Sato-Tate Conjecture

Yasutaka Ihara

(The third version *plus*;sumitted 2019/10/16,revised 2021/04/17)

1 Sato and Namba

In 1962, Mikio Sato came back to Tokyo from the Institute for Advanced Study, Princeton. He had then a strong interest also in the following question. Let E be an elliptic curve over the rational number field $\mathbb{Q}$ and N be its conductor. So, at each prime $p \nmid N$, E has a good reduction $E \bmod p$ and the numerator of its congruence zeta function has, due to H. Hasse, the following form:

$$1 - a_p u + pu^2 = (1 - p^{\frac{1}{2}} e^{i\theta_p} u)(1 - p^{\frac{1}{2}} e^{-i\theta_p} u), \tag{1}$$

with $0 \le \theta_p \le \pi$. Now let p run over all primes $p \nmid N$. Disregarding the (easier) exceptional case where E has CM (complex multiplications), his question was:

"*How is θ_p distributed on $[0, \pi]$ as p runs over all primes $\nmid N$?*"

He was interested in this, and closely related questions associated to modular cusp forms ("normalized eigenforms" with $\mathbb{Q}$-rational Fourier coefficients). He wished to use computers to obtain some convincing insight. He came back as a faculty member of Tokyo University of Education, where a computer, HIPAC 103, was newly installed and where several young members and students started working or "playing" with it. Among them was a (Master's course) graduate student, Kanji Namba. As Namba describes in [Nmb](a)(c) vividly, on their way home together on a nice summer evening, Sato and some of his colleagues including Namba, instead of parting at the Ikebukuro suburban train terminal, were drawn to a roof beer garden on a department store. Then, Sato, explaining the beauty of arithmetic of elliptic curves and modular forms, said to Namba something like "why not use the new computer for something more worthwhile than examining the Goldbach conjecture; for example, for collecting data for this question". Thus started down-to-earth activity on this question.

The first suggested set of examples included the elliptic curve defined by the equation $y^2 = x(x^2 + x - 1)$. The conductor $N = 20$, and its L-function outside $p = 2, 5$ is

$$\prod_{p \neq 2,5} (1 - a_p p^{-s} + p^{1-2s})^{-1}, \qquad a_p = p^{\frac{1}{2}}(e^{i\theta_p} + e^{-i\theta_p}),$$

with the a_p's determined by

$$(\eta(\tau)\eta(5\tau))^2 = \sum_{\substack{n\geq 1 \\ \text{odd}}} a_n q^{\frac{n}{2}},$$

$\eta(\tau)$ being the Dedekind η function

$$\eta(\tau) = q^{1/24} \prod_{m\geq 1} (1 - q^m) \qquad (q = e^{2\pi i\tau}).$$

Incidentally, the Euler factor at $p = 2$ is 1 (additive reduction), and at $p = 5$ is $(1 + 5^{-s})^{-1}$ (non-split multiplicative reduction). Namba managed to use the "infant computer for common use" at that time to obtain the values of a_p for all $p < 14000$. Then Sato asked T. Nagashima (a research associate and a senior colleague of Namba's) for the computations of "θ_p" using Namba's data for "a_p". Meanwhile, Sato moved to Osaka University (Spring 1963). In a letter to Namba from Osaka (May 13, 1963), Sato wrote [1]

"The hypothesis, that $\{\theta_p\}$ has the distribution density (at θ) proportional to $\sin^2\theta$, seems highly probable".

Computations for some other cases, including non-CM $E/\mathbb{Q}$, some modular forms of weight > 2, and hyperelliptic curves $/\mathbb{Q}$, had also been carried out by Namba and others [Nmb](b), but no explicit conjectures seem to have been raised outside non-CM elliptic curves.

2 Tate

The main reference is [Tate], but see also [Ser], [Yam]. The key sentence is [Tate] p 107:

"I understand that M. Sato has found this $\sin^2$ *distribution law experimentally with machine computations. Conjecture* 2 *seems to offer (a partial[2]) explanation for it!"*

It would be too complicated to formulate his Conjecture 2 itself here. So, following Serre [Ser], I state here a special case of Tate's conjecture for non-CM elliptic curves E over $\mathbb{Q}$.

Let

$$L^1(E,s) = \prod_{p\nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

[1] A copy of this letter is pasted on [Nmb](a). On reading this note, one learns how difficult it was to use the old computer of the time, and also how Namba and his colleagues in a sense enjoyed managing it. On reading the pasted letters from Sato, one gets an impression that Sato was so busy with his impending duties as Professor that he thought it not the time for serious "brain-works".

