CONGRUENCES OF CUSP FORMS AND HECKE ALGEBRAS

HARUZO HIDA

0 - We begin by giving a short summary of the theory of congruences of a fixed primitive cusp form \( f \), and then, we shall sketch how we can construct a theory which allows the cusp form \( f \) to vary.

Finally, we shall discuss some examples of our results. The detailed proofs of our theorems below will appear elsewhere.

1 - Fix a positive integer \( N \) and let \( \psi \) be a Dirichlet character modulo \( N \). Take a holomorphic cusp form \( f \not\equiv 0 \) on the upper half complex plane of weight \( k \) for the congruence subgroup \( \Gamma_0(N) \) of \( \text{SL}_2(\mathbb{Z}) \) with character \( \psi \). Write its Fourier expansion as

\[
f(z) = \sum_{n=1}^{\infty} a(n)e(nz) \quad (e(z) = \exp(2\pi i z))
\]

and suppose that \( f|\Gamma(n) = a(n)f \) for all Hecke operators \( \Gamma(n) \) for \( \Gamma_0(N) \) including those with \( n \) dividing \( N \). Any non-zero form with this property is said to be normalized. Every Fourier coefficient of a normalized form is an algebraic integer. As usual, let \( S_k(\Gamma_0(N), \psi) \) (resp. \( S_k(\Gamma_1(N)) \)) denote the space of cusp forms for \( \Gamma_0(N) \) of weight \( k \) with character \( \psi \) (resp. for the congruence subgroup \( \Gamma_1(N) \) of \( \Gamma_0(N) \)). A prime ideal \( p \) of the ring of all algebraic integers in \( \mathbb{C} \) and also its restriction \( p \cap \mathbb{Z} \) to \( \mathbb{Z} \) are said to be a congruence prime of \( f \) if the following conditions are satisfied:

1a) there is a normalized form \( g = \sum_{n=1}^{\infty} b(n)e(nz) \) in \( S_k(\Gamma_1(N)) \) with

\[
a(n) \equiv b(n) \mod{p}.
\]
\[ f = g \mod \mathbb{P} \quad \text{(i.e. } a(n) = b(n) \mod \mathbb{P} \text{ for all } n) \]

(1b) the normalized form \( g \) is different from any conjugates

\[ f^\sigma(z) = \sum_{n=1}^{\infty} a(n)^\sigma \rho(nz) \\text{ of } f \text{ under automorphisms } \sigma \text{ of } \mathbb{C}. \]

One of the key points in the study of congruence primes is to make use of the Hecke algebras associated with the cusp form \( f \). The Hecke algebra \( h_k \) is by definition the subalgebra of the linear endomorphism algebra of \( S_k(\Gamma_1(N)) \) and it is generated over \( \mathbb{Z} \) by all the Hecke operators \( T(n) \) acting on \( S_k(\Gamma_1(N)) \) (including those with \( n \) dividing \( N \)). Naturally, \( f \) is a common eigenvector of all operators in \( h_k \), and thus one can associate with \( f \) an algebra homomorphism \( \lambda \) of \( h_k \) into \( \mathbb{C} \) via \( f(T) = \lambda(T)f \) for \( T \in h_k \). As is well known, the scalar extension \( h_k(\mathbb{Q}) = h_k \otimes \mathbb{Q} \) is an Artin algebra over \( \mathbb{Q} \), and hence, \( \lambda \) has values in the field \( \mathbb{Q} \) consisting of all algebraic numbers of \( \mathbb{C} \). Then, we can find a unique local ring \( K \) of \( h_k(\mathbb{Q}) \) and a homomorphism \( \lambda' \) of \( K \) into \( \overline{\mathbb{Q}} \) which makes the following diagram commutative:

\[ \begin{array}{ccc}
\lambda : h_k(\mathbb{Q}) & \rightarrow & \overline{\mathbb{Q}} \subset \mathbb{C} \\
\downarrow & & \\
K & \xrightarrow{\lambda'} & \overline{\mathbb{Q}} \\
\end{array} \]

Decompose \( h_k(\mathbb{Q}) \) into an algebra direct sum \( K \otimes A \), which is certainly unique, and let \( h(K) \) and \( h(A) \) be the projected images of \( h_k \) in \( K \) and \( A \). This may be summarized by the diagram:

\[ h_k(\mathbb{Q}) = K \otimes A \]

Define a module \( C(f) \) by

\[ C(f) = (h(K) \otimes h(A))/h_k, \]

which has only finitely many elements. The importance of the module \( C(f) \) lies in the following fact:

(2a) a prime \( p \) divides the order of \( C(f) \) if and only if \( p \) is a
congruence prime of \( f \).

