PROOF OF A CONJECTURE BY AHLGREN AND ONO

SILVIU RADU

Abstract. Let $p(n)$ denote the number of partitions of n. In this paper we prove that if $\{An+B\}$ is an arithmetic progression and $\ell \geq 5$ a prime, such that

$$p(An+B) \equiv 0 \pmod{\ell}, \quad n \in \mathbb{N}.$$

Then $\ell | A$ and $\left(\frac{24B-1}{\ell}\right) \neq \left(\frac{-1}{\ell}\right)$. This settles an open problem by Scott Ahlgren and Ken Ono. Our proof is based on results by Deligne and Rapoport.

1. Introduction

For $\ell \geq 5$ a prime we define

$$\delta_\ell := \frac{\ell^2-1}{24}, \quad \epsilon_\ell := \left(\frac{-6}{\ell}\right)$$

and

$$S_\ell := \{\beta \in \{0,\dots,\ell-1\} : \left(\frac{\beta+\delta_\ell}{\ell}\right) = 0 \text{ or } -\epsilon_\ell\}.$$

Let $p(n)$ denote the number of partitions of $n \in \mathbb{N}$. The pourpose of this paper is to prove the following theorem conjectured by Scott Ahlgren and Ken Ono [2]:

Theorem 1.1. *Suppose that $\ell \geq 5$ is prime, $A, B \in \mathbb{N}$ such that $A > B$ and*

$$p(An+B) \equiv 0 \pmod{\ell}, \quad n \in \mathbb{N}.$$

Then $\ell | A$ and there exists $\beta \in S_\ell$ such that $B \equiv \beta \pmod{\ell}$.

The importance of this theorem is motivated by a previous paper [1] by the authors where they prove the following theorem:

Theorem 1.2 (Ahlgren and Ono)**.** *If $\ell \geq 5$ is prime, m is a positive integer, and $\beta \in S_\ell$, then there are infinitely many non-nested arithmetic progressions $\{An+B\} \subseteq \{\ell n+\beta\}$, such that for every integer n we have*

$$p(An+B) \equiv 0 \pmod{\ell^m}.$$

In [1, Sect. 1] the authors write: "In Section 4, we consider those progressions $\ell n+\beta$ for $\beta \notin S_\ell$. We give heuristics that cast doubt on the existence of congruences within these progressions." The proof of the Theorem 1.1 is based on deep results by Deligne and Rapoport [3] and some results in [5] or [7]. We are also using theorems 4.2, 4 and 4.4 which were used in a previous paper and are also based on

S. Radu was supported by DK grant W1214-DK6 of the Austrian Science Funds FWF.

results in [3]. Our contribution is the Lemma 5.5 which takes the main part of the last section.

The organization of this paper is as follows. In Section 2 we prove Theorem 1.1 by citing several theorems in Section 4. In Section 3 we give some preliminaries to modular forms. In Section 4 we make a classification of congruences in the sense that we show that some congruences are implied by others in a progression with smaller modulus. In Section 5 we prove our main result Lemma 5.5 which is needed for proving Lemma 4.6 in Section 4. Also in Section we prove Lemma 5.6 which is a technical result needed to prove Lemma 4.5 in Section 4.

We continue the introduction with the following reformulation of the set S_ℓ in Theorem 1.1.

Lemma 1.3. *For $\ell \geq 5$ a prime we have*

$$S_\ell = \left\{ \beta \in \{0, \dots, \ell - 1\} : \left(\frac{24\beta - 1}{\ell}\right) \neq \left(\frac{-1}{\ell}\right) \right\}.$$

Proof. First note that

$$\left(\frac{\beta + \delta_\ell}{\ell}\right) = 0 \Leftrightarrow \left(\frac{24}{\ell}\right)\left(\frac{\beta + \delta_\ell}{\ell}\right) = 0 \Leftrightarrow \left(\frac{24\beta - 1}{\ell}\right) = 0. \tag{1}$$

Similarly

(2)

$$\left(\frac{\beta + \delta_\ell}{\ell}\right) = -\epsilon_\ell \Leftrightarrow \left(\frac{24}{\ell}\right)\left(\frac{\beta + \delta_\ell}{\ell}\right) = -\left(\frac{24}{\ell}\right)\epsilon_\ell \Leftrightarrow \left(\frac{24\beta - 1}{\ell}\right) = -\left(\frac{-1}{\ell}\right).$$

Note that $\left(\frac{-1}{\ell}\right) = (-1)^{\frac{\ell-1}{2}} \neq 0$ implies that for any $\beta \in \{0, \dots, \ell - 1\}$

$$\left(\frac{24\beta - 1}{\ell}\right) = 0 \quad \text{or} \quad \left(\frac{24\beta - 1}{\ell}\right) = -\left(\frac{-1}{\ell}\right)$$

is equivalent to

$$\left(\frac{24\beta - 1}{\ell}\right) \neq \left(\frac{-1}{\ell}\right),$$

which together with (1) and (2) implies the desired result. □

2. The proof

Let $A, B \in \mathbb{N}$ with $A > B$ such that

$$p(An + B) \equiv 0 \pmod{\ell}, \quad n \in \mathbb{N}.$$

Then by Theorem 4.3 there exists a positive integer Q coprime to 6 dividing A and a $\bar{t} \in \{0, \dots, Q - 1\}$ with $\bar{t} \equiv B \pmod{Q}$ such that

$$p(Qn + \bar{t}) \equiv 0 \pmod{\ell}, \quad n \in \mathbb{N}.$$

Then $\ell | Q$ because if not, then by Theorem 4.4 there exists a positive integer n_0 such that $\ell \nmid p(Qn_0 + \bar{t})$. Hence we may write $Q = Q_0 \ell^r$ for some positive integers

Q_0, r with $\gcd(Q_0, \ell) = 1$. Now if $24\bar{t} - 1 \equiv 0 \pmod{\ell}$, then we are finished. So assume that $24\bar{t} - 1 \not\equiv 0 \pmod{\ell}$. Then by Lemma 4.5

$$p(\ell Q_0 n + \bar{t}^*) \equiv 0 \pmod{\ell}, \quad n \in \mathbb{N}, \tag{3}$$

where $\bar{t}^*$ is the minimal nonnegative integer such that $\bar{t}^* \equiv \bar{t} \pmod{\ell Q}$. Next we apply Lemma 4.6 to the congruence (3) and we obtain $\left(\frac{24\bar{t}^*-1}{\ell}\right) \neq \left(\frac{-1}{\ell}\right)$ which together with Lemma 1.3 implies the desired result.

