Higher moments of families of elliptic curves

Bartosz Naskręcki

Adam Mickiewicz University in Poznań

Representation Theory XVII

Dubrovnik, October 3rd 2022

Objects

Elliptic curve:

$$E_t : y^2 + a_1(t)xy + a_3(t) = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t)$$

with polynomial coefficients $a_i(t) \in \mathbb{Z}[t]$, $\Delta(t) = \Delta(E_t)$.

- p - prime number
- $E_{p,t}$ - reduction modulo p of the scheme E_t, $t \in \mathbb{F}_p$
- $a_{p,t} = (p+1) - |\overline{E_{p,t}}(\mathbb{F}_p)|$

We introduce a k-th moment of the family E_t

$$M_p^{(k)}(\{E_t\}) = \sum_{\substack{t \in \mathbb{F}_p \\ \Delta(t) \neq 0}} a_{p,t}^k$$

Michel's theorem

Let $a_{p,t} = 2\sqrt{p}\cos(\theta_{p,t})$ where $\theta_{p,t} \in [0, \pi]$. We define

$$sym_k(\theta) = \frac{\sin((k+1)\theta)}{\sin(\theta)}$$

P. Michel (1995)

Let $\{E_t\}$ be a family of elliptic curve with non-constant j-invariant. There exists a constant N such that for all primes $p \nmid N$ and for every positive integer k there exists a constant C such that

$$\left| \sum_{\substack{t \in \mathbb{F}_p \\ \Delta(t) \neq 0}} sym_k(\theta_{p,t}) \right| \leq C\sqrt{p}.$$

Sketch of proof of Michel's theorem

The sum

$$\sum_{\substack{t\in\mathbb{F}_p \\ \Delta(t)\neq 0}} sym_k(\theta_{p,t})$$

is interpreted as trace of Frobenius of a certain ℓ-adic sheaf $\mathcal{F}$ derived from the family $\{E_t\}$.

This sheaf has only three cohomology groups $H^i_c(U, Sym^k(\mathcal{F}))$, $i = 0, 1, 2$.

H^0 vanishes on the punctured affine line U.

H^2 vanishes due to Katz large monodromy results (essential to use the non-triviality of j-invariant!)

Naive second moment

Corollary

$$M_p^{(1)} = C^{(1)} p + O(p^{1/2})$$

$$M_p^{(2)} = p^2 + O(p^{3/2})$$

$$M_p^{(3)} = C^{(3)} p^2 + O(p^{3/2})$$

...

Adding values t such that $\Delta(t) = 0$ might affect the leading term.

How much is known about moments?

- When E_t is a universal family over a modular curve X we have $M_p^{(k)} \sim \sum_f a_p(f)$ ranging over modular forms of fixed level and bounded weight.

How much is known about moments?

- When E_t is a universal family over a modular curve X we have $M_p^{(k)} \sim \sum_f a_p(f)$ ranging over modular forms of fixed level and bounded weight.

- When the j-invariant is constant each moment is a simple character sum.

How much is known about moments?

- When E_t is a universal family over a modular curve X we have $M_p^{(k)} \sim \sum_f a_p(f)$ ranging over modular forms of fixed level and bounded weight.

- When the j-invariant is constant each moment is a simple character sum.

- Birch proved that $M_p^k(y^2 = x^3 + ax + b)$ is a polynomial in p (this uses monodromy results of Katz).

Higher moments

Steven J. Miller, Yan Weng, Jiefei Wu have found a few explicit examples of second moment derivation.
We set $\delta_{a,b}(p)$ to be 1 if p is a mod b and 0 otherwise.

