

Zeta functions of twisted modular curves

Cristian Virdol
Department of Mathematics
Columbia University

July 6, 2008

Abstract

In this paper we compute and continue meromorphically to the entire complex plane the zeta function of twisted modular curves. The twist of the modular curves is done by a mod p representation of the absolute Galois group.

2000 Mathematics subject classification: primary 11G18, 11R42, 11R65.

1 Introduction

In chapter 7 of his book [SH], Shimura computed the zeta function of modular curves and modular abelian varieties by relating the Frobenius morphism with the Hecke operators using some congruence relations. We use some of his ideas to compute the zeta function of the curves that we define below. When the mod p representation is associated to a rational elliptic curve, such a twisted modular curve was defined and used in a paper by A. Wiles [W] (see the end of §2 below). Let $X(p)/\mathbb{Q}$ be the modular curve of the principal congruence subgroup $\Gamma(p)$ of $SL_2(\mathbb{Z})$ for a prime $p \geq 7$ (we do not consider $5 \geq p$, since for these values, the modular curve has genus 0), which is a geometrically disconnected curve whose connected components are $p - 1$ copies of the half upper plane quotient out by $\Gamma(p)$. Let $\overline{X(p)}$ be the smooth compactification of $X(p)$. The curve $\overline{X(p)}$ has an action of $GL_2(\mathbb{Z}/p\mathbb{Z})$ as specified below (see §2.1). For a number field F we denote by G_F the Galois group $\text{Gal}(\overline{\mathbb{Q}}/F)$. We consider a continuous Galois representation $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}/p\mathbb{Z})$, and let $\overline{X'(p)}/\mathbb{Q}$ be the curve obtained from $\overline{X(p)}/\mathbb{Q}$ via twisting by ρ composed with the action of $GL_2(\mathbb{Z}/p\mathbb{Z})$ on $\overline{X(p)}$ (see §1.2 for the definition of $X'(p)$).

Let $\hat{\Gamma}(p)$ be the adelic principal congruence subgroup of level p in $GL_2(\mathbb{A}_f)$, where \mathbb{A}_f is the finite part of the adèle ring $\mathbb{A}_{\mathbb{Q}}$ of \mathbb{Q} . Let $\pi = \pi_f \otimes \pi_{\infty}$ be a cuspidal automorphic representation of $GL_2(\mathbb{A}_{\mathbb{Q}})$, where π_f and π_{∞} are representations of $GL_2(\mathbb{A}_f)$ and $GL_2(\mathbb{R})$, respectively. If K is an open compact subgroup of $GL_2(\mathbb{A}_f)$, let π_f^K denote the space of K -fixed vectors of π_f . One

can associate to a representation π an L -function $L(s, \pi)$ which has an analytic continuation to the entire complex plane as an entire function and satisfies a functional equation: $s \leftrightarrow 1 - s$ (see theorems 6.15 and 6.16 of [G]).

We fix an isomorphism $j : \overline{\mathbb{Q}}_l \rightarrow \mathbb{C}$. Let $\rho_{\pi, l} : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{Q}}_l)$, l prime, $l \neq p$ be the two dimensional continuous Galois representation associated to the cuspidal automorphic representation π . Define $L(s, \rho_{\pi, l}) := \prod_q L_q(s)$, where

$$L_q(s) := \det(1 - j(\rho_{\pi, l}(\text{Frob}_q))|_{V^{I_q} q^{-s}})^{-1},$$

and Frob_q is a Frobenius element at q , I_q is an inertia group at q and V is the space corresponding to $\rho_{\pi, l}$. Then $L(s, \rho_{\pi, l})$ has an analytic continuation to the entire complex plane as an entire function and satisfies a functional equation $s \leftrightarrow 2 - s$.

As Shimura proved, we have $L(s - 1/2, \pi) = L(s, \rho_{\pi, l})$. From the work of Shimura and others (see theorems 7.11 and 7.13 of [SH]), we know that the H^1 -part of the Hasse-Weil zeta functions of $\overline{X(p)}$ is given by:

$$L(s, \overline{X(p)}) = \prod_{\pi} L(s - 1/2, \pi)^{\dim \pi_f^{\hat{\Gamma}(p)}},$$

where the cuspidal automorphic representations π which appear in the product are of weight 2, satisfy $\pi_f^{\hat{\Gamma}(p)} \neq \{0\}$ and are cohomological, which means that $H^1(\mathfrak{gl}_2(\mathbb{R}), SO_2(\mathbb{R}); \pi_{\infty}) \neq 0$. Here, $H^1(\mathfrak{gl}_2(\mathbb{R}), SO_2(\mathbb{R}); \pi_{\infty})$ is the Lie algebra cohomology group with respect to $\mathfrak{gl}_2(\mathbb{R})$ relative to the maximal compact subgroup $SO_2(\mathbb{R})$.

The group $GL_2(\mathbb{Z}/p\mathbb{Z})$ acts on the modular curve $\overline{X(p)}$. The composition of this action with ρ gives us an action of $G_{\mathbb{Q}}$ on $\overline{X(p)}$. Taking complex points of $\overline{X(p)}$ we get that $G_{\mathbb{Q}}$ acts on $\overline{X(p)}(\mathbb{C})$ through this geometric action on $\overline{X(p)}$. Thus $G_{\mathbb{Q}}$ acts on $H^1(\overline{X(p)}, \mathbb{C})$. Using this commutativity of this action and of the Hecke operators outside p , we obtain the representation $\tilde{\varphi}_{\pi} \circ \rho$ of $G_{\mathbb{Q}}$ on $\pi_f^{\hat{\Gamma}(p)}$ (see the beginning of §2.6 for the definition of $\tilde{\varphi}_{\pi}$).

Let $L(s, \rho_{\pi, l} \otimes (\tilde{\varphi}_{\pi} \circ \rho)) := \prod_q L'_q(s)$, where we denote

$$L'_q(s) := \det(1 - j(\rho_{\pi, l}(\text{Frob}_q)|_{V^{I_q}} \otimes (\tilde{\varphi}_{\pi} \circ \rho)(\text{Frob}_q)|_{U^{I_q}}) q^{-s})^{-1}$$

and U is the space corresponding to $\tilde{\varphi}_{\pi} \circ \rho$.

