A PROOF OF SUBBARAO'S CONJECTURE

SILVIU RADU

Abstract. Let $p(n)$ denote the ordinary partition function. Subbarao conjectured that in every arithmetic progression $r \pmod t$ there are infinitely many integers $N \equiv r \pmod t$ for which $p(N)$ is even, and infinitely many integers $M \equiv r \pmod t$ for which $p(M)$ is odd. In the even case the conjecture was settled by Ken Ono. In this paper we prove the odd part of the conjecture which together with Ono's result implies the full conjecture. We also prove that for every arithmetic progression $r \pmod t$ there are infinitely many integers $N \equiv r \pmod t$ such that $p(N) \not\equiv 0 \pmod 3$, which settles an open problem posed by Scott Ahlgren and Ken Ono.

1. Introduction

Let $p(n)$ denote the number of partitions of the positive integer n. A well-known conjecture by Subbarao [19] asserts that every arithmetic progression contains infinitely many integers M for which $p(M)$ is odd, as well as infinitely many integers N for which $p(N)$ is even. Subbarao [19] proved that for the progression $1 \pmod 2$ the conjecture is true. The conjecture has been verified for other cases. Namely, it is known that $p(tn+r)$ is infinitely often odd and infinitely often even for $t = 1, 2, 3, 4, 5, 10, 12, 16$ and 40 thanks to the work of Garvan, Kolberg, Hirschhorn, Stanton and Subbarao (see [19], [6], [8], [9], [10] and [12]).

In [14] Ono makes the following breakthrough:

Theorem 1.1 (Ono)**.** *For any arithmetic progression $r \pmod t$, there are infinitely many integers $N \equiv r \pmod t$ for which $p(N)$ is even.*

This theorem settles half of the conjecture. The next theorem to be found in the same paper gives a very simple method to check whether $p(N)$ is infinitely often odd for a given arithmetic progression:

Theorem 1.2 (Ono)**.** *For any arithmetic progression $r \pmod t$, there are infinitely many integers $M \equiv r \pmod t$ for which $p(M)$ is odd, provided there is one such M. Furthermore, if there does exist an $M \equiv r \pmod t$ for which $p(M)$ is odd, then the smallest such M is less than $C_{r,t}$, where*

$$C_{r,t} := \frac{2^{23+j}.3^7t^6}{d^2} \prod_{p|6t} \left(1 - \frac{1}{p^2}\right) - 2^j,$$

S. Radu was supported by DK grant W1214-DK6 and by grant P2016-N18 of the Austrian Science Funds FWF.

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

Key words and phrases: Parity conjecture, partitions, modular forms.

with $d := \gcd(24r-1, t)$ *and* j *an integer satisfying* $2^j > \frac{t}{24}$.

This last theorem gives an explicit algorithm to prove the conjecture for any given progression. However the problem of finding infinitely many progressions for which the conjecture is true was solved by Getz [7]. He proves the conjecture for all progressions of the form $kl \pmod{l^n}$ where n is a positive integer, $l \geq 5$ is a prime and $k \in \{0, \ldots, l^{n-1} - 1\}$. Later Boylan and Ono [4] proved the conjecture for progressions of the form $r \pmod{2^n}$ with $r, n \in \mathbb{N}$.

The purpose of this paper is to prove the following theorem which together with Theorem 1.1 and 1.2 implies the truth of the conjecture of Subbarao.

Theorem 1.3. *Let* $\nu \in \{2, 3\}$ *and* A, B *integers such that* $A > B \geq 0$. *Then there exists a nonnegative integer* n_0 *such that*

$$p(An_0 + B) \not\equiv 0 \pmod{\nu}.$$

Proof. Let $\nu \in \{2, 3\}$. We assume the negation of Theorem 1.3. Namely, assume that there exist integers A, B with $A > B \geq 0$ such that

$$p(An + B) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}. \tag{1}$$

We first write A in the form $2^s 3^t Q$ where $s, t, Q \in \mathbb{N}$ and $\gcd(Q, 6) = 1$. Next we find because of Lemma 5.5 that (1) implies

$$p(Qn + \overline{B}) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}, \tag{2}$$

where $\overline{B}$ is the minimal nonnegative integer such that $B \equiv \overline{B} \pmod{Q}$. The congruence (2) is a contradiction to Lemma 5.6 because of $\gcd(Q, 6) = 1$. □

We obtain the following corollary:

Corollary 1.4. *Let* $\nu \in \{2, 3\}$ *and* A, B *integers such that* $A > B \geq 0$. *Then there are infinitely many integers* n *for which*

$$p(An + B) \not\equiv 0 \pmod{\nu}.$$

Proof. Assume that the statement is false. Then for some $\nu_0 \in \{2, 3\}$ there exist integers A_0, B_0 and $n_0 \geq 1$ with $A_0 > B_0 \geq 0$ such that

$$p(A_0 n + B_0) \equiv 0 \pmod{\nu_0}, \quad n \in \mathbb{N}, \quad n \geq n_0.$$

