AN INTRODUCTION TO CONGRUENCES BETWEEN MODULAR FORMS

EKNATH GHATE

The purpose of this note is to introduce the reader to some of the basic concepts in the theory of congruences between modular forms. Our exposition here has been distilled from various sources. We have especially benefited from reading the papers of Hida and Ribet some of which are listed in the references.

1. Congruence primes

Let S be a space of elliptic cusp forms of fixed level and weight. Let K denote a number field and let $\mathcal{O}$ be the ring of integers of K. Let $S(\mathcal{O})$ respectively $S(K)$ denote the space of cusp forms whose Fourier coefficients lie in $\mathcal{O}$ respectively K. Note that $S(\mathcal{O})$ is a lattice in $S(K)$ and for simplicity we shall denote it by M.

Definition 1. *Let $f = \sum c(n,f)q^n$ and $g = \sum c(n,g)q^n$ be elements of $M = S(\mathcal{O})$, and let $\wp \subset \mathcal{O}$ be a prime ideal. We say that f and g are congruent modulo $\wp$, and write $f \equiv g \bmod \wp$, if*

$$c(n,f) \equiv c(n,g) \bmod \wp$$

for each $n = 1, 2, \ldots$.

Now suppose that we can decompose

$$S(K) = X \oplus Y \tag{1}$$

into a direct sum. Then we have projection maps $\pi_X : S(K) \to X$ and $\pi_Y : S(K) \to Y$. Let us set

$$\begin{aligned} M_X &= M \cap X, & M^X &= \pi_X(M), \\ M_Y &= M \cap Y, & M^Y &= \pi_Y(M). \end{aligned}$$

Note that $M_X \subset M^X \subset X$ are lattices in X and that $M_Y \subset M^Y \subset Y$ are lattices in Y. We have the following chain of inclusions of lattices in $S(K)$

$$M_X \oplus M_Y \subset M \subset M^X \oplus M^Y.$$

Date: July 3, 2003.

1991 *Mathematics Subject Classification.* Primary: 11F33, Secondary: 11F67.

Key words and phrases. Modular forms, congruences, Hecke algebras.

Definition 2. *Call*

$$C(M) = \frac{M^X \oplus M^Y}{M}$$

the congruence module of the lattice M with respect to the decomposition (1) *above.*

Lemma 1. *We have*

- $$C(M) \cong \frac{M}{M_X \oplus M_Y},$$
- *The maps π_X and π_Y induce isomorphisms*

$$\tfrac{M^X}{M_X} \xleftarrow[\pi_X]{\sim} \tfrac{M}{M_X \oplus M_Y} \xrightarrow[\pi_Y]{\sim} \tfrac{M^Y}{M_Y}.$$

Proof. The proof is easy. □

Lemma 1 can be used to explain why $C(M)$ is called a congruence module. Choose a prime $\wp \subset \mathcal{O}$ in the support of $C(M)$. Say the residue characteristic of $\wp$ is p. Then $C(M)$ contains an element of order p. By Lemma 1 we may pick a non-zero element $h \in M$ whose class

$$\overline{h} \in \frac{M}{M_X \oplus M_Y}$$

has order p. Concretely this means that there exist $f \in M_X$ and $g \in M_Y$ such that

$$ph = f - g.$$

Clearly this means that f and g are congruent modulo $\wp$. Conversely, say that there is a congruence between $f \in X$ and $g \in Y$ mod $\wp$. Working the above argument backwards we see that $\wp$ is in the support of $C(M)$.

2. Hecke algebras and primes of fusion

Let us now introduce the Hecke algebra $\mathbb{T} \subset \mathrm{End}_{\mathcal{O}}(S)$ generated by all the Hecke operators T_n. Then $\mathbb{T}$ preserves the lattice M. Moreover $\mathbb{T}$ is free of finite type as an $\mathcal{O}$ module and thus is an integral extension of $\mathcal{O}$. Thus $\mathbb{T}$ has Krull dimension one. The following key fact tells us that the rank of $\mathbb{T}$ as an $\mathcal{O}$-module is $\mathrm{rank}_{\mathcal{O}}(M) = \dim_K S(K)$.

Lemma 2. *The pairing*

$$\begin{array}{ccc} \mathbb{T} \times M & \longrightarrow & \mathcal{O} \\ (T, f) & \mapsto & c(1, Tf) \end{array}$$

induces an isomorphism $M \cong \mathrm{Hom}_{\mathcal{O}}(\mathbb{T}, \mathcal{O})$*.*

Proof. The pairing is clearly $\mathcal{O}$-bilinear. It therefore induces two maps $M \to \mathrm{Hom}_{\mathcal{O}}(\mathbb{T}, \mathcal{O})$ and $\mathbb{T} \to \mathrm{Hom}_{\mathcal{O}}(M, \mathcal{O})$.

We claim that these maps are injective. We will need the following fact which follows from the explicit formula for the action of the n^{th} Hecke operator on q-expansions: $c(n, g) = c(1, T_n g)$ for $g \in M$. Now suppose that $(T, f) = 0$ for all $T \in \mathbb{T}$. Then $c(n, f) = c(1, T_n f) = (T_n, f) = 0$ for all n. Thus $f = 0$ and the first map is injective. For the second map suppose that $(T, f) = 0$ for all $f \in M$. Then

$$c(n, Tf) = c(1, T_n T f) = c(1, T T_n f) = (T, T_n f) = 0$$

for all n. So $Tf = 0$ for all $f \in M$. Thus $T = 0$ proving that the second map is injective.

