ℓ-adic properties of certain modular forms

By Hyunsuk MOON [*)] and Yuichiro TAGUCHI [**)]

(Communicated by Shigefumi MORI, M.J.A., Sept. 12, 2006)

Abstract: Nilpotence modulo powers of 3, 5 and 7 is proved for Hecke operators on the space of certain modular forms, and is applied to the arithemtic of quadratic forms and Fourier coefficients of modular forms.

Key words: Modular form; Hecke operator; mod ℓ Galois representation; Serre's ε-Conjecture.

In this paper, we prove the nilpotence modulo powers of 3, 5 and 7 of the action of the Hecke algebra on the space of certain modular forms. This extends Theorems 1.1 and 1.2 of [11], in which the nilpotence was proved modulo powers of 2. For a subring $\mathcal{O}$ of the complex number field $\mathbf{C}$, we denote by $M_k(\Gamma_0(M),\varepsilon;\mathcal{O})$ (resp. $S_k(\Gamma_0(M),\varepsilon;\mathcal{O})$) the $\mathcal{O}$-module of modular forms (resp. cusp forms) of integer weight k and Nebentypus character $\varepsilon:(\mathbf{Z}/M\mathbf{Z})^\times \to \mathcal{O}^\times$ whose Fourier coefficients lie in $\mathcal{O}$. Let $q=e^{2\pi\sqrt{-1}z}$. Our main result is:

Theorem 1. *Let $k\geq 1$ be a positive integer. Let (ℓ,N) be a pair of integers which is either $(3,4)$, $(5,2)$ or $(7,1)$, and $a\geq 0$ a non-negative integer. Let $\varepsilon:(\mathbf{Z}/\ell^a N\mathbf{Z})^\times\to\mathbf{C}^\times$ be a Dirichlet character. Let L be an algebraic number field of finite degree over $\mathbf{Q}$, with ring of integers $\mathcal{O}_L$. Let λ be a prime ideal of $\mathcal{O}_L$ lying above ℓ, and denote by $\mathcal{O}_{L,\lambda}$ the localization of $\mathcal{O}_L$ at λ. Then there exist integers $c\geq 0$ and $e\geq 1$, depending only on k, ℓ, N, a, ε, L and λ, such that for any modular form $f(z)=\sum_{n=0}^{\infty}a(n)q^n\in M_k(\Gamma_0(\ell^a N),\varepsilon;\mathcal{O}_{L,\lambda})$, any integer $t\geq 1$, and any $c+et$ primes $p_1,p_2,\cdots,p_{c+et}\equiv -1 \pmod{\ell N}$, we have*

$$(1)\qquad f(z)|T_{p_1}|T_{p_2}|\cdots|T_{p_{c+et}}\equiv 0 \pmod{\lambda^t}.$$

Furthermore, if the primes $p_1,p_2,\cdots,p_{c+et}$ are distinct, then for any positive integer m coprime to $p_1,p_2,\cdots,p_{c+et}$, we have

$$(2)\qquad a(p_1p_2\cdots p_{c+et}m)\equiv 0 \pmod{\lambda^t}.$$

The constant e can be taken to be 1 if L is so large that the actions of the Hecke operators T_p on $M_k(\Gamma_0(\ell^a N),\varepsilon;L)$ for all $p\nmid \ell N$ are diagonalizable.

Remark. The last condition on L is satisfied if it contains all the Fourier coefficients of the Eisenstein series in $M_k(\Gamma_0(\ell^a N),\varepsilon;\mathbf{C})$ and the newforms in $S_k(\Gamma_0(M),\varepsilon;\mathbf{C})$ for all divisors M of $\ell^a N$ which are divisible by the conductor of ε. Note also that the Fourier coefficients of the Eisenstein series in $M_k(\Gamma_0(\ell^a N),\varepsilon;\mathbf{C})$ are contained in a cyclotomic field.

