Effective Sato-Tate conjecture for abelian varieties with applications

Francesc Fité[1] (Universitat de Barcelona),
jointly with A. Bucur and K.S. Kedlaya

Representation theory XVIII (Dubrovnik)

22/6/2023

[1]Funded by the Ramón y Cajal fellowship RYC2019-027378-I.

Notations

Throughout the talk:

- k is a number field.
- A/k is an abelian variety of dimension $g \geq 1$.
- N denotes the absolute conductor of A.
- For a prime ℓ,

$$\varrho_{A,\ell} \colon G_k \to \mathrm{Aut}(V_\ell(A))$$

  the ℓ-adic representation attached to A, where

$$T_\ell(A) := \varprojlim A[\ell^n](\overline{\mathbb{Q}}) \simeq \mathbb{Z}_\ell^{2g}\,, \qquad V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell\,.$$

- $\mathfrak{p}$ is a prime of k not dividing $N\ell$.

Equidistribution of Frobenius traces

- The Frobenius trace at $\mathfrak{p}$ is

$$a_\mathfrak{p} := a_\mathfrak{p}(A) := \mathrm{Tr}(\varrho_{A,\ell}(\mathrm{Frob}_\mathfrak{p})).$$

- By the Hasse-Weil bound, the normalized Frobenius trace

$$\overline{a}_\mathfrak{p} := \frac{a_\mathfrak{p}}{\mathrm{Nm}(\mathfrak{p})^{1/2}} \in [-2g, 2g]\,.$$

- What is the distribution of the sequence $\{\overline{a}_\mathfrak{p}\}_\mathfrak{p}$?

  In oder words, for a subinterval $I \subseteq [-2g, 2g]$, does

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \text{ and } \overline{a}_\mathfrak{p} \in I\}}{\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x\}}$$

  exist and can it be predicted?

The Sato-Tate group

- Denote by G_ℓ the Zariski closure of the image of $\varrho_{A,\ell}$ in $\mathrm{GSp}_{2g}/\mathbb{Q}_\ell$.

Conjecture (Mumford-Tate; Serre)

- Let $\mathrm{MT}(A)/\mathbb{Q}$ be the Mumford-Tate group of A. Then

$$G_\ell^0 = \mathrm{MT}(A) \times_{\mathbb{Q}} \mathbb{Q}_\ell \qquad \text{for every prime } \ell\,.$$

- There is an algebraic subgroup G of $\mathrm{GSp}_{2g}/\mathbb{Q}$, with $G^0 = \mathrm{MT}(A)$, such that

$$G_\ell = G \times_{\mathbb{Q}} \mathbb{Q}_\ell \qquad \text{for every prime } \ell\,.$$

- From now on, we will assume the above conjecture.
- The *Sato–Tate group* of A is

$$\mathrm{ST}(A) = \text{maximal compact subgroup of } (G \cap \mathrm{Sp}_{2g})(\mathbb{C})\,.$$

The Sato-Tate measure

- By construction
$$\mathrm{ST}(A) \subseteq \mathrm{USp}(2g)\,,$$
and hence
$$\mathrm{Tr}\colon\ \mathrm{ST}(A) \to [-2g, 2g]\,.$$
- The *Sato–Tate measure* of A is
$$\mu = \mathrm{Tr}_*(\text{Haar measure of } \mathrm{ST}(A))$$

Example

If A is an elliptic curve without complex multiplication, then
$$\mathrm{ST}(A) = \mathrm{SU}(2)\,, \qquad \mu = \frac{1}{2\pi}\sqrt{4 - z^2}dz\,.$$

The Sato-Tate conjecture

Sato-Tate conjecture v1

For any subinterval $I \subseteq [-2g, 2g]$, we have

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \le x \text{ and } \overline{a}_{\mathfrak{p}} \in I\}}{\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \le x\}} = \mu(I)\,.$$

The prime number theorem gives

$$\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \le x\} = \mathrm{Li}(x) + o\left(\frac{x}{\log(x)}\right), \quad \mathrm{Li}(x) := \int_2^x \frac{dt}{\log(t)} \sim \frac{x}{\log(x)}.$$

