J. Math. Kyoto Univ. (JMKYAZ)
32-3 (1992) 515-526

On mod p cohomology of the space X_Γ and mod p trace formula for Hecke operators

By

Goro NISHIDA

1. Introduction

Let $M_2\mathbf{Z}$ denote the set of 2×2 matricies over $\mathbf{Z}$. The semigroup $M_2\mathbf{Z}$ acts on the 2-torus T^2 as endomorphisms in the standard way. For any subgroup Γ of $M_2\mathbf{Z}$, we can define the semi-direct product $\Gamma \ltimes T^2$. We denote the classifying space $B(\Gamma \ltimes T^2)$ by X_Γ. Our main interest is in the case of $\Gamma = SL_2\mathbf{Z}$ or congruent modular groups. In this case it is known [3] that there is an isomorphism

$$H^{2n+1}(X_\Gamma; \mathbf{R}) \cong H^1(\Gamma; H^{2n}(BT^2; \mathbf{R})),$$

where the right hand side is the cohomology of the group Γ with the coefficient module $H^{2n}(BT^2; \mathbf{R})$. Then the Eichler-Shimura homomorphism turns out to be a homomorphism

$$\phi: M_k \to H^{2k-3}(X_\Gamma; \mathbf{R}),$$

where M_k is the space of modular forms of weight k for Γ. Moreover it is known [6] that we can define a Hecke operator $T(n)$ on $H^*(X_\Gamma; M)$ for any module M induced from a stable self map of X_Γ, and ϕ commutes with Hecke operators. Now the theorem of Eichler and Shimura [7] asserts that $\phi: S_k \cong H^1_P(\Gamma; H^{2k-4}(BT^2; \mathbf{R}))$, where S_k is the space of cusp forms of weight k and H^1_P means the parabolic cohomology of Γ. Then it is also known [3] that

$$\dim_{\mathbf{R}} H^{2k-3}(X_\Gamma; \mathbf{R}) = \dim_{\mathbf{R}} H^1_P(\Gamma; H^{2k-4}(BT^2; \mathbf{R})) + \nu,$$

where ν is the number of equivalent classes of cusps.

In this note we study $H^*(X_\Gamma; \mathbf{F}_p)$, which has richer structure; the action of Steenrod algebra and the module structure over $H^{ev}(X_\Gamma; \mathbf{F}_p)$. We shall show that $H^{ev}(X_\Gamma; \mathbf{F}_p) \cong \mathbf{F}_p[x, y]^\Gamma$, the ring of Γ-invariants. In the case of $\Gamma = SL_2\mathbf{Z}$, $\mathbf{F}_p[x, y]^\Gamma \cong \mathbf{F}_p[q, q_1]$, $\deg q = p + 1$ and $\deg q_1 = p(p-1)$. It is shown (Corollary 3.3) that $H^*(X_\Gamma; \mathbf{F}_p)/qH^*(X_\Gamma; \mathbf{F}_p)$ satisfies certain periodicity. Using this the $\mathbf{F}_p[q, q_1]$-module structure of $H^*(X_\Gamma; \mathbf{F}_p)$ is determined (Theorem 5.3). As a corollary of those results, we give a formula on mod p value of the trace of Hecke operators acting on cusp forms.

Received October 8, 1990

2. Additive structure of $H^*(X_\Gamma; \mathbf{F}_p)$

Let Γ denote $SL_2\mathbf{Z}$ or a congruent subgroup of $SL_2\mathbf{Z}$. Let d be a positive integer such that for any Γ-module over $\mathbf{Z}[1/d]$, $H^i(\Gamma; M) = 0$ for all $i \geq 2$. It is well known that there exists such an integer d and one can take $d = 6$ for $\Gamma = SL_2\mathbf{Z}$ (see [6]). For a $\mathbf{Z}[1/d]$-module M, the Serre spectral sequence for the fibration

$$BT^2 \to X_\Gamma = B(\Gamma \ltimes T^2) \to B\Gamma$$

collapses and we have a short exact sequence

$$0 \to H^1(\Gamma; H^n(BT^2; M)) \to H^{n+1}(X_\Gamma; M) \to H^0(\Gamma; H^{n+1}(BT^2; M)) \to 0\,.$$

Let x and y be the standard basis of $H^2(BT^2; \mathbf{Z})$. Then we have $H^*(BT^2; M) \cong \mathbf{Z}[x, y] \otimes M$, and the above argument shows the following.

Lemma 2.1. *There are isomorphisms*

$$H^{2n}(X_\Gamma; M) \cong H^0(\Gamma; \mathbf{Z}[x, y]_n \otimes M)$$

and

$$H^{2n+1}(X_\Gamma; M) \cong H^1(\Gamma; \mathbf{Z}[x, y]_n \otimes M)\,,$$

where $\mathbf{Z}[x, y]_n$ denotes the module of homogeneous polynomials in x and y of degree n.

Now let p be a prime such that $(p, d) = 1$. Then $\oplus H^{2n}(X_\Gamma; \mathbf{F}_p) \cong H^0(\Gamma; \mathbf{F}_p[x, y]) \cong \mathbf{F}_p[x, y]^\Gamma$ is the ring of Dickson invariants. The additive structure of $H^{odd}(X_\Gamma; \mathbf{F}_p)$ is given as follows.