[2] according to his next paragraph.

be the partial L-function of E. For each such $p \nmid N$, put

$$1 - a_p u + p u^2 = (1 - \alpha_p u)(1 - \overline{\alpha}_p u) \qquad (u : \text{a variable},\ \alpha_p \overline{\alpha}_p = p),$$

with $\alpha_p = p^{\frac{1}{2}} e^{i\theta_p}$, $0 \le \theta_p \le \pi$. For each integer $m \ge 1$, consider the new L-function

$$L^1_m(E, s) = \prod_{p \nmid N} \prod_{a=0}^{m} (1 - \alpha_p^{m-a} \overline{\alpha}_p^a p^{-s})^{-1}.$$

This infinite product converges absolutely on $\mathcal{R}e(s) > \frac{m}{2} + 1$; hence it is holomorphic and non-zero there.

Conjecture. [Tate] $L^1_m(E, s)$ is holomorphic and $\neq 0$ on $\mathcal{R}e(s) \ge 1 + \frac{m}{2}$ for any $m \ge 1$.

Since Sato's conjecture on the $\sin^2 \theta$ distribution of $\{\theta_p\}$ is equivalent with that $L^1_m(E, s)$ is holomorphic and $\neq 0$ at $s = 1 + \frac{m}{2}$ for any $m \ge 1$, the validity of the above Conjecture will imply Sato's conjecture. This equivalence is obtained by easy Fourier analysis ("easy", after H. Weyl) cf. [Ser].

In his Master's thesis at Osaka University (1966 February), Y. Yamamoto [Yam] also described this relation, probably under the influence of Sato without yet knowing Tate's work.

3 The proof, by Taylor, Clozel, Harris, Shepherd-Barron et al.

(A) The Sato–Tate conjecture was proved for non-CM elliptic curves E over any totally real field F, and also for some wide class of elliptic modular cusp forms of weight > 2 that are "non-CM".

First, in [!3], a proof of the conjecture is given under an additional condition: E has multiplicative reduction, i.e., $\mathrm{ord}_v N = 1$ for some $v \mid N$ (which is satisfied by Sato's first example cited above where $N = 20, v = p = 5$). This proof stands on the previous pair of papers [!1],[!2].

Then, in [!4], the conjecture is proved unconditionally, based on *cit.loc.* and on other results mentioned in its Introduction. Notable also is that [!4] extends the results to elliptic modular forms of weight > 2.

As for the names of coauthors of these four papers, besides those in the section-title, T. Barnet-Lamb and D. Geraghty are among the coauthors of [!4], and the name R. Taylor, alone, appears as a (co-) author in all the four.

First, let me reproduce the *abstract* of the paper [!4].

> *"We prove new potential modularity theorems for n-dimensional essentially self-dual ℓ-adic representations of the absolute Galois group of a totally real field. Most notably, in the ordinary case we prove quite a general result. Our results suffice to show that all the symmetric powers of any non-CM, holomorphic, cuspidal, elliptic modular new form of weight greater than one are potentially cuspidal automorphic. This in turn proves the Sato-Tate conjecture for such*

forms. (In passing we also note that the Sato-Tate conjecture can now be proved for any elliptic curve over a totally real field.)"

These papers in fact do prove new significant cases of the global Langlands duality over number fields, i.e., the duality between

$(\mathrm{i})_n$ automorphic representations of a certain type, RAESDC *on* GL_n over totally real number fields, *and*

$(\mathrm{ii})_n$ (ℓ-adic) Galois representations *into* GL_n satisfying certain good properties.

Given an automorphic representation for $(\mathrm{i})_2$, with the Langlands dual $(\mathrm{ii})_2$, it is expected that the symmetric power $\otimes m$ of the latter, which belongs to $(\mathrm{ii})_n$ for $n = m+1$, also has a dual automorphic representation in $(\mathrm{i})_{m+1}$. In [!4], the authors prove more generally that any element of $(\mathrm{ii})_n$ possessing some good properties at each place $v \mid (\infty\ell)$ has, potentially, its dual in $(\mathrm{i})_n$ (Theorem A), and in particular, prove (Theorem B) a "potential modularity" for such $\otimes m$ of $(\mathrm{ii})_2$ that arises from $(\mathrm{i})_2$ (over $\mathbb{Q}$).

This focuses attention of a wider mathematical public, to the following general question as to whether the tensor product *operation* on the (ii)-side *itself* has a natural Langlands dual on the (i)-side.

(*Added in proof*) In February 2021, at the proof-reading stage, I asked R. Taylor whether there appeared a more general solution to this question and obtained a very kind and detailed explanation as to what are known or unknown. Here, I add only that no sufficiently general solutions are publicized.

