The Langlands Program (An overview)

G. Harder*

Mathematisches Institut der Universität Bonn, Bonn, Germany

Lectures given at the
School on Automorphic Forms on GL(n)
Trieste, 31 July - 18 August 2000

LNS0821005

*harder@math.uni-bonn.de

Contents

Introduction

The Langlands program predicts a correspondence between two types of objects. On the one side we have automorphic representations π and on the other side we have some arithmetic objects M which may be called motives or even objects of a more general nature. Both these objects produce L-functions and the correspondence should be defined by the equality of these L-functions. A special case is the Weil-Taniyama conjecture which has been proved by Wiles-Taylor and others.

I. A Simple Example

On his home-page under `www.math.ias.edu` Langlands considers a couple of very explicit and simple examples of this correspondence and here I reproduce one of these examples together with some further explanation. This example is so simple that the statement of the theorem can be explained to everybody who has some basic education in mathematics.

The **first object** is a pair of integral, positive definite, quaternary quadratic forms

$$P(x,y,u,v) = x^2 + xy + 3y^2 + u^2 + uv + 3v^2$$
$$Q(x,y,u,v) = 2(x^2 + y^2 + u^2 + v^2) + 2xu + xv + yu - 2yv$$

These forms have discriminant 11^2 and I mention that these two quadratic forms Q, P are the only integral, positive definite quaternary forms with discriminant 11^2. This may not be so easy to verify but it is true.

(Rainer Schulze-Pillot pointed out that this is actually **not true**; there is a third form

$$S(x,y,u,v) = x^2 + 4(y^2 + u^2 + v^2) + xu + 4yu + 3yv + 7uv$$

but the two forms above are sufficient for the following considerations (see [He1])).

This pair will give us automorphic forms, we come to this point later.

The **second object** is an elliptic curve E, for us this is simply a polynomial

$$G(x,y) = y^2 + y - x^3 + x^2 + 10x + 20.$$

This object is a diophantine equation, for any commutative ring R with identity we can consider the set of solutions

$$\{(a,b) \in R^2 | G(a,b) = 0\}$$

In the case where R is a field k we add a point at infinity (we should consider the homogenized polynomial $\tilde{G}(x,y,z) = y^2z+yz^2-x^3+x^2z+10xz^2+20z^3$) and define

$$\begin{aligned} E(k) &= \{(a,b) \in k^2 | G(a,b) = 0\} \cup \{\infty\} \\ &= \{(a,b,c) \in k^3 \setminus \{(0,0,0)\} \mid \tilde{G}(a,b,c) = 0\}/k^*. \end{aligned}$$

We come back to the first object. For any integer n we can define the numbers

$$r(P,n) = \#\{\gamma \in \mathbb{Z}^4 | P(\gamma) = n\}$$
$$r(Q,n) = \#\{\gamma \in \mathbb{Z}^4 | Q(\gamma) = n\}'$$

in classical terms: We consider the number of representations of n by the two forms.

We can encode these numbers in generating series

$$\Theta(P,t) = \sum_n r(P,n)t^n = \sum_{\gamma \in \mathbb{Z}^4} t^{P(\gamma)}$$

$$\Theta(Q,t) = \sum_n r(Q,n)t^n = \sum_{\gamma \in \mathbb{Z}^4} t^{Q(\gamma)}$$

Of course it is not so difficult to write a few terms of these series

$$\begin{aligned} \Theta(P,t) &= 1 + 4t + 4t^2 + 8t^3 + 20t^4 + 16t^5 + 32t^6 + 16t^7 + 36t^8 + 28t^9 + \\ &\quad 40t^{10} + 4t^{11} + 64t^{12} + 40t^{13} + 64t^{14} + 56t^{15} + 68t^{16} + 40t^{17} + \\ &\quad 100t^{18} + 48t^{19} + 104t^{20} + \ldots \end{aligned}$$

$$\Theta(Q,t) = 1 + 12t^2 + 12t^3 + 12t^4 + 12t^5 + 24t^6 + 24t^7 + 36t^8 + 36t^9 + 48t^{10} +$$
$$72t^{12} + 24t^{13} + 48t^{14} + 60t^{15} + 84t^{16} + 48t^{17} + 84t^{18} + 48t^{19} + 96t^{20} + \ldots.$$

Now we return to our second object. For any prime p we can reduce our polynomial $G(x,y) \mod p$ and we can look at the solutions of our equation $G(x,y) = 0$ in the field $\mathbb{F}_p$ with p elements. Actually this equation defines what is called a curve over $\mathbb{F}_p$ and if we add the point at infinity we get a projective curve. We say that this curve is smooth over $\mathbb{F}_p$ (or we say that we have good reduction) if for any point in the algebraic closure $(a,b) \in E(\bar{\mathbb{F}}_p)$ the vector of partial derivatives

$$(\frac{\partial G}{\partial x}(a,b), \frac{\partial G}{\partial y}(a,b)) \neq 0.$$

A simple calculation shows that we get a smooth curve over $\mathbb{F}_p$ except for $p = 11$. For any p we may ask:

What is the number of solutions of our equation over $\mathbb{F}_p$ *and this means we want to know what* $\#E(\mathbb{F}_p)$ *is.*

To get a rough idea of what will happen we do the following: We choose an $a \in \mathbb{F}_p$ and to find a point $(a, b) \in E(\mathbb{F}_p)$ we have to solve the quadratic equation $y^2 + y = a^3 - a^2 - 10a - 20$ in $\mathbb{F}_p$. If $p \neq 2$ then this equation has a solution in $\mathbb{F}_p$ if and only if the element $a^3 - a^2 - 10a - 20 + 1/4$ is a square in $\mathbb{F}_p$. Now we know that exactly half the elements in $\mathbb{F}_p^*$ are squares and hence our chance to hit a square is roughly $1/2$. But if we hit a square then we get two solutions for our equation -unless the number above should be zero- therefore we can expect that the number of solutions is roughly p. For $p \neq 11$ we define the number a_p by

$$\#E(\mathbb{F}_p) = p + 1 - a_p,$$

so this number a_p measures the deviation from our expectation.

We have the celebrated theorem by Hasse

$$\textit{For } p \neq 11 \textit{ we have the estimate } \mid a_p \mid \leq 2\sqrt{p}\ .$$

Again we can produce a list of values of a_p for small primes

2	3	5	7	13	17	19
-2	-1	1	-2	4	-2	0

Now we can formulate a theorem which is a special case of the Langlands correspondence but which was certainly known to Eichler:

Theorem *For all* $p \neq 11$ *we have*

$$a_p = \frac{1}{4}(r(P, p) - r(Q, p))$$

This is a surprising statement which is formulated in **completely elementary terms**. We have two diophantine problems of rather different nature, why are they related by the theorem above? I would like to say that the theorem in the form as it stands looks like a miracle.