We have two curves $\overline{X(p)}/\mathbb{Q}$ and the twisted one $\overline{X'(p)}/\mathbb{Q}$. Their jacobians J and J' are identical over $\overline{\mathbb{Q}}$, but the Galois actions on J and J' are different. The difference is described by the representation $\tilde{\varphi}_{\pi} \circ \rho$. Then we go through Shimura's computation of the zeta function of $\overline{X(p)}$ modifying the Galois action by $\tilde{\varphi}_{\pi} \circ \rho$ and we obtain the first part of the following theorem (which is a consequence of proposition 2.2 and multiplicity one for GL_2) (see §2.6 for details):

Theorem 1.1. *We have $L(s, \overline{X'(p)}) = \prod_{\pi} L(s, \rho_{\pi, l} \otimes (\tilde{\varphi}_{\pi} \circ \rho))$, where the cuspidal automorphic representations π 's which appear in the product are of weight*

2, satisfy $\pi_f^{\hat{\Gamma}(p)} \neq \{0\}$ and are cohomological. If the representation ρ factors through the Galois group of a solvable extension of a totally real field (i.e. the field $K := (\mathbb{Q})^{\ker(\rho)}$ is a solvable extension of a totally real field), then the L -function $L(s, \overline{X'(p)})$ has a meromorphic continuation to the entire complex plane and satisfies a functional equation.

In this theorem $L(s, \overline{X'(p)})$ represents the H^1 -part of the zeta function of $\overline{X'(p)}$. The meromorphic continuation is done by combining the technique of Artin-Brauer with a recent result of Taylor [T] and the GL_2 -base change for cyclic extensions proven by Langlands [L]. We shall compute the L -function in the following section and prove the meromorphic continuation in §3.

2 Computation of the zeta function

2.1 Known facts

Let us recall some known facts (see [H1] or [KM]) which will be used in the proof of theorem 1.1. Let N be a positive integer with $N > 2$, S a scheme, and E/S an elliptic curve over S . If $N : E \rightarrow E$ is the multiplication by N , then the kernel of this morphism $E[N]/S = \ker[N]$ is a locally free group scheme of rank N^2 over S . A level N -structure is by definition a group scheme isomorphism $\phi : (\mathbb{Z}/N\mathbb{Z})^2/S \rightarrow E[N]/S$. Let SCH be the category of schemes and SETS be the category of sets. We consider the following functor $\epsilon_N : \text{SCH}/\text{Spec}(\mathbb{Z}[1/N]) \rightarrow \text{SETS}$:

$$\epsilon_N(S) = [(E, \phi)/S | E/S \text{ an elliptic curve, } \phi \text{ a level } N \text{ structure}],$$

where “[.]” means the set of isomorphism classes of the objects in the brackets. Two structures (E, ϕ) and (E', ϕ') are isomorphic by $\varphi : E \rightarrow E'$ if φ is an isomorphism and $\varphi \circ \phi = \phi'$. It is known that the functor ϵ_N is representable over $\text{Spec}(\mathbb{Z}[1/N])$ by an affine curve $X(N)$. There is a natural action of $GL_2(\mathbb{Z}/N\mathbb{Z})$ on ϵ_N which is given by $(E, \phi) \rightarrow (E, \phi \circ g)$, if $g \in GL_2(\mathbb{Z}/N\mathbb{Z})$. The action of $-1 \in GL_2(\mathbb{Z}/N\mathbb{Z})$ is trivial because $-1 : E \rightarrow E$ induces an isomorphism $(E, \phi) \cong (E, \phi \circ (-1))$. Since ϵ_N is representable by $X(N)$ over $\text{Spec}(\mathbb{Z}[1/N])$, the group $GL_2(\mathbb{Z}/N\mathbb{Z})$ acts on $X(N)/\text{Spec}(\mathbb{Z}[1/N])$.

It is known also that (see [KM], lemma 10.3.2):

Proposition 2.1. *The group $GL_2(\mathbb{Z}/N\mathbb{Z})$ acts on the compactified modular curve $\overline{X(N)}$.*

2.2 The twisted curve

We fix a continuous representation

$$\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}/p\mathbb{Z})$$

where p is a prime number. Let K be the finite Galois extension of \mathbb{Q} defined by $K := (\overline{\mathbb{Q}})^{\ker(\rho)}$.

Suppose that a group G acts on an affine scheme $X = \text{Spec}(R)$. Then G determines an action on R . If we consider $R^G = \{r \in R \mid gr = r, \forall g \in G\}$, then R^G is a ring. We have that $\text{Spec}(R^G) = \text{Spec}(R)/G$ as a geometric quotient if R/R^G is étale (see proposition 1.8.4 of [H1]). If X is not affine and we can cover X by affine schemes which are stable under G , we similarly obtain a geometric quotient X/G .

Let

$$X' = \overline{X(p)} \times_{\text{Spec}(\mathbb{Z}[1/pd])} \text{Spec}(O_K[1/pd]),$$

where O_K is the ring of integers of K , d is the discriminant of K/\mathbb{Q} , and $O_K[1/pd]$ is the sub-ring of K in which pd is inverted. The group $GL_2(\mathbb{Z}/p\mathbb{Z})$ acts on $\overline{X(p)}$. Since $\rho : \text{Gal}(K/\mathbb{Q}) \hookrightarrow GL_2(\mathbb{Z}/p\mathbb{Z})$, the group $\text{Gal}(K/\mathbb{Q})$ acts on $\overline{X(p)}$. The Galois group $\text{Gal}(K/\mathbb{Q})$ has a natural action on $\text{Spec}(O_K[1/pd])$ and we can descend via the quotient process X' to $\overline{X'(p)}/\text{Spec}(\mathbb{Z}[1/pd])$ using the diagonal action

$$\text{Gal}(K/\mathbb{Q}) \ni \sigma \rightarrow \rho(\sigma) \otimes \sigma$$

on X' . Thus, we obtain a smooth projective curve $\overline{X'(p)}/\text{Spec}(\mathbb{Z}[1/pd])$. This is the twisted curve that we mentioned in the title. If we do descend as above the jacobian of $\overline{X(p)}/\text{Spec}(\mathbb{Z}[1/pd])$, we obtain the jacobian of $\overline{X'(p)}/\text{Spec}(\mathbb{Z}[1/pd])$.