We now prove the surjectivity of the first map. Before doing this we remark that if we extend scalars to K then the two maps above are automatically isomorphisms since both $\mathbb{T} \otimes K$ and $M \otimes K = S(K)$ have finite dimension over K. Now suppose that ϕ is an $\mathcal{O}$-linear form on $\mathbb{T}$. Then we may think of ϕ as a K-linear form on $\mathbb{T} \otimes K$ by extending scalars. By the remark we just made there is an element f, a priori in $S(K)$, such that $\phi(T) = (T, f)$ for all $T \in \mathbb{T} \otimes K$. Taking $T = T_n \in \mathbb{T}$ we see that $\phi(T_n) = c(n, f) \in \mathcal{O}$. In particular $f \in S(\mathcal{O}) = M$ proving the surjectivity. □

Let us now assume that the decomposition (1) is preserved by all the Hecke operators T_n. Write $\mathbb{T}^X$ respectively $\mathbb{T}^Y$ for the image of $\mathbb{T}$ in $\mathrm{End}_{\mathcal{O}}(X)$ respectively $\mathrm{End}_{\mathcal{O}}(Y)$. There is a natural inclusion

$$\begin{array}{rcl} \mathbb{T} & \hookrightarrow & \mathbb{T}^X \oplus \mathbb{T}^Y \\ T & \mapsto & (T|_X, T|_Y). \end{array}$$

Because of Lemma 2 the dimension of $\mathbb{T} \otimes K$ is the same as the dimension of $S(K)$. In particular the index $[\mathbb{T}^X \oplus \mathbb{T}^Y : \mathbb{T}]$ is finite. We now make the following definition.

Definition 3. *Call*

$$C(\mathbb{T}) = \frac{\mathbb{T}^X \oplus \mathbb{T}^Y}{\mathbb{T}}$$

the congruence module of the Hecke algebra $\mathbb{T}$ *with respect to the decomposition* (1) *.*

Let us explain why $C(\mathbb{T})$ is called a congruence module. We start with some general remarks. Let $\mathfrak{m}$ be a maximal ideal of $\mathbb{T}$. Let $\mathfrak{m}_X$

respectively $\mathfrak{m}_Y$ denote the images of $\mathfrak{m}$ in $\mathbb{T}^X$ respectively $\mathbb{T}^Y$. We have the following commutative diagram

$$\begin{tikzcd}
\mathbb{T}^X \arrow[d, two heads] & \mathbb{T} \arrow[l, two heads] \arrow[r, two heads] \arrow[d, two heads] & \mathbb{T}^Y \arrow[d, two heads] \\
\mathbb{T}^X/\mathfrak{m}_X & \mathbb{T}/\mathfrak{m} \arrow[l, two heads, "\sim"'] \arrow[r, two heads, "\sim"] & \mathbb{T}^Y/\mathfrak{m}_Y.
\end{tikzcd}$$

Choose minimal prime ideals $\mathfrak{q}_X \subset \mathfrak{m}_X$ and $\mathfrak{q}_Y \subset \mathfrak{m}_Y$, and let $\mathfrak{p}_X$ respectively $\mathfrak{p}_Y$ denote their pre-images under the maps $\mathbb{T} \twoheadrightarrow \mathbb{T}^X$ respectively $\mathbb{T} \twoheadrightarrow \mathbb{T}^Y$. We thus obtain two homomorphisms $\mathbb{T} \twoheadrightarrow \mathbb{T}/\mathfrak{p}_X$ and $\mathbb{T} \twoheadrightarrow \mathbb{T}/\mathfrak{p}_Y$ which modulo $\mathfrak{m}$ are the same. Let us now assume that $\mathcal{O}$ is large enough so that $\mathbb{T}/\mathfrak{p}_X$ and $\mathbb{T}/\mathfrak{p}_Y$ embed in $\mathcal{O}$. Let $\wp$ denote the maximal ideal of $\mathcal{O}$ corresponding to $\mathfrak{m}$. Then we have two algebra homomorphisms $\mathbb{T} \twoheadrightarrow \mathcal{O}$ which modulo $\wp$ are the same.

By Lemma 2 any algebra homomorphism of $\mathbb{T}$ into $\mathcal{O}$ may be identified with a cusp form in $M = S(\mathcal{O})$. Actually Lemma 2 shows that any map of $\mathcal{O}$ modules $\mathbb{T} \to \mathcal{O}$ gives rise to a cusp form; in our case since the maps are actually algebra homomorphisms the cusp forms we obtain are normalized simultaneous eigenforms. The upshot is that we have two normalized cusp forms that are simultaneous eigenforms of all the Hecke operators which are congruent modulo $\wp$.

It is not necessarily the case that these two homomorphisms are distinct so that we have a genuine congruence between cusp forms. However this is true if the maximal ideal $\mathfrak{m}$ lies in the support of $C(\mathbb{T})$. Indeed suppose that $\mathfrak{m} \supset I$ where $I = \mathrm{ann}_{\mathbb{T}}(C(\mathbb{T}))$. To show that two homomorphisms of $\mathbb{T}$ into $\mathcal{O}$ constructed above are distinct it suffices to show that $\mathbb{T} \twoheadrightarrow \mathbb{T}/\mathfrak{p}_X$ and $\mathbb{T} \twoheadrightarrow \mathbb{T}/\mathfrak{p}_Y$ are distinct. We do this by showing that $\mathfrak{p}_X \neq \mathfrak{p}_Y$. Now $I \not\subset \mathfrak{p}_X$ since otherwise the finite module $\mathbb{T}/I$ would surject to the infinite module $\mathbb{T}/\mathfrak{p}_X$. So there exists an element $T \in I \setminus \mathfrak{p}_X$. Since $T \in I$ we have that $T(1,0) \in \mathbb{T}$. That is, there exists an element $T' \in \mathbb{T}$ such that $T'|_X = T|_X$ and $T'|_Y = 0$. Clearly $T' \in \mathfrak{p}_Y$ and $T' \notin \mathfrak{p}_X$. This shows that $\mathfrak{p}_X \neq \mathfrak{p}_Y$ as desired.

Definition 4. *Call a maximal ideal in the support of* $C(\mathbb{T})$ *a prime of fusion with respect to the decomposition* (1).

We have just seen that primes of fusion yield congruences between normalized simultaneous eigenforms in X and Y (after a possible extension of the ring $\mathcal{O}$ so that it contains the Hecke eigenvalues of these eigenforms). The converse is also clearly true: if there is a congruence between normalized simultaneous eigenforms in X and Y which are congruent modulo $\wp$ then the maximal ideal $\mathfrak{m} \subset T$ which is the kernel of either homomorphism $T \twoheadrightarrow T^X \to \mathcal{O}/\wp$ or $T \twoheadrightarrow T^Y \to \mathcal{O}/\wp$ is a prime of fusion. In particular the residue characteristics of the primes of fusion $\mathfrak{m} \subset \mathbb{T}$ are the residue characteristics of the congruence prime $\wp \subset \mathcal{O}$.

