Current Trends
in Science

platinum jubilee special

Edited by N. Mukunda, Indian Academy of Sciences, 2009

The Sato–Tate conjecture and generalizations*

M RAM MURTY[1] and V KUMAR MURTY[2]

[1] *Department of Mathematics, Queen's University, Kingston, Ontario, K7L 3N6, Canada.*
e-mail: murty@mast.queensu.ca

[2] *Department of Mathematics, University of Toronto, Toronto, Ontario, M5S 2E4, Canada.*
e-mail: murty@math.toronto.edu

1. Introduction

Consider the elliptic curve E defined by the equation

$$y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{Z}.$$

Let $\Delta = -16(4a^3 + 27b^2)$. For each prime p with $(p, \Delta) = 1$, we can consider the congruence

$$y^2 \equiv x^3 + ax + b (\text{mod } p),$$

and count the number N_p of solutions (x, y). This quantity was first studied by Emil Artin [1] in his 1924 doctoral thesis in which he conjectured that

$$|N_p - p| \leq 2\sqrt{p}, \tag{1}$$

for all such primes. In many ways, his study was motivated by the classical Riemann hypothesis. To understand the nature of zeta functions in general, Artin defined the analogue of the Dedekind zeta function in the setting of a function field over a finite field. In the case of a quadratic extension of $\mathbb{F}_p(x)$ defined by

$$y^2 = x^3 + ax + b,$$

the analogue of the Riemann hypothesis for the function field zeta function turns out to be equivalent to (1). In his thesis, Artin verified his conjecture for many small primes p but could not prove it. In February, 1933, Hasse [14] proved the conjecture using techniques from algebraic geometry. One could say that understanding this function field analogue of the Riemann hypothesis was an important step in the annals of mathematics. The reader is referred to the historical document [11] for further discussions on this.

Artin's thesis was seminal in many ways. First, it opened up the study of algebraic geometry over finite fields and connected it to the study of exponential sums that occur in classical analytic number theory. Second, it inspired Weil [36] to formulate in 1949 general conjectures that led Grothendieck [13] to chart out a visionary program in algebraic geometry ultimately leading to a resolution of the Weil conjectures in the fundamental work on Deligne [8] in 1974.

Around 1960, Mikio Sato and John Tate [32] (independently) asked about the distribution of the numbers

$$N_p - p/\sqrt{p}$$

in the interval $[-2, 2]$, as p tends to infinity. For example, is it reasonable to expect that these numbers are uniformly distributed in the interval?

*Research of both authors partially supported by Natural Sciences and Engineering Research Council (NSERC) grants.

Keywords. Elliptic curves; Sato–Tate; symmetric power L-functions; Chebotarev density theorem.

In other words, is it true that for any interval $[a,b] \subseteq [-2,2]$, we have

$$\lim_{x\to\infty} \frac{\#\{p \le x : (N_p - p)/\sqrt{p} \in [a,b]\}}{\#\{p \le x\}} = b - a?$$

This question is the genesis of the Sato–Tate conjecture. Numerical evidence seemed to suggest otherwise. More precisely, Sato and Tate were led to predict that for a 'generic' elliptic curve E the following is true. If we write

$$(N_p - p)/\sqrt{p} = 2\cos\theta_p, \quad 0 \le \theta_p \le \pi,$$

and $[\alpha,\beta] \subseteq [0,\pi]$, then, their conjecture says

$$\lim_{x\to\infty} \frac{\#\{p \le x : \theta_p \in [\alpha,\beta]\}}{\#\{p \le x\}} = \frac{2}{\pi}\int_\alpha^\beta \sin^2\theta \, d\theta$$

$$= \frac{\beta-\alpha}{\pi} - \frac{1}{2\pi}(\sin 2\beta - \sin 2\alpha).$$

What 'generic' means is that the elliptic curve should be without complex multiplication (see [20] for details). If the elliptic curve has complex multiplication, then the (essentially) uniform distribution law for the angles was worked out by Deuring [10] building on earlier work of Hecke [15,16].

