Applications of Moments of Dirichlet Coefficients in Elliptic Curve Families

Steven J Miller (sjm1@williams.edu) – Williams College
(Joint with A. Lozano-Robledo, SMALL REU groups, . . .)

Murmurations in Arithmetic, ICERM, July 7, 2023

Seeing biases in many data sets.

Reporting on other situations and possible tests.
Random Matrix Ensembles with Split Limiting Behavior (with Paula Burkhardt, Peter Cohen, Jonathan Dewitt, Max Hlavacek, Carsten Sprunger, Yen Nhi Truong Vu, Roger Van Peski, and Kevin Yang, and an appendix joint with Manuel Fernandez and Nicholas Sieger), Random Matrices: Theory and Applications **7** (2018), no. 3, 1850006 (30 pages), DOI: 10.1142/S2010326318500065.

Checkerboard Matrices: $N \times N$ (k, w)-checkerboard ensemble

Matrices $M = (m_{ij}) = M^T$ with a_{ij} iidrv, mean 0, variance 1, finite higher moments, w fixed and

$$m_{ij} = \begin{cases} a_{ij} & \text{if } i \not\equiv j \bmod k \\ w & \text{if } i \equiv j \bmod k. \end{cases}$$

Example: $(3, w)$-checkerboard matrix:

$$\begin{pmatrix} w & a_{0,1} & a_{0,2} & w & a_{0,4} & \cdots & a_{0,N-1} \\ a_{1,0} & w & a_{1,2} & a_{1,3} & w & \cdots & a_{1,N-1} \\ a_{2,0} & a_{2,1} & w & a_{2,3} & a_{2,4} & \cdots & w \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{0,N-1} & a_{1,N-1} & w & a_{3,N-1} & a_{4,N-1} & \cdots & w \end{pmatrix}$$

Split Eigenvalue Distribution

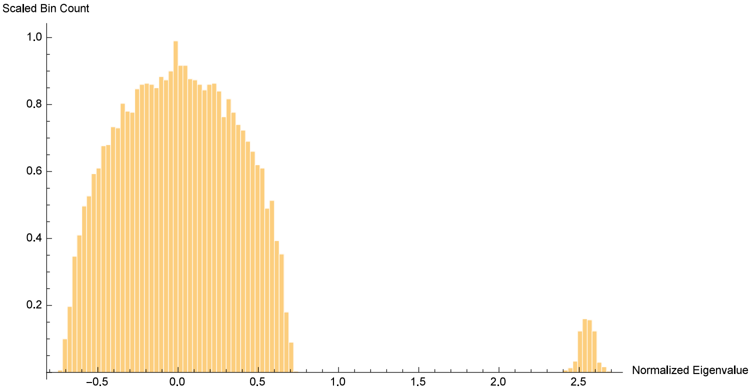


Figure: Histogram of normalized eigenvalues: 2-checkerboard 100×100 matrices, 100 trials.

Split Eigenvalue Distribution

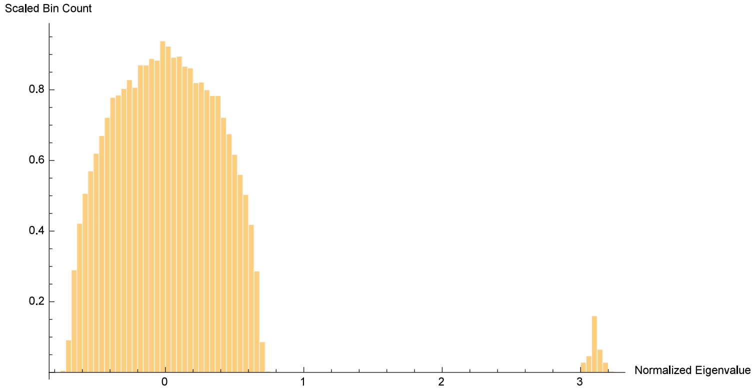


Figure: Histogram of normalized eigenvalues: 2-checkerboard 150×150 matrices, 100 trials.

Split Eigenvalue Distribution

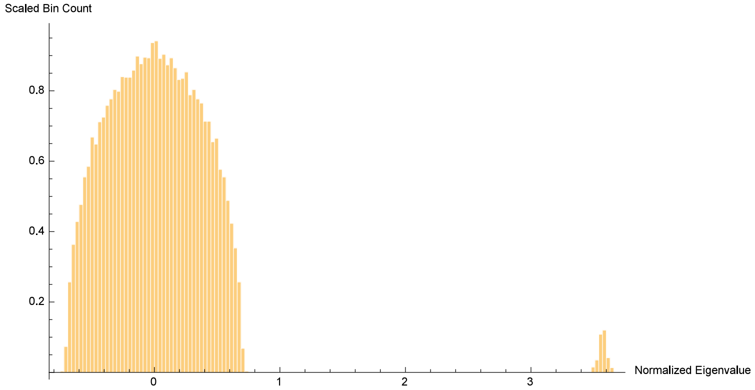


Figure: Histogram of normalized eigenvalues: 2-checkerboard 200×200 matrices, 100 trials.

