ACTA ARITHMETICA
106.2 (2003)

Sets of parts such that the partition function is even

by

F. Ben saïd (Monastir) and J.-L. Nicolas (Lyon)

1. Introduction. $\mathbb{N}_0$ and $\mathbb{N}$ denote the set of non-negative integers, resp. positive integers. $\mathcal{A}$ will denote a set of positive integers, and its counting function will be denoted by $A(x)$:

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

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

$$a_1x_1 + a_2x_2 + \ldots = n \tag{1.1}$$

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

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

We shall use the generating function

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

When $\mathcal{A} = \mathbb{N}$ it seems highly probable that the number of integers $n \le x$ 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 [7], [9], [10] and the references in them). That is the reason for which, in [7], 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

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

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

If $i = 0$ or 1, $\mathcal{B} = \{b_1, \ldots, b_k\} \ne \emptyset$ (where $b_1 < \ldots < b_k$) is a finite set of positive integers, $N \in \mathbb{N}$ and $N \ge b_k$, then there is (cf. [7]) a unique set

2000 *Mathematics Subject Classification*: Primary 11P81.

Research partially supported by Franch–Tunisian exchange program, C.M.C.U. no. 99/F 1507 and by CNRS, Institut Girard Desargues, UMR 5028.

$\mathcal{A} \subset \mathbb{N}$ such that

$$\mathcal{A} \cap \{1, \ldots, N\} = \mathcal{B} \tag{1.5}$$

and having 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 [7], when, for instance, $i = 0$. The set $\mathcal{A} = \mathcal{A}_0(\mathcal{B}, N)$ will be defined by recursion. We write $\mathcal{A}_n = \mathcal{A} \cap \{1, \ldots, n\}$ so that

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

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

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

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

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

which shows that $p(\mathcal{A}, n)$ is even for $n \geq N + 1$. Note that in the same way, any finite set $\mathcal{B} = \{b_1, \ldots, b_k\}$ 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 will be shown in Proposition 4 that, except in the case $i = 1$, $\mathcal{B} = \{1\}$, the set $\mathcal{A}_i(\mathcal{B}, N)$ is always infinite.

By the unicity of the above construction, if the set $\mathcal{A}$ has property $P_i(M)$, then, clearly, for any $N \geq M$ and $\mathcal{B} = \mathcal{A} \cap \{1, \ldots, N\}$ we have

$$\mathcal{A} = \mathcal{A}_i(\mathcal{B}, N). \tag{1.6}$$

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

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

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 [7], taking the logarithmic derivative of $F(z) = F_{\mathcal{A}}(z)$ defined by (1.3) yields

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

The main purpose of this paper is to show that for any positive integer k and any set $\mathcal{A} = \mathcal{A}_i(\mathcal{B}, N)$, the sequence

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

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

Note that (1.10) has already been proved for $k = 0$ in [7], and for $k = 1$ in [2]. The result (1.10) will be proved (Theorem 1) in Section 3, and, in the same section, Theorem 2 will specify the smallest period q_k of $\sigma(\mathcal{A}, 2^k n)$ mod 2^{k+1}; in particular, q_k is always odd. Property (1.10) seems a little surprising; the number 2 appears in it since the question we study is a parity problem.

By the Möbius inversion formula, (1.8) gives

$$n\chi(\mathcal{A}, n) = \sum_{d|n} \mu(d)\sigma(\mathcal{A}, n/d) \tag{1.11}$$

where μ is the Möbius function. If n is odd, by (1.10) with $k = 0$, we know the value of $\sigma(\mathcal{A}, n)$ mod 2, and this allows us to determine $\chi(\mathcal{A}, n)$ from (1.11) for any set $\mathcal{A} = \mathcal{A}_i(\mathcal{B}, N)$. This has been done in [8] for $\mathcal{A} = \mathcal{A}_0(\{1, 2, 3\}, 3)$ and in [6] for $\mathcal{A} = \mathcal{A}_0(\{1, 2, 3, 4, 5\}, 5)$. In [2], 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

$$S(m, k) = \chi(\mathcal{A}, m) + 2\chi(\mathcal{A}, 2m) + \ldots + 2^k \chi(\mathcal{A}, 2^k m). \tag{1.12}$$

