

SUBBARAO'S CONJECTURE ON THE PARITY OF THE PARTITION FUNCTION

REBECCA HOBERG, GIANG TRAN, AND MCKENZIE WEST

ABSTRACT. Let $p(n)$ denote the ordinary partition function. In 1966, Subbarao [18] conjectured that in every arithmetic progression $r \pmod{t}$ there are infinitely many integers N (resp. M) $\equiv r \pmod{t}$ for which $p(N)$ is even (resp. odd). We prove Subbarao's conjecture for all moduli t of the form $m \cdot 2^s$ where $m \in \{1, 5, 7, 17\}$. To obtain this theorem we make use of recent results of Ono and Taguchi [14] on the nilpotent action of Hecke algebras on certain spaces of modular forms modulo 2.

1. INTRODUCTION AND STATEMENT OF RESULTS

A *partition* of a positive integer n is defined to be any non-increasing sequence of positive integers whose sum is n , and the number of partitions of n is denoted by $p(n)$. It is agreed that $p(0) = 1$. Euler observed that the generating function for $p(n)$ is

$$(1.1) \quad \sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1 - q^n}.$$

In the early 1900s, Ramanujan [16] proved the following surprising congruences of the partition function:

$$\begin{aligned} p(5n + 4) &\equiv 0 \pmod{5}, \\ p(7n + 5) &\equiv 0 \pmod{7}, \\ p(11n + 6) &\equiv 0 \pmod{11}. \end{aligned}$$

It turns out that these three congruences are the simplest examples of congruences in infinite families where the modulus is a power of 5, 7 or 11. Even with the help of computers, by the early 1960s no congruences were found apart from those proved or conjectured by Ramanujan. In fact, quite recently, Ahlgren and Boylan [2] proved that there are no other congruences of the form

$$p(ln + r) \equiv 0 \pmod{l},$$

where l is a prime and $0 \leq r < l$. However, in 2000, Ono [12] was able to prove that there are infinitely many congruences of the form $p(tn + r) \equiv 0 \pmod{l}$ where t and r are integers and l is coprime to 6. For example, he shows that

$$p(4063467631n + 30064597) \equiv 0 \pmod{31}.$$

Despite these results, very little is known about the partition function modulo 2 and 3. Parkin and Shanks [15] conjectured that $p(n)$ is odd for half of the positive integers n . Though it has not been proven, numerical evidence strongly supports this conjecture. If we define $\delta_r(X)$ to be the proportion of values of $p(n)$ which are congruent to $r \pmod{2}$, where $0 \leq n < X$, then we see

X	$\delta_0(X)$	$\delta_1(X)$
200,000	0.5012	0.4988
400,000	0.5000	0.5000
600,000	0.5000	0.5000
800,000	0.5006	0.4994
1,000,000	0.5004	0.4996

Along these lines, Ahlgren [1] and Serre [10] proved that the number of n up to X for which $p(n)$ is even (resp. odd) is at least $c \cdot \sqrt{X}/\log X$ for some constant c .

In the 1960s, motivated by these numerics and the paucity of Ramanujan congruences, Subbarao made the following conjecture [18].

Conjecture (Subbarao’s Conjecture). *If t and r are integers with $0 \leq r < t$, then there are infinitely many integers N (resp. M) for which*

$$\begin{aligned} p(tN + r) &\equiv 0 \pmod{2}, \\ p(tM + r) &\not\equiv 0 \pmod{2}. \end{aligned}$$

By the early ’90s, Subbarao’s conjecture had only been verified for arithmetic progressions with modulus

$$t \in \{1, 2, 3, 4, 5, 6, 8, 10, 12, 16, 20, 40\}$$

thanks to Garvan, Kolberg, Hirschhorn, Stanton and Subbarao (see [11] for references). Then in 1996, Ono [11] proved that in every arithmetic progression, there are infinitely many n such that $p(n)$ is even, thereby proving the “even case” of Subbarao’s Conjecture. He also proved that if an arithmetic progression has at least one odd value for $p(n)$, then it has infinitely many. With the help of a computer, he proved the “full” conjecture for all arithmetic progressions with modulus $t < 100,000$.