3. Preliminaries

For f a holomorphic function on the upper half plane $\mathbb{H}$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ (the set of all 2×2 matrices with integer entries and determinant 1), we define

$$(f|_k\gamma)(\tau) := (c\tau + d)^{-k} f\left(\frac{a\tau + b}{c\tau + d}\right), \quad \tau \in \mathbb{H}.$$

For every positive integer M we denote by $\Gamma(M)$ the set of all matrices in $\mathrm{SL}_2(\mathbb{Z})$ congruent to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ modulo M. For k an integer and Γ a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing $\Gamma(N)$ for some N we denote by $M_k(\Gamma)$ the set of all holomorphic functions on the upper half plane $\mathbb{H}$ satisfying

- for all $\gamma \in \Gamma$ we have $f|_k\gamma = f$;
- for all $\xi \in \mathrm{SL}_2(\mathbb{Z})$ the function $(f|_k\xi)(\tau)$ admits a Laurent series expansion in the variable $q_N := e^{2\pi i\tau/N}$. We call this expansion the *q-expansion of* $f|_k\gamma$.

For N a positive integer let

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

and

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a, d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N} \right\}.$$

In particular $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$.

4. A Classification of Congruences

Definition 4.1. *For m a positive integer and $t \in \{0, \ldots, m-1\}$ we define $P_m(t)$ to be the set of all $t' \in \{0, \ldots, m-1\}$ such that*

$$t' \equiv ta^2 + \frac{1 - a^2}{24} \pmod{m},$$

for some $a \in \mathbb{Z}$ with $\gcd(a, 6m) = 1$.

We have the following important theorems:

Theorem 4.2. *Let m, l be positive integers and $t \in \{0, \dots, m-1\}$ such that*

$$p(mn+t) \equiv 0 \pmod{l}, \quad n \in \mathbb{N}.$$

Then for all $t' \in P_m(t)$ we have

$$p(mn+t') \equiv 0 \pmod{l}, \quad n \in \mathbb{N}.$$

Theorem 4.3. *Let $a, b, Q, \nu \in \mathbb{N}$ and $t \in \{0, \dots, 2^a 3^b Q - 1\}$ with $\nu, Q > 0$ and* $\gcd(Q, 6)$. *Assume that*

$$p(2^a 3^b Qn + t) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}. \tag{4}$$

Then

$$p(Qn + \bar{t}) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N},$$

where $\bar{t}$ is the minimal nonnegative integer such that $t \equiv \bar{t} \pmod{Q}$.

Theorem 4.4. *Let Q, ν be positive integers such that $\gcd(Q, 6\nu) = 1$, $\nu \neq 1$ and $t \in \{0, \dots, Q-1\}$. Then there exists an integer n such that $\nu \nmid p(Qn+t)$.*

We prove

Lemma 4.5. *Let r, Q, ν be positive integers, $\ell \geq 5$ a prime and $t \in \{0, \dots, \ell^r Q - 1\}$. Let b be the maximal integer such that $\ell^b | (24t-1)$. If $r \geq b+1$ and*

$$p(\ell^r Qn + t) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}, \tag{5}$$

then

$$p(\ell^{b+1} Qn + \bar{t}) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N},$$

where $\bar{t}$ is the minimal nonnegative integer such that $t \equiv \bar{t} \pmod{\ell^{b+1} Q}$.

Proof. By (6) and Theorem 4.2 we have

$$p(\ell^r Qn + t') \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}, \quad t' \in P_{\ell^r Q}(t). \tag{6}$$

By (4.1) $t' \in P_{\ell^r Q}(t)$ iff there exists $a \in \mathbb{Z}$ with $\gcd(a, 6\ell Q) = 1$ such that

$$a^2(24t-1) \equiv 24t' - 1 \pmod{\ell^r Q}, \tag{7}$$

and $t' \in \{0, \dots, \ell^r Q - 1\}$. By Lemma 5.6 we obatain that for each $l \in \mathbb{Z}$ there exist $a_{r,l}$ with $\gcd(a_{r,l}, 6\ell Q) = 1$ such that

$$a_{r,l}^2(24t-1) \equiv 24(t + l\ell^{b+1}Q) - 1 \pmod{\ell^r Q},$$

which implies by (7) that

$$\bar{t} + l\ell^{b+1}Q \in P_{\ell^r Q}(t)$$

for every $l \in \{0, \dots, \ell^{r-b-1} - 1\}$, implying together with Theorem 4.2 that

$$p(\ell^r Qn + \bar{t} + l\ell^{b+1}Q) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N},$$

for every $l \in \{0, \dots, \ell^{r-b-1} - 1\}$. Since

$$\ell^r Qn + \bar{t} + l\ell^{b+1}Q = \ell^{b+1}Q(\ell^{r-b-1}n + l) + \bar{t}$$

and every nonnegative integer m can be written as $m = \ell^{r-b-1}n + l$ for some nonnegative integers n, l with $l \in \{0, \dots, \ell^{r-b-1} - 1\}$ we conclude

$$p(\ell^{b+1}Qm + \bar{t}) \equiv 0 \pmod{\nu}, \quad m \in \mathbb{N}.$$

□

Lemma 4.6. *Let $\ell \geq 5$ be a prime, Q a positive integer such that $\gcd(Q, 6\ell) = 1$ and $\beta \in \{0, \dots, \ell Q - 1\}$. Assume that*

$$p(\ell Q n + \beta) \equiv 0 \pmod{\ell}, \quad n \in \mathbb{N}. \tag{8}$$

Then $\left(\frac{24\beta-1}{\ell}\right) \neq \left(\frac{-1}{\ell}\right)$.

