Extending Local Representations to Global Representations

Chandrashekhar Khare & Dipendra Prasad

1. Introduction.

It is a theorem of Deligne (and Deligne-Serre for weight 1) that for a cuspidal eigenform of the Hecke operators on the upper half plane which is of weight k, the eigenvalues of the Hecke operators T_p are algebraic integers a_p with $|a_p| \leq 2p^{(k-1)/2}$. In §2 of this note we pose a converse question to this, and analyse to what extent CM forms can be used to answer it. In §3 an analogous question is asked in the setting of Galois representations which can be thought of as the non-abelian analogue of the Grunwald-Wang theorem in Class Field Theory, and we answer it in one simple case. We may view these questions as asking for a kind of Chinese Remainder Theorem in the setting of automorphic and Galois representations respectively. In §4 we use the cohomology of modular curves to construct automorphic representations of $PGL_2(\mathbb{Q})$ with given local component at p and unramified outside p.

2. Chinese remainder theorem for automorphic representations

The aim of this section is to pose the following question and provide an answer to it in some very particular cases.

Question 1. Suppose that we are given finitely many primes $p_1, \cdots, p_r$, and algebraic integers α_i for every $i, 1 \leq i \leq r$, which have the property that $\sigma(\alpha_i)\overline{\sigma(\alpha_i)} = {p_i}^{k-1}$ for some integer $k \geq 1$ and for every embedding $\sigma : \overline{\mathbb{Q}} \to \mathbb{C}$. Then does there exist a cusp form f of weight k which is an eigenform of all the Hecke operators such that the Euler factor at p_i of the L-series of f, for every i, $1 \leq i \leq r$, is

$$L_{p_i}(f,s) = \frac{1}{(1-\frac{\alpha_i}{{p_i}^s})(1-\frac{\bar{\alpha}_i}{{p_i}^s})}?$$

The recent work of Wiles on the Taniyama-Weil conjecture, cf. [W], and its subsequent refinement by Diamond, cf. [D], proves that all elliptic curves defined over $\mathbb{Q}$ which are semi-stable at 3 and 5 are modular. Using this one may easily answer the above question in a particular case. We state this as the following proposition.

Proposition 1. *If $p_1, \cdots, p_r$ is a finite number of primes and if for each $1 \leq i \leq r$ we are given a rational integer a_i such that $|a_i| \leq 2{p_i}^{1/2}$ then there exists a newform f of weight 2 and of level prime to the primes p_i (for $1 \leq i \leq r$) such that the eigenvalue of the ${p_i}^{\text{th}}$ Hecke operator T_{p_i} acting on f is a_i (for $1 \leq i \leq r$). In fact one may choose f to have rational q-expansion and there exist infinitely many such distinct newforms.*

Proof. The main ingredient is the result of Wiles and Diamond that we have cited above. Namely by the theorem of Honda and Tate we construct elliptic curves E_i over the finite fields $\mathbb{F}_{p_i}$ with p_i elements such that the cardinality of $E_i(\mathbb{F}_{p_i})$ is $1 + p_i - a_i$. We further freely pick elliptic curves E_α defined over $\mathbb{F}_3$ (respectively E_β over $\mathbb{F}_5$) with the only restriction being that if 3 (respectively 5) is one of the primes p_i above, then the elliptic curve E_α (respectively E_β) is the same as the elliptic curve which has been selected over $\mathbb{F}_3$ (respectively over $\mathbb{F}_5$) in the earlier line. Let E be any elliptic curve whose reduction modulo p_i is the elliptic curve E_i for every i, $1 \leq i \leq r$, and whose reduction at 3 and 5 is E_α and E_β respectively (such a E exists by an application of the Chinese Remainder Theorem). As E has good reduction at 3 and 5 by construction, the work of Wiles and Diamond implies that E is modular. Then the L-function of E is the Mellin transform of a desired newform. The last line is easily seen to be a consequence of the construction in this proof.

