Number Theory for the Millennium III

Edited by

M. A. Bennett, B. C. Berndt,
N. Boston, H. G. Diamond,
A. J. Hildebrand, and W. Philipp

A K Peters, 2002
Natick, Massachusetts
p. 55-72.

On the Parity of Generalized Partition Functions

J.-L. Nicolas[1] and A. Sárközy[1]

1 Introduction

$\mathbb{N}_0$ and $\mathbb{N}$ denote the sets of the non-negative resp. positive integers; $\mathcal{A}, \mathcal{B}\ldots$ denote sets of positive integers, and their counting functions are denoted by $A(x), B(x), \ldots$, so that, e.g.,

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

If $\mathcal{A} = \{a_1, a_2, \ldots\} \subset \mathbb{N}$ (where $a_1 < a_2 < \ldots$), 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

$$a_1x_1 + a_2x_2 + \cdots = n$$

in non-negative integers $x_1, x_2, \ldots$. As usual, we set $p(\mathcal{A}, 0) = 1$.

For $i = 0$ or 1, if $\mathcal{A} \subset \mathbb{N}$ and there is a number N such that

$$p(\mathcal{A}, n) \equiv i \pmod 2 \quad \text{for all} \quad n \in \mathbb{N}, n > N,$$

then $\mathcal{A}$ is said to possess property P_i. If $i = 0$ or 1, $\mathcal{B} = \{b_1, \ldots, b_k\} \neq \emptyset$ (where $b_1 < \cdots < b_k$) is a finite set of positive integers, $N \in \mathbb{N}$ and $N \geq b_k$, then there is a unique set $\mathcal{A} \subset \mathbb{N}$ such that

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

and

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

We will denote this set $\mathcal{A}$ by $\mathcal{A}_i(\mathcal{B}, N)$ and, in particular, we will write $\mathcal{A}_i(\mathcal{B}, b_k) = \mathcal{A}_i(\mathcal{B})$. The construction of the set $\mathcal{A}_i(\mathcal{B}, N)$ is described in [3]; let us recall it when, for instance, $i = 0$. The set $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ will be defined by recursion. We write $\mathcal{A}_n = \mathcal{A} \cap \{1, 2, \ldots, n\}$, so that

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

[1]Research partially supported by Hungarian National Foundation for Scientific Research, Grant No. T 029759, MKM fund FKFP-0139/1997, French-Hungarian APAPE-OMFB exchange program F-5/1997 and CNRS, Institut Girard Desargues, UMR 5028.

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 $p(\mathcal{A},n) = 1 + p(\mathcal{A}_{n-1},n)$ if $n \in \mathcal{A}$, and $p(\mathcal{A},n) = p(\mathcal{A}_{n-1},n)$ if $n \notin \mathcal{A}$. This shows that $p(\mathcal{A},n)$ is even for $n \geq N+1$.

Note that, in the same way, any finite set $\mathcal{B} = \{b_1, b_2, \dots, b_k\}$ can be extended to an infinite set $\mathcal{A}$ so that $\mathcal{A}_{b_k} = \mathcal{B}$ and the parity of $p(\mathcal{A},n)$ is given for $n \geq N+1$ (where N is any integer such that $N \geq b_k$). The problem we will consider here is the estimation of $A(x)$.

In [4] we initiated the study of sets $\mathcal{A}$ possessing property P_0 or P_1. In [3] we asked the following question: *But what can one say on such a set $\mathcal{A}$...? In particular, how thin, or how dense can a set of this type be?* All we could prove in this direction was that there is an infinite set $\mathcal{A}$ which possesses property P_0 and for which $A(x) \gg x/\log x$; more precisely, $p(\mathcal{A},n)$ is even for $n \geq 4$ and

$$\liminf_{x\to\infty} \frac{A(x)\log x}{x} \geq \frac{1}{2}. \tag{1.1}$$

Indeed, we showed that the set

$$\mathcal{A} = \mathcal{A}_0(\mathcal{B}), \quad \text{where} \quad \mathcal{B} = \{1,2,3\} \tag{1.2}$$

has these properties. In [3] we wrote regarding this set $\mathcal{A}$: *First we thought that perhaps even*

$$A(x) = \left(\frac{1}{2} + o(1)\right)x$$

holds. However, computing the elements of $\mathcal{A}$ up to 10000, it turned out that $A(10000) = 2204$ *so that, probably,*

$$\liminf_{x\to\infty} \frac{A(x)}{x} < \frac{1}{2}.$$

In this paper we will first continue the study of the sequence $\mathcal{A}$ in (1.2). Then, in Section 3, we will show that there are numerous sequences $\mathcal{A}$ which possess property P_0 or P_1 and whose counting function grows very slowly: namely, we have

$$A(x) \ll \log x.$$

(Computer experiments lead us to the construction of sets $\mathcal{A}$ with those properties; it surprised us very much that such sets $\mathcal{A}$ exist.) In Section 4 we will prove a criterion which can be used to show that for fixed i, $\mathcal{B}$, N the set $\mathcal{A} = \mathcal{A}_i(\mathcal{B},N)$ satisfies an inequality like (1.1), i.e., we have

$$A(x) \gg \frac{x}{\log x}. \tag{1.3}$$

This criterion will suggest that for the most $\mathcal{B}$, N the set $\mathcal{A} = \mathcal{A}_i(\mathcal{B},N)$ (for both $i = 0$ and 1) satisfies (1.3). In Section 5 we will improve on (1.3) by constructing a set $\mathcal{A} = \mathcal{A}_0(\mathcal{B},N)$ with

$$A(x) \gg \frac{x}{(\log x)^{1-c}}$$

for some $c > 0$. Finally, in Section 6 we will formulate several problems and conjectures based on computer experiments.