The following Lemma is essentially a restatement of the discussion above.

Lemma 3. *We have*

$$\operatorname{ann}_{\mathbb{T}}\left(\frac{\mathbb{T}^X \oplus \mathbb{T}^Y}{\mathbb{T}}\right) = \operatorname{ann}_{\mathbb{T}}\left(\frac{M^X \oplus M^Y}{M}\right).$$

In particular

$$\operatorname{Supp}_{\mathbb{T}}(C(\mathbb{T})) = \operatorname{Supp}_{\mathbb{T}}(C(M)).$$

Proof. Let e denote the endomorphism of S which acts as the identity 1_X on X and as the zero map 0_Y on Y. Thus $e = (1_X, 0_Y) \in \mathbb{T}^X \oplus \mathbb{T}^Y$. Since $(\mathbb{T}^X \otimes K) \oplus (\mathbb{T}^Y \otimes K) = \mathbb{T} \otimes K$ we see that $e \in \mathbb{T} \otimes K$. We now claim that

$$\operatorname{ann}_{\mathbb{T}}\left(\frac{\mathbb{T}^X \oplus \mathbb{T}^Y}{\mathbb{T}}\right) = \{T \in \mathbb{T} \bigm| Te \in \mathbb{T}\}. \tag{2}$$

Suppose that $T \in$ LHS of (2). Then by definition $Te \in \mathbb{T}$ and so $T \in$ RHS of (2). For the converse suppose that $Te \in \mathbb{T}$. Let $f = (0_X, 1_Y) \in T^X \oplus \mathbb{T}^Y$. Then since $Te + Tf = T \in \mathbb{T}$ we see that $Tf \in \mathbb{T}$. Now pick an arbitrary element $(a, b) \in \mathbb{T}^X \oplus \mathbb{T}^Y$. Say $a = T'|_X$ and $b = T''|_Y$. Then $T(a, b) = T'(Te) + T''(Tf) \in \mathbb{T}$ so that $T \in$ LHS of (2).

On the other hand we claim that

$$\operatorname{ann}_{\mathbb{T}}\left(\frac{M^X \oplus M^Y}{M}\right) = \{T \in \mathbb{T} \bigm| Te(M) \subset M\}. \tag{3}$$

To see this suppose that $T \in$ LHS of (3). Let $m \in M$. Then $Te(m) = T(\pi_X(m), 0) = T(\pi_X(m), \pi_Y(0)) \in M$ showing that $T \in$ RHS of (3). Now suppose that $T \in$ RHS of (3). Then $Tf(M) \subset M$. Let $m_X = \pi_X(m)$ and let $m'_Y(m')$ for $m, m' \in M$. Then $T(m_X, m'_Y) = Te(m) + Tf(m') \in M$ showing that $T \in$ RHS of (3).

Let

$$\mathcal{O}_M := \{T \in \mathbb{T} \otimes K \bigm| T(M) \subset M\}$$

denote the order of the lattice M. Clearly $\mathbb{T} \subset \mathcal{O}_M$. Lemma 2 can be used to show that $\mathcal{O}_M = \mathbb{T}$. Now the Lemma follows from this and (2) and (3). □

3. The Eichler-Shimura isomorphism and cohomological congruence primes

Let H be a finite dimensional complex vector space with an action of all the Hecke operators T_n. In applications H will be (an eigenspace under complex conjugation) of a parabolic cohomology group that depends on the level and weight of the cusp forms in S. Suppose there is a Hecke equivariant isomorphism

$$S \xrightarrow{\sim} H \tag{4}$$

of complex vector spaces, which we shall formally call the Eichler-Shimura isomorphism. We shall assume that H comes equipped with a K-structure which we denote by $H(K)$. The Eichler-Shimura map does not take the K-structure on S to the K-structure on H, which is what makes the theory we wish to describe in this section interesting.

Let $L \subset H(K)$ be a Hecke stable lattice. Suppose that we have a Hecke stable decomposition

$$H(K) = A \oplus B \tag{5}$$

such that

$$X \otimes \mathbb{C} \xrightarrow{\sim} A \otimes \mathbb{C} \quad \text{and} \quad Y \otimes \mathbb{C} \xrightarrow{\sim} B \otimes \mathbb{C} \tag{6}$$

under the Eichler-Shimura isomorphism. Define the lattices $L_A \subset L^A$ and $L_B \subset L^B$ in A respectively B exactly as in Section 1.

Definition 5. *Call*

$$C^{\mathrm{coh}}(L) = \frac{L^A \oplus L^B}{L}$$

the cohomological congruence module of the lattice L with respect to the decomposition (5)*. The primes in* $\mathrm{Supp}_{\mathbb{T}}(C^{\mathrm{coh}}(L))$ *are called cohomological congruence primes.*

We could also define the obvious Hecke congruence module with respect to the decomposition (5) but by the Hecke equivariance of (4) and by (6) it would be isomorphic to the module $C(\mathbb{T})$ defined earlier using the decomposition (1).

Lemma 4. *We have*

$$\mathrm{ann}_{\mathbb{T}}(C(\mathbb{T})) \subset \mathrm{ann}_{\mathbb{T}}(C^{\mathrm{coh}}(L)).$$

Proof. The argument is a subset of the arguments used in the proof of Lemma 3, so we do not repeat it here. □

Lemma 4 shows that

$$\mathrm{Supp}_{\mathbb{T}}(C^{\mathrm{coh}}(L)) \subset \mathrm{Supp}_{\mathbb{T}}(C(\mathbb{T})). \tag{7}$$

Now let

$$\mathcal{O}_L = \{T \in \mathbb{T} \otimes K \mid T(L) \subset L\}$$

The reason that we do not obtain an equality in (7) as we did in Lemma 3 is that $\mathbb{T} \subset \mathcal{O}_L$ but it may very well turn out that $\mathbb{T} \neq \mathcal{O}_L$. Thus the cohomological congruence module $C^{\mathrm{coh}}(L)$ may *a priori* lose some information about the primes of congruence between cusp forms in X and cusp forms in Y. Let us give a toy example to drive home this point.