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

$$\sigma(\mathcal{A}, n) = \sigma(\mathcal{A}, 2^k m) = \sum_{d|m} dS(d, k), \tag{1.13}$$

which, by the Möbius inversion formula, gives

$$mS(m, k) = \sum_{d|m} \mu(d)\sigma(\mathcal{A}, n/d) = \sum_{d|\overline{m}} \mu(d)\sigma(\mathcal{A}, n/d), \tag{1.14}$$

where $\overline{m} = \prod_{p|m} p$ 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 (1.12), we can deduce the value of $\chi(\mathcal{A}, 2^i m)$ for $i \leq k$. But, for technical reasons, the calculation can be difficult. We hope to return to this subject in another article.

Finally, in Section 4, we prove in Theorem 3 that, for any $\mathcal{B}$ and N, there is a set $\mathcal{B}'$ such that $\mathcal{A}_1(\mathcal{B}, N)$ and $\mathcal{A}_0(\mathcal{B}', N + 1)$ have the same elements with the exception of powers of 2.

We are pleased to thank K. Belabas and A. Sárközy for several remarks.

2. The Graeffe transformation. 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

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

We shall write $g = \mathcal{G}(f)$ for 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

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

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

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

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

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

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

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

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

$$\begin{aligned} &f_0 = f, \quad f_1 = \mathcal{G}(f), \\ &f_2 = \mathcal{G}(f_1), \ \ldots, \ f_k = \mathcal{G}(f_{k-1}) = \mathcal{G}^{(k)}(f), \ \ldots \end{aligned} \tag{2.8}$$

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

Proof. From the relations

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

and

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

it follows that

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

and therefore, from (2.3),

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

In numerical analysis (cf. [4], [1] or [11]), 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 $|z_1|>\dots>|z_n|$, 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 computer algebra (cf. [3]).

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. Here and in what follows, f_k' will denote the derivative of f_k (and not the k-iterate of f').

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

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

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

Definition. 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 the same degree are congruent modulo M. In other words, if

$$f(z)=a_0+a_1z+a_2z^2+\dots+a_nz^n+\dots\in\mathbb{Z}[[z]]$$

and

$$g(z)=b_0+b_1z+b_2z^2+\dots+b_nz^n+\dots\in\mathbb{Z}[[z]]$$

then

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

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

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

One may differentiate (2.14) to 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 (2.14) holds, then

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

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),

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

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

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

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

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

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

and the proof of Proposition 3 is complete. ∎

3. Periodicity of $\sigma(\mathcal{A}, 2^k n) \bmod 2^{k+1}$. Let $\mathcal{B}$ be a finite set, and $N \ge \max \mathcal{B}$ be an integer. For $i=0$ or $i=1$ we consider the set $\mathcal{A} = \mathcal{A}_i(\mathcal{B}, N)$ introduced in Section 1.

• If $i=0$, define the polynomial P (already considered in [8]) by

$$P(z) = \sum_{0 \le n \le J} \varepsilon_n z^n \tag{3.1}$$

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

$$p(\mathcal{A}, n) \equiv \varepsilon_n \pmod 2, \qquad \varepsilon_n \in \{0,1\}. \tag{3.2}$$

It follows from (1.3) and (1.4) that

$$F \equiv P \pmod 2. \tag{3.3}$$

• If $i=1$, we define J as the smallest integer $\le N+1$ such that $p(\mathcal{A}, n)$ is odd for all $n \ge J$ and $p(\mathcal{A}, J-1)$ is even. As observed in [8], such a $J \ge 2$ always exists, except in the case $\mathcal{B} = \{1\}$ which leads to

$$\mathcal{A}_1(\{1\}, N) = \{1\} \quad \text{for all } N \ge 1. \tag{3.4}$$

The polynomial P is now defined by (3.1), with

$$\varepsilon_n = \begin{cases} 0 & \text{if } p(\mathcal{A}, n) - p(\mathcal{A}, n-1) \text{ is even} \\ 1 & \text{if } p(\mathcal{A}, n) - p(\mathcal{A}, n-1) \text{ is odd} \end{cases} \qquad (\text{for } n = 0, 1, \dots, J) \tag{3.5}$$

with the convention (1.2). Note that the degree of P is $J \le N+1$. We have, from (1.3) and (1.4),

$$F(z) \equiv \sum_{n=0}^{J-2} p(\mathcal{A}, n) z^n + \frac{z^J}{1-z} \equiv \frac{P(z)}{1-z} \pmod 2. \tag{3.6}$$