Split Eigenvalue Distribution

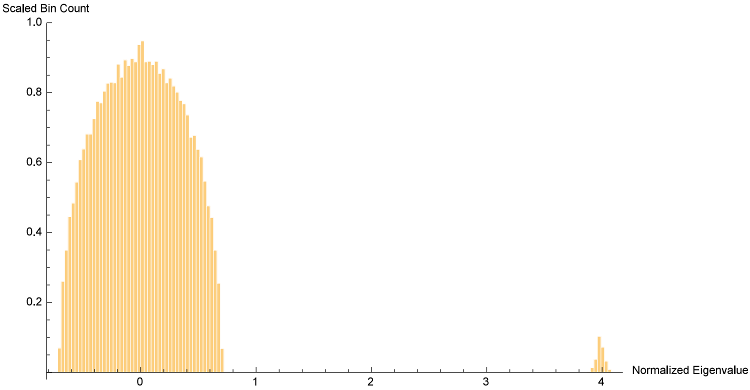


Figure: Histogram of normalized eigenvalues: 2-checkerboard 250×250 matrices, 100 trials.

Split Eigenvalue Distribution

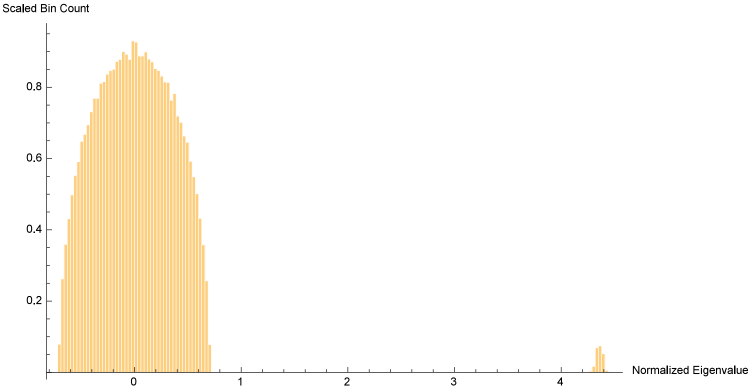


Figure: Histogram of normalized eigenvalues: 2-checkerboard 300×300 matrices, 100 trials.

Split Eigenvalue Distribution

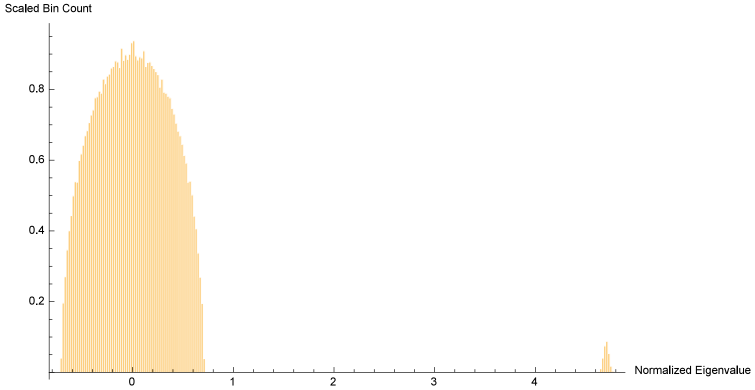


Figure: Histogram of normalized eigenvalues: 2-checkerboard 350×350 matrices, 100 trials.

The Weighting Function

Use weighting function $f_n(x) = x^{2n}(x-2)^{2n}$.

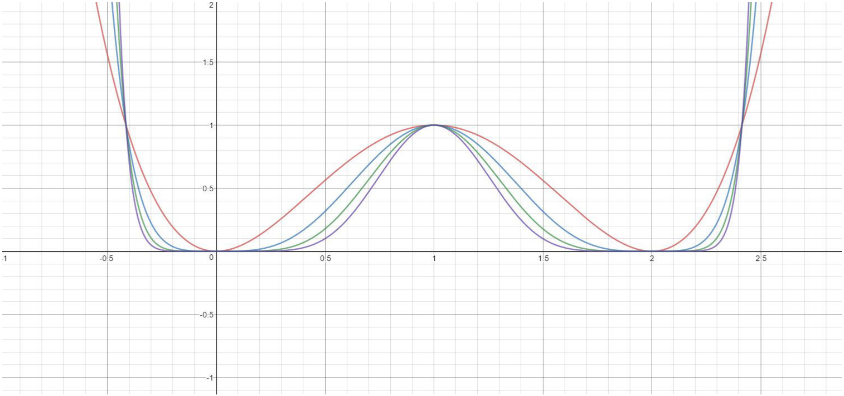


Figure: $f_n(x)$ plotted for $n \in \{1, 2, 3, 4\}$.

The Weighting Function

Use weighting function $f_n(x) = x^{2n}(x-2)^{2n}$.

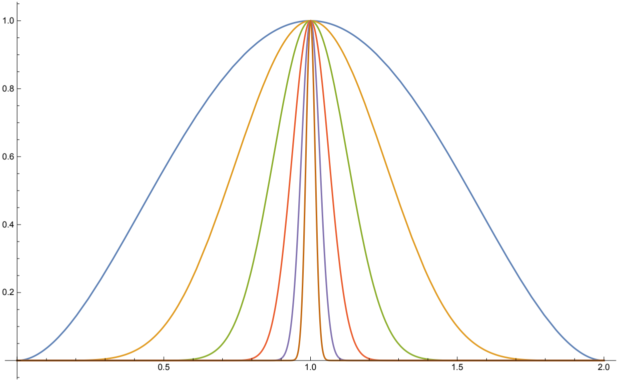


Figure: $f_n(x)$ plotted for $n = 4^m, m \in \{0, 1, \dots, 5\}$.