One can formulate a more general conjecture. Let E be an elliptic curve defined over a number field K. For each place v of K where E has good reduction, we may consider the group of points of E mod v. Its cardinality (including the identity element) can be written as

$$Nv + 1 - a_v,$$

where Nv denotes the norm of v and a_v is an integer satisfying Hasse's inequality $|a_v| \le 2(Nv)^{1/2}$. As before, one can therefore write

$$a_v = 2N(v)^{1/2}\cos\theta_v,$$

where $\theta_v(E) := \theta_v$ satisfies $0 \le \theta_v \le \pi$. The Sato–Tate conjecture now is a statement about how the angles θ_v are distributed in the interval $[0,\pi]$ as v varies. When E has complex multiplication (CM), the distribution law is known and again follows from the classical work of Deuring on Hecke L-series (see [26] for details). In the non-CM case, one expects that the angles are uniformly distributed with respect to the measure

$$\mu_{ST} := \frac{2}{\pi}(\sin^2\theta)d\theta.$$

On March 18, 2006, Taylor [33] (see also [5]) just published a proof of this conjecture, when E has at least one prime of multiplicative reduction. He was building on his earlier work with Clozel, Harris and Shepherd-Barron (see Carayol's Séminaire Bourbaki article [4]).

In this paper, we give an informal exposition of this recent development. We also indicate some modest generalizations that are obtained by slight modifications in the proof. Our first result is a hybrid Chebotarev–Sato–Tate theorem.

Theorem 1. *Let E be an elliptic curve defined over a totally real number field K with at least one prime of multiplicative reduction. If M/K is a solvable Galois extension of finite degree with $G = \mathrm{Gal}(M/K)$, and C is a conjugacy class of G, then the density of prime ideals $\mathfrak{p}$ for which the Artin symbol $\sigma_\mathfrak{p} \in C$ and the angle $\theta_\mathfrak{p} \in [\alpha,\beta]$ with $0 \le \alpha \le \beta \le \pi$ is*

$$\frac{2|C|}{\pi|G|}\int_\alpha^\beta \sin^2\theta d\theta.$$

In particular, we have the following corollary:

Corollary 2. *Let E be an elliptic curve defined over the rational number field with at least one prime of multiplicative reduction. Let q be a natural number and a an integer with $(a,q) = 1$. For $0 \le \alpha \le \beta \le \pi$, the density of primes p for which $\theta_p(E) \in [\alpha,\beta]$ and $p \equiv a \pmod q$ is*

$$\frac{2}{\pi\varphi(q)}\int_\alpha^\beta \sin^2\theta d\theta.$$

It is evident that by similar arguments, one can handle the joint distribution of angles of any finite set of elliptic curves provided that there is at most one elliptic curve in the set without CM (and having at least one prime of multiplicative reduction).

One can also study the joint distribution of angles of a finite collection of pairwise non-isogenous elliptic curves. This looks like a difficult question and Harris has recently announced some progress in this direction.

Though our treatment is informal, the background needed for a total understanding is quite formidable spanning representation theory, arithmetic algebraic geometry, analytic and algebraic number theory. Still, we hope that the presentation given here will enable the non-expert to see how the proof is put together and appreciate the interplay of ideas.

Recently, 'friendly' exposés of the Sato–Tate conjecture have appeared in various places. The papers by Mazur [22,23] are a good place to begin for the totally uninitiated reader. Here, our goal is more mathematical. We hope to give (without proofs) the main mathematical ingredients that enter into such equidistribution questions so that the reader may have a conceptual understanding of the results.

Because of the celebrated Taniyama conjecture (now proved by Wiles [37] and others [3]), one can view the a_v's as Fourier coefficients of certain modular forms of weight 2, at least in the case that E is defined over the rational number field. In the general number field case, it is still open whether the a_v's can be viewed as coming from automorphic representations as predicted by Langlands. Thus, one can view the Sato–Tate conjecture as a special case of a more general statement concerning distribution of eigenvalues of Hecke operators. (See [6] for more details.)

One can formulate a function field analogue of the Sato–Tate conjecture and this has been proved in various contexts. Let K be a rational function field in one variable over a finite field $\mathbb{F}$ and let E denote an elliptic curve over K with nonconstant j-invariant. Let Y denote the projective line over $\mathbb{F}$ and consider the Néron model $\mathcal{E} \longrightarrow Y$. This is a smooth group scheme whose general fibre is E and outside of a finite set S of points $y \in Y$, the fibre $\mathcal{E}_y$ at y is an elliptic curve (the 'reduction' of E modulo the residue field corresponding to y). Thus, as an elliptic curve over a finite field, its zeta function is of the form

$$\frac{(1-\alpha_y T)(1-\overline{\alpha_y}T)}{(1-T)(1-q^{\deg y}T)}.$$

Here $\alpha_y = q^{(\deg y)/2}e^{i\theta(y)}$, where $0 \le \theta(y) \le \pi$. Let $\mathbb{F}_n$ denote the unique extension of $\mathbb{F}$ of degree n. Then, the Sato–Tate conjecture in this context says that as $n \longrightarrow \infty$, we have

$$\#\{y \in Y(\mathbb{F}_n) : \alpha \le \theta_y \le \beta\}$$

$$\sim \left(\int_\alpha^\beta \frac{2}{\pi}\sin^2\theta d\theta\right)|Y(\mathbb{F}_n)|.$$