When $k = 2$ but a_i are not integers, we can't imitate the above proof even assuming the generalised form of the Taniyama-Weil conjecture according to which abelian varieties with real multiplication over $\mathbb{Q}$ also arise as factors of the Jacobians of the modular curves $X_0(N)$. The problem being that it is not clear if we can lift an abelian variety with real multiplication over the finite field $\mathbb{F}_{p_i}$ to one over $\mathbb{Q}$. There is then the problem of doing this for finitely many primes $p_1, \cdots, p_r$ simultaneously. We, however, don't even know if an abelian variety over $\mathbb{F}_p$ can be lifted to one over $\mathbb{Q}$!

We now analyse to what extent CM forms can be used to answer the question. Here is the main result. All the numbers α_i appearing in the theorem below will have the property that $\sigma(\alpha_i)\overline{\sigma(\alpha_i)} = {p_i}^{k-1}$ for some integer $k \geq 2$ and for every embedding $\sigma : \overline{\mathbb{Q}} \to \mathbb{C}$.

Theorem 1. *Assume that $a_i = \alpha_i + \overline{\alpha}_i$ is an integer such that p_i does not divide a_i for any i, $1 \leq i \leq r$. Then there is a CM cuspidal eigenform f such that the Euler factor at p_i of the L-series of f is*

$$L_{p_i}(f,s) = \frac{1}{(1 - \frac{\alpha_i}{{p_i}^s})(1 - \frac{\overline{\alpha}_i}{{p_i}^s})}$$

if and only if the quadratic imaginary fields $K_i = \mathbb{Q}(\sqrt{a_i^2 - 4p_i^{k-1}})$ are independent of i.

Proof. We first recall that a CM modular form $f = f_\lambda$ is associated to a Größencharakter λ of a quadratic imaginary extension K of $\mathbb{Q}$. This Größencharakter λ can be thought of as a homomorphism $\lambda : I_K(c) \to \mathbb{C}^*$ (where $I_K(c)$ is the group of fractional ideals prime to c where c is an ideal of K) such that for any $\alpha \epsilon \mathcal{O}_K$ with $\alpha \equiv 1 \pmod{c}$, where $\mathcal{O}_K$ is the ring of integers of K, $\lambda((\alpha)) = \alpha^a \overline{\alpha}^b$ for some integers a, b. As f_λ is a modular form, one moreover has $a \geq 0$, $b \geq 0$, and $ab = 0$. This follows for instance by comparing the Euler factor at infinity associated to the Größencharakter λ and to a modular form.

The modular form f_λ is an eigenform of the Hecke operators and has the following Euler factor at primes p coprime to c:

$$L_p(f_\lambda, s) = \begin{cases} \frac{1}{(1-\lambda(\pi)p^{-s})}\frac{1}{(1-\lambda(\overline{\pi})p^{-s})}, & \text{if } (p) = \pi\overline{\pi} \\ \frac{1}{(1-\lambda(p)p^{-2s})}, & \text{if } (p) \text{ is inert} \\ \frac{1}{1-\lambda(\pi)p^{-s}}, & \text{if } (p) = \pi^2. \end{cases}$$

We now assume that the quadratic imaginary fields $K_i = \mathbb{Q}(\sqrt{a_i^2 - 4p_i^{k-1}})$ are all the same, say K, and in that case we construct a Größencharakter λ of K such that the associated modular form f_λ has the desired Euler factors at p_i, $1 \leq i \leq r$. We first note that as $k \geq 2$ and $p_i \not| a_i$, the prime ideal (p_i) splits in the quadratic imaginary field $K = K_i = \mathbb{Q}(\sqrt{a_i^2 - 4p_i^{k-1}})$ (as one can take the square root of $a_i^2 - 4p_i^{k-1}$ in $\mathbb{Q}_{p_i}$). Let $(p_i) = \pi_i\overline{\pi}_i$ be the factorisation of the ideal (p_i) in K as the product of prime ideals in K. Since $\alpha_i\overline{\alpha}_i = p_i^{k-1}$, and $\pi_i\overline{\pi}_i = (p_i)$, it follows from the assumption $p_i \not| a_i$ (possibly after replacing α_i by $\overline{\alpha}_i$) that $(\alpha_i) = \pi_i^{k-1}$, $(\overline{\alpha}_i) = \overline{\pi}_i^{k-1}$.