Theorem 2.2. ([3]) *Let p be a prime such that $(d, p) = 1$. Let ν be the number of equivalence classes of cusps of Γ. Then*

$$\dim_{\mathbf{F}_p} H^{2n+1}(X_\Gamma; \mathbf{F}_p) = \dim_{\mathbf{F}_p} \mathbf{F}_p[x, y]_n^\Gamma + \dim_{\mathbf{R}} S_{n+2} + \nu\,,$$

where S_{n+2} is the space of cusp forms of weight $n + 2$.

Proof. Consider the short exact sequence

$$0 \to \mathbf{Z}_{(p)}[x, y] \xrightarrow{p} \mathbf{Z}_{(p)}[x, y] \xrightarrow{\rho} \mathbf{F}_p[x, y] \to 0$$

of $\mathbf{Z}_{(p)}[\Gamma]$-modules, where ρ is the reduction mod p. Then we have an exact sequence

$$\begin{aligned} 0 &\to H^0(\Gamma; \mathbf{Z}_{(p)}[x, y]) \xrightarrow{p} H^0(\Gamma; \mathbf{Z}_{(p)}[x, y]) \xrightarrow{\rho_*} H^0(\Gamma; \mathbf{F}_p[x, y]) \\ &\xrightarrow{\delta} H^1(\Gamma; \mathbf{Z}_{(p)}[x, y]) \xrightarrow{p} H^1(\Gamma; \mathbf{Z}_{(p)}[x, y]) \xrightarrow{\rho_*} H^1(\Gamma; \mathbf{F}_p[x, y]) \to 0\,. \end{aligned}$$

First we show that $H^0(\Gamma; \mathbf{Z}_{(p)}[x, y]) = 0$. Since Γ is a congruent modular group, $\Gamma \supset \Gamma(N)$, the principal congruent modular group for some N. Hence $\Gamma \ni \alpha = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ and $\Gamma \ni \beta = \begin{pmatrix} 1 & 0 \\ N & 1 \end{pmatrix}$. One can easily check that for any homogeneous polynomial $f(x, y) \in \mathbf{Q}[x, y]$, $\alpha f = f$ only if $f = ax^n$ for some $a \in \mathbf{Q}$ and $\beta f = f$ only if $f = by^n$ for some $b \in \mathbf{Q}$. Therefore $H^0(\Gamma; \mathbf{Q}[x, y]) = 0$ and so is for $H^0(\Gamma; \mathbf{Z}_{(p)}[x, y])$. Now note that

$$\operatorname{rank}(H^1(\Gamma; \mathbf{Z}_{(p)}[x, y]_n)/\mathrm{Tor}) = \dim_{\mathbf{R}} H^1(\Gamma; \mathbf{R}[x, y]_n).$$

By the Eichler-Shimura isomorphism we have

$$\dim_{\mathbf{R}} H^1(\Gamma; \mathbf{R}[x, y]_n) = \dim_{\mathbf{R}} S_{n+2} + \nu .$$

Then the theorem follows from the above exact sequence and Lemma 2.1.

3. A periodicity

In this section we suppose that $\Gamma = SL_2\mathbf{Z}$ and $p \geq 5$. Since $SL_2\mathbf{Z} \ni \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, we see that $H^1(SL_2\mathbf{Z}; \mathbf{Z}[x, y]_n \otimes A) = 0$ for odd n and a $\mathbf{Z}_{(p)}$-module A as shown in [7]. Let $q = xy^p - x^p y \in \mathbf{F}_p[x, y]_{p+1}$ and $q_1 = x^{p(p-1)} + x^{(p-1)^2}y^{p-1} + \cdots + x^{p-1}y^{(p-1)^2} + y^{p(p-1)} \in \mathbf{F}_p[x, y]_{p(p-1)}$. For a matrix $\alpha \in M_2\mathbf{Z}$ we have $\alpha(q) = (\det \alpha)q$ and for $\alpha \in M_2\mathbf{Z}$ such that $\det \alpha \not\equiv 0 \bmod p$, we have $\alpha(q_1) = q_1$. It is well known that the ring of Dickson invariants is given by

$$\mathbf{F}_p[x, y]^{SL_2\mathbf{Z}} = \mathbf{F}_p[q, q_1] .$$

Let (q) be the ideal of $\mathbf{F}_p[x, y]$ generated by q and let $Q_* = \mathbf{F}[x, y]/(q)$. Then Q_* is a graded $\mathbf{F}_p[M_2\mathbf{Z}]$-module. If $n \leq p$, then $Q_n \cong \mathbf{F}_p[x, y]_n$. If $n \geq p + 1$, then Q_n has a basis $[x^n]$, $[x^{n-1}y]$, $\ldots$, $[x^{n-p+1}y^{p-1}]$ and $[y^n]$, where $[f]$ means the class of $f \in \mathbf{F}_p[x, y]$ in Q_*, and we have $\dim Q_n = p + 1$.

Now let $\wp^s$ denote the reduced power operation. Note that $\wp^s\colon \mathbf{F}_p[x, y]_n = H^{2n}(BT^2; \mathbf{F}_p) \to \mathbf{F}_p[x, y]_{n+s(p-1)} = H^{2n+2s(p-1)}(BT^2; \mathbf{F}_p)$ commutes with the action of $M_2\mathbf{Z}$. The following lemma is obvious.