This was proved by Yoshida in [34] and in a different way by K Murty in [26]. Very general theorems of Sato–Tate type (in which the base Y is replaced by an arbitrary variety and $\mathcal{E}$ by families of ℓ-adic sheaves) are proved in Deligne [9], section 3.5.

2. Symmetric power L-series of elliptic curves

Let K be an algebraic number field. Let E be an elliptic curve defined over K. Let S be the (finite) set of places where E has bad reduction. For each finite place $v \notin S$ of K, we know that the number of points on $E \bmod v$ is given by

$$N(v) + 1 - a_v,$$

where a_v is an integer satisfying Hasse's inequality $|a_v| \le 2N(v)^{1/2}$. For each prime ℓ, the action of $\mathrm{Gal}(\bar{K}/K)$ on the ℓ-adic Tate module gives rise to an ℓ-adic representation

$$\rho := \rho_\ell : \mathrm{Gal}(\bar{K}/K) \to GL_2(\mathbb{Q}_\ell),$$

which is integral, that is, the characteristic polynomial of $\rho_\ell(F_v)$ where F_v denotes the Frobenius automorphism at $v \notin S$ has integer coefficients, independent of ℓ. In fact, this characteristic polynomial is $X^2 - a_vX + N(v)$. Let us write $\alpha_vN(v)^{1/2}$, $\beta_vN(v)^{1/2}$ for the two roots of the quadratic polynomial

$$X^2 - a_vX + N(v).$$

The (partial) m-th symmetric power L-function is defined as

$$L_S(s, \mathrm{Sym}^m\rho) := \prod_{v\notin S}\prod_{j=0}^{m}(1-\alpha_v^j\beta_v^{m-j}N(v)^{-s})^{-1}.$$

Clearly, the product converges absolutely for $\Re(s) > 1$. In [29], Serre showed that if for all m, $L_S(s, \mathrm{Sym}^m(\rho))$ extends to $\Re(s) \ge 1$ and does not vanish there, then the Sato–Tate conjecture follows. In [26], K Murty showed that the non-vanishing assumption is unnecessary. Thus, in this way, the Sato–Tate conjecture was reduced to a problem of analytic continuation of $L_S(s, \mathrm{Sym}^m(\rho))$ to the region $\Re(s) \ge 1$, for all values of m.

In 1970, Langlands [21] outlined a method of attacking the problem of analytic continuation. He suggested the existence of an automorphic representation π_m attached to $GL_{m+1}(\mathbb{A}_K)$, where $\mathbb{A}_K$ denotes the adele ring of K, such that $L_S(s, \pi_m) = L_S(s, \mathrm{Sym}^m(\rho))$ where $L_S(s, \pi_m)$ is the automorphic L-function attached to π_m with the Euler factors corresponding to the places $v \in S$ removed. In fact, it is conjectured that one can define the local factors for $v \in S$ in such a way that the completed L-function, $L(s, \mathrm{Sym}^m(\rho))$ (which we shall abbreviate as $L_m(s)$) satisfies a functional equation relating s to $1-s$. (See for example, [7] for details.) When $K = \mathbb{Q}$ and $m = 1$, this is the Taniyama conjecture. Langlands' functoriality conjecture predicts that the symmetric powers of π_1 are automorphic. This has been proved for some small values of m (see [6] for a survey of the present state of knowledge). If the Langlands conjecture about the existence of π_m is true, then by the theory of automorphic representations, one immediately has analytic continuation of $L_S(s, \mathrm{Sym}^m(\rho))$ to the entire complex plane and by the result of K Murty [26], the non-vanishing on the line $\Re(s) = 1$ follows and the Sato–Tate conjecture follows. The non-vanishing of the L-function on the line $\Re(s) = 1$ can also be deduced from a celebrated result of Jacquet and Shalika [17] who showed that for any automorphic representation π, we have $L(s, \pi) \neq 0$, for $\Re(s) = 1$. So, what is known about the analytic continuation of $L_S(s, \mathrm{Sym}^m(\rho))$?