2.3 The zeta function for curves

We recall briefly the definition of the H^1 -part of the Hasse-Weil zeta function of a smooth projective curve X over $S = \text{Spec}(\mathbb{Z}[1/N])$ where N is a positive integer. We hereafter call the H^1 -part, the zeta function of X for simplicity. First let us consider \mathbb{F}_p the finite field of cardinality p and J/\mathbb{F}_p an abelian variety. Let $J[l^n] := J[l^n](\overline{\mathbb{F}_p})$ be the l^n -torsion points for a prime number $l \neq p$. The Galois group $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ acts on $J[l^n]$ for all natural numbers n and taking the limit

$$T_l(J) = \varprojlim J[l^n],$$

we get the $\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ -module $T_l(J)$. We write

$$\rho_l : \text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \rightarrow GL(T_l(J))$$

for the resulting representation. Let $L_p(T) = \det(1 - \rho_l(\phi_p)T)$, where ϕ_p is the Frobenius element

$$\text{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \ni (x \rightarrow x^p).$$

The polynomial $L_p(T) \in \mathbb{Z}[T]$ does not depend on l .

Now, let X be a smooth proper curve over $S = \text{Spec}(\mathbb{Z}[1/N])$, and J be the jacobian of X . Then J is an abelian scheme over $S = \text{Spec}(\mathbb{Z}[1/N])$. We denote

$$J(l) = J \times_{\text{Spec}(\mathbb{Z}[1/N])} \text{Spec}(\mathbb{F}_l),$$

for l prime, $l \nmid N$. We define the zeta function of X over $S = \text{Spec}(\mathbb{Z}[1/N])$ as the product

$$L(s, X/S) = \prod_{l \nmid N} L_l(l^{-s})^{-1}$$

Here the definition of the zeta function is given up to the factors at $l|N$.

2.4 The twisted Galois action on J

To simplify the notations we regard our curves $\overline{X(p)}$ and $\overline{X'(p)}$ as curves over $\text{Spec}(\mathbb{Q})$. Let J and J' be the jacobians of $\overline{X(p)}$ and $\overline{X'(p)}$ respectively.

We obtained $\overline{X'(p)}$ from $\overline{X(p)}$ first tensoring by $\text{Spec}(O_K[1/pd])$ and then making the diagonal quotient. The difference of the action of $G_{\mathbb{Q}}$ on the Tate modules $T_l(J)$ and $T_l(J')$ can be described in the following way: as \mathbb{Z}_l -modules, we have $T_l(J) = T_l(J')$, but the Galois action is different. We write the Galois action of $\sigma \in G_{\mathbb{Q}}$ on $T_l(J)$ as $x \rightarrow x^\sigma$. We want to describe the action of $G_{\mathbb{Q}}$ on $T_l(J')$ in terms of the action of $G_{\mathbb{Q}}$ on $T_l(J)$ and

$$\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}/p\mathbb{Z}).$$

The Galois representation ρ composed with the action of $GL_2(\mathbb{Z}/p\mathbb{Z})$ on $\overline{X(p)}$ induces a representation

$$\rho'' : G_{\mathbb{Q}} \rightarrow \text{Aut}(T_l(J)).$$

Proposition 2.2. *The action of $\sigma \in G_{\mathbb{Q}}$ on $T_l(J')$ is given by*

$$x \mapsto \rho''(\sigma)x^\sigma.$$

Proof: Denote by $\rho' : G_{\mathbb{Q}} \rightarrow \text{Aut}(\overline{X(p)})$ be the composition of $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}/p\mathbb{Z})$ and of the action of $GL_2(\mathbb{Z}/p\mathbb{Z})$ on $\overline{X(p)}$. Let $W = \overline{X(p)} \times_{\text{Spec}(\mathbb{Q})} \text{Spec}(\overline{\mathbb{Q}})$. We have

$$W(\overline{\mathbb{Q}}) = \text{Hom}_{\text{Spec}(\mathbb{Q})}(\text{Spec}(\overline{\mathbb{Q}}), \overline{X(p)}) \times \text{Hom}_{\mathbb{Q}}(\overline{\mathbb{Q}}, \overline{\mathbb{Q}}).$$

An element $\tau \in G_{\mathbb{Q}}$ acts on $W(\overline{\mathbb{Q}})$ by

$$\tau(x, g) = (\rho'(\tau)(x), g\tau^{-1}),$$

where $(x, g) \in W(\overline{\mathbb{Q}})$. This is the diagonal action on $W(\overline{\mathbb{Q}})$ that we use to do descent. In this circumstance, we can realize the descent as a geometric quotient of W by the action of $G_{\mathbb{Q}}$.

Since $\overline{X'(p)}$ is obtained from $\overline{X(p)} \times_{\text{Spec}(\mathbb{Q})} \text{Spec}(K)$ by a twist of $\text{Gal}(K/\mathbb{Q})$ -action, we have

$$\overline{X(p)} \times_{\text{Spec}(\mathbb{Q})} \text{Spec}(K) = \overline{X'(p)} \times_{\text{Spec}(\mathbb{Q})} \text{Spec}(K).$$

Thus, we get $\overline{X(p)}(\overline{\mathbb{Q}}) = \overline{X'(p)}(\overline{\mathbb{Q}})$. Let $u = [(x, 1)] \in \overline{X'(p)}(\overline{\mathbb{Q}}) = \overline{X(p)}(\overline{\mathbb{Q}})$ be a class of the quotient of $W(\overline{\mathbb{Q}})$, determined by the above action. The group $G_{\mathbb{Q}}$ acts through its arithmetic action on $\overline{X(p)}(\overline{\mathbb{Q}})$ sending

$$u \rightarrow u^\sigma = [(x^\sigma, 1)].$$

Then we describe the action of $G_{\mathbb{Q}}$ on $\overline{X'(p)}(\overline{\mathbb{Q}})$ in terms of the action of $G_{\mathbb{Q}}$ on $\overline{X(p)}(\overline{\mathbb{Q}})$:

$$u \rightarrow u^{\sigma'} = [(x, 1)]^{\sigma'} =$$

$$[(x^{\sigma}, \sigma)] = [\sigma^{-1}(\rho'(\sigma)x^{\sigma}, 1)] = [(\rho'(\sigma)x^{\sigma}, 1)] = \rho'(\sigma)[(x^{\sigma}, 1)] = \rho'(\sigma)u^{\sigma},$$

where we attach a ' to σ to indicate when we refer to the action of $G_{\mathbb{Q}}$ on $\overline{X'(p)}(\overline{\mathbb{Q}})$.

