Séminaire Lotharingien de Combinatoire **46** (2002), Article B46i

EVEN PARTITION FUNCTIONS

by

F. Ben saïd[1]
Faculté des Sciences de Monastir
Avenue de l'environnement
5000, Monastir, Tunisie
e-mail : Fethi.BenSaid@fsm.rnu.tn

and

J.-L. Nicolas[1]
Institut Girard Desargues, UMR 5028,
Bât. Doyen Jean Braconnier,
Université Claude Bernard (Lyon 1),
21 Avenue Claude Bernard,
F-69622 Villeurbanne Cedex, France
e-mail : jlnicola@in2p3.fr

Abstract. Let $\mathcal{A}$ be a set of positive integers. Let us denote by $p(\mathcal{A}, n)$ the number of partitions of n with parts in $\mathcal{A}$. While the study of the parity of the classical partition function $p(\mathbb{N}, n)$ (where $\mathbb{N}$ is the set of positive integers) is a deep and difficult problem, it is easy to construct a set $\mathcal{A}$ for which $p(\mathcal{A}, n)$ is even for n large enough : as explained in a paper of I.Z. Ruzsa, A. Sárközy and J.-L. Nicolas published in 1998 in the *Journal of Number Theory*, if $\mathcal{B}$ is a subset of $\{1, 2, \ldots, N\}$, there is a unique set $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ such that $\mathcal{A} \cap \{1, 2, \ldots, N\} = \mathcal{B}$ and $p(\mathcal{A}, n)$ is even for $n > N$.

In this paper we recall some properties of the sets $\mathcal{A}_0(\mathcal{B}, N)$, we describe the factorization into primes of the elements of the set $\mathcal{A}_0(\{1, 2, 3\}, 3)$, and prove that the number of elements of this set up to x is asymptotically equivalent to $c\dfrac{x}{(\log x)^{3/4}}$, where $c = 0.937\ldots$.

Résumé. Si $\mathcal{A}$ est un ensemble d'entiers positifs, nous noterons $p(\mathcal{A}, n)$ le nombre de partitions de n dont les parts sont dans $\mathcal{A}$. L'étude de la parité de la fonction usuelle de partition $p(\mathbb{N}, n)$ (où $\mathbb{N}$ est l'ensemble des entiers

[1]Research partially supported by French-Tunisian exchange program, C.M.C.U. n^o 99/F 1507 and by CNRS, Institut Girard Desargues, UMR 5028.

positifs) est un problème profond et difficile ; mais il est facile de construire un ensemble $\mathcal{A}$ tel que le nombre $p(\mathcal{A}, n)$ soit pair pour tout n assez grand : dans un article paru au *Journal of Number Theory* en 1998, I.Z. Ruzsa, A. Sárközy et J.-L. Nicolas montrent que si $\mathcal{B}$ est un sous-ensemble de $\{1, 2, \ldots, N\}$, il existe un seul ensemble $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ tel que $\mathcal{A} \cap \{1, 2, \ldots, N\} = \mathcal{B}$ et $p(\mathcal{A}, n)$ est pair pour $n > N$.

Dans cet article, nous rappelons quelques propriétés des ensembles $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$, nous décrivons la décomposition en facteurs premiers des éléments de $\mathcal{A}_0(\{1, 2, 3\}, 3)$ et nous montrons que le nombre des éléments de cet ensemble inférieurs à x est équivalent à $c\dfrac{x}{(\log x)^{3/4}}$, où $c = 0.937\ldots$.

1 Introduction.

$\mathbb{N}_0$ 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 $A(x)$:

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

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

$$a_1 x_1 + a_2 x_2 + \ldots = n \tag{1.1}$$

in non negative integers $x_1, x_2, \ldots$. As usual, we shall set

$$p(\mathcal{A}, 0) = 1 \quad \text{ and } \quad p(\mathcal{A}, n) = 0 \text{ for } n < 0. \tag{1.2}$$

We shall use the generating function :

$$F(z) = F_{\mathcal{A}}(z) = \sum_{n=0}^{\infty} p(\mathcal{A}, n) z^n = \prod_{a \in \mathcal{A}} \frac{1}{1 - z^a}. \tag{1.3}$$

When $\mathcal{A} = \mathbb{N}$ it seems highly probable that the number of integers $n \leq x$ such that $p(\mathbb{N}, n)$ is even is close to $x/2$ as $x \to \infty$; but the known results are rather poor (see [11], [14], [15] and the references in them). That is the reason for which, in [11], it was observed that there exist sets $\mathcal{A}$ such that $p(\mathcal{A}, n)$ is even for n large enough. In this paper, we want to investigate the properties of such sets.

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

$$p(\mathcal{A}, n) \equiv i \pmod 2 \quad \text{for} \quad n \in \mathbb{N} \ , \ n > N. \tag{1.4}$$

then $\mathcal{A}$ is said to possess property $P_i(N)$.

If $i = 0$ or 1, $\mathcal{B}$ is a finite set of positive integers, and $N \in \mathbb{N}$ satisfying

$$\mathcal{B} = \{b_1, \dots, b_k\} \neq \emptyset, \quad 0 < b_1 < \cdots < b_k, \qquad N \geq b_k \tag{1.5}$$

then there is (cf. [11]) a unique set $\mathcal{A} \subset \mathbb{N}$ such that

$$\mathcal{A} \cap \{1, 2, \dots, N\} = \mathcal{B} \tag{1.6}$$

and possessing property $P_i(N)$; we will denote it by $\mathcal{A}_i(\mathcal{B}, N)$.

Let us recall the construction of $\mathcal{A}_i(\mathcal{B}, N)$ as described in [11], when, for instance, $i = 0$. The set $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ will be defined by recursion. We write $\mathcal{A}_n = \mathcal{A} \cap \{1, 2, \dots, n\}$ so that

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

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

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

which 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 a 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 $N \geq b_k$).

It has been shown in [5] (cf. Proposition 4) that, except the case $i = 1$, $\mathcal{B} = \{1\}$, the set $\mathcal{A}_i(\mathcal{B}, N)$ is always infinite.

If $\mathcal{A} \subset \mathbb{N}$, let $\chi(\mathcal{A}, n)$ denote the characteristic function of $\mathcal{A}$, i.e.,

$$\chi(\mathcal{A}, n) = \begin{cases} 1 & \text{if} \quad n \in \mathcal{A} \\ 0 & \text{if} \quad n \notin \mathcal{A}, \end{cases} \tag{1.7}$$

and for $n \geq 1$,

$$\sigma(\mathcal{A}, n) = \sum_{d \mid n} \chi(\mathcal{A}, d) d = \sum_{d \mid n,\, d \in \mathcal{A}} d. \tag{1.8}$$

It is relevant to consider $\sigma(\mathcal{A}, n)$, since, as shown in [11], taking the logarithmic derivative of $F(z) = F_{\mathcal{A}}(z)$ defined by (1.3) yields

$$z \frac{F'(z)}{F(z)} = \sum_{n=1}^{\infty} \sigma(\mathcal{A}, n) z^n. \tag{1.9}$$

It has been proved in [5] that for any positive integer k and any set $\mathcal{A} = \mathcal{A}_i(\mathcal{B}, N)$, the sequence

$$\left(\sigma(\mathcal{A}, 2^k n) \bmod 2^{k+1}\right)_{n \geq 1} \text{ is periodic.} \tag{1.10}$$

(We denote by $a \bmod b$ the remainder in the Euclidean division of a by b.) Note that (1.10) was already proved for $k = 0$ in [11], and for $k = 1$ in [3]. The value of the smallest period in (1.10) is recalled in Theorem A below, proved in [5]. Before stating Theorem A, we need to introduce two definitions.