Using these ideas, Boylan and Ono [4] proved Subbarao’s conjecture for all moduli of the form $t = 2^s$ where $s \geq 1$, finally confirming the conjecture for an infinite number of moduli t . They used the nilpotency of the action of Hecke algebras modulo 2 on modular forms on $SL_2(\mathbb{Z})$.

In this paper, we generalize this argument and use the local nilpotency of Hecke algebras modulo 2 on an infinite family of modular forms to prove the following theorem.

Theorem 1.1. *Subbarao’s Conjecture is true for all arithmetic progressions modulo $t = m \cdot 2^s$, where $m = 1, 5, 7$ or 17 .*

The paper is structured as follows. In Section 2, we give preliminary facts on modular forms, the Hecke algebra, and nilpotency. In Section 3, we prove Theorem 1.1.

2. PRELIMINARIES ON MODULAR FORMS

We begin by reviewing the definition of a modular form (for more, see [13]). Let

$$\Gamma_0(M) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{M} \right\},$$

where $M \in \mathbb{N}$ and $SL_2(\mathbb{Z})$ is the group of 2×2 integer matrices of determinant 1.

If we have a holomorphic function $f(z)$ on the upper half of the complex plane \mathcal{H} , we define the *weight k slash operator* $|_k$, $k \in \mathbb{N}$, with respect to a group $SL_2(\mathbb{Z})$ by

$$(f|_k\gamma)(z) := (cz + d)^{-k} f(\gamma z),$$

where for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ we let

$$(2.1) \quad \gamma z := \frac{az + b}{cz + d}.$$

Using these definitions, we define what it means for a function to be a modular form.

Definition 2.1. *Suppose that $f(z)$ is a holomorphic function on \mathcal{H} , and $k \in \mathbb{Z}$. Then $f(z)$ is called a modular form of weight k and level M if the following conditions hold:*

(1) *We have*

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z)$$

for all $z \in \mathcal{H}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$.

(2) *If $\gamma_0 \in SL_2(\mathbb{Z})$, then $(f|_k\gamma_0)(z)$ has a Fourier expansion of the form*

$$(f|_k\gamma_0)(z) = \sum_{n \geq n_{\gamma_0}} a_{\gamma_0}(n) q_M^n,$$

where $q_M := e^{2\pi iz/M}$ and $a_{\gamma_0}(n_{\gamma_0}) \neq 0$.

For a congruence subgroup $\Gamma_0(M) \subseteq SL_2(\mathbb{Z})$, a cusp is an equivalence class of $\mathbb{Q} \cup \{\infty\}$ under the action of $\Gamma_0(M)$ defined on $\mathbb{Q} \cup \{\infty\}$ as in (2.1). Given an integer weight modular form on the congruence subgroup $\Gamma_0(M)$, we say that $f(z)$ is a holomorphic modular (resp. cusp) form if $f(z)$ is holomorphic (resp. vanishes) at the cusps of $\Gamma_0(M)$. From now on we use the term modular (resp. cusp) form to refer to a holomorphic modular (resp. cusp) form. Define $M_k(\Gamma_0(M))$ to be the \mathbb{C} -vector space of modular forms with weight k and level M , and $S_k(\Gamma_0(M))$ the space of cusp forms.

Now that the spaces of modular forms have been defined, we give some examples of modular forms. A fundamental fact is that the weight 4 and 6 Eisenstein series,

$$\begin{aligned} E_4(z) &= 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n, \\ E_6(z) &= 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)q^n, \end{aligned}$$

where $\sigma_k(n) := \sum_{1 \leq d|n} d^k$, generate the algebra of all the modular forms on $SL_2(\mathbb{Z})$.