One-Parameter Family	Rank	$M_{1,\mathcal{F}}(p)$	$M_{2,\mathcal{F}}(p)$
$y^2 = x^3 - x^2 - x + t$	0	0	$p^2 - 2p - (-3/p)p$
$y^2 = x^3 - tx^2 + (x-1)t^2$	0	0 on average	$p^2 - \delta_{2,3}(p)(2p) - 2p(-3/p)$ $-p(-2/p) - \left[\sum_{x(p)}(x^3 - x^2 + x/p)\right]^2$
$y^2 = x^3 + tx^2 + t^2$	1	$-p$	$p^2 - 2p - (-3/p)p - 1$
$y^2 = x^3 + tx^2 + tx + t^2$	1	$-p$	$p^2 - p - 1 - \delta_{1,4}(p)(2p)$

Zeta function of a moment

To each sequence $M_{p^i}^{(k)}$ of k-th moments (over varying fields) of a family $\mathcal{F}$ we can associate a rational zeta function

$$Z(\mathcal{M}(\mathcal{F})_p, T) = \exp\left(\sum_{i=1}^{\infty} \frac{M_{2,p^i}}{i} T^i\right)$$

- This is provably a **rational function** (Deligne+Dwork)
- Rationality introduces a natural stratification with respect to weight of the algebraic integers,

$$M_p^{(k)} = \sum_{i=0}^{k} f_i(p)$$

where $f_i(p) = \sum_j \alpha_{i,j}^{(p)}$ with $|\alpha_{\mathrm{i,j}}^{(\mathrm{p})}| = \mathrm{p}^{\mathrm{i}/2}$ and $\alpha_{i,j}^{(p)} \in \overline{\mathbb{Q}}$.

$$|f_i(p)| \leq C \cdot p^{i/2}$$

Mixed motives

The moments zeta functions are **mixed motivic**. It is not clear what pure motives can occur for various families.

In what follows we will explain several cases where the decomposition can be obtained explicitely on the level of the zeta function.

Threefolds approach

Kazalicki-N (JNT, 2022)

Let $E_t : y^2 = x^3 + 2x^2 + \frac{t^2}{t^2+1}x$ be 1-parametric family (which is not universal!) It follows that for every odd prime p

$$M_{2,p}(E_k) = p^2 - c_f(p) - \left(3 + 2\left(\frac{-1}{p}\right)\right)p - 1$$

where f is a unique rational newform which spans $S_4(\Gamma_0(8))$

$$f = q - 4q^3 - 2q^5 + 24q^7 - 11q^9 - 44q^{11} + \dots$$

Exercise

Prove that

$$M_p^{(k)}(y^2 = x^2(x+t)) = 2^{k-1}(p-1).$$

Assume that $\Delta(t) = t$.

Threefolds approach

Let $X : (x^2 - 1)(y^2 - 1)(z^2 - 1) = k^2$ be a threefold in the affine space.

- It parametrizes Diophantine triples (Kazalicki)

Threefolds approach

Let $X : (x^2 - 1)(y^2 - 1)(z^2 - 1) = k^2$ be a threefold in the affine space.

- It parametrizes Diophantine triples (Kazalicki)

It is fibred in surfaces in two different ways:

- (A)X_z is a rational elliptic surface fibration
- (B) X_k is a K3 fibration (Picard rank = 19)

Fun fact: X is a rational threefold
The comparison of point counts with respect to fibrations (A) and (B) and the explicit construction of a correspondence on X_k leads to our theorem.

Correspondence

Let Z denote a K3 surface defined over the complex numbers. Suppose there exists an abelian surface A such that there is a diagram of finite maps

$$A \to Kum(A) \leftarrow Z$$

where $Kum(A)$ denotes the Kummer surface attached to A, i.e. a resolution of singularities of the quotient surface $A/\langle \pm 1 \rangle$.

Sketch of the proof

Starting from the threefold X we construct in several steps an isogeny η with a threefold M which is parametrized in Kummer surfaces $Kum(F_t \times F_t)$ where

- F_t is a universal family with $\mathbb{Z}/2 \oplus \mathbb{Z}/4$ torsion structure.
- Then Deligne's theory implies our result (+ a few technical details).

More details

Let $X_k : (x^2-1)(y^2-1)(z^2-1) = k^2$ be an affine variety defined over a field K of characteristic $\neq 2$. For $k = 0$ this is a union of six planes. For $k \neq 0$ it is a singular model of a K3 surface.

