Periodica Mathematica Hungarica Vol. 43 (1–2), (2001), pp. 177–189

ON THE PARITY OF GENERALIZED PARTITION FUNCTIONS II

JEAN-LOUIS NICOLAS (Lyon)

To Professors Kálmán Győry and András Sárközy
on the occasion of their 60th birthday

Abstract

Let $\mathcal{A} = \{a_1 < a_2 < \cdots\}$ be a set of positive integers and $A(x)$ its counting function. Let us denote the number of partitions of n with parts in $\mathcal{A}$ by $p(\mathcal{A}, n)$. Improving on two preceding papers jointly written with I.Z. Ruzsa and A. Sárközy (J. Number Theory, 1998) and with A. Sárközy (Millennial Conference on Number Theory, May 2000, Urbana, Illinois, U.S.A.), it is shown that there exists a set $\mathcal{A}$ satisfying $A(x) > c\dfrac{x \log\log x}{(\log x)^{1/3}}$, $c > 0$, such that, for n large enough, $p(\mathcal{A}, n)$ is always even.

1. Introduction

$\mathbb{N}^*$ and $\mathbb{N}$ denote the set of the non-negative integers, resp. positive integers. $\mathcal{A}$ will denote a set of positive integers, and its counting function will be denoted by $A(x)$ so that

$$A(x) = |\{a : a \leq x,\, a \in \mathcal{A}\}|$$

while $A^{\text{odd}}(x)$ will count the number of odd elements of $\mathcal{A}$ up to x:

$$A^{\text{odd}}(x) = |\{a : a \leq x,\, a \in \mathcal{A}, \quad a \text{ odd}\}|.$$

We shall denote by $a \bmod b$ the remainder in the Euclidean division of a by b.

If $\mathcal{A} = \{a_1, a_2, \dots\} \subset \mathbb{N}^*$ (where $a_1 < a_2 < \dots$), then $p(\mathcal{A}, n)$ denotes the number of partitions of n with parts in $\mathcal{A}$, that is the number of solutions of the equation

$$a_1 x_1 + a_2 x_2 + \cdots = n$$

in non-negative integers $x_1, x_2, \dots$. As usual, we shall set $p(\mathcal{A}, 0) = 1$. In the papers [3] and [4] we have shown that if $\mathcal{B} = \{b_1, \dots, b_k\} \neq \emptyset$ (where $b_1 < \cdots < b_k$) is a finite set of positive integers, $N = b_k = \max \mathcal{B}$, then there is a unique set $\mathcal{A} \subset \mathbb{N}$

Research partially supported by French–Hungarian APAPE-OMFB exchange program F-5/1997 and CNRS, Institut Girard Desargues, UMR 5028.
Mathematics subject classification number: 11P81.
Key words and phrases: partitions, generating functions, parity of partition functions.

0031-5303/01/$5.00
© Akadémiai Kiadó, Budapest

Akadémiai Kiadó, Budapest
Kluwer Academic Publishers, Dordrecht

such that

$$\mathcal{A} \cap \{1, 2, \ldots, N\} = \mathcal{B}$$

and

$$p(\mathcal{A}, n) \equiv 0 \,(\mathrm{mod}\, 2) \quad \text{for} \quad n \in \mathbb{N},\, n > N.$$

We will denote this set $\mathcal{A}$ by $\mathcal{A}_0(\mathcal{B})$. The construction of the set $\mathcal{A}_0(\mathcal{B})$ is described in [3] and in [4]; let us recall it below. The set $\mathcal{A} = \mathcal{A}_0(\mathcal{B})$ will be defined by recursion. We write $\mathcal{A}_n = \mathcal{A} \cap \{1, 2, \ldots, n\}$ so that

$$\mathcal{A}_N = \mathcal{A} \cap \{1, 2, \ldots, N\} = \mathcal{B}.$$

Assume that $n \geq N + 1$ and $\mathcal{A}_{n-1}$ has been defined so that $p(\mathcal{A}, m)$ is even for $N + 1 \leq m \leq n - 1$. Then set

$$n \in \mathcal{A} \quad \text{if and only if} \quad p(\mathcal{A}_{n-1}, n) \quad \text{is odd.}$$

It follows from the construction that for $n \geq N + 1$ we have

$$\text{if } n \in \mathcal{A}, \quad p(\mathcal{A}, n) = 1 + p(\mathcal{A}_{n-1}, n)$$

$$\text{if } n \notin \mathcal{A}, \quad p(\mathcal{A}, n) = p(\mathcal{A}_{n-1}, n)$$

which shows that $p(\mathcal{A}, n)$ is even for $n \geq N + 1$.

