Title: Even partition functions and 2-adic analysis

Author: N. Baccar

Abstract

Let $\mathcal{A}$ denote a set of positive integers, and let $p(\mathcal{A}, n)$ denote the associated partition function. Let β be an odd positive integer, and let $P(z)$ be a polynomial in $\mathbb{F}_2[z]$ of order β such that $P(0) = 1$. J.-L. Nicolas, I.Z. Ruzsa and A. Sárközy proved that there exists a unique set $\mathcal{A} = \mathcal{A}(P)$ such that $\sum_{n \geq 0} p(\mathcal{A}, n) z^n \equiv P(z) \pmod 2$; that is, the partition function $p(\mathcal{A}, n)$ is even from a certain point on. The problem of determining the elements of the set $\mathcal{A}(P)$ is not an easy one and several particular cases have already been studied; namely, when P is irreducible and $\beta = p$ a prime number such that the order of 2 modulo p is $p-1$, $(p-1)/2$, $(p-1)/3$ or $(p-1)/4$. In this paper, we consider the case P is irreducible such that the order of 2 modulo β is $\frac{\varphi(\beta)}{2}$ where φ is Euler's function.

Even partition functions and 2-adic analysis
by
N. Baccar
Université de Sousse
ISITCOM Hammam Sousse., Dép. de Math Inf.
5 Bis Rue 1 Juin 1955 - 4011 Hammam Sousse, Tunisie.
naceurbaccar@yahoo.fr

Abstract

Let $\mathcal{A}$ denote a set of positive integers, and let $p(\mathcal{A}, n)$ denote the associated partition function. Let β be an odd positive integer, and let $P(z)$ be a polynomial in $\mathbb{F}_2[z]$ of order β such that $P(0) = 1$. J.-L. Nicolas, I.Z. Ruzsa and A. Sárközy proved that there exists a unique set $\mathcal{A} = \mathcal{A}(P)$ such that $\sum_{n \geq 0} p(\mathcal{A}, n) z^n \equiv P(z) \pmod 2$; that is, the partition function $p(\mathcal{A}, n)$ is even from a certain point on. The problem of determining the elements of the set $\mathcal{A}(P)$ is not an easy one and several particular cases have already been studied; namely, when P is irreducible and $\beta = p$ a prime number such that the order of 2 modulo p is $p-1$, $(p-1)/2$, $(p-1)/3$ or $(p-1)/4$. In this paper, we consider the case P is irreducible such that the order of 2 modulo β is $\frac{\varphi(\beta)}{2}$ where φ is Euler's function.

Key words: Partitions, 2-adic integers, Dirichlet characters, Gauss sums, Ramanujan sums.

2010 MSC: 11P83, 11D88, 11L05, 11L40.

1 Introduction.

Let $\mathcal{A}$ be a non-empty set of positive integers, and let $p(\mathcal{A}, n)$ denote the number of partitions of n into parts belonging to the set $\mathcal{A}$; that is, the number of finite non-increasing sequences $n_1, n_2, \ldots, n_k$ belonging to $\mathcal{A}$ such that

$$n = n_1 + n_2 + \cdots + n_k.$$

By convention, we take $p(\mathcal{A}, 0) = 1$.

Let $\mathbb{F}_2$ be the field with two elements, and let $P(z) = 1 + \varepsilon_1 z + \cdots + \varepsilon_N z^N \in \mathbb{F}_2[z]$ of degree $N \geq 1$. It is known that (see [12]) there exists a unique set $\mathcal{A} = \mathcal{A}(P)$ of positive integers such that the generating function $\mathcal{F}(z)$ satisfies

$$\mathcal{F}(z) = \mathcal{F}_{\mathcal{A}}(z) = \prod_{a \in \mathcal{A}} \frac{1}{1 - z^a} = \sum_{n \geq 0} p(\mathcal{A}, n) z^n \equiv P(z) \pmod 2. \qquad (1.1)$$

The elements of the set $\mathcal{A} = \mathcal{A}(P)$ have been determined in some special cases but not for all P's, and it seems that the general case is a deep problem.

In fact the set $\mathcal{A} = \mathcal{A}(P)$ is constructed (cf. [12]) by recursion; we write $\mathcal{A}_n = \mathcal{A} \cap \{1, \ldots, n\}$ so that

$$p(\mathcal{A}_N, n) \equiv \varepsilon_n \pmod 2, \quad n = 1, \ldots, N.$$

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

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

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

$$\begin{cases} \text{if } n \in \mathcal{A}, & p(\mathcal{A}, n) = 1 + p(\mathcal{A}_{n-1}, n) \\ \text{if } n \notin \mathcal{A}, & p(\mathcal{A}, n) = p(\mathcal{A}_{n-1}, n). \end{cases} \tag{1.2}$$

which implies that $p(\mathcal{A}, n)$ is even for $n \geq N+1$. By computer, J.-L. Nicolas and A. Sárközy (see [13]) have studied all sets $\mathcal{A} = \mathcal{A}(P)$ for degree$(P) \leq 5$; for all of these sets, by using (1.2), they have computed the values of the first elements (up to 1000). As examples,

$$\mathcal{A}(1+z+z^4) = \{1, 2, 5, 6, 7, 10, 11, 13, 14, 16, 21, 22, 24, 28, 29, 33, \ldots\} \tag{1.3}$$

and

$$\mathcal{A}(1+z^3+z^4) = \{3, 4, 6, 7, 8, 10, 11, 12, 13, 15, 20, 21, 26, 29, 30, 32, \ldots\}. \tag{1.4}$$

Let $c \geq 2$ be an integer and $P_c(z) = P(z^c)$. By the algorithm (1.2), it is possible to see that the elements of $\mathcal{A}(P_c)$ are c-times the elements of $\mathcal{A}(P)$. Indeed, From (1.1),

$$\prod_{a \in \mathcal{A}(P)} \frac{1}{1 - z^{ca}} \equiv P(z^c) \pmod 2. \tag{1.5}$$

Let $\beta \geq 3$ be an odd positive integer and let $P(z) \in \mathbb{F}_2[z]$ be irreducible of order β; that is, β is the smallest positive integer such that $P(z)$ divides $1 + z^\beta$ in $\mathbb{F}_2[z]$. Let m be an odd positive integer and $\delta_\mathcal{A}$ is the characteristic function of the set $\mathcal{A}$; that is,

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

Throughout this paper, we denote by $\mathcal{A}^{<m>}$ the set of integers of the form $2^k m$ belonging to $\mathcal{A} = \mathcal{A}(P)$. One of the main problems that arise in the study of the set $\mathcal{A} = \mathcal{A}(P)$ is whether a positive integer $n = 2^j m$ is or is not in $\mathcal{A}^{<m>}$? An answer can be given by the algorithm (1.2) but for fairly large values of j. In order to overcome this difficulty, it has been convenient to consider the $2-$adic integer $S(\mathcal{A}, m)$ given by the expansion

$$S(\mathcal{A}, m) = \delta_\mathcal{A}(m) + 2\delta_\mathcal{A}(2m) + 2^2\delta_\mathcal{A}(2^2 m) + \cdots = \sum_{k=0}^{\infty} 2^k \delta_\mathcal{A}(2^k m), \tag{1.6}$$

Indeed, it is clear that by knowing the expansion $S(\mathcal{A}, m)$, one can compute $S(\mathcal{A}, m)$ mod 2^{j+1} then deduce $\delta_\mathcal{A}(2^k m)$ for all k, $0 \leq k \leq j$ and obtain all the elements of the set $\mathcal{A}^{<m>}$. Furthermore, it was proved in [2] that the $2-$adic integer $S(\mathcal{A}, m)$ is algebraic. Here and throughout

$$G_{m,\mathcal{A}}(x) \ \text{ denotes the minimal polynomial of } S(\mathcal{A}, m). \tag{1.7}$$

The method of proving that $S(\mathcal{A}, m)$ is algebraic is briefly recalled at the end of Section 2. To specify which root of $G_{m,\mathcal{A}}(x)$ corresponds to $S(\mathcal{A}, m)$, one just have to compute some first few elements of the set $\mathcal{A}$. For more clarity, it might be worthwhile to give an example illustrating how the polynomial $G_{m,\mathcal{A}}(x)$ provides a way to determine the set $\mathcal{A}^{<m>}$.

