DISTRIBUTION OF PARITY OF THE PARTITION FUNCTION IN ARITHMETIC PROGRESSIONS

Scott Ahlgren

Abstract. Let $p(n)$ be the number of partitions of a non-negative integer n. In this paper we prove that for any progression $r \pmod t$, and for large X, we have

(a) The number of $n \leq X$ such that $n \equiv r \pmod t$ and $p(n)$ is even is $\gg \sqrt{X}$, and
(b) The number of $n \leq X$ such that $n \equiv r \pmod t$ and $p(n)$ is odd is $\gg \sqrt{X}/\log X$, provided that one such n exists.

Résumé. Soit $p(n)$ le nombre de partitions de l'entier $n \geq 0$. Nous démontrons que pour toute progression $r \pmod t$, et pour un nombre X suffisamment grand,

(a) Le nombre d'entiers $n \leq X$ pour lesquels $n \equiv r \pmod t$ et $p(n)$ est pair est $\gg \sqrt{X}$, et
(b) Le nombre d'entiers $n \leq X$ pour lesquels $n \equiv r \pmod t$ et $p(n)$ est impair est $\gg \sqrt{X}/\log X$, pourvu qu'au moins un tel n existe.

1. Introduction and statement of results

Let $p(n)$ be the number of partitions of a non-negative integer n; $p(n)$ is the number of ways to express n as the sum of a non-increasing sequence of positive integers. It is conjectured that $p(n)$ is equally often even and odd, and computations suggest that this conjecture is almost certainly true. For example,

$$\#\{n \leq 10,000,000 : p(n) \text{ is odd}\} = 5,002,137.$$

Recently, Nicolas, Ruzsa, and Sárközy have proved

Theorem 1.1 ([3], Theorems 1 and 2).

(a) *For large X, we have $\#\{n \leq X : p(n) \text{ is even}\} \gg \sqrt{X}$.*
(b) *Suppose that $\epsilon > 0$. There exists a constant $X_0(\epsilon)$ such that for $X > X_0(\epsilon)$ we have*

$$\#\{n \leq X : p(n) \not\equiv p(n-1) \pmod 2\} > \sqrt{X} \exp\left(-(\log 2 + \epsilon)\frac{\log X}{\log\log X}\right).$$

Consequently the same lower bound holds for the number of $n \leq X$ for which $p(n)$ is odd.

These results improve upon previous lower bounds given by Nicolas and Sárközy [4] and Mirsky [2], which were of the order $(\log X)^c$ and $\log\log X$, respectively.

Ono [5] considered the parity of $p(n)$ for values of n lying in a fixed arithmetic progression $r \pmod t$, and proved the following

Theorem 1.2 ([5], Theorems 1 and 2).

(a) *In any arithmetic progression* $r \pmod t$, *there are infinitely many* n *such that* $p(n)$ *is even.*

(b) *In any arithmetic progression* $r \pmod t$, *there are infinitely many* n *such that* $p(n)$ *is odd, provided that there is one such* n. *Further, if such an* n *exists, then the smallest such* n *is* $< 10^{10}t^7$.

Apart from the assumption in part (b), this settles an old conjecture of Subbarao [9].

In this paper we will obtain quantitative estimates for the distribution of partity of $p(n)$ in arithmetic progressions. As a corollary, we obtain a slight improvement of the lower bound given by Theorem 1.1 for the number of odd values of $p(n)$. There are two main theorems.

