

NON-ABELIAN BASE CHANGE FOR TOTALLY REAL FIELDS

HARUZO HIDA AND YOSHITAKA MAEDA¹

In memory of Olga Taussky Todd

1. Introduction.

Let $f \in S_k(\Gamma_0(N), \chi)$ with $k \geq 2$ and $N \geq 1$ be a primitive Hecke eigenform normalized so that the first Fourier coefficient $a(1, f)$ is equal to 1. Let $\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\overline{\mathbb{Q}}_p)$ be the p -adic Galois representation attached to f . Then writing $f|T(n) = \lambda(T(n))f$ for the Hecke operators $T(n)$, we have $\lambda(T(n)) = a(n, f)$ and

$$L(s, \rho) = L(s, f) = L(s, \lambda) = \sum_{n=1}^{\infty} \lambda(T(n))n^{-s}.$$

Let F be a number field. A cohomological Hecke eigen cusp form \widehat{f} on $GL_2(F_{\mathbb{A}})$ for the adèle ring $F_{\mathbb{A}}$ of F is called a base change of f if $L(s, \widehat{f}) = L(s, \rho_F)$ for $\rho_F = \rho|_{\text{Gal}(\overline{\mathbb{Q}}/F)}$. When \widehat{f} exists, we call f “liftable to F ” or “ F -liftable”. When F is totally real, a Hilbert cusp form is cohomological if and only if it is holomorphic of weight $k \geq 2$ at every archimedean place of F . Since the definition of the base change \widehat{f} is given in purely algebraic terms, it is a non-trivial problem to find the base-change form \widehat{f} in the space of cohomological forms characterized by analytic means. This problem was first studied by Doi and Naganuma [DN] and [N] for quadratic extensions F/\mathbb{Q} , and the existence of \widehat{f} was later proved by Langlands [L] for relative prime cyclic cases (so eventually covering all solvable cases).

In this paper, under a simple ramification condition on totally real F , we prove the existence of infinitely many F -liftable holomorphic elliptic cusp forms of a given odd prime power level (including 1). Our idea is as follows. Let $p > 2$ be a prime. We start from a (minimally) modular Galois representation $\bar{\rho} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F})$ unramified outside $\{p, \infty\}$. Here the

¹Research of the first author is partially supported by an NSF grant; this paper was written while the second named author was visiting UCLA, and he likes to thank the Mathematics department of UCLA for their hospitality.

word: “modular” means that there exists a Hecke eigenform $f \in S_k(SL_2(\mathbb{Z}))$ such that its p -adic Galois representation $\rho = \rho_f : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathcal{O})$ is a deformation of $\bar{\rho}$, that is, $\bar{\rho} \cong \rho \pmod{\mathfrak{m}_{\mathcal{O}}}$, where \mathcal{O} is a valuation ring with maximal ideal $\mathfrak{m}_{\mathcal{O}}$ finite flat over the p -adic integer ring \mathbb{Z}_p . Suppose that $\bar{\rho}$ is minimally modular again over F in an obvious sense generalizing the above definition. Under certain assumptions on F and on $\bar{\rho}$ (like, p -ordinarity and absolute irreducibility), we can deduce from the Hilbert modular generalization by Fujiwara [F] of a result of Taylor and Wiles [TW] (see also [W]), any p -ordinary deformation ϱ of $\bar{\rho}_F = \bar{\rho}|_{\text{Gal}(\overline{\mathbb{Q}}/F)}$ unramified outside $\{p, \infty\}$ is associated to a Hilbert Hecke eigenform provided that $\det(\varrho)$ is an arithmetic character (Proposition 4.4). In this ideal situation, any p -ordinary deformation g of f is liftable to F , and if g is classical (not just a p -adic modular form), \widehat{g} is actually a classical Hilbert cusp form. Thus the idea is simple, but it is a bit hard to verify if $\bar{\rho}_F$ is modular or not. Anyway our approach to Langlands’ functoriality is from the Galois side not from the automorphic side, reversing the direction. This type of approach was first realized in a paper of Clozel [C], in which he applied the technique of Wiles to the descent problem of Galois invariant Hilbert modular forms.

We now ease the modularity condition a bit. Starting with f , try to find a sequence of elliptic Hecke eigenforms $f_j \in S_{k_j}(\Gamma_0(N_j), \chi_j)$ for a suitable level N_j such that $f_j \equiv f_{j-1}^{\sigma_j} \pmod{\mathfrak{l}_j}$ for $\sigma_j \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and for a prime \mathfrak{l}_j of $\overline{\mathbb{Q}}$ dividing an odd prime ℓ_j . We write $f \sim f_j$ if such a sequence of congruence (and Galois conjugation) exists. If we can find F -liftable f_j , then applying the above argument to the prime ℓ_j in place of p , the base change lift \widehat{f}_{j-1} would exist. Then applying the above argument for ℓ_{j-1} in place of p to f_{j-2} and \widehat{f}_{j-1} , f_{j-2} would be liftable to F , and so on, getting eventually the existence of f by induction. However at the present stage of knowledge, to make the above argument work, we need to assume the following conditions on $\chi = \chi_j$, $\ell = \ell_j$, $\mathfrak{l} = \mathfrak{l}_j$ and $\phi = f_j$ for all j (see Corollary 4.5 in the text):

- (1) ϕ is \mathfrak{l} -ordinary, that is, $a(\ell, \phi)$ is prime to \mathfrak{l} ;
- (2) The Galois representation $\bar{\rho}_{\mathfrak{l}, \phi}$ of ϕ modulo \mathfrak{l} is absolutely irreducible as a representation of $\text{Gal}\left(\overline{\mathbb{Q}}/F\left(\sqrt{(-1)^{(\ell-1)/2}\ell}\right)\right)$;
- (3) ℓ is odd and is unramified in F/\mathbb{Q} ;
- (4) χ has conductor equal to the level of ϕ and has order prime to ℓ .

Anyway, by the p -adic density of weight 2 modular forms in the space of p -adic modular forms [H86], we may assume that $k_j = 2$ for all j . Then by an observation of Mazur showing the connectedness of the spectrum of the Hecke algebra of weight 2 over \mathbb{Z} of a given level N , any two common eigenforms f, g of weight 2 are related, that is, $f \sim g$. Thus we can choose g

to be a Hecke eigenform congruent to a theta series $\theta(\varphi)$ for a Hecke character φ of a quadratic extension M/\mathbb{Q} . If MF/F remains to be quadratic, $\widehat{\theta(\varphi)} = \theta(\varphi \circ N_{MF/F})$, and our goal should be achieved if either we could remove the four assumptions mentioned above or could prove the connectedness of the Hecke algebra removing the primes not satisfying the four conditions. We have made an experiment with cusp forms of a prime power level to find a good $\theta(\varphi)$, since at this moment, it is hard to come by a proof of Fujiwara's result removing all the four conditions. In our experiment, it is enough to use three step congruence for forms of level one with weight ≤ 468 except for the case of weight 26, in which we need four step congruence. To state a typical example of our result, we introduce some notation: For a Hecke eigenform $f \in S_k(SL_2(\mathbb{Z}))$, let Σ_f be the (finite) set of odd primes ℓ for which the Galois representation $\bar{\rho}_{\ell, f}$ for $\mathbb{Q}(\sqrt{\ell})$ is reducible as a Galois representation of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell}))$. By Serre [Se1] Theorem 8 and [Se2] 3.2, if $\ell \notin \Sigma_f$, the Galois representation $\bar{\rho}_{\ell}$ satisfies the above condition (2) for $\phi = f$ assuming (3). We consider the following condition on F for a positive integer m :

$$(\text{Hyp}_m) \quad m \text{ is prime to } D_F,$$

where D_F is the discriminant of F . Here is the example of our result.

Proposition 1.1. *Let $f \in S_k(SL_2(\mathbb{Z}))$ be a Hecke eigenform for $12 \leq k \leq 468$. Let $\ell \notin \Sigma_f$ be an odd prime. Then there exists an explicitly computable positive integer m with the following property: Suppose*

- (i) $g \in S_{\kappa}(\Gamma_1(\ell^{\alpha}))$ is a Hecke eigenform for $\alpha \geq 0$ and $\kappa \geq 2$;
- (ii) g is $\mathbb{Q}(\sqrt{\ell})$ -ordinary for $\mathbb{Q}(\sqrt{\ell})$;
- (iii) $g \equiv f \pmod{\ell}$.

Then g is liftable to F provided that F is totally real and satisfies $(\text{Hyp}_{m\ell})$.

The set Σ_f is a finite set. When $f = \Delta \in S_{12}(SL_2(\mathbb{Z}))$, $\Sigma_{\Delta} = \{3, 5, 7, 23, 691\}$ (see [Se2] 3.3) and m is given by $m = 17 \cdot 67$ or $13 \cdot 131$.

Probably, the hypothesis $(\text{Hyp}_{m\ell})$ could be removed, replacing it by the condition that $\ell_j \notin \Sigma_{f_j}$ for each j (in the sequence of congruences), after analysing more the method in [F]. If we could prove the following conjecture of Maeda, we could have substantially generalized our result:

Conjecture 1.2 (Y. Maeda). *The Hecke algebra over \mathbb{Q} of $S_k(SL_2(\mathbb{Z}))$ is simple (that is, a single number field) whose Galois closure over \mathbb{Q} has Galois group isomorphic to a symmetric group \mathfrak{S}_n (with $n = \dim S_k(SL_2(\mathbb{Z}))$).*

The conjecture has been verified numerically to be true for weight $k \leq 468$. If $f \in S_k(SL_2(\mathbb{Z}))$ is liftable to F , then each Galois conjugate of f is F -liftable. Thus if the conjecture holds for k , to prove the proposition, we only need to find one form of weight k liftable to F . For small $k \in \{12, 16, 18, 20, 22, 24, 28, 32, 34\}$, we choose one (small) prime p and $\mathfrak{p}|p$ for which f is \mathfrak{p} -ordinary. By computation, we find a Hecke eigenform $\theta \in S_\kappa\left(\Gamma_0(p), \left(\frac{\cdot}{p}\right)\right)$ such that $\theta \equiv \theta(\varphi) \pmod{\mathfrak{q}}$ for another prime \mathfrak{q} of $\overline{\mathbb{Q}}$ and $\theta \equiv f \pmod{\mathfrak{p}}$. Then under (Hyp_{pq}) for rational primes p, q with $\mathfrak{p}|p$ and $\mathfrak{q}|q$, f is liftable to F . For $k = 26$, we need to use a four step congruence a bit different from the above (see Section 3 for details). For large $26 < k \leq 107126$, we can find a prime ℓ such that $\ell - 1 | k - k_0$ for $k_0 \in \mathcal{K} = \{12, 16, 18, 20, 22, 26\}$. If f is \mathfrak{l} -ordinary ($\mathfrak{l}|\ell$), by the theory of \mathfrak{l} -ordinary forms ([H86]), we can find f' of weight k_0 such that $f \equiv f' \pmod{\mathfrak{l}}$. Since $\ell \in \Sigma_f \iff \ell \in \Sigma_{f'}$, we can easily check numerically that $\ell \notin \Sigma_f$ by a table of Serre [Se2], and thus $m = pq\ell$ if $k_0 \neq 26$. We have tested numerically the \mathfrak{l} -ordinarity up to $\ell < 10000$ and verified the validity of our argument for $k \leq 44972$ (only using known ordinary primes supposing the conjecture for k). For $k = 44974$, $\ell - 1 = k - 12$ for the prime $\ell = 44963$. Thus if 44963 is ordinary for Δ , the argument still works. Since we can take any even weight k_0 less than a given k as an inductive step, our argument should presumably work for every weight, although we do not have a rigorous proof of the existence of ℓ and k_0 with $\ell - 1 | k - k_0 > 0$ satisfying the four conditions for the weight k_0 Hecke eigenform ϕ .

Although the above proposition has some technical assumptions, we like to emphasize the rather simple nature of our principle we described above, which virtually guarantees the existence of base change for any holomorphic form of weight ≥ 2 to any totally real field if we can improve further our technology in identifying Hecke algebras with universal deformation rings.

In the following section, we introduce tools to find $\theta(\varphi)$ and θ for general $k_0 \geq 2$, and in Section 3, we compute θ and explicit values of m for eigenforms f_0 of small weight k_0 . Each ordinary prime $\ell \notin \Sigma_{f_0}$ for such a low weight form f_0 yields F -liftability of forms of weight $k \equiv k_0 \pmod{\ell - 1}$, as long as the conjecture is true for weight k . Then for a given $k \leq 468$, we made a list of primes ℓ with $\ell - 1 | k - k_0$ for one of $k_0 \in \mathcal{K}$, and we verified by computation that we have a nice ℓ in the list such that $\ell \notin \Sigma_{f'}$ and ℓ is ordinary with respect to f_0 . This computation verifying Proposition 1.1 (for $k \leq 468$) is done by hand (one day work) and also by computer calculation (in this case, up to $k \leq 44972$ assuming the conjecture). Actually if $\ell \geq k - 1$ with $\ell \neq 2k - 1$ is ordinary for f and $\ell \in \Sigma_f$, then ℓ is an Eisenstein prime dividing the numerator of the Bernoulli number $\frac{B_k}{2k}$ (see the proof of Theorem 5.3 in

[H89c]). Some of the Hecke eigenvalues used in Section 3 are supplied to us from K. Doi and H. Ishii as indicated there. We are grateful to them for allowing us to use their numerical examples. In Section 4, we give a proof of the above result attributed to Fujiwara [F], reducing it to what is actually proven in [F], although it is a straightforward application of the theory in [H88] and [H89a]. In Section 5, we give numerical examples supporting Maeda’s conjecture and explain how we verify the conjecture for small weights. Proposition 5.1 is a key to checking the conjecture. It is supplied to one of the authors by K. Kubo, to whom we are grateful.

We like to thank the referee of this paper for his carefull reading.

