Lower Order Biases in Fourier Coefficients of Elliptic Curve and Cuspidal Newform families

Jared D. Lichtman & Jianing Yang
jared.d.lichtman.18@dartmouth.edu, jyang@colby.edu
with Ryan Chen, Yujin H. Kim & Eric Winsor
Advisor: Steven J. Miller

SMALL REU 2017 at Williams College

Elliptic Curve Groups Over Fields

Elliptic Curve Groups Over Fields

Definition

Given a field K with characteristic neither 2 nor 3, an **elliptic curve** $E(K)$ is the set

$$E(K) = \{(x, y) : y^2 = x^3 + ax + b \text{ where } a, b \in K\} \cup \{\infty\}$$

where $4a^3 + 27b^2 \neq 0$.

Elliptic Curve Groups Over Fields

Definition

Given a field K with characteristic neither 2 nor 3, an **elliptic curve** $E(K)$ is the set

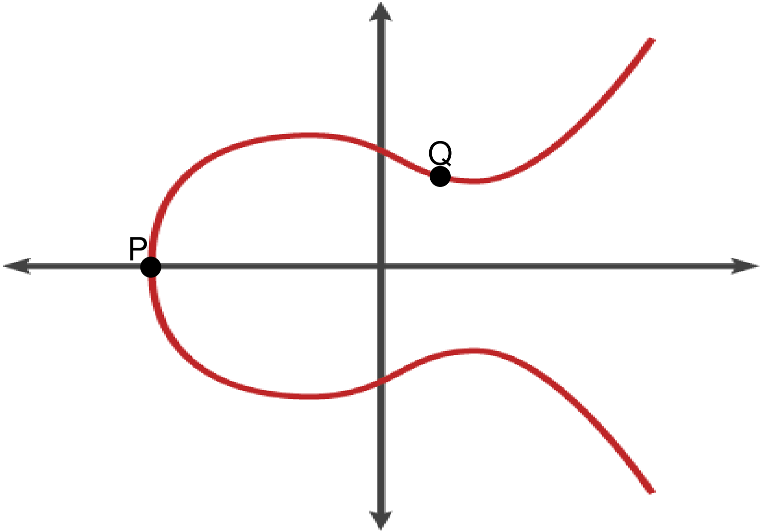
$$E(K) = \{(x, y) : y^2 = x^3 + ax + b \text{ where } a, b \in K\} \cup \{\infty\}$$

where $4a^3 + 27b^2 \neq 0$.

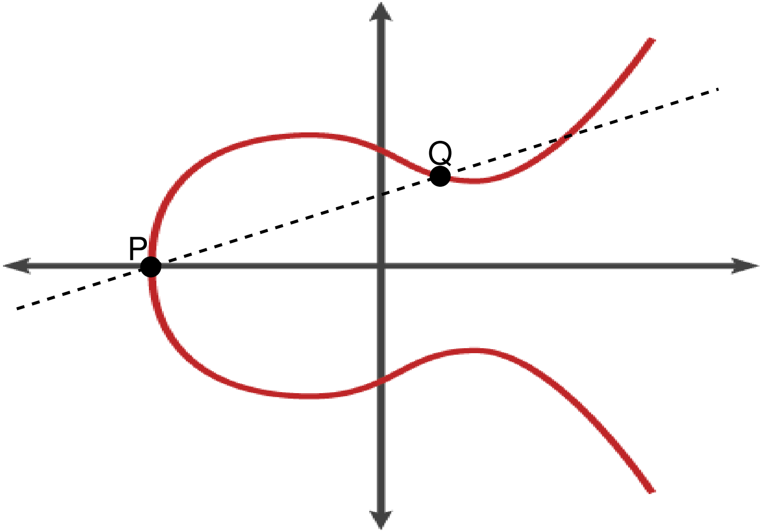
- The points of $E(K)$ form an abelian group, where the point at infinity serves as the group identity.

