Effective Sato–Tate under GRH

Alina Bucur

Department of Mathematics, UCSD; alina@math.ucsd.edu

joint work with Francesc Fité (MIT) and Kiran S. Kedlaya (UCSD)

Thanks to NSF, Simons Foundation, IAS.

The prime number theorem

Theorem (Hadamard, de la Vallée-Poussin)

Let $\pi(x)$ denote the number of prime numbers less than or equal to x. Then

$$\pi(x) = \Big(1 + o(1)\Big)\ \frac{x}{\log x}.$$

Basic idea: exploit the relationship between prime numbers and the zeroes of the Riemann zeta function.

Theorem (effective PNT under GRH)

Assume that the zeroes of the Riemann zeta function in the critical strip $0 \leq \mathrm{Re}(s) \leq 1$ all lie on the line $\mathrm{Re}(s) = 1/2$. Then

$$\pi(x) = \mathrm{Li}(x) + O(x^{1/2}\log x) \qquad \left(\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}\right).$$

Basic analytic number theory

Assume that for $\mathrm{Re}(s) > 1$

$$L(s) = \sum \frac{a_n}{n^s} = \prod (1 - a_p p^{-s} + \dots)^{-1}$$

We will use the following basic application of Cauchy's integral formula:

$$\int_{2-i\infty}^{2+i\infty} x^s \frac{ds}{s} = \begin{cases} 0 & 0 < x < 1 \\ 1/2 & x = 1 \\ 1 & x > 1. \end{cases}$$

Thus

$$\int_{2-i\infty}^{2+i\infty} L(s) x^s \frac{ds}{s} = \sum a_n \int_{2-i\infty}^{2+i\infty} \frac{x^s}{n^s} \frac{ds}{s} = \sum_{n<x} a_n.$$

Prime number theorem: we want to get $\sum_{p<x} 1$ not $\sum_{n<x} 1$.
Solution: logarithmic derivatives.
Namely, we will apply the previous strategy to

$$-\frac{L'(s)}{L(s)} = -\frac{d}{ds}\log L(s) = \sum_p \frac{d}{ds}\log(1 - a_p p^{-s} + \dots)$$
$$= \sum_p a_p \log(p) p^{-s} + \dots$$

This will lead us to an estimate of the form

$$\sum_{p<x} a_p \log p = \int_{2-i\infty}^{2+i\infty} -\frac{L'(s)}{L(s)} x^s \frac{ds}{s} + \text{ error term}$$

and then we use Abel summation to obtain an estimate for $\sum_{p<x} a_p$.

Other effective results

- The Chebotarev density theorem (describing the distribution of Frobenius classes for a fixed Galois extension of K)
  This effectivization process was described by Lagarias and Odlyzko (1977).
- The Sato–Tate conjecture (describing the distribution of Frobenius traces for a fixed elliptic curve over K)
  It was established for K totally real through the efforts of Taylor et al. (2011) and for CM fields by Allen et al. (2019).
  In this case, the effectivization process had been described previously by Kumar Murty (1985).

The previous two examples can both be subsumed into a generalized Sato–Tate conjecture for an arbitrary motive, taking an Artin motive in the case of Chebotarev and the 1-motive of an elliptic curve in the case of Sato–Tate.

Today

Under suitable analytic hypotheses on motivic L-functions, we will obtain effective error bounds for the generalized Sato−Tate conjecture and apply them to a question about abelian varieties.

Setup: B–Kedlaya

K is a number field.
E_1 and E_2 are nonisogenous elliptic curves over K, neither having complex multiplication.
For any "good" prime ideal $\mathfrak{p}$ of K the local L-factor is given by

$$1-a_{\mathfrak{p}}(E_j)T+\mathrm{Norm}(\mathfrak{p})T^2=(1-\mathrm{Norm}(\mathfrak{p})^{1/2}e^{i\theta_{j,\mathfrak{p}}}T)(1-\mathrm{Norm}(\mathfrak{p})^{1/2}e^{-i\theta_{j,\mathfrak{p}}}T).$$

Frobenius angle:

$$\theta_{j,\mathfrak{p}}=\theta_{\mathfrak{p}}(E_j)\in[0,\pi]$$

Trace of Frobenius:

$$a_{\mathfrak{p}}(E_j)=a_{j,\mathfrak{p}}=2\,\mathrm{Norm}(\mathfrak{p})^{1/2}\cos\theta_{\mathfrak{p}}(E_j)$$

Motivation

The isogeny theorem of Faltings (1983) implies that there exists a prime ideal $\mathfrak{p}$ of K at which E_1, E_2 both have good reduction and have distinct Frobenius traces.

