On the 2^n divisibility of the Fourier coefficients of J_q functions and the Atkin conjecture for $p = 2$

Shigeki Akiyama
College of General Education, Niigata University
Niigata, 950-21, JAPAN

§1. Introduction

Let f be the holomorphic modular form of weight $2k$, which is a normalized common eigenform with respect to Hecke operators. Then it is well known that the Fourier coefficient $\tau(n)$ of f satisfies the equation

$$\tau(np) - \tau(n)\tau(p) + p^{2k-1}\tau(n/p) = 0, \tag{1}$$

for any prime p and any positive integer n. Here $\tau(n/p)$ is defined to be zero when n/p is not an integer. In [2] and [3], Atkin made a similar conjecture for a modular function:

Conjecture (Atkin).
Let $j(z)$ be the modular invariant:

$$j(z) = \sum_{n \geq -1} c(n) x_3^n \quad = x_3^{-1} + 744 + 196884 x_3 + \cdots\cdots \quad ,$$

where $x_3 = \exp(2\pi\sqrt{-1}z)$. Let $p \leq 23$ be a fixed prime and l be a prime other than p. For any positive integer α, put $a_\alpha(n) = c(np^\alpha)/c(p^\alpha)$. Then the following congruences hold

$$a_\alpha(nl) - a_\alpha(n)a_\alpha(l) + l^{-1}a_\alpha(n/l) \equiv 0 \pmod{p^\alpha}, \tag{2}$$

$$a_\alpha(np) - a_\alpha(n)a_\alpha(p) \equiv 0 \pmod{p^\alpha}. \tag{3}$$

Remark 1.
Atkin asserted in [2] that $a_\alpha(n)$ are in $\mathbb{Q} \cap \mathbb{Z}_p$. The author knows the proof of this fact only for the case $p = 2, 3$ and 13. Atkin also announced in [2], that he had

proved the conjecture for $p = 2, 3, 5, 7$ and 13. But we cannot find his proofs in the literature. In [4], Atkin and O'Brien showed the congruence (3) for $p = 13$. Koike showed the congruence (2) for $p = 13$ in [8] and completed the proof for $p = 13$. Koike's work suggests us that, at least, Atkin had been in the right direction to the proof for $p = 13$. There seems no published proof for other primes.

Remark 2.

This conjecture is a p-adic version of (1). Thus the conjecture gives us the starting point of the vast theory of p-adic modular forms and p-adic Hecke operators (see Katz [7], Dwork [5], Serre [11]).

In this article, we will prove the Atkin conjecture for $p = 2$ in more precise form:

Theorem 1.

Let α be a positive integer and $a_\alpha(n) = c(2^\alpha n)/c(2^\alpha)$. Then we have, for any odd prime l,

$$a_\alpha(nl) - a_\alpha(n)a_\alpha(l) + l^{-1}a_\alpha(n/l) \equiv 0 \pmod{2^{4\alpha+4}}, \quad (4)$$

$$a_\alpha(2n) - a_\alpha(n)a_\alpha(2) \equiv 0 \pmod{2^{4\alpha+7}}. \quad (5)$$

Remark 3.

Atkin already noticed in [2], that when $p \leq 5$, the exponent of the prime p of the congruence (2) and (3) is not best possible. As for this exponent of (4) and (5), see the last part of §4 and Remark 7 in §5.

The original purpose of the study is to prove the 2^n divisibility property of Hecke's absolute invariant such as the conjecture (A) in §2. Fortunately, the author found that his argument was very close to the Atkin conjecture for $p = 2$. First, we will introduce Hecke's absolute invariants.

§2. Hecke's absolute invariants.

Let G_q be the Hecke group, which is a discontinuous subgroup of $PSL_2(\mathbb{R})$ generated by

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & \lambda_q \\ 0 & 1 \end{pmatrix},$$

where $\lambda_q = 2\cos(\pi/q)$ and $q = 3, 4, \cdots\cdot, \infty$. The standard fundamental domain of G_q, as a transformation group of a complex upper half plane $\mathbb{H}$, is given by

$$\mathcal{F}_q = \{z \in \mathbb{H} \ : \ |z| \geq 1, \ |Re(z)| \leq \lambda_q/2\}.$$

Let J_q be the bijective conformal mapping from " the half of $\mathcal{F}_q$", that is,

$$\{z \in \mathbb{H} \ : \ |z| \geq 1, \ -\lambda_q/2 \leq Re(z) \leq 0\} \cup \{\sqrt{-1}\infty\},$$

to $\mathbb{H}$. This mapping is uniquely determined by the conditions:

$$J_q(-\exp(-\pi\sqrt{-1}/q)) = 0, \quad J_q(\sqrt{-1}) = 1, \quad J_q(\sqrt{-1}\infty) = \infty.$$