We will use the following notation: If $\mathcal{A} \subset \mathbb{N}$, then $\chi(\mathcal{A}, n)$ denotes the characteristic function of $\mathcal{A}$, i.e.,

$$\chi(\mathcal{A}, n) = \begin{cases} 1 & \text{if } n \in \mathcal{A} \\ 0 & \text{if } n \notin \mathcal{A}. \end{cases}$$

Moreover, we define for $n \geq 1$

$$(1) \qquad \sigma(\mathcal{A}, n) = \sum_{d|n} \chi(\mathcal{A}, d) d = \sum_{d|n,\ d \in \mathcal{A}} d.$$

It was proved in [3] that for all sets $\mathcal{A} \subset \mathbb{N}^*$ and $n \geq 1$

$$(2) \qquad np(\mathcal{A}, n) = \sum_{k=0}^{n-1} p(\mathcal{A}, k) \sigma(\mathcal{A}, n - k).$$

As $p(\mathcal{A}, n)$ is even for $n > N = \max \mathcal{B}$, it follows from (2) that $\sigma(\mathcal{A}, n) \bmod 2$ satisfies a linear recurrence relation of order N (cf. (4.6) of [4]):

$$(3) \qquad \sigma(\mathcal{A}, n) \equiv \sum_{k=1}^{N} p(\mathcal{A}, k) \sigma(\mathcal{A}, n - k) \qquad (\mathrm{mod}\ 2),$$

and so, that $\sigma(\mathcal{A}, n) \bmod 2$ is periodic, and its period (let us denote it by $q = q(\mathcal{A})$) satisfies $q \leq 2^N$.

Let μ denote the Möbius function. By applying the Möbius inversion formula to (1), it was proved in Lemma 1 of [4] that

$$(4) \qquad n\chi(\mathcal{A}, n) = \sum_{d|n} \mu(d) \sigma(\mathcal{A}, n/d)$$

which implies, if n is odd, that

$$(5) \qquad \chi(\mathcal{A}, n) = \sum_{d|n} \mu(d) \sigma(\mathcal{A}, n/d) \bmod 2.$$

In [3] and [4] we paid some attention to two particular sets of this form, the sets $\mathcal{A} = \mathcal{A}_0(\mathcal{B})$ when $\mathcal{B} = \{1, 2, 3\}$ and $\mathcal{B} = \{1, 2, 3, 4, 5\}$.

For the first set $\mathcal{A} = \mathcal{A}_0(\{1, 2, 3\})$, it was proved in [3] that the period q of $\sigma(\mathcal{A}, n) \bmod 2$ is equal to 7. Further, in [4] (Theorem 1), by applying (5) and taking into account the periodicity of $\sigma(\mathcal{A}, n) \bmod 2$, it was proved that the odd elements of $\mathcal{A}$ are of the following form: $n = 1$, or $n = p^\alpha$ or $n = 7p^\alpha$ where p is a prime $\equiv 3, 5$ or $6 \pmod 7$ and $\alpha \geq 1$, so that

$$A(x) \geq A^{\mathrm{odd}}(x) = \left(\frac{4}{7} + o(1)\right) \frac{x}{\log x}, \quad x \to \infty.$$

Moreover, our calculations suggested that for any $h \geq 1$, the sequence

$$(6) \qquad \sigma(\mathcal{A}, 2^h n) \quad \mathrm{mod} \quad 2^{h+1} \quad \text{is periodic in } n$$

with period 7, and more precisely we have formulated the following conjecture:

CONJECTURE. *For $h \geq 1$, we write $u_h = \sigma(\mathcal{A}, 3 \cdot 2^h)$, $v_h = \sigma(\mathcal{A}, 2^h)$. If n is any positive integer, then*

$$(7) \qquad \sigma(\mathcal{A}, 2^h n) \equiv u_h, v_h, -3 \pmod{2^{h+1}} \quad \textit{as} \quad \left(\frac{n}{7}\right) = -1, +1, 0, \quad \textit{respectively.}$$

This conjecture has been checked up to $n = 10000$ by computer. By assuming this conjecture and using (4), a precise description of even elements of $\mathcal{A}$ can be given from which it follows that there exists a constant c_1 such that $A(x) \sim c_1 \dfrac{x}{(\log x)^{3/4}}$. I hope to return to this topics in another paper.

The second set $\mathcal{A} = \mathcal{A}_0(\{1, 2, 3, 4, 5\})$ was studied in [4]. The period q of $\sigma(\mathcal{A}, n) \bmod 2$ is equal to 31, and it was proved (cf. Lemma 4 of [4]) that if $q_1 < q_2 < \cdots < q_k$ are primes congruent to 5 modulo 31, and $k \equiv 1, 2 \pmod 3$ then $n = q_1 q_2 \ldots q_k \in \mathcal{A}$. The multiplicative structure of odd elements of $\mathcal{A}$ will be given in Section 3, Theorem 1, from which it will follow (cf. Theorem 2) that

$$(8) \qquad A(x) \geq A^{\mathrm{odd}}(x) \sim c_2 \frac{x \log\log x}{(\log x)^{1/3}}$$

for some constant c_2.

It has been observed that (6) is satisfied with period 31 up to $n = 10000$, so that a conjecture looking like (7) can be formulated, from which, in principle, the structure of even elements of $\mathcal{A}$ can be determined explicitly. But the calculation is not simple and has not yet been carried out.

The proof of Theorem 1 is mainly based upon formula (5). The behaviour of some sums involving binomial coefficients will also be needed and exposed in Section 2.