One possible interpretation is that it provides an elementary formula for the numbers a_p. But from the computational side it seems to me that the

a_p are easier to compute than the representation numbers. I come back to this further down.

The theorem becomes comprehensible if we establish the connection to modular forms. The following considerations go back into the 19-th century. We consider the two generating functions for our two quadratic forms. We make a substitution $t \to e^{2\pi iz}$ and we observe that the functions

$$z \mapsto \Theta(P,z), z \mapsto \Theta(Q,z)$$

are holomorphic functions on the upper half plane $\mathcal{H} = \{z \mid \Im(z) > 0\}$. It is a classical result that these two functions are in fact modular forms of weight 2 for the congruence subgroup

$$\Gamma_0(11) = \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z}, c \equiv 0 \mod 11\}.$$

This means that they satisfy $(? = P, Q)$

$$\Theta(?, \frac{az+b}{cz+d}) = (cz+d)^2\Theta(?,z)$$

for

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(11)$$

and in addition a certain growth condition for $\Im(z) \to \infty$ is satisfied. [This can be verified by a classical calculation. First of all it is easy to see that in both cases the forms are invariant under $z \mapsto z+1$ and then the Poisson summation formula implies the rule

$$\Theta(?,z) = \frac{1}{11z^2}\Theta(?, \frac{1}{-11z}).$$

(I skip the computation, it is based on the observation that for $x \in \mathbb{R}^4$ the function

$$x \mapsto \sum_{\omega \in \mathbb{Z}^4} e^{2\pi i z Q(x+\omega)}$$

is periodic with period $\mathbb{Z}^4$. Hence it has a Fourier expansion, writing down this expansion, putting $x = 0$ and another small manipulation yields the assertion). Now the modularity follows. (See also [He1])]

Hence we get two modular forms of weight 2 for the group $\Gamma_0(11)$ and by classical dimension formulae we know that they span the vector space

of these modular forms. We know that this space of modular forms is also spanned by two other forms: One of them is the Eisenstein series

$$E(z) = \sum_{\gamma, c \equiv 0 \mod 11} \frac{1}{(cz+d)^2} - \frac{1}{11} \sum_{\gamma, c \not\equiv 0 \mod 11} \frac{1}{(cz+d)^2}$$

(this is a difference of two divergent series and this difference makes sense (this is Hecke so we are in the 20-th century)) and the other one is a cusp form, which in this case is

$$f(z) = e^{2\pi i z} \prod_{n=1}^{\infty} (1 - e^{2\pi n i z})^2 (1 - e^{2\pi 11 n i z})^2$$

(also classical we have the Dedekind η-function $\eta(z) = e^{\pi i z/12} \prod_{n=1}^{\infty} (1 - e^{2\pi n i z})$)

It is now also in [He1] that

$$f(z) = \frac{1}{4}(\Theta(P, z) - \Theta(Q, z)).$$

A small digression: Of course we would like have information on the individual Theta series. In this context we still have another theorem by Siegel. Our two quadratic forms are in fact in the same genus, that means over any p-adic ring $\mathbb{Z}_p$ they become equivalent (but of course they are not equivalent over $\mathbb{Z}$). Then we have a very general theorem by C.L. Siegel which asserts that the sum over the Theta series over a genus where the summands are multiplied by suitable weight factors (densities) gives us an Eisenstein series. In our special situation we find

$$\frac{1}{4}\Theta(P, z) + \frac{1}{6}\Theta(Q, z) = E(z) = \sum_{n=0}^{\infty} \sigma_n e^{2\pi i n z}$$

where the coefficients σ_n are given rather explicitly, for instance for a prime $p \neq 11$ we have

$$\sigma_p = p + 1.$$

I will say more about the other coefficients in a minute (See A below).

At this point I want to meditate a second. Here are two important points to observe.

A) If we look at the problem to understand the representation numbers we want to know the $r(P,n)$ for all integers n. If we go back to our elliptic curve we get only numbers for each prime $p, (p \neq 11)$. Here the theory of automorphic forms provides another remarkable and fundamental fact. The coefficients in the two series

$$f(z) = \frac{1}{4}(\Theta(P, e^{2\pi z}) - \Theta(Q, e^{2\pi iz})) = \sum_{n=1}^{\infty} \tau_n e^{2\pi inz}$$

and

$$E(z) = \frac{1}{4}\Theta(P, e^{2\pi iz}) + \frac{1}{6}\Theta(Q, e^{2\pi iz}) = \sum_{n=0}^{\infty} \sigma_n e^{2\pi inz}$$

behave *multiplicatively* and I explain what this means: If we have any series $F(z) = \sum \lambda_n e^{2\pi inz}$ then we build formally the Mellin transform. This is a Dirichlet series, it is defined by

$$L_F(s) = \sum_{n=1}^{\infty} \lambda_n n^{-s} \ .$$

(Let us ignore convergence problems, this construction has also been discussed in J. Cogdell's lecture). Now multiplicativity means in our case that the two Mellin transforms have an Euler product expansion

$$L_f(s) = (\prod_{p \neq 11} \frac{1}{1 - \tau_p p^{-s} + p^{1-2s}}) \frac{1}{1 - 11^{-s}}$$

$$L_E(s) = (\prod_{p \neq 11} \frac{1}{1 - (p+1)p^{-s} + p^{1-2s}}) \frac{1}{1 - 11^{-s}}$$

and this is equivalent to some recursion formulae namely

$$\tau_{nm} = \tau_n \tau_m, \sigma_{nm} = \sigma_n \sigma_m \text{ if } n, m \text{ are coprime}$$

and for $p \neq 11$

$$\tau_{p^{r+1}} = \tau_{p^r}\tau_p + p\tau_{p^{r-1}}, \sigma_{p^{r+1}} = \sigma_{p^r}\sigma_p + p\sigma_{p^{r-1}} \text{ if } r \geq 1$$

and hence we know the σ, τ if we know them for prime indices.

This follows from the theory of the Hecke operators which was actually designed for proving such multiplicativity formulae (See [He2]). The two

functions are eigenfunctions for this Hecke algebra and this is equivalent to the multiplicativity of the coefficients. This makes it also clear that our two functions are the only ones which have multiplicative coefficients.