2. Cusp forms congruent to $\theta(\varphi)$.

Let $M = \mathbb{Q}(\sqrt{D})$ be a quadratic field with discriminant D and Galois group $\Gamma = \text{Gal}(M/\mathbb{Q})$ generated by σ . Let $\chi = \left(\frac{D}{\cdot}\right)$ be the Legendre symbol, and put $\widehat{\Gamma} = \{\text{id}, \chi\}$. Let $\psi \in \widehat{\Gamma}$, and consider the space of elliptic cusp forms $S_\kappa(\Gamma_0(C), \psi)$ of weight κ and of level given by the conductor $C = C(\psi)$ of ψ . Let A be a subring of \mathbb{C} . We write $h_\kappa(C(\psi), \psi; A)$ for the A -subalgebra of the linear endomorphism algebra of $S_\kappa(\Gamma_0(C), \psi)$ generated over A by Hecke operators $T(n)$ for all n . Let $\lambda = \lambda_\kappa : h_\kappa(C(\psi), \psi; \mathbb{Z}) \rightarrow \mathbb{C}$ be an algebra homomorphism and A be a valuation ring of $\mathbb{Q}(\lambda)$ with residual characteristic p . Here $\mathbb{Q}(\lambda)$ is the number field generated by $\lambda(T(n))$ for all n . As is well known, $\mathbb{Q}(\lambda)$ is totally real or a CM field. We write $\mathbb{Q}(\lambda)_+$ for the maximal real subfield of $\mathbb{Q}(\lambda)$. Let \mathcal{O} be the \mathfrak{m}_A -adic completion for the maximal ideal \mathfrak{m}_A of A . We write $\rho = \rho_\lambda : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathcal{O})$ for the Galois representation attached to λ . We write $\bar{\rho}$ for the semi-simplification of $\rho_\lambda \bmod \mathfrak{m}_\mathcal{O} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F})$ with $\mathbb{F} = \mathcal{O}/\mathfrak{m}_\mathcal{O}$. For the moment, we assume that M is real. Then $\mathbb{Q}(\lambda) \neq \mathbb{Q}(\lambda)_+$ if $\psi = \chi$. Since the Neben character ψ is even, the weight κ is even and hence $\kappa \geq 2$. We quote the following fact from [H97], which is a straightforward generalization of a well known result of Shimura [Sh] and [Sh1]:

Theorem 2.1. *Suppose that M is real, and let p be a prime number with $p \geq 3$ if $\kappa > 2$ and $p > 3$ if $\kappa \geq 2$. Let $\mathfrak{p}|p$ be a prime of $\mathbb{Q}(\lambda)$ associated to A . Let ε be a fundamental unit of M chosen to be positive at some real place of M .*

- (1) *If $\lambda(T(p)) \in A^\times$, $\bar{\rho} \cong \text{Ind}_M^{\mathbb{Q}} \bar{\varphi}$ for a character $\bar{\varphi}$ of $\text{Gal}(\overline{\mathbb{Q}}/M)$, and $\bar{\rho}$ is absolutely irreducible, then $\psi = \chi$, $\chi(p) = 1$ and $p|N(\varepsilon^{\kappa-1} - 1)$;*
- (2) *If $\psi = \chi$, $p = \mathfrak{P}\mathfrak{P}'$ with primes $\mathfrak{P} \neq \mathfrak{P}'$ in M ($\Leftrightarrow \chi(p) = 1$) and $p|N(\varepsilon^{\kappa-1} - 1)$ for even κ , then there exist $\lambda : h_\kappa(D, \chi; \mathbb{Z}) \rightarrow \mathbb{C}$ and \mathfrak{p} such that (i) $\lambda(T(p)) \in A^\times$, (ii) $\bar{\rho}$ is isomorphic to $\text{Ind}_M^{\mathbb{Q}} \bar{\varphi}$ for a*

- character $\bar{\varphi} : \text{Gal}(\bar{\mathbb{Q}}/M) \rightarrow \mathbb{F}^\times$ with conductor \mathfrak{P} , (iii) $\bar{\rho}$ is irreducible;
- (3) If $\psi = \chi$, $\lambda(T(p)) \in A^\times$, and \mathfrak{p} divides the relative different $\mathfrak{d} = \mathfrak{d}_\lambda$ of $\mathbb{Q}(\lambda)/\mathbb{Q}(\lambda)_+$, then $p|N(\varepsilon^{\kappa-1} - 1)$, $\chi(p) = 1$ and $\bar{\rho} \cong \text{Ind}_M^{\mathbb{Q}} \bar{\varphi}$, which is absolutely irreducible.

Moreover if $\chi(p) = 1$, $p|N(\varepsilon^{\kappa-1} - 1)$ and $\psi = \chi$, then $\bar{\rho}$ associated to λ in (2) satisfying the three conditions (i), (ii) and (iii) is p -ordinary and regular. Here we call a Galois representation ρ with values in $GL_2(A)$ for a p -adic local ring A “ p -ordinary” (and regular) if its restriction to each decomposition group at p is isomorphic to $\begin{pmatrix} \delta & * \\ 0 & \epsilon \end{pmatrix}$ for an unramified character δ (and $\delta \not\equiv \epsilon \pmod{\mathfrak{m}_A}$).

Proof. All but the assertion (3) of the theorem have been proven in [H97]. Note here that the complex conjugate of $\lambda(T(n))$ is equal to $\chi(n)\lambda(T(n))$ for n prime to D (see [Sh], Proposition 3.56). Thus $Tr(\bar{\rho}) = Tr(\bar{\rho} \otimes \chi)$, and by semi-simplicity of $\bar{\rho}$, we get $\bar{\rho} \cong \bar{\rho} \otimes \chi$. Then by [H97] Proposition 1.1, $p|N(\varepsilon^{\kappa-1} - 1)$ and $\chi(p) = 1$. Since M is real, $\bar{\rho}$ cannot be reducible as shown in the beginning of Section 1 of [H97]. The regularity of $\bar{\rho}$ associated to λ in (2) is not explicitly mentioned in [H97], but it follows from the fact that κ is even and $\epsilon = \omega_p^{\kappa-1}$ (on the inertia subgroup) for the Teichmüller character ω_p . \square

Remark 2.1. If $N(\varepsilon) = -1$ for the fundamental unit ε in the theorem, it is easy to see that any odd prime dividing $N(\varepsilon^{\kappa-1} - 1)$ for even κ splits in M/\mathbb{Q} . Thus in this case, the assumption: $\chi(p) = 1$ in Theorem 2.1 (2) is redundant.

Remark 2.2. We could have formulated the theorem a bit differently. Let W be the involution on $S_\kappa(\Gamma_0(D), \chi)$ induced by $\begin{pmatrix} 0 & -1 \\ D & 0 \end{pmatrix}$. Then $h \mapsto WhW$ induces an involution τ (that is, a ring automorphism of order 2) on $R = h_\kappa(D, \chi; \mathbb{Z})$. We write R_+ for the subring of R fixed by τ . Let c denote complex conjugation on \mathbb{C} . Since $\lambda \circ \tau = c \circ \lambda$ for $\lambda : h_\kappa(D, \chi; \mathbb{Z}) \rightarrow \mathbb{C}$, by the above proof of (3), $\bar{\rho} \cong \bar{\rho} \otimes \chi$ for an odd prime ideal $\mathfrak{p} \supset \text{Ker}(\lambda)$ of R ramifying in R/R_+ (that is, $\mathfrak{p}^\tau = \mathfrak{p}$ and τ acts trivially on R/\mathfrak{p}). In particular, if $N(\varepsilon) = -1$, $\bar{\rho}$ for \mathfrak{p} is ordinary, and hence by theorems of Deligne and Fontaine [E] 2.5 and 2.6, $\lambda(T(p)) \notin \mathfrak{p}$ if $p \geq \kappa - 1$. Thus under the hypothesis: $N(\varepsilon) = -1$, we know from Theorem 2.1 that the following two conditions are equivalent for primes $p \geq \max(5, \kappa - 1)$:

- (1) $p|N(\varepsilon^{\kappa-1} - 1)$
- (2) There exist an algebra homomorphism $\lambda : R \rightarrow \mathbb{C}$, a prime ideal $\mathfrak{p} \supset \text{Ker}(\lambda)$ with $\mathfrak{p}|p$ and a character $\bar{\varphi} : \text{Gal}(\bar{\mathbb{Q}}/M) \rightarrow \mathbb{F}^\times$ such that $\bar{\rho} \cong \text{Ind}_{\mathbb{Q}}^M \bar{\varphi}$ and $\lambda(T(p)) \notin \mathfrak{p}$.

Thus if R is an integral domain, for any given algebra homomorphism $\lambda : R \rightarrow \mathbb{C}$ and $p|N(\varepsilon^{\kappa-1} - 1)$ with $p \geq \max(5, \kappa - 1)$, there exists a prime ideal \mathfrak{p} in $\mathbb{Q}(\lambda)$ such that $\bar{\rho}$ for $\mathfrak{p}|p$ and λ satisfies $\bar{\rho} \cong \text{Ind}_{\mathbb{Q}}^M \bar{\varphi}$ and $\lambda(T(p)) \notin \mathfrak{p}$.

Now we assume that $M = \mathbb{Q}(\sqrt{-D})$ is imaginary with discriminant $-D < 0$. In this case, κ is odd if $S_{\kappa}(\Gamma_0(D), \chi)$ is non-trivial.

Proposition 2.2. *Let the notation be as in Theorem 2.1. Suppose that M is imaginary, $\lambda(T(p)) \in A^{\times}$, $\mathbb{Q}(\lambda) \neq \mathbb{Q}(\lambda)_+$, $\chi(p) = 1$, $\mathfrak{p}|\mathfrak{d}_{\lambda}$ and $\kappa + 2 < p$. Then $\bar{\rho} \cong \text{Ind}_{\mathbb{Q}}^M \bar{\varphi}$, which is absolutely irreducible, p -ordinary and regular.*

Proof. By the assumption: $\mathbb{Q}(\lambda) \neq \mathbb{Q}(\lambda)_+$, we have $\psi = \chi$. By the same argument as above, we see $\bar{\rho} \cong \bar{\rho} \otimes \chi$. Let ω_p be the Teichmüller character of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (at p). We suppose that $\bar{\rho} \otimes \chi \cong \bar{\rho}$. Suppose first that $\bar{\rho}$ is reducible. Then writing $\bar{\rho} \cong \begin{pmatrix} \bar{\delta} & * \\ 0 & \bar{\varepsilon} \end{pmatrix}$, we have $\bar{\delta}\bar{\varepsilon} = \chi\omega_p^{\kappa-1}$ and $\bar{\delta}\chi = \bar{\varepsilon}$, because $\bar{\delta}\chi = \bar{\delta}$ never happens if p is odd. This shows that $\bar{\delta}^2 = \omega_p^{\kappa-1}$ and $\bar{\delta} = \omega_p^{(\kappa-1)/2}$. Since $\lambda(T(p)) \in A^{\times}$ and $\kappa < p - 2$, by a theorem of Deligne [E] 2.5, $\bar{\rho}$ is p -ordinary, $\bar{\varepsilon} = \omega_p^{\kappa-1}$ on the inertia subgroup \mathcal{I}_p at p for the Teichmüller character ω_p . This shows that $\bar{\delta} \neq \bar{\varepsilon}$ and $\bar{\rho}$ is absolutely irreducible. Then by [DHI] Lemma 3.2, $\bar{\rho} = \text{Ind}_{\mathbb{Q}}^M \bar{\varphi}$. \square

Remark 2.3. Under the assumption of Theorem 2.1 or Proposition 2.2, the characteristic polynomial of $\lambda(T(q))$ for a prime q with $\chi(q) = -1$ has the form $f(X^2)$ for a monic $f(X) \in \mathbb{Z}[X]$. Each square-free factor of $f(0)$ divides \mathfrak{d}_{λ} provided that it is unramified in $\mathbb{Q}(\lambda)_+$. When $\chi(q) = 1$, the characteristic polynomial of $\lambda(T(q))$ has the form $f(X)^2$ for a monic $f(X) \in \mathbb{Z}[X]$.

Remark 2.4. Let $p \geq \max(5, \kappa - 1)$ be a prime with $p|N(\varepsilon^{\kappa-1} - 1)$ for an even integer κ . Then by Remark 2.2, we have an algebra homomorphism $\lambda : R \rightarrow \mathbb{C}$ and a prime $\mathfrak{p} \supset \text{Ker}(\lambda)$ such that $\bar{\rho} = \text{Ind}_{\mathbb{Q}}^M \bar{\varphi}$ for a character $\varphi : \text{Gal}(\overline{\mathbb{Q}}/M) \rightarrow \mathbb{F}^{\times}$. The restriction $\bar{\rho}_L$ of $\bar{\rho} = \text{Ind}_{\mathbb{Q}}^M \bar{\varphi}$ to $\text{Gal}(\overline{\mathbb{Q}}/L)$ for $L = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$ can be reducible even if $\bar{\rho}$ is absolutely irreducible. Since $\bar{\rho}_L = \text{Ind}_{LM}^L \bar{\varphi}_{ML}$, this happens when $\bar{\varphi}_{\sigma} \neq \bar{\varphi}$ but $\bar{\varphi}_{\sigma} = \bar{\varphi}$ on $\text{Gal}(\overline{\mathbb{Q}}/L)$ ($\Rightarrow \varphi|_{\mathcal{I}_p} = \omega_p^{\kappa-1}|_{\mathcal{I}_p}$ is of order 2 $\Rightarrow p = 2\kappa - 1$ if $p > \kappa$), where $\bar{\varphi}_{\sigma}(\tau) = \bar{\varphi}(\sigma\tau\sigma^{-1})$. By a simple computation, for any character $\xi : \text{Gal}(\overline{\mathbb{Q}}/M) \rightarrow \mathbb{F}^{\times}$ ramifying at p , the representation $\text{Ind}_{\mathbb{Q}}^M \xi$ is not p -ordinary if it is irreducible and p is inert in M/\mathbb{Q} .

3. Base change of elliptic cusp forms.

In this section, a gothic letter represents a prime of $\overline{\mathbb{Q}}$ dividing the rational prime denoted by its roman equivalent. Our strategy to find θ with $\theta \equiv \theta(\varphi) \pmod{\mathfrak{q}}$ and $\theta \equiv f \pmod{\mathfrak{p}}$ is as follows: Pick a normalized Hecke eigenform $f \in S_k(SL_2(\mathbb{Z}))$ whose p -adic Galois representation is p -ordinary with a p -adic unit $a(p, f)$. Then lift f to a p -adic family of ordinary forms $\{f_\kappa \in S_\kappa(\Gamma_0(p), \omega_p^{k-\kappa})\}_\kappa$ for the Teichmüller character ω_p modulo p (see [H86]). We choose κ so that $k - \kappa \equiv (p - 1)/2 \pmod{p - 1}$ and put $\theta = f_\kappa$. Let $M = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}p})$, and write χ for the Legendre symbol $\omega_p^{(p-1)/2}$ associated to M . Then compute the characteristic polynomial $H_\ell(X)$ of $T(\ell)$ in $h_\kappa(p, \chi; \mathbb{Q})$ by the trace formula in [Mi] and $H_\ell(0)$ to find an odd prime q such that $\mathfrak{q}|\mathfrak{d}_\lambda$.