Example: $\beta = 15$**.** The only irreducible polynomials in $\mathbb{F}_2[z]$ of order $\beta = 15$ are $1 + z + z^4$ and $1 + z^3 + z^4$; we take $\mathcal{A} = \mathcal{A}(1 + z + z^4)$, $\mathcal{A}' = \mathcal{A}(1 + z^3 + z^4)$. For instance, we aim to determine $\mathcal{A}^{<7>}$ and $\mathcal{A}'^{<7>}$. In Theorem 5.1 below, with $m = 7$, we obtain

$$G_{7,\mathcal{A}}(x) = G_{7,\mathcal{A}'}(x) = x^2 + \frac{15}{49}.$$

By using the function polrootspadic of PARI, it turns out that roots of $x^2 + \frac{15}{49}$ are

$$x_1 = 1 + 2 + 2^2 + 2^3 + 2^4 + 2^{10} + 2^{11} + 2^{12} + \cdots + 2^{996} + 2^{998} + \cdots$$

and

$$x_2 = 1 + 2^5 + 2^6 + 2^7 + 2^8 + 2^9 + 2^{13} + 2^{14} + \cdots + 2^{997} + 2^{999} + \cdots .$$

From (1.3) (resp. (1.4)) we observe that $7 \in \mathcal{A}$ and $14 = 2 \times 7 \in \mathcal{A}$ (resp. $7 \in \mathcal{A}'$ and $14 = 2 \times 7 \notin \mathcal{A}'$), so that from (1.6), $S(\mathcal{A}, 7) \equiv 3 \pmod 4$ (resp. $S(\mathcal{A}', 7) \equiv 1 \pmod 4$) and therefore $S(\mathcal{A}, 7) = x_1$ (resp. $S(\mathcal{A}', 7) = x_2$). Hence

$$\mathcal{A}^{<7>} = \{7, 14, 28, 56, 112, \ldots, 2^{996} \times 7, 2^{998} \times 7, \ldots\} \tag{1.8}$$

and

$$\mathcal{A}'^{<7>} = \{7, 224, 448, 896, \ldots, 2^{997} \times 7, 2^{999} \times 7, \ldots\} \tag{1.9}$$

For a positive integer n, denote by $\widetilde{n}$ the *square-free kernel* of n; that is,

$$\widetilde{n} = \prod_{p \mid n,\ p \text{ prime}} p \quad \text{with } \widetilde{1} = 1, \tag{1.10}$$

and we denote by $\omega(n)$ the number of prime factors of n without multiplicity; that is,

$$\omega(n) = \sum_{p \text{ prime},\ p \mid n} 1. \tag{1.11}$$

For an odd positive integer d, denote by $s(d)$ the order of 2 modulo d; that is, $s(d)$ is the smallest positive exponent for which

$$2^{s(d)} \equiv 1 \pmod d, \tag{1.12}$$

and denote by $r(d)$ the positive integer satisfying

$$\varphi(d) = s(d)r(d) \tag{1.13}$$

where φ is Euler's function.

For $\mathcal{A} = \mathcal{A}(P)$, the problem of determining the elements of the set $\mathcal{A}^{<m>}$ has been solved when the order β of the irreducible polynomial P is a prime number p such that $s(p) = (p-1)/2$ (see [1]), $s(p) = (p-1)/3$ (see [4]) and $s(p) = (p-1)/4$ (see [3]). If $s(p) = p-1$, it turns out that $P(z) = \frac{1-z^p}{1-z} = 1 + z + \cdots + z^{p-1}$ is the only irreducible polynomial of order p; in this case we have

$$\begin{aligned} \mathcal{F}_{\mathcal{A}}(z) &\equiv \frac{1-z^p}{1-z} \pmod 2 \\ &\equiv \frac{1}{1-z}\frac{1}{1-z^p}\frac{1}{1-z^{2p}}\frac{1}{1-z^{4p}}\cdots\frac{1}{1-z^{2^k p}}\cdots \pmod 2, \end{aligned}$$

which means that

$$\mathcal{A} = \{1, p, 2p, 4p, \ldots, 2^k p, \ldots\}.$$

In the present paper, we aim to treat the case P is irreducible of order β such that

$$s(\beta) = \varphi(\beta)/2.$$

An observation (cf. [10, Theorem 2.47]) of big importance is that there exist only two irreducible polynomials in $\mathbb{F}_2[z]$ of order β. Moreover, it turns out (cf. Section 3) that one also have $s(\widetilde{\beta}) = \varphi(\widetilde{\beta})/2$ which will allow us to restrict our study to the case β square-free. Indeed, if β is not square-free and $\widetilde{\beta}$ is the square-free kernel of β defined by (1.10) then (cf. Section 3)

$$\mathcal{A}(P) = c \cdot \mathcal{A}(R), \tag{1.14}$$

where $c = \beta/\widetilde{\beta}$ and R is an irreducible polynomial in $\mathbb{F}_2[z]$ of order $\widetilde{\beta}$. This may be interpreted as asserting that

$$\begin{cases} \mathcal{A}(P)^{<m>} = \emptyset & \text{if } c \nmid m \\ \mathcal{A}(P)^{<m>} = c \cdot \mathcal{A}(R)^{<m/c>} & \text{if } c \mid m. \end{cases}$$

It will be proved in Lemma 3.1 below that $\omega(\beta) = 1$ or 2. As has been mentioned above the case β square-free with $\omega(\beta) = 1$ (that is, $\beta = p$ is prime) was already treated, then we need only concern ourselves with the situation in which β is square-free with $\omega(\beta) = 2$. Hence, it is convenient to consider the set $\mathcal{L}$ defined by

$$\mathcal{L} = \{d \geq 3,\ d \text{ odd, square-free and not prime such that } s(d) = \varphi(d)/2\}; \tag{1.15}$$

the first elements (up to 100) of $\mathcal{L}$ are: $15, 21, 33, 35, 39, 55, 57, 69, 77, 87, 95$. The first part of Section 3 will be devoted to the study of the set $\mathcal{L}$.

For purpose of determining the set $\mathcal{A}(P)^{<m>}$, where P is irreducible of order $\beta \in \mathcal{L}$, we explicitly compute $G_{m,\mathcal{A}}(x)$ for all odd positive integers m: this result is given below in Theorem 5.1. Depending on the values of m, the polynomial $G_{m,\mathcal{A}}(x)$ is either x (which means that $S(\mathcal{A}, m) = 0$; that is, $\mathcal{A}(P)^{<m>} = \emptyset$) or a quadratic polynomial. We will start by recalling in Section 2 some of the main properties of the set $\mathcal{A} = \mathcal{A}(P)$. In Section 4, we give a brief survey on Dirichlet characters, Gauss sums and Ramanujan sums. We end this paper by giving a numerical example with $\beta = 15 = 3 \times 5$ and $m = 3^a 5^b 7$ ($a \geq 0$ and $b \geq 0$); we first determine the sets $\mathcal{A}^{<m>}$ and $\mathcal{A}'^{<m>}$ where $\mathcal{A} = \mathcal{A}(1 + z + z^4)$ and $\mathcal{A}' = \mathcal{A}(1 + z^3 + z^4)$ and then deduce the sets $\mathcal{A}(P)^{<m>}$, for any irreducible polynomial P of order $45 = 3^2 \times 5$.

2 Some results on the set $\mathcal{A} = \mathcal{A}(P)$

Let $\beta \geq 3$ be an odd positive integer. We shall call a prime number $p \geq 3$ a β-*bad prime* if there exists a positive integer t such that

$$p \equiv 2^t \pmod{\beta}. \tag{2.1}$$

In what follows we denote by $\mathcal{M}_\beta$ the set of all odd positive integers m for which there does not exist a β-*bad prime* p such that $p \,|\, m$.

Remark 2.1. Let $P(z) \in \mathbb{F}_2[z]$ be irreducible of order β and let $\mathcal{A} = \mathcal{A}(P)$ be the even partition set satisfying (1.1). It turns out (see [2] and [6, Theorem 1, III and IV]) that if $m \notin \mathcal{M}_\beta$ or $\widetilde{\beta}\beta \mid m$ then $S(\mathcal{A}, m)$ vanishes. Consequently, the elements of the set $\mathcal{A}$ are of the form

$$2^k m, \text{ where } m \in \mathcal{M}_\beta \text{ and } \widetilde{\beta}\beta \nmid m. \tag{2.2}$$

Let $s = s(\beta)$ and $r = r(\beta)$ be the integers defined by (1.12) and (1.13). Let $P_1, P_2, \ldots, P_r$ be all the distinct irreducible polynomials in $\mathbb{F}_2[z]$ of order β (see [10, Theorem 2.47]); it is also important to point out that each of these polynomials is of degree s. For all ℓ, $1 \leq \ell \leq r$, let $\mathcal{A}_\ell = \mathcal{A}(P_\ell)$ be the even partition set satisfying (1.1), and let $S(\mathcal{A}_\ell, m)$ be the 2-adic integer given by (1.6). Let the polynomial $H_m(x)$ defined by

$$H_m(x) = m^r(x - S(\mathcal{A}_1, m))(x - S(\mathcal{A}_2, m)) \cdots (x - S(\mathcal{A}_r, m)). \tag{2.3}$$

Interestingly(see [2, Proposition 3.1]), the polynomial $H_m(x)$ has integer coefficients, which means that for all ℓ, $1 \leq \ell \leq r$, the minimal polynomial $G_{m,\mathcal{A}_\ell}(x)$ of the algebraic number $S(\mathcal{A}_\ell, m)$ (cf. (1.7)) is a factor of $H_m(x)$.