Sato-Tate conjecture v2

For any subinterval $I \subseteq [-2g, 2g]$, we have

$$\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \le x \text{ and } \overline{a}_{\mathfrak{p}} \in I\} = \mu(I)\,\mathrm{Li}(x) + o\left(\frac{x}{\log(x)}\right)\,.$$

Effective Sato–Tate conjecture

Effective prime number theorem

Assuming the Riemann hypothesis, for $0 < \varepsilon < 1/2$, we have

$$\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x\} = \mathrm{Li}(x) + O_k(x^{1-\varepsilon}) \qquad \text{for } x \gg 0\,.$$

In analogy, one may expect:

Effective Sato-Tate conjecture

For $0 < \varepsilon < 1/2$ and for every subinterval $I \subseteq [-2g, 2g]$, we have

$$\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \text{ and } \overline{a}_{\mathfrak{p}} \in I\} = \mu(I)\,\mathrm{Li}(x) + O_{k,g,N}(x^{1-\varepsilon}) \qquad \text{for } x \gg_I 0\,.$$

Main result

Theorem (Bucur-F.-Kedlaya)

Suppose:

- *The Mumford-Tate conjecture holds;*
- $\mathrm{ST}(A)$ *is connected;*
- *GRH holds for the L-functions associated to the irreducible representations of* $\mathrm{ST}(A)$.

Let $\mathfrak{g} = \mathrm{Lie}(\mathrm{ST}(A))$ *and write*

$$\varepsilon := \frac{1}{2(q+\varphi)}, \quad \textit{where } \begin{cases} q = \textit{rank of } \mathfrak{g}, \\ \varphi = \textit{number of positive roots of } \mathfrak{g}^{\mathrm{ss}}. \end{cases}$$

Then, for any subinterval $I \subseteq [-2g, 2g]$, *we have*

$$\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \textit{ and } \overline{a}_{\mathfrak{p}} \in I\} = \mu(I)\,\mathrm{Li}(x) + O_{k,g}\left(\frac{x^{1-\varepsilon}(\log(Nx))^{2\varepsilon}}{\log(x)^{1-4\varepsilon}}\right)$$

for $x \gg_I 0$.

Predictions for dimensions $g = 1$ and $g = 2$

g	Splitting of A	ST(A)	q	φ	ε
1	E	SU(2)	1	1	1/4
1	E_{CM}	U(1)	1	0	1/2
2	S	USp(4)	2	4	1/12
2	S_{RM} $E \times E'$	SU(2) × SU(2)	2	2	1/8
2	$E \times E'_{CM}$	SU(2) × U(1)	2	1	1/6
2	$E_{CM} \times E'_{CM}$ S_{CM}	U(1) × U(1)	2	0	1/4
2	E^2 S_{QM}	SU(2)	1	1	1/4
2	E^2_{CM}	U(1)	1	0	1/2

- Case E above (non CM e.c.) extends work by Murty (1983).
- Case $E \times E'$ above (nonisogenous non CM e.c.) extends work by Bucur and Kedlaya (2015).

The Sato–Tate conjecture and L-functions

Let Γ be an irreducible representation of $\mathrm{ST}(A)$.

- One attaches to Γ an ℓ-adic representation $\Gamma\varrho_{A,\ell} : G_k \to \mathrm{Aut}(V_\Gamma)$.
- It is pure of some weight w_Γ.
- One attaches to $\Gamma\varrho_{A,\ell}$ an Euler product:

$$L(\Gamma(A), s) := \prod_{\mathfrak{p}} \det(1 - \Gamma\varrho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})\, \mathrm{Nm}(\mathfrak{p})^{-s-w_\Gamma} \mid V_\Gamma^{I_{\mathfrak{p}}})^{-1}\,,$$

  which is absolutely convergent for $\Re(s) > 1$.

Theorem (Serre '68)

Suppose that for every irreducible nontrivial representation Γ of $\mathrm{ST}(A)$

$L(\Gamma(A), s)$ extends to a holomorphic function on an open neighborhood of $\Re(s) \geq 1$ and that does not vanish at $\Re(s) = 1$.