Proposition 4. *Except the case* (3.4), *the set* $\mathcal{A} = \mathcal{A}_i(\mathcal{B}, N)$ *defined by* (1.5) *and* (1.4) *is infinite.*

Proof. If $\mathcal{A} = \mathcal{A}_i(\mathcal{B}, N)$ were finite, the product $\prod_{a \in \mathcal{A}} (1 - z^a)$ would be a polynomial, say $Q(z)$, of degree $s = \sum_{a \in \mathcal{A}} a \ge \sum_{a \in \mathcal{B}} a$ and leading coefficient ± 1 and, from (1.3), we should have

$$FQ = 1. \tag{3.7}$$

• If $i = 0$, it would follow from (3.7), (3.3) and (2.15) that

$$1 \equiv QP \pmod 2,$$

which is impossible, since the leading term of QP has a positive degree, and its coefficient is ± 1.

• If $i = 1$, (3.7), (3.6) and (2.15) would yield

$$1 - z \equiv Q(z)P(z) \pmod 2,$$

which is also impossible if $s \geq 2$, i.e. $\mathcal{B} \neq \{1\}$. ■

THEOREM 1. *For any set* $\mathcal{A} = \mathcal{A}_i(\mathcal{B}, N)$ (*defined by* (1.5) *and* (1.4)) *and for any non-negative integer* k, *the sequence* $(\sigma(\mathcal{A}, 2^k n))_{n\geq 1}$ (*where* σ *is defined by* (1.8)) *satisfies a linear recurrence congruence modulo* 2^{k+1}, *and therefore is periodic modulo* 2^{k+1}. *Moreover*, *if* q_k *denotes the smallest period*, *that is*, *the smallest positive integer* q_k *such that*

$$\sigma(\mathcal{A}, 2^k(n + q_k)) \equiv \sigma(\mathcal{A}, 2^k n) \pmod{2^{k+1}} \tag{3.8}$$

for all $n \geq 1$, *then*, *for all* $k \geq 0$,

$$q_k \text{ divides } q_{k+1}. \tag{3.9}$$

Proof. We start from the relation (1.9):

$$z\,\frac{F'(z)}{F(z)} = \sum_{n=1}^{\infty} \sigma(\mathcal{A}, n) z^n \tag{3.10}$$

where $F(z) = F_{\mathcal{A}}(z)$ is defined by (1.3). By Proposition 2,

$$\sum_{n=1}^{\infty} \sigma(\mathcal{A}, 2^k n) z^n = z\,\frac{F_k'(z)}{F_k(z)} \tag{3.11}$$

where F_k is the k-iterate of F under the transformation $\mathcal{G}$ (cf. (2.8)), and $F_k' = (d/dz)(F_k(z))$.

• Suppose that $i = 0$. The congruence (3.3) holds with the polynomial P defined by (3.1) and (3.2), and Proposition 3 implies that

$$F_k \equiv P_k \pmod{2^{k+1}} \tag{3.12}$$

for all $k \geq 0$, with $P_k = \mathcal{G}^{(k)}(P)$. It follows from (1.2), (2.1), (3.1) and (3.2) that

$$F_k(0) = P_k(0) = 1 \tag{3.13}$$

and thus, from (2.15)–(2.17), (3.12) implies

$$z\,\frac{F_k'(z)}{F_k(z)} \equiv z\,\frac{P_k'(z)}{P_k(z)} \pmod{2^{k+1}}. \tag{3.14}$$