The proof is based on the following lemma by Deligne and Rapoport:

Theorem 4.7. [3, VII, Cor. 3.12] *Let k, N be positive integers, p a prime number and p^m the highest power of p dividing N, $\gamma = \left(\begin{smallmatrix} a & b \\ p^m c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $f \in M_k(\Gamma(N))$. Let π be a prime ideal in $\mathbb{Z}[e^{2\pi i/N}]$ lying above p. Assume that the coefficients in the q-expansion of f are in $\mathbb{Z}[e^{2\pi i/N}]$. Let ν be a nonnegative integer such that $f \equiv 0 \pmod{\pi^\nu}$*[1]*. Then $f|_k\gamma \equiv 0 \pmod{\pi^\nu}$.*

Proof of Lemma 4.6: Assume that

$$\left(\frac{24\beta - 1}{\ell}\right) = \left(\frac{-1}{\ell}\right).$$

Then there exists $a \in \mathbb{Z}$ such that

$$(24\beta - 1)a^2 \equiv -1 \pmod{\ell}, \tag{9}$$

which implies together with $\gcd(Q, 6\ell) = 1$ that there exists $\overline{a} \in \mathbb{N}$ with $\gcd(\overline{a}, 6\ell Q) = 1$ such that

$$\overline{a} \equiv aQ \pmod{\ell}. \tag{10}$$

Let $\overline{\beta} \in \{0, \dots, \ell Q - 1\}$ be uniquely defined by the relation

$$\overline{a}^2(24\beta - 1) \equiv (24\overline{\beta} - 1) \pmod{\ell Q}. \tag{11}$$

By [7, Th. 2.14], we have for a suitable positive integer k

$$G^{(k)}_{\ell Q, \overline{\beta}} := \eta^{24k} \left(q^{\frac{24\overline{\beta}-1}{\ell Q}} \sum_{n=0}^{\infty} p(\ell Q n + \overline{\beta}) q^n \right)^{24\ell Q} \in M_{12(k-\ell Q)}(\Gamma_1(\ell Q)), \tag{12}$$

where $\eta(\tau) := e^{\pi i \tau/12} \prod_{n=1}^{\infty}(1 - e^{2\pi i n \tau})^{24}$, $\tau \in \mathbb{H}$ is the Dedekind eta function and satisfies $\eta^{24}|_{12}\gamma = \eta^{24}$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Let $X > 0$ and Y be integers such that

$$24^2\ell^2 X + YQ = 1. \tag{13}$$

Then $\left(\begin{smallmatrix} 1 & -24^2 X\ell \\ \ell & YQ \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. We apply Lemma 5.5 with $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & -24^2 X\ell \\ \ell & YQ \end{smallmatrix}\right)$, $x = 24\ell X$, $y = Y$, $m = \ell Q$, $t = \overline{\beta}$ and $r = -1$. We then obtain

[1]For given positive integers k, N and $f \in M_k(\Gamma(N))$ with the coefficients of the q-expansion of f in $\mathbb{Z}[1/N, e^{2\pi i/N}]$ we obtain by Theorem [3, VII, Cor. 3.13] that for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the coefficients in the q-expansion of $f|_k\gamma$ have the same property. In this case there exists also a power N^j of N such that for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the coefficients in the q-expansion of $N^j f|_k\gamma$ are in $\mathbb{Z}[e^{2\pi i/N}]$ (see for example [3, VII, Cor 3.11]). Consequently for a given prime p and a prime ideal π in $\mathbb{Z}[e^{2\pi i/N}]$ lying above p it makes sense to write $f|_k\gamma \equiv 0 \pmod{\pi^\nu}$ if all the coefficients in the q-expansion of $f|_k\gamma$ lie in the ideal π^ν.

$$\begin{aligned}(14)\quad & e^{\frac{\pi i(3-Q)}{12}} e^{-\frac{48\pi i X(24\overline{\beta}-1)}{Q}} g(\ell Q, \overline{\beta}, -1, \gamma\tau)(-i(\ell\tau+YQ))^{1/2} \\ &= \frac{1}{Q}\sum_{d|Q} d^{-1/2} e^{-\frac{\pi i(d-1)}{4}} \xi^{-1}(d) e^{\frac{2\pi i(24t_d-1)d^2\tau}{24\ell Q}} \times \sum_{n=0}^{\infty} e^{\frac{2\pi i n d^2\tau}{Q}} p(\ell n+t_d) T(n,d)\end{aligned}$$

where t_d is the unique integer satisfying

$$(15)\qquad (24\overline{\beta}-1) \equiv d^2(24t_d-1) \pmod{\ell}, \quad 0 \le t_d < \ell - 1,$$

$$\xi(d) = \left(\frac{24\ell}{Q/d}\right)(-1)^{\frac{Qd-1}{2}\frac{d-1}{2}},$$

$$T(n,d) = \sum_{\substack{0\le s<Q/d \\ \gcd(s,Q/d)=1}} \left(\frac{24\ell s}{Q/d}\right) e^{-\frac{48\pi i X}{Q/d}\{\iota_{s,d}(24(\ell n+t_d)-1)+s(24\overline{\beta}-1)\}}$$

and for $s, d \in \mathbb{Z}$ such that $d|Q$ and $\gcd(s, Q/d) = 1$, the symbol $\iota_{s,d}$ is any integer satisfying $s \cdot \iota_{s,d} \equiv 1 \pmod{Q/d}$. Next we observe that $T(n,Q) = 1$ for all $n \in \mathbb{N}$ because of $\left(\frac{a}{1}\right) = 1$ for $a \in \mathbb{Z}$. Because of (9),(10) and (15) we have $t_Q = 0$ and consequently (14) transforms into

$$\begin{aligned}(16)\quad & e^{\frac{\pi i(3-Q)}{12}} e^{-\frac{48\pi i X(24\overline{\beta}-1)}{Q}} g(\ell Q, \overline{\beta}, -1, \gamma\tau)(-i(\ell\tau+YQ))^{1/2} \\ &= \frac{1}{Q} Q^{-1/2} e^{-\frac{\pi i(Q-1)}{4}} \xi^{-1}(Q) q_m^{-\frac{Q^2}{24}} \sum_{n=0}^{\infty} q_m^{\ell Q^2 n} p(\ell n) \\ &\quad + \frac{1}{Q} \sum_{d|Q, d\neq Q} d^{-1/2} e^{-\frac{\pi i(d-1)}{4}} \xi^{-1}(d) q_m^{\frac{(24t_d-1)d^2}{24}} \sum_{n=0}^{\infty} q_m^{n\ell d^2} p(\ell n+t_d) T(n,d) \\ &= q_m^{-Q^2/24} F(q_m),\end{aligned}$$

where $m := \ell Q$, $q_m := e^{\frac{2\pi i\tau}{m}}$ and $F(q_m)$ is a Laurent series in q_m because of $d^2(24t_d-1)+Q^2 \equiv 0 \pmod{24}$ because of $Q^2, d^2 \equiv 1 \pmod{24}$[2]. Next note that $F(q^m)$ has coefficients in $\mathbb{Z}[1/m, e^{2\pi i/m}]$ because for $d|Q$ we have $d^{1/2}e^{\frac{\pi i(d-1)}{4}} = \pm\epsilon(d)d^{1/2}$ where