Goal

Find an upper bound for the norm of this $\mathfrak{p}$ in terms of invariants of K and the two elliptic curves.

Strategy

One idea: for any fixed prime ℓ, there exists a prime ideal $\mathfrak{p}$ of K at which the Frobenius traces of E_1, E_2 differ modulo ℓ.

Assuming the generalized Riemann hypothesis for Artin L-functions, one can use the effective form of the Chebotarev density theorem (as suggested by Serre in 1981) to show the least norm of such a prime ideal is

$$O((\log N)^2 (\log\log 2N)^b) \quad b \geq 0.$$

Assuming the generalized Riemann hypothesis for L-functions of the form $L(s, \mathrm{Sym}^m E_1 \otimes \mathrm{Sym}^n E_2)$, we use the effective form of the generalized Sato–Tate conjecture for the abelian surface $E_1 \times_K E_2$ to obtain a similar bound for the least norm of a prime ideal at which the Frobenius traces of E_1, E_2 have opposite sign.

Serre:	$b = 12$
B-Kedlaya:	$b = 2$

Related literature

Although we will not do so here, we mention that the framework of the generalized Sato–Tate conjecture includes many additional questions about distinguishing L-functions, a number of which have been considered previously.

For instance, Goldfeld and Hoffstein (1993) established an upper bound on the first distinguishing coefficient for a pair of holomorphic Hecke newforms, by an argument similar to ours but with a milder analytic hypothesis (the Riemann hypothesis for the Rankin-Selberg convolutions of the two forms with themselves and each other).

Sengupta (2004) carried out the analogous analysis with the Fourier coefficients replaced by normalized Hecke eigenvalues (this only makes a difference when the weights are distinct).

The analogue of Serre's argument for modular forms was given by Ram Murty (1997) and subsequently extended to Siegel modular forms by Ghitza (2011) for Fourier coefficients and Ghitza and Sayer (2014) for Hecke eigenvalues.

Our setup

Fix two number fields K, L.
Let $\mathcal{M}$ be a pure motive of weight w over K with coefficients in L.
For each prime ideal $\mathfrak{p}$ of K, let $G_\mathfrak{p}$ be a decomposition subgroup of $\mathfrak{p}$ inside the absolute Galois group G_K, let $I_\mathfrak{p}$ be the inertia subgroup of $G_\mathfrak{p}$, and let $\mathrm{Frob}_\mathfrak{p} \in G_\mathfrak{p}/I_\mathfrak{p}$ be a Frobenius element.

The *Euler factor* of $\mathcal{M}$ at $\mathfrak{p}$ (for the automorphic normalization) is the function

$$L_\mathfrak{p}(s, \mathcal{M}) = \det(1 - \mathrm{Norm}(\mathfrak{p})^{-s-w/2}\,\mathrm{Frob}_\mathfrak{p}, V_v(\mathcal{M})^{I_\mathfrak{p}} \otimes_{L_v} \mathbb{C})^{-1}$$

for v a finite place of L equipped with an embedding $L_v \hookrightarrow \mathbb{C}$ and $V_v(\mathcal{M})$ the v-adic étale realization of $\mathcal{M}$ equipped with its action of $G_\mathfrak{p}$.
It is clear that this definition does not depend on the choice of $G_\mathfrak{p}$; it is conjectured also not to depend on v or the embedding $L_v \hookrightarrow \mathbb{C}$, and this is known when $\mathcal{M}$ has good reduction at $\mathfrak{p}$ (which excludes only finitely many primes).