Therefore, by (3.11) and (3.14),

$$\sum_{n=1}^{\infty} \sigma(\mathcal{A}, 2^k n) z^n \equiv z\,\frac{P_k'(z)}{P_k(z)} \pmod{2^{k+1}}. \tag{3.15}$$

But, for k fixed, if $P_k(z) = a_0 + a_1 z + \ldots + a_J z^J$, then (3.15) implies that, for $n \geq J+1$,

$$\begin{aligned}(3.16)\qquad & a_0\sigma(\mathcal{A}, 2^k n) \\ & \equiv -a_1\sigma(\mathcal{A}, 2^k(n-1)) - \ldots - a_J\sigma(\mathcal{A}, 2^k(n-J)) \pmod{2^{k+1}}.\end{aligned}$$

It follows from (3.13) that $a_0 = 1$, so that (3.16) is a linear recurrence congruence, and, from a classical result based on the pigeonhole principle (cf. [2], for instance, for a detailed proof), it follows that $\sigma(\mathcal{A}, 2^k n) \bmod 2^{k+1}$ is periodic in n.

To show (3.9), observe first that a divisor of $2^{k+1}n$ is either a divisor of $2^k n$ or a multiple of 2^{k+1}, and thus, from (1.8),

$$(3.17)\qquad \sigma(\mathcal{A}, 2^{k+1}n) \equiv \sigma(\mathcal{A}, 2^k n) \pmod{2^{k+1}}.$$

But, from (3.8), q_{k+1} is a period of $\sigma(\mathcal{A}, 2^{k+1}n) \bmod 2^{k+2}$, and thus, is also a period of $\sigma(\mathcal{A}, 2^{k+1}n) \bmod 2^{k+1}$ which is, by (3.17), equal to $\sigma(\mathcal{A}, 2^k n) \bmod 2^{k+1}$ whose smallest period is q_k, and (3.9) is proved.

• Suppose now that $i = 1$. The congruence (3.6) will replace (3.3); (3.11), (3.14) and (3.15) will become

$$(3.18)\qquad \sum_{n=1}^{\infty} \sigma(\mathcal{A}, 2^k n) z^n = z\,\frac{F_k'(z)}{F_k(z)} \equiv z\left(\frac{P_k'(z)}{P_k(z)} + \frac{1}{1-z}\right) \pmod{2^{k+1}},$$

and since the right hand side of (3.18) is a rational fraction, we conclude in the same way as in the case $i = 0$. ∎

Lemma 1. *Let $Q(z) \in \mathbb{F}_2[z]$ be a polynomial of degree d with $Q(0) \neq 0$. The order β of Q is the least positive integer such that $Q(z)$ divides $1 + z^\beta$ in $\mathbb{F}_2[z]$. Then*

(i) *the positive integers n such that $Q(z)$ divides $1 + z^n$ in $\mathbb{F}_2[z]$ are the multiples of β*;

(ii) *the order of an irreducible polynomial of degree d divides $2^d - 1$ and thus is odd*;

(iii) *the order of a product of pairwise relatively prime polynomials is the lcm of the orders of the factors.*

Proof. These are classical results in the theory of finite fields (cf. [5, Chap. 3, 3.6, 3.4 and 3.9]. ∎

Lemma 2. *Let $m \geq 1$ be an integer and $Q_1, \ldots, Q_m \in \mathbb{F}_2[z]$ be coprime polynomials of positive degrees. Assume that there exists non-zero polynomials $A_1, \ldots, A_m$ satisfying $(A_j, Q_j) = 1$ and $\deg(A_j) < \deg(Q_j)$ for $1 \leq j \leq m$ and*

$$\frac{A_1(z)}{Q_1(z)} + \ldots + \frac{A_m(z)}{Q_m(z)} = \frac{A(z)}{1+z^T} \qquad \text{in } \mathbb{F}_2[z]$$

where $T \geq 1$ *is an integer and* $A(z) \in \mathbb{F}_2[z]$. *Then the order* β_j *of* Q_j (*cf. Lemma* 1) *satisfies*

$$\beta_j \text{ divides } T, \quad 1 \leq j \leq m.$$

Proof. Write $Q = Q_1 \dots Q_m$, $\widetilde{Q}_j = Q/Q_j$, $B = \sum_{j=1}^m A_j \widetilde{Q}_j$ so that

$$\frac{A_1}{Q_1} + \dots + \frac{A_m}{Q_m} = \frac{B}{Q}$$

and

$$B(z)(1 + z^T) = A(z)Q(z) = A(z)Q_1(z) \dots Q_m(z).$$

From our hypotheses, each Q_j is coprime to B; therefore, $Q_j(z)$ divides $1 + z^T$ and from Lemma 1(i), β_j divides T. ∎