Elliptic Curve Addition

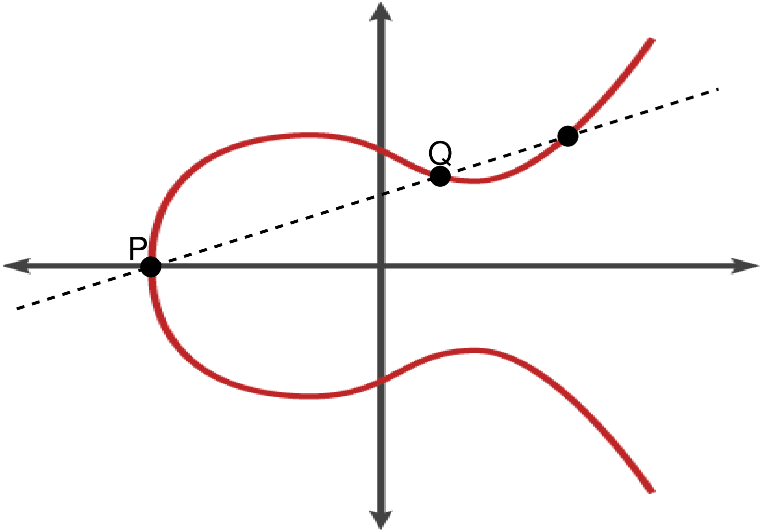
Elliptic Curve Addition



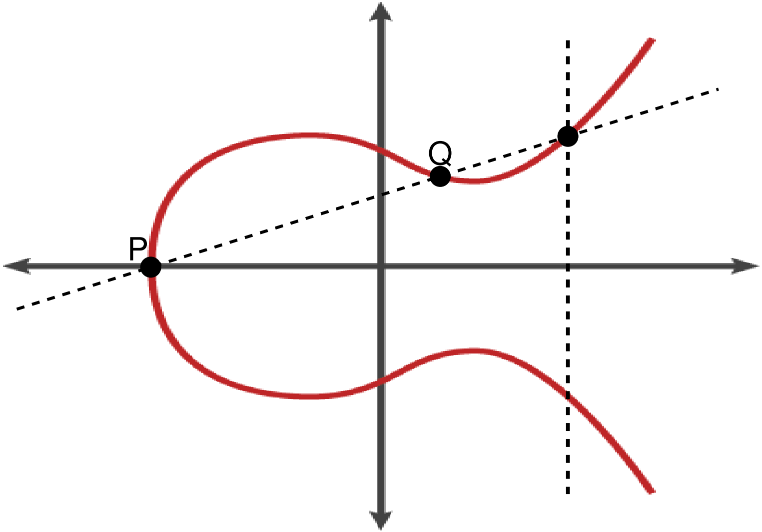
Elliptic Curve Addition



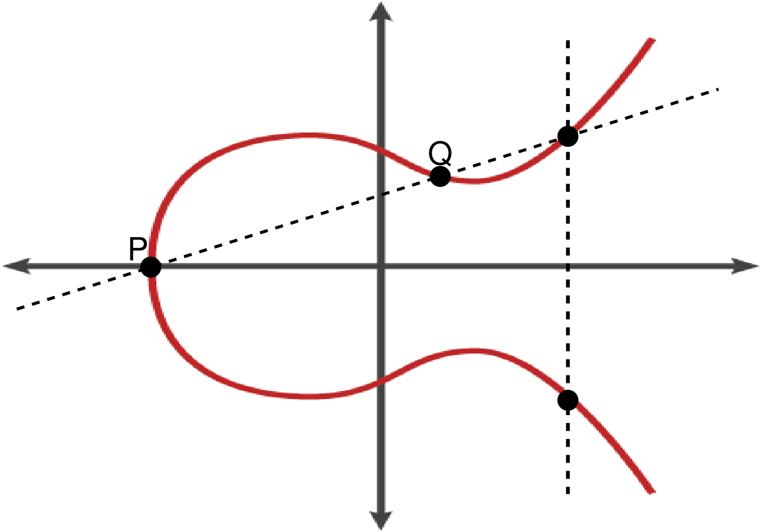
Elliptic Curve Addition



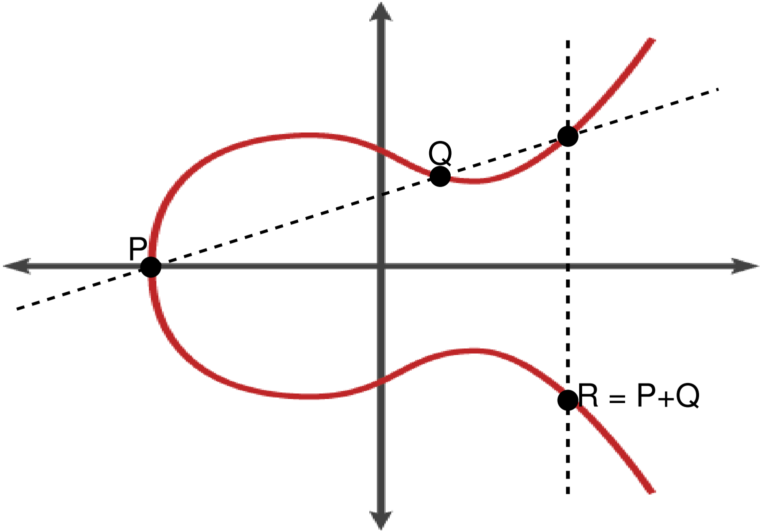
Elliptic Curve Addition



Elliptic Curve Addition



Elliptic Curve Addition



Good Reduction of Elliptic Curves over $\mathbb{Q}$

Good Reduction of Elliptic Curves over $\mathbb{Q}$

- Particularly interested in elliptic curves over $\mathbb{Q}$:

Good Reduction of Elliptic Curves over $\mathbb{Q}$

- Particularly interested in elliptic curves over $\mathbb{Q}$:

$$E/\mathbb{Q} : y^2 = x^3 + ax + b \cup \{\infty\}$$

where $a, b \in \mathbb{Q}$ and $4a^3 + 27b^2 \neq 0$.

Good Reduction of Elliptic Curves over $\mathbb{Q}$

- Particularly interested in elliptic curves over $\mathbb{Q}$:

$$E/\mathbb{Q} : y^2 = x^3 + ax + b \cup \{\infty\}$$

where $a, b \in \mathbb{Q}$ and $4a^3 + 27b^2 \neq 0$.

- Also interested in the "reduction" of these curves mod p.

Good Reduction of Elliptic Curves over $\mathbb{Q}$

- Particularly interested in elliptic curves over $\mathbb{Q}$:

$$E/\mathbb{Q} : y^2 = x^3 + ax + b \cup \{\infty\}$$

where $a, b \in \mathbb{Q}$ and $4a^3 + 27b^2 \neq 0$.

- Also interested in the "reduction" of these curves mod p.

Definition (Good reduction)