Lemma 3.1. *$\wp^p q = qq_1$, $\wp^{p+1}q = q^p$ and $\wp^s q = 0$ if $s \neq p$, $p + 1$.*

By the lemma, one can define an induced $\mathbf{F}_p[M_2\mathbf{Z}]$-homomorphism

$$\wp^s\colon Q_n \to Q_{n+s(p-1)} .$$

If $n \geq p + 1$, taking the basis $[x^n]$, $\ldots$, $[x^{n-p+1}y^{p-1}]$ and $[y^n]$ in this order we can identify Q_n with $\mathbf{F}_p^{p+1}$. Then we have

Lemma 3.2. *Suppose that $n \geq p + 1$. Then*

$$\wp^s = \binom{n}{s} \times : Q_n \to Q_{n+s(p-1)}.$$

The proof is easy from the Cartan formula. Then we have the following key observation.

Corollary 3.3. *Suppose that n, $m \geq p + 1$ and $n \equiv m \bmod (p - 1)$. Then $Q_n \cong Q_m$ as $\mathbf{F}_p[M_2\mathbf{Z}]$-modules.*

Proof. By the above lemma, we see that the action of reduced powers on Q_* is similar to the case of $H^*(CP; F_p)$. Then as shown in [1], we see that there are integers k_i and s_i and chains of isomorphisms

$$Q_n \xrightarrow{u_1} Q_{k_1} \xrightarrow{u_2} Q_{k_2} \to \cdots \to Q_m,$$

where $u_i = \wp^{p^{s_i}}$ or $(\wp^{p^{s_i}})^{-1}$.

Next let r be a positive integer. We denote the graded algebra $F_p[x, y]/(q^r)$ by $Q_*^{(r)}$. As for $Q_* = Q_*^{(1)}$, $Q_*^{(r)}$ is a graded $F_p[M_2 Z]$-module, and by Lemma 3.1 we can define the reduced power

$$\wp^s\colon Q_n^{(r)} \to Q_{n+s(p-1)}^{(r)}.$$

Lemma 3.4. *Let n and m be integers such that $n \geq 2(p+1)$ and $m \geq 2(p+1)$. Then there is an isomorphism $Q_n^{(2)} \cong Q_m^{(2)}$ as $F_p[SL_2 Z]$-modules if* i) *$n \equiv m$ mod $p(p-1)$ or* ii) *$n \equiv m$ mod $p-1$ and $nm \not\equiv 0$ mod p.*

Proof. Note that $\dim Q_n^{(2)} = 2p+2$ if $n \geq 2(p+1)$. It is clear that

$$q_1\colon Q_n^{(2)} \to Q_{n+p(p-1)}^{(2)}$$

is a monomorphism of $F_p[SL_2 Z]$-modules and hence an isomorphism if $n \geq 2(p+1)$. This shows the case i). Since $\wp^1 q = 0$, we have a following commutative exact diagram of $F[M_2 Z]$-modules

$$\begin{array}{ccccccccc}
0 & \longrightarrow & Q_{n-p-1} & \xrightarrow{q} & Q_n^{(2)} & \xrightarrow{\rho} & Q_n & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \wp^1} & & \downarrow{\scriptstyle \wp^1} & & \downarrow{\scriptstyle \wp^1} & & \\
0 & \longrightarrow & Q_{n-2} & \xrightarrow[q]{} & Q_{n+p-1}^{(2)} & \xrightarrow[\rho]{} & Q_{n+p-1} & \longrightarrow & 0,
\end{array}$$

where ρ is the reduction homomorphism. Then by Lemma 3.2 and by the five lemma we see that

$$\wp^1\colon Q_n^{(2)} \to Q_{n+p-1}^{(2)}$$

is an isomorphism if $n \geq 2(p+1)$ and $n \not\equiv 0, 1$ mod p. Suppose that $n \not\equiv 0$ mod p, then combining the q_1-periodicity we see that $Q_n^{(2)}, Q_{n+p-1}^{(2)}, \ldots, Q_{n+p(p-1)}^{(2)}$ are isomorphic to each other except $Q_{n+k(p-1)}^{(2)}$ such that $n + k(p-1) \equiv 0$ mod p. This completes the proof.

Remark. The isomorphism in the lemma is not an isomorphism of $F_p[M_2 Z]$-modules in general.

4. Computation of $H^0(SL_2 Z; Q_*)$

We regard $F_p[x, y]_n$ as a representation of $SL_2 F_p$ over F_p. We write this $F_p[SL_2 F_p]$-module $F_p[x, y]_n$ simply by V_n. Glover [4] has shown the following.

Theorem 4.1. i) $V_0, V_1, \ldots, V_{p-1}$ *is the set of all irreducible representation of* $SL_2\mathbf{F}_p$ *over* $\mathbf{F}_p$.

ii) V_{p-1} *is projective.*

iii) *There are exact sequences of* $SL_2\mathbf{F}_p$*-modules*

$$0 \to V_1 \to V_p \to V_{p-2} \to 0$$

and

$$0 \to V_i \oplus V_{i+2} \to V_{p+i+1} \to V_{p-i-3} \to 0$$

for $0 \le i \le p-3$.

Corollary 4.2. *Let* $0 \le k \le 2p-2$. *Then* V_k *contains the trivial representation as a composition factor if and only if* $k = 0$, $p+1$ *or* $2p-2$. *For* $k = 0$, $p+1$ *or* $2p-2$, *the multiplicity of the trivial factor is* 1.

