A REDUCTION THEOREM OF CERTAIN RELATIONS MODULO p INVOLVING MODULAR FORMS

CRISTIAN-SILVIU RADU

Dedicated to my advisor and friend Peter Paule on the occasion of his 60th birthday

Abstract. Let p be a prime. Let $\mathcal{A}_k^1(N)$ be the set of meromorphic modular forms of weight k for the group $\Gamma_1(N)$ and $\mathcal{A}^1(N) := \oplus_{k=-\infty}^{\infty}\mathcal{A}_k^1(N)$. Let $f_j(\tau) = \sum_{n=m_j}^{\infty} a_j(n)q^n \in \mathcal{A}^1(N)$, $j = 0, \ldots, \nu$ and $q = e^{2\pi i\tau}$ such that $a_j(n)$ are integers. The main result of this paper is that

$$f_0(\tau) + qf_1(\tau) + q^2f_2(\tau) + \cdots + q^{\nu}f_{\nu}(\tau) \equiv 0 \pmod{p}$$

iff

$$f_0(\tau) \equiv f_1(\tau) \equiv f_2(\tau) \equiv \cdots \equiv f_{\nu}(\tau) \equiv 0 \pmod{p}.$$

1. Introduction

Let p be a prime. Let $\mathcal{A}_k^1(N)$ be the set of meromorphic modular forms of weight k for the group $\Gamma_1(N)$ and $\mathcal{A}^1(N) := \oplus_{k=-\infty}^{\infty}\mathcal{A}_k^1(N)$. Let $f_j(\tau) = \sum_{n=m_j}^{\infty} a_j(n)q^n \in \mathcal{A}^1(N)$, $j = 0, \ldots, \nu$ and $q = e^{2\pi i\tau}$ such that the $a_j(n)$ are integers. The main result of this paper is that

$$f_0(\tau) + qf_1(\tau) + q^2f_2(\tau) + \cdots + q^{\nu}f_{\nu}(\tau) \equiv 0 \pmod{p} \tag{1}$$

iff

$$f_0(\tau) \equiv f_1(\tau) \equiv f_2(\tau) \equiv \cdots \equiv f_{\nu}(\tau) \equiv 0 \pmod{p}. \tag{2}$$

This result is also important from an algorithmic point of view because if we want to design an algorithm to prove relations like (1) we see that we only need to prove congruences modulo p between meromorphic modular forms.For this situation there are well-known proving tools like Sturm's theorem, etc.

In this regard there is a lot of theory developed which allows automatisation of proving such relations.

The organization of this paper is as follows. In Section 2 we introduce basic definitions and notions. In Section 3 the main result of this paper is proven, namely the implication (1)⇒(2).

The research was funded by the Austrian Science Fund (FWF), W1214-N15, project DK6 and by grant P2016-N18. The research was supported by the strategic program "Innovatives OÖ 2010 plus" by the Upper Austrian Government.

2010 Mathematics Subject Classification: primary 11P83; secondary 05A17.

Key words and phrases: relations modulo p, modular forms.

2. Basic Notions and Definitions

Let

$$\mathrm{M}_2(\mathbb{Z}) := \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc > 0 \Big\}$$

and

$$\mathrm{SL}_2(\mathbb{Z}) := \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}), ad - bc = 1 \Big\}.$$

For N a positive integer let

$$\Gamma_0(N) := \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \Big\},$$

$$\Gamma_1(N) := \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : a \equiv d \equiv 1 \pmod{N} \Big\},$$

and

$$\Gamma(N) := \Big\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) : b \equiv 0 \pmod{N} \Big\}.$$

Let

$$\mathbb{H} := \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0\}.$$

If f, g are meromorphic functions on $\mathbb{H}$ and $f(\tau) = g(\tau)$ for all values $\tau \in \mathbb{H}$ where f, g are defined, we simply write $f(\tau) = g(\tau)$ and omit to write where τ lives. There will be no confusion because we will always use the symbol τ for a generic $\tau \in \mathbb{H}$. For special values we will use τ with a subscript for example τ_0, τ_1,..., etc. Since the symbol τ is always used for generic $\tau \in \mathbb{H}$ we will often write $f(\tau)$ for the function f and for specializations of f at a point we use for the point the symbol τ_j for $j \in \mathbb{N}$. That is $f(\tau_j)$ is the value of f at the point τ_j.

For $k \in \mathbb{Z}$, f meromorphic on $\mathbb{H}$ and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z})$ we define

$$(f|_k\gamma)(\tau) := (ad - bc)^{k/2}(c\tau + d)^{-k} f\Big(\frac{a\tau + b}{c\tau + d}\Big).$$

Then for $\gamma_1, \gamma_2 \in \mathrm{M}_2(\mathbb{Z})$:

$$f|_k\gamma_1|_k\gamma_2 = f|_k\gamma_1\gamma_2.$$

A good reference for properties like this e.g. is [3].

Let N be a positive integer and k an integer. Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ such that $\Gamma(N) \subseteq \Gamma$. A *meromorphic modular form of weight k* for Γ is a meromorphic function f on $\mathbb{H}$ such that:

(i) for all $\gamma \in \Gamma$, $f|_k\gamma = f$;
(ii) for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $(f|_k\gamma)(\tau)$ admits a Laurent expansion in powers of $e^{\frac{2\pi i\tau}{N}}$ with finite principal part.

We denote the set of meromorphic modular forms of weight k for Γ by $\mathcal{A}_k(\Gamma)$.

A *weak modular form of weight k* for Γ is a meromorphic modular form of weight k for Γ which is holomorphic on $\mathbb{H}$. We denote the set of weak modular forms of weight k for Γ by $M_k^!(\Gamma)$.

A *modular form of weight k* for Γ is a weak modular form of weight k for Γ such that $(f|_k\gamma)(\tau)$ admits a Laurent expansion in powers of $e^{\frac{2\pi i\tau}{N}}$ with 0 principal part. We denote the set of modular forms of weight k for Γ by $M_k(\Gamma)$.

Remark 2.1. Let $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We note that if f is a meromorphic modular form of weight k for $\Gamma_1(N)$, then since $T \in \Gamma_1(N)$ and because of *(i)* we have

$$(f|_k T)(\tau) = f(\tau + 1) = f(\tau).$$

Because of *(ii)*, there exist $m \in \mathbb{Z}$ and $a(n) \in \mathbb{C}$, $n \geq m$, such that

$$f(\tau) = \sum_{n=m}^{\infty} a(n) e^{\frac{2\pi i n \tau}{N}} \text{ and consequently } f(\tau+1) = \sum_{n=m}^{\infty} a(n) e^{\frac{2\pi i n}{N}} e^{\frac{2\pi i n \tau}{N}}.$$

In particular $f(\tau + 1) = f(\tau)$ implies that $a(n)e^{\frac{2\pi i n}{N}} = a(n)$ which is only possible iff $a(n) = 0$ unless $N|n$. This implies that there exist $m' \in \mathbb{Z}$ and $b(n) \in \mathbb{C}$, $n \geq m'$, such that

$$f(\tau) = \sum_{n=m'}^{\infty} b(n) q^n \tag{3}$$

where here and in the following

$$q = q(\tau) := e^{2\pi i \tau}.$$

Note that in the sum (3) q should be understood as $q(\tau)$.