Suppose that M is real and that $h_\kappa(p, \chi; \mathbb{Q})$ is simple (as often happens). We define $\lambda : h_\kappa(p, \chi; \mathbb{Q}) \rightarrow \mathbb{C}$ by $\theta|T(n) = \lambda(T(n))\theta$. Then just to find a prime $\mathfrak{q}|q$ with $\theta \equiv \theta(\overline{\varphi})$ for a character $\overline{\varphi} : \text{Gal}(\overline{\mathbb{Q}}/M) \rightarrow \mathbb{F}^\times$, we only need to compute $N(\varepsilon^{\kappa-1} - 1)$ when M is real. Then we pick a prime factor $q \geq \max(\kappa - 1, 5)$ of $N(\varepsilon^{\kappa-1} - 1)$. Then by Remark 2.2, a prime factor \mathfrak{q} of q in $\mathbb{Q}(\lambda)$ does the job as long as $q \neq 2\kappa - 1$ (see Remark 2.4). According to the conjecture made in [H97], the prime factors q of $N(\varepsilon^{\kappa-1} - 1)$ with $q \geq \max(\kappa - 1, 5)$ should also divide \mathfrak{d}_λ if $h_\kappa(p, \chi; \mathbb{Q})$ is simple.

If q , which is either a square-free prime factor of $H_\ell(0)$ or a prime factor of $N(\varepsilon^{\kappa-1} - 1)$ with $q \geq 5$, exists for λ , we know from Theorem 2.1 and Proposition 2.2 that $\theta \equiv \theta(\varphi) \pmod{\mathfrak{q}}$ for a prime $\mathfrak{q}|q$ and the Teichmüller lift φ of $\overline{\varphi}$ with respect to \mathfrak{q} . By the theorems of Deligne and Fontaine [E] 2.5-6, if $\kappa \geq 2$, $\chi(q) = 1$ and $q \geq \kappa - 1$, the representation $\overline{\rho}$ is ordinary and $\lambda(T(q)) \notin \mathfrak{q}$. Under the condition that $h_\kappa(p, \chi; \mathbb{Q})$ is a single field, without assuming $q \geq \kappa - 1$, replacing \mathfrak{q} by its Galois conjugate, we may assume further that $\lambda(T(q)) \notin \mathfrak{q}$ (see Remark 2.2). Then by the argument we described in the introduction (Corollary 4.5), f_w for all weights $w \geq 2$, in particular f , are F -liftable under (Hyp_{pq}) provided that $p \notin \Sigma_f$, $q > \kappa + 2$ and $q \neq 2\kappa - 1$ (see Remark 2.4). Similarly, primitive forms of level p congruent to θ modulo \mathfrak{q} is F -liftable under (Hyp_{pq}) . If $h_\kappa(p, \chi; \mathbb{Q})$ is not simple, we need to find to which simple factor f_κ belongs. The F -liftable forms proliferate as we change primes p (and hence q). The above argument proves the following fact:

Proposition 3.1. *Let p be an odd prime. Let $\chi = \left(\frac{\cdot}{p}\right)$ be the Legendre symbol and $\lambda : h_\kappa(p, \chi; \mathbb{Z}) \rightarrow \overline{\mathbb{Q}}$ be an algebra homomorphism for $\kappa \geq 2$. Let $\phi \in S_\kappa(\Gamma_0(p), \chi)$ be the Hecke eigenform with $\phi|T(n) = \lambda(T(n))\phi$. Suppose*

$\mathbb{Q}(\lambda) \neq \mathbb{Q}(\lambda)_+$. If a prime factor \mathfrak{q} of \mathfrak{d}_λ satisfies $q \neq 2\kappa - 1$, $q > \kappa + 2$ and $\chi(q) = 1$, then each Hecke eigenform $g \in S_{\kappa'}(\Gamma_1(pq^\alpha))$ ($\kappa' \geq 2$, $\alpha \geq 0$) with $g \equiv \phi \pmod{\mathfrak{q}}$ is liftable to totally real F satisfying (Hyp_{pq}) .

Suppose that $p \equiv 1 \pmod{4}$ and $p > 5$. Then as shown in [H97] Lemma 3.1, unless $(2^{2n} + 1)/p$ is a square for an integer $n > 1$, we can find a non-trivial q . It is easy to see that $\chi(q) = 1$ provided that $q > 2$, $q|N(\varepsilon^{\kappa-1} - 1)$ for even positive κ and $N(\varepsilon) = -1$. Thus this proposition combined with Theorem 2.1 shows the existence of infinitely many primes q with a q -adic ordinary family (of level p cusp forms) liftable to totally real F under (Hyp_{pq}) .

Here is a list of primes q , that is, the set \mathbf{S}_e of odd primes dividing $N(\varepsilon^e - 1)$ (but not $N(\varepsilon^{e'} - 1)$ for $0 < e' < e$) when $p \equiv 1 \pmod{4}$ (see [H97] Section 3).

- $(p = 13)$ $\mathbf{S}_1 = \{3\}$, $\mathbf{S}_5 = \{131\}$, $\mathbf{S}_7 = \{1429\}$, $\mathbf{S}_9 = \{433\}$;
- $(p = 17)$
 $\mathbf{S}_3 = \{67\}$, $\mathbf{S}_5 = \{4421\}$, $\mathbf{S}_7 = \{127, 2297\}$, $\mathbf{S}_9 = \{19, 15121\}$;
- $(p = 29)$
 $\mathbf{S}_1 = \{5\}$, $\mathbf{S}_3 = \{7\}$, $\mathbf{S}_5 = \{151\}$, $\mathbf{S}_7 = \{20357\}$, $\mathbf{S}_9 = \{19603\}$;
- $(p = 37)$ $\mathbf{S}_1 = \{3\}$, $\mathbf{S}_3 = \{7\}$, $\mathbf{S}_5 = \{11, 1951\}$, $\mathbf{S}_7 = \{71, 44129\}$;
- $(p = 41)$ $\mathbf{S}_3 = \{4099\}$, $\mathbf{S}_5 = \{16797701\}$, $\mathbf{S}_7 = \{197, 13469, 25943\}$;
- $(p = 53)$ $\mathbf{S}_1 = \{7\}$, $\mathbf{S}_3 = \{13\}$, $\mathbf{S}_5 = \{11, 241\}$, $\mathbf{S}_7 = \{43, 449\}$;
- $(p = 61)$
 $\mathbf{S}_1 = \{3, 13\}$, $\mathbf{S}_3 = \{127\}$, $\mathbf{S}_5 = \{41, 56611\}$, $\mathbf{S}_7 = \{3534959149\}$.

We now give a list of $\Sigma_{k_0} = \Sigma_{\Delta_{k_0}}$ (made out of the data given in [Se2]) for the unique Hecke eigenform Δ_{k_0} in $S_{k_0}(SL_2(\mathbb{Z}))$ with $k_0 \in \{12, 16, 18, 20, 22, 26\}$:

$$\begin{aligned} \Sigma_{12} &= \{3, 5, 7, 23, 691\}, & \Sigma_{16} &= \{3, 5, 7, 11, 31, 3617\}, \\ \Sigma_{18} &= \{3, 5, 7, 11, 13, 43867\}, & \Sigma_{20} &= \{3, 5, 7, 11, 13, 283, 617\}, \\ \Sigma_{22} &= \{3, 5, 7, 13, 17, 131, 593\}, & \Sigma_{26} &= \{3, 5, 7, 11, 17, 19, 657931\}. \end{aligned}$$

To identify these primes, we have used the fact that for small weights, $\bar{\rho}_{p, \Delta_{k_0}}$ is dihedral if and only if $2k_0 - 1 = p$ is a prime and $\mathbb{Q}(\sqrt{-p})$ has class number > 1 .

Here is a table of known ordinary primes for Δ_{k_0} :

k_0	p
12	$11 \leq p < 2411, 2417 \leq p \leq 19597$
16	$17 \leq p < 59, 61 \leq p < 15271, 15277 \leq p \leq 19597$
18	$17 \leq p \leq 14879$
20	$19 \leq p < 3371, 3373 \leq p \leq 9973$
22	$p = 11, 23 \leq p \leq 9973$
26	$29 \leq p \leq 9973$

We start the description of our experiment with the Ramanujan's function $f = \Delta \in S_{12}(SL_2(\mathbb{Z}))$. The function Δ is p -ordinary for $11 \leq p < 2411$. We assume $p \notin \Sigma_{12}$. Thus the weight k Hecke eigenform f_k belonging to the p -adic family of Δ resides in $S_k(\Gamma_0(p), \omega_p^{12-k})$. We make $p = 13$ and $\kappa = 6$. Then $\theta = f_6 \in S_6(\Gamma_0(13), (\frac{\cdot}{13}))$. This space has dimension 6 (see [Mi] Numerical Tables). The Hecke polynomial $H_2(X)$ for $T(2)$ on this space is:

$$H_2(X) = X^6 + 161X^4 + 5856X^2 + 18864 \quad \text{with} \quad 18864 = 2^4 \cdot 3^2 \cdot 131,$$

which is irreducible over \mathbb{Q} . Since 131 is unramified in $\mathbb{Q}(\lambda)_+ = \mathbb{Q}[X]/(P(X))$ with $P(X) = H_2(\sqrt{X})$, the square-free factor 131 of $H_2(0)$ is a factor of \mathfrak{d}_λ . We put $q = 131$. Thus for a prime $\mathfrak{q}|131$ of $\overline{\mathbb{Q}}$, $\theta \equiv \theta(\varphi) \pmod{\mathfrak{q}}$ for a character $\varphi = \omega_q^5$ of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{13}))$. By Theorem 2.1 and Remark 2.2, θ has to be \mathfrak{q} -ordinary. Thus the \mathfrak{q} -ordinary family of θ is liftable to F satisfying (Hyp₁₃₁) (Proposition 3.1). Since $\overline{\rho}_{\mathfrak{p}, \Delta} \cong \overline{\rho}_{\mathfrak{p}, \theta}$ for $\mathfrak{p}|13$, the \mathfrak{p} -adic family of Δ is liftable to F satisfying (Hyp_{13,131}). We can use $p = 17$ and $\kappa = 4$ in place of $p = 13$ and $\kappa = 6$. In this case, on $S_4(\Gamma_0(17), (\frac{\cdot}{17}))$

$$H_3(X) = X^4 + 74X^2 + 1072 \quad \text{with} \quad 1072 = 2^4 \cdot 67,$$

which is irreducible over \mathbb{Q} . Thus $67|\mathfrak{d}$, and the 17-adic family of Δ is liftable to F satisfying (Hyp_{17,67}). Let $\ell \notin \Sigma_{12}$ be an odd prime for which Δ is ℓ -ordinary. Then each member of the ℓ -adic ordinary family of Δ is F -liftable if F is totally real and satisfies either (Hyp _{ℓ ,17,67}) or (Hyp _{ℓ ,13,131}).

We now take $\Delta_{16} \in S_{16}(SL_2(\mathbb{Z}))$. The form Δ_{16} is 19-ordinary. On $S_7(\Gamma_0(19), (\frac{\cdot}{19}))$, which is 9 dimensional, as computed by K. Doi, the characteristic polynomial $H_2(X)$ of $T(2)$ is given by

$$H_2(X) = X(X^8 + 483X^6 + 75582X^4 + 4242376X^2 + 71047680),$$

where $71047680 = 2^9 \cdot 3 \cdot 5 \cdot 11 \cdot 29^2$. The degree 8 factor is irreducible. Since 11 splits in $\mathbb{Q}(\sqrt{-19})$, the form belonging to the degree 8-factor is \mathfrak{q} -ordinary

for \mathfrak{q} with $\mathfrak{q}|11$ and $\mathfrak{q}|\mathfrak{d}$. Since the member $\theta = f_7$ of weight 7 in the 19-adic family of Δ_{16} is not of CM type, it belongs to the degree 8-factor. Thus by Propositions 2.2 and 3.1, each member of the \mathfrak{q} -adic family of θ is liftable to F satisfying (Hyp₁₁). Thus for odd primes $\ell \notin \Sigma_{16}$ for which Δ_{16} is ℓ -ordinary, each member of the ℓ -adic family of Δ_{16} is liftable to a totally real F satisfying (Hyp _{$\ell \cdot 11 \cdot 19$}).

We look at Δ_{18} . Then for $p = 19$, Δ_{18} is p -ordinary. Take $p = 19$. We have $f_9 \in S_9(\Gamma_0(19), (\frac{-}{19}))$. The Hecke algebra of this space is computed by H. Ishii, and we have

$$H_2(X) = X(X^{12} + 2323X^{10} + 2010462X^8 + 803113072X^6 + 150633270400X^4 + 12173735396352X^2 + 333034797957120).$$

We have $333034797957120 = 2^{15} \cdot 3^9 \cdot 5 \cdot 7 \cdot 14753$. Since $(\frac{14753}{19}) = 1$, we can take $q = 14753$. The above argument works for forms of $S_k(SL_2(\mathbb{Z}))$ for $k = 12, 16, 18, 20, 22, 24, 28, 32, 34$. We list (κ, p, q) for these values of k :

- Case $k = 12$: $(\kappa, p, q) = (6, 13, 131), (4, 17, 67)$;
- Case $k = 16$: $(\kappa, p, q) = (7, 19, 11), (8, 17, 127), (8, 17, 2297), (2, 29, 5)$;
- Case $k = 18$: $(\kappa, p, q) = (9, 19, 14753)$
- Case $k = 20$: $(\kappa, p, q) = (6, 29, 5), (6, 29, 151)$;
- Case $k = 22$: $(\kappa, p, q) = (8, 29, 5), (8, 29, 20357)$;
- Case $k = 24$: $(\kappa, p, q) = (6, 37, 1951), (4, 41, 4099)$;
- Case $k = 28$: $(\kappa, p, q) = (2, 53, 7)$;
- Case $k = 32$: $(\kappa, p, q) = (2, 61, 13)$;
- Case $k = 34$: $(\kappa, p, q) = (4, 61, 13), (4, 61, 127)$.

See [DHI] Section 2.2 for a table of \mathfrak{d} used to compute the above values when $p \equiv 1 \pmod{4}$.