Theorem 1.3. *Let* r *and* t *be integers with* $0 \leq r < t$. *For large* X, *we have*

$$\#\{n \leq X : n \equiv r \pmod t,\ p(n) \text{ is even}\} \gg \sqrt{X}.$$

Remark. In an appendix added to [3] by J.-P. Serre, a slightly stronger result than Theorem 1.3 is proved. Namely, Serre proves that

$$\frac{\#\{n \leq X : n \equiv r \pmod t,\ p(n) \text{ is even}\}}{\sqrt{X}} \to \infty \text{ as } X \to \infty.$$

The main contribution of the present work, therefore, comes in the odd case, where we can prove the following

Theorem 1.4. *Let* r *and* t *be integers with* $0 \leq r < t$. *Suppose that there exists an integer* $n \equiv r \pmod t$ *such that* $p(n)$ *is odd. Then*

$$\#\{n \leq X : n \equiv r \pmod t,\ p(n) \text{ is odd}\} \gg \sqrt{X}/\log X.$$

Putting $t = 1$ in this result, we obtain

Corollary 1.5. *For large* X *we have*

$$\#\{n \leq X :\ p(n) \text{ is odd}\} \gg \sqrt{X}/\log X.$$

Notice that for any positive constants c_1 and c_2 we have

$$\exp\left(-c_1 \frac{\log X}{\log\log X}\right) < \frac{c_2}{\log X} \quad \text{for large } X.$$

So the corollary does improve the estimate given by Theorem 1.1 in the odd case. In the case when $t = 4$ it is possible to obtain explicit constants in Theorems 1.3 and 1.4 (see the final example below).

2. Results on Modular Forms

If N is a positive integer, we define

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \ a \equiv d \equiv 1 \pmod N, \ c \equiv 0 \pmod N \right\}.$$

Elements of $\Gamma_1(N)$ act as fractional linear transformations on the upper half-plane $\mathfrak{H}$ of complex numbers. If k is an integer and $f(z)$ is a meromorphic function on $\mathfrak{H}$, then f is a *modular function* of weight k with respect to $\Gamma_1(N)$ if $f((az+b)/(cz+d)) = (cz+d)^k f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$ and $z \in \mathfrak{H}$. If $f(z)$ is holomorphic on $\mathfrak{H}$ as well as at the cusps of $\Gamma_1(N)$ (in other words, at the rationals), then f is called a *modular form* with respect to $\Gamma_1(N)$. If, in addition, $f(z)$ vanishes at all cusps, then f is called a *cusp form*. Denote the space of modular forms of weight k with respect to $\Gamma_1(N)$ by $M_k(N)$, and the corresponding space of cusp forms by $S_k(N)$. If $f \in M_k(N)$, then f has a Fourier expansion $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ in the variable $q = e^{2\pi i z}$; if f is a cusp form, then $a(0) = 0$.

We require two lemmas on the parity of Fourier coefficients of modular forms. For $s \geq 1$ we denote by P_s the set of positive square-free integers which are the product of exactly s primes. In [6, Fundamental Lemma], Ono and Skinner study divisibility properties of Fourier coefficients of half-integral weight eigenforms. Their argument may be applied in our situation in order to prove the following

Lemma 2.1. *Let $f(z) = \sum_{n=1}^{\infty} a(n)q^n$ be a cusp form of integer weight on $\Gamma_1(N)$ with integer coefficients $a(n)$. Suppose that $a(m)$ is odd for some integer $m = \ell d$, where $\ell \in P_s$ for some $s \geq 1$, and $\gcd(\ell, 2Nd) = 1$. Then $\#\{n \leq X : n \in dP_s, \ a(n) \text{ is odd}\} \gg X(\log\log X)^{s-1}/\log X$.*

Proof. Let m be as in the hypotheses; then $\sum_{n=1}^{\infty} a(nd)q^n$ is a cusp form on $\Gamma_1(Nd)$ whose ℓ-th Fourier coefficient is odd. After this observation, we may reduce ourselves to considering the case where $m = \ell$. In other words, we may suppose that

$$a(m) \quad \text{is odd, where} \quad m \in P_s, \quad \gcd(m, 2N) = 1.$$

The remainder of the proof follows the arguments in [6, Fundamental Lemma].

