ON THE RANK AND THE CONVERGENCE RATE TOWARDS THE SATO–TATE MEASURE

FRANCESC FITÉ AND XAVIER GUITART

ABSTRACT. Let A be an abelian variety defined over a number field and let G denote its Sato–Tate group. Under the assumption of certain standard conjectures on L-functions attached to the irreducible representations of G, we study the convergence rate of any virtual selfdual character of G. We find that this convergence rate is dictated by several arithmetic invariants of A, such as its rank or its Sato–Tate group G. The results are consonant with some previous experimental observations, and we also provide additional numerical evidence consistent with them. The techniques that we use were introduced by Sarnak, in order to explain the bias in the sign of the Frobenius traces of an elliptic curve without complex multiplication defined over $\mathbb{Q}$. We show that the same methods can be adapted to study the convergence rate of the characters of its Sato–Tate group, and that they can also be employed in the more general case of abelian varieties over number fields. A key tool in our analysis is the existence of limiting distributions for automorphic L-functions, which is due to Akbary, Ng, and Shahabi.

CONTENTS

1. Introduction

Let k be a number field and A an abelian variety defined over k of dimension $g \geq 1$. Following Serre [Ser94], Banaszak and Kedlaya [BK16a] have attached to A a compact real Lie subgroup G of $\mathrm{USp}(2g)$, the so-called Sato–Tate group of A, with the conjectural property that it governs the distribution of the Frobenius elements attached to A.

In order to make a more precise statement, let us introduce some notations. Let ℓ be a rational prime and let $V_\ell(A)$ denote the (rational) ℓ-adic Tate module of A. The action of the absolute Galois group G_k of k on $V_\ell(A)$ gives rise to an ℓ-adic representation

$$(1.1) \qquad \varrho_A : G_k \to \mathrm{Aut}(V_\ell(A)) \,.$$

Denote by P the set of nonzero prime ideals of k of good reduction for A, that is, the set of nonzero prime ideals of k not dividing the conductor $\mathfrak{N}$ of A. For a prime $\mathfrak{p}$ in P, set

$$(1.2) \qquad L_\mathfrak{p}(A, T) := \det(1 - \varrho_A(\mathrm{Frob}_\mathfrak{p})T \mid V_\ell(A)) \,,$$

where $\mathrm{Frob}_\mathfrak{p}$ denotes a Frobenius element at $\mathfrak{p}$. Attached to $\mathfrak{p}$, one can construct a semisimple conjugacy class $y_\mathfrak{p}$ in the set of conjugacy classes Y of G such that

$$(1.3) \qquad \det(1 - y_\mathfrak{p}T) = L_\mathfrak{p}(A, T/\sqrt{|\mathfrak{p}|}) \,,$$

where $|\mathfrak{p}|$ denotes the absolute norm of $\mathfrak{p}$. We will refer to the projection μ of the Haar measure μ_G of G on Y as the *Sato–Tate measure* of A. The conjectural property of G that we have alluded to before predicts that the sequence $\{y_\mathfrak{p}\}_{\mathfrak{p} \in P}$, where the ideals in P are ordered according to their absolute norm, is equidistributed on Y with respect to μ.

Let us recall what this means. For $x > 0$, let $\pi(x)$ denote the number of primes $\mathfrak{p}$ in P such that $|\mathfrak{p}| \leq x$. Set

$$\mu_x := \frac{1}{\pi(x)} \sum_{|\mathfrak{p}| \leq x} \delta_{y_\mathfrak{p}} \,,$$

where $\delta_{y_\mathfrak{p}}$ denotes the Dirac measure at $y_\mathfrak{p}$ and the sum runs over primes of P such that $|\mathfrak{p}| \leq x$. From now on, we make the convention that all sums of terms involving $y_\mathfrak{p}$ run over primes $\mathfrak{p} \in P$. By definition, we say that $\{y_\mathfrak{p}\}_{\mathfrak{p} \in P}$ is equidistributed on Y with respect to μ, or simply μ-equidistributed on Y, if

$$(1.4) \qquad \mu_x \to \mu \qquad \text{weakly as} \qquad x \to \infty \,.$$

As explained in [Ser68, Prop. 2, App. Chap. I], the sequence $\{y_\mathfrak{p}\}_{\mathfrak{p} \in P}$ is μ-equidistributed on Y if and only if for every irreducible character χ of G one has that

$$(1.5) \qquad \lim_{x \to \infty} \frac{1}{\pi(x)} \sum_{|\mathfrak{p}| \leq x} \chi(y_\mathfrak{p}) = \delta(\chi) \,,$$

where $\delta(\chi)$ is 1 or 0 depending on whether χ is trivial or not[1]. Recall that, by the Prime Number Theorem, (1.5) is equivalent to

$$(1.6) \qquad \lim_{x \to \infty} \frac{\log(x)}{x} \sum_{|\mathfrak{p}| \leq x} \chi(y_\mathfrak{p}) = \delta(\chi) \,,$$

---

[1]More in general and for future use, given a virtual character φ of G, let $\delta(\varphi)$ denote the multiplicity of the trivial representation in φ.

and that, by the Abel summation trick, (1.5) is also equivalent to

$$\sum_{|\mathfrak{p}| \leq x} \chi(y_{\mathfrak{p}}) \log(|\mathfrak{p}|) = \delta(\chi)x + o(x) \,. \tag{1.7}$$

It is of crucial importance that (1.5) is connected, via the Wiener–Ikehara Theorem, to the theory of L-functions (see [Ser68, Thm. 1, App. Chap. I]). For $\mathfrak{p} \in P$, set the polynomial

$$L_{\mathfrak{p}}(\chi, T) := \det(1 - \varrho(y_{\mathfrak{p}})T) \,,$$

where ϱ is an irreducible representation of G of character χ. The degree $d_{\chi}(\mathfrak{p})$ of $L_{\mathfrak{p}}(\chi, T)$ is the degree d_{χ} of the representation ϱ, and the roots of this polynomial all have absolute value 1. One finds that the sequence $\{y_{\mathfrak{p}}\}_{\mathfrak{p} \in P}$ is μ-equidistributed on Y if and only if, for every nontrivial irreducible character χ of G, the partial Euler product

$$L^P(\chi, s) := \prod_{\mathfrak{p} \in P} L_{\mathfrak{p}}(\chi, |\mathfrak{p}|^{-s})^{-1} \,, \qquad \text{defined for } \Re(s) > 1 \,, \tag{1.8}$$

extends to a holomorphic function on (an open neighborhood of) the halfplane $\Re(s) \geq 1$ and does not vanish at $s = 1$. This is unknown in general, but it would follow from the automorphy of $L^P(\chi, s)$, which is predicted by the global Langlands correspondences. Throughout the paper, we will assume the automorphy of $L^P(\chi, s)$, together with a number of conjectural properties that $L^P(\chi, s)$ is expected to satisfy on the halfplane $\Re(s) \geq 1/2$. More precisely, we will consider the following assumption.

Assumption 1.1. For every irreducible nontrivial representation ϱ of G of character χ:

(1) The L-function $L^P(\chi, s)$ is automorphic. By this we mean that, for each $\mathfrak{p} | \mathfrak{N}$, there exist polynomials $L_{\mathfrak{p}}(\chi, T)$ of degree $d_{\chi}(\mathfrak{p}) \leq d_{\chi}$ such that the Euler product

$$L(\chi, s) := L^P(\chi, s) \prod_{\mathfrak{p} | \mathfrak{N}} L_{\mathfrak{p}}(\chi, |\mathfrak{p}|^{-s})^{-1} \,, \qquad \text{defined for } \Re(s) > 1 \,, \tag{1.9}$$

coincides with the automorphic L-function $L(\pi, s)$ of some irreducible unitary algebraic cuspidal representation π of $\mathrm{GL}_{d_{\chi}[k:\mathbb{Q}]}(\mathbb{A}_{\mathbb{Q}})$. Thus, the function $L(\chi, s)$ extends to an analytic function on $\mathbb{C}$.

(2) The Riemann Hypothesis holds for $L^P(\chi, s)$ (equiv. for $L(\chi, s)$); that is, all the zeros $\sigma + i\gamma$ of $L^P(\chi, s)$ (equiv. of $L(\chi, s)$) in the critical region $0 \leq \sigma \leq 1$ have $\sigma = 1/2$.

Remark 1.2. Note that (1) is implied by standard conjectures on automorphic representations. Indeed, the global Langlands correspondence implies that $L(\chi, s)$, as the L-function of an irreducible representation of the motivic Galois group of k, is the L-function of an irreducible unitary cuspidal algebraic representation of $\mathrm{GL}_{d_{\chi}}(\mathbb{A}_k)$ (see for example [Cog03, §4.2]). By automorphic induction (a consequence of the Principle of Functoriality, see for example [Cog03, §4.1]), $L(\chi, s)$ is then expected to be the L-function of an irreducible unitary algebraic cuspidal representation of $\mathrm{GL}_{d_{\chi}[k:\mathbb{Q}]}(\mathbb{A}_{\mathbb{Q}})$.

Now, for a virtual character φ of G, that is, $\varphi \in \bigoplus_{\chi} \mathbb{Z} \cdot \chi$, where χ runs over the irreducible characters of G, set

$$\delta(\varphi, x) := \frac{1}{\pi(x)} \sum_{|\mathfrak{p}| \leq x} \varphi(y_{\mathfrak{p}}) \,. \tag{1.10}$$

It follows from Assumption 1.1 (1), that for every nontrivial irreducible character χ of G one has that

$$(1.11) \qquad \lim_{x \to \infty} \delta(\chi, x) = 0 \,.$$

It is then apparent that a way to estimate the velocity of convergence of the measures μ_x towards the measure μ is by studying how fast the function $\delta(\chi, x)$ approaches the function 0 as x tends to ∞. There are examples of this in the literature: By generalizing [Mur85, Prop. 4.1] and under Assumption 1.1 (2), in (2.4) of [BK16b] one finds that

$$(1.12) \qquad \delta(\chi, x) = O\left(d_\chi[k : \mathbb{Q}]x^{-1/2}\log(N(x + d_\chi[k : \mathbb{Q}]))\log(x)\right) \,,$$

where $N := |\mathfrak{N}|$. One may interpret the O-notation as a sort of *asymptotic supremum norm* (a supremum norm in a neighborhood of infinity) of the function $\delta(\chi, x)$. With this notion of convergence rate, Formula (1.12) makes apparent how the velocity of convergence depends on the conductor of A.

The goal of this note is to study the influence on the convergence rate of other invariants of A, most notably (although not only) of the rank of A. For this purpose, we instead propose to use what could be seen as a sort of *asymptotic L^2-norm*. For $X > 0$, and φ a virtual character of G not containing the trivial character, define

$$I(\varphi, X) := \frac{1}{\log(X)} \int_2^X \delta(\varphi, x)^2 dx \,.$$

We will restrict our attention to selfdual virtual characters. We will say that a virtual character $\varphi = \sum_\chi c_\chi \chi$, where $c_\chi \in \mathbb{Z}$ and χ runs over irreducible characters of G, is selfdual if[2] $c_\chi = c_{\bar\chi}$, where $\bar\chi$ denotes the dual (or complex conjugate) of χ. The main goal of the paper is to study the asymptotic behavior of $I(\varphi, X)$ as $X \to \infty$. The following is the main result.

Theorem 1.3. *Under Assumption 1.1, for every virtual selfdual character of the form $\varphi = \sum_{\chi \neq 1} c_\chi \chi$, where $c_\chi \in \mathbb{Z}$ and χ runs over the irreducible nontrivial characters of G, one has that*

$$(1.13) \qquad I(\varphi) := \lim_{X \to \infty} I(\varphi, X) = \left(\sum_\chi c_\chi(2r_\chi + u_\chi)\right)^2 + \sum_\chi \sum_{\gamma_\chi > 0} \frac{2c_\chi^2}{1/4 + \gamma_\chi^2} \,,$$

where r_χ denotes the order of the zero of $L(\chi, s)$ at $s = 1/2$, u_χ is the Frobenius–Schur index of χ, and γ_χ runs over the positive imaginary parts of the zeros of $L(\chi, s)$ on the critical region.

Observe that via this theorem, assuming the Birch and Swinnerton–Dyer conjecture and taking for χ the character of the tautological representation of G (seen as a subgroup of $\mathrm{USp}(2g)$), the influence of the rank of the Mordell-Weil group of A on the velocity of convergence of the measures μ_x towards the Sato–Tate measure μ becomes apparent[3].

The proof of Theorem 1.3 occupies §3. It relies on work of Akbary, Ng, and Shahabi [ANS14] on the existence of a limiting distribution attached to any unitary cuspidal automorphic selfdual L-function, and it follows the ideas that Sarnak introduced in [Sar07] to explain the bias in the sign

---

[2]Observe that this condition is trivially satisfied if χ is selfdual, since $\chi \simeq \bar\chi$ in this case.