Note 2.2. When $f \in \mathcal{A}_k(\Gamma_1(N))$ for convenience we will write

$$f(\tau) = \sum_{n=-\infty}^{\infty} a(n) q^n \tag{4}$$

although because of *(ii)*, there exists an integer m such that $a(n) = 0$ for all $n < m$.

For simplicity we define

$$\mathcal{A}_k^1(N) := \mathcal{A}_k(\Gamma_1(N)).$$

As we observed in Remark 2.1, if $f \in \mathcal{A}_k^1(N)$ then $f(\tau) = \sum_{n=-\infty}^{\infty} a(n) q^n$. Let R be a subring of $\mathbb{C}$. If $a(n) \in R$ for all $n \in \mathbb{Z}$, we say that $f \in \mathcal{A}_k^1(N, R)$.

Similarly if $f \in \mathcal{A}_k(\Gamma(N))$, then $f(\tau) = \sum_{-\infty}^{\infty} b(n) q_N$ with $q_N := e^{\frac{2\pi i \tau}{N}}$. If $b(n) \in R$ (for R as above), for all $n \in \mathbb{Z}$, then we say that $f \in \mathcal{A}_k(\Gamma(N), R)$. Analogously we define $M_k^!(\Gamma, R)$ and $M_k(\Gamma, R)$ for an arbitrary subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$.

3. Main Result

The goal of this section is to prove Theorem 3.18 which says that for given $f_j(\tau) \in \mathcal{A}^1(N) = \cup_{k=-\infty}^{\infty} \mathcal{A}_k^1(N)$ for $j = 0, \ldots, \nu$, we have

$$f_0(\tau) + q f_1(\tau) + \cdots + q^{\nu} f_\nu(\tau) \equiv 0 \pmod{p}$$

iff

$$f_0(\tau) \equiv f_1(\tau) \equiv \cdots \equiv f_\nu(\tau) \equiv 0 \pmod{p}.$$

We will need a couple of results for proving this and, for the sake of logical transparence we explain here shortly how they depend on each other. Lemma 3.1 and Lemma 3.2 are used for proving Lemma 3.3. Lemma 3.8 does not depend on any lemma proven in this paper. One of the crucial results of this section is Theorem 3.10, which is proven by using Lemma 3.8, Lemma 3.2, Lemma 3.3, and Deligne and

Rapoport's result Lemma 3.9. Theorem 3.10 says that for a given positive integer N, a prime p, and $\Phi \in \mathcal{A}_k^1(N, \mathbb{Z}_p)$ with

$$\Phi(\tau) = \sum_{n=-\infty}^{\infty} b(n)q^n$$

we have for any given prime ℓ and integers a and t with $\gcd(a, \ell N) = 1$:

$$\forall_{n\in\mathbb{Z}}\, b(\ell n + t) \equiv 0 \pmod{p} \Rightarrow \forall_{n\in\mathbb{Z}}\, b(\ell n + a^2 t) \equiv 0 \pmod{p}.$$

Here for p a prime

$$\mathbb{Z}_p := \{a/b | a, b \in \mathbb{Z}, p \nmid b\}.$$

Theorem 3.10 is only used to prove Theorem 3.11 which simply says that the q-expansion of a meromorphic modular form with integer coefficients cannot be congruent modulo p to a polynomial in q, unless this polynomial is a constant. As we will see this is the key tool needed in every intermediate result until we arrive at the proof of Theorem 3.18. A very simple but crucial ingredient needed for the induction proof of Theorem 3.18 is Lemma 3.13. For the proof of Lemma 3.13 one only needs Lemma 3.1. Lemma 3.14 is just a simple result needed when one divides two meromorphic modular forms modulo p. Theorem 3.15 is a weaker version of Theorem 3.18 which is based on Lemma 3.14, Lemma 3.13 and Theorem 3.11. One obtains Corollary 3.16 from Theorem 3.15 which is used to prove Lemma 3.17. Finally by using Lemma 3.17, Lemma 3.14 and Lemma 3.13 one proves Theorem 3.18.

Lemma 3.1. *Let m, N be positive integers with $m|N$ and k an integer. For $\lambda \in \mathbb{Z}$ let $M_{\lambda,m} := \left(\begin{smallmatrix} 1 & \lambda \\ 0 & m \end{smallmatrix}\right)$. Let $\Phi \in \mathcal{A}_k^1(N)$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. Then $\Phi|_k M_{\lambda,m}\gamma = (\Phi|_k\gamma)|_k M_{bd+\lambda d^2,m}$.*

Proof. The statement is equivalent to proving.

$$\Phi|_k M_{\lambda,m}\gamma M_{bd+\lambda d^2,m}^{-1}\gamma^{-1} = \Phi.$$

We have that

$$M_{\lambda,m}\gamma M_{bd+\lambda d^2,m}^{-1}\gamma^{-1} = \begin{pmatrix} a + \lambda c & -\frac{(bd+\lambda d^2)(a+\lambda c)+b+\lambda d}{m} \\ mc & (-bd + \lambda d^2)c + d \end{pmatrix} \gamma^{-1} \in \Gamma_1(N)$$

because $c \equiv 0 \pmod{m}$ and therefore $ad \equiv 1 \pmod{m}$ which implies that

$$-(bd + \lambda d^2)(a + \lambda c) + b + \lambda d \equiv -b - \lambda d + b + \lambda d \equiv 0 \pmod{m}.$$

□

Lemma 3.2. *Let m be a positive integer and t an integer. Let Φ be meromorphic on $\mathbb{H}$ and $\Phi(\tau) = \sum_{n=-\infty}^{\infty} a(n)q^n$. Then*

$$\frac{1}{m}\sum_{\lambda=0}^{m-1} e^{-\frac{2\pi i\lambda t}{m}}\Phi\Big(\frac{\tau+\lambda}{m}\Big) = q^{\frac{t}{m}}\sum_{n=-\infty}^{\infty} a(mn+t)q^n.$$

Proof.

$$\begin{aligned}
&\frac{1}{m}\sum_{\lambda=0}^{m-1} e^{-\frac{2\pi i\lambda t}{m}}\Phi\Big(\frac{\tau+\lambda}{m}\Big)\\
=&\frac{1}{m}\sum_{\lambda=0}^{m-1} e^{-\frac{2\pi i\lambda t}{m}}\sum_{n=-\infty}^{\infty} a(n)e^{2\pi in\frac{\tau+\lambda}{m}}\\
=&\frac{1}{m}\sum_{n=-\infty}^{\infty} a(n)e^{\frac{2\pi in\tau}{m}}\sum_{\lambda=0}^{m-1} e^{\frac{2\pi i\lambda(n-t)}{m}}\\
=&e^{\frac{2\pi it\tau}{m}}\sum_{n=-\infty}^{\infty} a(mn+t)e^{2\pi in\tau}.
\end{aligned}$$

□

Lemma 3.3. *Let m, N be positive integers and t an integer. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(mN)\cap\Gamma_1(N)$ and $\Phi \in \mathcal{A}_k^1(N)$ with $\Phi(\tau) = \sum_{n=-\infty}^{\infty} a(n)q^n$. Then*

$$q^{\frac{t}{m}}\sum_{n=-\infty}^{\infty} a(mn+t)q^n|_k\gamma = q^{\frac{a^2t}{m}}e^{\frac{2\pi ibat}{m}}\sum_{n=-\infty}^{\infty} a(mn+a^2t)q^n.$$