(B) The Sato–Tate conjecture is proved in [!4] in Tate's form:

Cor 0.1. Suppose that F is a totally real number field, that E/F is an elliptic curve and that $m \in \mathbb{Z}_{>0}$. The L-function $L(\mathrm{Symm}^m E, s)$ has meromorphic continuation to $\mathbb{C}$ and satisfies the expected functional equation relating the values at s and $m+1-s$. If E is not CM then $L(\mathrm{Symm}^m E, s)$ is holomorphic and non-zero [3] in $\mathcal{R}e(s) \geq 1 + m/2$.

The v-factor in the Euler product of $L(\mathrm{Symm}^m E, s)$ is equal to that of $L^1_m(E, s)$ above (replace p by v and p^{-s} by $N(v)^{-s}$). In Sato's form, see Cor 8.9 which is (equivalently) stated as the equidistribution of $\cos\theta_v$ in $[-1, 1]$.

(C) For similar results on modular cusp forms of weight not necessarily equal to 2, see Cor 8.4, 8.5 of [!4], among which is:

Cor 0.2. Write $\sum_{n=1}^{\infty} \tau(n) q^n = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$, i.e., $\tau(n)$ denotes Ramanujan's τ-function. Then the numbers $\tau(p)/(2p^{11/2})$ are equidistributed in $[-1, 1]$ with respect to the measure $(2/\pi)\sqrt{1 - t^2}dt$.

[3] I was informed that Thorne and Newton have recently proved its holomorphy on the whole complex plane when $F = \mathrm{Q}$.

In fact, this modular form satisfies the condition corresponding to being non-CM.

(D) Monuments stand above past great works, and in this case, not to be forgotten include the following works of Taniyama and of Shimura.

(1) The duality was first recognized and established by Y. Taniyama [Tan] for $n = 1$.

(2) The proofs in [!4] still needed Shimura varieties as parts of logical basis; i.e., for some construction from (i) $\to$ (ii), for some compatibility, as well as for the proof of the local Langlands conjecture.

Reading the manuscript version of [!4] and enjoying the beauty of their use of Calabi-Yau varieties, I became curious to know whether the use of Calabi-Yau varieties completely replaced that of Shimura varieties. So I asked R. Taylor whether there still remained some logical dependences on Shimura varieties, and on this occasion also, obtained a very prompt and helpful reply (March, 2010) upon which the above remark (2) depends.

References

[Nmb] K. Namba (in Japanese),

(a) Dedekind η-function and Sato's $\sin^2$-Conjecture. 難波完爾　津田塾大学数学，計算機科学研究所報 27，第 16 回数学史シンポジウム (2005), pp.95–149.

(b) Hyperelliptic curves of genus 2 and the $\sin^2$-Conjecture. 難波完爾　津田塾大学数学，計算機科学研究所報 28，第 17 回数学史シンポジウム (2006), pp.101–174.

(c) On Sato's $\sin^2$-Conjecture. 難波完爾　佐藤 $\sin^2$–予想の話,「佐藤幹夫の数学 [増補版]」木村達雄編，日本評論社 (2007) pp.344–367.

[Ser] J-P. Serre, "Abelian ℓ-adic representations and elliptic curves" (esp. I-Appendix); Benjamin (1968).

[Tan] Y. Taniyama, "L-functions of number fields and zeta functions of abelian varieties", J. Math. Soc. Japan 9 (1957), 330–366.

[Tate] J. Tate, "Algebraic cycles and poles of zeta functions" (esp. §4), Proc. Purdue Univ. Conf. 1963, pp. 93–110, New York (1965).

[Yam] Y. Yamamoto, "On Sato's conjecture", Master's thesis, Osaka Univ. (Feb., 1966).

[!1] L. Clozel, M. Harris and R. Taylor, "Automorphy for some ℓ-adic lifts of automorphic mod ℓ Galois representations", Publ. Math. IHES 108 (2008), 1–181.

[!2] R. Taylor, "Automorphy for some ℓ-adic lifts of automorphic mod ℓ representations II" , ibid. 183–239.

[!3] M. Harris, N. Shepherd-Barron and R. Taylor, "A family of Calabi-Yau varieties and potential automorphy", Ann. of Math. 171 (2010), 779–813.

[!4] T. Barnet-Lamb, D. Geraghty, M. Harris and R. Taylor, "A family of Calabi-Yau varieties and potential automorphy II", Publ. RIMS, Kyoto Univ. 47(2011), 29–98.