The Delta-function is the unique cusp form of weight 12 on $SL_2(\mathbb{Z})$ normalized so that its leading Fourier coefficient equals 1. In terms of $E_4(z)$ and $E_6(z)$, we have

$$\Delta(z) := \frac{E_4(z)^3 - E_6(z)^2}{1728} = q - 24q^2 + 252q^3 - \dots \in \mathbb{Z}[[q]].$$

Half-integral weight modular forms are defined similarly as in Definition 2.1 (see page 11 of [13]). Our main result uses a weight $\frac{1}{2}$ modular form, Dedekind's eta-function:

$$(2.2) \quad \eta(z) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n).$$

Products and quotients of eta-functions can be integer weight. For example, it is well known that that

$$\Delta(z) = \eta(z)^{24}.$$

An eta-quotient is a function of the form $f(z) = \prod_{\delta|M} \eta(\delta z)^{r_\delta}$, where $M \geq 1$ and each r_δ is an integer.

Theorem 2.2. [5, 8, 9] *If $f(z) = \prod_{\delta|M} \eta(\delta z)^{r_\delta}$ is an eta-quotient with $k = \frac{1}{2} \sum_{\delta|M} r_\delta \in \mathbb{Z}$, with the additional properties that*

$$\sum_{\delta|M} \delta r_\delta \equiv 0 \pmod{24}$$

and

$$\sum_{\delta|M} \frac{M}{\delta} r_\delta \equiv 0 \pmod{24},$$

then $f(z)$ satisfies

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for every $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(M)$.

To decide whether or not an eta quotient is a cusp form, it then suffices to check if its orders of vanishing at the cusps are positive.

Theorem 2.3. [3, 6, 7] *Let c, d and m be positive integers with $d|m$ and $\gcd(c, d) = 1$. If $f(z)$ is an eta-quotient satisfying the conditions of the previous theorem for M , then the order of vanishing of $f(z)$ at the cusp $\frac{c}{d}$ is*

$$\frac{M}{24} \sum_{\delta|M} \frac{\gcd(d, \delta)^2 r_\delta}{\gcd(d, \frac{M}{d}) d \delta}.$$

A lot of information about spaces of modular forms can be obtained by using some special linear transformations called Hecke operators, which are defined as follows. If $p \nmid M$ is prime and $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(M))$, then the action of the Hecke operator $T_{p,k}$ on $f(z)$ is defined by

$$(2.3) \quad f(z)|T_{p,k} := \sum_{n=0}^{\infty} (a(pn) + p^{k-1}a(n/p)) q^n.$$

Remark. If $p \nmid n$, then $a(n/p)$ is defined to be 0.

Remark. Throughout, for ease of notation, we will write T_p in place of $T_{p,k}$.

Serre observed that the action of Hecke algebras on spaces of modular forms of level 1 is *locally nilpotent modulo 2* [17]. This means that given an integer weight modular form $f(z) \in M_k(SL_2(\mathbb{Z}))$, there exists a positive integer c satisfying

$$(2.4) \quad f(z)|T_{p_1}|T_{p_2}|\dots|T_{p_c} \equiv 0 \pmod{2}$$

for every collection of odd primes p_1, p_2, \dots, p_c .

The following theorem is implied by a more general result of Ono and Taguchi [14] and classifies all of the spaces of modular forms that exhibit the same phenomenon. Define $S_k(\Gamma_0(m), \mathbb{Z})$ to be the space of cusp forms of weight k and level M with integer coefficients.

Theorem 2.4. [Theorem 1.3 of [14]] *Let a be a non-negative integer, and let k be a positive integer. If $m = 1, 5, 7$, or 17 , then there is an integer $c \geq 0$ such that for every $f(z) \in S_k(\Gamma_0(2^a m), \mathbb{Z})$, we have*

$$(2.5) \quad f(z)|T_{p_1}|T_{p_2}|\dots|T_{p_{c+1}} \equiv 0 \pmod{2},$$

whenever $p_1, \dots, p_{c+1} \equiv \pm 1 \pmod{m}$ are primes.

Our proof makes use of the nilpotency of Hecke algebras on spaces of integer weight modular forms of level m , where $m \in \{1, 5, 7, 17\}$.

3. LEMMAS AND PROOF OF THEOREM 1.1

3.1. Odd coefficients of modular forms on $\Gamma_0(m)$. We first establish a relation between the parity of $p(n)$ and the parity of the coefficients of certain families of modular forms.