Let $(\mathbb{Z}/\beta\mathbb{Z})^*$ be the group of invertible residues modulo β, and let $< 2 >$ be its subgroup generated by 2. Then $< 2 >$ acts on the set $\mathbb{Z}/\beta\mathbb{Z}$ by usual multiplication. Given such action and denoting the orbit of some n by $O_\beta(n)$, it follows that $\mathbb{Z}/\beta\mathbb{Z}$ is partitioned as follows

$$\mathbb{Z}/\beta\mathbb{Z} = O_\beta(y_1) \cup O_\beta(y_2) \cup \cdots O_\beta(y_f) \cup O_\beta(\beta),$$

with $y_1 = 1$. We will say that $O_\beta(y_i)$ is an invertible orbit if $\gcd(y_i, \beta) = 1$; then clearly, r is the number of invertible orbits and so $(\mathbb{Z}/\beta\mathbb{Z})^\star$ may be represented in the form

$$(\mathbb{Z}/\beta\mathbb{Z})^\star = O_\beta(y_1) \cup O_\beta(y_2) \cup \cdots O_\beta(y_r), \tag{2.4}$$

where $O_\beta(y_1), O_\beta(y_2), \ldots, O_\beta(y_r)$ are the invertible orbits. For $r + 1 \leq i \leq f$ the orbits $O_\beta(y_i)$ are those for which y_i is not coprime with β, but not a multiple of β. Here and throughout this paper we adopt the extension that the orbits are also considered as part of $\mathbb{Z}$: $n \in O_\beta(y)$ if there exists $t \geq 0$ such that

$$n \equiv 2^t y \pmod{\beta}. \tag{2.5}$$

One can easily observe that β-*bad primes* (defined in (2.1)) are elements of $O_\beta(1)$. Furthermore, it should be noted that (cf. [2, formula (2.11)])

$$|O_\beta(y)| = s\left(\frac{\beta}{\gcd(\beta, y)}\right). \tag{2.6}$$

Example: When $\beta = 15$, we obtain

$$\mathbb{Z}/15\mathbb{Z} = O_{15}(1) \cup O_{15}(7) \cup O_{15}(3) \cup O_{15}(5) \cup O_{15}(15),$$

so that $s = s(15) = 4$, $r = 2$, $f = 4$, $y_1 = 1$, $y_2 = 7$, $y_3 = 3$, $y_4 = 5$ and

$$\begin{array}{rcl} O_{15}(1) &=& \{1, 2, 4, 8\} \\ O_{15}(7) &=& \{7, 11, 13, 14\} \\ O_{15}(3) &=& \{3, 6, 9, 12\} \\ O_{15}(5) &=& \{5, 10\} \\ O_{15}(15) &=& \{15\}. \end{array}$$

We define the polynomial $D_m(z)$ (cf. [2, formula (3.8)]) by

$$D_m(z) = \sum_{h=1}^{f} \lambda(m, y_h) B(y_h, z) + s\gamma(m),$$

where $B(n, z)$ is the polynomial given by

$$B(n, z) = \sum_{j=0}^{s-1} z^{2^j n \bmod \beta}; \; n \in \mathbb{Z}, \tag{2.7}$$

$$\lambda(m, n) = \sum_{\substack{d \mid \widetilde{m} \\ \frac{m}{d} \in O_\beta(n)}} \mu(d), \tag{2.8}$$

$$\gamma(m) = \sum_{\substack{d \mid \widetilde{m} \\ \frac{m}{d} \equiv 0 \pmod{\beta}}} \mu(d),$$

μ is the Möbius's function, $s = s(\beta)$ is defined in (1.12) and $\widetilde{m}$ is defined by (1.10). We shall note that $B(n, z)$ is stable on the orbits of $\mathbb{Z}/\beta\mathbb{Z}$; that is,

$$\text{if } n_1 \in O_\beta(n_2) \text{ then } B(n_1, z) = B(n_2, z). \tag{2.9}$$

Consequently, using the fact that $B(\beta, z) = s$, we get

$$D_m(z) = \sum_{h=1}^{f} \left(\sum_{\substack{d \mid \widetilde{m} \\ \frac{m}{d} \in O_\beta(y_h)}} \mu(d) B(\frac{m}{d}, z) \right) + \sum_{\substack{d \mid \widetilde{m} \\ \frac{m}{d} \equiv 0 \pmod{\beta}}} \mu(d) B(\frac{m}{d}, z),$$

whence

$$D_m(z) = \sum_{d\,|\,\widetilde{m}} \mu(d) B(\frac{m}{d}, z). \tag{2.10}$$

Let ζ be a β-th primitive root of unity over the 2-adic field $\mathbb{Q}_2$. It was proved in [2, formula (3.13)] that, for all ℓ, $1 \leq \ell \leq r$, $S(\mathcal{A}_\ell, m)$ can be expressed in terms of ζ. More precisely, the sets $\mathcal{A}_\ell$ can be arranged so that,

$$mS(\mathcal{A}_\ell, m) = -D_m(\zeta^{y_\ell});\ 1 \leq \ell \leq r. \tag{2.11}$$

Knowing this, we may rewrite the polynomial $H_m(x)$ (cf. (2.3)) as

$$H_m(x) = (mx + D_m(\zeta^{y_1}))(mx + D_m(\zeta^{y_2})) \cdots (mx + D_m(\zeta^{y_r})). \tag{2.12}$$

Example: By way of illustration, we take $\beta = 15$. In this instance, we find that $B(1, z) = z + z^2 + z^4 + z^8$, $B(7, z) = z^7 + z^{11} + z^{13} + z^{14}$, $B(3, z) = z^3 + z^6 + z^9 + z^{12}$, $B(5, z) = 2z^5 + 2z^{10}$ and $B(15, z) = 4$. Next, choosing $m = 7$, we obtain

$$D_7(\zeta) = B(7, \zeta) - B(1, \zeta) = \zeta^7 + \zeta^{11} + \zeta^{13} + \zeta^{14} - \zeta - \zeta^2 - \zeta^4 - \zeta^8,$$

$$D_7(\zeta^7) = -D_7(\zeta),$$

and

$$\begin{aligned} H_7(x) &= (7x + D_7(\zeta))(7x + D_7(\zeta^7)) = 49x^2 - (D_7(\zeta))^2 \\ &= 49x^2 + \zeta^{14} + \zeta^{13} - 2\zeta^{12} + \zeta^{11} - 4\zeta^{10} - 2\zeta^9 + \zeta^8 + \zeta^7 - 2\zeta^6 - 4\zeta^5 + \\ &\quad \zeta^4 - 2\zeta^3 + \zeta^2 + \zeta + 8. \end{aligned}$$

3 A description of $\mathcal{L}$

Recall that $\mathcal{L}$ (cf. (1.15)) is the set of all odd integers $d \geq 3$ square-free and not prime satisfying $s(d) = \frac{\varphi(d)}{2}$, where $s(d)$ is defined by (1.12) and φ is Euler's function. In Theorem 3.1 below, we will give a description of the set $\mathcal{L}$; more precisely, by description, we mean necessary and sufficient conditions under which a given integer is in $\mathcal{L}$. From now on, we always use the letters p and q to denote distinct odd prime numbers, while η and ν will always denote positive integers.

Lemma 3.1. *Let β be an odd positive integer, and let ω be the arithmetic function given by (1.11). Then,*

$$s(\beta) = \varphi(\beta)/2 \Longrightarrow \omega(\beta) = 1 \text{ or } 2.$$

Proof. 1. Let the decomposition of β into irreducible factors be

$$\beta = q_1^{k_1} q_2^{k_2} \cdots q_\ell^{k_\ell},$$

with $\ell = \omega(\beta)$. Since $\varphi(q_1^{k_1}), \varphi(q_2^{k_2}), \cdots, \varphi(q_\ell^{k_\ell})$ are even, one can consider the integer Q_i given by

$$Q_i = \prod_{\substack{j=1 \\ j \neq i}}^{\ell} \frac{\varphi(q_j^{k_j})}{2},\ 1 \leq i \leq \ell.$$

By Euler's theorem we have for all i, $1 \leq i \leq \ell$,

$$2^{\frac{\varphi(\beta)}{2^{\ell-1}}} = \left(2^{\varphi(q_i^{k_i})}\right)^{Q_i} \equiv 1 \pmod{q_i^{k_i}}.$$

Together with the fact that the modulus are relatively prime, these congruences imply that

$$2^{\frac{\varphi(\beta)}{2^{\ell-1}}} \equiv 1 \pmod{\beta},$$

which means that

$$s(\beta) \leq \frac{\varphi(\beta)}{2^{\ell-1}}. \tag{3.1}$$

Finally, by taking $s(\beta) = \varphi(\beta)/2$ in (3.1) it follows that $\ell = \omega(\beta) \leq 2$, as desired. $\square$