Another interesting fact is a relation between the module \( C(f) \) and the special value at the weight \( k \) of a zeta function of \( f \), which is defined by

\[
L(s, f) = \left( \prod_{n=1}^{\infty} n^{2k-2-2s)} \right) \left( \sum_{n=1}^{\infty} \psi(n)a(n^2)n^{-s} \right)
\]

\[
= \prod_p (1 - \psi(p)a(p^2)p^{-s} + \psi(p)a(p^2)p^{k-1-s} - p^{3k-3-3s})^{-1}.
\]

We consider the product \( Z(s, f) = \prod (s, f^p) \) over all conjugates of \( f \).

As shown in [1, (7.1) and Cor. 6.3], there is a canonical integer part of \( Z(k, f) \), and by the results of [1, 2] and those of Ribet [4], when \( p \) is sufficiently large (i.e. \( p \geq 5 \), \( p \geq k \) and \( (p, N) = 1 \)) and if \( f \) is primitive, then

(2b) \( p \) divides the order of \( C(f) \) if and only if \( p \) divides the canonical integer part of \( Z(k, f) \).

It is an interesting problem to clarify the difference, if any, between the canonical integer part of \( Z(k, f) \) and the order of \( C(f) \). Some results in this direction can be found in [3, § 3].

2 - Let \( S_k(\Gamma_1(N); \mathbb{Q}) \) denote the subspace of \( S_k(\Gamma_1(N)) \) consisting of all cusp forms with rational Fourier coefficients. This space is known to be stable under the action of the Hecke algebra \( h_k(\mathbb{Q}) \). For any extension \( F \) over \( \mathbb{Q} \), put

\[
S_k(\Gamma_1(N); F) = S_k(\Gamma_1(N); \mathbb{Q}) \otimes_{\mathbb{Q}} F.
\]

Then, the Hecke algebra \( h_k(F) = h_k \otimes_{\mathbb{Q}} F \) acts on \( S_k(\Gamma_1(N); F) \) and may be considered as a \( F \)-subalgebra of the endomorphism algebra of \( S_k(\Gamma_1(N); F) \). If the character \( \psi \) has values in \( F \), we denote by \( S_k(\Gamma_1(N), \psi; F) \) the subspace of \( S_k(\Gamma_1(N); F) \) consisting of all forms transformed under \( \Gamma_0(N)^* \) via the character \( \psi \).

We hereafter fix a prime \( p \geq 5 \) and a prime ideal \( \mathfrak{p} \) over \( p \) in the ring of all algebraic integers in \( C \). Let \( \Omega \) be the quotient field of the \( \mathbb{P} \)-adic completion of this ring. By continuity, the morphism \( h_k(\mathbb{Q}) \rightarrow \mathbb{Q} \subset \Omega \) can be extended to a homomorphism \( \lambda_p : h_k(\mathbb{Q}_p) \rightarrow \Omega \). Then \( \lambda_p \) factors through a unique local ring \( k_p \) of \( h_k(\mathbb{Q}_p) \) (which is
a direct summand of \( K \otimes Q_p \). Decompose \( h_k(Q_p) = K_p \otimes A_p \) as an algebra direct sum and let \( h(K_p) \) and \( h(A_p) \) be the natural images of \( h_k(Z_p) = h_k \otimes Z_p \) in \( K_p \) and \( A_p \). Put
\[
C_p(f) = (h(K_p) \otimes h(A_p))/h_k(Z_p).
\]
So far, we have discussed only on the congruences of the fixed normalized form \( f \), but if \( p \) divides \( N \), there is a sequence of normalized forms \( f_\lambda \) in \( S_\lambda(\Gamma_1(N)) \) for each weight \( \lambda \) with \( f \equiv f_\lambda \mod P \). Then, we ask the following questions.

I. When \( C_p(f) \neq 0 \), are the modules \( C_p(f_\lambda) \) non-trivial?

II. If so, how does the structure of \( C_p(f_\lambda) \) depend on \( \lambda \)?

Under the hypothesis that \( a(p) \neq 0 \) mod \( P \) and with some additional assumptions, the answer to question I is affirmative, and \( C_p(f_\lambda) \) depends \( p \)-adically on \( \lambda \). The meaning of the analyticity is that there is a power series \( H(X) \) with coefficients in \( Z_p \) depending only on \( f \) and there is also a homomorphism of \( Z_p/H((1+p)^{k-1})Z_p \) into \( C_p(f_\lambda) \) with finite kernel and cokernel, whose orders are bounded independently on \( \lambda \). Furthermore, we know that \( C_p(f_\lambda) \cong C_p(f_\lambda') \) if \( \lambda \) and \( \lambda' \) are sufficiently close in the sense of the \( p \)-adic topology.

