Available online at www.sciencedirect.com

SCIENCE DIRECT

Discrete Mathematics 306 (2006) 1115–1125

DISCRETE MATHEMATICS

www.elsevier.com/locate/disc

On the counting function of the sets of parts $\mathscr{A}$ such that the partition function $p(\mathscr{A}, n)$ takes even values for n large enough

Fethi Ben Saïd[a], Houda Lahouar[a], Jean-Louis Nicolas[b,1]

[a]Département de Mathématiques, Faculté des Sciences de Monastir, Avenue de l'Environnement, 5000 Monastir, Tunisie

[b]Institut Camille Jordan, UMR 5208, Bâtiment Doyen Jean Braconnier, Université Claude Bernard (Lyon 1), 21 Avenue Claude Bernard, F-69622 Villeurbanne, France

Received 29 October 2003; received in revised form 21 October 2005; accepted 2 November 2005

Available online 18 April 2006

Abstract

If $\mathscr{A}$ is a set of positive integers, we denote by $p(\mathscr{A}, n)$ the number of partitions of n with parts in $\mathscr{A}$. First, we recall the following simple property: let $f(z) = 1 + \sum_{n=1}^{\infty} \varepsilon_n z^n$ be any power series with $\varepsilon_n = 0$ or 1; then there is one and only one set of positive integers $\mathscr{A}(f)$ such that $p(\mathscr{A}(f), n) \equiv \varepsilon_n \pmod 2$ for all $n \geqslant 1$. Some properties of $\mathscr{A}(f)$ have already been given when f is a polynomial or a rational fraction. Here, we give some estimations for the counting function $A(P, x) = \text{Card}\{a \in \mathscr{A}(P); a \leqslant x\}$ when P is a polynomial with coefficients 0 or 1, and $P(0) = 1$.

Keywords: Partitions; Generating functions; Mertens's formula; Cyclotomic polynomial

1. Introduction

Let us denote by $\mathbb{N}$ the set of positive integers. If $\mathscr{A}$ is a subset of $\mathbb{N}$, its characteristic function is denoted by $\chi(\mathscr{A}, n)$ or more simply by $\chi(n)$ when there is no confusion

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

If $\mathscr{A} = \{n_1, n_2, \ldots\} \subset \mathbb{N}$ with $1 \leqslant n_1 < n_2 < \ldots$ then $p(\mathscr{A}, n)$ denotes the number of partitions of n whose parts belong to $\mathscr{A}$: it is the number of solutions of the diophantine equation

$$n_1 x_1 + n_2 x_2 + \cdots = n,$$

in non-negative integers $x_1, x_2, \ldots$. The generating series associated to the set $\mathscr{A}$ is

$$F_{\mathscr{A}}(z) = \sum_{n=0}^{\infty} p(\mathscr{A}, n) z^n = \prod_{a \in \mathscr{A}} \frac{1}{1 - z^a} \tag{2}$$

E-mail addresses: Fethi.Bensaid@fsm.rnu.tn (F.B. Saïd), houda_lahouar@yahoo.fr (H. Lahouar), jlnicola@in2p3.fr (J.-L. Nicolas).

[1]Research partially supported by Région Rhône-Alpes, contract MIRA 2002 *Théorie des nombres Lyon-Monastir* and by CNRS, Institut Camille Jordan, UMR 5208.

0012-365X/$ - see front matter

doi:10.1016/j.disc.2005.11.022

and we shall set $p(\mathscr{A}, 0) = 1$. In [11], by considering the logarithmic derivative of $F_{\mathscr{A}}$, it was shown that

$$z\frac{F'_{\mathscr{A}}(z)}{F_{\mathscr{A}}(z)} = \sum_{n=1}^{\infty} \sigma(\mathscr{A}, n) z^n,$$

where

$$\sigma(n) = \sigma(\mathscr{A}, n) = \sum_{d \mid n} \chi(\mathscr{A}, d) d = \sum_{d \mid n, d \in \mathscr{A}} d. \tag{3}$$

Definition 1. 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 power of z are congruent modulo M. In other words, if

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

and

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

then

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

If $f \in \mathbb{F}_2[[z]]$,

$$f(z) = \sum_{n=0}^{\infty} \varepsilon_n z^n \quad \text{with } \varepsilon_n \in \{0, 1\} \quad \text{and} \quad \varepsilon_0 = 1, \tag{4}$$

it is proved in [2] and [7] that there exists a *unique* set $\mathscr{A}(f) \subset \mathbb{N}$ such that

$$F_{\mathscr{A}(f)}(z) = \prod_{a \in \mathscr{A}(f)} \frac{1}{1 - z^a} = \sum_{n=0}^{\infty} p(\mathscr{A}(f), n) z^n \equiv f(z) \pmod{2}, \tag{5}$$

in other words

$$p(\mathscr{A}(f), n) \equiv \varepsilon_n \pmod{2}, \quad n = 1, 2, 3, \ldots . \tag{6}$$

