Some Remarks on Automorphy and the Sato-Tate Conjecture

M. Ram Murty and V. Kumar Murty

Abstract We present an informal account of the evolution of the Sato-Tate conjecture and describe some recent work of the authors that it gave rise to.

1 The Conjecture

Let E be an elliptic curve defined over the rationals of conductor N. For any prime p not dividing N, we may consider the number of points N_p on the reduction of E mod p. Following Hasse, we have the inequality

$$|N_p - (p+1)| \le 2\sqrt{p}.$$

Thus, we may write the integer

$$a_p = N_p - (p+1)$$

as

$$a_p = 2\sqrt{p}\cos(\theta_p),\ 0 \le \theta_p \le \pi.$$

The Sato-Tate conjecture describes the distribution of the "angles of Frobenius" θ_p as p varies. if E has complex multiplication, one expects that the angles are essentially equidistributed (after one takes into account the fact that for half the primes, namely those that do not split in the field of multiplication, $\theta_p = \pi/2$). If E does not have complex multiplication, then the Sato-Tate conjecture predicts a skewed distribution, namely

M.R. Murty
Department of Mathematics, Queen's University, Kingston, ON, Canada K7L 3N6
e-mail: murty@mast.queensu.ca

V.K. Murty (✉)
Department of Mathematics, University of Toronto, Toronto, ON, Canada M5S 2E4
e-mail: murty@math.toronto.edu

A. Alaca et al. (eds.), *Advances in the Theory of Numbers*,
Fields Institute Communications 77, DOI 10.1007/978-1-4939-3201-6_7

$$\#\{p \le x : \theta_p \in [\alpha, \beta]\} \sim \left(\frac{2}{\pi}\int_\alpha^\beta \sin^2\theta \, d\theta\right)\pi(x)$$

where $\pi(x)$ as usual denotes the total number of primes $p \le x$. The integral can of course be evaluated, and so the right hand side may also be written

$$\left(\frac{\beta-\alpha}{\pi} - \frac{1}{2\pi}(\sin 2\beta - \sin 2\alpha)\right)\pi(x).$$

The Sato-Tate conjecture is actually a theorem now due to the work of Barnet-Lamb et al. [1].

2 Origin of the Conjecture

Where does such a conjecture come from? Mikio Sato was led to it by numerical calculations. This is described in the beautiful article [11]. It also occurs in Tate's 1964 talk [14] at the Woods Hole Summer Institute on Algebraic Geometry organized by the American Mathematical Society. In that talk, he formulated the following conjecture about algebraic cycles on algebraic varieties. Let X be a smooth projective variety over a number field K. Let $L \supseteq K$ be a finite extension. Consider the Abelian group $A^i(X; L)$ generated by codimension i subvarieties (modulo homological equivalence) which are homologically equivalent to one defined over L. The ℓ-adic cycle class gives a map

$$A^i(X; L) \otimes \mathbb{Q}_\ell \to H_\ell^{2i}(\overline{X})(i).$$

Here, $\overline{X}$ is the base-change of X to an algebraic closure $\overline{K}$ of K, and $H_\ell^*(\overline{X})$ is the ℓ-adic cohomology of X. This is a finite dimensional $\mathbb{Q}_\ell$-vector space on which there is a continuous action of $\mathrm{Gal}(\overline{K}/K)$. In the case X is an Abelian variety, we have

$$H_\ell^*(\overline{X}) = \wedge H_\ell^1(\overline{X}).$$

Moreover, $H_\ell^1(\overline{X})$ is the $\mathbb{Q}_\ell$-dual of the Tate module $V_\ell(X)$ defined by

$$V_\ell(X) = \lim X[\ell^n] \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

This is a $\mathrm{Gal}(\overline{K}/K)$ module in the evident way as $\mathrm{Gal}(\overline{K}/K)$ acts on $X[\ell^n]$.

The cyclotomic character

$$\chi_\ell : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(\mu_{\ell^\infty})$$

gives the action of Galois on ℓ-power roots of unity. The Tate twist $H_\ell^k(\overline{X})(i)$ is the Galois module $H_\ell^k(\overline{X}) \otimes \chi_\ell^i$.