[3]An effect of the rank on the convergence towards the Sato–Tate measure had been experimentally observed. On Drew Sutherland's web page:

https://math.mit.edu/~drew/g1_r28_a1f.gif,

one can visualize a very asymmetric convergence towards the Sato–Tate measure in the case of Elkies' elliptic curve (the highest rank elliptic curve known to present, of rank at least 28).

of the Frobenius traces of an elliptic curve in terms of the rank. Sarnak restricted his attention to elliptic curves without complex multiplication, in which case $G = \mathrm{USp}(2)$ and the nontrivial irreducible representations of G are the symmetric powers of its standard representation.

In §4, we use Theorem 1.3 to give a simple upper bound of the asymptotic L^2-norm $I(\varphi)$. This is used in §5 to analyze the velocity of convergence of certain virtual characters which are of interest in the numerical calculation of Sato–Tate groups. Indeed, the usual method for such calculations is to compute approximations to the limit values of a certain set of virtual characters, for which these limit values are known to determine the Sato–Tate group. A typical example are the moments of the coefficients of the polynomial $L_{\mathfrak{p}}(A, T/\sqrt{|\mathfrak{p}|})$ (cf. [KS09, FKRS12]) or the so-called power sums (cf. [KS09]). Formula (1.13) can then be used to determine how fast one can expect different families of virtual characters to converge. For instance, Shieh [Shi16] experimentally observed a better convergence of the set of irreducible characters than of the moments. This is consistent with the velocities of convergence predicted by (1.13), and in fact one can view Theorem 1.3 as a theoretical justification for Shieh's observation.

In §6 we report on some numerical experiments, carried out to test whether the predictions of convergence rate arising from Theorem 1.3 can actually be observed in concrete examples. The concrete choice of examples also responds to the goal of illustrating how the different invariants of abelian varieties (the various analytic ranks, the Frobenius–Schur index, the Sato–Tate group, etc.) affect the convergence velocity.

Notations. We use $|\cdot|$ to denote the absolute norm of ideals in rings of integers of number fields and the complex absolute value. Its use in one sense or the other should be clear from the context.

2. Background

In this section, we recall the results of [ANS14] that we will require in §3 and a few technical lemmas.

2.1. **Limiting distributions.** Let $\psi\colon \mathbb{R}_{>0} \to \mathbb{R}$ be a function admitting an expression of the form

$$(2.1) \qquad\qquad \psi(x) = c + S(x, T) + R(x, T),$$

for any $T \geq 2$, where $c \in \mathbb{R}$ and:

i) The main term $S(x, T)$ is of the form $\Re\left(\sum_{\gamma_n \leq T} \eta_n x^{i\gamma_n}\right)$, where $\{\gamma_n\}_{n \geq 1} \subseteq \mathbb{R}_{>0}$ is a non-decreasing sequence which tends to infinity, $\{\eta_n\}_{n \geq 1} \subseteq \mathbb{C}$, and there exists $\theta \in [0, 3 - \sqrt{3}]$ such that

$$(2.2) \qquad\qquad \sum_{\lambda_n \leq T} \gamma_n^2 |\eta_n|^2 = O(T^\theta).$$

ii) The error term $R(x, T)$ satisfies

$$(2.3) \qquad\qquad \lim_{X \to \infty} \frac{1}{\log(X)} \int_2^X |R(x, X)|^2 \frac{dx}{x} = 0.$$

The next statement is contained in [ANS14, Cor. 1.3].

Theorem 2.1 ([ANS14])**.** *The function ψ possesses a limiting distribution μ_ψ with respect to the measure dx/x. That is, for any continuous function $f : \mathbb{R} \to \mathbb{R}$ one has*

$$(2.4) \qquad \lim_{X \to \infty} \frac{1}{\log(X)} \int_2^X f(\psi(x)) \frac{dx}{x} = \int_\mathbb{R} f(x) \mu_\psi(x) \,.$$

Moreover, the expectation and variance of μ_ψ are respectively

$$\mathrm{E}[\mu_\psi] := \int_\mathbb{R} x \mu_\psi(x) = c \,, \qquad \mathrm{V}[\mu_\psi] := \int_\mathbb{R} (x - c)^2 \mu_\psi(x) = \frac{1}{2} \sum_{n \geq 1} |\eta_n|^2 \,.$$

Remark 2.2. Let ψ be as in (2.1) and let $\psi' : \mathbb{R}_{>0} \to \mathbb{R}$ be such that $\psi(x) = \psi'(x) + \Delta(x)$, where $\Delta(x) = o(1)$. If we write $\psi'(s)$ as

$$\psi'(x) = c + S(x, T) + R'(x, T) \,,$$

the main term $S(x, T)$ and the error term $R'(x, T) := R(x, T) - \Delta(x)$ also satisfy (2.2) and (2.3). Indeed, this amounts to show that

$$\lim_{X \to \infty} \frac{1}{\log(X)} \int_2^X |\Delta(x)|^2 \frac{dx}{x} = 0 \,.$$

To prove this, let $\epsilon > 0$ and note that, since $\Delta(x) = o(1)$, there exists $X_\epsilon > 0$ such that $|\Delta(x)|^2 < \epsilon$ for $x > X_\epsilon$. Then

$$\lim_{X \to \infty} \frac{1}{\log(X)} \int_2^X |\Delta(x)|^2 \frac{dx}{x} = \lim_{X \to \infty} \frac{1}{\log(X)} \int_{X_\epsilon}^X |\Delta(x)|^2 \frac{dx}{x} \leq \lim_{X \to \infty} \frac{\epsilon}{\log(X)} \int_{X_\epsilon}^X \frac{dx}{x} \leq \epsilon \,.$$

We finish this section by recording a property of the limit appearing on the left hand side of (2.4) that we will use in §3.

Lemma 2.3. *Let $f \colon \mathbb{R}_{>0} \to \mathbb{R}_{\geq 0}$ be a locally integrable function such that*

$$\lim_{X \to \infty} \frac{1}{\log(X)} \int_2^X f(x) dx = A \,,$$

for some $A \in \mathbb{R}$. Let $g \colon \mathbb{R}_{>0} \to \mathbb{R}$ be a function such that $\lim_{x \to \infty} g(x) = 1$ and such that fg is locally integrable. Then

$$\lim_{X \to \infty} \frac{1}{\log(X)} \int_2^X f(x) g(x) dx = A \,.$$

Proof. First of all, we observe that for any $M \geq 2$ we have that

$$(2.5) \qquad \lim_{X \to \infty} \frac{1}{\log(X)} \int_M^X f(x) dx = A.$$

Now fix $\epsilon > 0$ and let X_ϵ be such that $g(x)$ belongs to the interval $[1 - \epsilon, 1 + \epsilon]$ for all $x \geq X_\epsilon$. Then, for any $X \geq X_\epsilon$ we have

$$\frac{1}{\log(X)} \int_2^X f(x) g(x) dx = \frac{1}{\log(X)} \int_2^{X_\epsilon} f(x) g(x) dx + \frac{1}{\log(X)} \int_{X_\epsilon}^X f(x) g(x) dx$$

$$\leq \frac{1}{\log(X)} \int_2^{X_\epsilon} f(x) g(x) dx + \frac{(1 + \epsilon)}{\log(X)} \int_{X_\epsilon}^X f(x) dx.$$

Now, by (2.5) for X sufficiently large we will have that

$$\frac{1}{\log(X)} \int_{X_\epsilon}^{X} f(x)dx \leq A + \epsilon.$$

Also, for X large enough

$$\frac{1}{\log(X)} \int_{2}^{X_\epsilon} f(x)g(x)dx \leq \epsilon.$$

Therefore, we see that for X large enough we have that

$$\frac{1}{\log(X)} \int_{2}^{X} f(x)g(x)dx \leq \epsilon + (1 + \epsilon)(A + \epsilon) = A + \epsilon(2 + A + \epsilon).$$

Now, mutatis mutandis one can also show that for X large enough one has

$$\frac{1}{\log X} \int_{2}^{X} f(x)g(x)dx \geq A - \epsilon(2 + A - \epsilon)$$

and we see that the limit when $X \to \infty$ is also A. $\qquad\square$

2.2. **Limiting distributions of automorphic L-functions.** Let π be an irreducible unitary cuspidal automorphic representation of $\mathrm{GL}_r(\mathbb{A}_\mathbb{Q})$, for some $r \geq 1$, and let $L(\pi, s)$ denote the automorphic L-function attached to π. Suppose that $L(\pi, s) \neq \zeta(s - i\tau_0)$ for any $\tau_0 \in \mathbb{R}$, where ζ denotes the Riemann Zeta function. For $n \geq 1$, set the coefficients $\Lambda_\pi(n)$, by prescribing an equality of Dirichlet series

$$(2.6) \qquad\qquad -\frac{L(\pi, s)'}{L(\pi, s)} =: \sum_{n \geq 1} \Lambda_\pi(n)n^{-s},$$

and, for $x > 0$, define the function

$$(2.7) \qquad\qquad \psi(\pi, x) := \frac{1}{\sqrt{x}} \sum_{n \leq x} \Lambda_\pi(n).$$

The following is [ANS14, Prop. 4.2].

Theorem 2.4. *Under Assumption 1.1, for any $x > 0$ and $T \geq 2$, we have that*

$$(2.8) \qquad\qquad \psi(\pi, x) = -2r_\pi - \sum_{0 < |\gamma_\pi| \leq T} \frac{x^{i\gamma_\pi}}{1/2 + i\gamma_\pi} + R_\pi(x, T).$$

Here, r_π denotes the order of the zero of $L(\pi, s)$ at $s = 1/2$, γ_π runs over the non-zero imaginary parts of absolute value up to T of the zeros of $L(\pi, s)$ on the critical region, and the error term $R_\pi(x, T)$ satisfies

$$R_\pi(x, T) = O\left(\frac{x^{1/2+\beta} \log^2(x)}{T} + x^{\beta - 1/2} \log(x) + \frac{x^{1/2} \log^2(T)}{T \log(x)} + \frac{x^{1/2} \log(T)}{T} \right),$$

for some $\beta \in [0, 1/2)$.

Remark 2.5. By combining Theorems 2.4 and 2.1, one obtains as in [ANS14, §4.1] that if π is selfdual[4], then $\psi(\pi, x)$ has a limiting distribution with respect to the measure dx/x (see [ANS14, Cor. 1.5]). Indeed, if π is selfdual the zeros of $L(\pi, s)$ come in conjugate pairs, and by pairing

---

[4]We alert the reader that the selfduality condition on π does not appear in the statement of [ANS14, Cor. 1.5], although it is used in the proof (see the last display in page 767 of loc. cit.).

them one sees that $\psi(\pi, x)$ can be written as in (2.1) in such a way that $R_\pi(x, T)$ satisfies (2.3) and that, if $\{\gamma_n\}_{n\geq 1}$ is an ordering by size of the positive imaginary parts of the zeros of $L(\pi, s)$ in the critical region, then (2.2) is satisfied with $\eta_n := -2/(1/2 + i\gamma_n)$ and $\theta := \beta$. We will apply a similar argument to $\psi(\pi, x) + \psi(\pi^\vee, x)$ if π is not selfdual (see Corollary 3.3 below).

3. PROOF OF THEOREM 1.3

Resume the notations of §1. The first step towards the proof of Theorem 1.3 is to consider the case of a nontrivial irreducible character χ of G. For $x > 0$, define the function

$$\psi(\chi, x) := \frac{\log(x)}{\sqrt{x}} \sum_{|\mathfrak{p}| \leq x} \chi(y_\mathfrak{p}) \,.$$

Proposition 3.1. *Under Assumption 1.1, for a nontrivial character χ of G and for any $x > 0$ and $T \geq 2$, we have that*

$$(3.1) \qquad \psi(\chi, x) = -2r_\chi - u_\chi - \sum_{0 < |\gamma_\chi| \leq T} \frac{x^{i\gamma_\chi}}{1/2 + i\gamma_\chi} + R(x, T) \,,$$

where r_χ, u_χ are as in the statement of Theorem 1.3, γ_χ runs over the non-zero imaginary parts of absolute value up to T of the zeros of $L(\chi, s)$ on the critical region, and the error term $R(x, T)$ satisfies (2.3).