Indeed, for $n = 1$,

$$p(\mathscr{A}(f), 1) = \begin{cases} 1 & \text{if } 1 \in \mathscr{A}(f), \\ 0 & \text{if } 1 \notin \mathscr{A}(f) \end{cases}$$

and therefore, by (6),

$$1 \in \mathscr{A}(f) \iff \varepsilon_1 = 1. \tag{7}$$

Further, assuming that the elements of $\mathscr{A}(f)$ are known up to $n - 1$, we set $(\mathscr{A}(f))_{n-1} = \mathscr{A}(f) \cap \{1, 2, \ldots, n-1\}$; observing that there is only one partition of n using the part n, we see that

$$p(\mathscr{A}(f), n) = p((\mathscr{A}(f))_{n-1}, n) + \chi(\mathscr{A}(f), n)$$

and (1) and (6) yield

$$n \in \mathscr{A}(f) \Leftrightarrow \chi(\mathscr{A}(f), n) = 1 \Leftrightarrow p((\mathscr{A}(f))_{n-1}, n) \equiv 1 + \varepsilon_n \pmod{2}. \tag{8}$$

Let $P \in \mathbb{F}_2[z]$ be a polynomial of degree, say, N. Considering P as a power series allows one to define $\mathscr{A}(P)$ by (7) and (8). In [4,11,12], this set $\mathscr{A}(P)$ was introduced in a slightly different way: it was shown that, for any finite set $\mathscr{B} \subset \mathbb{N}$ and any integer $M \geqslant \max_{b \in \mathscr{B}} b$, there exists a unique set $\mathscr{A}_0 = \mathscr{A}_0(\mathscr{B}, M)$ such that $p(\mathscr{A}_0, n)$ is even for all

$n > M$. Clearly, from (6), the set $\mathscr{A}(P)$ has the property that $p(\mathscr{A}(P), n)$ is even for $n > N$ (since, in (4), $\varepsilon_n = 0$ for $n > N$) and so, by defining $\mathscr{B} = \mathscr{A}(P) \cap \{1, 2, \dots, N\}$, the two sets $\mathscr{A}(P)$ and $\mathscr{A}_0(\mathscr{B}, N)$ coincide. In other words, knowing $\mathscr{B}$ and M, the polynomial

$$P(z) \equiv \sum_{n=0}^{M} p(\mathscr{A}_0(\mathscr{B}, M), n) z^n \pmod 2$$

of degree $N \leqslant M$ satisfies $\mathscr{A}(P) = \mathscr{A}_0(\mathscr{B}, M)$.

Let the factorization of P into irreducible factors over $\mathbb{F}_2[z]$ be

$$P = Q_1^{\alpha_1} Q_2^{\alpha_2} \dots Q_\ell^{\alpha_\ell}. \tag{9}$$

We denote by β_i, $1 \leqslant i \leqslant \ell$, the order of $Q_i(z)$, that is the smallest integer such that $Q(z)$ divides $1 + z^\beta$ in $\mathbb{F}_2[z]$. It is known that β_i is odd (cf. [9, Chapter 3]). Let us set

$$q = \mathrm{lcm}(\beta_1, \beta_2, \dots, \beta_\ell) \quad (q \text{ is odd}). \tag{10}$$

It was proved in [4] (cf. also [11] and [1]) that, for all $k \geqslant 0$, the sequence $(\sigma(\mathscr{A}(P), 2^k n) \bmod 2^{k+1})_{n \geqslant 1}$ is periodic with period q defined by (10); in other words,

$$n_1 \equiv n_2 (\mathrm{mod}\, q) \Rightarrow \forall k \geqslant 0, \quad \sigma(\mathscr{A}(P), 2^k n_1) \equiv \sigma(\mathscr{A}(P), 2^k n_2) \pmod{2^{k+1}}. \tag{11}$$

Some attention has been paid to the counting function of the sets $\mathscr{A}(f)$:

$$A(f, x) = \mathrm{Card}\{a : a \leqslant x, a \in \mathscr{A}(f)\} = \sum_{n \leqslant x} \chi(\mathscr{A}(f), n). \tag{12}$$

It was observed in Reference [12] that for some polynomials P, the set $\mathscr{A}(P)$ is a union of geometric progressions of quotient 2, and so $A(P, x) = \mathcal{O}(\log x)$. For instance, from the classical identity

$$1 - z = \frac{1}{(1+z)(1+z^2)\dots(1+z^{2^n})\dots} \tag{13}$$

it is easy to see that the set $\mathscr{G} = \{1, 2, 4, 8, \dots, 2^n, \dots\}$ satisfies

$$\sum_{n=0}^{\infty} p(\mathscr{G}, n) z^n = \prod_{a \in \mathscr{G}} \frac{1}{1 - z^a} \equiv 1 + z \pmod 2$$

and thus, from the characteristic property (5), $\mathscr{A}(1 + z) = \mathscr{G}$.

