PARITY OF THE PARTITION FUNCTION IN ARITHMETIC PROGRESSIONS

Ken Ono

In memory of the late S. Janaki Ammal

Abstract. Let $p(n)$ denote the number of partitions of a non-negative integer n. A well-known conjecture 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 (see Subbarao [23]). In this paper we prove that there indeed are infinitely many integers N in every arithmetic progression for which $p(N)$ is even; and that there are infinitely many integers M in every arithmetic progression for which $p(M)$ is odd so long as there is at least one (actually, we prove that if there is no such M less than $10^{10}t^7$ where t is the modulus of the arithmetic progression, then $p(N)$ must be even for all N in the arithmetic progression). Using these results we have checked Subbarao's conjecture for all arithmetic progressions with modulus $\leq 100,000$. The main tools in our proofs are the methods developed by Deligne, Serre, and Sturm for the reduction of positive integer weight holomorphic modular forms.

1. Introduction

A partition of a non-negative integer n is a non-increasing sequence of positive integers whose sum is n. Euler gave the following generating function for $p(n)$, the number of partitions of an integer n:

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

Ramanujan observed various surprising congruences for $p(n)$ when n is in certain, very special, arithmetic progressions; for example:

$$p(5n+4) \equiv 0 \mod 5,$$

$$p(7n+5) \equiv 0 \mod 7,$$

and

$$p(11n+6) \equiv 0 \mod 11.$$

1991 *Mathematics Subject Classification.* Primary 05A17; Secondary 11P83.
Key words and phrases. Parity conjecture, partitions, modular forms.
The author is support by National Science Foundation grant DMS-9508976.

There are now many proofs of these congruences (and their generalizations) in the literature (see [1, 2, 3, 4, 5, 6, 7, 11, 12, 24] for instance), often involving modular equations and various exotic combinatorial objects.

Surprisingly there does not seem to be any such congruences modulo 2 or 3. In fact the parity of $p(n)$ seems to be quite random, and it is believed that the partition function is 'equally often' even and odd; that is that $p(n)$ is even for $\sim \frac{1}{2}x$ positive integers $n \leq x$ (see Parkin and Shanks [20]).

In [23] Subbarao made the following conjecture on the parity of $p(n)$, for those integers n belonging to any given arithmetic progression:

Conjecture. *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.*

This conjecture has been proved for $t = 1, 2, 3, 4, 5, 10, 12, 16$ and 40, using a variety of elegant combinatorial methods, from the works of Garvan, Kolberg, Hirschhorn, Stanton and Subbarao (see [6, 9, 10, 13, 16, 23]).

In this paper, using ideas from the theory of modular forms (as developed by Deligne, Ligozat, Serre, and Sturm), we go some way to proving Subbarao's conjecture, with the following two results:

Main Theorem 1. *For any arithmetic progression $r \pmod t$, there are infinitely many integers $N \equiv r \pmod t$ for which $p(N)$ is even.*

Main Theorem 2. *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*

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

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

¿From the two theorems we have an algorithm to determine the truth of our parity conjecture for any given arithmetic progression $r \pmod t$: Compute $p(N) \pmod 2$ for $N = r, r + t, r + 2t, \ldots$ for all such N up to $C_{r,t}$. As soon as we find one odd number we have verified the conjecture. If all these numbers are even then we have proved that the conjecture is false.

Ken Burrell ran an efficient version of this algorithm on a CRAY C-90, giving the following result which confirms the conjecture for all moduli up to $100,000$:

Main Corollary. *For all $0 \leq r < t \leq 10^5$, 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.*

2. Preliminaries

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ act on $\mathfrak{H}$, the upper half of the complex plane, by the linear fractional transformation $Az = \frac{az+b}{cz+d}$. If N is a positive integer, then we define

the following *congruence subgroups* of $SL_2(\mathbb{Z})$ of *level* N:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1,\ c \equiv 0 \mod N \right\}.$$

and

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid ad - bc = 1,\ a \equiv d \equiv 1 \mod N, \text{ and } c \equiv 0 \mod N \right\}.$$

A meromorphic function $f(z)$ on $\mathfrak{H}$ is called a *modular function* with positive integer weight k with respect to congruence subgroup Γ if

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

for all $z \in \mathfrak{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. If $f(z)$ is holomorphic on $\mathfrak{H}$ and at the cusps of Γ (i.e. the rationals), then $f(z)$ is known as a *modular form* of weight k with respect to Γ. If $f(z)$ vanishes at the cusps of Γ, then $f(z)$ is known as a *cusp form*.

