Biases in Second Moments of Elliptic Curves

Zoë Batterman (zxba2020@mymail.pomona.edu)
Aditya Jambhale (aj644@cam.ac.uk)
Akash L. Narayanan (anaray@umich.edu)
Chris Yao (chris.yao@yale.edu)

(joint with Kishan Sharma and Andrew Yang)

Advisor: Steven J. Miller
SMALL REU at Williams College

2023 Maine-Québec Number Theory Conference

September 30, 2023

Outline

- Moments of Elliptic Curves
- Bias Conjecture
- Explicit Formulas
- Second Moments of $\mathcal{F} : y^2 = x^3 + x + t^3$
- First Moments of $\mathcal{F} : y^2 = x^3 + x + t^3$

A *one-parameter family* of elliptic curves is given by

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

where $A(T)$, $B(T)$ are polynomials in $\mathbb{Z}[T]$.
Each specialization of T to an integer t gives an elliptic curve E_t over $\mathbb{Q}$.

A *one-parameter family* of elliptic curves is given by

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

where $A(T)$, $B(T)$ are polynomials in $\mathbb{Z}[T]$.
Each specialization of T to an integer t gives an elliptic curve E_t over $\mathbb{Q}$.

Moments of a family of elliptic curves

The r^{th} moment (note we do not normalize by $1/p$) is

$$\mathcal{A}_{r,\mathcal{E}}(p) \ = \ \sum_{t(p)} a_{E_t}(p)^r,$$

where $a_{\mathcal{E}(t)}(p) = p + 1 - \#(\text{solutions to } E_t \bmod p)$ is the Frobenius trace of E_t.

The first moment is related to the rank of the elliptic curve family:

$\mathcal{A}_{1,\mathcal{E}}(p)$ and Family Rank (Nagao, Rosen-Silverman, 1998)

Given certain technical assumptions (Tate's Conjecture) hold for $\mathcal{E}$, then

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

Negative Bias in the First Moment

The first moment is related to the rank of the elliptic curve family:

$\mathcal{A}_{1,\mathcal{E}}(p)$ and Family Rank (Nagao, Rosen-Silverman, 1998)

Given certain technical assumptions (Tate's Conjecture) hold for $\mathcal{E}$, then

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

- By the fact $\sum_{p\leq x} \log p \sim x$, if $\mathcal{A}_{1,\mathcal{E}}(p) = -rp + O(1)$, then $\operatorname{rank} \mathcal{E}(\mathbb{Q}(t)) = r$.

The first moment is related to the rank of the elliptic curve family:

$\mathcal{A}_{1,\mathcal{E}}(p)$ and Family Rank (Nagao, Rosen-Silverman, 1998)

Given certain technical assumptions (Tate's Conjecture) hold for $\mathcal{E}$, then

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

- By the fact $\sum_{p \le x} \log p \sim x$, if $\mathcal{A}_{1,\mathcal{E}}(p) = -rp + O(1)$, then $\operatorname{rank} \mathcal{E}(\mathbb{Q}(t)) = r$.
- The "rank" of the family means that except for finitely many t, the elliptic curve E_t has rank greater or equal to r.

- Moments of Elliptic Curves
- Bias Conjecture
- Explicit Formulas
- Second Moments of $\mathcal{F} : y^2 = x^3 + x + t^3$
- First Moments of $\mathcal{F} : y^2 = x^3 + x + t^3$

The $j(T)$-invariant is $j(T) = 1728\frac{4A(T)^3}{4A(T)^3+27B(T)^2}$.

Second Moment Asymptotic (Michel, 1995)

For an elliptic surface $\mathcal{E}$ with $j(T)$-invariant non-constant, the second moment is

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

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

The $j(T)$-invariant is $j(T) = 1728\frac{4A(T)^3}{4A(T)^3+27B(T)^2}$.

Second Moment Asymptotic (Michel, 1995)

For an elliptic surface $\mathcal{E}$ with $j(T)$-invariant non-constant, the second moment is

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

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

Strong and Weak Bias Conjectures (Miller)

- **Weak:** The largest lower term in the second moment expansion which does not average to 0 is on average **negative**.
- **Strong:** The largest lower term in the second moment expansion which does not average to 0 is **negative except for finitely many** p**.**

Relation with Excess Rank

- If we have lower order negative bias, then the bound for the average rank in families increases.

