Advances in Number Theory, edited by F. Q. Gouvea and N. Yui, Clarendon Press, Oxford, 1993.

A Motivated Introduction to the Langlands Program

M. Ram Murty
McGill University

Dedicated to the memory of Professor R. Sitaramachandra Rao

§1. Motivation.

This paper is partially expository and is intended as an introduction to the Langlands program for number theorists. The new theorem in the paper is that automorphic induction map for Hecke characters implies both the Artin conjecture and the Langlands reciprocity law. (See below for definitions.) In the last section, we describe some recent work with K. Murty [18] that applies the theory of base change to elliptic curves. The paper is not an exhaustive survey. We have tried to use some classical problems of number theory as motivation for discussion. For instance, we concentrate on GL_n though the functoriality conjecture predicts that this is not a limitation. Nevertheless, our discussion is sufficiently motivated from the number theoretic point of view that a non-specialist in the field can appreciate the depth and profundity of these ideas.

We begin by considering two open problems confronting number theory: Fermat's last theorem and the Sato-Tate conjecture.

First, we must understand the notion of a modular form. Let $SL_2(\mathbb{Z})$ denote the full modular group. That is,

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad : \quad a, b, c, d \in \mathbb{Z};\ ad - bc = 1 \right\}.$$

If $\mathfrak{h}$ denotes the upper half-plane, a holomorphic function $f : \mathfrak{h} \rightarrow \mathbb{C}$ is called a modular form for $SL_2(\mathbb{Z})$ of weight k if

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

and f is "holomorphic at infinity". Since $f(z+1) = f(z)$, such a function f has a Fourier expansion and the condition "holomorphic at infinity" can be stated by saying that f has a Fourier expansion of the form

Research partially supported by an NSERC grant.

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}.$$

More generally, we may consider for each natural number N, the subgroup $\Gamma_0(N)$ defined as the subgroup of matrices

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

of $SL_2(\mathbb{Z})$ satisfying $c \equiv 0(\bmod N)$. A modular form of weight k for $\Gamma_0(N)$ is defined analogously. (All rational numbers are $SL_2(\mathbb{Z})$-equivalent to $i\infty$. The $\Gamma_0(N)$ equivalence classes of rational numbers are called **cusps** for $\Gamma_0(N)$ and sometimes we refer to a representative of the class as a cusp. We require that the modular form for $\Gamma_0(N)$ be holomorphic at each of these cusps.)

Now let $A, B, C \in \mathbb{Z}$ be coprime integers such that $A + B + C = 0$ with $32|B$ and $4|(A+1)$. Let E be the curve

$$E: \qquad y^2 = x(x-A)(x+B).$$

For each prime p not dividing ABC let N_p be the number of solutions of E mod p. Define

$$a_p = p - N_p.$$

Then a classical theorem of Hasse (conjectured by E. Artin in his doctoral thesis) states that $|a_p| \leq 2\sqrt{p}$. Set

$$L_E(s) = F(s) \prod_{p \nmid ABC} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}$$

where

$$F(s) = \prod_{p|A} \left(1 - \left(\frac{B}{p}\right)\frac{1}{p^s}\right)^{-1} \prod_{p|B} \left(1 - \left(\frac{A}{p}\right)\frac{1}{p^s}\right)^{-1} \prod_{p|C} \left(1 - \left(\frac{-B}{p}\right)\frac{1}{p^s}\right)^{-1}$$

By virtue of Hasse's inequality, this infinite product converges for $\mathrm{Re}(s) > 3/2$ and so in this half-plane, we can write $L_E(s)$ as a Dirichlet series

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

This defines the a_n (which coincides with a_p when n is prime, so the notation is consistent). Define

$$N = \prod_{p|ABC} p, \qquad f_E(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}.$$

In 1955, Taniyama [32] made the astounding conjecture that $f_E(z)$ is a modular form of weight 2 for $\Gamma_0(N)$. In 1985, Frey [7] noticed that there may be a link between Taniyama's conjecture and Fermat's last theorem. This led Serre [28] to formulate more precise conjectures concerning the ramification of modular Galois representations which culminated in K. Ribet [22] proving in 1989 the following remarkable theorem:

THEOREM 1. (Ribet, 1989) Taniyama's conjecture implies Fermat's last theorem.

Taniyama's conjecture reduces to the problem of determining when a given sequence of numbers $\{a_n\}_{n=1}^{\infty}$ is the sequence of Fourier coefficients of a modular form. In 1967, A. Weil [34] answered this question in the following way. Let

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

and for each Dirichlet character χ mod c define

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{a_n \chi(n)}{n^s}.$$

Suppose that the a_n's are of polynomial growth and for each primitive character χ mod c and $(c, N) = 1$, $L(s, \chi)$ extends to an entire function and satisfies the functional equation

$$(c\sqrt{N}/2\pi)^s \Gamma(s) L(s, \chi) = w_\chi (c\sqrt{N}/2\pi)^{k-s} \chi(-N) L(k - s, \bar{\chi})$$

where w_χ is a complex number of absolute value 1. Then

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

is a modular form of weight k for $\Gamma_0(N)$.

In view of Weil's theorem, Theorem 1 reduces Fermat's last theorem to an assertion about analytic continuation of certain Dirichlet series. This is not the first time that such an event has taken place in number theory. In retrospect, we see that the introduction of the zeta function to solve problems of the distribution of prime numbers or the use of Dirichlet L-functions to describe the behaviour of primes in arithmetic progressions foreshadowed this event.

As we shall see, the Taniyama conjecture is a special case of the Langlands program which seeks to unify representation theory, number theory and arithmetic algebraic geometry. The binding link between all these diverse disciplines is the notion of an L-function of an automorphic representation and the relation between its analytic properties and the underlying algebraic structures. The L-functions of automorphic forms and automorphic representations generalise the classical zeta and L-functions of Riemann, Dirichlet and Hecke.

To further motivate our understanding, I would like to describe the Sato-Tate conjecture. Let E be an elliptic curve defined over $\mathbb{Q}$. By Hasse's inequality, we know $|a_p| \leq 2\sqrt{p}$. Let us write

$$a_p = \sqrt{p}(e^{i\theta_p} + e^{-i\theta_p}) = 2\sqrt{p}\cos\theta_p.$$

Sato and Tate independently asked the question how does θ_p vary as p varies and were led to conjecture that if the elliptic curve is not of CM type, then the θ_p's are uniformly distributed with respect to the measure

$$\frac{2}{\pi}\sin^2\theta d\theta.$$

In his McGill lectures given in 1967, Serre [27] reformulated this conjecture as follows. Let $\alpha_p = e^{i\theta_p}$ and $\beta_p = e^{-i\theta_p}$. For each m, define the L-series

$$L_m(s) = \prod_p \prod_{j=0}^{m} \left(1 - \frac{{\alpha_p}^{m-j}\beta_p^j}{p^s}\right)^{-1}.$$

Each $L_m(s)$ converges for $\mathrm{Re}(s) > 1$. Suppose that each $L_m(s)$ extends to an entire function for all $s \in \mathbb{C}$ and $L_m(1+it) \neq 0$ for all real values of t. Then, Serre [27] showed that the θ_p's are uniformly distributed with respect to the (Sato-Tate) measure $2\sin^2\theta/\pi$. In 1979, Kumar Murty [17] showed that analytic continuation of each $L_m(s)$ to $\mathrm{Re}(s) = 1$ alone suffices to imply the Sato-Tate conjecture.

Since the a_p's behave like Fourier coefficients of cusp forms of weight 2, it is reasonable to expect the same type of behaviour from Fourier coefficients of cusp forms which are eigenfunctions of Hecke operators. To illustrate, consider the Ramanujan τ function defined by the power series

$$q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n.$$

If we set $q = e^{2\pi iz}$, then the series defines a cusp form of weight 12 for the full modular group. In 1916, Ramanujan [20] conjectured that τ satisfies

(1) $\tau(nm) = \tau(n)\tau(m)$ if $(n, m) = 1$ and
(2) $|\tau(p)| \leq 2p^{11/2}$ whenever p is prime.

(1) was proved by Mordell in 1928, but he overlooked the depth of the ideas that went into his proof. Hecke [12] saw in it the theory of certain operators acting on the space of cusp forms. But (2) defied many attempts

until Deligne [4] in 1974 proved it as a consequence of his proof of the Weil conjectures. We can therefore write, in analogy with elliptic curves,

$$\tau(p) = p^{11/2}(e^{i\theta_p} + e^{-i\theta_p}) = p^{11/2}(\alpha_p + \beta_p).$$

With this notation, the series $L_m(s)$ can be analogously defined. Serre [27] conjectured that the θ_p's are uniformly distributed with respect to the Sato-Tate measure. In terms of L-functions and Kumar Murty's theorem, this means we must continue each $L_m(s)$ to the line $\mathrm{Re}(s) = 1$. If $m = 1$, $L_1(s)$ is the Mellin transform of a cusp form and so has analytic continuation by the work of Ramanujan and more generally by the work of Hecke. If $m = 2$, Rankin [21] and Selberg [26] (independently) showed in the 1940's that $\zeta(s)L_2(s)$ has an analytic continuation and satisfies a functional equation. Since the ζ-function does not vanish on the line $\mathrm{Re}(s) = 1$, it follows that $L_2(s)$ extends to an entire function to $\mathrm{Re}(s) = 1$. That in fact $L_2(s)$ extends to an entire function for all values of s was proved by Shimura [30] in 1975 by a slight modification of the Rankin-Selberg method. In 1982, Shahidi [29] showed that $L_3(s)$ and $L_4(s)$ have analytic continuation up to $\mathrm{Re}(s) = 1$. In 1985, Garrett [8] has also obtained results which imply these by another method. Their results imply

Theorem. If $L_1(s)$ has no real zeroes in $(1/2, 1)$, then $L_3(s)$ is entire.