When $charK = 2$ the variety X_k is not reduced. The reduced scheme $X_{k,red} : (x-1)(y-1)(z-1) = k$ is either a union of three lines for $k = 0$ or a rational cubic surface for $k \neq 0$.

Let X denote the total space of the fibration $\pi_{K3} : X \to \mathbb{A}^1$, $\pi_{K3}(x, y, z, k) = k$ where the fibers are varieties X_k. We have another fibration $\pi_{rat} : X \to \mathbb{A}^1$, $\pi_{rat}(x, y, z, k) = z$, where the fibers are denoted Y_z.

Let $\overline{X}$ denote the projective closure of the variety X

$$\overline{X} : (x^2 - w^2)(y^2 - w^2)(z^2 - w^2) - k^2 \cdot w^4 = 0.$$

We have natural extensions $\pi_{K3} : \overline{X} \to \mathbb{P}^1$, $\pi_{K3}([x : y : z : k : w]) = [k : w]$ and $\pi_{rat} : \overline{X} \to \mathbb{P}^1$, $\pi_{rat}([x : y : z : k : w]) = [z : w]$.

Theorem

The projective threefold $\overline{X}$ is birational to $\mathbb{P}^3$.

Let $\phi : \overline{X} \to \mathbb{P}^3$ denote the following rational map

$$\phi([x : y : z : k : w]) = [(x + w)y : (x + w)z : kw : (x + w)w] \tag{1}$$

and let $\psi : \mathbb{P}^3 \to \overline{X}$ denote the map

$$\begin{aligned} \psi([t_1 : t_2 : t_3 : u]) = [&\left(t_1^2 + t_2^2 - t_3^2\right) u^3 - t_1^2 t_2^2 u - u^5 : \\ &-t_1 u^4 + t_1 \left(t_1^2 + t_2^2 + t_3^2\right) u^2 - t_1^3 t_2^2 : \\ &-t_2 u^4 + t_2 \left(t_1^2 + t_2^2 + t_3^2\right) u^2 - t_1^2 t_2^3 : \\ &2t_3 \left(t_1 - u\right)\left(t_1 + u\right)\left(u - t_2\right)\left(t_2 + u\right) : \\ &\left(t_1^2 + t_2^2 + t_3^2\right) u^3 - t_1^2 t_2^2 u - u^5] \end{aligned} \tag{2}$$

We check by a direct computation that $\psi \circ \phi$ and $\phi \circ \psi$ are identity maps, hence both are birational and the proof is complete.

Let p be a prime and let $q = p^m$ for any $m \geq 1$. It follows that

$$\#\overline{X}(\mathbb{F}_q) = q^3 + 3q^2 + \max\{3 - p, 0\} \tag{3}$$

and

$$\#(X \setminus X_{k=0})(\mathbb{F}_q) = \begin{cases} q^3 - 6q^2 + 12q - 9, & p > 2 \\ q^3 - 3q^2 + 3q - 1, & p = 2 \end{cases} \tag{4}$$

We denote by $\tilde{Y}_k$ a minimal smooth projective model of

$$Y_k : Y^2 = X^3+(4z^4+(-2k^2-8)z^2+(2k^2+4))X^2+k^4(z^2-1)^2X,$$

which is an elliptic surface $\pi : \tilde{Y}_k \to \mathbb{P}^1$ with projection π obtained from the natural projection $(X, Y, z) \mapsto z$.

Theorem

Let p be an odd prime and $k \in \mathbb{F}_p$. If $k^2 \notin \{-1, 0\}$ then

$$\#X_k(\mathbb{F}_p) = \#\tilde{Y}_k(\mathbb{F}_p) - 24p + 6.$$

If $k^2 = -1$ then $\#X_k(\mathbb{F}_p) = \#\tilde{Y}_k(\mathbb{F}_p) - 25p + 6$.