3 - One point which we must keep in mind to solve these questions is that we have to specify \( f_\lambda \) somehow, because \( f_\lambda \) may not be uniquely determined only by the congruence \( f \equiv f_\lambda \mod P \). To accomplish this task, we are naturally led to consider some bigger Hecke algebras which act on \( f \) and \( f_\lambda \) for all \( \lambda \) simultaneously. To define this, we assume that

the prime \( p \) divides \( N \) but \( p^2 \) does not divide \( N \).

Then, we put
\[
S^j = \bigoplus_{\lambda=1}^j S_\lambda(\Gamma_1(N);Q_p) \quad \text{for} \quad j > 0
\]

and let \( h^j \) for the subalgebra of the endomorphism algebra of \( S^j \) which is generated over \( Z_p \) by all Hecke operators \( T(n) \) for \( \Gamma_1(N) \). Here, \( T(n) \) acts on the direct sum \( S^j \) diagonally. The restriction of operators in \( h^j \) to the subspace \( S^j_{(j > i)} \) induces a morphism of \( h^j \) onto \( h^i \), which defines a projective system \( [h^j] \). Forming the projective limit \( h = \lim_j h^j \), we obtain a compact ring acting on
\[ S = \lim_{j \to \infty} \mathcal{S}_j^{(1)} \subset \mathcal{S}_k(\Gamma_1(N); \mathcal{O}_p). \]

Our key idea is to consider the algebra \( h \) as an algebra over the Iwasawa algebra \( \Lambda \) for the multiplicative group \( \Gamma = 1 + p\mathbb{Z}_p \). Namely, let \( \Gamma \) act on \( S_k(\Gamma_1(N); \mathcal{O}_p) \) via \( g \gamma = \gamma g \) for \( \gamma \in \Gamma \). Then the diagonal action of \( \gamma \in \Gamma \) on \( S \) can be regarded as an operator in \( h \). In fact, the Hecke operator \( q(T(q)^2 - T(q)^{-1}) \) for each prime \( q \equiv 1 \mod N \) in \( h \) gives the action of \( q \) on \( S \) as an element of \( \Gamma \). Since such primes are dense in \( \Gamma \), \( h \) may be regarded as a continuous \( \Gamma \)-module, and hence, is an algebra over \( \Lambda = \lim_{n \to \infty} Z_p[\Gamma_p/1+p^n\mathbb{Z}_p] \).

The \( \Lambda \)-algebra \( h \) is too big to handle right now; so, let us make it a little smaller. Since \( h^j \) is a (commutative) finite \( Z_p \)-algebra, the limit \( e_j = \lim_{n \to \infty} T(p)^n(p^{r-1}) \) exists in \( h^j \) for a sufficiently large \( r \) and is an idempotent of \( h^j \). The formation of \( e_j \) is compatible with the projective system \( (h^j_j) \). Thus, the projective limit \( e = \lim_{j} e_j \) gives an idempotent of \( h \). Write \( k_0 = eh \) and \( h_0^0(\mathbb{Z}_p) = eh_0(\mathbb{Z}_p) \), etc. The restriction of operators in \( h \) to the subspace \( S_k(\Gamma_1(N); \mathcal{O}_p) \) of \( S \) defines a morphism of \( h_0 \) onto \( h_0^0(\mathbb{Z}_p) \). Now we identify \( \Lambda \) with \( Z_p[[X]] \) by assigning the topological generator \( 1 + p \) to the unit \( 1 + X \) in \( Z_p[[X]] \). Then we have

**Theorem 1.** The \( \Lambda \)-algebra \( h_0 \) is free of finite rank over \( \Lambda \). Moreover, if \( k \geq 2 \), then the natural morphism \( h_0 \to h_0^0(\mathbb{Z}_p) \) defined above induces an isomorphism \( h_0/p_kh_0 \cong h_0^0(\mathbb{Z}_p) \), where

\[ p_k = p_k(X) = (1 + X) - (1 + p^k). \]

We can naturally identify \( S_k(\Gamma_1(N); \mathcal{O}) \) with the subspace of \( S_k(\Gamma_1(N)) \) consisting of all forms with algebraic Fourier coefficients. Thus, every normalized form belongs to \( S_k(\Gamma_1(N); \mathcal{O}) \), and the Hecke algebra \( h_0(\mathcal{O}_p) \) acts on the space \( S_k(\Gamma_1(N); \mathcal{O}_p) \), hence, on \( S_k(\Gamma_1(N); \mathcal{O}) \). Thus, we can consider the action of the idempotent \( e \) on any normalized form \( g \in S_k(\Gamma_1(N)) \). By the definition of \( e \), if \( g \) is a normalized form in \( S_k(\Gamma_1(N)) \), then