Now note that $V_k = Q_k$ for $k \le p$ and there is a short exact sequence

$$0 \to V_{k-p-1} \xrightarrow{q} V_k \to Q_k \to 0$$

of $\mathbf{F}_p[SL_2\mathbf{F}_p]$-modules for $k \ge p+1$. Let α_2 be the class of $x^{2p-2} - x^{p-1}y^{p-1} + y^{2p-2}$ in Q_{2p-2}. One can easily check that α_2 is $SL_2\mathbf{F}_p$ (and hence $SL_2\mathbf{Z}$)-invariant. Then by Corollary 3.3, we have $SL_2\mathbf{Z}$-invariant elements $\alpha_k \in Q_{k(p-1)}$ for $k \ge 2$.

Theorem 4.3. *There is an isomorphism*

$$H^0(SL_2\mathbf{Z}; Q_*) \cong \mathbf{F}_p\{1, \alpha_2, \alpha_3, \ldots\}.$$

Proof. Note that there is no $SL_2\mathbf{Z}$-invariant in Q_k for $0 < k < 2p-2$ and $H^0(SL_2\mathbf{Z}; Q_{2p-2}) \cong \mathbf{F}_p\{\alpha_2\}$ by Corollary 4.2. Then the theorem follows from Corollary 3.3.

Lemma 4.4. $H^0(SL_2\mathbf{Z}; Q^{(2)}_{3(p-1)}) = 0$.

Proof. Consider the following commutative exact diagram

$$\begin{tikzcd}
0 \arrow[r] & Q_{p-3} \arrow[r, "q"] \arrow[d, "\wp^1"] & Q^{(2)}_{2(p-1)} \arrow[r, "p"] \arrow[d, "\wp^1"] & Q_{2(p-1)} \arrow[r] \arrow[d, "\wp^1"] & 0 \\
0 \arrow[r] & Q_{2(p-2)} \arrow[r, "q"'] & Q^{(2)}_{3(p-1)} \arrow[r, "p"'] & Q_{3(p-1)} \arrow[r] & 0.
\end{tikzcd}$$

By Corollary 4.2, Q_{p-3} and $Q_{2(p-2)}$ do not have the trivial factor. In particular we have $H^0(SL_2\mathbf{Z}; Q_{p-3}) \cong H^0(SL_2\mathbf{Z}; Q_{2(p-2)}) \cong H^0(SL_2\mathbf{Z}; Q_{2(p-2)}/\mathrm{Im}\,\wp^1) \cong 0$. From the exact sequence of the group cohomology associated with the short exact sequence $0 \to Q_{p-3} \xrightarrow{\wp^1} Q_{2(p-2)} \to \mathrm{Cok}\,\wp^1 \to 0$, we see that

$$\wp^1_*\colon H^1(SL_2\mathbf{Z}; Q_{p-3}) \to H^1(SL_2\mathbf{Z}; Q_{2(p-2)})$$

is a monomorphism. Then we have the following commutative exact diagram

$$\begin{tikzcd} 0 \arrow[r] & H^0(SL_2\mathbf{Z}; Q^{(2)}_{2(p-1)}) \arrow[r, "\rho_*"] \arrow[d, "\wp^1_*"] & H^0(SL_2\mathbf{Z}; Q_{2(p-1)}) \arrow[r, "\delta"] \arrow[d, "\wp^1_*"] & H^1(SL_2\mathbf{Z}; Q_{p-3}) \arrow[d, "\wp^1_*"] \\ 0 \arrow[r] & H^0(SL_2\mathbf{Z}; Q^{(2)}_{3(p-1)}) \arrow[r, "\rho_*"] & H^0(SL_2\mathbf{Z}; Q_{3(p-1)}) \arrow[r, "\delta"] & H^1(SL_2\mathbf{Z}; Q_{2(p-2)}) . \end{tikzcd}$$

Now the middle vertical arrow is an isomorphism by Corollary 3.3. Then the left $\wp^1_*$ is an isomorphism by the five lemma. Now $Q^{(2)}_{2(p-1)} = V_{2(p-1)}$ has no $SL_2\mathbf{Z}$-invariant and hence $H^0(SL_2\mathbf{Z}; Q^{(2)}_{3(p-1)}) \cong 0$.

Corollary 4.5. *There are isomorphisms*

$$\begin{aligned} &\operatorname{Im}[\rho_*\colon H^0(SL_2\mathbf{Z}; Q^{(2)}_*) \to H^0(SL_2\mathbf{Z}; Q_*)] \\ &\cong \operatorname{Im}[\rho_*\colon H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \to H^0(SL_2\mathbf{Z}; Q_*)] \\ &\cong \mathbf{F}_p\{1, \alpha_p, \alpha_{2p}, \dots\} . \end{aligned}$$

Proof. Since $p \geq 5$, we have $3(p-1) \geq 2(p+1)$. Then by Lemma 3.4, $H^0(SL_2\mathbf{Z}; Q^{(2)}_{s(p-1)}) \cong H^0(SL_2\mathbf{Z}; Q^{(2)}_{3(p-1)}) \cong 0$ if $s \geq 3$ and $s \not\equiv 0 \bmod p$. Now note that $\alpha_{pk} = [q_1^k]$, the class of q_1^k in Q_* and hence $\alpha_{pk} \in \operatorname{Im} \rho_*$. This completes the proof.

Corollary 4.6. *There is an isomorphism*

$$H^0(SL_2\mathbf{Z}; Q^{(2)}_*) \cong qH^0(SL_2\mathbf{Z}; Q_*) \oplus \mathbf{F}_p[q_1] .$$

Proof. Consider the exact sequence

$$0 \to H^0(SL_2\mathbf{Z}; Q_*) \xrightarrow{q} H^0(SL_2\mathbf{Z}; Q^{(2)}_*) \xrightarrow{\rho_*} H^0(SL_2\mathbf{Z}; Q_*) .$$

Then the corollary follows immediately from Corollary 4.5.