Theorem

Let p be an odd prime, and $k \in \mathbb{F}_p$. If $k^2 \notin \{-1, 0\}$ then

$$\#\tilde{Y}_k(\mathbb{F}_p) = 1 + 19p + p^2 + \phi_p(k^2+1)(a_{k,p}^2 - p),$$

where $E_k : y^2 = x(k^2(1+k^2)^3 + 2(1+k^2)^2 x + x^2)$ and $a_{k,p} = p + 1 - \#E_k(\mathbb{F}_p)$. Moreover, if $k^2 = -1$ then

$$\#\tilde{Y}_k(\mathbb{F}_p) = 1 + (20 - \phi_p(-1))p + p^2 + (\lambda(p)^2 - p).$$

$$\sum_{\substack{k\in\mathbb{F}_p,\\ k^2\notin\{-1,0\}}} \phi_p(k^2+1)a_{k,p}^2 = -\sum_{\substack{k\in\mathbb{F}_p,\\ k^2\notin\{-1,0\}}} a_{k,p}^2 + 2\sum_{\substack{k\in\mathbb{F}_p,\\ k^2\notin\{-1,0\},\\ k^2+1=\square}} a_{k,p}^2,$$

where $x = \square$ means that x is a square in $\mathbb{F}_p$. The main idea is to interpret two sums on the right-hand side as traces of Frobenii $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ of certain Galois representations attached to the elliptic surfaces with generic fibers

$$E_k : y^2 = x(k^2(1+k^2)^3 + 2(1+k^2)^2x + x^2),$$

$$F_k : y^2 = (x-(k-1)^2)(x-(k+1)^2)x.$$

To motivate the curve F_k, we start with the following observation. Let p be an odd prime and for $k \in \mathbb{F}_p\backslash\{-1,0,1\}$ let $b_{k,p} = p+1-\#F_k(\mathbb{F}_p)$.

Theorem

If p is an odd prime, then

$$2\lambda(p)^2 + 2 \sum_{\substack{k \in \mathbb{F}_p \\ k^2 \notin \{-1,0\} \\ k^2+1=\square}} a_{k,p}^2 = \sum_{\substack{k \in \mathbb{F}_p \\ k \notin \{-1,0,1\}}} b_{k,p}^2.$$

Galois reps

Let $h_1 : \mathcal{E} \to \mathbb{P}^1$ and $h_2 : \mathcal{F} \to \mathbb{P}^1$ denote two elliptic surfaces with generic fibers E_k and F_k, respectively. We will associate to each elliptic surface a compatible family of ℓ-adic Galois representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ as follows.

Denote by $h_1' : \mathcal{E} \to \mathbb{P}_1^1$ and $h_2' : \mathcal{F} \to \mathbb{P}_2^1$ the restrictions of elliptic surfaces h_1 and h_2 to the complements $\mathbb{P}_i^1 = \mathbb{P}^1 \setminus \{t \in \mathbb{P}^1 : h_i^{-1}(t) \text{ is singular}\}$.

Galois reps

For $j = 1, 2$, a prime ℓ, and a positive integer m, we obtain a sheaf

$$\mathcal{F}_\ell^j = R^1 h'_{j*} \mathbb{Q}_\ell$$

on $\mathbb{P}^1_j$, and also a sheaf $i_* \mathrm{Sym}^m \mathcal{F}_\ell$ on $\mathbb{P}^1_j$ (here $\mathbb{Q}_\ell$ is the constant sheaf on the elliptic surface h_j, R^1 is derived functor and $i : \mathbb{P}^1_j \to \mathbb{P}^1$ the inclusion).

The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the $\mathbb{Q}_\ell$-space

$$W^j_{m,\ell} = H^1_t(\mathbb{P}^1_j \otimes \overline{\mathbb{Q}}, i_* \mathrm{Sym}^m \mathcal{F}^j_\ell)$$

defines an ℓ-adic representation $\rho^m_{j,\ell}$ which is pure of weight $m+1$.

It follows that representations $\rho^m_{j,\ell}$ are unramified for $p > 5$. We denote by $Frob_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ a geometric Frobenius at p.