In the case of $\ell=2$ ([11]), K. Ono and the second author derived such a theorem from the non-existence of certain 2-dimensional mod 2 representations of the absolute Galois group $G_{\mathbf{Q}}$ of the rational number field $\mathbf{Q}$. In the case of $\ell\geq 3$, however, we may appeal instead to the proved part of Serre's ε-Conjecture. Stated in the form we need, it is:

Theorem 2. (cf. Th. 1.12 of [5]). *Let ℓ be an odd prime, and let $\rho: G_{\mathbf{Q}}\to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ be a continuous, odd and irreducible representation. If ρ is modular of some type $(\ell^a N,k,\varepsilon)_{\overline{\mathbf{Q}}}$ with N prime to ℓ, and if we assume further that $N>1$ when $\ell=3$, then it is isomorphic to a representation of the form $\chi^\alpha\otimes\rho'$, where χ is the mod ℓ cyclotomic character, $0\leq\alpha<\ell-1$, and ρ' is modular of type $(N',k',\varepsilon')_{\overline{\mathbf{Q}}}$ with $N'|N$, $2\leq k'\leq \ell+1$, and ε' is the "prime-to-ℓ part" of ε.*

Here, we say that a representation $\rho: G_{\mathbf{Q}}\to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ is modular of type $(N,k,\varepsilon)_{\overline{\mathbf{Q}}}$ if it comes (by Deligne's construction [4]) from an eigenform in $S_k(\Gamma_0(N),\varepsilon;\overline{\mathbf{Q}})$ (In other words, if it comes from a mod ℓ eigenform over $\overline{\mathbf{F}}_\ell$ of type (N,k,ε) in the sense of Serre [13]). Note that this theorem is often stated (as in [5]) with mod ℓ modular forms in the sense of Katz ([7]), but when the weight is ≥ 2 and either

2000 Mathematics Subject Classiffcation. 11F11, 11R32, 11S15.

[*)] Department of Mathematics, College of Natural Sciences, Kyungpook National University, Daegu 702–701, Korea

[**)] Graduate School of Mathematics, Kyushu University 33, Fukuoka 812–8581, Japan

$\ell > 3$ or $N > 1$, there is no distinction between mod ℓ modular forms in Serre's sense and Katz's sense ([5], Lemma 1.9).

In Theorem 2, that one can take ρ' to be of Serre weight $k' \leq \ell + 1$ follows from Theorem 3.4 of [6]. That one may assume $k' \geq 2$ is because if ρ' comes from an eigenform f of weight 1, then it also comes from $fE_{\ell-1}$ (mod ℓ), where $E_{\ell-1}$ is the Eisenstein series of weight $\ell - 1$, which has Fourier expansion $E_{\ell-1} \equiv 1$ (mod ℓ).

Proof of Theorem 1. In proving the theorem, we may replace (L, λ) by a finite extension (L', λ'), at the expense of multiplying the constant e by the ramification index. Thus we may assume L is so large that the actions of the Hecke operators T_p on $M_k(\Gamma_0(\ell^a N), \varepsilon; L)$ for all $p \nmid \ell N$ are diagonalizable.

Suppose first that $f \in M_k(\Gamma_0(\ell^a N), \varepsilon; \mathcal{O}_{L,\lambda})$ is a Hecke eigenform with T_p-eigenvalue $a(p)$;

$$f \mid T_p = a(p) f,$$

for each prime $p \nmid \ell N$. To prove (1) with $e = 1$ (and with $c = 0$ in this case), it is enough to show that

$$a(p) \equiv 0 \pmod{\lambda} \quad \text{if } p \equiv -1 \pmod{\ell N}.$$

By Hecke (cf. Chap. 7 of [9]) and Deligne ([4]), there exists a continuous representation

$$\rho_{f,\lambda} : G_{\mathbf{Q}} \to \mathrm{GL}_2(\kappa(\lambda)) \hookrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$$

such that

$$\mathrm{Tr}(\rho_{f,\lambda}(\mathrm{Frob}_p)) \equiv a(p) \pmod{\lambda} \tag{3}$$

for each prime $p \nmid \ell N$, where $\kappa(\lambda)$ denotes the residue field of λ and Frob_p denotes a Frobenius element at p. If $\rho_{f,\lambda}$ is irreducible (so in particular f is not an Eisenstein series), then by Theorem 2 it is of the form $\chi^\alpha \otimes \rho'$, where ρ' is modular of some type $(N', k', \varepsilon')_{\overline{\mathbf{Q}}}$ with $N' | N$ and $2 \leq k' \leq \ell + 1$. But for $(\ell, N) = (3, 4), (5, 2), (7, 1)$, there are no cusp forms of level N and weight $2 \leq k' \leq \ell + 1$. Hence $\rho_{f,\lambda}$ must be reducible;