By using modular forms, K. Ono has obtained in [5] and [6] nice results about the distribution of the values of the classical partition function $p(n) = p(\mathcal{N},n)$ in the different residues classes modulo m. By the above algorithm, it is possible to construct sets $\mathcal{A}$ such that, for $n \equiv a \pmod{m}$ and $n > N$, the parity of $p(\mathcal{A},n)$ is fixed.

2 Further Study of the Set $\mathcal{A}$ in (1.2)

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 write

$$\sigma(\mathcal{A},n) = \sum_{d|n} \chi(\mathcal{A},d)d = \sum_{d|n,\, d\in\mathcal{A}} d. \tag{2.1}$$

By (4.5) in [3] we have

$$np(\mathcal{A},n) = \sum_{k=0}^{n-1} p(\mathcal{A},k)\sigma(\mathcal{A},n-k). \tag{2.2}$$

Let μ denote the Möbius function. We shall need the following lemma which allows us to determine $\chi(\mathcal{A},n)$ for n odd if the σ function is known:

Lemma 1. *If n is odd, then*

$$\chi(\mathcal{A},n) \equiv \sum_{d|n} \mu(d)\sigma(\mathcal{A},n/d) \pmod 2, \tag{2.3}$$

while if $n = 2^\alpha m$, $\alpha \geq 1$, and m is odd, then

$$n\chi(\mathcal{A},n) = -\sum_{\beta=0}^{\alpha-1} 2^\beta m\chi(\mathcal{A},2^\beta m) + \sum_{d|m} \mu(d)\sigma(\mathcal{A},n/d). \tag{2.4}$$

Proof. Applying the Möbius inversion formula, it follows from (2.1) that

$$n\chi(\mathcal{A},n) = \sum_{d|n} \mu(d)\sigma(\mathcal{A},n/d), \tag{2.5}$$

which gives (2.3) for n odd. When n is even, we write the divisors d of n in the form $d = 2^\beta\delta$, where $\beta \leq \alpha$ and $\delta|m$, so that (2.5) can be written as

$$\begin{aligned} n\chi(\mathcal{A},n) &= \sum_{\delta|m}\sum_{\beta=0}^{\alpha} \mu(2^\beta\delta)\sigma(\mathcal{A},n/2^\beta\delta) \\ &= \sum_{\delta|m} \mu(\delta)\sigma(\mathcal{A},n/\delta) - \sum_{\delta|m} \mu(\delta)\sigma(\mathcal{A},n/2\delta). \end{aligned}$$

Here the last sum is

$$\begin{aligned} \sum_{\delta|m} \mu(\delta) \sum_{a|(n/2\delta)} \chi(\mathcal{A},a)a &= \sum_{a|(n/2)} a\chi(\mathcal{A},a) \sum_{\delta|(n/(2a),m)} \mu(\delta) \\ &= \sum_{\beta=0}^{\alpha-1} 2^\beta m\chi(\mathcal{A},2^\beta m). \end{aligned}$$

This completes the proof of Lemma 1. □

From now on $\mathcal{A}$ denotes the set (1.2). In [3] we showed that $\sigma(\mathcal{A},n)$ modulo 2 is periodic with period 7. More precisely, as

$$n \equiv 0,1,2,3,4,5 \text{ and } 6 \pmod 7,$$

we have

$$\sigma(\mathcal{A},n) \equiv 1,1,1,0,1,0 \text{ and } 0 \pmod 2.$$

This can be expressed in the following form:

$$\sigma(\mathcal{A},n) \equiv 1 + \frac{1}{2}\left(\left(\frac{n}{7}\right) - \left(\frac{n}{7}\right)^2\right) \pmod 2, \tag{2.6}$$

where $\left(\frac{n}{7}\right)$ is the Legendre symbol for $(n,7) = 1$, and $\left(\frac{n}{7}\right) = 0$ for $7|n$.

In [3] we proved that a prime p belongs to $\mathcal{A}$ if and only if $p \equiv 3,5$ or $6 \pmod 7$ (i.e., if $\left(\frac{p}{7}\right) = -1$). We will prove:

Theorem 1. *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 $\alpha \geq 1$.*

Proof. By Lemma 1 and (2.6) we have, for n odd, $n > 1$,

$$\begin{aligned} \chi(\mathcal{A},n) &\equiv \sum_{d|n} \mu(d)\left(1 + \frac{1}{2}\left(\left(\frac{n/d}{7}\right) - \left(\frac{n/d}{7}\right)^2\right)\right) \\ &\equiv \frac{1}{2}(f_1(n) - f_2(n)) \pmod 2 \end{aligned} \tag{2.7}$$

with

$$f_i(n) = \sum_{d|n} \mu(d)\left(\frac{n/d}{7}\right)^i.$$

But $f_1(n)$ and $f_2(n)$ are multiplicative functions, and $f_2(n) = 0$ for all n except for $n = 1$ and $n = 7$ when $f_2(1) = +1$ and $f_2(7) = -1$. Further, $f_1(p^\alpha) = 0$ for $\left(\frac{p}{7}\right) = +1$ and $f_1(p^\alpha) = (-1)^\alpha \cdot 2$ for $\left(\frac{p}{7}\right) = -1$, and $f_1(7) = -1$ and $f_1(7^\alpha) = 0$ for $\alpha \geq 2$. Thus it follows from (2.7) that $7 \notin \mathcal{A}$, and for n odd, $n \neq 1,7$,

$$\chi(\mathcal{A},n) \equiv \frac{1}{2} f_1(n) \pmod 2,$$

so that by using the multiplicativity of $f_1(n)$ and the values of $f_1(p^\alpha)$, $f_1(n) \equiv 2 \pmod 4$ holds only if $n = p^\alpha$ or $7p^\alpha$ with $\left(\frac{p}{7}\right) = -1$. This completes the proof of Theorem 1. □