Proof. Let ϱ be an irreducible representation of G of character χ, and let d_χ denote the degree of ϱ. For $n \geq 1$, define the von-Mangold function $\Lambda_\chi(n)$ by prescribing an equality of Dirichlet series

$$(3.2) \qquad -\frac{L(\chi, s)'}{L(\chi, s)} =: \sum_{n \geq 1} \Lambda_\chi(n) n^{-s} \,.$$

For a prime $\mathfrak{p}$ of k, let $\alpha_{\mathfrak{p},1}, \ldots, \alpha_{\mathfrak{p}, d_\chi(\mathfrak{p})}$ denote the recyprocal roots of $L_\mathfrak{p}(\chi, T)$. Taking the logarithmic derivative in (1.9), we find that

$$(3.3) \qquad -\frac{L(\chi, s)'}{L(\chi, s)} = \sum_\mathfrak{p} \sum_{j=1}^{d_\chi(\mathfrak{p})} \sum_{r \geq 1} \frac{\log(|\mathfrak{p}|)\alpha_{\mathfrak{p},j}^r}{|\mathfrak{p}|^{rs}} = \sum_{r \geq 1} \sum_\mathfrak{p} \log(|\mathfrak{p}|) \Big(\sum_{j=1}^{d_\chi(\mathfrak{p})} \alpha_{\mathfrak{p},j}^r \Big) |\mathfrak{p}|^{-rs} \,.$$

For $r \geq 1$, define[5]

$$\Lambda_\chi(\mathfrak{p}^r) := \log(|\mathfrak{p}|) \Big(\sum_{j=1}^{d_\chi(\mathfrak{p})} \alpha_{\mathfrak{p},j}^r \Big) \,.$$

Note that, if $\mathfrak{p} \in P$, then $\alpha_{\mathfrak{p},1}, \ldots, \alpha_{\mathfrak{p}, d_\chi(\mathfrak{p})}$ are the eigenvalues of $\varrho(y_\mathfrak{p})$ and thus $\Lambda_\chi(\mathfrak{p}^r) = \log(|\mathfrak{p}|)\chi(y_\mathfrak{p}^r)$. Observe also that we similarly find that

$$-\frac{L^P(\chi, s)'}{L^P(\chi, s)} = \sum_{r \geq 1} \sum_{\mathfrak{p} \in P} \Lambda(\mathfrak{p}^r) |\mathfrak{p}|^{-rs} \,,$$

For $x > 0$, define the function

$$(3.4) \qquad \psi_1(\chi, x) := \frac{1}{\sqrt{x}} \sum_{n \leq x} \Lambda_\chi(n) = \frac{1}{\sqrt{x}} \sum_{r \geq 1} \sum_{|\mathfrak{p}|^r \leq x} \Lambda_\chi(\mathfrak{p}^r) \,,$$

---

[5]Note that we are using the same notation Λ_χ to denote two different functions; since one is a function of the positive integers and the other is a function of the ideals of k, their argument is what makes clear which one we refer to (when $k = \mathbb{Q}$ the two functions coincide).

where the second equality follows from compairing (3.3) and (3.2). Under Assumption 1.1, there is an irreducible unitary cuspidal representation π of $\mathrm{GL}_{d_\chi[k:\mathbb{Q}]}(\mathbb{A}_\mathbb{Q})$ such that $\psi_1(\chi, x)$ coincides with $\psi(\pi, x)$, as defined in (2.7) (note that $L(\pi, s)$ is not of the form $\zeta(s - i\tau_0)$ since χ is nontrivial). Then, by Theorem 2.4 we can write

$$\psi_1(\chi, x) = c_1 + S_1(x, T) + R_1(x, T),$$

where $c_1 := -2r_\chi$, $S_1(T) := -\sum_{0 < |\gamma_\chi| \leq T} \frac{x^{i\gamma_\chi}}{1/2 + i\gamma_\chi}$ and $R_1(x, T)$ satisfies (2.3). Define

$$\psi_2(\chi, x) := \frac{1}{\sqrt{x}} \sum_{|\mathfrak{p}| \leq x} \Lambda_\chi(\mathfrak{p}), \qquad \Delta_1(x) := \frac{1}{\sqrt{x}} \left(\sum_{|\mathfrak{p}| \leq x^{1/2}} \Lambda_\chi(\mathfrak{p}^2) + \sum_{k \geq 3} \sum_{|\mathfrak{p}| \leq x^{1/k}} \Lambda_\chi(\mathfrak{p}^k) \right),$$

so that $\psi_1(\chi, x) = \psi_2(\chi, x) + \Delta_1(x)$. We proceed to study the size of $\Delta_1(x)$. On the one hand, we have

$$\sum_{|\mathfrak{p}| \leq x^{1/k}} \Lambda_\chi(\mathfrak{p}^k) \leq d_\chi \sum_{|\mathfrak{p}| \leq x^{1/k}} \log(|\mathfrak{p}|) \leq d_\chi[k : \mathbb{Q}]x^{1/k} \log(x).$$

Since there is no prime ideal $\mathfrak{p}$ of k such that $|\mathfrak{p}| \leq x^{1/k}$ when $k > \log_2(x)$, the sum indexed by k in $\Delta_1(x)$ has at most $O(\log(x))$ summands. Therefore the right most summand in $\Delta_1(x)$ is $O(x^{1/3} \log^2(x))$. On the other hand, (1.7) says that

$$\sum_{|\mathfrak{p}| \leq x^{1/2}} \Lambda_\chi(\mathfrak{p}^2) = \delta(\chi(\cdot^2))\sqrt{x} + o(\sqrt{x}),$$

where $\chi(\cdot^2)$ denotes the central function $g \mapsto \chi(g^2)$. Note that the multiplicity $\delta(\chi(\cdot^2))$ equals $u_\chi := \int_G \chi(g^2)\mu_G(g)$, the so-called Frobenius–Schur index of χ. It is known that $u_\chi = 0$ if χ takes some complex nonreal value, $u_\chi = 1$ if χ is attached to a representation realizable over $\mathbb{R}$, and $u_\chi = -1$ if χ is attached to a quaternionic representation (i.e., a representation that is not realizable over $\mathbb{R}$, even if its character takes values in $\mathbb{R}$). We deduce that

$$\psi_2(\chi, x) = \psi_1(\chi, x) - u_\chi + o(1),$$

and by Remark 2.2, we deduce that

(3.5) $$\psi_2(\chi, x) = c_2 + S_2(x, T) + R_2(x, T),$$

where $c_2 := c_1 - u_\chi$, $S_2(x, T) := S_1(x, T)$, and $R_2(x, T)$ satisfies (2.3). For $x > 0$, define the function

$$\psi_3(\chi, x) := \frac{1}{\sqrt{x}} \sum_{|\mathfrak{p}| \leq x, \mathfrak{p} \in P} \Lambda_\chi(\mathfrak{p}),$$

so that we have that

$$\psi_2(\chi, x) = \psi_3(\chi, x) + \Delta_2(x), \qquad \text{where} \qquad \Delta_2(x) := \frac{1}{\sqrt{x}} \sum_{\mathfrak{p} | \mathfrak{N}} \Lambda_\chi(\mathfrak{p}).$$

Provided that there is only a finite number of primes dividing $\mathfrak{N}$, we have that $\Delta_2(x) = o(1)$. But, by the Abel summation trick (see Lemma 3.2 below), we have that $\psi_3(\chi, x) = \psi(\chi, x) + o(1)$. It follows from Remark 2.2, that $\psi(\chi, x)$ admits an expression of the form $\psi(\chi, x) = c + S(x, T) + R(x, T)$, with $c = c_2$, $S(x, T) := S_2(x, T)$, and $R(x, T)$ satisfies (2.3).

$\square$

At the end of the previous proof we have applied the Abel summation trick. Following the lines of reasoning of [RS94, Lemma 2.1], we give the argument involved in gory detail.

Lemma 3.2. *For a nontrivial character χ of G, we have*

$$(3.6) \qquad \sum_{|\mathfrak{p}| \leq x} \log(|\mathfrak{p}|)\chi(y_\mathfrak{p}) = \log(x) \sum_{|\mathfrak{p}| \leq x} \chi(y_\mathfrak{p}) + o(\sqrt{x}).$$

Proof. Let us write

$$\vartheta(x) := \sqrt{x} \cdot \psi_3(\chi, x) = \sum_{|\mathfrak{p}| \leq x} \log(|\mathfrak{p}|)\chi(y_\mathfrak{p}).$$

Applying summation by parts[6], we have

$$(3.7) \qquad \sum_{|\mathfrak{p}| \leq x} \chi(y_\mathfrak{p}) = \frac{\vartheta(x)}{\log(x)} + \int_2^x \frac{\vartheta(t)}{t \log^2(t)} dt.$$

Then, integrating (3.5) times $\sqrt{x}$, letting T tend to infinity, and using that $\beta < 1/2$ we obtain that

$$(3.8) \qquad G(x) := \int_2^x \vartheta(t)dt = \frac{2}{3}(-2r_\chi - u_\chi)x^{3/2} - \sum_{\gamma_\chi \neq 0} \frac{x^{\frac{3}{2}+i\gamma_\chi}}{(\frac{1}{2}+i\gamma_\chi)(\frac{3}{2}+i\gamma_\chi)} + o(x^{3/2}).$$

Here, similarly as it is remarked in the proof of [RS94, Lemma 2.1], it is used that the series over γ_χ converges absolutely. This follows from the asymptotic formula for the number $N(T)$ of zeros in the critical region with imaginary part of absolute value $\leq T$ for automorphic L-functions, as in for example [IK04, Theorem 5.8]. It follows that $G(x) = O(x^{3/2})$.

Integrating by parts the rightmost integral in (3.7), we obtain

$$\int_2^x \frac{\vartheta(t)}{t \log^2(t)} dt = \frac{G(x)}{x \log^2 x} + \int_2^x G(t)\frac{\log(t)+2}{t^2 \log^3(t)} dt = O\left(\frac{\sqrt{x}}{\log^2(x)}\right) + O\left(\int_2^x \frac{dt}{\sqrt{t} \cdot \log^2(t)}\right).$$

Both O-terms in the above expression are $o\left(\frac{\sqrt{x}}{\log x}\right)$ (the first by trivial reasons and the second, by l'Hôpital, for example). We conclude that

$$(3.9) \qquad \sum_{|\mathfrak{p}| \leq x} \chi(y_\mathfrak{p}) = \frac{\vartheta(x)}{\log(x)} + o\left(\frac{\sqrt{x}}{\log(x)}\right),$$

and this implies the lemma. $\qquad\square$

Corollary 3.3. *With the notation and assumptions as in Proposition 3.1 we have that*

$$\psi(\chi, x) + \psi(\bar\chi, x) = -2(r_\chi + r_{\bar\chi}) - (u_\chi + u_{\bar\chi}) + S(x, T) + R(x, T),$$

where $S(x, T)$ and $R(x, T)$ are as in (2.1), $R(x, T)$ satisfies (2.3), and $S(x, T)$ satisfies (2.2) with $\{\gamma_n\}_{n \geq 1}$ being the positive imaginary parts of the zeros of $L(\chi, s)$ and $L(\bar\chi, s)$, $\eta_n := \frac{-2}{1/2+i\gamma_n}$, and $\theta = 1/2$.

Proof. This follows at once by adding the expressions for $\psi(\chi, x)$ and $\psi(\bar\chi, x)$ given in (3.1) and pairing each zero $\frac{1}{2} + i\gamma_\chi$ of $L(\chi, s)$ having $\gamma_\chi > 0$ with its conjugate, which is a zero of $L(\bar\chi, s)$ (and, similarly, pairing each zero $\frac{1}{2} + i\gamma_{\bar\chi}$ of $L(\bar\chi, s)$ having $\gamma_{\bar\chi} > 0$ with its conjugate, which is a zero of $L(\chi, s)$). $\qquad\square$

We can now prove Theorem 1.3.

---

[6]We apply the formula of [IK04, Chap. I, §1.5], with $f(p^r) = \sum_{|\mathfrak{p}|=p^r} \log(|\mathfrak{p}|)\chi(y_\mathfrak{p})$ (and $f(n) = 0$ if n is not a prime power) and $g(x) = 1/\log(x)$.

Proof of Theorem 1.3. By Corollary 3.3 and Theorem 2.1, we have that for each of the irreducible constituents χ of φ, the function $\psi(\chi, x) + \psi(\bar{\chi}, x)$ admits a limiting distribution μ_χ with

$$\mathrm{E}[\mu_\chi] = -2(r_\chi + r_{\bar\chi}) - (u_\chi + u_{\bar\chi}), \qquad \mathrm{V}[\mu_\chi] = \sum_{\gamma_\chi > 0} \frac{2}{1/4 + \gamma_\chi^2} + \sum_{\gamma_{\bar\chi} > 0} \frac{2}{1/4 + \gamma_{\bar\chi}^2}.$$

Define $\psi(\varphi, x) := \sum_\chi c_\chi \psi(\chi, x)$. By additivity and the fact that φ is selfdual, it follows again from Theorem 2.1 that the function $\psi(\varphi, x)$ admits a limiting distribution μ_φ with

$$\mathrm{E}[\mu_\varphi] = -\sum_\chi c_\chi (2r_\chi + u_\chi), \qquad \mathrm{V}[\mu_\varphi] = \sum_\chi \sum_{\gamma_\chi > 0} \frac{2c_\chi^2}{1/4 + \gamma_\chi^2}.$$

Therefore

$$\lim_{X \to \infty} \frac{1}{\log(X)} \int_2^X \psi(\varphi, x)^2 \frac{dx}{x} = \mathrm{E}[\mu_\varphi]^2 + \mathrm{V}[\mu_\varphi] = \left(\sum_\chi c_\chi (2r_\chi + u_\chi) \right)^2 + \sum_\chi \sum_{\gamma_\chi > 0} \frac{2c_\chi^2}{1/4 + \gamma_\chi^2}.$$

Since

$$\frac{\psi(\varphi, x)^2}{x} \sim \delta(\varphi, x)^2 \qquad \text{as} \qquad x \to \infty,$$

Lemma 2.3 concludes the proof. $\qquad\square$

4. An upper bound for the asymptotic L^2-norm

In this section we elaborate on Theorem 1.3 to obtain an explicit and simple upper bound for the asymptotic L^2-norm $I(\varphi)$ of a virtual selfdual character φ of G not containing the trivial character (see Corollary 4.4). We will need the following consequence of Assumption 1.1 (1).