Definition 1 *Let $\mathbb{F}_2$ be the field with two elements and $Q(z) \in \mathbb{F}_2[z]$ be a polynomial satisfying $Q(0) \neq 0$. The order β of Q is the least positive integer such that $Q(z)$ divides $1 + z^\beta$ in $\mathbb{F}_2[z]$ (cf. [9], chap. 3).*

From now on, we shall assume that $i = 0$, for simplicity (the case $i = 1$ can be found in [5]). For $\mathcal{B}$ and N as in (1.5) and $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$, let us define the polynomial P (already considered in [12] and [5]) :

$$P(z) = \sum_{0 \leq n \leq J} \varepsilon_n z^n \tag{1.11}$$

where J is the largest integer such that $p(\mathcal{A}, J)$ is odd (such a J does exist since, from (1.2), $p(\mathcal{A}, 0) = 1$), and ε_n is defined by

$$p(\mathcal{A}, n) \equiv \varepsilon_n \pmod 2, \quad \varepsilon_n \in \{0, 1\}. \tag{1.12}$$

Theorem A (cf. Theorem 2 of [5]). *Let $\mathcal{B}$ and N as in (1.5), $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$, and P be the polynomial defined by (1.11) and (1.12). Let the factorization of P into irreducible factors over $\mathbb{F}_2[z]$ be*

$$P = Q_1^{\alpha_1} Q_2^{\alpha_2} \dots Q_s^{\alpha_s}. \tag{1.13}$$

We denote by β_i the order of $Q_i(z)$ (cf. Definition 1), and for all $k \geq 0$, we set

$$J_k = \{j; 1 \leq j \leq s, \alpha_j \equiv 2^k \pmod{2^{k+1}}\}, \tag{1.14}$$

$$I_k = J_0 \cup J_1 \cup \ldots \cup J_k = \{j; 1 \leq j \leq s, \alpha_j \not\equiv 0 \pmod{2^{k+1}}\} \tag{1.15}$$

and

$$q_k = lcm_{\ j \in I_k}\ \beta_j \tag{1.16}$$

(with $q_k = 1$ if $I_k = \emptyset$). Then, for all $k \geq 0$, q_k is odd and is the smallest period of (1.10) so that

$$\sigma(\mathcal{A}, 2^k(n + q_k)) \equiv \sigma(\mathcal{A}, 2^k n) \pmod{2^{k+1}}. \tag{1.17}$$

Note that if 2^{k_0} is the highest power of 2 dividing any exponent α_j in (1.13), for $k > k_0$, we have $J_k = \emptyset$, $I_k = I_{k_0}$,

$$q_k = q \stackrel{def}{=} \text{ lcm } (\beta_1, \beta_2, \ldots, \beta_s)$$

and q is a common period for all the sequences $\left(\sigma(\mathcal{A}, 2^k n) \bmod 2^{k+1}\right)_{n\geq 1}$, $k \geq 0$.

Remark 1. *In [3], one can find examples of $\mathcal{B}$ and N such that $q_0 \neq q_1$.*

Note that (1.10) was already proved for $k = 0$ in [11], and for $k = 1$ in [3].

By Möbius inversion formula, (1.8) gives

$$n\chi(\mathcal{A}, n) = \sum_{d \mid n} \mu(d)\sigma(\mathcal{A}, n/d) \tag{1.18}$$

where μ is the Möbius function. If n is odd, by (1.10) with $k = 0$, we know the value of $\sigma(\mathcal{A}, n) \bmod 2$, and this allows us from (1.18) to determine $\chi(\mathcal{A}, n)$ for any set $\mathcal{A} = \mathcal{A}_i(\mathcal{B}, N)$. This has been done in [12] for $\mathcal{A} = \mathcal{A}_0(\{1, 2, 3\}, 3)$ and in [13] for $\mathcal{A} = \mathcal{A}_0(\{1, 2, 3, 4, 5\}, 5)$. In [3], the validity of (1.10) for $k = 1$ has been used to determine the elements of $\mathcal{A} = \mathcal{A}_0(\{1, 2, 3\}, 3)$ which are congruent to 2 modulo 4.

Similarly, it is possible to deduce from (1.10) the value of $\chi(\mathcal{A}, n)$ where n is any positive integer. For that, it is convenient for m odd to introduce the sum

$$S(m, k) = \chi(\mathcal{A}, m) + 2\chi(\mathcal{A}, 2m) + \ldots + 2^k\chi(\mathcal{A}, 2^k m). \tag{1.19}$$

If n writes $n = 2^k m$ with $k \geq 0$ and m odd, (1.8) implies

$$\sigma(\mathcal{A}, n) = \sigma(\mathcal{A}, 2^k m) = \sum_{d \mid m} dS(d, k), \tag{1.20}$$

which, by Möbius inversion formula, gives

$$mS(m, k) = \sum_{d \mid m} \mu(d)\sigma(\mathcal{A}, n/d) = \sum_{d \mid \overline{m}} \mu(d)\sigma(\mathcal{A}, n/d), \tag{1.21}$$

where $\overline{m} = \prod_{p \mid m} p$ denotes the radical of m. In the above sums, n/d is always a multiple of 2^k, so that, from (1.10) , the value of $\sigma(\mathcal{A}, n/d)$ and thus the value of $S(m, k)$ are known modulo 2^{k+1}. Therefore, from (1.19), we can deduce the value of $\chi(\mathcal{A}, 2^i m)$ for $i \leq k$.

In Section 4, by the above described method, the multiplicative structure of the elements of $\mathcal{A} = \mathcal{A}_0(\{1,2,3\},3)$ will be given (Theorem 2), with the surprising property that, for this set $\mathcal{A}$, the 2-adic expansion :

$$1 + 2\chi(\mathcal{A},2) + 4\chi(\mathcal{A},4) + \ldots + 2^k\chi(\mathcal{A},2^k) + \ldots \tag{1.22}$$

is one of the 2-adic roots of the equation $x^2 - x + 2 = 0$. From Theorem 2, and from an extension of the so-called Selberg-Delange formula given in [4], we shall give in Section 5 (Theorem 3) an asymptotic estimation for $A(x)$:

$$A(x) \sim c\frac{x}{(\log x)^{3/4}}, \quad x \to \infty \tag{1.23}$$

where c is a constant the value of which is approximately 0.937.

The work done in Sections 3 and 4 for the set $\mathcal{A} = \mathcal{A}_0(\{1,2,3\},3)$ could be done, in principle, for any set $\mathcal{A} = \mathcal{A}_i(\mathcal{B},N)$. But, for technical reasons, the calculation can be difficult. We hope to return to this subject in an other article.

We are pleased to thank M. Deléglise for computing the values of $A(x)$ (cf. Section 5), D. Barsky, K. Belabas and A. Sárközy for several remarks.

2 The Graeffe transformation.

Let us consider the ring of formal power series $\mathbb{C}[[z]]$. For an element

$$f(z) = a_0 + a_1 z + a_2 z^2 + \ldots + a_n z^n + \ldots$$

of this ring, the product

$$f(z)f(-z) = b_0 + b_1 z^2 + b_2 z^4 + \ldots + b_n z^{2n} + \ldots$$

is an even power series with

$$b_0 = a_0^2,\ b_1 = 2a_0a_2 - a_1^2, \ldots,\ b_n = 2\left(\sum_{i=0}^{n-1}(-1)^i a_i a_{2n-i}\right) + (-1)^n a_n^2. \tag{2.1}$$

We shall call $g = \mathcal{G}(f)$ the series

$$g(z) = \mathcal{G}(f)(z) = b_0 + b_1 z + b_2 z^2 + \ldots + b_n z^n + \ldots. \tag{2.2}$$

Note that we have

$$g(z^2) = \mathcal{G}(f)(z^2) = f(z)f(-z). \tag{2.3}$$

Example. If q is an odd integer and $f(z) = 1 - z^q$, we have $f(z)f(-z) = (1 - z^q)(1 + z^q) = 1 - z^{2q}$, and

$$\mathcal{G}(f) = f. \tag{2.4}$$

If f is a polynomial of degree n which does not vanish in 0, and if $\widetilde{f}(z) = z^n f(1/z)$ is the reciprocal polynomial of f, then we have

$$\mathcal{G}(\widetilde{f}) = (-1)^n \widetilde{\mathcal{G}(f)}. \tag{2.5}$$

It is obvious that, for any two series f and g, the formulas

$$\mathcal{G}(fg) = \mathcal{G}(f)\mathcal{G}(g) \tag{2.6}$$

and, if $g(0) = 1$,

$$\mathcal{G}(f/g) = \mathcal{G}(f)/\mathcal{G}(g) \tag{2.7}$$

hold. We shall often use the following notation for the iterates of f by the transformation $\mathcal{G}$:

$$f_0 = f, \quad f_1 = \mathcal{G}(f), \quad f_2 = \mathcal{G}(f_1), \quad \dots, \quad f_k = \mathcal{G}(f_{k-1}) = \mathcal{G}^{(k)}(f), \dots \tag{2.8}$$