(3) \( g|_e = g \) if and only if the \( p \)-th Fourier coefficient of \( g \) does not vanish modulo \( p \).
It is known that every normalized form \( g \) in \( S_k(\Gamma_1(N)) \) is a linear combination of a unique primitive form \( g_0 \) in \( S_k(\Gamma_1(t)) \) for some divisor \( t \) of \( N \) and its transforms \( g_0(sz) \) with \( s \mid N/t \). We say that a normalized form \( g \) of \( S_k(\Gamma_1(N)) \) is ordinary (of level \( N \)) if \( g|e = g \) and either \( g \) is primitive of conductor \( N \) (i.e., a new form in \( S_k(\Gamma_1(N)) \)) or the associated primitive form \( g_0 \) is a new form of \( S_k(\Gamma_1(N/p)) \). Then we have

**Corollary 1.** The number of ordinary forms in \( S_k(\Gamma_1(N)) \) is independent of the weight \( k \) provided that \( k \geq 2 \).

For each primitive form \( f \), there seems to be many primes at which \( f \) (or more precisely, \( f|e \)) is ordinary. For example, take \( f = \Delta = e(z) \prod_{m=1}^{24} (1-e(nz))^2 \) of \( S_{12}(\text{SL}_2(\mathbb{Z})) \). Then, it can be verified numerically that \( \Delta|e \) is ordinary for \( p \) with \( 11 \leq p \leq 1021 \), but at the primes \( 0 < p < 11 \), \( \Delta|e \) vanishes.

We can now specify \( f_k \) in Question 1 by assuming \( f \) to be ordinary. Let \( L \) be the quotient field of \( A \) and put \( F = h_0 \otimes_L \). Then \( F \) is an Artin algebra over \( L \) by Theorem 1. Take a local ring \( K \) of \( F \). Then \( K \) is finite over \( L \). Decompose \( F = K \oplus A \) as an algebra direct sum, and let \( h_0(K) \) and \( h_0(A) \) be the images of \( h_0 \) in \( K \) and \( A \). The projection morphism of \( h_0 \) onto \( h_0(K) \) induces a morphism:

\[
h_k(\mathbb{Z}_p) \longrightarrow h_k^0(\mathbb{Z}_p) = h_0/\mathbb{Z}_p h_0 \longrightarrow h_0(K)/\mathbb{Z}_p h_0(K).
\]

By tensoring with \( \mathbb{Q}_p \), this induces

\[
\phi_k : h_k(\mathbb{Q}_p) \longrightarrow (h_0(K)/\mathbb{Z}_p h_0(K)) \otimes \mathbb{Q}_p.
\]

We say that the normalized form \( f \) belongs to \( K \) if the homomorphism \( \lambda_p \) of \( h_k(\mathbb{Q}_p) \) into \( K \) associated with \( f \) factors through \( \phi_k \). By Theorem 1, any normalized form with \( f|e = f \) always belongs to some local ring of \( F \).

**Theorem 2.** If the fixed normalized form \( f \) of weight \( k \) is ordinary and if \( k \geq 2 \), then \( f \) belongs to a unique local ring \( K \) of \( F \) which is a field. Moreover, for every \( k \geq 2 \), the number of normalized forms in \( S_k(\Gamma_1(N)) \) which belong to \( K \) is exactly the index \([K: L] \), and all such forms are ordinary.
Let $K$ be a local ring of $F$ to which $f$ belongs. We assume that

(4a) the normalized form $f$ is ordinary,

(4b) the weight $k$ of $f$ is greater than one,

(4c) $[K:L] = 1$.

Then, the ring $k_0(K)$ coincides with the subalgebra $\Lambda$ of $L$ ($= K$), because $k_0(K)$ is integral over $\Lambda$. Let $A(n;K)$ be the image of the $n$-th Hecke operator $T(n)$ of $k$ in $k_0(K) = \Lambda = Z_p[[X]]$. Then, an explicit form of the ordinary forms belonging to $K$ may be given by

**Corollary 2.** Let $n$ be an arbitrary integer greater than 1. Under the assumption (4a,b,c), the unique ordinary form $f_\xi$ of weight $\lambda$ belonging to $K$ has the following Fourier expansion:

$$f_\xi(z) = \sum_{n=1}^{\infty} A(n; (1+p)^\xi - 1) \omega(nz).$$

This means that the element $A(n; (1+p)^\xi - 1)$ of the field $\Omega$ is contained in $\bar{\Omega}$ which is a subfield of $C$, and gives the $n$-th Fourier coefficient of $f$. By Corollary 2, we see easily that

$$f = f_\xi \mod P \text{ for all } \xi \geq 2.$$

After succeeding in specifying $f_\xi$ as above, we are now ready to give a precise formulation of the answer of Question I:

**Theorem 3.** Assume the conditions (4a,b,c) and define a $\Lambda$-module by $C_0 = (k_0(K) \otimes k_0(\Lambda))/k_0$. Then there exists a non-zero power series $H(X)$ in $Z_p[[X]]$ such that $C_0 \cong \Lambda/H(X)\Lambda$. Moreover, there is a finite torsion $\Lambda$-module $C$ such that:

(i) $C_0$ can be embedded into $C$ as $\Lambda$-modules and the quotient $N/C_0$ has only finitely many elements (i.e. $C$ is pseudoisomorphic to $C_0$);

(ii) For each $\xi \geq 2$, there is an exact sequence:

$$0 \longrightarrow C_0(f_\xi) \longrightarrow C/P_\xi C \longrightarrow N/P_\xi N \longrightarrow 0$$

where $f_\xi$ is the unique ordinary form of weight $\lambda$ belonging to $K$.

Here are some remarks about Theorem 3. Certainly, the module $C$
cannot be uniquely determined, but one may conjecture that \( C_0 \) itself 
can be taken as \( C \) in Theorem 3. If this is true, the module of 
congruences \( C_p(f') \) will be completely described by the module \( C_0 \). A suf-
ficient condition for the conjecture can be given as follows : For \( \ell \geq 2 \), 
write \( h_\ell(K_p) = K_\ell \otimes A_\ell \) as an algebra direct sum for 
\( K_\ell = (K_0(K)/P_{\ell}K_0(K)) \otimes \mathbb{Z}_p \). 
and let \( h(A_\ell) \) be the image of \( h_\ell^0(\mathbb{Z}_p) \) in 
\( A_\ell \). Then we have

(5) If \( h(A_\ell) \) is integrally closed in \( A_\ell \) for at least one \( \ell \geq 2 \), 
then we can take \( C_0 \) as \( C \) in Theorem 3.

This gives us an effective method to check numerically the conjecture to 
be true in each special case. Anyway, we can at least conclude the follow-
ing facts:

(6a) if \( C_p(f) \neq 0 \), then \( C_p(f') \neq 0 \) for all \( \ell \geq 2 \);

(6b) if \( p^i \) annihilates \( N \) and if \( \ell = k \mod p^i \) (and \( \ell \geq k \geq 2 \)), then 
\( N/P_k N = N/P_{k-1} N \) as \( \mathbb{Z}_p \)-modules.

As a \( p \)-adic version of (2b), one may conjecture that the power series 
\( H(X) \) as in Theorem 3 interpolates the algebraic part of \( L(\ell,f_\ell) \). Namely, a canonical \( P \)-integral part of \( L(\ell,f_\ell) \) can be defined, similarly 
to the definition of the integer part of \( Z(\ell,f_\ell) \), and then we make

Conjecture. For all integers \( \ell \geq 2 \), the number \( H(1+p^{-1}) \) coincides 
with the canonical \( P \)-integral part of \( L(\ell,f_\ell) \) up to the multiple of 
\( p \)-adic units.

4 - Before stating some examples for the local ring \( K \) and the Iwasawa 
module \( C_0 \), we extend the action of \( \Gamma \) on \( H_0 \) to that of \( \Gamma \times (\mathbb{Z}/N\mathbb{Z})^\times \).

As easily seen, we have that

\[
g|T(q)^2 - T(q^2) = q^{k-1}g|_q \quad \text{for every} \quad g \in S_2(\Gamma_1(N)),
\]

where \( a \equiv b \equiv d \equiv 0 \mod N \) and

\[
(g|_q)(z) = \frac{(az+b)(cz+d)^{-2}}{(cz+d)^2} \quad \text{is the usual transform of} \quad g \quad \text{under} \quad a_q.
\]

This shows that the finite group \( (\mathbb{Z}/N\mathbb{Z})^\times \) acts on \( S_2(\Gamma_1(N);\mathbb{Q}_p) \) and 
also, on \( S \), hence on \( h_0 \). This action is explicitly given by

\[
g|q = \omega(q)^{2}g|_q \quad \text{for} \quad g \in S_2(\Gamma_1(N);\mathbb{Q}_p) \quad \text{and} \quad q \in (\mathbb{Z}/N\mathbb{Z})^\times.
\]
where $\omega$ is a Dirichlet character modulo $p$ such that $\omega(a) = a \mod p$. Suppose that $\#(\mathbb{Z}/\mathbb{N})^\times$ is prime to $p$ and let $\xi$ be a character of $(\mathbb{Z}/\mathbb{N})^\times$ with values in $\mathbb{Z}_p^\times$. Then the subspace $h_0(\xi)$ of $h_0$ on which $(\mathbb{Z}/\mathbb{N})^\times$ acts via $\xi$ is an algebra direct summand of $h_0$. By Theorem 1, if the weight $k$ is greater than 1, then