An elliptic curve $E/\mathbb{Q} : y^2 = x^3 + ax + b$ has *good reduction* at a prime p if $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$. The reduction $E(\mathbb{F}_p)$ is defined as $y^2 = x^3 + [a]x + [b]$, where $[a], [b]$ are the reductions of a and $b \pmod{p}$.

Hasse's Theorem

Recall

$$E(\mathbb{F}_p) := \{(x, y) : y^2 = x^3 + ax + b\}$$

Then

$$\#E(\mathbb{F}_p) = \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) + 1$$

$$= p + 1 - \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right)$$

Hasse's Theorem

Recall

$$E(\mathbb{F}_p) := \{(x, y) : y^2 = x^3 + ax + b\}$$

Then

$$\begin{aligned} \#E(\mathbb{F}_p) &= \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) + 1 \\ &= p + 1 - \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right) \end{aligned}$$

Define the *Frobenius trace* as $a_E(p) := p + 1 - \#E(\mathbb{F}_p)$.

Hasse's Theorem

Recall

$$E(\mathbb{F}_p) := \{(x, y) : y^2 = x^3 + ax + b\}$$

Then

$$\begin{aligned}\#E(\mathbb{F}_p) &= \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) + 1 \\ &= p + 1 - \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right)\end{aligned}$$

Define the *Frobenius trace* as $a_E(p) := p + 1 - \#E(\mathbb{F}_p)$.

Theorem (Hasse, 1936)

$$|a_E(p)| \leq 2\sqrt{p}$$

Families and Moments

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 $\mathbb{Z}[T]$.

Families and Moments

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 $\mathcal{E}(t)$ over $\mathbb{Q}$.