The even elements of $\mathcal{A}$ could be determined if the following conjecture holds:

Conjecture. *If n is even then*

$$\sigma(\mathcal{A},n) \equiv 2,3,1 \pmod 4 \text{ for } \left(\frac{n}{7}\right) = -1,+1,0, \text{ respectively.} \tag{2.8}$$

More generally, if $k \geq 1$, $u_k = \sigma(\mathcal{A},3\cdot 2^k)$, $v_k = \sigma(\mathcal{A},2^k)$, and n is a multiple of 2^k, then

$$\sigma(\mathcal{A},n) \equiv u_k, v_k, -3 \pmod{2^{k+1}} \text{ for } \left(\frac{n}{7}\right) = -1,+1,0, \text{ respectively.} \tag{2.9}$$

This conjecture has been checked up to $n = 10000$ by computer. By an argument similar to the proof of Theorem 1, one may deduce from the validity of (2.8) for $n \leq n_0$ that the elements n of $\mathcal{A}$ with $n \equiv 2 \pmod 4$ and $n \leq n_0$ are $n = 2$; $n = 2p^\alpha 7^\gamma$, $\left(\frac{p}{7}\right) = -1$, $p \equiv 1 \pmod 4$, α odd, $\gamma = 0$ or 1; or $n = 2p^\alpha q^\beta 7^\gamma$, $\left(\frac{p}{7}\right) = \left(\frac{q}{7}\right) = -1$, $p \neq q$, $\alpha \geq 1$, $\beta \geq 1$, $\gamma = 0$ or 1.

3 Thin Sets with Properties P_0, P_1

We will show that there are sets $\mathcal{B}$, $\mathcal{C}$ such that $\mathcal{A}_0(\mathcal{B})$ and $\mathcal{A}_1(\mathcal{C})$ are geometric progressions (apart from a single exceptional element):

Theorem 2. *(i) For all $a, b \in \mathbb{N}$ such that $a|b$, we have*

$$\mathcal{A}_0(\{a,b\}) = \{a, b, 2b, \ldots, 2^k b, \ldots\}. \tag{3.1}$$

(ii) We have

$$\mathcal{A}_1(\{1\}) = \{1\} \tag{3.2}$$

and, for all $k \in \mathbb{N}$,

$$\mathcal{A}_1(\{2, 2k+1\}) = \{2, 2k+1, 2(2k+1), \ldots, 2^\ell(2k+1), \ldots\}. \tag{3.3}$$

Proof. (i) By the uniqueness of $\mathcal{A}_0(\{a,b\})$, it suffices to show that, writing $\mathcal{D} = \{a, b, 2b, \ldots, 2^k b, \ldots\}$, we have

$$\mathcal{D} \cap \{1, 2, \ldots, b\} = \{a, b\} \tag{3.4}$$

and

$$p(\mathcal{D}, n) \equiv 0 \pmod 2 \quad \text{for} \quad n > b. \tag{3.5}$$

(3.4) is trivial, so it remains to prove (3.5). Clearly we have

$$\begin{aligned} \sum_{n=0}^{+\infty} p(\mathcal{D}, n) x^n &= \prod_{d \in \mathcal{D}} \frac{1}{1 - x^d} = \frac{1}{1 - x^a} \prod_{k=0}^{+\infty} \frac{1}{1 - x^{2^k b}} \\ &\equiv \frac{1}{1 - x^a} \prod_{k=0}^{+\infty} \frac{1}{1 + x^{2^k b}} \\ &= \frac{1 - x^b}{1 - x^a} = 1 + x^a + x^{2a} + \cdots + x^{b-a} \pmod 2, \end{aligned}$$

which proves (3.5). (Here the notation $\equiv \pmod 2$ means that the corresponding coefficients are congruent modulo 2.)

(ii) (3.2) is trivial, while (3.3) can be proved in the same way as (3.1). □

The sets constructed in Theorem 2, possessing properties P_0, resp. P_1, consist of a single geometric progression, apart from their smallest elements. We can show that a set possessing property P_0 or P_1 may consist of arbitrarily many geometric progressions. Here we will consider only the even case (P_0), since the other case is similar but slightly more complicated.

Theorem 3. *Let $k \in \mathbb{N}$ and let $q_1 < q_2 < \cdots < q_k$ be arbitrary positive odd integers. Then defining $\mathcal{D}$, M and $\mathcal{B}$ by $\mathcal{D} = \bigcup_{i=1}^k \{q_i, 2q_i, \ldots, 2^\ell q_i, \ldots\}$, $M = \sum_{i=1}^k q_i$ and $\mathcal{B} = \mathcal{D} \cap \{1, 2, \ldots, M\}$, respectively, we have*

$$\mathcal{A}_0(\mathcal{B}, M) = \mathcal{D}. \tag{3.6}$$

Note that the function $\sigma(\mathcal{D}, n)$ defined by (2.1) satisfies

$$\sigma(\mathcal{D}, n) \equiv \sum_{i=1, q_i \mid n}^{k} 1 \pmod 2$$

and is periodic in n with period $\operatorname{lcm}(q_1, q_2, \ldots, q_k)$.

Proof. To prove (3.6) we have to show that

$$\mathcal{D} \cap \{1, 2, \ldots, M\} = \mathcal{B} \tag{3.7}$$

and

$$p(\mathcal{D}, n) \equiv 0 \pmod 2 \quad \text{for} \quad n > M. \tag{3.8}$$

(3.7) holds by the definition of $\mathcal{B}$. Thus it remains to show that (3.8) also holds.