We denote the finite dimensional space of modular forms (resp. cusp forms) of weight k with respect to $\Gamma_1(N)$ by $M_k(N)$ (resp. $S_k(N)$). In the variable $q = e^{2\pi iz}$, a holomorphic modular form $f(z) \in M_k(N)$ admits a Fourier expansion of the form

$$f(z) = \sum_{n=0}^{\infty} a(n) q^n.$$

Of particular interest are certain modular forms in $M_k(N)$ with nice modular transformation properties with respect to $\Gamma_0(N)$. If χ is a Dirichlet character $\mod N$, then we say that a form $f(z) \in M_k(N)$ (resp. $S_k(N)$) is modular form of weight k with Nebentypus character χ if

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

for all $z \in \mathfrak{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. The space of such modular forms (resp. cusp forms) is denoted by $M_k(N, \chi)$ (resp. $S_k(N, \chi)$).

The spaces $M_k(N)$ and $S_k(N)$ have the following decomposition where the sums are over all Dirichlet characters $\chi \mod N$:

$$M_k(N) = \oplus_\chi M_k(N, \chi) \tag{2}$$

$$S_k(N) = \oplus_\chi S_k(N, \chi).$$

The Dedekind Eta-function is the principal modular form of interest in this paper; it is defined by the infinite product

$$\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 - q^n). \tag{3}$$

The generating function (1) for $p(n)$ is $q^{\frac{1}{24}}\eta^{-1}(z)$.

A function $f(z)$ is called an *Eta-product* if it is expressible as a finite product of the form

$$f(z) = \prod_{\delta|N} \eta^{r_\delta}(\delta z)$$

where N and each r_δ is an integer. Probably the most famous of all Eta-products is Ramanujan's $\Delta-$function, defined by $\Delta(z) := \eta^{24}(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$. This is the unique normalized weight 12 cusp form on $SL_2(\mathbb{Z})$. More generally, Gordon, Hughes, and Newman established the following theorem regarding the modular properties of Eta-products [8, 18, 19].

Theorem 1. *(***Gordon, Hughes, Newman***) If $f(z) = \prod_{\delta|N} \eta^{r_\delta}(\delta z)$ is an Eta-product for which*

$$\sum_{\delta|N} \delta r_\delta \equiv 0 \pmod{24} \tag{4}$$

and

$$\sum_{\delta|N} \frac{N}{\delta} r_\delta \equiv 0 \pmod{24}, \tag{5}$$

then $f(z)$ satisfies

$$f(Az) = \chi(d)(cz+d)^k f(z)$$

for all $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ where $k = \frac{1}{2}\sum_{\delta|N} r_\delta$. Here the character χ is defined by $\chi(d) = \left(\frac{(-1)^k s}{d}\right)$ and $s = \prod_{\delta|N} \delta^{r_\delta}$.

In particular, if k is a positive integer and $f(z)$ is holomorphic (resp. vanishes) at all of the cusps of $\Gamma_0(N)$, then $f(z) \in M_k(N,\chi)$ (resp. $S_k(N,\chi)$).

The following theorem will be used to determine whether certain Eta-products are modular forms: since $\eta(z)$ is analytic and never vanishes on $\mathfrak{H}$, it suffices for the orders at the cusps be non-negative. The following theorem due to Ligozat [17] is the necessary criterion for determining orders of an Eta-product at a cusp.

Theorem 2. *(***Ligozat***) Let c, d and N be positive integers with $d \mid N$ and $\gcd(c,d) = 1$. With the notation as above, if the Eta-product $f(z)$ satisfies* (4) *and* (5)*, then the order of vanishing of $f(z)$ at the cusp $\frac{c}{d}$ is*

$$\frac{1}{24}\sum_{\delta|N} \frac{N(d,\delta)^2 r_\delta}{(d,\frac{N}{d})d\delta}. \tag{6}$$

Equipped with Theorems 1 and 2 we construct holomorphic modular forms that are Eta-products whose Fourier expansions $\pmod 2$ are determined by the values of $p(n)$ modulo 2.

Proposition 1. *For a given positive integer t, let j be an integer satisfying $2^j > \frac{t}{24}$. Define $f_t(z)$ by*

$$f_t(z) := \frac{\eta(24z)}{\eta(48z)}\Delta^{2^j}(24tz) = \sum_{n\geq 1} a_t(n)q^{24n-1}.$$

Then $f_t(z)$ is a cusp form in $S_{2^j\cdot 12}(1152t, \left(\frac{2}{d}\right))$. Moreover the Fourier expansion of $f_t(z) \mod 2$ can be factored as:

$$f_t(z) = \sum_{n=0}^{\infty} a_t(n)q^{24n-1} \equiv \left(\sum_{n=0}^{\infty} p(n)q^{24n-1}\right)\left(\sum_{n=0}^{\infty} q^{2^j\cdot 24t(2n+1)^2}\right) \mod 2. \tag{7}$$

Proof. $f_t(z)$ is an Eta-product with $r_{24} = 1, r_{48} = -1, r_{24t} = 24\cdot 2^j$ and $r_\delta = 0$ otherwise. Thus N must be a multiple of $48t = [24, 48, 24t]$. If we let $N = 1152 = 24\cdot 48t$ then 24 divides δ and N/δ for each of $\delta = 24, 48, 24t$, so that the congruences (4) and (5) are evidently true.

