ON THE PARITY OF PARTITION FUNCTIONS

J.L. NICOLAS AND A. SÁRKÖZY¹

Section 1

For n = 1, 2, ..., p(n) denotes the number of unrestricted partitions of n, and q(n) the number of partitions of n into distinct parts, and we write p(0) = q(0) = 1, $p(-1) = q(-1) = p(-2) = q(-2) = \cdots = 0$. If N, b are positive integers, a is an integer, then let $E_{a,b}(N)$ denote the number of non-negative integers n such that $n \le N$ and $p(n) \equiv a \mod b$.

Starting out from a question of Ramanujan, in 1920 MacMahon [3] gave an algorithm for determining the parity of p(n). Since then, many papers have been written on the parity of p(n). In particular, in 1959 Kolberg proved that p(n) assumes both even and odd values infinitely often (for $n \ge 0$). His proof was based on Euler's identity

$$p(n) + \sum_{k\geq 1} (-1)^{k} (p(n-s_{k}) + p(n-t_{k})) = 0$$

where $s_k = \frac{1}{2}k(3k - 1)$, $t_k = \frac{1}{2}k(3k + 1)$ and the summation extends over all terms with a non-negative argument. It follows from this identity that

$$p(n) + \sum_{k \ge 1} \left(p(n - s_k) + p(n - t_k) \right) \equiv 0 \mod 2.$$
 (1)

Other proofs have been given for Kolberg's theorem by Newman [5] and Fabrykowski and Subbarao [1]. Parkin and Shanks [7] have computed the parity of p(n) up to n = 2039999. Their calculation suggest that $E_{0,2}(N) \sim E_{1,2}(N) \sim N/2$. Mirsky [4] has proved the only quantitative result on the frequency of the odd values and even values of p(n). In fact, starting out

Received June 25, 1993.

¹⁹⁹¹ Mathematics Subject Classification. Primary 11P83.

¹Research partially supported by the Hungarian Foundation for Scientific Research, Grant No. 1901, by CNRS, GDR Mathématiques Informatique, and by MEN, EA 619.

^{© 1995} by the Board of Trustees of the University of Illinois Manufactured in the United States of America

form (1), he proved that for $N > N_0$ we have

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

Note that he claims the following result: for each b there exist at least two distinct values of a (with $0 \le a < b$) such that, whenever N is sufficiently large,

$$E_{a,b}(N) > \frac{\log \log N}{b \log 2}.$$
(3)

However, his proof seems to give only the following slightly weaker result: for each b and $N > N_0(b)$ there exist at least two distinct values $a_1 = a_1(N)$, $a_2 = a_2(N)$ depending on N (with $0 \le a_1 < a_2 < b$) such that

$$\min\left(E_{a_1,b}(N), E_{a_2,b}(N)\right) > \frac{\log\log N}{b\log 2}.$$

This implies that there exist at least two distinct values of a (with $0 \le a < b$) such that (3) holds for *infinitely many N*, and it gives also (2).

In this paper, first we will improve on (2) by showing that there is a constant c > 0 such that

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

Moreover, we will point out that the parity of the values of q(n) can be determined easily. Motivated by this fact, we will show that the parities of p(n) and q(n) are different for infinitely many n. Finally, we will discuss several related unsolved problems.

We are pleased to thank P. Bateman who introduced us in the subject, and M. Deléglise for kindly computing the parity of p(f(n)) displayed at the end of this paper.