Since $a(m) \neq 0$, where m is coprime to the level of f, it follows that the new part of f, say f_{new}, is not identically zero. We may write

$$f_{\text{new}} = \sum_{i=1}^{h} \alpha_i f_i, \qquad \alpha_i \neq 0, \tag{2.1}$$

where each f_i is a newform of level dividing N. Write the Fourier expansions of these forms as $f_i(z) = \sum_{n=1}^{\infty} a_i(n)q^n$, and let K be a finite extension of $\mathbb{Q}$ which contains all of the coefficients $a_i(n)$, as well as all of the α_i in (2.1). We know that the $a_i(n)$ are algebraic integers; further, we have

$$a(n) = \sum_{i=1}^{h} \alpha_i a_i(n) \quad \text{if} \quad \gcd(n, N) = 1. \tag{2.2}$$

Let v be a place of K over 2 and let $\mathcal{O}_v$ denote the completion of the ring of integers of K at v. For each newform f_i, the work of Shimura, Deligne, and Deligne-Serre guarantees the existence of a continuous representation $\rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{O}_v)$ which is unramified outside of $2N$ and such that

$$\mathrm{Trace}\, \rho_i(\mathrm{Frob}_p) = a_i(p) \quad \text{for all primes } p \nmid 2N. \tag{2.3}$$

Here Frob_p is any Frobenius element for p. Define

$$E := \max_{1 \le i \le h} |\operatorname{ord}_v(\alpha_i)|, \tag{2.4}$$

and let λ be a uniformizer for $\mathcal{O}_v$. Consider the representation

$$\rho := \bigoplus_{i=1}^{h} \rho_i \bmod \lambda^{E+1}.$$

Suppose that $m = p_1 \dots p_s$, with $s \ge 1$ and distinct primes p_j. By the Chebotarev Density Theorem, for each j there are $\gg X/\log X$ primes $q \le X$ such that $\rho(\mathrm{Frob}_q) = \rho(\mathrm{Frob}_{p_j})$. By (2.3), if q is such a prime, then $a_i(q) \equiv a_i(p_j) \pmod{\lambda^{E+1}}$ for all i. Since the Fourier coefficients of newforms are multiplicative, we may conclude that there are $\gg X(\log\log X)^{s-1}/\log X$ square-free integers $n = q_1 \dots q_s \in P_s$, $n \le X$, such that

$$\gcd(n, 2N) = 1 \quad \text{and} \quad a_i(n) \equiv a_i(m) \pmod{\lambda^{E+1}}, \quad 1 \le i \le h.$$

If n is such an integer, then we may conclude from (2.2) and (2.4) that $a(n) \equiv a(m) \pmod{\lambda}$. Since $a(n)$ and $a(m)$ are integers, it follows that $a(n) \equiv a(m) \pmod 2$, whence $a(n)$ is odd. This finishes the proof of Lemma 2.1. $\square$

For the even case we will use a well-known result of Serre [7, Thèoréme 1] (or see [8] for more details) which yields the following as a corollary:

Lemma 2.2. *Let $f(z) = \sum_{n=1}^{\infty} a(n)q^n$ be a cusp form of integer weight on $\Gamma_1(N)$ with integer coefficients $a(n)$. Then $\#\{n \le X : a(n) \text{ is odd}\} = o(X)$.*

3. A lemma on power series.

This section contains the main counting argument, which will be employed below in order to pass from the results of the last section to the desired conclusions about the partition function.

Lemma 3.1. *Let ℓ and s be positive integers. Suppose that we have the power series identity*

$$\sum_{n=0}^{\infty} a(n)q^n \equiv \sum_{n=n_0}^{\infty} c(n)q^n \sum_{n=0}^{\infty} q^{\ell(2n+1)^2} \pmod 2, \tag{3.1}$$

where the $a(n)$ and $c(n)$ are integers.