B) Now we have the formula

$$\frac{1}{4}r(P,p)+\frac{1}{6}r(Q,p)=p+1$$

and together with our theorem we can say that we can express the representation numbers in terms of p and a_p. Combined with the theorem by Hasse we get a consequence for the asymptotic behavior of the representation numbers and this was an application Eichler had in mind. From $|\tau_p|=|\frac{1}{4}(r(P,p)-r(Q,p))|\leq 2\sqrt{p}$ we get the asymptotic formulae

$$r(P,p)=\frac{12}{5}p+O(p^{1/2})$$

$$r(Q,p)=\frac{12}{5}p+O(p^{1/2}).$$

Now we return to our elliptic curve and I want to give a very sketchy outline of the proof of the theorem. We consider the Riemann surface $\Gamma_0(11)\backslash\mathcal{H}$. It was known to Fricke that this is a curve of genus 1 over $\mathbb{C}$ from which two points are removed. These two points are the cusps of the action of $\Gamma_0(11)$ on $\mathcal{H}$, they can be represented by $0, i\infty$. The curve of genus 1 can also be interpreted as $\Gamma_0(11)\backslash\mathcal{H}^*$ where $\mathcal{H}^*=\mathcal{H}\cup\mathbb{Q}\cup\{\infty\}=\mathcal{H}\cup\mathbb{P}^1(\mathbb{Q})$ where this space is endowed with a suitable topology. Fricke found an equation for this curve which after some manipulation can be transformed into

$$y^2+y=x^3-x^2-10x-20$$

and in modern language this means that that we have a model $X_0(11)/\mathrm{Spec}(\mathbb{Z})$ of our complex curve which has good reduction at all primes $p\neq 11$.

The Hecke operators T_p are so-called correspondences, they can be interpreted as curves $T_p\subset\Gamma_0(11)\backslash\mathcal{H}^*\times\Gamma_0(11)\backslash\mathcal{H}^*$ which consist of the following points: If a first coordinate is represented by $z\in\mathcal{H}$ then the second coordinate is represented by one of the points $\{pz, z/p, (z+1)/p, \ldots, (z+p-1)/p\}$; so in general there are $p+1$ second coordinates corresponding to a first coordinate and vice versa. (Of course one has to check that replacing z by another representative gives the same set of corresponding points). These Hecke operators extend to correspondences also called T_p on the model $X_0(11)$. To

see that this is so one has to go to the modular interpretation of $X_0(11)$, this means roughly that $X_0(11)$ is the parameter space for the elliptic curves with a cyclic subgroup of order 11. Then Eichler showed that these correspondences T_p have a reduction $\mod p$ and this reduction is given by the congruence formula ([Ei])

$$T_p \mod p = F_p +^t F_p.$$

Here F_p is given by the graph $\{(x, x^p) \in E(\bar{\mathbb{F}}_p) \times E(\bar{\mathbb{F}}_p)\}$ and ${}^tF_p$ is given by $\{(x^p, x) \in E(\bar{\mathbb{F}}_p) \times E(\bar{\mathbb{F}}_p)\}$. Using the trace formula the coefficient τ_p can be expressed in terms of the fixed points of T_p. But $\mod p$ the fixed points of F_p and ${}^tF_p$ are the points in $E(\mathbb{F}_p)$, and this gives a very rough indication how the theorem can be proved.

The Taniyama-Shimura - Weil conjecture

Wiles, Taylor and others proved the general Taniyama-Weil conjecture. I want to give some indication of the content of this general theorem. The precise statement needs some finer concepts and results from the theory of automorphic forms and the arithmetic of elliptic curves.

A *congruence subgroup* $\Gamma \subset SL_2(\mathbb{Z})$ is a subgroup of finite index which can be defined by congruence conditions on the entries. To any integer N we define the subgroup

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \;\mid\; a \equiv d \equiv 1 \mod N \right\},$$

and a given subgroup Γ is called a congruence subgroup, if we can find an integer N such that

$$\Gamma(N) \subset \Gamma \subset SL_2(\mathbb{Z}).$$

Such a group operates on the upper half plane $\mathbb{H}$ and the quotient $\Gamma\backslash\mathbb{H}$ carries the structure of a Riemann surface, more precisely we can compactify it to a compact Riemann surface by adding a finite number of points. These finitely many points are called the *cusps*.

A holomorphic modular form for a given congruence subgroup Γ of weight $k > 0$ is a holomorphic function on the upper half plane

$$f : \mathbb{H} \longrightarrow \mathbb{C}$$

which satisfies

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

for all $\gamma \in \Gamma$, and which satisfies a growth condition in the cusps (see 4.11 (2) in [V]). Now I need some results and concepts which I cannot explain in detail. On the space of modular forms of weight k for $\Gamma_0(N)$ we have an action of a commutative algebra $\mathbb{T}$ which is generated by operators T_p for the primes $p \not| N$. In this space of modular forms we have the subspace of *cusp forms*. These are forms which vanish at infinity (see [V], ...), and this subspace is invariant under the Hecke operators. It is a classical result of Hecke that this space of cusp forms is a direct sum of spaces of common eigenforms for the Hecke operators.

A modular form f for $\Gamma_0(N)$ is called a *new form* if

i) The form f and certain transforms of it is not a modular form for a congruence subgroup $\Gamma_0(N')$ where $N' \mid N$ and $N' < N$.

ii) The form f is an eigenform for all the Hecke operators T_p where $p \not| N$.

It requires a little bit of work to show that this is a reasonable concept. To such a new form f we can attach an L-function

$$L(f,s) = \prod_p L_p(f,s),$$

where we have attached a local Euler factor $L_p(s)$ to any prime p:

i) For the primes $p \not| N$ our form is an eigenform for T_p, i.e.

$$T_p\ f = a_p\ f \qquad\qquad a_p \in \mathbb{C},$$

and we put

$$L_p(f,s) = \frac{1}{1 - a_p p^{-s} + p^{k-1-2s}}.$$

ii) For the primes $p \mid N$ and $p \neq 2, 3$ we have

$$L_p(s) = \begin{cases} \frac{1}{1-\varepsilon_p p^{-s}} & \varepsilon_p = \pm 1 \quad \text{if } p^2 \not| N \\ 1 & \text{if } p^2 \mid N. \end{cases}$$

The determination of the ε_p requires some knowledge of local representation theory.

iii) For the primes $p \mid N$ and $p = 2$ or 3 we also have

$$L_p(s) = \begin{cases} \frac{1}{1-\varepsilon_p p^{-s}} & \varepsilon_p = \pm 1 \\ 1 \end{cases}$$

but here the formulation of the conditions for the cases is even more subtle.

Now it is a general theorem that the completed L function $\Lambda(f,s) = \frac{\Gamma(s)}{\pi^s} \cdot L(f,s)$ is a holomorphic function in the entire plane and satisfies the functional equation

$$\Lambda(2-s) = N^{1-s} W(f) N^{s-1} \Lambda(s),$$

where $W(f) = \pm 1$. This is a so-called automorphic L-function.