Spectral distribution of hollow GOE

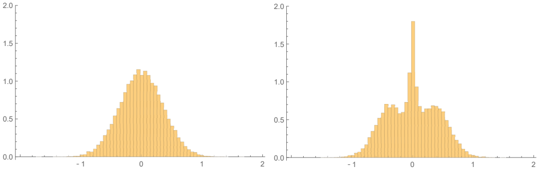


Figure: Hist. of eigenvals of 32000 (Left) 2×2 hollow GOE matrices, (Right) 3×3 hollow GOE matrices.

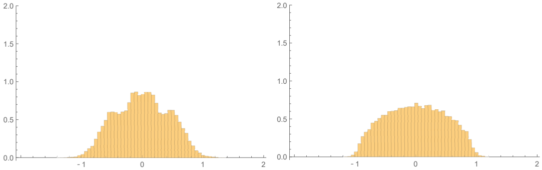


Figure: Hist. of eigenvals of 32000 (Left) 4×4 hollow GOE matrices, (Right) 16×16 hollow GOE matrices.

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* (note not normalizing by $1/p$) is

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

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

First moment related to the rank of the elliptic curve family.

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

Given technical assumptions (Tate's conjecture) related to L-functions associated with $\mathcal{E}$,

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

Bias Conjecture

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

Second Moment Asymptotic (Michel)

For families with $j(T)$ non-constant, the second moment is

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

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

Bias Conjecture

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

Second Moment Asymptotic (Michel)

For families with $j(T)$ non-constant, the second moment is

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

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

In every family studied before July 2023, observe:

Bias Conjecture

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

Comments

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.
- Unfortunately only a *small* amount, not enough to explain observed excess rank.

Results to date

- Very special families, Legendre sums computable, not generic.
- Confirmed for additional families by M. Kazalicki and B. Naskrecki.

Methods for Obtaining Explicit Formulas

For a family $\mathcal{E} : y^2 = x^3 + A(T)x + B(T)$, we can write

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

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

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

Lemmas on Legendre Symbols

Linear and Quadratic Legendre Sums

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

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

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.

Small Rank

Moderate Rank

Rank 6 Family

Rational Surface of Rank 6 over $\mathbb{Q}(T)$:

$$\begin{aligned} y^2 &= x^3 + (2aT - B)x^2 + (2bT - C)(T^2 + 2T - A + 1)x \\ &\quad + (2cT - D)(T^2 + 2T - A + 1)^2 \end{aligned}$$

$$\begin{aligned}
A &= 8,916,100,448,256,000,000 \\
B &= -811,365,140,824,616,222,208 \\
C &= 26,497,490,347,321,493,520,384 \\
D &= -343,107,594,345,448,813,363,200 \\
a &= 16,660,111,104 \\
b &= -1,603,174,809,600 \\
c &= 2,149,908,480,000
\end{aligned}$$

Constructing Rank 6 Family

Idea: can explicitly evaluate linear and quadratic Legendre sums.

Use: a and b are not both zero mod p and $p > 2$, then for $t \in \mathbb{Z}$

$$\sum_{t=0}^{p-1} \left(\frac{at^2+bt+c}{p}\right) = \begin{cases} (p-1)\left(\frac{a}{p}\right) & \text{if } p|(b^2-4ac) \\ -\left(\frac{a}{p}\right) & \text{otherwise.} \end{cases}$$

Thus if $p|(b^2-4ac)$, the summands are $\left(\frac{a(t-t')^2}{p}\right) = \left(\frac{a}{p}\right)$, and the t-sum is large.

Constructing Rank 6 Family

$$\begin{aligned} y^2 = f(x,T) &= x^3T^2 + 2g(x)T - h(x) \\ g(x) &= x^3 + ax^2 + bx + c, \ \ c \neq 0 \\ h(x) &= (A-1)x^3 + Bx^2 + Cx + D \\ D_T(x) &= g(x)^2 + x^3h(x). \end{aligned}$$

$D_T(x)$ is one-fourth of the discriminant of the quadratic (in T) polynomial $f(x,T)$.

$\mathcal{E}$ not in standard form, as the coefficient of x^3 is T^2, harmless. As $y^2 = f(x,T)$, for the fiber at $T = t$:

$$a_t(p) = -\sum_{x(p)} \left(\frac{f(x,t)}{p}\right) = -\sum_{x(p)} \left(\frac{x^3t^2 + 2g(x)t - h(x)}{p}\right).$$

Constructing Rank 6 Family

We study $-pA_{\mathcal{E}}(p) = \sum_{x=0}^{p-1} \sum_{t=0}^{p-1} \left(\frac{f(x,t)}{p}\right)$.
When $x \equiv 0$ the t-sum vanishes if $c \not\equiv 0$, as it is just $\sum_{t=0}^{p-1} \left(\frac{2ct-D}{p}\right)$.

Assume now $x \not\equiv 0$. By the lemma on Quadratic Legendre Sums

$$\sum_{t=0}^{p-1} \left(\frac{x^3t^2 + 2g(x)t - h(x)}{p}\right) = \begin{cases} (p-1)\left(\frac{x^3}{p}\right) & \text{if } p \mid D_t(x) \\ -\left(\frac{x^3}{p}\right) & \text{otherwise.} \end{cases}$$

Goal: find coefficients a, b, c, A, B, C, D so that $D_t(x)$ has six distinct, non-zero roots that are squares.