Let P_c denote the group of principal ideals (x) with $x \equiv 1 \pmod{c}$. Denote by μ_{00} the character on P_c given by $\mu_{00}((x)) = x^{k-1}$. (This is well defined for c large enough as the group of units of K is finite; moreover, c can be taken to be coprime to any given ideal which we take to be $\prod(p_i)$.) Let μ_0 be any extension of μ_{00} to $I(c)$. Our problem of the construction of λ will be solved as soon as we can demonstrate the existence of a Größencharakter λ which is unramified at π_i and $\overline{\pi}_i$ for all i, $1 \leq i \leq r$, with $\lambda(\pi_i) = \alpha_i$, and $\lambda(\overline{\pi}_i) = \overline{\alpha}_i$ and whose infinity type is either $(a, 0)$ or $(0, a)$ for some integer $a \geq 1$. From the relation $(\alpha_i) = \pi_i^{k-1}$, it follows that for the desired λ, $\lambda/\mu_0(\pi_i)$ and $\lambda/\mu_0(\overline{\pi}_i)$ must be roots of unity, say ω_i, ω_i'. Conversely if we can construct a Größencharakter ν which is unramified at π_i and $\overline{\pi}_i$ for all i, $1 \leq i \leq r$, with $\nu(\pi_i) = \omega_i$, and $\nu(\overline{\pi}_i) = \omega_i'$, then $\lambda = \nu\mu_0$ will be the desired Größencharakter. The existence of such a Größencharakter ν is a consequence of the theorem of Grunwald and Wang, cf. [A-T], completing this part of the theorem.

To prove that the fields K_i must be the same for the existence of a CM form f, it suffices to prove the following lemma.

Lemma 1. *Let f be a CM form such that the Euler factor at p of the L-series of f is $[1 - a_p p^{-s} + p^{k-1-2s}]^{-1}$. Assume that a_p is an integer with $p \not| a_p$. Then f arises from a Größencharakter on the quadratic imaginary field $K = \mathbb{Q}(\sqrt{a_p^2 - 4p^{k-1}})$.*

Proof. Suppose that f arises from a Größencharakter λ on a quadratic imaginary field L. Looking at the Euler factor at p attached to the L-series of f, we find that p must split in L. Write the factorisation of (p) in L as $(p) = \pi\overline{\pi}$. Since the Euler factor at p of the L-series of f is $[1 - a_p p^{-s} + p^{k-1-2s}]^{-1}$, it follows that $\lambda(\pi) + \lambda(\overline{\pi}) = a_p$, and $\lambda(\pi)\lambda(\overline{\pi}) = p^{k-1}$. Therefore $\lambda(\pi)$ and $\lambda(\overline{\pi})$ lie in K. From the defining condition of a Größencharakter, it follows that there is an integer $h \geq 1$ such that $\lambda(\pi)^h \in L$. It can be checked that a power of $x + \sqrt{y}$ with x, y rational, $y \leq 0$, and $xy \neq 0$, is rational only if $x + \sqrt{y}$ is a rational multiple of the third root of unity w. It follows that $\lambda(\pi)^h$ is an element of K but not of $\mathbb{Q}$ if p does not divide a_p (we are using the condition $k \geq 2$ here). As $\lambda(\pi)^h$ lies in L, $K = L$.

The case when a_p is a non-zero integer but $p|a_p$ can't be obtained by CM forms as the next lemma shows. As the case when $a_p = 0$ can be obtained by any Größencharakter of any quadratic imaginary field in which (p) is inert, this completes all the cases in which CM forms can be used.