Proposition 1. *Let f be a polynomial of degree n whose roots are z_1, $z_2, \dots, z_n$ and leading coefficient is a_n. Then the polynomial $g = \mathcal{G}(f)$, where $\mathcal{G}$ is defined by (2.2), has a leading coefficient equal to $(-1)^n a_n^2$ and its roots are z_1^2, $z_2^2, \dots, z_n^2$.*

Proof. From the relations

$$f(z) = a_n(z - z_1)(z - z_2)\dots(z - z_n)$$

and

$$f(-z) = a_n(-z - z_1)(-z - z_2)\dots(-z - z_n)$$

it follows that

$$f(z)f(-z) = (-1)^n a_n^2(z^2 - z_1^2)(z^2 - z_2^2)\dots(z^2 - z_n^2)$$

and therefore, from (2.3)

$$g(z) = \mathcal{G}(f)(z) = (-1)^n a_n^2(z - z_1^2)(z - z_2^2)\dots(z - z_n^2), \tag{2.9}$$

which completes the proof of Proposition 1. □

In numerical analysis (cf. [8], [2] or [16]), the Graeffe method is used to compute an approximate value of the roots of a polynomial equation $f(x) =$

0. The first step of the method is to calculate f_k defined by (2.8) for k large enough. From Proposition 1, the roots of f_k are $z_1^{2^k}, \dots, z_n^{2^k}$, and, if we assume that $|z_1| > |z_2| > \dots > |z_n|$, the sum of the roots of f_k is close to $z_1^{2^k}$ which yields an approximate value for $|z_1|$. This old method is being revisited in the frame of computer algebra (cf. [7]).

Proposition 2. *Let $f(z) \in \mathbb{C}[[z]]$, $f(0) \neq 0$, and*

$$z\frac{f'(z)}{f(z)} = \sum_{n=1}^{\infty} a_n z^n. \tag{2.10}$$

Then, for $k \geq 1$, we have

$$\sum_{n=1}^{\infty} a_{2^k n} z^n = z\frac{f_k'(z)}{f_k(z)} = \frac{z}{f_k(z)}\frac{d}{dz} f_k(z), \tag{2.11}$$

where $f_k = \mathcal{G}^{(k)}(f)$ is defined by (2.2) and (2.8).

Remark 2. *Here and in the sequence, f_k' will denote the derivative of f_k (and not the k-iterate of f').*

Proof. We shall prove Proposition 2 by induction on k. For $k = 1$ and $z = y^2$, we have from (2.10) and (2.3)

$$\begin{aligned}
\sum_{n=1}^{\infty} a_{2n} z^n &= \sum_{n=1}^{\infty} a_{2n} y^{2n} = \frac{1}{2}\sum_{n=1}^{\infty}(a_n y^n + a_n(-y)^n) \\
&= \frac{1}{2}\left(y\frac{f'(y)}{f(y)} - y\frac{f'(-y)}{f(-y)}\right) = \frac{y}{2}\frac{f'(y)f(-y) - f(y)f'(-y)}{f(y)f(-y)} \\
&= \frac{y}{2f_1(y^2)}\frac{d}{dy} f_1(y^2) = z\frac{f_1'(z)}{f_1(z)}.
\end{aligned} \tag{2.12}$$

Further, the induction on k is easy, by substituting $a_{2^k n}$ to a_{2n} and f_{k-1} to f in (2.12). $\square$

Definition 2. *We shall say that two power series f, g with integral coefficients are congruent modulo M (where M is any positive integer) if their coefficients of same degree are congruent modulo M. In other words, if*

$$f(z) = a_0 + a_1 z + a_2 z^2 + \dots + a_n z^n + \dots \quad \in \mathbb{Z}[[z]]$$

and

$$g(z) = b_0 + b_1 z + b_2 z^2 + \dots + b_n z^n + \dots \quad \in \mathbb{Z}[[z]]$$

then,

$$f \equiv g \pmod{M} \iff \forall n \geq 0, \quad a_n \equiv b_n \pmod{M}. \tag{2.13}$$

Congruences of formal power series may be added or multiplied. If

$$f \equiv g \pmod{M} \tag{2.14}$$

and

$$u \equiv v \pmod{M}, \qquad u \in \mathbb{Z}[[z]], \ \ v \in \mathbb{Z}[[z]]$$

then

$$f + u \equiv g + v \pmod{M} \quad \text{and} \quad fu \equiv gv \pmod{M}. \tag{2.15}$$

You may derivate (2.14) and get

$$f' \equiv g' \pmod{M}. \tag{2.16}$$

Moreover, if $f(0) = g(0) = 1$, $1/f$ and $1/g$ have integer coefficients and we have, if (2.14) holds

$$\frac{1}{f} \equiv \frac{1}{g} \pmod{M}. \tag{2.17}$$

It is also easy to see that, for $f \in \mathbb{Z}[[z]]$ and $\mathcal{G}$ defined by (2.2) we have

$$\mathcal{G}(f) \equiv f \pmod{2}. \tag{2.18}$$

Proposition 3. *Let f and g be two formal power series with integral coefficients such that $f \equiv g \pmod{2}$. Then, for $k \geq 0$, we have*

$$f_k \equiv g_k \pmod{2^{k+1}}, \tag{2.19}$$

where $f_k = \mathcal{G}^{(k)}(f)$ and $g_k = \mathcal{G}^{(k)}(g)$ are defined by (2.2) and (2.8).

Proof. Let us start by proving that if $u, v \in \mathbb{Z}[[z]]$ satisfy

$$u \equiv v \pmod{2M} \tag{2.20}$$

where M is any positive integer, then $u_1 = \mathcal{G}(u)$ and $v_1 = \mathcal{G}(v)$ satisfy

$$u_1 \equiv v_1 \pmod{4M}. \tag{2.21}$$

It follows from (2.20) that there exists $w \in \mathbb{Z}[[z]]$ such that

$$u(z) = v(z) + 2Mw(z).$$

Further, from (2.3)

$$\begin{aligned} u_1(z^2) &= u(z)u(-z) = (v(z)+2Mw(z))(v(-z)+2Mw(-z)) \\ &= v_1(z^2)+2M[v(z)w(-z)+w(z)v(-z)]+4M^2w_1(z^2), \end{aligned}$$

where $w_1 = \mathcal{G}(w)$. But the above bracket is obviously congruent to 0 modulo 2 so that

$$u_1(z^2) \equiv v_1(z^2) \pmod{4M}$$

which, by substituting z to z^2, yields (2.21).

We shall prove Proposition 3 by induction on k. For $k = 0$, from (2.8), (2.19) is just our hypothesis $f \equiv g \pmod 2$. Let us assume that (2.19) holds for a non negative value of k ; then applying (2.21) with $u = f_k$, $v = g_k$ and $M = 2^k$ will give

$$f_{k+1} \equiv g_{k+1} \pmod{2^{k+2}}$$

and the proof of Proposition 3 is completed. □

3 The set $\mathcal{A} = \mathcal{A}_0(\{1,2,3\},3)$.

In all this Section, $\mathcal{A}$ will denote the set $\mathcal{A}_0(\{1,2,3\},3)$; we shall write $p(n), \sigma(n), \chi(n)$ instead of $p(\mathcal{A},n), \sigma(\mathcal{A},n), \chi(\mathcal{A},n)$ respectively. We shall recall in Lemma 1 some classical results on congruences modulo 2^k.

Lemma 1. *Let a, b and c be integers.*

(i) If a is odd and $k \geq 3$, the congruence

$$x^2 \equiv a \pmod{2^k} \tag{3.1}$$

has no solution if $a \not\equiv 1 \pmod 8$, and has four solutions if $a \equiv 1 \pmod 8$. Two of them satisfy

$$x^2 \equiv a \pmod{2^{k+1}}. \tag{3.2}$$

If ρ_k is a solution of (3.1) which satisfies (3.2) then the four solutions of (3.1) are $\pm\rho_k$ and $\pm\rho_k + 2^{k-1}$. By the method of Hensel, ρ_k can be calculated by induction : if $\rho_k^2 \equiv a + \varepsilon 2^{k+1} \pmod{2^{k+2}}$, $\varepsilon \in \{0,1\}$, then $\rho_{k+1} = \rho_k + \varepsilon 2^{k+1}$.