Families and Moments

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 $\mathcal{E}(t)$ over $\mathbb{Q}$.
- The r^{th} *moment* of the Fourier coefficients is

$$A_{r,\mathcal{E}}(p) \;=\; \sum_{t \mod p} a_{\mathcal{E}(t)}(p)^r,$$

where $a_{\mathcal{E}(t)}(p) = p + 1 - \#\mathcal{E}_t(\mathbb{F}_p)$ is the Frobenius trace of $\mathcal{E}(t)$.

Negative Bias in the First Moment

The first moment is related to the rank of the elliptic curve family. Note here that we normalize by $\frac{1}{p}$ when taking the average over the primes.

$A_{1,\mathcal{E}}(p)$ and Family Rank (Rosen-Silverman)

Given technical assumptions related to L-functions associated with $\mathcal{E}$,

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p\le X} \frac{A_{1,\mathcal{E}}(p)\log p}{p} = -\text{rank}(\mathcal{E}/\mathbb{Q}).$$

The $j(T)-$invariant and moment calculations

The $j(T)-$invariant and moment calculations

Definition ($j(T)$-invariant)

For an elliptic curve family $\mathcal{E}(T) : y^2 = x^3 + A(T)x + B(T)$, we define the $j(T)$*-invariant* as

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

Bias Conjecture

We write $f(x) = O(g(x))$ to mean there exists $c > 0$ such that $|f(x)| \leq cg(x)$ for all x.

Bias Conjecture

We write $f(x) = O(g(x))$ to mean there exists $c > 0$ such that $|f(x)| \leq cg(x)$ for all x.

Second Moment Asymptotic (Michel)

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

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

Bias Conjecture

We write $f(x) = O(g(x))$ to mean there exists $c > 0$ such that $|f(x)| \leq cg(x)$ for all x.

Second Moment Asymptotic (Michel)

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

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

- The lower order terms are of sizes $p^{3/2}$, p, $p^{1/2}$, and 1.

Bias Conjecture

We write $f(x) = O(g(x))$ to mean there exists $c > 0$ such that $|f(x)| \le cg(x)$ for all x.

Second Moment Asymptotic (Michel)

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

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

- The lower order terms are of sizes $p^{3/2}$, p, $p^{1/2}$, and 1.

In every family that has been studied, it has been observed:

Bias Conjecture

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

Relation with Excess Rank

- Lower order negative bias increases the bound for average rank in families through statistics of zero densities near the central point

Relation with Excess Rank

- Lower order negative bias increases the bound for average rank in families through statistics of zero densities near the central point
- This contributes to an explanation of observed excess rank.

Preliminary Evidence and Patterns

Let $n_{3,2,p}$ equal the number of cube roots of 2 modulo p, and set $c_0(p) = \left[\left(\frac{-3}{p}\right) + \left(\frac{3}{p}\right)\right] p$, $c_1(p) = \left[\sum_{x \bmod p} \left(\frac{x^3-x}{p}\right)\right]^2$, $c_{3/2}(p) = p\sum_{x(p)} \left(\frac{4x^3+1}{p}\right)$.

Family	$A_{1,\mathcal{E}}(p)$	$A_{2,\mathcal{E}}(p)$
$y^2 = x^3 + Sx + T$	0	$p^3 - p^2$
$y^2 = x^3 + 2^4(-3)^3(9T+1)^2$	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	$p^2 - 2p - \left(\frac{-3}{p}\right)$
$y^2 = x^3 + Tx^2 + 1$	$-p$	$p^2 - n_{3,2,p}p - 1 + c_{3/2}(p)$
$y^2 = x^3 - T^2x + T^2$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 - T^2x + T^4$	$-2p$	$p^2 - p - c_1(p) - c_0(p)$
$y^2 = x^3 + Tx^2 - (T+3)x + 1$	$-2c_{p,1;4}p$	$p^2 - 4c_{p,1;6}p - 1$

where $c_{p,a;m} = 1$ if $p \equiv a \bmod m$ and otherwise is 0.