$$\epsilon(d) := \begin{cases} 1, & \text{if } d \equiv 1 \pmod{4} \\ i, & \text{if } d \equiv 3 \pmod{4}\end{cases}$$

and by [4, p. 87] we have

$$\epsilon(d)d^{1/2} = \sum_{\lambda=0}^{d-1} e^{2\pi i\lambda^2/d}$$

which is obviously in $\mathbb{Z}[1/m, e^{2\pi i/m}]$. Furthermore, if π is a prime ideal in $\mathbb{Z}[e^{\frac{2\pi i}{\ell Q}}]$ lying above ℓ, then it makes sense to reduce the coefficients of $F(q_m)$ modulo π because all denominators in the coefficients of $F(q_m)$ are invertible modulo π. We observe that

$$(17)\qquad F(q_m) \not\equiv 0 \pmod{\pi}$$

because by (16) the order of $F(q_m)$ is 0 and the coefficient of the term constant term is equal to $\frac{1}{Q^{3/2}} e^{-\frac{\pi i(Q-1)}{4}} \xi^{-1}(Q) \not\equiv 0 \pmod{\pi}$.

[2]In fact $F(q_m)$ is a Laurent series in q_m^{ℓ} because of $d^2(24t_d-1)+Q^2 \equiv 0 \pmod{\ell}$ because of (9)-(11) and (15).

By (16), Definition 5.3 and Lemma 5.4 we have

$$G^{(k)}_{\ell Q,\overline{\beta}}|_\kappa \begin{pmatrix} 1 & -24^2\ell X \\ \ell & QY \end{pmatrix} = \eta^{12k} q^{-1} F^{24\ell Q}(q_m)$$

where $\kappa := 12(k - \ell Q)$. Then (17) implies

$$G^{(k)}_{\ell Q,\overline{\beta}}|_\kappa \begin{pmatrix} 1 & -24^2\ell X \\ \ell & QY \end{pmatrix} \not\equiv 0 \pmod{\pi},$$

and by Theorem 4.7

$$G^{(k)}_{\ell Q,\overline{\beta}} \not\equiv 0 \pmod{\pi},$$

and consequently $p(\ell Qn + \overline{\beta}) \not\equiv 0 \pmod{\ell}$ for some $n \in \mathbb{N}$ and since $\beta \in P_{\ell Q}(\overline{\beta})$ because of (11) and Definition 4.1 we obtain by Theorem 4.2 that $p(\ell Qn + \beta) \not\equiv 0 \pmod{\ell}$ for some $n \in \mathbb{N}$ which is a contradiction to our assumption (8).

5. A Modular Substitution Formula

Definition 5.1. *Let m be a positive integer and $c \in \mathbb{Z}$. Then we define $\pi(m, c) := (m_0, m_c)$ where*

- *m_0, m_c are positive integers such that $m_0 m_c = m$;*
- *$\gcd(m_0, c) = 1$;*
- *for every prime p we have $p|m_c$ implies $p|c$.*

We also define the set

$$\Delta(m_0, m_c) := \{(d, l, s) \in \mathbb{Z}^3 | d|m_0, d > 0, 0 \le s < m_0/d, \gcd(s, m_0/d) = 1, 0 \le l < m_c\}.$$

Lemma 5.2. *Let m be a positive integer coprime to 6 and $a, c, m_0, m_c, x, y \in \mathbb{Z}$ such that*

(i) *$\gcd(a, c) = 1$;*
(ii) *$(m_0, m_c) := \pi(m, c)$;*
(iii) *$24xc + m_0 y = 1$.*

Then

(a) *for any $\lambda \in \mathbb{Z}$ such that*

$$\lambda \equiv -ax + sd + lm_0 \pmod{m} \tag{18}$$

for some $(d, l, s) \in \Delta(m_0, m_c)$ we have

$$\gcd(a + 24\lambda c, m) = d; \tag{19}$$

(b) *for any $\lambda \in \mathbb{Z}$ there exists unique $(d, l, s) \in \Delta(m_0, m_c)$ such that (18). Consequently, we have a mapping $\lambda \mapsto (d, l, s)$ and the restriction of this mapping to a complete set of representatives of the residue classes modulo m is a bijection.*

Proof. (a): First we note that $\gcd(a+24\lambda c, m) = \gcd(a+24\lambda c, m_0)$ because of *(i)-(ii)*. Next we have

$$a + 24\lambda c \equiv a + 24(-ax+sd)c \equiv a(1-24cx) + 24sdc \equiv am_0y + 24sdc \pmod{m_0},$$

which implies

$$\gcd(a+24\lambda c, m_0) = \gcd(24sdc, m_0) = d\gcd(24sc, m_0/d) = d.$$

This proves *(a)*.

(b): We need to show that for any $\lambda \in \mathbb{Z}$ there exist $d|m_0$ with $d > 0$ and $s \in \mathbb{Z}$ with $\gcd(s, m_0/d) = 1$ and $0 \leq s < m_0/d$ such that

$$\lambda \equiv -ax + sd \pmod{m_0}.$$

We set $d := \gcd(a+24\lambda c, m_0)$ and $s := \frac{(a+24\lambda c)x}{d}$. Obviously we have $\gcd(s, m_0/d) = 1$ and

$$-ax + sd = -ax + (a+24\lambda c)x = 24\lambda cx \equiv \lambda \pmod{m_0}.$$

It remains to show uniqueness. Let $(d_1, l_1, s_1), (d_2, l_2, s_2) \in \Delta(m_0, m_c)$ be such that

$$\lambda \equiv -ax + s_1d_1 + l_1m_0 \equiv -ax + s_2d_2 + l_2m_0 \pmod{m}.$$

Then because of (19) we have $d := d_1 = d_2$ which implies that

$$(s_1 - s_2)d + (l_1 - l_2)m_0 \equiv 0 \pmod{m} \tag{20}$$

and consequently $s_1 \equiv s_2 \pmod{m_0/d}$. Because of $s_1, s_2 \in \{0, \ldots, m_0/d - 1\}$ we have $s_1 = s_2$ which together with (20) gives $l_1 \equiv l_2 \pmod{m_c}$.

The final fact that the association $\lambda \mapsto (d, l, s)$ indeed is a bijection modulo m is just straight forward verification. □

Definition 5.3. *For m a positive integer coprime to 6, $t \in \{0, \ldots, m-1\}$ and $r \in \mathbb{Z}$. Then we define*

$$g(m,t,r,\tau) := \frac{1}{m}\sum_{\lambda=0}^{m-1} e^{\frac{2\pi i\lambda(-24t-r)}{m}} \eta^r\left(\frac{\tau+24\lambda}{m}\right), \quad \tau \in \mathbb{H}.$$

A proof of the following lemma can be found in [7, Lem. 1.12].

