# PARITY OF THE PARTITION FUNCTION IN ARITHMETIC PROGRESSIONS, II

Matthew Boylan and Ken Ono

*Appearing in the Bulletin of the London Mathematical Society.*

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. We prove the conjecture for every arithmetic progression whose modulus is a power of 2.

## 1. Introduction and Statement of Results

A partition of a non-negative integer $n$ is a non-increasing sequence of positive integers whose sum is $n$. It is well known, by the work of Euler, that the generating function for $p(n)$ is given by the infinite product

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n} = 1 + q + 2q^2 + 3q^3 + 5q^4 + 7q^5 + \cdots . \tag{1}$$

Although it is widely believed that $p(n)$ is equally often even and odd, little is known. In this note we consider the following conjecture due to M. Subbarao [7].

**Conjecture.** (Subbarao) *For any arithmetic progression $r \pmod t$, there are infinitely many integers $M \equiv r \pmod t$ for which $p(M)$ is odd, and there are infinitely many integers $N \equiv r \pmod t$ for which $p(N)$ is even.*

Works by F. Garvan, O. Kolberg, M. Hirschhorn, D. Stanton and M. Subbarao (see [5] for references) verified this conjecture for every arithmetic progression with modulus

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

---

2000 *Mathematics Subject Classification.* 11P83

The second author is supported by NSF grant DMS-9874947, an Alfred P. Sloan Foundation Fellowship and a David and Lucile Packard Research Fellowship.

More recently, the second author [5] was able to prove the conjecture for every arithmetic progression with modulus $t \leq 10^5$.

This was obtained by combining two results. The first result in [5] establishes that in every arithmetic progression $r \pmod t$ there are infinitely many integers $N \equiv r \pmod t$ for which $p(N)$ even. Obviously, this settles the "even case" of the conjecture. However, the "odd case" of the conjecture remains open. The second result in [5] shows that there are infinitely many integers $M \equiv r \pmod t$ for which $p(M)$ is odd, provided there is at least one such $M$. Unfortunately, the possibility remains that there are rogue progressions $r \pmod t$ for which $p(N)$ is even for every $N \equiv r \pmod t$.

With the aid of a computer, one may presumably use the results in [5] to prove the conjecture for many more moduli $t$. Unfortunately, the total number would be finite. In this note we exhibit the first infinite family of moduli $t$ for which we are able to settle the conjecture.

**Theorem 1.** *If $s$ is a positive integer, then Subbarao's Conjecture is true for every arithmetic progression with modulus $t = 2^s$.*

Combined with works by S. Ahlgren [Th. 1.4, 1] and J.-P. Serre [Th. 3, 4], this result immediately implies the following corollary.

**Corollary 2.** *If $s$ is a positive integer and $0 \leq r < 2^s$, then*

$$\#\{N \equiv r \pmod{2^s} \ : \ N \leq X \text{ and } \ p(N) \equiv 0 \pmod 2\} \gg_{r,s} \sqrt{X},$$
$$\#\{M \equiv r \pmod{2^s} \ : \ M \leq X \text{ and } \ p(M) \equiv 1 \pmod 2\} \gg_{r,s} \sqrt{X}/\log X.$$

In §2 we present a proposition which implies Theorem 1, and in §3 we prove it.

## 2. An important proposition

We begin by recalling Ramanujan's Delta function, the unique cusp form of weight 12 with respect to the full modular group $SL_2(\mathbb{Z})$. It is given by the infinite product

$$\Delta(z) := q\prod_{n=1}^{\infty}(1-q^n)^{24} = q - 24q^2 + 252q^3 - \cdots \qquad (q := e^{2\pi i z} \text{ throughout}). \tag{2}$$

If $s > 1$ is a positive integer, then define integers $a_s(n)$ by

$$\Delta(z)^{(4^s-1)/3} := \sum_{n=0}^{\infty} a_s(n) q^n. \tag{3}$$

The following lemma relates the parity of these coefficients to the parity of the partition function in arithmetic progressions $\pmod{4^s}$.

**Lemma 2.1.** *If $s > 1$ is a positive integer, then define integers $r_s(j)$ by*

$$1 + \sum_{j=1}^{\infty} r_s(j) q^{8\cdot 4^s j} := \prod_{n=1}^{\infty} (1 - q^{8\cdot 4^s n}).$$

*Then we have*

$$a_s(n) \equiv p\left(\frac{n - \frac{4^s-1}{3}}{8}\right) + \sum_{j=1}^{\infty} r_s(j) p\left(\frac{n - \frac{4^s-1}{3}}{8} - 4^s j\right) \pmod 2.$$

*Proof.* By (1) and (2), we find that

$$\begin{aligned}
\Delta(z)^{(4^s-1)/3} &= \left(q \prod_{n=1}^{\infty} (1-q^n)^{24}\right)^{(4^s-1)/3} \\
&\equiv q^{(4^s-1)/3} \prod_{n=1}^{\infty} (1 - q^{8\cdot 4^s n}) \cdot \prod_{n=1}^{\infty} \left(\frac{1}{1-q^{8n}}\right) \pmod 2 \\
&\equiv \left(1 + \sum_{j=1}^{\infty} r_s(j) q^{8\cdot 4^s j}\right) \cdot \left(\sum_{k=0}^{\infty} p(k) q^{8k + \frac{4^s-1}{3}}\right) \pmod 2.
\end{aligned}$$

The result follows by comparing coefficients.