(7) $h_0(\xi)/P^k h_0(\xi)$ is isomorphic to the Hecke algebra of the space $S_\xi(\Gamma_0(N), \omega^{-k}, \xi; \mathbb{Q}_p)[e].$

It is well known that:

(8a) The idempotent $e$ sends $S_\xi(\Gamma_0(N/p), \mathbb{Q}_p)$ surjectively to $S_\xi(\Gamma_0(N); \xi; \mathbb{Q}_p)[e]$ if $\xi$ is defined modulo $N/p$;

(8b) If $g$ is a primitive form in $S_\xi(\Gamma_1(N); \mathbb{Q})$ whose $p$-th Fourier coefficient is non-vanishing modulo $p$, $g|e$ does not vanish. Moreover, if the conductor of $g$ is $N/p$ or $N$, then $g|e$ is a constant multiple of an ordinary form.

Now, we start with a simplest example of $K$ with $[K:L] = 1$. We take $p$ as the level $N$ and consider the unique primitive form $\Delta$ of $S_{12}(\mathbb{SL}_2(\mathbb{Z}))$. Then, if the $p$-th Fourier coefficient of $\Delta$ does not vanish modulo $p$ (as already mentioned, this is at least true for primes $p$ with $11 \leq p \leq 1021$), then $\Delta|e$ is a constant multiple of an ordinary form $f$. Thus, we know from (8a) that $f$ is a unique ordinary form in $S_{12}(\Gamma_0(p); \mathbb{Q}_p)$. Then, (7) shows that $h_0(\mathbb{Q}_p^{12}) \otimes \Lambda$. Certainly, the local ring $K$ corresponding to the direct summand $h_0(\mathbb{Q}^{12})$ of $h_0$ is isomorphic to $L$.

Next, we shall associate a local ring $K$ of $F$ with an imaginary quadratic field $M$ with discriminant $-d$. We have to assume that

(9) the prime $p$ is split in $M$.

For simplicity, we also assume the class number of $M$ to be one. Put $p = P \cap M$. Then, the prime $p$ is decomposed in $M$ as $p = pP$, and the closure $M_p$ of $M$ in $\mathbb{Q}$ coincides with $\mathbb{Q}_p$. Write $R$ for the ring of integers in $M$, and denote by $w$ the number of roots of unity in $R$. Let $a$ be an integer with $0 < a < p-1$ and $a \equiv 1 \mod w$. It is known by Hecke that the formal Fourier series

$$f_\xi(z) = \frac{1}{w} \sum_{\omega \in R - p} \omega^{a-\xi}(x) x^{k-1} e(xz)$$

for $k \geq 2$

is in fact the Fourier expansion of an ordinary form in $S_\xi(\Gamma_0(dp), \omega^{a-\xi}; \mathbb{Q})$. 

where \( \chi(q) \) is the Legendre symbol \( \left( \frac{r}{q} \right) \) and \( \omega \) is a character of \( R \) with \( \omega(x) = x \mod P \).

**Theorem 4.** Take \( dp \) as the level \( N \). Then, for each integer \( a \) as above, there is a unique local ring \( K \) of \( F \) to which \( f_a \) belongs for all \( \ell \geq 2 \). Moreover, we have \(|K:F|=1\) and for every prime \( q \), the power series \( A(q;X) \) in Corollary 2 for this \( K \) is given by

\[
A(q;X) = \begin{cases} 
\omega^a(r)^{-1}(1+X)^{\log(\langle r \rangle)/\log(u)} + a(r)^{-1}(1+X)^{\log(\langle r \rangle)/\log(u)}, & \text{if } q = r^k \text{ for } r \in R, \\
\omega^a(r)^{-1}(1+X)^{\log(\langle r \rangle)/\log(u)}, & \text{if } q = r^2 \text{ for } r \in R, \\
0, & \text{otherwise},
\end{cases}
\]

where \( u = 1+p, \langle r \rangle = r_0(r)^{-1}, (1+X)^S = \sum_{n=0}^{\infty} \binom{S}{n} X^n \in \mathbb{Z}_p[[X]] \) with the binomial polynomial \( \binom{S}{n} \) in \( s \) and \( \log \) denotes the \( p \)-adic logarithm.