Constructing Rank 6 Family

Assume we can find such coefficients. Then

$$\begin{aligned}
-pA_{\mathcal{E}}(p) &= \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) = \sum_{x=0}^{p-1}\sum_{t=0}^{p-1}\left(\frac{x^3t^2+2g(x)t-h(x)}{p}\right) \\
&= \sum_{x=0}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) + \sum_{x:D_t(x)\equiv 0}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) \\
&\quad + \sum_{x:xD_t(x)\not\equiv 0}\sum_{t=0}^{p-1}\left(\frac{f(x,t)}{p}\right) \\
&= 0 + 6(p-1) - \sum_{x:xD_t(x)\not\equiv 0}\left(\frac{x^3}{p}\right) = 6p.
\end{aligned}$$

Constructing Rank 6 Family

We must find $a, \dots, D$ such that $D_t(x)$ has six distinct, non-zero roots ρ_i^2:

$$\begin{aligned}
D_t(x) &= g(x)^2 + x^3 h(x) \\
&= Ax^6 + (B+2a)x^5 + (C+a^2+2b)x^4 \\
&\quad + (D+2ab+2c)x^3 \\
&\quad + (2ac+b^2)x^2 + (2bc)x + c^2 \\
&= A(x^6 + R_5x^5 + R_4x^4 + R_3x^3 + R_2x^2 + R_1x + R_0) \\
&= A(x-\rho_1^2)(x-\rho_2^2)(x-\rho_3^2)(x-\rho_4^2)(x-\rho_5^2)(x-\rho_6^2).
\end{aligned}$$

Constructing Rank 6 Family

Because of the freedom to choose B, C, D there is no problem matching coefficients for the x^5, x^4, x^3 terms. We must simultaneously solve in integers

$$\begin{aligned} 2ac + b^2 &= R_2 A \\ 2bc &= R_1 A \\ c^2 &= R_0 A. \end{aligned}$$

For simplicity, take $A = 64R_0^3$. Then

$$\begin{array}{rclcrcl} c^2 &=& 64R_0^4 & \longrightarrow & c &=& 8R_0^2 \\ 2bc &=& 64R_0^3 R_1 & \longrightarrow & b &=& 4R_0 R_1 \\ 2ac + b^2 &=& 64R_0^3 R_2 & \longrightarrow & a &=& 4R_0 R_2 - R_1^2. \end{array}$$

Constructing Rank 6 Family

For an explicit example, take $r_i = \rho_i^2 = i^2$. For these choices of roots,

$$R_0 \;=\; 518400,\;\; R_1 \;=\; -773136,\;\; R_2 \;=\; 296296.$$

Solving for a through D yields

$$\begin{aligned}
A &= 64R_0^3 &&= 8916100448256000000\\
c &= 8R_0^2 &&= 2149908480000\\
b &= 4R_0R_1 &&= -1603174809600\\
a &= 4R_0R_2 - R_1^2 &&= 16660111104\\
B &= R_5A - 2a &&= -811365140824616222208\\
C &= R_4A - a^2 - 2b &&= 26497490347321493520384\\
D &= R_3A - 2ab - 2c &&= -343107594345448813363200
\end{aligned}$$

Constructing Rank 6 Family

We convert $y^2 = f(x,t)$ to $y^2 = F(x,T)$, which is in Weierstrass normal form. We send $y \to \frac{y}{T^2+2T-A+1}$, $x \to \frac{x}{T^2+2T-A+1}$, and then multiply both sides by $(T^2+2T-A+1)^2$. For future reference, we note that

$$\begin{aligned} T^2+2T-A+1 &= (T+1-\sqrt{A})(T+1+\sqrt{A}) \\ &= (T-t_1)(T-t_2) \\ &= (T-2985983999)(T+2985984001). \end{aligned}$$

We have

$$\begin{aligned} f(x,T) &= T^2x^3+(2x^3+2ax^2+2bx+2c)T-(A-1)x^3-Bx^2-Cx-D \\ &= (T^2+2T-A+1)x^3+(2aT-B)x^2+(2bT-C)x+(2cT-D) \\ F(x,T) &= x^3+(2aT-B)x^2+(2bT-C)(T^2+2T-A+1)x \\ &\quad +(2cT-D)(T^2+2T-A+1)^2. \end{aligned}$$

Constructing Rank 6 Family

We now study the $-pA_{\mathcal{E}}(p)$ arising from $y^2 = F(x, T)$. It is enough to show this is $6p + O(1)$ for all p greater than some p_0. Note that t_1, t_2 are the unique roots of $t^2 + 2t - A + 1 \equiv 0 \bmod p$. We find

$$-pA_{\mathcal{E}}(p) = \sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right) = \sum_{t\neq t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{F(x,t)}{p}\right).$$

For $t \neq t_1, t_2$, send $x \longrightarrow (t^2 + 2t - A + 1)x$. As $(t^2 + 2t - A + 1) \not\equiv 0$, $\left(\frac{(t^2+2t-A+1)^2}{p}\right) = 1$. Simple algebra yields

$$\begin{aligned} -pA_{\mathcal{E}}(p) &= 6p + O(1) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{f_t(x)}{p}\right) + O(1) \\ &= 6p + O(1) + \sum_{t=t_1,t_2}\sum_{x=0}^{p-1}\left(\frac{(2at-B)x^2 + (2bt-C)x + (2ct-D)}{p}\right). \end{aligned}$$