2. Binomial coefficients

For $m \geq 0$, a any integer, and $s \geq 1$, let us define

$$S(m;s,a) = \sum_{\substack{0 \leq r \leq m \\ r \equiv a \pmod{s}}} \binom{m}{r}.$$

The following lemmas hold:

LEMMA 1. *For a fixed, the function $m \mapsto S(m;3,a)$ is periodic with period 3 for $m \geq 1$. More precisely, for $m \geq 1$*

$$S(m;3,a) \equiv \begin{cases} 0 \pmod 2 & \text{if } m+a \equiv 0 \pmod 3 \\ 1 \pmod 2 & \text{if } m+a \equiv 1 \text{ or } 2 \pmod 3. \end{cases} \tag{9}$$

PROOF. This is Lemma 3 of [4]. The proof is easy. Note that the function $m \mapsto S(m;3,a)$ is periodic from $m = 1$ but not from $m = 0$.

LEMMA 2. *For a fixed, the function $m \mapsto S(m;6,a)$ is periodic with period 6 for $m \geq 2$. More precisely, for $m \geq 2$*

(10) *if m is even,* $S(m;6,a) \equiv 1 \pmod 2 \iff m+a \equiv 2$ *or* $4 \pmod 6$

and

(11) *if m is odd,* $S(m;6,a) \equiv 0 \pmod 2 \iff m+a \equiv 1$ *or* $2 \pmod 6$.

PROOF. The classical relation

$$\binom{m}{r} = \binom{m-1}{r} + \binom{m-1}{r-1}$$

implies for $m \geq 1$

$$S(m;6,a) = S(m-1;6,a) + S(m-1;6,a-1)$$

and for $m \geq 2$

$$S(m;6,a) = S(m-2;6,a) + 2S(m-2;6,a-1) + S(m-2;6,a-2).$$

By reduction modulo 2, we get

$$S(m;6,a) \equiv S(m-2;6,a) + S(m-2;6,a-2) \pmod 2. \tag{12}$$

Substituting $m-2$ to m and $a-2$ to a in the above congruence yields for $m \geq 4$

$$S(m-2;6,a-2) \equiv S(m-4;6,a-2) + S(m-4;6,a-4) \pmod 2. \tag{13}$$

But, for $m \geq 6$, the right hand side of (13) is congruent to $S(m-4;6,a)$ modulo 2 since

$$S(m-4;6,a) + S(m-4;6,a-2) + S(m-4;6,a-4) = S(m-4;2,a) = 2^{m-5},$$

so that, from (12) and (13), it follows for $m \geq 6$

$$S(m;6,a) \equiv S(m-2;6,a) + S(m-4;6,a) \pmod 2. \tag{14}$$

Let us set $x_n = S(2n;6,a) \bmod 2$ and $y_n = S(2n+1;6,a) \bmod 2$. Then, from (14), for any a, the sequences x_n and y_n satisfy a linear recurrence relation modulo 2, $x_{n+2} = x_{n+1} + x_n$ and $y_{n+2} = y_{n+1} + y_n$. There are exactly four such possible sequences, they are all periodic of period 3, and so the function $m \mapsto S(m;6,a) \bmod 2$ is periodic with period 6 for $m \geq 2$. The following array completes the proof of Lemma 2.

Table of $S(m;6,a) \bmod 2$

	$a=0$	$a=1$	$a=2$	$a=3$	$a=4$	$a=5$
$m=0$	1	0	0	0	0	0
$m=1$	1	1	0	0	0	0
$m=2$	1	0	1	0	0	0
$m=3$	1	1	1	1	0	0
$m=4$	1	0	0	0	1	0
$m=5$	1	1	0	0	1	1
$m=6$	0	0	1	0	1	0
$m=7$	0	0	1	1	1	1

3. Odd elements of the set $\mathcal{A} = \mathcal{A}_0(\{1,2,3,4,5\})$

In this section, $\mathcal{A}$ will be the set $\mathcal{A} = \mathcal{A}_0(\{1,2,3,4,5\})$. By a simple computation, the period $q = q(\mathcal{A})$ of $\sigma(\mathcal{A},n) \bmod 2$ is shown to be 31 and

$$\sigma(\mathcal{A},n) \equiv 0 \pmod 2$$

if and only if

$$n \equiv 3,5,6,7,9,10,12,14,17,18,19,20,24,25,28 \pmod{31}. \tag{15}$$

Fortunately, the set of the fifteen residue classes of (15) is not completely random. It is stable by multiplication by 2. This is a general phenomenon since, indeed, for all $\mathcal{A}$ and n, we have

$$\sigma(\mathcal{A},2n) \equiv \sum_{d \mid n,\ d \text{ odd}} d \equiv \sigma(\mathcal{A},n) \pmod 2. \tag{16}$$

The order of 2 in $(\mathbb{Z}/31\mathbb{Z})^*$ is 5, so that (15) can be reformulated as

$$n \equiv 3 \cdot 2^a \text{ or } 5 \cdot 2^a \text{ or } 7 \cdot 2^a \pmod{31}, \quad 0 \le a \le 4. \tag{17}$$