Lemmas on Legendre Symbols

Linear and Quadratic Legendre Sums

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

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

Lemmas on Legendre Symbols

Linear and Quadratic Legendre Sums

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

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

Average Values of Legendre Symbols

The value of $\left(\frac{x}{p}\right)$ for $x \in \mathbb{Z}$, when averaged over all primes p, is 1 if x is a non-zero square, and 0 otherwise.

Lemma (SMALL '14)

Consider a one-parameter family of elliptic curves of the form

$$\mathcal{E} : y^2 \ = \ P(x)T + Q(x),$$

where $P(x), Q(x) \in \mathbb{Z}[x]$ have degrees at most 3. Then the second moment can be expanded as

$$A_{2,\mathcal{E}}(p) = p\left[\sum_{P(x)\equiv 0}\left(\frac{Q(x)}{p}\right)\right]^2 - \left[\sum_{x(p)}\left(\frac{P(x)}{p}\right)\right]^2 + p\sum_{\Delta(x,y)\equiv 0}\left(\frac{P(x)P(y)}{p}\right)$$

where $\Delta(x,y) = (P(x)Q(y) - P(y)Q(x))^2$.

Second Moments of Linear-coefficient Families

We computed explicit formulas for the second moments of some one-parameter families with linear coefficients in T:

Family	$A_{2,\mathcal{E}}(p)$
$y^2 = (ax+b)(cx^2+dx+e+T)$	$\begin{cases} p^2 - p\left(2 + \left(\frac{-1}{p}\right)\right) & \text{if } p \nmid ad-2bc \\ (p^2-p)\left(1+\left(\frac{-1}{p}\right)\right) & \text{if } p \mid ad-2bc \end{cases}$
$y^2 = (ax^2+bx+c)(dx+e+T)$	$\begin{cases} p^2 - p\left(1 + \left(\frac{b^2-4ac}{p}\right)\right) - 1 & \text{if } p \nmid b^2-4ac \\ p-1 & \text{if } p \mid b^2-4ac \end{cases}$
$y^2 = x(ax^2+bx+c+dTx)$	$-1 - p\left(\frac{ac}{p}\right)$
$y^2 = x(ax+b)(cx+d+Tx)$	$p-1$

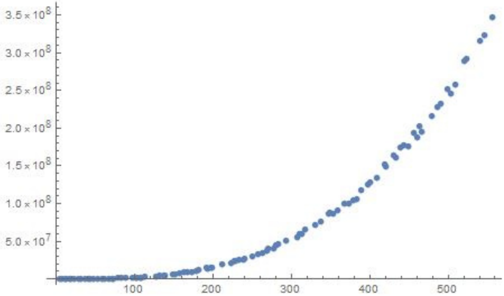
Numerics for Higher Even Moments

Ideally, we want to compute all higher moments. However, going beyond the second moment leads to intractable Legendre sums. Consequently, we have some numerical results for higher moments.

Numerics for Higher Even Moments

Ideally, we want to compute all higher moments. However, going beyond the second moment leads to intractable Legendre sums. Consequently, we have some numerical results for higher moments.

For example, the following is the 4-th moment of elliptic curve family $y^2 \equiv x^3 + (t+1)x^2 + tx$



Constant $j(T)-$invariant families

Constant $j(T)-$invariant families

- **Question:** What happens if we study elliptic curve families of constant $j(T)-$ invariant?

Constant $j(T)-$invariant families

- **Question:** What happens if we study elliptic curve families of constant $j(T)-$ invariant?
- Example: $\mathcal{E}(T) : y^2 = x^3 + A(T)x$ has $j(T) = 1728$, $\forall T \in \mathbb{Z}$.

Constant $j(T)-$invariant families

- **Question:** What happens if we study elliptic curve families of constant $j(T)-$ invariant?
- Example: $\mathcal{E}(T) : y^2 = x^3 + A(T)x$ has $j(T) = 1728$, $\forall T \in \mathbb{Z}$.
- Similarly, $\mathcal{E}(T) : y^2 = x^3 + B(T)$ has $j(T) = 0$.

