EXPOSITIONES MATHEMATICAE

Expo. Math. 19 (2001): 193–211

www.urbanfischer.de/journals/expomath

Partition Function Congruences: Some Flowers and Seeds from 'Ramanujan's Garden'

Sukumar Das Adhikari, Anirban Mukhopadhyay

Harish-Chandra Research Institute (Formerly, Mehta Research Institute),
Chhatnag Road, Jhusi, Allahabad 211 019, India

"The seeds from Ramanujan's garden have been blowing on the wind and have been sprouting all over the landscape". – FREEMAN J. DYSON

Abstract

The discovery of some partition function congruences by Ramanujan, and subsequent research motivated by these congruences as well as some of his questions and conjectures, have brought forth a beautiful bower in 'Ramanujan's Garden'.

In this short expository article, starting from Ramanujan's pioneering work in this area, we have some glimpses of contributions of many of the later researchers like Atkin, Watson, Newman, Winquist, Zuckerman, Dyson, Andrews, Garvan, Schinzel, Wirsing, Nicolas, Ruzsa, Sárközy, Serre, Berndt and Ono. While we dwell mainly on the question of parity of $p(n)$ and related topics, we try to mention other important achievements in the area.

1. Introduction. The *partition function* $p(n)$ is defined as follows. For a positive integer n, $p(n)$ is the number of partitions of n into positive integral parts. Here, in a partition, the parts are not necessarily distinct and the order in which the parts are arranged is irrelevant.

In our discussions, $q(n)$ will denote the number of partitions of n into distinct parts. The domain of definitions of the functions $p(n)$ and $q(n)$ are extended by defining

$$p(0) = q(0) = 1,\ p(-1) = q(-1) = p(-2) = q(-2) = \cdots = 0.$$

E-mail addresses: adhikari@mri.ernet.in
anirban@mri.ernet.in

0732-0869/01/19/3-193 $15.00/0

From MacMahon's table for $p(n)$ for $1 \leq n \leq 200$, Ramanujan conjectured [39] the following congruence properties of $p(n)$:

If $24m \equiv 1 \pmod{5^a 7^b 11^c}$, *then*

$$p(m) \equiv 0 \pmod{5^a 7^b 11^c}. \tag{1}$$

In the same paper [39], Ramanujan proved the particular cases:

$$p(5n+4) \equiv 0 \pmod{5}, \tag{2}$$

and

$$p(7n+5) \equiv 0 \pmod{7}. \tag{3}$$

Later, in a posthumous paper [41], prepared by Hardy with materials extracted from Ramnujan's manuscript [42], along with new proofs of (2) and (3), the proof of the following congruence appeared:

$$p(11n+6) \equiv 0 \pmod{11}. \tag{4}$$

We shall come back to [42] and the recent article [9] of Berndt and Ono which provides clarifications, corrections and a highly valuable commentary on [42].

From extended tables of $p(n)$ computed by H. Gupta, it was observed by Chowla [10] in 1934 that $p(243)$ is not divisible by 7^3, although we have $24.243 \equiv 1 \pmod{7^3}$.

Therefore, Ramanujan's conjecture (1) was suitably modified by Watson as follows:

If $24m \equiv 1 \pmod{5^a 7^b 11^c}$, *then*

$$p(m) \equiv 0 \pmod{5^a 7^\beta 11^c}, \tag{5}$$

where β *is the integral part of* $\frac{b+2}{2}$.

In Section 2, we shall briefly sketch the history of the proof of (5) and discovery of further congruences. After that, in Section 3, we shall come to the main theme of this expository article, namely, the question of parity of $p(n)$ and the related topics.

Acknowledgements. We would like to thank Professor Bruce C. Berndt for going through an earlier version of the manuscript and providing some valuable informations. We also thank Professor Ken Ono for making some of his unpublished manuscripts available to us.

2. History of the proof of (5) and discovery of further congruences. In the paper [39] mentioned before, Ramanujan had also proved the congruences:

$$p(25n+24) \equiv 0 \pmod{25}, \tag{6}$$

and

$$p(49n+47) \equiv 0 \pmod{49}. \tag{7}$$

Watson [47] proved (5) for arbitrary powers of 5 and 7; his proof for powers of 5 is identical to that sketched by Ramanujan in his unpublished manuscript [42]. As pointed out by Berndt and Ono [9], Watson (as had been confirmed by Rushforth [43]) had a copy of [42]. Therefore, though Watson [47] does not explicitly mention Part II of Ramanujan's unpublished manuscript [42] which contains Ramanujan's proof of his congruence for $p(n)$ modulo any positive integral power of 5, Watson just expanded Ramanujan's idea into a more detailed proof. Regarding the congruence modulo powers of 7, it has been explained in [9]:

"*Clearly, Ramanujan intended to follow the same lines of attack for powers of 7 as he did for powers of 5 in Sections 20-23. If he had completed his argument, he would have undoubtedly seen that his original conjecture modulo powers of 7 needed to be corrected. Most likely, his declining health prevented him from working out the remaining details, which were completed by Watson* [47]".