(ii) the congruence

$$x^2 - x + a \equiv 0 \pmod{2^k} \tag{3.3}$$

has no solution if a is odd; if a is even, it has two solutions, one is even and the other one is odd. They can be calculated by Hensel's method : if τ_k satisfies (3.3), then $\tau_{k+1} = \tau_k + \varepsilon 2^k$ is determined from

$$\varepsilon \equiv \frac{\tau_k^2 - \tau_k + a}{2^k} \pmod 2. \tag{3.4}$$

(iii) Any congruence $x^2 + bx + c \equiv 0 \pmod{2^k}$ can be put on the form (3.1) or (3.3) after a change of variable $y = x + \lfloor b/2 \rfloor$.

(iv) In the 2-adic field $\mathbb{Q}_2$, the equation $x^2 - a = 0$ has two roots if and only if $a \equiv 1 \pmod 8$. If x_1 and x_2 are the two solutions, we have $x_i \equiv \pm\rho_k \pmod{2^k}$.

(v) In the 2-adic field $\mathbb{Q}_2$, the equation $x^2 - x + a = 0$ has two roots x_1 and x_2 if and only if a is even. Moreover, $x_i \bmod 2^k$ are solutions of (3.3).

Proof of (i). It is a classical result that each odd residue class modulo 2^k for $k \geq 3$ can be written $\pm 5^\lambda$ with $0 \leq \lambda < 2^{k-2}$. From this result, it is not difficult to prove (i). We may observe that, if ρ is a solution of (3.2),

$$(\pm\rho + 2^{k-1})^2 \equiv a + 2^k \pmod{2^{k+1}}$$

so that $\pm\rho + 2^{k-1}$ are solutions of (3.1) but not of (3.2).

The Hensel method can be found in [1] or [10]. It can be accelerated to calculate $\rho_{k+1}, \ldots, \rho_{2k-1}$ in terms of ρ_k.

Proof of (ii). If τ_k is a solution of (3.3), $\tau_k \bmod 2$ is a solution of $x^2 - x + a \equiv 0 \pmod 2$. But if a is odd this last congruence has no solution while, if a is even, it has two solutions 0 and 1. Both can be extended to solutions of (3.3), by using (3.4) with $k = 1, 2, \ldots$.

An other possibility to solve (3.3) is to set $y = 2x - 1$. We have $y^2 = 4x^2 - 4x + 1 \equiv 1 - 4a \pmod{2^{k+2}}$. But the four solutions of this last congruence give only two solutions to (3.3).

Since the sum of the two roots is 1 they must have a different parity. To show (3.4), we calculate

$$(\tau_k + \varepsilon 2^k)^2 - (\tau_k + \varepsilon 2^k) + a \equiv \tau_k^2 - \tau_k + a - \varepsilon 2^k \pmod{2^{k+1}}.$$

Proof of (iii). It is obvious.

Proof of (iv). If

$$x_1 = \varepsilon_0 + \varepsilon_1 2 + \varepsilon_2 2^2 + \ldots + \varepsilon_k 2^k + \ldots$$

is a 2-adic solution of $x^2 - a = 0$, then, by writing $x_1 = U_k + 2^k R_k$, we have $U_k = x_1 \bmod 2^k$ and $x_1^2 = a \equiv U_k^2 \pmod{2^{k+1}}$, so that U_k satisfies (3.1) and (3.2) and thus, from (i), $U_k = \pm\rho_k$. In the other way, by the Hensel method, each root of (3.1) satisfying (3.2) can be extended in a 2-adic solution.

Proof of (v). The proof of (v) looks like the one of (iv), but it is easier since (3.3) has only two solutions while (3.1) has four solutions, and the proof of Lemma 1 is completed. $\square$

Theorem 1. *Let $\mathcal{A} = \mathcal{A}_0(\{1,2,3\},3)$. Then :*

(i) For all $k \geq 0$, the sequence $\sigma(2^k n) \mod 2^{k+1}$ is periodic in n with period $q_k = 7$.

(ii) If $u_k = \sigma(2^k) \bmod 2^{k+1}$ and $v_k = \sigma(3.2^k) \bmod 2^{k+1}$ then

$$\sigma(2^k n) \equiv u_k, v_k, -3 \pmod{2^{k+1}}, \text{ respectively as } \left(\frac{n}{7}\right) = 1, -1, 0. \tag{3.5}$$

where $\left(\frac{n}{7}\right)$ is the Legendre symbol.

(iii) u_k and v_k are the two solutions of the congruence

$$x^2 - x + 2 \equiv 0 \pmod{2^{k+1}} \tag{3.6}$$

and satisfy

$$u_k + v_k \equiv 1 \pmod{2^{k+1}} \quad \text{and} \quad u_k \cdot v_k \equiv 2 \pmod{2^{k+1}}. \tag{3.7}$$

Moreover, if $k \geq r$,

$$u_k \equiv u_r \pmod{2^{r+1}}. \tag{3.8}$$

(iv) The equation

$$x^2 - x + 2 = 0 \tag{3.9}$$

has two solutions in the 2-adic field $\mathbb{Q}_2$; the odd one is

$$x_1 = 1 + 2 + 2^3 + 2^4 + 2^6 + 2^{13} + 2^{14} + 2^{18} + 2^{19} + 2^{22} + 2^{25} + \dots. \tag{3.10}$$

We have

$$u_k \equiv x_1 \pmod{2^{k+1}}. \tag{3.11}$$

Moreover, the elements of $\mathcal{A}$ which are powers of 2 are $1, 2, 2^3, 2^4, 2^6, 2^{13}, \dots$; they are determined by

$$x_1 = \sum_{k=0}^{\infty} \chi(2^k) 2^k. \tag{3.12}$$

Proof of (i). The polynomial P defined by (1.11) and (1.12) is

$$P(z) = 1 + z + z^3 \tag{3.13}$$

since $p(0) = 1, p(1) = 1, p(2) = 2$ and $p(3) = 3$. It is irreducible over $\mathbb{F}_2[z]$ so that, in (1.13), $s = 1$ and $Q_1 = P$. So, it follows from Theorem A that $\beta_1 = 7$ and $q_k = 7$ for all $k \geq 0$, which proves (i).

Proof of (ii). We shall denote by H the other irreducible polynomial of degree 3 over $\mathbb{F}_2[z]$,

$$H(z) = 1 + z^2 + z^3. \tag{3.14}$$

From (2.8) and Proposition 1, the leading coefficient of $P_k = \mathcal{G}^{(k)}(P)$ is -1, and from (2.2), (1.2), (1.11) and (1.12)

$$P_k(0) = 1 \tag{3.15}$$

so that we can write

$$P_k(z) = \mathcal{G}^{(k)}(P)(z) = 1 + a_k z + b_k z^2 - z^3. \tag{3.16}$$

Now, we observe that, from (3.13) and (3.14) the polynomials P and H are reciprocal. So, from (3.16) and (2.5) we have

$$H_k(z) = \mathcal{G}^{(k)}(H)(z) = 1 - b_k z - a_k z^2 - z^3. \tag{3.17}$$

But we have

$$\frac{1-z^7}{1-z} = 1 + z + z^2 + z^3 + z^4 + z^5 + z^6 \equiv P(z)H(z) \pmod 2, \tag{3.18}$$

and this implies, from (2.7), (2.4), (2.6) and Proposition 3 that

$$\frac{1-z^7}{1-z} = 1 + z + z^2 + z^3 + z^4 + z^5 + z^6 \equiv P_k(z)H_k(z) \ (\mathrm{mod}\ 2^{k+1}). \tag{3.19}$$

By expanding the product $P_k H_k$ from (3.16) and (3.17), we get from (3.19)

$$a_k - b_k \equiv 1 \pmod{2^{k+1}} \quad \text{and} \quad a_k \cdot b_k \equiv -2 \pmod{2^{k+1}}. \tag{3.20}$$

By applying Proposition 2 to (1.9) (where $F(z) = F_{\mathcal{A}}(z)$ is defined by (1.3), we get :

$$\sum_{n=1}^{\infty} \sigma(2^k n) z^n = z \frac{F_k'(z)}{F_k(z)} \tag{3.21}$$

where F_k is the k-iterate of F by the transformation $\mathcal{G}$ (cf. (2.8)), and $F_k' = \dfrac{d}{dz}(F_k(z))$. It follows from (1.3), (1.4), (1.11) and (1.12) that

$$F \equiv P \pmod 2 \tag{3.22}$$

and Proposition 3 implies that

$$F_k \equiv P_k \pmod{2^{k+1}} \tag{3.23}$$

for all $k \geq 0$. We deduce from (3.15) and (3.23) that

$$F_k(0) = P_k(0) = 1 \tag{3.24}$$

and thus, from (2.15), (2.16) and (2.17), (3.23) implies

$$z\frac{F_k'(z)}{F_k(z)} \equiv z\frac{P_k'(z)}{P_k(z)} \pmod{2^{k+1}}. \tag{3.25}$$