Remark 4.1. If χ is an irreducible nontrivial character of G, as a consequence of the fact that $L(\chi, s)$ is automorphic, we have that (see [IK04, §5]) there exist a positive integer N_χ (the so-called *absolute conductor* of χ) and complex numbers $\kappa_{\chi,j}$ with $\Re(\kappa_{\chi,j}) > -1$ for $j = 1, \ldots, d_\chi$ (the so-called *local parameters at infinity* of $L(\chi, s)$), such that the completed L-function

$$(4.1) \qquad \Lambda(\chi, s) := N_\chi^{s/2} \Gamma(\chi, s) L(\chi, s), \qquad \text{with } \Gamma(\chi, s) := \pi^{-d_\chi s/2} \prod_{j=1}^{d_\chi} \Gamma\left(\frac{s + \kappa_{\chi,j}}{2} \right),$$

defined for $\Re(s) > 1$, extends to an analytic function on $\mathbb{C}$ and satisfies a functional equation

$$(4.2) \qquad\qquad\qquad\qquad \Lambda(\chi, s) = \varepsilon_\chi \Lambda(\bar{\chi}, 1 - s).$$

Here, $\varepsilon_\chi \in \mathbb{C}$ is such that $|\varepsilon_\chi| = 1$, and one has that

$$(4.3) \qquad\qquad\qquad\qquad |\kappa_{\chi,j}| \le w_\chi, \qquad N_\chi \le N^{d_\chi},$$

where $N := |\mathfrak{N}|$ and w_χ is the weight[7] of χ. For the precise definitions of N_χ and $\kappa_{\chi,j}$, we refer to [Ser70]. The inequalities in (4.3) follow directly from the definitions.

Proposition 4.2. *Under Assumption 1.1, there exists an absolute constant $K_1 > 0$ such that, for every virtual selfdual character $\varphi = \sum_{\chi \neq 1} c_\chi \chi$ not containing the trivial character, one has that*

$$I(\varphi) \le K_1 \left(\left(\sum_\chi |c_\chi| S_\chi \right)^2 + \sum_\chi c_\chi^2 S_\chi \right),$$

---

[7] We define the weight w_χ of an irreducible character χ of G as the weight of the ℓ-adic representation $\chi \circ \varrho_A$.

where

$$S_\chi := d_\chi[k:\mathbb{Q}]\log(N(w_\chi+3)).$$

Proof. By Theorem 1.3, we have that $I(\varphi) = I_1(\varphi) + I_2(\varphi)$, where

$$(4.4) \qquad I_1(\varphi) := \left(\sum_\chi c_\chi(2r_\chi + u_\chi)\right)^2, \qquad I_2(\varphi) := \sum_\chi \sum_{\gamma_\chi>0} \frac{2c_\chi^2}{1/4 + \gamma_\chi^2}.$$

Note that $r_\chi \leq m(\chi,0)$, where $m(\chi,0)$ is as in Lemma 4.3 below. The Lemma implies then that $I_1(\varphi) \leq K_2 \cdot (\sum_\chi c_\chi S_\chi)^2$ for some $K_2 > 0$. It suffices to prove that there exists $K_3 > 0$ such that

$$\sum_{\rho_\chi} \frac{1}{|\rho_\chi|^2} \leq K_3 S_\chi,$$

where ρ_χ runs over the set zeros of $L(\chi,s)$ (equiv. $\Lambda(\chi,s)$) on the critical line. Again by Lemma 4.3 below, we have that there exists $K_4 > 0$ such that

$$\sum_{\gamma_\chi} \frac{1}{1/4 + \gamma_\chi^2} \leq K_4\left(\sum_{m\geq 1} d_\chi \log\left(N(m+5)(w_\chi+3)\right)\frac{1}{1/4 + (m-1)^2}\right).$$

and the proposition follows. $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

The next result is well known. Provided that it is usually presented only in a form asymptotic in T (which is not precise enough for our purposes), we have decided to include it in the form that we will require; that is, in the form of a statement valid for any $T \geq 0$.

Lemma 4.3. *Under Assumption 1.1, for any irreducible character χ and any $T \geq 0$, the number $m(\chi,T)$ of zeros $\rho_\chi = 1/2 + \gamma_\chi$ (counted with multiplicity) of $\Lambda(\chi,s)$ with $|\gamma_\chi - T| \leq 1$ satisfies*

$$m(\chi,T) \leq K_4 d_\chi[k:\mathbb{Q}]\log(N(T+5)(w_\chi+3)),$$

for an absolute constant $K_4 > 0$.

Proof. By taking the logarithmic derivative of Hadamard's factorization of $\Lambda(\chi,s)$ (see [IK04, Thm. 5.6]) and using [IK04, (5.29)], one obtains that

$$\Re\left(\frac{\Lambda(\chi,s)'}{\Lambda(\chi,s)}\right) = \sum_{\rho_\chi} \Re\left(\frac{1}{s-\rho_\chi}\right),$$

for any $s \in \mathbb{C}$ distinct from a zero of $\Lambda(\chi,s)$. Thus, by taking $s = 2 + iT$, we get on the one hand

$$\left|\frac{\Lambda(\chi,2+iT)'}{\Lambda(\chi,2+iT)}\right| \geq \sum_{\gamma_\chi} \frac{3/2}{(3/2)^2 + (T-\gamma_\chi)^2} \geq \sum_{|\gamma_\chi - T|\leq 1} \frac{3/2}{(3/2)^2 + (T-\gamma_\chi)^2} \geq \frac{6}{13}m(\chi,T).$$

On the other hand, by logarithmically differentiating (4.1), we obtain

$$\left|\frac{\Lambda(\chi,2+iT)'}{\Lambda(\chi,2+iT)}\right| \leq \frac{1}{2}\log N_\chi + \left|\frac{\Gamma'(\chi,2+iT)}{\Gamma(\chi,2+iT)}\right| + \left|\frac{L'(\chi,2+iT)}{L(\chi,2+iT)}\right|.$$

But

$$\left|\frac{L'(\chi,2+iT)}{L(\chi,2+iT)}\right| \leq d_\chi[k:\mathbb{Q}]\left|\frac{\zeta(2+iT)'}{\zeta(2+iT)}\right|$$

and by [IK04, (5.116)] and [IK04, (5.8)], we have that there exists $K_5 > 0$ such that

$$\left| \frac{\Gamma'(\chi, 2 + iT)}{\Gamma(\chi, 2 + iT)} \right| \leq K_5 \cdot \log(N_\chi \prod_{j=1}^{d_\chi} (|\kappa_{\chi,j}| + 3)(T + 5)^{d_\chi}) \,.$$

The lemma now follows from (4.3) applied to the previous inequality. $\qquad\square$

A direct application of the Cauchy-Schwarz inequality yields the following corollary.

Corollary 4.4. *Assume the hypotheses of Proposition 4.2. Let S_φ be $\max_\chi \{S_\chi\}$, let R_φ denote the number of irreducible constituents of φ, and write $C_\varphi := \sum_\chi c_\chi^2$. Then there exists $K_6 > 0$ such that*

$$I(\varphi) \leq K_6 R_\varphi S_\varphi^2 C_\varphi \,.$$

5. An application to the numerical identification of Sato–Tate groups

Let the notations be as in §1. In particular, A is an abelian variety defined over k of dimension $g \geq 1$, G denotes the Sato–Tate group of A, and $\mathfrak{p}$ is a prime of k of good reduction for A.

In the last years, the development of fast methods for the computation of the polynomial $L_\mathfrak{p}(A, T)$ (as defined in (1.2)) has made possible numerical approaches to the identification of the group G, under the assumption of its conjectural equidistribution property (see [FKRS12], [KS09] for example).

Let us briefly describe these numerical approaches. One starts by selecting a family of virtual characters $\{\varphi_n\}_n$ of $\mathrm{USp}(2g)$ such that $\{\delta(\varphi_n|_G)\}_n$ identifies G as a subgroup up to conjugation inside $\mathrm{USp}(2g)$. Provided that the sets of characteristic polynomials and conjugacy classes of $\mathrm{USp}(2g)$ are in bijection, one can find an expression for $\varphi_n(y_\mathfrak{p})$ in terms of $L_\mathfrak{p}(A, T)$. Then, thanks to the efficient methods of computation of $L_\mathfrak{p}(A, T)$, one can compute the sum

$$\delta(\varphi_n, X) := \frac{1}{\pi(X)} \sum_{|\mathfrak{p}| < X} \varphi_n(y_\mathfrak{p})$$

for some large value of $X > 0$. By (1.5), we have that $\delta(\varphi_n, x)$ is expected to approach the multiplicity $\delta(\varphi_n|_G)$ as $x \to \infty$. If X is large enough, the quantities $\delta(\varphi_n, X)$ will provide good approximations of the integer $\delta(\varphi_n|_G)$.

Example 5.1. Let V denote the standard representation of $\mathrm{USp}(2g)$. For $n \geq 0$ and $0 \leq k \leq 2g$, define the *n-th moment of the k-th coefficient* as the character

$$(5.1) \qquad\qquad a_k^n := \mathrm{Tr}\left((\Lambda^k V)^{\otimes n}\right) \,.$$

Write simply $a_k := a_k^1$. For $g = 2$, it is shown in [FKRS12, Table 8] that the sequence of multiplicities[8] $\{\delta(a_1^n|_G), \delta(a_2^n|_G)\}_n$ identifies the group G. In [FKRS12, §5], the method described above for the family of coefficient moments $\{a_1^n, a_2^n\}_n$ is used to numerically identify Sato–Tate groups of several abelian surfaces.

One may wonder whether the efficiency of the above approach varies depending on the choice of the testing family of virtual characters. Shieh [Shi16] has proposed to use the family of irreducible characters $\{\chi_n\}_n$ of $\mathrm{USp}(2g)$ instead of the family of coefficient moments $\{a_k^n\}_{n,k}$. Shieh applies the Brauer-Klymik formula to recover $\chi_n(y_\mathfrak{p})$ from $L_\mathfrak{p}(A, T)$, and presents some numerical examples, where the family $\{\chi_n\}_n$ exhibits a much faster convergence than $\{a_k^n\}_{n,k}$. As remarked by Shieh

---

[8]Note that $\delta(a_k^n)$ is denoted by $M_n[a_k]$ in [FKRS12].

(see comment at the last paragraph of [Shi16, §1]), the difference between convergence rates of the two families is specially noticeable in the "generic cases", that is, when $G = \mathrm{USp}(2g)$.

For a virtual character φ of $\mathrm{USp}(2g)$, write

$$(5.2) \qquad \tilde{\varphi} := \varphi|_G - \delta(\varphi|_G) \,.$$

As discussed in §1, the asymptotic L^2-norm $I(\tilde{\varphi})$ can be seen as an estimate of the velocity convergence of $\delta(\varphi, X)$ towards $\delta(\varphi|_G)$. Under this perspective, we can see Corollary 4.4 as a justification of the efficiency of Shieh's proposal in the generic cases. Indeed, when χ_n is a nontrivial irreducible character of $\mathrm{USp}(2g)$ and $G = \mathrm{USp}(2g)$, the quantities $R_{\tilde{\chi}_n} = C_{\tilde{\chi}_n} = 1$ are smallest possible[9].

We remark, however, that $\{R_{\tilde{\chi}_n}\}_n$ and $\{C_{\tilde{\chi}_n}\}_n$ can grow unboundedly when we take certain nongeneric $G \subseteq \mathrm{USp}(2g)$. We will now introduce a family of virtual characters $\{s_n\}_n$ of $\mathrm{USp}(2g)$, for which the sequence $\{C_{\tilde{s}_n}\}_n$ (and thus also the sequence $\{R_{\tilde{s}_n}\}_n$) stays bounded for every Sato–Tate group $G \subseteq \mathrm{USp}(2g)$. Let V denote the standard representation of $\mathrm{USp}(2g)$. For $n \geq 0$ and $0 \leq k \leq 2g$, the (n, k)-th power sum is the virtual character

$$(5.3) \qquad s_n^k(\cdot) := \mathrm{Tr}(\Lambda^k V(\cdot^n)) \,.$$

To ease notation, we simply write $s_n := s_n^1$. We remark that the family of virtual characters $\{s_n\}_n$ had already been considered in [KS09].