5. $\mathbf{F}_p[q, q_1]$-module structure of $H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$

Let $u \in \mathbf{F}_p[q, q_1]$ be a Dickson invariant. Then $u\cdot\colon \mathbf{F}_p[x, y] \to \mathbf{F}_p[x, y]$ induces a homomorphism $H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \to H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ and we see that $H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ is an $\mathbf{F}_p[q, q_1]$-module. If we identify $\mathbf{F}_p[q, q_1] = H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ with $H^{ev}(X_{SL_2\mathbf{Z}}; \mathbf{F}_p)$ and $H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ with $H^{odd}(X_{SL_2\mathbf{Z}}; \mathbf{F}_p)$ (Lemma 2.1), then it is easy to see that this module structure is the same as one induced from the cup product.

Now let M_* denote the graded $\mathbf{F}_p[SL_2\mathbf{Z}]$-module $\mathbf{F}_p[x, y]/(q, q_1) = \mathbf{F}_p[x, y] \otimes_{\mathbf{F}_p[q, q_1]} \mathbf{F}_p$. By Corollary 3.3, we easily see that $M_k = 0$ for $k \geq p^2$. Moreover it is known [5] that M_* is a Poincaré duality module.

Lemma 5.1. *$H^1(SL_2\mathbf{Z}; Q_*)$ is $\mathbf{F}_p[q_1]$-free.*

Proof. By Corollary 3.3 and Corollary 4.2, we see that the trivial factor in Q_* appears as a submodule. Consider the short exact sequence

$$0 \to Q_* \xrightarrow{q_1} Q_* \xrightarrow{\rho} M_* \to 0\,,$$

where ρ is the reduction. Then the above argument shows that ρ_*: $H^0(SL_2\mathbf{Z}; Q_*) \to H^0(SL_2\mathbf{Z}; M_*)$ is an epimorphism and hence we have an exact sequence

$$0 \to H^0(SL_2\mathbf{Z}; Q_*) \xrightarrow{q_1} H^1(SL_2\mathbf{Z}; M_*) \xrightarrow{\rho} M_* \to 0\,.$$

This shows $H^1(SL_2\mathbf{Z}; Q_*)$ is $\mathbf{F}_p[q_1]$-free.

Let T_*^q denote the subspace of $H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ consisting of q-torsion elements.

Lemma 5.2. i) *Every q-torsion element is single torsion, i.e., if* $q^2u = 0$ *then* $qu = 0$ *for* $u \in H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$.

ii) $T_k^q \cong \mathbf{F}_p$ *if* $k = s(p-1) - 2$, $s \not\equiv 0 \bmod p$, *and* $T_k^q \cong 0$ *otherwise.*

Proof. Consider the exact sequence

$$0 \to \mathbf{F}_p[x, y] \xrightarrow{q} \mathbf{F}_p[x, y] \xrightarrow{\rho} Q_* \to 0$$

and the associated exact sequence

$$\begin{aligned} 0 &\to H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \xrightarrow{q} H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \xrightarrow{\rho_*} H^0(SL_2\mathbf{Z}; Q_*) \\ &\xrightarrow{\delta} H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \xrightarrow{q} H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \xrightarrow{\rho_*} H^1(SL_2\mathbf{Z}; Q_*) \to 0\,. \end{aligned}$$

Then by Theorem 4.3 and Corollary 4.5, $T_*^q = \operatorname{Im}\delta$ is spanned by $\delta(\alpha_k)$, $k \not\equiv 0 \bmod p$. This shows ii). Let $u \in H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ be such that $q^2u = 0$. Then $u = \delta^{(2)}(v)$ for some $v \in H^0(SL_2\mathbf{Z}; Q_*^{(2)})$, where $\delta^{(2)}$: $H^0(SL_2\mathbf{Z}; Q_*^{(2)}) \to H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ is the coboundary associated with the exact sequence $0 \to \mathbf{F}_p[x, y] \xrightarrow{q^2} \mathbf{F}_p[x, y] \to Q_*^{(2)} \to 0$. By Corollary 4.6, $H^0(SL_2\mathbf{Z}; Q_*^{(2)}) \cong qH^0(SL_2\mathbf{Z}; Q_*) \oplus \mathbf{F}_p[q_1]$. If $v \in qH^0(SL_2\mathbf{Z}; Q_*)$, say, $v = qw$, then $\delta^{(2)}(v) = \delta(w)$ where δ is the coboundary associated with $0 \to \mathbf{F}_p[x, y] \xrightarrow{q} \mathbf{F}_p[x, y] \xrightarrow{\rho} Q_* \to 0$. Hence $qu = 0$. This completes the proof.