Section 2

We write

$$g(n) = \begin{cases} 1 & \text{if } p(n) \neq p(n-1) \mod 2\\ 0 & \text{if } p(n) \equiv p(n-1) \mod 2 \end{cases}$$

and

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

We will prove:

THEOREM 1. Let r be an integer ≥ 2 . For $M \geq 2r^2$, we have

$$G(M) \ge \frac{2}{3\log(2r^2)} (\log M)^{c_r}$$
 (4)

where

$$c_r = \log\left(\frac{3}{2} - \frac{1}{2r}\right) / \log 2.$$

COROLLARY 1. For any $c < \log(3/2) / \log 2 = 0.585 ...,$ we have

$$\min(E_{0,2}(N), E_{1,2}(N)) \ge \frac{1}{2}G(N) \gg (\log N)^{c}.$$
 (5)

Proof of the theorem. The proof of (4) will be based on Euler's identity (1) (although a lower bound of type (4) could be derived from (27) below as well). First we will prove that for every positive integer M we have

$$G(2r^2M^2) \ge \frac{3r-1}{2r}G(M).$$
 (6)

Replacing n by n-1 in (1) and subtracting the congruence obtained in this way from (1), we get

$$g(n) + \sum_{k \ge 1} \left(g(n - s_k) + g(n - t_k) \right) \equiv 0 \mod 2$$
 (7)

where the summation extends over all terms with a non-negative argument (note that g(0) = p(0) - p(-1) = p(0) = 1).

Let U denote the set of the integers u with $1 \le u \le M$, g(u) = 1 so that |U| = G(M). Let us consider the congruence (7) with $t_j + u$ in place of n for all $u \in U$ and j = M + 1, M + 2, ..., rM:

$$g(t_j + u) + \sum_{k \ge 1} \left(g(t_j + u - s_k) + g(t_j + u - t_k) \right) \equiv 0 \mod 2$$
 (8)

where

$$u \in U, j = M + 1, \dots, rM.$$
(9)

We have

$$t_{j} + u - t_{j+1} < t_{j} + u - s_{j+1} = \frac{1}{2}j(3j+1) + u - \frac{1}{2}(j+1)(3j+2)$$

= $-2j - 1 + u < -2M - 1 + M = -M - 1 < 0$

and

$$t_j + u - s_j > t_j + u - t_j = u > 0.$$

Thus the greatest s_k , resp. t_k , appearing in the sum in (8) is s_j , resp. t_j , so that (8) can be rewritten in the form

$$g(t_j + u) + \sum_{k=1}^{J} (g(t_j + u - s_k) + g(t_j + u - t_k)) \equiv 0 \mod 2.$$

The term $g(t_j + u - t_j) = g(u) = 1$ (since $u \in U$) appears on the left hand side. Thus there is another term equal to 1 on the left hand side, in other words, there is a v = v(j, u) such that

$$g(v) = 1, \tag{10}$$

 $v \neq u$ and v can be represented in one of the forms

$$v = t_i + u, \tag{11}$$

$$v = t_j + u - s_k \quad (\text{with } 1 \le k \le j) \tag{12}$$

and

$$v = t_j + u - t_k \quad (\text{with } 1 \le k \le j - 1).$$
 (13)

The smallest of the numbers on the right hand sides of (11), (12) and (13) is $t_i + u - s_i$ and the largest is $t_i + u$ so that

$$v \ge t_j + u - s_j = j + u > j > M$$
 (14)

and

$$v \le t_j + u \le t_{rM} + M = \frac{3}{2}r^2M^2 + \frac{1}{2}rM + M \le M^2(\frac{3}{2}r^2 + \frac{1}{2}r + 1) \le 2r^2M^2.$$
(15)

Let V denote the set of the distinct integers v that can be obtained as

$$v = v(j, u) \tag{16}$$

for some u, j satisfying (9), and let h(v) denote the number of the solutions of (16) in j and u. The number of pairs (j, u) satisfying (9) is |U|(r-1)M =

(r-1)MG(M) so that clearly,

$$|V| \ge \frac{(r-1)MG(M)}{\max_{v} h(v)}.$$
(17)

To obtain an upper bound for h(v), we will first show that the numbers $t_i + u$ (with j, u satisfying (9)) are distinct. In fact, assume that

$$t_j + u = t_{j'} + u'$$

whence

$$t_{j'} - t_j = u - u'. (18)$$

If j' > j, then

$$t_{j'} - t_j \ge t_{j+1} - t_j = 3j + 2 > M.$$
⁽¹⁹⁾

Moreover, we have

$$|u - u'| \le M. \tag{20}$$

(18), (19) and (20) imply j = j', u = u'.