Proof. We have

$$q^{\frac{t}{m}}\sum_{n=-\infty}^{\infty} a(mn+t)q^n|_k\gamma = \frac{1}{m}\sum_{\lambda=0}^{m-1} e^{-\frac{2\pi i\lambda t}{m}}m^{k/2}(\Phi|_kM_{\lambda,m})|_k\gamma$$

because of Lemma 3.2

$$= \frac{1}{m}\sum_{\lambda=0}^{m-1} e^{-\frac{2\pi i\lambda t}{m}}m^{k/2}(\Phi|_k\gamma)|_kM_{\lambda d^2+bd,m}$$

because of Lemma 3.1

$$= \frac{1}{m}\sum_{\lambda=0}^{m-1} e^{-\frac{2\pi i\lambda t}{m}}m^{k/2}\Phi|_kM_{\lambda d^2+bd,m}$$

because of $\Phi \in \mathcal{A}_k^1(N)$

$$= \frac{1}{m}e^{\frac{2\pi ibat}{m}}\sum_{\lambda'=0}^{m-1} e^{-\frac{2\pi ia^2\lambda' t}{m}}\Phi\Big(\frac{\tau+\lambda'}{m}\Big)$$

by using the substitution $\lambda' \equiv \lambda d^2 + bd \pmod m$, with inverse $\lambda \equiv a^2\lambda' - ba \pmod m$.

$$= q^{\frac{a^2t}{m}}e^{\frac{2\pi ibat}{m}}\sum_{n=-\infty}^{\infty} a(mn+a^2t)q^n$$

because of Lemma 3.2.

□

Definition 3.4. *We define* $\eta : \mathbb{H} \to \mathbb{C}$ *by*

$$\eta(\tau) = e^{\frac{\pi i \tau}{12}} \prod_{n=1}^{\infty}(1-q^n)$$

and

$$\Delta := \eta^{24}.$$

Remark 3.5. By [4, Th. 1.64] we find that $(\eta(24\tau))^2 \in M_1(\Gamma_0(576)) \subseteq M_1(\Gamma_1(576))$ and $\Delta \in M_{12}(\mathrm{SL}_2(\mathbb{Z}))$.

Definition 3.6. *We denote by* $j(\tau)$ *the classical modular invariant.*

Remark 3.7. Note that $j(\tau) \in M_0^!(\mathrm{SL}_2(\mathbb{Z}), \mathbb{Z})$. Furthermore, $j(\tau) = q^{-1} + \dots$.

For meromorphic functions f, g on $\mathbb{H}$ which additionally have Laurent expansions in q with coefficients in $\mathbb{Z}_p$ for some prime p, that is $f(\tau) = \sum_{n=-\infty}^{\infty} a(n)q^n$ and $g(\tau) = \sum_{n=-\infty}^{\infty} b(n)q^n$, with $a(n), b(n) \in \mathbb{Z}_p$ for all $n \in \mathbb{Z}$ we write

$$f(\tau) \equiv g(\tau) \pmod{p}$$

iff $\frac{a(n)-b(n)}{p} \in \mathbb{Z}_p$ for all $n \in \mathbb{Z}$.

Lemma 3.8. *Let* p *be a prime. Let* $f \in \mathcal{A}_k^1(N, \mathbb{Z}_p)$. *Then there exist* $g \in M_k^!(\Gamma_1(N)), \mathbb{Z})$ *and a monic* $p(X) \in \mathbb{Z}[X]$ *such that*

$$\frac{g(\tau)}{p(j(\tau))} \equiv f(\tau) \pmod{p}.$$

Proof. Assume that the $f(\tau)$ has n poles in the fundamental domain of $\Gamma_1(N)$ counted with multiplicity. Let $\tau_1, \dots, \tau_n$ be the poles of $f(\tau)$. Then

$$G(\tau) := f(\tau) \prod_{j=1}^{n} j(\tau) - j(\tau_j) \tag{5}$$

has no poles in $\mathbb{H}$, that is $G \in M_k^!(\Gamma_1(N))$. Furthermore, there exists an $u \in \mathbb{Z}$ such that $\Delta(\tau)^u G(\tau) \in M_{k+12u}(\Gamma_1(N))$. From [6, Th. 3.52] we know that there exist

$$b_1, \dots, b_s \in M_{k+12u}(\Gamma_1(N), \mathbb{Z})$$

such that

$$M_{k+12u}(\Gamma_1(N)) = \{c_1 b_1(\tau) + \dots + c_s b_s(\tau), c_1, \dots, c_s \in \mathbb{C}\}.$$

In particular there exist $c_1, \dots, c_s \in \mathbb{C}$ such that

$$\Delta(\tau)^u G(\tau) = c_1 b_1(\tau) + \dots + c_s b_s(\tau)$$

or equivalently

$$G(\tau) = c_1 \frac{b_1(\tau)}{\Delta(\tau)^u} + \dots + c_s \frac{b_s(\tau)}{\Delta(\tau)^u}. \tag{6}$$

Let

$$p(X) := \prod_{j=1}^{n} X - j(\tau_j) = X^n + a_{n-1}X^{n-1} + \dots + a_1 X + a_0. \tag{7}$$

Let $a_n := 1$ and V be the vector space over $\mathbb{Q}$ generated by

$$\{c_1, \dots, c_s\} \cup \{a_0, \dots, a_n\}.$$

Let $r_1, \dots, r_m$ be a basis of V over $\mathbb{Q}$. Then for $i = 1, \dots, m$

$$a_i = d_1^{(i)} r_1 + \dots + d_m^{(i)} r_m$$

for some rational numbers $d_k^{(i)}$, $k = 1, \dots, m$. Then by (7)

$$p(X) = \sum_{i=0}^{n} X^i a_i = \sum_{i=0}^{n} X^i \sum_{j=1}^{m} d_j^{(i)} r_j = \sum_{j=1}^{m} r_j \underbrace{\sum_{i=0}^{n} d_j^{(i)} X^i}_{=d_j p_j(X)}.$$

where $p_1(X), \dots, p_m(X) \in \mathbb{Z}[X]$ and $d_1, \dots, d_m \in \mathbb{Q}$ are chosen such that $p_1(X), \dots, p_m(X)$ are primitive in the sense of Gauss. Hence

$$p(X) = r_1 d_1 p_1(X) + r_2 d_2 p_2(X) + \cdots + r_m d_m p_m(X). \tag{8}$$

Similarly for $i = 1, \dots, s$

$$c_i = e_1^{(i)} r_1 + \cdots + e_m^{(i)} r_m$$

for some rational numbers $e_k^{(i)}$, $k = 1, \dots, m$. Then by (6) we have that

$$G(\tau) = \sum_{i=1}^{s} c_i \frac{b_i(\tau)}{\Delta(\tau)^u} = \sum_{i=1}^{s} \sum_{j=1}^{m} e_j^{(i)} r_j \frac{b_i(\tau)}{\Delta(\tau)^u} = \sum_{j=1}^{m} r_j \underbrace{\sum_{i=1}^{s} e_j^{(i)} \frac{b_i(\tau)}{\Delta(\tau)^u}}_{=e_j f_j(\tau)}$$

where $f_j(\tau) = \sum_{n=-\infty}^{\infty} b_j(n) q^n$ and $e_1, \dots, e_m \in \mathbb{Q}$ are chosen such that

$$\not\exists_{\ell \text{ prime}} \forall_{n \in \mathbb{Z}} \ell | b_j(n). \tag{9}$$

Hence

$$G(\tau) = e_1 r_1 f_1(\tau) + \cdots + e_m r_m f_m(\tau) \tag{10}$$

Note that $f_i(\tau) = \frac{1}{e_i} \sum_{i=1}^{s} e_j^{(i)} \frac{b_i(\tau)}{\Delta(\tau)^u} \in M_k^!(\Gamma_1(N), \mathbb{Z})$.