The cycle class map is Galois equivariant, and so the image lies in the subspace of $H_\ell^{2i}(\overline{X})(i)$ fixed by $\mathrm{Gal}(\overline{K}/L)$.

Conjecture 1 (Tate Conjecture 1). The map

$$A^i(X;L) \otimes \mathbb{Q}_\ell \rightarrow H_\ell^{2i}(\overline{X})(i)^{\mathrm{Gal}(\overline{K}/L)}$$

is surjective.

This conjecture is still open in general, though there is now a vast literature on establishing it in special cases. One can get a (by now partial) picture of what is known from Tate's article [15] in the Motives volume.

In [14], Tate computed that for $X = E^m$, with E an elliptic curve defined over $K = \mathbb{Q}$, we have

$$\dim A^i(X,L) = \begin{cases} \binom{m}{i}^2 & \text{if } E \text{ has } CM \\ \binom{m}{i}^2 - \binom{m}{i-1}\binom{m}{i+1} & \text{if } E \text{ does not have } CM. \end{cases} \tag{1}$$

Here $L = \mathbb{Q}$ in the non CM case, and L is the field of multiplication in the CM case. To do this calculation, he did first the case $i = 1$ and then proved that A^i is generated by A^1. Soon afterwards, Mumford introduced the Mumford-Tate group and using the invariant theory of this group, the calculation becomes somewhat simpler.

Let us consider Tate's formula (1) in some special cases. For example, for $m = 2$ and $i = 1$, we have $X = E \times E$ and the codimension 1 cycles are (up to algebraic equivalence) $E \times \{0\}$, $\{0\} \times E$, and the diagonal Δ. In the CM case one has, in addition, the graph Δ_{CM} of the complex multiplication. Thus, the dimension of $A^1(X;L)$ is either 4 or 3 depending on whether E does or does not have CM. Here, we can take $L = \mathbb{Q}$ if E does not have CM. If E does have CM, the field L should contain the CM field.

Similarly, for $m = 3$, and $i = 1$, and E without CM, we have $X = E \times E \times E$. Denoting by E_1, E_2 and E_3 the three copies of E, we have the 6 generic cycles $E \times E \times \{0\}$, $E \times \{0\} \times E$, $\{0\} \times E \times E$, $\Delta_{12} \times E$, $E \times \Delta_{23}$ and $\Delta_{13} \times E$ where Δ_{ab} is the diagonal in $E_a \times E_b$. Note that

$$6 = \binom{3}{1}^2 - \binom{3}{0}\binom{3}{2}.$$

3 L-Functions

For a smooth projective variety over K, consider the Euler product

$$\Phi_i(X,s) = \prod_v \det(I - Frob_v | H_\ell^i(\overline{X})^{I_v}(Nv)^{-s})^{-1}.$$

Here the product is over finite primes v of K. This converges for $\Re(s) > 1 + \frac{i}{2}$. Thus, when $X = E$ and $i = 1$, we have the Hasse L-function of E:

$$\Phi_1(E,s) = \prod_v \left(1 - \frac{e^{i\theta_v}}{(Nv)^{s-\frac{1}{2}}}\right)^{-1} \left(1 - \frac{e^{-i\theta_v}}{(Nv)^{s-\frac{1}{2}}}\right)^{-1}.$$

For L a finite extension of K, we may also consider the base change $X_{/L}$ (in other words, X viewed as a variety over L) and in this case, we have the corresponding Euler product $\Phi_i(X_{/L}, s)$.

Conjecture 2 (Tate Conjecture 2). $\Phi_{2i}(X_{/L}, s)$ has a pole at $s = 1 + i$ of order equal to $\dim A^i(X, L)$.