In [7], it is shown that, if the power series f is a rational fraction, say P/Q, there exists a polynomial $U \in \mathbb{F}_2[z]$ such that

$$A\left(\frac{P}{Q}, x\right) = A(U, x) + \mathcal{O}(\log x), \quad x \to \infty.$$

In the paper [3], it is shown that the counting function of the set $\mathscr{A}(1 + z + z^3) = \mathscr{A}_0(\{1, 2, 3\}, 3)$ satisfies

$$A(1 + z + z^3, x) \sim c \frac{x}{(\log x)^{3/4}}, \quad x \to \infty,$$

where $c = 0.937\dots$ is a constant. In [10], it is shown that the number of *odd* elements of the set $\mathscr{A}(1 + z + z^3 + z^4 + z^5) = \mathscr{A}_0(\{1, 2, 3, 4, 5\}, 5)$ up to x is asymptotic to $c_2 x(\log \log x/(\log x)^{1/3})$; the constant c_2 is estimated in [5], where the approximate value $c_2 = 0.070187\dots$ is given.

In [2], a law for determining $\mathscr{A}(f_1 f_2)$ in terms of $\mathscr{A}(f_1)$ and $\mathscr{A}(f_2)$ is given, which yields an estimation of the counting function $A(f_1 f_2, x)$ in terms of $A(f_1, x)$ and $A(f_2, x)$. For instance, if $f_1(z) = 1 + z + z^3$ and $f_2(z) = 1 + z + z^3 + z^4 + z^5$, it is proved that

$$A(f_1 f_2, x) \sim A(f_2, x), \quad x \to \infty.$$

The aim of this paper is to give some general estimates for $A(P,x)$, the counting function (12) of the set $\mathscr{A}(P)$, when $P \in \mathbb{F}_2[z]$ is a polynomial and x tends to infinity. We shall prove

Theorem 1. *Let $P \in \mathbb{F}_2[z]$ be a polynomial such that $P(0)=1$, let $\mathscr{A}=\mathscr{A}(P)$ be the set defined by* (7) *and* (8) *and let q, defined by* (10), *be an odd period of the sequences $(\sigma(\mathscr{A},2^k n) \bmod 2^{k+1})_{n\geqslant 1}$. Let r be the order of 2 modulo q, that is the smallest positive integer such that $2^r \equiv 1 \pmod q$. We shall say that a prime $p \neq 2$ is a bad prime if*

$$\exists s, \quad 0\leqslant s\leqslant r-1 \quad \text{such that } p \equiv 2^s \pmod q. \tag{14}$$

Then

(i) *if p is a bad prime, we have $(p,n)=1$, for all $n \in \mathscr{A}$;*
(ii) *there exists an absolute constant C_1 such that, for all $x>1$,*

$$A(P,x) \leqslant 7(C_1)^r \frac{x}{(\log x)^{r/\varphi(q)}}, \tag{15}$$

where φ is Euler's function.

Theorem 2. *Let $P \in \mathbb{F}_2[z]$ be a polynomial such that $P(0)=1$, let $\mathscr{A}=\mathscr{A}(P)$ be the set defined by* (7) *and* (8) *and let q* (cf. (10)) *be a period of the sequences $(\sigma(\mathscr{A},2^k n) \bmod 2^{k+1})_{n\geqslant 1}$.*

- *Case* 1: *If the property*

$$\text{all the odd prime divisors of any } n \in \mathscr{A} \text{ divide } q \tag{16}$$

is true, then we have

$$A(P,x) = \mathcal{O}_q((\log x)^{\omega(q)+1}), \tag{17}$$

where $\omega(q)$ is the number of prime factors of q.

- *Case* 2: *If* (16) *is not true, there exists a positive real number λ depending on n_0 and q, such that*

$$\liminf_{x\to\infty} \frac{A(P,x)\log x}{x^{\lambda}} > 0. \tag{18}$$

What Theorem 2 says is that there exist two kinds of sets $\mathscr{A}(P)$: those of the first case are thin while those of the second case are denser. We shall prove

Theorem 3. *Let $f_1, f_2 \in \mathbb{F}_2[[z]]$ be such that $f_1(0)=f_2(0)=1$. Let us assume that there exist two polynomials $P_1, P_2 \in \mathbb{F}_2[z]$ which are products in $\mathbb{F}_2[z]$ of cyclotomic polynomials and satisfy $f_1P_1=f_2P_2$. Then the set $\mathscr{A}(f_1)\,\Delta\,\mathscr{A}(f_2) = (\mathscr{A}(f_1)\backslash\mathscr{A}(f_2)) \cup (\mathscr{A}(f_2)\backslash\mathscr{A}(f_1))$ is included in a finite union of geometric progressions of quotient* 2, *and thus*

$$|A(f_1,x)-A(f_2,x)| = \mathcal{O}(\log x). \tag{19}$$

In particular, let $P \in \mathbb{F}_2[z]$ be a polynomial which is a product of cyclotomic polynomials. Then the set $\mathscr{A}(P)$ is included in a finite union of geometric progressions of quotient 2, *and thus*

$$A(P,x) = \mathcal{O}(\log x). \tag{20}$$

We formulate the following conjecture:

Conjecture 1. Let $P \in \mathbb{F}_2[z]$ be a polynomial which is not congruent modulo 2 to any product of cyclotomic polynomials. Then there exists a constant $c(P)<1$ such that

$$A(P,x) \asymp \frac{x}{(\log x)^{c(P)}}. \tag{21}$$

One of the tools of the proofs of Theorems 1 and 2 will be the following. Let $\mathscr{A}$ be any subset of $\mathbb{N}$. If m is an odd positive integer, we set, as in [4], for $k \geqslant 0$

$$S(m,k) = \chi(\mathscr{A}, m) + 2\chi(\mathscr{A}, 2m) + \cdots + 2^k \chi(\mathscr{A}, 2^k m). \tag{22}$$

It follows from (3) that for $n = 2^k m$, we have

$$\sigma(\mathscr{A}, n) = \sigma(\mathscr{A}, 2^k m) = \sum_{d \mid m} d S(d,k). \tag{23}$$

By applying Möbius's inversion formula, (23) yields

$$m S(m,k) = \sum_{d \mid m} \mu(d) \sigma\left(\mathscr{A}, \frac{n}{d}\right) = \sum_{d \mid \overline{m}} \mu(d) \sigma\left(\mathscr{A}, \frac{n}{d}\right), \tag{24}$$

where μ is Möbius's function and $\overline{m} = \prod_{p \mid m} p$ is the radical of m. Another useful remark is that, if $0 \leqslant j < k$ and m is odd, a divisor of $2^k m$ is either a divisor of $2^j m$ or a multiple of 2^{j+1}, so that, for $0 \leqslant j \leqslant k$, we have

$$\sigma(\mathscr{A}, 2^k m) \equiv \sigma(\mathscr{A}, 2^j m) \pmod{2^{j+1}} \tag{25}$$

(note that (25) trivially holds for $j = k$).

2. Proof of Theorem 1

Let us start with two lemmas:

Lemma 1. *Let K be any positive integer and let $x \geqslant 1$ be any real number. Then we have*

$$\mathrm{Card}\{n \leqslant x;\, n \text{ coprime with } K\} = \sum_{n \leqslant x;\ (n,K)=1} 1 \leqslant 7 \frac{\varphi(K)}{K} x, \tag{26}$$

where φ is Euler's function.

Proof. This is a classical result from sieve theory: see Theorems 3–5 of [6]. □

Lemma 2 (*Mertens's formula*). *Let a and q be two positive coprime integers. There exists an absolute constant C_1 such that, for all $x > 1$,*

$$\Pi(x; q, a) \stackrel{\text{def}}{=} \prod_{\substack{p \leqslant x \\ p \equiv a \pmod q}} \left(1 - \frac{1}{p}\right) \leqslant \frac{C_1}{(\log x)^{1/\varphi(q)}}. \tag{27}$$

Proof. We have

$$\log \Pi(x; q, a) = - \sum_{\substack{p \leqslant x \\ p \equiv a \pmod q}} \frac{1}{p} + \sum_{\substack{p \leqslant x \\ p \equiv a \pmod q}} \left(\frac{1}{p} + \log\left(1 - \frac{1}{p}\right)\right). \tag{28}$$

The second sum satisfies:

$$0 \geqslant \sum_{\substack{p \leqslant x \\ p \equiv a \pmod q}} \left(\frac{1}{p} + \log\left(1 - \frac{1}{p}\right)\right) \geqslant \sum_{p} \left(\frac{1}{p} + \log\left(1 - \frac{1}{p}\right)\right) = -0.3157\ldots \tag{29}$$

as quoted in [15], 2.7 and 2.10. The first sum in (28) was estimated by Mertens who proved (cf. [8, Sections 7 and 110])

$$\sum_{\substack{p \leqslant x \\ p \equiv a \pmod q}} \frac{1}{p} = \frac{\log \log x}{\varphi(q)} + \mathcal{O}_q(1). \tag{30}$$

But Ramaré has told us that it is possible to prove (30) with an error term independent of q: in his paper [13], p. 496, the formula below is given

$$\sum_{\substack{n\leqslant x\\ n\equiv a(\bmod q)}} \frac{\Lambda(n)}{n} = \frac{\log x}{\varphi(q)} + C(q,a) + \mathcal{O}\left(\frac{\sqrt{q}\log^3 q}{\varphi(q)}\right) \tag{31}$$

where $\Lambda(n)$ is the Von Mangoldt function

$$\Lambda(n) = \begin{cases} \log p & \text{if } n \text{ is a power of a prime } p,\\ 0 & \text{if not} \end{cases} \tag{32}$$

and $C(q,a)$ is a constant depending on q and a. Since Euler's function satisfies $\varphi(q) \geqslant \log 2(q/\log(2q))$ (cf. [14], p. 316), the error term in (31) is bounded, and setting $x=1$ in (31) shows that $C(q,a)$ is also bounded. So, (31) implies

$$\sum_{\substack{n\leqslant x\\ n\equiv a(\bmod q)}} \frac{\Lambda(n)}{n} = \frac{\log x}{\varphi(q)} + \mathcal{O}(1) \tag{33}$$

and the constant involved in the $\mathcal{O}$ term is absolute. Let us set

$$W(x;q,a) \stackrel{\text{def}}{=} \sum_{\substack{p\leqslant x\\ p\equiv a(\bmod q)}} \frac{\log p}{p}. \tag{34}$$