Theorem 2. *Let* P *be the polynomial defined by* (3.1) *and* (3.2) *if* $i = 0$ *and by* (3.1) *and* (3.5) *if* $i = 1$. *Let the factorization of* P *into irreducible factors over* $\mathbb{F}_2[z]$ *be*

$$P = Q_1^{\alpha_1} \dots Q_s^{\alpha_s}. \tag{3.19}$$

Denote by d_i *the degree of* Q_i, *by* β_i *the order of* $Q_i(z)$ (*cf. Lemma* 1), *and for all* $k \geq 0$, *set*

$$J_k = \{j : 1 \leq j \leq s, \alpha_j \equiv 2^k \pmod{2^{k+1}}\}, \tag{3.20}$$

$$I_k = J_0 \cup \dots \cup J_k = \{j : 1 \leq j \leq s, \alpha_j \not\equiv 0 \pmod{2^{k+1}}\}, \tag{3.21}$$

$$T_k = \mathrm{lcm}_{j \in I_k} \beta_j \tag{3.22}$$

(*with* $T_k = 1$ *if* $I_k = \emptyset$). *Then, for all* $k \geq 0$, *we have* $q_k = T_k$, *and* q_k *is odd.*

Note that if 2^{k_0} *is the highest power of* 2 *dividing any exponent* α_j *in* (3.19), *then for* $k > k_0$, *we have* $J_k = \emptyset$, $I_k = I_{k_0}$,

$$q_k = q := \mathrm{lcm}(\beta_1, \dots, \beta_s)$$

and moreover, *from* (3.9), q *is a common period for all the sequences* $(\sigma(\mathcal{A}, 2^k n) \bmod 2^{k+1})_{n \geq 1}$, $k \geq 0$.

Remark. Theorem 2 explains the examples given in [2] with $q_0 \neq q_1$.

Proof of Theorem 2. In the whole proof, k is a fixed non-negative integer.

• Assume $i = 0$. To prove Theorem 2, we first consider polynomials P and Q_j as polynomials of $\mathbb{Z}[z]$ with coefficients 0 or 1, so that (3.19) implies

$$P \equiv Q_1^{\alpha_1} \dots Q_s^{\alpha_s} \pmod 2. \tag{3.23}$$

Then, it follows from (3.23), Proposition 3 and (2.6) that

$$P_k \equiv (Q_1)_k^{\alpha_1} \dots (Q_s)_k^{\alpha_s} \pmod{2^{k+1}}, \tag{3.24}$$

where $P_k = \mathcal{G}^{(k)}(P)$ and $(Q_j)_k^{\alpha_j} = (\mathcal{G}^{(k)}(Q_j))^{\alpha_j}$. By taking the logarithmic derivative of (3.24), we get (as in (3.14)) from (3.21)

$$\frac{F_k'}{F_k} \equiv \frac{P_k'}{P_k} \equiv \sum_{j\in I_k} \alpha_j \frac{(Q_j)_k'}{(Q_j)_k} \pmod{2^{k+1}}. \tag{3.25}$$