Constructing Rank 6 Family

The last sum above is negligible (i.e., is $O(1)$) if

$$D(t) \;=\; (2bt-C)^2-4(2at-B)(2ct-D)\not\equiv 0(p).$$

Calculating yields

$$\begin{aligned}
D(t_1) &= 4291243480243836561123092143580209905401856\\
&= 2^{32}\cdot 3^{25}\cdot 7^{5}\cdot 11^{2}\cdot 13\cdot 19\cdot 29\cdot 31\cdot 47\cdot 67\cdot 83\cdot 97\cdot 103\\
D(t_2) &= 4291243816662452751895093255391719515488256\\
&= 2^{33}\cdot 3^{12}\cdot 7\cdot 11\cdot 13\cdot 41\cdot 173\cdot 17389\cdot 805873\cdot 9447850813.
\end{aligned}$$

Constructing Rank 6 Family

Hence, except for finitely many primes (coming from factors of $D(t_i)$, $a, \dots, D$, t_1 and t_2), $-A_{\mathcal{E}}(p) = 6p + O(1)$ as desired.

We have shown: There exist integers a, b, c, A, B, C, D so that the curve $\mathcal{E} : y^2 = x^3T^2 + 2g(x)T - h(x)$ over $\mathbb{Q}(T)$, with $g(x) = x^3 + ax^2 + bx + c$ and $h(x) = (A-1)x^3 + Bx^2 + Cx + D$, has rank 6 over $\mathbb{Q}(T)$. In particular, with the choices of a through D above, $\mathcal{E}$ is a rational elliptic surface and has Weierstrass form

$$\begin{aligned} y^2 &= x^3 + (2aT - B)x^2 + (2bT - C)(T^2 + 2T - A + 1)x \\ &\quad + (2cT - D)(T^2 + 2T - A + 1)^2 \end{aligned}$$

Constructing Rank 6 Family

We show $\mathcal{E}$ is a rational elliptic surface by translating $x \mapsto x - (2aT - B)/3$, which yields $y^2 = x^3 + A(T)x + B(T)$ with $\deg(A) = 3, \deg(B) = 5$.

The Rosen-Silverman theorem is applicable, and as we can compute $A_{\mathcal{E}}(p)$, we know the rank is exactly 6 (and we never need to calculate height matrices). $\square$

1-Parameter Families

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.

Tools: 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.

Simple Second Moment: Not Generic Family!

Family: $y^2 = x^2(x+1) + x(x+1)t$.

$$A_{1,\mathcal{E}}(p) \;=\; \sum_{t(p)} a_t(p) \;=\; -\sum_{t=0}^{p-1}\sum_{x=0}^{p-1}\left(\frac{x^2(x+1)+x(x+1)t}{p}\right).$$

If x equals 0 or -1, then the t-sum is zero.

Otherwise $t \to x^{-1}(x-1)^{-1}t$ and get zero from the t-sum.

Hence $A_{1,\mathcal{E}}(p)$ vanishes.

Simple Second Moment: Not Generic Family!

Family: $y^2 = x^2(x+1) + x(x+1)t$.

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

The t-sum is $p-1$ if $x = y$ and -1 otherwise.

Simple Second Moment: Not Generic Family!

Family: $y^2 = x^2(x+1) + x(x+1)t$.

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

thus $A_{2,\mathcal{E}}(p) = p^2 - 2p - 1$.

More Involved Second Moment: $y^2 = x^3 + tx^2 + 1$

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

so family has rank 1.

For completeness will paste second moment calculation from my thesis.

More Involved Second Moment: $y^2 = x^3 + tx^2 + 1$

https://web.williams.edu/Mathematics/sjmiller/public_html/math/thesis/SJMthesis_Rev2005.pdf

We use the Gauss sum expansion (Equation 2.4) to calculate $A_{2,\mathcal{F}}(p)$.

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= \sum_{t(p)} \sum_{x(p)} \sum_{y(p)} \left(\frac{x^3+1+x^2t}{p}\right)\left(\frac{y^3+1+y^2t}{p}\right) \\ &= \sum_{x,y(p)} \sum_{c,d=1}^{p-1} \frac{1}{p}\left(\frac{cd}{p}\right) \mathbf{e}\left(\frac{c(x^3+1)-d(y^3+1)}{p}\right) \sum_{t(p)} \mathbf{e}\left(\frac{(cx^2-dy^2)t}{p}\right). \end{aligned} \tag{13.7}$$

Note 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 $\overline{G}_p$, for a total contribution of p.

More Involved Second Moment: $y^2 = x^3 + tx^2 + 1$

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

$$\begin{aligned}
A_{2,\mathcal{F}}(p) &= \sum_{x,y=1}^{p-1}\sum_{c=1}^{p-1}\frac{1}{p}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x^3y^2+y^2-x^2y^3-x^2)}{p}\right)p+p \\
&= \sum_{x,y=1}^{p-1}\sum_{c=1}^{p-1}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-(x+y))}{p}\right)+p \\
&= \sum_{x,y=1}^{p-1}\sum_{c=0}^{p-1}\left(\frac{x^2y^2}{p}\right)\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-(x+y))}{p}\right)+p-\sum_{x,y=1}^{p-1}\left(\frac{x^2y^2}{p}\right) \\
&= \sum_{x,y=1}^{p-1}\sum_{c=0}^{p-1}\mathbf{e}\left(\frac{cy^{-2}(x-y)(x^2y^2-(x+y))}{p}\right)+p-(p-1)^2.
\end{aligned} \tag{13.8}$$

If $g(x,y) = (x-y)(x^2y^2-(x+y)) \equiv 0(p)$ 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.