It follows from (32) that

$$W(x;q,a) \leqslant \sum_{\substack{n\leqslant x\\ n\equiv a(\bmod q)}} \frac{\Lambda(n)}{n} \leqslant W(x;q,a) + \sum_{p}\sum_{m\geqslant 2} \frac{\log p}{p^m} \leqslant W(x;q,a) + 0.76$$

as mentioned in [15], 2.8 and 2.11, and (33) yield

$$W(x;q,a) = \frac{\log x}{\varphi(q)} + \mathcal{O}(1), \tag{35}$$

where the constant involved in the $\mathcal{O}$ term is absolute. By using Stieltjes's integral and partial summation, it follows from (35) that

$$\begin{aligned}\sum_{\substack{p\leqslant x\\ p\equiv a(\bmod q)}} \frac{1}{p} &= \int_{2^-}^{x} \frac{d[W(t;q,a)]}{\log t} = \frac{W(x;q,a)}{\log x} + \int_2^x \frac{W(t;q,a)}{t(\log t)^2}\,\mathrm{d}t\\ &= \frac{\log\log x}{\varphi(q)} + \mathcal{O}(1)\end{aligned} \tag{36}$$

and the constant involved in the $\mathcal{O}$ term is absolute; therefore, from (28), (36) and (29), Lemma 2 follows. Unfortunately no precise value for C_1 seems to be known. □

Proof of Theorem 1. (i) Let p be a bad prime, let m be an odd multiple of p and let j be any non-negative integer. We have to prove that

$$n = 2^j m \notin \mathscr{A} = \mathscr{A}(P). \tag{37}$$

It follows from (24), with $\mathscr{A} = \mathscr{A}(P)$, that

$$mS(m,j) = \sum_{d\,|\,\overline{m}} \mu(d)\sigma\left(\frac{n}{d}\right) = \sum_{d\,|\,\overline{m}/p} \mu(d)\left(\sigma\left(\frac{n}{d}\right) - \sigma\left(\frac{n}{dp}\right)\right). \tag{38}$$

But, from (14), there exists s, $0\leqslant s\leqslant r-1$, such that $p\equiv 2^s \pmod q$; therefore, for each divisor d of $\overline{m}/p$, we have

$$\frac{n}{d}\equiv 2^s\frac{n}{dp} \pmod q. \tag{39}$$

Since $n=2^j m$, (25) gives

$$\sigma\left(2^s\frac{n}{dp}\right)\equiv\sigma\left(\frac{n}{dp}\right) \pmod{2^{j+1}}. \tag{40}$$

From (11), (39) implies

$$\sigma\left(\frac{n}{d}\right)\equiv\sigma\left(2^s\frac{n}{dp}\right) \pmod{2^{j+1}} \tag{41}$$

while (40) and (41) imply

$$\sigma\left(\frac{n}{d}\right)-\sigma\left(\frac{n}{dp}\right)\equiv 0 \pmod{2^{j+1}},$$

and (38) becomes $mS(m,j)\equiv 0 \pmod{2^{j+1}}$ which yields, since m is odd,

$$S(m,j)\equiv 0 \pmod{2^{j+1}}. \tag{42}$$

From (22) and (1), it follows that

$$0\leqslant S(m,j)<2^{j+1}. \tag{43}$$

So, (42) and (43) give $S(m,j)=0$, which, from (22), yields $\chi(\mathscr{A},2^j m)=0$, which, by applying (1), proves (37).

(ii) Let us denote by $K=K(x)$ the product of the bad primes (see (14)) up to x. It follows from (i), Lemmas 1 and 2 that

$$A(P,x)\leqslant\sum_{\substack{n\leqslant x\\(n,K)=1}}1\leqslant 7\frac{\varphi(K)}{K}x=7x\prod_{s=0}^{r-1}\prod_{\substack{p\leqslant x\\ p\equiv 2^s \pmod q}}\left(1-\frac{1}{p}\right)\leqslant\frac{7(C_1)^r x}{(\log x)^{r/\varphi(q)}}$$

which completes the proof of Theorem 1. □

3. Proof of Theorem 2

Lemma 3. *Let $a_1,a_2,\ldots,a_k$ and y be positive real numbers. The number $N(a_1,a_2,\ldots,a_k;y)$ of solutions of the diophantine inequality*

$$a_1x_1+a_2x_2+\cdots+a_kx_k\leqslant y \tag{44}$$

in non-negative integers $x_1,x_2,\ldots,x_k$ satisfies

$$N(a_1,a_2,\ldots,a_k;y)\leqslant\frac{\left(y+\sum_{i=1}^k a_i\right)^k}{k!}\prod_{i=1}^k\left(\frac{1}{a_i}\right). \tag{45}$$