$$\rho_{f,\lambda} \sim \begin{pmatrix} \psi_1 & * \\ & \psi_2 \end{pmatrix}.$$

The character $\psi_i : G_{\mathbf{Q}} \to \overline{\mathbf{F}}_\ell^\times$ factors through the group $(\mathbf{Z}/\ell^b N\mathbf{Z})^\times$ for some $b \geq 1$ (cf. [3, 8]) and, further, through the quotient $(\mathbf{Z}/\ell N\mathbf{Z})^\times$ since $\overline{\mathbf{F}}_\ell^\times$ has no elements of order divisible by ℓ. Since $\rho_{f,\lambda}$ is odd, if $c \in G_{\mathbf{Q}}$ is a complex conjugation, we have

$$\det(\rho_{f,\lambda}(c)) = (\psi_1\psi_2)(c) = (\psi_1\psi_2^{-1})(c) = -1.$$

Since c and Frob_p for $p \equiv -1 \pmod{\ell N}$ are both mapped to -1 in $(\mathbf{Z}/\ell N\mathbf{Z})^\times$ by the canonical map $G_{\mathbf{Q}} \to \mathrm{Gal}(\mathbf{Q}(\zeta_{\ell N})/\mathbf{Q}) \simeq (\mathbf{Z}/\ell N\mathbf{Z})^\times$, we have

$$(\psi_1\psi_2^{-1})(\mathrm{Frob}_p) = -1$$

for $p \equiv -1 \pmod{\ell N}$. On the other hand, for any $\sigma \in G_{\mathbf{Q}}$, we have

$$\begin{aligned} \mathrm{Tr}(\rho_{f,\lambda}(\sigma)) &= \psi_1(\sigma) + \psi_2(\sigma) \\ &= \psi_2(\sigma)((\psi_1\psi_2^{-1})(\sigma) + 1). \end{aligned}$$

Then it follows that, for any $p \equiv -1 \pmod{\ell N}$, we have

$$\mathrm{Tr}(\rho_{f,\lambda}(\mathrm{Frob}_p)) = 0,$$

and hence by (3),

$$a(p) \equiv 0 \pmod{\lambda}.$$

To prove (1) with $e = 1$ for a general f in $M_k(\Gamma_0(\ell^a N), \varepsilon; \mathcal{O}_{L,\lambda})$, let $f_1, \ldots, f_r$ be a set of Hecke eigenforms which forms a basis of the L-vector space $M_k(\Gamma_0(\ell^a N), \varepsilon; L)$ (cf. [1]). Then since the $\mathcal{O}_{L,\lambda}$-module $\sum_{i=1}^r \mathcal{O}_{L,\lambda} \cdot f_i$ is of finite index in $M_k(\Gamma_0(\ell^a N), \varepsilon; \mathcal{O}_{L,\lambda})$, there is an integer $c \geq 0$ such that $\lambda^c M_k(\Gamma_0(\ell^a N), \varepsilon; \mathcal{O}_{L,\lambda}) \subset \sum_{i=1}^r \mathcal{O}_{L,\lambda} \cdot f_i$. Thus for any $f \in M_k(\Gamma_0(\ell^a N), \varepsilon; \mathcal{O}_{L,\lambda})$, if we write

$$f \ = \ a_1 f_1 + \cdots + a_r f_r \quad \text{ with } a_i \in L,$$

then we have $\mathrm{ord}_\lambda(a_i) \geq -c$ for all $i = 1, \ldots, r$. Now the congruence (1) follows from the case of eigenforms.