The ordinary L-function of $\mathcal{M}$ is the the Euler product

$$L(s,\mathcal{M}) = \prod_{\mathfrak{p}} L_{\mathfrak{p}}(s,\mathcal{M}).$$

For each infinite place ∞ of K, there is also an archimedean Euler factor defined as follows. Put

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2), \qquad \Gamma_{\mathbb{C}}(s) = 2^{-s}\pi^{-s}\Gamma(s).$$

Form the Betti realization of $\mathcal{M}$ at ∞ and the spaces $H^{p,q}$ for $p+q=w$, and put $h^{p,q} = \dim H^{p,q}$. Note that complex conjugation takes $H^{p,q}$ to $H^{q,p}$ and thus acts on $H^{w/2,w/2}$; let h^+ and h^- be the dimensions of the positive and negative eigenspaces (both taken to be 0 if w is odd). Then put

$$L_\infty(s,\mathcal{M}) = \Gamma_{\mathbb{R}}(s)^{h^+}\Gamma_{\mathbb{R}}(s+1)^{h^-} \prod_{p+q=w, p<q} \Gamma_{\mathbb{C}}(s+w/2-p)^{h^{p,q}}.$$

The completed L-function is then defined as

$$\Lambda(s,\mathcal{M}) = N^{s/2} L(s,\mathcal{M}) \prod_{\infty} L_\infty(s,\mathcal{M}),$$

GRH in our case

Conjecture 1

Fix two number fields K, L. Let $\mathcal{M}$ be a pure motive of weight w over K with coefficients in L. Let d be the dimension of the fixed subspace of the motivic Galois group of $\mathcal{M}(-w/2)$ (taken to be 0 if w is odd).

(a) *The function $s^d(1-s)^d\Lambda(s,\mathcal{M})$ (which is defined a priori for $\mathrm{Re}(s) > 1$) extends to an entire function on $\mathbb{C}$ of order 1 which does not vanish at $s = 0, 1$. (Recall that an entire function $f : \mathbb{C} \to \mathbb{C}$ is of order 1 if $f(z)e^{-\mu|z|}$ is bounded for each $\mu > 1$.)*

(b) *Let $\mathcal{M}^*$ denote the Cartier dual of $\mathcal{M}$. Then there exists $\epsilon \in \mathbb{C}$ with $|\epsilon| = 1$ such that $\Lambda(1-s,\mathcal{M}) = \epsilon\Lambda(s,\mathcal{M}^*)$ for all $s \in \mathbb{C}$.*

(c) *The zeroes of $\Lambda(s,\mathcal{M})$ all lie on the line $\mathrm{Re}(s) = 1/2$.*

The case of one elliptic curve

For E an elliptic curve over a number field K
$\mathfrak{p}$ a prime ideal of K at which E has good reduction
$a_{\mathfrak{p}} = a_{\mathfrak{p}}(E)$ the Frobenius trace of E at $\mathfrak{p}$, so that $\mathrm{Norm}(\mathfrak{p}) + 1 - a_{\mathfrak{p}}$ is the number of rational points on the reduction of E modulo $\mathfrak{p}$.
Recall: Frobenius angle $\theta_{\mathfrak{p}} = \theta_{\mathfrak{p}}(E) \in [0, \pi]$ such that

$$1 - a_{\mathfrak{p}}(E)T + \mathrm{Norm}(\mathfrak{p})T^2 = (1 - \mathrm{Norm}(\mathfrak{p})^{1/2}e^{i\theta}T)(1 - \mathrm{Norm}(\mathfrak{p})^{1/2}e^{-i\theta}T).$$

Let μ_{ST} denote the Sato–Tate measure, so that

$$\mu_{\mathsf{ST}}(f) = \int_0^\pi \frac{2}{\pi}\sin^2\theta f(\theta)\,d\theta.$$

For I an interval, let δ_I denote the characteristic function.

Theorem 1 (after Murty)

Let E be an elliptic curve over a number field K without complex multiplication. Let N denote the absolute conductor of E. Assume that $L(s, \mathrm{Sym}^k E)$ satisfies Conjecture 1 for all $k \geq 0$. Then for any closed subinterval I of $[0, \pi]$,

$$\sum_{\mathrm{Norm}(\mathfrak{p}) \leq x, \mathfrak{p} \nmid N} \delta_I(\theta_\mathfrak{p}) = \mu_{\mathrm{ST}}(I)\,\mathrm{Li}(x) + O([K:\mathbb{Q}]^{1/2} x^{3/4} (\log(Nx))^{1/2}).$$

The weaker statement that

$$\sum_{\mathrm{Norm}(\mathfrak{p}) \leq x, \mathfrak{p} \nmid N} \delta_I(\theta_\mathfrak{p}) \sim \mu_{\mathrm{ST}}(I)\,\mathrm{Li}(x)$$

is the Sato–Tate conjecture.