In particular (5), (8) and (10) implies

$$\begin{aligned} &e_1 r_1 f_1(\tau) + \cdots + e_m r_m f_m(\tau) \\ &\quad = \{r_1 d_1 p_1(j(\tau)) + r_2 d_2 p_2(j(\tau)) + \cdots + r_m d_m p_m(j(\tau))\} f(\tau). \end{aligned} \tag{11}$$

Since $r_1, \dots, r_m$ is a basis, (11) implies that

$$e_i f_i(\tau) = d_i f(\tau) p_i(j(\tau)), \quad i = 1, \dots, m.$$

In particular, writing $\frac{e_1}{d_1} = \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$ we obtain

$$\frac{a f_1(\tau)}{b p_1(j(\tau))} = f(\tau).$$

This implies that

$$\frac{a f_1(\tau)}{b} = f(\tau) p_1(j(\tau))$$

Since the coefficients in the q-expansion of $f(\tau)p_1(j(\tau))$ are in $\mathbb{Z}_p$ and because of (9) it follows that $p \nmid b$. Let b' be an integer such that $bb' \equiv 1 \pmod{p}$ and define

$$g(\tau) := ab' f_1(\tau).$$

Then $g(\tau) \in M_k^!(\Gamma_1(N), \mathbb{Z})$. In particular

$$g(\tau) \equiv f(\tau) p_1(j(\tau)) \pmod{p}.$$

Next we observe that there exists $c \in \{1, \dots, p-1\}$ and monic $r(X) \in \mathbb{Z}[X]$ such that $p_1(X) \equiv c r(X) \pmod{p}$, since $p_1(X)$ is primitive. This implies that

$$g(\tau) \equiv c f(\tau) r(j(\tau)) \pmod{p}$$

or equivalently

$$\frac{c' g(\tau)}{r(j(\tau))} \equiv f(\tau) \pmod{p},$$

where c' is an integer such that $cc' \equiv 1 \pmod{p}$. □

As a simple consequence of [1, VII, Cor. 3.12] we have:

Lemma 3.9. *Let k, N be positive integers and $f \in M_k(\Gamma(N), \mathbb{Z}[\xi])$ where $\xi := e^{\frac{2\pi i}{N}}$. Then for all $\gamma \in \Gamma_0(N)$, $f|_k\gamma \in M_k(\Gamma(N), \mathbb{Z}[\xi])$.*

Theorem 3.10. *Let ℓ, p be primes. Let N be a positive integer and t an integer. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\ell N) \cap \Gamma_1(N)$. Let $\Phi \in \mathcal{A}_k^1(N, \mathbb{Z}_p)$ and $\sum_{n=-\infty}^{\infty} b(n)q^n := \Phi(\tau)$. Then*

$$\sum_{n=-\infty}^{\infty} b(\ell n + t)q^n \equiv 0 \pmod{p} \Rightarrow \sum_{n=-\infty}^{\infty} b(\ell n + a^2 t)q^n \equiv 0 \pmod{p}.$$

Proof. By Lemma 3.8 there exists $f \in M_k^!(\Gamma_1(N), \mathbb{Z})$ and a monic $p(X) \in \mathbb{Z}[X]$ such that

$$\Phi(\tau) \equiv \frac{f(\tau)}{p(j(\tau))} \pmod{p}.$$

Let

$$\sum_{n=-\infty}^{\infty} a(n)q^n := \frac{f(\tau)}{p(j(\tau))}.$$

We define

$$F(\tau) := p(j(\ell\tau)) \prod_{\lambda=0}^{\ell-1} p\Big(j\big(\frac{\tau+\lambda}{\ell}\big)\Big). \tag{12}$$

If the degree of $p(X)$ is n, we observe directly from (12) that the q-expansion of $F(\tau)$ has the form

$$F(\tau) = q^{-n(\ell+1)} + O(q^{-n(\ell+1)+1}), \tag{13}$$

and we need later in the proof that the coefficient of $q^{-n(\ell+1)}$ is 1. Let

$$Q(X) := (X - j(\ell\tau)) \prod_{j=0}^{\ell-1} X - j\big(\frac{\tau+\lambda}{\ell}\big) \tag{14}$$

and define $e_n(\tau)$ by the relation

$$Q(X) = X^{\ell+1} + \sum_{n=1}^{\ell} e_n(\tau) X^n.$$

By [5, §4, Th. 16], $Q(X) \in \mathbb{Z}[j(\tau)][X]$. We observe from (14) that $e_n(\tau) = E_n(Y_0(\tau), Y_1(\tau), \ldots, Y_\ell(\tau))$ where

$$(Y_0(\tau), Y_1(\tau), \ldots, Y_\ell(\tau)) := \Big(j(\ell\tau), j\big(\frac{\tau}{\ell}\big), \ldots, j\big(\frac{\tau+\ell-1}{\ell}\big)\Big)$$

and $E_n(X_0, X_1, \ldots, X_\ell) \in \mathbb{Z}[X_0, X_1, \ldots, X_\ell]$ are the elementary symmetric polynomials. Furthermore, $F(j(\tau)) = f(Y_0(\tau), Y_1(\tau), \ldots, Y_\ell(\tau))$ where $f(X_0, X_1, \ldots, X_\ell) \in \mathbb{Z}[X_0, X_1, \ldots, X_\ell]$ is a symmetric polynomial and since every integer symmetric polynomial in $X_0, \ldots, X_\ell$ is an integer polynomial in the elementary symmetric functions $E_1, \ldots, E_n$ by [2, p. 20, (2.4)], it follows that

$$f(X_0, \ldots, X_n) = h(E_0(X_0, \ldots, X_n), \ldots, E_n(X_0, \ldots, X_n))$$

for some $h(X_0, \ldots, X_n) \in \mathbb{Z}[X_0, \ldots, X_n]$. This implies that

$$F(\tau) = h(e_0(\tau), \ldots, e_n(\tau)) \in \mathbb{Z}[j(\tau)]$$

or in other words there exists $r(X) \in \mathbb{Z}[X]$ such that $F(\tau) = r(j(\tau))$ and because of (13) it follows that $r(X)$ is monic.