We take Δ_{26} . The only prime which seems to be small enough for actual computation is 47. We look at $S_3(\Gamma_0(47), (\frac{-}{47}))$. According to H. Ishii, the Hecke polynomial is given by

$$H_2(X) = (X^5 - 20X^3 + 80X - 17)(X + 1)^2, \quad H_5(X) = X^5(X^2 + 78).$$

Let $g \in S_3(\Gamma_0(47), (\frac{-}{47}))$ be a Hecke eigenform associated to the factor $X^2 + 78$ of H_5 . The odd prime factor 13 of 78 in the second factor of $H_5(X)$ remains prime in $\mathbb{Q}(\sqrt{-47})$, and hence it is not an ordinary prime for $f_3 = g$ in the 47-adic family of Δ_{26} . Although the other odd factor 3 splits in $\mathbb{Q}(\sqrt{-47})$, we can show that $3 \in \Sigma_g$. Thus they do not work for our purpose, and we

need to go a different way. Δ_{26} is 29-ordinary ($a(29, \Delta_{26}) \equiv 15 \pmod{29}$). Thus its member Δ_{54} (or rather, associated primitive form) of 29-adic family falls in $S_{54}(SL_2(\mathbb{Z}))$. By computation (see Section 5) the Hecke algebra of $S_{54}(SL_2(\mathbb{Z}))$ is simple (that is, a single field), and hence $\Delta_{54} = f^\sigma$ for a member f of 43-adic family of Δ . Thus we get 4 step congruence:

$$\begin{aligned} \Delta_{26} &\equiv \Delta_{54} \pmod{\mathfrak{l}} \quad (\mathfrak{l}|29), & \Delta_{54} &\equiv \Delta \pmod{\mathfrak{q}} \quad (\mathfrak{q}|43), \\ \Delta &\equiv \theta \pmod{\mathfrak{p}} \quad (\mathfrak{p}|13), & \theta &\equiv \theta(\varphi) \pmod{\mathfrak{r}} \quad (\mathfrak{r}|131). \end{aligned}$$

Thus Δ_{26} is liftable to a totally real F satisfying (Hyp₁₃₋₂₉₋₄₃₋₁₃₁).

There is one more way of getting level 1 F -liftable forms. For each prime $\ell > 13$, there is a unique $\nu = \nu(\ell) \in \{-1, 1, 3, 5, 7\}$ such that $\ell - \nu \equiv 12 \pmod{10}$. Thus in $S_{\ell-\nu}(SL_2(\mathbb{Z}))$, there is a unique Hecke eigenform f such that $f \equiv \Delta \pmod{\mathfrak{p}}$ for a given prime $\mathfrak{p}|11$. For any given prime $\mathfrak{l}|\ell$, every Hecke eigenform in $S_{\ell-\nu}(SL_2(\mathbb{Z}))$ is \mathfrak{l} -ordinary (see [J] Corollary 7.7 and [Se] Theorem 11). Thus any Hecke eigenform $g \in S_\kappa(\Gamma_1(\ell^\alpha))$ with $g \equiv f \pmod{\mathfrak{l}}$ is F -liftable under (Hyp _{$m\ell$}) for $m = 11 \cdot 17 \cdot 67$ or $11 \cdot 13 \cdot 131$ as long as $\ell \notin \Sigma_f$. By \mathfrak{l} -ordinarity, we can conclude $\ell \notin \Sigma_f$ if ℓ is prime to the numerator of $\frac{B_{\ell-\nu}}{\ell-\nu}$. We record this as:

Proposition 3.2. *Let $m = 11 \cdot 17 \cdot 67$ or $11 \cdot 13 \cdot 131$. Let $\ell > 13$ be a prime and $\mathfrak{p}|11$ be a prime of $\overline{\mathbb{Q}}$. Suppose that ℓ is prime to the numerator of $\frac{B_{\ell-\nu}}{\ell-\nu}$. If Conjecture 1.2 is true for the weight $\ell - \nu$, then for every $\mathfrak{l}|\ell$, congruence $g \equiv f \pmod{\mathfrak{l}}$ of Hecke eigenforms $g \in S_\kappa(\Gamma_1(\ell^\alpha))$ ($\kappa \geq 2$) and $f \in S_{\ell-\nu}(SL_2(\mathbb{Z}))$ implies the liftability of g to a totally real F satisfying (Hyp _{$m\ell$}). Without assuming Conjecture 1.2, the assertion holds for the unique Hecke eigenform $f \in S_{\ell-\nu}(SL_2(\mathbb{Z}))$ with $f \equiv \Delta \pmod{\mathfrak{p}}$.*

The above proposition implies the existence of ℓ -adic families of ordinary cusp forms of level 1 F -liftable under (Hyp _{$m\ell$}), as long as $\ell \equiv 1, 3 \pmod{10}$. In the above argument, one could have used a prime p different from 11, for example 13.

If one supposes that ordinary primes for a given Hecke eigenform f (of level 1) have Dirichlet density 1, we can find a specific m so that f is liftable to F under (Hyp _{m}) and the conjecture.

Proposition 3.3. *If the Dirichlet density of ordinary primes for a Hecke eigenform $f \in S_k(SL_2(\mathbb{Z}))$ is equal to 1, then under the conjecture, we can always find m such that f is F -liftable under (Hyp _{m}).*

Proof. Because of the density assumption, we can find an ordinary prime $l \in \Sigma_f$ for f as in the proposition such that $\gcd(l - 1, 10) = 2$. Choose

positive integers i and j such that $k - 2 = 10i - j(l - 1)$. Choose a prime $l \nmid l$ so that f is l -ordinary. Then we pick a member g of the l -adic ordinary family of f of weight $k + j(l - 1)$. Then $g \equiv \Delta \pmod{\mathfrak{p}}$ for a prime $\mathfrak{p} \nmid 11$ supposing the conjecture. Thus $f \equiv g \pmod{l}$ is F -liftable under (Hyp_{ml}) for m as in Proposition 3.2. \square

It is plain from the argument proving the above proposition, actually it is enough to assume, for the validity of the assertion of Proposition 3.3, the density of ordinary primes for f is bigger than $\frac{1}{5}$.

4. p -Ordinary deformation.

4.1. Deformation problems. We fix a finite set of places Σ of F and consider the maximal extension F_Σ of F unramified outside $\Sigma \cup \{\infty\}$. We write $\mathcal{G} = \text{Gal}(F_\Sigma/F)$. Then we fix a 2-dimensional continuous Galois representation $\bar{\rho} : \mathcal{G} \rightarrow GL_2(\mathbb{F})$ for a finite field \mathbb{F} of characteristic p for an odd prime p .

We fix a valuation ring \mathcal{O} finite flat over \mathbb{Z}_p with residue field \mathbb{F} and consider the category $CNL = CNL_{\mathcal{O}}$ of complete noetherian local \mathcal{O} -algebras with residue field \mathbb{F} . A deformation of $\bar{\rho}$ is a continuous representation $\rho : \mathcal{G} \rightarrow GL_2(A)$ for an object A of CNL such that $\rho \pmod{\mathfrak{m}_A} = \bar{\rho}$. We call a deformation ρ nearly p -ordinary, if for a decomposition subgroup $\mathcal{D}_{\mathfrak{P}}$ of \mathcal{G} at each p -adic place \mathfrak{P} , $\rho|_{\mathcal{D}_{\mathfrak{P}}} \cong \begin{pmatrix} \delta & * \\ 0 & \varepsilon \end{pmatrix}$. Thus we have characters $\delta = \delta_{\mathfrak{P},\rho}$ and $\varepsilon = \varepsilon_{\mathfrak{P},\rho}$ of $\mathcal{D}_{\mathfrak{P}}$ realized as diagonal entries. When $\delta_{\mathfrak{P},\rho}$ is unramified for all \mathfrak{P} , we call ρ p -ordinary.

Following Wiles [W], we consider the following conditions on deformations of $\bar{\rho}$. For a prime \mathfrak{q} of F , we write \mathcal{D}_{Ω} for the decomposition subgroup of \mathcal{G} at a prime $\Omega|\mathfrak{q}$ (of F_Σ) and let \mathcal{I}_{Ω} be its inertia subgroup. We split

$$\Sigma = \{\mathfrak{p}|p\} \sqcup \mathcal{M} \sqcup \mathcal{M}' \sqcup \mathcal{M}''.$$

For $\mathfrak{q} \in \mathcal{M}''$, there is no restriction on deformations. For $\mathfrak{q} \in \mathcal{M} \cup \mathcal{M}'$, we impose minimality condition $(\chi_{\mathfrak{q}})$ ($\mathfrak{q} \in \mathcal{M}$) and $(\mathcal{N}_{\mathfrak{q}})$ ($\mathfrak{q} \in \mathcal{M}'$) described in [H96a] 2.1. Let us recall briefly these conditions. We fix a non-trivial character $\chi_{\mathfrak{q}}$ of \mathcal{I}_{Ω} with values in \mathbb{F}^\times . We regard $\chi_{\mathfrak{q}}$ having values in A^\times for any $A \in CNL_{\mathcal{O}}$ through Teichmüller lift. We write $\mathfrak{f}_{\mathfrak{q}}$ for the conductor of $\chi_{\mathfrak{q}}$ and put $\mathfrak{f} = \prod_{\mathfrak{q} \in \mathcal{M}} \mathfrak{f}_{\mathfrak{q}}$. Thus $\mathfrak{q}|\mathfrak{f} \iff \mathfrak{q} \in \mathcal{M}$. Writing $V(\rho)$ for the representation space of ρ , we impose for $\mathfrak{q} \in \mathcal{M} \cup \mathcal{M}'$,

- ($\chi_{\mathfrak{q}}$) As \mathcal{I}_{Ω} -modules, $V(\rho) \cong V(\text{id}) \oplus V(\chi_{\mathfrak{q}})$ with $V(\chi_{\mathfrak{q}})$ A -free of rank 1 for $\mathfrak{q} \in \mathcal{M}$,

(\mathcal{N}_q) For $q \in \mathcal{M}'$, we have an exact sequence of \mathcal{D}_Ω -modules, non-split over \mathcal{I}_Ω :

$$0 \longrightarrow V(\rho_{1,q}) \longrightarrow V(\rho) \longrightarrow V(\rho_{2,q}) \longrightarrow 0$$

where $V(\rho_{2,q})$ is A -free of rank 1, $\rho_{i,q}$ ($i = 1, 2$) is unramified and $\rho_{1,q}\rho_{2,q}^{-1} = \mathcal{N}_q$ for the p -cyclotomic character \mathcal{N}_q of \mathcal{D}_q .

We call such ρ a deformation of type $D = D|_F$ for

$$D = \{(\chi_q)|q \in \mathcal{M}\} \cup \{(\mathcal{N}_q)|q \in \mathcal{M}'\} \cup \mathcal{M}''.$$

We then consider the following two deformation functors: $CNL \rightarrow SETS$ given by

$$\begin{aligned} \mathcal{F}_F^\emptyset(A) &= \mathcal{F}_{F,\bar{\rho}}^\emptyset(A) = \{\rho : \mathcal{G} \rightarrow GL_2(A) \text{ is a deformation of } \bar{\rho} \text{ of type } D\} / \approx, \\ \mathcal{F}_F(A) &= \mathcal{F}_{F,\bar{\rho}}(A) = \left\{ \rho \in \mathcal{F}_F^\emptyset(A) \text{ is nearly } p\text{-ordinary} \right\}, \end{aligned}$$

where “ \approx ” is the strict equivalence, that is, conjugation by elements in $\widehat{GL}_2(A) = 1 + \mathfrak{m}_A M_2(A)$. For a finite extension E/F , we consider

$$(AI_E) \quad \bar{\rho}_E = \bar{\rho}|_{\text{Gal}(\bar{\mathbb{Q}}/E)} \text{ is absolutely irreducible.}$$

It is shown by Mazur that \mathcal{F}_F^\emptyset is representable under (AI_F) . In addition to the above condition, to assure the representability of \mathcal{F}_F , we need to assume

$$(Reg_F) \quad \delta_{\mathfrak{p},\bar{\rho}} \neq \varepsilon_{\mathfrak{p},\bar{\rho}} \quad \text{on the inertia group } \mathcal{I}_{\mathfrak{p}}.$$

For assuring representability, it is enough to assume $\delta_{\mathfrak{p},\bar{\rho}} \neq \varepsilon_{\mathfrak{p},\bar{\rho}}$ over the decomposition group. But the stronger condition listed above is unaffected under p -unramified base-change. Thus for our purpose, it is convenient to assume the above condition. We list here two more restrictions we like to study: Let $\mathfrak{p}|p$ be a prime ideal of F . We hereafter write \mathfrak{P} for a prime of $\bar{\mathbb{Q}}$ above \mathfrak{p} . We call a nearly p -ordinary deformation ρ \mathfrak{p} -ordinary if $\delta_{\mathfrak{p},\rho}$ is unramified for every decomposition subgroup $\mathcal{D}_{\mathfrak{p}}$ of \mathcal{G} for $\mathfrak{P}|\mathfrak{p}$. We call ρ p -ordinary if it is \mathfrak{p} -ordinary for every $\mathfrak{p}|p$. For a given character $\eta : \mathcal{G} \rightarrow \mathcal{O}^\times$, we say that a deformation ρ has fixed determinant η if $\det \rho = \eta$ in A^\times . Then we define the following subfunctors of \mathcal{F}_F :

$$\begin{aligned} \mathcal{F}_F^{\text{ord}}(A) &= \{\rho \in \mathcal{F}_F(A) | \rho \text{ is } p\text{-ordinary}\}, \\ \mathcal{F}_F^\eta(A) &= \{\rho \in \mathcal{F}_F(A) | \det \rho = \eta\}, \\ \mathcal{F}_F^{\text{ord},\eta}(A) &= \mathcal{F}_F^\eta(A) \cap \mathcal{F}_F^{\text{ord}}(A). \end{aligned}$$

It is easy to check that the above subfunctors of \mathcal{F}_F are representable under (AI_F) and (Reg_F) (see [H96a] Appendix and [Ti]). When representable, write (R_F, ϱ_F) for the universal couple representing \mathcal{F}_F . In this paper, “near p -ordinarity” is always put in force. When we consider a deformation problem with additional restriction “?”, (for example $? = \text{ord}$), we write $(R_F^?, \varrho_F^?)$ for the universal couple with the condition “?” and the near p -ordinarity.