Clearly we have

$$\begin{aligned} \sum_{n=0}^{+\infty} p(\mathcal{D}, n) x^n &= \prod_{d \in \mathcal{D}} \frac{1}{1 - x^d} \\ &= \prod_{i=1}^{k} \prod_{\ell=0}^{+\infty} \frac{1}{1 - x^{2^\ell q_i}} \equiv \prod_{i=1}^{k} \prod_{\ell=0}^{+\infty} \frac{1}{1 + x^{2^\ell q_i}} \\ &= \prod_{i=1}^{k} (1 - x^{q_i}) = a_0 + a_1 x + \cdots + a_M x^M \pmod 2, \end{aligned}$$

where $a_0, a_1, \ldots, a_M$ are integers, and this proves (3.8). □

4 Dense Sets with Properties P_0, P_1

We believe that the sets $\mathcal{A}_0$, $\mathcal{A}_1$ of "geometric progression type", described in Section 3, are exceptional, and that typically, the sets $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$, $\mathcal{A} = \mathcal{A}_1(\mathcal{B}, N)$ are "dense" in the sense that they satisfy (1.3). We will prove a criterion which provides a simple algorithm to show that, for fixed $\mathcal{B}$, N, the sets $\mathcal{A}_0(\mathcal{B}, N)$ and $\mathcal{A}_1(\mathcal{B}, N)$ are indeed of this type:

Theorem 4. *For every finite set $\mathcal{B} = \{b_1, \dots, b_k\}$ (where $b_1 < \dots < b_k$), every $N \in \mathbb{N}$, $N \geq b_k$, and for both $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ and $\mathcal{A} = \mathcal{A}_1(\mathcal{B}, N)$, there is a $q = q(\mathcal{A}) \in \mathbb{N}$ such that q is odd,*

$$q(\mathcal{A}_0(\mathcal{B}, N)) \leq 2^N, \qquad q(\mathcal{A}_1(\mathcal{B}, N)) \leq 2^{N+1} \tag{4.1}$$

and

$$\sigma(\mathcal{A}, n) \equiv \sigma(\mathcal{A}, n+q) \pmod 2 \quad \text{for } n \geq 1; \tag{4.2}$$

i.e., $\sigma(\mathcal{A}, n)$ is periodic modulo 2 for $n \geq 1$ with period q satisfying (4.1).

The proof will be based on the following lemma:

Lemma 2. *For every finite set $\mathcal{B} = \{b_1, \dots, b_k\}$ (where $b_1 < \dots < b_k$) and every $N \in \mathbb{N}$, $N \geq b_k$, both $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ and $\mathcal{A} = \mathcal{A}_1(\mathcal{B}, N)$ satisfy a congruence of form*

$$\sigma(\mathcal{A}, n) \equiv \varepsilon_0 + \sum_{j=1}^{J} \varepsilon_j \sigma(\mathcal{A}, n-j) \pmod 2 \quad \text{for } n = J+1, J+2, .., \tag{4.3}$$

where each of $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{J-1}$ is equal to 0 or 1, $\varepsilon_J = 1$, and J is a positive integer satisfying $J \leq N$ if $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ and $J \leq N+1$ if $\mathcal{A} = \mathcal{A}_1(\mathcal{B}, N)$.

Proof. (i) Consider first the case $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ ("even case") where $p(\mathcal{A}, n) \equiv 0 \pmod 2$ for $n \geq N+1$. Let us define J as the smallest integer such that $p(\mathcal{A}, J) \equiv 1 \pmod 2$ and $p(\mathcal{A}, j) \equiv 0 \pmod 2$ for $j \geq J+1$. (Note that $J \geq b_1 = \min \mathcal{B}$, since $p(\mathcal{A}, b_1) = 1$.) From the definition of J it follows that $J \leq N$ and

$$p(\mathcal{A}, n) \equiv 0 \pmod 2 \quad \text{for} \quad n = J+1, J+2, \dots. \tag{4.4}$$

The proof will be based on identity (2.2), which can be rewritten as

$$np(\mathcal{A}, n) = \sigma(\mathcal{A}, n) + \sum_{k=1}^{n-1} p(\mathcal{A}, k)\sigma(\mathcal{A}, n-k), \quad n \geq 1. \tag{4.5}$$

By (4.4), it follows that for $n \geq J+1$ we have

$$0 \equiv \sigma(\mathcal{A}, n) + \sum_{k=1}^{J} p(\mathcal{A}, k)\sigma(\mathcal{A}, n-k) \pmod 2. \tag{4.6}$$

Writing $\varepsilon_k = p(\mathcal{A}, k) \pmod 2$, that is

$$\varepsilon_k = \begin{cases} 1 & \text{if } p(\mathcal{A}, k) \text{ is odd,} \\ 0 & \text{if } p(\mathcal{A}, k) \text{ is even,} \end{cases}$$

for $k = 1, 2, \dots, J$, it follows from (4.6) that

$$\sigma(\mathcal{A}, n) \equiv \sum_{k=1}^{J} \varepsilon_k \sigma(\mathcal{A}, n-k) \pmod 2,$$

which is a congruence of form (4.3) with $\varepsilon_0 = 0$.