Lemma 3.2. *Let $u \geq 3$ and $v \geq 3$ be relatively prime odd integers.*

1) *If $s(uv) = \varphi(uv)/2$ then $\gcd(s(u), s(v)) = 1$ or 2.*

2) *If $\gcd(s(u), s(v)) = 1$ then*

$$s(uv) = \varphi(uv)/2 \Longleftrightarrow \begin{cases} s(u) = \varphi(u) \quad \textit{and } s(v) = \varphi(v)/2 \\ \textit{or} \\ s(u) = \varphi(u)/2 \quad \textit{and } s(v) = \varphi(v) \end{cases}$$

3) *If $\gcd(s(u), s(v)) = 2$ then*

$$s(uv) = \varphi(uv)/2 \Longleftrightarrow s(u) = \varphi(u) \quad \textit{and } s(v) = \varphi(v).$$

Proof. Using the fact that $\gcd(u, v) = 1$, it follows that $s(uv)$ is the lcm of $s(u)$ and $s(v)$, so that one can write

$$s(uv) = \frac{s(u)s(v)}{\gcd(s(u), s(v))}. \tag{3.2}$$

But $\gcd(u, v) = 1$, φ is multiplicative and $s(uv) = \varphi(uv)/2$, whence

$$\frac{\varphi(u)\varphi(v)}{2} = \frac{\varphi(uv)}{2} = s(uv) = \frac{s(u)s(v)}{\gcd(s(u), s(v))}$$

and

$$\frac{\varphi(u)}{s(u)} \frac{\varphi(v)}{s(v)} = \frac{2}{\gcd(s(u), s(v))}.$$

As $s(u)$ divides $\varphi(u)$ and $s(v)$ divides $\varphi(v)$, the product of the two integers $\varphi(u)/s(u)$ and $\varphi(v)/s(v)$ must be ≥ 1. The only possibility is that $\varphi(u)/s(u)$ and $\varphi(v)/s(v)$ are both equal to 1, which proves 3) or one of them is equal to 2 and the other one is equal to 1 which proves 2). $\square$

Thanks to Lemma 3.1, the set $\mathcal{L}$ can be rewritten as follows

$$\mathcal{L} = \{pq \text{ such that } s(pq) = (p-1)(q-1)/2\}. \tag{3.3}$$

Let us associate to the couple (p, q) the integer $\vartheta(p, q)$ defined by

$$\vartheta(p, q) = \gcd(s(p), s(q)).$$

Let us define the sets $\mathcal{P}_1$ and $\mathcal{P}_2$ containing odd primes with the restrictions:

$$\mathcal{P}_1 : s(p) = p - 1 \tag{3.4}$$

$$\mathcal{P}_2 : s(p) = (p-1)/2; \tag{3.5}$$

the first elements (up to 100) of $\mathcal{P}_1$ are: $3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83$ while those of $\mathcal{P}_2$ are: $7, 17, 23, 41, 47, 71, 79, 97$. Thanks to Euler's criterion, 2 is a square modulo $p \in \mathcal{P}_2$ but not a square modulo $p \in \mathcal{P}_1$.

Theorem 3.1.

$$pq \in \mathcal{L} \Longleftrightarrow \begin{cases} p \in \mathcal{P}_1,\ q \in \mathcal{P}_1 & \textit{and } \vartheta(p, q) = 2 \\ \textit{or} & \\ ((p \in \mathcal{P}_1,\ q \in \mathcal{P}_2)\ \textit{or } (p \in \mathcal{P}_2,\ q \in \mathcal{P}_1)) & \textit{and } \vartheta(p, q) = 1. \end{cases} \tag{3.6}$$

Proof. The proof is an immediate consequence of (3.3) and Lemma 3.2. □

We now change focus somewhat and take up the study of the sets $\mathcal{A}(P)$ (cf. (1.1)), when P is irreducible in $\mathbb{F}_2[z]$ of order an odd positive integer β such that $s(\beta) = \varphi(\beta)/2$. More particularly, we aim asserting that we shall restrict the determination of $\mathcal{A}(P)^{<m>}$ (the set of the elements of $\mathcal{A}(P)$ of the form $2^k m$) to the more interesting situation, that where β is square-free. Before going further, it is worth noting that there exist exactly 2 different irreducible polynomials in $\mathbb{F}_2[z]$ of order β.

Lemma 3.3. *Let $n \geq 3$ be an odd positive integer, s the function defined in (1.12), and let p be such that $p \mid n$. Then for all $k \geq 0$,*

$$s(p^k n) \mid p^k s(n). \tag{3.7}$$

Proof. When $k = 0$, the stated conclusion obviously holds, whereas when $k = 1$ then from (1.12), we may write $2^{s(n)} = 1 + gn$, for some positive integer g. Raising to the pth power, we obtain

$$\begin{aligned} 2^{ps(n)} &= (1+gn)^p = 1 + \binom{p}{1}(gn) + \binom{p}{2}(gn)^2 + \cdots + \binom{p}{p-1}(gn)^{p-1} + (gn)^p \\ &\equiv 1 + \binom{p}{1}(gn) \pmod{n^2}. \end{aligned}$$

But $pn \mid n^2$ and $p \mid \binom{p}{1}$; therefore the last congruence becomes

$$2^{ps(n)} \equiv 1 \pmod{pn},$$

which means that $s(pn) \mid ps(n)$. Next, by induction on k, we show that $2^{p^k s(n)} = 1 + g_k p^k n$ for some integer g_k. □

.

Lemma 3.4. *Let β be an odd positive integer such that $s(\beta) = \varphi(\beta)/2$. Then*

(i) $s(\widetilde{\beta}) = \varphi(\widetilde{\beta})/2$.

(ii) If $p^2 \mid \beta$ *then* $s(p\widetilde{\beta}) = \varphi(p\widetilde{\beta})/2$.

Proof. We assume that $s(\beta) = \varphi(\beta)/2$ and recall that from Lemma 3.1, one have $\omega(\beta) = 1$ or 2. We treat the case $\omega(\beta) = 2$; that is, $\beta = p^\eta q^\nu$ (the proof of the case $\omega(\beta) = 1$ is quite analogous).
(i) It follows from Lemma 3.3 and (3.1) that

$$\frac{\varphi(p^\eta q^\nu)}{2} = s(p^\eta q^\nu) \leq p^{\eta-1}q^{\nu-1}s(pq) \leq p^{\eta-1}q^{\nu-1}\frac{\varphi(pq)}{2} = \frac{\varphi(p^\eta q^\nu)}{2}$$

whence $s(pq) = \frac{\varphi(pq)}{2}$ as claimed.
(ii) If $p^2 \mid \beta$ then $\eta \geq 2$, which as in (i), gives

$$\frac{\varphi(p^\eta q^\nu)}{2} = s(p^\eta q^\nu) \leq p^{\eta-2}q^{\nu-1}s(p^2 q) \leq p^{\eta-2}q^{\nu-1}\frac{\varphi(p^2 q)}{2} = \frac{\varphi(p^\eta q^\nu)}{2}$$

whence $s(p^2 q) = \frac{\varphi(p^2 q)}{2}$ as claimed. □

Lemma 3.5. *([10, Theorem 3.35]) Let $R_1(z), R_2(z), \ldots, R_N(z)$ be all the distinct irreducible polynomials in $\mathbb{F}_2[z]$ of degree u and order e, and let $t \geq 2$ be an integer whose prime factors divide e but not $(2^u - 1)/e$. Then $R_1(z^t), R_2(z^t), \ldots, R_N(z^t)$ are all the distinct monic irreducible polynomials in $\mathbb{F}_2[z]$ of degree ut and order et.*

Corollary 3.1. *Let β be an odd positive integer such that $s(\beta) = \varphi(\beta)/2$ and let $\widetilde{P}(z)$ and $\widetilde{Q}(z)$ be all the distinct irreducible polynomials in $\mathbb{F}_2[z]$ of order $\widetilde{\beta}$. If $c = \beta/\widetilde{\beta}$ then $\widetilde{P}(z^c)$ and $\widetilde{Q}(z^c)$ are all the distinct irreducible polynomials in $\mathbb{F}_2[z]$ of order β.*

Proof. If $\beta = \widetilde{\beta}$, there is nothing to prove. Assume then, that $c = \beta/\widetilde{\beta} \neq 1$ and let p be a prime factor of $c = \beta/\widetilde{\beta}$. Clearly, p divides $\widetilde{\beta}$, p^2 divides β and $s(p\widetilde{\beta}) = \varphi(p\widetilde{\beta})/2$ (as seen in (ii) of Lemma 3.4). Suppose that p divides $(2^{s(\widetilde{\beta})} - 1)/\widetilde{\beta}$; that is, $2^{s(\widetilde{\beta})} \equiv 1 \pmod{p\widetilde{\beta}}$. Thus, $s(p\widetilde{\beta}) \leq s(\widetilde{\beta})$, whence $\varphi(p\widetilde{\beta})/2 = p\varphi(\widetilde{\beta})/2 \leq \varphi(\widetilde{\beta})/2$, which is impossible. For the rest of the proof, we just apply Lemma 3.5. □