The smallest primitive root modulo 31 is 3 that we shall choose as a generator of $(\mathbb{Z}/31\mathbb{Z})^*$. For every integer n not divisible by 31, there is a unique residue class $\log_3(n) \in (\mathbb{Z}/30\mathbb{Z})$ such that

$$n \equiv 3^{\log_3(n)} \pmod{31}. \tag{18}$$

Let us define the function $\ell : \mathbb{Z} \setminus 31\mathbb{Z} \to (\mathbb{Z}/6\mathbb{Z})$ by

$$\ell(n) = \log_3(n) \bmod 6. \tag{19}$$

Table of $\ell(n)$

$n =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\log_3(n) =$	30	24	1	18	20	25	28	12	2	14	23	19	11	22	21
$\ell(n) =$	0	0	1	0	2	1	4	0	2	2	5	1	5	4	3

$n =$	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\log_3(n) =$	6	7	26	4	8	29	17	27	13	10	5	3	16	9	15
$\ell(n) =$	0	1	2	4	2	5	5	3	1	4	5	3	4	3	3

Since the discrete logarithm is completely additive, the funtion ℓ is also completely additive, which means $\ell(mn) = \ell(m) + \ell(n)$ for all m, n coprime with 31. It follows from the definition of ℓ that (15) or (17) are equivalent to

$$\sigma(\mathcal{A}, n) \equiv 0 \pmod 2 \quad \text{if and only if} \quad \ell(n) \equiv 1 \text{ or } 2 \text{ or } 4 \pmod 6. \tag{20}$$

Now, let us split the odd primes (different from 31) in six classes according to the value of ℓ. More precisely, for $0 \le i \le 5$,

$$p \in \mathcal{P}_i \quad \text{if and only if} \quad \ell(p) = i. \tag{21}$$

Further, we define the functions $\omega_i(n)$ by

$$\omega_i(n) = \sum_{p \mid n,\ p \in \mathcal{P}_i} 1. \tag{22}$$

We shall prove

THEOREM 1. (a) *The odd elements of $\mathcal{A} = \mathcal{A}_0(\{1,2,3,4,5\})$ which are primes or powers of primes are of the form p^α, $\alpha \ge 1$, satisfying one of the following four conditions:*

$$\begin{array}{lll} p \in \mathcal{P}_1 & \text{and} & \alpha \equiv 1,3,4,5 \pmod 6 \\ p \in \mathcal{P}_2 & \text{and} & \alpha \equiv 0,1 \pmod 3 \\ p \in \mathcal{P}_4 & \text{and} & \alpha \equiv 0,1 \pmod 3 \\ p \in \mathcal{P}_5 & \text{and} & \alpha \equiv 0,2,3,4 \pmod 6. \end{array}$$

(b) *No odd element of $\mathcal{A}$ is a multiple of 31^2. If m is odd, $m \ne 1$, and not a multiple of 31, then*

$$m \in \mathcal{A} \quad \text{if and only if} \quad 31 \cdot m \in \mathcal{A}. \tag{23}$$

(c) *An odd element $n \in \mathcal{A}$ satisfies $\omega_0(n) = 0$ and $\omega_3(n) = 0$ or 1; in other words, n is free of prime factors $p \in \mathcal{P}_0$ and has at most one prime factor in $\mathcal{P}_3$.*

(d) *The odd elements of $\mathcal{A}$ different from 1, not divisible by 31, which are not primes or powers of primes are exactly the odd n's, $n \ne 1$, such that (where $\overline{n} = \prod_{p \mid n} p$ is the radical of n):*

(i) $\omega_0(n) = 0$ *and* $\omega_3(n) = 0$ *or* 1;

(ii) *If* $\omega_3(n) = 1$ *then* $\ell(n) + \ell(\overline{n}) \equiv 0$ *or* $1 \pmod 3$.

(iii) *If* $\omega_3(n) = 0$ *and* $\omega_1(n) + \ell(n) - \ell(\overline{n})$ *is even then*

$$2\ell(n) - \ell(\overline{n}) \equiv 2 \quad \text{or} \quad 3 \quad \text{or} \quad 4 \quad \text{or} \quad 5 \pmod 6.$$

(iv) *If* $\omega_3(n) = 0$ *and* $\omega_1(n) + \ell(n) - \ell(\overline{n})$ *is odd then*

$$2\ell(n) - \ell(\overline{n}) \equiv 0 \quad \text{or} \quad 4 \pmod 6.$$

PROOF OF (a). When n is a prime p, formula (5) writes

$$\chi(\mathcal{A}, p) = (\sigma(\mathcal{A}, p) + 1) \bmod 2$$

so that $p \in \mathcal{A}$ if and only if $\sigma(\mathcal{A}, p) \equiv 1 \pmod 2$ which, from (20), is equivalent to $p \in \mathcal{P}_1 \cup \mathcal{P}_2 \cup \mathcal{P}_4$.

For $n = p^\alpha$, $\alpha \ge 2$, formula (5) writes

$$\chi(\mathcal{A}, p^\alpha) = (\sigma(\mathcal{A}, p^\alpha) + \sigma(\mathcal{A}, p^{\alpha-1})) \bmod 2. \tag{24}$$

If $p \in \mathcal{P}_0$, $\ell(p^\alpha) = \ell(p^{\alpha-1}) = 0$, and, by (20), $\sigma(\mathcal{A}, p^\alpha) \equiv \sigma(\mathcal{A}, p^{\alpha-1}) \equiv 1 \pmod 2$ which implies, from (24), that $p^\alpha \notin \mathcal{A}$ for all α.

