PM 59
Séminaire de Théorie des Nombres
Paris 1983–84

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 ψ be a Dirichlet character modulo N. Take a holomorphic cusp form $f\ (\neq 0)$ on the upper half complex plane of weight k for the congruence subgroup $\Gamma_0(N)$ of $SL_2(Z)$ with character ψ. Write its Fourier expansion as

$$f(z) = \sum_{n=1}^{\infty} a(n)e(nz) \qquad (e(z) = \exp(2\pi iz))$$

and suppose that $f|T(n) = a(n)f$ for all Hecke operators $T(n)$ 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 ψ (resp. for the congruence subgroup $\Gamma_1(N)$ of $\Gamma_0(N)$). A prime ideal P of the ring of all algebraic integers in C and also its restriction $p = P \cap Z$ to Z are said to be a congruence prime of f if the following conditions are satisfied :

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

$f \equiv g \bmod P$ (i.e. $a(n) \equiv b(n) \bmod P$ *for all* n);

(1b) *the normalized form* g *is different from any conjugates*
$f^{\sigma}(z) = \sum_{n=1}^{\infty} a(n)^{\sigma} e(nz)$ *of* f *under automorphisms* σ *of* 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 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 λ of h_k into C via $f|T = \lambda(T)f$ for $T \in h_k$. As is well known, the scalar extension $h_k(Q) = h_k \otimes_Z Q$ is an Artin algebra over Q, and hence, λ has values in the field $\overline{Q}$ consisting of all algebraic numbers of C. Then, we can find a unique local ring K of $h_k(Q)$ and a homomorphism λ' of K into $\overline{Q}$ which makes the following diagram commutative :

$$\begin{array}{ccc} \lambda : h_k(Q) & \longrightarrow & \overline{Q} \subset C \\ \downarrow & \nearrow \lambda' & \\ K & & \end{array}$$

Decompose $h_k(Q)$ into an algebra direct sum $K \oplus A$, 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 :

$$\begin{array}{ccc} h_k(Q) & = & K \oplus A \\ \cup & & \cup \\ h_k & \subset & h(K) \oplus h(A). \end{array}$$

Define a module $C(f)$ by

$$C(f) = (h(K) \oplus h(A))/h_k,$$

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*

<u>congruence prime of</u> 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

$$L(s,f) = \Big(\sum_{\substack{n=1\\(n,N)=1}}^{\infty} n^{2k-2-2s}\Big)\Big(\sum_{n=1}^{\infty} \overline{\psi}(n)a(n^2)n^{-s}\Big)$$

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

We consider the product $Z(s,f)=\prod_\sigma L(s,f^\sigma)$ 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 <u>divides the order of</u> C(f) <u>if and only if</u> p <u>divides the canonical integer part of</u> 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 result in this direction can be found in [3, § 3].

2 - Let $S_k(\Gamma_1(N);Q)$ 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 $h_k(Q)$. For any extension F over Q, put

$$S_k(\Gamma_1(N);F) = S_k(\Gamma_1(N);Q)\otimes_Q F.$$

Then, the Hecke algebra $h_k(F)=h_k\otimes_Z F$ 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 ψ has values in F, we denote by $S_k(\Gamma_0(N),\psi;F)$ the subspace of $S_k(\Gamma_1(N);F)$ consisting of all forms transformed under $\Gamma_0(N)$ via the character ψ.

We hereafter fix a prime $p \geq 5$ and a prime ideal P over p in the ring of all algebraic integers in C. Let Ω be the quotient field of the P-adic completion of this ring. By continuity, the morphism $\lambda : h_k(Q) \longrightarrow \overline{Q} \subset \Omega$ can be extended to a homomorphism $\lambda_P : h_k(Q_p) \to \Omega$. Then λ_P factors through a unique local ring K_P of $h_k(Q_p)$ (which is a direct summand of $K \otimes_Q Q_p$). Decompose $h_k(Q_p) = K_p \oplus A_p$ as an algebra direct sum and let $h(K_p)$ and $h(A_p)$ be the natural images of $h_k(Z_p) = h_k \otimes_Z Z_p$ in K_p and A_p. Put

$$C_p(f) = (h(K_p) \oplus h(A_p))/h_k(Z_p).$$

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_ℓ in $S_\ell(\Gamma_1(N))$ for each weight ℓ with $f \equiv f_\ell \bmod P$. Then, we ask the following questions.