In the unpublished manuscript [42], Ramanujan indicates some line of proof for the congruence

$$p(121n-5) \equiv 0 \pmod{121}. \tag{8}$$

This was later completed by Rushforth [43], though not exactly in the same way. Following Rademacher, Lehner [27] [28] developed an essentially different method than that of Ramanujan - Watson and in particular proved (5) for 11^3. For 11^3 and 11^4, Lehmer [25] [26] had already proved (5). Later, it was Atkin [4] who first proved (5) for 11^n for all positive integers n.

The literature on congruences of partition functions modulo powers of $5, 7$ and 11 is extensive. We do not attempt to give a complete bibliography. However, we mention few papers of interest. The congruence modulo 11 was considered more difficult than the ones corresponding to 5 and 7. In 1969, Winquist [49] published an elementary proof of $p(11n+6) \equiv 0 \pmod{11}$.

Very recently Hirschhorn [21], following the works of Gravan and Stanton [18] and Gravan, Kim and Stanton [17], gave a simplified version of a uniform proof of all three congruences

$$p(5n+4) \equiv 0 \pmod 5, \; p(7n+5) \equiv 0 \pmod 7, \; p(11n+6) \equiv 0 \pmod{11}.$$

In 1981, Hirschhorn and Hunt [22] provided a simple proof of (5) for powers of 5. Later, a proof in the same vein for powers of 7 was given by Garvan [15].

In another direction, Ramanujan's congruence $p(5n+4) \equiv 0 \pmod 5$ (and the corresponding ones modulo 7 and 11) raised a question in the mind of Freeman J. Dyson. He was sure that the partitions of $(5n+4)$ must be divisible into five classes with the same number of partitions in each class. Soon he found [11] a criterion. For each partition he defined *rank* to be the greatest part minus the number of parts. He proposed [11] that the value of the rank read mod 5 splits the set of partitions of $(5n+4)$ into five equal classes. He also conjectured that similar splitting holds for partitions of $(7n+5)$. In 1953, Atkin and Swinnerton-Dyer [8] proved these conjectures, thereby providing new proofs of (2) and (3). A quote from an article [12] of Dyson will be appropriate at this juncture:

" *The proof which Oliver and Peter constructed is a great work of art, in the best Ramanujan tradition. ⋯ As Frank Garvan noticed thirty years later, Atkin and Swinnerton-Dyer had rediscovered for the purposes of their proof several of the striking mock-theta-function identities which were in 1953 lying buried in Ramanujan's lost notebook*".

Regarding the congruence $p(11n+6) \equiv 0 \pmod{11}$, however, Dyson [11] observed that the rank did not separate the partitions of $(11n+6)$ into 11 equal classes. But he went on to conjecture the existence of another 'partition statistic' (which he called *crank*), which would provide a combinatorial interpretation of the congruence $p(11n+6) \equiv 0 \pmod{11}$. In 1987, the day after the Ramanujan Centenary Conference at University of Illinois at Urbana-Champaign ended, Andrews and Garvan [16] [3] came out with the definition of the crank.

Now, we come to the discussion about congruences of partition functions other than those given by (5). We shall also touch upon some related questions. Atkin [5] [6] and Atkin and O' Brien [7] obtained new partition congrences like:

$$p(11^3 \cdot 13n + 237) \equiv 0 \pmod{13},$$
$$p(23^3 \cdot 17n + 2623) \equiv 0 \pmod{17},$$
$$p(59^4 \cdot 13n + 111247) \equiv 0 \pmod{13}.$$

Coming back to congruence modulo small primes, for instance, regarding congruence mod 5, a natural question arises:

'How many' more integers N other than those of the type $5n + 4$ satisfy $p(N) \equiv 0 \pmod 5$.

In an answer to this question, Newman [33] proved that the lower natural density of positive integers N satisfying $p(N) \equiv 0 \pmod 5$ is strictly greater than $1/5$. To prove this, Newman [33] exhibited arithmetic progressions, disjoint from $5n + 4$, on which $p(N)$ vanishes modulo 5. In particular, he shows that

$$p(5 \cdot 19^3 n + 22006) \equiv 0 \pmod 5, \quad n \not\equiv 3 \pmod{19}$$

$$p(5 \cdot 19^3 n + 15147) \equiv 0 \pmod 5 \quad n \not\equiv 7 \pmod{19}.$$

This is in contrast with the expectation (see the next section) regarding the distribution of positive integers N such that $p(N)$ is even.