This implies that

$$p(A_1 n + B_1) \equiv 0 \pmod{\nu_0}, \quad n \in \mathbb{N},$$

where $A_1 := 2A_0 n_0$ and $B_1 := A_0 n_0 + B_0$. In particular $A_1 > B_1 \geq 0$. This contradicts Theorem 1.3. □

Remark 1.5. For $\nu = 3$, Corollary 1.4 implies Conjecture 5.2 of [3]. It should be mentioned that Ono (in unpublished work which is widely circulated), proved several years ago that $p(n) \not\equiv 0 \pmod 3$ for infinitely many n using Borcherds products.

Using the results of Scott Ahlgren [1] combined with Theorem 1.3 we obtain immediately:

Corollary 1.6. *The number of $n \leq X$ such that $n \equiv r \pmod{t}$ and $p(n)$ is odd is $\gg \sqrt{X}/\log X$.*

For more results of this type see Ken Ono's book [16].

Remark 1.7. Theorem 1.3 implies that there exist no integers $A > B \geq 0$ such that

$$p(An + B) \equiv 0 \pmod{\nu},$$

for $\nu \in \{2, 3\}$. This is certainly not true for primes different from $2, 3$. Namely, Ken Ono [15] proved that for every prime $M \geq 5$ there exist infinitely many non-nested arithmetic progressions $\{An+B\}$ such that $p(An+B) \equiv 0 \pmod{M}$. Scott Ahlgen [2] extended this result for arbitrary integers M coprime to 6. In the course of proving these results one needs to apply Atkin's U_m-operator that maps $\sum_{n=-\infty}^{\infty} a(n)q^n$ to $\sum_{n=-\infty}^{\infty} a(mn)q^n$ to the partition generating function $P(q) := \sum_{n=0}^{\infty} p(n)q^{24n-1}$ to obtain an element congruent to a nonzero modular form. Modular forms are well understood objects and the authors exploit this. However when $m = 2, 3$ we see that $U_m(P(q)) = 0$. This is the reason why these results could not be extended for the primes $2, 3$.

We are not sure how to contrast our result with $p(n)$ mod M when M is coprime to 6. As we have seen in this case there are arithmetic progressions $\{An + B\}$ within which the partition function $p(n)$ vanishes and so a new strategy is required. However a result in this direction is the following.

Theorem 1.8. *Let ν be a prime, $Q > 1$ a positive integer such that $\gcd(Q, 6\nu) = 1$ and $t \in \{0, \ldots, Q-1\}$. Then there are infinitely many n such that $p(Qn + t) \not\equiv 0 \pmod{\nu}$.*

Proof. Assume that there are only finitely many n such that $p(Qn+t) \not\equiv 0 \pmod{\nu}$. Then there exists a n_0 such that $p(Qn + t) \equiv 0 \pmod{\nu}$ for all $n \geq n_0$. Let l be such that $Q^l > Qn_0 + t$. Set $Q' = Q^l$ and $t' := Qn_0 + t$. Then $p(Q'n + t') \equiv 0 \pmod{\nu}$ for all $n \in \mathbb{N}$. This contradicts Lemma 5.6. □

2. Modular Forms

For an analytic function f on the upper half complex plane $\mathbb{H}$, k an integer and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we define

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

Then for analytic functions f, g on $\mathbb{H}$, integers i, j and $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ we have

$$(f|_i\gamma)(g|_j\gamma) = (fg|_{i+j}\gamma). \tag{3}$$

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 a modular form of weight k for Γ is an analytic function on $\mathbb{H}$ satisfying:

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

We denote by $M_k(\Gamma)$ the set of all modular forms of weight k for Γ. The set of modular forms for Γ is then defined to be the set $\cup_{k=0}^{\infty} M_k(\Gamma)$. If f is a modular form for Γ, then we define $f|\gamma := f|_k\gamma$ where k is such that $f \in M_k(\Gamma)$.

For a positive integer N 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, $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N)$.

The Dedekind eta function η plays an important role throughout the paper. Furthermore, by [18, Th 6. p. 95] we have

$$\eta^{24} = q\prod_{n=1}^{\infty}(1-q^n)^{24} \in M_{12}(\mathrm{SL}_2(\mathbb{Z})) \subseteq M_{12}(\Gamma_0(N)). \tag{4}$$

3. Outline of the Article

The proof of Subbarao's conjecture follows from Ono's Theorem 1.1 and 1.2 together with Theorem 1.3. Theorem 1.1 solves the even case of the problem while Theorem 1.2 solves the odd case provided that we can find a first odd which is provided by Theorem 1.3. We continue by providing an outline of the proof of Theorem 1.3 where we show the role of each result in this paper.

