



## CENTRE DE RECERCA MATEMÀTICA

Title: *Arithmetic invariants from Sato-Tate moments*  
Journal Information: *Comptes Rendus Mathématique*  
Author(s): Edgar Costa and Francesc Fité and Andrew V. Sutherland.  
Volume, pages: 823-826, DOI:[[www.doi.org/10.1016/j.crma.2019.11.008](http://www.doi.org/10.1016/j.crma.2019.11.008)]

## ARITHMETIC INVARIANTS FROM SATO–TATE MOMENTS

EDGAR COSTA, FRANCESC FITÉ, AND ANDREW V. SUTHERLAND

ABSTRACT. We give some arithmetic-geometric interpretations of the moments  $M_2[a_1]$ ,  $M_1[a_2]$ , and  $M_1[s_2]$  of the Sato–Tate group of an abelian variety  $A$  defined over a number field by relating them to the ranks of the endomorphism ring and Néron–Severi group of  $A$ .

Let  $A$  be an abelian variety of dimension  $g \geq 1$  defined over a number field  $k$ . For a rational prime  $\ell$ , let

$$\rho_{A,\ell}: G_k \rightarrow \text{Aut}(V_\ell(A))$$

denote the  $\ell$ -adic representation attached to  $A$  given by the action of the absolute Galois group of  $G_k$  on the rational Tate module of  $A$ . Let  $G_\ell$  denote the Zariski closure of the image of  $\rho_{\ell,A}$ , viewed as a subgroup scheme of  $\text{GSp}_{2g}$ , let  $G_\ell^1$  denote the kernel of the restriction to  $G_\ell$  of the similitude character, and fix an embedding  $\iota$  of  $\mathbb{Q}_\ell$  into  $\mathbb{C}$ . The *Sato–Tate group*  $\text{ST}(A)$  of  $A$  is a maximal compact subgroup of the  $\mathbb{C}$ -points of the base change  $G_\ell^1 \times_{\mathbb{Q}_\ell, \iota} \mathbb{C}$  (see [FKRS12, §2] and [Ser12, Chap. 8]).

Throughout this note we shall assume that the algebraic Sato–Tate conjecture of Banaszak and Kedlaya [BK16, Conjecture 2.3] holds for  $A$ . This conjecture is known, for example, when  $g \leq 3$  (see [BK16, Thm. 6.10]), or more generally, whenever the Mumford–Tate conjecture holds for  $A$  (see [CC]). It predicts the existence of an algebraic reductive group  $\text{AST}(A)$  defined over  $\mathbb{Q}$  such that

$$\text{AST}(A) \times_{\mathbb{Q}} \mathbb{Q}_\ell \simeq G_\ell^1$$

for every prime  $\ell$ . In this case  $\text{ST}(A)$  can be defined as a maximal compact subgroup of the  $\mathbb{C}$ -points of  $\text{AST}(A) \times_{\mathbb{Q}} \mathbb{C}$ , which depends neither on the choice of a prime  $\ell$  nor on the choice of an embedding  $\iota$ .

By construction  $\text{ST}(A)$  comes equipped with a faithful self-dual representation

$$\rho: \text{ST}(A) \rightarrow \text{GL}(V),$$

where  $V$  is a  $\mathbb{C}$  vector space of dimension  $2g$ . We call  $\rho$  the standard representation of  $\text{ST}(A)$  and use it to view  $\text{ST}(A)$  as a compact real Lie subgroup of  $\text{USp}(2g)$ .

In this note we are interested in the following three virtual characters of  $\text{ST}(A)$ :

$$a_1 = \text{Tr}(V), \quad a_2 = \text{Tr}(\wedge^2 V), \quad s_2 = a_1^2 - 2a_2.$$

For a nonnegative integer  $j$ , define the  $j$ th moment of a virtual character  $\varphi$  as the virtual multiplicity of the trivial representation in  $\varphi^j$ . In particular, we have

$$\begin{aligned} (1) \quad M_2[a_1] &= \dim_{\mathbb{C}}(V^{\otimes 2})^{\text{ST}(A)}, \\ M_1[a_2] &= \dim_{\mathbb{C}}(\wedge^2 V)^{\text{ST}(A)}, \\ M_1[s_2] &= M_2[a_1] - 2M_1[a_2]. \end{aligned}$$

Let  $\text{End}(A)$  denote the ring of endomorphisms of  $A$  (defined over  $k$ ).