Now I explain how we can attach an L function to an elliptic curve E over $\mathbb{Q}$. Let us consider an elliptic curve over $\mathbb{Q}$. This is simply an equation

$$G(x,y,z) = y^2 z + a_1 xyz + a_3 yz^2 - x^3 - a_2 x^2 z - a_4 xz^2 - a_6 z^3 = 0$$

with rational coefficients a_1, a_3, a_2, a_4, a_6. (This is a traditional notation, these a_i are not the a_p which occur in the local L-factors.) We assume that this equation defines a non singular curve and this means that for any solution $(x_0, y_0, z_0) \in \mathbb{C}^3$, $(x_0, y_0, z_0) \neq 0$ we have

$$\left(\frac{\partial G}{\partial x}\ (x_0,y_0,z_0), \frac{\partial G}{\partial y}\ (x_0,y_0,z_0), \frac{\partial G}{\partial z}\ (x_0,y_0,z_0) \right) \neq (0,0,0).$$

This is equivalent to the non vanishing of the discriminant

$$\Delta = \Delta(a_1, a_2, a_3, a_4, a_6),$$

this is a complicated expression in the coefficients. ([Mod], the articles of Tate and Deligne (Formulaire)). A special point is the point at infinity

$$O = (0,1,0).$$

It is the only point with $z_0 = 0$.

Now we can perform substitutions in the variables, and we get new Weierstraß equations. There is a so-called minimal Weierstraß equation

$$y^2 z + \tilde{a}_1 xyz + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6,$$

where all the $\tilde{a}_i \in \mathbb{Z}$, and where the discriminant Δ is minimal. (See Silverman [Si], Chap. III, § 1, VIII, § 8, [Hu], Chap. 5, § 2 and [Mod], articles by Tate and Deligne.) We have an algorithm – which is implemented in Pari – which produces this minimal equation.

If now p is a prime, we can consider the reduction $\mod p$. This gives us an equation over the finite field $\mathbb{F}_p$, and we say that our equation has good reduction $\mod p$, if the reduced equation defines an elliptic curve, i.e. it is smooth.

If the $\mod p$ reduced curve is not smooth then we have exactly one singular point $P_0 = (x_0, y_0, z_0) \in E(\mathbb{F}_p)$ which is different from the point O, we may assume $z_0 = 1$. Then we can introduce variables $u = x - x_0, v = y - y_0$ and our equation $\mod p$ becomes

$$\alpha u^2 + \beta uv + \gamma v^2 + \text{ higher order terms } = 0.$$

It is not hard to see that the quadratic leading term is not identically zero. Then we have two possibilities:

i) Over $\mathbb{F}_{p^2}$ we have $\alpha u^2 + \beta uv + \gamma v^2 = (u - \xi_1 v)(u - \xi_2 v)$ where $\xi_1 \neq \xi_2$

ii) The quadratic form is itself a square, i.e. $\alpha u^2 + \beta uv + \gamma v^2 = (u - \xi v)^2$

In the first case we say that E has multiplicative reduction $\mod p$, in the second case we say that E has potentially good reduction at p. (Potentially good is much more unpleasant than multiplicative reduction.)

If we are in the case i) we define

$$\varepsilon_p = \begin{cases} 1 & \text{if} \xi_1, \xi_2 \in \mathbb{F}_p, \\ -1 & else. \end{cases}$$

From this type of bad reduction we can produce a number $n_p(E) > 0$. If $p \neq 2, 3$ then

$$n_p(E) = \begin{cases} 1 & \text{multiplicative reduction,} \\ 2 & \text{potentially good reduction.} \end{cases}$$

If we have $p = 2$ or $p = 3$ then the rule is more complicated, in this case we need something finer than the minimal Weierstrass-equation, we need the Neron model (see [O]) to produce $n_p(E)$.

We define

$$N = \prod_p p^{n_p(E)},$$

where p runs over the primes with bad reduction. This number N is the conductor of our curve.

Now in [We] Weil defines an Euler factor $L_p(E,s)$ for any prime p. If we have good reduction at p, we define as before

$$L_p(E,s) = \frac{1}{1 - a_p p^{-s} + p^{1-2s}}$$

where $E(\mathbb{F}_p) = p + 1 - a_p$.

If we have bad reduction, then the Euler factor depends on the type of the bad reduction. The precise rule is (see [We] 2).

$$L_p(E,s) = \begin{cases} 1 & \text{if we have potentially good reduction,} \\ \frac{1}{1-\varepsilon_p p^{-s}} & \text{if we have multiplicative reduction.} \end{cases}$$

Then we can define

$$L(E,s) = \frac{\Gamma(s)}{\pi^s} \prod_p L_p(E,s).$$

(Here $\Gamma(s)$ is the Γ-function.)

Then the theorem of Wiles-Taylor asserts that to any elliptic curve $E/\mathbb{Q}$ with conductor N we can find a new form f on $\Gamma_0(N)$ such that

$$L_f(s) = L(E,s).$$

Our first example is a special case of this theorem.

Converse theorems

I come back to the L-function to a newform f. I introduced the Mellin transform very formally but as explained in Cogdell's lecture we can also define it by the integral

$$\Lambda(f,s) = \frac{\Gamma(s)}{(2\pi)^s} L(f,s) = \int_0^{i\infty} f(iy) y^s \frac{dy}{y}$$

where f has to be suitably normalized. Now we can conclude from the theory of automorphic forms that our newform satisfies

$$f(-\frac{1}{Nz}) = W(f) N z^2 f(z),$$

where $W(f) = \pm 1$. We apply this to the integral representation: We choose a positive real number $A > 0$ and split the integral into an integral from A

to ∞ and the integral from 0 to A. Into the second term we plug in the above transformation formula and get

$$\Lambda(f,s) = \int_A^\infty f(iy)y^s \frac{dy}{y} + W(f)N^{1-s}\int_{1/(NA)}^\infty f(iy)y^{2-s}\frac{dy}{y}$$

From this integral representation we can derive that $\frac{\Gamma(s)}{(2\pi)^s}L(f,s)$ has an analytic continuation into the entire plane and that we have the functional equation

$$\Lambda(2-s) = W(f)N^{1-s}\Lambda(s).$$

Already Hecke observed that under certain circumstances we can go the other way round. If we have a Dirichlet series

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

which defines a holomorphic function, which satisfies some boundedness conditions and satisfies a suitable functional equation then it comes from a modular form. Hecke considered the case of $Sl_2(\mathbb{Z})$ and Weil generalized it in ([We]) but he had to assume that these properties remained true if the series is twisted by Dirichlet characters. (See Venkataramas's and Cogdell's lectures.) Such a theorem is called a *converse theorem.*

Of course one would like to prove that the L-function of an elliptic curve has these nice analytic properties and then we could get a proof of Wiles theorem. But this is not the way it works.