For $\nu \in \{2, 3\}$ assume there exist integers $A > B \geq 0$ such that

$$p(An + B) \equiv 0 \pmod{\nu}. \tag{5}$$

We are next considering the modular forms

$$G_{m,t}^{(s)} := \eta^{24k}\left(q^{\frac{24t-1}{24m}}\sum_{n=0}^{\infty} p(mn+t)q^n\right)^{24m}$$

where $s, m, t \in \mathbb{Z}$ and $m > t \geq 0$.

By using the work of Richard Lewis [13, Th. 1] we find that there exist positive integers N and k such that $G_{A,B}^{(k)}$ becomes a modular form for the group $\Gamma_1(N)$. Again from [13, Th. 1] one observes that for $\gamma \in \Gamma_0(N)$

$$G_{A,B}^{(k)}|\gamma = G_{A,B_\gamma}^{(k)}. \tag{6}$$

for some integer B_γ with $A > B_\gamma \geq 0$. From Corollary 5.3 below which follows immediately from Theorems 5.1 and 5.2 of Deligne and Rapoport [5] we find that if f is a modular form for $\Gamma_1(N)$ with coefficients in the q-expansion divisible by ν then

also the coefficients in the q-expansion of $f|\gamma$ are divisible by ν for all $\gamma \in \Gamma_0(N)$. From this together with (6) we observe immediately that if the coefficients in the q-expansion of $G^{(k)}_{A,B}$ are divisible by ν then so are the coefficients in the q-expansion of $G^{(k)}_{A,B_\gamma}$ for $\gamma \in \Gamma_0(N)$ which is exactly Theorem 5.4. In Theorem 4.2 we prove that if $A = 2^s 3^t Q$ for some $s, t, Q \in \mathbb{N}$ with $\gcd(Q, 6) = 1$, then $\overline{B} + lQ \in \{B_\gamma : \gamma \in \Gamma_0(N)\}$ for all $l \in \{0, \cdots, 2^s 3^t - 1\}$ where $\overline{B}$ is the minimal nonnegative integer such that $B \equiv \overline{B} \pmod{Q}$. This implies that the coefficients in the q-expansion of $G^{(k)}_{A,\overline{B}+lQ}$ are divisible by ν. This is equivalent to

$$p(An + \overline{B} + lQ) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}, \quad l \in \{0, \cdots, 2^s 3^t - 1\},$$

which is equivalent to

$$p(Qn + \overline{B}) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}. \tag{7}$$

That the congruence (5) implies the congruence (7) is the content of Lemma 5.5 below. To prove Lemma 5.5 we need Theorem 4.2 and Theorem 5.4 mentioned above.

For the second part of the proof we use the crucial fact that $\gcd(Q, 6) = 1$ together with [13, Th. 1] to prove that there exists an integer j such that $G^{(j)}_{Q,\overline{B}}$ is a modular form for the group $\Gamma_1(Q)$. Next we apply the transformation $\gamma_0 = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ to $G^{(l)}_{Q,\overline{B}}$. By using Lemma 4.7 below we find that the coefficients in the q-expansion of $G^{(l)}_{Q,\overline{B}}|\gamma_0$ are not all divisible by ν. However because of Theorem 5.1 again by Deligne and Rapaport we observe that if the coefficients in the q-expansion of a modular form f for $\Gamma_1(Q)$ are divisible by a prime not dividing Q, then so are the coefficients in the q-expansion of $f|\gamma$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. This fails for the prime ν, $\gamma = \gamma_0$ and $f = G^{(l)}_{Q,\overline{B}}$. Thus we obtained a contradiction so that (7) can not hold true which implies that (5) is false. This is the content of Lemma 5.6 which says that for every prime ν and integers Q, t with $Q > t \geq 0$ and $\gcd(Q, 6\nu) = 1$ there exists $n_0 \in \mathbb{N}$ such that $\nu \nmid p(Qn_0 + t)$. As we have seen Lemma 5.6 is proven using Lemma 4.7 and Theorem 5.1.

Summarizing, the crucial results in the paper needed to prove Theorem 1.3 are the Lemmas 5.5 and 5.6 which are based on work of Richard Lewis [13], Pierre Deligne and Michael Rapaport [5].

It should be mentioned that the results in the work of Richard Lewis [13] needed in this paper are also contained in the author's paper [17]. In this paper we will also use some terminology in [17].

4. Some Technical Lemmas

In the previous section we observed that the modular form $G^{(s)}_{m,t}$ for the group $\Gamma_1(N)$ turns into the modular form $G^{(s)}_{m,t_\gamma}$ after application of a transformation

$\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$. It turns out that t_γ can be described explicitly as seen from [13, p. 248, (2.5)]. Namely,

$$t_\gamma \equiv ta^2 + \frac{1-a_*^2}{24} \pmod{m}$$

and $0 \leq t_\gamma < m$. Here a_* is any integer coprime to 6 such that $a_* \equiv a \pmod{m}$. Consequently, $1 - a_*^2$ is divisible by 24 so that the above formula makes sense. The set $P_m(t) := \{t_\gamma : \gamma \in \Gamma_0(N)\}$ is crucial for our further investigations and we will derive some of its properties.