There are some relations between the above functors. Here we list one of them. We suppose that $\eta = \chi_{\mathfrak{q}}$ on \mathcal{I}_{Ω} for all $\mathfrak{q} \in \mathcal{M}$ and η is unramified at each $\mathfrak{q} \in \mathcal{M}'$ to make η compatible with the condition $(\chi_{\mathfrak{q}})$. Hereafter we suppose that $p > 2$. Since $(\det \rho)^{-1}\eta$ for $\rho \in \mathcal{F}_F^?$ has values in the p -profinite subgroup $\widehat{\mathbf{G}}_m(A) = 1 + \mathfrak{m}_A$, it has a unique square root $\sqrt{(\det \rho)^{-1}\eta}$. Thus $\rho \mapsto (\rho^\eta = \rho \otimes \sqrt{(\det \rho)^{-1}\eta}, \det \rho \eta^{-1})$ gives a natural transformation: $\mathcal{F}_F \cong \mathcal{F}_F^\eta \times \mathcal{F}_{F,\text{id}}$, where

$$\begin{aligned} & \mathcal{F}_{F,\text{id}}(A) \\ &= \left\{ \phi : \mathcal{G} \rightarrow A^\times : \text{a character} \mid \phi \bmod \mathfrak{m}_A = \text{id}, \phi|_{\mathcal{I}_{\Omega}} = \text{id} \text{ for all } \mathfrak{q} \in \mathcal{M} \right\}. \end{aligned}$$

Let $\mathcal{G}^{\mathcal{M}''} = \text{Gal}(F_{\Sigma'}/F)$ for $\Sigma' = \Sigma - \mathcal{M} \cup \mathcal{M}'$, and \mathcal{W} be the maximal p -profinite abelian quotient of $\mathcal{G}^{\mathcal{M}''}$. Then the functor $\mathcal{F}_{F,\text{id}}$ is represented by $(\mathcal{O}[[\mathcal{W}]], \nu)$ for the projection ν of \mathcal{G} onto $\mathcal{W} \subset \mathcal{O}[[\mathcal{W}]]^\times$. Thus we get

$$(T) \quad (R_F, \varrho_F) \cong (R_F^\eta \widehat{\otimes}_{\mathcal{O}} \mathcal{O}[[\mathcal{W}]], \varrho_F^\eta \otimes \sqrt{\nu}).$$

4.2. Nearly ordinary Hecke algebras. Fix an integral ideal N of F prime to p . Let χ' be a character modulo N with conductor $\mathfrak{f}|N$. Suppose that $N = \mathfrak{f}N'$ with square-free N' prime to \mathfrak{f} . Suppose that there exist a Hecke character $\chi : F^\times \backslash F_{\mathbb{A}}^\times \rightarrow \mathcal{O}^\times$ such that

- (1) χ is of finite order, and its order is prime to p ;
- (2) the conductor of χ is a factor of $\mathfrak{f}p$;
- (3) the restriction of χ to $(\mathcal{O}_F/\mathfrak{f})^\times$ coincides with χ' .

Let

$$D = \{(\chi_{\mathfrak{q}}) \mid \mathfrak{q} \mid \mathfrak{f}\} \cup \{(\mathcal{N}_{\mathfrak{q}}) \mid \mathfrak{q} \mid N'\}.$$

We take a maximal ideal \mathfrak{m} of the nearly ordinary Hecke algebra $h^{n,\text{ord}}(N, p^\infty; \mathcal{O})$ with certain properties. These properties should include that the residual modular Galois representation $\rho_{\mathfrak{m}} : \mathcal{G} \rightarrow GL_2(\mathbb{F})$ associated to \mathfrak{m} satisfies D . Then we set $\bar{\rho} = \rho_{\mathfrak{m}}$.

We now describe the nearly ordinary Hecke algebra $h^{n,\text{ord}}(N, p^\infty; \mathcal{O})$ of (prime-to- p) level N , which corresponds to \mathcal{F}_F if $\bar{\rho}$ is minimally modular in the sense (of Fujiwara) described below 4.3. We follow the treatment of

[H96b] Section 2 where the case with $N = 1$ is treated. We write Z (resp. $C_{\infty+}$) for the center of $G = \text{Res}_{F/\mathbb{Q}} GL(2)$ (resp. the connected component of the standard maximal compact subgroup of $G(\mathbb{R})$). We consider for each open compact subgroup U of $G(\mathbb{A}^{(\infty)})$ the complex modular variety

$$X(U) = G(\mathbb{Q}) \backslash G(\mathbb{A})_+ / UZ(\mathbb{R})C_{\infty+},$$

where $G(\mathbb{A})_+ = G(\mathbb{A}^{(\infty)})G(\mathbb{R})_+$ for the identity connected component $G(\mathbb{R})_+$ of the Lie group $G(\mathbb{R})$. We take \mathcal{O} to be sufficiently large so that its field K of fractions contains all conjugates of F over \mathbb{Q} . Let $O = O_F$ be the integer ring of F . We define an open compact subgroup of $G(\mathbb{A}^{(\infty)})$ for an ideal N of F by

$$U_0(N) = \left\{ x \in G(\widehat{\mathbb{Z}}) \mid x \bmod N \in B(O/N) \right\},$$

where B is the standard upper triangular Borel subgroup of $GL(2)_{/\mathbb{Z}}$. Then for each field embedding $\sigma : F \hookrightarrow K$, we have the projection $\sigma : G(\mathbb{Q}_p) \rightarrow GL_2(K)$. Hereafter we suppose that $U \subset U_0(\mathfrak{f})$. Then $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \chi'_f(d_f)$ is a character of U . Now we consider the space of a polynomial representation of U

$$L(n, v, \chi'; K) \cong \chi'_f \otimes \left\{ \bigotimes_{\sigma} (\det(\sigma)^{v_{\sigma}} \otimes \text{Sym}^{\otimes n_{\sigma}}(\sigma)) \right\}$$

for the symmetric m -th tensor representation $\text{Sym}^{\otimes m}(\sigma)$ of $\sigma : G(\mathbb{Q}_p) \rightarrow GL_2(K)$. Thus we regard n and v as a linear combination of embeddings of F into K with coefficients n_{σ} and v_{σ} . To make things more precise, we take $L(n, v, \chi'; A)$ to be the space of polynomials in $\{(X_{\sigma}, Y_{\sigma})\}_{\sigma}$, with coefficients in a general \mathcal{O} -module A , homogeneous of degree n_{σ} for each pair (X_{σ}, Y_{σ}) . We let $\gamma \in U$ act on $P \in L(n, v, \chi'; A)$ by

$$\gamma P((X_{\sigma}, Y_{\sigma})) = \chi'_f(d_f) \det(\gamma)^v P((X_{\sigma}, Y_{\sigma})^t \sigma(\gamma)^t),$$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $a^v = \prod_{\sigma} \sigma(a)^{v_{\sigma}}$. Then we define a covering space $\mathcal{X}(U)$ of $X(U)$ by

$$G(\mathbb{Q}) \backslash (G(\mathbb{A}) \times L(n, v, \chi'; K)) / UZ(\mathbb{R})C_{\infty+},$$

where the action is given by $\gamma(x, P)u = (\gamma x u, u_p^t P)$ for $\gamma \in G(\mathbb{Q})$ and $u \in UZ(\mathbb{R})C_{\infty+}$ with $u^t = \det(u)u^{-1}$.

Now we consider the sheaf of locally constant sections of $\mathcal{X}(U)$ over $X(U)$, which we write again as $L(n, v, \chi'; A)$. For $q = [F : \mathbb{Q}]$, we consider

$$S(U; A) = H_{\text{cusp}}^q(X(U), L(n, v, \chi'; A)).$$

Writing simply $L(A)$ for $L(n, v, \chi'; A)$, we recall the definition of $H_{\text{cusp}}^q(X(U), L(A))$. When $n \neq 0$ or $[F : \mathbb{Q}]$ is odd, $H_{\text{cusp}}^q(X(U), L(\mathcal{O}))$ is defined to be the natural image of the compactly supported cohomology group $H_c^q(X(U), L(\mathcal{O}))$ in $H^q(X(U), L(K))$. When $n = 0$ and $[F : \mathbb{Q}]$ is even, in $H^q(X(U), L(K))$, we have the space $\text{Inv}(U)$ of invariant classes $\text{Inv}(U)$ spanned by cohomology classes of the connected components of $X(U)$ (see [H88] Theorem 6.2). We then define

$$H_{\text{cusp}}^q(X(U), L(\mathcal{O})) = \text{Im} \left(H_c^q(X(U), L(\mathcal{O})) \rightarrow \frac{H^q(X(U), L(K))}{\text{Inv}(U)} \right).$$

Once $H_{\text{cusp}}^q(X(U), L(\mathcal{O}))$ is defined, we just put

$$H_{\text{cusp}}^q(X(U), L(A)) = H_{\text{cusp}}^q(X(U), L(\mathcal{O})) \otimes_{\mathcal{O}} A.$$

We suppose that $S(U; K) \neq 0$ for sufficiently small U , and hence $n + 2v = [n + 2v]t$ for $[n + 2v] \in \mathbb{Z}$ and $t = \sum_{\sigma} \sigma$. On this space, Hecke operators $T(y) = \left[U \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} U \right]$ naturally acts as described in [H88] Section 7; further, $\mathbb{T}(y) = y_p^{-v} T(y)$ preserves the image of $H_{\text{cusp}}^q(X(U), L(n, v, \chi'; \mathcal{O}))$.

We consider the \mathcal{O} -subalgebra $h_{n,v,\chi'}(U)$ of $\text{End}_K(S(U; K))$ generated by $\mathbb{T}(y)$ for all integral ideles y , which is an algebra free of finite rank over \mathcal{O} . Then it is easy to see that the central action $\langle z \rangle = \mathcal{N}_p^{-[n+2v]} \chi^{-1}(z) [UzU]$ of $z \in Z(\mathbb{A}^{(\infty)})$ is naturally contained in $h_{n,v,\chi'}(U)$ where \mathcal{N}_p is the p -adic cyclotomic character, and χ is the Teichmüller lift of a global Hecke character (of finite order) extending $\chi' \chi_p$ with values in \mathbb{F}^\times . Thus $h_{n,v,\chi'}(U)$ is an algebra over $\mathcal{O}[[\mathbf{G}]]$ via the character $z \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} \mapsto \langle z \rangle \mathbb{T}(y)$, where $\mathbf{G} = Cl_F(p^\infty) \times O_p^\times$ ($O_p = O \otimes_{\mathbb{Z}} \mathbb{Z}_p$) for the ray class group $Cl_F(p^\infty)$ modulo p^∞ . Now we define more open compact subgroups of $U_0(N)$. For that, we write U for the unipotent radical of B . For each ideal \mathfrak{m} of O

$$U_{11}(\mathfrak{m}) = \left\{ u \in G(\widehat{\mathbb{Z}}) \mid u \bmod \mathfrak{m} \in U(O/\mathfrak{m}) \right\}.$$

We put $U_\alpha = U_{11}(p^\alpha) \cap U_0(N)$. Then we have a commutative diagram for $0 < \alpha < \beta$

$$\begin{array}{ccc} S(U_\alpha; K) & \longrightarrow & S(U_\beta; K) \\ T \downarrow & & T \downarrow \\ S(U_\alpha; K) & \longrightarrow & S(U_\beta; K) \end{array}$$

where $T = \mathbb{T}(y)$ and $\langle z \rangle$, respectively. Thus restriction of operators gives surjective \mathcal{O} -algebra homomorphisms: $h(U_\beta) \rightarrow h(U_\alpha)$. We then define

$$h(N, p^\infty; \mathcal{O})_{/F} = \varprojlim_{\alpha} h(U_\alpha),$$

which is a compact semi local ring. Since the projection maps take $\mathbb{T}(y)$ to $\mathbb{T}(y)$, we have well defined $\mathbb{T}(y)$ in $h(N, p^\infty; \mathcal{O})$. In particular, for a prime element $\varpi_{\mathfrak{q}}$ of $F_{\mathfrak{q}}$ ($\mathfrak{q} \nmid p$), $\mathbb{T}(\varpi_{\mathfrak{q}})$ is independent of the choice of $\varpi_{\mathfrak{q}}$, which we therefore write as $\mathbb{T}(\mathfrak{q})$.

Writing $h(N, p^\infty; \mathcal{O})_{/F} = \prod_h h_{/F}$ as a product of local rings $h_{/F}$ with maximal ideal \mathfrak{m}_h , we write $\mathbb{T}_h(y)$ for the projection of $\mathbb{T}(y)$ to h . Then we define the nearly p -ordinary part of $h(N, p^\infty; \mathcal{O})_{/F}$ by

$$h^{n.\text{ord}}(N, p^\infty; \mathcal{O})_{/F} = \prod_{\mathbb{T}_h(p) \in h^\times} h_{/F}.$$

We write W (resp. \mathbb{W}) for the maximal torsion-free quotient (resp. the maximal p -profinite quotient) of \mathbf{G} . The projector $e = \lim_n \mathbb{T}(p)^{n!}$ onto the nearly p -ordinary part kills the p -old part, and the prime-to- p part of $N' = N/\mathfrak{f}$ for the conductor \mathfrak{f} of χ' is square-free. From this, if $\bar{\rho} = \rho_{\mathfrak{m}}$ satisfies the conditions of D , we conclude that the local component h of $\bar{\rho}$ of the algebra $h^{n.\text{ord}}(N, p^\infty; \mathcal{O})$ is reduced. For each character $\kappa = (n, v, \varepsilon, \xi) : \mathbf{G} \rightarrow \mathcal{O}^\times$ given by

$$\langle z \rangle \mathbb{T}(y) \mapsto \mathcal{N}_p^{-[n+2v]} \varepsilon(z) y^{-v} \xi(y),$$

we consider the κ -eigen subspace $S(U_\alpha; K)[\kappa]$ of $S(U_\alpha; K)$ for sufficiently large α so that $\varepsilon\xi$ factors through $Cl_F(p^\alpha) \times (O_F/p^\alpha)^\times$. Then we define the Hecke algebra $h_\kappa^{n.\text{ord}}(\mathcal{O})$ by the \mathcal{O} -subalgebra of $\text{End}_{\mathcal{O}}(S(U_\alpha; K)[\kappa])$ generated by $\mathbb{T}(y)$ and $\langle z \rangle$. Then this algebra is well determined only by κ and is independent of α . As shown in [H89a] Theorem 2.4 (see also Lemma 3.10), we have a canonical morphism

$$(\kappa) \quad h^{n.\text{ord}}(N, p^\infty, \mathcal{O}) \otimes_{\mathcal{O}[[\mathbf{G}], \kappa]} \mathcal{O} \twoheadrightarrow h_\kappa^{n.\text{ord}}(\mathcal{O}),$$

which is a priori surjective and proven to be of finite kernel. Further, as seen in [H89a] Section 3, we have

- (FF) *There exists a $\mathcal{O}[[\mathbb{W}]]$ -free module X of finite rank on which $h^{n.\text{ord}}(N, p^\infty; \mathcal{O})$ acts faithfully; in particular $h^{n.\text{ord}}(N, p^\infty; \mathcal{O})$ is a torsion-free $\mathcal{O}[[W]]$ -module of finite type;*
- (red) $h^{n.\text{ord}}(N, p^\infty; \mathcal{O})$ is reduced;
- (Inj) $\mathcal{O}[[\mathbb{W}]]$ injects into $h^{n.\text{ord}}(N, p^\infty; \mathcal{O})$.