For a prime $p > 5$, we have that

a)

$$Trace(\rho^2_{1,\ell}(\mathrm{Frob}_p)) = p^2 - 3p - 2\phi_p(-1)p - 2 - \sum_{\substack{k \in \mathbb{F}_p \\ k^2 \notin \{-1,0\}}} a^2_{k,p},$$

b)

$$Trace(\rho^2_{2,\ell}(\mathrm{Frob}_p)) = p^2 - 3p - 4 - \sum_{\substack{k \in \mathbb{F}_p \\ k \notin \{-1,0,1\}}} b^2_{k,p}.$$

Consider the newform

$$f(\tau) = \sum_{n=1}^{\infty} c_f(n) q^n = q - 4q^3 - 2q^5 + 24q^7 + \ldots \in S_4(\Gamma_0(8)).$$

Theorem

Let $p > 5$ be a prime, and $\ell \neq p$. We have that

$$Trace(\rho^2_{1,\ell}(\mathrm{Frob}_p)) = Trace(\rho^2_{2,\ell}(\mathrm{Frob}_p)) = c_f(p).$$

Second equality $Trace(\rho^2_{2,\ell}(\mathrm{Frob}_p)) = c_f(p)$: the equality follows from Deligne's formula relating the trace of Frobenius acting on Galois representation of a universal family of elliptic curves over a modular curve and the trace of Hecke operator T_p acting on corresponding space of cusp forms. In this particular case, the family F_k is a twist by $\sqrt{-1}$ of a universal family

$$y^2 + xy + \left(-\frac{1}{16}k^2 + \frac{1}{16}\right)y = x^3 + \left(-\frac{1}{16}k^2 + \frac{1}{16}\right)x^2$$

of elliptic curves with $\mathbb{Z}/2 \oplus \mathbb{Z}/4$ torsion subgroup.

The corresponding modular curve is $X(\Gamma)$ for $\Gamma = \Gamma_1(4) \cap \Gamma^0(2)$, a congruence subgroup of index 12, with cusps $\{\infty, 0, 1/3, 1/2\}$. The following equalities

$$\begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & \sqrt{2} \end{bmatrix}^{-1} \Gamma_0(8) \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ 0 & \sqrt{2} \end{bmatrix} = \Gamma_0(4) \cap \Gamma^0(2) = \{\pm I\}\Gamma,$$

imply that the map $S_4(\Gamma_0(8)) \to S_4(\Gamma)$, $g(\tau) \mapsto g(\tau/2)$ is an isomorphism. Hence, the space $S_4(\Gamma)$ is 1-dimensional and spanned by $f(\tau/2)$.

First equality $Trace(\rho^2_{1,\ell}(\mathrm{Frob}_p)) = Trace(\rho^2_{2,\ell}(\mathrm{Frob}_p))$:
Our claim is equivalent to:

$$\sum_{\substack{k\in\mathbb{F}_p \\ k\notin\{-1,0,1\}}} b^2_{k,p} - 2\phi_p(-1)p + 2 = \sum_{\substack{k\in\mathbb{F}_p \\ k^2\notin\{-1,0\}}} a^2_{k,p}.$$

We need to prove:

$$\sum_{\substack{k\in\mathbb{F}_p \\ k^2\notin\{-1,0\}}} \phi_p(k^2+1)a^2_{k,p} = -2 - 2\lambda(p)^2 + 2\phi_p(-1)p. \quad (*)$$

(*) follows from the comparison of the point counts on X.

Recent modularity proofs (jointly with Bidisha Roy)

Since the moment sums are motivic (actually mixed motivic), we could match them with (several) modular motives of Scholl.

In her work with Pal and Sadek, Bidisha Roy (arXiv:2111.08393) has proved that finite field analogues of hypergeometric periods of Calabi-Yau manifolds are connected to higher moments of the twisted Legendre and Clausen family of elliptic curves

Using this work we reprove modularity of the rigid Calabi-Yau threefold

$$x + 1/x + y + 1/y + z + 1/z + w + 1/w = 0$$

without Faltings-Serre method and auxiliary trace formulas (Frechette- Ono-Papanikolas).

In our approach we use the explicit computation of higher moments of the higher moments of the Legendre and Clausen family. This is based on the same trick as a key step of Kazalicki-N JNT paper.