Relation with Excess Rank

- If we have lower order negative bias, then the bound for the average rank in families increases.
- However, lower order negative biases increases bound only by a small amount, which is not enough to explain observed excess rank.

Outline

- Moments of Elliptic Curves
- Bias Conjecture
- Explicit Formulas
- Second Moments of $\mathcal{F} : y^2 = x^3 + x + t^3$
- First Moments of $\mathcal{F} : y^2 = x^3 + x + t^3$

For a specialization of the one-parameter family $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$, we may write

$$a_{E_t}(p) = -\sum_{x(p)} \left(\frac{x^3 + A(t)x + B(t)}{p} \right)$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol mod p given by

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & x \text{ a non-zero square modulo } p, \\ 0 & x \equiv 0 \mod p, \\ -1 & \text{otherwise.} \end{cases}$$

For a specialization of the one-parameter family $\mathcal{E} : y^2 \;=\; x^3 + A(T)x + B(T)$, we may write

$$a_{E_t}(p) \;=\; -\sum_{x(p)} \left(\frac{x^3 + A(t)x + B(t)}{p} \right)$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol mod p given by

$$\left(\frac{x}{p}\right) \;=\; \begin{cases} 1 & x \text{ a non-zero square modulo } p, \\ 0 & x \equiv 0 \mod p, \\ -1 & \text{otherwise.} \end{cases}$$

Observe that $\left(\dfrac{x}{p}\right) + 1$ is precisely the number of solutions to $x = y^2 \pmod{p}$.

Linear and quadratic Legendre sums

We have the following

$$\sum_{x(p)} \left(\frac{ax+b}{p}\right) = 0 \qquad p \nmid a,$$

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

Linear and quadratic Legendre sums

We have the following

$$\sum_{x(p)} \left(\frac{ax+b}{p}\right) = 0 \qquad p \nmid a,$$

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

Average values of Legendre symbols

Taking the limit of the average of the Legendre symbol over all primes gives

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\le x} \left(\frac{x}{p}\right) = \begin{cases} 1 & x \text{ a non-zero square}, \\ 0 & \text{otherwise}. \end{cases}$$

- The moments become intractible when $A(T)$ and $B(T)$ have high degree.
- For the following special families, the following is known:

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

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

- Moments of Elliptic Curves
- Bias Conjecture
- Explicit Formulas
- Second Moments of $\mathcal{F} : y^2 = x^3 + x + t^3$
- First Moments of $\mathcal{F} : y^2 = x^3 + x + t^3$

- We computationally evaluated second moments of various families of elliptic curves.
- By Michel's theorem, we assume that

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

where $\alpha(p)$ and $\beta(p)$ are $O(1)$. To investigate the $\alpha(p)$ coefficient, we graphed the *bias* of the second moment.

- We computationally evaluated second moments of various families of elliptic curves.
- By Michel's theorem, we assume that

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

where $\alpha(p)$ and $\beta(p)$ are $O(1)$. To investigate the $\alpha(p)$ coefficient, we graphed the *bias* of the second moment.

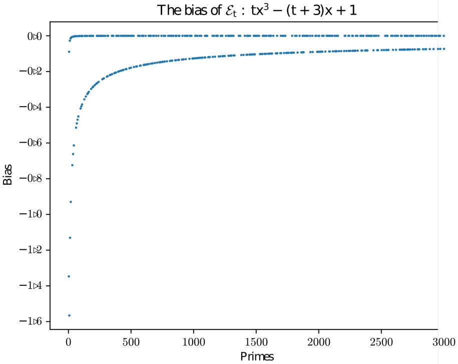
Bias

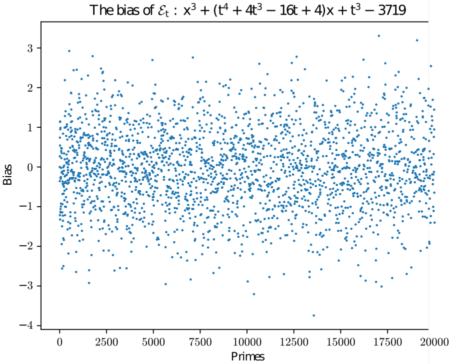
We compute the *bias* of $\mathcal{A}_{2,\mathcal{E}}$ defined by