II. The General Picture

Now I want to give some vague idea of the general Langlands program. I must confess that my own understanding is very limited. But on the other hand the entire picture is so vast and a precise formulation requires an explanation of so many subtle notions that I believe that a very rough approximation may be even more helpful than a precise presentation.

The first datum is a reductive group $G/\mathbb{Q}$, we may very well think that $G = Gl_n$. During this summer school we have seen that automorphic cusp forms should be understood as irreducible subrepresentations of the adele group $G(\mathbb{A})$ occurring in the space of cusp forms. So this is an irreducible submodule

$$H_\pi \subset L_0^2(G(\mathbb{Q})\backslash G(\mathbb{A}))$$

where the subscript π stands for the isomorphism class of our module. Several lecturers told us that such a π is in fact a restricted tensor product of local representations π_v of $G(\mathbb{Q}_v)$ and we write

$$\pi = \bigotimes{}' \pi_v.$$

These local representations have to satisfy some constraints. For instance for almost all finite primes π_p has to be in the unramified principal series (see Prasad's notes and below) and they must be unitary.

In Raghunathan's lecture it was explained that

$$L_0^2(G(\mathbb{Q})\backslash G(\mathbb{A})) = \bigoplus m(\pi) H_\pi$$

and we state a fundamental problem:

Let us assume that there is a restricted product $\pi = \bigotimes{}' \pi_v$ given to us, which fulfills the above constraints. When does π occur in the space of automorphic forms and what is $m(\pi)$?

Of course this question is rather vague because we should know how π is given to us, i.e. what is the rule which produces the local data $\{\pi_v\}$. The speculative answer to this question is, that the rule should come from some kind of arithmetic object.

The classical case again

We come back briefly to the special case Gl_2. In our example a modular form was a holomorphic function f on the upper half plane which satisfied

$$f(\gamma(z)) = (cz+d)^2 f(z) \text{ for } \gamma \text{ in some congruence subgroup } \Gamma \subset Sl_2(\mathbb{Z}).$$

In addition we required that it should be an eigenform for the so-called Hecke operators and I explained briefly that this was equivalent to the requirement that the Mellin transform of the Fourier expansion has an Euler product expansion. Actually the Hecke operators T_p are only defined for primes p not dividing the so-called level N of our form. In our example we had $N = 11$. Hence we see that f provides a collection of local data $\{\tau_p\}_{p,p\not|N}$ the eigenvalues of T_p. In our example we had in fact a rather simple rule which provided the local data, we took the difference of the representation numbers.

If we want to translate from the classical language to the modern language then we have to assign a representation $\pi(f)$ of $Gl_2(\mathbb{A})$ to our classical

modular form: This representation should occur in the space of cusp forms $L_0^2(Gl_2(\mathbb{Q})\backslash Gl_2(\mathbb{A}))$. I do not construct it but I make a list of its properties which define it uniquely. If we write

$$\pi(f) = \bigotimes{}' \pi_v$$

then

i) At the finite primes p not dividing the level the representation $\pi(f)_p$ *is in the unramified principal series and hence a unitarily induced representation*

$$\mathrm{Ind}_{B(\mathbb{Q}_p)}^{G(\mathbb{Q}_p)} \lambda_p$$

where λ_p *is a quasicharacter* $\lambda_p(\begin{pmatrix} t_1 & u \\ 0 & t_2 \end{pmatrix}) = |t_1|^{s_1}|t_2|^{s_2}$. *It gives two numbers*

$$\alpha_p = \lambda_p(\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}) \text{ and } \beta_p = \lambda_p(\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}).$$

Then these numbers are related to the p-th Fourier coefficient of f by the formula

$$\tau_p = \sqrt{p}(\alpha_p + \beta_p) \text{ and } \alpha_p\beta_p = \omega(p).$$

Here ω *is the so-called central character, it is the restriction of* $\pi(f)$ *to the center.*

ii) In our special situation where f is holomorphic of weight two the representation $\pi(f)_\infty$ *of* $Gl_2(\mathbb{R})$ *will be the first discrete series representation.*

If we have holomorphic modular form of weight k we get the $(k-1)$-th representation of the discrete series a infinity and in the formula for the a_p the $\sqrt{p}$ gets changed into $p^{\frac{k-1}{2}}$.

The second player in the game is our elliptic curve $E/\mathbb{Q}$. This elliptic curve yields an object $h^1(E)$, this is a motive. It is not entirely clear what this means but it creates some other objects

A) A compatible system of ℓ-adic representations of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

B) The Betti cohomology $H^1(E(\mathbb{C}), \mathbb{Z})$ together with a so-called Hodge filtration on $H^1(E(\mathbb{C}), \mathbb{C})$.

I want to say a word about A). For any prime ℓ we can look on the ℓ^n division points

$$E[\ell^n] = \{x \in E(\bar{\mathbb{Q}}) \mid \ell^n x = 0\}$$

and at this point I assume that we know that $E(\bar{\mathbb{Q}})$ is an abelian group and that $E[\ell^n]$ is isomorphic to $\mathbb{Z}/\ell^n\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}$. Of course these division points will have coordinates in larger and larger extensions of $\mathbb{Q}$ if n goes to infinity. This means that we have a natural action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on all these groups and if we form the projective limit

$$T_\ell = \lim_{\leftarrow n} E[\ell^n]$$

the result is a free $\mathbb{Z}_\ell$ -module of rank 2 together with a continuous action of the Galois group.

I explained what it means that E has good reduction at a prime p. It is not so difficult to see that for a prime ℓ which is different from p the action of the Galois group is unramified at this prime p, in other words the inertia group acts trivially. Hence we can define a conjugacy class $[F_p]$ defined by the action of the Frobenius at p and the characteristic polynomial

$$\det(\mathrm{Id} - F_p p^{-s} \mid T_\ell(E)) \in \mathbb{Z}_\ell[p^{-s}]$$

is a well-defined quantity. Now it follows from the Lefschetz fixed point formula that in fact

$$\det(\mathrm{Id} - F_p p^{-s} \mid T_\ell(E)) = 1 - a_p p^{-s} + p^{1-2s}.$$

This has important consequences

1) $\det(\mathrm{Id} - F_p p^{-s} \mid T_\ell(E)) \in \mathbb{Z}[p^{-s}]$

2) $\det(\mathrm{Id} - F_p p^{-s} \mid T_\ell(E))$ *does not depend on* ℓ.

Finally we have that

3) $\det(\mathrm{Id} - F_p p^{-s} \mid T_\ell(E))$ *is defined outside a finite set of primes* $S \cup \{\ell\}$.

These three properties of our different Galois modules (ℓ varies) are the defining properties for compatible systems of Galois modules.