Therefore, from (3.21) and (3.25), it follows :

$$\sum_{n=1}^{\infty} \sigma(2^k n) z^n \equiv z\frac{P_k'(z)}{P_k(z)} \pmod{2^{k+1}}. \tag{3.26}$$

From (3.26) and (3.19), we have

$$\sum_{n=1}^{\infty} \sigma(2^k n) z^n \equiv z\frac{P_k'(z)}{P_k(z)} \equiv z\frac{(1-z)P_k'(z)H_k(z)}{1-z^7} \pmod{2^{k+1}}. \tag{3.27}$$

The expansion of the numerator of the right hand side of (3.27) from (3.16), (3.17) and (3.20) yields

$$\begin{aligned} & z(1-z)P_k'(z)H_k(z) \equiv \\ & \quad a_k z + a_k z^2 - b_k z^3 + a_k z^4 - b_k z^5 - b_k z^6 - 3z^7 \pmod{2^{k+1}}. \end{aligned} \tag{3.28}$$

By expanding the denominator of the right hand side of (3.27) :$\dfrac{1}{1-z^7} = 1 + z^7 + z^{14} + \ldots$, it follows from (3.27) and (3.28) that

$$\left.\begin{array}{rcccccccl} \sigma(2^k n) \equiv & a_k & a_k & -b_k & a_k & -b_k & -b_k & -3 & \pmod{2^{k+1}} \\ \text{resp. as } n \equiv & 1 & 2 & 3 & 4 & 5 & 6 & 0 & \pmod{7}. \end{array}\right\} \tag{3.29}$$

The congruences (3.29) give for $n = 1$ and $n = 3$

$$u_k = \sigma(2^k) \equiv a_k \pmod{2^{k+1}} \text{ and } v_k \equiv \sigma(3 \cdot 2^k) \equiv -b_k \pmod{2^{k+1}}. \tag{3.30}$$

Since the quadratic residue classes modulo 7 are $1, 2$ and 4, (3.29) and (3.30) prove (ii).

Proof of (iii). Formula (3.7) follows from (3.20) and (3.30), and yields $u_k(1-u_k) \equiv 2 \pmod{2^{k+1}}$; so, u_k is a solution of the congruence (3.6). By the same way v_k can be proved to be also a solution of (3.6).

Finally, if $k \geq r$,

$$u_k = \sigma(2^k) = u_r + \sum_{j=r+1}^{k} \chi(2^j)2^j \equiv u_r \pmod{2^{r+1}},$$

which shows (3.8) and completes the proof of (iii).

Proof of (iv). Note that $u_k = \sigma(2^k)$ is odd (since $1 \in \mathcal{A}$) while v_k is even (since $1, 3 \in \mathcal{A}$). Since its discriminant -7 is congruent to 1 modulo 8 (cf. Lemma 1), the equation (3.9) has two roots in $\mathbb{Q}_2$, $x_1 \equiv 1 \pmod 2$ and $x_2 \equiv 0 \pmod 2$. Moreover, $x_1 \bmod 2^{k+1}$ is solution of (3.6), and as it is smaller than 2^{k+1} (like u_k) it is equal to u_k (because $u_k \equiv 1 \pmod 2$) and so, (3.11) is proved. Similarly, $v_k = x_2 \bmod 2^{k+1}$.

The expansion (3.10) has been calculated with the function *polrootspadic* of PARI. The expansion of x_2 is

$$x_2 = 2 + 2^2 + 2^5 + 2^7 + 2^8 + 2^9 + 2^{10} + 2^{11} + 2^{12} + 2^{15} + 2^{16} + \dots \quad (3.31)$$

At the exception of 2^1, the powers of 2 appear either in x_1 or in x_2 ; the reason is that

$$x_1 + x_2 = 1 = 2 + \frac{1}{1-2} = 2 + \sum_{n=0}^{\infty} 2^n.$$

Since u_k has been defined as equal to $\sigma(2^k) = \sum_{i=0}^{k} \chi(2^i)2^i$, (3.12) follows from (3.11) and this completes the proof of Theorem 1. □

Numerical table

$k =$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
$u_k =$	1	3	3	11	27	27	91	91	91	91	91	91	91	8283
$v_k =$	0	2	6	6	6	38	38	166	422	934	1958	4006	8102	8102

4 The elements of $\mathcal{A} = \mathcal{A}_0(\{1,2,3\},3)$.

Let us define two classical arithmetic functions. If n is a positive integer, $\omega(n)$ will denote the number of distinct primes dividing n while $\Omega(n)$ will be the number of primes dividing n according to multiplicity. We are now ready to state Theorem 2 which gives the multiplicative structure of the elements of $\mathcal{A}$.

Theorem 2. *Let $\mathcal{A} = \mathcal{A}_0(\{1,2,3\},3)$. Then :*

(i) The elements of $\mathcal{A}$ of the form 2^k are determined by Theorem 1 (iv). Similarly, the elements of $\mathcal{A}$ of the form $7 \cdot 2^k$ are determined by the even solution x_7 of the 2-adic equation $7x^2 + 7x + 2 = 0$

$$\begin{aligned} x_7 &= \sum_{k=0}^{\infty} \chi(7 \cdot 2^k)2^k && (4.1) \\ &= 2 + 2^2 + 2^3 + 2^6 + 2^7 + 2^9 + 2^{10} + 2^{12} + 2^{16} + 2^{18} + 2^{20} + 2^{21} + \dots \end{aligned}$$

(ii) Let p be an odd prime congruent to $1, 2$ or 4 modulo 7 (i.e.,$\left(\frac{p}{7}\right) = 1$). Then $(p, a) = 1$ for all $a \in \mathcal{A}$.

(iii) If $n \in \mathbb{N}$ and 49 divides n, then $n \notin \mathcal{A}$.

(iv) Let $n = 2^k m$, and

$$m = p_1^{\lambda_1} p_2^{\lambda_2} \dots p_h^{\lambda_h} \tag{4.2}$$

where p_i are primes, distinct and congruent to $3, 5$ or 6 modulo 7 and λ_i are positive integers. We assume that $h = \omega(m) \geq 1$ (i.e. $m \neq 1$) and recall that $\Omega(m) = \lambda_1 + \ldots + \lambda_h$.

- *(a) If $k \leq h - 2$, then $n \notin \mathcal{A}$ and $7n \notin \mathcal{A}$.*
- *(b) If $k = h - 1$, then, without any restriction, $n \in \mathcal{A}$ and $7n \in \mathcal{A}$.*
- *(c) If $k = h - 1 + r$, with $r \geq 1$, then $n \in \mathcal{A}$ if and only if*

$$m \equiv (-1)^{\Omega(m)}(1 - 2u_r)\ell^{-1} \pmod{2^{r+1}}, \quad \ell = 1, 3, 5, \ldots, 2^r - 1. \tag{4.3}$$

Moreover, the expansion

$$x_m = 1 + \chi(2^h m)2 + \chi(2^{h+1} m)2^2 + \ldots + \chi(2^{h+j} m)2^{j+1} + \ldots \tag{4.4}$$

is one of the two 2-adic solutions of the equation

$$m^2 x^2 + 7 = 0. \tag{4.5}$$

- *(d) If $k = h - 1 + r$, with $r \geq 1$, then $7n \in \mathcal{A}$ if and only if*

$$m \equiv (-1)^{\Omega(m)}(2u_r - 1)7^{-1}\ell^{-1} \pmod{2^{r+1}}, \; \ell = 1, 3, 5, \ldots, 2^r - 1. \tag{4.6}$$

Moreover, the expansion

$$x_{7,m} = 1 + \chi(7 \cdot 2^h m)2 + \ldots + \chi(7 \cdot 2^{h+j} m)2^{j+1} + \ldots \tag{4.7}$$

is one of the two 2-adic solutions of the equation

$$7m^2 x^2 + 1 = 0. \tag{4.8}$$

We may observe that for $k = 0, 1, 2$, we have for m odd, $m \neq 1$

$$n = 2^k m \in \mathcal{A} \Longleftrightarrow 7n = 7 \cdot 2^k m \in \mathcal{A}. \tag{4.9}$$

Remark 3. *Theorem 2 has been proved for $k = 0$ in [12] and for $k = 1$ in [3].*

Proof of (i). From (1.19), we have

$$S(7,k) = \chi(7) + \chi(7\cdot 2)2 + \ldots + \chi(7\cdot 2^k)2^k \tag{4.10}$$

and by (1.21) and (3.5)

$$\begin{aligned} 7S(7,k) &= \sum_{d\,|\,7} \mu(d)\sigma\left(\frac{7\cdot 2^k}{d}\right) \\ &= \sigma(7\cdot 2^k) - \sigma(2^k) \equiv -3 - u_k \pmod{2^{k+1}}, \end{aligned} \tag{4.11}$$

so that $S(7,k) \equiv (-3-u_k)7^{-1} \pmod{2^{k+1}}$. Since, from Theorem 1 (iii), u_k is solution of (3.6), a simple calculation shows that $S(7,k)$ is a solution of $7x^2+7x+2 \equiv 0 \pmod{2^{k+1}}$. From (3.5), $\sigma(7) = 1 + 7\chi(7) \equiv -3 \pmod 2$ so that $\chi(7) = 0$ and, from (4.10), $S(7,k)$ is even, which proves (i).