For $m = 1$, this is the (partial) Hasse–Weil L-series attached to the elliptic curve E. It is possible to define the Euler factors at places in S as well so that the completed L-function conjecturally admits an analytic continuation to the entire complex plane and satisfies a suitable functional equation. In the case $K = \mathbb{Q}$, the Taniyama conjecture, proved by Wiles (in the semistable case) [37] and by Breuil, Conrad, Diamond and Taylor (in the general case) [3] asserts that there is a classical cusp form f of weight 2 and level N (the conductor of E) such that the Hecke L-series $L(s, f)$ attached to f agrees with $L_1(s - 1/2)$. If π_f is the automorphic representation associated to f, then, in the context of the Langlands program, we have $L(s, \pi_f) = L_1(s)$. The series $L_1(s)$ is essentially the L-function attached to ρ, coming from the action of $\mathrm{Gal}(\bar{K}/K)$ on the Tate module.

More generally, $L_m(s)$ is essentially the L-function attached to the representation $\mathrm{Sym}^m(\rho)$, which comes from the action of $\mathrm{Gal}(\bar{K}/K)$ on the m-fold symmetric product of the Tate module. As alluded to above, one expects the existence of an automorphic representation π_m attached to $GL_{m+1}(\mathbb{A}_K)$ satisfying $L(s, \pi_m) = L_m(s)$. This expectation is far from being realized, though important advances have been made in this direction.

What Taylor proves is not the automorphy of $L_m(s)$ but rather its 'potential automorphy.' This fact, combined with other results in the analytic theory of automorphic L-functions, leads to the Sato–Tate conjecture. This result of 'potential automorphy' builds on a massive collection of earlier work that can be traced back to the celebrated conjecture of Serre.

Serre [30] formulated a general conjecture about representations

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}),$$

with $\mathbb{F}$ a finite field, which are odd, and absolutely irreducible. More precisely, he predicted that such representations arise from classical modular forms. Serre [30] showed that his conjecture implies the Taniyama conjecture. On the other hand, Frey [12] had a remarkable insight which was completed and made more precise by Ribet [27] who showed that the Taniyama conjecture implies Fermat's last theorem. Thus, Serre's conjecture offered a new approach to Fermat. Wiles [37] proved an important case of Serre's conjecture that was enough to deduce Taniyama. This work led to further developments. Most recently, Chandrashekhar Khare [18] proved the level 1 case of the Serre conjecture. In very recent work, Khare and Wintenberger [19] have settled the odd conductor case. This last development not only gives a new proof of Fermat's last theorem, but it also implies the strong Artin conjecture [2] for 2-dimensional Galois representations of odd conductor.

In his recent paper, Taylor [33] made substantial progress towards this conjecture. If K is a totally real field and m is odd, he showed that there is a finite, totally real Galois extension L/K such that $(\mathrm{Sym}^m\rho)$ restricted to L is automorphic over L. One can choose an L that works simultaneously for any finite set of odd numbers. One can also choose it to be unramified at any finite set of places. Once this theorem is in hand, Taylor uses standard results from the theory of automorphic L-functions to deduce the Sato–Tate conjecture. We will give an outline of this deduction below.

Before we do this, let us review some essential theorems from the theory of automorphic L-functions. We refer the reader to [24] for details, definitions and additional references to the literature. More precisely, we highlight pages 119 and 215 of [2] for the exact definitions of the notions of base change and automorphic induction. Here are the key theorems we will need.

First is the theorem of base change and automorphic induction, due to Arthur and Clozel [2]. This says the following. Suppose that L/K is a cyclic extension and π, Π are cuspidal representations of $GL_n(\mathbb{A}_K)$ and $GL_n(\mathbb{A}_L)$, respectively. Then, the base change of π, denoted $B(\pi)$ and the automorphic induction $I(\Pi)$ of Π exist.

The second fact we need is a celebrated theorem of Jacquet and Shalika [17] which states that for any unitary cuspidal automorphic representation π, of $GL_n(\mathbb{A}_K)$, we have $L(1 + it, \pi) \neq 0$.

The third fact needed is a non-vanishing theorem due to Shahidi [31]. This states that the Rankin–Selberg L-function $L(s, \pi_1 \times \pi_2)$ does not vanish on the line $\Re(s) = 1$, whenever π_1 and π_2 are unitary cuspidal automorphic representations.