Lemma 3.1. *Suppose that*

$$(3.1) \quad A(q) = 1 + \sum_{n \geq 1} \alpha(n)q^{tk\beta n} = \prod_{n=1}^{\infty} (1 - q^{tk\beta n})^{\gamma} \in \mathbb{Z}[[q]],$$

where $t, k, \beta \geq 1$ and $24 \mid k(t\beta\gamma - 1)$. If we let $\delta = \frac{k(t\beta\gamma - 1)}{24}$, and

$$(3.2) \quad \widehat{A}(q) = \sum_{n=0}^{\infty} \widehat{\alpha}(n)q^n := A(q) \cdot \left(\sum_{n=0}^{\infty} p(n)q^{kn+\delta} \right),$$

then Subbarao's Conjecture is true for the arithmetic progressions $r + nt$ where $0 \leq r < t$ if and only if there is at least one $N \equiv kr + \delta \pmod{t}$ such that $\widehat{\alpha}(N)$ is odd.

Proof. By direct calculation, we have

$$\begin{aligned} \sum_{n=0}^{\infty} \widehat{\alpha}(n)q^n &= A(q) \cdot \left(\sum_{n=0}^{\infty} p(n)q^{kn+\delta} \right), \\ &= \left(1 + \sum_{n=1}^{\infty} \alpha(n)q^{tk\beta n} \right) \left(\sum_{n=0}^{\infty} p(n)q^{kn+\delta} \right), \\ &= \sum_{n=0}^{\infty} \left(p\left(\frac{n-\delta}{k}\right) + \sum_{j=1}^{\infty} \alpha(j)p\left(\frac{n-\delta}{k} - t\beta j\right) \right) q^n. \end{aligned}$$

Thus we have that

$$(3.3) \quad \widehat{\alpha}(n) = p\left(\frac{n-\delta}{k}\right) + \sum_{j=1}^{\infty} \alpha(j)p\left(\frac{n-\delta}{k} - t\beta j\right).$$

Note that $p(n)$ is defined to be zero for $n \notin \mathbb{Z}_{\geq 0}$, and so the sum on the right hand side of (3.3) is finite. Now observe that when $(n-\delta)/k \in \mathbb{N}$, the integers

$$\frac{n-\delta}{k}, \frac{n-\delta}{k} - t\beta, \frac{n-\delta}{k} - 2t\beta, \dots, \frac{n-\delta}{k} - t\beta \left\lfloor \frac{n-\delta}{k+\beta} \right\rfloor$$

are congruent modulo t . By Ono's result (see page 2 of this paper or [11]), it is sufficient to show that there exists one $N \equiv kr + \delta \pmod{t}$ such that $p(N)$ is odd. If $\widehat{\alpha}(N) \equiv 1 \pmod{2}$, then $p\left(\frac{N-\delta}{k} - t\beta j\right)$ is odd for at least one j , which implies Subbarao's Conjecture. Conversely, if Subbarao's Conjecture is true, then in each residue class modulo t , there exists a smallest $\frac{N-\delta}{k} \equiv r \pmod{t}$ such that $p\left(\frac{N-\delta}{k}\right)$ is odd. For such N , $\widehat{\alpha}(N)$ is odd. \square

The following two lemmas will also be useful in proving the main theorem, the first of which is a standard fact from algebra.

Lemma 3.2 (Hensel's Lemma). *Let $f(x) \in \mathbb{Z}[x]$, and let p be prime. Suppose $f(x) \equiv 0$ has a solution x_0 modulo p satisfying $f'(x_0) \not\equiv 0 \pmod{p}$. Then for all $n \in \mathbb{N}$, there exists $x_n \in \mathbb{Z}/p^n\mathbb{Z}$ such that $f(x_n) \equiv 0 \pmod{p^n}$.*