For each local ring $h = h_{/F}$ of $h^{n.\text{ord}}(N, p^\infty; \mathcal{O})_{/F}$ and prime ideal P of h , we know from [Ta] and [BR] (see also [H89b]) the existence of a semi-simple Galois representation $\rho_P : \text{Gal}(\mathbb{Q}/F) \rightarrow GL_2(k(P))$ for the residue field $k(P) = h_P/P$ satisfying the following six conditions:

- (Ct) ρ_P preserves an h -submodule L of finite type generating $k(P)^2$ over $k(P)$ and is \mathfrak{m}_h -adically continuous as a map from $\text{Gal}(\overline{\mathbb{Q}}/F)$ into $\text{Aut}_h(L)$;
- (unr) ρ_P is unramified outside Σ ;
- (n.ord) ρ_P is nearly p -ordinary and satisfies: $\delta_{\mathfrak{q},\rho}([y; F_{\mathfrak{p}}]) = \mathbb{T}_h(y)$ for $y \in F_{\mathfrak{p}}^\times$,

where $[y, F_{\mathfrak{p}}]$ is the Artin symbol of local class field theory. For primes \mathfrak{q} dividing \mathfrak{f} , write $\chi_{\mathfrak{q}}$ for the character of \mathcal{I}_{Ω} corresponding to χ restricted to $O_{\mathfrak{q}}^\times$. Then

$$(\mathcal{M}) \quad \rho_P \text{ satisfies } (\chi_{\mathfrak{q}}) \text{ for } \mathfrak{q}|\mathfrak{f}.$$

For primes $\mathfrak{q} \in \mathcal{M}' \Leftrightarrow \mathfrak{q}|N'$,

$$(\mathcal{M}') \quad \rho_P \text{ satisfies } (\mathcal{N}_{\mathfrak{q}}) \text{ or is unramified for } \mathfrak{q}|N'.$$

Finally for primes \mathfrak{q} outside pN ,

$$(\text{Ch}) \quad \det(1_2 - \rho_P(\text{Frob}_{\mathfrak{q}})X) = 1 - \mathbb{T}(\mathfrak{q})X + \chi_{\mathcal{N}_p}(\text{Frob}_{\mathfrak{q}})\langle \mathfrak{q} \rangle X^2 \in k(P)[X]$$

for the p -cyclotomic character \mathcal{N}_p . When $\rho_{\mathfrak{m}}$ for the maximal ideal \mathfrak{m} of h is absolutely irreducible, we have a unique isomorphism class of representations $\rho_h : \text{Gal}(\overline{\mathbb{Q}}/F) \rightarrow GL_2(h)$ satisfying the above conditions [C]. Thus supposing $(\mathcal{N}_{\mathfrak{q}})$ for $\bar{\rho} = \rho_{\mathfrak{m}}$ for all $\mathfrak{q} \in \mathcal{M}'$, we know $\rho_h \in \mathcal{F}_{F,\bar{\rho}}(h)$.

4.3. Universality of the Hecke algebras. We continue to use the notation and keep the assumption introduced in 4.1, and assume hereafter $\bar{\rho}$ is “minimally modular” in the following sense:

- (1) $\mathcal{M}'' = \emptyset$;
- (2) There exists a connected component $\text{Spec}(h)$ of $\text{Spec}(h^{n \cdot \text{ord}}(N, p^\infty; \mathcal{O}))$ such that $\bar{\rho} \cong \rho_h \pmod{\mathfrak{m}_h} = \rho_{\mathfrak{m}_h}$ for the maximal ideal \mathfrak{m}_h of h ;
- (3) $\bar{\rho} = \rho_{\mathfrak{m}_h}$ satisfies the conditions of

$$D = \{(\chi_{\mathfrak{q}})|_{\mathfrak{q}|\mathfrak{f}}\} \cup \{(\mathcal{N}_{\mathfrak{q}})|_{\mathfrak{q}|N'}\}$$

described in the previous section.

Here the word “minimally” means that there exists a Hilbert Hecke eigenform of weight 2, exact prime-to- p level N and the central character χ whose Galois representation is a deformation of $\bar{\rho}$ of type D . This conditions follow from the above three conditions. Because of nearly ordinarity, we can always find such f of weight 2 with optimal p -level and optimal p -primary part of the central character, and by (3) and the construction of the Hecke algebra done in the previous section, the prime-to- p part of the central character is already optimal (cf. [H89a] Lemma 3.10). Note here that we have assumed that χ is of order prime to p . Thus $\chi\omega$ is the Teichmüller lift of $\det \bar{\rho}$.

Let $\kappa \in \text{Spec}(\mathcal{O}[[\mathbb{W}]]) (\mathcal{O})$. Then by (κ) , $h \otimes_{\mathcal{O}[[\mathbb{W}]], \kappa} \mathcal{O}$ is an \mathcal{O} -module of finite type, and the maximal torsion-free quotient $(h \otimes_{\mathcal{O}[[\mathbb{W}]], \kappa} \mathcal{O})_f$ is canonically isomorphic to the local ring h_κ of $h_\kappa^{n, \text{ord}}(\mathcal{O})$ corresponding to the deformation of $\bar{\rho}$. Write $\rho_\kappa : \text{Gal}(\bar{\mathbb{Q}}/F) \rightarrow GL_2(h_\kappa)$ for the deformation. For the trivial character $\kappa_0 : \mathbb{W} \rightarrow \mathcal{O}^\times$, h_{κ_0} is the local ring associated to $\bar{\rho}$ of the Hecke algebra of weight 2, prime-to- p level N and with central character χ . The following result is shown by K. Fujiwara [F]:

Theorem 4.1 (Fujiwara). *Let p be an odd prime, and suppose that p is unramified in F/\mathbb{Q} : (Hyp $_p$). Let χ be a Hecke character of order prime to p with prime-to- p conductor \mathfrak{f} . Let $N = N'\mathfrak{f}$ for a square free ideal N' of F prime to p . Suppose that $\bar{\rho}$ is minimally modular and is associated to a local ring h of $h^{n, \text{ord}}(N, p^\infty; \mathcal{O})$ in the sense described above; in particular, we assume that $\bar{\rho}$ satisfies the conditions of $D = \{(\chi_q) | \mathfrak{q} | \mathfrak{f}\} \cup \{(\mathcal{N}_q) | \mathfrak{q} | N'\}$. Assume further the following two conditions on $\bar{\rho} = \rho_{\mathfrak{m}_h} : \left(\text{AI}_F(\sqrt{(-1)^{(p-1)/2p}}) \right)$ and (Reg_F) . Let $\kappa_0 : \mathbb{W} \rightarrow \mathcal{O}^\times$ be the trivial character. Then the couple $(h_{\kappa_0}, \rho_{\kappa_0})$ represents the functor $\mathcal{F}_F^{\text{ord}, \chi \mathcal{N}_p}$.*

In [F], the above assertion is proven by assuming that p is also prime to the class number of F . Under this assumption, the functor $\mathcal{F}_F^{\text{ord}, \chi \mathcal{N}_p}$ is identical to the subfunctor of $\mathcal{F}_F^{\text{ord}}$ made of deformations ρ with $\det(\rho) = \chi \mathcal{N}_p$ locally on each inertia group at primes dividing the level. Imposing the determinant condition globally, it is easy to check the argument given in [F] still works without this extra hypothesis. According to the lecture of Fujiwara given in Paris at the Poincaré Institute on June 23 (1997), a further progress has been made: the assertion of the theorem is valid even if we replace the assumption (Hyp $_p$) by the following weaker condition:

(LD $_p$)
 F is linearly disjoint from $\mathbb{Q}(\mu_p)$ over \mathbb{Q} and $\mu_p(F_{\mathfrak{p}}) = \{1\}$ for all $\mathfrak{p} | p$.

Anyway until a written version of the above theorem under this weaker hypothesis appears in print, we would only rely on the theorem as stated above.

We now extend the assertion of Fujiwara’s theorem to more bigger Hecke algebras. For that, we prepare some notation. Let $\mathbb{W}_{\mathfrak{p}} \hookrightarrow \mathcal{O}_{\mathfrak{p}}^\times$ (resp. $W_{\mathfrak{p}}$) be the maximal p -profinite part (resp. the maximal p -torsion-free quotient) of the image of the inertia group in the maximal abelian quotient of $\mathcal{D}_{\mathfrak{p}}$ ($\mathfrak{P} | \mathfrak{p}$). Let $\mathbb{W}^- = \prod_{\mathfrak{p} | p} \mathbb{W}_{\mathfrak{p}}$ and $W^- = \prod_{\mathfrak{p} | p} W_{\mathfrak{p}}$. Then $\mathbb{W} \cong \mathbb{W}^- \times \mathbb{W}^+(p)$ (resp. $W \cong W^- \times W^+(p)$) for the maximal p -profinite part $\mathbb{W}^+(p)$ (resp. the maximal torsion-free quotient $W^+(p)$) of $Cl_F(p^\infty)$. Hereafter we identify

\mathbb{W} with $\mathbb{W}^- \times \mathbb{W}^+(p)$. Then $\mathcal{O}[[W^-]]$ is isomorphic to a power series ring of $[F : \mathbb{Q}]$ variables over \mathcal{O} . The ring $\mathcal{O}[[O_p^\times]]$ is isomorphic to a product of copies of $\mathcal{O}[[\mathbb{W}^-]]$. Let h^χ be the subalgebra of h generated by $\text{Tr}(\rho_h^{\chi \mathcal{N}_p})$, where $\rho_h^{\chi \mathcal{N}_p} = \rho_h \otimes (\chi \mathcal{N}_p \det(\rho_h)^{-1})^{1/2}$. In the same manner as in [H96b] Proposition 2.1, we can prove, on the automorphic side,

(FF') *There exists a $\mathcal{O}[[\mathbb{W}^-]]$ -free module of finite type on which h^χ acts faithfully, in particular, h^χ is a torsion-free $\mathcal{O}[[\mathbb{W}^-]]$ -module of finite type;*

(T')
$$h \cong h^\chi \widehat{\otimes}_{\mathcal{O}} \mathcal{O}[[\mathbb{W}^+(p)]] .$$

On the Galois side, we have seen in 4.1

(T)
$$R_F \cong R_F^{\chi \mathcal{N}_p} \widehat{\otimes}_{\mathcal{O}} \mathcal{O}[[\mathbb{W}^+(p)]] .$$

We now prove the universality of h^χ and h assuming that $(h_{\kappa_0}, \rho_{\kappa_0})$ represents the functor $\mathcal{F}_F^{\text{ord}, \chi \mathcal{N}_p}$. For simplicity, we further assume that $\mu_p(F_p) = \{1\}$ for all $\mathfrak{p}|p$ ($\Leftrightarrow \mathbb{W}^- = W^-$). By definition, ρ is p -ordinary if and only if $\delta_{\mathfrak{p}, \rho}$ is trivial on $\mathbb{W}_{\mathfrak{p}}$ for all $\mathfrak{p}|p$ because $\bar{\rho}$ is p -ordinary. Thus writing $\mathfrak{a}_{\text{ord}}$ for the augmentation ideal of $\mathcal{O}[[\mathbb{W}^-]]$,

$$R_F^{\text{ord}, \chi \mathcal{N}_p} \cong R_F^{\chi \mathcal{N}_p} / \mathfrak{a}_{\text{ord}} R_F^{\chi \mathcal{N}_p} .$$

Then we have the following commutative diagram for the identity character $\kappa_0 : \mathbb{W} \rightarrow \mathcal{O}^\times$:

$$\begin{array}{ccc} \iota : R_F^{\chi \mathcal{N}_p} & \longrightarrow & h^\chi \\ \downarrow & & \downarrow \\ \iota' : R_F^{\chi \mathcal{N}_p} / \mathfrak{a}_{\text{ord}} R_F^{\chi \mathcal{N}_p} & \longrightarrow & h^\chi / \mathfrak{a}_{\text{ord}} h^\chi \\ \downarrow \cong & & \downarrow \beta \\ \iota'' : R_F^{\text{ord}, \chi \mathcal{N}_p} & \longrightarrow & h_{\kappa_0} . \end{array}$$

Suppose that ι'' is an isomorphism. Then ι' has to be an isomorphism because of the surjectivity of ι' and β . The surjectivity of ι and ι' follows from the properties (χ_q) and (\mathcal{N}_q) (cf. [MT]). Hence $h^\chi / \mathfrak{a}_{\text{ord}} h^\chi \cong h_{\kappa_0}$ is \mathcal{O} -free of rank $r < \infty$. Choose an \mathcal{O} -base $\{\bar{\theta}_1, \dots, \bar{\theta}_r\}$ of h_{κ_0} and lift it to a subset $\{\theta_1, \dots, \theta_r\}$ of h^χ . By Nakayama's lemma, $\{\theta_1, \dots, \theta_r\}$ generates h^χ . Since h^χ is $\mathcal{O}[[\mathbb{W}^-]]$ -torsion-free (and acts faithfully on an $\mathcal{O}[[\mathbb{W}^-]]$ -free module of finite type (FF')), h^χ has to be $\mathcal{O}[[\mathbb{W}^-]]$ -free of rank r . This implies, again by Nakayama's lemma, ι has to be an isomorphism. Then by (T) and (T'), we get $R_F \cong h$. Thus we get:

Theorem 4.2 *Let p be an odd prime, and suppose $\mu_p(F_p) = \{1\}$ for all $\mathfrak{p}|p$. Let χ be a Hecke character of order prime to p with prime-to- p conductor*

f. Let $N = N'\mathfrak{f}$ for a square free ideal N' of F prime to p . Suppose that $\bar{\rho}$ is minimally modular and is associated to a local ring h of $h^{n, \text{ord}}(N, p^\infty; \mathcal{O})$; in particular, we assume that $\bar{\rho}$ satisfies the conditions of $D = \{(\chi_{\mathfrak{q}})|\mathfrak{q}|\mathfrak{f}\} \cup \{(\mathcal{N}_{\mathfrak{q}})|\mathfrak{q}|N'\}$. Assume further the following conditions on $\bar{\rho} = \rho_{\mathfrak{m}} : (\text{AI}_F)$ and (Reg_F) . If h_{κ_0} for the identity character $\kappa_0 : \mathbb{W} \rightarrow \mathcal{O}^\times$ as above represents the functor $\mathcal{F}_F^{\text{ord}, \chi^{N_p}}$, then $(h^\chi, \rho_h^{\chi^{N_p}})$ represents $\mathcal{F}_F^{\chi^{N_p}}$, and (h, ρ_h) represents \mathcal{F}_F .