Proposition 5.2. *Let G denote the Sato–Tate group of an abelian variety A of dimension g. Then, the sequence $\{C_{\tilde{s}_n}\}_n$ is bounded.*

Proof. Let $\mathfrak{g}$ denote the Lie algebra of G. Group representations of G correspond to Lie algebra representations of $\mathfrak{g}$. For every $n \geq 0$, one can write s_n as a finite sum of at most $2g$ weights of $\mathfrak{g}$. Since $\mathfrak{g}$ is semisimple, by [Gup87, Thm. 3.8] each weight of $\mathfrak{g}$ can be written as a bounded finite sum of distinct irreducible characters of $\mathfrak{g}$. Moreover, one easily sees from its description in [Gup87, Thm. 3.8], that the multiplicity of every irreducible constituent of a weight is also bounded. The proposition follows. $\qquad\square$

In the next section, we compare the convergence rates of the families $\{s_n\}_n$ and $\{a_1^n\}_n$ by computing the respective explicit bounds of Corollary 4.4 for some of the Sato–Tate groups G arising for $g = 1$ and $g = 2$.

5.1. **Rate of convergence of moments and power sums.**

5.1.1. *Dimension $g = 1$: non CM case.* The Sato–Tate group of an elliptic curve over k without CM is $G := \mathrm{USp}(2)$. If we denote by V the standard representation of G, then the irreducible characters of G are given by

$$(5.4) \qquad \chi_n := \mathrm{Tr}(\mathrm{Sym}^n(V)) \qquad \text{for } n \geq 0 \,.$$

For a virtual character φ of G, let $\tilde{\varphi}$ be as in (5.2), and let $R_{\tilde{\varphi}}$, $C_{\tilde{\varphi}}$, and $S_{\tilde{\varphi}}$ be as defined in Corollary 4.4. For $n \geq 2$, easy computations writing a_1^n and s_n in terms of the χ_n show that $S_{\tilde{a}_1^n} = S_{\tilde{s}_n}$ and that

$$R_{\tilde{a}_1^n} = \left\lceil \frac{n}{2} \right\rceil \,,\ C_{\tilde{a}_1^n} = 1 + \sum_{0 < j < n/2} \left(\binom{n}{j} - \binom{n}{j-1} \right)^2 \,, \quad \text{while} \quad R_{\tilde{s}_n} = 2 \,,\ C_{\tilde{s}_n} = 2 \,.$$

---

[9]However, we do not claim optimality of the family of irreducible characters (in terms of the velocity of convergence) among the class of families of central functions (see §6.1.7).

5.1.2. *Dimension $g = 1$: CM case.* Let E be an elliptic curve over k with CM defined over k. Its Sato–Tate group is

$$G := \left\{ A_u := \begin{pmatrix} u & 0 \\ 0 & \bar{u} \end{pmatrix} : |u| = 1 \right\} \simeq \mathrm{U}(1).$$

The irreducible characters of G are

(5.5) $$\nu_m \colon \mathrm{U}(1) \to \mathbb{C}^\times, \qquad \nu_m(A_u) = u^m \qquad \text{for } m \in \mathbb{Z}.$$

For $n \geq 1$, writing a_1^n and s_n in terms of the ν_m, one easily finds that $S_{\tilde{a}_1^n} = S_{\tilde{s}_n}$ and that

$$R_{\tilde{a}_1^n} = 2 \left\lceil \frac{n}{2} \right\rceil, \; C_{\tilde{a}_1^n} = \sum_{0 \leq j < n/2} 2 \binom{n}{j}^2, \quad \text{while} \quad R_{\tilde{s}_n} = 2, \, C_{\tilde{s}_n} = 2.$$

5.1.3. *Dimension $g = 2$: generic case.* The Sato–Tate group of an abelian surface A with trivial endomorphism ring is $G := \mathrm{USp}(4)$. The conjugacy classes of G are in bijection with $[0, \pi]^2/\mathfrak{S}_2$, where $\mathfrak{S}_2$ denotes the symmetric group on two letters. From [Wey97, Thm. 7.8.C, Chap. VII] one finds that the irreducible characters $\chi_{m,n}$ of G, for $m \geq n \geq 0$, are given by the formula

(5.6) $$\chi_{m,n}(\alpha, \beta) = \frac{\sin((m+2)\alpha)\sin((n+1)\beta) - \sin((m+2)\beta)\sin((n+1)\alpha)}{\sin(2\alpha)\sin(\beta) - \sin(2\beta)\sin(\alpha)},$$

where $(\alpha, \beta) \in [0, \pi]^2/\mathfrak{S}_2$. Note that $\chi_{1,0}$ is the trace of the standard representation of G. From (5.6), one finds by direct computation that

$$s_n = \chi_{n,0} - \chi_{n-1,1} + \chi_{n-3,1} - \chi_{n-4,0}$$

for $n \geq 4$. Similarly one computes that $s_2 = -\chi_{0,0} - \chi_{1,1} + \chi_{2,0}$ and $s_3 = -\chi_{2,1} + \chi_{3,0}$, and concludes that $R_{\tilde{s}_n}, C_{\tilde{s}_n} \leq 4$.

Let us show on the other hand that the sequence $\{R_{\tilde{a}_1^n}\}_n$ (and thus also $\{C_{\tilde{a}_1^n}\}_n$) grows unboundedly[10] in n. Let now V denote the standard representation of $\mathrm{USp}(4)$. Let W be the representation defined by $\Lambda^2 V = W \oplus \mathbb{C}$, which has character $\chi_{1,1}$. By [FH91, p.248] the character $\chi_{m,n}$ is the character of a subrepresentation[11] of

(5.7) $$\mathrm{Sym}^{m-n}(V) \otimes \mathrm{Sym}^n(W).$$

But note that the above representation is a subrepresentation of $V^{(m+n)\otimes}$, from which we deduce that a_1^t contains all the irreducible characters $\chi_{m,n}$ for which $m + n = t$ and $m \geq n$.

Finally, one can use [FH91, Ex. 24.20] to show that $S_{\tilde{a}_1^n}$ and $S_{\tilde{s}_n}$ are of comparable size.

---

[10]Using [Wey97, §9, Chap. VII], one can obtain a closed formula for $C_{\tilde{a}_1^n}$, but we will not pursue this here. We will content ourselves with listing a few of them:

$$C_{\tilde{a}_1^2} = 1^2 + 1^2 + 1^2, \quad C_{\tilde{a}_1^3} = 3^2 + 2^2 + 1^2, \quad C_{\tilde{a}_1^4} = 3^2 + 5^2 + 6^2 + 2^2 + 3^2 + 1^2.$$

[11]Note that in [FH91, §16.2], it is written $\Gamma_{m-n,n}$ to denote the representation that is attached to the character that we denote by $\chi_{m,n}$.

6. Examples

In this section, we illustrate the content of Theorem 1.3 by means of considering a few examples. Except of the example in §6.1.7 (which has a different purpose), they all follow the same pattern: we take two abelian varieties A and A' defined over k, of the same dimension $g \geq 1$, and similar conductors, but with distinct arithmetic invariants such as the rank or the Sato–Tate group. Let G (resp. G') denote the Sato–Tate groups of A (resp. A'). We take a selfdual character φ_0 of $\mathrm{USp}(2g)$ such that its restriction φ (resp. φ') to G (resp. G') does not contain the trivial character. We then plot the functions $\delta(\varphi, x)^2$ and $\delta(\varphi', x)^2$ for x in a wide range of values, and certify that they exhibit the behaviour predicted by Theorem 1.3.

Recall that we can write

$$I(\varphi) = I_1(\varphi) + I_2(\varphi),$$

where $I_1(\varphi)$ and $I_2(\varphi)$ are as defined in (4.4). If $\varphi = \sum_\chi c_\chi \chi$, let us write $r_\varphi := \sum_\chi c_\chi r_\chi$. In the examples below, it will be convenient to use the suggestive notation $r_{\varphi_0(A)} := r_\varphi$. In the case that φ is the character of the tautological representation of G, we will simply write r_A for r_φ. Note that r_A is the so called *analytic rank of A*, that is, the order of vanishing of the Hasse–Weil L-function of A at the central point. By definition, we have

$$I_1(\varphi) = (2r_\varphi + u_\varphi)^2,$$

where u_φ denotes the Frobenius–Schur index of φ.

As one can see from the proof of Proposition 4.2, a large conductor N of A with respect to the rank makes the term $I_2(\varphi)$ dominant, blurring the contribution of $I_1(\varphi)$ in the asymptotic L^2-norm $I(\varphi)$. In order to illustrate the influence in the convergence rate of the arithmetic invariants of A appearing in $I_1(\varphi)$ (the rank and the Sato–Tate group), we will often consider examples for which r_φ or r'_φ is exceptionally large with respect to the conductor N. This is what we call examples of 'relatively large rank with respect to the conductor'. In the examples considered, it is $I_1(\varphi)$ which happens to dominate $I_2(\varphi)$.

In §6.1 and §6.2, we will use the following lemma.

Lemma 6.1. *Let ν_m, χ_n, and $\chi_{m,n}$ denote the irreducible characters of $\mathrm{U}(1)$, $\mathrm{USp}(2)$, and $\mathrm{USp}(4)$ as defined in (5.5), (5.4), and (5.6). Their respective Frobenius–Schur indices are*

$$u_{\nu_m} = \begin{cases} 1 & \text{if } m = 0, \\ 0 & \text{otherwise,} \end{cases} \qquad u_{\chi_n} = (-1)^n, \qquad u_{\chi_{m,n}} = (-1)^{n+m}.$$

Proof. The statement for ν_m is clear, provided that ν_m takes complex values if and only if $m \neq 0$. By [Ser77, Prop. 38], a character χ of a compact group G has $u_\chi = 1$ (resp. $u_\chi = -1$) if it corresponds to a representation ϱ which is symmetric (resp. alternating)[12]. Since the standard representation of $\mathrm{USp}(2)$ is alternating, we deduce that $u_{\chi_n} = (-1)^n$ from the fact that the product of an alternating representation and a symmetric one is alternating, and that the product of two alternating (resp. symmetric) representations is symmetric. Let V denote the standard representation of $\mathrm{USp}(4)$ and W be the representation of $\mathrm{USp}(4)$ defined in §5.1.3, so that $\chi_{m,n}$ is the character of a subrepresentation of $\mathrm{Sym}^{m-n}(V) \otimes \mathrm{Sym}^n(W)$. Note that since V is alternating, we have that W is symmetric. Since a subrepresentation of an alternating (resp. symmetric) representation is alternating (resp. symmetric), we find that $u_{\chi_{m,n}} = (-1)^{m-n} = (-1)^{m+n}$. □

---

[12]By this we mean that the module V affording ϱ possesses a nonzero nondegenerate G-invariant bilinear form which is symmetric (resp. alternating).

Remark 6.2. If χ is an irreducible character of G, recall that we denote by w_χ its weight (as defined in Remark 4.1). By deep conjectures (see §6.2) one expects a different behaviour of r_χ depending on whether w_χ is odd or even. In order to isolate these two typical behaviors, and although there is no such restriction in Theorem 1.3, in all the examples below we consider virtual characters φ such that their constituents are either all of odd weight or all of even weight.

Remark 6.3. In order to determine the value of the function $\delta(\varphi, x)$, we use Sutherland's library Smalljac [KS08], which computes the polynomials $L_{\mathfrak{p}}(A, T)$. One limitation of the version that we use is that it only works for abelian varieties defined over $\mathbb{Q}$. However, this is enough to deal with abelian varieties over an arbitrary number field k which are the base change of an abelian variety defined over $\mathbb{Q}$ (see §6.1.4).

6.1. **Odd weight.** In the following examples, all the irreducible constituents of φ and φ' have odd weight.

6.1.1. *Example 1: The rank matters ($g = 1$).* Let A, A' be two elliptic curves defined over $\mathbb{Q}$ without CM (i.e. with Sato–Tate groups $G = G' = \mathrm{USp}(2)$) with similar conductor and analytic ranks $r_A = 1$ and $r_{A'} = 2$. Let $\varphi_0 = a_1$ be the character of $\mathrm{USp}(2)$ defined in (5.1). Using Lemma 6.1, we obtain that

$$I_1(\varphi) = (2 \cdot 1 - 1)^2 = 1\,, \qquad I_1(\varphi') = (2 \cdot 2 - 1)^2 = 9\,.$$

In Figure 1 we plot the function $\delta(a_1, x)^2$ for two elliptic curves A and A' of similar conductor and ranks 1 and 2 (this is a slight abuse of notation to mean that we plot $\delta(\varphi, x)^2$ and $\delta(\varphi', x)^2$, as explained above). We indeed observe a better convergence of the curve of rank 1.