Thus $\sigma \in G_{\mathbb{Q}}$ acts on $\overline{X'(p)}(\overline{\mathbb{Q}})$ by sending $u \rightarrow \rho'(\sigma)u^{\sigma}$. We explained above the action of $G_{\mathbb{Q}}$ on $\overline{X'(p)}(\overline{\mathbb{Q}})$ in terms of the action of $G_{\mathbb{Q}}$ on $\overline{X(p)}(\overline{\mathbb{Q}})$. We obtain the same result if we replace $\overline{X(p)}$ and $\overline{X'(p)}$ by their jacobians and by their Tate modules. ■

2.5 Complex points on the modular curve

We have:

$$X(p)(\mathbb{C}) = GL_2(\mathbb{Q}) \backslash GL_2(\mathbb{A}_{\mathbb{Q}}) / \hat{\Gamma}(p) SO_2(\mathbb{R}) \mathbb{R}^{\times}$$

where $\mathbb{A}_{\mathbb{Q}}$ is the adèle ring of \mathbb{Q} and

$$\hat{\Gamma}(p) = \{x \in GL_2(\hat{\mathbb{Z}}) | x \equiv 1(p)\}$$

with $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

The group $GL_2(\mathbb{Z}/p\mathbb{Z})$ acts on $X(p)(\mathbb{C})$. This action can be described as follows: $GL_2(\mathbb{Z}_p) \hookrightarrow GL_2(\mathbb{A}_{\mathbb{Q}})$ by $\alpha \mapsto (1, \dots, \alpha, 1, \dots, 1)$ (α is the p -component). Using the isomorphism $GL_2(\mathbb{Z}/p\mathbb{Z}) \cong GL_2(\mathbb{Z}_p) / \hat{\Gamma}(p)_p$, where

$$\hat{\Gamma}(p)_p = \{x \in GL_2(\mathbb{Z}_p) | x \equiv 1(p)\},$$

we get the action of $g \in GL_2(\mathbb{Z}_p)$ on $X(p)(\mathbb{C})$ which is given by the right multiplication at the p -component.

2.6 The zeta function of the twisted curve

Let $\pi = \pi_f \otimes \pi_{\infty}$ be a cuspidal automorphic representation of $GL_2(\mathbb{A}_{\mathbb{Q}})$, where π_f and π_{∞} are representations of $GL_2(\mathbb{A}_f)$ and $GL_2(\mathbb{R})$, respectively. Let

$$\rho_{\pi, l} : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{Q}}_l),$$

l prime, $l \neq p$ be the two dimensional continuous Galois representation associated to π . If K is an open compact subgroup of $GL_2(\mathbb{A}_f)$, let π_f^K denote the space of K -fixed vectors of π_f .

By the work of Shimura and others we know that

$$L(\overline{X(p)}, s) = \prod_{\pi} L(s - 1/2, \pi)^{\dim \pi_f^{\hat{\Gamma}(p)}},$$

where the π' s which appear in the product are of weight 2, satisfy $\pi_f^{\hat{\Gamma}(p)} \neq \{0\}$ and are cohomological i.e. $H^1(\mathfrak{gl}_2(\mathbb{R}), SO_2(\mathbb{R}); \pi_\infty) \neq 0$.

We consider the decomposition of the cohomology with compact support of $\overline{X(p)}$:

$$H_c^1(\overline{X(p)}, \mathbb{C}) = \oplus_\pi H^1(\mathfrak{gl}_2(\mathbb{R}), SO_2(\mathbb{R}); \pi_\infty) \otimes \pi_f^{\hat{\Gamma}(p)},$$

where the π' s which appear in the product are of weight 2, satisfy $\pi_f^{\hat{\Gamma}(p)} \neq \{0\}$ and are cohomological. The space $H^1(\mathfrak{gl}_2(\mathbb{R}), SO_2(\mathbb{R}); \pi_\infty)$ is a 2-dimensional complex vector space. On each of the above summands, $GL_2(\mathbb{Z}/p\mathbb{Z})$ acts through a representation of the form $1 \otimes {}^t \varphi_\pi^{-1}$, where φ_π is the natural representation of $GL_2(\mathbb{Z}/p\mathbb{Z})$ on $\pi_f^{\hat{\Gamma}(p)}$. The space $H_{et}^1(\overline{X(p)}, \overline{\mathbb{Q}}_l)$ has a decomposition of the same form as $H_c^1(\overline{X(p)}, \mathbb{C})$:

$$H_{et}^1(\overline{X(p)}, \overline{\mathbb{Q}}_l) = \oplus_\pi U_{\overline{\mathbb{Q}}_l}(\pi) \otimes_{\overline{\mathbb{Q}}_l} \tilde{\pi}_f^{\hat{\Gamma}(p)},$$