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

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

Under the hypothesis that $a(p) \not\equiv 0 \bmod P$ and with some additional assumptions, the answer to question I is affirmative, and $C_p(f_\ell)$ depends p-adic analytically on ℓ. The meaning of the analycity 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 $Z_p/H((1+p)^\ell-1)Z_p$ into $C_p(f_\ell)$ with finite kernel and cokernel, whose orders are bounded independtly on ℓ. Furthermore, we know that $C_p(f_\ell) \simeq C_p(f_{\ell'})$ if ℓ and ℓ' 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_ℓ somehow, because f_ℓ may not be uniquely determined only by the congruence $f \equiv f_\ell \bmod P$. To accomplish this task, we are naturally led to consider some bigger Hecke algebras which act on f and f_ℓ for all ℓ simultaneously. To define this, we assume that

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

Then, we put

$$S^j = \bigoplus_{\ell=1}^{j} S_\ell(\Gamma_1(N);Q_p) \quad \text{for} \quad j > 0$$

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^i $(j > i)$ induces a morphism of h^j onto h^i, which defines a projective system $\{h^j\}_j$. Forming the projective limit $h = \varprojlim_j h^j$, we obtain a compact ring acting on

$$S = \varprojlim_{j} S^j = \bigoplus_{\ell=1}^{\infty} S_\ell(\Gamma_1(N);Q_p).$$

Our key idea is to consider the algebra h as an algebra over the Iwasawa algebra Λ for the multiplicative group $\Gamma = 1+pZ_p$. Namely, let Γ act on $S_\ell(\Gamma_1(N);Q_p)$ via $g|\gamma = \gamma^\ell g$ 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 $q(T(q)^2 - T(q^2))$ for each prime $q \equiv 1 \bmod N$ in h gives the action of q on S as an element of Γ. Since such primes are dense in Γ, h may be regarded as a continuous Γ-module, and hence, is an algebra over $\Lambda = \varprojlim_{n} Z_p[\Gamma/1+p^nZ_p]$.

The Λ-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 $e_j = \lim_{n\to\infty} T(p)^{p^{rn}(p^r-1)}$ 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 $e = \varprojlim_{j} e_j$ gives an idempotent of h. Write $h_0 = eh$ and $h^0_\ell(Z_p) = eh_\ell(Z_p)$, etc. The restriction of operators in h to the subspace $S_\ell(\Gamma_1(N);Q_p)$ of S defines a morphism of h_0 onto $h^0_\ell(Z_p)$. Now we identify Λ with $Z_p[[X]]$ by assigning the topological generator $1+p\in\Gamma$ to the unit $1+X$ in $Z_p[[X]]$. Then we have

<u>Theorem 1</u>. The Λ-algebra h_0 is free of finite rank over Λ. Moreover, if $\ell\geq 2$, then the natural morphism : $h_0 \longrightarrow h^0_\ell(Z_p)$ defined above induces an isomorphism $h_0/P_\ell h_0 \simeq h^0_\ell(Z_p)$, where

$$P_\ell = P_\ell(X) = (1+X) - (1+p)^\ell \in \Lambda.$$

We can naturally identify $S_\ell(\Gamma_1(N);\bar{Q})$ with the subspace of $S_\ell(\Gamma_1(N))$ consisting of all forms with algebraic Fourier coefficients. Thus, every normalized form belongs to $S_\ell(\Gamma_1(N);\bar{Q})$, and the Hecke algebra $h_\ell(Q_p)$ acts on the space $S_\ell(\Gamma_1(N);Q_p)$, hence, on $S_\ell(\Gamma_1(N);\Omega)$. Thus, we can consider the action of the idempotent e on any normalized form g in $S_\ell(\Gamma_1(N))$. By the definition of e, if g is a normalized form in $S_\ell(\Gamma_1(N))$, then

(3) $g|e = g$ <u>if and only if the</u> p-th <u>Fourier coefficient of</u> g <u>does not vanishes</u> modulo P.

It is known that every normalized form g in $S_\ell(\Gamma_1(N))$ is a linear combination of a unique primitive form g_0 in $S_\ell(\Gamma_1(t))$ for some divisor t of N and its transforms $g_0(sz)$ with $s|N/t$. We say that a normalized form g of $S_\ell(\Gamma_1(N))$ is ordinary (of level N) if $g|e = g$ and either g is primitive of conductor N (i.e. a new form in $S_\ell(\Gamma_1(N))$) or the associated primitive form g_0 is a new form of $S_\ell(\Gamma_1(N/p))$. Then we have

Corollary 1. The number of ordinary forms in $S_\ell(\Gamma_1(N))$ is independent of the weight ℓ provided that $\ell \geq 2$.