If $p \in \mathcal{P}_3$, $\{\ell(p^\alpha), \ell(p^{\alpha-1})\} = \{0, 3\}$, and, by (20), $\sigma(\mathcal{A}, p^\alpha) \equiv \sigma(\mathcal{A}, p^{\alpha-1}) \equiv 1 \pmod 2$ which, as above, implies that $p^\alpha \notin \mathcal{A}$ for all α.

If $p \in \mathcal{P}_i$, for $i \ne 0, 3$ it follows from the periodicity of ℓ that $\chi(\mathcal{A}, p^\alpha)$ is periodic in α, with period 6. So we have to examine the six possibilities $2 \le \alpha \le 7$. For instance, when $p \in \mathcal{P}_1$,

$\alpha =$	2	3	4	5	6	7
$\ell(p^\alpha) =$	2	3	4	5	0	1
$\ell(p^{\alpha-1}) =$	1	2	3	4	5	0
$\sigma(\mathcal{A},p^\alpha) \bmod 2 =$	1	0	1	0	0	1
$\sigma(\mathcal{A},p^{\alpha-1}) \bmod 2 =$	1	1	0	1	0	0
$\chi(\mathcal{A},p^\alpha) =$	0	1	1	1	0	1

The case $p \in \mathcal{P}_5$ is similar. In the cases $p \in \mathcal{P}_2$ or $p \in \mathcal{P}_4$ it suffices to consider $2 \le \alpha \le 4$.

Proof of (b). Let us suppose that some odd element of $\mathcal{A}$ is a multiple of 31^2, and let us choose n as the smallest integer having this property. Let us write $n = 31^2 \cdot m$. From the choice of n, the only divisor of n such that $31^2 \mid d$ and $d \in \mathcal{A}$ is n, so that from (1),

$$\sigma(\mathcal{A},n) = \sigma(\mathcal{A},31\cdot m) + n. \tag{25}$$

But, from (15), $\sigma(\mathcal{A},n) \equiv \sigma(\mathcal{A},31\cdot m) \equiv 1 \pmod 2$, which contradicts (25).

Now, let m be an odd element of $\mathcal{A}$, not divisible by 31, and let us set $n = 31 \cdot m$. From (5), we have

$$\chi(\mathcal{A},n) = \left(\sum_{d\mid m} \mu(d)\sigma\left(\frac{n}{d}\right) + \sum_{d\mid m} \mu(d)\sigma\left(\frac{n}{31\cdot d}\right)\right) \bmod 2. \tag{26}$$

But, in (26), the second sum is, by (5), congruent to $\chi(\mathcal{A},m) = 1$ modulo 2, while, since n/d is a multiple of 31, the first sum is, from (15), equal to $\sum_{d\mid m} \mu(d) = 0$, for $m \ne 1$. Therefore, $\chi(\mathcal{A},n) = \chi(\mathcal{A},m) = 1$ which completes the proof of (b).

Proof of (c). First, we shall prove that no odd element of $\mathcal{A}$ is a multiple of a prime $p \in \mathcal{P}_0$. Let us suppose the contrary, and let us denote by $n = pm$ the smallest odd element of $\mathcal{A}$ which is a multiple of a prime $p \in \mathcal{P}_0$. From our minimality hypothesis, the only divisor of n which is a multiple of p and belongs to $\mathcal{A}$ is n so that (1) becomes

$$\sigma(\mathcal{A},n) = \sigma(\mathcal{A},m) + n. \tag{27}$$

But $\ell(n) = \ell(m) + \ell(p) = \ell(m)$ which implies by (20) that $\sigma(\mathcal{A},n) \equiv \sigma(\mathcal{A},m) \pmod 2$, in contradiction with (27).

We shall now prove that, if n is odd and belongs to $\mathcal{A}$, $\omega_3(n) \le 1$. Let us assume that there is some odd integer in $\mathcal{A}$ divisible by two distinct primes $p, q \in \mathcal{P}_3$, and let us denote the smallest such element by n. We can write

$$n = p^\alpha q^\beta m, \qquad (pq,m) = 1, \quad \alpha \ge 1, \quad \beta \ge 1. \tag{28}$$

The only divisor d of n which is a multiple of pq and belongs to $\mathcal{A}$ is n itself, and from (1), we have

$$\sigma(\mathcal{A},n) = \sigma(\mathcal{A},p^\alpha m) + \sigma(\mathcal{A},q^\beta m) - \sigma(\mathcal{A},m) + n. \tag{29}$$

But, from (28), $\ell(n) \equiv \ell(m) + 3(\alpha+\beta) \pmod 6$.

- If $\alpha \equiv \beta \pmod 2$, we have $\ell(n) = \ell(m)$ and thus, from (15), $\sigma(\mathcal{A},n) \equiv \sigma(\mathcal{A},m) \pmod 2$; moreover, $\ell(p^\alpha m) = \ell(q^\beta m)$ and thus

$$\sigma(\mathcal{A},p^\alpha m) \equiv \sigma(\mathcal{A},q^\beta m) \pmod 2,$$

so that (29) leads to a contradiction.