In particular, (1) and the above conjecture predict that

$$-\mathrm{ord}_{s=k+1}\Phi_{2k}(E^m_{/L}, s) = \begin{cases} \binom{m}{k}^2 & \text{if } E \text{ has } CM \\ \binom{m}{k}^2 - \binom{m}{k-1}\binom{m}{k+1} & \text{if } E \text{ does not have } CM. \end{cases}$$

Here, $L = \mathbb{Q}$ if E does not have CM and the field of multiplication in the CM case. Tate also suggests that $\Phi_{2k+1}(X, s)$ does not have a pole or zero at the edge of its critical strip, namely

$$s = 1 + \frac{1}{2}(2k+1) = k + \frac{3}{2}.$$

These analytic conjectures are motivated by analogy with Artin L-functions and by the Birch and Swinnerton-Dyer conjecture. Again, for $X = E^m$, he computes

$$\Phi_k(X, s) = \prod_{0 \le i \le k/2} M_{k-2i}\left(s - \frac{k}{2}\right)^{\binom{m}{i}\binom{m}{k-i}}.$$

Here,

$$M_0(s) = \zeta(s)$$

and for $k > 0$,

$$M_k(s) = \prod_v \left(1 - \frac{e^{ik\theta_v}}{(Nv)^s}\right)^{-1} \left(1 - \frac{e^{-ik\theta_v}}{(Nv)^s}\right)^{-1}.$$

If $E_{/\mathbb{Q}}$ has CM, the M_k are Hecke L-functions and we know they have analytic continuation to $\Re(s) = 1$ and are non-vanishing on that line. Hence, with L the CM field, the order of pole at $s = k+1$ of $\Phi_{2k}(E^m_{/L}, s)$ is the contribution from $i = k$ and this is

$$\binom{m}{k}^2 = \dim A^k(E^m, L).$$

Now consider the case $E_{/\mathbb{Q}}$ does not have CM. Let c_k denote the order of M_k at $s = 1$ (assuming that M_k is meromorphic at $s = 1$). Then, we have $c_0 = 1$. Moreover, as

$$\Phi_2(X, s) = M_2(s-1)^{\binom{m}{0}\binom{m}{2}} M_0(s-1)^{\binom{m}{1}\binom{m}{1}}$$

we expect that $c_2 = -1$. Also, we expect $c_{2k} = 0$ for all $k > 1$. Indeed, we have

$$\Phi_{2k}(X, s) = \prod_{0 \le i \le k} M_{2k-2i}(s-k)^{\binom{m}{i}\binom{m}{2k-i}}.$$

The factors on the right corresponding to $i = k$ and $i = k - 1$ account for the expected pole of the left hand side.

Suppose also that $c_{2k+1} = 0$ for all $k \geq 0$. Then by a Tauberian argument, we might expect

$$\frac{1}{\pi(x)} \sum_{p \le x} \left(e^{ik\theta_p} + e^{-ik\theta_p}\right) \longrightarrow c_k.$$

Consider

$$F(x) = \frac{1}{\pi} \sum c_k \cos kx.$$

This should then be the distribution function for the θ_v. In other words,

$$F(x) = \frac{1}{\pi}(1 - \cos 2x) = \frac{2}{\pi} \sin^2 x.$$

4 Modular Forms

At the time, arguing by analogy, Serre formulated a conjecture to describe the distribution of the "angles of Frobenius" for any holomorphic cusp form of weight $k \geq 2$, level N and trivial character that is a normalized eigenform for the Hecke operators. For such a form f, let us write

$$f(z) = \sum_{n \ge 1} a_f(n) e^{2\pi i n z}$$

for the Fourier expansion at the cusp $i\infty$. Let us suppose that it is not of CM-type (in the sense of Ribet). That is, there does not exist a Dirichlet character χ with the property that $a_f(p) = \chi(p) a_f(p)$ for almost all p. Then, the Sato-Tate conjecture formulated by Serre in this context is as follows. As before, we can write

$$a_f(p) = 2p^{(k-1)/2} \cos \theta_p$$

for some $\theta_p \in [0, \pi]$. Then

$$\#\{p \leq x : \theta_p \in [\alpha, \beta]\} \sim \left(\frac{2}{\pi} \int_\alpha^\beta \sin^2 \theta d\theta \right) \pi(x).$$

At the time that Serre proposed this, the Taniyama conjecture was not yet proven and so it could not be considered a generalization of the original Sato-Tate conjecture for elliptic curves.