If we set

$$V = \prod_{j\in I_k} Q_j, \tag{3.26}$$

then $V_k = \mathcal{G}^{(k)}(V) = \prod_{j\in I_k}(Q_j)_k$ is a common denominator for the right hand side of (3.25), and, if S is the corresponding numerator, we have $\deg S < \deg V_k$ and (3.25) reads

$$\frac{P_k'}{P_k} \equiv \frac{S}{V_k} \pmod{2^{k+1}}. \tag{3.27}$$

Further, from Lemma 1(iii) and (3.22), the order in $\mathbb{F}_2[z]$ of $V(z)$, defined by (3.26), is equal to T_k. So, there exists a polynomial $R \in \mathbb{Z}[z]$ such that

$$V(z)R(z) \equiv 1 - z^{T_k} \pmod{2}. \tag{3.28}$$

Now we consider V as a polynomial of $\mathbb{Z}[z]$. By (2.6) and (2.4), Proposition 3 implies

$$V_k(z)R_k(z) \equiv 1 - z^{T_k} \pmod{2^{k+1}} \tag{3.29}$$

where $V_k = \mathcal{G}^{(k)}(V)$ and $R_k = \mathcal{G}^{(k)}(R)$. Then it follows from (3.15), (3.27) and (3.29) that

$$\sum_{n=1}^{\infty} \sigma(\mathcal{A}, 2^k n) z^n \equiv z\,\frac{S(z)R_k(z)}{1 - z^{T_k}} \pmod{2^{k+1}}. \tag{3.30}$$

Since $\deg S < \deg V_k$, the degree of SR_k is smaller than T_k, and (3.30) shows that $\sigma(\mathcal{A}, 2^k n) \bmod 2^{k+1}$ is purely periodic with period T_k; therefore

$$q_k \text{ divides } T_k. \tag{3.31}$$

Let us show now $q_k = T_k$ by induction. The definition of q_k implies from (3.8) and (3.11) that for all $k \geq 0$,

$$z\,\frac{F_k'(z)}{F_k(z)} \equiv z\,\frac{W_k(z)}{1 - z^{q_k}} \pmod{2^{k+1}} \tag{3.32}$$

where $W_k(z) = \sum_{n=1}^{q_k} \sigma(\mathcal{A}, 2^k n) z^{n-1}$.

For $k = 0$, from (3.25), (2.8), (3.20) and (3.21), we have

$$\frac{F'}{F} \equiv \frac{P'}{P} \equiv \sum_{j\in I_0} \alpha_j \frac{Q_j'}{Q_j} \equiv \sum_{j\in J_0} \frac{Q_j'}{Q_j} \pmod{2}. \tag{3.33}$$

If $I_0 = J_0 = \emptyset$, the above sum is empty and from (3.10), $\sigma(\mathcal{A}, n) \equiv 0 \pmod{2}$ for all $n \geq 1$. Therefore, $q_0 = T_0 = 1$. If $I_0 = J_0 \neq \emptyset$, from (3.32) (with $k=0$) and (3.33) we deduce

$$\sum_{j\in J_0} \frac{Q'_j(z)}{Q_j(z)} \equiv \frac{W_0(z)}{1-z^{q_0}} \pmod 2.$$

For each $j \in J_0$, it follows from Lemma 2 that $\beta_j \mid q_0$; thus, from (3.22), $T_0 \mid q_0$, which, by (3.31), yields $q_0 = T_0$.

Assume now that $k \geq 1$ and

$$q_l = T_l \qquad \text{for } 0 \leq l \leq k-1. \tag{3.34}$$

From (3.25) and (3.21) we have

$$\frac{F'_k(z)}{F_k(z)} \equiv \frac{P'_k(z)}{P_k(z)} \equiv \sum_{j\in I_{k-1}} \alpha_j \frac{(Q'_j)_k(z)}{(Q_j)_k(z)} + \sum_{j\in J_k} \alpha_j \frac{(Q'_j)_k(z)}{(Q_j)_k(z)} \pmod{2^{k+1}}. \tag{3.35}$$

From our induction hypothesis (3.34) and from (3.22), for all $j \in I_{k-1}$, we have $\beta_j \mid q_{k-1} = T_{k-1}$; thus, from Lemma 1(i), $Q_j(z) \mid 1 - z^{q_{k-1}}$ in $\mathbb{F}_2[z]$. Therefore, there exists a polynomial $Y_j(z) \in \mathbb{Z}[z]$ such that $1 - z^{q_{k-1}} \equiv Y_j(z)Q_j(z) \pmod 2$. From (2.6), (2.4) and Proposition 3, we have $1-z^{q_{k-1}} \equiv (Y_j)_k(z)(Q_j)_k(z) \pmod{2^{k+1}}$ so that we can write

$$\sum_{j\in I_{k-1}} \alpha_j \frac{(Q'_j)_k(z)}{(Q_j)_k(z)} \equiv \frac{B(z)}{1-z^{q_{k-1}}} \pmod{2^{k+1}} \tag{3.36}$$

where $B(z) \in \mathbb{Z}[z]$.