For each primitive form f, there seems to be many primes at which f (or more precisely, $f|e$) is ordinary. For example, take $f = \Delta = e(z) \prod_{n=1}^{\infty} (1-e(nz))^{24}$ of $S_{12}(SL_2(Z))$. 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_ℓ in Question I by assuming f to be ordinary . Let L be the quotient field of Λ and put $F = h_o \otimes_\Lambda L$. 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 $h_o(K)$ and $h_o(A)$ be the images of h_o in K and A. The projection morphism of h_o onto $h_o(K)$ induces a morphism :

$$h_\ell(Z_p) \longrightarrow h_\ell^o(Z_p) = h_o/P_\ell h_o \longrightarrow h_o(K)/P_\ell h_o(K).$$

By tensoring Q_p, this induces

$$\Phi_\ell : h_\ell(Q_p) \longrightarrow (h_o(K)/P_\ell h_o(K)) \otimes_{Z_p} Q_p.$$

We say that the normalized form f belongs to K if the homomorphism λ_p of $h_k(Q_p)$ into Ω associated with f factors through Φ_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 $\ell \geq 2$, the number of normalized forms in $S_\ell(\Gamma_1(N))$ 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 $h_0(K)$ coincides with the subalgebra Λ of L (= K), because $h_0(K)$ is integral over Λ. Let $A(n;X)$ be the image of the n-th Hecke operator $T(n)$ of h in $h_0(K) = \Lambda = Z_p[[X]]$. Then, an explicit form of the ordinary forms belonging to K may be given by

Corollary 2. Let ℓ be an arbitrary integer greater than 1. Under the assumption (4a,b,c), the unique ordinary form f_ℓ of weight ℓ belonging to K has the following Fourier expansion :

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

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

$$f \equiv f_\ell \bmod P \quad \text{for all} \quad \ell \geq 2.$$

After succeeding in specifying f_ℓ 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 Λ-module by $C_0 = (h_0(K) \oplus h_0(A))/h_0$. Then there exists a non-zero power series $H(X)$ in $Z_p[[X]]$ such that $C_0 \simeq \Lambda/H(X)\Lambda$. Moreover, there is a finite torsion Λ-module C such that :

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

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

$$0 \longrightarrow C_p(f_\ell) \longrightarrow C/P_\ell C \longrightarrow N/P_\ell N \longrightarrow 0$$

where f_ℓ is the unique ordinary form of wieght ℓ 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 $C_p(f_\ell)$ will be completely described by the module C_0. A sufficient condition for the conjecture can be given as follows : For $\ell \geq 2$, write $h_\ell(Q_p) = K_\ell \oplus A_\ell$ as an algebra direct sum for $K_\ell = (h_0(K)/P_\ell h_0(K)) \otimes_{Z_p} Q_p$, and let $h(A_\ell)$ be the image of $h_\ell^0(Z_p)$ in A_ℓ. Then we have

(5) <u>If</u> $h(A_\ell)$ <u>is integrally closed in</u> A_ℓ <u>for at least one</u> $\ell \geq 2$, <u>then we can take</u> C_0 <u>as</u> C <u>in Theorem</u> 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 following facts :

(6a) <u>if</u> $C_p(f) \neq 0$, <u>then</u> $C_p(f_\ell) \neq 0$ <u>for all</u> $\ell \geq 2$;

(6b) <u>if</u> p^i <u>annihilates</u> N <u>and if</u> $\ell \equiv k \bmod p^i$ (<u>and</u> $\ell \geq k \geq 2$), <u>then</u> $N/P_k N \simeq N/P_\ell N$ <u>as</u> Z_p<u>-modules</u>.