(ii) Consider now the odd case, i.e., a set $\mathcal{A} = \mathcal{A}_1(\mathcal{B}, N)$ so that

$$p(\mathcal{A}, n) \equiv 1 \pmod 2 \quad \text{for} \quad n = N+1, N+2, \dots. \tag{4.7}$$

Replacing n by $n-1$ in (2.2) we obtain for $n \geq 1$

$$(n-1)p(\mathcal{A}, n-1) = \sum_{k=0}^{n-2} p(\mathcal{A}, k)\sigma(\mathcal{A}, n-1-k) = \sum_{j=1}^{n-1} p(\mathcal{A}, j-1)\sigma(\mathcal{A}, n-j) \tag{4.8}$$

Subtracting (4.8) from (2.2) yields for $n \geq 1$

$$np(\mathcal{A}, n) - (n-1)p(\mathcal{A}, n-1) = \sigma(\mathcal{A}, n) + \sum_{j=1}^{n-1} t_j \sigma(\mathcal{A}, n-j) \tag{4.9}$$

with $t_j = p(\mathcal{A}, j) - p(\mathcal{A}, j-1)$. Here we define J as the smallest integer such that $p(\mathcal{A}, J-1) \equiv 0 \pmod 2$ and $p(\mathcal{A}, j) \equiv 1 \pmod 2$ for $j \geq J$. Except for the case $\mathcal{B} = \{1\}$ (which leads to $\mathcal{A}_1(\mathcal{B}, N) = \{1\}$ for all $N \geq 1$), such a J always exists: if $1 \notin \mathcal{B}$, $p(\mathcal{A}, b_1 - 1) = 0$ so that $J \geq b_1$, while, if $1 = b_1 \in \mathcal{B}$, $p(\mathcal{A}, b_2) = 2$ and $J \geq b_2 + 1$. From (4.7), $J \leq N+1$ holds, and for $j \geq J+1$, we have $t_j \equiv 0 \pmod 2$. Defining ε_j by

$$\varepsilon_j = \begin{cases} 0, & \text{if } t_j = p(\mathcal{A}, j) - p(\mathcal{A}, j-1) \text{ is even} \\ 1, & \text{if } t_j = p(\mathcal{A}, j) - p(\mathcal{A}, j-1) \text{ is odd} \end{cases} \quad (\text{for } j = 1, \dots, J),$$

(4.9) implies

$$\sigma(\mathcal{A}, n) \equiv 1 + \sum_{j=1}^{J} \varepsilon_j \sigma(\mathcal{A}, n-j) \pmod 2 \quad (\text{for } n \geq J+1) \tag{4.10}$$

which is again of form (4.3). This completes the proof of Lemma 2. □

Proof of Theorem 4. We start out from the characteristic polynomial of the linear recurrence relation (4.3):

$$P(X) = X^J + \sum_{k=1}^{J} \varepsilon_k X^{J-k}. \tag{4.11}$$

Let us consider this polynomial on the finite field $\mathbb{F}_2$, and let $K = \mathbb{F}_{2^u}$ be a finite extension of $\mathbb{F}_2$ on which P splits into linear factors. Let $\xi_1, \dots, \xi_J$ be the (not necessarily distinct) roots of P on K and

$$S_n = \xi_1^n + \xi_2^n + \cdots + \xi_J^n, \quad n = 1, 2, 3, \dots$$

the associated Newton sums. These sums belong to $\mathbb{F}_2$ and, by a classical result in elementary algebra, they satisfy the following identities:

$$S_1 + \varepsilon_1 = 0,$$

$$S_2 + \varepsilon_1 S_1 + 2\varepsilon_2 = 0,$$

$$\cdots\cdots\cdots$$

$$S_n + \varepsilon_1 S_{n-1} + \cdots + \varepsilon_{n-1} S_1 + n\varepsilon_n = 0, \quad \text{for } 1 \le n \le J,$$

$$S_n + \varepsilon_1 S_{n-1} + \cdots + \varepsilon_{J-1} S_{n-J+1} + \varepsilon_J S_{n-J} = 0, \quad \text{for } n \ge J+1.$$

In the even case, since $\varepsilon_k \equiv p(\mathcal{A}, k) \pmod 2$, it follows by induction on n from (4.5) that

$$\sigma(\mathcal{A}, n) \equiv S_n \pmod 2. \tag{4.12}$$

But each non-zero root ξ_j has an order in K which divides $2^u - 1$, and so S_n is periodic in $n \ge 1$ with a period dividing $2^u - 1$. Then it follows from (4.12) that the period q of $\sigma(\mathcal{A}, n)$ mod 2 is a divisor of $2^u - 1$ and so is odd, and that (4.2) holds.

The odd case is similar, with (4.12) replaced by

$$\sigma(\mathcal{A}, n) \equiv 1 + S_n \pmod 2.$$

If the polynomial P is irreducible over $\mathbb{F}_2$, we can choose $K = \mathbb{F}_{2^J}$, since J is the degree of P. If P is reducible, let us write its factorisation as

$$P = P_1 P_2 \dots P_r,$$

where $P_1, P_2, \dots, P_r$ are the (not necessary distinct) irreducible factors of P over $\mathbb{F}_2$. If we denote by $S_n^{(i)}$ the Newton sum of index n associated to the polynomial P_i, $S_n^{(i)}$ is periodic in n with period q_i dividing $2^{d_i} - 1$, where d_i is the degree of P_i. Clearly,

$$S_n = S_n^{(1)} + S_n^{(2)} + \cdots + S_n^{(r)},$$

and the period of S_n is a divisor of lcm $(q_1, q_2, \dots, q_r)$ so that

$$\begin{aligned} q \le q_1 q_2 \dots q_r &\le (2^{d_1} - 1)(2^{d_2} - 1) \dots (2^{d_r} - 1) \\ &< 2^{d_1 + d_2 + \cdots + d_r} = 2^J, \end{aligned}$$

which, from the definition of J, implies (4.1). This completes the proof of Theorem 4. □

Theorem 5. *Let $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ or $\mathcal{A} = \mathcal{A}_1(\mathcal{B}, N)$, let $q = q(\mathcal{A})$ be the period of $\sigma(\mathcal{A}, n)$ (mod 2) as described in Theorem 4, and c the number of m with $1 \le m \le q$, such that*

$$(m, q) = 1 \quad \textit{and} \quad \sigma(\mathcal{A}, m) \equiv 1 - \chi(\mathcal{A}, 1) \pmod 2, \tag{4.13}$$

(where $\chi(\mathcal{A}, n)$ is the characteristic function of the set $\mathcal{A}$ as in Section 2). Then any prime $p \equiv m \pmod q$, where m is any integer satisfying (4.13), belongs to $\mathcal{A}$, and thus

$$\liminf_{x \to \infty} \frac{A(x) \log x}{x} \ge \frac{c}{\varphi(q)}, \tag{4.14}$$

where φ is Euler's function.