**Proposition 1.** *We have*

$$M_2[a_1] = \text{rk}_{\mathbb{Z}}(\text{End}(A)).$$

*Proof.* By Faltings isogeny theorem [Fal83], we have

$$\text{rk}_{\mathbb{Z}}(\text{End}(A)) = \dim_{\mathbb{Q}_\ell}(\text{End}(A) \otimes \mathbb{Q}_\ell) = \dim_{\mathbb{Q}_\ell}(\text{End}_{G_\ell}(V_\ell(A))).$$

Observing that homotheties centralize  $V_\ell(A) \otimes V_\ell(A)^\vee$  and Weyl’s unitarian trick allows us to pass from  $G_\ell^1$  to the maximal compact subgroup  $\text{ST}(A)$ , we obtain

$$\dim_{\mathbb{Q}_\ell}((V_\ell(A) \otimes V_\ell(A)^\vee)^{G_\ell}) = \dim_{\mathbb{Q}_\ell}((V_\ell(A) \otimes V_\ell(A)^\vee)^{G_\ell^1}) = \dim_{\mathbb{C}}((V \otimes V^\vee)^{\text{ST}(A)}).$$

The proposition follows from the definition of  $M_2[a_1]$  and the self-duality of  $V$ .  $\square$

Let  $\text{NS}(A)$  denote the Néron–Severi group of  $A$ .

**Proposition 2.** *We have*

$$M_1[a_2] = \text{rk}_{\mathbb{Z}}(\text{NS}(A)).$$

*Proof.* As explained in [Tat65, §2] (and in [Tat66, Eq. (9)] using the same argument over finite fields), Faltings isogeny theorem provides an isomorphism

$$\text{NS}(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \simeq (H_{\text{ét}}^2(A_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)(1))^{G_k} \simeq ((\wedge^2 V_\ell(A))(-1))^{G_\ell},$$

where we have denoted Tate twists in the usual way and we have used the isomorphism  $V_\ell(A) \simeq H_{\text{ét}}^1(A_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)(1)$ . Then, as in the proof of Proposition 1, we have

$$\text{rk}_{\mathbb{Z}}(\text{NS}(A)) = \dim_{\mathbb{Q}_\ell}((\wedge^2 V_\ell(A))(-1))^{G_\ell^1} = \dim_{\mathbb{C}}(\wedge^2 V)^{\text{ST}(A)} = M_1[a_2],$$

which completes the proof.  $\square$

In order to obtain a description of  $M[s_2]$ , we will first relate  $\text{rk}_{\mathbb{Z}}(\text{End}(A))$  with  $\text{rk}_{\mathbb{Z}}(\text{NS}(A))$ . There are three division algebras over  $\mathbb{R}$ : the quaternions  $\mathbb{H}$ , the complex field  $\mathbb{C}$ , and the real field  $\mathbb{R}$  itself. By Wedderburn’s theorem we have

$$(2) \quad \text{End}(A) \otimes \mathbb{R} \simeq \prod_i M_{t_i}(\mathbb{R}) \times \prod_i M_{n_i}(\mathbb{H}) \times \prod_i M_{p_i}(\mathbb{C}),$$

for some nonnegative integers  $t_i, n_i, p_i$ , where  $M_n$  denotes the  $n \times n$  matrix ring.