A related conjecture by Erdős and Ivić [13] says that:

Conjecture 2.1. (Erdős and Ivić) *There are infinitely many primes P such that for each of them, there is a positive integer $N = N(P)$ such that P divides $p(N)$.*

Erdős, in private comunications (see [37]) made the following stronger conjecture:

Conjecture 2.2. (Erdős) *For each prime P, there is a positive integer $N = N(P)$ such that P divides $p(N)$.*

Using Hardy-Ramanujan-Rademacher asymptotic formula for $p(n)$, Schinzel (see [13]) proved Conjecture 2.1. Later, Schinzel and Wirsing [44] made progress towards Conjecture 2.2.

From a recent work of Ono [37], it follows that

Theorem 2.1. (Ono) *For every prime $P \geq 5$, there is a constant $C(P) > 0$ such that*

$$|\{0 < n \leq X : p(n) \equiv 0 \pmod P\}| > C(P)X.$$

Since $p(2) = 2$ and $p(3) = 3$, by the above result Conjecture 2.2 is established.

In view of the known results regarding the parity of $p(n)$, which will be discussed in the next section, regarding Conjecture 2.2, only in the case of the prime 3, it is not known whether there are infinitely many n for which $p(n) \equiv 0 \pmod 3$.

We end this section with a short discussion on the following conjecture of Newman [31]:

Conjecture 2.3. (Newman) *For any positive integer m, for every residue class $r \pmod m$, there are infinitely many nonnegative integers n for which $p(n) = r \pmod m$.*

Atkin, Newman and Kolberg [5] [31] [32] [24] verified the conjecture for $m = 2, 5, 7, 13$ and 65.

From the above mentioned work of Ono [37], it follows that

Theorem 2.2. (Ono) *Conjecture 2.3 is true for every prime $P < 1000$ with the possible exception of $P = 3$.*

3. The question of parity of $p(n)$ and related topics. The parity of $p(n)$ seems to be quite random. In a letter to MacMahon [29], Ramanujan wanted to know some simple way of ascertaining whether $p(1000)$ is odd or even. Even though MacMahon [29] did find out the answer after about a year, Ramanujan was not alive to see the answer. As we see from his unpublished manuscript [42] (see also [9]), the observation that $p(n)$ is odd for 110 values of n not exceeding 200, made Ramanujan think that $p(n)$ is odd more often than it is even. More extensive calculations supports the 'Folklore Conjecture' [38] that the number of $n \leq x$ for which $p(n)$ is even is $\sim \frac{1}{2}x$. In other words, it is believed that the partition function takes odd and even values 'equally often'. We do not know whether Ramanujan himself had a doubt about what is suggested by the knowledge of parity of the first 200 integers and wanted to have informations about the parity of more numbers (as is evident from his letter to MacMahon) to have a better idea. Ramanujan also had conjectures on the distribution of $p(n)$ modulo $5, 7, 11$ and 3 in the unpublished manuscript [42]. Berndt and Ono examines these conjectures in detail in Section 11 of their commentary in [9].

Regarding the question of parity of $p(n)$, in the paper [29], which we have already mentioned, MacMahon gave an algorithm for determining the parity of $p(n)$.

Later, in 1959, Kolberg [24] proved

Theorem 3.1. **(Kolberg)** *For $n \geq 1$, $p(n)$ assumes both even and odd values infinitely often.*

Proof. Kolberg's proof [24] of Theorem 3.1 is based on Euler's identity (for a proof of a version of the identity, see [19], for instance):

$$p(n) + \sum_{k \geq 1} (-1)^k \left(p(n - s_k) + p(n - t_k) \right) = 0, \tag{9}$$

where

$$s_k = \frac{1}{2}k(3k-1),\ t_k = \frac{1}{2}k(3k+1) \tag{10}$$

and the summation extends over all non-negative arguments of the partition function.

Reading modulo 2, from the above identity (9) we have:

$$p(n) + \sum_{k \geq 1} \left(p(n - s_k) + p(n - t_k) \right) \equiv 0 \pmod 2. \tag{11}$$

Now suppose that for some positive integer a, $p(n)$ is even for all $n \geq a$. Taking $n = \frac{1}{2}a(3a-1)$, from (11) we have

$$p\left(\frac{1}{2}a(3a-1)\right) + p\left(\frac{1}{2}a(3a-1) - 1\right) + \cdots + p(2a-1) + p(0) \equiv 0 \pmod 2.$$

Since $p(0) = 1$ and all the remaining terms in the above are even by our assumption, we get a contradiction. Therefore, $p(n)$ takes odd values infinitely often.

Similarly, supposing that for some positive integer b, $p(n)$ is odd for all $n \geq b$, taking $n = \frac{1}{2}b(3b+1)$, from (11) we see that the left hand side contains an odd number of odd terms and we arrive at a contradiction.

Later, different proofs for Kolberg's result were given by Newman [31] and Fabrykowski and Subbarao [14]. Also, unaware of Kolberg's paper (Makowski brought it to the Editor's notice), J. H. van Lint [46] also gave a proof similar to Kolberg's as a solution to Advanced problem No. 4944 (**76**, 1961) proposed by Newman in American Math. Monthly.