In 1952, Gelfand and Fomin [9] showed how a modular form gives rise to a representation of $SL_2(\mathbb{R})$. Langlands' idea is to look at representations of GL_2 of the adele ring of the rational numbers. More generally, he attaches L-functions to representations of adele groups. These L-functions play a central role in the Langlands program.

2. Artin L-series and Hecke's L-series.

One can view the construction of L-series in a purely formal way. This is described by Serre [27] in his McGill lectures alluded to earlier. Let G be a compact group and μ its normalised Haar measure. Let X be the space of conjugacy classes. Suppose S is a finite set of primes and for each prime $p \notin S$, let X_p be a conjugacy class. We can ask the question of how the X_p's are distributed as p varies.

Let ρ be an irreducible representation of G and define

$$L(s,\rho) = \prod_{p \notin S} \det(1 - \rho(X_p)p^{-s})^{-1}.$$

This defines an analytic function for $\mathrm{Re}(s) > 1$. Suppose that each $L(s,\rho)$ extends to an analytic function on $\mathrm{Re}(s) = 1$ and does not vanish there. Then, the X_p's are uniformly distributed with respect to the image of the

Haar measure in X. This theorem is proved using the standard Tauberian theory.

Examples.

1. Let $\tau(p) = 2p^{11/2}\cos\theta_p$ or $a_p = 2p^{1/2}\cos\theta_p$. For each prime p, we can associate
$$\begin{pmatrix} e^{i\theta_p} & \\ & e^{-i\theta_p} \end{pmatrix} \in SU(2,\mathbb{C}).$$
Let ρ be the standard representation of $SU(2,\mathbb{C})$. Then, all irreducible representations of $SU(2,\mathbb{C})$ are $\mathrm{Sym}^m(\rho)$ and $L(s, \mathrm{Sym}^m(\rho))$ is $L_m(s)$ defined in the previous lecture. The image of the Haar measure in the space of conjugacy classes of $SU(2,\mathbb{C})$ is $2\sin^2\theta/\pi$.

2. Artin L-series. Let F be an algebraic number field and K/F be a Galois extension. For each prime ideal $\mathfrak{p}$ of F, we have the factorization
$$\mathfrak{p}O_K = \mathcal{P}_1^e \cdots \mathcal{P}_r^e,$$
where $\mathcal{P}_1$, ..., $\mathcal{P}_r$ are prime ideals of K. There is a finite set of primes S (namely the ramified primes of K) such that for $p \notin S$, the decomposition group
$$D_{\mathcal{P}} = \{\sigma \in G : \mathcal{P}^\sigma = \mathcal{P}\}$$
is cyclic. One can show that this group is canonically isomorphic to the Galois group of the extension of finite fields $O_K/\mathcal{P}$ over $O_F/\mathfrak{p}$ which is generated by $x \mapsto x^{N_{F/\mathbb{Q}}(\mathfrak{p})}$. We denote by $\sigma_{\mathcal{P}} \in D_{\mathcal{P}}$ which corresponds to this element. That is,
$$\sigma_{\mathcal{P}}(x) \equiv x^{N_{F/\mathbb{Q}}(\mathfrak{p})} (\bmod \mathcal{P})$$
for all $x \in O_K$. If $\mathcal{P}|\mathfrak{p}$, then the $\sigma_{\mathcal{P}}$ are conjugate and we denote by $\sigma_{\mathfrak{p}}$ the conjugacy class to which the $\sigma_{\mathcal{P}}$ belong. $\sigma_{\mathfrak{p}}$ is called the Artin symbol of $\mathfrak{p}$. It is a generalisation of the familiar Legendre symbol which distinguishes quadratic residues from non-residues. For each irreducible complex representation of G, $L(s,\rho)$ is called the Artin L-series attached to ρ.

Artin's conjecture. If ρ is irreducible and $\neq 1$, then $L(s,\rho)$ extends to an entire function of s.

This is one of the major unsolved problems in number theory. If ρ has degree 1, then Artin showed that his conjecture is true by showing that $L(s,\rho) = L(s,\psi)$ where ψ is a Hecke character. Hecke had already shown that such L-series $L(s,\psi)$ arise as Mellin transforms of generalised theta functions and so established their analytic continuation and functional equation. This equality is a deep statement which is called the Artin reciprocity law. In the simplest case when $F = \mathbb{Q}$ and K is a quadratic extension, the identity is equivalent to the law of quadratic reciprocity. In the general case, Brauer showed that each $L(s,\rho)$ has a meromorphic continuation for all $s \in \mathbb{C}$. This was a consequence of his induction theorem which says that every character of a finite group G can be written as an integral linear combination of monomial characters. Thus, every non-Abelian L-series can be written as a quotient of two entire functions each of which is a product of abelian L-series. Since these L-series do not vanish on the line $\mathrm{Re}(s) = 1$, we deduce immediately that the Artin symbols are uniformly distributed in G. This is the famous Chebotarev density theorem, which plays a central role in many problems of number theory. For instance, if $F = \mathbb{Q}$ and $K = \mathbb{Q}(\zeta_k)$, then $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/k\mathbb{Z})^*$ and the Artin symbol of p is $p \mod k$. Thus, we recover Dirichlet's theorem on primes in arithmetic progressions.

Brauer's theorem is essentially group theoretic in nature. By a similar argument, one can show that Artin's conjecture is true for all supersolvable groups where every irreducible character is monomial. But these are group theoretic arguments which have limitations. The natural question is what can we say about representations of degree 2. As we shall see, the Langlands program will make a precise conjecture as to what $L(s,\rho)$ should be in general. In 1975, Langlands made significant progress by proving Artin's conjecture in the "tetrahedral case" by using ideas of representation theory. More precisely, if

$$\rho : G \to GL_2(\mathbb{C}) \overset{nat}{\to} PGL_2(\mathbb{C})$$

is a 2 dimensional representation, then the image of G in $PGL_2(\mathbb{C})$ is one of five possibilities: cyclic, dihedral, A_4, S_4 or A_5. It was the case of A_4 (tetrahedral) that Langlands [14] dealt with after developing the theory of base change for GL_2. Tunnell [33] in 1982 showed the same ideas work for S_4 (the octahedral case). In his doctoral thesis, Buhler [2] showed that Artin's conjecture is true in the icosahedral case for certain cases. The general case is still open.

Artin's conjecture suggests the following question: given a sequence $\{a_n\}_{n=1}^{\infty}$, define

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

When does $L(s)$ have analytic continuation and functional equation. Hecke obtained such L-series as Mellin transforms of theta functions of several variables. These are L-series attached to grossencharactere. He also considered Mellin transforms of modular forms and showed that these series also enjoyed analytic continuation and functional equations. Let me illustrate with a concrete example. Let

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) e^{2\pi i n z}.$$

Let $SL_2(\mathbb{Z})$ be the group of matrices

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a, b, c, d \in \mathbb{Z}, \quad ad - bc = 1.$$

Then,

$$\Delta\left(\frac{az+b}{cz+d}\right) = (cz+d)^{12} \Delta(z)$$

and in particular $\Delta(-1/z) = z^{12}\Delta(z)$. Consider the Mellin transform

$$\begin{aligned}
\int_0^{\infty} \Delta(iy) y^s \frac{dy}{y} &= \int_0^{\infty} \sum_{n=1}^{\infty} \tau(n) e^{-2\pi n y} y^s \frac{dy}{y} \\
&= (2\pi)^{-s} \Gamma(s) \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s} \\
&= \int_0^1 \Delta(iy) y^s \frac{dy}{y} + \int_1^{\infty} \Delta(iy) y^s \frac{dy}{y} \\
&= \int_1^{\infty} \Delta(i/y) y^{-s} \frac{dy}{y} + \int_1^{\infty} \Delta(iy) y^s \frac{dy}{y}
\end{aligned}$$

from which we get analytic continuation and functional equation upon using the modular relation.