By using this theorem, we can give several examples of non-trivial torsion modules \( C_0 \) as in Theorem 3. By (7) and (8a, b), if the local ring \( K \) corresponds to an integer \( a \) with \( 0 < a < p-1 \) and \( a = 1 \mod w \), we can get some information of \( K \) by examining the space \( S_k(f_0(d), \chi) \) for \( k = a \mod p-1 \) instead of \( S_k(f_0(dp), \chi) \). We take \( 7 \equiv 0 \pmod{7} \). Here, we give a table, due to the calculation done by Y. Maeda, of primes \( p \) and the number \( a \) at which \( K \) as in Theorem 4 has non-trivial module \( C_0 \) of congruences.

<table>
<thead>
<tr>
<th>( p )</th>
<th>( a )</th>
<th>( \dim (S_k(f_0(7), \chi)) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>23</td>
<td>11</td>
<td>5 = 1 + 4</td>
</tr>
<tr>
<td>79</td>
<td>13</td>
<td>7 = 1 + 6</td>
</tr>
<tr>
<td>191</td>
<td>9</td>
<td>5 = 1 + 4</td>
</tr>
<tr>
<td>331</td>
<td>13</td>
<td>7 = 1 + 6</td>
</tr>
</tbody>
</table>

Here are some remarks about the table. The expression, for example, 5 = 1 + 4 in the last column at the line of \( p = 23 \) means that the Hecke algebra of \( S_1(f_0(7), \chi) \) over \( \mathbb{Q} \) splits into the sum of two fields of degree 1 and 4 over \( \mathbb{Q} \). The one dimensional component of the Hecke algebra of each weight listed above corresponds to the imaginary quadratic
field $\mathbb{Q}(\sqrt{-7})$ as in Theorem 4. In the cases listed above, one can check numerically (cf. (5)) that the module $C_0$ can be taken as $C$ in Theorem 3. It should be also noted that the primes in the table are irregular for $\mathbb{Q}(\sqrt{-7})$ in the sense of [3, paragraph 1].

Finally, we shall give a numerical example of the local ring $K$ with the following properties:

(10a) $[K:L]=2$;

(10b) For any finite extension $E$ of $\mathbb{Q}_p$, $K \otimes_{\mathbb{Q}_p} E$ is a field (i.e. $K$ is not a scalar extension of $L$).

We take $13$ as $p$ and $39=3\times13$ as the level $N$. Let $\xi$ be the character of $(\mathbb{Z}/N\mathbb{Z})^\times$ such that $\xi(m) = (\frac{m}{3})\omega(m)$, where $(\frac{m}{3})$ is the Legendre symbol and $\omega(x) = x \mod p$. Since $\xi$ is $\mathbb{Z}_p$-rational, we can decompose $h_0 = h_0(\xi) \otimes \mathbb{Q}$ as an algebra direct sum. Let $t$ be an integer with $t \equiv 1 \mod 12$ and $t \geq 2$. Then, by (7) and (8a), the algebra $h_0(\xi)/P_{h_0}(\xi)$ is the Hecke algebra over $\mathbb{Z}_p$ of the space $S_{k_0}(\mathbb{F}_p(3),\chi;\mathbb{Q}_p)$, where $\chi(m)$ is the Legendre symbol $(\frac{m}{3})$. Here, we list, from the calculation done by Y. Maeda, the characteristic polynomial $P(X)$ of $T(2)$ on $S_{k_0}(\mathbb{F}_p(3),\chi)$ for each $k=13, 25$ and $k=37$.

(11a) $k=13$: $P(X) = X^{13}(x^2)$ with

$k=25$: $P(X) = X^{25}(x^2)$ with $F_{25}(X) = x^3 + 82005048x^2 + 1029235783453696x + 8525473984011546132400$,

the discriminant of $F_{25} = 2^{26} \cdot 3^{26} \cdot 5^3 \cdot 7^4 \cdot 13^2 \cdot 271 \cdot 20753 \cdot 618707$,

the constant term of $F_{25} = 2^{23} \cdot 3^{14} \cdot 5 \cdot 7 \cdot 13 \cdot 457003$;

$k=37$: $P(X) = X^{37}(x^2)$.