In a work in progress with Kazalicki and Roy we plan to directly reprove all modularity results about rigid CY which have hypergeometric periods (a recent result established with different methods by Dieulefait, Gouvea and Yui).

A recent calculation allowed me to prove the modularity of the CY threefold emerging from quantum process and which has the (singular) equation

$$X : w^2 = xy(x-z)(y-z)(yz-(x-t)^2)(xz-(y-t)^2)$$

Bert van Geemen and Dino Festi found (experimentally) that

$$\#X_p(\mathbb{F}_p) = p^3 + 4p^2 - 8p + 1 - b_p$$

where b_p is the p-coefficient of a unique newform for $\Gamma_1(6)$ for primes up to 100.
Using second moments and Kummer surface construction I prove that this holds for every prime p.

Bias

What links all these examples is the **negative** bias of the highest order lower term in the sum

$$M_p^{(2)} = p^2 + A_3(p)p^{3/2} + A_2(p)p^{2/2} + A_1(p)p^{1/2} + A_0 \dots$$

and $\mu_i = \lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} A_i(p)$
First we have $\mu_i = 0$ and then
$\mu_k < 0$ (if it ever happens)

First moment and Nagao conjecture

Nagao conjecture

$$\lim_{x\to\infty} \frac{1}{x} \sum_{p\leq x} M_p^{(1)}(\{E_t\}) \frac{logp}{p} = -\mathrm{rank}\mathcal{E}(\mathbb{Q}(t))$$

$\mathcal{E} \to \mathbb{P}^1$ is an elliptic surface with generic fibre E_t.

The right-hand side is negative of the rank of the part of Picard group of $\mathcal{E}$ of algebraic classes defined over $\mathbb{Q}$

First moment and Nagao conjecture

Rosen-Silverman, 1998

Nagao conjecture holds for elliptic curve with $\deg a_i(t) \leq i$, i.e. $\mathcal{E} \to \mathbb{P}^1$ is a **rational elliptic surface**

Bias

- For the first moment we also had a negative bias (Nagao conjecture)
- We don't really see yet what happens for higher moments (difficult heuristic)
- We need to quantify the statement a bit...

Averages

For each sequence $a = \{a_p\}$ indexed by prime numbers we introduce its average

$$\mu(a) = \lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p\leq x} \frac{a_p}{p^\alpha}$$

where $\alpha = \min\{\beta \geq 0 : \exists_{A\geq 0} \forall_p |a_p| \leq Ap^\beta\}$

- Michel's results says that for non-constant j-invariant families $\mu(f_4(p)) = 1$

Bias conjecture

Bias conjecture

Let E_t be a one-parameter family of elliptic curves over $\mathbb{Q}(t)$. The averages of the lower order terms in the second moment expansion of $M_{2,p}(E_t)$ exist, and the largest lower order term that does not average to 0 is on the average negative.

Extended second moment

It is natural to extend a definition of the second moment to include the fiber at infinity E_∞, so we define

$$\tilde{M}_{2,p}(E_t) = M_{2,p}(E_t) + a^2_{\infty,p}.$$

Pencils of cubics

Theorem (Kazalicki-N,2021(arXiv:2012.11306))

Let $E_t : y^2 = P(x) + tQ(x)$, $P, Q \in \mathbb{Z}[x]$ *typical and* $\max\{\deg P, \deg Q\} = 3$,

$$\widetilde{M}_2^{(p)}(E_t) = \underbrace{p^2}_{=f_4(p)} \underbrace{-p \cdot d_p}_{=f_3(p)} \underbrace{-p \cdot \#S(\mathbb{F}_p)}_{=f_2(p)}$$

where $d_p = p + 1 - \overline{C}(\mathbb{F}_p)$, $\overline{C}$ *is a certain genus* 2 *smooth curve and* S *is a finite scheme.*

Theorem (Kazalicki-N, 2021 (arXiv:2012.11306))

The bias conjecture for the family $\{E_t\}$ *holds under the Sato-Tate conjecture (or rather potential modularity - proved cases) for the curve* $\overline{C}$ *and the negative bias varies between -5 and -1.*

