JP Journal of Algebra, Number Theory and Applications
Volume 8, Number 2, 2007, Pages 187-192
Published online: December 5, 2007
This paper is available online at http://www.pphmj.com

A CONGRUENCE RELATION ON A HECKE MODULE ASSOCIATED WITH A QUATERNION ALGEBRA

S. TAKAHASHI

Department of Mathematics
University of North Dakota
Grand Forks, ND 58202-8376, U. S. A.
e-mail: shuzo.takahashi@und.nodak.edu

Abstract

A congruence relation on the space of weight-2 cusp forms has been intensively studied. In this paper, we introduce a congruence relation on a Hecke module associated with a definite quaternion algebra and investigate a relationship between the two congruence relations.

1. Introduction

It is well known that there is a close connection between the theory of cusp forms and the arithmetic theory of quaternion algebras. In this paper, we study a connection between a congruence relation defined on the space of weight-2 cusp forms of prime level and a congruence relation defined on a Hecke module associated with a rational definite quaternion algebra of prime discriminant.

A congruence relation on the space of cusp forms has been studied by Doi, Hida, Ohta, Ribet, Zagier, and others (see, for example, in [1, 5, 9]).

2000 Mathematics Subject Classification: 11F11, 11F33, 11R52.

Keywords and phrases: quaternion algebras, modular forms, congruences, Hecke algebras.

Communicated by Roger C. Alperin

Received April 23, 2007

Let p be a prime number and $\mathbb{S}$ be the space of weight-2 cusp forms on $\Gamma_0(p)$ with integral Fourier coefficients. The space $\mathbb{S}$ is a free $\mathbb{Z}$-module. Let $\mathbb{T}$ be the Hecke ring acting on $\mathbb{S}$ and $\langle , \rangle_{\mathbb{S}}$ be the Peterson inner product on $\mathbb{S}$. Thus, $\mathbb{S}$ is a $\mathbb{T}$-module with a pairing. Given a positive integer ℓ, two cusp forms f and g in $\mathbb{S}$ are said to be congruent modulo ℓ if the n-th Fourier coefficient of f is congruent to the n-th Fourier coefficient of g modulo ℓ for all positive integers n. Then, given a Hecke eigenform f in $\mathbb{S}$ whose first Fourier coefficient is equal to 1, a positive integer r is defined as the largest positive integer such that there is a g in $\mathbb{S}$ that satisfies the following conditions: f and g are congruent modulo r, and $\langle f, g\rangle_{\mathbb{S}} = 0$.

Let $\mathcal{X}$ be the group of degree-0 divisors on the set of left ideal classes of a fixed maximal order in a rational definite quaternion algebra of discriminant p. It is known that the rank of $\mathcal{X}$ as a free $\mathbb{Z}$-module is the same as the rank of $\mathbb{S}$. The Hecke ring $\mathbb{T}$ acts on $\mathcal{X}$ and a pairing can be defined on $\mathcal{X}$. Thus, we have another $\mathbb{T}$-module with a pairing. (This module has been studied in various contexts, for example, [2, 3], and will be described in more detail in the next section.) We say two elements x and y in $\mathcal{X}$ are congruent modulo ℓ if the corresponding multiplicities of x and y (being considered as divisors) are congruent modulo ℓ. A positive integer s is defined in a manner similar to the way r was defined, using the Hecke eigenform in $\mathcal{X}$ corresponding to f in $\mathbb{S}$. (The integer s will be defined more precisely later.)

We prove that r and s are equal. The proof is a rather simple consequence of some results from [4, 8, 9], but the statement that r and s are equal is not trivial in the sense that the proof depends on a deep result of Ribet [6] in an essential way, as explained after the proof.

2. Description of a $\mathbb{T}$-Module $\mathcal{X}$

We describe a $\mathbb{T}$-module $\mathcal{X}$ with a pairing. Let H be a definite quaternion algebra defined over $\mathbb{Q}$. Suppose that the discriminant of H is

p, that is, H is ramified at the two places p and ∞. Let R be a fixed maximal order in H. The set of left ideal classes of R is finite of order $d+1$ for a positive integer d. Let $\{I_0, \ldots, I_d\}$ be a set of left ideals representing the distinct ideal classes, with $I_0 = R$, and denote the ideal classes by $[I_0], \ldots, [I_d]$. Let R_i be the right order of the ideal I_i, and let w_i be a half of the number of the units in R_i. The number w_i is independent of the representative I_i. Let $\mathcal{D}$ be the group of divisors on the set $\{[I_0], \ldots, [I_d]\}$. Define a pairing $\langle , \rangle_{\mathcal{D}}$ on $\mathcal{D}$ with values in $\mathbb{Z}$ by setting