Example 1. Let $K = \mathbb{Q}$ and $\mathcal{O} = \mathbb{Z}$. Suppose that $H = A \oplus B$ where $A = \mathbb{C}$ and $B = \mathbb{C}$. Then the standard lattice $L = \mathbb{Z}^2$ sits inside $H(\mathbb{Q}) = \mathbb{Q}^2$ and clearly $C^{\mathrm{coh}}(L) = 0$. Now suppose that

$$\mathbb{T} = \left\{ A \in \mathrm{M}_2(\mathbb{Z}) \mid A = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \text{ and } a \equiv b \bmod p \right\}.$$

Then $\mathbb{T} \subset \mathrm{End}(H)$ in a natural way. Note that $T^A = \mathbb{Z} = \mathbb{T}^B$, so that $C(\mathbb{T}) = \mathbb{Z}/p$. Thus p is a genuine congruence prime that is not captured by the cohomological congruence module $C^{\mathrm{coh}}(L)$. The problem of course is that $\mathbb{T} \neq \mathcal{O}_L$. Indeed the matrix $\frac{1}{p}\left(\begin{smallmatrix} p & 0 \\ 0 & 0 \end{smallmatrix}\right)$ lies in $\mathbb{T} \otimes \mathbb{Q}$ and preserves L but it does not lie in $\mathbb{T}$.

For a finite $\mathbb{T}$-module Z let $\mathrm{Supp}'_{\mathbb{T}}(Z)$ denote the primes in the support of Z whose residue characteristics do not divide $[\mathcal{O}_L : \mathbb{T}]$. Then the following corollary is immediate.

Corollary 1. *We have*

$$\mathrm{Supp}'_{\mathbb{T}}(C^{\mathrm{coh}}(L)) = \mathrm{Supp}'_{\mathbb{T}}(C(M)).$$

4. Congruence module of a primitive form

Let us assume that K contains the Hecke fields of the set of normalized common eigenforms in S.

Let f be a normalized common eigenform that is a newform. Such a cusp form is called a primitive form. Let $X = X(f)$ denote the 1-dimensional subspace of S spanned by f. Note that X is defined over K. Let Y be the space of cusp forms that are orthogonal to f under the Petersson inner product. Let us set $C(f) = C(M)$ where we use the decomposition

$$S = X(f) \oplus Y. \tag{8}$$

Definition 6. *Call $C(f)$ the congruence module of f.*

Definition 7. *A prime ideal $\wp \subset \mathcal{O}$ is a prime of congruence for f if there is a normalized simultaneous eigenform $g \in S$ different from f with $f \equiv g \bmod \wp$.*

After what has already been said primes occurring in the support of $C(f)$ are exactly the congruence primes for f.

5. Adjoint L-values

We keep the notation of the previous sections. Thus f is a primitive form in S, say of weight $k \geq 2$ and level N. Let $\mathcal{B}$ denote the finite set of primes of K whose residue characteristics consist of the primes dividing $6N$ and the primes less than $k-2$.

The following theorem due to Hida [7], [8] (with a technical contribution due to Ribet [12]) completely characterizes the congruence primes of f outside $\mathcal{B}$ in terms of a special value of an L-function.

Theorem 1 (Hida). *Let $L^{\mathrm{alg}}(1, \mathrm{Ad}(f))$ denote the 'algebraic part' of the value at $s = 1$ of the adjoint L-function $L(s, \mathrm{Ad}(f))$ attached to f. Let $\wp$ be a prime of K with $\wp \notin \mathcal{B}$. Then $\wp$ is a congruence prime for f if and only $\wp \,\big|\, L^{\mathrm{alg}}(1, \mathrm{Ad}(f))$.*

Let $C^{\mathrm{coh}}(f)$ be the cohomological congruence module with respect to the analogue of the decomposition (8) of H. The proof of Theorem 1 proceeds in three main steps the last of which we have already taken care of in these notes.

(1) Outside $\mathcal{B}$, the primes dividing the 'algebraic part' of the adjoint L-value are the same as the primes in the support of the cohomological congruence module $C^{\mathrm{coh}}(f)$.

(2) The index $[\mathcal{O}_L : \mathbb{T}]$ is divisible only by the primes in $\mathcal{B}$.

(3) Corollary 1 which in this case yields that
$$\mathrm{Supp}'_{\mathbb{T}}(C^{\mathrm{coh}}(f)) = \mathrm{Supp}'_{\mathbb{T}}(C(f)).$$

There is a more precise version of Theorem 1 which relates the 'algebraic part' of $L(1, \mathrm{Ad}(f))$ to the cardinality of a certain Selmer group attached to the adjoint motive of f. For further details we refer the reader to [9, Theorem 5.20].

Generalizations of Theorem 1 in the Hilbert modular setting have been obtained by the author [5], [6] and in the imaginary quadratic setting by Urban [16].

6. Discriminants of Hecke algebras

In this section we show that there is one number, namely the discriminant of the Hecke algebra $\mathbb{T}$, that captures all congruence primes in S.

We start by recalling some basic linear algebra. Let V denote a finite dimensional vector space over $\mathbb{Q}$ with a non-degenerate pairing

$$t : V \times V \to \mathbb{Q}$$

Let $L \subset V$ be a lattice which satisfies $t(L, L) \subset \mathbb{Z}$. Then there is the notion of the discriminant of the lattice L with respect to the pairing t given by

$$d(L) = |\det(t(e_i, e_j))|$$

where $e_1, e_2, \ldots, e_{\dim(V)}$ is any basis of L.

Now let L_1, L_2 denote two lattices in V such that $t(L_i, L_i) \subset \mathbb{Z}$ for $i = 1, 2$. Suppose that there is an exact sequence

$$0 \to L_1 \to L_2 \to L_2/L_1 \to 0$$

where L_2/L_1 is a finite abelian group. Then (see Proposition 5, Section 2, Chapter 3 of Serre's *Local Fields*)

$$d(L_1) = d(L_2) \cdot [L_2 : L_1]^2. \tag{9}$$

Now let S be a space of elliptic cusp forms of weight k, level N and nebentypus ψ. We assume for simplicity that

- S does not contain any old forms (this happens for instance if the conductor of ψ is N), and,
- S has a basis of cusp forms with integral coefficients (this happens if ψ is either the trivial character or a quadratic character).