We also observed in the second part of Section 3 that $G_{m,t}^{(s)}$ need to be evaluated also when applying the transformation $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. To this end we will use Lemma 4.7 which will be proven in this section.

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

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

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

Theorem 4.2. *Let m be a positive integer, $t \in \{0, \dots, m-1\}$ and let s, ν, Q be nonnegative integers defined by $m = 2^s 3^\nu Q$ and $\gcd(Q, 6) = 1$. Let $\bar{t}$ be the minimal nonnegative integer satisfying $\bar{t} \equiv t \pmod{Q}$. Then for all $l \in \{0, \dots, 2^s 3^\nu - 1\}$ we have $\bar{t} + lQ \in P_m(t)$.*

In order to prove Theorem 4.2 we need the following two lemmas.

Lemma 4.3. *Let $\lambda \in \mathbb{Z}$, $\nu \in \mathbb{N}$, Q a positive integer and $t \in \{0, \dots, Q-1\}$. Let $a_\nu \in \mathbb{Z}$ with $\gcd(a_\nu, 6Q) = 1$ be such that*

$$\frac{1-a_\nu^2}{24} \equiv t(1-a_\nu^2) + \lambda \pmod{3^\nu Q}. \tag{8}$$

Then there exists an $a_{\nu+1} \in \mathbb{Z}$ with $\gcd(a_{\nu+1}, 6Q)$ such that

$$\frac{1-a_{\nu+1}^2}{24} \equiv t(1-a_{\nu+1}^2) + \lambda \pmod{3^{\nu+1} Q}. \tag{9}$$

Proof. From (8) we see that there exists an unique integer α such that

$$\frac{1-a_\nu^2}{24} - t(1-a_\nu^2) - \lambda = \alpha 3^\nu Q. \tag{10}$$

Define $a_{\nu+1} := a_\nu + \alpha a_\nu 2^4 3^{\nu+1} Q$. Then

$$\begin{aligned} 1 - a_{\nu+1}^2 &\equiv 1 - a_\nu^2 - \alpha a_\nu^2 2^5 3^{\nu+1} Q - \alpha^2 a_\nu^2 2^8 3^{2\nu+2} Q^2 \\ &\equiv 1 - a_\nu^2 - \alpha a_\nu^2 2^5 3^{\nu+1} Q \pmod{24 \cdot 3^{\nu+1} Q}, \end{aligned} \tag{11}$$

and consequently

$$\frac{1-a_{\nu+1}^2}{24} \equiv \frac{1-a_\nu^2}{24} - \alpha a_\nu^2 2^2 3^\nu Q \pmod{3^{\nu+1} Q}. \tag{12}$$

By (8)-(12) we have

$$\begin{aligned}
&\frac{1-a_{\nu+1}^2}{24} - t(1-a_{\nu+1}^2) - \lambda \\
\equiv &\frac{1-a_\nu^2}{24} - \alpha a_\nu^2 2^2 3^\nu Q - t(1-a_\nu^2) + \alpha t a_\nu^2 2^5 3^{\nu+1} Q - \lambda && \text{by (11) and (12)} \\
\equiv &\alpha 3^\nu Q - \alpha a_\nu^2 2^2 3^\nu Q + \alpha t a_\nu^2 2^5 3^{\nu+1} Q && \text{by (10)} \\
\equiv &\alpha 3^\nu Q(1-a_\nu^2 2^2) \\
\equiv &0 \pmod{3^{\nu+1}Q} && \text{because of } 3|(1-a_\nu^2 2^2).
\end{aligned}$$

□

Lemma 4.4. *Let $\lambda \in \mathbb{Z}$, $s, \nu \in \mathbb{N}$, Q a positive integer and $t \in \{0, \dots, Q-1\}$. Let $b_s \in \mathbb{Z}$ with $\gcd(b_s, 6Q) = 1$ be such that*

$$\frac{1-b_s^2}{24} \equiv t(1-b_s^2) + \lambda \pmod{2^s 3^\nu Q}. \tag{13}$$

Then there exists an $b_{s+1} \in \mathbb{Z}$ with $\gcd(b_{s+1}, 6Q) = 1$ such that

$$\frac{1-b_{s+1}^2}{24} \equiv t(1-b_{s+1}^2) + \lambda \pmod{2^{s+1} 3^\nu Q}. \tag{14}$$