Let β be an odd positive integer such that $s(\beta) = \varphi(\beta)/2$ and let $P(z)$ and $Q(z)$ be all the distinct irreducible polynomials in $\mathbb{F}_2[z]$ of order β. In agreement with the last corollary, $P(z)$ and $Q(z)$ can be arranged so that $P(z) = \widetilde{P}(z^c)$ and $Q(z) = \widetilde{Q}(z^c)$, which with (1.5), yields

$$\mathcal{A}(P) = c \cdot \mathcal{A}(\widetilde{P}) \text{ and } \mathcal{A}(Q) = c \cdot \mathcal{A}(\widetilde{Q}).$$

Therefore, the elements of $\mathcal{A}(P)$ and $\mathcal{A}(Q)$ must be multiple of c. Moreover, if $c \mid m$ then the elements of $\mathcal{A}(P)^{<m>}$ (resp. $\mathcal{A}(Q)^{<m>}$) can be deduced from those of $\mathcal{A}(\widetilde{P})^{<m/c>}$ (resp. $\mathcal{A}(\widetilde{Q})^{<m/c>}$);

$$\mathcal{A}(P)^{<m>} = c \cdot \mathcal{A}(\widetilde{P})^{<m/c>} \text{ and } \mathcal{A}(Q)^{<m>} = c \cdot \mathcal{A}(\widetilde{Q})^{<m/c>}. \tag{3.8}$$

Example: As a concrete example, we take $\beta = 45$. We have $s(\beta) = s(45) = 12 = \varphi(45)/2$, $\widetilde{\beta} = 15$ and $c = \beta/\widetilde{\beta} = 3$. The only irreducible polynomials in $\mathbb{F}_2[z]$ of order $\beta = 45$ are

$$P(z) = 1 + z^3 + z^{12} \text{ and } Q(z) = 1 + z^9 + z^{12}.$$

Here, for instance, we aim to determine the sets $\mathcal{A}(P)^{<21>}$ and $\mathcal{A}(Q)^{<21>}$. To this end, we just need to determine the sets $\mathcal{A}(\widetilde{P})^{<7>}$ and $\mathcal{A}(\widetilde{Q})^{<7>}$ with

$$\widetilde{P}(z) = 1 + z + z^4 \text{ and } \widetilde{Q}(z) = 1 + z^3 + z^4$$

Indeed, since $P(z) = \widetilde{P}(z^3)$ and $Q(z) = \widetilde{Q}(z^3)$ then, from (3.8),

$$\mathcal{A}(P)^{<21>} = 3 \cdot \mathcal{A}(\widetilde{P})^{<7>} \text{ and } \mathcal{A}(Q)^{<21>} = 3.\mathcal{A}(\widetilde{Q})^{<7>}.$$

Recalling that the sets $\mathcal{A}(\widetilde{P})^{<7>}$ and $\mathcal{A}(\widetilde{Q})^{<7>}$ are those corresponding to those given respectively by (1.8) and (1.9), we obtain

$$\mathcal{A}(P)^{<21>} = \{21, 42, 84, 168, 336, \ldots 2^{996} \times 21, 2^{998} \times 21, \ldots\}$$

and

$$\mathcal{A}(Q)^{<21>} = \{21, 672, 1344, 2688, \ldots, 2^{997} \times 21, 2^{999} \times 21, \ldots\}$$

4 Dirichlet character and Gauss sums

We begin by recalling some basic facts concerning the theory of Dirichlet characters and Gauss sums. Let $\beta \geq 3$ be an odd positive integer and let χ be a Dirichlet character mod β. Let κ be a positive divisor of β: we say that a character $\chi^\star$ mod κ induces χ if

$$\chi(n) = \begin{cases} \chi^\star(n) & \text{if } \gcd(n, \beta) = 1; \\ 0 & \text{otherwise.} \end{cases}$$

In this case κ is called an induced modulus for χ; and the smallest induced modulus κ for χ is called the conductor of χ. The Dirichlet character χ is said to be primitive mod β if it has no induced modulus $\kappa < \beta$. The following characterization of primitive Dirichlet characters will be useful (see [9, Theorem 9.4] for a more general version of this result).

Lemma 4.1. *Under the above notation, the following are equivalent:*

(1) χ *is primitive.*

(2) If $d \,|\, \beta$ *and* $d < \beta$*, then there is an integer* n *such that* $n \equiv 1 \pmod{d}$*,* $\gcd(n, \beta) = 1$ *and* $\chi(n) \neq 1$*.*

Let ζ be a β-th primitive root of unity, and let n be a positive integer. The sum

$$\tau(n, \chi) = \sum_{\nu} \chi(\nu)\zeta^{n\nu}, \tag{4.1}$$

where ν runs through a full (or reduced) system of residues modulo β, is called the Gauss sum associated with χ. It turns out that, if χ is induced by the primitive character $\chi^\star$ modulo κ then (see [9, Theorem 9.12]),

$$\begin{cases} \tau(n,\chi) = 0 & \text{if } \kappa \nmid \rho \\ \tau(n,\chi) = \overline{\chi}^\star(n/\gcd(\beta,n))\chi^\star(\rho/\kappa)\frac{\varphi(\beta)}{\varphi(\rho)}\mu(\rho/\kappa)\tau(\chi^\star) & \text{if } \kappa \mid \rho \end{cases} \tag{4.2}$$

where $\tau(\chi^\star) = \tau(1,\chi^\star)$ is the normed Gaussian sum, $\overline{\chi}^\star$ is the complex conjugate of $\chi^\star$ and

$$\rho = \rho(\beta, n) = \frac{\beta}{\gcd(\beta, n)}.$$

If χ is the principal character mod β (χ assumes the value 1 for all n coprime with β) then $\tau(n,\chi)$ reduces to the Ramanujan sum $c(n,\beta)$;

$$c(n,\beta) = \sum_{\nu} \zeta^{n\nu}, \tag{4.3}$$

where ν runs through a reduced system of residues modulo β. It is known that the Ramanujan sum satisfies Hölder's formula (see [9], p.110),

$$c(n,\beta) = \frac{\varphi(\beta)}{\varphi(\rho)}\mu(\rho), \tag{4.4}$$

which when taking $n = 1$ reduces to the Möbius function: $c(1,\beta) = \mu(\beta)$.

From now on, we assume that β is an element of $\mathcal{L}$ and recall that, in this case, $r = r(\beta) = 2$ where $r(\beta)$ is that integer defined by (1.13). From (2.4), one may write

$$(\mathbb{Z}/\beta\mathbb{Z})^\star = O_\beta(1) \cup O_\beta(y). \tag{4.5}$$

where y is a positive integer coprime with β, but does not belong to $O_\beta(1)$. Under these assumptions, one can define the map χ by

$$\begin{cases} \chi(n) = 1 & \text{if } n \in O_\beta(1) \\ \chi(n) = -1 & \text{if } n \in O_\beta(y) \\ \chi(n) = 0 & \text{if } \gcd(n,\beta) > 1. \end{cases} \tag{4.6}$$

We may easily verify that χ is indeed a quadratic Dirichlet character mod β. Moreover, the Gauss sum associated with χ (cf. (4.1)) may be written as

$$\tau(n,\chi) = \sum_{j=0}^{s-1} (\zeta^n)^{2^j} - \sum_{j=0}^{s-1} (\zeta^n)^{2^j y},$$

where $s = s(\beta) = \frac{\varphi(\beta)}{2}$. The last equality can be rewritten as

$$\tau(n,\chi) = B(n,\zeta) - B(ny,\zeta), \tag{4.7}$$

where $B(n,z)$ is the polynomial defined by (2.7). On the other hand, the Ramanujan sum $c(n,\beta)$ (cf. (4.3)) can be written as

$$c(n,\beta) = B(n,\zeta) + B(ny,\zeta). \tag{4.8}$$

The following Lemmas will be needed in the proof of Theorem 5.1.