The first hypothesis implies that S has a basis of primitive forms. Let us choose a set of representatives f of the Galois orbits of this basis. Then we have the decomposition

$$S(\mathbb{Q}) = \oplus_f X_f$$

where X_f denotes the space spanned by f and its Galois conjugates.

Let $\mathbb{T}$ denote the Hecke algebra over $\mathbb{Z}$. Since S has a basis over $\mathbb{Z}$, we can think of $\mathbb{T}$ as the subalgebra of $\mathrm{End}_{\mathbb{Z}}(S(\mathbb{Z}))$ generated by all the Hecke operators. Similarly we let $\mathbb{T}^f$ denote the subalgebra of $\mathrm{End}_{\mathbb{Z}}(X_f)$ generated by all the Hecke operators.

Both $\mathbb{T}$ and $\oplus_f \mathbb{T}^f$ are lattices in $\mathbb{T} \otimes \mathbb{Q}$ and they are related by the exact sequence

$$0 \to \mathbb{T} \to \oplus_f \mathbb{T}^f \to C \to 0$$

where $C = (\oplus_f \mathbb{T}^f)/\mathbb{T}$. The vector space $\mathbb{T} \otimes \mathbb{Q}$ has the natural trace pairing

$$t(A, B) = \mathrm{tr}(AB)$$

which takes values in $\mathbb{Q}$, and values in $\mathbb{Z}$ on $\mathbb{T}$ and on each $\mathbb{T}^f$. By (9) we have

$$d(\mathbb{T}) = |C|^2 \cdot \prod_f d(\mathbb{T}^f).$$

From what we have said in previous sections it is clear that C measures congruences between primitive forms in distinct Galois orbits.

On the other hand let $\mathcal{O}(f)$ denote the order generated by the Fourier coefficients of f. Clearly $\mathbb{T}^f \xrightarrow{\sim} \mathcal{O}(f)$ where the isomorphism is induced by $T_n \mapsto c(n, f)$ so that $d(\mathbb{T}^f) = d(\mathcal{O}(f))$. Let K_f denote the quotient field of $\mathcal{O}(f)$ and let $\mathcal{O}_f$ denote its ring of integers. We have $\mathcal{O}(f) \subset \mathcal{O}_f$. Let $\bar{K}_f$ denote the Galois closure of K_f.

Lemma 5. *Assume $\mathcal{O}(f) = \mathcal{O}_f$ and $\bar{K}_f = K_f$. Then $p \bigm| d(\mathcal{O}(f))$ if and only if there exists a prime $\wp$ of K_f with $\wp | p$ and a non-trivial element $\gamma \in \mathrm{Gal}(K_f/\mathbb{Q})$ such that*

$$f^\gamma \equiv f \bmod \wp. \tag{10}$$

Proof. Suppose $p \bigm| d(\mathcal{O}(f)) = d(\mathcal{O}_f)$. Fix a prime $\wp$ of K_f lying over p. Let $I(\wp)$ denote the inertia subgroup of $K_f/\mathbb{Q}$ at $\wp$. Since p ramifies in K_f there exists a non-trivial $\gamma \in I(\wp)$. Since

$$\gamma(x) \equiv x \bmod \wp \tag{11}$$

for all x in $\mathcal{O}_f$, the congruence holds in particular for all $x = a(n, f) \in \mathcal{O}(f)$ and (10) follows.

Conversely, if $\wp \subset \mathcal{O}_f$ and $1 \neq \gamma \in \mathrm{Gal}(K_f/\mathbb{Q})$ satisfy (10) then (11) holds for all x in $\mathcal{O}(f) = \mathcal{O}_f$. This implies that γ fixes $\wp$. and moreover that $\gamma \in I(\wp)$. Thus p ramifies and $p \bigm| d(\mathcal{O}_f) = d(\mathcal{O}(f))$. □

The lemma says that, at least under the assumptions that $\mathcal{O}(f) = \mathcal{O}_f$ and that $K_f/\mathbb{Q}$ is a Galois extension, the term $d(\mathbb{T}_f)$ measures congruences between f and other forms in the same Galois orbit. In general K_f is rarely a Galois extension of $\mathbb{Q}$ and $\mathcal{O}_f \subset \mathcal{O}(f)$ may be a proper containment. We leave to the reader to investigate what happens in this situation. We only note that in general

$$d(\mathcal{O}(f)) = d(\mathcal{O}_f) \cdot [\mathcal{O}_f : \mathcal{O}(f)]^2.$$

7. Galois representation

Let $f \in S_k(N, \chi)$ be a cusp form of weight k, level N and nebentypus χ. Assume that f is a normalized common eigenform for all the Hecke operators T_p for $p \not| N$. Let K be a sufficiently large number field so that it contains the Hecke field of f and let $\wp$ be a prime of K. Eichler-Shimura and Deligne attach a Galois representation to f when $k \geq 2$:

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(K_\wp)$$

which is unramified outside Np and is characterized by the property that it is irreducible and

- $\mathrm{tr}(\rho_f(\mathrm{Frob}_\ell)) = c(\ell, f)$
- $\det(\rho_f(Frob_\ell)) = \ell^{k-1}\chi(\ell)$

for all $l \not| Np$.

Choosing a Galois stable lattice in the space of ρ_f we may assume that ρ_f takes values in $\mathrm{GL}_2(\mathcal{O}_\wp)$ and therefore by reduction in $\mathrm{GL}_2(\mathbb{F})$ where $\mathbb{F}$ is the residue field of $\mathcal{O}_\wp$. Let

$$\bar{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$$

denote the semi-simplification of the representation so obtained; it is independent of the choice of the Galois stable lattice we started with.

When $k = 1$ Deligne and Serre have shown that it is still possible to attach a $\mathrm{GL}_2(\mathbb{C})$-valued Galois representation ρ_f to f which is unramified outside N such that the Frobenius elements outside N satisfy properties similar to the ones above. Given a prime $\wp$ of $\overline{\mathbb{Q}}$ one can similarly construct the reduced representation $\bar{\rho}_f$.