Lemma 3.3. *Let δ be odd, let c be any number congruent to $\delta \pmod{8}$, and let $s \in \mathbb{N}$. Then for all $0 \leq r < 2^s$, there exist infinitely many odd primes l for which*

$$\frac{cl^2 - \delta}{8} \equiv r \pmod{2^s}.$$

Proof. Let $0 \leq r < 2^s$ and define

$$f(x) := \frac{c(4x+1)^2 - \delta}{8} - r.$$

We will use Hensel's Lemma to show that $f(x)$ has a root modulo 2^s . It is clear that

$$f(x) \equiv x + \frac{c - \delta}{8} - r \pmod{2},$$

so there exists x_0 such that $f(x_0) \equiv 0 \pmod{2}$. Note that $f'(x_0) \not\equiv 0 \pmod{2}$ for every x_0 . Therefore, by Hensel's lemma, there exists a non-negative integer x_s such that $f(x_s) \equiv 0 \pmod{2^s}$

Thus, for all odd primes $l \equiv 4x_s + 1 \pmod{2^s}$, we have

$$\frac{cl^2 - \delta}{8} \equiv r \pmod{2^s}.$$

By Dirichlet's theorem on primes in arithmetic progressions, there exist infinitely many such l . \square

3.2. Proof of Theorem 1.1. For the remainder of the paper, we assume that

$$\sum_{n=1}^{\infty} a(n)q^n$$

is an integer weight cusp form of level m with integer coefficients where

$$m \in \{1, 5, 7, 17\}.$$

Given a set L of odd primes l_1, \dots, l_c congruent to $\pm 1 \pmod{m}$ and a positive integer $i \leq c$, we define $a_{i,L}$ by

$$(3.4) \quad \sum_{n=1}^{\infty} a_{i,L}(n)q^n := \left(\sum_{n=1}^{\infty} a(n)q^n \right) \Big|_{T_{l_1}} \Big| \dots \Big|_{T_{l_i}}.$$

We also let $a_{0,\emptyset}(n) = a(n)$. For all $i \geq 0$, we have

$$(3.5) \quad \sum_{n=1}^{\infty} a_{i+1,L}(n)q^n = \left(\sum_{n=1}^{\infty} a_{i,L}(n)q^n \right) \Big|_{T_{l_{i+1}}}$$

$$(3.6) \quad \equiv \sum_{n=1}^{\infty} (a_{i,L}(nl_{i+1}) + a_{i,L}(n/l_{i+1})) q^n \pmod{2}.$$

Suppose that $n_0 \in \mathbb{N}$ and $a(n_0)$ is odd. Define $n_{i,L}$ by $n_{i,L} := n_0 l_1 l_2 \dots l_i$. We say that $n_{0,\emptyset} = n_0$. Thus, we have

$$a_{i+1,L}(n_{i+1,L}) \equiv a_{i,L}(n_{i,L} l_{i+1}^2) + a_{i,L}(n_{i,L}) \pmod{2}.$$

By the work of Ono and Taguchi [14], we obtain the following lemma for forms of level m .

Lemma 3.4. *For any $m \in \{1, 5, 7, 17\}$, there exists an integer $c \geq 0$ and a set L of odd primes l_1, \dots, l_c congruent to $\pm 1 \pmod{m}$ (if $c = 0$, then $L = \emptyset$) such that $a_{c,L}(n_{c,L} l^2) \equiv 1 \pmod{2}$ for all odd primes l congruent to $\pm 1 \pmod{m}$.*

Proof. By Theorem 2.4 we can find an integer $c \geq 0$ and a set L satisfying the above conditions such that $a_{c,L}(n_{c,L}) \equiv 1 \pmod{2}$ but $a_{c+1,L \cup \{l\}}(n_{c,L} l) \equiv 0 \pmod{2}$ for any odd prime $l \equiv \pm 1 \pmod{m}$. Therefore it is clear that $a_{c,L}(n_{c,L} l^2) \equiv 1$ for any odd prime $l \equiv \pm 1 \pmod{m}$. \square