While the proof of Fabrykowski and Subbarao [14] depends on a recursion formula analogous to (9), the proof by Newman [31] goes as follows.

Newman observes that

Lemma 3.1. *If a sequence of integers $T = \{t_n\}$, $n \geq 0$ is ultimately periodic modulo a positive integer m, then the formal power series $f(x) = \sum_{n=0}^{\infty} t_n x^n$ is congruent modulo m to a quotient of polynomials with integral coefficients, the denominator having constant term* 1. (Here by congruence of $f(x)$ modulo m, it is understood that the coefficients of the corresponding powers of x are congruent modulo m.)

Proof. If T is ultimately periodic modulo m, then there exist two polynomials $\alpha(x)$ and $\beta(x)$ with integral coefficients and a positive integer d such that

$$f(x) \equiv \alpha(x) + \beta(x) + x^d\beta(x) + x^{2d}\beta(x) + \cdots \pmod{m}.$$

Therefore,

$$f(x) \equiv \frac{\alpha(x)(1-x^d) + \beta(x)}{1-x^d} \pmod{m}.$$

Remark. In fact, the converse of the above lemma is also true and Newman's paper [31] supplies a simple proof of this converse as well. However, we shall not need the converse for our purpose.

We now state another result of Newman [31] which is very interesting on its own.

Lemma 3.2. *Let*

$$f(x) = \sum_{n=0}^{\infty} c_n x^{d_n}, \quad 0 \leq c_0 < c_1 < c_2 < \cdots,$$

be a power series with integral coefficients and exponents such that

$$d_{n+1} - d_n \to \infty \tag{12}$$

and

$$\gcd(c_n, c_{n+1}, \cdots) = 1, \quad \text{for all } n \geq 0. \tag{13}$$

Then there do not exist two polynomials $\alpha(x)$ and $\beta(x)$ with integral coefficients such that $\alpha(0) = 1$ and

$$f(x) \equiv \frac{\beta(x)}{\alpha(x)} \pmod{m} \quad \text{for some integer } m > 1.$$

Before proceeding for the proof of Lemma 3.2, we deduce Theorem 3.1 from it. From Lemma 3.2, we observe that in particular,

$$\phi(x) \stackrel{\text{def}}{=} \prod_{n=0}^{\infty}(1-x^n) = 1 + \sum_{k=1}^{\infty}(-1)^k \left(x^{\frac{1}{2}k(3k-1)} + x^{\frac{1}{2}k(3k+1)}\right)$$

(and hence $1/\phi(x)$, the generating function of $p(n)$) is never congruent to modulo m to a quotient of the type $\beta(x)/\alpha(x)$, where $\alpha(x)$ and $\beta(x)$ are polynomials with integral coefficients and $\alpha(0) = 1$.

Therefore, by Lemma 3.1, it can not happen that for some integer m_0, $p(n)$ is even for all $n \geq m_0$ or odd for all $n \geq m_0$.

Proof of Lemma 3.2. Let

$$\alpha(x) = \sum_{n=0}^{r} a_n x^n, \qquad a_0 = 1,$$

and

$$\beta(x) = \sum_{n=0}^{s} b_n x^n.$$

Now, for an integer $m > 1$,

$$\alpha(x)f(x) \equiv \beta(x) \pmod{m}$$

implies that

$$\sum_{d_k \leq n} c_k a_{n-d_k} \equiv b_n \pmod{m}.$$

Replacing n by d_n in the above, we have

$$\sum_{k=0}^{n} c_k a_{d_n-d_k} = c_n + \sum_{k=0}^{n-1} c_k a_{d_n-d_k} \equiv b_{d_n} \pmod{m}. \tag{14}$$

By given condition (12), we can choose n_0 so large such that for all $n \geq n_0$, $d_n - d_{n-1} > r$, $d_n > s$. Then (14) implies that for all $n \geq n_0$,

$$c_n \equiv 0 \pmod{m}.$$

This contradicts (13), since $m > 1$. This proves Lemma 3.2.

By a more effective exploitation of Kolberg's idea [24], Mirsky [30] obtained a two-fold improvement of Kolberg's result. Mirsky's result not only quantifies Kolberg's result, it generalizes the result for congruences for general modulus.

For $q \geq 2$, $0 \leq r < q$, writing $E_{r,q}(N)$ to denote the number of positive integers $n \leq N$ such that $p(n) \equiv r \pmod q$, Mirsky [30] shows that for each $q \geq 2$, and $N > N_0(q)$, there exist at least two distinct values $r_1 = r_1(N)$, $r_2 = r_2(N)$ depending on N with $0 \leq r_1 < r_2 < q$ such that

$$\min\ (E_{r_1,q}(N), E_{r_2,q}(N)) > \frac{\log\log N}{q\log 2}. \tag{15}$$

In the particular case $q = 2$, the quantitative result given by (15) on the frequency of the odd values and even values of $p(n)$ has been improved by Nicolas and Sárközy [35] and Nicolas, Ruzsa and Sárközy [34]. As in Kolberg [24] and Mirsky [30], the starting point in [35] and [34] is Euler's identity (9).