First we see that

$$G(\tau) := r(j(\tau))^{\ell}\Big(q^{\frac{t}{\ell}}\sum_{n=-\infty}^{\infty}\frac{a(\ell n+t)}{p}q^n\Big)^{\ell} \in \mathcal{A}_{k\ell}^1(N,\mathbb{Z})$$

because of Lemma 3.3. Furthermore, by Lemma 3.2

$$\begin{aligned} r(j(\tau))\times q^{\frac{t}{\ell}}\sum_{n=-\infty}^{\infty}\frac{a(\ell n+t)}{p}q^n &= F(\tau)\times\frac{1}{p^2}\sum_{\lambda=0}^{\ell-1}e^{-\frac{2\pi i\lambda t}{\ell}}\frac{f\big(\frac{\tau+\lambda}{\ell}\big)}{p\Big(j\big(\frac{\tau+\lambda}{\ell}\big)\Big)}\\ =p(j(\ell\tau))\times\frac{1}{\ell^2}\sum_{\lambda=0}^{\ell-1}e^{-\frac{2\pi i\lambda t}{\ell}}f\big(\frac{\tau+\lambda}{\ell}\big)\prod_{\alpha\neq\lambda}p\Big(j\big(\frac{\tau+\alpha}{\ell}\big)\Big).& \end{aligned}$$

which is holomorphic on $\mathbb{H}$ because $j(\tau)$ and $f(\tau)$ are holomorphic on $\mathbb{H}$. This implies that $G(\tau)$ is holomorphic on $\mathbb{H}$ so that $G(\tau)\in M_k^!(\Gamma_1(N),\mathbb{Z})$.

Because of $\Delta\in M_{12}(\mathrm{SL}_2(\mathbb{Z}))$, we also have $\Delta\in M_{12}(\Gamma_1(N))$ and $\Delta|_{12}\gamma$ is a q-series with positive order for all $\gamma\in\mathrm{SL}_2(\mathbb{Z})$. Because of this there exists a positive integer i such that

$$r(j(\tau))^{\ell}\Delta(\tau)^i\Big(q^{\frac{t}{\ell}}\sum_{n=-\infty}^{\infty}\frac{a(\ell n+t)}{p}q^n\Big)^{\ell}\in M_{12i+k}(\Gamma_1(N),\mathbb{Z}).$$

By Lemma 3.3:

$$\begin{aligned} r(j(\tau))^{\ell}\Delta(\tau)^i\Big(q^{\frac{t}{\ell}}\sum_{n=-\infty}^{\infty}\frac{a(\ell n+t)}{p}q^n\Big)^{\ell}|_{k+12i\gamma}&\\ = r(j(\tau))^{\ell}\Delta(\tau)^i\Big(q^{\frac{a^2t}{\ell}}\sum_{n=-\infty}^{\infty}\frac{a(\ell n+a^2t)}{p}q^n\Big)^{\ell}.& \end{aligned}$$

Then by Lemma 3.9 the q-series

$$r(j(\tau))^{\ell}\Delta(\tau)^i\Big(q^{\frac{a^2t}{\ell}}\sum_{n=-\infty}^{\infty}\frac{a(\ell n+a^2t)}{p}q^n\Big)^{\ell},$$

has integer coefficients. This implies that

$$\sum_{n=-\infty}^{\infty}a(\ell n+a^2t)\equiv 0 \pmod p,$$

finishing the proof. □

Theorem 3.11. *Let p be a prime. Let N be a positive integer and let $f\in\mathcal{A}_k^1(N,\mathbb{Z}_p)$. Assume that for some $r(q)\in\mathbb{Z}[q,q^{-1}]$ we have*

$$f(\tau)=\sum_{n=-\infty}^{\infty}a(n)q^n\equiv r(q) \pmod p.$$

Then $f(\tau)\equiv a(0) \pmod p$.

Proof. Let r and u be such that

$$r(q)\equiv a(r)q^r+a(r-1)q^{r-1}+\cdots+a(u+1)q^{u+1}+a(u)q^u.$$

Let $t \neq 0$ be such that $a(t) \not\equiv 0 \pmod{p}$ and let $v := r+1$ if $r \neq -1$ or $v := 1$ if $r := -1$. Let $a, b, c, d \in \mathbb{Z}$ and ℓ a prime such that

$$\ell > r + 2 - u \tag{15}$$
$$a^2 v \equiv t \pmod{\ell} \tag{16}$$
$$a \equiv 1 \pmod{N} \tag{17}$$
$$c \equiv 0 \pmod{\ell N} \tag{18}$$
$$ad - bc = 1. \tag{19}$$

Then $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\ell N) \cap \Gamma_1(N)$. Furthermore, $\sum_{n=-\infty}^{\infty} a(\ell n + v) \equiv 0 \pmod{p}$. Then because of Theorem 3.10

$$\sum_{n=-\infty}^{\infty} a(\ell n + a^2 v) q^n = \sum_{n=-\infty}^{\infty} a(\ell n + t) q^n \equiv 0 \pmod{p}.$$

This is false because $a(t) \not\equiv 0 \pmod{p}$. It is left to show that there exist a, b, c, d, ℓ satisfying (15)-(19). Let $vt = 2^s m$ where m is odd. By standard properties of the Legendre symbol we obtain for any prime $\ell \neq 2$:

$$\left(\frac{vt}{\ell}\right) = \left(\frac{2^s m}{\ell}\right) = \left(\frac{2}{\ell}\right)^s \left(\frac{m}{\ell}\right) = (-1)^{s\frac{\ell^2-1}{8}} (-1)^{\frac{m-1}{2}\frac{\ell-1}{2}} \left(\frac{\ell}{m}\right).$$

Assuming that $\ell \equiv 1 \pmod{8}$ we obtain

$$\left(\frac{vt}{\ell}\right) = \left(\frac{\ell}{m}\right).$$

Assuming further that $\ell \equiv 1 \pmod{m}$ we obtain that

$$\left(\frac{vt}{\ell}\right) = 1. \tag{20}$$

We have proven that vt is a square modulo ℓ for all primes $\ell \equiv 1 \pmod{8m}$. By Dirichlet's theorem there are infinitely many such primes ℓ. In particular there exists a prime ℓ with $\ell \nmid N$ and such that (15) is satisfied. We fix such an ℓ. Then $vt \equiv x^2 \pmod{\ell}$ because of (20). Let $a \in \mathbb{Z}$ such that

$$a \equiv xv^{-1} \pmod{\ell}$$
$$a \equiv 1 \pmod{N}.$$

Such an a clearly exists because of the Chinese remainder theorem. In particular for this a, (16)-(17) are satisfied. Set $c := \ell N$. Then we can find integer b, d such that $ad - bc = 1$ because $\gcd(a, c) = 1$. Hence we have constructed a, b, c, d and ℓ with the desired properties. □

Definition 3.12. *Let d be a positive integer. For f meromorphic on $\mathbb{H}$ we define $U_d(f)$ and $V_d(f)$ meromorphic on $\mathbb{H}$ by*

$$U_d(f)(\tau) := \frac{1}{d} \sum_{\lambda=0}^{d-1} f\Big(\frac{\tau + \lambda}{d}\Big)$$

and $V_d(f)(\tau) := f(d\tau)$.

Lemma 3.13. *Let k and t be integers and m a positive integer and $f(\tau) \in \mathcal{A}_k^1(N)$. Then*

$$V_m U_m(q^t f)(\tau) = q^t G(\tau),$$

where $G \in \mathcal{A}_k^1(Nm^2)$.