Hence we can reformulate the specific result in the first section:

In our example the modular form of weight two and the elliptic curve provide a collection of local data

∞) A representation π_∞ and a real Hodge structure on $H^1(E(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C}$

For almost all primes an unramified local representation π_p of $Gl_2(\mathbb{Q}_p)$ and an unramified two dimensional representation $\rho(\pi_p)$ of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ *such that* (in the notation used in the example)

p) the automorphic Euler factor $L(\pi_p, s) = (1 - \tau_p p^{-s} + p^{1-2s})$ is equal to the arithmetic L- factor $\det(\mathrm{Id} - F_p p^{-s} \,|T_\ell(E))$.

This means that in our example we have a second rule which produces the local components of a cusp form. This rule is provided by the elliptic curve. In this particular case it is also possible to establish the local correspondence also for the ramified primes, this has been shown by Langlands, Deligne and Carayol.

It is now Langlands' idea that such a correspondence between automorphic representations $\pi = \bigotimes' \pi_v$ and some kind of arithmetic objects $\mathcal{M}(\pi)$ should always exist. The ideas of what nature these objects are, are also conjectural.

Satake's theorem

Let us assume that we picked a prime p such that $G \times \mathbb{Q}_p$ is split. If $G = Gl_n$ this can be any prime. Let $K_p = G(\mathbb{Z}_p)$ be the maximal compact subgroup defined by some Chevalley scheme structure $\mathcal{G}/\mathbb{Z}_p$, if $G = Gl_n$ this could be $Gl_n(\mathbb{Z}_p)$. To these data we attach the Hecke algebra $\mathcal{H}_p = \mathcal{C}(K_p \backslash G(\mathbb{Q}_p)/K_p)$: It consists of the $\mathbb{C}$ valued functions on $G(\mathbb{Q}_p)$ which are compactly supported and biinvariant under K_p and the algebra structure is given by convolution.

We choose a Borel subgroup $B \subset G$ and a maximal torus $T \subset B$ such that $T(\mathbb{Q}_p) \cap K = T(\mathbb{Z}_p)$ is the maximal compact subgroup our torus $T(\mathbb{Q}_p)$. Let $X_*(T) = \mathrm{Hom}(G_m, T)$ be the module of cocharacters, let W be the Weyl group. We introduce the module of unramified characters on the torus, this is

$$\mathrm{Hom}_{\mathrm{unram}}(T(\mathbb{Q}_p), \mathbb{C}^*) = \mathrm{Hom}(T(\mathbb{Q}_p)/T(\mathbb{Z}_p), \mathbb{C}^*) = \mathrm{Hom}(X_*(T), \mathbb{C}^*) = \Lambda(T).$$

We also view $\lambda \in \Lambda(T)$ as a character $\lambda : B(\mathbb{Q}_p) \to \mathbb{C}^*,\ \lambda \mapsto \lambda(b) = b^\lambda$.

We will consider the group of characters $\mathrm{Hom}(T \times_{\mathbb{Q}} \mathbb{Q}_p, G_m) = X^*(T)_{\mathbb{Q}_p}$ as a subgroup of $\Lambda(T)$. An element $\gamma \in X^*(T)$ defines a homomorphism $T(\mathbb{Q}_p) \to \mathbb{Q}_p^*$ and this gives us the following element $\{x \mapsto |\gamma(x)|_p\} \in \Lambda(T)$ which we denote by $|\gamma|$.

Since we have the Iwasawa decomposition $G(\mathbb{Q}_p) = B(\mathbb{Q}_p)K_p$ we can attach to any $\lambda \in \Lambda(T)$ a spherical function

$$\phi_\lambda(g) = \phi_\lambda(b_p k_p) = (\lambda + |\rho|)(b_p)$$

where $\rho \in \Lambda(T)$ is the half sum of positive roots. This spherical function is of course an eigenfunction for $\mathcal{H}_p$ under convolution, i.e. for $h_p \in \mathcal{H}_p$

$$\int \phi_\lambda(gx^{-1}) h_p(x) dx = \hat{h}_p(\lambda)\phi_\lambda(g)$$

and $h_p \mapsto \hat{h}_p(\lambda)$ is a homomorphism from $\mathcal{H}_p$ to $\mathbb{C}$.

The theorem of Satake asserts that this provides an identification

$$\mathrm{Hom}(\mathcal{H}_p, \mathbb{C}) \xrightarrow{\sim} \Lambda(T)/W.$$

To such a character we can attach an induced representation

$$\mathrm{Ind}_{B(\mathbb{Q}_p)}^{G(\mathbb{Q}_p)}(\lambda) = \{f : G(\mathbb{Q}_p) \to \mathbb{C} \mid f(bg) = (\lambda + |\rho|)(b) f(g)\}$$

where in addition $f|K$ is locally constant. These representations are called the principal series representations. We denote these irreducible modules by $\pi_p = \pi_p(\lambda_p)$ and λ_p is the so-called Satake parameter of π_p.

Let us now assume for simplicity that our group $G/\mathbb{Q}$ is split, for instance $G = Gl_n/\mathbb{Q}$. In this case we may choose a split torus $T/\mathbb{Q}$. We have the canonical isomorphism

$$\mathrm{Hom}(X_*(T), \mathbb{C}^*) \xrightarrow{\sim} X^*(T) \otimes \mathbb{C}^*$$

and the character module $X^*(T)$ can be interpreted as the cocharacter module of the dual torus $\hat{T}$. If we interchange the roots and the coroots then $\hat{T}$ becomes the maximal split torus of the dual group $\hat{G}$, which is now a reductive group over $\mathbb{C}$. If our group is $G = Gl_n/\mathbb{Q}$ then the dual group is $Gl_n(\mathbb{C})$.

A general philosophy

Now we come back to our automorphic form π. If we write it as a restricted tensor product, then almost all the components are in the unramified principal series and now we can view the collection of unramified components $\{\pi_p(\lambda_p)\}$ as a collection of semi simple conjugacy classes in the dual group.

Now Langlands philosophy assumes the existence of a very big group $\mathcal{L}$ and I cannot say exactly what properties this group should have. It certainly should somehow have the Weil group $W(\bar{\mathbb{Q}}/\mathbb{Q})$ in it. This Weil group is some kind of complicated modification of the Galois group. We have also the local Weil groups $W(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and these are easier to explain: The group $W(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \subset \mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ and consists of those elements whose image in $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ is an integral power of the Frobenius.

The arithmetic object $\mathcal{M}(\pi)$ attached to π should be a representation

$$\rho(\pi) : \mathcal{L} \to \hat{G}$$

which at least fulfills the following requirement:

At any prime p at which π is unramified the representation $\rho(\pi)$ is also "unramified". The structure of $\mathcal{L}$ should be such that for an unramified π_p it provides an unramified representation

$$\rho(\pi_p) : W(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \hat{G}(\mathbb{C})$$

such that the image of the Frobenius F_p under $\rho(\pi_p)$ is in the conjugacy class of the Satake parameter of π_p.