where the π' s which appear in the product are of weight 2, satisfy $\pi_f^{\hat{\Gamma}(p)} \neq \{0\}$ and are cohomological, $U_{\overline{\mathbb{Q}}_l}(\pi)$ is the $\overline{\mathbb{Q}}_l$ -space of dimension 2 and $\tilde{\pi}_f^{\hat{\Gamma}(p)}$ is a $\overline{\mathbb{Q}}_l$ -space. The group $G_{\mathbb{Q}}$ acts on each summand of $H_{et}^1(\overline{X(p)}, \overline{\mathbb{Q}}_l)$ by a representation of the form ${}^t \rho_{\pi,l}^{-1} \otimes 1$. We denote by $\tilde{\varphi}_\pi$ the representation on $\tilde{\pi}_f^{\hat{\Gamma}(p)}$ which corresponds to φ_π . Since $H_{et}^1(\overline{X(p)}, \overline{\mathbb{Q}}_l) \cong T_l(J)^\vee \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}}_l$ (here $T_l(J)^\vee$ is the dual space of $T_l(J)$) we obtain a decomposition of the same form as above for $V = T_l(J) \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}}_l$ and write $V[\pi]$ (see the above decomposition) for the π component. By the result of Shimura and the irreducibility of $\rho_{\pi,l}$ (the irreducibility of $\rho_{\pi,l}$ is proved in §3.2) and multiplicity one of π combined, $V[\pi]$ is isomorphic to $\rho_{\pi,l} \otimes \tilde{\varphi}_\pi$ as $(G_{\mathbb{Q}}, GL_2(\mathbb{Z}/p\mathbb{Z}))$ -module. For the twist J' of J we put $V' = T_l(J') \otimes_{\mathbb{Z}_l} \overline{\mathbb{Q}}_l$. Then by proposition 2.2, the action of $G_{\mathbb{Q}}$ on $V'[\pi]$ is given by $\rho_{\pi,l} \otimes (\tilde{\varphi}_\pi \circ \rho)$. Thus, we get

$$L(s, \overline{X'(p)}) = \prod_\pi L(s, \rho_{\pi,l} \otimes (\tilde{\varphi}_\pi \circ \rho)).$$

Hence, we proved the following result, which is the first part of the theorem 1.1 in the introduction:

Proposition 2.3. *The zeta function of the curve $\overline{X'(p)}$ which is obtained from the compactified modular curve $\overline{X(p)}$ via twisting by a continuous Galois representation $\rho : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}/p\mathbb{Z})$ composed with the natural action of $GL_2(\mathbb{Z}/p\mathbb{Z})$ on $\overline{X(p)}$ is equal to:*

$$L(s, \overline{X'(p)}) = \prod_\pi L(s, \rho_{\pi,l} \otimes (\tilde{\varphi}_\pi \circ \rho))$$

where the π' s which appear in the product are of weight 2, with $\pi_f^{\hat{\Gamma}(p)} \neq \{0\}$ and are cohomological.

Remark 2.4. We computed the zeta function of $\overline{X'(p)}$ only up to Euler factors at the prime numbers $l|pd$, where d is the discriminant of K/\mathbb{Q} .

Remark 2.5. We can replace p and $\overline{X(p)}$ in the proof of the theorem 1.1 by an arbitrary positive integer N and $\overline{X(N)}$ and obtain essentially the same result.

Actually we studied the twisted curves slightly different from those used in [W] in order to treat the general ρ . The Galois representation ρ that Wiles used in [W] comes from an elliptic curve over \mathbb{Q} . Thus its action on $\mathbb{Q}(\zeta_p)$ is given by $\det \rho$ composed with the cyclotomic character $(\mathbb{Z}/p\mathbb{Z})^\times \cong \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$. Hence the action coincides with the action of $GL_2(\mathbb{Z}/p\mathbb{Z}) \subset \text{Aut}(\overline{X(p)})$ on $\mathbb{Q}(\zeta_p)$; so, we can actually make quotient of $\overline{X(p)} \otimes_{\text{Spec}(\mathbb{Q}(\zeta_p))} \text{Spec}(K)$ by the diagonal action. The new curve thus obtained, slightly different from the one we studied, is the curve Wiles used whose zeta function can be computed in the same manner as we described.

3 Meromorphic continuation

In this section we prove that the zeta function $L(s, \overline{X'(p)})$ can be continued meromorphically to the entire complex plane and satisfies a functional equation. Since

$$L(s, \overline{X'(p)}) = \prod_{\pi} L(s, \rho_{\pi, l} \otimes (\tilde{\varphi}_{\pi} \circ \rho)),$$

it is sufficient to continue meromorphically the function $L(s, \rho_l \otimes \omega)$, where ρ_l is the Galois representation

$$\rho_l : G_{\mathbb{Q}} \rightarrow GL_2(\overline{\mathbb{Q}}_l) \cong GL_2(\mathbb{C}),$$

l prime, $l \neq p$ associated to a cuspidal automorphic representation π of weight 2, with $\pi_f^{\hat{\Gamma}(p)} \neq \{0\}$ and $\omega : G_{\mathbb{Q}} \rightarrow GL_N(\mathbb{C})$ is an Artin representation.

Let $Q_f := \mathbb{Q}(a(q)|q \text{ prime}, q \nmid lp)$, where $a(q) := \text{Tr}(\rho_l(\text{Frob}_q))$ if $q \nmid lp$, and Frob_q is the Frobenius element at q (ρ_l is unramified outside lp). If we change the prime l , then we obtain also the value of $a(l)$. It is known that Q_f is a finite extension of \mathbb{Q} . The field Q_f is the minimal field of rationality of π . Let O_f be the integer ring of Q_f and O_l the l completion of O_f for a prime factor l of l in Q_f . Then, $\rho_l : G_{\mathbb{Q}} \rightarrow GL_2(O_l)$ is continuous, unramified outside lp and satisfies $\text{Tr}(\rho_l(\text{Frob}_q)) = a(q)$ and $\det(\rho_l(\text{Frob}_q)) = \epsilon(q)q$ for q prime, $q \nmid lp$, where ϵ is a Dirichlet character. Strictly speaking, we should have written ρ_l instead of ρ_l , but we keep the symbol ρ_l to simplify our notation. We say that π is of CM type if the associated representation ρ_l is an induced from a Galois character of G_M for a quadratic imaginary extension M/\mathbb{Q} .

Define $K := \overline{\mathbb{Q}}^{\text{Ker}(\omega)}$.

3.1 CM case

First we consider the case when π is of CM type. By the work of Langlands and Jacquet (see theorem 7.4 of [G]) for any number field E , one can find an

automorphic representation φ of $GL_2(\mathbb{A}_E)$ and a place λ of the minimal field of rationality of φ above l such that $\rho_{\varphi,\lambda} \cong \rho_l|_{G_E}$. We take the number field E to be a Galois extension of \mathbb{Q} which contains K .