Lemma 2. *Let f be a CM form such that the Euler factor at p of the L-series of f is $[1 - a_p p^{-s} + p^{k-1-2s}]^{-1}$. Assume that a_p is a non-zero integer. Then p does not divide a_p.*

Proof. Suppose that f arises from a Größencharakter λ on a quadratic imaginary field L. Looking at the Euler factor at p attached to the L-series of f, we find that p must split in L. Write the factorisation of (p) in L as $(p) = \pi\overline{\pi}$. Since the Euler factor at p of the L-series of f is $[1 - a_p p^{-s} + p^{k-1-2s}]^{-1}$, it follows that $\lambda(\pi) + \lambda(\overline{\pi}) = a_p$, and $\lambda(\pi)\lambda(\overline{\pi}) = p^{k-1}$. If $p|a_p$, then for all integers $h \geq 1$, $p|\lambda(\pi^h) + \lambda(\overline{\pi}^h)$.

Assume without loss of generality that the infinity type of λ is $(a, 0)$. Then there is an integer $h \geq 1$ such that $(\pi)^h$ is a principal ideal generated by, say γ, and such that

$$\lambda(\pi^h) = \gamma^a$$

and

$$\lambda(\overline{\pi}^h) = \overline{\gamma}^a.$$

Therefore $\gamma^a + \overline{\gamma}^a$ is divisible by p which is obviously not possible.

Remark 1. The weight 1 case of Question 1 can be completely answered using CM forms. One simply has to take a quadratic imaginary field in which the prime ideals (p_i) split as $(p_i) = \pi_i \overline{\pi}_i$ and construct a finite order Größencharakter λ on L using the Grunwald-Wang theorem which is unramified at the primes π_i and $\overline{\pi}_i$, and has the property that $\lambda(\pi_i) = \alpha_i$, and $\lambda(\overline{\pi}_i) = \overline{\alpha}_i$ for every i, $1 \leq i \leq r$.

Remark 2. We also remark that one can ask a question related to Question 1 which has a negative answer. So we may fix a totally real algebraic integer, say α, and a positive integer N, and a prime p which does not divide N, and then ask if there exists a cuspidal eigenform, say f, of some weight $k > 1$, for the group $\Gamma_0(N)$, such that the eigenvalue of the p th Hecke operator T_p on f is α. Then the answer is no as the part of the Gouvea-Mazur conjectures already proven by Coleman [Co], implies that the "slopes" of the eigenvalues of the Atkin operator U_p, acting on the space of cusp forms of all weights, for the group $\Gamma_0(Np)$, are discrete. Thus in particular there exists a number ε in the interval $(0, 1)$, such that there are no "slopes" in the interval $(0, \varepsilon)$. Then any α with the property that its p-adic valuation, with respect to which the slopes have been measured, is in the interval $(0, \varepsilon)$, provides a negative answer to the question. We see this, as if there is a $f \epsilon S_k(\Gamma_0(N))$, $k > 1$, which is an eigenvector for T_p, with eigenvalue α, then at least one of the roots, which we will call a and b, of the equation $x^2 - \alpha x + p^{k-1}$, say a, has valuation in the interval $(0, \varepsilon)$. But then $f'(z) = f(z) - bf(pz)$, is an element of $S_k(\Gamma_0(Np))$, which is an eigenvector for U_p, with eigenvalue a. This contradicts the choice of ε. We refer to [Co] for the precise definition of "slopes" and more about the Gouvea-Mazur conjecture.

Remark 3. There is by now a well-known result for automorphic representations, cf. Rogawski [Ro], that there are automorphic representations whose local components are pre-assigned discrete series representations at finitely many places. However, in question 1 we want to construct automorphic representations whose local components are pre-assigned unramified principal series at finitely many finite places, and a discrete series at infinity when $k \geq 2$. It is unlikely that this question can be handled by techniques of harmonic analysis alone, as it is essential to specify the data which is used to define the unramified principal series at the finitely many local places, in the situation of question 1, to be of arithmetic kind.