The cusps of $\Gamma_0(1152t)$ are represented by fractions $\frac{c}{d}$ where $d \mid 1152t$ and $\gcd(c, d) = 1$. By Ligozat's formula (6), the order of vanishing is $N/(24(d, \frac{N}{d})d)$ times

$$\frac{(d,24)^2}{24} - \frac{(d,48)^2}{48} + \frac{(d,24t)^2 24\cdot 2^j}{24t} \geq \frac{(d,24)^2}{24}\left\{1 - 2 + \frac{2^j}{t/24}\right\} > 0$$

since $2^j > t/24$ by the hypothesis. Thus $f_t(z)$ is a cusp form in $S_{2^j\cdot 12}(1152t, \left(\frac{2}{d}\right))$, by Theorems 1 and 2.

Now we shall establish the $\mod 2$ factorization of $f_t(z)$. The following infinite product identity was proved by Jacobi:

$$\frac{\eta^2(16z)}{\eta(8z)} = q\prod_{n=1}^{\infty}\frac{(1-q^{16n})^2}{(1-q^{8n})} = \sum_{n=0}^{\infty} q^{(2n+1)^2} = q + q^9 + q^{25} + q^{49} + \dots.$$

Now, since $(1-Q)^2 \equiv 1 - Q^2 \equiv 1 + Q^2 \mod 2$, we have

$$\Delta(z) := q\prod_{n=1}^{\infty}\frac{(1-q^n)^{32}}{(1-q^n)^8} \equiv q\prod_{n=1}^{\infty}\frac{(1-q^{16n})^2}{(1-q^{8n})} = \sum_{n=0}^{\infty} q^{(2n+1)^2} \mod 2, \tag{8}$$

so that

$$\Delta^{2^j}(24tz) \equiv \Delta(24\cdot 2^j tz) \equiv \sum_{n=0}^{\infty} q^{2^j\cdot 24t(2n+1)^2} \mod 2.$$

Moreover

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty}\frac{1}{1-q^n} = \prod_{n=1}^{\infty}\frac{1+q^n}{1-q^{2n}} \equiv \prod_{n=1}^{\infty}\frac{1-q^n}{1-q^{2n}} \mod 2, \tag{9}$$

so that

$$\frac{\eta(24z)}{\eta(48z)} = \frac{1}{q}\prod_{n=1}^{\infty}\frac{1-q^{24n}}{1-q^{48n}} \equiv \sum_{n=0}^{\infty} p(n)q^{24n-1} \mod 2.$$

(7) now follows from multiplying together the two congruences above. □

3. The even case

Using $\ell-$adic Galois representations attached to certain modular forms by Deligne, Serre [21] proved the following remarkable theorem about the divisibility of Fourier coefficients of holomorphic modular forms.

Theorem 3. (Serre) *Let $f(z)$ be a holomorphic modular form of positive integer weight k on some congruence subgroup of $SL_2(\mathbb{Z})$ with Fourier expansion*

$$f(z) = \sum_{n=0}^{\infty} a(n)q^n$$

where $a(n)$ are algebraic integers in some number field. If m is a positive integer, then there exists a constant α such that there are $O(\frac{x}{log^{\alpha} x})$ integers $n \leq x$ such that $a(n)$ is not divisible by m.

In particular almost all of the Fourier coefficients of a modular form are divisible by any given integer m.

Corollary 1. *If $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ is the Fourier expansion of the form above, then*

$$a(n) \equiv 0 \pmod{m}$$

for almost all n in any given fixed arithmetic progression $r \pmod{t}$.

With this corollary we obtain

Main Theorem 1. *For any arithmetic progression $r \pmod{t}$, there are infinitely many integers $N \equiv r \pmod{t}$ for which $p(N)$ is even.*

Proof. In Proposition 1 we defined an Eta-product $f_t(z)$ for any given integer t, which we proved is a cusp form. Therefore by Serre's Theorem we see that almost all of the coefficients $a_t(n)$, in the Fourier expansion of $f_t(z)$, are even. Now, by multiplying (7) through by q, and replacing q by $q^{\frac{1}{24}}$, we get

$$\sum_{n\geq 0} a_t(n)q^n \equiv \left(\sum_{n=0}^{\infty} p(n)q^n\right)\left(\sum_{n=0}^{\infty} q^{2^j t(2n+1)^2}\right) \pmod{2}. \tag{10}$$