A few words must be said about why we cooked up this family. If, instead of x^2t we had xt, we would have found the condition $d = c(x/y)$. As we have $\left(\frac{cd}{p}\right)$ this would lead to $\left(\frac{c^2}{p}\right)\left(\frac{xy}{p}\right)$ times a similar c-exponential. It would not be sufficient to find how often a similar $g(x,y)$ vanished; we would need to know at which x and y (or, slightly weaker, the value of $\left(\frac{xy}{p}\right)$).

Clearly, whenever $x = y$, $g(x,y) \equiv 0$; therefore there are $p-1$ solutions from this term. For x non-zero, each such pair contributes p, for a total contribution of $(p-1)p$.

More Involved Second Moment: $y^2 = x^3 + tx^2 + 1$

Consider now $x^2y^2 \equiv x + y$, which we may rewrite as a quadratic: $x^2y^2 - y - x \equiv 0$. By Lemma C.3 (the Quadratic Formula mod p), if the discriminant $1 + 4x^3$ is a square mod p there are roots; if it is not a square mod p there are no roots. The roots would be

$$y \equiv \frac{1 \pm \sqrt{1 + 4x^3}}{2x^2}, \tag{13.9}$$

where the square-root and divisions are operations mod p. If $1 + 4x^3$ is a non-zero square, there will be two distinct choices for y. If $1 + 4x^3 \equiv 0$, there is one choice for y, and if $1 + 4x^3$ is not a square mod p, there are no y such that $x^2y^2 \equiv x + y$.

First, a note about our previous conditions. Neither x nor y is allowed to be zero. If $y = 0$ then $x^2y^2 = x + y$ reduces to $x = 0$ (similarly if $x = 0$). Hence we do not need to worry about our

More Involved Second Moment: $y^2 = x^3 + tx^2 + 1$

solutions violating x, y non-zero.

From the above, we've seen that for a given non-zero x, the number of non-zero y with $x^2y^2 \equiv x + y$ is $1 + \left(\frac{4x^3+1}{p}\right)$. Hence the number of non-zero pairs with $x^2y^2 \equiv x + y$ is

$$\sum_{x \neq 0} \left(1 + \left(\frac{4x^3+1}{p}\right)\right) = p - 1 + \sum_{x=0}^{p} \left(\frac{4x^3+1}{p}\right) - 1. \tag{13.10}$$

Each of these pairs contributes p. Thus, these pairs contribute $p^2 - 2p + p\sum_x \left(\frac{4x^3+1}{p}\right)$.

We must be careful about double counting. If both $x - y \equiv 0$ and $x^2y^2 \equiv x + y$, then we find $x^4 \equiv 2x$. As $x \neq 0$, we obtain $x^3 \equiv 2$. If 2 has a cube root mod p, we have double counted three solutions; if it does not, we have counted correctly. Let $h_{3,p}(2)$ denote the number of cube roots of 2 modulo p.

Thus

$$\begin{aligned} A_{2,\mathcal{F}}(p) &= p^2 - 2p + p\sum_{x(p)} \left(\frac{4x^3+1}{p}\right) + p(p-1) - ph_{3,p}(2) + p - (p-1)^2 \\ &= p^2 - ph_{3,p}(2) - 1 + p\sum_{x(p)} \left(\frac{4x^3+1}{p}\right) = p^2 + O(p^{\frac{3}{2}}). \end{aligned} \tag{13.11}$$

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

Kazalicki and Naskrecki proved Bias Conjecture for these families.

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

Numerics

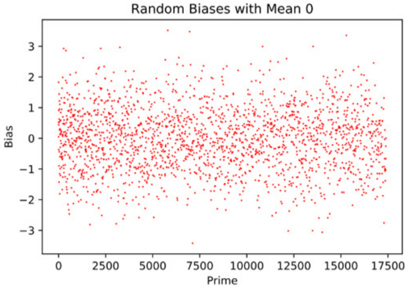
Want to compute all higher moments; however, going beyond the second leads to intractable Legendre sums. Have some numerical results for higher moments.

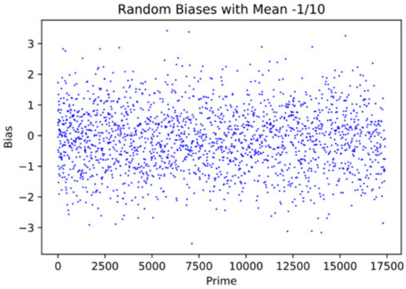
Current SMALL REU has found families with potential positive bias:

- Zoe Batterman <zxba2020@mymail.pomona.edu>
- Aditya Jambhale <adijambhale@gmail.com>
- Akash Narayanan <anaray@umich.edu>
- Kishan Sharma <kds43@cam.ac.uk>
- Andrew Yang <andrewkelvinyang@gmail.com>
- Chris Yao <chris.yao@yale.edu>