The polynomial $F_{37}(X)$ is of degree 5 and the coefficients of $x^1$ for $F_{37}$ and the discriminant $D$ of $F_{37}$ are given as follows:
\begin{align*}
\begin{array}{c|l}
\text{(11b)} & \text{i} \\
0 & 2^{58} \cdot 3^{22} \cdot 5^2 \cdot 7 \cdot 11^3 \cdot 13^2 \cdot 6311 \cdot 32567^2 \cdot 1304543 \\
1 & 286049606581241273364345057869224571350648480 \\
2 & 8830719713450547606263642355400704 \\
3 & 10938184596941655267328 \\
4 & 561197528712 \\
\end{array}
\end{align*}

D \quad 2^{150} \cdot 3^{92} \cdot 5^{12} \cdot 7^7 \cdot 3413 \cdot \text{a big factor of 112 digits}

The polynomials \( F_{13}, F_{25}, F_{37} \) are irreducible over \( \mathbb{Q} \) and every factor less than \( 10^{10} \) of the prime factorization given above is a prime, and even if the factor exceeds \( 10^{10} \), it is not divisible by primes less than \( 10^5 \). Now we give the factorization of \( F_{\mathfrak{L}}(x^2) \mod 13 \) and \( \mod 13^3 \):

\begin{align*}
\text{(12a)} & \quad F_{25}(x^2) : x^2(x^2+7)(x+8)(x+5) \mod 13, \\
& \quad G_1(x)G_2(x)(x+1984)(x+213) \mod 13^3, \\
& \quad (1984 \equiv 8 \mod 13, \quad 213 \equiv 5 \mod 13),
\end{align*}

where \( G_1 \) and \( G_2 \) are irreducible quadratic polynomials over \( \mathbb{Z}/13^3\mathbb{Z} \).

\begin{align*}
\text{(12b)} & \quad F_{37}(x^2) : x^2(x^2+7)(x+8)(x+5)(x+6)(x+7)(x+10)(x+3) \mod 13, \\
& \quad G'_1(x)G'_2(x)(x-1643)(x-1643)(x-1749)(x-448)(x-1693)(x-504) \mod 13^3
\end{align*}

where \( G'_1 \) and \( G'_2 \) are irreducible over \( \mathbb{Z}/13^3\mathbb{Z} \), and all the factors of \( F_{37} \mod 13^3 \) correspond to those \( \mod 13 \) in order.

The factor \( X \) in \( P(X) \) corresponds to the ordinary forms belonging to the local ring \( \mathcal{M} \) associated with \( \mathbb{Q}(\sqrt{-3}) \) as in Theorem 4 for \( a=1 \). The factor \( x^2 \) in the factorization of \( F_{\mathfrak{L}}(x) \mod 13 \) corresponds to the two primitive forms congruent with the ordinary form belonging to \( \mathcal{M} \) modulo a prime ideal \( \mathfrak{p} \) over \( \mathfrak{p} \) (cf. [1, (8.11)]). Thus, the module \( C_0 \) for \( \mathcal{M} \) is non-trivial.

Since \( \dim S_{13}(\Gamma_0(3), \chi) = 3 \) and since every primitive form in this space is known to be congruent modulo \( \mathfrak{p} \) with each other, the rank of \( h_0(\xi) \) over \( \mathbb{A} \) is 3 by Theorem 1. Thus, we can decompose \( h_0(\xi) \otimes_{\mathbb{A}} \mathbb{L} = \mathbb{M} \otimes K \) as an algebra direct sum. We claim that \( K \) is a field with \( [K: \mathbb{L}] = 2 \).

The ring \( K \) is semi-simple by Theorem 2. Then \( K \) must be a field, because, \( K_{13} = (h_0(\xi)/P_{13}h_0(\xi)) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \) is isomorphic to the field
$Q_p[X]/(X^2+8424)$. Since 8424 is divisible by 13 exactly, $K_{13}/Q_p$ is a ramified extension. Thus, if $K$ is split over a finite extension $E$ of $Q_p$ (i.e. $K \otimes Q_p E \cong (L \otimes Q_p E)^{2}$), then $E/Q_p$ must be a ramified extension, and for any weight $\xi$, $K_\xi = (h_0(k)/p \cdot h_0(k)) \otimes Q_p$ must ramify over $Q_p$. We shall show that the extension $K_{37}/Q_p$ is unramified. Then, $(10a,b)$ will be proved for the field $K$. This unramifiedness is obvious from $(11b)$, because the constant term of $F_{37}(X)$ is divisible by $13^2$ exactly. The factorization of $F_{37}$ mod $13^3$ shows that $K_{37}$ is a quadratic field unramified over $Q_p$.

It may be noted that by $(12a,b)$, we can conclude that for the ordinary forms $f_k$ belonging to $M$,

$$C_p(f_{13}) \cong C_p(f_{25}) \cong Z/13Z$$

and it is quite plausible that $C_p(f_{37}) \cong Z/13^2Z$.

It is an interesting problem to determine when the local rings of $F$ satisfy $(10a,b)$. 
BIBLIOGRAPHIE


H. Hida
Department of Mathematics
Faculty of Science
Hokkaido University
Sapporo 060, Japan

and

Université Paris-Sud
Mathématique Bât 425
91405 Orsay cedex
France