An unramified representation of the Weil group is of course a representation of the image $\mathbb{Z} =< F_p >$ of $W(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ in $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$, therefore it is enough to know the image of the Frobenius F_p.

Local Langlands correspondence

Of course we can also consider ramified representations

$$\rho : W(\bar{\mathbb{Q}}_p/\mathbb{Q}_p) \to \hat{G}(\mathbb{C})$$

and the general Langlands programme predicts also a correspondence between these representations ρ and the admissible irreducible representations of $G(\mathbb{Q}_p)$. Actually the situation is more complicated than that, one has to replace the Weil group be the Weil-Deligne group. This is a difficult subject, we have seen a little bit of the difficulties when we discussed the Euler

factors of the automorphic and the arithmetic L-function in our discussion of the Taniyama-Weil conjecture.

The local Langlands conjecture is proved for the group Gl_n by work of Laumon-Rapoport-Stuhler ([L-R-S]) in characteristic $p > 0$ and by Harris-Taylor ([H-T]) in characteristic 0. This is discussed in Wedhorns lectures at this summer school ([Wed]).

Representations with cohomology and motives

I want to discuss a special case in which I feel a bit happier. Among the representations of $G(\mathbb{R})$ there is a certain class consisting of representations π_∞ which have non trivial cohomology. This means that there is a finite dimensional, irreducible rational G-module $\mathcal{E}$ such that

$$H^\bullet(\mathfrak{g}, K_\infty, \pi_\infty \otimes \mathcal{E}) \neq \{0\}.$$

Then $\mathcal{E}$ is determined by π_∞ and for any choice of $\mathcal{E}$ the number of such π_∞ is finite.

We say that an automorphic representation π is cohomological if the component π_∞ has cohomology in some module $\mathcal{E}$. In this case one might speculate whether we can attach a motive or better a family of motives to it. A motive is still a conjectural object but certainly simpler in nature than $\mathcal{L}$.

I want to give a rough idea what a motive should be. First of all I refer to Delignes theorem that for a smooth projective scheme $X/\mathbb{Q}$ the ℓ adic cohomology groups $H^i(\bar{X}, \mathbb{Q}_\ell)$ provide a compatible system of Galois modules. A motive M is a piece in the cohomology which is defined by a projector obtained from correspondences. (In the classical case these correspondences are provided by Hecke operators).

Then it is clear that M also provides a compatible system of Galois representations

$$\rho(M) : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to Gl(H(\bar{M}, \mathbb{Q}_\ell))$$

and the Euler factor at an unramified prime is defined as before by

$$\det(\mathrm{Id} - F_p p^{-s} \mid H(\bar{M}, \mathbb{Q}_\ell)) \in \mathbb{Z}[p^{-s}].$$

If we have an unramified principal series representation $\pi_p(\lambda_p)$ and we choose in addition a finite dimensional irreducible representation $r : \hat{G}(\mathbb{C}) \to Gl_n(\mathbb{C})$, then we define the Euler factor

$$L(\pi_p(\lambda_p), r, s) = det(\mathrm{Id} - r(\pi_p(\lambda_p))p^{-s}).$$

If we know all these Euler factors for all choices of r then we know the conjugacy class of $\pi_p(\lambda_p)$ viewed as an element in $\hat{G}(\mathbb{C})$. Now we can speculate

To any cohomological π and which occurs in the space of (cuspidal) automorphic forms on G and to any representation $r : \hat{G}(\mathbb{C}) \to Gl_n(\mathbb{C})$ we can find a motive $M(\pi, r)$ such that for all unramified primes p we have an equality of local Euler factors

$$L(r(\pi_p(\lambda_p), r, s) = \det(\mathrm{Id} - \rho(M)(F_p)p^{-s})$$

There should also be a matching between π_∞ and the Hodge structure on the Betti cohomology of the motive.

This system of ℓ representations (now r varies) should have the property that is compatible with the operations in linear algebra: If we decompose a tensor product $r_1 \otimes r_2$ into irreducibles then the Galois representations should decompose accordingly, at least if we pass to a subgroup of finite index in the Galois group.

Already in the formulation we need the properties of compatible system. The right-hand side has a property which we a priori can not expect from the left hand side: Why should the automorphic Euler factors be in $\mathbb{Z}[p^{-s}]$?? Can such a statement ever be true? Here the assumption that π_∞ has cohomology helps. Using the rational (or even the integral structure) on the cohomology we can show that in fact that $L(\pi_p, r, s)$ viewed as polynomial in p^{-s} has coefficients which are algebraic integers and which all lie in a finite extension of $\mathbb{Q}$ which depends on π_f. We say that a cohomological form π is rational if these coefficients are in $\mathbb{Z}$ (this was so in our example). Otherwise we say that π is defined over F if $F \subset \mathbb{C}$ is generated by the coefficients of all our Euler factors.

Then we can add to our assumption in our statement above that π should be rational. Otherwise we have to invent the notion of a motive with coefficients in F. This notion has been introduced by Deligne and then we can formulate the above assertion using this concept.

Of course one can ask the question in the opposite direction: Given a motive is there somewhere an automorphic cohomological representation π such that $M = M(\pi, r)$ for some r? Can we find such a representation even in the space of automorphic forms on Gl_n? The theorem of Wiles is a special case where the answer to this question turns out to be yes.

Functoriality

If we believe in this kind of correspondence between automorphic forms and some sort of arithmetic objects, then we get remarkable consequences for automorphic forms. Let us just stick to the cohomological case. If we have two such motives we can form their product, which for the Galois modules amounts to take their tensor product. Going backwards we should be able to construct an automorphic form $\pi_1 \times \pi_2$ on some bigger group. This is the *principle of functoriality*, which is suggested by the philosophy.

Let me give an example. We consider holomorphic modular forms of weight 2, we can even go back to our example. We have seen that our modular form provides a compatible system of two dimensional ℓ-adic representations

$$\rho(H^1(E)) : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) :\to Gl(H^1(\bar{E}, \mathbb{Q}_\ell))$$

Now we take symmetric powers of these representations, this means that we take the k-fold tensor product of these representations first and this amounts to taking the k-fold product of $h^1(E)$ by itself. Then we have an action of the symmetric group and we can take the symmetric part. In terms of the Galois representations this means that we get an representation on the symmetric tensors

$$\rho(\mathrm{Sym}^k(H^1(E))) : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) :\to Gl(\mathrm{Sym}^k(H^1(\bar{E}, \mathbb{Q}_\ell)))$$

and it is certainly a legitimate question whether this comes from an automorphic form.