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

Graphs of Biases

Here are two examples for the graph of the biases, one for a tractable family, and one for not





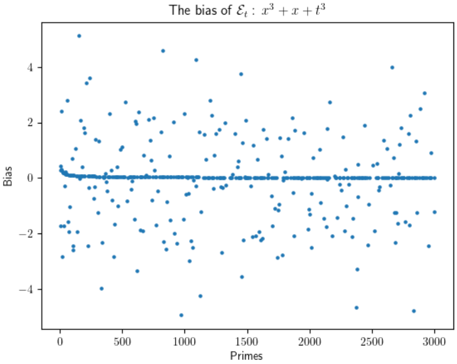
Eventually, we found the family

$$\mathcal{F} : y^2 \ = \ x^3 + x + T^3.$$

Eventually, we found the family

$$\mathcal{F} : y^2 \;=\; x^3 + x + T^3.$$

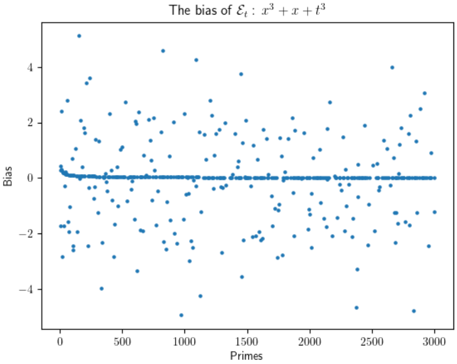
Our reason for suspecting this family was the graph of the bias:



Eventually, we found the family

$$\mathcal{F} : y^2 \; = \; x^3 + x + T^3.$$

Our reason for suspecting this family was the graph of the bias:



The graph indicates a clear line where the bias is positive, compared to the graphs in the previous slides.

Consider the family

$$\mathcal{F}\colon y^2 \;=\; x^3 + x + T^3.$$

Notice for primes p such that $3 \nmid p$, we have $T \mapsto T^3$ a bijection.

Consider the family

$$\mathcal{F}\colon y^2 \ = \ x^3 + x + T^3.$$

Notice for primes p such that $3 \nmid p$, we have $T \mapsto T^3$ a bijection.
So, we sample the simpler elliptic curve family

$$\widetilde{\mathcal{F}}\colon y^2 = x^3 + x + T$$

when $p \equiv 2(3)$, which is half of the primes!

Consider the family

$$\mathcal{F}\colon y^2 \;=\; x^3 + x + T^3.$$

Notice for primes p such that $3 \nmid p$, we have $T \mapsto T^3$ a bijection.
So, we sample the simpler elliptic curve family

$$\widetilde{\mathcal{F}}\colon y^2 = x^3 + x + T$$

when $p \equiv 2(3)$, which is half of the primes! This immediately gives us that for such primes,

$$\begin{aligned}
\mathcal{A}_{2,\mathcal{F}}(p) &= \sum_{t(p)} \sum_{x,y(p)} \left(\frac{x^3+x+t^3}{p}\right)\left(\frac{y^3+y+t^3}{p}\right) \\
&= \sum_{t(p)} \sum_{x,y(p)} \left(\frac{x^3+x+t}{p}\right)\left(\frac{y^3+y+t}{p}\right) \\
&= \mathcal{A}_{2,\widetilde{\mathcal{F}}}(p) \;=\; p^2 - \left(\frac{-3}{p}\right)p \;=\; p^2 + p.
\end{aligned}$$

Bias Revisited

We graph the *bias* of $\mathcal{A}_{2,\mathcal{E}}$, for calculated values, defined by

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

Recall by Michel's theorem, we have

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

where $\alpha(p)$ and $\beta(p)$ are $O(1)$. To disprove the bias conjectures, we would need to do two things:

Bias Revisited

We graph the *bias* of $\mathcal{A}_{2,\mathcal{E}}$, for calculated values, defined by

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

Recall by Michel's theorem, we have

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

where $\alpha(p)$ and $\beta(p)$ are $O(1)$. To disprove the bias conjectures, we would need to do two things:

- Show that $\alpha(p)$ averages to 0, i.e.,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} \alpha(p) = 0.$$

Bias Revisited

We graph the *bias* of $\mathcal{A}_{2,\mathcal{E}}$, for calculated values, defined by

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

Recall by Michel's theorem, we have

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

where $\alpha(p)$ and $\beta(p)$ are $O(1)$. To disprove the bias conjectures, we would need to do two things:

- Show that $\alpha(p)$ averages to 0, i.e.,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\le x} \alpha(p) = 0.$$

- Show that $\beta(p)$ averages to a positive number.