The congruence (2) then follows by using Proposition 6.1 of [11], which we record here for the convenience of the reader:

Lemma 3. *If a modular form* $f(z) = \sum_{n=0}^\infty a(n)q^n \in M_k(\Gamma_0(M), \varepsilon; \mathcal{O}_{L,\lambda})$ *satisfies*

$$f(z)|T_{p_1}|T_{p_2}|\cdots|T_{p_c} \equiv 0 \pmod{\lambda^t}$$

for c *distinct primes* $p_i \nmid M$, *then one has*

$$a(p_1 p_2 \cdots p_c m) \equiv 0 \pmod{\lambda^t}$$

for any positive integer m *coprime to* $p_1 p_2 \ldots p_c$.

□

Next we give some applications of Theorem 1. The first one is to the Fourier coefficients of ℓ-adic modular forms. Let $\mathbf{C}_\ell$ be the completion of $\overline{\mathbf{Q}}$ with respect to an extension to $\overline{\mathbf{Q}}$ of the ℓ-adic valuation of $\mathbf{Q}$, and let $\mathcal{O}_{\mathbf{C}_\ell}$ be the valuation ring of $\mathbf{C}_\ell$. For our purpose, an ℓ-adic modular form $f = \sum_{n=0}^{\infty} a(n)q^n$ of weight $k \in \mathbf{Z}_\ell$, tame level N and character $\varepsilon : (\mathbf{Z}/\ell N\mathbf{Z})^\times \to \mathcal{O}_{\mathbf{C}_\ell}^\times$ is a power series in $\mathcal{O}_{\mathbf{C}_\ell}[\![q]\!]$ such that, for any integer $t \geq 1$, there exists a modular form $f_t = \sum_{n=0}^{\infty} a_t(n)q^n \in M_{k_t}(\Gamma_0(\ell^{a_t}N), \varepsilon; \overline{\mathbf{Q}})$ in the classical sense such that

$$f \equiv f_t \pmod{\ell^t},$$

where k_t is an integer ≥ 1 with the sequence $(k_t)_{t\geq 1}$ converging ℓ-adically to k and a_t is any integer ≥ 0. Theorem 1 implies:

Corollary 4. *Let $(\ell, N) = (3,4), (5,2)$ or $(7,1)$. If $f = \sum_{n=0}^{\infty} a(n)q^n \in \mathcal{O}_{\mathbf{C}_\ell}[\![q]\!]$ is an ℓ-adic modular form of tame level N, then for any integer $t \geq 1$, there exists an integer $c \geq 0$ such that for any c distinct primes $p_1, p_2, \ldots, p_c \equiv -1 \pmod{\ell N}$ and any positive integer m coprime to $p_1 p_2 \cdots p_c$, we have*

$$a(p_1 p_2 \cdots p_c m) \equiv 0 \pmod{\ell^t}.$$

Here, we applied Theorem 1 to each f_t approximating the ℓ-adic modular form f, and so the constant c depends on f and t.

Let us look at an example coming from the "modular invariant" $j(z) = \sum_{n=-1}^{\infty} c(n)q^n = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$, which is a modular function of weight 0 and level 1. It is known ([12], Th. 5.2) that the series

$$j'(z) := \sum_{n=0}^{\infty} c(\ell n)q^n \quad \text{and} \quad j_-(z) := \sum_{(\frac{-n}{\ell})=-1} c(n)q^n$$

are ℓ-adic modular forms of weight 0, tame level 1, and trivial character. Hence Corollary 4 implies:

Corollary 5. *Let $\ell = 3$, 5 or 7. For any integer $t \geq 1$, there exists an integer $c \geq 0$ such that for any c distinct primes $p_1, p_2, \ldots, p_c \equiv -1 \pmod{\ell}$ and any positive integer m coprime to $p_1 p_2 \cdots p_c$, we have*

$$c(p_1 p_2 \cdots p_c m) \equiv 0 \pmod{\ell^t}$$

whenever either $\ell | m$ or

$$\left(\frac{m}{\ell}\right) = \begin{cases} (-1)^c & \text{if } \ell = 3, 7, \\ -1 & \text{if } \ell = 5. \end{cases}$$