Lemma 4.2. *Let χ be the quadratic Dirichlet character mod β defined by (4.6), and let $\chi^\star$ be the primitive Dirichlet character mod κ that induces χ. Let $\mathcal{P}_1$ and $\mathcal{P}_1$ the sets defined respectively by (3.4) and (3.5).*

1. *If $\beta = pq$ where $p \in \mathcal{P}_1$ and $q \in \mathcal{P}_1$, then*

$$\kappa = pq \text{ and } \chi^\star = \chi \tag{4.9}$$

2. *If $\beta = pq$ where $p \in \mathcal{P}_2$ and $q \in \mathcal{P}_1$, then*

$$\kappa = p \text{ and } \chi^\star(n) = \begin{cases} 1 & \text{if } n \in O_p(1) \\ -1 & \text{if } n \in O_p(y) \end{cases} \tag{4.10}$$

Proof. 1. We assume that $\beta = pq$ where $p \in \mathcal{P}_1$, $q \in \mathcal{P}_1$ and we shall prove that χ is primitive. In anticipation of a contradiction, we suppose (cf. Lemma 4.1) that there exists a positive integer $d < \beta = pq$ dividing β such for all integers n satisfying

$$n \equiv 1 \pmod{d} \text{ and } \gcd(n, pq) = 1, \tag{4.11}$$

we have $\chi(n) = 1$. For instance, let us take $d = p$ and then let $\mathcal{R}$ be the set of all residues modulo pq satisfying (4.11); that is,

$$\mathcal{R} = \{1 + kp,\ k = 0, 1, \dots, q-1 \text{ and } \gcd(1 + kp, q) = 1\}.$$

For t, $0 \le t \le p-2$, we define the set $\mathcal{R}_t$ by

$$\mathcal{R}_t = \{2^t n \bmod pq,\ n \in \mathcal{R}\}.$$

If $n \in \mathcal{R}$, we have $\chi(n) = 1$ and thus $n \in O_{pq}(1)$, which implies that $2^t n \in O_{pq}(1)$; that is,

$$\bigcup_{t=0}^{p-2} \mathcal{R}_t \subset O_{pq}(1). \tag{4.12}$$

From (2.6) and the fact that $\beta = pq \in \mathcal{L}$, it follows that $\mid O_{pq}(1) \mid = s(pq) = (p-1)(q-1)/2$, which with (4.12) yields

$$\mid \bigcup_{t=0}^{p-2} \mathcal{R}_t \mid \le (p-1)(q-1)/2. \tag{4.13}$$

We claim that for all t, $0 \le t \le p-2$, we have

$$\mid \mathcal{R}_t \mid = \mid \mathcal{R} \mid = q - 1 \text{ or } q.$$

For a fixed t ($0 \le t \le p-2$), it is clear that if n and n' are distinct elements of $\mathcal{R}$ then $2^t n$ and $2^t n'$ are incongruent modulo pq; therefore, $\mid \mathcal{R}_t \mid = \mid \mathcal{R} \mid$. Now, we shall prove that $\mid \mathcal{R} \mid = q-1$ or q; in other words at most one term of the progression $1, 1+p, \dots, 1+(q-1)p$ is divisible by q. Suppose to the contrary, that there exist two distinct integers k and k', $0 \le k < k' \le q-1$ such that the numbers $1 + kp$

and $1 + k'p$ are divisible by q. Then q divides their difference $(k' - k)p$. But p and q are distinct prime numbers, and thus $q \,|\, (k' - k)$ which is nonsense in light of the inequality $0 < k' - k < q$.

We shall now prove that the $\mathcal{R}_t$'s are pairwise disjoint. If it happened that

$$2^t n \equiv 2^{t'} n' \pmod{pq},$$

where $0 \leq t, t' \leq p-2$, $n \in \mathcal{R}$ and $n' \in \mathcal{R}$, then, by passing to a congruence modulo p, we would have

$$2^t \equiv 2^{t'} \pmod{p}.$$

Therefore, since $s(p) = p - 1$, it follows that $t \equiv t' \pmod{p-1}$ which implies that $t = t'$ (since $|t - t'| \leq p - 2$) establishing the result claimed. Consequently,

$$| \bigcup_{t=0}^{p-2} \mathcal{R}_t | = \sum_{t=0}^{p-2} | \mathcal{R}_t | = (p-1) \mid \mathcal{R} \mid \geq (p-1)(q-1),$$

which contradicts (4.13).

2. We assume that $\beta = pq$ where $p \in \mathcal{P}_2$ and $q \in \mathcal{P}_1$. According to Theorem 3.1, $\gcd((p-1)/2, q-1) = 1$, and thus $(p-1)/2$ must be odd, which implies that -1 is not a square modulo p. But, $p \in \mathcal{P}_2$, and thus 2 is square modulo p; hence 2 and -1 can not lie in a same orbit of $(\mathbb{Z}/p\mathbb{Z})^\star$. Consequently, $(\mathbb{Z}/p\mathbb{Z})^\star$ can be partitioned as follows

$$(\mathbb{Z}/p\mathbb{Z})^\star = O_p(1) \cup O_p(-1).$$

From (4.5), it follows that $-1 \notin O_\beta(1)$ which with the fact that $\gcd(-1, \beta) = 1$ yields $-1 \in O_\beta(y)$, say $y \in O_p(-1)$. Hence,

$$(\mathbb{Z}/p\mathbb{Z})^\star = O_p(1) \cup O_p(y). \tag{4.14}$$

It now follows that the Dirichlet character $\chi^\star$ mod κ with $\kappa = p$ (cf. (4.10)) is well-defined; moreover, it clearly induces the character χ given by (4.6). The proof is completed by noting that the modulus p is prime which makes $\chi^\star$ primitive. $\square$

Remark 4.1. As it can be seen in the last Lemma, $\chi^\star$ is a primitive quadratic character modulo κ; hence (cf. [8, Theorem 7, p. 392])

$$\begin{cases} \tau(\chi^\star) = \sqrt{\kappa} & \text{if } \chi^\star(-1) = 1 \\ \tau(\chi^\star) = i\sqrt{\kappa} & \text{if } \chi^\star(-1) = -1, \end{cases} \tag{4.15}$$

where $\tau(\chi^\star) = \tau(1, \chi^\star)$ is the normed Gaussian sum (cf. (4.1)) and i is the imaginary unit.

Lemma 4.3. *For a positive integer n, let $\psi(n)$ and $\phi(n)$ be the expressions defined by*

$$\psi(n) = B(n, \zeta) \text{ and } \phi(n) = B(ny, \zeta) \tag{4.16}$$

where $B(n, z)$ is the polynomial defined by (2.7) and ζ is a β-th primitive root of unity. Let χ be the quadratic Dirichlet character mod β given by (4.6), and let $\chi^\star$ be the primitive character mod κ inducing χ. With $\tau(\chi^\star) = \tau(1, \chi^\star)$ as defined by (4.1), a and b positive integers, we have

- $\beta = pq$, $p \in \mathcal{P}_1$ *and* $q \in \mathcal{P}_1$*:*

  1. $\psi(1) = \dfrac{1+\tau(\chi^\star)}{2}$ *and* $\phi(1) = \dfrac{1-\tau(\chi^\star)}{2}$
  2. *If* $b \geq 1$*, then* $\psi(q^b) = \phi(q^b) = -\dfrac{(q-1)}{2}$ *and* $\psi(pq^b) = \phi(pq^b) = \varphi(\beta)/2$
  3. *If* $a \geq 1$*, then* $\psi(p^a) = \phi(p^a) = -\dfrac{(p-1)}{2}$ *and* $\psi(p^a q) = \phi(p^a q) = \varphi(\beta)/2$

- $\beta = pq$, $p \in \mathcal{P}_2$ *and* $q \in \mathcal{P}_1$*:*

  1. $\psi(1) = \dfrac{1-\chi^\star(q)\tau(\chi^\star)}{2}$ *and* $\phi(1) = \dfrac{1+\chi^\star(q)\tau(\chi^\star)}{2}$
  2. *If* $b \geq 1$*, then*
     - $\psi(q^b) = -(q-1)\dfrac{1-\chi^\star(q^{b-1})\tau(\chi^\star)}{2}$, $\phi(q^b) = -(q-1)\dfrac{1+\chi^\star(q^{b-1})\tau(\chi^\star)}{2}$
     - $\psi(pq^b) = \phi(pq^b) = \varphi(\beta)/2$
  3. *If* $a \geq 1$*, then* $\psi(p^a) = \phi(p^a) = -\dfrac{(p-1)}{2}$ *and* $\psi(p^a q) = \phi(p^a q) = \varphi(\beta)/2.$

Proof. From (4.7) and (4.8), we obtain

$$\psi(n) + \phi(n) = c(n, \beta) \text{ and } \psi(n) - \phi(n) = \tau(n, \chi),$$

whence

$$\psi(n) = \frac{1}{2}(c(n, \beta) + \tau(n, \chi)) \text{ and } \phi(n) = \frac{1}{2}(c(n, \beta) - \tau(n, \chi)).$$

For the rest of the proof, we just have to apply (4.2) and (4.4). □

5 The minimal polynomial $G_{m,\mathcal{A}}(x)$ of $S(\mathcal{A}, m)$

Let $\mathcal{L}$ be the set defined by (1.15), and let $\beta = pq$ be an element of $\mathcal{L}$. Let $\widetilde{P}$ and $\widetilde{Q}$ be all the distinct irreducible polynomials in $\mathbb{F}_2[z]$ of order β; and let $\mathcal{A} = \mathcal{A}(\widetilde{P})$ and $\mathcal{A}' = \mathcal{A}(\widetilde{Q})$ be the even partition sets satisfying (1.1). For an odd positive integer m, we recall that $\mathcal{A}^{<m>}$ (resp. $\mathcal{A}'^{<m>}$) denotes the set of the elements of $\mathcal{A}$ (resp. $\mathcal{A}'$) of the form $2^k m$. Let $S(\mathcal{A}, m)$ and $S(\mathcal{A}', m)$ be the 2−adic integers defined by (1.6) and we recall that $G_{m,\mathcal{A}}(x)$ and $G_{m,\mathcal{A}'}(x)$ (cf. (1.7)) denote the minimal polynomials of $S(\mathcal{A}, m)$ and $S(\mathcal{A}', m)$, respectively. In this Section, for purpose of determining the sets $\mathcal{A}^{<m>}$ and $\mathcal{A}'^{<m>}$, we aim to obtain formulae for $G_{m,\mathcal{A}}(x)$ and $G_{m,\mathcal{A}'}(x)$.