Now let us suppose that $p(n)$ is odd for all but finitely many $n \equiv r \pmod{t}$; in particular that $p(n)$ is odd for all $n \geq n_0$ with $n \equiv r \pmod{t}$. Then, comparing the coefficient of $q^{2^j tk^2+n}$ on both sides of (10) we find that

$$a_t(2^j tk^2 + n) \equiv \sum_{i\geq 1,\ i \text{ odd}} p(2^j t(k^2 - i^2) + n) \pmod{2}.$$

Note that each $2^j t(k^2 - i^2) + n \equiv n \equiv r \pmod{t}$. Now if $i \leq k$ then $2^j t(k^2 - i^2) + n \geq n \geq n_0$ so that $p(2^j t(k^2 - i^2) + n)$ is odd. If k is odd and $i > k > \frac{n}{2^{j+2}t} - 1$ then $2^j t(k^2 - i^2) + n < 0$ so that $p(2^j t(k^2 - i^2) + n) = 0$. Therefore, for such k, we have $a_t(2^j tk^2 + n) \equiv \frac{k+1}{2} \pmod{2}$. We have now proved that for all sufficiently large $k \equiv 1 \pmod{4}$ we have $a_t(n)$ odd for all $n \equiv r \pmod{t}$ in the interval $[2^j tk^2 + n_0, 2^j t(k+2)^2 + r - t]$ (assuming, without loss of generality that $0 \leq r \leq t-1$). By taking all such intervals into account we have a positive proportion of $a_t(n)$ with $n \equiv r \pmod{t}$ are odd, contradicting Corollary 1 to Serre's Theorem. □

4. The odd case

In this section we establish that there are infinitely many $M \equiv r \pmod{t}$ where $p(M)$ is odd provided that there is at least one M. To do this we prove a technical lemma about the reduction $\mod m$ of the Fourier expansions of holomorphic modular forms. The main result of this section follows as a consequence, for if there were only finitely many $M \equiv r \pmod{t}$ for which $p(M)$ is odd, then the reduction $\mod 2$ of the relevant modular form contradicts the lemma.

For a given positive integer m and formal power series $f := \sum_{n\in\mathbb{Z}} a(n)q^n$ with algebraic integer coefficients, we define $\mathrm{Ord}_m(f)$ to be the smallest integer n for which $a(n)$ is not divisible by m. A special case of a theorem of Sturm [22] allows us to computationally determine whether m divides $a(n)$ for every integer n (that is, to determine whether $\mathrm{Ord}_m(f) = \infty$).

Theorem 4. (Sturm) *Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(N)$ for some positive integer N with algebraic integer Fourier coefficients from a fixed number field. If m is a positive integer and*

$$\mathrm{Ord}_m(f) > \frac{k}{12}N^2 \prod_{p|N}(1 - \frac{1}{p^2}),$$

then $\mathrm{Ord}_m(f) = \infty$. (i.e. $a(n) \equiv 0 \mod m$ for all n)

Before proceeding to the crucial lemma about the reduction of a modular form $\mod m$, we first state a proposition concerning the solutions of Pell's equation that is used in the proof.

Proposition 2. *Let D be a positive integer and c a nonzero integer. Then the set of primes p such that there is an integral solution of the form $(x, 2p)$ to the Pell equation*

$$x^2 - Dy^2 = c$$

has density zero in the set of primes.

Proof. If D is a square, then the unique factorization of integers establishes that there are finitely many solutions (x, y); and hence only finitely many of the form $(x, 2p)$ where p is prime.

If D is not a square, then consider the ring of integers of $\mathbb{Q}(\sqrt{D})$. There are finitely many principal ideals with norm $\mid c \mid$, and pick a single generator α_i for each such ideal. Then every integer solution to $x^2 - Dy^2 = c$ is of the form

$$\pm\alpha_i(x_0 + \sqrt{D}y_0)^k$$

for some i and some integer k where (x_0, y_0) corresponds to the fundamental unit in $\mathbb{Q}(\sqrt{D})$. Since the solutions (x, y) grow exponentially with k, the set of primes p such that $(x, 2p)$ is a solution has density zero in the set of primes by the Prime Number Theorem. □

Now we prove the essential lemma about the reduction of a holomorphic modular form $\mod m$.

Lemma 1. *Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ where the coefficients $a(n)$ are algebraic integers in some number field. Let s and w be positive integers and $b_1, b_2, \dots b_s$ distinct non-zero integers. If m is a positive integer and*

$$f(z) \equiv \sum_{1 \le i \le s} \sum_{n=0}^{\infty} a_i(n) q^{w(2n+1)^2+b_i} \mod m$$

where $a_i(n) \not\equiv 0 \mod m$ for all $n \ge 0$, then $f(z)$ is not in $M_k(N)$ for any pair of positive integers k, and N.