Proof. From (13) we see that there exists an unique integer α such that

$$\frac{1-b_s^2}{24} - t(1-b_s^2) - \lambda = \alpha 2^s 3^\nu Q. \tag{15}$$

Define $b_{s+1} := b_s + \alpha 2^{s+2} 3^{\nu+1} Q$. Then

$$\begin{aligned}
1 - b_{s+1}^2 &\equiv 1 - b_s^2 - \alpha b_s 2^{s+3} 3^{\nu+1} Q - \alpha^2 2^{2s+4} 3^{2\nu+2} Q^2 \\
&\equiv 1 - b_s^2 - \alpha b_s 2^{s+3} 3^{\nu+1} Q \pmod{24 \cdot 2^{s+1} 3^\nu Q},
\end{aligned} \tag{16}$$

and consequently

$$\frac{1-b_{s+1}^2}{24} \equiv \frac{1-b_s^2}{24} - \alpha b_s 2^s 3^\nu Q \pmod{2^{s+1} 3^\nu Q}. \tag{17}$$

By (13)-(17) we have

$$\begin{aligned}
&\frac{1-b_{s+1}^2}{24} - t(1-b_{s+1}^2) - \lambda \\
\equiv &\frac{1-b_s^2}{24} - \alpha b_s 2^s 3^\nu Q - t(1-b_s^2) + \alpha t b_s 2^{s+3} 3^{\nu+1} Q - \lambda && \text{by (16) and (17)} \\
\equiv &\alpha 2^s 3^\nu Q - \alpha b_s 2^s 3^\nu Q + \alpha t b_s 2^{s+3} 3^{\nu+1} Q && \text{by (15)} \\
\equiv &\alpha 2^s 3^\nu Q(1-b_s) \\
\equiv &0 \pmod{2^{s+1} 3^\nu Q} && \text{because of } 2|(1-b_s).
\end{aligned}$$

□

Proof of Theorem 4.2: For $\lambda := lQ$ and $a_0 := 1$ we have

$$\frac{1-a_0^2}{24} \equiv t(1-a_0^2) + \lambda \pmod{Q}.$$

Then by applying Lemma 4.3 inductively we find that there exists $a_\nu \in \mathbb{Z}$ with $\gcd(a_\nu, 6Q) = 1$ such that

$$\frac{1-a_\nu^2}{24} \equiv t(1-a_\nu^2) + \lambda \pmod{3^\nu Q}.$$

By setting $b_0 = a_\nu$ and by applying Lemma 4.4 inductively we find that there exists $b_s \in \mathbb{Z}$ with $\gcd(b_s, 6Q) = 1$ such that

$$\frac{1-b_s^2}{24} \equiv t(1-b_s^2) + \lambda \pmod{2^s 3^\nu Q}. \tag{18}$$

Next we note that (18) is equivalent to

$$tb_s^2 + \frac{1-b_s^2}{24} \equiv t + lQ \pmod{2^s 3^\nu Q}. \tag{19}$$

For $x \in \mathbb{Z}$ we denote by $[x]$ the minimal nonnegative integer x such that $x \equiv [x] \pmod{2^s 3^\nu Q}$. Then obviously

$$\{[t+lQ] | l \in \mathbb{Z}\} = \{[\overline{t}+lQ] | l \in \mathbb{Z}\} = \{\overline{t}+lQ | 0 \le l \le 2^s 3^\nu - 1\},$$

which together with Definition 4.1 completes the proof. □

Definition 4.5. *For c, d integers with $\gcd(c,d) = 1$ and d odd, we define*

$$\left(\frac{c}{d}\right)_* := \begin{cases} \left(\frac{c}{|d|}\right), & \text{if } c \neq 0, \\ 1, & \text{otherwise.} \end{cases}$$

Definition 4.6. *Let r, m, t be integers such that $m \ge 1$ and $t \in \{0, \dots, m-1\}$. We define*

$$\sum_{m=0}^{\infty} p_r(m) q^m := \prod_{n=1}^{\infty} (1-q^n)^r$$

and

$$g_{m,t,r}(\tau) := q^{\frac{24t+r}{24m}} \sum_{n=0}^{\infty} p_r(mn+t) q^n(\tau), \quad \tau \in \mathbb{H},$$

where we recall that $q(\tau) = e^{2\pi i \tau}$.

Lemma 4.7. *Let $m, r \in \mathbb{Z}$ and $t \in \{0, \dots, m-1\}$ with $m > 0$ and $\gcd(m, 6) = 1$. For $\lambda, d \in \mathbb{Z}$ with $d|m$ and $\gcd(d, \lambda) = 1$ let $x_{\lambda,d}$ be any integer satisfying*

$$24^2 \lambda x_{\lambda,d} \equiv 1 \pmod{m/d}.$$

Then

$$\tau^{-r/2} g_{m,t,r}(-1/\tau) = \frac{1}{m} \sum_{d|m} d^{r/2} e^{-\frac{\pi i r m}{4d}} e^{\frac{\pi i r d^2 \tau}{12m}} \sum_{n=0}^{\infty} p_r(n) e^{\frac{2\pi i n d^2 \tau}{m}} A_r(m,d,t,n), \tag{20}$$

where

$$A_r(m,d,t,n) := \sum_{\substack{0 \le \lambda \le m/d-1 \\ \gcd(\lambda, m/d) = 1}} \left(\frac{24\lambda}{m/d}\right)_*^r e^{-\frac{2\pi i}{m/d}\{(24t+r)\lambda + (24n+r)x_{\lambda,d})\}}.$$