Proof.

$$\begin{aligned} U_m(q^t f)(\tau) &= \frac{1}{m}\sum_{\lambda=0}^{m-1} e^{\frac{2\pi i t(\tau+\lambda)}{m}} f\Big(\frac{\tau+\lambda}{m}\Big) \\ &= e^{\frac{2\pi i t\tau}{m}} \frac{1}{m}\sum_{\lambda=0}^{m-1} e^{\frac{2\pi i t\lambda}{m}} f\Big(\frac{\tau+\lambda}{m}\Big) \\ &= q^{t/m} g(\tau). \end{aligned}$$

If $f \in \mathcal{A}_k(\Gamma_1(N))$ then $f|M_{\lambda,m} \in \mathcal{A}_k(\Gamma_1(N)\cap\Gamma(m))$ because of Lemma 3.1. In particular $g(\tau) \in \mathcal{A}_k(\Gamma_1(N)\cap\Gamma(m))$. Consequently, $G := V_m g \in \mathcal{A}_k(\Gamma_1(Nm^2))$, because for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(Nm^2)$ we have $\left(\begin{smallmatrix} a & bm \\ c/m & d \end{smallmatrix}\right) \in \Gamma_1(N)\cap\Gamma(m)$ which implies

$$V_m g|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} = V_m\Big(g|_k \begin{pmatrix} a & bm \\ c/m & d \end{pmatrix}\Big) = V_m g.$$

□

Lemma 3.14. *Let p be a prime and $a(\tau) \in \mathcal{A}_k^1(576N, \mathbb{Z}_p)$. Let*

$$a(\tau) = pb_s q^s + pb_{s+1}q^{s+1} + \cdots + pb_{s+m-1}q^{s+m-1} + \sum_{n\geq s+m} b_n q^n, \quad p \nmid b_{s+m}.$$

Then there exists $\tilde{a}(\tau) = \sum_{n\geq s+m} c_n q^n \in \mathcal{A}_k^1(576N, \mathbb{Z}_p)$ such that $\tilde{a}(\tau) \equiv a(\tau) \pmod p$.

Proof. Let

$$a_1(\tau) := a(\tau) - pb_s j(\tau)^{-s+2k}(\eta(24\tau))^{2k}.$$

Then

$$a_1(\tau) = pb_{s+1}^{(1)}q^{s+1} + \cdots + pb_{s+m-1}^{(1)}q^{s+m-1} + \sum_{n\geq s+m} b_n^{(1)} q^n.$$

Let

$$a_2(\tau) := a_1(\tau) - pb_{s+1}^{(1)} j(\tau)^{-(s+1)+2k}(\eta(24\tau))^{2k}.$$

Then

$$a_2(\tau) = pb_{s+2}^{(2)}q^{s+2} + \cdots + pb_{s+m-1}^{(2)}q^{s+m-1} + \sum_{n\geq s+m} b_n^{(2)} q^n.$$

Define analogously $a_3(\tau), \ldots, a_m(\tau)$. Then $\tilde{a}(\tau) := a_m(\tau)$ satisfies $a(\tau) \equiv \tilde{a}(\tau) \pmod p$. By Remark 3.7 and Remark 3.5 it follows that $\tilde{a}(\tau) \in \mathcal{A}_k^1(576N, \mathbb{Z}_p)$. □

Theorem 3.15. *Let N be a positive integer. Let $\phi_0(\tau), \ldots, \phi_n(\tau) \in \mathcal{A}_0^1(N, \mathbb{Z}_p)$. Assume that*

$$\phi_n(\tau)q^n + \phi_{n-1}(\tau)q^{n-1} + \cdots + \phi_0(\tau) \equiv 0 \pmod p.$$

Then $\phi_0(\tau) = \phi_1(\tau) = \cdots = \phi_n(\tau) \equiv 0 \pmod p$.

Proof. We proceed by induction on the degree with respect to q of the left hand side of the relation. We assume now that the theorem is valid for any relation of degree less than n. We assume that $\phi_0(\tau) \not\equiv 0$ because otherwise we may divide the relation by q and by the induction hypothesis we are finished. So assume $\phi_0(\tau) \not\equiv 0 \pmod p$. We can also assume that $\phi_n(\tau) \not\equiv 0 \pmod p$ because otherwise again we are finished by induction.

By Lemma 3.14 there exists $\tilde{\phi}_0 \in \mathcal{A}_0^1(576N, \mathbb{Z}_p)$ such that $\tilde{\phi}_0(\tau) = b_s q^s + O(q^{s+1})$, $p \nmid b_s$ and $\tilde{\phi}_0(\tau) \equiv \phi_0(\tau) \pmod p$. Then $\frac{\phi_\kappa(\tau)}{\tilde{\phi}_0(\tau)} \in \mathcal{A}_0^1(576N, \mathbb{Z}_p)$, for $\kappa \in 0, \ldots, n$.

Let $\kappa > 0$ be minimal such that $\frac{\phi_\kappa(\tau)}{\tilde{\phi}_0(\tau)} \not\equiv 0 \pmod p$. We divide the relation by $q^\kappa \tilde{\phi}_0(\tau)$ and obtain:

$$\frac{\phi_n(\tau)}{\tilde{\phi}_0(\tau)} q^{n-\kappa} + \frac{\phi_{n-1}(\tau)}{\tilde{\phi}_0(\tau)} q^{n-2-\kappa} + \cdots + \frac{\phi_\kappa(\tau)}{\tilde{\phi}_0(\tau)} + q^{-\kappa} \equiv 0 \pmod p. \tag{21}$$

Let

$$\frac{\phi_\kappa(\tau)}{\tilde{\phi}_0(\tau)} = \sum_{j=-\infty}^{\infty} a(j) q^j.$$

By Theorem 3.11 there exists a minimal $d > \kappa$ such that $a(d) \not\equiv 0 \pmod p$ or $\sum_{n=m}^{\infty} a(n) q^n \equiv a(0) \pmod p$. Let

$$s := \begin{cases} \kappa + 1 & \text{if } \sum a(n) q^n \equiv a(0) \pmod p, \\ d & \text{otherwise.} \end{cases}$$

Then applying the operator $V_s U_s$ to the relation (21) yields

$$b_n(\tau) q^{n-\kappa} + b_{n-1}(\tau) q^{n-\kappa-1} + \cdots + b_\kappa(\tau) \equiv 0 \pmod p, \tag{22}$$

where for $i = \kappa, \ldots, n$:

$$b_i(\tau) := q^{\kappa - i} V_s U_s \Big(q^{i-\kappa} \frac{\phi_i(\tau)}{\tilde{\phi}_0(\tau)} \Big).$$

Note that since $s > \kappa$ we have $V_s U_s(q^{-\kappa}) = 0$.

In particular by Lemma 3.13 $b_i(\tau) \in \mathcal{A}_k^1(576 N s^2, \mathbb{Z}_p)$. Next note that

$$b_\kappa(\tau) = V_s U_s(\sum a(n) q^n) = \sum a(ns) q^{ns}$$

and hence $b_\kappa(\tau) \equiv a(0) \pmod p$ if $\sum a(n) q^n \equiv a(0) \pmod p$ or $b_\kappa(\tau)$ contains the term $q^d a(d) \not\equiv 0 \pmod p$, in any case $b_\kappa(\tau) \not\equiv 0 \pmod p$.