Note that Theorems 4 and 5 also provide a simple algorithm to show that for fixed $\mathcal{B}$, N, (4.14) holds for both sets $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ and $\mathcal{A} = \mathcal{A}_1(\mathcal{B}, N)$ (and, indeed, for the most $\mathcal{B}$ and N this is expected to happen). Namely, we first look for a period q satisfying (4.1) and (4.2), and then we count the m's satisfying $1 \le m \le q$ and (4.13) to get c; if $c \ne 0$, then (4.14) is proved.

Proof of Theorem 5. If p is a prime congruent to m modulo q, then by (4.2) and (4.13) we have

$$\sigma(\mathcal{A}, p) \equiv \sigma(\mathcal{A}, m) \equiv 1 - \chi(\mathcal{A}, 1) \pmod 2,$$

so that by Lemma 1

$$\begin{aligned} \chi(\mathcal{A}, p) &\equiv \sum_{d \mid p} \mu(d) \sigma(\mathcal{A}, p/d) \\ &\equiv \sigma(\mathcal{A}, p) - \sigma(\mathcal{A}, 1) \equiv 1 - \chi(\mathcal{A}, 1) - \sigma(\mathcal{A}, 1) \equiv 1 \pmod 2, \end{aligned}$$

whence $p \in \mathcal{A}$. By the prime number theorem for arithmetic progressions, it follows that for each m coprime to q,

$$|\{p : p \le x, \ p \equiv m \pmod q\}| = (1 + o(1)) \frac{x}{\varphi(q) \log x},$$

whence the result follows. □

5 Improving on (1.3)

We will prove:

Theorem 6. *There is an absolute constant $c > 0$ such that for $\mathcal{A} = \mathcal{A}_0(\{1,2,3,4,5\})$ we have*

$$A(x) > \frac{x}{(\log x)^{1-c}} \quad \textit{for } x > x_0 \tag{5.1}$$

Proof. A simple computation (cf. Example 2 in Section 7) shows that for this set $\mathcal{A}$ the period q defined in Theorem 4 is $q = 31$, and $\sigma(\mathcal{A}, n) \equiv 0 \pmod 2$ if and only if n is congruent to 3, 5, 6, 7, 9, 10, 12, 14, 17, 18, 19, 20, 24, 25, 28 modulo 31. Thus for

$$n = q_1 q_2 \dots q_k, \tag{5.2}$$

where $q_1, q_2, \dots, q_k$ are distinct primes $\equiv 5 \pmod{31}$, we have

$$\sigma(\mathcal{A}, n) \equiv 1 \pmod 2 \text{ if and only if } 3|k. \tag{5.3}$$

By (2.3) in Lemma 1, for the n in (5.2) we have

$$\chi(\mathcal{A}, n) \equiv \sum_{d|q_1 q_2 \dots q_k} \sigma(\mathcal{A}, q_1 q_2 \dots q_k/d) \pmod 2$$

so that, by (5.3),

$$\chi(\mathcal{A}, n) \equiv \sum_{\substack{0 \le r \le k \\ r \equiv 0 \,(\mathrm{mod}\, 3)}} \binom{k}{r} \pmod 2. \tag{5.4}$$

Now we need the following lemma:

Lemma 3. *Write*

$$S(a,k) = \sum_{\substack{0 \le r \le k \\ r \equiv a \,(\mathrm{mod}\, 3)}} \binom{k}{r}.$$

Then for $k \in \mathbb{N}$ we have

$$S(a,k) \equiv \begin{cases} 0 & (mod\, 2) \text{ if } a + k \equiv 0 \,(mod\, 3) \\ 1 & (mod\, 2) \text{ if } a + k \equiv 1 \text{ or } 2 \,(mod\, 3). \end{cases} \tag{5.5}$$

Proof. By the identity

$$\binom{t}{i} = \binom{t-1}{i} + \binom{t-1}{i-1},$$

we have for $k \ge 4$

$$\begin{aligned} S(a,k) &= S(a,k-1) + S(a-1,k-1) \\ &= S(a,k-2) + 2S(a-1,k-2) + S(a-2,k-2) \\ &= S(a,k-3) + 3S(a-1,k-3) + 3S(a-2,k-3) + S(a-3,k-3) \\ &= 2S(a,k-3) + 3S(a-1,k-3) + 3S(a-2,k-3) \\ &= 3 \sum_{0 \le r \le k-3} \binom{k-3}{r} - S(a,k-3) = 3\, 2^{k-3} - S(a,k-3), \end{aligned}$$

and finally

$$S(a,k) \equiv S(a,k-3) \pmod 2. \tag{5.6}$$

(5.5) follows by induction from (5.6) and

$$\begin{array}{lll} S(0,1) = 1, & S(1,1) = 1, & S(2,1) = 0 \\ S(0,2) = 1, & S(1,2) = 2, & S(2,2) = 1 \\ S(0,3) = 2, & S(1,3) = 3, & S(2,3) = 3. \end{array}$$ □

By Lemma 3, it follows from (5.4) that if n is of the form (5.2), where

$$k \equiv 1 \text{ or } 2 \pmod 3, \tag{5.7}$$

then we have $n \in \mathcal{A}$. The following lemma then completes the proof of Theorem 6. □