Constant $j(T)-$invariant families

- **Question:** What happens if we study elliptic curve families of constant $j(T)-$ invariant?
- Example: $\mathcal{E}(T): y^2 = x^3 + A(T)x$ has $j(T) = 1728$, $\forall T \in \mathbb{Z}$.
- Similarly, $\mathcal{E}(T): y^2 = x^3 + B(T)$ has $j(T) = 0$.
- For these families of elliptic curves of fixed $j(T)-$invariant, we can compute arbitrarily high moments.
- In practice, computation is *fast* when $j(T)$ is constant.

$j = 0$ Curves

$j = 0$ Curves

Consider an elliptic curve of the form $E : y^2 = x^3 + B$ over $\mathbb{F}_p$.

$j = 0$ Curves

Consider an elliptic curve of the form $E : y^2 = x^3 + B$ over $\mathbb{F}_p$.

If $p \equiv 2 \pmod 3$, then $a_E(p) = 0$.

$j = 0$ Curves

Consider an elliptic curve of the form $E : y^2 = x^3 + B$ over $\mathbb{F}_p$.

If $p \equiv 2 \pmod 3$, then $a_E(p) = 0$.

Gauss' Six-Order Theorem

If $p \equiv 1 \pmod 3$, then write $p = a^2 + 3b^2$, $a \equiv 2 \pmod 3$, $b > 0$. We have:

$j = 0$ Curves

Consider an elliptic curve of the form $E : y^2 = x^3 + B$ over $\mathbb{F}_p$.

If $p \equiv 2 \pmod 3$, then $a_E(p) = 0$.

Gauss' Six-Order Theorem

If $p \equiv 1 \pmod 3$, then write $p = a^2 + 3b^2$, $a \equiv 2 \pmod 3$, $b > 0$. We have:

$$a_E(p) = \begin{cases} -2a & B \text{ is a sextic residue in } \mathbb{F}_p \\ 2a & B \text{ cubic, non-sextic residue} \\ a \pm 3b & B \text{ quadratic, non-sextic} \\ -a \pm 3b & B \text{ non-quadratic, non-cubic} \end{cases}$$

Moments of One-Parameter $j = 0$ Families

Moments of One-Parameter $j = 0$ Families

For $r \geq 0$, consider an the family of elliptic curves $\mathcal{E}_T : y^2 = x^3 - AT^r$ over $\mathbb{F}_p$. We compute the kth moment.

Moments of One-Parameter $j = 0$ Families

For $r \geq 0$, consider an the family of elliptic curves $\mathcal{E}_T : y^2 = x^3 - AT^r$ over $\mathbb{F}_p$. We compute the kth moment. We have $A_k(p) = 0$ when $p \equiv 3(4)$.

Moments of One-Parameter $j = 0$ Families

For $r \geq 0$, consider an the family of elliptic curves $\mathcal{E}_T : y^2 = x^3 - AT^r$ over $\mathbb{F}_p$. We compute the kth moment. We have $A_k(p) = 0$ when $p \equiv 3(4)$.

$$r \equiv 1, 5(6) \ : A_k(p) = \begin{cases} 0 & k \text{ is odd} \\ \frac{p-1}{3}\left((2a)^k + (a-3b)^k + (a+3b)^k\right) & k \text{ is even} \end{cases}$$

$$r \equiv 2, 4(6) \ : A_k(p) = \begin{cases} \frac{p-1}{3}\left((-2a)^k + (a-3b)^k + (a+3b)^k\right) & A \text{ quadratic residue} \\ \frac{p-1}{3}\left((2a)^k + (-a-3b)^k + (-a+3b)^k\right) & A \text{ quadratic nonresidue} \end{cases}$$

$$r \equiv 3 \ : A_k(p) = \begin{cases} \frac{p-1}{2}\left((-2a)^k + (2a)^k\right) & A \text{ cubic residue} \\ \frac{p-1}{2}\left((a \pm 3b)^k + (-a \mp 3b)^k\right) & A \text{ cubic nonresidue} \end{cases}$$

Moments determined only by $r \pmod 6$.

$j = 1728$ Curves

Consider an elliptic curve of the form $\mathcal{E} : y^2 = x^3 - Ax$ over $\mathbb{F}_p$.

If $p \equiv 1 \pmod 4$, then $a_E(p) = 0$.

$j = 1728$ Curves

Consider an elliptic curve of the form $\mathcal{E} : y^2 = x^3 - Ax$ over $\mathbb{F}_p$.