Now let k and l be integers larger than 1, and let let $f \in S_k(N, \chi)$ and $g \in S_l(M, \psi)$ be normalized common eigenforms outside their respective levels. Let K be a number field that contains both their Hecke fields and $\wp$ be a prime of K. We broaden the notion of congruence and say that f and g are congruent modulo $\wp$ if

$$c(\ell, f) \equiv c(\ell, g) \bmod \wp$$

for all but finitely many primes ℓ. We sometimes write

$$f \equiv' g \bmod \wp$$

using the symbol $\equiv'$ instead of $\equiv$ to alert the reader that the Fourier coefficients may fail to be congruent at finitely many primes. In terms of the mod $\wp$ Galois representations attached to f and g, we have

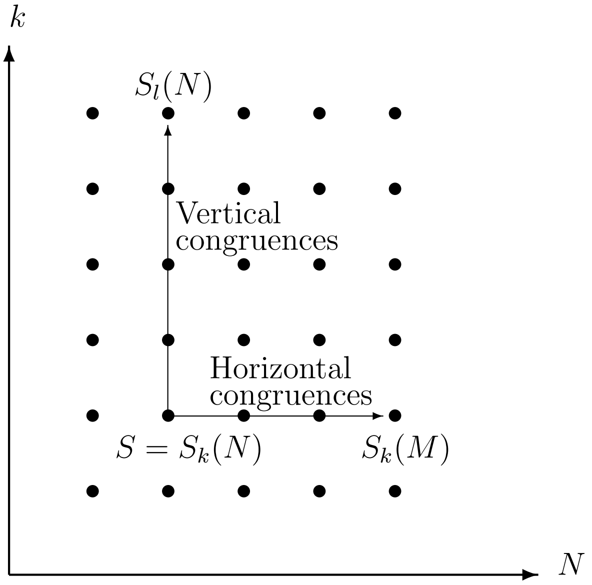
$$\bar{\rho}_f \sim \bar{\rho}_g \iff f \equiv' g \bmod \wp$$

since the isomorphism class of a semisimple representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into GL_2 of a finite field is determined by the traces and the determinants of the Frobenius elements outside a finite set of primes, and in the setting of modular Galois representations it is well known that the determinants are determined by the traces.

8. Horizontal congruences

Consider the 2 by 2 grid indexed by level $N \geq 1$ on the x-axis and by weight $k \geq 1$ on the y-axis. The space $S = S_k(N)$ depends on k and N. We leave ambiguous whether we are fixing a nebentypus, such as the trivial one, or are considering all nebentypus characters simultaneously. Then $S = S_k(N)$ corresponds to one point on this grid. So far we have restricted our attention to congruences between modular forms in the same space of cusp forms $S = S_k(N)$. However, as we have already hinted at in the section on Galois representations, there is nothing to stop one from asking whether or not eigenforms in spaces of cusp forms of *different* levels and/or weights can be congruent. In fact this happens frequently and is the source of much interesting mathematics.

For convenience let us introduce some terminology. If there is a congruence between $S_k(N)$ and $S_k(M)$ for $N \neq M$ we shall say that we have a horizontal congruence. Likewise congruences between $S_k(N)$ and $S_l(N)$ for $k \neq l$ will be referred to as vertical congruences. These notions are illustrated in the diagram below.



In this section we describe some results on horizontal congruences. Vertical congruences will be considered in the next section.

Assume that the notation $S_k(N)$ means cusp form of level N, even weight $k \geq 2$ and trivial nebentypus. Let f be a newform in $S_k(N)$ that is a simultaneous eigenform of all the Hecke operators of level N. Let q be a prime such that $q \not| N$. The simplest question regarding horizontal congruences that one might ask is whether, given a prime $\wp$ in a sufficiently large number field K, there is a cusp form $g \in S_k(Nq)$ which is q-new and a simultaneous eigenform of all the Hecke operators of level Nq such that $f \equiv g \bmod \wp$. There is a slight technical problem that arises. Let U_q be the Hecke operator at q acting on $S_k(Nq)$. Then f is not an eigenvector of U_q considered as an oldform in $S_k(Nq)$. But there is a standard procedure to alter f slightly to make it an eigenform of U_q. Let α and β be the roots of the polynomial

$$x^2 - c(q,f)X + q^{k-1}.$$

Then $\alpha\beta = q^{k-1}$ and $\alpha + \beta = c(q,f)$. Let

$$\begin{aligned} f_\alpha &= f(z) - \beta f(qz) \\ f_\beta &= f(z) - \alpha f(qz). \end{aligned}$$

Then f_α and f_β are q-old forms in $S_k(Nq)$ that *are* eigenvectors of U_q with respective eigenvalues α and β. Of course they are also eigenvectors of the other Hecke operators and so are simultaneous eigenforms.

It makes more sense then to ask if say $f_\alpha \equiv g \bmod \wp$ for a q-new simultaneous eigenform $g \in S_k(Nq)$. Assume that this is true. Then we have $c(n, f_\alpha) \equiv c(n, g) \bmod \wp$ for all n. In particular we have

$$c(q, f_\alpha) \equiv c(q, g) \bmod \wp.$$

Now it is well known (see for instance Miyake's book [10, Theorem 4.6.17]) that $c(q,g) = \pm q^{(k-2)/2}$. On the other hand $c(q, f_\alpha) = \alpha$. We conclude that $\alpha \equiv \pm q^{(k-2)/2} \bmod \wp$. Multiplying this by β we get $\beta \equiv \pm q^{k/2} \bmod \wp$. We conclude that

$$c(q,f) = \alpha + \beta \equiv \pm q^{(k-2)/2}(q+1) \bmod \wp. \tag{12}$$

The condition (12) is thus a necessary condition for f_α to be congruent to g modulo $\wp$. In fact this condition is also sufficient:

Theorem 2 (Ribet, Diamond)**.** *Let f be a primitive form in $S_k(N)$ of weight $k \geq 2$. Then f has the same mod $\wp$ Hecke eigenvalues outside q as some q-new eigenform in $S_k(Nq)$ if and only if*

$$c(q,f)^2 \equiv q^{k-2}(1+q)^2 \bmod \wp.$$

Ribet [13] proved the above theorem in the case $k = 2$. The case of weight $k \geq 2$ was treated by Diamond [4] (he also considers the case when f has a non-trivial nebentypus).

Theorem 2 is often described as a 'level raising' theorem. But horizontal congruences are equally concerned with 'level lowering' results. We now state a theorem in this direction. Below p denotes the residue characteristic of a prime $\wp \subset \mathcal{O}$ where $\mathcal{O}$ is the ring of integers of a sufficiently large number field.