Random Experiment

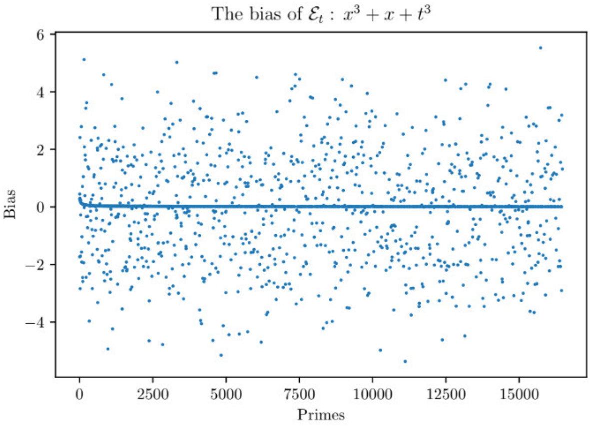
If your experiment needs statistics, you ought to have done a better experiment. – Ernest Rutherford





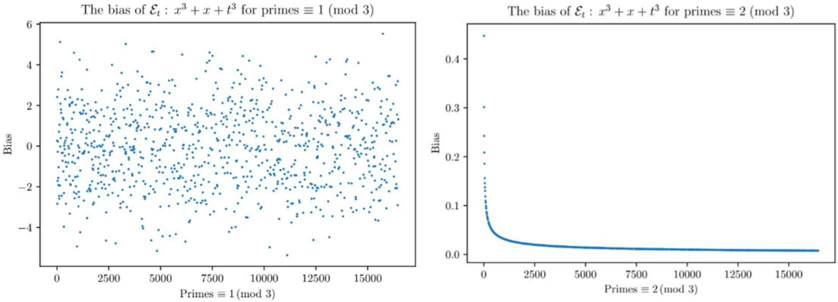
Second Moment: Positive Bias for $y^2 = x^3 + x + T^3$?

Study $(A_{2,\mathcal{E}}(p) - p^2)/p^{3/2}$.



Second Moment: Positive Bias for $y^2 = x^3 + x + T^3$?

Study $(A_{2,\mathcal{E}}(p) - p^2)/p^{3/2}$.



Applications

Biases in Lower Order Terms

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.

Biases in Lower Order Terms

The first family is the family of all elliptic curves; it is a two parameter family and we expect the main term of its second moment to be p^3.

Note that except for our family $y^2 = x^3 + Tx^2 + 1$, all the families $\mathcal{E}$ have $A_{2,\mathcal{E}}(p) = p^2 - h(p)p + O(1)$, where $h(p)$ is non-negative. Further, many of the families have $h(p) = m_{\mathcal{E}} > 0$.

Note $c_1(p)$ is the square of the coefficients from an elliptic curve with complex multiplication. It is non-negative and of size p for $p \not\equiv 3 \bmod 4$, and zero for $p \equiv 1 \bmod 4$ (send $x \mapsto -x \bmod p$ and note $\left(\frac{-1}{p}\right) = -1$).

It is somewhat remarkable that all these families have a correction to the main term in Michel's theorem in the same direction, and we analyze the consequence this has on the average rank. For our family which has a $p^{3/2}$ term, note that on average this term is zero and the p term is negative.

Lower order terms and average rank

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

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

Lower order terms and average rank (cont)

The main term of the first and second moments of the $a_t(p)$ give $r\phi(0)$ and $-\frac{1}{2}\phi(0)$.

Assume the second moment of $a_t(p)^2$ is $p^2 - m_{\mathcal{E}}p + O(1)$, $m_{\mathcal{E}} > 0$.

We have already handled the contribution from p^2, and $-m_{\mathcal{E}}p$ contributes

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

Thus there is a contribution of size $1/\log R$.

Lower order terms and average rank (cont)

A good choice of test functions (see Appendix A of Iwaniec-Luo-Sarnak (ILS)) is the Fourier pair

$$\phi(x) \;=\; \frac{\sin^2(2\pi\frac{\sigma}{2}x)}{(2\pi x)^2}, \qquad \widehat{\phi}(u) \;=\; \begin{cases} \frac{\sigma-|u|}{4} & \text{if } |u| \le \sigma \\ 0 & \text{otherwise.} \end{cases}$$

Note $\phi(0) = \frac{\sigma^2}{4}$, $\widehat{\phi}(0) = \frac{\sigma}{4} = \frac{\phi(0)}{\sigma}$, and evaluating the prime sum gives

$$S_2 \;\sim\; \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2\log R}\right)\frac{m_{\mathcal{E}}}{\log R}\,\phi(0).$$

Lower order terms and average rank (cont)

Let r_t denote the number of zeros of E_t at the central point (i.e., the analytic rank). Then up to our $O\left(\frac{\log\log R}{\log R}\right)$ errors (which we think should be smaller), we have

$$\begin{aligned}
\frac{1}{N}\sum_{t=N}^{2N} r_t\phi(0) &\leq \frac{\phi(0)}{\sigma} + \left(r+\frac{1}{2}\right)\phi(0) + \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2\log R}\right)\frac{m_{\mathcal{E}}}{\log R}\phi(0)\\
\text{Ave Rank}_{[N,2N]}(\mathcal{E}) &\leq \frac{1}{\sigma} + r + \frac{1}{2} + \left(\frac{.986}{\sigma} - \frac{2.966}{\sigma^2\log R}\right)\frac{m_{\mathcal{E}}}{\log R}.
\end{aligned}$$

$\sigma = 1$, $m_{\mathcal{E}} = 1$: for conductors of size 10^{12}, the average rank is bounded by $1 + r + \frac{1}{2} + .03 = r + \frac{1}{2} + 1.03$. This is significantly higher than Fermigier's observed $r + \frac{1}{2} + .40$.