Thus for fixed v, (11) has at most one solution in j and u. Moreover, if (12) holds for some v, j, u and k, then we have $1 \le k \le j \le rM$ so that k can be chosen in at most rM ways. If v and k in (12) are fixed, then, by the argument above, $v + s_k = t_j + u$ has at most one solution in j and u, so that for fixed v the total number of solutions of (12) is at most rM. A similar argument gives that (13) has at most rM - 1 solutions. Summarizing, we obtain that

$$h(v) \le 1 + rM + (rM - 1) = 2rM.$$

Thus it follows form (17) that

$$|V| \ge \frac{(r-1)MG(M)}{2rM} = \frac{r-1}{2r}G(M).$$
 (21)

By (10), (14), (15) and (21) we have

$$G(2r^{2}M^{2}) = (G(2r^{2}M^{2}) - G(M)) + G(M)$$

$$\geq |V| + G(M) \geq \frac{3r - 1}{2r}G(M)$$
(22)

which completes the proof of (6). Let us write $M_k = (2r^2)^{2^k-1}$ for k = 1, 2, ... so that $M_1 = 2r^2$ and $M_{k+1} = 2r^2M_k^2$ for k = 1, 2, ... Clearly we have g(2) = g(3) = 1 so that

$$G(M_1) \ge G(8) = \sum_{n=1}^8 g(n) \ge g(2) + g(3) = 2 > (3r-1)/2r.$$

Thus it follows form (6) by straightforward induction that

$$G(M_k) > \left(\frac{3r-1}{2r}\right)^k$$
 for $k = 1, 2, \dots$ (23)

To complete the proof of the theorem, assume that $M \ge 8$ and define k by

$$M_k \le M < M_{k+1} = 2r^2 M_k^2.$$

Then we have

$$\log \log M < \log \log M_{k+1} = \log \log (2r^2)^{2^{k+1}-1} < \log \log (2r^2)^{2^{k+1}}$$
$$= (k+1)\log 2 + \log \log (2r^2).$$

Thus it follows from (23) that

$$G(M) \ge G(M_k) > \left(\frac{3r-1}{2r}\right)^k > \left(\frac{3r-1}{2r}\right)^{(\log \log M - \log 2 - \log \log(2r^2))/\log 2}$$
$$= \left(\frac{2r}{3r-1}\right) (\log(2r^2))^{-c_r} (\log M)^{c_r} > \frac{2}{3\log(2r^2)} (\log M)^{c_r}$$

which completes the proof of Theorem 1.

Proof of the corollary. Clearly, g(n) = 1 if and only if one of 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. Thus for both i = 0 and 1 we have

$$\sum_{n=1}^{N} g(n) = \sum_{m=1}^{\lfloor N/2 \rfloor} g(2m) + \sum_{m=1}^{\lfloor (N+1)/2 \rfloor} g(2m-1)$$

$$\leq \sum_{m=1}^{\lfloor N/2 \rfloor} (E_{i,2}(2m) - E_{i,2}(2m-2))$$

$$+ \sum_{m=1}^{\lfloor (N+1)/2 \rfloor} (E_{i,2}(2m-1) - E_{i,2}(2m-3))$$

$$= (E_{i,2}(2\lfloor N/2 \rfloor) - E_{i,2}(0))$$

$$+ (E_{i,2}(2\lfloor (N+1)/2 \rfloor - 1) - E_{i,2}(-1))$$

$$\leq 2E_{i,2}(N).$$
(24)

(5) follows from (4) (with r chosen large enough to ensure $c_r > c$) and (24), and this completes the proof of the corollary.