5 The Symmetric Power L-Functions

We now know that the M_k do *not* have good analytic properties and the "correct" L-functions to consider are

$$L_k(s) = \prod_v \prod_{j=0}^{k} \left(1 - \frac{e^{i\theta_v(k-2j)}}{(Nv)^s}\right)^{-1}.$$

The product converges absolutely for $\Re(s) > 1$ so defines an analytic function in that half plane. There is a simple relation between the L_k and the M_k. We have

$$L_0(s) = M_0(s) = \zeta(s)$$

$$L_1(s) = M_1(s) = L(E, s + \frac{1}{2})$$

$$L_2(s) = \prod_v \left(1 - \frac{e^{2i\theta_v}}{(Nv)^s}\right)^{-1} \left(1 - \frac{1}{(Nv)^s}\right)^{-1} \left(1 - \frac{e^{-2i\theta_v}}{(Nv)^s}\right)^{-1}$$

which can be rewritten as

$$L_2(s) = M_0(s) M_2(s).$$

We note that if the middle factor in the above Euler product for L_2 were removed, we would get good analytic properties for the resulting function only in the CM case. In general, we have the relations

$$L_{2k}(s) = M_0(s)M_2(s)M_4(s) \cdots M_{2k}(s)$$

and

$$L_{2k+1}(s) = M_1(s)M_3(s)M_5(s) \cdots M_{2k+1}(s)$$

Using the L_m, Serre proposed a conjectural approach to proving this. If it can be shown that all the $L_m(s)$ are analytic for $\Re s \geq 1$ and non vanishing on the line $\Re(s) = 1$, then Serre showed [12] that Tauberian theorems could be used to deduce the above conjecture. Soon afterwards, Ogg [9] showed that if one had the analytic continuation of the L_m for $\Re(s) > \frac{1}{2} - \epsilon$ for some $\epsilon > 0$, then the non-vanishing on the line $\Re(s) = 1$ could be deduced. In the work of the second author [5], it was shown that non-vanishing was in fact a consequence of the analytic continuation just to $\Re(s) \geq 1$.

In [6], it is shown that if we had the analytic continuation of all the L_m at $s = 1$ (that is, just the point and not the whole line), we could deduce the following weaker version of the Sato-Tate conjecture, namely

$$\sum_{\substack{p \leq x \\ \theta_p \in [\alpha,\beta]}} \frac{\log p}{p} \sim \left(\frac{2}{\pi} \int_\alpha^\beta \sin^2 \theta \, d\theta \right) \log x.$$

The question of how to prove the analytic continuation remained. A conjectural approach to proving it was provided by Langlands.

6 Langlands' Conjecture

Now let us restrict to the case $E_{/\mathbb{Q}}$ does not have CM and consider the family of L-functions $L_m(s)$ introduced above.

Conjecture 3 (Langlands, 1970). There exists $\pi_m \in \mathcal{A}(GL_{m+1})$ a cuspidal automorphic representation such that

$$L(s, \pi_m) = L_m(s)$$

for all $m \geq 1$.

Given the known analytic properties of the standard L-function associated to a cuspidal automorphic representation of GL_m, a consequence of Langlands' conjecture would be the analytic continuation of the $L_m(s)$ for all s.

It is interesting to note that the Sato-Tate conjecture (both the original version as well as Serre's generalization) was proved by Barnet-Lamb et al. [1]. However, this was achieved without proving Langlands' conjecture. What the authors of [1] *did* prove is the *potential* automorphy of the symmetric power L-functions. This means that when the corresponding Galois representation is restricted to a subgroup of finite index, it's L-function is the L-function of an automorphic representation. This, therefore, still leaves open the automorphy of the $L_m(s)$ itself.

Conjecture 3 is a special case of the Langlands Functoriality conjecture. Indeed, beginning with an automorphic representation π of GL_2, and considering the m-th symmetric power of the standard representation

$$r_m : \mathrm{GL}_2(\mathbb{C}) \to \mathrm{GL}_{m+1}(\mathbb{C})$$

the Langlands L-function $L(s, \pi, r_m)$ is $L_m(s)$. Viewing r_m as a map between the complex L-groups of GL_2 and GL_{m+1}, functoriality would predict the existence of a π_m as above.