$\sigma = 2$: lower order correction contributes .02 for conductors of size 10^{12}, the average rank bounded by $\frac{1}{2} + r + \frac{1}{2} + .02 = r + \frac{1}{2} + .52$. Now in the ballpark of Fermigier's bound (already there without the potential correction term!).

References

References

- M. Kazalicki and B. Naskrecki, *Diophantine triples and K3 surfaces*, Journal of Number Theory **236** (2022), 41–70, https://arxiv.org/pdf/2101.11705.
- M. Kazalicki and B. Naskrecki, *Second moments and the Bias Conjecture for the family of cubic pencils*, preprint, https://arxiv.org/pdf/2012.11306.pdf.
- 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.

Thank you!

Questions?

Work supported by NSF Grants DMS1561945, DMS1659037, and DMS2241623, the Churchill Program, Dartmouth College, Princeton University and Williams College and the Williams-Exeter Programme.

Families with Constant $j(T)$

Constant $j(T)-$invariant families

Question: What happens in families with constant $j(T)$?

- $\mathcal{E}(T): y^2 = x^3 + A(T)x$ has $j(T) = 1728, \forall T \in \mathbb{Z}$.
- $\mathcal{E}(T): y^2 = x^3 + B(T)$ has $j(T) = 0$.

For these families we can compute any moment.

Computation is *fast* when $j(T)$ is constant.

$j = 0$ Curves

Consider $\mathcal{E} : y^2 = x^3 + B$ over $\mathbb{F}_p$.

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

Gauss' Six-Order Theorem

If $p \equiv 1 \pmod 3$, can write $p = a^2 + 3b^2$, $a \equiv 2 \pmod 3$, $b > 0$, and

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

Moments of One-Parameter $j = 0$ Families

For $r \geq 0$, compute k^{th} moment of $\mathcal{E}_T : y^2 = x^3 - AT^r$.

Have $A_k(p) = 0$ when $p \equiv 3(4)$, and moments determined only by $r \pmod 6$:

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

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

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

$j = 1728$ Curves

Consider $\mathcal{E} : y^2 = x^3 - Ax$ over $\mathbb{F}_p$.

If $p \equiv 3 \pmod 4$, then $a_E(p) = 0$.

Gauss' Four-Order Theorem

If $p \equiv 1 \pmod 4$, then write $p = a^2 + b^2$, 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 $\mathcal{E}(T): y^2 = x^3 - AT^r x$. When $p \equiv 3 \pmod 4$, all moments are 0. Have

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

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

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

Bias in L-functions of Cuspidal Newforms

Cuspidal Newforms

Definition (Holomorphic Form of Weight k, level N)

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

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

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

Modular forms are *periodic* and have a Fourier expansion, if constant term equals 0 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 of a square-free level N.

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 of a square-free level N.

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

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

Study the asymptotic behavior of the moments 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)

Let $\mathcal{F}_{X,\delta,N}$ be the family of cuspidal newforms of weights $k \leq X^\delta$ of a square-free level N, and $M_{r,\sigma}(\mathcal{F}_{X,\delta})$ the limiting r^{th} moment of the family as the level $N \to \infty$. Then

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

where $C_n = \frac{1}{n+1}\binom{2n}{n}$ is the n^{th} Catalan number.

Bias for cuspidal newforms is a positive integer, instead of the negative bias in elliptic curve families.

An Important Tool: Petersson Trace Formula

Petersson Trace Formula

For any $n, m \geq 1$, we have

$$\frac{\Gamma(k-1)}{(4\pi p)^{k-1}} \sum_{f \in H^*_{k,N}(\chi_0)} |\lambda_f(p)|^2 = \delta(p,p) + 2\pi i^{-k} \sum_{c \equiv 0(N)} \frac{S_c(p,p)}{c} J_{k-1}\left(\frac{4\pi p}{c}\right)$$

where $\lambda_f(n)$ is the n-th Hecke eigenvalue of f,
$\delta(m,n)$ is Kronecker's delta,
$S_c(m,n)$ is the classical Kloosterman sum, and
$J_{k-1}(t)$ is the k-Bessel function.

An Important Tool: Petersson Trace Formula

[ILS] gives the following bound for the Petersson Trace Formula:

$$\sum_{f \in H_k^*(N)} \lambda_f(n) = \begin{cases} \delta_{n,\square} \frac{k-1}{12} \frac{\varphi(N)}{\sqrt{n}} & n^{\frac{9}{7}} \leq k^{\frac{16}{21}} N^{\frac{6}{7}} \\ 0 & \text{else} \end{cases} + O\left((n,N)^{-\frac{1}{2}} n^{\frac{1}{6}} k^{\frac{2}{3}} N^{\frac{2}{3}}\right)$$

where level N and n are square-free, $(n, N^2) \mid N$, and $\varphi(n)$ denotes the Euler totient function.

We also find the following relation that allows us to compute higher moments of cuspidal newform families.

$$\lambda_f(p)^r = \sum_{0 \leq l \leq r/2} \mathrm{C}(r-l, l) \lambda_f(p^{r-2l})$$

where $C(n,k) = \binom{n+k}{k} - \binom{n+k}{k-1}$ are numbers in the Catalan's Triangle.

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?