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

<u>Conjecture</u>. 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 Γ on h_0 to that of $\Gamma \times (Z/NZ)^\times$. As easily seen, we have that

$$g|(T(q)^2 - T(q^2)) = q^{\ell-1} g|\sigma_q \quad \text{for every} \quad g \in S_\ell(\Gamma_1(N)),$$

where $\sigma_q = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ with $d \equiv q \bmod N$ and $(g|\sigma_q)(z) = g(\frac{az+b}{cz+d})(cz+d)^{-\ell}$ is the usual transform of g under σ_q. This shows that the finite group $(Z/NZ)^\times$ acts on $S_\ell(\Gamma_1(N);Q_p)$ and also, on S, hence on h_0. This action is explicitly given by

$$g|q = \omega(q)^\ell g|\sigma_q \qquad (g \in S_\ell(\Gamma_1(N);Q_p) \text{ and } q \in (Z/NZ)^\times),$$

where ω is a Dirichlet character modulo p such that $\omega(a) \equiv a \bmod P$. Suppose that $\#(Z/NZ)^{\times}$ is prime to p and let ξ be a character of $(Z/NZ)^{\times}$ with values in $Z_p^{\times}$. Then the subspace $h_0(\xi)$ of h_0 on which $(Z/NZ)^{\times}$ acts via ξ is an algebra direct summand of h_0. By Theorem 1, if the weight ℓ is greater than 1, then

(7) $h_0(\xi)/P_\ell h_0(\xi)$ is isomorphic to the Hecke algebra of the space $S_\ell(\Gamma_0(N),\xi\omega^{-\ell};Q_p)|e$.

It is well known that :

(8a) The idempotent e sends $S_\ell(\Gamma_0(N/p),\xi;Q_p)$ surjectively to $S_\ell(\Gamma_0(N);\xi;Q_p)|e$, if ξ is defined modulo N/p;

(8b) If g is a primitive form in $S_\ell(\Gamma_1(N);\Omega)$ 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 Δ of $S_{12}(SL_2(Z))$. Then, if the p-th Fourier coefficient of Δ does not vanish modulo p (as already mentioned, this is at least true for primes p with $11 \le p \le 1021$), 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 $S_{12}(\Gamma_0(p);Q_p)$. Then, (7) shows that $h_0(\omega^{12}) \simeq \Lambda$. Certainly, the local ring K corresponding to the direct summand $h_0(\omega^{12})$ 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 $p = p\bar{p}$, and the closure M_p of M in Ω coincides with 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 $a \equiv 1 \bmod w$. It is known by Hecke that the formal Fourier series

$$f_\ell(z) = \frac{1}{w} \sum_{w \in R-p} \omega^{a-\ell}(x)x^{\ell-1}e(x\bar{x}z) \qquad \text{for } \ell \ge 2$$

is in fact the Fourier expansion of an ordinary form in $S_\ell(\Gamma_0(dp),\omega^{a-\ell}\chi)$, where $\chi(q)$ is the Legendre symbol $(\frac{-d}{q})$ and ω is a character of R with $\omega(x) \equiv x \bmod P$.

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_ℓ belongs for all $\ell \geq 2$. Moreover, we have $[K:L]=1$ and for every prime q, the power series $A(q;X)$ in Corollary 2 for this K is given by

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

where $u = 1+p$, $\langle r\rangle = r\omega(r)^{-1}$, $(1+X)^s = \sum_{n=0}^{\infty} \binom{s}{n} X^n \in Z_p[[X]]$ 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 $a \equiv 1 \bmod w$, we can get some information of K by examining the space $S_k(\Gamma_0(d),\chi)$ for $k \equiv a \bmod p-1$ instead of $S_k(\Gamma_0(dp),\chi)$. We take 7 as d (i.e. $M = Q(\sqrt{-7})$). 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.

p	a	dim $(S_a(\Gamma_0(7),\chi))$
23	11	5 = 1 + 4
79	13	7 = 1 + 6
191	9	5 = 1 + 4
331	13	7 = 1 + 6

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 $S_{11}(\Gamma_0(7),\chi)$ over Q splits into the sum of two fields of degree 1 and 4 over Q. The one dimensional component of the Hecke algebra of each weight listed above corresponds to the imaginary quadratic field $Q(\sqrt{-7})$ 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 $Q(\sqrt{-7})$ 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 Q_p, $K \otimes_{Q_p} E$ is a field (i.e. K is not a scalar extension of L).

We take 13 as p and $39 = 3 \cdot 13$ as the level N. Let ξ be the character of $(Z/NZ)^{\times}$ such that $\xi(m) = (\frac{m}{3})\omega(m)$, where $(\frac{m}{3})$ is the Legendre symbol and $\omega(x) \equiv x \bmod P$. Since ξ is Z_p-rational, we can decompose $h_0 = h_0(\xi) \oplus k$ as an algebra direct sum. Let ℓ be an integer with $\ell \equiv 1 \bmod 12$ and $\ell \geq 2$. Then, by (7) and (8a), the algebra $h_0(\xi)/P_\ell h_0(\xi)$ is the Hecke algebra over Z_p of the space $S_\ell(\Gamma_0(3),\chi;Q_p)|e$, 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 $S_\ell(\Gamma_0(3),\chi)$ for each $\ell = 13$, 25 and $\ell = 37$.