Lemma 4. *For $x > x_0$ the number of the integers n of form (5.2), where $n \le x$, $q_1 < q_2 < \dots < q_k$ are primes $\equiv 5$ (mod 31) and $k \equiv 1, 2 \pmod 3$, is $\gg \frac{x}{(\log x)^{1-c}}$ for a positive constant c.*

Lemma 4 will follow from the following theorem:

Theorem 7. *Let ℓ and m be two positive coprime integers. Let ρ be the multiplicative function defined by*

$$\begin{cases} \rho(p) = 1 & \text{if } p \equiv \ell \pmod m \\ \rho(p) = 0 & \text{if } p \not\equiv \ell \pmod m \end{cases}$$

and $\rho(p^\alpha) = 0$ for all primes p and all exponents $\alpha \ge 2$. Let $\omega(n)$ denote the number of prime factors of n, let φ be Euler's function, z any complex number and

$$U(x,z) = \sum_{n \le x} \rho(n) z^{\omega(n)}.$$

Then, for x going to infinity, we have

$$U(x,z) \sim \frac{C^z}{\Gamma(z/\varphi(m))} \prod_{p \equiv \ell \pmod m} \left(1 + \frac{z}{p}\right)\left(1 - \frac{1}{p}\right)^z \frac{x}{(\log x)^{1-z/\varphi(m)}}, \tag{5.8}$$

where

$$C := \left\{ \frac{\varphi(m)}{m} g(1) \prod_{\chi \neq \chi_0} (L(1,\chi))^{\overline{\chi}(l)} \right\}^{1/\varphi(m)}, \tag{5.9}$$

$L(s,\chi)$ is the Dirichlet function associated to a character χ modulo m, and g is the function (holomorphic in $\Re s > 1/2$)

$$g(s) = \exp\left(\sum_{\chi} \overline{\chi}(l) \sum_{p} \sum_{j=2}^{\infty} \frac{\chi(p) - \chi(p^j)}{j p^{js}} \right). \tag{5.10}$$

Proof. Theorem 7 is an extension of the so-called Selberg-Delange formula (cf. [7], II.5) by considering only the squarefree integers composed of primes congruent to ℓ modulo m. A sketch of the proof is given (for the case $z = 1$) in [8], as the solution to Exercise II.8.6, p. 124-125. A detailed proof will appear in [1]. □

Proof of Lemma 4. Let us set $\xi = e^{2i\pi/3}$. In Theorem 7, let us fix $\ell = 5$ and $m = 31$. The number $V(x,a)$ of integers $n \le x$ satisfying (5.2) with $k = \omega(n) \equiv a \pmod 3$ is, by (5.8), equal to

$$V(x,a) = \sum_{\substack{n \le x \\ \omega(n) \equiv a \pmod 3}} \rho(n) = \frac{1}{3} \sum_{n \le x} \sum_{r=0}^{2} \xi^{r(\omega(n)-a)} = \frac{1}{3} \sum_{r=0}^{2} \xi^{-ra} U(x, \xi^r). \tag{5.11}$$

But, from (5.8) it follows that, for $r = 1$ or 2,

$$U(x,\xi^r) = O\left(x(\log x)^{\Re\xi/\varphi(31)-1}\right) = O\left(x(\log x)^{-\frac{61}{60}}\right)$$

while $U(x,1) \asymp x(\log x)^{-\frac{29}{30}}$. Therefore, (5.11) yields for $a = 0, 1$ or 2

$$V(x,a) \sim \frac{1}{3} U(x,1) \gg x(\log x)^{-\frac{29}{30}}.$$

This completes the proof of Lemma 4. □

An improvement of Theorem 6 is given in [2].

6 Problems

In this section we list several unsolved problems and conjectures based on the computer experiments carried out by us (see the examples below).

- *Is it true that for all $\mathcal{B}$ and $\mathbb{N}$, and for both $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ and $\mathcal{A} = \mathcal{A}_1(\mathcal{B}, N)$, we have $A(x) = o(x)$?* We believe that $A(x) \ll x/(\log x)^c$ with some $c > 0$. However, we cannot even show that there is an $\mathcal{A}$ with $A(x) \neq O(\log x)$, and

$$\liminf_{x \to \infty} \frac{A(x)}{x} < \frac{1}{2}.$$

  To show this, it would suffice to show that for the set $\mathcal{A} = \mathcal{A}_0(\{1,2,3\})$ studied in Section 2, the number of the even elements of $\mathcal{A}$ not exceeding x is $\le (\frac{1}{2} - \varepsilon)x$ for infinitely many $x \in \mathbb{N}$.

- *Is it true that if $A(x) \neq O(\log x)$ so that $\mathcal{A}$ is not of the "geometric progression type" (see Section 3), then we have $\frac{A(x)}{\log x} \to \infty$?* Perhaps, in this case even

$$\lim_{x \to \infty} \frac{A(x) \log x}{x} = \infty$$

  must hold.

- *Is it true that for all $\mathcal{B}$ and N, and for both $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ and $\mathcal{A} = \mathcal{A}_1(\mathcal{B}, N)$, denoting the smallest period of $\sigma(\mathcal{A}, n)$ by q we have*

$$\sigma(\mathcal{A}, 2(n+q)) \equiv \sigma(\mathcal{A}, 2n) \pmod 4$$

  and more generally,

$$\sigma(\mathcal{A}, 2^{h-1}(n+q)) \equiv \sigma(\mathcal{A}, 2^{h-1}n) \pmod{2^h}?$$

7 Examples

By computer, we have studied all sets $\mathcal{A}_i(\mathcal{B}, N)$ for $\mathcal{B} \subset \{1,2,3,4,5\}$, $i = 0$ or 1 and $\max_{b \in \mathcal{B}} b \le N \le 10$. For all of these sets, we have computed the period q of $\sigma(\mathcal{A}, n)$ mod 2, the constants c and $c/\varphi(q)$ introduced in Theorem 5, the characteristic polynomial P defined by (4.11) and its factorisation into irreducible factors over $\mathbb{F}_2$, the values of the first elements of $\mathcal{A}$ (up to 1000), and the values of $p(\mathcal{A}, n)$ for small n.