In [35], the following was proved

Theorem 3.2. **(Nicolas and Sárközy)** *There are constants $c > 0$, $d > 0$ such that for $N > N_0$,*

$$\min(E_{0,2}(N), E_{1,2}(N)) > d(\log N)^c.$$

Later, in [34] the result in Theorem 3.2 was further improved. More precisely, the following theorems were proved in [34].

Theorem 3.3. **(Nicolas, Ruzsa and Sárközy)** *There is a constant $C_1 > 0$ and a positive integer N_0 such that for $N > N_0$, there are at least $C_1 N^{1/2}$ integers $n \leq N$ such that $p(n)$ is even.*

Theorem 3.4. **(Nicolas, Ruzsa and Sárközy)** *For each $\epsilon > 0$, there is a positive integer $N_1 = N_1(\epsilon)$ such that if $N > N_1$ then there are at least $N^{1/2}\exp(-(\log 2+\epsilon)\log N/\log\log N)$ integers $n \leq N$ such that $p(n)$ is odd.*

Proof of Theorem 3.3. We start with Euler's identity (9). Consider the set

$$\mathcal{M}_n \stackrel{\text{def}}{=} \{n\} \cup \{n - s_k : 1 \leq s_k \leq n\} \cup \{n - t_k : 1 \leq t_k \leq n\}.$$

From (9),

$$\sum_{m \in \mathcal{M}_n} p(m) \equiv 0 \pmod{2}.$$

Therefore, if $|\mathcal{M}_n|$ is odd, then there is at least one $m \in \mathcal{M}_n$ for which $p(m)$ is even.

Now, observing the sequence $n > n - s_1 > n - t_1 > n - s_2 > \cdots$, $|\mathcal{M}_n|$ is odd if and only if n is in an interval of type $[t_j, s_{j+1})$.

Therefore,

$$|\{(m,n) : n \leq N, m \in \mathcal{M}_n, p(m) \equiv 0 \pmod{2}\}| > c'N$$

for some positive constant c'.

For a fixed m, the number of integers n of the form $m + t_j$ or $m + s_j$ is at most the number of j's satisfying $t_j \leq N$ or $s_j \leq N$ which is, clearly, $\leq c''N^{1/2}$ for some positive constant c''.

Thus there are at least $c'N/c''N^{1/2} = C_1 N^{1/2}$ distinct values of $m \leq N$ for which $p(m)$ is even.

Proof of Theorem 3.4. First, we make the following claim:

Claim. *For each $\epsilon > 0$, there is a positive integer $N_1 = N_1(\epsilon)$ such that if $N > N_1$ then there are at least $N^{1/2}\exp(-(\log 2+\epsilon)\log N/\log\log N)$ integers $n \leq N$ such that*

$$p(n) \not\equiv p(n-1) \pmod{2}.$$

We define

$$g(n) = \begin{cases} 1, & \text{if } p(n) \not\equiv p(n-1) \pmod{2} \\ 0, & \text{if } p(n) \equiv p(n-1) \pmod{2}. \end{cases}$$

Further, let

$$G(N) \stackrel{\text{def}}{=} \sum_{n=1}^{N} g(n).$$

Once the above claim is established, we have

$$G(N) > N^{1/2}\exp(-(\log 2 + \epsilon/2)\log N/\log\log N) \quad \text{for} \quad N > N_1. \tag{16}$$

Now, $g(n) = 1$ if and only if one of the $p(n)$ and $p(n-1)$ is odd and the other one is even and this is so if and only if $E_{i,2}(n) - E_{i,2}(n-2) = 1$ for both $i = 0$ and 1.

Therefore, for both $i = 0$ and 1 we have, $G(N)$

$$\begin{aligned}
&= \sum_{m=1}^{[N/2]} g(2m) + \sum_{m=1}^{[(N+1)/2]} g(2m-1) \\
&\leq \sum_{n=1}^{[N/2]} (E_{i,2}(2m) - E_{i,2}(2m-2)) + \sum_{n=1}^{[(N+1)/2]} (E_{i,2}(2m-1) - E_{i,2}(2m-3)) \\
&= (E_{i,2}(2[N/2]) - E_{i,2}(0)) + (E_{i,2}(2[(N+1)/2]) - E_{i,2}(-1)) \\
&\leq 2E_{i,2}(N).
\end{aligned}$$

This together with (16) implies Theorem 3.4.

Now, we proceed to prove our claim.