Proof. Let k and N be positive integers and suppose that $f(z) \in M_k(N)$. We now analyze the action of the Hecke operators T_p on $f(z)$ and determine that the proposed congruence contradicts Sturm's theorem. The Hecke operators are linear transformations which preserve $S_k(N, \chi)$ and $M_k(N, \chi)$. If p is a rational prime and $F(z) = \sum_{n=0}^{\infty} A(n)q^n \in M_k(N, \chi)$, then the modular form $F(z) \mid T_p \in M_k(N, \chi)$ is defined by

$$F(z) \mid T_p = \sum_{n \ge 0} (A(pn) + \chi(p)p^{k-1}A(n/p))q^n. \tag{11}$$

Here $A(n/p) = 0$ if n/p is not an integer.

Now if $p \equiv 1 \mod N$ is prime, then the action of the Hecke operator T_p on $f(z)$ is well defined and is given by

$$f(z) \mid T_p = \sum_{n \ge 0} (a(pn) + p^{k-1}a(n/p))q^n \tag{12}$$

since $\chi(p) = 1$ for all Dirichlet characters $\chi \mod N$. Therefore throughout this proof we consider primes $p \equiv 1 \mod N$.

The contradiction to the proposed congruence is established by proving the existence of infinitely many primes p (although only one is needed) where

$$\frac{k}{12} N^2 \prod_{p \mid N} (1 - \frac{1}{p^2}) < \mathrm{Ord}_m(f(z) \mid T_p) < +\infty.$$

By Sturm's theorem the left inequality asserts that $f(z) \mid T_p \equiv 0 \mod m$ but the right inequality asserts that $f(z) \mid T_p \not\equiv 0 \mod m$; this is the contradiction.

Let $f_i(z) = \sum_{n=0}^{\infty} a_i(n)q^{w(2n+1)^2+b_i}$. So we find that

$$f(z) \equiv \sum_{1 \le i \le s} f_i(z) \mod m.$$

We first establish that $\mathrm{Ord}_m(f_i(z) \mid T_p)$ is unbounded over the primes $p \equiv 1 \mod N$. We now rename, for convenience, the Fourier expansions of $f_i(z)$ by $f_i(z) = \sum_{n=0}^{\infty} c_i(n)q^n$. Suppose there exists a constant C such that $\mathrm{Ord}_m(f_i(z) \mid T_p) < C$ for all such primes. If $p > C > n$, then $c_i(n/p) = 0$; thus if $\mathrm{Ord}_m(f_i(z) \mid T_p) = h < C$,

then by (12) we obtain $c_i(ph) \not\equiv 0 \mod m$. Therefore $ph = wn^2 + b_i$ for some positive odd integer n. This implies that

$$wn^2 + b_i \in \{0, p, 2p, \dots, (C-1)p\}. \tag{13}$$

For sufficiently large x, we now count the number of primes p in $(x, 2x]$ for which (13) holds. Since $p \leq 2x$ we find that $wn^2 + b_i < 2Cx$ and so $n < \sqrt{2Cx}$ for x sufficiently large. Now at most one prime $p > x$ divides an integer $< 2Cx$ if $x > 2C$. The number of primes p in $(x, 2x]$ is $\sim \frac{x}{logx}$ by Dirichlet's theorem. So for x sufficiently large we find that there are $\sim \frac{x}{\phi(N)logx}$ many primes $p \equiv 1 \mod N$ in $(x, 2x]$ where $\mathrm{Ord}_m(f_i(z) \mid T_p) > C$.

Given a constant $C > 0$, we now show that for almost all primes $p \equiv 1 \mod N$ where $\left(\frac{-b_i w}{p}\right) = 1$ that $C < \mathrm{Ord}_m(f_i(z) \mid T_p) < +\infty$. Let $n \leq p$ be the minimal positive odd integer where

$$wn^2 + b_i \equiv 0 \mod p.$$

By (12) the only way that

$$\mathrm{Ord}_m(f_i(z) \mid T_p) \neq \frac{wn^2 + b_i}{p}$$

is if there exists another positive odd integer l such that

$$\frac{wn^2 + b_i}{p} \geq p(wl^2 + b_i) > 0. \tag{14}$$

If p is sufficiently large, then since $n \leq p$ we find that

$$wp \geq p(wl^2 + b_i).$$

Moreover this forces $wl^2 + b_i \in \{1, 2, \dots w\}$. However if there exists a positive odd integer l for which

$$\frac{wn^2 + b_i}{p} > p(wl^2 + b_i), \tag{15}$$

then by (12) this would mean that

$$\mathrm{Ord}_m(f_i(z) \mid T_p) \in \{p, 2p, \dots, wp\}.$$

Therefore those primes p where there exists a positive odd integer l for which (15) holds have the property that

$$\mathrm{Ord}_m(f_i(z) \mid T_p) < +\infty. \tag{16}$$

Suppose that in (14) we have the equality

$$\frac{wn^2 + b_i}{p} = p(wl^2 + b_i).$$

Since $n \leq p$ we obtain

$$wl^2 + b_i = \frac{wn^2 + b_i}{p^2} \leq w + \frac{b_i}{p^2}. \tag{17}$$

If $b_i > 0$, then there are no such l.