Proof. This is a classical lemma that can be found, for instance, in [16], III.5.2. □

Proof of Theorem 2. *Case* 1: Let us write the standard factorization of q into primes: $q=q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_s^{\alpha_s}$ with $s=\omega(q)$. From (16), we have

$$A(P,x)\leqslant\mathrm{Card}\{n\leqslant x,\ n=2^{i_0}q_1^{i_1}q_2^{i_2}\ldots q_s^{i_s},\ i_0\geqslant 0,\ldots,i_s\geqslant 0\}. \tag{46}$$

By using the notation of Lemma 3, the right-hand side of (46) can be written as $N(\log 2, \log q_1, \dots, \log q_s; \log x)$ and (45) yields, since $\log q_j \geqslant \log 3 \geqslant 1$,

$$A(P,x) \leqslant \frac{1}{(\omega(q)+1)!\log 2}(\log x + \log(2q))^{\omega(q)+1} \prod_{j=1}^{\omega(q)} \frac{1}{\log q_j}$$
$$\leqslant \frac{(\log x)^{\omega(q)+1}}{(\omega(q)+1)!\log 2}\left(1+\frac{\log(2q)}{\log x}\right)^{\omega(q)+1}$$

which, for $x \to \infty$, implies (17).

Case 2: Here, (16) does not hold; so, there exists an odd prime p_0 which is coprime to q and divides some element $n_0 \in \mathscr{A}(P)$; such an element can be written as

$$n_0 = 2^{k_0} m_0 \in \mathscr{A}(P), \quad k_0 \geqslant 0, \;\; m_0 \text{ odd}, \;\; m_0 = p_0^{\alpha} a_0, \;\; \alpha \geqslant 1, \;\; (p_0, a_0) = 1 \tag{47}$$

and (22) and (24) yield

$$m_0 S(m_0, k_0) = \sum_{d \mid \overline{m_0}} \mu(d)\sigma\left(\frac{n_0}{d}\right) = \sum_{d \mid \overline{a_0}} \mu(d)\left(\sigma\left(2^{k_0}\frac{m_0}{d}\right) - \sigma\left(2^{k_0}\frac{m_0}{dp_0}\right)\right), \tag{48}$$

where $\sigma(n) = \sigma(\mathscr{A}(P), n)$ is defined in (3).

Let p be an odd prime satisfying

$$p \equiv p_0 \pmod{2^{k_0+1} q} \quad \text{and} \quad (p, a_0) = 1 \tag{49}$$

and let us set

$$m = p^{\alpha} a_0, \quad n = 2^{k_0} m. \tag{50}$$

We want to show that

$$n \in \mathscr{A}(P). \tag{51}$$

As in (48), we have

$$m S(m, k_0) = \sum_{d \mid \overline{a_0}} \mu(d)\left(\sigma\left(2^{k_0}\frac{m}{d}\right) - \sigma\left(2^{k_0}\frac{m}{dp}\right)\right). \tag{52}$$

It follows from (49), (50) and (47), that

$$m \equiv m_0 \pmod{2^{k_0+1} q} \tag{53}$$

which implies that $m \equiv m_0 \pmod q$; further, for any divisor d of $\overline{a_0}$, we have $2^{k_0}(m/d) \equiv 2^{k_0}(m_0/d) \pmod q$ and $2^{k_0}(m/dp) \equiv 2^{k_0}(m_0/dp_0) \pmod q$. By applying (11), it follows that $\sigma(2^{k_0}(m/d)) \equiv \sigma(2^{k_0}(m_0/d)) \pmod{2^{k_0+1}}$ and $\sigma(2^{k_0}(m/dp)) \equiv \sigma(2^{k_0}(m_0/dp_0)) \pmod{2^{k_0+1}}$, which, from (48) and (52) implies

$$m S(m, k_0) \equiv m_0 S(m_0, k_0) \pmod{2^{k_0+1}}. \tag{54}$$

But, from (53), $m \equiv m_0 \pmod{2^{k_0+1}}$ holds, and, as m is odd, (54) yields

$$S(m, k_0) \equiv S(m_0, k_0) \pmod{2^{k_0+1}}.$$

Since, from (22), the inequalities $0 \leqslant S(m, k_0) < 2^{k_0+1}$ and $0 \leqslant S(m_0, k_0) < 2^{k_0+1}$ hold, we have

$$S(m, k_0) = S(m_0, k_0)$$

and, from the unicity of the binary expansion of (22), it follows that

$$\chi(2^j m) = \chi(2^j m_0), \quad j = 0, 1, \dots, k_0$$

which, for $j = k_0$, implies $\chi(n) = \chi(n_0) = 1$ and proves (51).