To describe Hecke theory in some more detail, let $\mathfrak{h}$ denote the upper half plane. Let $GL_2^+(\mathbb{R})$ denote the non-singular 2×2 matrices with positive determinant. $GL_2^+(\mathbb{R})$ acts on $\mathfrak{h}$. Consider Γ, a congruence subgroup of $SL_2(\mathbb{Z})$. That is, $\Gamma \supseteq \Gamma(N)$ where

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv I(\bmod N) \right\}$$

for some natural number N. For example, Hecke's group

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad c \equiv 0(\bmod N) \right\}$$

a congruence subgroup. Define $j(g, z) = (cz + d)(\det g)^{-1/2}$ for all $g \in GL_2^+(\mathbb{R})$ and

$$g = \begin{pmatrix} * & * \\ c & d \end{pmatrix}.$$

Set

$$(f|_k \sigma)(z) = j(\sigma, z)^{-k} f(\sigma z)$$

for all positive integers k. A fundamental domain $\mathfrak{F}$ for Γ is any connected set in $\mathfrak{h}$ such that no two interior points of $\mathfrak{F}$ are Γ equivalent and every point in $\mathfrak{h}$ is equivalent to some point in $\mathfrak{F}$. For example, for $\Gamma = SL_2(\mathbb{Z})$, it is easy to see that a fundamental domain is $\mathfrak{F} = \{z = x + iy : \quad -1/2 \le x \le 1/2, \quad |z| \ge 1\}$ because $SL_2(\mathbb{Z})$ is generated by

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

For an arbitrary Γ, a fundamental domain is easily derived from this one as follows. Let $\gamma_1, \gamma_2 ...$ be the left coset representatives of Γ in $SL_2(\mathbb{Z})$. Then a fundamental domain for Γ is $\cup_i \gamma_i^{-1}\mathfrak{F}$.

A **cusp** for Γ is an element of $\mathbb{Q} \cup \{i\infty\}$ which is fixed by an element of trace ± 2. In the case of $SL_2(\mathbb{Z})$, $i\infty$ is the only cusp up to equivalence. Let $\mathfrak{h}^* = \mathfrak{h} \cup \text{cusps of } \Gamma$. Then, $\Gamma\backslash\mathfrak{h}^*$ has a complex analytic structure of a Riemann surface. We also identify this with a fundamental domain of Γ.

An **automorphic form** for Γ of weight k is a complex valued function f on $\mathfrak{h}$ such that

(1) $f|_k\gamma = f$ for all $\gamma \in \Gamma$,

(2) f is holomorphic on $\mathfrak{h}^*$.

A **cusp form** for Γ is an automorphic form which vanishes at all the cusps of Γ. Let $M_k(\Gamma)$ denote the space of modular forms for Γ and $S_k(\Gamma)$ the space of cusp forms. For $SL_2(\mathbb{Z})$, dim $M_k(\Gamma)$ = dim $S_k(\Gamma) + 1$ where the term $+1$ arises from the subspace spanned by the Eisenstein series:

$$E_k(z) = \sum_{(m,n)\neq(0,0)} (mz+n)^{-k}.$$

In the general case for k even and $k > 2$, dim $M_k(\Gamma)$ - dim $S_k(\Gamma)$ is equal to the number of inequivalent cusps of Γ so that there is an Eisenstein series attached to each cusp. The space of cusp forms is an inner product space where the inner product is defined by

$$(f,g) = \int\int_{\Gamma\backslash\mathfrak{h}^*} f(z)\overline{g(z)}y^k \frac{dxdy}{y^2}.$$

Hecke's First theorem. Let $f \in S_k(\Gamma_0(N))$ and write

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

for its Fourier expansion at $i\infty$. Then,

$$L(s,f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

has an analytic continuation and functional equation relating $L(s,f)$ and $L(s, f|w_N)$ where $w_N = \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}$.

The Artin conjecture for 2-dimensional Galois representations can now be reformulated and made more precise. Every 2-dimensional Artin L-series is the Mellin transform of a cusp form of weight 1 on $\Gamma_0(N)$ for some natural number N. This can be viewed as the "2-dimensional reciprocity law".

Hecke was led to ask which $L(s, f)$ have Euler product expansions because only these will correspond to Artin L-series. He defined certain linear operators (called Hecke operators) on the space $S_k(\Gamma)$ and showed that if f is an eigenfunction of these operators, then $L(s, f)$ has an Euler product. Such f's are called eigenforms. In 1976, Deligne and Serre showed that for each eigenform of weight one on $\Gamma_0(N)$ of "odd type", there is a 2-dimensional Galois representation ρ_f over $\mathbb{Q}$ such that $L(s, \rho_f) = L(s, f)$.

3. Hecke operators.

Let $\Gamma = \Gamma_0(N)$ and let $S_k(\Gamma)$ be the space of cusp forms of Γ of weight k. Define operators

$$T_p(f) = p^{k-1} f(pz) + \frac{1}{p} \sum_{b \bmod p} f(\frac{z+b}{p})$$

where $p \nmid N$ is a prime. Then, T_p is a linear operator on $S_k(\Gamma)$.

Hecke's Second Theorem. Let

$$f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}, \qquad a_1 = 1.$$

The a_n's are multiplicative if and only if f is an eigenfunction of all the T_p's. In this case, $L(s, f)$ has an Euler product of the form

$$L(s, f) = \prod_{p \nmid N} \left(1 - \frac{a_p}{p^s} + \frac{1}{p^{2s+1-k}}\right)^{-1} \prod_{p \mid N} \left(1 - \frac{a_p}{p^s}\right)^{-1}$$

Another way of thinking about the T_p's is via double cosets. Let

$$\Gamma \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma = \cup \Gamma \gamma_i .$$

The γ_i can be taken to be

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} \qquad b \bmod p.$$

It is then easily verified that

$$T_p(f) = \sum_i f|\gamma_i .$$

This interpretation will be useful in later generalizations.

4. Modular forms as representations of $SL_2(\mathbb{R})$.

In 1952, Gelfand and Fomin [9] noticed that cusp form of $S_k(\Gamma)$ define representations of $SL_2(\mathbb{R})$ in the following way. In $SL_2(\mathbb{R})$, let

$$N = \{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\}, \quad A = \{\begin{pmatrix} a & \\ & a^{-1} \end{pmatrix}\},$$

$$K = \{\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = R_\theta : 0 \leq \theta \leq 2\pi\}.$$

Then, $SL_2(\mathbb{R}) = NAK$ (Iwasawa decomposition).

If G is any group acting transitively on a set S, then S can be identified with the coset space G/Γ_x where Γ_x is the stabilizer of any $x \in S$. Since $SL_2(\mathbb{R})$ acts transitively on $\mathfrak{h}$, and $\Gamma_i = K$, we can identify the upper half plane with $SL_2(\mathbb{R})/K$. Thus, elements of $SL_2(\mathbb{R})$ can be thought of as pairs (z, θ) with $z \in \mathfrak{h}$. Let $G = SL_2(\mathbb{R})$. Define for $g \in G$ and $f \in S_k(\Gamma)$,

$$\phi_f(g) = j(g, i)^{-k} f(g \cdot i).$$

This satisfies

(1) $\phi(\gamma g) = \phi(g)$ for all $\gamma \in \Gamma$,
(2) $\phi(gR_\theta) = e^{-ik\theta}\phi(g)$,
(3) $\int_{\Gamma\backslash G} |\phi(g)|^2 dg < \infty$,
(4) for all $\rho \in SL_2(\mathbb{Z})$, and all $g \in G$,

$$\int_{\mathbb{Z}\backslash\mathbb{R}} \phi\left(\rho \begin{pmatrix} 1 & xh \\ 0 & 1 \end{pmatrix} g\right) dx = 0$$

where h is the "width" of the cusp $\rho(i\infty)$.

Define the Laplace operator on G

$$\Delta = -y^2 \left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right) - y\frac{\partial^2}{\partial x \partial \theta}.$$

Then ϕ_f satisfies

(5') $\Delta\phi_f = -k(k-2)\phi_f/4$.

Theorem. Any function $\phi \in L^2(\Gamma\backslash G)$ satisfying (1) - (4) and (5') is necessarily a ϕ_f for some $f \in S_k(\Gamma)$.

If we replace (5') by

(5) ϕ is an eigenfunction of Δ

we get real analytic forms in addition to holomorphic forms. Such forms were first studied by Maass and are called Maass wave forms. They have a Fourier expansion of the type

$$f(z) = \sum_n a_n e^{2\pi i n x} \sqrt{y} K_{ir}(2\pi |n| y)$$

where $r^2 + 1/4$ is an eigenvalue of

$$-y^2 \left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} \right)$$

and

$$K_v(z) = \int_0^\infty e^{-z \cosh t} \cosh vt \, dt$$

is the Bessel function. Connected with these eigenvalues is the famous conjecture of Selberg that predicts that if $\lambda = r^2 + 1/4$ is an eigenvalue for $\Gamma_0(N)$, then $\lambda \geq 1/4$. This is equivalent to saying that r cannot be purely imaginary. This conjecture is known if $\Gamma = SL_2(\mathbb{Z})$. Selberg [26] showed that $\lambda \geq 3/16$ for $\Gamma_0(N)$. Iwaniec and Selberg have noted that there are arithmetic applications of this conjecture.

Let $L^2(\Gamma \backslash G/K) = V$ be the vector space of square integrable, left-invariant by Γ and right K-invariant functions on G. Define the right regular representation of G by

$$(R(g) \cdot \phi)(h) = \phi(hg).$$

Then, $\Delta R = R\Delta$. Thus, irreducible representations occurring in R coincide with eigenfunctions of Δ. (We are ignoring certain growth conditions.) These ideas can be generalised to $GL_n(\mathbb{R})$.

5. $GL_n(\mathbb{R})$.