In this particular case we can look at our problem from a different point of view. We look at the L function (let us stick to our example)

$$L_E(s) = (\prod_{p \neq 11} \frac{1}{1 - \tau_p p^{-s} + p^{1-2s}}) \frac{1}{1 - 11^{-s}}$$

and we rewrite the Euler factors

$$L(\pi_p, s) = \frac{1}{1 - \tau_p p^{-s} + p^{1-2s}}) = \frac{1}{(1 - \alpha_p p^{-s})(1 - \bar{\alpha}_p p^{-s})}$$

and we mention that it follows from Hasse's theorem that $\bar{\alpha}_p$ is in fact the complex conjugate of α_p.

Now we form a new L-function, we pick a $k > 1$ and write a local L-factor at p

$$L(\pi_p, r, s) = \frac{1}{(1 - \alpha_p^k p^{-s})(1 - \alpha_p^{k-1} \bar{\alpha}_p p^{-s}) \dots (1 - \bar{\alpha}_p^k p^{-s})}$$

We can form a global L-function attached to the k-th symmetric power

$$L(\pi, r, s) = \prod_{p;p\not|\mathcal{N}} \frac{1}{(1-\alpha_p^k p^{-s})(1-\alpha_p^{k-1}\bar{\alpha}_p p^{-s})\dots(1-\bar{\alpha}_p^k p^{-s})} L_N(\pi, r, s),$$

where I do not say anything about the factors at the ramified primes. In our case where $N = 11$ the Euler factor at 11 should not depend on k.

Of course we can ask whether this is again an L-function attached to an automorphic cusp form on Gl_{k+1}. This has been shown by Gelbart and Jacquet for $k = 2$. Here we are again in the situation where we could try to apply converse theorems, but we do not have methods to verify the necessary analytic properties of the L-Functions (see Cogdell's Notes). But the cases $k = 3, 4$ have been treated successfully by Shahidi and Kim.

We come to the concept of base change. Let us assume we have a (cuspidal) automorphic form π on some reductive group over $\mathbb{Q}$. Let us assume we attached to it a representation

$$\rho(\pi) : \mathcal{L} \to \hat{G}(\mathbb{C})$$

of our group $\mathcal{L}$. Let us assume that we have a field extension $K/\mathbb{Q}$, then it should be possible to restrict the group $\mathcal{L}$ to K and we would get a restricted representation

$$\rho(\pi)_K : \mathcal{L}_K \to \hat{G}(\mathbb{C}).$$

(This is another of the requirements one should put on $\mathcal{L}$, if we work with motives then we would just extend the motive or restrict the Galois representations to $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$).

Hence we should expect that this restriction of the representation $\rho(\pi)_K$ would provide an automorphic form on the group $G \times K$ which then would be the lift of π to $G \times K$.

The existence of such a lifting has indeed been proved for solvable extensions by Langlands in the case $G = Gl_2/F$ and by Arthur and Clozel for $G = Gl_n/F$. This result plays a fundamental role in the proof of the Taniyama-Weil conjecture for elliptic curves and the local Langlands correspondence for Gl_n by Harris and Taylor.

References

[A-C] Arthur, J.; Clozel, L.; Simple algebras, base change, and the advanced theory of the trace formula. Annals of Mathematics Studies, 120. Princeton University Press, Princeton, NJ, 1989. xiv+230 pp.

[Ca] Carayol, H.; Formes automorphes et représentations galoisiennes. (French) [Automorphic forms and Galois representations] Seminar on Number Theory, 1981/1982, Exp. No. 31, 20 pp., Univ. Bordeaux I, Talence, 1982.

[Co] Cogdell, J.; Notes on L-functions for Gl_n, this volume.

[De1] Deligne, P.; Formes modulaires et représentations ℓ-adiques. Séminaire Bourbaki, 1968/69, Exp. 335.

[Ei] Eichler, M.; Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzetafunktion, Arch. 5 (1954), 355-366.

[H-T] Harris, M.; Taylor, R.; The geometry and cohomology of some simple Shimura varieties. With an appendix by Vladimir G. Berkovich. Annals of Mathematics Studies, 151. Princeton University Press, Princeton, NJ, 2001. viii+276 pp.

[He1] Hecke, E.; Analytische Arithmetik der positiven quadratischen Formen, Kgl. Danske Selskab, Mathematisk-fysiske Meddelser. XIII, 12, 1940, 134 S.

[He2] Hecke, E.; Über Modulformen und Dirichletsche Reihen mit Eulerscher Produktentwicklung I,II (Mathematische Annalen Bd. 114, 1937, S.1-28, S. 316-351).

[He3] E. Hecke, E.; Mathematische Werke, Vandenhoeck & Ruprecht, Göttingen, 1959.

[Hu] Husemoller, D.; Elliptic curves. With an appendix by Ruth Lawrence. Graduate Texts in Mathematics, 111. Springer-Verlag, New York, 1987. xvi+350 pp.

[La1] Langlands, R.; Euler products. A James K. Whittemore Lecture in Mathematics given at Yale University, 1967. Yale Mathematical Monographs, 1. Yale University Press, New Haven, Conn.-London, 1971. v+53 pp.

[La2] Langlands, R.; Modular forms and ℓ-adic representations. Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 361-500. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[La3] Langlands, R.; Base change for $Gl(2)$, Ann. of Math. Studies **96**, Princeton University Press, 1980.

[La4] Langlands, R.; Automorphic representations, Shimura varieties, and motives. Ein Märchen. Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 205–246, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I.

[L-R-S] Laumon, G.; Rapoport, M.; Stuhler, U. $\mathcal{D}$-elliptic sheaves and the Langlands correspondence. Invent. Math. 113 (1993), no. 2, 217-338.

[Mod] Modular Functions of One Variable IV, ed. Proc. Int. summer school, Antwerp, ed. B.J. Birch and W. Kyuk, Springer Lecture Notes 476.

[O] Ogg, A. Elliptic curves and wild ramification, Am. Journal of Math. 89, p. 1-21.

[P-R] Prasad, D. - A. Raghuram; Representation theory of $GL(n)$ over non-Archimedean local fields, this volume.

[Si] Silverman, J. H.; The arithmetic of elliptic curves. Corrected reprint of the 1986 original. Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1992. xii+400 pp.

[V] Venkataramana, T.; Classical Modular Forms, this volume.

[Wed] Wedhorn, T.; The local Langlands correspondence for GL(n) over p-adic fields, this volume.

[We] Weil, A.; Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Ann., 168, 1967, S. 149-156.

[Wi] Wiles, A.; Modular elliptic curves and Fermats Last Theorem. Ann. of Math., 142 (1995), 443 -551.