- If $\alpha \not\equiv \beta \pmod 2$, we can assume for instance that α is even and β is odd. Then, from (28), we have $\ell(n) = \ell(q^\beta m)$, so that $\sigma(\mathcal{A},n) \equiv \sigma(\mathcal{A},q^\beta m) \pmod 2$ and $\ell(m) = \ell(p^\alpha m)$, which implies $\sigma(\mathcal{A},m) \equiv \sigma(\mathcal{A},p^\alpha m)$, which again contradicts (29).

Proof of (d). Now, an odd element of $n \in \mathcal{A}$, $n \ne 1$, $31 \nmid n$, can be written as

$$n = p_{1,1}^{\alpha_{1,1}} \cdots p_{1,k_1}^{\alpha_{1,k_1}} p_{2,1}^{\alpha_{2,1}} \cdots p_{2,k_2}^{\alpha_{2,k_2}} \cdots\cdots p_{5,1}^{\alpha_{5,1}} \cdots p_{5,k_5}^{\alpha_{5,k_5}}, \tag{30}$$

with $k_r = \omega_r(n)$, $p_{r,j} \in \mathcal{P}_r$ (for $1 \le r \le 5$ and $j \ge 1$) and $0 \le k_3 = \omega_3(n) \le 1$. The radical $\overline{n}$ of n writes

$$\overline{n} = p_{1,1} \cdots p_{1,k_1} p_{2,1} \cdots p_{2,k_2} \cdots\cdots p_{5,1} \cdots p_{5,k_5} = \overline{n_1}\,\overline{n_2}\,\overline{n_3}\,\overline{n_4}\,\overline{n_5},$$

with $\overline{n_r} = \prod_{p\mid n,\ p\in\mathcal{P}_r} p = p_{r,1} \cdots p_{r,k_r}$. A divisor d of $\overline{n}$ can be written in one and only one way as $d = d_1d_2d_3d_4d_5$, with d_r dividing $\overline{n_r}$, so that, (5) can be written as

$$\chi(\mathcal{A},n) = \left(\sum_{d_1\mid\overline{n_1}} \sum_{d_2\mid\overline{n_2}} \cdots \sum_{d_5\mid\overline{n_5}} \sigma(\mathcal{A},n'd_1d_2d_3d_4d_5)\right) \bmod 2, \tag{31}$$

where $n' = n/\overline{n}$. In (31), the value of $\sigma(\mathcal{A},n'd_1d_2d_3d_4d_5) \bmod 2$ depends only, by (20), on $\ell(n'), \ell(d_1), \dots, \ell(d_5)$, i.e. on the values of $\ell(n')$ and of $i_r = \omega_r(d_r)$, $1 \le r \le 5$. So, taking (20) into account, (31) can be rewritten as

$$\chi(\mathcal{A},n) = \sum_{i_1=0}^{k_1}\binom{k_1}{i_1}\sum_{i_2=0}^{k_2}\binom{k_2}{i_2}\cdots\sum_{\substack{i_5=0\\ i_1+2i_2+\cdots+5i_5+\ell(n')\equiv 1,2,4 \pmod 6}}^{k_5}\binom{k_5}{i_5} \bmod 2. \tag{32}$$

By defining

(33)

$$f(k_1,k_2,k_3,k_4,k_5,b) = \left(\sum_{i_1=0}^{k_1}\binom{k_1}{i_1}\sum_{i_2=0}^{k_2}\binom{k_2}{i_2}\cdots\sum_{\substack{i_5=0\\ i_1+2i_2+\cdots+5i_5+b\equiv 1,2,4 \pmod 6}}^{k_5}\binom{k_5}{i_5}\right) \bmod 2,$$

formula (32) becomes

$$\chi(\mathcal{A}, n) = f(k_1, k_2, k_3, k_4, k_5, \ell(n')). \tag{34}$$

For i_1, i_2, i_3, i_4, b fixed, the last summation of (33) can be evaluated in terms of sums $S(m; 6, a)$ introduced in Section 2. We have

$$\sum_{\substack{i_5=0 \\ i_1+2i_2+\cdots+5i_5+b\equiv 1,2,4 \pmod 6}}^{k_5} \binom{k_5}{i_5} \equiv \tag{35}$$

$$S(k_5; 6, a-1) + S(k_5; 6, a-2) + S(k_5; 6, a-4) \pmod 2, \tag{36}$$

where $a = i_1 + 2i_2 + 3i_3 + 4i_4 + b$, and, from Lemma 2, the sum in (35) is periodic of period 6 for all quintuplets (i_1, i_2, i_3, i_4, b). Therefore, $f(k_1, k_2, k_3, k_4, k_5, b)$ is periodic in k_5 with period 6 for $k_5 \geq 2$. Similarly, by changing the order of summation in (33), it is possible to show that f is periodic in $k_1 \geq 2$ with period 6, and on $k_2, k_4 \geq 1$ with period 3. Clearly f is also periodic in b with period 6.

First proof of (ii), (iii) and (iv). From (34) and the periodicity of f, it follows that $\chi(\mathcal{A}, n)$ is periodic in k_1,k_2, k_4, k_5 and $\ell(n')$, so that, it suffices to calculate $f(k_1, k_2, k_3, k_4, k_5, b)$ for

$$0 \leq k_1, k_5 \leq 7, \quad 0 \leq k_2, k_4 \leq 3, \quad 0 \leq k_3 \leq 1, \quad 0 \leq b \leq 5, \tag{37}$$

that is 12288 values of f.