Proof. By [17, Lemma 1.12] together with $\gcd(m,6)$ we have

$$g_{m,t,r}(\tau)=\frac{1}{m}\sum_{\lambda=0}^{m-1}e^{-\frac{2\pi i\lambda(24t+r)}{m}}\eta^r\left(\frac{\tau+24\lambda}{m}\right),$$

which is equivalent to

$$g_{m,t,r}(\tau)=\frac{1}{m}\sum_{d|m}\sum_{\substack{0\le\lambda\le m/d-1\\ \gcd(\lambda,m/d)=1}}e^{-\frac{2\pi i\lambda d(24t+r)}{m}}\eta^r\left(\frac{\tau+24\lambda d}{m}\right),$$

which after applying $\tau\mapsto -1/\tau$ turns into

$$g_{m,t,r}(-1/\tau)=\frac{1}{m}\sum_{d|m}\sum_{\substack{0\le\lambda\le m/d-1\\ \gcd(\lambda,m/d)=1}}e^{-\frac{2\pi i\lambda d(24t+r)}{m}}\eta^r\left(\frac{24\lambda d\tau-1}{m\tau}\right). \tag{21}$$

Next we see that for any divisor d of m and integer λ with $\gcd(\lambda,m/d)=1$ we have

$$\frac{24\lambda d\tau-1}{m}=\frac{24\lambda\frac{d\tau-24x_{\lambda,d}}{m/d}-y_{\lambda,d}}{(m/d)\frac{d\tau-24x_{\lambda,d}}{m/d}+24x_{\lambda,d}}, \tag{22}$$

where the integer $y_{\lambda,d}$ satisfies

$$24^2\lambda x_{\lambda,d}+\frac{m}{d}y_{\lambda,d}=1.$$

In particular, we obtain from [11, p. 51]

$$\eta\left(\frac{24\lambda\frac{d\tau-24x_{\lambda,d}}{m/d}-y_{\lambda,d}}{(m/d)\frac{d\tau-24x_{\lambda,d}}{m/d}+24x_{\lambda,d}}\right)=(d\tau)^{1/2}\left(\frac{24x_{\lambda,d}}{m/d}\right)_*e^{-\frac{\pi im}{4d}}\eta\left(\frac{d\tau-24x_{\lambda,d}}{m/d}\right),$$

which together with (21) and (22) implies that $g_{m,t,r}(-1/\tau)$ is given by

$$\frac{1}{m}\sum_{d|m}(d\tau)^{r/2}\sum_{\substack{0\le\lambda\le m/d-1\\ \gcd(\lambda,m/d)=1}}e^{-\frac{2\pi i\lambda d(24t+r)}{m}}\left(\frac{24x_{\lambda,d}}{m/d}\right)_*^r e^{-\frac{\pi irm}{4d}}\eta^r\left(\frac{d\tau-24x_{\lambda,d}}{m/d}\right). \tag{23}$$

Next recall that

$$\eta^r(\tau)=e^{\frac{\pi i\tau r}{12}}\sum_{n=0}^{\infty}p_r(n)e^{2\pi in\tau},$$

which used on (23) gives

$$\begin{aligned}g_{m,t,r}(-1/\tau)=&\frac{1}{m}\sum_{d|m}(d\tau)^{r/2}\sum_{\substack{0\le\lambda\le m/d-1\\ \gcd(\lambda,m/d)=1}}e^{-\frac{2\pi i\lambda d(24t+r)}{m}}\left(\frac{24x_{\lambda,d}}{m/d}\right)_*^r e^{-\frac{\pi irm}{4d}}\\ &\times e^{\frac{\pi ir\frac{d\tau-24x_{\lambda,d}}{m/d}}{12}}\sum_{n=0}^{\infty}p_r(n)e^{2\pi in\frac{d\tau-24x_{\lambda,d}}{m/d}}.\end{aligned}$$

This last formula translates into (20) after changing the summation order and using $\left(\frac{24x_\lambda}{m/d}\right)\left(\frac{24\lambda}{m/d}\right)=\left(\frac{1}{m/d}\right)=1$ because of $24^2\lambda x_{\lambda,d}\equiv 1 \pmod{m/d}$. □

5. The Ingredients in the Proof of our Main Result

The proof of the results in this section is standing on the following two key theorems and on the results of the previous section.