A fourth fact needed is the Artin reciprocity law which states that every abelian Artin L-function of any Galois extension of K is a Hecke L-function and corresponds to a cuspidal automorphic representation of $GL_1(\mathbb{A}_K)$.

3. An outline of Taylor's theorem

Here is a brief outline of Taylor's proof of the Sato–Tate conjecture. His main theorem is: let K be a totally real field and E/K an elliptic curve with multiplicative reduction at some prime. For any odd number m, there is a finite, totally real Galois extension L/K such that $\mathrm{Sym}^m\rho$ becomes automorphic over L. In other words, $(\mathrm{Sym}^m\rho)|_L$ is automorphic over L. (One can also choose an L that will work simultaneously for any finite set of **odd** positive numbers.)

From this result, he deduces the Sato–Tate conjecture in three steps. Here is an outline.

Step 1: For any intermediate field $K \subset F \subset L$, with L/F solvable, $\mathrm{Sym}^m\rho$ is automorphic over F. In other words, $(\mathrm{Sym}^m\rho)|_F$ is automorphic over F for every F with L/F solvable.

This is proved in his earlier paper: M Harris, N Shepherd-Baron and R Taylor, Ihara's lemma and potential automorphy, (preprint available at www.math.harvard.edu/∼rtaylor).

Essentially, it applies the Arthur–Clozel theory of base change, the key idea being that the base change lift of $\mathrm{Sym}^m\rho$ to L, which exists by Taylor's main theorem, is Galois invariant and so must be the base change lift of an automorphic representation π_F for every intermediate F, with L/F solvable. This is because one can find a chain

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_m = L$$

of extensions so that F_{i+1}/F_i is cyclic for $0 \le i \le m-1$ and apply the Arthur–Clozel theorem for automorphic induction successively, in stages, to each of the cyclic extensions $F_m/F_{m-1}, \ldots, F_1/F_0$. We refer the reader to [2] for precise details concerning automorphic induction.

Step 2: Let $G = \mathrm{Gal}(L/K)$. Now apply Brauer induction to write

$$1 = \sum_i a_i \,\mathrm{Ind}_{H_i}^G \,\psi_i,$$

with a_i integers and ψ_i 1-dimensional characters of nilpotent subgroups H_i of G. Then,

$$L(s, (\mathrm{Sym}^m\rho)\otimes 1) = \prod_i L(s, (\mathrm{Sym}^m\rho) \otimes \mathrm{Ind}_{H_i}^G \psi_i)^{a_i}.$$

By Frobenius reciprocity,

$$(\mathrm{Sym}^m\rho) \otimes \mathrm{Ind}_{H_i}^G \psi_i = \mathrm{Ind}_{H_i}^G((\mathrm{Sym}^m\rho)|_{L^{H_i}} \otimes \psi_i).$$

By step 1, $(\mathrm{Sym}^m\rho)|_{L^{H_i}}$ is automorphic over L^{H_i}. By Artin reciprocity, ψ_i is a Hecke character χ_i of L^{H_i}. Thus, $(\mathrm{Sym}^m\rho)|_{L^{H_i}} \otimes \psi_i$ is automorphic over L^{H_i}. By invariance of L-series under induction, we deduce

$$L(s, \mathrm{Sym}^m\rho) = \prod_i L(s, (\mathrm{Sym}^m\rho)|_{L^{H_i}} \otimes \chi_i)^{a_i},$$

and the product on the right hand side, being a product of automorphic L-functions by step 1, represents a meromorphic function of s. In this way, one derives the meromorphic continuation of the **odd** symmetric power L-functions attached to E.

Step 3: If we apply the Jacquet–Shalika theorem which assures us that there are no poles on $\Re(s) = 1$ for a cuspidal automorphic L-function $L(s, \pi)$, as well as the non-vanishing of $L(s, \pi)$ on $\Re(s) = 1$ for any automorphic representation π, we obtain from the above product the analytic continuation and non-vanishing on $\Re(s) = 1$ of $L(s, \mathrm{Sym}^m\rho)$ for m odd. To treat m even, one uses induction and the identity

$$\mathrm{Sym}^{m-1}\rho \oplus \mathrm{Sym}^{m+1}\rho = \mathrm{Sym}^m\rho \otimes \mathrm{Sym}^1\rho,$$

which is essentially the trigonometric identity

$$\frac{\sin m\theta}{\sin\theta} + \frac{\sin(m+2)\theta}{\sin\theta} = \left(\frac{\sin(m+1)\theta}{\sin\theta}\right)\left(\frac{\sin 2\theta}{\sin\theta}\right)$$