Proof of Theorem 1

- Note that the number of primes dividing N (which includes all primes of bad reduction) is $O(\log N)$, which is subsumed by our error term.
- Since E has no complex multiplication, its Sato–Tate group is SU(2).
- Any function of the Frobenius angles will be a function on the conjugacy classes of the Sato–Tate group of E.
- By the Peter-Weyl theorem, any such function has an expansion as

$$F = \sum_{\chi} \mu(F\overline{\chi})\chi \tag{1}$$

where the sum runs over irreducible characters χ of the Sato–Tate group.

- One can obtain information about the average behavior of $\chi(\mathfrak{p})$ by computing a suitable contour integral of the logarithmic derivative of its L-function $L(s,\chi)$, namely

$$\sum_{\mathrm{Norm}(\mathfrak{p})\le x} \chi(\mathfrak{p}) \log \mathrm{Norm}(\mathfrak{p}) = \mu(\chi)x + O(d_\chi x^{1/2} \log x \log(N(x+d_\chi))).$$

  where $d_\chi = \dim(\chi)[K:\mathbb{Q}]$.
- Using Abel partial summation, it then follows that

$$\sum_{\mathrm{Norm}(\mathfrak{p})\le x} \chi(\mathfrak{p}) = \mu(\chi)\,\mathrm{Li}(x) + O(d_\chi x^{1/2} \log(N(x+d_\chi))). \qquad (2)$$

- The irreducible characters of SU(2) are

$$\chi_k(\theta) = \sum_{j=0}^{k} e^{(k-2j)i\theta} \qquad (k = 0, 1, \ldots).$$

The secret sauce: Fourier analysis

Note that expanding F in terms of the χ_k amounts to ordinary Fourier analysis.

Basic idea: introduce a family of functions F for which we have control over the coefficients appearing in (1), which we will use to approximate the characteristic function δ_I.

For that, we will formally extend F to an even function on $[-\pi, \pi]$ and avail ourselves of a construction of Vinogradov.

Vinogradov's Lemma

Lemma

Let r be a positive integer, and let A, B, Δ be real numbers satisfying

$$0 < \Delta < \frac{1}{2}, \qquad \Delta \leq B - A \leq 1 - \Delta.$$

Then there exists a continuous periodic function $D_{A,B} = D : \mathbb{R} \to \mathbb{R}$ with period 1 that satisfies the following conditions.

- *For $A + \frac{1}{2}\Delta \leq x \leq B - \frac{1}{2}\Delta$, $D(x) = 1$.*
- *For $B + \frac{1}{2}\Delta \leq x \leq 1 + A - \frac{1}{2}\Delta$, $D(x) = 0$.*
- *For x in the remainder of the interval $\left[A - \frac{1}{2}\Delta, 1 + A - \frac{1}{2}\Delta\right]$, $0 \leq D(x) \leq 1$.*

Vinogradov's Lemma

Lemma (cont.)

- *$D(x)$ has a Fourier series expansion of the form*

$$D(x) = \sum_{m \geq 0} (a_m \cos(2m\pi x) + b_m \sin(2m\pi x))$$

in which $a_0 = B - A$ and for all $m \geq 1$,

$$|a_m|, |b_m| \leq \min \left\{ 2(B-A), \frac{2}{\pi m}, \frac{2}{\pi m} \left(\frac{r}{\pi m \Delta} \right)^r \right\}. \tag{3}$$

Back to the proof

Leaving the choices of A, B, Δ, r unspecified for the moment, let us define D as in Lemma 19, then define the function $F_{A,B} : \mathbb{R} \to \mathbb{R}$ by
$F_{A,B}(\theta) = D\left(\frac{\theta}{2\pi}\right) + D\left(-\frac{\theta}{2\pi}\right)$.
Its Fourier series has the form