3. Chinese remainder theorem for Galois representations

Here is the non-abelian version of the Grunwald-Wang theorem, and is the Galois theoretic analogue of question 1 for weight 1.

Question 2. Suppose that we are given semi-simple matrices $A_1, \cdots, A_r$ in $GL(n, \mathbb{C})$ such that the eigenvalues of A_i are roots of unity. Then is there a continuous irreducible representation $\Phi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL(n, \mathbb{C})$ which is unramified at the primes p_i such that the conjugacy class of the image of the Frobenius at p_i under the representation Φ contains A_i for every i, $1 \leq i \leq r$?

Remark 4.

4.1. If we do not insist on the irreducibility of the representation Φ, then such a representation can be easily constructed by the Grunwald-Wang theorem.

4.2. The answer to question 2 is no in the generality in which it has been posed here. The reason is that even though there are semi-simple matrices, say in $GL(2, \mathbb{C})$, for which the ratio of the eigenvalues are arbitrary large roots of unity, the finite subgroups of $GL(2, \mathbb{C})$ which act irreducibly on $\mathbb{C}^2$ are much more restricted.

4.3. One should therefore consider question 2 only for those matrices $A_1, \cdots, A_r$ which belong to a finite subgroup $G \subset GL(n, \mathbb{C})$ which acts irreducibly on $\mathbb{C}^n$. However, the example of Wang, cf. [A-T], shows that one may not be able to construct a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with values in G with the above local constraints.

4.4. We can ask more generally for the existence of a representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with given restriction to the decomposition groups $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ which takes values in a finite subgroup $G \subset GL(n, \mathbb{C})$ for finitely many primes p.

At the moment we are unable to say anything about question 2, or its more general form in remark 3.4, except for the following proposition. In the following proposition, we have fixed embeddings of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$ for every prime p; we will abuse notation to include the prime at infinity also in the following proposition.

Proposition 2. *Let $G = S_n$, and suppose we are given $\rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}_{p_i}/\mathbb{Q}_{p_i}) \to G$ for $1 \leq i \leq r$. Then there exists $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to G$ such that the restriction of ρ to $\mathrm{Gal}(\overline{\mathbb{Q}}_{p_i}/\mathbb{Q}_{p_i})$ is conjugate in G to ρ_i for every i.*

Proof. Let G_i denote the image in G of $\mathrm{Gal}(\overline{\mathbb{Q}}_{p_i}/\mathbb{Q}_{p_i})$ under ρ_i. Let X be the set $X = \{1, 2, \cdots, n\}$ on which S_n, and therefore every G_i, operates. Write $X = \sqcup_\alpha X_{\alpha,i}$, a disjoint union, such that every $X_{\alpha,i}$ is invariant under G_i, and G_i operates transitively on the set $X_{\alpha,i}$. If $n_{\alpha,i}$ denotes the cardinality of $X_{\alpha,i}$, let $G_{\alpha,i}$ denote the image of G_i in the symmetric group $S_{n_{\alpha,i}}$. Therefore we have maps $\pi_{\alpha,i} : G_i \to G_{\alpha,i}$, and $\pi_i : G_i \to \prod_\alpha G_{\alpha,i}$.