Let $\mathcal{P}_1$ and $\mathcal{P}_2$ be the sets of odd primes defined by (3.4) and (3.5). In what follows, we always use the letters a and b to denote non negative integers and we take p as the prime number dividing β that may belong to $\mathcal{P}_2$. As it has already been mentioned in Section 2 (cf. (2.2)), if $m \notin \mathcal{M}_\beta$ or if $\beta^2 \mid m$ then $S(\mathcal{A}, m)$ and

$S(\mathcal{A}', m)$ vanish; in other words, $\mathcal{A}^{<m>} = \mathcal{A}'^{<m>} = \emptyset$. Thus, we may hereafter restrict our study to odd integers of the form

$$p^a q^b m \;\text{ such that } \gcd(m, pq) = 1 \text{ and } (a \leq 1 \text{ or } b \leq 1), \tag{5.1}$$

where $m \in \mathcal{M}_\beta$ (cf. Remark 2.1).

Theorem 5.1. *Let $\beta = pq \in \mathcal{L}$ defined in (1.15), $m \neq 1$ be an odd positive integer belonging to $\mathcal{M}_\beta$ such that $\gcd(m, \beta) = 1$, and let $\alpha(m)$ be the integer defined by*

$$\alpha(m) = 2^{\omega(m)-1},$$

where $\omega(m)$ is given by (1.11). We let χ, $\chi^\star$ as in Lemma 4.3, κ is the conductor of χ and we define the integer $i^\star$ by

$$i^\star = \chi^\star(-1).$$

1. $G_{1,\mathcal{A}}(x) = x^2 + x + \dfrac{1 - i^\star\kappa}{4}$ *and* $G_{m,\mathcal{A}}(x) = x^2 - \dfrac{\alpha^2(m)}{m^2} i^\star\kappa$.
2. $G_{q,\mathcal{A}}(x) = x^2 - x + \dfrac{q^2 - (q - 1 + \chi^\star(q))^{2g}\, i^\star\kappa}{4q^2}$ *and*
   $G_{qm,\mathcal{A}}(x) = x^2 - \dfrac{\alpha^2(m)\,(q - 1 + \chi^\star(q))^{2g}}{q^2m^2} i^\star\kappa$, *where $g = 0$ if $p \in \mathcal{P}_1$ and $g = 1$ if $p \in \mathcal{P}_2$.*
3. $G_{p,\mathcal{A}}(x) = x^2 - x + \dfrac{p^2 - i^\star\kappa}{4p^2}$ *and* $G_{pm,\mathcal{A}}(x) = x^2 - \dfrac{\alpha^2(m)}{p^2m^2} i^\star\kappa$.
4. $G_{pq,\mathcal{A}}(x) = x^2 + x + \dfrac{p^2q^2 - (q - 1 + \chi^\star(q))^{2g}\, i^\star\kappa}{4p^2q^2}$ *and*
   $G_{pqm,\mathcal{A}}(x) = x^2 - \dfrac{\alpha^2(m)\,(q - 1 + \chi^\star(q))^{2g}}{p^2q^2m^2} i^\star\kappa$.
5. *If $a \leq 1$, $b \geq 2$ and $p \in \mathcal{P}_1$ then $G_{p^aq^b,\mathcal{A}}(x) = x$ and $G_{p^aq^bm,\mathcal{A}}(x) = x$.*
6. *If $a \leq 1$, $b \geq 2$ and $p \in \mathcal{P}_2$ then*
   - $G_{p^aq^b,\mathcal{A}}(x) = x$ *and* $G_{p^aq^bm,\mathcal{A}}(x) = x$ *when* $\chi^\star(q) = 1$.
   - $G_{p^aq^b,\mathcal{A}}(x) = x^2 - \dfrac{(q-1)^2}{p^{2a}q^{2b}} i^\star\kappa$ *and* $G_{p^aq^bm,\mathcal{A}}(x) = x^2 - \dfrac{4\alpha^2(m)(q-1)^2}{p^{2a}q^{2b}m^2} i^\star\kappa$ *when* $\chi^\star(q) = -1$.
7. *If $a \geq 2$ and $b \leq 1$, then $G_{p^aq^b,\mathcal{A}}(x) = x$ and $G_{p^aq^bm,\mathcal{A}}(x) = x$.*

Proof. We let $m \in \mathcal{M}_\beta$ such that $\gcd(m, pq) = 1$ and we shall look for formulae for $G_{p^aq^bm,\mathcal{A}}(x)$ and $G_{p^aq^bm,\mathcal{A}'}(x)$. For this purpose, we shall make explicit the polynomial $H_{p^aq^bm}(x)$ defined by (2.3); this interest comes from the fact (cf. Section 2) that $G_{p^aq^bm,\mathcal{A}}(x)$ and $G_{p^aq^bm,\mathcal{A}'}(x)$ are irreducible factors of $H_{p^aq^bm}(x)$.

Let $D_{p^aq^bm}(z)$ be the polynomials given by (2.10), and let y be an integer defined by (4.5). From (2.12), we know that there exists a β-th primitive root of unity ζ such that

$$H_{p^aq^bm}(x) = (p^aq^bmx + D_{p^aq^bm}(\zeta))(p^aq^bmx + D_{p^aq^bm}(\zeta^y));$$

so that

$$H_{p^aq^bm}(x) = a_2x^2 + a_1x + a_0, \tag{5.2}$$

where

$$a_2 = p^{2a}q^{2b}m^2,\ a_1 = p^aq^bm\left(D_{p^aq^bm}(\zeta) + D_{p^aq^bm}(\zeta^y)\right) \text{ and } a_0 = D_{p^aq^bm}(\zeta)D_{p^aq^bm}(\zeta^y).$$

From (2.10), it follows that

$$D_{p^aq^bm}(z) = \sum_{d\,|\,\widetilde{m}} \mu(d)U_{\frac{m}{d}}(z), \tag{5.3}$$

where $U_\ell(z)$ is the polynomial given by

$$U_\ell(z) = B(p^aq^b\ell,z) - \varepsilon(a)B(p^{a-1}q^b\ell,z) - \varepsilon(b)B(p^aq^{b-1}\ell,z) + \varepsilon(a)\varepsilon(b)B(p^{a-1}q^{b-1}\ell,z),$$

where $\varepsilon(n) = 0$ or 1 according as $n = 0$ or not, and $B(n,z)$ is the polynomial defined by (2.7). But, for all d dividing $\widetilde{m}$, one easily see that $\dfrac{m}{d} \in O_\beta(1)$ or $\dfrac{m}{d} \in O_\beta(y)$, so that (5.3) becomes

$$D_{p^aq^bm}(z) = \lambda(m,1)U_1(z) + \lambda(m,y)U_y(z), \tag{5.4}$$

where $\lambda(m,n)$ is the integer given by (2.8).

In order to obtain formulae for $\lambda(m,1)$ and $\lambda(m,y)$, we first note that $\lambda(1,1) = 1$ and $\lambda(1,y) = 0$. Next, we assume that $m \neq 1$ and recall that all prime divisors of m lie in $O_\beta(y)$. By observing that the product of two elements of $O_\beta(1)$ or $O_\beta(y)$ is an element of $O_\beta(1)$ whereas the product of an element of $O_\beta(1)$ with another of $O_\beta(y)$ gives an element of $O_\beta(y)$, we obtain for $d\,|\,\widetilde{m}$

$$\frac{m}{d} \in O_\beta(1) \iff \Omega(\frac{m}{d}) \text{ is even},$$

$$\frac{m}{d} \in O_\beta(y) \iff \Omega(\frac{m}{d}) \text{ is odd},$$

where $\Omega(n)$ denotes the number of prime factors of n counted with multiplicity. Hence, from (2.8),

$$\lambda(m,1) = \sum_{\substack{d\,|\,\widetilde{m} \\ \Omega(\frac{m}{d}) \text{ is even}}} \mu(d) = \sum_{\substack{d\,|\,\widetilde{m} \\ \Omega(m)-\Omega(d) \text{ is even}}} \mu(d).$$

Since, in the last sum, d is square-free then $\Omega(d) = \omega(d)$ along with the fact that

$$\sum_{\substack{d \mid \widetilde{m} \\ \omega(d) \text{ is even}}} 1 = \sum_{\substack{d \mid \widetilde{m} \\ \omega(d) \text{ is odd}}} 1 = 2^{\omega(m)-1},$$

yields

$$\lambda(m,1) = (-1)^{\Omega(m)} 2^{\omega(m)-1} = (-1)^{\Omega(m)} \alpha(m).$$

Similarly, we obtain

$$\lambda(m,y) = -(-1)^{\Omega(m)} 2^{\omega(m)-1} = -(-1)^{\Omega(m)} \alpha(m).$$

Now, by replacing in (5.4), z first by ζ and then by ζ^y, we obtain

$$D_{p^a q^b}(\zeta) = U_1(\zeta) \text{ and } D_{p^a q^b}(\zeta^y) = U_y(\zeta)$$

and

$$D_{p^a q^b m}(\zeta) = -D_{p^a q^b m}(\zeta^y) = (-1)^{\Omega(m)} \alpha(m) \left(U_1(\zeta) - U_y(\zeta)\right), \text{ if } m \neq 1,$$

with

$$U_1(\zeta) = \psi(p^a q^b) - \varepsilon(a)\psi(p^{a-1} q^b) - \varepsilon(b)\psi(p^a q^{b-1}) + \varepsilon(a)\varepsilon(b)\psi(p^{a-1} q^{b-1})$$

and

$$U_y(\zeta) = \phi(p^a q^b) - \varepsilon(a)\phi(p^{a-1} q^b) - \varepsilon(b)\phi(p^a q^{b-1}) + \varepsilon(a)\varepsilon(b)\phi(p^{a-1} q^{b-1}),$$

where ψ and ϕ are defined by (4.16).