Section 3

Let q(n) denote the number of partitions of n into unequal parts, and let E(n), resp. U(n), be the number of partitions of n into an even, resp. odd, number of unequal parts. It follows from an identity of Euler (see Theorem 358 in [2]) that E(n) = U(n) except when n is a pentagonal number, i.e., $n = s_k = \frac{1}{2}k(3k - 1)$ or $n = t_k = \frac{1}{2}k(3k + 1)$; in these latter cases we have $E(n) - U(n) = (-1)^k$. Since

$$q(n) = E(n) + U(n) \equiv E(n) - U(n) \mod 2,$$

thus q(n) is odd if and only if n is a pentagonal number. In view of this fact, one might like to see that the parities of p(n) and q(n) are independent. We will prove the following result in this direction:

THEOREM 2. Both

$$p(n) \equiv q(n) \bmod 2, n \le N$$

and

$$p(n) \equiv q(n) + 1 \mod 2, n \le N$$

have more than $(\log N)^c$ solutions for N large enough, where c is a fixed positive constant.

Proof. We start out from the well-known recursion formula (cf. [6], p. 44).

$$np(n) = \sum_{i=0}^{n-1} p(i) \sigma(n-i)$$
 (25)

where $\sigma(n)$ denotes the sum of the positive divisors of the positive integer *n*. If *p* is a prime and *r* is a positive integer, then $\sigma(p^r) = 1 + p + p^2 + \dots + p^r$ is odd if and only if either p = 2 or $p \neq 2$ and *r* is even. By the multiplicativity of $\sigma(n)$, it follows that $\sigma(n)$ is odd if and only if *n* is of the form either $n = k^2$ or $n = 2k^2$. Thus we obtain from (25) that

$$np(n) \equiv \sum_{k=1}^{\left[\sqrt{n}\right]} p(n-k^2) + \sum_{k=1}^{\left[\sqrt{n}/2\right]} p(n-2k^2) \mod 2.$$
 (26)

Next, we shall prove a similar formula for q(n), namely,

$$nq(n) \equiv \sum_{k=1}^{\left[\sqrt{n}\right]} q(n-k^2) + \sum_{k=1}^{\left[\sqrt{n}/2\right]} q(n-2k^2) \mod 2.$$
 (27)

Differentiating the function

$$F(x) = \sum_{n=0}^{\infty} q(n) x^n = \prod_{i=1}^{\infty} (1 + x^i), \qquad (28)$$

we get

$$\sum_{n=0}^{\infty} nq(n) x^{n-1} = F(x) \sum_{i=1}^{\infty} \frac{i x^{i-1}}{1+x^{i}}.$$

Multiplying by *x*, we have

$$\sum_{n=0}^{\infty} nq(n) x^n \equiv F(x) \sum_{i=1}^{\infty} \frac{ix^i}{1-x^i} \mod 2.$$
 (29)

Now,

$$\sum_{i=1}^{\infty} \frac{ix^{i}}{1-x^{i}} = \sum_{i=1}^{\infty} \sum_{k=1}^{\infty} ix^{ki} = \sum_{m=1}^{\infty} \left(\sum_{i|m} i\right) x^{m} = \sum_{m=1}^{\infty} \sigma(m) x^{m},$$

and (28) and (29) yield

$$nq(n) \equiv \sum_{i=0}^{n-1} q(i) \sigma(n-i) \mod 2.$$
(30)

Finally (27) follows from (30) in the same way as (26) from (25). Now, write F(n) = p(n) - q(n). From (26) and (30), we get

$$nF(n) \equiv \sum_{k^2 \le n} F(n-k^2) + \sum_{2k^2 \le n} F(n-2k^2) \mod 2.$$
(31)