Let K_i be the fixed field of the kernel of ρ_i so that K_i is a Galois extension of $\mathbb{Q}_{p_i}$ whose Galois group is canonically isomorphic to G_i. Let $K_{\alpha,i}$ denote the extension of $\mathbb{Q}_{p_i}$ contained in K_i which corresponds to the surjection $\pi_{\alpha,i} : G_i \to G_{\alpha,i}$. As $\pi_i : G_i \to \prod_\alpha G_{\alpha,i}$ is an injection, the compositum of $K_{\alpha,i}$ is K_i. Let $H_{\alpha,i} \subset G_{\alpha,i}$ denote the subgroup of $G_{\alpha,i}$ which is the stabiliser of an element (which will be arbitrarily chosen) of the set $X_{\alpha,i}$. Let $L_{\alpha,i}$ be the subfield of $K_{\alpha,i}$ fixed by $H_{\alpha,i}$. The degree of $L_{\alpha,i}$ over $\mathbb{Q}_{p_i}$ is $n_{\alpha,i}$. Let $f_{\alpha,i}$ denote an irreducible monic polynomial over $\mathbb{Q}_{p_i}$ of degree $n_{\alpha,i}$ one of whose roots generate $L_{\alpha,i}$. We assume, as we may, that the polynomials $f_{\alpha,i}$ are distinct for distinct α. Then $K_{\alpha,i}$ will be the splitting field of $f_{\alpha,i}$, and K_i will be the splitting field of the degree n polynomial $f_i = \prod_\alpha f_{\alpha,i}$ which has no multiple roots. Now let f be a polynomial over $\mathbb{Q}$ which approximates f_i well enough so that the roots of f generate the field extension K_i of $\mathbb{Q}_{p_i}$ and such that there is a matching of the roots of f with those of f_i over K_i such that the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_{p_i}/\mathbb{Q}_{p_i})$ on the roots of f and f_i is the same after this identification. This is possible by an extension of Krasner's lemma which does this when f_i is irreducible. For the general case we claim that any monic polynomial f which is near enough to f_i also has factorisation $f = \prod f_\alpha$ with $\deg f_\alpha = \deg f_{\alpha,i}$, f_α

irreducible monic and near to $f_{\alpha,i}$. For this it is enough to check that the mapping which takes the n-tuple consisting of the coefficients of f_α to the n-tuple consisting of the coefficients of f is an open mapping. Because of the open mapping theorem for $\mathbb{Q}_p^n$, it suffices to prove that the jacobian of such a mapping is non-zero at the point defined by $f_{\alpha,i}$. This is a simple consequence of the well-known fact that the mapping $(x_1, \cdots, x_n) \rightarrow (s_1, \cdots, s_n)$ where s_i is the i-th elementary symmetric function has non-zero jacobian at any point $(x_1, \cdots, x_n)$ with $x_l \neq x_k$ if $l \neq k$. This completes the proof of the claim from which we deduce that the roots of f_i and f generate the same field. Now using the roots of the degree n equation f, we get the desired map $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow S_n$ whose restriction to $\mathrm{Gal}(\overline{\mathbb{Q}}_{p_i}/\mathbb{Q}_{p_i})$ is conjugate in S_n to ρ_i for every i.

Remark 5. We don't know if the Proposition above is true even for $G = A_n$.

Remark 6. The problem of extending local representations to a global one is much subtler than the problem of constructing extensions of global fields with given local extensions. This is evident even in the case of a global cyclic extension in which case when the local field extension is unramified extension of the same degree, the local representation will be the additional data specifying which generator of the cyclic group the Frobenius corresponds to.

4. Cohomology of modular curves

In this section we use the cohomology of modular curves to find cuspidal automorphic representations of $PGL(2)$ over $\mathbb{Q}$ which are holomorphic discrete series of weight 2, are ramified only at the prime p, and have a fixed vector for the congruence subgroup $\Gamma(p)$. A similar treatment can be made for higher weight and higher ramification.