Let now $B_* = \rho_*(T_*^q)$, where ρ_*: $H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \to H^1(SL_2\mathbf{Z}; M_*)$ is the reduction homomorphism. Then we have

Theorem 5.3. *There is an isomorphism of* $\mathbf{F}_p[q, q_1]$-*modules*

$$H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \cong \mathbf{F}_p[q, q_1] \otimes (H^1(SL_2\mathbf{Z}; M_*)/B_*) \oplus \mathbf{F}_p[q, q_1]/(q) \otimes B_*\,.$$

Proof. We take $\mathbf{F}_p[q, q_1]$-indecomposable elements $u_1, \ldots, u_r$ in T_*^q. Adding other $\mathbf{F}_p[q, q_1]$-indecomposables $v_1, \ldots, v_s$ in $H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$, we can take a set $S = \{u_1, \ldots, u_r, v_1, \ldots, v_s\}$ such that ρ_*: $\mathbf{F}_p\{S\} \to H^1(SL_2\mathbf{Z}; M_*)$ is isomorphism. We are sufficient to show that if there is a relation $R = \sum f_i u_i + \sum g_j v_j = 0$, f_i, $g_j \in \mathbf{F}_p[q, q_1]$, then $f_i \in q\mathbf{F}_p[q, q_1]$ and $g_j = 0$ for all i, j. We prove this by induction on the degree of R. We suppose that there is no non-trivial relation R in $H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]_k)$ for $k < n$. This is obviously true for $n = p$. Now let $R = \sum f_i u_i + \sum g_j v_j$ be a relation in degree n. Let $\overline{u_i}$ and $\overline{v_j}$ be the classes of u_i and v_j in $H^1(SL_2\mathbf{Z}; Q_*)$, respectively. By Lemma 5.1, $\{\overline{u_1}, \dots, \overline{u_r}, \overline{v_1}, \dots, \overline{v_s}\}$ is a basis of the free $\mathbf{F}_p[q_1]$-module $H^1(SL_2\mathbf{Z}; Q_*)$. Then $\overline{R} = \sum f_i \overline{u_i} + \sum g_j \overline{v_j} = 0$ implies that f_i, $g_j \in q\mathbf{F}_p[q, q_1]$ for all i, j. Let $g_j = qh_j$, then we have $\sum qh_j v_j = q \sum h_j v_j = 0$, i.e., $\sum h_j v_j$ is a q-torsion. Then we have a relation $\sum h_j v_j = \sum k_i u_i$ for some k_j. But by the assumption of the induction we have $h_j = 0$ and hence $g_j = 0$ for all j. This completes the proof.

For $p = 5$, $\deg q = 6$, $\deg q_1 = 20$, $p - 1 = 4$ and $p^2 - 1 = 24$. We list the dimension of $H^1(SL_2\mathbf{Z}; M_*)$.

k	0	2	4	6	8	10	12	14	16	18	20	22	24
$\dim H^1(SL_2\mathbf{Z}; M_k)$	0	1	1	2	1	2	1	2	1	2	1	1	0
$\dim B_k$	0	1	0	1	0	1	0	0	0	1	0	0	0

6. Mod p trace formula of Hecke operators

In this section we study the Hecke operators acting on $H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$. Let A be a commutative algebra over $\mathbf{Z}[1/6]$. Let V be an $A[M_2\mathbf{Z}]$-module and let $\alpha \in M_2\mathbf{Z}$ such that $\det \alpha > 0$. Then one can define a Hecke operator

$$T(\alpha): H^i(SL_2\mathbf{Z}; V) \to H^i(SL_2\mathbf{Z}; V)$$

for $i = 0$ and 1, as follows (see [7]). Let $SL_2\mathbf{Z}\alpha SL_2\mathbf{Z}$ be the double coset, then there is a splitting

$$SL_2\mathbf{Z}\alpha SL_2\mathbf{Z} = \coprod SL_2\mathbf{Z}\alpha_i$$

into finite disjoint sum of left cosets for some $\alpha_i \in M_2\mathbf{Z}$. For $u \in H^0(SL_2\mathbf{Z}; V)$, we define

$$T(\alpha) = \sum \alpha_i u .$$

It is easy to see that this gives a well defined class in $H^0(SL_2\mathbf{Z}; V)$.

Next let $\gamma \in SL_2\mathbf{Z}$, then by the above splitting we have $\alpha_i\gamma = \gamma_i\alpha_j$ for some $\gamma_i \in SL_2\mathbf{Z}$ and some j. Let $u \in H^1(SL_2\mathbf{Z}; V)$ and let $c: SL_2\mathbf{Z} \to V$ be a 1-cocycle representing u. Then the function $\tilde{c}: SL_2\mathbf{Z} \to V$ defined by

$$\tilde{c}(\gamma) = \sum \overline{\alpha_i} c(\gamma_i) , \qquad \overline{\alpha_i} = (\det \alpha_i)\alpha^{-1}$$

is a 1-cocycle and $T(\alpha)(u)$ is defined to be the cohomology class $[\tilde{c}]$.

It is clear that a Hecke operator is natural with respect to $A[M_2\mathbf{Z}]$-homomorphisms. Let $0 \to V \to W \to U \to 0$ be a exact sequence of $A[M_2\mathbf{Z}]$-modules, then one can easily check that the connecting homomorphism

$$\delta: H^0(SL_2\mathbf{Z}; U) \to H^1(SL_2\mathbf{Z}; V)$$

commutes with Hecke operators.

For the matrix $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$, $T(\alpha)$ is denoted by $T(n)$. When we need to specify the module M on which $T(n)$ acts, we write as $T(n)|M$. In the folowing we fix a prime $p \geq 5$ and l denotes a prime different from p.

Lemma 6.1. *For $q_1 \in H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ we have*
i) $T(p)q_1^n \in q\mathbf{F}_p[x, y]$
ii) $T(l)q_1^n = (l+1)q_1^n$.