Using reflection principle repeatedly, we can define the value of J_q on $\mathbb{H}$ and consider J_q as a mapping from $\mathbb{H}$ to $\mathbb{C}$. From this construction we see that

$$J_q(\gamma z) = J_q(z)$$

for any $\gamma \in G_q$. The automorphic function field of G_q is nothing but a rational function field generated by J_q over $\mathbb{C}$. This function J_q is called Hecke's absolute invariant with respect to G_q. Since J_q is invariant under the transformation $z \longrightarrow z+\lambda_q$, we have the Fourier expansion of J_q at $\sqrt{-1}\infty$:

$$J_q(z) = \sum_{n\geq -1} A_q(n) x_q^n,$$

where $x_q = \exp(2\pi\sqrt{-1}z/\lambda_q)$. J. Raleigh [10] showed

$$A_q(n) = r_q^n B_q(n),$$

where $r_q \in \mathbb{R},\ B_q(n) \in \mathbb{Q}$. The value r_q is determined up to rational multiples, so we put $r_q^{-1} = A_q(-1)$ and $B_q(-1) = 1$. The actual value is

$$r_q = \exp\left(2\frac{\Gamma'(1)}{\Gamma(1)} - \frac{\Gamma'(1/4+1/2q)}{\Gamma(1/4+1/2q)} - \frac{\Gamma'(1/4-1/2q)}{\Gamma(1/4-1/2q)} - \frac{1}{\cos(\pi/q)}\right),$$

where $\Gamma(s)$ is the gamma function. Further, J. Wolfart [12] showed that r_q is algebraic if and only if $q = 3, 4, 6, \infty$. So we treat only the case $q = 3, 4, 6, \infty$ in the following. Let $j_q(z) = r_q J_q(z)$ then $j_q(z)$ is contained in $\mathbb{Z}[x_q, x_q^{-1}]$. Put

$$j_q(z) = \sum_{n\geq -1} c_q(n) x_q^n,$$

where $c_q(n) \in \mathbb{Z}$ and $c_q(-1) = 1$. Consider the case $q = 3$. Then $G_3 = PSL(2,\mathbb{Z})$ and $j_3(z)$ coincides with the modular invariant $j(z)$ appeared in the introduction. From now on, write $c(n)$ instead of $c_3(n)$. The first few values of $c_q(n)$ are found in Table 1.

The author proposed conjectures concerning $c_q(n)$ as a rational function of q in [1]. As a special case, we see:

Conjecture.

For all integer n, we have

$$ord_2(c(n)) = ord_2(c_4(n)) = ord_2(c_\infty(n)),$$

$$ord_3(c(n)) = ord_3(c_6(n)).$$

For the later convenience, we call the statement

$$ord_2(c(n)) = ord_2(c_\infty(n))$$

to be conjecture (A). In the next section, we will take a close look at this conjecture (A).

§3. O.Kolberg's results and the conjecture (A).

Note that G_∞ is a subgroup of index 3 of G_3, this is the reason why we first treat the conjecture (A) among others. (The group G_∞ is called theta group.) Thus there exist an algebraic relation between j and j_∞:

$$j(z) = (j_\infty(z) - 2^4)^3/j_\infty(z).$$

Considering $x_\infty^2 = x_3$, we easily see that

$$c(n) \equiv c_\infty(n) \pmod 2, \tag{6}$$

which is our first knowledge about the conjecture (A). Using the famous λ-invariant, which is a generator of the automorphic function field with respect to principal congruence subgroup of level two, we can express j_∞ as

$$j_\infty(z) = -\frac{16}{\lambda(z)(\lambda(z)-1)}.$$

Moreover, employing the expression of $\lambda(z)$ by theta null series, we have

$$j_\infty(z) = x_\infty^{-1} \prod_{n \geq 1} (1 + x_\infty^{2n-1})^{24}.$$

From this infinite product representation, we see

$$j_\infty\left(\frac{z-1}{2}\right) j_\infty\left(\frac{z+1}{2}\right) = j_\infty(z). \tag{7}$$

And we also have

$$j_\infty\left(\frac{z-1}{2}\right) + j_\infty\left(\frac{z+1}{2}\right) = 48 - \frac{2^{12}}{j_\infty(z)}. \tag{8}$$

Note that the left hand side of (8) is the result of the action of the double coset $G_\infty\left(\begin{smallmatrix} 1 & 1 \\ 0 & 2 \end{smallmatrix}\right)G_\infty$ as a Hecke operator on j_∞.