Lemma 5.4. *Let m be a positive integer coprime to 6, $t \in \{0, \ldots, m-1\}$ and $r \in \mathbb{Z}$. Then*

$$g(m,t,r,\tau) = q^{\frac{24t+r}{24m}} \sum_{n=0}^{\infty} p_r(mn+t)q^n, \quad \tau \in \mathbb{H}, \quad (q = e^{2\pi i\tau}).$$

Lemma 5.5. *Let m be a positive integer coprime to 6, $t \in \{0, \ldots, m-1\}$, $r \in \mathbb{Z}$, $\gamma = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $\gcd(A, 6) = 1$, $A > 0$, $C > 0$ and $(m_0, m_C) := \pi(m, C)$ and assume that $m_C|C$. For any integers s and $d|m_0$ such that $\gcd(s, m_0/d) = 1$ let $\iota_{s,d}$ be any integer satisfying $s \cdot \iota_{s,d} \equiv 1 \pmod{m_0/d}$. Let x, y, A' be any integers such that*

(i) $24xC + ym_0 = 1$ *and* $x \equiv 0 \pmod{24C}$, $x < 0$;
(ii) $AA' \equiv 1 \pmod{24C}$.

Define

$$\tau'(s,d) := \frac{d\tau + 24x(-x\iota_{s,d} + dD)}{m_0/d} + d^2y(BA' + 24sdD^2)$$

and

$$\xi(d) := \left(\frac{24C}{m_0/d}\right)\left(\frac{Ad}{Cm_C}\right)(-1)^{\frac{Cmd-1}{2}\frac{Ad-1}{2}}.$$

Then

$$\begin{aligned}(21)\qquad & e^{\frac{\pi i Ar(mC-3)}{12}}e^{-\frac{2\pi i Ax(24t+r)}{m}}g(m,t,r,\gamma\tau)(-i(C\tau+D))^{-r/2}\\ =&\frac{1}{m}\sum_{d|m_0} d^{r/2}e^{\frac{\pi i Ar(d-1)}{4}}\xi^r(d)\sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)}}\left(\frac{s}{m_0/d}\right)^r e^{\frac{2\pi i(-24t-r)s}{m/d}}\\ &\times\sum_{l=0}^{m_C-1} e^{\frac{2\pi i l(Am_0y/d)^2(-24t-r)}{m_C}}\eta^r\left(\frac{\tau'(s,d)+24l}{m_C}\right)\end{aligned}$$

and

$$\begin{aligned}(22)\qquad & e^{\frac{\pi i Ar(mC-3)}{12}}e^{-\frac{2\pi i Ax(24t+r)}{m}}g(m,t,r,\gamma\tau)(-i(C\tau+D))^{-r/2}\\ =&\frac{1}{m_0}\sum_{d|m_0} e^{\frac{\pi i Ar(d-1)}{4}}d^{r/2}\xi^r(d)e^{\frac{2\pi i(24t_d+r)d^2(\tau+24xD+m_0yBA')}{24m}}\\ &\times\sum_{n=0}^{\infty} e^{\frac{2\pi i n d^2(\tau+24xD)}{m_0}}p_r(m_Cn+t_d)T(n,d)\end{aligned}$$

where t_d *is the unique integer satisfying*

$$(23)\qquad A^2(24t+r)\equiv d^2(24t_d+r)\pmod{m_C}$$

and $0\le t_d<m_C-1$ *and*

$$T(n,d) := \sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)=1}}\left(\frac{24Cs}{m_0/d}\right)^r e^{-\frac{2\pi i x/m_C}{m_0/d}\{\iota_{s,d}(24(nm_C+t_d)+r)+s(24t+r)\}}.$$

Proof. Proof of (21)*:* By Lemma 5.2 and Definition we have

(24)

$$\begin{aligned}& g(m,t,r,\gamma\tau)\\ =&\frac{1}{m}\sum_{d|m_0}\sum_{\substack{0\le s<\frac{m_0}{d}-1\\ \gcd(s,m_0/d)=1}}\sum_{l=0}^{m_C-1}e^{\frac{2\pi i(-Ax+sd+lm_0)(-24t-r)}{m}}\eta^r\left(\frac{\gamma\tau+24(-Ax+sd+lm_0)}{m}\right).\end{aligned}$$

Next we note that for $(d,l,s)\in\Delta(m_0,m_c)$ we have

$$(25)\qquad \frac{\gamma\tau+24\lambda}{m} = M_\lambda\frac{d\tau+(B+24\lambda D)x_\lambda+24mDy_\lambda}{m/d},$$

where

$$(26)\qquad \lambda := -Ax+sd+lm_0,$$

$M_\lambda := \begin{pmatrix}\frac{A+24\lambda C}{d} & -24y_\lambda\\ \frac{Cm}{d} & x_\lambda\end{pmatrix}$ and x_λ, y_λ are integers such that

$$(27)\qquad (A+24\lambda C)x_\lambda+24mCy_\lambda = d.$$

Newman [6] proved that for each $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $a, c > 0$ and $\gcd(a,6) = 1$ we have

$$\eta(\gamma\tau) = (-i(c\tau+d))^{1/2}\epsilon(a,b,c,d)\eta(\tau), \quad \tau \in \mathbb{H}, \tag{28}$$

where

$$\epsilon(a,b,c,d) := \left(\frac{c}{a}\right) e^{-\frac{\pi i a}{12}(c-b-3)}. \tag{29}$$

By (25) and (28) we obtain

(30)
$$\eta\left(\frac{\gamma\tau+24\lambda}{m}\right) = (-id(C\tau+D))^{1/2}$$
$$\times\epsilon\left(\frac{A+24\lambda C}{d}, -24y_\lambda, Cm/d, x_\lambda\right)\eta\left(\frac{d\tau+(B+24\lambda D)x_\lambda+24mDy_\lambda}{m/d}\right).$$