How many such n's do we get? Let us denote by $\pi(y; k, \ell) = \sum_{\substack{p \leqslant y \\ p \equiv \ell (\mathrm{mod}\ k)}} 1$ the number of primes up to y in the arithmetic progression $p \equiv \ell (\mathrm{mod}\, k)$. If k and ℓ are fixed and coprime, it is known that (cf. [8, Section 120, 16, Section II.8])

$$\pi(y; k, \ell) \sim \frac{y}{\varphi(k) \log y}, \quad y \to \infty. \tag{55}$$

The number of n's, $n \leqslant x$, satisfying (50) and (49) is certainly not less than

$$\pi\left(\left(\frac{x}{2^{k_0} a_0}\right)^{1/\alpha}; 2^{k_0+1} q, p_0\right) - \omega(a_0)$$

(where $\omega(a_0)$ is the finite number of prime factors of a_0) so that, from (51) and (55),

$$A(P, x) \geqslant \pi\left(\left(\frac{x}{2^{k_0} a_0}\right)^{1/\alpha}; 2^{k_0+1} q, p_0\right) - \omega(a_0) \geqslant \frac{1}{2\varphi\left(2^{k_0+1} q\right)} \frac{y}{\log y}$$

holds for x large enough with $y = (x/2^{k_0} a_0)^{1/\alpha}$. Since $\log y \leqslant \log x/\alpha$,

$$A(P, x) \geqslant \frac{\alpha}{2^{k_0+1} \varphi(q) \left(2^{k_0} a_0\right)^{1/\alpha}} \frac{x^{1/\alpha}}{\log x}.$$

This implies (18), with $\lambda = 1/\alpha$, which completes the proof of Theorem 2. □

4. Proof of Theorem 3

Lemma 4. *Let $f \in \mathbb{F}_2[[z]]$, $f(0) = 1$ and $\alpha \in \mathbb{N}$. We have*:

$$\mathscr{A}((1 - z^{\alpha}) f(z)) = \begin{cases} \mathscr{A}(f) \backslash \{\alpha\} \\ \quad \text{if } \alpha \in \mathscr{A}(f) \\ \mathscr{A}(f) \backslash \{2^h \alpha\} \cup \{\alpha, 2\alpha, \ldots, 2^{h-1}\alpha\} \\ \quad \text{if } h \text{ is the smallest integer such that } 2^h \alpha \in \mathscr{A}(f) \\ \mathscr{A}(f) \cup \{\alpha, 2\alpha, \ldots, 2^h \alpha, \ldots\} \\ \quad \text{if for all non-negative } h,\ 2^h \alpha \notin \mathscr{A}(f) \end{cases} \tag{56}$$

and

$$\mathscr{A}(f(z)/(1 - z^{\alpha})) = \begin{cases} \mathscr{A}(f) \cup \{\alpha\} \\ \quad \text{if } \alpha \notin \mathscr{A}(f) \\ \mathscr{A}(f) \cup \{2^h \alpha\} \backslash \{\alpha, 2\alpha, \ldots, 2^{h-1}\alpha\} \\ \quad \text{if } h \text{ is the smallest integer such that } 2^h \alpha \notin \mathscr{A}(f) \\ \mathscr{A}(f) \backslash \{\alpha, 2\alpha, \ldots, 2^h \alpha, \ldots\} \\ \quad \text{if for all non-negative } h,\ 2^h \alpha \in \mathscr{A}(f). \end{cases} \tag{57}$$

Proof. To prove (56), let us first assume that

$$\forall h \geqslant 0, \quad 2^h \alpha \notin \mathscr{A}(f). \tag{58}$$

If we denote by

$$\mathscr{G}(\alpha) = \{\alpha, 2\alpha, 4\alpha, \ldots\} \tag{59}$$

the infinite geometric progression with first term α and quotient 2, we have from (2) and (13)

$$F_{\mathscr{A}(f)\cup\mathscr{G}(\alpha)}(z) = F_{\mathscr{A}(f)}(z)\prod_{n=0}^{\infty}\frac{1}{1-z^{\alpha 2^n}} \equiv F_{\mathscr{A}(f)}(z)(1+z^{\alpha}) \pmod 2$$

which, from the characteristic property (5), proves the third case of (56).

If (58) does not hold, let us denote by $h \geqslant 0$ the smallest integer such that $2^h\alpha \in \mathscr{A}(f)$ and by $\mathscr{A}'$ the set $\mathscr{A}' = \mathscr{A}(f)\backslash\{2^h\alpha\} \cup \{\alpha, 2\alpha, \ldots, 2^{h-1}\alpha\}$ (if $h \neq 0$) and $\mathscr{A}' = \mathscr{A}(f)\backslash\{\alpha\}$ (if $h = 0$). From (2), we have

$$F_{\mathscr{A}'}(z) = F_{\mathscr{A}(f)}(z)\frac{1-z^{\alpha 2^h}}{(1-z^{\alpha})\ldots(1-z^{\alpha 2^{h-1}})} \equiv F_{\mathscr{A}(f)}(z)(1+z^{\alpha}) \pmod 2$$

which, from the characteristic property (5), proves the first case ($h = 0$) and the second case ($h \geqslant 1$) of (56).