Yet another threefold

The second moment sum for the family $\mathcal{F}_k : y^2 = P(x) + kQ(x)$ is linked to a point count on the following threefold. Let M_{aff} be threefold associated to the Kummer surface $Kum(\mathcal{F}_k \times \mathcal{F}_k)$ over $\mathbb{Q}(k)$

$$M_{aff} : (P(x_1)k + Q(x_1))\cdot(P(x_2)k + Q(x_2)) = y^2 \subset \mathbb{A}^1 \times \mathbb{A}^1 \times \mathbb{A}^1 \times \mathbb{A}^1$$

and let

$$M_\infty : P(x_1)P(x_2) = y^2 \subset \mathbb{A}^1 \times \mathbb{A}^1 \times \mathbb{A}^1$$

be a fiber of threefold M_{aff} at $k = \infty$.

Yet another threefold

Denote by $\iota_{aff} : M_{aff} \to \mathbb{A}^1 \times \mathbb{A}^1 \times \mathbb{P}^1 \times \mathbb{A}^1$ a map

$$\iota_{aff}(x_1, x_2, k, y) \mapsto (x_1, x_2, (k : 1), y)$$

and let

$$\iota_\infty : M_\infty \to \mathbb{A}^1 \times \mathbb{A}^1 \times \mathbb{P}^1 \times \mathbb{A}^1$$

be a map $\iota_\infty(x_1, x_2, y) \mapsto (x_1, x_2, (1 : 0), y)$.
Define

$$M = \iota_{aff}(M_{aff}) \cup \iota_\infty(M_\infty).$$

Extended second moment

In the case when $\mathcal{F}_k$ we have

$$a_{\infty,p} = p - \#\{(x,y) \in \mathbb{F}_p^2 : P(x) = y^2\}$$

Threefold count

Our starting point is the observation that the number of $\mathbb{F}_q$-rational points on a threefold M is equal to

$$q^3 + q^2 + \tilde{M}_{2,q}(\mathcal{F}_k)$$

for any prime power q.

Threefold fibration no.3

The threefold M has two fibrations which we saw previously (rational and K3).
We can compare it, but it also carries a third fibration (a conic bundle) $\pi : M \to \mathbb{A}^2$ where

$$\pi(x_1, x_2, (k : s), y) = (x_1, x_2).$$

Beauville theory tells us the following:

A complete non-singular model $\tilde{M}$ of M has an interesting motive $h^3(\tilde{M})$ which can be related in the case of conic bundles to the Prym variety of the pair of curves $\tilde{C} \to \tilde{\Delta}$.

Curves

- Curve $\Delta : P(x_1)Q(x_2) - P(x_2)Q(x_1) = 0$ is the locus of the discriminant of a conic $\pi^{-1}(x_1, x_2)$.
- For a point $(x_1, x_2) \in \Delta$, the slopes of the degenerate conic $\pi^{-1}(x_1, x_2)$ are described by a point in the curve $C = M_\infty \cap \pi^{-1}(\Delta)$. Suppose $\deg P = 3$, then

$$C : P(x_1)P(x_2) = y^2 \quad \Delta(x_1, x_2) = 0$$

Both curves Δ and C are reducible. In fact, we have

$$\Delta = \tilde{\Delta} \cup \{x_1 = x_2\}.$$

We define also

$$\tilde{C} = M_\infty \cap \pi^{-1}(\tilde{\Delta}).$$

Threefold fibration no.3

The curve $\tilde{\Delta}$ has a natural interpretation as the discriminant curve of the conic bundle π and $\tilde{C}$ corresponds to the Fano variety of lines on $\tilde{C}$.

In fact, as proved by Mumford the Prym variety $Prym(\overline{C}/\overline{\Delta})$ has dimension 2 (in the generic case) and has a polarization of type $(1,2)$ and is linked to a genus 2 curve constructed from $\overline{C}$.