Let $K = O_n(\mathbb{R})$ be the orthogonal group, Z the group of scalar matrices. Let $\Gamma = GL_n(\mathbb{Z})$. The analog of the upper half plane is the symmetric space

$$\mathcal{H} = \Gamma \backslash GL_n(\mathbb{R})/KZ.$$

Every element of G/KZ can be written as a product

$$g = \begin{pmatrix} 1 & x_{12} & \cdots & \cdots & x_{1n} \\ & 1 & x_{23} & \cdots & x_{2n} \\ & \cdots & \cdots & \cdots & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} y_1 y_2 \cdots y_n & & & & \\ & y_2 \cdots y_n & & & \\ & & \cdots & \cdots & \\ & & & y_{n-1} & \\ & & & & 1 \end{pmatrix}.$$

For example, if $n = 2$,

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$$

corresponds to $x + iy \in \mathfrak{h}$.

We will consider functions satisfying

(1) $\phi(\gamma g) = \phi(g)$ for all $\gamma \in \Gamma$.
(2) ϕ is square integrable,
(3) ϕ should be an eigenfunction of $n-1$ "Laplacians". More precisely, if $\mathcal{D}$ is algebra of G-invariant differential operators, it is isomorphic to a polynomial ring of rank $n-1$. We require $D\phi = \rho(D)\phi$ for all $D \in \mathcal{D}$.

If these conditions are satisfied by ϕ in addition to the following growth condition

(4) $|\phi(g)| \le C(y_1 \cdots y_{n-1})^A$

then we say that ϕ is an automorphic form for G. An automorphic form is called **cuspidal** if

(5) $\int \phi\left(\begin{pmatrix} I & X \\ 0 & I \end{pmatrix} g\right) dx = 0$ for all $g \in G$ and X is an $n_1 \times n_2$ matrix with $n_1 + n_2 = n$.

(This definition is due to Gelfand.)

One can equally well develop the theory of Hecke operators. Let

$$\xi(p, i) = \begin{pmatrix} pI_i & \\ & I_{n-i} \end{pmatrix}.$$

Let

$$\Gamma\xi(p, i)\Gamma = \cup \Gamma\gamma_{p,i,v}$$

be a double coset decomposition. Define the Hecke operator $T_{p,i}$ by

$$(T_{p,i}\phi)(g) = \sum_v \phi(g\gamma_{p,i,v}).$$

If ϕ is an eigenfunction for all Hecke operators $T_{p,i}$, we will write

$$T_{p,i}\phi = \lambda_{p,i}p^{i(n-i)}\phi, \quad 1 \le i \le n.$$

Define for such a ϕ,

$$L(s, \phi) = \prod_p \left(1 - \lambda_{p,1}p^{-s} + \lambda_{p,2}p^{-2s} + \cdots \pm \lambda_{p,n}p^{-ns}\right)^{-1}.$$

One has the contragredient form $\tilde{\phi}$ defined by $\tilde{\phi}(g) = \phi({}^{\iota}g)$ where

$${}^{\iota}g = w\,{}^{t}g^{-1}w$$

and

$$w = \begin{pmatrix} & & & -1 \\ & & -1 & \\ & \cdots & & \\ -1 & & & \end{pmatrix}.$$

Then, it is known that:

Theorem. $L(s, \phi)$ has an analytic continuation and functional equation relating $L(s, \phi)$ to $L(s, \tilde{\phi})$ where $\tilde{\phi}$ is the contragredient automorphic form.

These L-functions are related to the ones described previously in the case $n = 1$ (Hecke L-series attached to grossencharactere) and $n = 2$ (Hecke L-series attached to modular forms or L-series attached to Maass wave forms).

Langlands has formulated a strong reciprocity conjecture: every Artin L-series $L(s, \rho)$ is an $L(s, \phi)$ for some automorphic form ϕ on $GL_r(\mathbb{R})$, where $r = \deg \rho$. The truth of this conjecture implies Artin's conjecture in view of the Theorem above. With reference to the Sato-Tate conjecture, it is also conjectured that $L_m(s)$ should be $L(s, \phi)$ for some automorphic form ϕ on $GL_{m+1}(\mathbb{R})$. Again, such a reciprocity conjecture would imply the Sato-Tate conjecture. One can also show that Selberg's eigenvalue conjecture and Ramanujan conjectures also follow from this reciprocity. Thus, reciprocity is the problem of converse theory (that is generalisation of Weil's theorem) to higher GL_n.

6. Adeles and ideles.

For $x \in \mathbb{Q}$, put $v_p(x) = \operatorname{ord}_p(x)$. Then,

(1) $v_p(x+y) \geq \min(v_p(x), v_p(y))$,

(2) $v_p(xy) = v_p(x) + v_p(y)$,

(3) $v_p(0) = \infty$.

Define a metric on $\mathbb{Q}$ by $|x-y|_p = e^{-v_p(x-y)}$. Denote by $\mathbb{Q}_p$ the completion of $\mathbb{Q}$ with respect to this p-adic metric. We call $\mathbb{Q}_p$ the p-adic number field. Let $\mathbb{Z}_p$ be the subring of p-adic integers. Every p-adic number x can be written uniquely as

$$x = \sum_{i=-N}^{\infty} a_i p^i, \qquad a_i \in \{0, 1, \ldots, p-1\}.$$

We will say that two metrics are equivalent if they induce the same topology on $\mathbb{Q}$. We have the famous:

Theorem. (Ostrowski) Up to equivalence, the only metrics on $\mathbb{Q}$ are $|\cdot|_p$ and $|\cdot|_\infty$ (the usual absolute value).

A similar result holds for any algebraic number field. Metrics which do not correspond to a finite prime (ideal) are called Archimedean valuations (or infinite primes). Thus, for a number field K, we can consider analogously K_v the field of v-adic numbers and the ring O_v of v-adic integers.

Consider the following problem: what are the characters of the additive group of rational numbers $\mathbb{Q}$?

We can write down some obvious ones: given $\alpha \in \mathbb{R}$, let $\chi_\alpha(x) = e^{2\pi i \alpha x}$. If $\beta \in \mathbb{Q}_p$, then $\beta = \sum_{i=-N}^{\infty} a_i p^i$. Let $\tilde{\beta} = \sum_{i=-N}^{-1} a_i p^i$ be the "fractional part" of β. Define $\chi_\beta(x) = e^{2\pi i \tilde{\beta} x}$ is also a character of $\mathbb{Q}$. It turns out that all characters of $\mathbb{Q}$ are finite products of such characters. To state this neatly, we can say every character of $\mathbb{Q}$ is given by a sequence

$$a = (a_\infty, a_2, a_3, a_5, \ldots)$$

where $a_\infty \in \mathbb{R}$ and $a_p \in \mathbb{Q}_p$ and $a_p \in \mathbb{Z}_p$ for all p sufficiently large. Such a sequence is called an **adele**. Defining componentwise addition and multiplication, we see that the set of all adeles is a ring, called the adele ring of $\mathbb{Q}$ and denoted $\mathbb{A}_\mathbb{Q}$ or simply $\mathbb{A}$. Hence, for $a \in \mathbb{A}_\mathbb{Q}$ we set

$$\chi_a(x) = e^{2\pi i(a_\infty x + a_2 x + \cdots)}$$

then every character of $\mathbb{Q}$ is of this form. Is this a one-one correspondence? It turns out to be not. It is a simple exercise to show that two characters χ_a and χ_b are equal if and only if $a - b = (x, x, x, \ldots)$ for some rational number x. Thus, we can view $\mathbb{Q}$ as a subgroup of $\mathbb{A}_\mathbb{Q}$ embedded diagonally in this way. Then we have:

Theorem. The character group of $\mathbb{Q}$ is isomorphic to $\mathbb{A}_\mathbb{Q}/\mathbb{Q}$ as an abstract group.

Since $\mathbb{Q}$ has a natural topology on it, one can ask whether this isomorphism can be made as topological groups. For this purpose, it is necessary to define a topology on $\mathbb{A}_\mathbb{Q}$ so as to have this. To this end, we begin by putting the product topology on

$$\mathbb{A}^0 = \mathbb{R} \times \prod_p \mathbb{Z}_p$$

and declaring that $\mathbb{A}^0$ is an open neighbourhood of 0. Thus, a sequence of adeles $a^{(n)} = (a_\infty^{(n)}, a_2^{(n)}, \cdots)$ tends to zero if and only if $a_p^{(n)}$ tends to zero and $a_p \in \mathbb{Z}_p$ for all n sufficiently large. Thus, this is stronger than the product topology. Thus, the adele ring with this topology is the restricted direct product

$$\mathbb{A} = \prod_p (\mathbb{Q}_p : \mathbb{Z}_p).$$

In general, if K is a number field, the adele ring $\mathbb{A}_K$ is the restricted direct product

$$\mathbb{A}_K = \prod_v (K_v : O_v).$$

If G is a linear algebraic group, we can define topological group of its adelic points by the restricted direct product

$$G(\mathbb{A}_K) = \prod_v (G(K_v) : G(O_v)).$$

$\mathbb{A}_K$ becomes locally compact topological group and as such has a Haar measure on it. A similar result holds for $G(\mathbb{A})$. In the course of this paper, we will be interested in $G = GL_n$. If $G = GL_1$, then $G(K)\backslash G(\mathbb{A}_K)$ is called **the idele class group of** K.