6.1.2. *Example 2: The Frobenius–Schur index matters ($g = 1$).* Let A, A', and φ_0 be as in §6.1.1, but suppose that now $r_A = 1$ and $r_{A'} = 0$. Now we have

$$I_1(\varphi) = (2 \cdot 1 - 1)^2 = 1\,, \qquad I_1(\varphi') = (2 \cdot 0 - 1)^2 = 1\,.$$

In Figure 2 we plot $\delta(a_1, x)^2$ for two non-CM elliptic curves of the same conductor and ranks 0 and 1. In this case we observe a similar convergence rate.

6.1.3. *Example 3: The Sato–Tate group matters ($g = 1$).* Let A (resp. A') be an elliptic curve defined over $\mathbb{Q}$ without (resp. with) complex multiplication, and let $\varphi_0 = a_1^3$ be the cube of the trace character of $\mathrm{USp}(2)$. We have $G = \mathrm{USp}(2)$ and $G' = \mathrm{U}(1) \rtimes \mathbb{Z}/2\mathbb{Z}$.

Proposition 6.4. *If φ_0, A and A' are as above, then*

$$I_1(\varphi) = (4r_A + 2r_{\mathrm{Sym}^3(A)} - 3)^2\,, \qquad I_1(\varphi') = (4r_{A'} + 2r_{\mathrm{Sym}^3(A')} - 4)^2\,.$$

Proof. From [Ser77, §8.2], one easily finds that the irreducible characters of G' are

$$\varrho_m := \mathrm{Tr}(\mathrm{Ind}_{\mathrm{U}(1)}^{G'}(\nu_m))$$

for $m \geq 0$, where ν_m is as in (5.5). Let σ denote the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$. For $(A_u, s) \in \mathrm{U}(1) \rtimes \mathbb{Z}/2\mathbb{Z}$, one has

$$\varrho_m(A_u, s) = \begin{cases} u^m + u^{-m} & \text{if } s \text{ is trivial,} \\ 0 & \text{if } s = \sigma. \end{cases}$$

It follows that $\varphi' = 3\varrho_1 + \varrho_3$ and then, using Lemma 6.1, that

$$I_1(\varphi') = (2(r_{\mathrm{Sym}^3(A')} - r_{A'}) - 1 + 3(2 \cdot r_{A'} - 1))^2 = (4r_{A'} + 2r_{\mathrm{Sym}^3(A')} - 4)^2$$
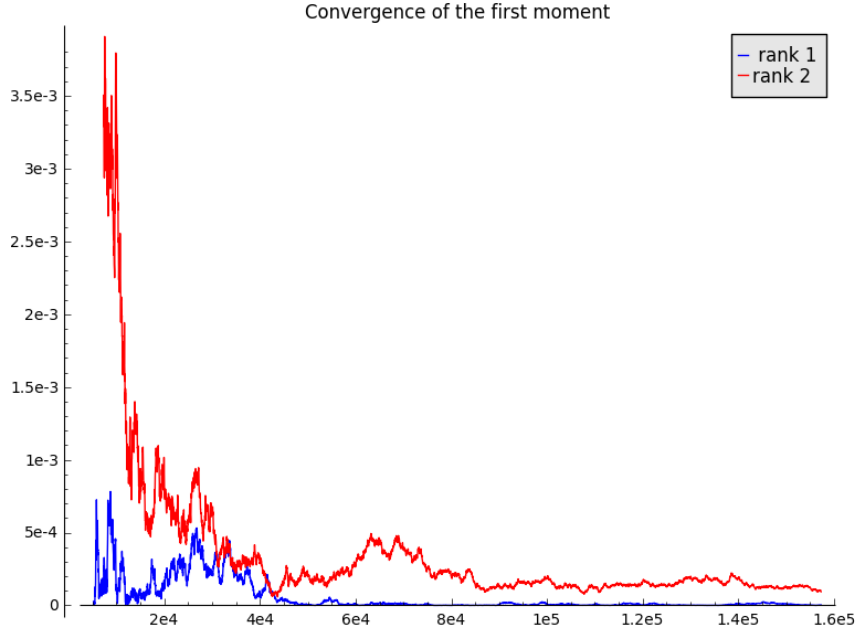
FIGURE 1. Plot of $\delta(a_1, x)^2$ for the non-CM elliptic curves with LMFDB label 390.a1 (of rank 1) and 389.a1 (of rank 2).

Provided that $\varphi = 2\chi_1 + \chi_3$, where χ_n is as in (5.4), we obtain that

$$I_1(\varphi) = \left((2 \cdot r_{\chi_3} - 1) + 2(2 \cdot r_{\chi_1} - 1)\right)^2 = (4r_A + 2r_{\mathrm{Sym}^3(A)} - 3)^2 \,,$$

and the proposition follows. $\qquad\square$

One can take now A and A' with similar conductors and such that $r_{\mathrm{Sym}^3(A)} = r_{\mathrm{Sym}^3(A')}$ and $r_A = r_{A'}$. If we take these analytic ranks to be respectively 1 and 0, we find

$$I_1(\varphi) = 1 \,, \qquad I_1(\varphi') = 4 \,.$$

In Figure 3 we plot $\delta(a_1^3, x)^2$ for two curves A, A' with the above invariants. We observe that for large values of x, even though the two plots cross many times, the one corresponding to the CM curve seems to have a larger asymptotic L^2-norm.

Remark 6.5. Note that, in the situation considered, if we had we taken $\varphi_0 = a_1$, no significant difference would have been observed between the convergence of $\delta(\varphi, x)$ and $\delta(\varphi', x)$. Indeed, in this case, one finds $I_1(\varphi) = (2 \cdot r_A - 1)^2 = (2 \cdot r_{A'} - 1)^2 = I_1(\varphi')$ (compare with §6.1.4).

6.1.4. *Example 3': The Sato–Tate group matters (g = 1).* We will now consider an example over a finite extension of $\mathbb{Q}$. Let K be a quadratic imaginary field, A be an elliptic curve defined over K without CM, and A' an elliptic curve defined over K with CM precisely by K. As in the previous example, let $\varphi_0 = a_1^3$. Note that φ' is a selfdual character of U(1), even if its irreducible constituents are not.
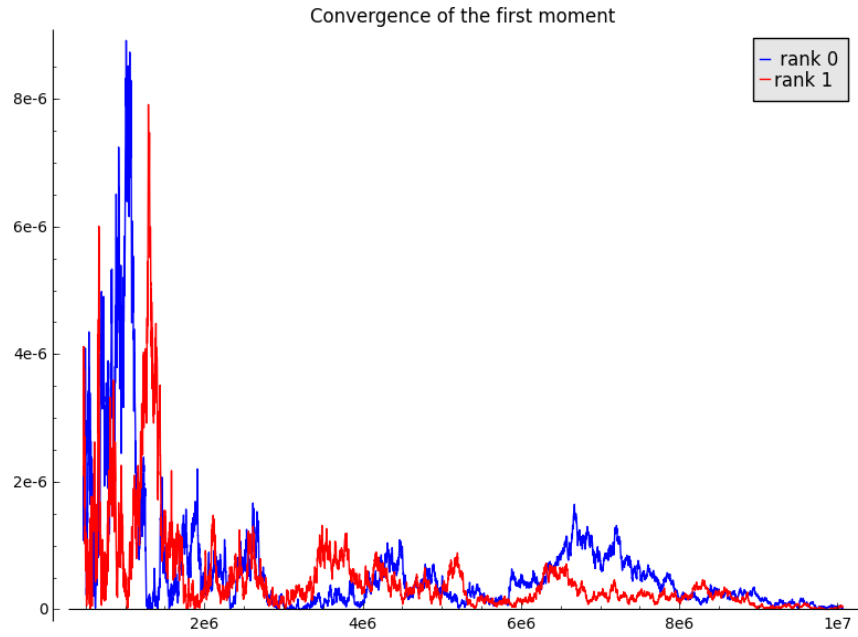
FIGURE 2. Plot of $\delta(a_1, x)^2$ for the non-CM elliptic curves with LMFDB label 37.b2 (of rank 0) and 37.a1 (of rank 1).
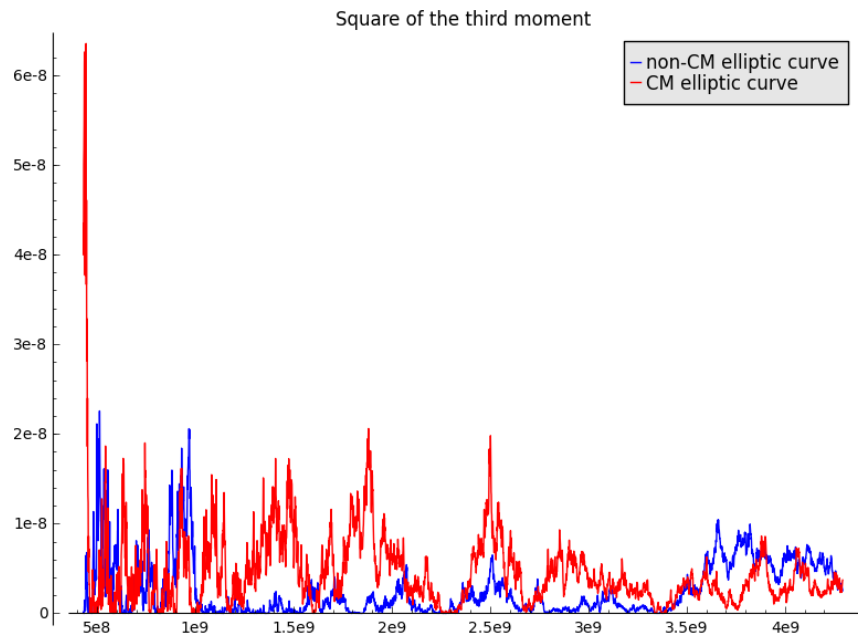

FIGURE 3. Plot of $\delta(a_1^3, x)^2$ for the rank 0 curves 40.a1 (non-CM) and 49.a1 (CM).

Proposition 6.6. *If φ_0, A and A' are as above, then*

$$I_1(\varphi) = (4r_A + 2r_{\mathrm{Sym}^3(A)} - 3)^2, \qquad I_1(\varphi') = (4r_{A'} + 2r_{\mathrm{Sym}^3(A')})^2.$$

Proof. Note that $\varphi' = \nu_{-3} + 3\nu_{-1} + 3\nu_1 + \nu_3$, where ν_m is as in (5.5). Using Lemma 6.1, one finds that

$$I_1(\varphi') = \left((2 \cdot r_{\nu_{-3}} - 0) + 3(2 \cdot r_{\nu_{-1}} - 0) + 3(2 \cdot r_{\nu_1} - 0) + (2 \cdot r_{\nu_3} - 0)\right)^2 = (4r_{A'} + 2r_{\mathrm{Sym}^3(A')})^2.$$

The computation of $I_1(\varphi)$ is exactly as in Proposition 6.4. $\qquad\square$

One can take now A and A' with similar conductors and such that $r_{\mathrm{Sym}^3(A)} = r_{\mathrm{Sym}^3(A')}$ and $r_A = r_{A'}$. By Remark 6.3, we are forced to take A and A' to be the base change of elliptic curves A_0 and A_0' defined over $\mathbb{Q}$. Then the following lemma implies that these two analytic ranks must be even and satisfy $r_{\mathrm{Sym}^3(A')} \geq r_{A'}$.

Lemma 6.7. *Let E be an elliptic curve over $\mathbb{Q}$ and $\tilde{E}$ the quadratic twist of E by the quadratic extension $K/\mathbb{Q}$. Then*

$$r_{E_K} = r_E + r_{\tilde{E}}, \qquad r_{\mathrm{Sym}^3(E_K)} = r_{\mathrm{Sym}^3(E)} + r_{\mathrm{Sym}^3(\tilde{E})}.$$

Moreover, if K is imaginary and E has CM by K, then

$$r_{E_K} = 2r_E, \qquad r_{\mathrm{Sym}^3(E_K)} = 2r_{\mathrm{Sym}^3(E)}, \qquad r_{\mathrm{Sym}^3(E_K)} \geq r_{E_K}.$$

Proof. Let ε denote the quadratic character of $K/\mathbb{Q}$. We have isomorphisms of $\mathbb{Q}_\ell[G_\mathbb{Q}]$-modules

$$\mathrm{Ind}_{G_\mathbb{Q}}^{G_K} \mathrm{Sym}^3(V_\ell(E_K)) \simeq \mathrm{Sym}^3(V_\ell(E)) \oplus \mathrm{Sym}^3(V_\ell(E)) \otimes \varepsilon \simeq \mathrm{Sym}^3(V_\ell(E)) \oplus \mathrm{Sym}^3(V_\ell(\tilde{E})),$$

and the first part of the lemma follows from the Artin Formalism of L-functions. For the second part, one first needs to note that, under the additional hypothesis, one has

$$V_\ell(E) \simeq V_\ell(E) \otimes \varepsilon \simeq V_\ell(\tilde{E}).$$

This follows from the fact that $\mathrm{Tr}(V_\ell(E))(\sigma) = 0$, whenever $\varepsilon(\sigma) \neq 1$ for $\sigma \in G_\mathbb{Q}$. One then concludes by noting that there is a Hecke character Φ such that

$$\mathrm{Sym}^m V_\ell(E_K) \simeq \bigoplus_{j=0}^m \Phi^{m-2j}(j),$$

where $\Phi^{m-2j}(j)$ denotes the j-th Tate twist of Φ^{m-2j}. $\qquad\square$

If we take for example $r_{\mathrm{Sym}^3(A)} = r_{\mathrm{Sym}^3(A')} = 4$ and $r_A = r_{A'} = 2$, we obtain that

$$I_1(\varphi) = 144, \qquad I_2(\varphi') = 256.$$

In order to find examples of this type we have used [MW06, Table 7] for the non-CM curves, and Watkins's `Sympow` package to find the CM curves with appropriate order of vanishing of the third symmetric power.