Curves

Let q be a prime power such that $2 \nmid q$. We have

$$\#M(\mathbb{F}_q) = q^3+q^2-q\#\Delta(\mathbb{F}_q)+q\#C(\mathbb{F}_q)+q\left[\sum_{P(x)\equiv 0}\phi_q(Q(x))\right]^2.$$

In particular

$$\tilde{M}_{2,q}(\mathcal{F}_k) = q\left(-\#\Delta(\mathbb{F}_q)+\#C(\mathbb{F}_q)+\left[\sum_{P(x)\equiv 0}\phi_q(Q(x))\right]^2\right).$$

Curves

Generically curves $\tilde{\Delta}$ and $\tilde{C}$ are geometrically irreducible.

There is a natural double cover $\tilde{C} \to \tilde{\Delta}$ and the smooth models $\overline{\Delta}$ and $\overline{C}$ have genus 1 and 3, respectively. We call such a pair typical.

Let q be an odd prime power. Assume that $(\tilde{\Delta}, \tilde{C})$ is typical and $\deg P = 3$. We have the equality

$$\tilde{M}_{2,q}(\mathcal{F}) = q \cdot (\#\overline{C}(\mathbb{F}_q) - \#\overline{\Delta}(\mathbb{F}_q) + q - \#S(\mathbb{F}_q))$$

where $S : \Delta(x, x) = 0$

Curve quotients

Suppose that $\tilde{C}$ is geometrically irreducible and geometrically reduced.
Let τ_1, τ_2 and τ_3 be three involutions of $\overline{C}$ whose restriction to $\tilde{C}$ are equal to

- $(x_1, x_2, y) \mapsto (x_1, x_2, -y)$,
- $(x_1, x_2, y) \mapsto (x_2, x_1, -y)$,
- $(x_1, x_2, y) \mapsto (x_2, x_1, y)$

Denote by $\phi_i : \overline{C} \to C_i$: non-singular projective quotients of $\overline{C}$ by τ_i

- Note that $C_1 =: \overline{\Delta}$ is nonsingular projective closure of $\tilde{\Delta}$.
- Denote by $\phi_4 : \overline{C} \to C_4$ the nonsingular projective quotient of $\overline{C}$ by the group G generated by involutions τ_i.

Point counts

For a prime power q and $\tilde{C}$ geometrically irreducible and geometrically reduced over $\mathbb{F}_q$ we have

$$\#\overline{C}(\mathbb{F}_q) + 2\#C_4(\mathbb{F}_q) = \#C_1(\mathbb{F}_q) + \#C_2(\mathbb{F}_q) + \#C_3(\mathbb{F}_q).$$

In fact, formula above is a finite field analogue of a theorem of Accola applied to the automorphism group $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ acting on $\overline{C}$:

$$g(\overline{C}) + 2g(C_4) = g(C_1) + g(C_2) + g(C_3)$$

when the field characteristic of the curves $\overline{C}$, C_i is odd or zero.

Genera of curves

Let q be an odd prime power. Let K denote a field such that $char(K) \neq 2$. For a typical pair $(\tilde{\Delta}, \tilde{C})$ we have that

- $g(C_4) = 0$
- $g(C_3) = 0$
- $g(C_2) = 2$
- $g(C_1) = 1$
- $g(\overline{C}) = 3$

Hence, the curve $\overline{C}$ is bielliptic and hyperelliptic. When the pair $(\tilde{\Delta}, \tilde{C})$ is typical we have

$$\#\overline{C}(\mathbb{F}_q) - \#\overline{\Delta}(\mathbb{F}_q) = \#C_2(\mathbb{F}_q) - (q+1).$$

Final step

So for a typical pair $\overline{\Delta}, \overline{C}$ we have

$$\widetilde{M}_2^{(p)}(\mathcal{F}_k) = \underbrace{p^2}_{=f_4(p)} \underbrace{-p \cdot d_p}_{=f_3(p)} \underbrace{-p \cdot \#S(\mathbb{F}_p)}_{=f_2(p)}$$

where $d_p = p + 1 - \#C_2(\mathbb{F}_p)$.

- Sato-Tate conjecture implies that $\mu(d_p) = 0$.
- The average $\mu(\#S(\mathbb{F}_p))$ is always positive by Chebotarev theorem.

Thank you