(a) *If $\#\{n \le X : a(n) \text{ is odd}\} = o(X)$, then $\#\{n \le X : c(n) \text{ is even}\} \gg \sqrt{X}$.*
(b) *If $\#\{n \le X : a(n) \text{ is odd}\} \gg X(\log\log X)^{s-1}/\log X$, then*

$$\#\{n \le X : c(n) \text{ is odd}\} \gg \sqrt{X}(\log\log X)^{s-1}/\log X.$$

Proof. For $k = 0, 1, \ldots$, set $u_k := \ell(2k+1)^2$. For every $n \geq n_0$, define the set

$$\mathcal{M}_n := \{n - u_k : 0 \leq u_k \leq n - n_0\}.$$

With this notation, comparing coefficients on q^n in (3.1) gives

$$a(n) \equiv \sum_{m \in \mathcal{M}_n} c(m) \pmod 2. \tag{3.2}$$

We can now prove assertion (a) (we use a counting argument as in [3]). Notice that if $u_{k-1} \leq n - n_0 < u_k$, then $|\mathcal{M}_n| = k$. Therefore $|\mathcal{M}_n|$ is odd precisely when n is contained in an interval of the form $I_k := [u_{2k} + n_0, u_{2k+1} + n_0)$. There exists a constant $C > 0$ such that for large X we have $I_k \subseteq [n_0, X], \quad 0 \leq k < C\sqrt{X}$. Since the length of I_k is $\gg k$, we have

$$\#\{n \leq X : n \in I_k \text{ for some } k\} \gg \sum_{k=0}^{C\sqrt{X}} k \gg X.$$

Therefore, $\#\{n \leq X : |\mathcal{M}_n| \text{ is odd}\} \gg X$, and by our assumption in (a),

$$\#\{n \leq X : |\mathcal{M}_n| \text{ is odd, } a(n) \text{ is even}\} \gg X.$$

For every such n, (3.2) shows that $c(m)$ is even for some $m \in \mathcal{M}_n$. Therefore

$$\#\{(n, m) : n \leq X,\ m \in \mathcal{M}_n,\ c(m) \text{ is even}\} \gg X.$$

It remains to count the multiplicity of the numbers m. We have $m \in \mathcal{M}_n$ if $n = m + u_k$. So for fixed m, the number of $n \leq X$ such that $m \in \mathcal{M}_n$ is not more than the number of k such that $0 \leq u_k \leq X - n_0$, and this number is clearly $\ll \sqrt{X}$. Therefore $\#\{m \leq X : c(m) \text{ is even}\} \gg \sqrt{X}$, which establishes (a).

We turn to the proof of (b). By (3.2) we see that if $a(n)$ is odd, then $c(m)$ is odd for at least one $m \in \mathcal{M}_n$. By our hypothesis, we may conclude that

$$\#\{(n, m) : n \leq X,\ m \in \mathcal{M}_n,\ c(m) \text{ is odd}\} \gg X(\log\log X)^{s-1}/\log X.$$

Counting multiplicities as above, we find that

$$\#\{m \leq X : c(m) \text{ is odd}\} \gg \sqrt{X}(\log\log X)^{s-1}/\log X,$$

and our lemma is proved. $\square$

4. Proof of Theorems 1.3 and 1.4

In what follows we shall require the following result of Erdös [1].

Lemma 4.1 (Erdös). *Let a and b be coprime integers such that $1 \leq a < b$. There exists an absolute constant c_1 such that the smallest squarefree number in the arithmetic progression $a + k\,b, \quad k = 0, 1, \ldots$ is less than $c_1 b^{3/2}/\log b$.*

Recall the definitions of the two well-known functions $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1 - q^n)$ and $\Delta(z) = \eta^{24}(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$. Our next lemma follows immediately from Proposition 1 of [5], with t replaced by tc.

Lemma 4.2 (Ono). *Given a fixed positive integer t, let $j \geq 0$ and $c > 0$ be integers satisfying $2^j > tc/24$. Define*

$$f_{j,c}(z) := \frac{\eta(24z)}{\eta(48z)} \Delta^{2^j}(24tcz).$$

Then $f_{j,c}(z) \in S_{2^j \cdot 12}\left(2^7 3^2 tc\right)$. Further, the Fourier expansion of $f_{j,c}(z)$ has integer coefficients, and satisfies the congruence

$$f_{j,c}(z) = \sum_{n=1}^{\infty} a_{j,c}(n) q^n \equiv \sum_{n=0}^{\infty} p(n) q^{24n-1} \sum_{n=0}^{\infty} q^{24 \cdot 2^j tc(2n+1)^2} \pmod{2}. \tag{4.1}$$