Proof of (ii). Let us suppose that $n = 2^k m \in \mathcal{A}$, m odd and multiple of a prime $p \equiv 1, 2, 4 \pmod 7$. Here we have from (1.19)

$$S(m,k) = \chi(m) + \chi(2m)2 + \ldots + \chi(2^k m)2^k < 2^{k+1}. \tag{4.12}$$

We get from (1.21)

$$mS(m,k) = \sum_{d\,|\,\overline{m}} \mu(d)\sigma\left(\frac{n}{d}\right) = \sum_{d\,|\,(\overline{m}/p)} \mu(d)\left[\sigma\left(\frac{n}{d}\right) - \sigma\left(\frac{n}{pd}\right)\right]. \tag{4.13}$$

But, from (3.5), the above bracket is congruent to 0 modulo 2^{k+1}, since $\left(\frac{n/d}{7}\right) = \left(\frac{n/pd}{7}\right)\times\left(\frac{p}{7}\right) = \left(\frac{n/pd}{7}\right)$. This implies that $S(m,k)$ is congruent to 0 modulo 2^{k+1}, and as $0 \le S(m,k) < 2^{k+1}$, $S(m,k)$ vanishes and, from (4.12), $\chi(n) = \chi(2^k m)$ also vanishes which proves (ii).

Proof of (iii). Let us now suppose that $n = 2^k m \in \mathcal{A}$, m odd and multiple of 49. If we define $S(m,k)$ by (4.12), (4.13) still holds if we replace p by 7. Now, in the bracket, both $\frac{n}{d}$ and $\frac{n}{7d}$ are multiple of 7, so that, from (3.5), again the bracket is congruent to 0 modulo 2^{k+1}. The proof of (iii) ends in the same terms than the one of (ii) above.

Proof of (iv). We shall need the following lemma :

Lemma 2. *With m, n, h, k as in Theorem 2 (iv), u_k as defined in Theorem 1, $S(m,k)$ as defined by (4.12) (or 1.19), we have*

$$mS(m,k) \equiv 2^{h-1}(2u_k - 1)(-1)^{\Omega(m)} \pmod{2^{k+1}}, \tag{4.14}$$

and

$$7mS(7m,k) \equiv -2^{h-1}(2u_k-1)(-1)^{\Omega(m)} \pmod{2^{k+1}}. \tag{4.15}$$

Proof of Lemma 2. With $n = 2^k m$, we have from (1.21),

$$mS(m,k) = \sum_{d\,|\,\overline{m}} \mu(d)\sigma\left(\frac{n}{d}\right) = \sum_{\substack{d\,|\,\overline{m}\\ \mu(d)=1}} \sigma\left(\frac{n}{d}\right) - \sum_{\substack{d\,|\,\overline{m}\\ \mu(d)=-1}} \sigma\left(\frac{n}{d}\right) \tag{4.16}$$

with $\overline{m} = p_1 \dots p_h$. Since $\left(\frac{2}{7}\right) = 1$ and $\left(\frac{p_i}{7}\right) = -1$, we have

$$\left(\frac{n}{7}\right) = (-1)^{\Omega(m)} \quad \text{and} \quad \left(\frac{n/d}{7}\right) = (-1)^{\Omega(m)}\mu(d).$$

Let us assume that $\Omega(m)$ is even ; then we get from (4.16) and (3.5)

$$mS(m,k) \equiv u_k \left(\sum_{\substack{d\,|\,\overline{m}\\ \mu(d)=1}} 1\right) - v_k \left(\sum_{\substack{d\,|\,\overline{m}\\ \mu(d)=-1}} 1\right) \pmod{2^{k+1}}. \tag{4.17}$$

The first (resp. second) sum is the number of subsets of $\{1,2,\dots,h\}$ with an even (resp. odd) cardinal ; they are both equal to 2^{h-1} (since $h \geq 1$), and from (3.7), (4.17) yields

$$mS(m,k) \equiv 2^{h-1}(2u_k-1) \pmod{2^{k+1}}. \tag{4.18}$$

If $\Omega(m)$ is odd, the same calculation leads to a formula looking like (4.18) where $(2u_k-1)$ is replaced by $(1-2u_k)$ so that, in both cases, (4.14) is proved.

With n still being equal to $2^k m$, we have from (1.21)

$$7mS(7m,k) = \sum_{d\,|\,(7\overline{m})} \mu(d)\sigma\left(\frac{7n}{d}\right) = \sum_{d\,|\,\overline{m}} \mu(d)\sigma\left(\frac{7n}{d}\right) - \sum_{d\,|\,\overline{m}} \mu(d)\sigma\left(\frac{n}{d}\right). \tag{4.19}$$

But, $7n/d \equiv 0 \pmod 7$ so that, by (3.5), $\sigma\left(\dfrac{7n}{d}\right) \equiv -3 \pmod{2^{k+1}}$ and since $\overline{m} \neq 1$, $\sum_{d\,|\,\overline{m}} \mu(d) = 0$. Therefore, it follows from (4.19) and (4.16) that

$$7mS(7m,k) \equiv -\sum_{d\,|\,\overline{m}} \mu(d)\sigma\left(\frac{n}{d}\right) \equiv -mS(m,k) \pmod{2^{k+1}}, \tag{4.20}$$

which, together with (4.14) proves (4.15). □

Let us prove now Theorem 2 (iv) :

Proof of (iv) (a). If $k \leq h-2$, it follows from Lemma 2 (4.14) that

$$S(m,k) \equiv 0 \pmod{2^{k+1}}.$$

From (4.12), this implies $S(m,k) = 0$ (since $0 \leq S(m,k) < 2^{k+1}$), and, therefore, $\chi(n) = \chi(2^k n) = 0$, i.e. $n \notin \mathcal{A}$.

By using (4.15) instead of (4.14), it can be proved in the same way that $\chi(7n) = 0$, i.e. $7n \notin \mathcal{A}$.

Proof of (iv) (b). If $k = h-1$, (4.14) writes

$$mS(m,k) \equiv 2^k(2u_k - 1)(-1)^{\Omega(m)} \pmod{2^{k+1}} \tag{4.21}$$

so that $S(m,k)$ is a multiple of 2^k, and, by dividing (4.21) by 2^k, $S(m,k)/2^k$ is odd. But then, from (4.12), $S(m,k) = 2^k\chi(2^k m) = 2^k\chi(n)$ and thus $\chi(n) = 1$ and $n \in \mathcal{A}$. A similar proof shows that $7n \in \mathcal{A}$.

Proof of (iv) (c). It follows from (4.14) that $S(m,k)$ is a multiple of 2^{h-1} and by dividing (4.14) by 2^{h-1} and using (3.8), we get

$$m\frac{S(m,k)}{2^{h-1}} \equiv (2u_k - 1)(-1)^{\Omega(m)} \equiv (2u_r - 1)(-1)^{\Omega(m)} \pmod{2^{r+1}}. \tag{4.22}$$

But, from (4.12), we have

$$\frac{S(m,k)}{2^{h-1}} = 1 + \chi(2^h m)2 + \ldots + \chi(2^k m)2^r, \tag{4.23}$$

since, by (b), $\chi(2^{h-1}m) = 1$. Let x be the solution of the congruence

$$mx \equiv -(2u_r - 1)(-1)^{\Omega(m)} \pmod{2^{r+1}}, \tag{4.24}$$

satisfying $0 \leq x < 2^{r+1}$; then, from (4.22), $2^{r+1} - x$ is equal to $\dfrac{S(m,r)}{2^{h-1}}$. So, if $x < 2^r$, it follows from (4.23) that $\chi(n) = \chi(2^k m) = 1$ while, if $x > 2^r$, $\chi(n) = 0$.