Then the Sato–Tate conjecture holds for A.

Ingredients in the proof (I): Murty's estimate

- $L(\Gamma(A), s)$ gives rise to a completed L-function

$$\Lambda(\Gamma(A), s) := B^{s/2} \cdot L(\Gamma(A), s) \cdot L_\infty(\Gamma(A), s)\,.$$

Conjecture (Generalized Riemann hypothesis for $\Lambda(\Gamma(A), s)$)

- $\Lambda(\Gamma(A), s)$ extends to a meromorphic function over $\mathbb{C}$. It has simple poles at $s = 0, 1$ if Γ is trivial and it is analytic otherwise.
- $\Lambda(\Gamma(A), s) = \varepsilon \cdot \Lambda(\Gamma^\vee(A), 1 - s)$ for some $\varepsilon \in \mathbb{C}$ with $|\varepsilon| = 1$.
- All zeroes of $\Lambda(\Gamma(A), s)$ lie on the line $\Re(s) = 1/2$.

Theorem (Murty '83; Bucur-Kedlaya 2015)

Let Γ be nontrivial. Suppose that GRH holds for $\Lambda(\Gamma(A), s)$.

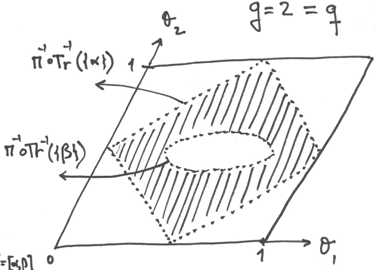
Let $\chi = \mathrm{Tr}(\Gamma)$, $d_\chi = \dim(\Gamma)$, and $w_\chi = w_\Gamma$. Then

$$\sum_{\mathrm{Nm}(\mathfrak{p}) \le x} \chi(\mathrm{Frob}_\mathfrak{p}) = O_{k,g}(d_\chi x^{1/2} \log(N(x + w_\chi)))\,.$$

Ingredients in the proof (II): the Vinogradov function

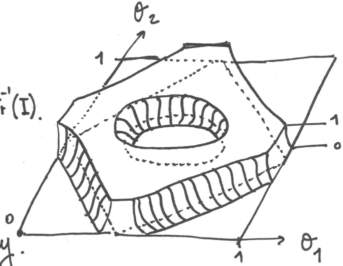
We construct a function:

$$\begin{array}{ccc} F_I : \mathbb{R}^q & \longrightarrow & [0,1] \\ \pi \searrow & & \nearrow \\ & [0,1]^q / W \simeq \mathrm{Conj}(ST(A)) & \\ & \downarrow \mathrm{Tr} & \\ & [-2g, 2g] \supseteq I = [\alpha, \beta] & \end{array}$$



with the properties:

- F_I is a continuous approximation of the characteristic function of $\pi^{-1} \circ \mathrm{Tr}^{-1}(I)$.
- $F_I(\underline{\theta}) = \sum_{\underline{m} \in \mathbb{Z}^q} c_{\underline{m}} e^{2\pi i \underline{\theta} \cdot \underline{m}}$ has Fourier coefficients of rapid decay.



Ingredients of the proof (III): Gupta's formula

- $\varrho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ uniquely determines $\theta_{\mathfrak{p}} \in \mathrm{Conj}(\mathrm{ST}(A)) \simeq [0,1]^q/\mathcal{W}$.

  We have $\mathrm{Tr}(\theta_{\mathfrak{p}}) = \overline{a}_{\mathfrak{p}}$.
- By construction

$$\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \leq x \text{ and } \overline{a}_{\mathfrak{p}} \in I\} \approx \sum_{\mathrm{Nm}(\mathfrak{p}) \leq x} F_I(\theta_{\mathfrak{p}})\,.$$

- F_I is a class function of $\mathrm{ST}(A)$, and hence is a linear combination of irreducible characters

$$F_I(\theta) = \sum_{\theta \in \mathbb{Z}^q} c_m e^{2\pi i \theta \cdot m} = \sum_{\chi} c_\chi \chi\,.$$

- Gupta's formula expresses the c_χ in terms of the c_m. It allows to see that the c_χ are still of rapid decay.