In Figure 3' we plot $\delta(a_1^3, x)^2$ for two elliptic curves A/K and A'/K, where $K = \mathbb{Q}(\sqrt{-3})$. The curve A is the base change to K of the curve with LMFDB label 97448.a2; its conductor is the ideal of K generated by 97448, it does not have CM and its ranks are $r_A = 2$ and $r_{\mathrm{Sym}^3(A)} = 4$. The curve A' is the base change to K of the CM curve with LMFDB label 248004.g1; its conductor is the ideal of K generated by 82668, it has CM by K, and its ranks are $r_{A'} = 2$ and $r_{\mathrm{Sym}^3(A')} = 4$. We observe a better convergence for the non-CM curve.
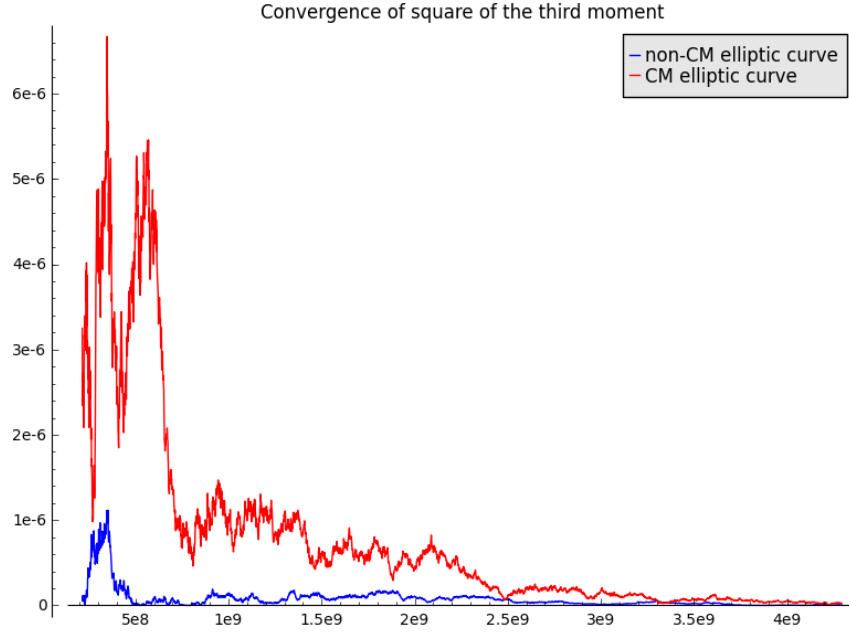
FIGURE 3'. Plot of $\delta(a_1^3, x)^2$ for two elliptic curves over $\mathbb{Q}(\sqrt{-3})$ of rank 2 and rank of the symmetric cube 4, without CM and the other with CM by K.

Remark 6.8. In order to plot $\delta(a_1^3, x)^2$ one needs to recover the polynomials $L_{\mathfrak{p}}(A, T)$ from the polynomials $L_p(A_0, T)$ computed by Smalljack. This is straightforward. Let $\mathfrak{p}$ be an unramified prime of K lying over p. If $\mathfrak{p}$ is split over $\mathbb{Q}$, then Smalljac directly returns $L_{\mathfrak{p}}(A, T) = L_p(A_0, T)$. If $\mathfrak{p}$ is inert over $\mathbb{Q}$, then

$$L_{\mathfrak{p}}(A, T) = (1 - \alpha_p^2)(1 - \bar{\alpha}_p^2) = 1 - (a_p^2 - 2)T + T^2 \,,$$

where

$$L_p(A_0, T) = (1 - \alpha_p)(1 - \bar{\alpha}_p) = 1 - a_p T + T^2 \,.$$

Remark 6.9. For this example we could have taken $\varphi_0 = a_1$. Similar computations show that then $I_1(\varphi) = 4r_A^2$ and $I_1(\varphi') = (2r_A - 1)^2$.

6.1.5. *Example 4: The rank matters ($g = 2$).* Let A, A', A'', and A''' be abelian surfaces of similar conductor, with Sato–Tate group $\mathrm{USp}(4)$, and respective ranks 0, 1, 2, and 3. Letting $\varphi_0 = a_1$ and φ, φ'',... have the obvious meaning, we have that

$$I_1(\varphi) = 1 \,, \qquad I_1(\varphi') = 1 \,, \qquad I_1(\varphi'') = 9 \,, \qquad I_1(\varphi''') = 25 \,.$$

In Figure 4 we plot the function $\delta(a_1, x)^2$ for four abelian surfaces of similar conductors and ranks 0, 1, 2, and 3.

6.1.6. *Example 5: The Sato–Tate group matters ($g = 2$).* Let A and A' be abelian surfaces defined over $\mathbb{Q}$ of similar conductor, with analytic rank $r_A = r_{A'} = 2$, but with Sato–Tate groups $G = \mathrm{USp}(4)$ and $G' = \mathrm{USp}(2) \times \mathrm{USp}(2)$ (the group denoted by $G_{3,3}$ in [FKRS12]). More specifically,
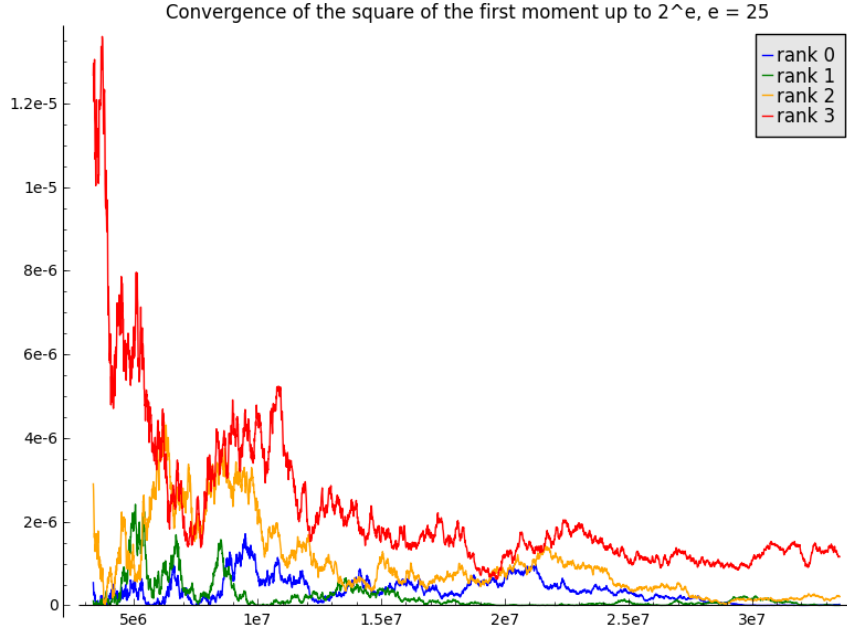
FIGURE 4. Plot of $\delta(a_1, x)^2$ for the (Jacobians of the) genus two curves with LMFDB labels 62127.a (of rank 0), 61929.a (rank 1), 62090.a (rank 2), and 62411.b (rank 3). They all have Sato–Tate group $\mathrm{USp}(4)$, and the number in the label indicates the conductor of the curve.

suppose that A' decomposes over $\mathbb{Q}$ as the product of two nonisogenous elliptic curves of rank 1. Taking $\varphi_0 = a_1$, we obtain

$$I_1(\varphi) = (2 \cdot 2 - 1)^2 = 9\,, \qquad I_1(\varphi') = (2 \cdot 1 - 1 + 2 \cdot 1 - 1)^2 = 4\,.$$

An example of this phenomenon is shown in Figure 5.

6.1.7. *Example 6: Non-optimality of the irreducible characters.* The goal of this example is to show that, although in §5 we demonstrated that the irreducible characters of $\mathrm{USp}(2g)$ exhibit an extremely good convergence in the *generic cases* (and, in fact, almost optimal), one can find particular examples for which their convergence is beaten by some other family of characters, which are still a basis of the central functions. For example, let A be an elliptic curve without CM such that $r_A = 2$ and $r_{\mathrm{Sym}^3(A)} = 0$. Let χ_n be as in (5.4), and for $n \geq 0$ set

$$\chi'_n := \begin{cases} \chi_1 + \chi_3 & \text{if } n = 1, \\ \chi_n & \text{otherwise.} \end{cases}$$

Clearly, $\{\chi'_n\}_{n \geq 0}$ is also a basis of the central functions on G, and $I_1(\chi_n) = I_1(\chi'_n)$ for every $n \neq 1$. However,

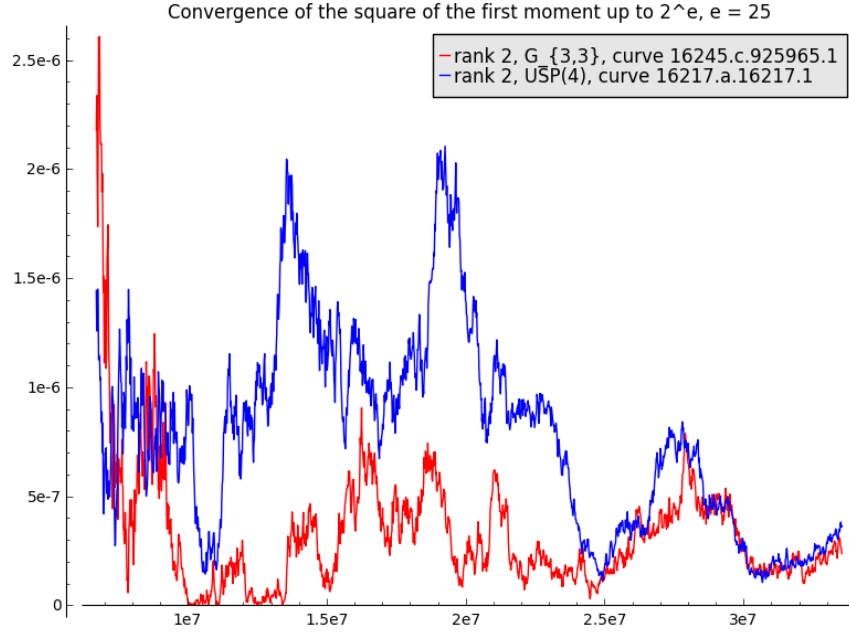$$I_1(\chi_1) = (2 \cdot 2 - 1)^2 > (2 \cdot 2 - 1 + 2 \cdot 0 - 1)^2 = I_1(\chi'_1)\,.$$

FIGURE 5. Plot of $\delta(a_1, x)^2$ for the genus two curves with LMFDB labels 16217.a (of rank 2 and Sato–Tate group USp(4)) and 16245.c (of rank 2 and Sato–Tate group $G_{3,3}$).

In Figure 6 we plot $\delta(\chi_1, x)^2$ and $\delta(\chi_1 + \chi_3, x)^2$ for the elliptic curve E with LMFDB label 389.a1. It has $r_E = 2$ and $r_{\mathrm{Sym}^3 E} = 0$. Even though $\chi_1 + \chi_3$ is not always below χ_1, it does seem to close a smaller area.

6.2. **Even weight.** Let χ be an irreducible character of G and let w_χ denote its weight. If w_χ is odd, then $(w_\chi + 1)/2$ is an integer, and the Bloch–Kato conjecture predicts the order of the zero at $(w_\chi + 1)/2$ of the L-function attached to $\chi \circ \varrho_A$, which is precisely r_χ.

If w_χ is even, then $(w_\chi + 1)/2$ is no longer an integer and the Bloch–Kato conjecture makes no prediction for the order of vanishing of the L-function attached to $\chi \circ \varrho_A$ at this point. The general philosophy is that r_χ should be 0 unless there is a specific reason for the contrary to happen, and one thus expects $r_\chi = 0$ for χ of even weight.