If $p \equiv 1 \pmod 4$, then $a_E(p) = 0$.

Gauss' Four-Order Theorem

If $p \equiv 3 \pmod 4$, then write $p = a^2 + 3b^2$, where b is even and $a + b \equiv 1 \pmod 4$. We have:

$$a_E(p) = \begin{cases} 2a & A \text{ is a quartic residue} \\ -2a & A \text{ quadratic, non-quartic residue} \\ \pm 2b & A \text{ not a quadratic residue} \end{cases}$$

Moments of One-Parameter $j = 1728$ Families

For $r \geq 0$, consider the family $\mathcal{E}(T) : y^2 = x^3 - AT^r x$ over $\mathbb{F}_p$.

Moments of One-Parameter $j = 1728$ Families

For $r \geq 0$, consider the family $\mathcal{E}(T) : y^2 = x^3 - AT^r x$ over $\mathbb{F}_p$. When $p \equiv 3 \pmod 4$, all moments are 0.

Moments of One-Parameter $j = 1728$ Families

For $r \geq 0$, consider the family $\mathcal{E}(T): y^2 = x^3 - AT^r x$ over $\mathbb{F}_p$. When $p \equiv 3 \pmod 4$, all moments are 0.

$$r \equiv 1, 3(4) \quad : A_k(p) = \begin{cases} 0 & k \text{ is odd} \\ (p-1)2^{k-1}(a^k + b^k) & k \text{ is even} \end{cases}$$

$$r \equiv 2(4) \quad : A_k(p) = \begin{cases} 0 & k \text{ is odd} \\ (p-1)(2a)^k & A \text{ quadratic residue, } k \text{ is even} \\ (p-1)(2b)^k & A \text{ quadratic nonresidue, } k \text{ is even} \end{cases}$$

For $r \equiv 0(4)$, we get similar but more elaborate results.

Bias in L-functions of Cuspidal Newforms

Cuspidal Newforms

Cuspidal Newforms

Definition (Holomorphic Form of Weight k, level N)

A holomorphic function $f(z) : \mathbb{H} \to \mathbb{C}$, of moderate growth, for which

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

where

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \right\}$$

Cuspidal Newforms

Definition (Holomorphic Form of Weight k, level N)

A holomorphic function $f(z) : \mathbb{H} \to \mathbb{C}$, of moderate growth, for which

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

where

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \right\}$$

Note modular forms are *periodic* (take $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$).

Cuspidal Newforms

Definition (Holomorphic Form of Weight k, level N)

A holomorphic function $f(z) : \mathbb{H} \to \mathbb{C}$, of moderate growth, for which

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

where

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \; : \; c \equiv 0 \pmod{N} \right\}$$

Note modular forms are *periodic* (take $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$). When a modular form has constant coefficient equal to 0 in its Fourier expansion, it is called a **cusp form**.

Cuspidal Newforms

Definition (Holomorphic Form of Weight k, level N)

A holomorphic function $f(z) : \mathbb{H} \to \mathbb{C}$, of moderate growth, for which

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z), \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$$

where

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ c \equiv 0 \pmod{N} \right\}$$

Note modular forms are *periodic* (take $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$). When a modular form has constant coefficient equal to 0 in its Fourier expansion, it is called a **cusp form**.

A cuspidal **newform** of level N is a cusp form that cannot be reduced to a cusp form of level M, where $M \mid N$.

Averaging over Weights

Let $\mathcal{F}_{X,\delta,N}$ be the family of cuspidal newforms of weights smaller than some positive X^δ.

Averaging over Weights

Let $\mathcal{F}_{X,\delta,N}$ be the family of cuspidal newforms of weights smaller than some positive X^δ.

Averaging over primes less than X^σ, define the r-th moment of the family $\mathcal{F}_{X,\delta,N}$ as:

$$M_{r,\sigma}(\mathcal{F}_{X,\delta,N}) = \frac{1}{\pi(X^\sigma)} \sum_{p<X^\sigma} \frac{1}{\sum_{k<X^\delta} |H_k^*(N)|} \sum_{k<X^\delta} \sum_{f\in H_k^*(N)} \lambda_f^r(p)$$

Averaging over Weights

Let $\mathcal{F}_{X,\delta,N}$ be the family of cuspidal newforms of weights smaller than some positive X^δ.