Since u_k satisfies (3.6),

$$\left((2u_r - 1)(-1)^{\Omega(m)}\right)^2 = 4u_r^2 - 4u_r + 1 \equiv -7 \pmod{2^{r+3}} \tag{4.25}$$

and, so, from (4.22), $\dfrac{S(m,r)}{2^{h-1}}$ is a solution of $m^2x^2 + 7 \equiv 0 \pmod{2^{r+3}}$, and thus, from (4.23) and Lemma 1, x_m is a solution of the 2-adic equation (4.5).

By using (4.3) with $r=1$ we know that $2^h m \in \mathcal{A}$ if and only if $m(-1)^{\Omega(m)} \equiv 3 \pmod 4$. Thus

$$\chi(2^h m) \equiv \frac{(-1)^{\Omega(m)} m - 1}{2} \pmod 2 \tag{4.26}$$

which allows us to distinguish for x_m between the two roots of (4.5).

Proof of (iv) (d). It is the same proof than the proof of (c). We just have to show (4.9), which follows immediately from (4.3) and (4.6) by noting that $7^{-1} \equiv -1 \pmod 8$. In particular, for $r=1$, (4.3) and (4.6) coïncide so that $\chi(7 \cdot 2^h m) = \chi(2^h m)$, and thus, formula (4.26) still holds when replacing $\chi(2^h m)$ by $\chi(7 \cdot 2^h m)$. □

If $m = p_1^{\lambda_1} \dots p_h^{\lambda_h}$, for $r \le 5$, (4.3) and (4.6) can be written as

$$\chi(2^h m) = \chi(7 \cdot 2^h m) = 1 \iff (-1)^{\Omega(m)} m \equiv 3 \pmod 4$$
$$\chi(2^{h+1} m) = \chi(7 \cdot 2^{h+1} m) = 1 \iff (-1)^{\Omega(m)} m \equiv 1, 3 \pmod 8$$
$$\chi(2^{h+2} m) = 1 \iff (-1)^{\Omega(m)} m \equiv 9, 11, 13, 15 \pmod{16}$$
$$\chi(7 \cdot 2^{h+2} m) = 1 \iff (-1)^{\Omega(m)} m \equiv 1, 3, 5, 7 \pmod{16}$$
$$\chi(2^{h+3} m) = 1 \iff (-1)^{\Omega(m)} m \equiv 1, 5, 11, 15, 19, 23, 25, 29 \pmod{32}$$
$$\chi(7 \cdot 2^{h+3} m) = 1 \iff (-1)^{\Omega(m)} m \equiv 1, 3, 5, 7, 9, 11, 13, 15 \pmod{32}$$

$$\begin{aligned} \chi(2^{h+4} m) &= 1 \iff \\ (-1)^{\Omega(m)} m &\equiv 1, 3, 5, 7, 11, 15, 17, 21, 25, 27, 29, 31, 41, 45, 51, 55 \pmod{64} \end{aligned}$$

$$\begin{aligned} \chi(7 \cdot 2^{h+4} m) &= 1 \iff \\ (-1)^{\Omega(m)} m &\equiv 5, 7, 9, 11, 21, 23, 25, 27, 33, 35, 45, 47, 49, 51, 61, 63 \pmod{64}. \end{aligned}$$

5 Estimation of $A(x)$

In this Section, we want to estimate $A(x)$ where $\mathcal{A}$ will denote the set $\mathcal{A}_0(\{1, 2, 3\}, 3)$; in view of using the description of the elements of $\mathcal{A}$ given in Theorem 2, we need some definitions.

Let us denote by $\mathcal{F}$ the set of the integers

$$n = 2^h p_1^{\lambda_1} p_2^{\lambda_2} \dots p_h^{\lambda_h}, \quad h \ge 1, \quad p_i \equiv 3, 5, 6 \pmod 7. \tag{5.1}$$

The elements of $\mathcal{F}$ are

$$\mathcal{F} = \{6, 10, 18, 26, 34, 38, 50, 54, 60, 62, 82, 94, \dots\}. \tag{5.2}$$

In [4], it has been proved that the asymptotic equivalence

$$F(x) = |\{n \in \mathcal{F}; n \leq x\}| \sim \gamma \frac{x}{(\log x)^{3/4}} \tag{5.3}$$

holds for $x \to \infty$, with

$$\gamma = \frac{1}{4\Gamma(5/4)} \left(\frac{6}{\pi\sqrt{7}}\right)^{1/4} \gamma_1 \tag{5.4}$$

and

$$\gamma_1 = \prod_{p \equiv 3,5,6 \pmod 7} \left(\left(1 + \frac{1}{2p-2}\right) \left(1 - \frac{1}{p}\right)^{1/2} \left(1 - \frac{1}{p^2}\right)^{-1/4} \right). \tag{5.5}$$

Calculating the product (5.5) with the primes up to 100000 yields for γ_1 the approximate value 1.07517. Note that, with the method described in [6], it is possible to calculate γ_1 with a very high precision. From $\Gamma(5/4) = 0.906402$ and (5.4) the approximate value of γ is

$$\gamma = 0.2733. \tag{5.6}$$

If $\delta(n)$ is the characteristic function of $\mathcal{F}$, the Dirichlet's series $\sum_{n=1}^{\infty} \frac{\delta(n)}{n^s}$ has an Eulerian product for $\Re s > 1$

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\delta(n)}{n^s} &= \prod_{p \equiv 3,5,6 \pmod 7} \left(1 + \frac{1}{(2p)^s} + \frac{1}{2^s p^{2s}} + \ldots + \frac{1}{2^s p^{ks}} + \ldots\right) \\ &= \prod_{p \equiv 3,5,6 \pmod 7} \left(1 + \frac{1}{2^s(p^s - 1)}\right). \end{aligned} \tag{5.7}$$

In [4], the proof of (5.3) starts from formula (5.7).

For $i = 0$ or 1, ℓ odd, and $r \geq 0$ we define

$$\mathcal{F}_{i;\ r,\ \ell} = \{2^h m \in \mathcal{F}, \quad \Omega(m) \equiv i \pmod 2, \quad m \equiv \ell \pmod{2^{r+1}}\}. \tag{5.8}$$

It has been proved in [4] that for r fixed, and x going to infinity, we have for any i and ℓ

$$F_{i;\ r,\ \ell}(x) = |\{n \in \mathcal{F}_{i;\ r,\ \ell}\ ,\ \ n \leq x\}| \sim \frac{\gamma}{2^{r+1}} \frac{x}{(\log x)^{3/4}}. \tag{5.9}$$

From (5.3), (5.9) and Theorem 2, we shall prove

Theorem 3. *Let $\mathcal{A} = \mathcal{A}_0(\{1,2,3\},3)$. The number $A(x)$ of elements of $\mathcal{A}$ up to x satisfies, when x tends to infinity :*

$$A(x) \sim \frac{24\gamma}{7} \frac{x}{(\log x)^{3/4}} \tag{5.10}$$

where γ is defined by (5.4); an approximate value of $24\gamma/7$ is 0.937.

Proof. Let $\mathcal{A}'$ be the subset of $\mathcal{A}$ whose elements are of the form 2^k or $7 \cdot 2^k$. The number of such elements up to x is clearly

$$A'(x) = O(\log(x)), \quad x \to \infty. \tag{5.11}$$

Now, it follows from Theorem 2 (i) and (iv) that

$$\mathcal{A} = \mathcal{A}' \cup \bigcup_{r=0}^{\infty} \left(\mathcal{A}^{(r)} \cup \mathcal{A}^{(r,7)}\right) \tag{5.12}$$

where the elements of $\mathcal{A}^{(r)}$ are the n's, $n \in \mathcal{A}$, $n = 2^{h-1+r} p_1^{\lambda_1} \dots p_h^{\lambda_h}$ and similarly, the elements of $\mathcal{A}^{(r,7)}$ are the n's, $n \in \mathcal{A}$, $n = 7 \cdot 2^{h-1+r} p_1^{\lambda_1} \dots p_h^{\lambda_h}$.