Simultaneously, the conditions in (ii), (iii), (iv) bearing on $\omega_1(n) = k_1$, $\ell(\overline{n}) = k_1 + 2k_2 + 3k_3 + 4k_4 + 5k_5 \bmod 6$, $\ell(n) = \ell(n') + \ell(\overline{n})$ are also periodic with period 6 on $k_1, k_5, \ell(n')$ and with period 3 on k_2, k_4 so that, to prove (ii), it suffices to check that, in the ranges (37), (38) is equivalent to (39), with

$$f(k_1, k_2, 1, k_4, k_5, b) = 1, \tag{38}$$

$$b + 2(k_1 + 2k_2 + 3 + 4k_4 + 5k_5) \equiv 0, 1 \pmod 3. \tag{39}$$

Similarly, to prove (iii) and (iv), it suffices to check that, in the ranges (37), (40) is equivalent to (41) or (42), with

$$f(k_1, k_2, 0, k_4, k_5, b) = 1, \tag{40}$$

$$k_1 + b \ \text{ is odd and } 2b + (k_1 + 2k_2 + 4k_4 + 5k_5) \equiv 2, 3, 4, 5 \pmod 6, \tag{41}$$

or

$$k_1 + b \ \text{ is even and } 2b + (k_1 + 2k_2 + 4k_4 + 5k_5) \equiv 0, 4 \pmod 6. \tag{42}$$

By computer, these equivalences have been checked for all the values of (37) except the cases where one of the k_i is equal to 1 and the four others vanish, which correspond to those n's that are primes or powers of primes.

A theoretical proof for (ii). In the case $k_3 = 1$, and $k_i \geq 1$ for $i = 1, 2, 4, 5$, we shall give a theoretical proof of (ii); it would be also possible to extend this proof to the case $k_3 = 0$, but then we should have to use Lemma 2 instead of Lemma 1, and it is more complicated.

Let us start with the value of f given by (33), and let us permute the summations so that to finish by the summation on i_3. So, the last sum writes, for i_1, i_2, i_4, i_5, b fixed

$$W_3 = \left(\sum_{\substack{i_3=0 \\ i_1+2i_2+3i_3+4i_4+5i_5+b\equiv 1,2,\text{ or } 4 \pmod 6}}^{k_3} \binom{k_3}{i_3} \right) \bmod 2. \tag{43}$$

Let us define

$$T(k_3, u) = \left(\sum_{\substack{i_3=0 \\ 3i_3\equiv u \pmod 6}}^{k_3} \binom{k_3}{i_3} \right) \bmod 2. \tag{44}$$

As in (35) and (36), the sum W_3 in (43) satisfies

$$W_3 \equiv T(k_3, v_3 - 1) + T(k_3, v_3 - 2) + T(k_3, v_3 - 4) \pmod 2, \tag{45}$$

with $v_3 = i_1 + 2i_2 + 4i_4 + 5i_5 + b$.

Note that the congruence

$$3i_3 \equiv w \pmod 6 \tag{46}$$

either has no solution, or has $i_3 \equiv 0$ or $1 \pmod 2$ as solution, so that, if in (44), k_3 were larger than 1, $T_3(k, u)$ would be either the empty sum, or equal to $S(k_3; 2, a)$ for $a = 0$ or $a = 1$. In any case, $T_3(k, u)$ would vanish; so would do W_3 from (45), f from (33) and $\chi(\mathcal{A}, n)$ from (32), and we find again a proof that $k_3 = \omega_3(n)$ should be at most 1 for an odd element $n \in \mathcal{A}$.

For $k_3 = 1$, we have $T(1, u) = 1$ if and only if $u \equiv 0 \pmod 3$, so that, in (45), $T(k_3, v_3 - 1) = T(k_3, v_3 - 4)$ and $W_3 = T(k_3, v_3 - 2)$, whence $W_3 = 1$ if and only if $v_3 \equiv 2 \pmod 3$.

Further, to evaluate f, we have to calculate

$$W_5 = \left(\sum_{i_5=0}^{k_5} \binom{k_5}{i_5} W_3 \right) \bmod 2 = \left(\sum_{\substack{i_5=0 \\ v_3\equiv 2 \pmod 3}}^{k_5} \binom{k_5}{i_5} \right) \bmod 2, \tag{47}$$

and, since $v_3 \equiv 2 \pmod 3$ can be written as $i_5 \equiv v_5 \pmod 3$, with $v_5 = i_1 + 2i_2 + 4i_4 + b + 1$, it follows from (47) that

$$W_5 = \left(\sum_{\substack{i_5=0 \\ i_5\equiv v_5 \pmod 3}}^{k_5} \binom{k_5}{i_5} \right) \bmod 2 = S(k_5; 3, v_5) \bmod 2.$$

From Lemma 1, since $k_5 \geq 1$, $W_5 = 1$ if and only if $k_5 + v_5 \equiv 1, 2 \pmod 3$.