(or the Clebsch–Gordon branching rule for SL_2). Thus,

$$L(s, \mathrm{Sym}^{m-1}\rho)L(s, \mathrm{Sym}^{m+1}\rho)$$
$$= L(s, (\mathrm{Sym}^m\rho) \otimes \mathrm{Sym}^1\rho).$$

Now apply step 1, with the two odd numbers $1, m$ to get the base change to L of both $\mathrm{Sym}^m\rho$ and $\mathrm{Sym}^1\rho$ automorphic. By the same Brauer induction trick of step 2 applied to the right hand side, one deduces that the right hand side has a meromorphic continuation for all complex s. To get analytic continuation to $\Re(s) = 1$, one needs to apply Shahidi's results on the non-vanishing of Rankin–Selberg L-functions which appear on the right hand side. Poles on the line $\Re(s) = 1$ can also be ruled out by the same theory. This completes the proof.

In many respects, this is the elliptic analogue of Brauer's theorem of the meromorphy of Artin L-series. As can be seen, the non-vanishing of the L-series on the line $\Re(s) = 1$ is essential in the proof. This was ensured by an application of theorems of Jacquet, Shalika and Shahidi. The Jacquet–Shalika theorem and the Shahidi theorem rely on the theory of Eisenstein series (à la Langlands). There are other ways of establishing non-vanishing of the L-series concerned without using the theory of Eisenstein series. Indeed, if one is willing to admit Rankin–Selberg theory and existence and analyticity of these L-functions, then classical non-vanishing techniques (of the type used by Hadamard and de la Vallée Poussin) actually work. This method is outlined in a recent paper of Sarnak [28].

4. A Chebotarev–Sato–Tate theorem and generalizations

There are some natural generalizations of the Sato–Tate conjecture that one can consider. We indicate briefly how this can be done and what can actually be proved. Firstly, we can take two non-isogenous elliptic curves and consider the joint distribution of the angles. For instance, if E_1 and E_2 are non-isogenous elliptic curves, both without CM, defined over $\mathbb{Q}$, and $\theta_p(E_1)$ and $\theta_p(E_2)$ are the angles respectively, it is reasonable to expect that the distribution of the pair of angles $(\theta_p(E_1), \theta_p(E_2))$ is given by the product distribution

$$\frac{4}{\pi^2} \sin^2\theta_1 \sin^2\theta_2 d\theta_1 d\theta_2.$$

To prove such an assertion, we can use the formalism of Serre [29]. Using the formalism of [29], it is not difficult to show that this involves the study of certain L-series. Indeed, if both curves are non-CM and have associated Galois representations ρ_1 and ρ_2 respectively, then one needs to show that the L-series

$$L(s, \mathrm{Sym}^{m_1}(\rho_1) \otimes \mathrm{Sym}^{m_2}(\rho_2))$$

extends to $\Re(s) \geq 1$ and does not vanish there. This looks like a difficult question to answer with the present state of knowledge. However, Harris has recently announced some progress in this direction.

If however, one of the curves has CM and corresponds to a Hecke character ψ, then one needs to study the L-series

$$L(s, \psi^{m_1} \otimes \mathrm{Sym}^{m_2}(\rho_2)),$$

and establish analytic continuation and non-vanishing in the region $\Re(s) \geq 1$. This can be done since only Hecke characters intervene and these can be base-changed to any field by a well-known theorem of Weil [36]. It is also clear one can take any number of CM elliptic curves and derive a similar theorem for the same reasons.

Here is the proof of theorem 1.

By standard Tauberian theory, as discussed in [29], we need to show that for any irreducible representation τ of $G = \mathrm{Gal}(M/K)$, the L-function

$$L(s, \tau \otimes \mathrm{Sym}^m \rho)$$

is analytic and non-vanishing in the region $\Re(s) \geq 1$. Using Brauer induction, we write

$$\tau = \sum_i c_i \mathrm{Ind}_{H_i}^G \phi_i,$$

where the c_i are integers, and ϕ_i is an abelian character of H_i, with H_i certain nilpotent subgroups of G. In Taylor's theorem, we can choose L so that L and M are disjoint. Thus, $\mathrm{Gal}(LM/L) = G$ and

$$L(s, \mathrm{Sym}^m \rho \otimes \tau) = \prod_i L(s, \mathrm{Sym}^m \rho \otimes \mathrm{Ind}_{H_i}^G \phi_i)^{c_i}.$$