By (26) and *(i)* we have

(31)
$$\begin{aligned}\frac{A+24\lambda C}{d} &= \frac{A+24(-Ax+sd+lm_0)C}{d} = \frac{A(1-24Cx)+24Csd+24lm_0C}{d}\\ &= \frac{Aym_0+24Csd+24lm_0C}{d} = \frac{Aym_0}{d}+24(Cs+lm_0C/d),\end{aligned}$$

which together with (29) implies that

$$\begin{aligned}&\epsilon\left(\frac{A+24\lambda C}{d}, -24y_\lambda, Cm/d, x_\lambda\right)\\ =&\epsilon(Aym_0/d+24(Cs+lm_0C/d), -24y_\lambda, Cm/d, x_\lambda)\\ =&\left(\frac{Cm/d}{Aym_0/d+24(Cs+lm_0C/d)}\right)e^{-\frac{\pi i Aym_0/d}{12}(Cm/d-3)}\end{aligned}$$

and by standard properties of the jacobi symbol

$$\begin{aligned}&\left(\frac{Cm/d}{Aym_0/d+24(Cs+lm_0C/d)}\right)\\ =&(-1)^{\frac{Cm/d-1}{2}\frac{Aym_0d-1}{2}}\left(\frac{Aym_0/d+24(Cs+lm_0C/d)}{Cm/d}\right)\\ =&(-1)^{\frac{Cm/d-1}{2}\frac{Aym_0d-1}{2}}\left(\frac{24Cs}{m_0/d}\right)\left(\frac{Aym_0/d}{Cm_c}\right)\\ =&(-1)^{\frac{Cm/d-1}{2}\frac{Aym_0d-1}{2}}\left(\frac{24Cs}{m_0/d}\right)\left(\frac{Aym_0d}{Cm_c}\right)\\ =&(-1)^{\frac{Cm/d-1}{2}\frac{Ad-1}{2}}\left(\frac{24Cs}{m_0/d}\right)\left(\frac{Ad}{Cm_c}\right),\end{aligned}$$

because by *(i)* we have $ym_0 \equiv 1 \pmod{24C}$. By the above calculation we have

$$(32)\quad \begin{aligned} &\epsilon\left(\frac{A+24\lambda C}{d}, -24y_\lambda, Cm/d, x_\lambda\right) \\ =&(-1)^{\frac{Cm/d-1}{2}\frac{Ad-1}{2}}\left(\frac{24Cs}{m_0/d}\right)\left(\frac{Ad}{Cm_C}\right)e^{-\frac{\pi i A y m_0/d}{12}(Cm/d-3)} \\ =&(-1)^{\frac{Cmd-1}{2}\frac{Ad-1}{2}}\left(\frac{24Cs}{m_0/d}\right)\left(\frac{Ad}{Cm_C}\right)e^{-\frac{\pi i Ad}{12}(Cmd-3)} \\ =&e^{\frac{\pi i A(3-mC)}{12}}e^{\frac{\pi i A(d-1)}{4}}\xi(d)\left(\frac{s}{m_0/d}\right), \end{aligned}$$

by using $ym_0 \equiv 1 \pmod{24}$ and $d^2 \equiv 1 \pmod{24}$. By (30) and (32) and because of $\eta(\tau+24) = \eta(\tau)$ we obtain

$$(33)\quad \begin{aligned} &e^{\frac{\pi i A(mC-3)}{12}}(-i(C\tau+D))^{-1/2}\eta\left(\frac{\gamma\tau+24\lambda}{m}\right) = \\ &\qquad d^{1/2}e^{\frac{\pi i A(d-1)}{4}}\xi(d)\left(\frac{s}{m_0/d}\right)\eta\left(\frac{d\tau+(B+24\lambda D)x_\lambda}{m/d}\right). \end{aligned}$$

Next we obtain a better expression for x_λ. By (27):

$$\frac{A+24\lambda C}{d}x_\lambda \equiv 1 \pmod{m_0/d}$$

and by (31):

$$\frac{A+24\lambda C}{d} \equiv 24Cs \pmod{m_0/d}$$

which implies

$$24Csx_\lambda \equiv 1 \pmod{m_0/d}$$

which together with *(i)* implies

$$(34)\quad x_\lambda \equiv x\iota_{s,d} \pmod{m_0/d}.$$

By (34) we conclude that

$$(35)\quad x_\lambda = x\iota_{s,d} + vm_0/d.$$

By (27), (35) and *(i)* we find

$$(36)\quad A(x\iota_{s,d} + vm_0/d) \equiv Avm_0/d \equiv d \pmod{24C}$$

because by assumption *(i)* we have $x \equiv 0 \pmod{24C}$. By (36), i and *(ii)* we obtain

$$v \equiv A'd^2y \pmod{24C},$$

which togeter with (35) implies

$$(37)\quad x_\lambda \equiv x\iota_{s,d} + A'ydm_0 \pmod{24m_0C/d}$$

Using the above formulas we compute $(B+24\lambda D)x_\lambda$ modulo $24Cm_0/d$. By using (37) and (26) we find

$$\begin{aligned} &(B+24\lambda D)x_\lambda \\ =&(24Dlm_0A'yd + BA'yd - 24AA'Ddxy + 24Dsd^2A'y + 24Dlx\iota_{s,d})m_0 \\ &+ Bx\iota_{s,d} - 24ADx^2\iota_{s,d} + 24Ddxs\iota_{s,d} \\ \equiv&(24Dlm_0A'yd + BA'yd + 24Dsd^2A'y)m_0 + Bx\iota_{s,d} - 24ADx^2\iota_{s,d} + 24Ddxs\iota_{s,d} \end{aligned}$$

because of $x \equiv 0 \pmod{24C}$ by *(i)*

$$\equiv (24D^2ld + BA'yd + 24D^2sd^2y)m_0 + Bx\iota_{s,d} - 24ADx^2\iota_{s,d} + 24Ddxs\iota_{s,d}$$

because of $ym_0 \equiv 1 \pmod{24C}$ by *(i)* and $24A' \equiv 24D \pmod{24C}$ because of $AD - BC = 1$

$$\equiv (24D^2ld + BA'yd + 24D^2sd^2y)m_0 + x(B\iota_{s,d} - 24ADx\iota_{s,d} + 24Dd) \pmod{\frac{24m_0C}{d}}$$

because of *(ii)* and $x \equiv 0 \pmod{24C}$ by *(i)*

$$\equiv (24D^2ld + BA'yd + 24D^2sd^2y)m_0 + x(-24x\iota_{s,d} + 24Dd) \pmod{\frac{24m_0C}{d}}$$

because of $B - 24ADx = B(1 - 24Cx) - 24x = Bym_0 - 24x$ by *(i)* and because of $AD - BC = 1$.