Let h(n) = 0 for $n \le 1$ and

$$h(n) = 0 \text{ if } F(n) \equiv F(n-2) \mod 2$$

$$h(n) = 1 \text{ if } F(n) \not\equiv F(n-2) \mod 2$$

for $n \ge 2$, and

$$H(N) = \sum_{1 \le n \le N} h(n)$$

We shall prove

$$H(N) \gg (\log N)^{c}, \qquad (32)$$

and then the proof of Theorem 2 can be completed similarly to the proof of the corollary of Theorem 1. Indeed, let us define

$$T_i(N) = \operatorname{card}\{1 \le n \le N, n \equiv N \mod 2, F(n) \equiv i \mod 2\}$$

and $T_i(N) = 0$ for N < 0. Then we have h(n) = 1 if and only if one of F(n)and F(n-2) is odd, and the other even, and this is so if and only if $T_i(n) - T_i(n-4) = 1$ for both i = 0 and i = 1. Thus for both i = 0 and 1, we have

$$H(N) = \sum_{1 \le n \le N} h(n) \le \sum_{n=1}^{N} (T_i(n) - T_i(n-4))$$

= $T_i(N) + T_i(N-1) + T_i(N-2) + T_i(N-3)$
 $\le 2(T_i(N) + T_i(N-1))$
= $2 \operatorname{card} \{n \le N; F(n) \equiv i \mod 2\}$

which, assuming (32), completes the proof of Theorem 2.

Since the proof of (32) is similar to the proof of Theorem 1, we shall leave some details to the reader. Replacing n by n - 2 in (31), and then subtracting we obtain

$$nh(n) \equiv \sum_{k^2 \le n} h(n-k^2) + \sum_{2k^2 \le n} h(n-2k^2) \mod 2.$$
(33)

Let M be a positive integer and let

$$U = \{u, 1 \le u \le M, h(u) = 1\},\$$

$$J = \left\{j, rM < j \le sM, \frac{1}{2r\sqrt{2}} \le \left\{j\sqrt{2}\right\} \le 1 - \frac{1}{2r\sqrt{2}}\right\}$$

where $\{x\}$ denotes the fractional part of x, and r and s are two integers to be

fixed, but such that $2 \le r < s$. Substituting $n = 2u + j^2$ in (33) where $u \in U$, $j \in J$, we obtain

$$\varepsilon_{u}h(2j^{2}+u) + \sum_{k=1}^{\lfloor j\sqrt{2} \rfloor}h(2j^{2}+u-k^{2}) + \sum_{k=1}^{j}h(2j^{2}+u-2k^{2}) \equiv 0 \mod 2$$
(34)

where $\varepsilon_u \equiv u \mod 2$. Here the term $h(2j^2 + u - 2j^2) = h(u) = 1$ appears, thus there is another term equal to 1 so that there is a

$$v = v(j, u) \tag{35}$$

such that h(v) = 1, $v \neq u$, and v can be represented in the form

$$v = 2j^{2} + u, 2j^{2} + u - k^{2} \text{ (with } 1 \le k \le \lfloor j\sqrt{2} \rfloor \text{) or}$$

$$2j^{2} + u - 2k^{2} \text{ (with } 1 \le k \le j - 1).$$
(36)

It follows form (36) that

$$M < v \le (2s^2 + 1)M^2$$
.

If V denotes the number of distinct integers v that can be obtained in form (35) for some $j \in J$, $u \in U$, and for a fixed $v \in V$, l(v) denotes the number of solutions of (35) in j, u, then a simple computation shows that if r, s and $\varepsilon > 0$ are fixed, then for $M > M_0(r, s, \varepsilon)$ we have

$$H((2s^{2}+1)M) - H(M) \ge |V| \ge \frac{|J|H(M)}{\max_{v} l(v)}$$
$$\ge \frac{(1 - 1/(2r\sqrt{2}) - \varepsilon)(s - r)}{(1 + \sqrt{2})s}H(M). \quad (37)$$

The proof can be completed in the same way as the proof of Theorem 1. Observe that choosing r large and, say, $s = r^2$, the constant factor on the right of (37) is close to $1/(1 + \sqrt{2})$, which yields c in Theorem 2 as close to 1/2 as we wish.

Section 4

The problems discussed so far can be generalized by studying the parity of generalized additive representation functions. Indeed, for $A \subset \mathbb{N}$ let r(A, n)

and p(A, n) denote the number of solutions of

$$a + a' = n, a \in A, a' \in A, a \leq a',$$

and

$$a_{i_1} + a_{i_2} + \dots + a_{i_k} = n, a_{i_1}, \dots, a_{i_k} \in A, a_{i_1} \leq \dots \leq a_{i_k}$$

respectively.