If $J_k = \emptyset$, it follows from (3.35), (3.36) and (3.11) that q_{k-1} is a period of $\sigma(\mathcal{A}, 2^k n) \bmod 2^{k+1}$ so that $q_{k-1} \mid q_k$ which, by (3.9), implies $q_k = q_{k-1}$. Since $I_k = I_{k-1}$, from (3.21) and (3.34) we have $T_k = T_{k-1} = q_{k-1} = q_k$.

If $J_k \neq \emptyset$, (3.35) can be rewritten, by (3.36), (3.32) and (3.9), as

$$\begin{aligned}\sum_{j\in J_k} \alpha_j \frac{(Q'_j)_k(z)}{(Q_j)_k(z)} &\equiv \frac{F'_k(z)}{F_k(z)} - \sum_{j\in I_{k-1}} \alpha_j \frac{(Q'_j)_k(z)}{(Q_j)_k(z)} \\ &\equiv \frac{W_k(z)}{1-z^{q_k}} - \frac{B(z)}{1-z^{q_{k-1}}} \equiv \frac{B_1(z)}{1-z^{q_k}} \pmod{2^{k+1}}\end{aligned} \tag{3.37}$$

where $B_1(z) \in \mathbb{Z}[z]$ is a polynomial of degree less than q_k. In (3.37), from (3.20), the α_j's are multiples of 2^k, so are also the coefficients of B_1, and (3.37) implies

$$\sum_{j\in J_k} \frac{\alpha_j}{2^k} \cdot \frac{(Q'_j)_k(z)}{(Q_j)_k(z)} \equiv \frac{B_1(z)/2^k}{1-z^{q_k}} \pmod 2.$$

From (3.20), $\alpha_j/2^k$ is odd, and from (2.18), (2.17) and (2.15), we get

$$\sum_{j\in J_k} \frac{Q'_j(z)}{Q_j(z)} \equiv \frac{B_1(z)/2^k}{1-z^{q_k}} \pmod 2.$$

By Lemma 2, this implies that, for $j \in J_k$, we have $\beta_j \mid q_k$ so that $T_k \mid q_k$, which, together with (3.31), yields $q_k = T_k$.

The oddness of $q_k = T_k$ results from Lemma 1(ii) and (3.22), and the proof of Theorem 2 is complete when $i = 0$.

- Assume $i = 1$. From (3.18), (3.25) becomes

$$\frac{F_k'(z)}{F_k(z)} \equiv \frac{P_k'(z)}{P_k(z)} + \frac{1}{1-z} \equiv \frac{1}{1-z} + \sum_{j \in I_k} \alpha_j \frac{(Q_j)_k'}{(Q_j)_k} \pmod{2^{k+1}}. \tag{3.38}$$

The polynomial $1 - z^{T_k}$, where T_k is defined by (3.22), is still a common denominator for the right hand side of (3.38), and (3.31) can be proved in the same way as in the case $i = 0$. The proof of $q_k = T_k$ follows by replacing (3.25) by (3.38). ■

4. Relations between $\mathcal{A}_1(\mathcal{B}, N)$ and $\mathcal{A}_0(\mathcal{B}', N')$. In this section, we want to show that the sets $\mathcal{A}_1(\mathcal{B}, N)$ do not differ very much of the sets $\mathcal{A}_0(\mathcal{B}, N)$. More precisely, by adding or subtracting powers of 2 to $\mathcal{A}_1(\mathcal{B}, N)$, one can get a set $\mathcal{A}_0(\mathcal{B}', N+1)$ for a suitable set $\mathcal{B}' \subset \{1, \ldots, N+1\}$.