$$\langle [I_i], [I_j] \rangle_{\mathcal{D}} = w_i \delta_{ij}$$

and extending bilinearly to $\mathcal{D}$. Let $\mathcal{X}$ be the subgroup of degree-0 divisors of $\mathcal{D}$. The space $\mathcal{X}$ is a free $\mathbb{Z}$-module of rank d. The pairing $\langle , \rangle_{\mathcal{X}}$ is defined to be the restriction of $\langle , \rangle_{\mathcal{D}}$ to $\mathcal{X}$. It is well known that $\mathcal{X}$ is isomorphic to the character group of the toric part of the mod p reduction of the Néron model of the Jacobian $J_0(p)$ of the modular curve $X_0(p)$. In the proof of our result, the description of $\mathcal{X}$ as the character group is essential. From now on, we identify $\mathcal{X}$ with this character group. Then, the pairing $\langle , \rangle_{\mathcal{X}}$ is the monodromy pairing on $\mathcal{X}$. An action of the Hecke ring $\mathbb{T}$ on $\mathcal{X}$ is carefully described in Section 3 of [6]. (The action of $\mathbb{T}$ on $\mathcal{X}$ can also be concretely described in terms of Brandt matrices; for example, see [2].) Thus, we have a $\mathbb{T}$-module $\mathcal{X}$ with a pairing.

3. Congruence Relations on $\mathcal{S}$ and $\mathcal{X}$

We have two $\mathbb{T}$-modules $\mathcal{S}$ and $\mathcal{X}$ with respective pairings $\langle , \rangle_{\mathcal{S}}$ and $\langle , \rangle_{\mathcal{X}}$. A congruence relation $\equiv$ on $\mathcal{S}$ is defined as follows: for $f(\tau) = \sum_{n \geq 1} a_n e^{2\pi i n \tau}$, $g(\tau) = \sum_{n \geq 1} b_n e^{2\pi i n \tau}$ in $\mathcal{S}$ and a positive integer ℓ, $f \equiv g \bmod \ell$ if $a_n \equiv b_n \bmod \ell$ for all positive integers n. Let $f(\tau) = \sum_{n \geq 1} a_n e^{2\pi i n \tau}$ be a Hecke eigenform in $\mathcal{S}$ with $a_1 = 1$. Define r to be the largest positive integer such that there is a cusp form g in $\mathcal{S}$ that satisfies the following conditions:

$$f \equiv g \bmod r \text{ and } \langle f, g \rangle_{\mathcal{S}} = 0.$$

On the other hand, a congruence relation $\equiv$ on $\mathcal{X}$ is defined as follows: for $x = \sum_{i=0}^{d} x_i \cdot [I_i]$, $y = \sum_{i=0}^{d} y_i \cdot [I_i]$ in $\mathcal{X}$ and a positive integer ℓ, $x \equiv y \bmod \ell$ if $x_i \equiv y_i \bmod \ell$ for $i = 0, 1, \ldots, d$. Consider an eigenspace $\mathcal{L} = \{x \in \mathcal{X} \mid T_n x = a_n x$ for all T_n in $\mathbb{T}\}$ of $\mathcal{X}$. The rank of $\mathcal{L}$ is 1. Let v be a generator of $\mathcal{L}$. (The eigenspace $\mathcal{L}$ and the eigenvector v have been studied, for example, in [2, 7].) Define s to be the largest positive integer such that there is a y in $\mathcal{X}$ that satisfies the following conditions:

$$v \equiv y \bmod s \text{ and } \langle v, y \rangle_{\mathcal{X}} = 0.$$

Theorem. *We have the equality* $r = s$.

To prove the theorem, we first express s with v and $\langle , \rangle_{\mathcal{X}}$.

Lemma. *Let x be an element in $\mathcal{X}$ such that $\langle v, x \rangle_{\mathcal{X}}$ is the smallest positive integer expressible in this way. Then, $\langle v, x \rangle_{\mathcal{X}}$ divides $\langle v, v \rangle_{\mathcal{X}}$ and we have the following equality*:

$$s = \frac{\langle v, v \rangle_{\mathcal{X}}}{\langle v, x \rangle_{\mathcal{X}}}.$$

Proof. Note that considering $\mathcal{X}$ as a free $\mathbb{Z}$-module, $\langle , \rangle_{\mathcal{X}}$ is a bilinear pairing on $\mathcal{X}$ with integral values. Let x be an element in $\mathcal{X}$ such that $\langle v, x \rangle_{\mathcal{X}}$ is the smallest positive integer expressible in this way. Let $I = \{\langle v, z \rangle_{\mathcal{X}} \mid z \in \mathcal{X}\}$. Then, I is an ideal of $\mathbb{Z}$. Thus, $\langle v, x \rangle_{\mathcal{X}}$ is a generator of I. Hence, $\langle v, x \rangle_{\mathcal{X}}$ divides $\langle v, z \rangle_{\mathcal{X}}$ for any z in $\mathcal{X}$. In particular, $\langle v, x \rangle_{\mathcal{X}}$ divides $\langle v, v \rangle_{\mathcal{X}}$. Let t be the integer $\langle v, v \rangle_{\mathcal{X}} / \langle v, x \rangle_{\mathcal{X}}$. (We have to show that $s = t$.) By the definition of s, there is a y in $\mathcal{X}$ such that $v \equiv y \bmod s$ and $\langle v, y \rangle_{\mathcal{X}} = 0$. Then, $v - y = sz$ for some z in $\mathcal{X}$. Thus, we have