Corollary 4.3 *Let the assumption be as in Theorem 4.2. Suppose that h_{κ_0} represents the functor $\mathcal{F}_F^{\text{ord}, \chi^{N_p}}$. Then h^χ (resp. h) is $\mathcal{O}[[\mathbb{W}^-]]$ -free (resp. $\mathcal{O}[[\mathbb{W}]]$ -free) of finite rank. For every arithmetic character $\kappa = (n, v, \varepsilon, \xi)$ of \mathbb{W} , we have $h \otimes_{\mathcal{O}[[\mathbb{W}]], \kappa} \mathcal{O} \cong h_\kappa$.*

We now fix field embeddings $i_p : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$ and $i_\infty : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$. We write \mathfrak{P} for the prime of \mathbb{Q} over p corresponding to i_p . By (κ) combined with the Eichler-Shimura isomorphism proven by Harder (cf. [H93] Section 4), we recover a result in [H89a]:

Proposition 4.4 *Let κ be an arithmetic character (n, v, ε, ξ) of \mathbb{W} with (ε, ξ) factoring through $Cl_F(p^\alpha) \times (O/p^\alpha O)^\times$. For any \mathcal{O} -algebra homomorphism $\lambda : h_\kappa \rightarrow \bar{\mathbb{Q}}_p$, there exists a unique holomorphic Hilbert modular form f of weight κ on U_α such that $f|\mathbb{T}(\mathfrak{q}) = i_\infty \circ i_p^{-1}(\lambda(\mathbb{T}(\mathfrak{q})))f$ for all ideal \mathfrak{q} prime to p .*

4.4. Base change and ordinary deformation. We first apply the theory described in 4.3 when $F = \mathbb{Q}$. In our application, we anyway assume $\mathcal{M}' = \emptyset$. We therefore fix a primitive Dirichlet character χ' of conductor N prime to p . We fix a Dirichlet character χ modulo Np with $\chi|_{(\mathbb{Z}/N\mathbb{Z})^\times} = \chi'$. We consider the deformation data:

$$D_{\mathbb{Q}} = \{(\chi_{\mathfrak{q}})|\mathfrak{q}|N\}.$$

Let $\bar{\rho} : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{F})$ be a minimally modular representation of type $D_{\mathbb{Q}}$ satisfying $\left(\text{AI}_{\mathbb{Q}}(\sqrt{(-1)^{(p-1)/2p}})\right)$ and $(\text{Reg}_{\mathbb{Q}})$. By our choice, we have $\Sigma = \{q|Np\} \cup \{\infty\}$.

We now take a totally real finite extension F/\mathbb{Q} . As long as Np is unramified in F/\mathbb{Q} , for the restriction $\bar{\rho}_F$ of $\bar{\rho}$ to $\text{Gal}(\bar{\mathbb{Q}}/F)$, we see that $\left(\text{AI}_F(\sqrt{(-1)^{(p-1)/2p}})\right) \iff \left(\text{AI}_{\mathbb{Q}}(\sqrt{(-1)^{(p-1)/2p}})\right)$ and $(\text{Reg}_F) \iff (\text{Reg}_{\mathbb{Q}})$. We regard the Dirichlet character χ we have chosen for \mathbb{Q} as a Galois character of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. We write χ_F for the restriction of χ to $\text{Gal}(\bar{\mathbb{Q}}/F)$. Let N_F be the prime-to- p conductor of χ_F . We then define Σ_F by the set of

infinite places of F , places of F appearing in N_F and places of F above p . We then consider the deformation data:

$$D_F = \{(\chi_{F,\mathfrak{q}})|_{\mathfrak{q}}|N_F\}.$$

Then combining all what we have said, we get:

Corollary 4.5 *Let the notation be as above. Suppose $f \in S_k(\Gamma_1(Np^\alpha))$ with $k \geq 2$ be a primitive form whose \mathfrak{B} -adic Galois representation ρ is a p -ordinary deformation of $\bar{\rho}$ of type $D_{\mathbb{Q}}$. Suppose (Hyp_{Np}) for a totally real field F , $(\text{Reg}_{\mathbb{Q}})$ and $\left(\text{AI}_{\mathbb{Q}}(\sqrt{(-1)^{(p-1)/2}p})\right)$ for $\bar{\rho}$ and that $\bar{\rho}_F$ is minimally modular over F , that is, there exists a Hilbert primitive form g of prime-to- p level N_F on $GL(2)_F$ such that its \mathfrak{B} -adic Galois representation ρ_g is a deformation of type D_F with $\det(\rho_g) = \chi_F \mathcal{N}_p$. If p is unramified in F/\mathbb{Q} , then there exists a holomorphic primitive Hilbert cusp form \hat{f} whose Mellin transform is $L(s, \rho_F)$.*

As already remarked, When p is unramified in F/\mathbb{Q} , we know (Reg_F) for $\bar{\rho}_F \iff (\text{Reg}_{\mathbb{Q}})$ for $\bar{\rho}$. Thus the four conditions in the introduction are enough to apply the above corollary.

We close this section giving an example of minimally modular Galois representations. The example is given by a theta series of a quadratic extension M/F . Thus in particular, we have $\mathcal{M}' = \emptyset$. We take a finite order character $\bar{\varphi} : \text{Gal}(\bar{\mathbb{Q}}/M) \rightarrow \mathbb{F}^\times$. Let $\varphi : \text{Gal}(\bar{\mathbb{Q}}/M) \rightarrow \mathcal{O}^\times$ be the Teichmüller lift of $\bar{\varphi}$. We regard φ as a Hecke character $\varphi : M^\times \backslash M_{\mathbb{A}}^\times \rightarrow \mathcal{O}^\times$, and write $\check{\varphi}$ for the restriction of φ to $F_{\mathbb{A}}^\times$. Let \mathfrak{c} be the conductor of φ . Let $N = (\mathfrak{c} \cap F)\mathfrak{d}$ for the relative discriminant \mathfrak{d} for M/F . We assume

- (1) Every prime factor \mathfrak{q} of $(\mathfrak{c} \cap F)p$ in F splits in M ;
- (2) For each prime factor \mathfrak{q} of $(\mathfrak{c} \cap F)p$ in F , φ is unramified at one prime factor \mathfrak{Q} of \mathfrak{q} in M , and φ is ramified for the other factor \mathfrak{Q}' of \mathfrak{q} ;
- (3) For each real place σ of F which remains real in M , φ is trivial at one factor of σ in M and is non-trivial at the other factor.

Then, as is well known, we can find a holomorphic theta series $\theta(\varphi)$ with $L(s, \theta(\varphi)) = L(s, \varphi)$. The modular form $\theta(\varphi)$ is of weight 1, has exact prime-to- p level N and the central character $\check{\varphi}\alpha$, where α is the quadratic character associated to M/F . By definition, $\theta(\varphi)$ is p -ordinary ($\theta(\varphi)|_{T(\mathfrak{q})} = \varphi(\mathfrak{Q})\theta(\varphi)$ under the notation of (2)). The Galois representation of $\theta(\varphi)$ is given by $\text{Ind}_M^F \varphi$. Since $\theta(\varphi)$ is p -ordinary, we can lift $\theta(\varphi)$ to a p -adic family of p -ordinary forms. This is possible even for weight 1 forms $\theta(\varphi)$ because of the existence of a higher weight p -power level form E with $E \equiv 1 \pmod{p}$. Then

weight 2 member θ of the family satisfies the conditions for $\text{Ind}_M^F \bar{\varphi}$ being minimally modular.

Choose φ as above for $F = \mathbb{Q}$. Then M is just a quadratic field. Now for a general totally real field F , we consider composite MF and the restriction $\varphi_{MF} : \text{Gal}(\bar{\mathbb{Q}}/MF) \rightarrow \mathcal{O}^\times$ of φ . As long as F/\mathbb{Q} is unramified at N , $\text{Ind}_{MF}^F \varphi_{MF}$ remains absolutely irreducible and p -ordinary. In particular, $\theta(\varphi_{MF})$ is the base change lift of $\theta(\varphi)$ to F . By Theorem 4.1, Theorem 4.2 and Proposition 4.4 combined (in short, Corollary 4.5), a weight $k \geq 2$ member of the p -adic family of $\theta(\varphi_{MF})$ is the base change lift of each weight k member of the p -adic family of $\theta(\varphi)$.

5. Characteristic polynomials for the Hecke operator $T(2)$.

Write simply S_k for $S_k(SL_2(\mathbb{Z}))$. For a primitive form $f_k \in S_k$, we denote by $\mathbb{Q}(f_k)$ the field generated over \mathbb{Q} by all Fourier coefficients of f_k , by $\mathbb{Q}(f_k)^{\text{Gal}}$ the Galois closure of $\mathbb{Q}(f_k)$, and by $G(f_k)$ the Galois group $\text{Gal}(\mathbb{Q}(f_k)^{\text{Gal}}/\mathbb{Q})$. We call S_k *non-splitting* if S_k is spanned by all Galois conjugates of f_k . Let $\phi_k(x)$ be the characteristic polynomial of the Hecke operator $T(2)$ on S_k . *If $\phi_k(x)$ is irreducible over \mathbb{Q} , then $\mathbb{Q}(f_k) = \mathbb{Q}(\alpha)$ with a root α of $\phi_k(x) = 0$, $\mathbb{Q}(f_k)^{\text{Gal}}$ is the minimal splitting field of $\phi_k(x)$, and S_k is non-splitting.* We have calculated $\phi_k(x)$ using Eichler-Selberg trace formula (see [Mi] pp. 266-267) for $k \leq 468$. About 20 years ago, Maeda observed that $\phi_k(x)$ are irreducible over \mathbb{Q} for all the cases where $\dim_{\mathbb{C}} S_k \leq 12$ and later checked the fact up to $k \leq 468$; thus S_k is *non-splitting* if $k \leq 468$. We denote by \mathfrak{S}_n the symmetric group of degree n . Recently, first Lee and Hung [LH] and then Buzzard [Bu] have observed that $G(f_k)$ is isomorphic to \mathfrak{S}_n with $n = \dim_{\mathbb{C}} S_k$ for several values of k , in particular, the cases where $\dim_{\mathbb{C}} S_k \leq 7$ and $k = 12\ell$ with prime $\ell \leq 19$ are treated in [Bu]. Learning this phenomenon, we have checked that $G(f_k) \cong \mathfrak{S}_n$ with $n = \dim_{\mathbb{C}} S_k$ for $k \leq 468$. This is the origin of Conjecture 1.2. The validity of the conjecture is checked numerically for weight ≤ 468 by using the following fact which is pointed out to Maeda by K. Kubo.

Proposition 5.1 *Let $\phi(x) \in \mathbb{Z}[x]$ be a monic polynomial. Suppose that there exist three primes p_1, p_2, p_3 satisfying the following conditions:*

- (1) $\phi(x) \pmod{p_1}$ is irreducible over \mathbb{F}_{p_1} ;
- (2) $\phi(x) \equiv \varphi_1(x) \cdots \varphi_n(x) \pmod{p_2}$ with distinct irreducible polynomials $\varphi_i(x) \in \mathbb{F}_{p_2}[x]$ such that $\deg \varphi_1(x) = 2$ and $\deg \varphi_i(x)$ are odd for $i \geq 2$;
- (3) $\phi(x) \equiv \psi_1(x)\psi_2(x) \pmod{p_3}$ with distinct irreducible polynomials $\psi_i(x) \in \mathbb{F}_{p_3}[x]$ such that $\deg \psi_1(x) = 1$ and $\deg \psi_2(x) = \deg \phi(x) - 1$.

Then $\phi(x)$ is irreducible over \mathbb{Q} and the Galois group of the minimal splitting field of $\phi(x)$ is isomorphic to \mathfrak{S}_n with $n = \deg \phi(x)$. Here \mathbb{F}_ℓ stands for a finite field with ℓ elements.

This follows from the following lemmas, whose proof we leave to the reader.

Lemma 5.2 *Let G be a transitive subgroup of \mathfrak{S}_n . If G contains a transposition and a cycle of length $n - 1$, then $G = \mathfrak{S}_n$.*

Lemma 5.3 (van der Waerden). *Let $\phi(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial over \mathbb{Q} and G be the Galois group of the minimal splitting field of $\phi(x)$. We consider G as a permutation group over the set of all roots of $\phi(x) = 0$. Suppose for a prime p that $\phi(x) \equiv \varphi_1(x) \cdots \varphi_h(x) \pmod{p}$ with distinct irreducible polynomials $\varphi_i(x) \in \mathbb{F}_p[x]$. Then G contains a permutation of type $(1, 2, \dots, \ell_1)(\ell_1 + 1, \dots, \ell_1 + \ell_2) \cdots (\ell_1 + \dots + \ell_{h-1}, \dots, \ell_1 + \dots + \ell_h)$. Here $\ell_i = \deg \varphi_i(x)$.*

Here we list $\phi_k(x)$ and the prime factorization¹ of their discriminants D_k for some of small weights with $2 \leq \dim_{\mathbb{C}} S_k \leq 3$.