For $m = 2$, this is the work of Shimura and Gelbart-Jacquet. For $m = 3$ this is due to Kim and Shahidi [4] and for $m = 4$, to Kim [3]. The main result of our work is to show that the holomorphy for all m follows from the automorphy of a restricted class of Rankin-Selberg products, as we explain below. (After this work was completed, we learnt[1] of recent work of Clozel and Thorne [2] that outlines a similar strategy. However, there seem to be differences as the approach of these authors involves local conditions and deformations of Galois representations. Using their approach, they have now proved the automorphy of L_m for $m \leq 8$.)

7 Rankin-Selberg Convolution

Another instance of functoriality is the Rankin-Selberg convolution. Denote by $\mathcal{A}_0(n, F)$ the set of cuspidal automorphic representations of GL_n over F and let $\pi_i \in \mathcal{A}_0(n_i, F)$ for $i = 1, 2$ and assume both are unitary. The Rankin-Selberg convolution provides an L-function $L(s, \pi_1 \times \pi_2)$ which by the work of Jacquet and Shalika extends to a function analytic everywhere except possibly at $s = 1$ where it has a simple pole if and only if $\pi_1 \simeq \pi_2^*$ (the dual of π_2). Another special case of functoriality would be the following hypothesis.

Conjecture 4. There exists a map

$$H_F(n_1, n_2) \; : \; \mathcal{A}_0(n_1, F) \times \mathcal{A}_0(n_2, F) \rightarrow \mathcal{A}(n_1 n_2, F)$$

in which a pair (π_1, π_2) is mapped to π_3 in such a way that

$$L(s, \pi_3) = L(s, \pi_1 \times \pi_2).$$

It is known that $H_F(n, 1)$ exists for all n. This is due to Godement-Jacquet. The work of Ramakrishnan [10] shows that $H_F(2, 2)$ exists and the work of Kim and Shahidi [4] shows that $H_F(2, 3)$ exists. Our main result is the following.

Theorem 1. *Suppose $H_{\mathbb{Q}}(n, 2)$ exists for all n. Then all the L_m are automorphic.*

---

[1]Thanks to Florian Herzig for informing us of this.

8 Brief Outline of the Proof

We will outline the main steps in the proof of Theorem 1. The details will be presented elsewhere. We note that contrary to the expectation that the proof of the analytic continuation of the L_m could be used to prove the Sato-Tate conjecture, our argument *uses* the Sato-Tate theorem to deduce the analytic continuation.

There are three main steps of the proof. The first is to define the notion of *virtual automorphy*. We say that a Dirichlet series

$$F(s) = \sum a_n n^{-s}$$

is *virtually automorphic* if

$$F(s) = \prod L(s, \pi_j)^{b_j}$$

where each π_j is an element of $\mathcal{A}(n_j, \mathbb{Q})$ for some positive integer n_j and some $b_j \in \mathbb{Z}$. We say it is virtually cuspidal if all the π_j in the above factorization are in $\mathcal{A}_0(n_j, \mathbb{Q})$. Now, we use the hypothesis $H(n, 2)$ to show that the L_m are virtually cuspidal.

In the second step, we have a natural notion of Rankin-Selberg convolution $F \times G$ of two virtually cuspidal Dirichlet series F and G. Using this, and the self-duality of the L_m, we deduce that

$$L_m \times L_m = \prod_{j,k} L(s, \pi_j \times \pi_k^*)^{b_j b_k}.$$

The right hand side has a pole at $s = 1$ of order $= \sum b_j^2$ using a result of Shahidi on Rankin-Selberg convolutions.

The third step is to show that the left hand side in fact has a simple pole at $s = 1$ as a consequence of the Sato-Tate theorem and an application of a Tauberian theorem. This implies that only one of the b_j is non-zero and must in fact be ± 1. It can be deduced (using the location of trivial zeros) that it is in fact equal to 1 and thus L_m is automorphic. The details are presented in [7].

9 Variants

Let $S(N, k)$ denote the space of holomorphic cusp forms of weight k for $\Gamma_0(N)$ and denote by $T_n = T_n(N, k)$ the n-th Hecke operator acting on $S(N, k)$. Then the eigenvalues of the normalized operator $T_p/p^{(k-1)/2}$ lie in the interval $[-2, 2]$. The Sato-Tate conjecture (in the general form given to it by Serre) concerns the distribution of these eigenvalues as N and k are fixed and p varies. In [13], Serre began a study of the distribution properties when p is fixed and N and k vary.