If $b_i < 0$, then by (17) we find that $l = 1$ for all p sufficiently large. By letting $x = 2wn, y = 2p$, and $D = w(w + b_i)$ we find that this equality reduces to the Pell equation

$$x^2 - Dy^2 = -4wb_i. \tag{18}$$

By Proposition 2, we know that the set of primes where there exists a positive integer x such that $(x, 2p)$ is a solution to (18) has density zero. Therefore we can now conclude that for almost all primes $p \equiv 1 \mod N$ where $\left(\frac{-b_i w}{p}\right) = 1$ that

$$\mathrm{Ord}_m(f_i(z) \mid T_p) < +\infty.$$

Combining this with our earlier observation we obtain that for any constant C, that for x sufficiently large there are $\sim \frac{x}{2\phi(N)logx}$ many primes $p \equiv 1 \mod N$ in $(x, 2x]$ with $\left(\frac{-b_i w}{p}\right) = 1$ such that

$$C < \mathrm{Ord}_m(f_i(z) \mid T_p) < +\infty. \tag{19}$$

Now we apply these results to describe the behavior of $\mathrm{Ord}_m(f(z) \mid T_p)$. If $1 \leq i \neq j \leq s$, then there are only finitely many n such that $c_i(n)$ and $c_j(n)$ are both non-zero mod m. To see this we only need to note that this occurs precisely when there exists positive odd integers l and n such that $wn^2 + b_i = wl^2 + b_j$ which reduces to

$$w(l + n)(l - n) = b_i - b_j.$$

Given w, b_i, and b_j, there are only finitely many solutions l and n (if any). As a consequence, for all but finitely many primes $p \equiv 1 \mod N$, we obtain

$$\mathrm{Ord}_m(f(z) \mid T_p) = \min\{\mathrm{Ord}_m(f_i(z) \mid T_p) \mid 1 \leq i \leq s\}. \tag{20}$$

By (19), (20) and Dirichlet's theorem again, there are infinitely many primes $p \equiv 1 \mod N$ such that

$$\frac{k}{12}N^2 \prod_{p|N}(1 - \frac{1}{p^2}) < \mathrm{Ord}_m(f(z) \mid T_p) < +\infty.$$

This contradicts Sturm's theorem.

□

In the next lemma we use the orthogonality relations of Dirichlet characters to show that the restriction of the Fourier expansion of a modular form to those terms whose powers of q are in a fixed arithmetic progression is a modular form.

Lemma 2. *Let $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ be a modular form in $M_k(N, \chi)$ and let $d := \gcd(r, t)$. If $0 \le r < t$, then*

$$f_{r,t}(z) = \sum_{n \equiv r \mod t} a(n)q^n$$

is the Fourier expansion of a modular form in $M_k\left(\frac{Nt^2}{d}\right)$.

Proof. First we recall the orthogonality relations for Dirichlet characters. If a and b are any pair of integers where $\gcd(b, N) = 1$, then

$$\sum_{\chi \mod N} \chi(a)\overline{\chi(b)} = \begin{cases} \phi(N) & \text{if } a \equiv b \mod N \\ 0 & \text{otherwise.} \end{cases}$$

Here ϕ is Euler's function and the sum is over all Dirichlet characters $\mod N$.

Now we cite basic facts concerning the *twisting* of modular forms by Dirichlet characters [15]. Let ϵ be a Dirichlet character $\mod M$. If $f(z) = \sum_{n \ge 0} a(n)q^n \in M_k(N, \chi)$, then define $f_\epsilon(z)$ by

$$f_\epsilon(z) = \sum_{n \ge 0} \epsilon(n)a(n)q^n.$$

Then $f_\epsilon(z) \in M_k(NM^2, \epsilon^2\chi)$.