Theorem 3 (Mazur, Ribet)**.** *Suppose that $p \geq 3$. Let q be a prime such that $q|N$ but $q^2 \not| N$. Let f be a primitive form in $S_2(N)$. Assume that the mod $\wp$ Galois representation $\bar{\rho}_f$ attached to f is irreducible and finite at q. Assume also that either*

(1) *$q \not\equiv 1 \bmod p$, or,*

(2) *p is prime to N.*

Then

$$f \equiv' g \bmod \wp$$

for some primitive form $g \in S_2(N/q)$.

Theorem 3 was proved by Mazur under condition 1) above and by Ribet [14] under condition 2) above. The condition that the mod $\wp$-Galois representation $\bar{\rho}_f$ attached to f is 'finite at q' is a technical one. It means that there is finite flat $\mathbb{F}_p$-vector space scheme H over $\mathbb{Z}_q$ such that the representation $\bar{\rho}_f$ restricted to a decomposition group D_q at q is isomorphic to the natural representation of D_q on the $\mathbb{F}_p$-vector space $H(\overline{\mathbb{Q}}_q)$. When $q \neq p$ the condition that $\bar{\rho}_f$ is finite at q is equivalent to ρ_f being unramified at q.

For an improved version of Theorem 3 we refer the reader to Theorem 1.5 of [15]. In [15], the author also gives an excellent survey of other level lowering theorems in the literature, and explains how level lowering is connected to Serre's conjecture on the modularity of irreducible, odd, two-dimensional mod p representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

9. Vertical congruences

We now turn our attention to vertical congruences.

Let $S_k(N, \chi)$ denote the space of cusp of forms of weight $k \geq 1$, level N and nebentypus χ. Fix an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$. For each prime p fix an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$ and let $\wp$ denote the prime of $\overline{\mathbb{Q}}$ determined by this embedding.

Definition 8. *Let $f \in S_k(N, \chi)$ be a primitive form. Then f is said to be ordinary at p if $c(p, f)$ is a $\wp$-adic unit.*

Remark 1. Even if we fix the embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$, the notion of ordinarity of f at p depends on the embeddings of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$. For instance if one takes f to be a primitive form in $S_2(43, 1)$ then the prime $17 = \wp\wp'$ splits into two primes in the real quadratic number field generated by the Fourier coefficients of f, but since the norm of $c = c(17, f)$ is 17 we see that either c is a $\wp$-adic unit and c is divisible by $\wp'$ or vice versa.

Let f be a primitive modular in $S_k(N, \chi)$. Let p be a prime that does not divide N and assume that f is ordinary at p with respect to some once and for all fixed embeddings of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ and $\overline{\mathbb{Q}}_p$. Let ω denote the Teichmüller character of level p. Then Hida has proved that f lives in a family of p-ordinary modular forms. More precisely let α denote the unique $\wp$-adic unit root of $x^2 - c(p, f)x + \chi(p)p^{k-1}$ and let β be the other root. Let $f_\alpha = f(z) - \beta f(pz)$ be the p-stable form constructed from f as in the previous section. Then one has:

Theorem 4 (Hida)**.** *There are modular forms*

$$f_l \in S_l(Np, \chi\omega^{k-l}) \quad \textit{for} \quad l = 1, 2, 3 \ldots$$

(where f_1 may be a 'p-adic modular form') such that

- $f_k = f_\alpha$*,*
- f_l *is a normalized eigenform of level Np for each $l \geq 1$,*
- f_l *is ordinary at p for each $l \geq 1$,*
- $f_{l_1} \equiv' f_{l_2} \bmod \wp$ *for all l_1, $l_2 \geq 1$.*

It is the last condition on the members of this so called Hida family that shows that vertical congruences exist in abundance: f_k and therefore f is congruent mod $\wp$ to a modular form of weight l for each weight $l \geq 1$.

The work of Coleman [2], Coleman-Mazur [3] and numerical data of Gouvea (see http://www.colby.edu/personal/f/fqgouvea/slopes) shows that non-ordinary eigenforms also live in families, so that such eigenforms are vertically congruent to every other member of their family.

10. Dihedral congruence primes

Let $f = \sum c(n, f)q^n$ be a cusp form without complex multiplication. Let χ be a quadratic Dirichlet character and let $f \otimes \chi$ be the cusp form whose q-expansion is given by $\sum \chi(n)c(n, f)q^n$. Let K_f denote the Hecke field for f. The Hecke field of $f \otimes \chi$ is contained in K_f.

Definition 9. *A prime $\wp$ of K_f is a dihedral congruence prime for f with respect to χ if there is a congruence of the form $f \equiv' f \otimes \chi \bmod \wp$.*

Lemma 6. *Let f be a primitive cusp form and let $\wp$ be a dihedral congruence prime for f with respect to a quadratic character χ. If $\bar{\rho}_f$,* *the mod $\wp$ Galois representation attached to f, is absolutely irreducible, then*

$$\bar{\rho}_f = \mathrm{Ind}_{\mathbb{Q}}^{F_\chi} \phi$$

for a mod $\wp$ character ϕ of the Galois group of F_χ, where F_χ is the quadratic field corresponding to χ.

The lemma explains why $\wp$ is called a dihedral congruence prime: it can be checked that the image of $\bar{\rho}_f$ in $\mathrm{PGL}_2(\mathbb{F})$ is a dihedral group.

Now suppose that f is a primitive cusp form and that $\wp$ is a dihedral congruence prime with respect to a real quadratic character χ. The lemma above produces a character $\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/F_\chi) \to \mathbb{F}^\times$ where F_χ is the real quadratic field corresponding to χ and $\mathbb{F}$ is the residue field of the ring of integers of K_f at $\wp$. By composing ϕ with the reciprocity map

$$\mathbb{A}_{F_\chi}^\times \to \mathrm{Gal}(F_\chi^{\mathrm{ab}}/F_\chi)$$

we may think of ϕ as a finite order Hecke character of F_χ. Let $\mathfrak{c}$ be its conductor and let $\phi_0 : (\mathcal{O}_{F_\chi}/\mathfrak{c})^\times \to \mathbb{F}^\times$ be the associated Dirichlet character. Then $\phi_0(\epsilon_+) = 1$ for each totally positive unit ϵ of F_χ. On the other hand since

$$\phi\phi^\sigma = \psi\omega^{k-1}$$

where ψ is the nebentypus of f and ω is the mod p Teichmüller character, one can often compute what ϕ_0 is explicitly. As a consequence one can characterise the dihedral congruence primes of f with respect to χ in terms of a totally positive fundamental unit of F_χ.