Q.E.D.

The next proposition is vital for our result.

**Proposition 2.2.** *If $s > 1$ is a positive integer, then there is an odd positive integer $n_s$ for which $a_s(n_s)$ is odd with the additional property that*

$$a_s(n_s \ell^2) \equiv 1 \pmod 2$$

*for every prime $\ell \nmid 2n_s$.*

**Lemma 2.3.** *Proposition 2.2 implies Theorem 1.*

*Proof.* We begin by noting that Theorem 1 is implied by the truth of Subbarao's Conjecture for all arithmetic progressions with moduli of the form $4^s$. Therefore, our objective is to prove the conjecture in these cases.

By [Main Theorem 1, 5], it suffices to prove the "odd case" of the Subbarao's Conjecture. Moreover, by [Main Theorem 2, 5], it suffices to establish that in each arithmetic progression $r \pmod{4^s}$ there is at least one integer $M \equiv r \pmod{4^s}$ for which $p(M)$ is odd.

Suppose that $\ell \nmid 2n_s$ is prime. If Proposition 2.2 is true, then Lemma 2.1 implies that

$$a_s(n_s\ell^2) \equiv 1 \equiv p\left(\frac{n_s\ell^2 - \frac{4^s-1}{3}}{8}\right) + \sum_{j=1}^{\infty} r_s(j) p\left(\frac{n_s\ell^2 - \frac{4^s-1}{3}}{8} - 4^s j\right) \pmod 2.$$

Therefore, it follows that

$$p\left(\frac{n_s\ell^2 - \frac{4^s-1}{3}}{8} - 4^s j\right) \equiv 1 \pmod 2 \tag{4}$$

for some non-negative integer $j$. Notice that the arguments for the partition function lie in a fixed arithmetic progression $\pmod{4^s}$ which is independent of $j$.

Hence, it suffices to show, by varying the primes $\ell$, that the numbers $\frac{1}{8}\left(n_s\ell^2 - \frac{4^s-1}{3}\right)$ cover all of the arithmetic progression modulo $4^s$. This follows by an easy application of Hensel's Lemma and Dirichlet's Theorem on Primes in Arithmetic Progressions.

Q.E.D.

## 3. Proof of Theorem 1.

In view of Lemma 2.3, it suffices to prove Proposition 2.2. In this section we prove Proposition 2.2 using the nilpotency of the action of the Hecke operators on the space of modular forms on $SL_2(\mathbb{Z})$ modulo 2.

We begin by fixing notation. If $k$ is a positive integer, then let $M_k$ denote the space of weight $k$ modular forms with respect to $SL_2(\mathbb{Z})$ (see [3] for background on modular forms). If $p$ is prime, then let $T_{p,k}$

$$T_{p,k} : M_k \ \rightarrow \ M_k$$

denote the usual $p$th Hecke operator for $M_k$. If $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k$, then

$$f(z) \mid T_{p,k} = \sum_{n=0}^{\infty} \left(a(pn) + p^{k-1}a(n/p)\right) q^n. \tag{5}$$

Note that $a(\alpha) = 0$ if $\alpha \notin \mathbb{Z}$. If $m$ is a positive integer and $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in \mathbb{Z}[[q]]$ has the property that $a(n) \equiv 0 \pmod m$ for every $n$, then we say that

$$f(z) \equiv 0 \pmod m.$$

**Proposition 3.1.** *If $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k \cap \mathbb{Z}[[q]]$ has the property that*

$$f(z) \mid T_{p,k} \equiv 0 \pmod 2$$

*for every prime $p$, then either $f(z) \equiv 0 \pmod 2$ or*

$$f(z) \equiv \Delta(z) \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod{2}.$$

*Proof.* Without loss of generality, we may assume that $k$ is an even integer since every modular form on $SL_2(\mathbb{Z})$ with odd weight is the function which is identically zero. By (5), we have that

$$0 \equiv f(z) \mid T_{2,k} \equiv \sum_{n=0}^{\infty} a(2n)q^n.$$

Therefore, if $a(n)$ is odd, then $n$ must be odd.