7. Automorphic representations of adele groups.

Let Z be the group of scalar adeles and consider the vector space

$$V = L^2(ZG(\mathbb{Q})\backslash G(\mathbb{A}_{\mathbb{Q}}).$$

We will be interested in irreducible unitary representations of $G(\mathbb{A})$. Every such representation π factors as a restricted tensor product:

$$\pi = \otimes_p \pi_p$$

where π_p is an irreducible unitary representation of $G(\mathbb{Q}_p)$. In case $G = GL_1$, these are Hecke's grossencharactere. In case $G = GL_2$, every irreducible unitary representation arises from either a modular form or a Maass wave form. Our goal will be to attach an L-function to such a representation π. There is a finite set S of primes (namely the ramified primes of π) such that for each prime $p \notin S$, we can associate a conjugacy class A_p in $GL_n(\mathbb{C})$. The exact assignment needs more background (see [15]) which we will not discuss here. Suffice it to say that in case f is a Hecke eigenform, and π_f is the corresponding automorphic representation, then $\pi_{f,p}$ is associated to $\begin{pmatrix} \alpha_p & \\ & \beta_p \end{pmatrix}$ with notation as in §1.

$G(\mathbb{A})$ acts on $L^2(ZG(\mathbb{Q})\backslash G(\mathbb{A}))$ by right translation:

$$(R(g) \cdot \phi)(x) = \phi(xg).$$

An automorphic representation is an irreducible constituent of R. (Cuspidal automorphic representations form a subspace corresponding to cusp forms.)

Let K be a number field and π an automorphic representation of $G(\mathbb{A}_K)$. Let A_v be the conjugacy class attached to π_v. Define

$$L(s, \pi_v) = \det(1 - A_v N v^{-s})^{-1}$$

for non-Archimedean valuations. Set

$$L_S(s, \pi) = \prod_{v \notin S} L(s, \pi_v).$$

Theorem. $L_S(s, \pi)$ has an analytic continuation and at the places $v \in S$, $L(s, \pi_v)$ can be defined so that the global L-function $L(s, \pi)$ has a functional equation.

This theorem, for $n = 1$ is the theory of Hecke's L-series attached to grossencharacter and Tate, who formulated it adelically in his doctoral thesis. For $n = 2$, it is due to Hecke, Maass and the final adelic formulation is the work of Jacquet and Langlands [13]. The general case for GL_n is due to Godement and Jacquet. A good write up for the Jacquet-Langlands theory is found in Robert [23].

In this adelic framework, Langlands conjectures that every Artin L-series $L(s, \rho)$ is and $L(s, \pi)$ for some automorphic representation π on $GL_n(\mathbb{A}_K)$ where $n = \deg \rho$. Thus, to each ρ there should be an automorphic representation $\pi(\rho)$. In case $\deg \rho = 1$, this is Artin's reciprocity law since Hecke's grossencharactere are automorphic representations of $GL_1(\mathbb{A})$. We have already discussed the situation if $\deg \rho = 2$.

To make further progress, we must clarify the converse problem and resolve it. Namely, given a Dirichlet series

$$L(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

when is $L(s) = L(s, \pi)$ for some automorphic representation π of $GL_n(\mathbb{A})$. Weil's theorem is an incomplete converse theorem for GL_2 in that it applies to only modular forms. Jacquet-Langlands [13] filled this gap to cover Maass forms as well and generalised to an arbitrary number field. Thus the analog of Weil's theorem holds for GL_2. For GL_3, Gelbart, Jacquet and Piatetski-Shapiro proved an analogous result. However, it was already shown by Piatetski-Shapiro [19] that for GL_4, one needs to twist by not just abelian characters but all 2-dimensional representations and establish analytic continuation and functional equations of the right type before one can conclude that $L(s) = L(s, \pi)$ for some automorphic representation π on $GL_4(\mathbb{A})$. In general, one expects to twist by all representations of degree $d \leq m - 2$ before we can conclude that π lives on $GL_m(\mathbb{A})$. To establish continuation and functional equations, one needs the Rankin-Selberg method.

8. The Rankin-Selberg method.

Recall that the problem of the Sato-Tate conjecture was equivalent to the problem of analytic continuation of $L_m(s)$ to the line $\mathrm{Re}(s) = 1$. $L_1(s)$ was treated by Hecke. We have mentioned that $\zeta(s)L_2(s)$ was shown to extend to a meromorphic function with only a simple pole at $s = 1$ by Rankin and Selberg (independently) in the 1940's. Their idea is fundamental in understanding the mechanism of converse theory so we will describe this in some detail. I will illustrate it for the full modular group $SL_2(\mathbb{Z})$.

Suppose that $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ and $g(z) = \sum_{n=1}^{\infty} b_n e^{2\pi i n z}$ are two cusp forms of weight k for the full modular group. (Weaker assumptions on f and g still lead to the same results but then, our exposition will be bogged down by unnecessary technical details.) Define the Eisenstein series

$$E(z,s) = \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} Im(\gamma z)^s$$

where

$$\Gamma_\infty = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}.$$

Note that

$$y^k f(z)\overline{g(z)}$$

is $SL_2(\mathbb{Z})$-invariant. Consider

$$\int\int_{\Gamma\backslash\mathfrak{h}} y^k f(z)\overline{g(z)} E(z,s) \frac{dxdy}{y^2}.$$

Inserting the definition of $E(z,s)$ as a sum and interchanging the sum and integration we get

$$\sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \int\int_{\Gamma\backslash\mathfrak{h}} (\operatorname{Im}(\gamma y))^k f(\gamma z)\overline{g(\gamma z)} (\operatorname{Im}(\gamma z))^s \frac{dxdy}{y^2}$$
$$= \sum_{\gamma \in \Gamma_\infty \backslash \Gamma} \int\int_{\Gamma\backslash\mathfrak{h}} y^k f(z)\overline{g(z)} y^s \frac{dxdy}{y^2}$$
$$= \int\int_{\Gamma_\infty\backslash\mathfrak{h}} y^k f(z)\overline{g(z)} y^s \frac{dxdy}{y^2}$$

because

$$\Gamma_\infty \backslash \mathfrak{h} = \cup_{\gamma \in \Gamma_\infty \backslash \Gamma} \gamma(\Gamma\backslash\mathfrak{h})$$

which can be taken to be the region $-1/2 \le x \le 1/2,\ y > 0$. Thus, the above is

$$= \int_0^\infty \int_{-1/2}^{1/2} y^k f(z)\overline{g(z)} y^s \frac{dxdy}{y^2}$$
$$= \int_0^\infty y^{k+s} \sum_{n,m} a_n \overline{b_m} e^{-2\pi(n+m)y} \int_{-1/2}^{1/2} e^{2\pi i(n-m)x} dx \frac{dy}{y^2}$$
$$== \int_0^\infty \sum_{n=1}^\infty a_n \overline{b_n} y^{k+s} e^{-4\pi n y} \frac{dy}{y^2}$$
$$= (4\pi)^{k+s+1} \Gamma(k+s+1) \sum_{n=1}^\infty \frac{a_n \overline{b_n}}{n^s}.$$

It is known that

$$E^*(z,s) = \zeta(2s)E(z,s)$$

has an analytic continuation except for a simple pole at $s = 1$ and satisfies a functional equation relating the value at s to the value at $1-s$. Therefore, from this integral representation, we obtain the analytic continuation of the series

$$\sum_{n=1}^{\infty} \frac{a_n \overline{b_n}}{n^s}.$$

Now suppose that f and g are Hecke eigenforms. That is, a_n and b_n are multiplicative. Our goal is to write the above Dirichlet series as an Euler product. Let us write

$$a_p = 2p^{(k-1)/2}(\alpha_p + \beta_p), \quad b_p = 2p^{(k-1)/2}(\gamma_p + \delta_p).$$

Let $\tilde{a_n} = a_n/n^{(k-1)/2}$ and $\tilde{b_n} = b_n/n^{(k-1)/2}$. It is not difficult to show that

$$\tilde{a_{p^n}} = \frac{\alpha_p^{n+1} - \beta_p^{n+1}}{\alpha_p - \beta_p}$$

and a similar formula holds for $\tilde{b_{p^n}}$ whenever p is prime. Then,

$$\sum_{n=1}^{\infty} \frac{\tilde{a_n}\tilde{b_n}}{n^s} = \prod_p \left(\sum_{n=1}^{\infty} \left(\frac{\alpha_p^{n+1} - \beta_p^{n+1}}{\alpha_p - \beta_p} \right) \left(\frac{\gamma_p^{n+1} - \delta_p^{n+1}}{\gamma_p - \delta_p} \right) p^{-ns} \right).$$

Now we invoke Ramanujan's identity:

$$\sum_{n=1}^{\infty} \left(\frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \right) \left(\frac{\gamma^{n+1} - \delta^{n+1}}{\gamma - \delta} \right) T^n =$$

$$= \frac{1 - \alpha\beta\gamma\delta T^2}{(1-\alpha\gamma T)(1-\alpha\delta T)(1-\beta\gamma T)(1-\beta\delta T)}.$$

Thus, we get the product equal to

$$\zeta(2s)^{-1} \prod_p \left(1 - \frac{\alpha_p\gamma_p}{p^s}\right)^{-1} \left(1 - \frac{\alpha_p\delta_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p\gamma_p}{p^s}\right)^{-1} \left(1 - \frac{\beta_p\delta_p}{p^s}\right)^{-1}.$$

This is precisely $L(s, \pi_f \otimes \pi_g)$ in the notation of the Langlands' L-function. We have therefore

$$L(s, \pi_f \otimes \pi_g) = \int_{\Gamma\backslash\mathfrak{H}} y^k f(z) g(z) E^*(z,s) \frac{dx\,dy}{y^2}.$$

If we let $f = g$, we get

$$L(s, \pi_f \otimes \pi_f) = \zeta(s) L_2(s)$$

since $\pi \otimes \pi = \mathrm{Alt}(\pi) \oplus \mathrm{Sym}^2(\pi)$. Since the zeta function does not vanish on the line $\mathrm{Re}(s) = 1$, this gives the analytic continuation of $L_2(s)$ until this line.