From Theorem 2 (iv) (b) it follows that for $r = 0$,

$$\mathcal{A}^{(0)} = \frac{1}{2}\mathcal{F} \quad \text{and} \quad A^{(0)}(x) = F(2x), \tag{5.13}$$

and

$$\mathcal{A}^{(0,7)} = \frac{7}{2}\mathcal{F} \quad \text{and} \quad A^{(0,7)}(x) = F\left(\frac{2x}{7}\right). \tag{5.14}$$

In the same way, if a^{-1} denotes an inverse of a modulo 2^{r+1}, Theorem 2 (iv) (c) and (d) implies for $r \geq 1$

$$A^{(r)}(x) = \sum_{\ell \in \{1,3,\dots,2^r-1\}} \left(F_{0;\ r,\ (1-2u_r)\ell^{-1}} \left(\frac{x}{2^{r-1}}\right) + F_{1;\ r,\ (2u_r-1)\ell^{-1}} \left(\frac{x}{2^{r-1}}\right)\right) \tag{5.15}$$

and

$$\begin{aligned} A^{(r,7)}(x) &= \sum_{\ell \in \{1,3,\dots,2^r-1\}} F_{0;\ r,\ (2u_r-1)(7\ell)^{-1}} \left(\frac{x}{7 \cdot 2^{r-1}}\right) \\ &+ \sum_{\ell \in \{1,3,\dots,2^r-1\}} F_{1;\ r,\ (1-2u_r)(7\ell)^{-1}} \left(\frac{x}{7 \cdot 2^{r-1}}\right). \end{aligned} \tag{5.16}$$

It also follows from Theorem 2 that, for any $r \geq 0$, $\mathcal{A}^{(r)} \subset 2^{r-1}\mathcal{F}$ and $\mathcal{A}^{(r,7)} \subset 7 \cdot 2^{r-1}\mathcal{F}$ so that

$$A^{(r)}(x) \leq F\left(\frac{x}{2^{r-1}}\right) \quad \text{and} \quad A^{(r,7)}(x) \leq F\left(\frac{x}{7 \cdot 2^{r-1}}\right) \leq F\left(\frac{x}{2^{r-1}}\right). \tag{5.17}$$

Moreover, from (5.3) and (5.2), there exists an absolute constant K such that

$$F(x) \le K \frac{x}{(\log x)^{3/4}} \qquad \text{for } x > 1 \text{ and } F(x) = 0 \qquad \text{for } x < 6. \tag{5.18}$$

It follows from (5.17) and (5.18) that $A^{(r)}(x) = A^{(r,7)}(x) = 0$ for $r > \dfrac{\log(x/3)}{\log 2}$ so that (5.12) implies

$$A(x) = A'(x) + \sum_{r=0}^{R''} \left(A^{(r)}(x) + A^{(r,7)}(x)\right), \quad R'' = \left\lfloor \frac{\log(x/3)}{\log 2} \right\rfloor. \tag{5.19}$$

Now, we cut the sum (5.19) in three parts :

$$A(x) = A'(x) + \sum_{r=0}^{R} + \sum_{r=R+1}^{R'} + \sum_{r=R'+1}^{R''} \stackrel{def}{=} A'(x) + S + S' + S'', \tag{5.20}$$

where R is a large but fixed integer, and R' is defined by $2^{R'-1} \le \sqrt{x} < 2^{R'}$. We have from (5.17)

$$S'' = \sum_{r=R'+1}^{R''} \left(A^{(r)}(x) + A^{(r,7)}(x)\right) \le 2 \sum_{r=R'+1}^{R''} F\left(\frac{x}{2^{r-1}}\right) \;;$$

and, by observing that, for $r \le R''$, $\dfrac{x}{2^{r-1}} \ge 6$, we get from (5.18)

$$S'' \le 2K \sum_{r=R'+1}^{R''} \frac{x}{(2^{r-1})(\log 6)^{3/4}} \le \frac{2Kx}{2^{R'-1}} \le 4K\sqrt{x}. \tag{5.21}$$

Similarly, we get

$$\begin{aligned} S' &= \sum_{r=R+1}^{R'} \left(A^{(r)}(x) + A^{(r,7)}(x)\right) \le 2 \sum_{r=R+1}^{R'} F\left(\frac{x}{2^{r-1}}\right) \\ &\le 2K \sum_{r=R+1}^{R'} \frac{x}{(2^{r-1})(\log(x/2^{R'-1}))^{3/4}} \le 2K \sum_{r=R+1}^{R'} \frac{x}{2^{r-1}(\log\sqrt{x})^{3/4}} \\ &\le 2^{1+3/4} K \frac{x}{(\log x)^{3/4}} \sum_{r=R+1}^{\infty} \frac{1}{2^{r-1}} \le \frac{8K}{2^R} \frac{x}{(\log x)^{3/4}}. \end{aligned} \tag{5.22}$$

We deduce from (5.15), (5.16) and (5.9) that, for $r \ge 1$ and r fixed,

$$A^{(r)}(x) \sim \frac{\gamma}{2^r} \frac{x}{(\log x)^{3/4}} \quad \text{and} \quad A^{(r,7)}(x) \sim \frac{\gamma}{7 \cdot 2^r} \frac{x}{(\log x)^{3/4}} \quad (x \to \infty). \tag{5.23}$$

Since R is fixed, we get from (5.13), (5.14), (5.3) and (5.23) for x tending to infinity

$$\begin{aligned} S &= A^{(0)}(x) + A^{(0,7)}(x) + \sum_{r=1}^{R} \left(A^{(r)}(x) + A^{(r,7)}(x)\right) \\ &\sim \frac{8\gamma}{7}\frac{x}{(\log x)^{3/4}}\left(2 + \sum_{r=1}^{R}\frac{1}{2^r}\right) = \frac{8\gamma}{7}\left(3 - \frac{1}{2^R}\right)\frac{x}{(\log x)^{3/4}}. \end{aligned} \tag{5.24}$$

By making R going to infinity, (5.10) follows from (5.20), (5.11), (5.21), (5.22) and (5.24) and the proof of Theorem 3 is completed. $\square$

The following table has been calculated by M. Deléglise by using the multiplicative structure of the elements of $\mathcal{A} = \mathcal{A}_0(\{1,2,3\}),3)$ given by Theorem 2. The last line is the asymptotic result of Theorem 3.

Numerical table

x	$A(x)$	$A(x)\,(\log x)^{3/4}/x$
10^2	47	1.48
10^3	293	1.25
10^4	2 204	1.16
10^5	17 604	1.100
10^6	148 834	1.066
10^7	1 297 167	1.043
10^8	11 562 386	1.028
....	......	...
∞		0.937

References

[1] E.J. Barbeau, Polynomials, Springer-Verlag, 1989.

[2] E.H. Bareiss, Resultant procedure and the mecchanisation of the Graeffe process, Journal of the ACM, **7** (1960), 346-386.

[3] F. Ben saïd, On a conjecture of Nicolas-Sárközy about partitions, to appear in J. Number Theory.

[4] F. Ben saïd et J.-L. Nicolas, Sur une extension de la formule de Selberg-Delange, to be published.

[5] F. Ben saïd et J.-L. Nicolas, Sets of parts such that the partition function is even, submitted to Acta Arithmetica.

[6] H. Cohen, High precision computation of Hardy-Littlewood constants, preprint.

[7] X. Gourdon, Thèse, http ://pauillac.inria.fr/algo/gourdon/thesis /html

[8] C.H. Graeffe, Die Auflösung der höheren numerischen Gleichungen, Zurich, 1837.

[9] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, revised edition, 1994.

[10] M.Mignotte, Mathématiques pour le calcul formel, P.U.F., Paris, 1989 ; english translation : Mathematics for computer algebra, Springer-Verlag, 1992.

[11] J.-L. Nicolas, I.Z. Ruzsa and A. Sárközy, On the parity of additive representation functions, J. Number Theory **73** (1998), 292-317.

[12] J.-L. Nicolas and A. Sárközy, On the parity of generalized partition functions, to appear in the proceedings of the Millennium Conference, Urbana, Illinois, May 2000.

[13] J.-L. Nicolas, On the parity of generalised partition functions II, Periodica Mathematica Hungarica, **43** (2001), 177-189.

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

[15] K. Ono, Distribution of the partition function modulo m, Ann. of Math. **151** (2000), 293-307.

[16] A. Ralston and P. Rabinowitz, A first course in numerical analysis, McGraw-Hill, 1978.