Theorem 5.1. [5, VII, Cor. 3.13] *Let k, N be positive integers and $f \in M_k(\Gamma(N))$. Assume that the coefficients in the q-expansion of f are in $\mathbb{Z}[1/N, e^{2\pi i/N}]$. Then for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ the coefficients in the q-expansion of $f|_k\gamma$ are in $\mathbb{Z}[1/N, e^{2\pi i/N}]$.*

Theorem 5.2. [5, 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 $f \equiv 0 \pmod{\pi^\nu}$. Then $f|_k\gamma \equiv 0 \pmod{\pi^\nu}$*[1].

Corollary 5.3. *Let k, N be positive integers and $f \in M_k(\Gamma(N))$. If the coefficients in the q-expansion of f are in $\mathbb{Z}[e^{2\pi i/N}]$, then for all $\gamma \in \Gamma_0(N)$ the coefficients in the q-expansion of $f|_k\gamma$ are in $\mathbb{Z}[e^{2\pi i/N}]$.*

Proof. Let p be a prime dividing N. Since the coefficients in q-expansion of f have no denominators we obtain by Theorem 5.2 that the coefficients in the q-expansion of $f|_k\gamma$ cannot have any denominators divisible by p. Now let p' be a prime not dividing N. Then by Theorem 5.1 no denominator in the q-expansion of $f|_k\gamma$ is divisible by p'. This finishes the proof. □

Let m be a positive integer and $t \in \{0, \ldots, m-1\}$. Then by [13, Th. 1] or [17, Th. 2.14] there exist positive integers k, N such that

$$G_{m,t}^{(k)} := \eta^{24k}\left(q^{\frac{24t-1}{m}} \sum_{n=0}^{\infty} p(mn+t)q^n\right)^{24m} \tag{24}$$

is an element of $M_{12(k-m)}(\Gamma_1(N))$. Again by [13, Th. 1] or [17, Th. 2.14] for all $\gamma \in \Gamma_0(N)$ there exists $t_\gamma \in \{0, \ldots, m-1\}$ such that

$$G_{m,t}^{(k)}|_w\gamma = G_{m,t_\gamma}^{(k)}, \quad w := 12(k-m). \tag{25}$$

We recall that $P_m(t)$ the set of all such t_γ that can arise in (25) while varying $\gamma \in \Gamma_0(N)$.

Because of $\mathbb{Q} \cap \mathbb{Z}[e^{2\pi i/N}] = \mathbb{Z}$ we obtain by Corollary 5.3 together with (24) and (25) that if for some integer l we have that $\frac{p(mn+t)}{l}$ is an integer for all nonnegative integers n, then for all t' in $P(t)$ also $\frac{p(mn+t')}{l}$ is an integer for all nonnegative integers n. In other words we have proven:

[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 [5, 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 [5, 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 there exists $M \in \mathbb{Z}$ with $M \notin \pi$ such that all the coefficients in the q-expansion of $Mf|_k\gamma$ lie in the ideal π^ν.

Theorem 5.4. *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

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

We note that Theorem 1.3 claims that there exist no congruences of the form

$$p(An+B) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}, \tag{26}$$

if $\nu \in \{2, 3\}$. We prove this theorem by first showing that if a congruence of the form (26) exists then there exists a congruence of the form (26) where the modulus A satisfies $\gcd(A, 6) = 1$. This latter congruence is given explicitly in the next lemma.

Lemma 5.5. *Let $a, b, Q, \nu \in \mathbb{N}$ and $t \in \{0, \dots, 2^a 3^b Q - 1\}$ with $\nu, Q > 0$ and $\gcd(Q, 6) = 1$. Assume that*

$$p(2^a 3^b Qn + t) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}. \tag{27}$$

Then

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

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

Proof. By Theorem 4.2 we have $\overline{t} + lQ \in P_m(t)$ for all $l \in \{0, \dots, 2^a 3^b - 1\}$. Then because of (27), we have by Theorem 5.4 that

$$p(2^a 3^b Qn + \overline{t} + lQ) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}, \tag{28}$$

for every $l \in \{0, \dots, 2^a 3^b - 1\}$. Because of (28) and the equality

$$\{2^a 3^b Qn + \overline{t} + lQ : l \in \{0, \dots, 2^a 3^b - 1\}, n \in \mathbb{N}\} = \{Qn + \overline{t} : n \in \mathbb{N}\},$$

we conclude that

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

□

As we have seen in Section 3, Theorem 1.3 is a corollary of Lemma 5.5 and the following lemma.