By the prime number theorem, one shows

$$\frac{1}{\pi(x)}\sum_{p\leq x}\alpha(p) \;=\; \frac{1}{\pi(x)}\sum_{p\leq x}\mathcal{B}_{\mathcal{E}}(p)+O(x^{-1/2}\log x)$$

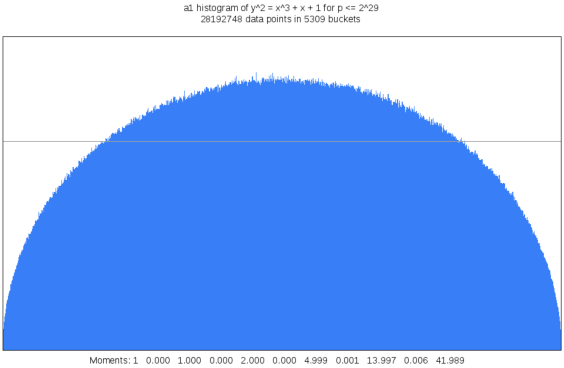
Problem: The constant in the big O term might dominate.

By the prime number theorem, one shows

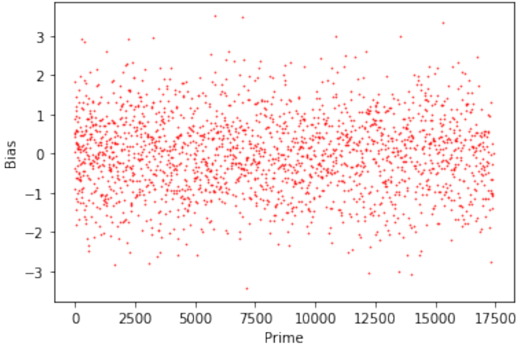
$$\frac{1}{\pi(x)}\sum_{p\leq x}\alpha(p) \;=\; \frac{1}{\pi(x)}\sum_{p\leq x}\mathcal{B}_{\mathcal{E}}(p)+O(x^{-1/2}\log x)$$

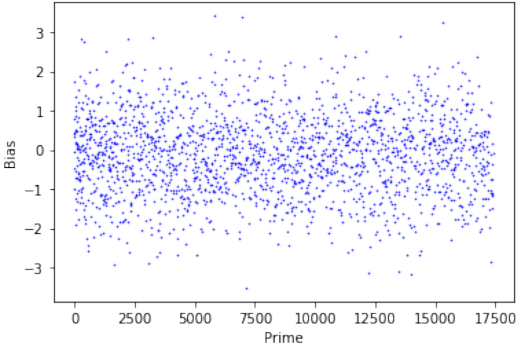
Problem: The constant in the big O term might dominate.

Solution: Randomly simulate elliptic moments using the *Sato-Tate distribution*.

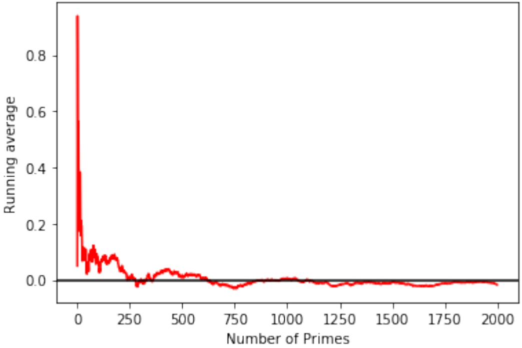


The following are two graphs which randomly simulate the bias.
One graph has coefficient $\alpha(p) = -.1$ and the other has $\alpha(p) = 0$.
Can you guess which is which?