Next note that if v_1 and v_2 are integers such that $v_2 = v_1 + i(24m_0C/d)$ for some integer i, then

$$\eta\left(\frac{d\tau + v_2}{m/d}\right) = \eta\left(\frac{d\tau + v_1}{m/d} + i24m_0C/m\right) = \eta\left(\frac{d\tau + v_1}{m/d}\right),$$

because of $\eta(\tau + 24) = \eta(\tau)$ and $m_C|C$ by assumption. Using this fact with $v_1 = (B + 24\lambda D)x_\lambda$ and $v_2 = 24D^2ld + BA'yd + 24D^2sd^2y)m_0 + x(-24x\iota_{s,d} + 24Dd)$ on (33) we obtain

$$\begin{aligned} &(-i(C\tau + D))^{-1/2} e^{\frac{\pi i A(mC-3)}{12}} \eta\left(\frac{\gamma\tau + 24\lambda}{m}\right) \\ =& d^{1/2} e^{\frac{\pi i A(d-1)}{4}} \xi(d) \left(\frac{s}{m_0/d}\right) \eta\left(\frac{d\tau + (B + 24\lambda D)x_\lambda}{m/d}\right) \\ =& d^{1/2} e^{\frac{\pi i A(d-1)}{4}} \xi(d) \left(\frac{s}{m_0/d}\right) \\ &\times\eta\left(\frac{\frac{d\tau + x(-24x\iota_{s,d} + 24Dd)}{m_0/d} + (24D^2l + BA'y + 24D^2sdy)d^2}{m_C}\right) \\ =& d^{1/2} e^{\frac{\pi i A(d-1)}{4}} \xi(d) \left(\frac{s}{m_0/d}\right) \eta\left(\frac{\tau'(s,d) + 24D^2d^2l}{m_C}\right) \end{aligned} \tag{38}$$

By (38) and (24)

$$
\begin{aligned}
&e^{\frac{\pi i A r(mC-3)}{12}}(-i(C\tau+D))^{-r/2}g(m,t,r,\gamma\tau)\\
=&\frac{1}{m}\sum_{d|m_0}\sum_{\substack{0\le s<\frac{m_0}{d}-1\\ \gcd(s,m_0/d)=1}}\sum_{l=0}^{m_C-1}e^{\frac{2\pi i(-Ax+sd+lm_0)(-24t-r)}{m}}\\
&\times d^{r/2}e^{\frac{\pi i A r(d-1)}{4}}\xi^r(d)\left(\frac{s}{m_0/d}\right)^r\eta^r\left(\frac{\tau'(s,d)+24D^2d^2l}{m_C}\right)\\
=&e^{\frac{2\pi i A x(24t+r)}{m}}\frac{1}{m}\sum_{d|m_0}d^{r/2}e^{\frac{\pi i A r(d-1)}{4}}\sum_{\substack{0\le s<\frac{m_0}{d}-1\\ \gcd(s,m_0/d)=1}}e^{\frac{2\pi i s(-24t-r)}{m/d}}\\
&\times\sum_{l=0}^{m_C-1}e^{\frac{2\pi i l(-24t-r)}{m/m_0}}e^{\frac{\pi i A r(d-1)}{4}}\xi^r(d)\left(\frac{s}{m_0/d}\right)^r\eta^r\left(\frac{\tau'(s,d)+24D^2d^2l}{m_C}\right).
\end{aligned}
\tag{39}
$$

Summing in the last sum over any set of modulo m_C representatives does not change the value of the sum. In particular, we make the substitution $l=A^2(ym_0/d)^2l'$ and observe that $D^2d^2A^2(ym_0/d)^2\equiv 1 \pmod{m_C}$ because of *(i)* and $AD-BC=1$. Thus we obtain (21).

Proof of (22)*:* By (21) and Definition 5.3

(40)

$$
\begin{aligned}
&e^{\frac{\pi i A r(mC-3)}{12}}e^{-\frac{2\pi i A x(24t+r)}{m}}g(m,t,r,\gamma\tau)(-i(C\tau+D))^{-r/2}\\
=&\frac{m_C}{m}\sum_{d|m_0}d^{r/2}e^{\frac{\pi i A r(d-1)}{4}}\xi^r(d)\sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)}}\left(\frac{s}{m_0/d}\right)^r e^{\frac{2\pi i(-24t-r)s}{m/d}}g(m_C,t_d,r,\tau'(s,d))
\end{aligned}
$$

By Lemma 5.4

$$
g(m_C,t_d,r,\tau)=e^{\frac{2\pi i\tau(24t+r)}{24m_C}}\sum_{n=0}^{\infty}p(m_Cn+t_d)e^{2\pi i\tau n},\qquad \tau\in\mathbb{H}. \tag{41}
$$

By (41)