By Brauer's theorem (see theorems 16 and 19 of [SE]), we can find some fields $F_i \subset E$ such that $\text{Gal}(E/F_i)$ are solvable and some characters $\chi_i : \text{Gal}(E/F_i) \rightarrow \mathbb{C}^\times$ and some integers m_i such that the representation

$$\omega : \text{Gal}(E/\mathbb{Q}) \rightarrow \text{Gal}(K/\mathbb{Q}) \rightarrow GL_N(\mathbb{C}),$$

can be written as

$$\omega = \sum_{i=1}^{i=k} m_i \text{Ind}_{G_{F_i}}^{G_{\mathbb{Q}}} \chi_i,$$

as a virtual sum. We denote also by χ_i the corresponding character of $\mathbb{A}_{F_i}^\times/F_i^\times$ by class field theory. We know (see [L], lemma 11.6) that there is a cuspidal automorphic representation φ_i of $GL_2(\mathbb{A}_{F_i})$ and a prime λ_1 above l such that $\rho_l|_{G_{F_i}} \cong \rho_{\varphi_i,\lambda_1}$. Then we have

$$\begin{aligned} L(s, \rho_l \otimes \omega) &= \prod_{i=1}^{i=k} L(s, \rho_l \otimes \text{Ind}_{G_{F_i}}^{G_{\mathbb{Q}}} \chi_i)^{m_i} = \\ &= \prod_{i=1}^{i=k} L(s, \text{Ind}_{G_{F_i}}^{G_{\mathbb{Q}}} (\rho_l|_{G_{F_i}} \otimes \chi_i))^{m_i} = \prod_{i=1}^{i=k} L(s - 1/2, \varphi_i \otimes \chi_i \circ \det)^{m_i} \end{aligned}$$

which is a product of L-functions that have a meromorphic continuation to the entire complex plane and satisfy a functional equation. Thus $L(s, \rho_l \otimes \omega)$ can be meromorphically continued to the entire complex plane when π is of CM type.

3.2 Solvable extension of a totally real field and non-CM case

We consider the case when K/\mathbb{Q} is a solvable extension of a totally real field F and π is not of CM type. We prove in this case that $L(s, \rho_l \otimes \omega)$ has a meromorphic continuation and satisfies a functional equation. Let ϵ_l be the l -adic cyclotomic character: $\epsilon_l : G_M \rightarrow \mathbb{Z}_l^\times$ for l a prime number and M a number field. We want to use the following theorem of R. Taylor (this statement is a combination of theorem 1.6 and Corollary 1.7 of [T]):

Theorem 3.1 (R.Taylor). *Suppose that l is an odd prime and that k/\mathbb{F}_l is a finite extension. Let F be a totally real field and $\rho' : G_F \rightarrow GL_2(k)$ a continuous representation. Suppose that the following conditions hold:*

1. *the representation ρ' is irreducible,*
2. *for every place v of F above l we have*

$$\rho'|_{G_v} \cong \begin{pmatrix} \epsilon_l \chi_{v,1} & * \\ 0 & \chi_{v,2} \end{pmatrix}$$

where G_v is the decomposition group above v ,

3. for every complex conjugation c , we have $\det \rho'(c) = -1$.

Then there exists a finite Galois totally real extension E/F in which every prime of F above l splits completely, a cuspidal automorphic representation φ of $GL_2(\mathbb{A}_E)$ and a place λ' of the minimal field of rationality of φ above l such that $\bar{\rho}_{\varphi, \lambda'} \cong \rho'|_{G_E}$, where $\rho_{\varphi, \lambda'} : G_E \rightarrow GL_2(M_{\lambda'})$ is the continuous irreducible representation associated to φ , the field M is the minimal field of rationality of φ and $\bar{\rho}_{\varphi, \lambda'}$ is the reduction of $\rho_{\varphi, \lambda'}$ modulo λ' .

Moreover, if $\rho'(I_{v'})$ does not consist of scalar matrices for every place v' of E above l ($I_{v'}$ is the inertia group at v'), then the representation φ can be chosen such that

$$\rho_{\varphi, \lambda'}|_{G_{v'}} \cong \begin{pmatrix} \mu_{v', 1} & * \\ 0 & \mu_{v', 2} \end{pmatrix}$$

where $G_{v'}$ is the decomposition group above v' and the characters $\mu_{v', 1}$ and $\mu_{v', 2}$ are the lifts of $\epsilon_l \chi_{v, 1}$ and $\chi_{v, 2}$ respectively, if v' divides v .

One can prove that the field E which appears in the above theorem can be taken to be Galois over \mathbb{Q} by the following argument. By a M -HBAV over a field E we mean a triple (A, i, j) , where

1. A/E is an abelian variety of dimension $[M : \mathbb{Q}]$,
2. $i : O_M \hookrightarrow \text{End}(A/E)$ (algebra homomorphism which takes 1 to identity),
3. j is an isomorphism of ordered invertible O_M -modules (see the page 133 of [T] for details).

In his paper (see the page 136 of [T]), Taylor finds a prime p , a totally real field M , a totally real extension E/F in which p splits completely, a quadratic extension L/F in which every place above l and p splits and a M -HBAV $(A, i, j)/E$ such that the representation of G_E on $A[\lambda]$ is equivalent to $\rho'|_{G_E}$, and the representation of G_E on $A[\mathfrak{p}]$ is equivalent to $\text{Ind}_{G_L}^{G_E} \psi|_{G_E}$ for some character ψ of G_L . Here λ and \mathfrak{p} are primes of M over l and p (then he uses theorem 5.1 of [SW], i.e. theorem 3.6 below, to prove theorem 3.1). Taking the Galois closure E^{gal} of E , the prime p also splits completely in E^{gal} and the above properties are satisfied for M -HBAV $(A, i, j)/E^{gal}$. Thus we obtain the result that we wanted.

We shall now verify the conditions of theorem 3.1 for some prime number l and $\rho' := \bar{\rho}_l|_{G_F}$. We remark that in order to find a M -HBAV (A, i, j) as above, in [T] it was assumed that the image of the representation ρ' is not solvable, but using proposition 3.5 below, we can assume this fact.