Though we have not mentioned it explicitly, the above construction is a special case of a more general construction of Langlands of L-functions attached to the tensor product of two automorphic representations. Indeed, Gelbart, Jacquet and Piatetski-Shapiro [11] showed that $L(s, \pi_1 \otimes \pi_2)$ has analytic continuation and functional equation except when π_2 is the contragredient of π_1 in which case it has a simple pole at $s = 1$.

The method however does not give the continuation of $L_2(s)$ for all values of s. This was done by Shimura [30] by making an ingenious observation. He noticed that $L_2(s)$ is essentially

$$\sum_{n=1}^{\infty} \frac{a_{n^2}}{n^s}$$

and so this should be obtained by taking the Rankin-Selberg convolution of f with the classical theta function (which is a modular form of half integral weight). He was able to show that the theory extends to such a situation and obtained an integral representation

$$\sum_{n=1}^{\infty} \frac{a_{n^2}}{n^s} = (fudge\ factor) \int_{\Gamma_0(4)\backslash \mathfrak{h}} y^{k+1/2} f(z)\overline{\theta(z)} E_{\Gamma_0(4)}(z, s) \frac{dxdy}{y^2}$$

where $E_{\Gamma_0(4)}(z, s)$ is a half-integral weight Eisenstein series belonging to $\Gamma_0(4)$. Therefore, we obtain the analyticity of $L_2(s)$.

But can we establish Langlands' conjecture for $L_2(s)$, namely that it is an L-series attached to an automorphic representation of GL_3 ? As mentioned earlier, Gelbart and Jacquet proved a converse theorem for GL_3 which requires twisting our original series by Dirichlet characters. The method of Shimura extends to give analytic continuation and functional equations for all these twists and so Gelbart and Jacquet were able to prove Langlands' conjecture for $L_2(s)$. We state their theorem more precisely:

Theorem. If π is an irreducible unitary automorphic representation of $GL_2(\mathbb{A}_K)$, then the map $\pi \mapsto \mathrm{Sym}^2(\pi)$ (Gelbart-Jacquet lift) is a map into irreducible unitary automorphic representations on $GL_3(\mathbb{A}_K)$.

For further discussion, let us introduce the notation $\mathcal{A}(GL_n)$ to denote the space of irreducible unitary automorphic representations of $GL_n(\mathbb{A}_K)$. With the information at hand, we can take Rankin-Selberg convolutions:

$$\pi \otimes \mathrm{Sym}^2(\pi) = \pi \oplus \mathrm{Sym}^3(\pi)$$
$$\mathrm{Sym}^2(\pi) \otimes \mathrm{Sym}^2(\pi) = 1 \oplus \mathrm{Sym}^2(\pi) \oplus \mathrm{Sym}^4(\pi).$$

From the first equation, we deduce that $L_3(s)$ is analytic for $\mathrm{Re}(s) \geq 1$ upon showing that $L(s, \pi)$ does not vanish on this line. This is a minor modification of the classical argument of Hadamard and de la Vallée

Poussin. The second equation shows that $L_4(s)$ is analytic for $\mathrm{Re}(s) \geq 1$ by a similar process. If we can consider $\mathrm{Sym}^2(\pi) \otimes \mathrm{Sym}^3(\pi)$ then we would obtain information on $L_5(s)$. This however we cannot do because we do not know that $\mathrm{Sym}^3(\pi) \in \mathcal{A}(GL_4)$. We need a converse theorem for GL_4.

Piatetski-Shapiro showed that the analog of Weil's theorem does not hold for GL_4 and we need the analyticity of additional twists. It turns out that these additional twists are representations of GL_2. Thus, the converse theory for GL_4 requires analytic continuations of $L(s, \phi \otimes \pi)$ as π ranges over $\mathcal{A}(GL_2)$. It is in this context that the result of Paul Garrett [8] in 1985 on triple convolutions was intriguing. (We shall see later other reasons for the intrigue.) Namely, Garrett [8] showed that if f, g and h are modular cusp forms of weight k, with Fourier coefficients a_n, b_n and c_n respectively, then

$$\sum_{n=1}^{\infty} \frac{a_n b_n c_n}{n^s}$$

can be written as an integral transform of Rankin-Selberg type and an analytic continuation can be obtained for it. In the notation of Langlands, this corresponds to $L(s, \pi_f \otimes \pi_g \otimes \pi_h)$, an L-function attached to $GL_2 \times GL_2 \times GL_2$. In the context of converse theory, this result implies that we will have a map

$$\mathcal{A}(GL_2) \times \mathcal{A}(GL_2) \rightarrow \mathcal{A}(GL_4).$$

From this, we would obtain the analytic continuation of $L_5(s), L_6(s), L_7(s)$ and $L_8(s)$ up to $\mathrm{Re}(s) = 1$. At the end of this paper, we will see another fundamental reason for the interest in this map.

For the general converse theory on GL_n, one needs to twist by representations of GL_{n-2} though this has not been formally written up. There are informal notes of Piatetski-Shapiro which prove this theorem for function fields.

9. Base change and automorphic induction.

Let K/k be a Galois extension and let $G = \mathrm{Gal}(K/k)$. If ρ is an irreducible representation of G, then $L(s, \rho, K/k)$ was conjectured by Artin to be entire if $\rho \neq 1$. We can extend the definition of Artin L-series to an arbitrary representation of G by additivity:

$$L(s, \rho_1 \oplus \rho_2, K/k) = L(s, \rho_1, K/k) L(s, \rho_2, K/k).$$

If now ψ is a representation of a subgroup H of G, then $L(s, \psi, K/K^H)$ is the Artin L-series belonging to the extension K/K^H where K^H denotes the field fixed by H. A simple calculation shows that Artin L-series are invariant under induction:

$$L(s, \mathrm{Ind}_H^G \psi, K/k) = L(s, \psi, K/K^H).$$

This last property implies a corresponding property for L-series attached to automorphic representations. Recall the Langlands' reciprocity conjecture: for each ρ, there is $\pi(\rho) \in \mathcal{A}(GL_n(\mathbb{A}_K))$ so that

$$L(s, \rho, K/k) = L(s, \pi).$$

The natural question is, how does the map $\rho \mapsto \pi(\rho)$ behave under restriction to a subgroup? By the reciprocity conjecture, we should have $\rho|_H \mapsto \pi(\rho|_H) \in \mathcal{A}(GL_n(\mathbb{A}_{K^H}))$. What is $L(s, \rho|_H, K/K^H)$? A standard group theoretic result is

$$\mathrm{Ind}_H^G(\rho|_H \otimes \psi) = \rho \otimes \mathrm{Ind}_H^G \psi.$$

Thus,

$$L(s, \mathrm{Ind}_H^G(\rho|H \otimes \psi), K/k) = L(s, \rho \otimes \mathrm{Ind}_H^G \psi, K/k).$$

But the former L-function is $L(s, \rho|_H \otimes \psi, K/K^H)$ by the invariance of Artin L-series. Therefore,

$$L(s, \rho|_H, K/K^H) = L(s, \rho \otimes \mathrm{Ind}_H^G 1, K/k).$$

But $\mathrm{Ind}_H^G 1 = reg_{G/H}$ is the permutation representation on the cosets of H. This suggests that we make the following definition. Let $\pi \in \mathcal{A}(GL_n(\mathbb{A}_K))$. For each π_v, we associated an $A_v \in GL_n(\mathbb{C})$. Define,

$$L_v(s, B(\pi)) = \det(1 - A_v \otimes reg_{G/H}(\sigma_v) Nv^{-s})^{-1},$$

where σ_v is the Artin symbol of v. Set

$$L(s, B(\pi)) = \prod_v L_v(s, B(\pi)).$$

$B(\pi)$ should correspond to an element of $\mathcal{A}(GL_n(A_M))$ where $M = K^H$. The problem of base change is to determine when this map exists.

For $n = 2$, this was done by Langlands [14] when M/k is cyclic. He then used these ideas to deal with the tetrahedral case of Artin's conjecture. For arbitrary n, it is the recent work of Arthur and Clozel [1] Again, the situation is for M/k cyclic.

Now suppose the ψ is a representation of H. Corresponding to ψ there should be a $\pi \in \mathcal{A}(GL_n(\mathbb{A}_M))$ where $n = deg\,\psi$. But the invariance of

Artin L-series under induction implies that there should be an $I(\pi) \in \mathcal{A}(GL_{nr}(\mathbb{A}_k))$ $(r = [G:H])$ so that

$$L(s, I(\pi)) = L(s, \operatorname{Ind}_H^G \psi, K/k).$$

This map $\pi \mapsto I(\pi)$, called the automorphic induction map, is conjectured to exist. Again, Arthur and Clozel showed this exists when M/k is cyclic and arbitrary n. Thus, if M/k is contained in a solvable extension of k, the base change maps and automorphic induction maps exist.