For the remainder we consider fixed integers r and t with $0 \leq r < t$. Define $\delta := \gcd(24r-1, t)$, and let j and c be as in Lemma 4.2. By Lemma 2 of [5] (recall that $S_k(N)$ is the direct sum of the spaces $S_k(N, \chi)$), we may conclude that

$$g_{j,c}(z) := \sum_{n \equiv 24r-1 \pmod{24t}} a_{j,c}(n) q^n \in S_{2^j \cdot 12}\left(\frac{2^{13} 3^4 t^3 c}{\delta}\right).$$

The factorization (4.1) gives

$$g_{j,c}(z) = \sum_{n \equiv 24r-1 \pmod{24t}} a_{j,c}(n) q^n \equiv \sum_{n \equiv r \pmod{t}} p(n) q^{24n-1} \sum_{n=0}^{\infty} q^{24 \cdot 2^j tc(2n+1)^2} \pmod{2}. \tag{4.2}$$

We can now prove Theorem 1.3. By Lemma 2.2, we know that

$$\#\{n \leq X : n \equiv 24r-1 \pmod{24t},\ a_{j,c}(n) \text{ is odd }\} = o(X).$$

Therefore, by Lemma 3.1, we may conclude that

$$\#\{n \leq X : n \equiv r \pmod{t},\ p(n) \text{ is even }\} \gg \sqrt{X}.$$

We turn to Theorem 1.4. Let n_0 be the smallest integer in the progression $r \pmod{t}$ such that $p(n_0)$ is odd, and let n_1 be the second smallest such integer. (Indeed, by Ono's theorem we know that infinitely many such integers exist.) Let c_1 be given by Lemma 4.1 and fix an integer j such that

$$2^{j/2} > \max(1, c_1) \cdot (24n_1 - 1)^{3/2} (24)^{1/2} t^{3/2}. \tag{4.3}$$

If we write out the expansion (4.2), we obtain

$$\begin{aligned} g_{j,c}(z) \equiv p(n_0) q^{24n_0 - 1 + 24 \cdot 2^j tc} &+ p(n_1) q^{24n_1 - 1 + 24 \cdot 2^j tc} + \dots \\ &+ p(n_0) q^{24n_0 - 1 + 24 \cdot 2^j tc \cdot 9} + \dots \pmod{2}. \end{aligned} \tag{4.4}$$

Notice that by (4.3), the terms in (4.4) are written in strictly ascending order. We shall show that c may be chosen so that the second term is "well-placed"; in other words, placed such that we may apply Lemma 2.1 to the form $g_{j,c}$.

Lemma 4.3. *Suppose that t and n_1 are as above and that j satisfies* (4.3). *Then we can choose an integer c, $1 \le c \le 12 \cdot 2^j/t$, such that if*

$$m := 24n_1 - 1 + 24 \cdot 2^j tc,$$

then $m = \ell d$, where $\ell \in P_s$ for some $s \ge 1$, and

$$\gcd(\ell, 2Nd) = 1, \qquad \text{where} \qquad N := \frac{2^{13}3^4t^3c}{\delta} = \text{ level of } g_{j,c}.$$

Proof. Define $d := \gcd(24n_1 - 1, t)$, and define

$$a := \frac{24n_1 - 1}{d} \quad \text{and} \quad b := \frac{24 \cdot 2^j t}{d}. \tag{4.5}$$

Then $\gcd(a, b) = 1$; also, since $n_1 \ge t$, we have $d \ne 24n_1 - 1$, whence $a \ne 1$. Consider the progression

$$(a + b) + k\,ab, \qquad 0 \le k < \frac{6 \cdot 2^j}{at}. \tag{4.6}$$

Since $a > 1$ and $b > 24$, we have $1 \le a + b < ab$. Moreover, $\gcd(a + b, ab) = 1$. Using (4.3), we see that the largest integer among (4.6) is easily $> 2^j b/t > c_1(ab)^{3/2}$.