For l rational prime we say that π is l -ordinary if $a(l)$ is a unit in O_l . We have the following result (see proposition 2.2 of [F]):

Proposition 3.2 (Serre). *Any cuspidal automorphic representation π of weight 2 as above is l -ordinary for a set of primes of density 1.*

Using the same notations as above, we know by the work of Deligne, Mazur and Wiles the following result (see theorem 3.26 of [H2]):

Theorem 3.3 (Deligne, Mazur-Wiles). *If $a(l)$ is a unit in O_l for a prime factor l of l , then*

$$\rho_l|_{G_l} \cong \begin{pmatrix} \epsilon_l \delta_2 & * \\ 0 & \delta_1 \end{pmatrix}$$

where G_l is the decomposition group at l , δ_2 and δ_1 are finite order characters, and the character δ_1 is unramified.

We remark that we can use proposition 3.2 to find a prime l and a prime ideal \mathfrak{l} , such that $a(l)$ is a unit in O_l . Thus, the conditions of theorem 3.3 are satisfied and we can choose l such that $\bar{\rho}_l|_{G_F}$ satisfies the condition 2 of the theorem 3.1. Also, it is known that $\det \rho_l(c) = -1$, so we have $\det \rho_l|_{G_F}(c) = -1$ for all the complex conjugations c , thus the condition 3 of the theorem 3.1 is satisfied.

We now verify the condition 1 of theorem 3.1 i.e. the irreducibility of $\bar{\rho}_l|_{G_F}$.

Let \mathbb{F}_l be the residue field of O_l mod the maximal ideal and $\bar{\rho}_l$ be the reduction of $\rho_l : G_{\mathbb{Q}} \rightarrow GL_2(O_l)$. By a nice result of Ribet (see §4 of [R]) we have:

Proposition 3.4 (K. Ribet). *For all but finite l , the representation $\bar{\rho}_l$ is full if π is not of CM type, i.e. $SL_2(\mathbb{F}_l) \subset \bar{\rho}_l(G_{\mathbb{Q}})$.*

Actually Ribet proved a slightly stronger result concerning $SL_2(\mathbb{F}_l^s)$ for an explicit $0 < s \leq r$. Thus we can choose an odd prime l such that $SL_2(\mathbb{F}_l) \subset \bar{\rho}_l(G_{\mathbb{Q}})$. We prove the following result:

Proposition 3.5. *For all but finite l , the representation $\bar{\rho}_l|_{G_E}$ is full and hence irreducible for any totally real extension E/F .*

Proof: By using proposition 3.4 we may assume that l is odd and that $SL_2(\mathbb{F}_l) \subset \bar{\rho}_l(G_{\mathbb{Q}})$. For any $x \in G_{\mathbb{Q}}$, xcx^{-1} fixes E , because E is totally real. Since $\text{im}(\bar{\rho}_l)$ contains $SL_2(\mathbb{F}_l)$, we have that $\text{im}(\bar{\rho}_l|_{G_E})$ contains all the $SL_2(\mathbb{F}_l)$ conjugates of $\bar{\rho}_l(c)$. We can choose a basis for ρ_l such that $\rho_l(c)$ is the diagonal matrix with diagonal entries 1 and -1 . Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{F}_l)$. Then we

have that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad + bc & -2ab \\ 2cd & -bc - da \end{pmatrix} \in \text{im}(\bar{\rho}_l|_{G_E})$. For $a = d = 1$ and $c = 0$ we get that

$\begin{pmatrix} 1 & 2b \\ 0 & -1 \end{pmatrix} \in \text{im}(\bar{\rho}_l|_{G_E})$. Thus, we have $\begin{pmatrix} 1 & -2b \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & -2b \\ 0 & 1 \end{pmatrix} \in \text{im}(\bar{\rho}_l|_{G_E})$. Since 2 is invertible in \mathbb{F}_l and b is an arbitrary element of \mathbb{F}_l ,

we get that $\text{im}(\bar{\rho}_l|_{G_E})$ contains all the elements of the form $\begin{pmatrix} 1 & e \\ 0 & -1 \end{pmatrix}$ with

$e \in \mathbb{F}_l$. For $a = d = 1$ and $b = 0$ we get $\begin{pmatrix} 1 & 0 \\ 2c & -1 \end{pmatrix} \in \text{im}(\bar{\rho}_l|_{G_E})$. Thus,

$\begin{pmatrix} 1 & 0 \\ 2c & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 2c & 1 \end{pmatrix} \in \text{im}(\bar{\rho}_l|_{G_E})$ and we obtain that $\text{im}(\bar{\rho}_l|_{G_E})$ contains all the elements of the form $\begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix}$ for $f \in \mathbb{F}_l$. But the elements $\begin{pmatrix} 1 & e \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ f & 1 \end{pmatrix}$ with $e, f \in \mathbb{F}_l$ generate $SL_2(\mathbb{F}_l)$, so $\bar{\rho}_l|_{G_E}$ is full. Thus, $\bar{\rho}_l|_{G_E}$ is irreducible. ■

So we proved that we can find l such that $\bar{\rho}_l|_{G_F}$ is irreducible and satisfies the conditions 2 and 3 of the theorem 3.1. We fix an l which satisfies these proprieties. Thus, we can conclude using theorem 3.1, that there exists a Galois totally real extension E of \mathbb{Q} , which contains F , a cuspidal automorphic representation φ' of $GL_2(\mathbb{A}_E)$ and a place λ' of the field of coefficients of φ' above l such that $\bar{\rho}_{\varphi', \lambda'} \cong \bar{\rho}_l|_{G_E}$.