We illustrate the above discussion with the following theorem. Let D denote the discriminant of a quadratic field and let $D = D_1 D_2$ denote a factorisation of D into two fundamental discriminants with $D_1 > 0$. Let χ_D and χ_{D_1} denote the quadratic characters corresponding to D and D_1.

Theorem 5 (Hida, Brown-Ghate). *Let $f \in S_k(|D|, \chi_D)$ be a primitive form. Let $p \geq 3$ be a prime such that $p \nmid D$ and let $\wp$ be a prime of $\overline{\mathbb{Q}}$ lying over p. Assume that $k-1$ is not a multiple of $p-1$. If f satisfies a congruence of the form*

$$f \equiv' f \otimes \chi_{D_1} \bmod \wp$$

and f is ordinary at $\wp$ and $\bar{\rho}_f$ is absolutely irreducible then

$$p \mid \mathrm{N}_{F_1/\mathbb{Q}}(\epsilon_+^{k-1} \pm 1)$$

for some (any) totally positive fundamental unit ϵ_+ of F_1.

Under certain conditions one can also establish a converse to this result using theta series and Hida families; for the details we refer the reader to [1].

11. Congruences with Eisenstein series

So far in this article we have only considered congruences between cusp forms. However one could equally well consider congruences between modular forms. For instance let Δ be the unique primitive cusp form of level one and weight 12 given by

$$\Delta = q\prod_{n}(1-q^n)^{24} = \sum \tau(n)q^n$$

and let E_k denote Eisenstein series of level one and (even) weight $k \geq 4$ given by

$$E_k(z) = \frac{(-1)^{k/2}(k-1)!}{2(2\pi)^k}\cdot\sum\frac{1}{(mz+n)^{12}} = -\frac{B_k}{2k} + \sum \sigma_{k-1}(n)q^n,$$

where B_k is the k^{th} Bernoulli number and $\sigma_r(n) = \sum_{d|n} d^r$. When $k = 12$ one checks that $691|B_{12}$ and Ramanujan proved the pretty congruence

$$\tau(n) \equiv \sigma_{11}(n) \bmod 691$$

for all $n \geq 1$. More generally one has the following result.

Proposition 1. *Let $k \geq 4$ be an even integer. Let $p > k$ be a prime such that $p|B_k$. Then there is a primitive cusp form $f = \sum c(n,f)q^n$ of weight k and level 1 and a prime $\wp$ of K_f lying over p such that $c(n,f) \equiv \sigma_{k-1}(n) \bmod \wp$ for all $n \geq 1$.*

Let p be an odd prime. Let i be an odd integer with $3 \leq i \leq p-2$. Let A_i be the eigenspace under the action of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ of the class group of the p^{th} cyclotomic field $\mathbb{Q}(\mu_p)$ corresponding to the i^{th} power of the Teichmüller character. Herbrand's theorem is that if $A_i \neq 0$ then $p|B_{p-i}$. Conversely Ribet has shown [11] that if $p|B_{p-i}$ then $A_i \neq 0$. The proposition can be viewed as the starting point for Ribet's proof of the converse of Herbrand's theorem.

References

[1] A. Brown and E. Ghate. Dihedral congruence primes and class fields of real quadratic fields. *J. Number Theory*, 95(1):14–37, 2002.

[2] R. Coleman. p-adic Banach spaces and families of modular forms. *Invent. Math.*, 127(3):417–479, 1997.

[3] R. Coleman and B. Mazur. The eigencurve. In *Galois representations in arithmetic algebraic geometry (Durham, 1996)*, volume 254 of *London Math. Soc. Lecture Note Ser.*, pages 1–113. Cambridge Univ. Press, 1999.

[4] F. Diamond. Congruence primes for cusp forms of weight $k \geq 2$. In *Courbes modulaires et courbes de Shimura (Orsay, 1987/1988)*, number 196-197 (1991) in Astrisque, pages 205–213. 1992.

[5] E. Ghate. Adjoint L-values and primes of congruence for Hilbert modular forms. *Compositio Math.*, 132(3):243–281, 2002.

[6] E. Ghate. On the freeness of the integral cohomology groups of Hilbert-Blumenthal varieties as Hecke-modules. *In preparation*, 2003.

[7] H. Hida. Congruence of cusp forms and special values of their zeta functions. *Invent. Math.*, 63:225–261, 1981.

[8] H. Hida. On congruence divisors of cusp forms as factors of the special values of their zeta functions. *Invent. Math.*, 64:221–262, 1981.

[9] H. Hida. *Modular Forms and Galois Cohomology.* Cambridge University Press, Cambridge, 2000.

[10] T. Miyake. *Modular Forms.* Springer-Verlag, 1989.

[11] K. Ribet. A modular construction of unramified p-extensions of $Q(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.

[12] K. Ribet. Mod p Hecke operators and congruences between modular forms. *Invent. Math.*, 71(1):193–205, 1983.

[13] K. Ribet. Congruence relations between modular forms. In *Proceedings of the International Congress of Mathematicians, Warsaw (1983)*, pages 503–514. PWN, Warsaw, 1984.

[14] K. Ribet. On modular representations of $\mathrm{Gal}(\overline{Q}/Q)$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[15] K. Ribet. Report on mod l representations of $\mathrm{Gal}(\overline{Q}/Q)$. In *Motives (Seattle, WA, 1991)*, Proc. Sympos. Pure Math., 55, Part 2, pages 639–676. Amer. Math. Soc., Providence, RI, 1994.

[16] E. Urban. Formes automorphes cuspidales pour GL(2) sur un corps quadratique imaginare. Valeurs spéciales de fonctions L et congruences. *Compositio Math.*, 99(3):283–324, 1995.

School of Mathematics, Tata Institute of Fundamental Research, Homi Bhabha Road, Mumbai 400 005, India.

E-mail address: eghate@math.tifr.res.in