By Lemma 4.1, we may fix some k as in (4.6) such that

$$\ell := a + b + k\,ab \quad \text{is squarefree .} \tag{4.7}$$

Let $c := ka + 1$; then $1 \le c \le 12 \cdot 2^j/t$. By (4.7) we see that, with this choice of c,

$$m := 24n_1 - 1 + 24 \cdot 2^j tc = \ell d. \tag{4.8}$$

Write $\ell = p_1p_2 \dots p_m$ with distinct primes p_i. We need only to show that one of the p_i is coprime to $2Nd$. If this were not the case, we would have

$$p_i \mid 2 \cdot 3tcd \qquad 1 \le i \le m.$$

By (4.8) and the definition of d, this implies that

$$p_i \mid 24n_1 - 1 \qquad 1 \le i \le m,$$

whence $\ell \le 24n_1 - 1$. However, by (4.7) , (4.5), and (4.3) we see that $\ell \ge a + b \ge 2^j > (24n_1 - 1)^3$, and we obtain the desired contradiction. $\square$

We can now finish the proof of Theorem 1.4. Fix values for c and m as given by Lemma 4.3 (notice that $2^j > tc/24$, as required by Lemma 4.2). Then $a_{j,c}(m)$ is odd, where $g_{j,c}$ and m satisfy the hypotheses of Lemma 2.1 with some $s \ge 1$. By Lemma 2.1 we may conclude that

$$\#\{n \le X : n \equiv 24r - 1 \pmod{24t},\, a_{j,c}(n) \text{ is odd }\} \gg X/\log X.$$

By Lemma 3.1, we conclude that

$$\#\{n \leq X : n \equiv r \pmod t,\ p(n) \text{ is odd } \} \gg \sqrt{X}/\log X,$$

as desired.

Example. One can give explicit versions of Theorems 1.3 and 1.4 in the case when $t = 4$ (in the interest of space, we shall not provide the details here). Let r be any of the integers 0, 1, 2, or 3. Then for large X we have

(a) $\#\{n \leq X : n \equiv r \pmod 4,\ p(n) \text{ is even}\} > \sqrt{X}/12$.
(b) $\#\{n \leq X : n \equiv r \pmod 4,\ p(n) \text{ is odd}\} > \sqrt{X}/\log 8X$.

Remark. In light of evidence obtained by computing the parity of $p(n)$ for $n \leq 10,000,000$, it seems certain that for $r = 0, 1, 2, 3$, we have

$$\#\{n \leq X : n \equiv r \pmod 4,\ p(n) \text{ is odd}\} \sim X/8.$$

References

1. P. Erdös, *Über die kleinste quadratfreie Zahl einer arithmetischen Reihe*, Monatsh. Math **64** (1960), 314-316.
2. L. Mirsky, *The distribution of values of the partition function in residue classes*, J. Math. Anal. Appl. **93** (1983), 593–598.
3. J.L. Nicolas, I.Z. Ruzsa, and A. Sárközy (with an appendix by J.-P. Serre), *On the parity of additive representation functions*, J. Number Theory (to appear).
4. J.L. Nicolas and A. Sárközy, *On the parity of partition functions*, Illinois J. Math. **39** (1995), 586–597.
5. K. Ono, *Parity of the partition function in arithmetic progressions*, J. reine angew. Math. **472** (1996), 1–15.
6. K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Invent. Math. (to appear).
7. J. -P. Serre, *Divisibilité des coefficients des formes modulaires de poids entier*, C. R. Acad. Sci. Paris, ser. A **279** (1974), 679–682.
8. J. -P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseign. Math **22** (1976), 227-260.
9. M. Subbarao, *Some remarks on the partition function*, Amer. Math. Monthly **73** (1966), 851–854.

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802-6401
E-mail address: ahlgren@math.psu.edu