Answering a question of the authors, V. Flynn (in a letter written to one of the authors) and I.Z. Ruzsa (oral communication) showed that there are infinitely many (but only countably many) infinite sets $A \subset \mathbf{N}$ such that r(A, n) is either odd or it is even from a certain point on, and the same is true with p(A, n) in place of r(A, n). One might like to study density and other properties of the sets A with these properties; we will return to these problems in a subsequent paper.

In both recursion formulas (1) and (26), sums of the form $\sum_k p(f(k))$ appear where f(k) is a quadratic polynomial. This suggests that, perhaps, there is a quadratic polynomial f(k) such that p(f(k)) is more often odd, than even, or vice versa. Thus we have computed the parity of p(f(k)) up to $k \le 16,000,000$ for each of the polynomials $f(k) = k^2 \pm a$, $a = 0, 1, 2, \ldots, 9$ and, in view of Theorem 2, $f(k) = \frac{1}{2}k(3k \pm 1) \pm a$, $a = 0, 1, 2, \ldots, 9$ (cf. Table 1).

k(3k - 1)k(3k + 1) $k^{2} + a$ + a +an p(n)odd even odd odd even even a = -9-8-7-6 -5 -4 -3-2-1

Table 1

For $-9 \le a \le 9$, this table shows the number of *n*'s satisfying $0 \le n < 16,000,000$ which are of the form $n = k^2 + a$, or n = k(3k - 1)/2 + a or n = k(3k + 1)/2 + a and such that p(n) is odd or even.

It turned out that in each of these cases, the odd values and the even values occur with about the same frequency. This fact, together with several results [1], [7] of the type that p(f(k)) assumes both odd and even values infinitely often for certain special linear polynomials f(k), suggests the following conjecture: If f(k) is a polynomial whose coefficients are integers, then p(f(k)) assumes both odd and even values infinitely often, and, indeed, we have

$$\lim_{N \to +\infty} |\{n: n \le N, p(f(n)) \equiv 0 \mod 2\} | N^{-1} = \frac{1}{2}.$$

Table 1 was calculated by Marc Deléglise on an HP 730. In a first step he calculated $p(n) \mod 2$ up to $n = 16 \cdot 10^6$ by Euler's identity (1), and next he extracted the values of p(f(k)) from the memory.

REFERENCES

- 1. J. FABRYKOWSKI and M.V. SUBBARAO, "Some new identities involving the partition function p(n)" in *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, 1990, pp. 125–138.
- 2. G.H. HARDY and E.M. WRIGHT, An introduction to the theory of numbers, 4th ed., Oxford, Clarendon Press, 1960.
- 3. O. KOLBERG, Note on the parity of the partition function, Math. Scand. 7 (1959), 377-378.
- 4. P.A. MACMAHON, Note on the parity of the number which enumerates the partitions of a number, Proc. Cambridge Philos. Soc. 20 (1920–21), 281–283.
- L. MIRSKY, The distribution of values of the partition function in residue classes, J. Math. Anal. Appl. 93 (1983), 593-598.
- 6. M. NEWMAN, Periodicity modulo m and divisibility properties of the partition function, Trans. Amer. Math. Soc. 97 (1960), 225–236.
- 7. H.H. OSTMANN, Additive zahlentheorie, vol. 1, Springer-Verlag, New York, 1956.
- T.R. PARKIN and D.SHANKS, On the distribution of parity in the partition function, Math. Comp. 21 (1967), 466–480.
- 9. M.V. SUBBARAO, Some remarks on the partition function, Amer. Math. Monthly 73 (1966), 851–854.
- UNIVERSITÉ CLAUDE BERNARD (LYON I) VILLEURBANNE, FRANCE
- MATHEMATICAL INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES BUDAPEST, HUNGARY