Averaging over primes less than X^σ, define the r-th moment of the family $\mathcal{F}_{X,\delta,N}$ as:

$$M_{r,\sigma}(\mathcal{F}_{X,\delta,N}) = \frac{1}{\pi(X^\sigma)} \sum_{p<X^\sigma} \frac{1}{\sum_{k<X^\delta} |H_k^*(N)|} \sum_{k<X^\delta} \sum_{f\in H_k^*(N)} \lambda_f^r(p)$$

Then we study the asymptotic behavior of the moment as $N \to \infty$.

$$M_{r,\sigma}(\mathcal{F}_{X,\delta}) = \lim_{N\to\infty} M_{r,\sigma}(\mathcal{F}_{X,\delta,N}).$$

Averaging over Weights

Theorem (SMALL '17)

$$M_{r,\sigma}(\mathcal{F}_{X,\delta}) = \begin{cases} C_{r/2} + C_{r/2-1}\frac{\log\log X^\sigma}{\pi(X^\sigma)} \\ \qquad +O\left(\frac{1}{X^{2\delta}} + \frac{1}{\pi(X^\sigma)}\right) & \text{even r} \\ 0 & \text{odd } r \end{cases}$$

Notice that the bias in moments of cuspidal newforms is $C_{r/2} + C_{r/2-1}$, a positive integer, instead of the negative bias in moments of elliptic curve subfamilies.

Questions for Further Study

- Does the Bias Conjecture hold for elliptic families with constant j-invariant?

Questions for Further Study

- Does the Bias Conjecture hold for elliptic families with constant j-invariant?
- Are there cuspidal newform families with negative biases in their moments?

Questions for Further Study

- Does the Bias Conjecture hold for elliptic families with constant j-invariant?
- Are there cuspidal newform families with negative biases in their moments?
- Does the average bias always occur in the terms of size p or 1?

Questions for Further Study

- Does the Bias Conjecture hold for elliptic families with constant j-invariant?
- Are there cuspidal newform families with negative biases in their moments?
- Does the average bias always occur in the terms of size p or 1?
- How is the Bias Conjecture formulated for all higher even moments? Can they be modeled by polynomials?

Questions for Further Study

- Does the Bias Conjecture hold for elliptic families with constant j-invariant?
- Are there cuspidal newform families with negative biases in their moments?
- Does the average bias always occur in the terms of size p or 1?
- How is the Bias Conjecture formulated for all higher even moments? Can they be modeled by polynomials?
- What other families obey the Bias Conjecture? Kloosterman sums? Higher genus curves?

References

- B. Mackall, S.J. Miller, C. Rapti, K. Winsor, *Lower-Order Biases in Elliptic Curve Fourier Coefficients in Families*, Frobenius Distributions: Lang-Trotter and Sato-Tate Conjectures (David Kohel and Igor Shparlinski, editors), Contemporary Mathematics 663, AMS, Providence, RI 2016.https://web.williams.edu/Mathematics/sjmiller/public_html/math/papers/BiasCIRM30.pdf

- S.J. Miller, 1- *and* 2*-level densities for families of elliptic curves: evidence for the underlying group symmetries*, Compositio Mathematica **140** (2004), 952–992. http://arxiv.org/pdf/math/0310159.

- 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. http://arxiv.org/abs/math/0506461.

- S.J. Miller, *Investigations of zeros near the central point of elliptic curve L-functions*, Experimental Mathematics **15** (2006), no. 3, 257–279. http://arxiv.org/pdf/math/0508150.

- S.J. Miller, *Lower order terms in the 1-level density for families of holomorphic cuspidal newforms*, Acta Arithmetica **137** (2009), 51–98. http://arxiv.org/pdf/0704.0924v4.

- S.J. Miller, S. Wong, *Moments of the rank of elliptic curves*, Canad. J. of Math. **64** (2012), no. 1, 151–182. http://web.williams.edu/Mathematics/sjmiller/public_html/math/papers/mwMomentsRanksEC812final.pdf

Thank you!

Thank you!

Questions?