These two relations (7) and (8) seem to be fundamental. Define the action V by

$$f(z)|V = f\left(\frac{z-1}{2}\right) + f\left(\frac{z+1}{2}\right).$$

Remark that $j(2z) + j(z/2)$ is invariant under G_∞ and

$$j(z)|T(2) = j(2z) + j(z/2) + j\left(\frac{z+1}{2}\right).$$

Here $T(n)$ is the Hecke operator of degree n with respect to G_3. This shows that $j\left(\frac{z+1}{2}\right)$ is contained in $\mathbb{C}(j_\infty)$. A precise calculation shows

$$j\left(\frac{z+1}{2}\right) = -j_\infty(z)^{-2}(j_\infty(z) - 2^8)^3 \tag{9}$$

$$= -j_\infty(z) + 2^5 \cdot 3 \cdot 7 + j_\infty|V^2. \tag{10}$$

Here the symbol $j_\infty|V^2$ means $(j_\infty|V)|V$. The last formula (10) is verified by the repeated use of (7) and (8). Comparing coefficients of (10), we have, for $n \geq 1$,

$$c(n) = (-1)^{n-1}c_\infty(n) + 4c_\infty(4n). \tag{11}$$

This formula, together with the product (or theta) representation of j_∞, gives us an easy alternative way of calculating $c(n)$. The author does not know that someone had mentioned this formula (11) before. Using (11) , by the aid of computer calculations, our conjecture (A) is reduced to the following:

Conjecture (B).

For any positive integer n, we have $ord_2(c_\infty(2n)) \geq 3 + ord_2(c_\infty(n))$.

Conjecture (B')

For any positive integer n, we have $ord_2(c(2n)) \geq 3 + ord_2(c(n))$.

Note that the conjecture (B) and the conjecture (B') are equivalent, which is easily seen by (11). Numerical calculations suggest that the equality holds in both (B) and (B') when n is even. Concerning the conjecture (B'), O. Kolberg [9] showed:

Proposition 1 (O.Kolberg).

For any positive integer α and odd integer n, we have

$$c(2^\alpha n) \equiv -2^{3\alpha+8}3^{\alpha-1}\sigma_7(n) \pmod{2^{3\alpha+13}}. \tag{12}$$

For any positive integer n,

$$c(8n+1) \equiv 20\sigma_7(8n+1) \pmod{2^7},$$

$$c(8n+3) \equiv \sigma_1(8n+3)/2 \pmod{2^3},$$

$$c(8n+5) \equiv -12\sigma_7(8n+5) \pmod{2^8},$$

where $\sigma_s(n) = \sum_{d|n} d^s$. The value of $c(8n+7)$ becomes both even and odd infinitely often.

This proposition implies the validity of the conjecture (B) and (A) for a certain type of n. For example, if

$$n = 2^\beta m, \;\; m \equiv 1 \pmod 8, \;\; \sigma_7(m) \not\equiv 0 \pmod{2^5}, \tag{13}$$

where β is any non negative integer. Then

$$ord_2(c(2n)) \geq 3 + ord_2(c(n))$$

holds. Using (11), we see that

$$ord_2(c_\infty(2n)) \geq 3 + ord_2(c_\infty(n)).$$

Thus again by (11),

$$ord_2(c(n)) = ord_2(c_\infty(n))$$

holds for every n of type (13). To prove Proposition 1, O. Kolberg explicitly calculated $j_\infty^{-n}|V^k$ for each positive integer n and k. And this calculation is crucial in proving the Atkin conjecture for $p = 2$ in §4.

Remark 4.

Define the operator $U(2)$ by

$$\sum a(n) x_3^n | U(2) = \sum a(2n) x_3^n.$$

By using the results of Koike [8], there exists a unique modular cusp form F of weight 2^{t-1} such that

$$j(z)|U(2)^m - 744 \equiv F(z) \pmod{2^t}. \tag{14}$$

It is well known that the space of modular cusp forms is decomposed into common eigenspaces with respect to Hecke operators. Thus

$$F(z) = \sum_i F_i(z),$$

and each F_i is a common eigenfunction of eigenvalue λ_i. If $t \geq 3$ then the action of Hecke operator of degree two and of weight 2^{t-1} coincides with that of $U(2)$ modulo 2^t. K. Hatada showed in [6],

$$\lambda_i \equiv 0 \pmod 8.$$

Thus we have

$$j(z)|U(2)^{m+1} - 744 \equiv \sum \lambda_i F_i(z) \pmod{2^t}. \tag{15}$$

Comparing (14) and (15), we see that the conjecture (B') seems to be reasonable.

§4. Proof of the Atkin conjecture for $p = 2$.

In this section, we prove Theorem 1 cited in the introduction in a slightly stronger form. Our discussion is almost the same as in the proof of Koike [8]. So the precise description will be omitted if not necessary. We also use the idea of Atkin-O'Brien [4] and the results of O. Kolberg [9].