However by the induction hypothesis $b_n(\tau) \equiv \cdots b_\kappa(\tau) \equiv 0 \pmod p$. This contradicts $b_\kappa(\tau) \not\equiv 0 \pmod p$ hence we have $\phi_n(\tau) \equiv \cdots \equiv \phi_0(\tau) \equiv 0 \pmod p$. □

Corollary 3.16. *Let p be a prime. Let $a_0(\tau), a_1(\tau), \ldots, a_n(\tau) \in M_0^!(\Gamma_1(N), \mathbb{Z}_p)$. Let $r(q) \in \mathbb{Z}[q, q^{-1}]$ be non-constant modulo p. Assume that*

$$a_n(\tau) r(q)^n + a_{n-1}(\tau) r(q)^{n-1} + \cdots + a_0(\tau) \equiv 0 \pmod p.$$

Then $a_0(\tau) \equiv a_1(\tau) \equiv \cdots \equiv a_n(\tau) \equiv 0 \pmod p$.

Proof. We proceed by induction on n. Assume that $r(q)$ has positive degree and let d be its degree. Then there exist $b_{dn-1}(\tau), \ldots, b_0(\tau) \in M_0^!(\Gamma_1(N), \mathbb{Z}_p)$ such that

$$a_n(\tau) q^{dn} + b_{dn-1}(\tau) q^{dn-1} + \cdots + b_0(\tau) \equiv 0 \pmod p$$

Then by Theorem 3.15 we have $a_n(\tau) \equiv 0 \pmod p$. By induction we are finished.

Next assume that $r(q)$ has negative degree and let $-d$ be its low-degree. Then there exist $b_{-dn+1}(\tau), \ldots, b_0(\tau) \in M_0^!(\Gamma_1(N), \mathbb{Z}_p)$ such that

$$a_n(\tau) q^{-dn} + b_{-dn+1}(\tau) + \cdots + b_0(\tau) \equiv 0 \pmod p.$$

After multiplication of both sides by q^{dn}, we obtain by Theorem 3.15 that $a_n(\tau) \equiv 0 \pmod p$. By induction we are finished. □

Lemma 3.17. *Let N be a positive integer and p a prime. For $i = 1, \ldots, n$ let $\Phi_i \in \mathcal{A}_{k_i}^1(N, \mathbb{Z}_p)$, $k_i \in \mathbb{Z}$. Let $r(q) \in \mathbb{Z}[q, q^{-1}]$ be such that*

$$\Phi_1(\tau) + \Phi_2(\tau) + \cdots + \Phi_n(\tau) \equiv r(q) \pmod p. \tag{23}$$

Then $r(q) \equiv j \pmod p$ for some $j \in \mathbb{Z}$.

Proof. Let

$$\nu := \frac{12(p-1)}{\gcd(p^2-1,24)}.$$

Let $b_i^{(0)}(\tau) := \sum_{\substack{1\le j\le n\\ k_j\equiv i \pmod{\nu}}} \Phi_j(\tau)\left(\frac{\eta(\tau)^p}{\eta(p\tau)}\right)^{\frac{2(i-k_j)}{p-1}}$. Then $\Phi_1(\tau)+\cdots+\Phi_n(\tau) \equiv b_0^{(0)}(\tau)+b_1^{(0)}(\tau)+\cdots+b_{\nu-1}^{(0)}(\tau) \pmod p$ because of $\left(\frac{\eta(\tau)^p}{\eta(p\tau)}\right)^{\frac{2\nu}{p-1}} \equiv 1 \pmod p$. In particular $b_i^{(0)}(\tau) \in \mathcal{A}_i^1(576pN)$ because by [4, Th. 1.64], $\left(\frac{\eta(\tau)^p}{\eta(p\tau)}\right)^{\frac{2\nu}{p-1}} \in A_\nu(\Gamma_0(p)) \subseteq A_\nu^1(p)$. This shows in particular that any sum $\Phi_1'(\tau)+\cdots+\Phi_{n'}'(\tau)$ with $\Phi_j'(\tau) \in \mathcal{A}_j^1(576pN)$ can be written as $b_0'(\tau)+\cdots+b_\nu'(\tau)$ with $b_i'(\tau) \in \mathcal{A}_j^1(576pN)$. Taking both sides of (23) to the power of k for $k=1,\dots,\nu$ and applying this rewriting to the left hand side we obtain the following system:

$$\begin{aligned}
r(q) &\equiv b_0^{(0)}(\tau)+b_1^{(0)}(\tau)+\cdots+b_{\nu-1}^{(0)}(\tau)\\
r(q)^2 &\equiv b_0^{(1)}(\tau)+b_1^{(1)}(\tau)+\cdots+b_{\nu-1}^{(1)}(\tau)\\
&\vdots\ \ \vdots\ \ \vdots\\
r(q)^\nu &\equiv b_0^{(\nu-1)}(\tau)+b_1^{(\nu-1)}(\tau)+\cdots+b_{\nu-1}^{(\nu-1)}(\tau),
\end{aligned}$$

for some $b_i^{(j)} \in \mathcal{A}_i^1(N)$. Let $T(\tau) := \eta(24\tau)^2$. By Remark 3.5, $T \in \mathcal{A}_1^1(576pN,\mathbb{Z}_p)$. We define

$$A := \begin{pmatrix}
\frac{b_0^{(0)}(\tau)}{T(\tau)^0} & \frac{b_1^{(0)}(\tau)}{T(\tau)} & \cdots & \frac{b_{\nu-1}^{(0)}(\tau)}{T(\tau)^{\nu-1}}\\
\frac{b_0^{(1)}(\tau)}{T(\tau)^0} & \frac{b_1^{(1)}(\tau)}{T(\tau)^1} & \cdots & \frac{b_{\nu-1}^{(1)}(\tau)}{T(\tau)^{\nu-1}}\\
\frac{b_0^{(2)}(\tau)}{T(\tau)^0} & \frac{b_1^{(2)}(\tau)}{T(\tau)^1} & \cdots & \frac{b_{\nu-1}^{(2)}(\tau)}{T(\tau)^{\nu-1}}\\
\vdots & \vdots & \vdots & \vdots\\
\frac{b_0^{(\nu-1)}(\tau)}{T(\tau)^0} & \frac{b_1^{(\nu-1)}(\tau)}{T(\tau)^1} & \cdots & \frac{b_{\nu-1}^{(\nu-1)}(\tau)}{T(\tau)^{\nu-1}}
\end{pmatrix}.$$

Then

$$\begin{pmatrix} r(q)\\ r(q)^2\\ \vdots\\ r(q)^\nu \end{pmatrix} \equiv A \begin{pmatrix} T(\tau)^0\\ T(\tau)^1\\ \vdots\\ T(\tau)^{\nu-1} \end{pmatrix} \pmod p. \tag{24}$$

Note that the entries of A are in $\mathcal{A}_0^1(576pN)$. If A is not invertible modulo p, then there exists modular functions $x_1(\tau), x_2(\tau), \dots, x_\nu(\tau)$ not all identically zero such that

$$(x_1,x_2,\dots,x_\nu)A \equiv (0,0,\dots,0)$$

which together with (24) implies that

$$x_1(\tau)r(q)+x_2(\tau)r(q)^2+\cdots+x_\nu(\tau)r(q)^\nu \equiv 0 \pmod p.$$

which is impossible by Corollary 3.16 unless $r(q)$ is constant modulo p.