If $\gcd(r, t) = 1$, then define $f_{r,t}(z)$ by

$$f_{r,t}(z) = \frac{1}{\phi(t)} \sum_{\epsilon \mod t} \epsilon(r) f_{\overline{\epsilon}}(z).$$

Here the sum is over all Dirichlet characters $\epsilon \mod t$. The Fourier expansion of $f_{r,t}(z)$ is

$$f_{r,t}(z) = \frac{1}{\phi(t)} \sum_{n=0}^{\infty} \sum_{\epsilon \mod t} \epsilon(r)\overline{\epsilon(n)}a(n)q^n.$$

So the coefficient of q^n in $f_{r,t}(z)$ is $a(n)$ if $n \equiv r \mod t$ and 0 otherwise. Therefore we obtain

$$f_{r,t}(z) = \sum_{n \equiv r \mod t} a(n)q^n.$$

Since each $f_\epsilon(z)$ is a modular form of weight k with respect to $\Gamma_1(Nt^2)$ and since the sum of any two such forms is also a modular form of weight k with respect to $\Gamma_1(Nt^2)$, we find that $f_{r,t}(z) \in M_k(Nt^2)$.

Now suppose that $1 < d = \gcd(t, r)$. Then let $f_d(z) := f(z)|T_d := \sum_{n \ge 0} a(dn)q^n$, also a modular form in $M_k(N, \chi)$. By replacing z by dz, we obtain a new modular form

$$F(z) := f_d(dz) = \sum_{n \ge 0} a(dn)q^{dn}$$

with respect to $\Gamma_0(dN)$. Now to isolate those terms whose powers of q belong to the arithmetic progression $r \mod t$ we apply the orthogonality relations again using Dirichlet characters $\mod \frac{t}{d}$. To isolate the class $r \mod t$, we simply define

$$f_{r,t}(z) := \frac{1}{\phi\left(\frac{t}{d}\right)} \sum_{\epsilon \mod \frac{t}{d}} \epsilon(r) F_{\overline{\epsilon}}(z).$$

Here the sum is over all Dirichlet characters $\epsilon \mod \frac{t}{d}$. The Fourier expansion of $f_{r,t}(z)$ is:

$$f_{r,t}(z) = \sum_{n \equiv r \mod t} a(n) q^n.$$

By the theory of twists we find that $f_{r,t}(z) \in M_k\left(\frac{Nt^2}{d}\right)$. This completes the proof of this Lemma.

□

We now combine these facts to establish the main theorem of this section.

Main Theorem 2. *For any arithmetic progression $r(\mod t)$, 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*

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

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

Proof. Recall from Proposition 1 that

$$f_t(z) := \frac{\eta(24z)}{\eta(48z)} \Delta^{2^j}(24tz) = \sum_{n \geq 1} a_t(n) q^{24n-1} \in S_{2^j \cdot 12}(1152t, \chi).$$

and

$$f_t(z) \equiv \sum_{n=0}^{\infty} p(n) q^{24n-1} \sum_{n=0}^{\infty} q^{24 \cdot 2^j t(2n+1)^2} \mod 2.$$

Let $d := \gcd(24r-1, t)$. Therefore by Lemma 2 we define

$$f_{24r-1,24t}(z) = \sum_{n \equiv 24r-1 \mod 24t} a_t(n) q^n \in S_{2^j \cdot 12}\left(\frac{2^{13} \cdot 3^4 t^3}{d}\right),$$

which when reduced $\mod 2$ is:

$$f_{24r-1,24t}(z) \equiv \sum_{n \equiv r \mod t} p(n) q^{24n-1} \sum_{n=0}^{\infty} q^{24 \cdot 2^j t(2n+1)^2} \mod 2. \tag{21}$$

Note that the arithmetic progression $r \mod t$ corresponds to the arithmetic progression $24r-1 \mod 24t$. If $p(M)$ is odd for at least one $M \equiv r \pmod t$ but only finitely

many, then the $\mod 2$ factorization in (21) contradicts Lemma 1. This proves that if $p(M)$ is odd for at least one $M \equiv r \pmod t$, then $p(M)$ is odd for infinitely many such M.

Now we prove the second part of the theorem. Assume that $p(M)$ is even for all $M \equiv r \pmod t$ where $0 \le M \le C_{r,t}$. Then it is easy to see that this implies that $p(M)$ is even for all $M \equiv r \pmod t$ where

$$r \le M \le \frac{2^{23+j} \cdot 3^7 t^6}{d^2} \prod_{p|6t} \left(1 - \frac{1}{p^2}\right) - 2^j t + r.$$

Since the exponent associated with $p(M)$ is $24M - 1$, the first exponent in the left factor of the product (19) which cannot vanish $\mod 2$ is

$$\frac{2^j \cdot 12}{12} \left[\frac{2^{13} \cdot 3^4 t^3}{d}\right]^2 \prod_{p|6t} \left(1 - \frac{1}{p^2}\right) - 24 \cdot 2^j t + 24r - 1 + 24t.$$

Thus since the first exponent in the right hand factor of (19) is $24 \cdot 2^j t$, we find that

$$\mathrm{Ord}_2(f_{24r-1,24t}(z)) \ge \frac{2^j \cdot 12}{12} \left[\frac{2^{13} \cdot 3^4 t^3}{d}\right]^2 \prod_{p|6t} \left(1 - \frac{1}{p^2}\right) + 24(t + r) - 1.$$

By Sturm's theorem this forces $f_{24r-1,24t}(z) \equiv 0 \mod 2$. By Main Theorem 1, this means that $p(M)$ is even for all $M \equiv r \pmod t$.