Let S_k be the space of modular cusp forms of weight k and $S(\alpha, \lambda)$ be the $\mathbb{Z}$ sub-module of $S_{\lambda+2^{\alpha-1}}$ whose elements have integer Fourier coefficients in the expansion at the cusp $\sqrt{-1}\infty$. Denote by $d(\alpha, \lambda)$ the dimension of $S_{\lambda+2^{\alpha-1}}$. Then $S(\alpha, \lambda)$ has rank $d(\alpha, \lambda)$. Let $\alpha' > \alpha \geq 3$ be two positive integers. Then for each $f \in S(\alpha, \lambda)$, there exists $f' \in S(\alpha', \lambda)$ such that $f' \equiv f \pmod{2^\alpha}$, where the symbol $\equiv$ means that the corresponding Fourier coefficients are congruent modulo 2^α. Thus there exists a system of free basis $\{f_{\alpha,i}^{(\lambda)}\}_{i=1}^{d(\alpha,\lambda)}$ of $S(\alpha, \lambda)$ such that

$$f_{\alpha,i}^{(\lambda)} \equiv f_{\alpha',i}^{(\lambda)} \pmod{2^\alpha}$$

for any $\alpha' > \alpha \geq 3$. Let $\tilde{f}_i^{(\lambda)}$ be the 2-adic limit of $f_{\alpha,i}^{(\lambda)}$ when α tends to infinity. Define by $S(\lambda)$ the set consisting of all elements $\sum a_i \tilde{f}_i^{(\lambda)}$ such that $a_i \in \mathbb{Q}_2$ and there are only finitely many a_i's for which $ord_2(a_i) < t$ for any positive integer t. This space is called 2-adic Banach space admitting orthonormal basis $\{\tilde{f}_i^{(\lambda)}\}_i$ over $\mathbb{Q}_2$. Itis known that $S(0)$ admits orthonormal basis $\{j(z)^{-i}\}_{i=1}^{\infty}$. Let l be an odd prime. The 2-adic Hecke operator $\tilde{U}_\lambda(2)$ and $\tilde{T}_\lambda(l)$ acting on $S(\lambda)$ is defined by

$$\tilde{f}|\tilde{U}_\lambda(2) = \sum A(2n) x_3^n,$$

$$\tilde{f}|\tilde{T}_\lambda(l) = \sum \{A(nl) + l^{\lambda-1} A(n/l)\} x_3^n,$$

for $\tilde{f} = \sum A(n) x_3^n$. We define $A(n/l)$ to be zero when n is not a multiple of l.

Proposition 2.
The space $S(0)$ admits orthonormal basis $\{j_\infty(2z+1)^{-i}\}_{i=1}^{\infty}$.

Proof) Let $j^{(0)}(z) = j(z) - 744$ and $j_\infty^{(0)}(z) = j_\infty(z) - 24$. Then by (11),

$$j^{(0)}(z) = -j_\infty^{(0)}(2z+1) + 4 j_\infty^{(0)}(2z+1)|U(2)^2.$$

Thus $j_\infty^{(0)}(2z+1)$ is 2-adically approximated by $-\sum_{i=0}^{\infty} 2^{2i} j^{(0)}(z)|U(2)^{2i}$. By using Theorem 1 of Koike [8], $j^{(0)}(z)|U(2)^i$ belongs to $S(0)$ when $i \geq 1$. From (8),

$$j_\infty(2z+1)^{-1} = 2^{-12}\{48 - 2 j_\infty(2z+1)|U(2)\}.$$

This shows $j_\infty(2z+1)^{-1}$, so $j_\infty(2z+1)^{-i}$ for $i \geq 1$, belongs to $S(0)$. By the congruence (6), we have

$$j_\infty^{-i}(2z+1) \equiv j(z)^{-i} \pmod 2.$$

Recalling $S(0)$ admits an orthonormal basis $\{j(z)^{-i}\}_{i=1}^{\infty}$, we see the assertion.

Note that

$$\xi = -j_\infty(2z+1)^{-1} = x_3 \prod_{n\geq 1}(1+x_3^n)^{24}.$$

In [9], O. Kolberg showed, for any positive integer k

$$\xi^{2k-1}|U(2) = \sum_{j=0}^{3k-2} 2^{8j+3}\frac{6k-3}{2j+1}\binom{3k+j-2}{2j}\xi^{k+j}, \tag{16}$$

$$\xi^{2k}|U(2) = \sum_{j=0}^{3k} 2^{8j}\frac{3k}{3k+j}\binom{3k+j}{2j}\xi^{k+j}. \tag{17}$$

He derived these formulas by the elementary argument of trigonometric function. Koike's proof of the Atkin conjecture for $p = 13$ essentially needs the same type of calculation due to Atkin-O'Brien [4].