$\langle v, y\rangle_{\mathcal{X}} = \langle v, v - sz\rangle_{\mathcal{X}} = 0$. Hence, $\langle v, v\rangle_{\mathcal{X}} = s\langle v, z\rangle_{\mathcal{X}}$. Dividing both sides of the equation by $\langle v, x\rangle_{\mathcal{X}}$, we have $t = s(\langle v, z\rangle_{\mathcal{X}}/\langle v, x\rangle_{\mathcal{X}})$. Hence, we have $s \mid t$. Also, from the definition of t, we have $\langle v, v - tx\rangle_{\mathcal{X}} = 0$. Since $v \equiv v - tx \mod t$, by the definition of s, we have $s = t$.

Proof of Theorem. Let E be the elliptic curve associated with the cusp form f. Consider the parametrization $\xi : X_0(p) \to E$. We assume that ξ is optimal in the sense that the induced map $\xi : J_0(p) \to E$ on Jacobians has the connected kernel. Let δ be the degree of $\xi : X_0(p) \to E$. Theorem 3 in [9] states that $r = \delta$. Thus, by the lemma, it is sufficient to show that $\delta = \langle v, v\rangle_{\mathcal{X}}/\langle v, x\rangle_{\mathcal{X}}$. Let $\Phi(J_0(p))$ and $\Phi(E)$ be the groups of connected components of mod p reductions of Néron models of $J_0(p)$ and E, respectively. Consider the map $\xi_* : \Phi(J_0(p)) \to \Phi(E)$ which is induced from $\xi : J_0(p) \to E$. Let j be the order of the cokernel of the map ξ_*. Theorem 2.3 together with Lemma 2.2 in [8] implies that $\delta = (\langle v, v\rangle_{\mathcal{X}}/\langle v, x\rangle_{\mathcal{X}}) \cdot j$. (We are using the theorem and the lemma for the case that $D = 1$ and $M = p$. Moreover, notationally, we have that $g_r = v$, $h_r = \langle v, v\rangle_{\mathcal{X}}$, $i_r = \langle v, x\rangle_{\mathcal{X}}$, $j_r = j$, and $u_J(,)$ is $\langle,\rangle_{\mathcal{X}}$.) Corollary 3 of Theorem 2 in [4] states that the map $\xi : \Phi(J_0(p)) \to \Phi(E)$ is surjective, i.e., $j = 1$. Hence, we have $\delta = \langle v, v\rangle_{\mathcal{X}}/\langle v, x\rangle_{\mathcal{X}}$.

The statement $r = s$ of the theorem is not trivial. In the above proof, the only place where we need the level-lowering theorem of Ribet [6] is in the proof of Corollary 3 of [4]. On the other hand, from the proof, we see that the equality $r = s$ is equivalent to the equality $j = 1$ without using the level-lowering theorem. Moreover, the equality $j = 1$, together with the fact that the group $\Phi(J_0(p))$ is Eisenstein (see Theorem 3.12 in [6]), implies the following form of the level-lowering theorem concerning the elliptic curve E: for every prime ℓ, if the representation ρ_ℓ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ giving the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the group $E[\ell]$ of ℓ-division points of E

is irreducible, then the representation ρ_ℓ is ramified at p. Thus, the statement of the theorem is as strong as this last non-trivial result.

References

[1] K. Doi and M. Ohta, On some congruences between cusp forms on $\Gamma_0(N)$, Modular functions of one variable *V*, Lecture Notes in Math. Vol. 601, Springer-Verlag, Berlin, Heidelberg, New York, 1977, pp. 91-105.

[2] B. H. Gross, Heights and the special values of *L*-series, Conference Proceedings, Canadian Mathematical Society 7 (1987), 115-187.

[3] D. Kohel, Hecke module structure of quaternions, Class Field Theory – Its Centenary and Prospect, K. Miyake, ed., Vol. 30, The Advanced Studies in Pure Mathematics Series, Math. Soc. Japan, Tokyo, 2001, pp. 177-196.

[4] J.-F. Mestre and J. Oesterlé, Courbes de Weil semi-stables de discriminant une puissance *m*-ième, J. reine angew. Math. 400 (1989), 173-184.

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

[6] K. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, Invent. Math. 100 (1990), 431-476.

[7] K. Ribet and S. Takahashi, Parametrizations of elliptic curves by Shimura curves and by classical modular curves, Proc. Natl. Acad. Sci. 94 (1997), 11110-11114.

[8] S. Takahashi, Degrees of parametrizations of elliptic curves by Shimura curves, J. Number Theory 90 (2001), 74-88.

[9] D. Zagier, Modular parametrizations of elliptic curves, Canad. Math. Bull. 28 (1985), 372-384.