Taking the running average of the biases, it is clear there is a bias:



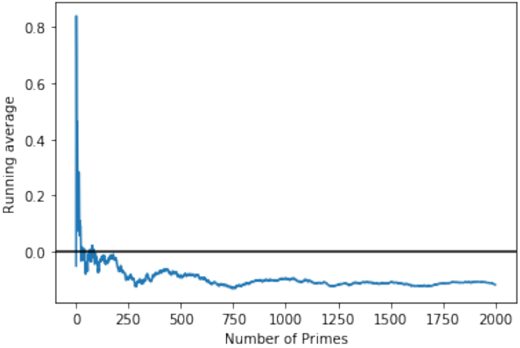
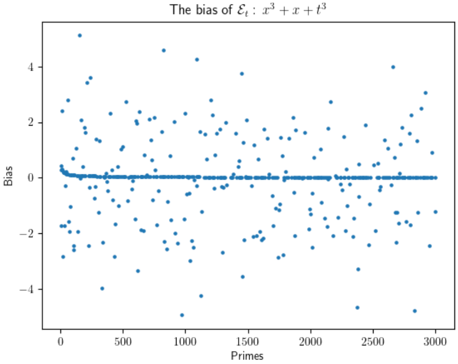
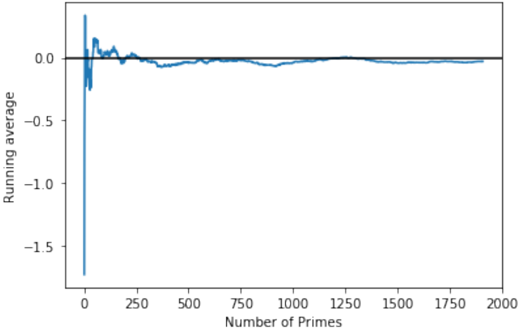


Figure: Unbiased Running Averages (Red) versus Biased Running Averages (Blue) for a random simulation

Computational Success!

Doing the same with our family of interest, that is, $y^2 = x^3 + x + t^3$, we get





So we have strong computational evidence the largest term averages to 0.

- Moments of Elliptic Curves
- Bias Conjecture
- Explicit Formulas
- Second Moments of $\mathcal{F} : y^2 = x^3 + x + t^3$
- First Moments of $\mathcal{F} : y^2 = x^3 + x + t^3$

Conjecture (First Moment of $y^2 = x^3 + x + t^3$)

The first moment $\mathcal{A}_{1,p}$ satisfies

$$|\mathcal{A}_{1,p}| = \begin{cases} 4p & p \text{ is of the form } a^2 + 36b^2, \\ 0 & \text{otherwise.} \end{cases}$$

Conjecture (First Moment of $y^2 = x^3 + x + t^3$)

The first moment $\mathcal{A}_{1,p}$ satisfies

$$|\mathcal{A}_{1,p}| = \begin{cases} 4p & p \text{ is of the form } a^2 + 36b^2, \\ 0 & \text{otherwise.} \end{cases}$$

For a prime $p \not\equiv 1(12)$, the Chinese remainder theorem in conjunction with the changes of variable yields

$$t \mapsto tx, \quad \text{and} \quad t \mapsto t^3 \implies \mathcal{A}_{1,p} = 0.$$

Conjecture (First Moment of $y^2 = x^3 + x + t^3$)

The first moment $\mathcal{A}_{1,p}$ satisfies

$$|\mathcal{A}_{1,p}| = \begin{cases} 4p & p \text{ is of the form } a^2 + 36b^2, \\ 0 & \text{otherwise.} \end{cases}$$

For a prime $p \not\equiv 1(12)$, the Chinese remainder theorem in conjunction with the changes of variable yields

$$t \mapsto tx, \quad \text{and} \quad t \mapsto t^3 \implies \mathcal{A}_{1,p} = 0.$$

Using binary quadratic forms, $\mathcal{A}_{1,p} \neq 0$ forces p to be of the form

$$p = a^2 + 36b^2 \quad \text{or} \quad p = 4a^2 + 9b^2.$$

We have evidence for $|\mathcal{A}_{1,p}| = 4p$ in the former and $\mathcal{A}_{1,p} = 0$ in the latter.

Acknowledgements

Special thanks to Professor Steven J. Miller and the Churchill Foundation.

Thanks to our SMALL 2023 faculty, research assistants, and peers for their support.

Thanks to the National Science Foundation for making SMALL 2023 possible.