Let $\mathcal{F}$ be the $\mathbb{Z}_2$ submodule of $S(0)$ consisting of all elements:

$$\sum_{r\geq 1} a_r \xi^r,$$

where $a_r \in \mathbb{Z}_2$ and $ord_2(a_r) \geq 8(r-1)$. We define the operator $U'(2) = 2^{-3}U(2)$ on $S(0)$. Then by (16) and (17), we see

$$2^{8r-8}\xi^r|U'(2) = \sum_{j\geq r/2}^{2r} 2^{8j-8}c_{r,j}\xi^j, \tag{18}$$

where $c_{r,j}$ are integers for which $ord_2(c_{r,j}) \geq 4r-4$ and $c_{1,1}$ is odd. This shows that $U'(2)$ acts on $\mathcal{F}$. Moreover, also by (18), the eigenfunction of $\tilde{U}'(2) = 2^{-3}\tilde{U}_0(2)$ on $\mathcal{F}$ whose eigenvalue is a unit of $\mathbb{Z}_2$ exists uniquely up to $\mathbb{Q}_2^\times$ multiples. For abbreviation, we call an eigenfunction with a unit eigenvalue to be a unit eigenfunction.

Remark 5.

For the case $p = 13$, the action of $\tilde{U}_0(13)$ and the uniqueness of the unit eigenfunction were considered on the <u>whole</u> space. But in our case, we must restrict the action to $\mathcal{F}$ and consider $\tilde{U}'(2)$ instead of $\tilde{U}(2)$ to separate a unique unit eigenfunction.

Let $\mathcal{M}$ be the $\mathbb{Z}_2$ module generated by $\{\ f|U'(2)^n\colon\ f \in \mathbb{Z}_2[j(z)],\ n \geq 0\ \}$. Then we have

Proposition 3.

For any $f \in \mathcal{M}$, there exist a unique $h \in \mathbb{Z}_2[j(z)]$ and $g \in \mathcal{F}$ such that $f = h + 2^8 g$.

Proof) By the Theorem 1 of Koike [8], there exist a unique $h \in \mathbb{Z}_2[j(z)]$ and $g \in S(0)$ such that $f = h + g$. Thus we have to show $g \in 2^8\mathcal{F}$. As the operator $U'(2)$ acts on $\mathcal{F}$, it suffices to show the assertion on $j(z)^k|U'(2)$ for $k \geq 1$. From (9), we have

$$j(z) = -j_\infty(2z+1) + 3 \cdot 2^8 - 3 \cdot 2^{16} j_\infty(2z+1)^{-1} + 2^{24} j_\infty(2z+1)^{-2}.$$

By the repeated use of this formula, it is sufficient to show that $j_\infty(2z+1)^k|U'(2)$ can be decomposed into $h_1 \in \mathbb{Z}_2[j_\infty(2z+1)]$ and $g_1 \in 2^8\mathcal{F}$. We proceed this proof by induction. By (8), we see

$$j_\infty(2z+1)|U'(2) - 3 = -2^8 j_\infty(2z+1)^{-1} \in 2^8\mathcal{F}.$$

So it is true for $k = 1$. Note that by (7),

$$j_\infty(2z+1)^{k+1}|U'(2) =$$
$$2^4 \left(j_\infty(2z+1)^k|U'(2)\right)\left(j_\infty(2z+1)|U'(2)\right) - j_\infty(2z+1)\left(j_\infty(2z+1)^{k-1}|U'(2)\right).$$

We easily complete the proof from this formula.

Proposition 4.

Let $2^8 f \in \mathcal{M}$ such that $f = \sum_{n\geq 1} a(n)x_3^n$ with $a(1) \not\equiv 0 \pmod 2$. Then there exists a constant $k_\alpha \in \mathbb{Z}_2^\times$ such that

$$f|\tilde{U'}(2)^{\alpha+1} \equiv k_\alpha f|\tilde{U'}(2)^\alpha \pmod{2^{4\alpha+8}},$$

for each non negative integer α.

Proof) The idea of the proof is due to Atkin-O'Brien [4]. So precise calculations will be omitted. By Proposition 3, we see $f|\tilde{U'}(2)^\alpha \in \mathcal{F}$. Thus $f|\tilde{U'}(2)^\alpha$ is written in the form

$$\sum_{j\geq 1} 2^{8(j-1)} d_j(\alpha)\xi^j, \tag{19}$$

where $d_j(\alpha) \in \mathbb{Z}_2$. Then by (18),

$$d_j(\alpha+1) = \sum_{r\geq j/2}^{2j} d_r(\alpha)c_{r,j},$$

and $ord_2(c_{r,j}) \geq 4r - 4$. Put

$$\gamma_{ij}(\alpha) = d_j(\alpha+1)d_i(\alpha) - d_j(\alpha)d_i(\alpha+1).$$

The key of the proof is the relation;

