x^{14} - 641204821805389714820452\,x^{13} \\
&+ 341540521573270425663392 2\,x^{12} - 1151430732725949462860399 6\,x^{11} + 1719601454577608974886520 0\,x^{10} \\
&- 11607867051263915093257704\,x^{9} + 63896590907239331589164012\,x^{8} - 39088201039540271237475581 2\,x^{7} \\
&+ 13836130258123308731867154 0\,x^{6} + 58981913387870804608259748 8\,x^{5} \\
&+ 23286683232119198731566244 13\,x^{4} - 35010634631456615433165328 16\,x^{3} \\
&- 46921466766642043757855307 94\,x^{2} + 41965623779588954001569107 84\,x \\
&+ 8236204150604868555410746909
\end{aligned}
$$

Zarhin 1994:

$\delta(A) = g \iff$ no exceptional Hodge classes on products

- Tate class = element of $H^{2i}_\ell(X)(i)^G$

- <u>exceptionality</u>: $\eta \in H^{2i}_\ell(X)(i)$ <u>exceptional</u>

$\iff \eta \notin \mathrm{Span}\{$Hodge classes of wt 2$\}$.

- Tate class = element of $H^{2c}_\ell(X)(c)^G$

- Cycle Class Map:

$$\begin{aligned} A^c(X) &\longrightarrow H^{2c}_\ell(X)(c)^G \\ [Z] &\longmapsto cl(Z) \end{aligned}$$

- <u>Tate Conjecture</u>:

  Tate classes spanned by images of cl (using cup product)

???

Angle Rank

- Hodge class = element of $H^{2e}_{\ell}(X)(\mathbb{C})^G$

Basic Idea:

δ small $\rightsquigarrow$ $\dfrac{\alpha_1}{\alpha_2^{3}}\alpha_4$ = root of unity

$\rightsquigarrow$ comes from eigenvectors

(Tate class!)