$$F_{A,B}(\theta) = \sum_{m \in \mathbb{Z}} c_{m,A,B} e^{im\theta}, \tag{4}$$

where

$$c_{0,A,B} = 2a_0 = 2(B - A)$$

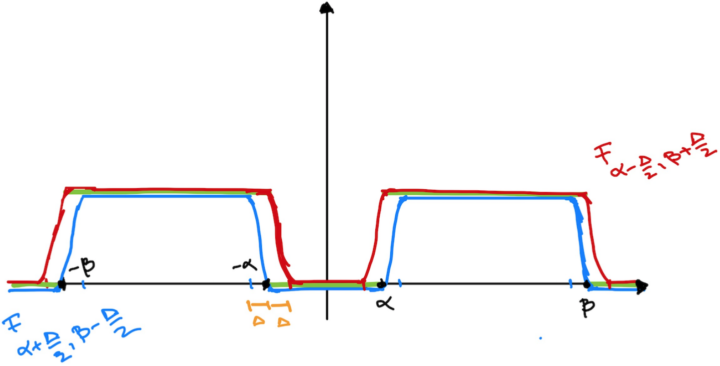
and

$$c_{m,A,B} = c_{-m,A,B} = a_m \text{ for all } m \geq 1.$$

Summing over Frobenius angles we get

$$\sum_{\mathrm{Norm}(\mathfrak{p})\le x,\mathfrak{p}\nmid N} F_{A,B}(\theta_{\mathfrak{p}}) = (c_{0,A,B} - c_{2,A,B})\,\mathrm{Li}(x) + O\left(\frac{[K:\mathbb{Q}]x^{1/2}\log(N(x+M))\log M}{\Delta}\right) + O\left(\frac{x}{M\Delta\log x}\right). \tag{5}$$

The characteristic function of the interval $I = [2\pi\alpha, 2\pi\beta]$ is bounded from above by $F_{\alpha-\Delta/2,\beta+\Delta/2}$ and from below by $F_{\alpha+\Delta/2,\beta-\Delta/2}$.



On the other hand, the quantities $c_{0,\alpha-\Delta/2,\beta+\Delta/2} - c_{2,\alpha-\Delta/2,\beta+\Delta/2}$ and $c_{0,\alpha+\Delta/2,\beta-\Delta/2} - c_{2,\alpha+\Delta/2,\beta-\Delta/2}$ each differ from $\mu_{ST}(I)$ by $O(\Delta)$.

We obtain the theorem by balancing the error terms in (5) with each other and with $O(\Delta \operatorname{Li}(x))$ by setting

$$\Delta = x^{-1/4}[K:\mathbb{Q}]^{1/2}(\log x)(\log(Nx))^{1/2}, \qquad M = \lceil \Delta^{-2} \rceil.$$

Namely, we obtain

$$\sum_{\mathrm{Norm}(\mathfrak{p})\leq x, \mathfrak{p}\nmid N} \delta_I(\theta_\mathfrak{p}) = \mu_{\mathrm{ST}}(I)\operatorname{Li}(x) + O([K:\mathbb{Q}]^{1/2}x^{3/4}(\log(Nx))^{1/2}).$$

Theorem 2 (B-Kedlaya)

Let E_1, E_2 be two $\overline{\mathbb{Q}}$-nonisogenous elliptic curves over a number field K, neither having complex multiplication. Let N be the product of the absolute conductors of E_1 and E_2. For each prime ideal $\mathfrak{p}$ of K not dividing N, let $\theta_{1,\mathfrak{p}}, \theta_{2,\mathfrak{p}}$ be the Frobenius angles of E_1, E_2 at $\mathfrak{p}$. Assume that the L-functions $L(s, \mathrm{Sym}^i E_1 \otimes \mathrm{Sym}^j E_2)$ for $i, j = 0, 1, \dots$ all satisfy Conjecture 1. Then there exists a prime ideal $\mathfrak{p}$ not dividing N with

$$\mathrm{Norm}(\mathfrak{p}) = O([K:\mathbb{Q}]^2 (\log N)^2 (\log\log 2N)^2)$$

such that $a_\mathfrak{p}(E_1)$ and $a_\mathfrak{p}(E_2)$ are nonzero and of opposite sign.

Note: we have to go back and redo the Fourier analysis, except that now we take $r = 2$ in Vinogradov's Lemma and optimize again.

Setup for abelian varieties: B–Fité–Kedlaya

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

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

For a prime $\mathfrak{p}$ of K not dividing $N\ell$, denote by

- $a_\mathfrak{p} := a_\mathfrak{p}(A) := \mathrm{Trace}(\varrho_{A,\ell}(\mathrm{Frob}_\mathfrak{p}))$ the Frobenius trace at $\mathfrak{p}$.
- $\overline{a}_\mathfrak{p} := \dfrac{a_\mathfrak{p}}{\mathrm{Norm}(\mathfrak{p})^{1/2}} \in [-2g, 2g]$ the normalized Frobenius trace at $\mathfrak{p}$.

Sato-Tate group and Sato-Tate measure

- From now on, we will assume the following conjecture.