We begin by recalling the representation theory of $SL(2, \mathbb{F}_p)$. The principal series representations $Ps(\chi)$ of $SL(2, \mathbb{F}_p)$ are parametrized by non-trivial characters $\chi : \mathbb{F}_p^* \rightarrow \mathbb{C}^*$. We have $Ps(\chi_1) = Ps(\chi_2)$ if and only if $\chi_1 = \chi_2$, or $\chi_1 = \chi_2^{-1}$. If

$\chi \neq 1$, but $\chi^2 = 1$, then the principal series representation $Ps(\chi)$ splits into two irreducible representations P^+ and P^- of dimensions $(p+1)/2$. The discrete series representations $Ds(\chi)$ of $SL(2, \mathbb{F}_p)$ are parametrized by non-trivial characters χ of N, the norm one subgroup of $\mathbb{F}_{p^2}^*$, $\chi : N \to \mathbb{C}^*$. We have $Ds(\chi_1) = Ds(\chi_2)$ if and only if $\chi_1 = \chi_2$, or $\chi_1 = \chi_2^{-1}$. If $\chi \neq 1$, but $\chi^2 = 1$, then the discrete series representation $Ds(\chi)$ splits into two irreducible representations D^+ and D^- of dimensions $(p-1)/2$. Besides the representations listed above, there is the trivial representation and the Steinberg.

The following lemma about action of finite groups on algebraic curves can be proved using a triangulation of the curve compatible with the group action. We will not give details of the simple proof.

Lemma 3. Let G be a finite group acting faithfully on an algebraic curve X. Let $Y = X/G$ be the quotient curve. Let $\chi(X) = 2 - H^1(X, \mathbb{C})$ be the Euler characteristic of X thought of as an element of the Grothendieck group of representations of G. For any subgroup H of G, let $r(G/H)$ denote the representation of G on functions on G/H; let $r(G)$ denote the regular representation of G. Let $\chi(Y) = 2 - H^1(Y)$ denote a virtual vector space with trivial G action. Then we have

$$\chi(X) = r(G) \otimes \chi(Y) - \sum_H [r(G) - r(G/H)]$$

where the subgroups H in the summation above are the stabilisers of the fixed points of the action of G on X, taking only one stabiliser out of a G-orbit of fixed points.

We will apply this lemma in the case when $X = X(p)$ is the compactification of $\mathbb{H}/\Gamma(p)$ on which $G = SL(2, \mathbb{F}_p)/\pm 1$ acts faithfully. In this case $Y = \mathbb{P}^1$, and the only points of $\mathbb{P}^1$ above which the action of G on $X(p)$ has fixed points correspond to the points i, ω, ∞ on the extended upper-half plane. The stabiliser of i is the subgroup $H(i)$ generated by

$$s(i) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

the stabiliser of ω is the subgroup $H(\omega)$ generated by

$$s(\omega) = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},$$

and the stabiliser of ∞ is the subgroup $H(\infty)$ generated by

$$s(\infty) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

As,

$$r(G/H) = \sum_V \dim(V^H)V,$$

the calculation of $\dim(V^H)$ for irreducible representations V of G will give the representation $r(G/H)$. This can be obtained from the character table of $SL(2,\mathbb{F}_p)$. The results depend on the congruence of p modulo 12, as the condition for the elements i and ω to be diagonalisable in $SL(2,\mathbb{F}_p)$ depends on this congruence.

We state the results only for $p \equiv \pm 1 \bmod 12$.

Proposition 3. *If* $p \equiv -1 \pmod{12}$, *then*

$$H^1(X,\mathbb{C}) = \frac{p-11}{6}\sum_\chi Ps(\chi) + \frac{p-11}{6}\sum_\chi Ds(\chi) + 2\sum_{\chi(i)=1} Ds(\chi) + 2\sum_{\chi(\omega)=1} Ds(\chi)$$

$$+\frac{p+1}{6}St - \frac{p-11}{12}(P^+ + P^-) - \frac{p+1+12a}{12}(D^+ + D^-)$$

Here the summation is over only those χ which give rise to distinct $Ps(\chi)$ (or, $Ds(\chi)$); $a = 1$ if the unique quadratic character of N takes the value 1 on i, and $a = 0$ otherwise, so $a = 1$ if $p \equiv -1 \bmod 24$ and zero otherwise.