Proof. Let $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}$. Then in the splitting $SL_2\mathbf{Z}\alpha SL_2\mathbf{Z} = \coprod_{i=0}^{l} SL_2\mathbf{Z}\alpha_i$, we can take $\alpha_0 = \begin{pmatrix} l & 0 \\ 0 & 1 \end{pmatrix}$ and $\alpha_i = \begin{pmatrix} 1 & i \\ 0 & l \end{pmatrix}$ for $1 \leq i \leq l$. (Here l may be p). If $l \neq p$, then $\det \alpha_i = l \not\equiv 0 \mod p$ and hence $\alpha_i q_1^n = q_1^n$. Then by definition, $T(l)q_1^n = (l+1)q_1^n$. This shows ii). For $l = p$, $\alpha_0 x = 0$, $\alpha_0 y = y$, $\alpha_i x = x + iy$ and $\alpha_i y = 0$ in $\mathbf{F}_p[x, y]$. Then

$$T(p)q_1^n = y^{pn(p-1)} + (x+y)^{pn(p-1)} + \cdots + (x+(p-1)y)^{pn(p-1)} + x^{pn(p-1)}.$$

We write this polynomial by $f(x, y)$. Then $f(x, ix) = 0$ for any $i \in \mathbf{F}_p$ and hence

$$T(p)q_1^n = x(x+y)\dots(x+(p-1)y)yg(x, y)$$

for some $g(x, y)$. Since $x(x+y)\dots(x+(p-1)y)y = q$, the lemma is proved.

Lemma 6.2. *For $\alpha_k \in H^0(SL_2\mathbf{Z}; Q_{k(p-1)})$, we have*
i) $T(p)\alpha_k = 0$
ii) $T(l)\alpha_k = (l+1)\alpha_k$.

Proof. By Corollary 3.3, we are sufficient to show the lemma for $k = 2$. But the computation for α_2 is similar to q_1^n.

Now let $V_* = \bigoplus_{i \geq 0} V_i$ be a graded $K[M_2\mathbf{Z}]$-module over a field K. We define a power series in $K[[t]]$

$$H_t(V_*; n) = \sum_{k \geq 0} (\text{Trace}\,[T(n)|H^1(SL_2\mathbf{Z}; V_k)] - \text{Trace}\,[T(n)|H^0(SL_2\mathbf{Z}; V_k)])t^{k+2}.$$

Here $+2$ in the exponent is added to adjust the degree with the weight of modular forms.

Recall that q is not $M_2\mathbf{Z}$-invariant, in fact $\alpha q = (\det \alpha)q$. Let D be the 1-dim representation of $M_2\mathbf{Z}$ over $\mathbf{F}_p$ defined by $\alpha(v) = (\det \alpha)v$ for $\alpha \in M_2\mathbf{Z}$ and $v \in D$. Then we have an exact sequence

$$0 \to \mathbf{F}_p[x, y] \otimes D \xrightarrow{q} \mathbf{F}_p[x, y] \xrightarrow{\rho} Q_* \to 0$$

of $\mathbf{F}_p[M_2\mathbf{Z}]$-modules. The associated exact sequence

$$0 \to H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y] \otimes D) \xrightarrow{q} H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \xrightarrow{\rho_*} H^0(SL_2\mathbf{Z}; Q_*)$$
$$\xrightarrow{\delta} H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y] \otimes D) \xrightarrow{q} H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \xrightarrow{\rho_*} H^1(SL_2\mathbf{Z}; Q_*) \to 0$$

is compatible with Hecke operators. Hence we have

$$H_t(\mathbf{F}_p[x, y] \otimes D; n)t^{p+1} - H_t(\mathbf{F}_p[x, y]; n) + H_t(Q_*; n) = 0 .$$

As $\mathbf{F}_p[SL_2\mathbf{Z}]$-module, $\mathbf{F}_p[x, y] \otimes D = \mathbf{F}_p[x, y]$. Therefore we can identify $H^i(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ with $H^i(SL_2\mathbf{Z}; \mathbf{F}_p[x, y] \otimes D)$ as modules. Let $T(l)_1$ and $T(l)_2$ be Hecke operators acting on $H^i(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ and $H^i(SL_2\mathbf{Z}; \mathbf{F}_p[x, y] \otimes D)$, respectively. Then from the definition we easily have

Lemma 6.3. *$T(l)_2 = lT(l)_1$ for any prime l.*

Now the above argument shows the following

Theorem 6.4. *For any prime l, we have*

$$H_t(\mathbf{F}_p[x, y]; l) = \frac{1}{1 - lt^{p+1}} H_t(Q_*; l) .$$

Next we consider $H_t(\mathbf{R}[x, y]; l)$. Note that $H^1(SL_2\mathbf{Z}; \mathbf{R}[x, y]) \cong H^1(SL_2\mathbf{Z}; \mathbf{Z}[x, y]) \otimes \mathbf{R}$ and $H^0(SL_2\mathbf{Z}; \mathbf{R}[x, y]) \cong 0$. Hence we have

$$H_t(\mathbf{R}[x, y]; l) \in \mathbf{Z}[[t]] .$$

Lemma 6.5. *$H_t(\mathbf{R}[x, y]; l) \equiv H_t(\mathbf{F}_p[x, y]; l)$ mod p.*

Proof. Let T_* be the subgroup of p-torsion elements in $H^1(SL_2\mathbf{Z}; \mathbf{Z}_{(p)}[x, y])$. Then

$$\text{Trace}\,[T(l)|H^1(SL_2\mathbf{Z}; \mathbf{R}[x, y])] = \text{Trace}\,[T(l)|H^1(SL_2\mathbf{Z}; \mathbf{Z}_{(p)}[x, y])/T_*]$$

as above. By Theorem 2.2, we have an exact sequence

$$\begin{aligned} 0 \to H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) &\xrightarrow{\delta} H^1(SL_2\mathbf{Z}; \mathbf{Z}_{(p)}[x, y]) \\ &\xrightarrow{p} H^1(SL_2\mathbf{Z}; \mathbf{Z}_{(p)}[x, y]) \xrightarrow{\rho_*} H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \to 0 \end{aligned}$$

commuting with Hecke operators. Then we have an exact sequence

$$0 \to H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]) \to T_* \xrightarrow{p} T_* \to T_* \otimes \mathbf{F}_p \to 0 .$$