Conjecture 2 (Banaszak-Kedlaya)

Denote by G_ℓ the Zariski closure of the image of $\varrho_{A,\ell}$ in $\mathrm{GSp}_{2g}/\mathbb{Q}_\ell$. Then there exists an algebraic subgroup G of $\mathrm{GSp}_{2g}/\mathbb{Q}$ such that

$$G_\ell = G \times_{\mathbb{Q}} \mathbb{Q}_\ell \,.$$

- Known in many cases: it is implied by the Mumford–Tate conjecture.
- The *Sato–Tate group* of A, denoted $\mathrm{ST}(A)$, is a maximal compact subgroup of $(G \cap \mathrm{Sp}_{2g})(\mathbb{C})$. It is thus a subgroup of $\mathrm{USp}(2g)$.
- Let μ denote the push forward of the Haar measure of $\mathrm{ST}(A)$ via

$$\mathrm{Trace}\colon\ \mathrm{ST}(A) \to [-2g, 2g] \,.$$

We call μ the *Sato–Tate measure* of A.

The Sato-Tate conjecture

Sato-Tate conjecture for abelian varieties

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

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

Equivalently,

$$\sum_{\mathrm{Norm}(\mathfrak{p})\leq x} \delta_I(\overline{a}_{\mathfrak{p}}) = \mu(I)\,\mathrm{Li}(x) + o\left(\frac{x}{\log(x)}\right)\,.$$

The effective Sato–Tate conjecture

Effective Sato-Tate conjecture for abelian varieties

There exists $\varepsilon > 0$ depending exclusively on $\mathrm{ST}(A)$ (and therefore, in fact, only on g) such that, for every subinterval I of $[-2g, 2g]$, we have

$$\sum_{\mathrm{Norm}(\mathfrak{p}) \leq x} \delta_I(\overline{a}_{\mathfrak{p}}) = \mu(I)\,\mathrm{Li}(x) + O(x^{1-\varepsilon}) \qquad \text{for } x \gg_I 0\,,$$

where the implicit constant in the O-notation depends exclusively on the field K, the dimension g, and the absolute conductor N.

The Sato–Tate conjecture and L-functions

- To every irreducible representation Γ of $\mathrm{ST}(A)$, one attaches *à la Artin* an Euler product:

$$L(\Gamma, s) := \prod_{\mathfrak{p}} L_{\mathfrak{p}}(\Gamma, \mathrm{Norm}(\mathfrak{p})^{-s})^{-1},$$

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

Theorem 3 (Serre '68)

Suppose that $L(\Gamma, s)$ extends to a holomorphic function on an open neighborhood of $\mathrm{Re}(s) \geq 1$ and that does not vanish at $\mathrm{Re}(s) = 1$ for every irreducible nontrivial representation Γ of $\mathrm{ST}(A)$.
Then the Sato–Tate conjecture holds for A.

Main result

Theorem 4 (B–Fité–Kedlaya)

Suppose that $\mathrm{ST}(A)$ *is connected and that* $\Lambda(\Gamma, s)$ *satisfies Conjecture 1 for every irreducible representation* Γ *of* $\mathrm{ST}(A)$. *Set*

$$\varepsilon := \frac{1}{2(q+\varphi)},$$

where q *denotes the rank of the Lie algebra of* $\mathrm{ST}(A)$ *and* φ *denotes the number of positive roots of its semisimple part. Then, for every subinterval* I *of* $[-2g, 2g]$, *we have*

$$\sum_{\mathrm{Norm}(\mathfrak{p})\le x} \delta_I(\overline{a}_{\mathfrak{p}}) = \mu(I)\,\mathrm{Li}(x) + O\left(\frac{x^{1-\varepsilon}(\log(Nx))^{2\varepsilon}}{\log(x)^{1-4\varepsilon}}\right) \qquad \text{for } x \gg_I 0\,,$$

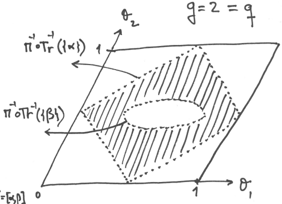
where the implicit constant in the O*-notation depends exclusively on* K *and* g.