Proof of the claim. Defining $f(n) = p(n) - p(n-1)$, as in the proof of Theorem 3.3, from Euler's identity (9) we obtain

$$\sum_{m \in \mathcal{M}_n} f(m) \equiv 0 \pmod 2,$$

for any integer $n \geq 1$, where, as before,

$$\mathcal{M}_n \stackrel{\text{def}}{=} \{n\} \cup \{n - s_k : 1 \leq s_k \leq n\} \cup \{n - t_k : 1 \leq t_k \leq n\}.$$

Now, if we take n to be of the form s_k or t_k, then $0 \in \mathcal{M}_n$ and since $f(0) = 1$, the set $\{m : m \in \mathcal{M}_n, f(m) \equiv 1 \pmod 2\}$ must have at least one further element.

But there are at least $C_2 N^{1/2}$ numbers $\leq N$, which are of the form t_k or s_k where C_2 is a positive constant. To each of these, there corresponds a non-zero integer where the partition function takes odd value. Now, since putting $l = -k$, s_k can be written as $\frac{1}{2}k(3k-1) = \frac{1}{2}l(3l+1)$, elements of $\{t_k - s_j : 1 \leq s_j < t_k \leq n\} \cup \{s_k - t_j : 1 \leq t_j < s_k \leq n\}$ are of the form

$$m = \frac{u(3u+1)}{2} - \frac{v(3v+1)}{2} = \frac{(u-v)(3u+3v+1)}{2} \tag{17}$$

with certain integers u and v.

Since from (17), we see that for a particular m, the value of $(u-v)$ determines the value of $(u+v)$ and the values of $(u-v)$ and $(u+v)$ together determine u and v, the number of distinct expressions of a particular m can be at most twice the number of divisors of $2m$.

Therefore, by Wigert's theorem [48] (may also refer to [19] for instance) on the order of magnitude of the divisor function, for $N > N(\epsilon)$, the number of distinct expressions of a particular m is less than

$$\exp\left((\log 2 + \epsilon/2)\frac{\log N}{\log\log N}\right).$$

Therefore, for $N > N(\epsilon)$, the total number of distinct m values counted is at least

$$\begin{aligned} &C_2 N^{1/2}/\exp\left((\log 2 + \epsilon/2)\frac{\log N}{\log\log N}\right) \\ &> N^{1/2}\exp\left(-(\log 2 + \epsilon)\frac{\log N}{\log\log N}\right) \quad (\text{for } N > N_1(\epsilon)) \end{aligned}$$

and this completes the proof of Theorem 3.4.

In an Appendix to the paper of Nicolas, Ruzsa and Sárközy [34] mentioned above, J. -P. Serre gives a proof of Theorem 3.4 in a larger frame dealing with the parity of coefficients of modular forms. We shall come back to the result of Serre in the context of the partition function.

We shall now briefly discuss the question of parity of $p(n)$ for n in a given arithmetic progression. Subbarao [45] made the following conjecture:

Conjecture 3.1. (Subbarao) *For every positive integer m, on every arithmetic progression $r \pmod m$, $0 \le r < m-1$, $p(n)$ assumes both even and odd values infinitely often.*

We have already discussed the case $m = 1$ in details. For the cases $m = 2, 3, 4, 5, 6, 8, 10, 12, 16, 20, 40$, the conjecture had been established by the efforts of many mathematicians. The works of Subbarao [45], Hirschhorn and Subbarao [23] and Hirschhorn [20] established those cases by elegant combinatorial methods. It should be mentioned that the congruences modulo 2 for certain generating functions, from where Hirschhorn [20] derived his results, had been also proved by Garvan and Stanton [18] by different methods.

In an major achievement, Ono [36] proved the following.

Theorem 3.5. **(Ono)** *For every positive integer m, on every arithmetic progression $r \pmod{m}$, $0 \leq r < m-1$, $p(n)$ assumes even values infinitely often. Also, if $p(n)$ assumes odd value for a single n in an arithmetical progression, then $p(n)$ assumes odd values for infinitely many n in that arithmetical progression.*

Following quantified versions of the above result were proved afterwards:

Theorem 3.6. (**Ahlgren** [1], **Serre** [34]) *Given an arithmetic progression $r \pmod{m}$, for some r, $0 \leq r < m$, there is a positive constant $C_3 = C_3(r, m)$ such that the number of integers $n \leq X$ in that arithmetic progression such that $p(n)$ is even is at least $C_3\sqrt{X}$.*

Theorem 3.7. (**Ahlgren** [1]) *Given an arithmetic progression $r \pmod{m}$, for some r, $0 \leq r < m$, if there is at least one integer M in that arithmetic progression such that $p(M)$ is odd, then there is a positive constant $C_4 = C_4(r, m)$ such that the number of integers $n \leq X$ in that arithmetic progression such that $p(n)$ is odd is at least $C_4\sqrt{X}$.*

We should mention that for odd values of $p(n)$, Ono [36] proved more than what has been stated in Theorem 3.5. Given an arithmetic progression $r \pmod{m}$, $0 \leq r < m$, if $p(n)$ assumes odd value for some n belonging to that progression, then Ono gave an explicit upper bound for the least such n. This helped him to establish the following.