Taking generators of T_* if necessary, we easily see that

$$\text{Trace}\,[T(l)|H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]_k)] = \text{Trace}\,[T(l)|\,T_k \otimes \mathbf{F}_p] .$$

Since $H^1(SL_2\mathbf{Z}; \mathbf{Z}_{(p)}[x, y]) \otimes \mathbf{F}_p \cong H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y])$ we have

$$\begin{aligned} &\text{Trace}\,[T(l)|H^1(SL_2\mathbf{Z}; \mathbf{Z}_{(p)}[x, y]_k)/T_*] \\ &\equiv \text{Trace}\,[T(l)|H^1(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]_k)/T_*] - \text{Trace}\,[T(l)|H^0(SL_2\mathbf{Z}; \mathbf{F}_p[x, y]_k)/T_*] . \end{aligned}$$

This completes the proof.

Now let S_k be the space of cusp forms of weight k. Hecke operator $T(l)$ acts on S_k as a complex linear map and one can define $\text{Trace}\,[T(l)|S_k]$ as a complex linear map. It is known [7] that using a suitable base of S_k, $T(l)$ is represented by an integral matrix. Hence we can define

$$H_t(l) = \sum \mathrm{Trace}\,[T(l)|S_k]t^k \in \mathbf{Z}[[t]]\,.$$

Theorem 6.6. *For any prime l we have*

$$2H_t(l) \equiv \frac{1}{1 - lt^{p+1}} H_t(Q_*; l) - \sum_{k \geq 2} (1 + l^{2k-1})t^{2k} \ mod\ p\,.$$

Proof. Recall that the Eichler-Shimura theorem [7] asserts that there is an isomorphism for even integer k

$$S_k \oplus \mathbf{R}\{E_k\} \to H^1(SL_2\mathbf{Z}; \mathbf{R}[x, y]_{k-2})$$

of real vector spaces commuting with Hecke operators, where $\mathbf{R}\{E_k\}$ is the $\mathbf{R}$-vector space spanned by the Eisenstein series E_k. It is known [7] that $T(l)E_k = (1 + l^{k-1})E_k$. Note that the trace of $T(l)$ on S_k as a real linear map is the twice of that as a complex linear map. Then the theorem follows from Theorem 6.4 and Lemma 6.5.

Remark. Since $H^i(SL_2\mathbf{Z}; Q_k)$ is periodic for $k \geq p + 1$ with period $p - 1$, $H_t(Q_*; l)$ is determined from the coefficient of t^k for $k \leq 2p$. If one knows $\mathrm{Trace}\,[T(l)|S_k]$ for $k \leq 2p + 2$, then using Theorem 6.6 one can compute the mod p value of $\mathrm{Trace}\,[T(l)|S_k]$ for all k. For example let $p = 5$. We can compute $H_t(Q_*; p)$ as follows. In this case we have

$$2H_t(p) \equiv H_t(Q_*; p) + \sum_{k \geq 2} t^{2k}\,.$$

Up to weight 14 there is only one cusp form Δ of weight 12. It is known that $T(5)\Delta \equiv 0$ mod 5 and hence $H_t(5) \equiv 0$ mod 5 up to degree 14. Then by the periodicity we have

$$H_t(Q_*; 5) \equiv -\sum_{k \geq 2} t^{2k} \qquad \mathrm{mod}\ 5\,.$$

and hence we have $H_t(5) \equiv 0$ mod 5.

DEPARTMENT OF MATHEMATICS
KYOTO UNIVERSITY

References

[1] J. F. Adams, The Kahn-Priddy theorem, Proc. Camb. Phil. Soc., **73** (1973), 45–55.

[2] D. Carlisle, P. Eccles, S. Hilditch, N. Ray, L. Schwartz, G. Walker and R. Wood, Modular representations of $GL(n, p)$, splitting $\sum(\mathbf{C}P^\infty \times \cdots \times \mathbf{C}P^\infty)$, and the β-family as framed hypersurfaces, Math. Z., **189** (1985), 239–261.

[3] M. Furusawa, M. Tezuka and N. Yagita, On the cohomology of classifying spaces of torus bandle and automorphic forms, J. London Math. Soc., **37** (2) (1988), 520–534.

[4] D. J. Glover, A study of certain modular representations, J. Algebra, **51** (1978), 425–475.
[5] S. A. Mitchell, Finite complexs with $A(n)$-free cohomology, Topology, **24** (1985), 227–248.
[6] G. Nishida, Modular forms and the double transfer for BT^2.
[7] G. Shimura, Introduction to the arithmetic theory of automorphic functions, Iwanami Shoten; Tokyo, University Press; Princeton, 1971.