Lemma 3.5. *Suppose $L = \{l_1, l_2, \dots, l_i\}$ is a set of odd primes congruent to $\pm 1 \pmod{m}$. If $a_{i,L}(n_{i,L} l^2) \equiv 1 \pmod{2}$ for all odd primes l congruent to $\pm 1 \pmod{m}$, then for each prime l congruent to $\pm 1 \pmod{m}$, there exists an odd square C_l congruent to 1 \pmod{m} such that $a(n_0 C_l l^2) \equiv 1 \pmod{2}$.*

Proof. We first prove inductively, for any C , that

$$(3.7) \quad a_{i,L}(n_{i,L} C) \equiv \sum_{(w_1, \dots, w_i)} a(n_0 l_1^{w_1} \dots l_i^{w_i} C) \pmod{2},$$

where the sum is over all i -tuples (w_1, \dots, w_i) of elements in $\{0, 2\}$. Clearly this is true for $i = 1$. Suppose that the hypothesis is true for $i = k$ and all integers C . Let C_0 be an integer. Consider

$$\begin{aligned} a_{k+1,L}(n_{k+1,L} C_0) &\equiv a_{k,L}(n_{k,L} l_{k+1}^2 C_0) + a_{k,L}(n_{k,L} C_0) \pmod{2}, \\ &\equiv \sum_{(w_1, \dots, w_{k+1})} a(n_0 l_1^{w_1} \dots l_{k+1}^{w_{k+1}} C_0) \pmod{2}. \end{aligned}$$

This proves 3.7 Now note that if $a_{i,L}(n_{i,L} l^2) \equiv 1 \pmod{2}$ for all odd $l \equiv \pm 1 \pmod{m}$ then for at least one odd $C_l = l_1^{v_1} \dots l_i^{v_i}$, where $v_j \in \{0, 2\}$ for all j , we have $a(n_0 C_l l^2) \equiv 1 \pmod{2}$. \square

Without loss of generality, we assume that $s \geq 3$. To prove our theorem, we now construct modular forms which encode the relevant partition values. Let

$$(3.8) \quad \widehat{A}_{s,m}(q) = \sum_{n=0}^{\infty} \widehat{\alpha}_{s,m}(n) q^n := \frac{\eta(mz)^{2^{2s+3}m}}{\eta(z)^8},$$

where $s \in \mathbb{N}$. We see that $\widehat{A}_{s,m}$ is congruent modulo 2 to a power series of the form specified in (3.2) of Lemma 3.1, with $k = 8$, $t = m \cdot 2^s$, $s \geq 3$, $\delta = \frac{m^{2 \cdot 2^{2s}-1}}{3}$, $\beta = 2^s$

and $\gamma = m$. By Theorem 2.2 $\widehat{A}_{s,m}(z)$ is a weight 2^{2s+2} meromorphic modular form on $\Gamma_0(m)$. It suffices to check that

$$\begin{aligned} m^2 2^{2s+3} - 8 &\equiv 0 \pmod{24}, \\ m(2^{2s+3} - 8) &\equiv 0 \pmod{24}. \end{aligned}$$

By Theorem 2.3 it follows that $\widehat{A}_{s,n}(z)$ is a cusp form. To see this, we simply need to verify that the order of vanishing at the cusps is positive, so we need

$$\frac{\gcd(d, m)^2 \cdot 2^{2s+3}}{m} - \frac{\gcd(d, 1)^2 \cdot 8}{1} > 0$$

for all $d|m$, which is clearly true. Now we prove the theorem case by case.

Case 1. $m = 1$.

This was proven by Boylan and Ono [4]. It follows immediately from Lemmas 3.1 and 3.3.

Case 2. $m = 5, 7, 17$.

For $m \in \{5, 7, 17\}$, let O_m be the set $\{k_0, \dots, k_{m-1}\}$ where for all $0 \leq r < m$, k_r is the smallest integer congruent to $r \pmod{m}$ such that $p(k_r)$ is odd. Specifically, $O_5 = \{0, 1, 3, 4, 7\}$, $O_7 = \{0, 1, 3, 4, 5, 6, 16\}$, and $O_{17} = \{0, 1, 3, 4, 5, 6, 7, 12, 13, 14, 16, 32, 36, 43, 44, 67, 89\}$.