Formula (57) is identical to formula (56), but expressed in a different way. □

Proof of Theorem 3. By using the notation (59), it follows from Lemma 4 that, for any $\alpha \in \mathbb{N}$ and $f \in \mathbb{F}_2[[z]]$,

$$\mathscr{A}\left((1-z^{\alpha})^{\pm 1} f(z)\right) \subset \mathscr{A}(f) \cup \mathscr{G}(\alpha). \tag{60}$$

Let us call $\Phi_n(z) \in \mathbb{Z}[z]$ the cyclotomic polynomial of index n. From the classical formula

$$\Phi_n(z) = \prod_{d\,|\,n}(1-z^d)^{\mu(n/d)}$$

and from our hypothesis, it follows that there exists a finite sequence $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_\ell$ of positive integers such that

$$f_2(z) = f_1(z)\prod_{i=1}^{\ell}(1-z^{d_i})^{\varepsilon_i}, \quad \varepsilon_i = -1 \text{ or } 1.$$

By applying (60) ℓ times, we have

$$\mathscr{A}(f_2) \subset \mathscr{A}(f_1) \cup \left(\bigcup_{i=1}^{\ell}\mathscr{G}(d_i)\right)$$

and, symmetrically,

$$\mathscr{A}(f_1) \subset \mathscr{A}(f_2) \cup \left(\bigcup_{i=1}^{\ell}\mathscr{G}(d_i)\right)$$

so that

$$\mathscr{A}(f_1)\,\Delta\,\mathscr{A}(f_2) = (\mathscr{A}(f_1)\backslash\mathscr{A}(f_2)) \cup (\mathscr{A}(f_2)\backslash\mathscr{A}(f_1)) \subset \left(\bigcup_{i=1}^{\ell}\mathscr{G}(d_i)\right) \tag{61}$$

which proves the first part of Theorem 3; (19) is an easy consequence of (61).

To prove the second part of Theorem 3, let us set $f_1(z) = P_2(z) = 1$ and $f_2(z) = P_1(z) = P(z)$. Since $\mathscr{A}(f_1) = \mathscr{A}(1) = \emptyset$, it follows from (61) that there exist $d_1 \leqslant d_2 \leqslant \cdots \leqslant d_\ell$ such that

$$\mathscr{A}(P) \subset \bigcup_{i=1}^{\ell}\mathscr{G}(d_i)$$

which completes the proof of Theorem 3. □

Acknowledgement

We are pleased to thank O. Ramaré for the proof of Lemma 2, A. Sárközy for fruitful discussions and J.A. Bondy for carefully reading our manuscript.

References

[1] F. Ben Saïd, On a conjecture of Nicolas–Sárközy about partitions, J. Number Theory 95 (2002) 209–226.
[2] F. BenSaïd, On some sets with even valued partition function, The Ramanujan J. 9 (2005) 63–75.
[3] F. Ben Saïd, J.-L. Nicolas, Even partition functions, Séminaire Lotharingien de Combinatoire ⟨http://www.mat.univie.ac.at/∼slc/⟩, 46 (2002), B 46i.
[4] F. Ben Saïd, J.-L. Nicolas, Sets of parts such that the partition function is even, Acta Arith. 106 (2003) 183–196.
[5] F. BenSaïd, J.-L. Nicolas, Sur une application de la formule de Selberg-Delange, Colloq. Math. 98 (2003) 223–247.
[6] H. Halberstam, H.-E. Richert, Sieve Methods, Academic Press, New York, 1974.
[7] H. Lahouar, Fonction de partitions à parité périodique, European J. Combin. 24 (2003) 1089–1096.
[8] E. Landau, Handbuch der Lehre von der Verteilung der Primzahlen, second ed., Chelsea, New-York, 1953.
[9] R. Lidl, H. Niederreiter, Introduction to Finite Fields and their Application, Cambridge University Press, Cambridge, 1994.
[10] J.-L. Nicolas, On the parity of generalized partition functions II, Period. Math. Hungar. 43 (2001) 177–189.
[11] J.-L. Nicolas, I.Z. Ruzsa, A. Sárközy, On the parity of additive representation function, J. Number Theory 73 (1998) 292–317.
[12] J.-L. Nicolas, A. Sárközy, On the parity of generalized partition functions, in: M.A. Bennett, B.C. Berndt, N. Boston, H.G. Diamond, A.J. Hildebrand, W. Philip, A.K. Peters (Eds.), Number Theory for the Millennium, vol. 3, 2002, pp. 55–72.
[13] O. Ramaré, Sur un théorème de Mertens, Manuscripta Math. 108 (2002) 495–513.
[14] P. Ribenboim, The New Book of Prime Numbers Record, third ed., Springer, Berlin, 1995.
[15] J.B. Rosser, L. Schoenfeld, Approximate formulas for some functions of prime numbers, Illinois J. Math. 6 (1962) 64–94.
[16] G. Tenenbaum, Introduction à la théorie analytique et probabiliste des nombres, S.M.F., Paris (1995). Introduction to Analytic and Probabilistic Number Theory, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.