If $p$ is an odd prime, then the coefficient of $q^n$ in $f(z) \mid T_{p,k}$ satisfies

$$a(pn) + a(n/p) \equiv 0 \pmod{2}. \tag{6}$$

Therefore, if $p \nmid n$, then $a(pn) \equiv 0 \pmod 2$. By replacing $n$ by $p^2n$ where $p \nmid n$, (6) implies that

$$0 \equiv a(p^3n) + a(pn) \equiv a(p^3n) \pmod{2}.$$

Arguing in this way, we find that if $a(n)$ is odd, then $n$ must be an odd square.

If $p$ is an odd prime, then (6) implies that

$$0 \equiv a(p^2n) + a(n) \pmod{2} \tag{7}$$

for every positive integer $n$. If $a(1)$ is even, then (7) implies that $f(z) \equiv 0 \pmod 2$. On the other hand, if $a(1)$ is odd, then (7) implies that

$$f(z) \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod{2}.$$

To complete the proof, it suffices to show that

$$\Delta(z) \equiv q\prod_{n=1}^{\infty}(1-q^{8n})^3 \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod{2}.$$

This follows immediately from Jacobi's Triple Product Identity [Th. 2.8, 2].

Q.E.D.

J.-P. Serre noticed that (see [p. 115, 6] and [p. 251, 7]) the action of the Hecke algebras on the space of modular forms modulo 2 is locally nilpotent. This implies that if $f(z) \in M_k \cap \mathbb{Z}[[q]]$, then there is a positive integer $i$ with the property that

$$f(z) \mid T_{p_1,k} \mid T_{p_2,k} \mid \cdots \mid T_{p_i,k} \equiv 0 \pmod{2}$$

for every collection of primes $p_1, p_2, \ldots p_i$. For convenience we make the following definition.

**Definition 3.2.** *Suppose that* $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k \cap \mathbb{Z}[[q]]$ *is a modular form for which*

$$f(z) \not\equiv 0 \pmod 2 \quad \text{and} \quad f(z) \not\equiv \Delta(z) \pmod 2.$$

*We say that* $f(z)$ *has degree of nilpotency* $i$ *if there are distinct primes* $p_1, p_2, \dots p_{i-1}$ *for which*

$$f(z) \mid T_{p_1,k} \mid T_{p_2,k} \mid \cdots \mid T_{p_{i-1},k} \not\equiv 0 \pmod 2$$

*and*

$$f(z) \mid T_{\ell_1,k} \mid T_{\ell_2,k} \mid \cdots \mid T_{\ell_i,k} \equiv 0 \pmod 2$$

*for every collection of distinct primes* $\ell_1, \ell_2, \dots, \ell_i$.

**Proposition 3.3.** *Suppose that* $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k \cap \mathbb{Z}[[q]]$ *has degree of nilpotency* $i > 0$. *Then there are distinct primes* $p_1, p_2, \dots p_{i-1}$ *with the property that*

$$a(n_0 p_1 p_2 \cdots p_{i-1}) \equiv 1 \pmod 2$$

*for every odd square* $n_0$ *which is coprime to* $p_1 p_2 \cdots p_{i-1}$.

*Proof.* By Proposition 3.1 and the definition of the degree of nilpotency, there are distinct primes $p_1, p_2, \dots p_{i-1}$ for which

$$f(z) \mid T_{p_1,k} \mid T_{p_2,k} \mid \cdots \mid T_{p_{i-1},k} \equiv \Delta(z) \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod 2. \tag{8}$$

Define integers $b_j(n)$ by

$$\begin{aligned} \sum_{n=0}^{\infty} b_1(n)q^n &:= f(z) \mid T_{p_1,k}, \\ \sum_{n=0}^{\infty} b_2(n)q^n &:= f(z) \mid T_{p_1,k} \mid T_{p_2,k}, \\ &\vdots \\ \sum_{n=0}^{\infty} b_{i-1}q^n &:= f(z) \mid T_{p_1,k} \mid T_{p_2,k} \mid \cdots \mid T_{p_{i-1},k}. \end{aligned} \tag{9}$$

By (5), (8), and (9), if $n_0$ is an odd square which is coprime to $p_1 p_2 \cdots p_{i-1}$, then

$$\begin{aligned} 1 &\equiv b_{i-1}(n_0) \\ &\equiv b_{i-2}(n_0 p_{i-1}) \\ &\equiv b_{i-3}(n_0 p_{i-2} p_{i-1}) \\ &\vdots \\ &\equiv b_1(n_0 p_2 p_3 \cdots p_{i-1}) \\ &\equiv a(n_0 p_1 p_2 \cdots p_{i-1}) \pmod 2. \end{aligned}$$

This completes the proof.

Q.E.D.