$$
\begin{aligned}
&\sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)}}\left(\frac{s}{m_0/d}\right)^r e^{\frac{2\pi i(-24t-r)s}{m/d}}g(m_C,t_d,r,\tau'(s,d))\\
=&\sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)}}\left(\frac{s}{m_0/d}\right)^r e^{\frac{2\pi i(-24t-r)s}{m/d}}e^{\frac{2\pi i\tau'(s,d)(24t_d+r)}{24m_C}}\sum_{n=0}^{\infty}p(m_Cn+t_d)e^{2\pi i\tau'(s,d)n}\\
=&\sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)}}\left(\frac{s}{m_0/d}\right)^r e^{\frac{2\pi i(-24t-r)s}{m/d}}e^{\frac{2\pi i\left\{\frac{d\tau+24x(-x\iota_{s,d}+dD)}{m_0/d}+d^2y(BA'+24sdD^2)\right\}(24t_d+r)}{24m_C}}\\
&\times\sum_{n=0}^{\infty}p(m_Cn+t_d)e^{2\pi i\left\{\frac{d\tau+24x(-x\iota_{s,d}+dD)}{m_0/d}+d^2y(BA'+24sdD^2)\right\}n}
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)}} \left(\frac{s}{m_0/d}\right)^r e^{\frac{2\pi i(-24t-r)s}{m/d}} e^{\frac{2\pi i\left\{\frac{d\tau+24x(-x\iota_{s,d}+dD)}{m_0/d}+d^2y(BA'+24sdD^2)\right\}(24t_d+r)}{24m_C}} \\
&\quad\times \sum_{n=0}^{\infty} p(m_C n+t_d) e^{2\pi i\frac{d\tau+24x(-x\iota_{s,d}+dD)}{m_0/d}n} \\
&= \sum_{n=0}^{\infty} p(m_C n+t_d) e^{\frac{2\pi i n(\tau+24xD)d^2}{m_0}} e^{\frac{2\pi i\tau d^2(\tau+24xD+m_0yBA')(24t_d+r)}{24m}} \\
&\quad\times \sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)}} \left(\frac{s}{m_0/d}\right)^r e^{\frac{2\pi i(-24t-r)s}{m/d}} e^{\frac{2\pi i\left\{\frac{-24x^2\iota_{s,d}}{m_0/d}+24d^3yD^2s\right\}(24t_d+r)}{24m_C}} e^{-2\pi i\frac{24x^2\iota_{s,d}}{m_0/d}n} \\
&= e^{\frac{2\pi i d^2(\tau+24xD+m_0yBA')(24t_d+r)}{24m}} \sum_{n=0}^{\infty} p(m_C n+t_d) e^{\frac{2\pi i n(\tau+24xD)d^2}{m_0}} \\
&\quad\times \sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)}} \left(\frac{s}{m_0/d}\right)^r e^{-\frac{2\pi i}{m/d}\{x^2\iota_{s,d}((24t_d+r)+24nm_C)+s(24t+r-(24t_d+r)d^2D^2ym_0)\}} \\
&= e^{\frac{2\pi i d^2(\tau+24xD+m_0yBA')(24t_d+r)}{24m}} \sum_{n=0}^{\infty} p(m_C n+t_d) e^{\frac{2\pi i n(\tau+24xD)d^2}{m_0}} \\
&\quad\times \underbrace{\sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)}} \left(\frac{s}{m_0/d}\right)^r e^{-\frac{2\pi i x}{m/d}\{x\iota_{s,d}((24t_d+r)+24nm_C)+24Cs(24t+r)\}}}_{=T(n,d)},
\end{aligned}
$$

by first substituting $d^2D^2ym_0(24t_d+r) \equiv ym_0(24t+r) \pmod{m}$ which follows from (23) and $AD-BC=1$ and next substituting $1-ym_0=24xC$ because of *(i)*. Next we exploit the identity,

$$
\begin{aligned}
T(n,d) &= \sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)=1}} \left(\frac{s}{m_0/d}\right)^r e^{-\frac{2\pi i x}{m/d}\{x\iota_{s,d}((24t_d+r)+24nm_C)+24Cs(24t+r)\}} \\
&= \sum_{\substack{0\le s<m_0/d\\ \gcd(s,m_0/d)=1}} \left(\frac{24Cs}{m_0/d}\right)^r e^{-\frac{2\pi i x/m_C}{m_0/d}\{\iota_{s,d}((24t_d+r)+24nm_C)+s(24t+r)\}},
\end{aligned}
$$

because $s \mapsto xs$ is a bijection modulo m_0/d together with $24xC \equiv 1 \pmod{m_0/d}$.

Finally substituting in (40) we obtain (22). □

Lemma 5.6. *Let Q be a positive integer, $v \in \mathbb{Z}$ with $v \neq 0$ and $p \geq 5$ a prime. Let b be maximal such that $p^b|v$. Then for any integer $r \geq b+1$ and $l \in \mathbb{Z}$ there exists $a_{r,l} \in \mathbb{Z}$ with $\gcd(a_{r,l}, 6pQ) = 1$ such that*

$$a_{r,l}^2 v \equiv v + 24lp^{b+1}Q \pmod{p^rQ}.$$

Proof. Fix $l \in \mathbb{Z}$. Then the statement holds for $r = b+1$ with $a_{r,l} = 1$. Next assume that the statement is true for $r = R \geq b+1$ and prove it for $r = R+1$.

That is there exists $a_{R,l}$ such that

$$a_{R,l}^2 v \equiv v + 24lp^{b+1}Q \pmod{p^R Q}. \tag{42}$$

We make the "ansatz" $a_{R+1,l} := a_{R,l} + 24p^{R-b}Qx$. Because of (42) it makes sense to define s to be the integer satisfying

$$a_{R,l}^2 v - v - 24lp^{b+1}Q = sp^R Q. \tag{43}$$

Then we need to show that there exists x such that

$$(a_{R,l} + 24p^{R-b}Qx)^2 v \equiv v + 24lp^{b+1}Q.$$

We have

$$\begin{aligned}&(a_{R,l}^2 + 48a_{R,l}xQp^{R-b} + 24^2p^{2R-2b}Q^2x^2)v - v - 24lp^{b+1}Q\\ \equiv&(a_{R,l}^2 + 48a_{R,l}xQp^{R-b})v - v - 24lp^{b+1}Q\end{aligned}$$

because of $24^2x^2Q^2p^{2R-2b}v \equiv 0 \pmod{p^{R+1}Q}$ becuase of $v \equiv 0 \pmod{p^b}$ and $R \geq b+1$

$$\equiv 48a_{R,l}p^{R-b}Qxv + sp^RQ \equiv 0 \pmod{p^{R+1}Q},$$

because of (43).

This implies

$$48a_{R,l}xvp^{-b} + s \equiv 0 \pmod{p},$$

which is solvable for x because of $\gcd(48a_{R,l}Qvp^{-b}, p) = 1$. Hence the proof is finished by the induction principle. □

References

[1] S. Ahlgren and K. Ono. Congruence Properties for the Partition Function. *Proceedings of the National Academy of Science*, 98(23):12882–12884, 2001.

[2] S. Ahlgren and K. Ono. Congruences and Conjectures for the Partition Function. In B. C. Berndt and K. Ono, editors, *Proceedings of the Conference on q-series with Applications to Combinatorics, Number Theory and Physics*, AMS Contemporary Mathematics 291, pages 1–10. AMS, 2001.

[3] P. Deligne and M. Rapoport. Les schémas de modules de courbes elliptiques. In P. Deligne and Willem Kuyk, editors, *Modular functions of one variable. II*, Lecture Notes in Mathematics 349, pages 143–316. Springer-Verlag Berlin, 1973.

[4] S. Lang. *Algebraic Number Theory*. Addison-Wesley Publishing Company, Inc., 1970.

[5] R. Lewis. The Components of Modular Forms. *J. London Math. Soc.*, 52:245–254, 1995.

[6] M. Newman. Construction and Application of a Class of Modular Functions 2. *Proceedings London Mathematical Society*, 3(9):373–387, 1959.

[7] S. Radu. An Algorithmic Approach to Ramanujan's Congruences. *Ramanujan Journal*, 20:215–251, 2009.

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