Theorem 3.8. **(Ono)** *For all $0 \leq r < m \leq 10^5$, there are infinitely many integers*

$$M \equiv r \pmod{m}$$

for which $p(M)$ is odd.

In a recent work, using certain facts about the theory of Galois representations associated to modular forms and Shimura's theory of half integral weight modular forms, Ahlgren and Ono [2] has provided a theoretical framework explaining the known congruences for the partition function.

We state the results obtained in [2].

For primes $l \geq 5$, let the integer $\epsilon_l \in \{\pm 1\}$ be defined by $\epsilon_l = \left(\frac{-6}{l}\right)$.

Let S_l denote the set of $(l+1)/2$ integers $\beta \in \{0, 1, \cdots, l-1\}$ satisfying $\left(\frac{\beta+\delta_l}{l}\right) = 0$ or $-\epsilon_l$ where $\delta_l = (l^2-1)/24$.

Theorem 3.9. **(Ahlgren and Ono)** *If $l \geq 5$ is prime, m is a positive integer and $\beta \in S_l$, then a positive proportions of the primes $q \equiv -1 \pmod{24l}$*

have the property that

$$p(T) \equiv 0 \pmod{l^m} \quad \text{where } T = \frac{q^3 n + 1}{24},$$

for all $n \equiv 1 - 24\beta \pmod{24l}$ *with* $gcd(q, n) = 1$.

Ahlgren and Ono [2] have deduced the following result from Theorem 3.9.

Theorem 3.10. (Ahlgren and Ono) *If* $l \geq 5$ *is prime,* m *is a positive integer and* $\beta \in S_l$*, then there are infinitely many non-nested arithmetic progressions* $\{An + B\} \subset \{ln + \beta\}$ *such that for every integer* n *we have*

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

References

[1] S. Ahlgren, *The distribution of parity of the partition function in arithmetic progressions.* Indagationes Math., to appear.

[2] S. Ahlgren and Ken Ono, *Congruence properties for the partition function.* Proceedings of the National Academy of Sciences, USA, to appear.

[3] G. E. Andrews and F. G. Garvan, *Dyson's crank of a partition.* Bull. Amer. math. Soc. **18**, 167-171 (1988).

[4] A. O. L. Atkin, *Proof of a conjecture of Ramanujan.* Glasgow Math. J., **8**, 14-32 (1967).

[5] A. O. L. Atkin, *Multiplicative congruence properties and density problems for* $p(n)$. Proc. London Math. Soc., **18**, 563-576 (1968).

[6] A. O. L. Atkin, *Congruence Hecke operators.* American Math. Soc. Proceedings of Symposia in Pure Mathematics, **12**, 33-40 (1969).

[7] A. O. L. Atkin and J. N. O' Brien, *Some properties of* $p(n)$ *and* $c(n)$ *modulo powers of 13.* Trans. Amer. Math. Soc., **126**, 442-459 (1967).

[8] A. O. L. Atkin and P. Swinnerton-Dyer, *Some properties of partitions.* Proc. London Math. Soc. (3) **4**, 84-106 (1953).

[9] Bruce C. Berndt and Ken Ono, *Ramanujan's unpublished manuscript on the partition and tau functions with proofs and commentary.* The Andrews Festschrift (Maratea, 1998), Sém. Lothar. Combin., **42** (1999).

[10] S. D. Chowla, *Congruence properties of partitions*, J. London Math. Soc., **9**, 247 (1934).

[11] Freeman J. Dyson, *Some guesses in the Theory of Partitions.* Eureka (Cambridge) 10-15 (1944).

[12] Freeman J. Dyson, *A walk through Ramanujan's Garden.* Ramanujan Revisited, Proceedings of the Centenary Conference, University of Illinois at Urbana-Champaign, June 1-5, 1987. Andrews, Askey, Berndt, Ramanathan, Rankin eds. Academic Press. 7-28 (1988).

[13] P. Erdős and A. Ivić, *The distribution of certain arithmetical functions at consecutive integers*, Coll. Math. soc. J. Bolyai, North-Holland, Amsterdam, **51**, 45-91 (1989).

[14] J. Fabrykowski and M. V. Subbarao, *Some new identities involving the partition function $p(n)$.* Number Theory, Proceedings of the First Conference of the Canadian Number Theory Association (Banff, Alberta, April 17-27, 1988), ed. R. A. Mollin, Walter de Gruyter, New York, 125-138 (1900).

[15] F. Garvan, *A simple proof of Watson's partition congruences for powers of* 7. J. Austral. Math. Soc. **36**, 316-334 (1984).

[16] F. Garvan, *Combinatorial interpretations of Ramanujan's partition congruences.* Ramanujan Revisited, Proceedings of the Centenary Conference, University of Illinois at Urbana-Champaign, June 1-5, 1987. Andrews, Askey, Berndt, Ramanathan, Rankin eds. Academic Press. 29-45 (1988).

[17] F. Garvan, D. Kim and D. Stanton, *Cranks and t-cores*, Invent. Math., **101**, 1-17 (1990).