Lemma 5.6. *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 $n \in \mathbb{N}$ such that $\nu \nmid p(Qn+t)$.*

Proof. Assume that

$$p(Qn+t) \equiv 0 \pmod{\nu}, \quad n \in \mathbb{N}. \tag{29}$$

Then by [13, Th. 1] or [17, Lem. 2.10] there is a positive integer k such that

$$F := \frac{1}{\nu^{24Q}} G_{Q,t}^{(k)}$$

is an element of $M_{12(k-Q)}(\Gamma_1(Q))$. By (24) and Definition 4.6 we have

$$F = \frac{1}{\nu^{24Q}} \eta^{24k} g_{Q,t,-1}^{24Q}.$$

By Lemma 4.7, for each $d|Q$ there exists $a_d : \mathbb{N} \to \mathbb{C}$ such that for

$$f_d(q) := A_{-1}(Q, d, t, 0) + \sum_{n=1}^{\infty} a_d(n) q^n$$

with A_{-1} defined as in Lemma 4.7 we have

$$g_{Q,t,-1}^{24Q}|_{-12Q} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \left(\frac{1}{Q} \sum_{d|Q} e^{\frac{\pi i Q}{4d}} d^{-1/2} q^{-\frac{d^2}{24Q}} f_d(q^{d^2/Q}) \right)^{24Q}. \tag{30}$$

Furthermore, by Lemma 4.7 we have $A_{-1}(Q, Q, t, 0) = 1$ which implies together with (30) that the coefficient of q^{-Q^2} in the q-expansion of $g_{Q,t,-1}^{24Q}|_{-12Q} \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is given by

$$(e^{\frac{\pi i Q}{4d}} Q^{-3/2})^{24Q} = Q^{-36Q}.$$

Thus together with

$$\eta^{24k}|_{12k} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = q^k \prod_{n=1}^{\infty} (1 - q^n)^{24k}$$

because of (4) implies by (3) that the coefficient of q^{-Q^2+k} in the q-expansion of $F|_{12(k-Q)} \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ is equal to $\nu^{-24Q} Q^{-36Q}$. Because of (29) the coefficients in the q-expansion of F are integers and hence by Theorem 5.1,

$$\nu^{-24Q} Q^{-36Q} \in \mathbb{Z}[1/Q, e^{2\pi i/Q}]. \tag{31}$$

The relation (31) implies that there exists $l \in \mathbb{N}$ and integers $a_0, \ldots, a_{Q-1}$ such that

$$\nu^{-24Q} = Q^{-l} \sum_{\lambda=0}^{Q-1} a_\lambda e^{2\pi i \lambda/Q},$$

which imply that Q^l/ν^{24Q} is an algebraic integer and consequently an integer. This is clearly false because of $\gcd(Q, \nu) = 1$. This proves that (29) is impossible which concludes the proof. □

6. Acknowledgments

I want to thank Peter Paule who gave me important suggestions which significantly improved the quality of this paper. Furthermore, the results of this paper are natural consequences of the problems Peter Paule proposed during the time he guided me while working on the paper [17].

I would also like to thank the referee for helping to further improve the content of this paper.

References

[1] S. Ahlgren. Distribution of Parity of the Partition Function in Arithmetic Progressions. *Indagationes Mathematicae. New Series*, 10(2):173–181, 1999.

[2] S. Ahlgren. Distribution of the Partition Function Modulo Composite Integers M. *Mathematische Annalen*, 318(4):795–803, 2000.

[3] 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.

[4] M. Boylan and K. Ono. On the Parity of the Partition Function in Arithmetic Progressions, II. *Bulletin of the London Mathematical Society*, 33:558–564, 2001.

[5] 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.

[6] F. Garvan and D. Stanton. Sieved Partition Functions and q-Binomial Coefficients. *Mathematics of Computation*, 55(191):299–311, 1990.

[7] J. R. Getz. On Congruence Properties of the Partition Function. *International Journal of Mathematics and Mathematical Sciences*, 23:493–496, 2000.

[8] M. Hirschhorn. On the Residue mod 2 and mod 4 of $p(n)$. *Acta Arithmetica*, 38:105–109, 1980.

[9] M. Hirschhorn. On the Parity of $p(n)$ II. *Journal of Combinatorial Theory*, 62:128–138, 1993.

[10] M. Hirschhorn and M. V. Subbarao. On the Parity of $p(n)$. *Acta Arithmetica*, 50:355–356, 1988.

[11] M. I. Knopp. *Modular Functions in Analytic Number Theory*. American Mathematical Society, 1993.

[12] O. Kolberg. Note on the Parity of the Partition Function. *Mathematica Scandinavica*, 7:377–378, 1959.

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

[14] K. Ono. On the Parity of the Partition Function in Arithmetic Progressions. *Journal für die Reine und Angewandte Mathematik*, 472:1–15, 1996.

[15] K. Ono. Distribution of the Partition Function Modulo m. *Annals of Mathematics*, 151(1):293–307, 2000.

[16] 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.

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

[18] J. P. Serre. *A Course in Arithmetic*. Springer, 1973.

[19] M. V. Subbarao. Remarks on the Partition Function. *The American Mathematical Monthly*, 73(8):851–854, 1966.

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