Then, we have to calculate

$$W_4 = \left(\sum_{i_4=0}^{k_4} \binom{k_4}{i_4} W_5 \right) \bmod 2 = \left(\sum_{\substack{i_4=0 \\ v_5+k_5 \equiv 1,2 \pmod 3}}^{k_4} \binom{k_4}{i_4} \right) \bmod 2,$$

and we find, with $v_4 = -(k_5 + i_1 + 2i_2 + b + 1)$

$$W_4 = (S(k_4; 3, v_4 + 1) + S(k_4; 3, v_4 + 2)) \bmod 2 = S(k_4; 3, v_4) \bmod 2,$$

since we have assumed $k_4 \geq 1$.

Similarly, the next sum is

$$W_2 = \left(\sum_{i_2=0}^{k_2} \binom{k_2}{i_2} W_4 \right) \bmod 2 = \left(\sum_{\substack{i_2=0 \\ v_4+k_4 \equiv 1,2 \pmod 3}}^{k_2} \binom{k_2}{i_2} \right) \bmod 2$$
$$= S(k_2; 3, v_2) \bmod 2,$$

with $v_2 = -k_4 + k_5 + i_1 + b + 1$.

The last sum is

$$W_1 = \left(\sum_{i_1=0}^{k_1} \binom{k_1}{i_1} W_4 \right) \bmod 2 = \left(\sum_{\substack{i_1=0 \\ v_2+k_2 \equiv 1,2 \pmod 3}}^{k_1} \binom{k_1}{i_1} \right) \bmod 2$$
$$= S(k_1; 3, v_1) \bmod 2,$$

with $v_1 = -k_2 + k_4 - k_5 - b - 1$. From Lemma 1, it follows that (38), i.e. $f(k_1, k_2, 1, k_4, k_5, b) = W_1 = 1$ is equivalent to $k_1 + v_1 \equiv 1, 2 \pmod 3$, which is exactly (39).

THEOREM 2. *Let $\mathcal{A} = \mathcal{A}_0(\{1, 2, 3, 4, 5\})$. The number $A^{\mathrm{odd}}(x)$ of odd elements of $\mathcal{A}$ up to x satisfies the following asymptotic estimate:*

$$A^{\mathrm{odd}}(x) = (c_2 + o(1))x \frac{\log\log x}{(\log x)^{1/3}}, \tag{48}$$

for some positive constant c_2.

SKETCH OF THE PROOF OF THEOREM 2. Let $\mathcal{E}$ be the set of odd integers free of primes $p \in \mathcal{P}_0 \cup \mathcal{P}_3$. By classical sieve methods (cf., for instance, [2], Theorem 3.5), it is easy to see that

$$E(x) \ll \frac{x}{(\log x)^{1/3}} \cdot \tag{49}$$

The number of $n \in \mathcal{A}$, not multiple of 31, with $\omega_3(n) = 1$ is, from Theorem 1, smaller than

$$\sum_{p^\alpha \leq x,\ p \in \mathcal{P}_3} E\left(\frac{x}{p^\alpha}\right). \tag{50}$$

By usual methods in prime number theory, the sum in (50) can be, from (49), bounded above by $Cx\frac{\log\log x}{(\log x)^{1/3}}$, where C is a large enough constant. So, from Theorem 1, an upper bound for $A^{\mathrm{odd}}(x)$ can be given which is of the same order of magnitude as the right hand side of (48).

It is possible to prove (48) by using a Selberg–Delange type formula (cf. [5], II.5) to estimate the sum

$$U(x, y, z) = \sum_{n \leq x} \rho(n) y^{\omega_3(n)} z^{\ell(n)+\ell(\overline{n})} \tag{51}$$

where $\rho(n)$ is the completely multiplicative function defined by $\rho(p) = 0$ if $p \in \mathcal{P}_0$ and $\rho(p) = 1$ if $p \notin \mathcal{P}_0$, and z is a cubic root of unity. A similar evaluation was outlined in [4]. The full proof will appear in [1].

REFERENCES

[1] F. BEN SAÏD AND J.-L. NICOLAS, Sur une extension de la formule de Selberg–Delange, to be published.

[2] H. HALBERSTAM AND H.-E. RICHERT, *Sieve Methods*, Academic Press, 1974.

[3] J.-L. NICOLAS, I. Z. RUZSA AND A. SÁRKÖZY, On the parity of additive representation functions, *J. Number Theory* **73** (1998), 292–317.

[4] J.-L. NICOLAS AND A. SÁRKÖZY, On the parity of generalized partition functions, submitted to the proceedings of the Millennium Conference, Urbana, Illinois, May 2000.

[5] G. TENENBAUM, Introduction à la théorie analytique et probabiliste des nombres, S.M.F., Paris, 1995, or *Introduction to analytic and probabilistic number theory*, Cambridge studies in advanced mathematics, n° 46, Cambridge University Press, 1995.

(Received: June 20, 2000)

JEAN-LOUIS NICOLAS
INSTITUT GIRARD DESARGUES, UMR 5028
BÂT. 101, UNIVERSITÉ CLAUDE BERNARD (LYON 1)
F-69622 VILLEURBANNE CEDEX
FRANCE
E-MAIL: jlnicola@in2p3.fr