Main Theorem. Let K be an algebraic number field of degree n over $\mathbb{Q}$, and ψ a Hecke character of K. If there exists an automorphic representation $I(\psi)$ of $\mathcal{A}(GL_n(\mathbb{A}_\mathbb{Q}))$ such that

$$L(s, \psi) = L(s, I(\psi))$$

for every Hecke character ψ of K, then both Artin's conjecture and the Langlands reciprocity conjecture are true.

Proof. Let $L/\mathbb{Q}$ be a Galois extension of finite degree and Galois group G. If ρ is an irreducible representation of G, and χ is its character, we can write by the Brauer induction theorem,

$$\chi = \sum_i m_i \operatorname{Ind}_{H_i}^G \chi_i,$$

where m_i are integers, χ_i are abelian characters of certain subgroups H_i of G. By the abelian reciprocity law, $L(s, \chi_i, L/L^{H_i})$ is equal to a Hecke L-series $L(s, \psi_i)$ where ψ_i is a Hecke character of L^{H_i}. As such, we can therefore write

$$L(s, \rho, L/\mathbb{Q}) = \prod_i L(s, \pi_i)^{m_i}$$

where π_i are automorphic representations of $\mathbb{Q}$. By a theorem of Langlands [15], we can further decompose the product so that each constituent L-function corresponds to an irreducible automorphic representation of $\mathbb{Q}$. Thus, without loss, in the above product, we can suppose that each π_i is irreducible and distinct from π_j when $i \neq j$. The identity reveals that

$$\chi(p) = \sum_i m_i a_p^{(i)}$$

where $a_p^{(i)}$ denotes the p-th coefficient in the Dirichlet series of $L(s, \pi_i)$. On one hand, the Chebotarev density theorem shows that

$$\sum_p \frac{|\chi(p)|^2}{p^s}$$

has a simple pole at $s = 1$. On the other hand, the series

$$\sum_p |\sum_i m_i a_p^{(i)}|^2/p^s$$

is on expanding

$$\sum_{i,j} m_i m_j \sum_p a_p^{(i)}\overline{a_p^{(j)}}p^{-s}.$$

By a result of Jacquet, Piatetski-Shapiro and Shalika [11], the inner sum has a simple pole if and only if $i = j$. Thus, the order of the pole is

$$\sum_i m_i^2$$

which must equal 1. This forces m_1 (say) to be ± 1 and the remaining ones to be zero. The possibility $m_1 = -1$ implies that $L(s, \chi)$ has no trivial zeroes which is not the case. Hence, $m_1 = 1$ and $L(s, \chi, L/\mathbb{Q}) = L(s, \pi_1)$ as desired.

Unfortunately, the hypothesis of the theorem is known to be satisfied only if K is a solvable extension of $\mathbb{Q}$ by the theorem of Arthur and Clozel [1]. In the next section, we apply these ideas to the theory of elliptic curves.

10. Application to elliptic curves.

Let E/k be an elliptic curve defined over a number field k. One can think of this as the set of solutions of an equation of the form

$$E: \qquad y^2 = x^3 + ax + b, \qquad\qquad a, b \in k.$$

Let $E(k)$ be the set of k-rational points of E. Then, $E(k)$ can be given the structure of an additive abelian group. We have the classical:

Mordell-Weil theorem. $E(k)$ is finitely generated.

Thus,

$$E(k) \simeq \mathbb{Z}^r \oplus E(k)_{tors}.$$

There is a folklore conjecture that $|E(k)_{tors}| \leq C_k$ where C_k is a constant depending only on the field. For $k = \mathbb{Q}$, Mazur proved that $C_{\mathbb{Q}} = 16$. Recently, Kamienny established this for quadratic fields. Given any curve, there is a finite algorithm which enables us to find $E(k)_{tors}$.

More intriguing is to find $r = r_k$, called the rank of E over k. It is unknown at present whether the rank of E over $\mathbb{Q}$ is unbounded though this is known in the function field case. Birch and Swinnerton-Dyer made an analytic conjecture about the rank in the following way: for each prime ideal $\mathfrak{p}$ of k, let $E(O_k/\mathfrak{p})$ have cardinality $N\mathfrak{p}+1-a_\mathfrak{p}$. We know, $|a_\mathfrak{p}| \leq (N\mathfrak{p})^{1/2}$. Define

$$L(E/k,s) = \prod_{\mathfrak{p}} \left(1 - \frac{a_\mathfrak{p}}{N\mathfrak{p}^s} + \frac{1}{N\mathfrak{p}^{2s-1}}\right)^{-1},$$

where the product is defined over primes where E has good reduction. This defines an analytic function for $\mathrm{Re}(s) > 3/2$. We have the famous:

Birch and Swinnerton-Dyer conjecture: $L(E/k,s)$ extends to an analytic function for all $s \in \mathbb{C}$ and

$$\mathrm{ord}_{s=1} L(E/k,s) = \text{rank } E(k).$$

If K/k is an arbitrary extension, then we can consider E over K and it is easy to see that rank $E(K) \geq$ rank $E(k)$. This raises two questions. First, does $L(E/K,s)$ have analytic continuation given that $L(E/k,s)$ does. Second, if it does, then can we prove that

$$\mathrm{ord}_{s=1} L(E/K,s) \geq \mathrm{ord}_{s=1} L(E/k,s).$$

If we consider the ring of endomorphisms of E, then it is not difficult to show that there are two possibilities for this. Either it is isomorphic to $\mathbb{Z}$ or an order in an imaginary quadratic field. In the latter case, we say E has CM (complex multiplication). The latter case is easier to deal with. For instance, we shall see that the answer to the first question is affirmative in this case.

Deuring [5] showed that if E has CM by an order in F, then $L(E/k,s)$ is a product of two Hecke L-series of k if $k \supset F$ or equal to a Hecke L-series of kF which is a quadratic extension of k.

Thus if E has CM, then $L(E/k,s)$ extends to an entire function of s. But recall Taniyama's conjecture, namely that $L(E/k,s)$ should be an $L(s,\pi)$ for some $\pi \in \mathcal{A}(GL_2(\mathbb{A}_k))$. We can verify this conjecture for E with CM by using automorphic induction.

Suppose that Taniyama's conjecture is true. Let K/k be any Galois extension with group G. Then, the theory of ℓ-adic representations shows that

$$L(E/K,s) = \prod_{\rho\, irred} L(E/k,s,\rho)^{\rho(1)},$$

where $L(E/k,s,\rho)$ is the "twist" by ρ. On Taniyama's conjecture, this corresponds to $L(s,\pi \otimes reg_G)$ where reg_G is the regular representation of G. By what we have seen in the previous section, this is the base change of π, $B(\pi)$. We can prove the following theorem:

Theorem. (joint with Kumar Murty) ([18])

(1) If E over k has CM then, $L(E/k, s)$ extends to an entire function for all values of s.

(2) Suppose that E/k satisfies Taniyama's conjecture and K is a finite extension of k. If K is a solvable extension of k, then, $L(E/K, s)$ extends to an entire function of s.

(3) In both cases, if K is a solvable extension, then $L(E/K, s)/L(E/k, s)$ is entire. In particular,

$$\text{ord}_{s=1} L(E/K, s) \geq \text{ord}_{s=1} L(E/k, s).$$

If the base change map always exists, one would not have to make the assumption that K is a solvable extension of k for part (3) of the theorem. In the CM case, one could strengthen the result by allowing K to be contained in a solvable extension.

This is highly reminiscent of the Brauer-Aramata theorem that states that if K/k is Galois, then $\zeta_K(s)/\zeta_k(s)$ is entire, where $\zeta_k(s)$ denotes the zeta function of k. There is a classical conjecture of Dedekind that predicts that this should be true even if K/k is not Galois. This is of course implied by Artin's conjecture. All these would follow from the development of the theory of base change.

Our method of proof deviates from the method of Brauer or Aramata. Instead, we use a device exploited by Kumar Murty in his exceedingly simple proof of the Brauer-Aramata theorem (see [6]).

Fix $s_0 \in \mathbb{C}$. Let K/k be Galois with group G. For each character χ of G, let

$$n_\chi = \text{ord}_{s=s_0} L(s, \chi, K/k).$$

Theorem. (Kumar Murty) $\sum_\chi n_\chi^2 \leq (n_{reg})^2$.

Corollary. $\zeta_K(s)/\zeta_k(s)$ is entire.

Proof. From the inequality, we get

$$n_1^2 \leq n_{reg}^2$$

from which the result follows.