$$\gamma_{ij}(\alpha+1) = \sum_{k,l} \gamma_{kl}(\alpha)c_{k,i}c_{l,j},$$

where integers k, l are taken over $i/2 \le k \le 2i$ and $j/2 \le l \le 2j$. By induction, we have

$$ord_2(\gamma_{ij}(\alpha)) \ge 4\alpha + 4\max\{0, [(i+j-5)/2]\},$$

where $[x]$ stands for the greatest integer not exceeding x. Especially we see

$$d_j(\alpha+1)d_1(\alpha) \equiv d_j(\alpha)d_1(\alpha+1) \pmod{2^{4\alpha}}.$$

Our assumption implies $d_1(\alpha) \not\equiv 0 \pmod 2$. So we put $k_\alpha = d_1(\alpha+1)/d_1(\alpha)$. Thus

$$d_j(\alpha+1) \equiv k_\alpha d_j(\alpha) \pmod{2^{4\alpha}}.$$

Substitute this congruence into (19), we get

$$f|\tilde{U'}(2)^{\alpha+1} = \sum_{j\ge1} 2^{8j-8} d_j(\alpha+1)\xi^j$$

$$\equiv k_\alpha \sum_{j\ge1} 2^{8j-8} d_j(\alpha)\xi^j = k_\alpha f|\tilde{U'}(2)^\alpha \pmod{2^{4\alpha+8}}.$$

Here we use the fact $d_1(\alpha+1) = k_\alpha d_1(\alpha)$ to make bigger the exponent of 2 of the congruence. This completes the proof.

Remark 6.
Put $a(n) = 2^{-11}c(2n)$, then $f = \sum_{n\ge1} a(n)x_3^n$ satisfies the assumption of Proposition 4. So we have

$$2^{-3\alpha-11}c(2^{\alpha+1}n) \equiv k_{\alpha-1}2^{-3\alpha-8}c(2^\alpha n) \pmod{2^{4(\alpha-1)+8}},$$

for any positive integer n and α. Using this, we have

$$c(2^{\alpha+1}n)c(2^\alpha) \equiv c(2^\alpha n)c(2^{\alpha+1}) \pmod{2^{10\alpha+23}}.$$

This implies the congruence (5) in Theorem 1, because

$$ord_2(c(2^\alpha)) = 3\alpha + 8,$$

which is seen by (12).

Now we state our main theorem.

Theorem 2.
Let l be an odd prime. Let $2^8 f$ be an element of $\mathcal{M}$ expanded as $f = \sum_{n\ge1} a(n)x_3^n$ with $a(1) \not\equiv 0 \pmod 2$. Then we have, for any positive integer n,

$$b_\alpha(nl) - b_\alpha(n)b_\alpha(l) + l^{-1}b_\alpha(n/l) \equiv 0 \pmod{2^{4\alpha+8}},$$

where $b_\alpha(n) = a(2^\alpha n)/a(2^\alpha)$ and α is any non negative integer.

Proof) By Proposition 4, we have

$$f|\tilde{U}'(2)^\alpha = 2^{-3\alpha}\sum_{n\geq 1} a(2^\alpha n)x_3^n \quad \equiv k_{\alpha-1}k_{\alpha-2}\cdot\cdots\cdot k_0 f \qquad (\text{mod } 2^8).$$

Especially, this shows $ord_2(a(2^\alpha n)) \geq 3\alpha$ and equality holds when $n = 1$. Thus $b_\alpha(n) \in \mathbb{Z}_2$. Put $f_\alpha = \sum b_\alpha(n)x_3^n$ then, by Proposition 4,

$$f_{\alpha+1} \equiv f_\alpha \quad (\text{mod } 2^{4\alpha+8}).$$

Let f' be the 2-adic limit of $\{f_\alpha\}$. Then, by definition

$$f|\tilde{U}'(2) = \kappa f,$$

where $\kappa \in \mathbb{Z}_2^\times$. Recalling that $\tilde{U}'(2)$ and $\tilde{T}_0(l)$ are commutative, $f'|\tilde{T}_0(l)$ is also an eigenfunction of $\tilde{U}'(2)$. By the uniqueness of the unit eigenfunction of $\tilde{U}'(2)$, we see $f'|\tilde{T}_0(l) = b(l)f'$ for some $b(l)$. Considering this equality modulo $2^{4\alpha+8}$, we get the result.

From this theorem, we can show Theorem 1 as a corollary. To see this we have to specialize $a(n) = 2^{-11}c(2n)$, as in Remark 6.