We give below the description of some of these sets which seem to us particularly interesting: in Examples 1 and 7, the elements greater than 5 of $\mathcal{A}$ coincide; in Examples 3 and 8, we have $c/\varphi(q) \neq 0, 1/2$; the sets $\mathcal{A}$ in Examples 5 and 6 coincide apart from the first element; in Example 5, the elements are twice the elements of $\mathcal{A}$ of Example 4.

Example 1: $\mathcal{B} = \{1,2,3\}$; $N = 3$; $i = 0$.

$$q = 7,\ c = 3,\ c/\varphi(q) = 1/2,$$

$$P = X^3 + X^2 + 1 : \text{ irreducible },$$

$$A = \{1,2,3,5,8,9,10,13,14,16,17,19,20,21,24,25,26,27,28,30,31,$$
$$34,35,36,40,41,47,48\ldots\};\quad A(1000) = 293.$$

Example 2: $\mathcal{B} = \{1,2,3,4,5\}$; $N = 5$; $i = 0$.

$$q = 31,\ c = 15,\ c/\varphi(q) = 1/2,$$

$$P = X^5 + X^4 + X^2 + X + 1 : \text{ irreducible },$$

$$A = \{1,2,3,4,5,7,8,10,12,14,16,17,19,20,22,26,27,28,33,34,36,$$
$$37,38,39,41,42,43,45,46,48,50\ldots\};\quad A(1000) = 480.$$

Example 3: $\mathcal{B} = \{1,2,4\}$; $N = 8$; $i = 0$.

$$q = 63,\ c = 24,\ c/\varphi(q) = 2/3,$$

$$P = X^8 + X^7 + 1 = (X^2 + X + 1)(X^6 + X^4 + X^3 + X + 1),$$

$$A = \{1,2,4,9,10,11,12,13,14,15,18,19,22,23,25,26,28,29,31,32$$
$$33,34,36,37,41,43,44,45,46,47,48,50,\ldots\};\quad A(1000) = 496.$$

Example 4: $\mathcal{B} = \{1,2\}$; $N = 4$; $i = 0$.

$$q = 15,\ c = 4,\ c/\varphi(q) = 1/2,$$

$$P = X^4 + X^3 + 1 : \text{ irreducible },$$

$$A = \{1,2,5,6,7,10,11,13,14,16,21,22,24,28,29,33,35,37,39,$$
$$41,42,43,48,49,\ldots\};\quad A(1000) = 307.$$

Example 5: $\mathcal{B} = \{2,4\}$; $N = 8$; $i = 0$.

$$q = 1,\ c = 0,\ c/\varphi(q) = 0,$$

$$P = X^8 + X^6 + 1 = (X^4 + X^3 + 1)^2,$$

$$A = \{2,4,10,12,14,20,22,26,28,32,42,44,48,\ldots\};\ A(1000) = 171.$$

Example 6: $\mathcal{B} = \{1,4\}$; $N = 9$; $i = 0$.

$$q = 1,\ c = 0,\ c/\varphi(q) = 0,$$

$$P = X^9 + X^8 + X^7 + X^6 + X + 1 = (X+1)(X^4 + X^3 + 1)^2,$$

$$A = \{1,4,10,12,14,20,22,26,28,32,42,44,48,\ldots\};\ A(1000) = 171.$$

Example 7: $\mathcal{B} = \{3,4\}$; $N = 4$; $i = 1$.

$$q = 7,\ c = 3,\ c/\varphi(q) = 1/2,$$

$$P = X^3 + X^2 + 1 : \text{ irreducible },$$

$$A = \{3,4,5,8,9,10,13,14,16,17,19,20,21,24,25,26,27,28,30,31,$$
$$34,35,36,40,41,47,48\ldots\};\quad A(1000) = 292.$$

Example 8: $\mathcal{B} = \{6\}$; $N = 9$; $i = 1$,

$$q = 31,\ c = 10,\ c/\varphi(q) = 1/3,$$

$$P = X^{10}+X^9+X^4+X^3+1 = (X^5+X^3+X^2+X+1)(X^5+X^4+X^3+X+1).$$

$$A = \{6,10,11,13,14,15,20,21,22,23,27,29,30,31,32,33,$$
$$34,38,39,40,45,46,48,\ldots\};\quad A(1000) = 479.$$

References

[1] F. Ben Saïd and J.-L. Nicolas, *Sur une extension de la formule de Selberg-Delange*, to appear.

[2] J.-L. Nicolas, *On the parity of generalized partition functions. II*, Period. Math. Hungar. **43** (2001), 177–189.

[3] J.-L. Nicolas, I. Z. Ruzsa, and A. Sárközy, *On the parity of additive representation functions*, J. Number Theory **73** (1998), 292–317, With an appendix in French by J.-P. Serre.

[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] ———, *Distribution of the partition function modulo m*, Ann. of Math. (2) **151** (2000), 293–307.

[7] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, Cambridge, 1995, Translated from the second French edition (1995) by C. B. Thomas.

[8] G. Tenenbaum and J. Wu, *Exercices corrigés de théorie analytique et probabiliste des nombres*, Société Mathématique de France, Paris, 1996.