In particular, he proved that for a sequence (N_λ, k_λ) with $N_\lambda + k_\lambda \to \infty$, and for p a prime that does not divide any of the N_λ, the eigenvalues of $T_p(N_\lambda, k_\lambda)/p^{(k_\lambda-1)/2}$ are distributed in $[-2, 2]$ according to the measure

$$\mu_p = \frac{p+1}{\pi} \frac{(1-x^2/4)^{\frac{1}{2}}}{(p^{\frac{1}{2}}+p^{-\frac{1}{2}})^2 - x^2} dx.$$

This was made effective in the work of the first author and Sinha [8]. Denote by $s(N, k)$ the dimension of $S(N, k)$. Let $a_{p,i}$ for $1 \leq i \leq s(N, k)$ denote the eigenvalues of T_p acting on $S(N, k)$ (counted with multiplicity). Then, in ([8], Theorem 2), it is proved that

$$\frac{1}{s(N,k)} \#\{1 \leq i \leq s(N,k) : \frac{a_{p,i}}{p^{(k-1)/2}} \in [\alpha, \beta]\} = \int_\alpha^\beta \mu_p + \mathrm{O}(\frac{\log p}{\log kN})$$

where the implied constant is effectively computable.

Acknowledgements It is a pleasure to thank Florian Herzig for some helpful comments and especially for bringing [2] to our attention.

References

1. T. Barnet-Lamb, D. Geraghty, M. Harris, R. Taylor, A family of Calabi-Yau varieties and potential automorphy II. Publ. Res. Inst. Math. Sci. **7**, 29–98 (2011)
2. L. Clozel, J. Thorne, Level raising and symmetric power functionality, I. Preprint (2013)
3. H. Kim, Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2. J. Am. Math. Soc. **16**, 139–183 (2003)
4. H. Kim, F. Shahidi, Functorial products for $GL_2 \times GL_3$ and the symmetric cube for GL_2. Ann. Math. **155**, 837–893 (2002)
5. V.K. Murty, On the Sato-Tate conjecture, in *Number Theory Related to Fermat's Last Theorem*, ed. by N. Koblitz. Progress in Mathematics, vol. 26 (Birkhauser, Boston, 1982)
6. V.K. Murty, On the Sato-Tate conjecture II, in *On Certain L-Functions*, ed. by J. Arthur et al. Clay Mathematics Proceedings, vol. 13 (American Mathematical Society, Providence, 2011), pp. 471–482
7. M.R Murty, V.K. Murty, Automorphy and the Sato-Tate conjecture. Preprint (2013)
8. M.R. Murty, K. Sinha, Effective equidistribution of eigenvalues of Hecke operators. J. Number Theory **129**, 681–714 (2009)
9. A. P. Ogg, A remark on the Sato-Tate conjecture. Invent. Math. **9**, 198–200 (1969/1970)
10. D. Ramakrishnan, Modularity of the Rankin-Selberg L-series and multiplicity one for SL_2. Ann. Math. **152**, 45–111 (2000)
11. P. Schapira, Mikio Sato: a visionary of mathematics. Not. Am. Math. Soc. **54**, 243–245 (2007)
12. J.-P. Serre, *Abelian ℓ-Adic Representations and Elliptic Curves* (Benjamin, New York, 1968)
13. J.-P. Serre, Répartition asymptotique des valeurs propres de l'operateur de Hecke T_p. J. Am. Math. Soc. **10**, 75–102 (1997)
14. J. Tate, Algebraic cycles and poles of Zeta functions, in *Arithmetic Algebraic Geometry*, ed. by O. Schilling, (Harper and Row, New York, 1965), pp. 93–110
15. J. Tate, Conjectures on algebraic cycles in ℓ-adic cohomology, in *Motives*, Part 1, ed. by U. Jannsen et al. Proceedings of Symposia in Pure Mathematics, vol. 55 (American Mathematical Society, Providence, 1994), pp. 71–83