From (3.3), one can directly check that $\widehat{\alpha}(\delta + 8k_r)$ is odd for all $k_r \in O_m$. Since $\widehat{A}_{s,m}$ is an integer weight cusp form of level m and with integer coefficients, by Lemma 3.4 and Lemma 3.5, for each $k_r \in O_m$ and for each odd prime l congruent to $\pm 1 \pmod{m}$, there exist odd squares $C_{k_r,l}$ congruent to $1 \pmod{m}$ such that $\widehat{\alpha}(C_{k_r,l}(\delta + 8k_r)l^2) \equiv 1 \pmod{2}$.

We want to prove that Subbarao's conjecture is true for all arithmetic progressions modulo $m \cdot 2^s$. By Lemma 3.1, it suffices to show that as k_r ranges over O_m and as l ranges over all odd primes congruent to $\pm 1 \pmod{m}$

$$\frac{(C_{k_r,l}(\delta + 8k_r)l^2) - \delta}{8}$$

covers all residue classes modulo $m \cdot 2^s$. But $C_{k_r,l}l^2 \equiv 1 \pmod{m}$ and 8 is invertible modulo m . By Lemma 3.3 and the Chinese Remainder Theorem, we simply need to show that k_r covers all residue classes modulo m . This is clear from the way O_m is defined. \square

REFERENCES

- [1] S. Ahlgren, *Distribution of the parity of the partition function in arithmetic progressions*, *Indagationes Math.* **10** (1999), 173-181.
- [2] S. Ahlgren and M. Boylan, *Arithmetic properties of the partition function*, *Invent. Math.* **153** (2003), 487-502.
- [3] A. J. F. Biagioli, *The construction of modular forms as products of transforms of the Dedekind eta function*, *Acta Arith.* **54** (1990), 273-300.

- [4] M. Boylan and K. Ono, *Parity of the partition function in arithmetic progressions II*, Bull. London Math. Soc. **33** (2001) 558-564.
- [5] B. Gordon and K. Hughes, *Multiplicative properties of η -products II*, A tribute to Emil Grosswald: Number Theory and related analysis, Cont. Math. of the Amer. Math. Soc. **143** (1993), 415-430.
- [6] G. Ligozat, *Courbes modulaires de genre 1*, Bull. Soc. Math. France [Mémoire 43] (1972), 1-80.
- [7] Y. Martin, *Multiplicative η -quotients*, Trans. Amer. Math. Soc. **348** (1996), 4825-4856.
- [8] M. Newman, *Construction and application of a certain class of modular functions*, Proc. London Math. Soc. (3) **7** (1956), 334-350.
- [9] M. Newman, *Construction and application of a certain class of modular functions II*, Proc. London Math. Soc. (3) **9** (1959), 373-387.
- [10] J.-L. Nicolas, I. Z. Ruzsa, and A. Sárközy *On the parity of additive representation functions*, J. Number Th. **73** (1998), 292-317.
- [11] K. Ono, *Parity of the partition function in arithmetic progressions*, J. reine angew. Math. **472** (1996), 1-15.
- [12] K. Ono, *Distribution of the partition function modulo m* , Ann. of Math. **151** (2000), 293-307.
- [13] K. Ono, *The Web of Modularity: Arithmetic of the Coefficients of Modular Forms and q -series*. CBMS Regional Conference Series in Mathematics, **102**. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004.
- [14] K. Ono and Y. Taguchi, *2-Adic properties of certain modular forms and their applications to arithmetic functions*, Int. J. Number Theory **1** (2005), 75-101.
- [15] T. R. Parkin and D. Shanks, *On the distribution of parity in the partition function*, Math. Comp. **21** (1967), 466-480.
- [16] S. Ramanujan, *Congruence properties of partitions*, Proc. London Math. Soc. **19** (1919), 207-210.
- [17] J.-P. Serre, *Valeurs propres des opérateurs de Hecke modulo l* , Astérisque **24-25** (1975), 109-117.
- [18] M. Subbarao, *Some remarks on the partition function*, Amer. Math. Monthly **73** (1966), 851-854.