**Lemma 3.** *With the notation of equation (2), we have*

$$\text{rk}_{\mathbb{Z}}(\text{End}(A)) - 2 \cdot \text{rk}_{\mathbb{Z}}(\text{NS}(A)) = 2 \sum_i n_i - \sum_i t_i.$$

*In particular, we have the following inequality*

$$(3) \quad 2 \cdot \text{rk}_{\mathbb{Z}}(\text{NS}(A)) - g \leq \text{rk}_{\mathbb{Z}}(\text{End}(A)) \leq 2 \cdot \text{rk}_{\mathbb{Z}}(\text{NS}(A)) + g.$$

*Proof.* Let  $\dagger$  denote the Rosati involution of  $\text{End}(A) \otimes \mathbb{R}$ . As explained in [Mum70, p. 190], we have  $\text{rk}_{\mathbb{Z}}(\text{NS}(A)) = \dim_{\mathbb{R}}((\text{End}(A) \otimes \mathbb{R})^\dagger)$ . For the first part of the lemma, it thus suffices to prove

$$(4) \quad \dim_{\mathbb{R}}(\text{End}(A) \otimes \mathbb{R}) - 2 \cdot \dim_{\mathbb{R}}((\text{End}(A) \otimes \mathbb{R})^\dagger) = 2 \sum_i n_i - \sum_i t_i.$$

We say that an abelian variety defined over  $k$  is isotypic if it is isogenous (over  $k$ ) to the power of a simple abelian variety. Since both the left-hand and right-hand

sides of (4) are additive in the isotypic components of  $A$ , we may reduce to the case that  $A$  is isotypic. We thus may assume that  $A$  is the  $r$ th power of a simple abelian variety  $B$ . By Albert's classification of division algebras with a positive involution [Mum70, Thm. 2, §21], there are four possibilities for  $\text{End}(A) \otimes_{\mathbb{Z}} \mathbb{R}$ , namely

$$(I) M_r(\mathbb{R}^e), \quad (II) M_r(M_2(\mathbb{R})^e), \quad (III) M_r(\mathbb{H}^e), \quad (IV) M_r(M_d(\mathbb{C})^e),$$

where  $e$  and  $d$  are nonnegative integers. The action of the Rosati involution  $\dagger$  on  $\text{End}(A) \otimes_{\mathbb{Z}} \mathbb{R}$  is also described in [Mum70, Thm. 2, §21], and the dimension of its fixed subspace can be easily read from the parameter  $\eta$  listed on [Mum70, Table on p. 202]. The first part of the lemma then follows from the computations listed in Table 1.

For the second part of the lemma we need to show that

$$\left| 2 \sum_i n_i - \sum_i t_i \right| \leq g.$$

This is immediate from Table 1 once we take into account that  $e \leq \dim(B)$  for type (I), and  $2e \leq \dim(B)$  for types (II) and (III) (see [Mum70, Table on p. 202]).  $\square$

TABLE 1.  $\mathbb{R}$ -algebra dimensions for isotypic  $A$  by Albert type.

Type	$\dim_{\mathbb{R}}(\text{End}(A) \otimes \mathbb{R})$	$\dim_{\mathbb{R}}((\text{End}(A) \otimes \mathbb{R})^{\dagger})$	$2 \sum_i n_i - \sum_i t_i$
(I)	$er^2$	$er(r+1)/2$	$-er$
(II)	$4er^2$	$e(r+2r^2)$	$-2er$
(III)	$4er^2$	$e(-r+2r^2)$	$2er$
(IV)	$2er^2d^2$	$er^2d^2$	$0$

As an immediate consequence of Proposition 1, Proposition 2, and Lemma 3, we obtain the following corollary.

**Corollary 4.** *With the notation of equation (2), we have*

$$M_1[s_2] = 2 \sum_i n_i - \sum_i t_i.$$

*Remark 5.* The moment  $M_1[s_2]$  can also be interpreted as a Frobenius–Schur indicator, which allows us to give an alternative proof of (4), conditional on the Mumford–Tate conjecture, that does not make use of Albert's classification. Recall that  $\rho : \text{ST}(A) \rightarrow \text{GL}(V)$  denotes the standard representation of  $\text{ST}(A)$  and let  $\Psi^2(\rho)$  be the central function defined as  $\Psi^2(\rho)(g) = \rho(g^2)$  for every  $g \in \text{ST}(A)$ ; note that  $s_2$  is simply  $\text{Tr} \Psi^2(\rho)$ . Thus the moment  $M_1[s_2]$  is the Frobenius–Schur indicator  $\mu(\rho)$  of the standard representation  $\rho$ , which is just the multiplicity of the trivial representation in  $\Psi^2(\rho)$ . Inequality (4) simply asserts that the trivial bound  $|\mu(\rho)| \leq 2g$  can be improved to the sharper bound  $|\mu(\rho)| \leq g$ . Recall that the Frobenius–Schur indicator of an irreducible representation can only take the values 1,  $-1$ , and 0 depending on whether the representation is realizable over  $\mathbb{R}$ , has real trace but it is not realizable over  $\mathbb{R}$ , or has trace taking some value in  $\mathbb{C} \setminus \mathbb{R}$ , respectively (see [Ser77, p. 108]). To obtain the sharper bound, it suffices to show that any irreducible constituent  $\sigma$  of the standard representation  $\rho$  having