(11a) $\ell = 13 : P(X) = XF_{13}(X^2)$ with

$\ell = 25 : P(X) = XF_{25}(X^2)$ with $F_{25}(X) = X^3 + 82005048X^2 +$

$F_{25}(X) = X^3+82005048X^2+1829235783453696X+852547398401154613248O$,

the discriminant of $F_{25} = 2^{26}\cdot 3^{26}\cdot 5^3\cdot 7^4\cdot 73\cdot 271\cdot 20753\cdot 618707$,

the constant term of $F_{25} = 2^{23}\cdot 3^{14}\cdot 5\cdot 7\cdot 13\cdot 467003$;

$\ell = 37 : P(X) = XF_{37}(X)$.

The polynomial $F_{37}(X)$ is of degree 5 and the coefficients of X^i for F_{37} and the discriminant D of F_{37} are given as follows :

(11b)

i	
0	$2^{58} \cdot 3^{22} \cdot 5^2 \cdot 7 \cdot 11^3 \cdot 13^2 \cdot 6311 \cdot 32587^2 \cdot 1304543$
1	286049606581241273364343505789224571350548480
2	8830719713450547606263642355400704
3	109381854596941655267328
4	561197528712
D	$2^{150} \cdot 3^{92} \cdot 5^{12} \cdot 7^7 \cdot 3413 \cdot a$ big factor of 112 digits

The polynomials F_{13}, F_{25}, F_{37} are irreducible over 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 $F_\ell(X^2)$ mod 13 and mod 13^3:

(12a) $F_{25}(X^2)$: $X^2(X^2+7)(X+8)(X+5)$ mod 13,

$G_1(X)G_2(X)(X+1984)(X+213)$ mod 13^3,

$(1984 \equiv 8 \bmod 13,\ \ 213 \equiv 5 \bmod 13)$,

where G_1 and G_2 are irreducible quadratic polynomials over $Z/13^3Z$.

(12b) $F_{37}(X^2)$: $X^2(X^2+7)(X+8)(X+5)(X+6)(X+7)(X+10)(X+3)$ mod 13,

$G_1'(X)G_2'(X)(X-1643)(X-554)(X-1749)(X-448)(X-1693)(X-504)$ mod 13^3

where G_1' and G_2' are irreducible over $Z/13^3Z$, 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 M associated with $Q(\sqrt{-3})$ as in Theorem 4 for $a = 1$. The factor X^2 in the factorization of $F_\ell(X)$ mod 13 corresponds to the two primitive forms congruent with the ordinary form belonging to M modulo a prime ideal P over 13 (cf. [1, (8.11)]). Thus, the module C_0 for 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 P with each other, the rank of $h_0(\xi)$ over Λ is 3 by Theorem 1. Thus, we can decompose $h_0(\xi) \otimes_\Lambda L = M \oplus K$ as an algebra direct sum. We claim that K is a field with $[K:L] = 2$. The ring K is semi-simple by Theorem 2. Then K must be a field, because, $K_{13} = (h_0(K)/P_{13}h_0(K)) \otimes_{Z_p} Q_p$ 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. $K \otimes_{Q_p} E \simeq (L \otimes_{Q_p} E)^2$), then E/Q_p must be a ramified extension, and for any weight ℓ, $K_\ell = (h_0(K)/P_\ell h_0(K)) \otimes_{Z_p} Q_p$ 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_ℓ belonging to M,

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

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

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

BIBLIOGRAPHIE

[1] H. Hida.- Congruences of cusp forms and special values of their zeta functions, Inventiones Math. 63 (1981), 225-261.

[2] H. Hida.- On congruence divisors of cusp forms as factors of the special values of their zeta functions, Inventiones Math. 64 (1981), 221-262.

[3] H. Hida.- Kummer's criterion for the special values of Hecke L-functions of imaginary quadratic fields and congruences among cusp forms, Inventiones Math. 66 (1982), 415-459.

[4] K.A. Ribet.- Mod p Hecke operators and congruences between modular forms, Inventiones Math. 71 (1983), 193-205.

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

and

Université Paris-Sud
Mathématique Bât 425
91405 Orsay cedex
France