The three ingredients combined

- One has $c_1 \approx \mu(I)$, and then

$$\begin{aligned}\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \le x \text{ and } \overline{a}_\mathfrak{p} \in I\} &\approx \sum_{\mathrm{Nm}(\mathfrak{p}) \le x} F_I(\theta_\mathfrak{p}) \\ &\approx \mu(I)\,\mathrm{Li}(x) + \sum_{\chi \ne 1} c_\chi \sum_{\mathrm{Nm}(\mathfrak{p}) \le x} \chi(\theta_\mathfrak{p})\,.\end{aligned}$$

- For $\chi \neq 1$ Murty's estimate gives

$$\sum_{\mathrm{Nm}(\mathfrak{p}) \le x} \chi(\mathrm{Frob}_\mathfrak{p}) = O_{k,g}(d_\chi x^{1/2} \log(N(x + w_\chi)))\,.$$

- The *rapid decay* of the coefficients c_χ compensates the *rapid growth* of the dimensions d_χ, which is exponential in φ.

Interval variant of Linnik's problem for abelian varieties

Corollary 1

Assume the hypotheses of the main result.

For any nonempty subinterval $I \subseteq [-2g, 2g]$, there exists a prime $\mathfrak{p} \nmid N$ such that $\overline{a}_{\mathfrak{p}} \in I$ and

$$\mathrm{Nm}(\mathfrak{p}) = O_{k,g,I}(\log(2N)^2 \cdot \log(\log(4N))^4) \,.$$

- This generalizes work of Chen–Park–Swaminathan, who considered the case in which A is an elliptic curve.

Proof

One needs to ensure that:

The main term $\frac{x}{\log(x)}$ dominates the error term $\frac{x^{1-\varepsilon}\log(Nx)^{2\varepsilon}}{\log(x)^{1-4\varepsilon}}$.

This amounts to asking $x \gg_{k,g,I} \log(x)^4 \log(Nx)^2$.

Sign variant of Linnik's problem for two elliptic curves

- On this slide, let $A, A'/\mathbb{Q}$ be elliptic curves of conductors N, N'.

Theorem (Faltings '83; corollary of the Isogeny theorem)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \neq a_p(A')$.

- Under GRH for Artin L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^{12})$$

(Serre '86; using "Effective Chebotarev").

Theorem (Harris '09; corollary of Sato-Tate for $A \times A'$ over $\mathbb{Q}$)

If A, A' are not isogenous, then there exists $p \nmid NN'$ such that $a_p(A) \cdot a_p(A') < 0$.

- Under GRH for Symmetric power L-functions, such a p can be taken with

$$p = O(\log(NN')^2 \log(\log(2NN'))^{6})$$

(Bucur and Kedlaya 2015; using "Effective Sato-Tate").

Sign variant of Linnik's problem for two abelian varieties

Corollary 2

Let A, A' be abelian varieties. Suppose:

- The Mumford–Tate conjecture holds for A and A';
- $\mathrm{ST}(A)$, $\mathrm{ST}(A')$ are connected;
- GRH holds for $\Lambda(\Gamma(A) \otimes \Gamma'(A'), s)$ for all irreducible rep. Γ, Γ'.
- $\mathrm{ST}(A \times A') \simeq \mathrm{ST}(A) \times \mathrm{ST}(A')$.

Then, there exists $\mathfrak{p} \nmid NN'$ such that $a_{\mathfrak{p}}(A) \cdot a_{\mathfrak{p}}(A') < 0$ and

$$\mathrm{Nm}(\mathfrak{p}) = O_{k,g}(\log(2NN')^2 \log(\log(4NN'))^6)\,.$$

- Condition $\mathrm{ST}(A \times A') \simeq \mathrm{ST}(A) \times \mathrm{ST}(A')$ can be replaced by the weaker condition $\mathrm{Hom}(A, A') = 0$.