real trace must have dimension at least 2. This follows from our assumption that the Mumford–Tate conjecture holds for  $A$ .

The results in this note explain, in particular, certain redundancies in Table 8 of [FKRS12] that Seouyoung Kim used to prove Proposition 1 in the case where  $A$  is an abelian surface [Kim, Proof of Thm. 3.4].

#### ACKNOWLEDGMENTS.

The main results of this paper were discovered during the *Arithmetic of Curves* workshop held at Baskerville Hall in Hay-on-Wye Wales in August 2018. We thank the organizers Alexander Betts, Tim and Vladimir Dokchitser, and Celine Maistret for their kind invitation to participate. We also thank Seouyoung Kim for her interest in this note. The authors were financially supported by the Simons Collaboration in Arithmetic Geometry, Number Theory, and Computation via Simons Foundation grant 550033.

#### REFERENCES

- [BK16] G. Banaszak, K.S. Kedlaya, *Motivic Serre Group, Algebraic Sato–Tate Group and Sato–Tate Conjecture*. In *Frobenius Distributions: Lang–Trotter and Sato–Tate Conjectures*, edited by D. Kohel and I. Shparlinski, 11–44. Contemp. Math. **663**, American Mathematical Society, Providence, 2016.
- [CC] V. Cantoral Farfán, J. Commelin, *The Mumford–Tate conjecture implies the algebraic Sato–Tate conjecture of Banaszak and Kedlaya*, arXiv:1905.04086.
- [Fal83] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.
- [FKRS12] F. Fité, K.S. Kedlaya, A.V. Sutherland, and V. Rotger, *Sato–Tate distributions and Galois endomorphism modules in genus 2*, Compos. Math. **148** (2012), 1390–1442.
- [Kim] S. Kim, *The Sato–Tate conjecture and Nagao’s conjecture*, arXiv:1712.02775.
- [Mum70] D. Mumford, *Abelian Varieties*, Tata Institute of Fundamental Research, Bombay, Oxford University Press, 1970.
- [Ser77] J.-P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977.
- [Ser12] J.-P. Serre, *Lectures on  $N_X(p)$*  (CRC Press, Boca Raton, FL, 2012).
- [Tat65] J. Tate, *Algebraic cycles and poles of zeta functions*, in *Arithmetical Algebraic Geometry* (Proc. Conf. Purdue Univ., 1963), pp. 93–110. Harper & Row, New York, 1965.
- [Tat66] J. Tate, *Endomorphisms of abelian varieties over finite fields*. Invent. Math. **2** (1966), 134–144.

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 77 MASSACHUSETTS AVE., CAMBRIDGE, MA 02139, UNITED STATES

*E-mail address:* [edgarc@mit.edu](mailto:edgarc@mit.edu)

*URL:* <https://edgarcosta.org>

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 77 MASSACHUSETTS AVE., CAMBRIDGE, MA 02139, UNITED STATES

*E-mail address:* [ffite@mit.edu](mailto:ffite@mit.edu)

*URL:* <https://math.mit.edu/~ffite/>

DEPARTMENT OF MATHEMATICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY, 77 MASSACHUSETTS AVE., CAMBRIDGE, MA 02139, UNITED STATES

*E-mail address:* [drew@math.mit.edu](mailto:drew@math.mit.edu)

*URL:* <https://math.mit.edu/~drew/>