Proof of the theorem. Let $H \leq G$. For each character ψ of H define

$$n_\psi = \text{ord}_{s=s_0} L(s, \psi, K/K^H).$$

Define

$$\theta_H = \sum_{\psi \in \hat{H}} n_\psi \psi,$$

where $\hat{H}$ denotes the set of irreducible characters of H. Then,

$$\theta_G|_H = \sum_{\chi \in \hat{G}} n_\chi \chi|_H = \sum_{\chi \in \hat{G}} n_\chi \sum_{\psi \in \hat{H}} (\chi|_H, \psi)\psi.$$

The inner sum is by Frobenius reciprocity

$$= \sum_{\psi \in \hat{H}} (\chi, \operatorname{Ind}_H^G \psi)\psi.$$

Inserting this and interchanging summation we obtain

$$\theta_G|_H = \sum_{\psi \in \hat{H}} \left(\sum_{\chi \in \hat{G}} n_\chi (\chi, \operatorname{Ind}_H^G \psi) \right) \psi.$$

We recognise the inner sum as n_ψ because Artin L-series are invariant under induction. Thus, $\theta_G|_H = \theta_H$. Now,

$$(\theta_G, \theta_G) = \sum_{\chi \in \hat{G}} n_\chi^2 = \frac{1}{|G|} \sum_{g \in G} |\theta_G(g)|^2.$$

But by what was shown above, $\theta_G(g) = \theta_{\langle g \rangle}(g)$. If H is cyclic,

$$|\theta_H(g)| \leq \sum_{\psi \in \hat{H}} n_\psi = n_{reg}$$

by the abelian reciprocity law. This gives

$$(\theta_G, \theta_G) \leq (n_{reg})^2.$$

This same proof carries over with a few modifications to show that if ρ is an arbitrary representation, then

$$L(s, \rho \otimes reg_G, K/k)/L(s, \rho, K/k)$$

is entire. By a similar method, one can show that if π is an automorphic cuspidal representation and $B(\pi)$ is the base change of it, then the L-function $L(s, B(\pi))/L(s, \pi)$ is entire.

11. Concluding remarks.

We therefore see that Artin Galois representations should correspond to automorphic representations. The Taniyama conjecture predicts the same should happen for elliptic curves. But there are more automorphic representations than Galois representations or elliptic curves. This led Langlands to conjecture a super-reciprocity law in the following form.

If K is a field and G is a group, we can consider the category of all K representations of G. This is a category with tensor products and fibre functor (namely the map that takes each representation to its underlying vector space). Langlands drew attention to the fact that there is a result of Rivano Saavedra [24] that the converse of this is true. That is, if $\mathcal{C}$ is a category with tensor products and fibre functors (together with a few other minor compatibility assumptions), then $\mathcal{C}$ is the category of representations of a group G. Such a category with tensor products is called a Tannakian category. Is the category of automorphic representations Tannakian ? If so, then there is a giant (or monstrous) group which we can call the automorphic Galois group from which all L-functions arise. Such a situation is not outlandish. In the context of converse theory, it requires us to show that the Rankin-Selberg convolution is the L-series of an automorphic representation. More precisely, there should be a map

$$\mathcal{A}(GL_n) \times \mathcal{A}(GL_m) \rightarrow \mathcal{A}(GL_{mn}).$$

By the predicted converse theory of GL_{mn}, we must twist the Rankin-Selberg convolution by automorphic representations of GL_r for all $r \leq mn-2$, and so we are in the case of triple convolutions. That is why it is tantalizing to understand Garrett's work and extend it (if possible) to higher GL_n. Such a step would be a major one in establishing a super-reciprocity law and which would resolve a huge chunk of the classical unsolved problems of number theory.

REFERENCES

[1] J. Arthur and L. Clozel, Simple algebras, base change and the advanced theory of the trace formula, *Annals of Math. Studies 120,* Princeton University Press (1990).

[2] J. Buhler, Icosahedral Galois representations, *Springer Lecture Notes* **654** Springer-Verlag, Berlin - New York, 1978.

[3] D. Bump and D. Ginzburg, Symmetric square L-functions on $GL(r)$, *Annals of Math.*, **136** (1992) 137-205.

[4] P. Deligne, La conjecture de Weil, I, *Publ. Math. I.H.E.S.*, **43** (1974) 273-307.

[5] M. Deuring, Die Zetafunktion einer algebraischen Kurve vom Geschlechte Eins, *Nach. Akad. Wiss. Göttingen*, Math.-Phys. Kl. I - III, 1953-1956.

[6] R. Foote and K. Murty, Zeros and poles of Artin L-series, *Math. Proc. Camb. Phil. Soc.*, **105**, 5 (1989) 5 - 11.

[7] G. Frey, Links between elliptic curves and solutions of $A - B = C$, *J. Indian Math. Soc.*, **51** (1987) 117-145.

[8] P. Garrett, Decompositions of Eisenstein series: Rankin triple products, *Annals of Math.*, **125** (1987) 209-235.

[9] I. Gelfand and S. Fomin, Geodesic glows on manifolds of constant negative curvature, *Uspekhi Mat. Nauk.*, **7** (1952) no. 1, 118-137.

[10] S. Gelbart and H. Jacquet, A relation between automorphic representations of $GL(2)$ and $GL(3)$, *Annales Sci. École Normale Sup.*, **11** (1978) 471-552.

[11] E. Hecke, Mathematische Werke, Herausgegeben im Auftrage der Akademie der Wissenschaften zu Göttingen, Vandenhoeck and Ruprecht, Göttingen, 1959, pp. 955.

[12] H. Jacquet, I. Piatetskii-Shapiro and J. Shalika, Rankin-Selberg convolutions, *Amer. J. Math.*, **105** (1983) 367-464.

[13] H. Jacquet and R. Langlands, Automorphic forms on $GL(2)$, *Lecture notes in Mathematics*, **114** Springer-Verlag, Berlin-New York 1970.

[14] R. Langlands, Base change for $GL(2)$, *Annals of Math. Studies* **96**, Princeton University Press (1980).

[15] R. Langlands, Automorphic representations, Shimura varieties and motives, in *Automorphic forms, representations and L-functions* (ed. A. Borel and W. Casselman) Proc. Symp. Pure Math., Parts I and II, Vol. 33, pp. 205-246, American Math. Society, Providence, 1979.

[16] H. Maass, Über eine neue Art von nichtanalytischen automorphen Funktionen und die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Ann.* **121** (1949) 141-183.

[17] K. Murty, On the Sato-Tate conjecture, in *Number Theory related to Fermat's last theorem*, (ed. N. Koblitz) (1982) 195-205, Birkhauser-Verlag, Boston.

[18] K. Murty and R. Murty, Base change and the Birch-Swinnerton-Dyer conjecture, *to appear in the Grosswald volume.*

[19] I. Piatetski-Shapiro, Converse theorem for $GL(n)$, Festschrift in honour of I. Piatetski-Shapiro, *Israel Mathematical Conference Proceedings* (Ed. S. Gelbart, R. Howe, P. Sarnak) Weizmann Science Press of Israel, 1990.

[20] S. Ramanujan, On certain arithmetical functions, *Trans. Camb. Phil. Soc.*, **22** (1916) 159-184.

[21] R. Rankin, Contributions to the theory of Ramanujan's function $\tau(n)$ and similar arithmetical functions, II. The order of the Fourier coefficients of integral modular forms, *Proc. Camb. Phil. Soc.*, **35** (1939) 351-372.

[22] K. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Inv. Math.*, **100** (1990) 431-476.

[23] A. Robert, Formes automorphes sur GL_2, *Lecture notes in mathematics* **317** pp. 295-318, Springer-Verlag, Berlin-New York, 1973.

[24] R. Saavedra, Categories Tannakienne, *Lecture notes in mathematics* **265**, Springer-Verlag, Berlin-New York 1972.

[25] A. Selberg, On the estimation of Fourier coefficients of modular forms, Proc. Sympos. Pure Math., Vol. VIII, 1-15, Amer. Math. Soc., Providence, R.I., 1965.

[26] A. Selberg, Bemerkung über eine Dirichletsche Reihe die mit der Theorie der Modulformen nahe verbunden ist, *Arch. Math. Naturvid.* **43** (1940) 47-50.

[27] J.-P. Serre, Abelian ℓ-adic representations and elliptic curves, McGill University lecture notes, (written in collaboration with W. Kuyk and J. Labute), W. A. Benjamin Inc., New York - Amsterdam, 1968.

[28] J.-P. Serre, Sur les representations modulaires de degré 2 de Gal($\overline{\mathbb{Q}}/\mathbb{Q}$), *Duke Math. J.* **54** (1987) 179-230.

[29] F. Shahidi, On certain L-functions, *Amer. J. Math.*, **103** (1981) 297-355.

[30] G. Shimura, On the holomorphy of certain Dirichlet series, *Proc. London Math. Soc.* **(3) 31** (1975) no. 1, 79-98.

[31] G. Shimura, Yukata Taniyama and his time, *Bull. London Math. Soc.*, **21** (1989) 186-196.

[32] Y. Taniyama, Jacobian varieties and number fields, *Proceedings of the international symposium on algebraic number theory,* Tokyo and Nikko, 1955, Science Council of Japan, Tokyo, 1956, pp. 31-45.

[33] J. Tunnell, Artin's conjecture for representations of octahedral type, *Bull. Amer. Math. Soc. N.S.* **5**(1981) no. 2, 173-175.

[34] A. Weil, Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, *Math. Annalen* **168** (1967) 149-156.

M. Ram Murty
Department of Mathematics
McGill University
Montreal H3A 2K6, Canada
e-mail murty@shiva.math.mcgill.ca