THEOREM 3. *Let $\mathcal{A} = \mathcal{A}_1(\mathcal{B}, N)$ be defined by* (1.5) *and* (1.4) *with $\mathcal{B}$ any set different from $\{1\}$, and N any integer satisfying $N \geq \max \mathcal{B}$.*

(i) *Denote by 2^h, $h \geq 0$, the smallest element* (*if it exists*) *of $\mathcal{A}$ which is a power of* 2. *Then*

$$\mathcal{A}' = \mathcal{A} \cup \{1, 2, \ldots, 2^{h-1}\} \setminus \{2^h\} = \mathcal{A}_0(\mathcal{B}', N+1) \tag{4.1}$$

with

$$\mathcal{B}' = \mathcal{A}' \cap \{1, 2, \ldots, N+1\}. \tag{4.2}$$

(ii) *If $\mathcal{A} \cap \{1, 2, \ldots, 2^h, \ldots\} = \emptyset$, then*

$$\mathcal{A}' = \mathcal{A} \cup \{1, 2, \ldots, 2^h, \ldots\} = \mathcal{A}_0(\mathcal{B}', N+1) \tag{4.3}$$

with $\mathcal{B}'$ still defined by (4.2).

Proof. (i) From (1.3), we have

$$\begin{aligned}\sum_{n=0}^{\infty} p(\mathcal{A}', n) z^n = \prod_{a \in \mathcal{A}'} \frac{1}{1-z^a} &= \frac{1-z^{2^h}}{(1-z)\ldots(1-z^{2^{h-1}})} \prod_{a \in \mathcal{A}} \frac{1}{1-z^a} \\ &\equiv \frac{1-z^{2^h}}{(1+z)\ldots(1+z^{2^{h-1}})} \prod_{a \in \mathcal{A}} \frac{1}{1-z^a} \pmod 2 \\ &\equiv (1-z) \prod_{a \in \mathcal{A}} \frac{1}{1-z^a} \equiv (1-z) \sum_{n=0}^{\infty} p(\mathcal{A}, n) z^n \pmod 2.\end{aligned}$$

Hence

$$p(\mathcal{A}', n) \equiv p(\mathcal{A}, n) - p(\mathcal{A}, n-1) \pmod 2,$$

so that, from (1.4), $p(\mathcal{A}', n)$ is even for $n \geq N + 2$; therefore, (4.1) follows from (1.6).

(ii) The argument is similar, by observing that

$$(1+z)(1+z^2)\ldots(1+z^{2^h})\ldots = \frac{1}{1-z}. \blacksquare$$

References

[1] E. H. Bareiss, *Resultant procedure and the mechanisation of the Graeffe process*, J. Assoc. Comput. Mach. 7 (1960), 346–386.
[2] F. Ben saïd, *On a conjecture of Nicolas–Sárközy about partitions*, J. Number Theory 95 (2002), 209–226.
[3] X. Gourdon, thèse, http://pauillac.inria.fr/algo/gourdon/thesis/html
[4] C. H. Graeffe, *Die Auflösung der höheren numerischen Gleichungen*, Zurich, 1837.
[5] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications*, Cambridge Univ. Press, revised edition, 1994.
[6] J.-L. Nicolas, *On the parity of generalised partition functions II*, Period. Math. Hungar. 43 (2001), 177–189.
[7] 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.
[8] J.-L. Nicolas and A. Sárközy, *On the parity of generalized partition functions*, in: Proc. Millennium Conference (Urbana, IL, 2000), to appear.
[9] K. Ono, *Parity of the partition function in arithmetic progressions*, J. Reine Angew. Math. 472 (1996), 1–15.
[10] —, *Distribution of the partition function modulo m*, Ann. of Math. 151 (2000), 293–307.
[11] A. Ralston and P. Rabinowitz, *A First Course in Numerical Analysis*, McGraw-Hill, 1978.

Faculté des Sciences de Monastir
Avenue de l'environnement
5000, Monastir, Tunisie
E-mail: Fethi.BenSaid@fsm.rnu.tn

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

Received on 23.10.2001
and in revised form on 7.3.2002 (4133)