If $\chi_{m,n}$ is as in (5.6), then (5.7) implies that $\chi_{m,n}$ has even weight if and only if $m + n$ is even. One thus expects $r_{\chi_{m,n}} = 0$ whenever $m + n$ is even. Using [Wey97, §9, Chap. VII] again, one easily finds that

$$a_2 - 1 = \chi_{1,1}, \qquad a_1^2 - 1 = \chi_{1,1} + \chi_{2,0}, \qquad s_2 + 1 = -\chi_{1,1} + \chi_{2,0}.$$

Let now A be an abelian surface with Sato–Tate group USp(4). By Lemma 6.1, we have that

$$I_1(a_2 - 1) = (2 \cdot 0 + 1)^2 = 1, \quad I_1(a_1^2 - 1) = (2 \cdot 0 + 1 + 2 \cdot 0 + 1)^2 = 4 \quad I_1(s_2 + 1) = (-(2 \cdot 0 + 1) + (2 \cdot 0 + 1))^2 = 0.$$

In Figure 7 we plot $\delta(a_1^2 - 1, x)^2$, $\delta(a_2 - 1, x)^2$, and $\delta(s_2 + 1, x)^2$. Observe that, even though $I_1(a_2 - 1) > I_1(s_2 + 1)$, it is not clear from the figure whether the convergence for $s_2 + 1$ is better than the convergence for $a_2 - 1$. This seems to be explained by the fact that the difference
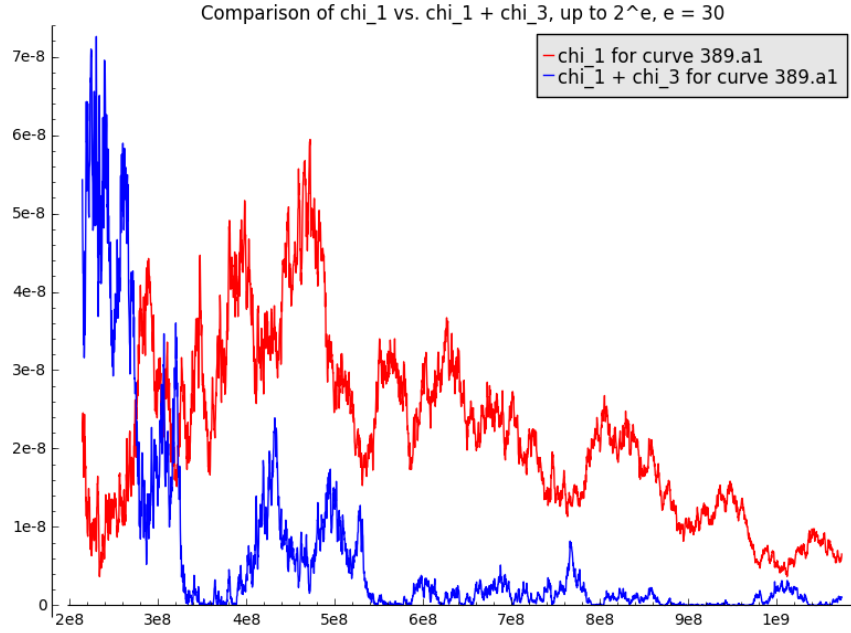
FIGURE 6. Plot of $\delta(\chi_1, x)^2$ and $\delta(\chi_1 + \chi_3, x)^2$ for the elliptic curve E with label 389.a1
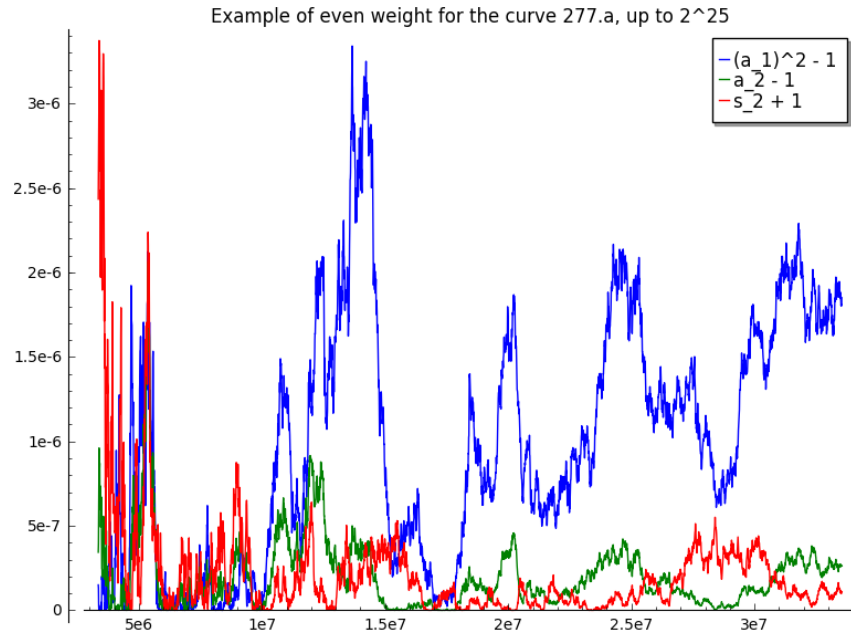

FIGURE 7. Plot of $\delta(a_1^2 - 1, x)^2$, $\delta(a_2 - 1, x)^2$, and $\delta(s_2 + 1, x)^2$ for the genus two curve 277.a

$I_1(a_2 - 1) - I_1(s_2 + 1)$ is small together with the fact that $I_2(a_2 - 1) \leq I_2(s_2 + 1)$. Nonetheless, in the range of primes that we have considered, one clearly appreciates a worse convergence for $a_1^2 - 1$ than for $a_2 - 1$ and $s_2 + 1$.

7. Chebyshev bias for abelian varieties

As we noted in §1, the circle of ideas we used to study the convergence rate towards the Sato–Tate measure was introduced by Sarnak in his letter to Barry Mazur [Sar07], in order to explain the bias that the Frobenius traces of elliptic curves have towards being positive or negative, and how the rank determines the sign of the bias.

Not surprisingly, then, one can also use this approach to study this phenomenon for general abelian varieties. Indeed, resuming the notations of §1, for a selfdual virtual character $\varphi = \sum_{\chi \neq 1} c_\chi \chi$ of G, recall the function

$$(7.1) \qquad \psi(\varphi, x) = \frac{\log(x)}{\sqrt{x}} \sum_{|\mathfrak{p}| \leq x} \varphi(y_\mathfrak{p}).$$

If in the proof of Theorem 1.3 we apply the formula for the expectation, rather than the variance, from Proposition 3.1 we see that

$$(7.2) \qquad \lim_{X \to \infty} \frac{1}{\log(X)} \int_2^X \frac{\psi(\varphi, x))}{x} dx = -\sum_\chi c_\chi (2r_\chi + u_\chi).$$

In the case of elliptic curves, the bias of a_1 towards being positive or negative only depends on the rank. In higher dimensions, the above formula shows that it also depends on the Sato–Tate group. For example, suppose that A is an abelian surface of rank $r_A = 1$. Then the right hand side of (7.2) equals $-(2r_A - 1) = -1$, and a_1 has a bias towards being negative. Suppose now that A' is an abelian surface of rank $r_{A'} = 1$ and Sato–Tate group $G_{3,3}$. Suppose that A' is isogenous to the product of two elliptic curves, say E and E', of ranks $r_E = 1$ and $r_{E'} = 0$. Then the right hand side of (7.2) equals $-(2r_E - 1) - (2r_{E'} - 1) = 0$, and the a_1's do not have bias towards being positive nor negative. In Figure 8 we plot the function $\delta(a_1, x)$ for two abelian surfaces A and A' having these ranks and Sato–Tate groups. The prediction on the bias of the sign of a_1 can be clearly observed.

References

[ANS14] Amir Akbary, Nathan Ng, and Majid Shahabi, *Limiting distributions of the classical error terms of prime number theory*, Q. J. Math. **65** (2014), no. 3, 743–780. MR 3261965

[BK16a] Grzegorz Banaszak and Kiran S. Kedlaya, *Motivic Serre group, algebraic Sato-Tate group and Sato-Tate conjecture*, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 11–44. MR 3502937

[BK16b] Alina Bucur and Kiran S. Kedlaya, *An application of the effective Sato-Tate conjecture*, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, Contemp. Math., vol. 663, Amer. Math. Soc., Providence, RI, 2016, pp. 45–56. MR 3502938

[Cog03] J. W. Cogdell, *Langlands conjectures for* GL_n, An introduction to the Langlands program (Jerusalem, 2001), Birkhäuser Boston, Boston, MA, 2003, pp. 229–249. MR 1990381

[FH91] William Fulton and Joe Harris, *Representation theory*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991, A first course, Readings in Mathematics. MR 1153249

[FKRS12] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*, Compos. Math. **148** (2012), no. 5, 1390–1442. MR 2982436

[Gup87] R. K. Gupta, *Characters and the q-analog of weight multiplicity*, J. London Math. Soc. (2) **36** (1987), no. 1, 68–76. MR 897675
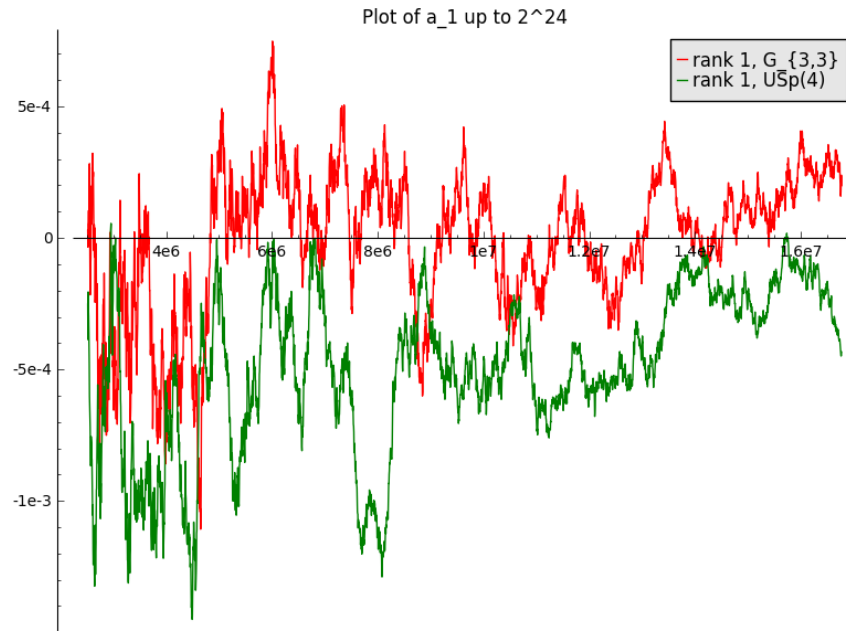
FIGURE 8. Plot of $\delta(a_1, x)$ for the genus two curve 2165.a (rank 1 and Sato–Tate group USp(4)) and for 2156.b (rank 1 and Sato–Tate group $G_{3,3}$).

[IK04]   Henryk Iwaniec and Emmanuel Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004. MR 2061214

[KS08]   Kiran S. Kedlaya and Andrew V. Sutherland, *Computing L-series of hyperelliptic curves*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 312–326. MR 2467855

[KS09]   ———, *Hyperelliptic curves, L-polynomials, and random matrices*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 487, Amer. Math. Soc., Providence, RI, 2009, pp. 119–162. MR 2555991

[Mur85]   V. Kumar Murty, *Explicit formulae and the Lang-Trotter conjecture*, Rocky Mountain J. Math. **15** (1985), no. 2, 535–551, Number theory (Winnipeg, Man., 1983). MR 823264

[MW06]   Phil Martin and Mark Watkins, *Symmetric powers of elliptic curve L-functions*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 377–392. MR 2282937

[RS94]   Michael Rubinstein and Peter Sarnak, *Chebyshev's bias*, Experiment. Math. **3** (1994), no. 3, 173–197. MR 1329368

[Sar07]   Peter Sarnak, *Letter to Barry Mazur on "Chebyshev's bias" for $\tau(p)$*.

[Ser68]   Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968. MR 0263823

[Ser70]   ———, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou. Théorie des nombres 11.2, 1969-1970, pp. 1–15.

[Ser77]   ———, *Linear representations of finite groups*, Springer-Verlag, New York-Heidelberg, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42. MR 0450380

[Ser94]   ———, *Propriétés conjecturales des groupes de Galois motiviques et des représentations l-adiques*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 377–400. MR 1265537

[Shi16]   Yih-Dar Shieh, *Character theory approach to Sato-Tate groups*, LMS J. Comput. Math. **19** (2016), no. suppl. A, 301–314. MR 3540962

[Wey97]   Hermann Weyl, *The classical groups*, Princeton Landmarks in Mathematics, Princeton University Press, Princeton, NJ, 1997, Their invariants and representations, Fifteenth printing, Princeton Paperbacks. MR 1488158

Departament de Matemàtiques, Universitat Politècnica de Catalunya/BGSmath, Edifici Omega, C/Jordi Girona 1–3, 08034 Barcelona, Catalonia
    E-mail address: francesc.fite@gmail.com
    URL: https://mat-web.upc.edu/people/francesc.fite/

Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Gran via de les Corts Catalanes, 585, 08007 Barcelona, Catalonia
    E-mail address: xevi.guitart@gmail.com
    URL: http://atlas.mat.ub.edu/personals/guitart/