Proposition 4. *If* $p \equiv 1 \pmod{12}$, *then*

$$H^1(X,\mathbb{C}) = \frac{p-1}{6}\sum_\chi Ps(\chi) + \frac{p-1}{6}\sum_\chi Ds(\chi) - 2\sum_{\chi(-1)=1} Ps(\chi) - 2\sum_{\chi(\omega)=1} Ps(\chi)$$

$$+\frac{p-13}{6}St - \frac{p-25}{12}(P^+ + P^-) - \frac{p-1}{12}(D^+ + D^-),$$

where again the summation is over only those χ which give rise to distinct $Ps(\chi)$ (or, $Ds(\chi)$).

Remark 7. All the representations of $SL(2,\mathbb{F}_p)$ have their characters defined over $\mathbb{R}$ except for P^+, P^-, D^+, D^- in the case when $p \equiv 3 \bmod 4$. Since $H^1(X(p),\mathbb{C}) = H^0(X(p),\Omega^1) \oplus \overline{H^0(X(p),\Omega^1)}$, knowing the $SL(2,\mathbb{F}_p)/\pm 1$ module structure of $H^1(X(p),\mathbb{C})$ lets us deduce the $SL(2,\mathbb{F}_p)/\pm 1$ module structure of $H^0(X(p),\Omega^1)$ except that we will be able to determine only the sum of multiplicities of P^+, P^-, and the sum of multiplicities of D^+, D^-. See Casselman [Ca, page 122] for the decomposition of $H^0(X(p),\Omega^1)$ in the case $p = 11$ which is in accordance with our Proposition 3.

Let $X(p)^e = X(p) \times_{SL(2,\mathbb{F}_p)} PGL(2,\mathbb{F}_p)$. Clearly, $X(p)^e$ is a disjoint union of two copies of $X(p)$, and the representation of $PGL(2,\mathbb{F}_p)$ on $H^0(X(p)^e,\Omega^1)$ or on $H^1(X(p)^e,\mathbb{C})$ is the induction from $SL(2,\mathbb{F}_p)/\pm 1$ to $PGL(2,\mathbb{F}_p)$ of $SL(2,\mathbb{F}_p)/\pm 1$ module $H^0(X(p),\Omega^1)$ or $H^1(X(p),\mathbb{C})$. This allows us to calculate $H^0(X^e,\Omega^1)$ as $PGL(2,\mathbb{F}_p)$ module from the results obtained above. The results obtained above can be summarised in the following theorem.

Theorem 2. *For $p \geq 23$, the representations of the adele group $PGL(2,\mathbb{A})$ appearing in the discrete spectrum of $L^2(PGL(2,\mathbb{Q})\backslash PGL(2,\mathbb{A}))$ with the discrete series D_2 at the infinite place, unramified outside p, and at p having a vector invariant under $\Gamma(p)$ are finitely many, and their local components at p is any possible representation of $PGL(2,\mathbb{Q}_p)$ with a vector invariant under $\Gamma(p)$ except that in the principal series case, the inducing character may have to be altered by an unramified character.*

References.

[A-T] E. Artin, J. Tate, *Class Field Theory*, Benjamin, Reading, Mass. 1974.

[Ca] W. Casselman, On Representations of GL(2) and Arithmetic of Modular Curves, Springer Lecture Notes in Mathematics, vol 349, editors: P. Deligne and W. Kuijk.

[Co] R. Coleman, *p-adic Banach spaces*, preprint.

[D] F. Diamond, *On deformation rings and Hecke rings*, preprint.

[Mi] T. Miyake, *Modular forms*, Springer-Verlag, 1989.

[Ro] J. Rogawski, *Representations of GL(n) and division algebras over p-adic fields*, Duke Math. J. 50 (1983), 161-196.

[W] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Mathematics (1995).

CK: Tata Institute, Colaba, Bombay 400 005, INDIA e-mail : khare@tifrvax.tifr.res.in

DP: Mehta Research Insitute, Allahabad, 211002, INDIA

and

Tata Institute, Colaba, Bombay, 400005, INDIA e-mail : dprasad@mri.ernet.in