The next application is to the number of representations of an integer by quadratic forms. Let $Q(x_1, \ldots, x_k) = \frac{1}{2}\sum_{1\leq i,j\leq k} a_{ij}x_i x_j$ be a positive definite quadratic form in k variables over $\mathbf{Z}$; thus the coefficient matrix $A = (a_{ij})$ is positive definite and is in the set $\mathbf{E}_k$ of $k\times k$ symmetric matrices (a_{ij}) with $a_{ij} \in \mathbf{Z}$ and $a_{ii} \in 2\mathbf{Z}$. For any integer n, let $r(Q,n)$ denote the number of representations of n by Q;

$$r(Q,n) := \#\{(n_1, \ldots, n_k) \in \mathbf{Z}^k \mid n = Q(n_1, \ldots, n_k)\}.$$

The generating function for the sequence $(r(Q,n))_{n\geq 0}$,

$$\theta(z,Q) := \sum_{(n_1,\ldots,n_k)\in\mathbf{Z}^k} q^{Q(n_1,\ldots,n_k)} = \sum_{n=0}^{\infty} r(Q,n)q^n,$$

is called the *theta series* associated with the quadratic form Q ([2], Chap. 1, §1, (1.13)). The *level* M of the quadratic form Q (or of the coefficient matrix A) is by definition the smallest positive integer M such that MA^{-1} is in $\mathbf{E}_k$ ([2], Chap. 1, §3). It is known ([2], Chap. 2, Th. 2.2) that, if Q is of k variables and level M, then $\theta(z,Q)$ is a modular form of weight $k/2$ on $\Gamma_0(M)$ with some quadratic character ε_Q. By Theorem 1, we obtain:

Corollary 6. *Let $(\ell, N) = (3,4)$, $(5,2)$ or $(7,1)$. Suppose Q is a positive definite quadratic form over $\mathbf{Z}$ in an even number of variables and of level dividing $\ell^a N$ for some $a \geq 0$. Then there exist integers $c \geq 0$ and $e \geq 1$ such that for any integer $t \geq 1$, any $c + et$ distinct primes $p_1, p_2, \ldots, p_{c+et} \equiv -1 \pmod{\ell N}$, and any positive integer m coprime to $p_1 p_2 \cdots p_{c+et}$, we have*

$$r(Q, p_1 p_2 \cdots p_{c+et} m) \equiv 0 \pmod{\ell^t}.$$

For example, this applies to the quadratic form $Q = x_1^2 + x_2^2 + \cdots + x_{2k}^2$, which is of level 4.

Acknowledgements. Most ideas in this paper come from [10] and [11]. The authors are grateful to Ken Ono for sharing his insights with them and suggesting the possibility of further applications of the results of this paper.

References

[1] A. O. L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[2] A. N. Andrianov and V. G. Zhuravlev, Modular forms and Hecke Operators, Math. Monographs vol.145, A.M.S., Providence, 1995.

[3] H. Carayol, Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires, Duke Math. J. **59** (1989), 785–801.

[4] P. Deligne, Formes modulaires et représentations ℓ-adiques, Séminaire Bourbaki, 1968/69, Exp. 355, Lect. Notes in Math. **179**, Springer-Verlag, 1971.

[5] B. Edixhoven, Serre's conjecture, in *Modular forms and Fermat's last theorem*, (*Boston*, *MA*, 1995), 209–242, Springer, New York.

[6] B. Edixhoven, The weight in Serre's conjectures on modular forms, Invent. Math. **109** (1992), no.3, 563–594.

[7] N. Katz, p-adic properties of modular schemes and modular forms, in *Modular functions of one variable, III* (*Proc. Internat. Summer School, Univ. Antwerp, Antwerp*, 1972), 69–190, Lecture Notes in Math., 350, Springer, Berlin, 1973.

[8] R. Livné, On the conductors of mod ℓ Galois representations coming from modular forms, J. Number Theory **31** (1989), 133–141.

[9] T. Miyake, *Modular Forms*, Springer-Verlag, New York, 1989.

[10] K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series*, A.M.S., Providence, 2004.

[11] K. Ono and Y. Taguchi, 2-adic properties of certain modular forms and their applications to arithmetic functions, Int. J. Number Theory **1** (2005), 75–101.

[12] J.-P. Serre, Divisibilité de certaines fonctions arithmétiques, L'Enseignement Math. **22** (1976), 227–260.

[13] J.-P. Serre, Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$), Duke Math. J. **54** (1987), 179–230.