□

This theorem proves that if $0 \le r < t$, then if $p(M)$ is ever odd for an $M \equiv r \pmod t$ (hence infinitely often), the first odd value must occur where $M < C_{r,t}$. It is easy to verify that $C_{r,t} < 10^{10} t^7$ since $\frac{t}{12} > 2^j$ when we choose the minimal j such that $2^j > \frac{t}{24}$. As a consequence of the two main theorems we verified the conjecture for lots of arithmetic progressions. By computing $p(n) \mod 2$ for all $n \le 5,000,000$ we obtain:

Main Corollary. *For all $0 \le r < t \le 10^5$, 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.*

5. Acknowledgements

I am indebted Ken T. Burrell (Universal Analytics, Inc.) whose computations are the content of the Main Corollary. The computations were completed on a CRAY C-90 at the San Diego Supercomputing Center. I am indebted to Andrew Granville whose suggestions dramatically clarified and improved the content of this paper. I also thank Bruce Berndt and Brad Wilson for previewing preliminary versions of this paper.

References

1. G. Andrews, *The Theory of Partitions*, Addison-Wesley, 1976.
2. G. Andrews and F. Garvan, *Dyson's crank of a partition*, Bull. Am. Math. Soc. **18** (1988), 167-171.
3. A.O.L. Atkin, *Proof of a conjecture of Ramanujan*, Glasgow Math. J. **8** (1967), 14-32.
4. F. Garvan, *A simple proof of Watson's partition congruence for powers of 7*, J. Australian Math. Soc. (A) **36** (1984), 316-334.
5. F. Garvan, *New combinatorial interpretations of Ramanujan's partition congruences* mod *5, 7 and* 11, Trans. Am. Math. Soc. **305** (1988), 47-77.
6. F. Garvan and D. Stanton, *Sieved partition functions and $q-$binomial coefficients*, Math. Comp. **55 191** (1990), 299-311.
7. F. Garvan and D. Stanton, *Cranks and $t-$cores*, Invent. Math. **101** (1990), 1-17.
8. B. Gordon and K. Hughes, *Multiplicative properties of $\eta-$products II*, A tribute to Emil Grosswald: Number Theory and related analysis, Cont. Math. **143** (1993), Amer. Math. Soc., 415-430.
9. M. Hirschhorn, *On the residue mod 2 and mod 4 of $p(n)$*, Acta Arithmetica **38** (1980), 105-109.
10. ———, *On the parity of $p(n)$ II*, J. Combin. Theory (A) **62** (1993), 128-138.
11. ———, *Ramanujan's partition congruences*, Discrete Math. **131** (1994), 351-355.
12. M. Hirschhorn and D.C. Hunt, *A simple proof of the Ramanujan conjecture for powers of* 5, J. Reine Angew. Math. **336** (1981), 1-17.
13. M. Hirschhorn and M. Subbarao, *On the parity of $p(n)$*, Acta Arith. **50 4** (1988), 355-356.
14. M. Knopp, *Modular functions in analytic number theory*, Markham, 1970.
15. N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, 1984.
16. O. Kolberg, *Note on the parity of the partition function*, Math. Scand. **7** (1959), 377-378.
17. G. Ligozat, *Courbes modulaires de genre 1*, Bull. Soc. Math. France [Memoire 43] (1972), 1-80.
18. M. Newman, *Construction and application of a certain class of modular functions*, Proc. London Math. Soc. (3) **7** (1956), 334-350.
19. M. Newman, *Construction and application of a certain class of modular functions II*, Proc. London Math. Soc. (3) **9** (1959), 373-387.
20. T. R. Parkin and D. Shanks, *On the distribution of parity in the partition function*, Math. Comp. **21** (1967), 466-480.
21. J.-P. Serre, *Divisibilité des coefficients des formes modulaires de poids entier*, C.R. Acad. Sci. Paris (A) **279** (1974), 679-682.
22. J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes **1240** (1984), Springer-Verlag.
23. M. Subbarao, *Some remarks on the partition function*, Amer. Math. Monthly **73** (1966), 851-854.
24. G.N. Watson, *Ramanujan's vermutung über zerfällungsanzahlen*, J. Reine Angew. Math. vol 179 (1938), 97-128.

Department of Mathematics, The University of Illinois, Urbana, Illinois 61801

Current address: School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540

E-mail address: ono@symcom.math.uiuc.edu