If A is invertible modulo p, then

$$\operatorname{adj}(A)\begin{pmatrix} r(q)\\ r(q)^2\\ \vdots\\ r(q)^\nu \end{pmatrix} = \det(A)\begin{pmatrix} T(\tau)^0\\ T(\tau)^1\\ \vdots\\ T(\tau)^{\nu-1} \end{pmatrix}.$$

where $\mathrm{adj}(A)$ is the adjoint of A and $\det(A) \not\equiv 0 \pmod p$. In particular, since A is invertible modulo p it follows that the first row of $\mathrm{adj}(A)$ contains at least one entry which is nonzero modulo p. This leads to a relation of the form

$$r(q)a_1(\tau) + r(q)^2 a_2(\tau) + \cdots + r(q)^\nu a_\nu(\tau) \equiv \det(A)T(\tau)^0 = \det(A) \pmod p$$

which is impossible because of Corollary 3.16 unless $r(q)$ is constant modulo p. □

Theorem 3.18. *Let p be a prime. Let N be a positive integer. Let $S_j \subset \mathbb{Z}$ be finite for $0 \leq j \leq m$. Assume that we have a relation of the form*

$$\sum_{0\leq j\leq m} q^j \sum_{i\in S_j} \Phi_{i,j}(\tau) \equiv 0 \pmod p,$$

where $\Phi_{i,j} \in \mathcal{A}_i^1(N, \mathbb{Z}_p)$ and $\Phi_{i,j}(\tau) \not\equiv 0 \pmod p$, for $0 \leq j \leq m$ and $i \in S_j$. Then $\sum_{i\in S_j} \Phi_{i,j}(\tau) \equiv 0 \pmod p$ for $j \in \{0, \ldots, m\}$.

The proof of this theorem follows similar steps as the proof of Lemma 3.15, therefore in this proof we will not repeat certain minor arguments.

Proof. We proceed using induction on the length $|S_0| + |S_1| + \cdots + |S_m|$ of the relation. Assume that the statement hold for all relations of length less than M and we wish to prove it for a relation of length M.

Therefore assume that the length of the relation is M. Assume that the theorem is false. Without loss of generality we may assume that $\sum_{i\in S_0} \Phi_{i,0}(\tau) \not\equiv 0 \pmod p$ because in case not we divide the relation by an appropriate power of q to make it into the desired form. Then there exists a minimal $\kappa > 0$ such that $\sum_{i\in S_\kappa} \Phi_{i,\kappa} \not\equiv 0 \pmod p$.

Take $I \in S_0$, then by assumption $\Phi_{I,0}(\tau) \not\equiv 0 \pmod p$. By Lemma 3.14 there exists $\tilde{\Phi}_{I,0} \in \mathcal{A}_I^1(576N, \mathbb{Z}_p)$ such that $\tilde{\Phi}_{I,0}(\tau) \equiv \Phi_{I,0}(\tau)$ and

$$\tilde{\Phi}_{I,0}(\tau) = b_r q^r + O(q^{r+1}), \quad p \nmid b_r.$$

Divide the relation by $\tilde{\Phi}_{I,0}(\tau)q^\kappa$. We obtain the relation

$$\sum_{\kappa\leq j\leq M} q^{j-\kappa} \sum_{i\in S_j} \frac{\Phi_{i,j}(\tau)}{\tilde{\Phi}_{I,0}(\tau)} + q^{-\kappa} + \sum_{i\in S_0, i\neq I} q^{-\kappa} \frac{\Phi_{i,0}(\tau)}{\tilde{\Phi}_{I,0}(\tau)} \equiv 0 \pmod p. \tag{25}$$

Let $\sum a(n)q^n = \sum_{i\in S_\kappa} \frac{\Phi_{i,\kappa}(\tau)}{\tilde{\Phi}_{I,0}(\tau)}$. By Lemma 3.17 there exists a minimal integer $d > \kappa$ such that $a(n) \not\equiv 0 \pmod p$ or $\sum a(n)q^n \equiv a(0) \pmod p$. Let

$$s := \begin{cases} \kappa + 1 & \text{if } \sum a(n)q^n \equiv a(0) \pmod p, \\ d & \text{otherwise.} \end{cases}$$

Then applying $V_s U_s$ to the relation (25) and defining for $j \in \{0\} \cup \{\kappa, \ldots, m\}$ and $i \in S_j$:

$$B_{i-I,j}(\tau) := q^{-j+\kappa} V_s U_s \left(q^{j-\kappa} \frac{\Phi_{i,j}(\tau)}{\tilde{\Phi}_{I,0}(\tau)}\right)$$

yields a relation of the form

$$\sum_{\kappa\leq j\leq M} q^{j-\kappa} \sum_{i\in S_j} B_{i-I,j}(\tau) + \sum_{i\in S_0, i\neq I} B_{i-I,0}(\tau) \equiv 0 \pmod p \tag{26}$$

and $\sum_{i\in S_\kappa} B_{i-I,\kappa}(\tau) \not\equiv 0 \pmod p$ by construction. Multiplying the above relation by q^κ we obtain

$$\sum_{\kappa\leq j\leq M} q^{j} \sum_{i\in S_j} B_{i-I,j}(\tau) + \sum_{i\in S_0, i\neq I} B_{i-I,0}(\tau) \equiv 0 \pmod p \tag{27}$$

Note that $B_{i,j}(\tau) \in \mathcal{A}_i^1(576Ns^2)$ because of Lemma 3.13. Thus we obtain a new relation with length $< M$ which implies by induction that $\sum_{i \in S_j} B_{i-I,j}(\tau) \equiv 0 \pmod{p}$ for all $j \in \{0, \ldots, m\}$ in particular also for $j = \kappa$ which is a contradiction. □

4. Conclusion

The conclusion of this paper is that relations of the general form in the abstract can be reduced to much simpler relations, therefore it is not very likely that one would find in the literature such general relations, at least we are not aware of any. This paper can serve as a proof of nonexistence of nontrivial relations of such general form. Here by nontrivial we mean such that are not composed by simpler relations, that is irreducible in some sense. This paper also answers a question by Peter Paule communicated to the author in a private discussion. For this reason it is published with the occasion of his 60th birthday.

References

[1] P. Deligne and M. Rapoport. Les Schémas de Modules de Courbes Elliptiques. In *Modular Functions of one Variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer-Verlag Berlin, 1973.

[2] I. G. MacDonald. *Symmetric Functions and Hall Polynomials*. Oxford University Press, 1995.

[3] A. Ogg. *Modular Forms and Dirichlet Series*. W. A. Benjamin, Inc., New York-Amsterdam, 1969.

[4] K. Ono. *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q-Series*, volume 102 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[5] B. Schoeneberg. *Elliptic Modular Functions*. Springer-Verlag, 1974.

[6] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971.

Research Institute for Symbolic Computation (RISC), Johannes Kepler University, A-4040 Linz, Austria