Since we are viewing G as the Galois group of LM/L, we can re-write this, by Frobenius reciprocity, as

$$\prod_i L(s, \mathrm{Ind}_{H_i}^G (\mathrm{Sym}^m \rho|_{(LM)^{H_i}} \otimes \psi_i)^{c_i}),$$

where ψ_i is the Hecke character corresponding to ϕ_i via Artin reciprocity. As $(\mathrm{Sym}^m \rho)|_L$ is automorphic by Taylor's theorem, $(\mathrm{Sym}^m \rho)|_{LM}$ is automorphic by the theory of base change applied to the solvable extension LM/L. As in step 1 of Taylor's theorem, we deduce that $(\mathrm{Sym}^m \rho)|_{(LM)^{H_i}}$ is automorphic over $(LM)^{H_i}$ by an application of the Arthur–Clozel theory. Since ψ_i is a Hecke character, we deduce that

$$(\mathrm{Sym}^m \rho)|_{(LM)^{H_i}} \otimes \psi_i$$

is automorphic over $(LM)^{H_i}$. Consequently, by the invariance of L-series under induction, we deduce that

$$L(s, \mathrm{Ind}_{H_i}^{G}((\mathrm{Sym}^m \rho)|_{(LM)^{H_i}} \otimes \psi_i))$$

is automorphic. Thus, it is analytic and non-vanishing for $\Re(s) \geq 1$. This proves that

$$L(s, (\mathrm{Sym}^m \rho) \otimes \chi)$$

extends to an analytic function for $\Re(s) \geq 1$ and does not vanish there. This proves the required assertion for m odd. For m even, we proceed as before, by induction to obtain the desired result. This completes the proof of theorem 1.

5. Concluding remarks

We conclude this section with an alternate argument in the case that M/K is a nilpotent Galois extension which is simpler. In future variations, this alternate argument may be useful.

By standard Tauberian theory, as discussed in [29], we need to show that for any irreducible representation τ of $\mathrm{Gal}(\bar{K}/K)$, with nilpotent image, the L-function

$$L(s, \tau \otimes \mathrm{Sym}^m \rho)$$

is analytic and non-vanishing in the region $\Re(s) \geq 1$. Since any irreducible representation of a finite nilpotent group is induced from an abelian character χ of a subgroup H, so

$$\tau \otimes \mathrm{Sym}^m(\rho) = \mathrm{Ind}_H^G(\chi \otimes \mathrm{Sym}^m(\rho)|_{L^H}).$$

By Arthur–Clozel, $\chi \otimes \mathrm{Sym}^m(\rho)|_{L^H}$ is automorphic. We now complete the proof as before.

It is clear from the preceding arguments that if one had the automorphic induction of Hecke characters, the proof would go through for any Galois setting and not just in the nilpotent or solvable setting. Future advances in the Langlands program should translate into general theorems of Chebotarev–Sato–Tate type.

Acknowledgements

We would like to thank Fernando Gouvêa, Sanoli Gun, Chandrashekhar Khare, Dipendra Prasad and the referee for helpful remarks on an earlier version of this paper.

References

[1] Artin E 1924 Quadratische Körper im Gebiete der höheren Kongruenzen, I, II; *Math. Zeit.* **19** 153–246.

[2] Arthur J and Clozel L 1989 Simple algebras, base change and the advanced theory of the trace formula; Annals of Math. Studies, **120**, Princeton University Press.

[3] Breuil C, Conrad B, Diamond F and Taylor R 2001 On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises; *J. Am. Math. Soc.* **14(4)** 843–939.

[4] Carayol H 2006–07 La conjecture de Sato–Tate (d'après Clozel, Harris, Shepherd-Barron, Taylor), *Sem. Bourbaki* **59** Exp. 977, pp. 345–391.

[5] Clozel L, Harris M and Taylor R 2008 Automorphy of some ℓ-adic lifts of automorphic mod ℓ Galois representations; *Publ. Math. IHES* **108(1)** 1–182.

[6] Cogdell J, Kim H and Murty R 2006 *Lectures on automorphic L-functions*; Fields Institute Lecture Notes, Am. Math. Soc., Providence.

[7] Cogdell J and Michel P 2004 On the complex moments of symmetric power L-functions at $s = 1$; *Int. Math. Res. Notices* **31** 1561–1617.

[8] Deligne P 1974 La conjecture de Weil, I; *Inst. Hautes Études Sci. Publ. Math.* **43** 273–307.