The exponent $4\alpha + 8$ of Theorem 2 can be replaced by $4\alpha + 9$. So we can also show that (4) holds modulo $2^{4\alpha+5}$. This little improvement follows from the fact that $b(l) \equiv 0$ (mod 2) in the above proof, which is shown by the precise argument similar to the proof of (12). We expect that the exponent of Theorem 2 will be improved to $4\alpha + 15$, as in Remark 7.

§5. Further conjectures.

By the aid of computer calculations, we will propose a more precise conjecture. To describe this, define

$$\Xi(n,\alpha,p) = \left(\begin{array}{ll} ord_2(a_\alpha(np) - a_\alpha(n)a_\alpha(p) + p^{-1}a_\alpha(n/p)), & \text{for odd prime } p, \\ ord_2(a_\alpha(2n) - a_\alpha(2)a_\alpha(n)), & \text{for } p = 2, \end{array}\right.$$

for any positive integer α and $n \geq 2$. Recall that $a_\alpha(n) = c(2^\alpha n)/c(2^\alpha)$. Then we have

Conjecture (C).

There exists non negative integer valued function γ from the set of integers greater than 1 such that

$$\Xi(n, \alpha, p) = 4\alpha + 7 + \gamma(p) + \gamma(n).$$

For odd n, we have

$$\gamma(n) \geq (1 + (2/n))/2 + (1 + (-1/n)) + 4,$$

where $(\cdot/n)$ is the Jacobi symbol. Equality holds when $(2/n) = -1$ and n is an odd prime. For even integers, we have

$$\gamma(2^\beta m) = 3(\beta - 1) + ord_2(\sigma_1(m)),$$

for any odd integer m and positive integer β.

Remark 7.

In special cases, the above conjecture (C) says that the exponent $4\alpha + 7$ of (5) is best possible and that of (4) can be replaced by $4\alpha + 11$, which is best possible. To see this, consider the case $p = 2$ or $p \equiv 3 \pmod 8$ and $n = 2m^2$ with an odd integer m.

The conjecture (C) gives us an impression that something interesting remain unrecognized in the Atkin conjecture for $p = 2$. We give first 100 values of $\gamma(n)$ in Table 2.

Table 1.

n	$q=3$
0	$2^3 \cdot 3 \cdot 31$
1	$2^2 \cdot 3^3 \cdot 1823$
2	$2^{11} \cdot 5 \cdot 2099$
3	$2 \cdot 3^5 \cdot 5 \cdot 355679$
4	$2^{14} \cdot 3^3 \cdot 45767$
5	$2^3 \cdot 5^2 \cdot 2143 \cdot 777421$
6	$2^{13} \cdot 3^6 \cdot 11 \cdot 13^2 \cdot 383$
7	$3^3 \cdot 5 \cdot 7 \cdot 271 \cdot 174376673$
8	$2^{17} \cdot 3 \cdot 5^3 \cdot 199 \cdot 41047$
9	$2^2 \cdot 3^7 \cdot 5 \cdot 4723 \cdot 15376021$
10	$2^{12} \cdot 3^5 \cdot 5^2 \cdot 13^2 \cdot 5366467$
11	$2 \cdot 3 \cdot 11 \cdot 13^3 \cdot 1008344102147$
12	$2^{16} \cdot 3^5 \cdot 5 \cdot 10980221089$
13	$2^3 \cdot 3^3 \cdot 5 \cdot 23 \cdot 112291 \cdot 1746673133$
14	$2^{14} \cdot 7 \cdot 281 \cdot 96457 \cdot 8202479$
15	$3^6 \cdot 5^2 \cdot 7 \cdot 1483 \cdot 666739430527$