Now we use the following result (this is theorem 5.1 of [SW]):

Theorem 3.6. *Let F be a totally real number field and let $\rho : \text{Gal}(\bar{F}/F) \rightarrow GL_2(\mathbb{Q}_l)$ be a representation satisfying:*

1. ρ is continuous and irreducible,
2. ρ is unramified at all but a finite number of finite places,
3. $\det \rho(c) = -1$ for all complex conjugations c ,
4. $\det \rho = \psi \epsilon_l$, where ψ is a character of finite order,
5. $\rho|_{D_i} \cong \begin{pmatrix} \psi_1^i & * \\ 0 & \psi_2^i \end{pmatrix}$, with $\psi_2|_{I_i}$ having finite order, where D_i , for $i = 1, \dots, t$ are decomposition groups at the places v_1, \dots, v_t of F dividing l , and $I_i \subset D_i$ are inertia groups,
6. $\bar{\rho}$ is irreducible and $\bar{\rho}|_{D_i} \cong \begin{pmatrix} \chi_1^i & * \\ 0 & \chi_2^i \end{pmatrix}$, $i = 1, \dots, t$, with $\chi_1^i \neq \chi_2^i$ and $\chi_2^i = \psi_2^i \pmod{\lambda}$,
7. there exists an automorphic representation π_0 of $GL_2(\mathbb{A}_F)$ and a prime λ_0 of the field of coefficients of π_0 above l such that $\bar{\rho}_{\pi_0, \lambda_0} \cong \bar{\rho}$ and $\rho_{\pi_0, \lambda_0}|_{D_i} \cong \begin{pmatrix} \phi_1^i & * \\ 0 & \phi_2^i \end{pmatrix}$, $i = 1, \dots, t$, and $\chi_2^i = \phi_2^i \pmod{\lambda}$.

Then we have $\rho \cong \rho_{\pi, \lambda_1}$ for some automorphic representation π and some prime λ_1 of the field of coefficients of π above l .

Now we show that the representation $\rho_l|_{G_E}$ satisfies all the conditions of the theorem 3.6: the representation $\rho_l|_{G_E}$ is irreducible, since we have chosen l so that $\bar{\rho}_l|_{G_E}$ is irreducible; the conditions 1, 2, 3, 4 are satisfied (see the beginning of §2); the condition 5 is proved by theorem 3.3 out of our choice of l ; the condition 6 is satisfied also (for a big l), since we proved that $\bar{\rho}_l|_{G_E}$ is irreducible by our choice of l and (using the notations of the theorem 3.3) we have $\epsilon_l \delta_2 \pmod{\lambda} \neq \delta_1 \pmod{\lambda}$ for l sufficiently large, since δ_2 is a finite character independent of l and $\epsilon_l(I_i)$ increases linearly with l , while δ_1 is unramified; the condition 7 is satisfied by theorem 3.1 by our choice of l . Thus we can choose l such that all the conditions of theorem 3.6 are satisfied.

Hence we can apply theorem 3.6 to find an automorphic representation φ of $GL_2(\mathbb{A}_E)$ and a place λ of the field of coefficients of φ above l such that $\rho_{\varphi, \lambda} \cong$

$\rho_l|_{G_E}$. The field K is a solvable extension of F , so the field KE is a solvable extension of E . By Langlands base change for Galois cyclic extensions (see proposition 11.5 of [L]), we get an automorphic representation φ'' of $GL_2(\mathbb{A}_{KE})$ and a place λ'' of the field of the coefficients of φ'' above λ such that $\rho_{\varphi'', \lambda''} \cong \rho_l|_{G_{KE}}$.

Thus we proved the following theorem, which is a combination of the above discussion and the beginning of §3.1:

Theorem 3.7. *If π is a cuspidal automorphic representation of $GL_2(\mathbb{A}_{\mathbb{Q}})$, of weight 2 and K is a solvable extension of a totally real field, then there is a solvable extension of a totally real field K' which contains K , and K' is Galois over \mathbb{Q} , and an automorphic representation φ'' of $GL_2(\mathbb{A}_{K'})$ and a prime λ'' of the field of coefficients of φ'' above l such that $\rho_{\pi, l}|_{G_{K'}} \cong \rho_{\varphi'', \lambda''}$.*

In order to prove the meromorphic continuation of $L(s, \rho_l \otimes \omega)$ we can use the same method as in §3.1. To find φ_i as in §3.1 out of φ'' (in §3.1 the representation was φ), we use the result of Langlands (see lemma 11.6 of [L]) that φ'' descends to φ_i , because KE/F_i is a solvable extension. We deduce that $L(s, \rho_l \otimes \omega)$ can be meromorphically continued to the entire complex plane and satisfies a functional equation when K is solvable extension of a totally real field and π is not of CM type.

Combining this section where we treated the non-CM type case and §3.1, where we treated the CM type case, we can conclude in particular that when the field K is a solvable extension of a totally real field, the function $L(s, \overline{X'(p)})$ has a meromorphic continuation to the entire complex plane and satisfies a functional equation. Thus, we proved the second part of theorem 1.1.

ACKNOWLEDGMENTS

We would like to thank Professor Hida for many helpful discussions and suggestions. The research in this paper has been supported partially by Prof. Hida's NSF grant: DMS 9988043 through the graduate student support.

References

- [F] A. Fischman, *On the image of λ -adic Galois representations*, Ann. de l'Institute Fourier 52, fasc.2 ,(2002), 351-378.
- [G] S.S. Gelbart, *Automorphic forms on adèle groups*, Ann. of Mathematics Studies, Princeton University Press, 1975.
- [H1] H. Hida, *Geometric modular forms and elliptic curves*, World Scientific 2000.
- [H2] H. Hida, *Modular forms and Galois cohomology*, Cambridge Studies in Advanced Mathematics 69, Cambridge University Press, 2000.

- [KM] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Ann. of Mathematics Studies 108, Princeton University Press, 1985.
- [L] R. P. Langlands, *Base change for GL_2* , Ann. of Mathematics Studies 96, Princeton University Press, 1980.
- [R] K.A. Ribet *On l -adic Representations attached to modular forms II*, Glasgow Math. J. 27 (1985),185-195.
- [SE] J.-P.Serre, *Linear representations of finite groups*, Springer 1977.
- [SH] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1971.
- [SW] C. Skinner and A. Wiles, *Nearly ordinary deformations of irreducible residual representations*, Ann. Fac. Sci. Toulouse MATH.(6) 10(2001),no. 1, 185-215.
- [T] R.Taylor, *remarks on a conjecture of Fontaine and Mazur*, Journal of the Institute of Mathematics of Jussieu 1 (2002), 125-143.
- [W] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics 141, (1995), 443-551.