Table 1. Characteristic Polynomials of $T(2)$ and their discriminants.

k	$\phi_k(x)$	D_k
24	$x^2 - 1080x - 20468736$	$2^6 \cdot 3^2 \cdot 144169$
28	$x^2 + 8280x - 195250176$	$2^6 \cdot 3^6 \cdot 131 \cdot 139$
30	$x^2 - 8640x - 454569984$	$2^{12} \cdot 3^2 \cdot 51349$
32	$x^2 - 39960x - 2235350016$	$2^6 \cdot 3^2 \cdot 67 \cdot 273067$
34	$x^2 + 121680x - 8513040384$	$2^8 \cdot 3^4 \cdot 479 \cdot 4919$
36	$x^3 - 139656x^2 - 59208339456x - 1467625047588864$	$2^{30} \cdot 3^{10} \cdot 5^2 \cdot 7^2 \cdot 23 \cdot 1259 \cdot 269461929553$
38	$x^2 + 194400x - 137403408384$	$2^{10} \cdot 3^2 \cdot 181 \cdot 349 \cdot 1009$
40	$x^3 - 548856x^2 - 810051757056x + 213542160549543936$	$2^{26} \cdot 3^{12} \cdot 5^2 \cdot 7^2 \cdot 13^2 \cdot 73 \cdot 59077 \cdot 92419245301$
42	$x^3 + 344688x^2 - 6374982426624x - 520435526440845312$	$2^{34} \cdot 3^{10} \cdot 5^2 \cdot 7^2 \cdot 1465869841 \cdot 578879197969$

¹Here and in other computations, we have used “UBASIC86” which was created by Y. Kida.

As explained in [H] Theorem 5.2.1, $S_k(SL_2(\mathbb{Z}))$ has a \mathbb{Z} -base of \mathbb{Z} -integral cusp forms $\{h_1, \dots, h_d\}$ with $a(i, h_j) = \delta_{ij}$ as long as $j \geq i$. From this, it is easy to conclude that the Hecke algebra $h_k(1, \text{id}; \mathbb{Z})$ has a \mathbb{Z} -base $\{T(1), \dots, T(d)\}$. Thus we have the formula of the exact discriminant of the Hecke algebra:

$$(\text{disc}) \quad d(h_k(1, \text{id}; \mathbb{Z})/\mathbb{Z}) = \det(\text{Tr}(T(i)T(j)))_{1 \leq i, j \leq d},$$

where $d = \dim_{\mathbb{C}} S_k(SL_2(\mathbb{Z}))$. Using this, we can compute the discriminant of the Hecke algebra as follows:

Table 2. Discriminant of Hecke algebras.

weight	dim	Discriminant
24	2	$2^6 \cdot 3^2 \cdot 144169$
28	2	$2^6 \cdot 3^6 \cdot 131 \cdot 139$
30	2	$2^{12} \cdot 3^2 \cdot 51349$
32	2	$2^6 \cdot 3^2 \cdot 67 \cdot 273067$
34	2	$2^8 \cdot 3^4 \cdot 479 \cdot 4919$
36	3	$2^{24} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 23 \cdot 1259 \cdot 269461929553$
38	2	$2^{10} \cdot 3^2 \cdot 181 \cdot 349 \cdot 1009$
40	3	$2^{20} \cdot 3^{10} \cdot 5^2 \cdot 13^2 \cdot 73 \cdot 59077 \cdot 92419245301$
42	3	$2^{22} \cdot 3^6 \cdot 5^2 \cdot 7^2 \cdot 1465869841 \cdot 578879197969$
44	3	$2^{22} \cdot 3^8 \cdot 5^2 \cdot 7^2 \cdot 37 \cdot 92013596772457847677$
46	3	$2^{31} \cdot 3^{12} \cdot 5^2 \cdot 227 \cdot 454287770269681529$
48	4	$2^{40} \cdot 3^{14} \cdot 5^6 \cdot 7^4 \cdot 31 \cdot 6093733$ $\cdot 1675615524399270726046829566281283$
50	3	$2^{22} \cdot 3^{10} \cdot 5^4 \cdot 7^4 \cdot 12284628694131742619401$

We now give a table of prime factorizations of $\phi_k(x) \pmod{p}$ in \mathbb{F}_p in the cases where $8 \leq \dim_{\mathbb{C}} S_k \leq 9$, which confirms the conjecture for these weights.

Table 3. $\phi_k(x) \pmod p$.

k	p	$\phi_k(x) \pmod p$
96	149	$x^8 + 52x^7 + 132x^6 + 40x^5 + 3x^4 + 38x^3 + 83x^2 + 92x + 11$
	23	$(x + 3)(x + 5)(x + 8)(x + 10)(x + 13)(x + 22)(x^2 + 8x + 5)$
	101	$(x + 97)(x^7 + 35x^6 + 4x^5 + 96x^4 + 26x^3 + 35x^2 + 9x + 83)$
100	179	$x^8 + 54x^7 + 145x^6 + 5x^5 + 85x^4 + 169x^3 + 9x^2 + 102x + 83$
	41	$(x + 1)(x + 6)(x + 8)(x + 31)(x + 36)(x + 38)(x^2 + 17x + 27)$
	107	$(x + 51)(x^7 + 21x^6 + 41x^5 + 50x^4 + 72x^3 + 103x^2 + 62x + 25)$
102	109	$x^8 + 58x^7 + 98x^6 + 83x^5 + 64x^4 + 39x^3 + 21x^2 + 42x + 10$
	37	$(x + 5)(x + 7)(x + 13)(x + 23)(x + 27)(x + 33)(x^2 + 21x + 32)$
	107	$(x + 39)(x^7 + 59x^6 + 97x^5 + 36x^4 + 83x^3 + 36x^2 + 78x + 17)$
104	127	$x^8 + 41x^7 + 86x^6 + 70x^5 + 9x^4 + 66x^3 + 2x^2 + 64x + 107$
	37	$(x + 9)(x + 10)(x + 14)(x + 23)(x + 24)(x + 26)(x^2 + 5x + 17)$
	107	$(x + 50)(x^7 + 45x^6 + 83x^5 + 90x^4 + 50x^3 + 74x^2 + 63x + 14)$
106	151	$x^8 + 142x^7 + 138x^6 + 98x^5 + 122x^4 + 135x^3 + 87x^2 + 2x + 141$
	41	$(x + 1)(x + 2)(x + 4)(x + 7)(x + 23)(x + 29)(x^2 + 13x + 6)$
	113	$(x + 26)(x^7 + 73x^6 + 34x^5 + 7x^4 + 59x^3 + 65x^2 + 66x + 70)$
108	223	$x^9 + 106x^8 + 194x^7 + 210x^6 + 80x^5 + 114x^4 + 123x^3 + 190x^2 + 8x + 96$
	29	$(x + 1)(x + 3)(x + 8)(x + 19)(x + 22)(x + 25)(x + 27)(x^2 + 22x + 15)$
	127	$x(x^8 + 51x^7 + 24x^6 + 69x^5 + 125x^4 + 102x^3 + 112x^2 + 39x + 19)$
110	127	$x^8 + 110x^7 + 91x^6 + 66x^5 + 125x^4 + 34x^3 + 7x^2 + 67x + 40$
	29	$(x + 6)(x + 7)(x + 15)(x + 16)(x + 19)(x + 21)(x^2 + 15x + 2)$
	137	$(x + 96)(x^7 + 59x^6 + 136x^5 + 91x^4 + 89x^3 + 40x^2 + 33x + 84)$
112	127	$x^9 + 45x^8 + 27x^7 + 121x^6 + 47x^5 + 104x^4 + 108x^3 + 60x^2 + 89x + 37$
	23	$(x + 1)(x + 4)(x + 7)(x + 9)(x + 15)(x + 16)(x + 17)(x^2 + x + 22)$
	137	$(x + 87)(x^8 + 3x^7 + 110x^6 + 61x^5 + 17x^4 + 128x^3 + 75x^2 + 4x + 116)$
114	137	$x^9 + 33x^8 + 38x^7 + 86x^6 + 7x^5 + 82x^4 + 94x^3 + 60x^2 + 29x + 21$
	47	$(x + 6)(x + 28)(x + 29)(x + 39)(x + 40)(x + 42)(x + 44)(x^2 + x + 33)$
	199	$(x + 134)(x^8 + 172x^7 + 144x^6 + 11x^5 + 110x^4 + 37x^3 + 58x^2 + 20x + 59)$
116	263	$x^9 + 246x^8 + 70x^7 + 260x^6 + 14x^5 + 40x^4 + 90x^3 + 118x^2 + 68x + 194$
	53	$(x + 3)(x + 14)(x + 24)(x + 34)(x^2 + 48x + 51)(x^3 + 7x^2 + 29x + 49)$
	139	$(x + 50)(x^8 + 60x^7 + 31x^6 + 28x^5 + 48x^4 + 129x^3 + 69x^2 + 94x + 12)$
118	163	$x^9 + 72x^8 + x^7 + 68x^6 + 143x^5 + 117x^4 + 115x^3 + 60x^2 + 17x + 63$
	31	$(x + 3)(x + 7)(x + 8)(x + 10)(x + 12)(x + 26)(x + 27)(x^2 + 3x + 7)$
	109	$(x + 69)(x^8 + 24x^7 + 30x^6 + 29x^5 + 4x^4 + 79x^3 + 15x^2 + 50x + 6)$
122	179	$x^9 + 61x^8 + 80x^7 + 146x^6 + 163x^5 + 107x^4 + 154x^3 + x^2 + 51x + 27$
	37	$(x + 4)(x + 9)(x + 11)(x + 14)(x + 20)(x + 27)(x + 29)(x^2 + 7x + 20)$
	173	$x(x^8 + 87x^7 + 56x^6 + 121x^5 + 18x^4 + 17x^3 + 7x^2 + 83x + 11)$

References

- [BR] D. Blasius and J.D. Rogawski, *Motives for Hilbert modular forms*, Inventiones Math., **114** (1993), 55-87.
- [Bu] K. Buzzard, *On the eigenvalues of the Hecke operator T_2* , J. Number Theory, **57** (1996), 130-132.
- [C] H. Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local compact*, Contemporary Math., **165** (1994), 213-237.
- [Cl] L. Clozel, *Sur la théorie de Wiles et le changement de base nonabélien*, IMRN No. 9, 1995.
- [DHI] K. Doi, H. Hida and H. Ishii, *Discriminants of Hecke fields and the twisted adjoint L -values for $GL(2)$* , to appear in Inventiones Math.
- [DN] K. Doi and H. Naganuma, *On the functional equation of certain Dirichlet series*, Inventiones Math., **9** (1969), 1-14.
- [E] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Inventiones Math., **109** (1992), 563-594.
- [F] K. Fujiwara, *Deformation rings and Hecke algebras in the totally real case*, preprint, 1996.
- [H86] H. Hida, *Galois representations into $GL_2(\mathbb{Z}_p[[X]])$ attached to ordinary cusp forms*, Inventiones Math., **85** (1986), 545-613.
- [H88] ———, *On p -adic Hecke algebras for GL_2 over totally real fields*, Ann. of Math., **128** (1988), 295-384.
- [H89a] ———, *On nearly ordinary Hecke algebras for $GL(2)$ over totally real fields*, Adv. Studies in Pure Math., **17** (1989), 139-169.
- [H89b] ———, *Nearly ordinary Hecke algebras and Galois representations of several variables*, Proc. JAMI Inaugural Conference, Supplement to Amer. J. Math., (1989), 115-134.
- [H89c] ———, *Theory of p -adic Hecke algebras and Galois representations*, Sugaku Expositions, **2** (1989), 75-102.
- [H93] ———, *p -Ordinary cohomology groups for $SL(2)$ over number fields*, Duke Math. J., **69** (1993), 259-314.
- [H] ———, *Elementary Theory of L -functions and Eisenstein series*, LMSST **26**, Cambridge University Press, 1993.
- [H96a] ———, *On Selmer groups of adjoint modular Galois representations*, Number Theory, Paris, 1993-94, LMS Lecture notes series, **235** (1996), 89-132.
- [H96b] ———, *Hecke algebras, Selmer groups and base change*, Number Theory, Paris, 1994-95, LMS Lecture notes series, 1997.
- [H97] ———, *Global quadratic units and Hecke algebras*, preprint, 1997.
- [J] N. Jochnowitz, *A study of the local components of the Hecke algebra mod ℓ* , Trans. Amer. Math. Soc., **270** (1982), 253-267.
- [L] R.P. Langlands, *Base change for $GL(2)$* , Annals of Math. Studies, **96**, Princeton University Press, 1980.
- [LH] H.-C. Lee and W.-H. Hung, *Galois groups of Hecke eigenforms*, Chinese J. Math., **23** (1995), 329-342.
- [M] B. Mazur, *Deforming Galois representations*, Publ. MSRI, **16** (1989), 385-437.

- [MT] B. Mazur and J. Tilouine, *Représentations Galoisiennes, différentielles de Kähler et “conjectures principales”*, Publ. IHES, **71** (1990), 65-103.
- [Mi] T. Miyake, *Modular Forms*, Springer, 1989.
- [N] H. Naganuma, *On the coincidence of two Dirichlet series associated with cusp forms of Hecke’s “Neben”-type and Hilbert modular forms over a real quadratic field*, J. Math. Soc. Japan, **25** (1973), 547-555.
- [Se] J.-P. Serre, *Formes modulaires et fonctions zêta p -adiques*, Lecture notes in Math., **350** (1973), 191-268.
- [Se1] ———, *Modular forms of weight one and Galois representations*, in “Algebraic number fields” edited by A. Fröhlich, Academic Press, (1977), 193-268.
- [Se2] ———, *Congruences et formes modulaires (d’après H.P.F. Swinnerton-Dyer)*, Séminaire Bourbaki, 1971/72.
- [Sh] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Iwanami-Shoten and Princeton University Press, 1971.
- [Sh1] ———, *Class fields over real quadratic fields and Hecke operators*, Ann of Math., **95** (1972), 130-190.
- [Ta] R. Taylor, *On Galois representations associated to Hilbert modular forms*, Inventiones Math., **8** (1989), 265-280.
- [TW] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Ann. of Math., **142** (1995), 553-572.
- [Ti] J. Tilouine, *Deformation of Galois representations and Hecke algebras*, Publ. Mehta Res. Inst., Narosa Publ., New Delhi, India, 1996.
- [W] A. Wiles, *Modular elliptic curves and Fermat’s last theorem*, Ann. of Math., **142** (1995), 443-551.

UCLA
LOS ANGELES, CA 90095-1555
E-mail address: hida@math.ucla.edu

AND

HOKKAIDO UNIVERSITY
SAPPORO 060, JAPAN
E-mail address: maeda@math.hokudai.ac.jp