[18] F. Garvan and D. Stanton, *Sieved partition functions and q-binomial coefficients.* Math. Comp., **55**, 299-311 (1990).

[19] G.H. Hardy & E. M. Wright, *An introduction to the Theory of Numbers*, 5th edition, Oxford University Press, (1981).

[20] M. D. Hirschhorn, *On the parity of* $p(n)$, *II.* Journal of Combinatorial Theory, Series A **62**, 128-138 (1993).

[21] M. D. Hirschhorn, *Ramanujan's partition congruences.* Discrete Math. **131**, 351-355 (1994).

[22] M. D. Hirschhorn and D. C. Hunt, *A simple proof of the Ramanujan conjecture for powers of* 5. J. Reine Angew. Math. **326**, 1-17 (1981).

[23] M. D. Hirschhorn and M. V. Subbarao, *On the parity of* $p(n)$. Acta Arith. **50**, 355-356 (1988).

[24] O. Kolberg, *Note on the parity of the partition function.* Math. Scand. **7**, 377 -378 (1959).

[25] D. H. Lehmer, *On a conjecture of Ramanujan.* J. London Math. Soc., **11**, 114-118 (1936).

[26] D. H. Lehmer, *An application of Schläfli's modular equation to a conjecture of Ramanujan.* Bull. Amer. Math. Soc., **44**, 84-90 (1938).

[27] J. Lehner, *Ramanujan identities involving the partition function for the moduli* 11^α. Amer. J. Math., **65**, 492-520 (1943).

[28] J. Lehner, *Proof of Ramanujan's partition congruence for the modulus* 11^3. Proc. Amer. Math. Soc., **1**, 172-181 (1950).

[29] Major P. A. MacMahon, *Note on the parity of the number which enumerates the partitions of a number.* Proc. Cambridge Phil. Soc., **20**, 281-283 (1921).

[30] L. Mirsky, *The distribution of values of the partition function in residue classes.* J. Math. Anal. Appl., **93**, 593-598 (1983).

[31] M. Newman, *Periodicity modulo m and divisibility properties of the partition function.* Trans. Amer. Math. Soc., **97**, 225-236 (1960).

[32] M. Newman, *Congruences of the partition function to composite moduli.* Illinois J. of Math., **6**, 59-63 (1962).

[33] M. Newman, *Note on partitions modulo 5.* Math. Comp., **21**, 481-482 (1967).

[34] 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 Theory, **73**, 292-317 (1998).

[35] J. -L. Nicolas and A. Sárközy, *On the parity of partition functions.* Illinois J. Math., **39**, 586-597 (1995).

[36] K. Ono, *Parity of the partition function in arithmetic progressions.* J. Reine Angew. Math., **472**, 1-15 (1996).

[37] K. Ono, *Distribution of the partition function modulo m.* Ann. of Math. (2) **151**, no. 1, 293-307 (2000).

[38] T. R. Parkin and D. Shanks, *On the distribution of parity in the partition function.* Math. Comp. **21**, 466-480 (1967).

[39] S. Ramanujan, *Some properties of $p(n)$, the number of partitions of n.* Proc. Cambridge Phil. Soc., **19**, 207-210 (1919).

[40] S. Ramanujan, *Congruence properties of partitions.* Proc. London Math. Soc. 2, **18** (1920), Records for 13 March 1919.

[41] S. Ramanujan, *Congruence properties of partitions.* Math. Z., 8, 147-153 (1921). Phil. Soc., **19**, 207-210 (1919).

[42] S. Ramanujan, *Unpublished manuscript on the partition and tau functions.* The Lost Notebook and Other Unpublished Papers, Narosa, New Delhi, (1988).

[43] J. M. Rushforth, *Congruence properties of the partition function and associated functions.* Proc. Cambridge Phil. Soc. **48**, 402-413 (1952).

[44] A. Schinzel and E. Wirsing, *Multiplicative properties of the partition function*. Proc. Indian Acad. Sci. (Math. Sci.), **97**, Nos 1-3, December, 297 - 303 (1987).

[45] M. V. Subbarao, *Some remarks on the partition function*. Amer. Math. Monthly, **73**, 851-854 (1966).

[46] J. H. van Lint, *Advanced problems and solutions, 4944 [1961,67], Proposed by Morris Newman*. Amer. Math. Monthly, **69** (1962).

[47] G. N. Watson, *Ramanujans Vermutung über Zerfällungsanzahlen*. J. Reine Angew. Math. **179**, 97-128 (1938).

[48] S. Wigert, *Sur l'ordre de grandeur du nombre de diviseurs d'un entier*. Arkiv för matematik, **3**, 1-9 (1907).

[49] L. Winquist, *An elementary proof of* $p(11n+6) \equiv 0 \pmod{11}$. J. Combinatorial Theory, **6**, 56-59 (1969).

Received: 01.02.2001
Revised: 04.04.2001