*Proof of Proposition 2.2.* Let $s > 1$ be a positive integer, and recall that the integers $a_s(n)$ are defined by

$$\sum_{n=1}^{\infty} a_s(n)q^n := \Delta(z)^{(4^s-1)/3} = q^{(4^s-1)/3} - \cdots .$$

It is easy to see that $(4^s - 1)/3 \equiv 5 \pmod 8$. Therefore,

$$\Delta(z)^{(4^s-1)/3} \not\equiv 0 \pmod 2 \quad \text{and} \quad \Delta(z)^{(4^s-1)/3} \not\equiv \Delta(z) \equiv \sum_{n=0}^{\infty} q^{(2n+1)^2} \pmod 2.$$

By Proposition 3.3, there is a positive integer $i \geq 2$ and distinct primes $p_1, p_2, \ldots p_{i-1}$ for which

$$a_s(n_0 p_1 p_2 \cdots p_{i-1}) \equiv 1 \pmod 2 \tag{10}$$

for every odd square $n_0$ which is relatively prime to $p_1 p_2 \cdots p_{i-1}$. In addition, each of the primes $p_1, p_2, \ldots, p_{i-1}$ is odd. This follows immediately from (5) and the fact that $a_s(n)$ is even for every integer $n \not\equiv (4^s - 1)/3 \equiv 5 \pmod 8$.

Let $\ell \nmid 2n_0 p_1 p_2 \cdots p_{i-1}$ be prime. Define modular forms $h_0(z), h_1(z), \ldots, h_{i-1}(z)$ by

$$\begin{aligned}
h_0(z) &= \sum_{n=0}^{\infty} c_0(n)q^n := \Delta(z)^{(4^s-1)/3} \mid T_{\ell,k_s}, \\
h_1(z) &= \sum_{n=0}^{\infty} c_1(n)q^n := \Delta(z)^{(4^s-1)/3} \mid T_{\ell,k_s} \mid T_{p_1,k_s}, \\
h_2(z) &= \sum_{n=0}^{\infty} c_2(n)q^n := \Delta(z)^{(4^s-1)/3} \mid T_{\ell,k_s} \mid T_{p_1,k_s} \mid T_{p_2,k_s}, \\
&\ \ \vdots \\
h_{i-1}(z) &= \sum_{n=0}^{\infty} c_{i-1}(n)q^n := \Delta(z)^{(4^s-1)/3} \mid T_{\ell,k_s} \mid T_{p_1,k_s} \mid T_{p_2,k_s} \mid \cdots \mid T_{p_{i-1},k_s}.
\end{aligned} \tag{11}$$

Here the weight $k_s$ is $4^{s+1} - 4$.

By nilpotency, we have that $h_{i-1}(z) \equiv 0 \pmod 2$. Therefore, by (5) we have that

$$\begin{aligned}
0 &\equiv c_{i-1}(n_0\ell) \\
&\equiv c_{i-2}(n_0 p_{i-1}\ell) \\
&\equiv c_{i-3}(n_0 p_{i-2} p_{i-1}\ell) \\
&\qquad\vdots \\
&\equiv c_1(n_0 p_2 p_3 \cdots p_{i-1}\ell) \\
&\equiv c_0(n_0 p_1 p_2 \cdots p_{i-1}\ell) \\
&\equiv a_s(n_0 p_1 p_2 \cdots p_{i-1}\ell^2) + a_s(n_0 p_1 p_2 \cdots p_{i-1}) \pmod 2.
\end{aligned}$$

However, this congruence together with (10) implies that

$$a_s(n_0 p_1 p_2 \cdots p_{i-1}\ell^2) \equiv 1 \pmod 2.$$

This proves Proposition 2.2 with $n_s = n_0 p_1 p_2 \cdots p_{i-1}$.

Q.E.D.

## References


1. S. Ahlgren, *Distribution of parity of the partition function in arithmetic progressions*, Indagationes Math. (N.S.) **10** (1999), 173-181.
2. G. E. Andrews, *The theory of partitions*, Cambridge University Press, Cambridge, 1984.
3. N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, New York, 1984.
4. J.-L. Nicolas, I. Z. Ruzsa and A. Sárközy, *On the parity of additive representation functions (with an appendix by J.-P. Serre)*, J. Number Th. **73** (1998), 292-317.
5. K. Ono, *Parity of the partition function in arithmetic progressions*, J. reine angew. math. **472** (1996), 1-15.
6. J.-P. Serre, *Valeurs propres des opérateurs de Hecke modulo $\ell$*, Asterisque **24-25** (1975), 109-117.
7. J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, L'Enseignement Math. **22** (1976), 227-260.
7. M. Subbarao, *Some remarks on the partition function*, Amer. Math. Monthly **73** (1966), 851-854.



Dept. of Mathematics, University of Wisconsin, Madison, Wisconsin 53706 USA.
*E-mail address*: boylan@math.wisc.edu

Dept. of Mathematics, University of Wisconsin, Madison, Wisconsin 53706 USA.
*E-mail address*: ono@math.wisc.edu