[9] Deligne P 1980 La conjecture de Weil, II; *Inst. Hautes Études Sci. Publ. Math.* **52** 138–252.

[10] Deuring M 1941 Die Typen der Multiplikatorenringe elliptischer Funktionenkörper; *Abh. Math. Zem. Hansischen Univ.* **14** 197–272.

[11] Frei G and Roquette P 2008 *Emil Artin and Helmut Hasse, Die Korrespondenz 1923–1934*; Universitätsverlag Göttingen.

[12] Frey G 1989 Links between solutions of $A - B = C$ and elliptic curves; *Lecture Notes Math.* **1380** 31–62.

[13] Grothendieck A 1958 The cohomology theory of abstract algebraic varieties; *Proc. Int. Congr. Math. Edinburgh* 103–118.

[14] Hasse H 1933 Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F K Shmidtschen Kongruenzzetafunktionen in gewissen zykischen Fällen, Vorläufige Mitteilung; *Nachr. Ges. Wiss. Göttingen I. Math.-Phys. Kl. Fachgr. I Math. Nr.* **42** 253–262.

[15] Hecke E 1918 Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzalhen, I; *Math. Zeit.* **1** 357–376.

[16] Hecke E 1920 Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, II; *Math. Zeit.* **6** 11–51.

[17] Jacquet H and Shalika J 1976–77 A non-vanishing theorem for zeta functions of GL_n; *Inventiones Math.* **38(1)** 1–16.

[18] Khare C 2006 Serre's modularity conjecture: The level one case; *Duke Math. J.* **134(3)** 557–589.

[19] Khare C and Wintenberger J-P, Serre's modularity conjecture I (to appear).

[20] Lang S 1987 *Elliptic Functions* Graduate Texts in Mathematics, Second Edition (New York: Springer-Verlag).

[21] Langlands R P 1970 Problems in the theory of automorphic forms, in Lectures in Modern Analysis and Applications; *Lecture Notes in Math.* **170** Springer-Verlag, 18–86.

[22] Mazur B 2006 Controlling our errors; *Nature* **443** 38–40.

[23] Mazur B 2008 Finding meaning in error terms; *Bull. Am. Math. Soc.* **45** 185–228.

[24] Ram Murty M 2002 Recent developments in the Langlands program; *Comptes Rendus Math. Rep. Sci. Canada* **24(2)** 33–54.

[25] Ram Murty M 1983 Oscillations of Fourier coefficients of modular forms; *Math. Annalen* **262** 431–446.

[26] Kumar Murty V 1981 On the Sato–Tate conjecture; in *Number theory related to Fermat's last theorem* (Cambridge, Mass.); 1982 *Progress in Math.* **26** 195–205 (Boston: Birkhäuser).

[27] Ribet K 1990 From the Taniyama–Shimura conjecture to Fermat's last theorem; *Annales de la faculté des sciences de Toulouse, Ser. 5* **11(1)** 116–139.

[28] Sarnak P 2004 Non-vanishing of L-functions on $\Re(s) = 1$; in *Contributions to automorphic forms, geometry, and number theory* 719–732 (Baltimore: Johns Hopkins University Press).

[29] Serre J-P 1998 *Abelian ℓ-adic representations and elliptic curves*; Research Notes in Mathematics **7** (Massachusetts: A K Peters, Wellesley).

[30] Serre J-P 1987 Sur les répresentations modulaires de degré 2 de Gal($\bar{\mathbb{Q}}/\mathbb{Q}$); *Duke Math. J.* **54** 179–230.

[31] Shahidi F 1981 On certain L-functions; *Am. J. Math.* **103(2)** 297–355.

[32] Tate J 1965 Algebraic cycles and poles of zeta functions; in *Arithmetic Algebraic Geometry* (ed.) Schilling F G, 93–110 (New York: Harper and Row).

[33] Taylor R 2008 Automorphy of some ℓ-adic lifts of automorphic mod ℓ representations, II; *Publ. Math. IHES* **108(1)** 183–239.

[34] Yoshida H 1973 An analogue of the Sato–Tate conjecture; *Inv. Math.* **19** 261–277.

[35] Weil A 1949 Number of solutions of equations in finite fields; *Bull. Am. Math. Soc.* **55** 497–508.

[36] Weil A 1971 Dirichlet series and automorphic forms; *Springer Lecture Notes* **189**.

[37] Wiles A 1995 Modular elliptic curves and Fermat's last theorem; *Ann. Math.* **141(2, 3)** 443–551.