Ingredients in the proof

- Vinogradov's function

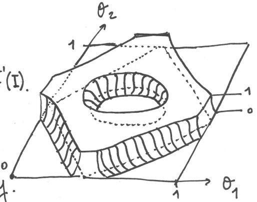
We construct a function :

$$\begin{tikzcd} \mathbb{R}^q \arrow[rr, "F_I"] \arrow[dr, "\pi"'] & & {[0,1]} \\ & {[0,1]^q} \simeq \mathrm{Conj}(ST(A)) \arrow[ur] \arrow[d, "\mathrm{Tr}"] & \\ & {[-2g,2g]} \supseteq I=[\alpha,\beta] & \end{tikzcd}$$



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.



(courtesy of Francesc Fité)

- By construction

$$\sum_{\mathrm{Norm}(\mathfrak{p})\le x} \delta_I(\overline{a}_{\mathfrak{p}}) \approx \sum_{\mathrm{Norm}(\mathfrak{p})\le x} F_I(\mathrm{Frob}_{\mathfrak{p}})\,.$$

- Write $F_I = \sum_\chi c_\chi \chi$. The c_χ are still of rapid decay and $c_1 \approx \mu(I)$.
- Then

$$\sum_{\mathrm{Norm}(\mathfrak{p})\le x} \delta_I(\overline{a}_{\mathfrak{p}}) \approx \mu(I)\,\mathrm{Li}(x) + \sum_{\chi\neq 1} c_\chi \sum_{\mathrm{Norm}(\mathfrak{p})\le x} \chi(\mathrm{Frob}_{\mathfrak{p}})\,.$$

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

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

- 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 every subinterval I of $[-2g, 2g]$, there exists a prime $\mathfrak{p}$ not dividing N such that $\overline{a}_{\mathfrak{p}} \in I$ and

$$\mathrm{Norm}(\mathfrak{p}) = O(\nu(\min\{|I|, \mu(I)\}) \cdot \log(2N)^2 \cdot \log(\log(4N))^4)\,.$$

The implicit constant in the O-notation depends exclusively on K and g, and $\nu : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ is defined by

$$\nu(z) := \max\left\{1, \frac{\log(z)^6}{z^{1/\varepsilon}}\right\}\,.$$

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

Conjecture 3

If $\mathrm{Hom}(A, A') = 0$*, then there exists* $\mathfrak{p} \nmid NN'$ *such that* $a_{\mathfrak{p}}(A) \cdot a_{\mathfrak{p}}(A') < 0$*.*

Corollary 2

Let A, A' be abelian varieties such that $\mathrm{ST}(A)$, $\mathrm{ST}(A')$ are connected, and

$$\mathrm{ST}(A \times A') \simeq \mathrm{ST}(A) \times \mathrm{ST}(A') \,. \tag{6}$$

Assume that GRH (Conjecture 1) for $\Lambda(\Gamma \otimes \Gamma', s)$ holds for all irreducible rep. Γ, Γ' of A and A' respectively. Then, there exists $\mathfrak{p} \nmid NN'$ such that $a_{\mathfrak{p}}(A) \cdot a_{\mathfrak{p}}(A') < 0$ and

$$\mathrm{Norm}(\mathfrak{p}) = O(\log(2NN')^2 \log(\log(4NN'))^6) \,. \tag{7}$$

- Using the Bach kernel integration, we can
  - replace (6) with the weaker condition $\mathrm{Hom}(A, A') = 0$.
  - improve (7) to $O(\log(2NN')^2)$.

Frobenius traces attaining the Weil bound

- Let E be an elliptic curve with CM (defined over K).
- Consider the set of "record primes"

$$R(x) = \{\mathfrak{p};\ \mathrm{Norm}(\mathfrak{p}) \leq x \text{ and } a_{\mathfrak{p}} = \lfloor 2\sqrt{\mathrm{Norm}(\mathfrak{p})} \rfloor\}.$$

- Serre has conjectured

$$\#R(x) \sim \frac{4}{3\pi} \frac{x^{3/4}}{\log(x)} \qquad \text{as } x \to \infty.$$

Corollary 3

Suppose that GRH holds for the Hecke L-function attached to any integral power of the Hecke character of E. Then

$$\#R(x) \asymp \frac{x^{3/4}}{\log(x)} \qquad \text{for } x \gg 0\,.$$

This recovers a weaker version of a theorem of James–Pollack (2017), which asserts (unconditionally) that

$$\#R(x) \sim \frac{4}{3\pi}\frac{x^{3/4}}{\log(x)}.$$

A different result in a similar spirit, concerning numbers of points on diagonal curves, is due to Duke (1989).