n	$q=4$	$q=6$	$q=\infty$
0	$2^3 \cdot 13$	$2 \cdot 3 \cdot 7$	$2^3 \cdot 3$
1	$2^2 \cdot 1093$	$3^3 \cdot 29$	$2^2 \cdot 3 \cdot 23$
2	$2^{11} \cdot 47$	$2^5 \cdot 271$	2^{11}
3	$2 \cdot 3^3 \cdot 22963$	$3^5 \cdot 269$	$2 \cdot 3 \cdot 1867$
4	$2^{14} \cdot 653$	$2^6 \cdot 3^3 \cdot 5 \cdot 43$	$2^{14} \cdot 3$
5	$2^3 \cdot 5 \cdot 13 \cdot 41 \cdot 3491$	$5 \cdot 163 \cdot 2137$	$2^3 \cdot 23003$
6	$2^{13} \cdot 3^3 \cdot 1951$	$2^5 \cdot 3^6 \cdot 307$	$2^{13} \cdot 3 \cdot 5^2$
7	$3^4 \cdot 7 \cdot 1801 \cdot 2161$	$2 \cdot 3^3 \cdot 53 \cdot 9283$	$3 \cdot 337 \cdot 1861$
8	$2^{17} \cdot 77191$	$2^7 \cdot 3 \cdot 19^2 \cdot 653$	$2^{17} \cdot 41$
9	$2^2 \cdot 3^5 \cdot 59 \cdot 743129$	$3^7 \cdot 157 \cdot 839$	$2^2 \cdot 3 \cdot 5 \cdot 241303$
10	$2^{12} \cdot 5 \cdot 7 \cdot 1063 \cdot 1093$	$2^6 \cdot 3^5 \cdot 5 \cdot 7^2 \cdot 227$	$2^{12} \cdot 3^2 \cdot 19 \cdot 53$
11	$2 \cdot 23 \cdot 281 \cdot 523 \cdot 90499$	$2 \cdot 3 \cdot 17 \cdot 97 \cdot 103 \cdot 2423$	$2 \cdot 5^2 \cdot 53 \cdot 173 \cdot 199$
12	$2^{16} \cdot 3^3 \cdot 17^2 \cdot 4157$	$2^6 \cdot 3^5 \cdot 433931$	$2^{16} \cdot 3 \cdot 7 \cdot 157$
13	$2^3 \cdot 5 \cdot 491 \cdot 953 \cdot 376153$	$3^3 \cdot 613 \cdot 1072231$	$2^3 \cdot 3 \cdot 11 \cdot 1875943$
14	$2^{14} \cdot 3^3 \cdot 7 \cdot 7210349$	$2^{10} \cdot 5 \cdot 37 \cdot 238001$	$2^{14} \cdot 3 \cdot 11 \cdot 2039$
15	$3^4 \cdot 5 \cdot 7 \cdot 24033246929$	$3^6 \cdot 5 \cdot 31 \cdot 43 \cdot 22859$	$3^2 \cdot 15913 \cdot 16691$

Table 2.

n	$\gamma(n)$	n	$\gamma(n)$	n	$\gamma(n)$	n	$\gamma(n)$	n	$\gamma(n)$
1		21	8	41	8	61	6	81	7
2	0	22	2	42	5	62	5	82	1
3	4	23	5	43	4	63	5	83	4
4	3	24	8	44	5	64	15	84	8
5	6	25	8	45	6	65	8	85	7
6	2	26	1	46	3	66	4	86	2
7	5	27	5	47	6	67	4	87	5
8	6	28	6	48	11	68	4	88	8
9	7	29	6	49	9	69	8	89	7
10	1	30	3	50	0	70	4	90	1
11	4	31	7	51	5	71	5	91	6
12	5	32	12	52	4	72	6	92	6
13	6	33	7	53	6	73	7	93	10
14	3	34	1	54	3	74	1	94	4
15	5	35	6	55	5	75	4	95	5
16	9	36	3	56	9	76	5	96	14
17	7	37	6	57	7	77	8	97	7
18	0	38	2	58	1	78	3	98	0
19	4	39	5	59	4	79	6	99	4
20	4	40	7	60	6	80	10	100	3

References

1. S. Akiyama, A note on Hecke's absolute invariants, J. Ramanujan Math. Soc., **7** (1992), 65-81.
2. A.O.L. Atkin, Congruence for modular forms, Proc. IBM Conf. on computers mathematical research, Blaricum 1966, (North Holland).
3. A.O.L. Atkin, Congruence Hecke operators, Proc. Symp. Pure Math., vol. **12**, 33-40.
4. A.O.L. Atkin and J.N. O'Brien, Some properties of $p(n)$ and $c(n)$ modulo powers of 13, Trans. Amer. Math. Soc., **126** (1967), 442-459.
5. B. Dwork, The U_p operator of Atkin on modular functions of level 2 with growth conditions, Lecture Notes in Math., **350** (1973), 57-67
6. K. Hatada, Eigenvalues of Hecke Operators on $SL(2,\mathbb{Z})$, Math. Ann.,**239** (1979), 75-96.
7. N. Katz, p-adic properties of modular schemes and modular forms, Lecture Notes in Math., **350** (1973), 69-190

8. M. Koike, Congruences between modular forms and functions and applications to the conjecture of Atkin, J. Fac. Sci. Univ. Tokyo Sect. IA Math., **20** (1973), 129-169.
9. O. Kolberg, Congruences for the coefficients of the modular invariant $j(\tau)$ modulo powers of 2, Årbok Univ. Bergen, **16** (1961), 1-9.
10. J. Raleigh, On the Fourier coefficients of triangle groups, Acta Arith., **8** (1962), 107-111.
11. J-P. Serre, Formes modulaires et fonctions zêta p-adiques, Lecture Notes in Math., **350** (1973), 191-268.
12. J. Wolfart, Transzendente Zahlen als Fourierkoeffizienten von Heckes Modulformen, Acta Arith., **39** (1981), 193-205.