Lastly, the calculations leading to the expressions of the terms a_1 and a_0 are a bit long but straightforward, so it is convenient that we omit them. Without embarking on the details, we apply Lemma 4.3 to calculate $U_1(\zeta)$ and $U_y(\zeta)$, which will allow us to obtain the coefficient a_1, a_0 and make explicit the polynomial $H_{p^a q^b m}(x)$. It turns out that $H_{p^a q^b m}(x)$ is either $p^{2a} q^{2b} m^2 x^2$ (which means that $G_{p^a q^b m, \mathcal{A}}(x) = G_{p^a q^b m, \mathcal{A}'}(x) = x$) or an irreducible quadratic polynomial (which means that $G_{p^a q^b m, \mathcal{A}}(x) = G_{p^a q^b m, \mathcal{A}'}(x) = \dfrac{1}{p^{2a} q^{2b} m^2} H_{p^a q^b m}(x)$). In fact, this may be interpreted as asserting that $S(\mathcal{A}, p^a q^b m)$ and $S(\mathcal{A}', p^a q^b m)$ are conjugate. $\square$

Example: We take $\beta = 3 \times 5 = 15$. The irreducible polynomials of order $\beta = 15$ over $\mathbb{F}_2[z]$ are $\widetilde{P}(z) = 1 + z + z^4$ and $\widetilde{Q}(z) = 1 + z^3 + z^4$. Let $\mathcal{A} = \mathcal{A}(\widetilde{P})$ and $\mathcal{A}' = \mathcal{A}(\widetilde{Q})$ be the sets defined by (1.1). For $m \geq 3$, recall that the $2-$adic integer $S(\mathcal{A}, m)$ can be written as follows

$$S(\mathcal{A}, m) = \epsilon_0 + \epsilon_1 \cdot 2 + \epsilon_2 \cdot 2^2 + \epsilon_3 \cdot 2^3 + \cdots$$

where $\epsilon_k \in \{0, 1\}$. We also recall that by knowing the last expansion, one can deduce the elements of the set $\mathcal{A}^{<m>}$ since

$$2^k m \in \mathcal{A}^{<m>} \iff \epsilon_k = 1.$$

We begin by looking for the elements of the sets $\mathcal{A}^{<3^a5^b7>}$ and $\mathcal{A}'^{<3^a5^b7>}$. For that, we first have to calculate $G_{3^a5^b7,\mathcal{A}}(x)$ (for all values of a and b), and then determine its roots; namely the expansions $S(\mathcal{A},3^a5^b7)$ and $S(\mathcal{A}',3^a5^b7)$. In order to specify which root of $G_{3^a5^b7,\mathcal{A}}(x)$ corresponds to $S(\mathcal{A},3^a5^b7)$, we just need to compute the first few elements of the sets $\mathcal{A}$ and $\mathcal{A}'$.

• ($a \le 1$ and $b \ge 2$) or ($a \ge 2$ and $b \le 1$): $G_{3^a5^b7,\mathcal{A}}(x) = G_{3^a5^b7,\mathcal{A}'}(x) = x$.
$\mathcal{A}^{<3^a5^b7>} = \mathcal{A}'^{<3^a5^b7>} = \emptyset$.

• $G_{7,\mathcal{A}}(x) = x^2 + \frac{15}{49}$.
$\mathcal{A}^{<7>} = \{7, 14, 28, 56, 112, 2^{10}\times 7, 2^{11}\times 7, 2^{12}\times 7, 2^{15}\times 7, 2^{17}\times 7, 2^{18}\times 7, 2^{22}\times 7, \ldots\}$
$\mathcal{A}'^{<7>} = \{7, 224, 448, 896, 1792, 2^9\times 7, 2^{13}\times 7, 2^{14}\times 7, 2^{16}\times 7, 2^{19}\times 7, 2^{20}\times 7, \ldots\}$

• $G_{35,\mathcal{A}}(x) = x^2 + \frac{3}{245}$.
$\mathcal{A}^{<35>} = \{35, 140, 280, 1120, 8960, 2^9\times 35, 2^{10}\times 35, 2^{14}\times 35, 2^{19}\times 35, 2^{20}\times 35, \ldots\}$
$\mathcal{A}'^{<35>} = \{35, 70, 560, 2240, 4480, 2^{11}\times 35, 2^{12}\times 35, 2^{13}\times 35, 2^{15}\times 35, 2^{16}\times 35, \ldots\}$

• $G_{21,\mathcal{A}}(x) = x^2 + \frac{5}{147}$.
$\mathcal{A}^{<21>} = \{21, 42, 168, 1344, 2^8\times 21, 2^{13}\times 21, 2^{16}\times 21, 2^{17}\times 21, 2^{20}\times 21, 2^{23}\times 21, \ldots\}$
$\mathcal{A}'^{<21>} = \{21, 84, 336, 672, 2^7\times 21, 2^9\times 21, 2^{10}\times 21, 2^{11}\times 21, 2^{12}\times 21, 2^{14}\times 21, \ldots\}$

• $G_{105,\mathcal{A}}(x) = x^2 + \frac{1}{735}$.
$\mathcal{A}^{<105>} = \{105, 1680, 3360, 2^6\times 105, 2^7\times 105, 2^9\times 105, 2^{12}\times 105, 2^{15}\times 105, \ldots\}$
$\mathcal{A}'^{<105>} = \{105, 210, 420, 840, 2^8\times 105, 2^{10}\times 105, 2^{11}\times 105, 2^{13}\times 105, 2^{14}\times 105, \ldots\}$

Recall that $P(z) = \widetilde{P}(z^3) = 1 + z^3 + z^{12}$ and $Q(z) = \widetilde{Q}(z^3) = 1 + z^9 + z^{12}$ are all the distinct irreducible polynomials in $\mathbb{F}_2[z]$ of order 45. Let $\mathcal{A}(P)$ and $\mathcal{A}(Q)$ be the sets defined by (1.1). Looking for the elements of the sets $\mathcal{A}(P)^{<3^a5^b7>}$ and $\mathcal{A}(Q)^{<3^a5^b7>}$, it turns out that if $3 \nmid 3^a5^b7$ ($a = 0$) then

$$\mathcal{A}(P)^{<3^a5^b7>} = \mathcal{A}(Q)^{<3^a5^b7>} = \emptyset.$$

From (3.8), it follows that if $3 \mid 3^a5^b7$ ($a \ge 1$) then

$$\mathcal{A}(P)^{<3^a5^b7>} = 3\cdot\mathcal{A}^{<3^{a-1}5^b7>} \text{ and } \mathcal{A}(Q)^{<3^a5^b7>} = 3\cdot\mathcal{A}'^{<3^{a-1}5^b7>},$$

which can be expressed in more detail by:

• ($a \le 2$ and $b \ge 2$) or ($a \ge 3$ and $b \le 1$): $\mathcal{A}(P)^{<3^a5^b7>} = \mathcal{A}(Q)^{<3^a5^b7>} = \emptyset$

• $\mathcal{A}(P)^{<21>} = 3\cdot\mathcal{A}^{<7>}$ and $\mathcal{A}(Q)^{<21>} = 3\cdot\mathcal{A}'^{<7>}$;
$\mathcal{A}(P)^{<21>} = \{21, 42, 84, 168, 336, 2^{10}\times 21, 2^{11}\times 21, 2^{12}\times 21, 2^{15}\times 21, 2^{17}\times 21, \ldots\}$
$\mathcal{A}(Q)^{<21>} = \{21, 672, 1344, 2688, 5376, 2^9\times 21, 2^{13}\times 21, 2^{14}\times 21, 2^{16}\times 21, 2^{19}\times 21, \ldots\}$

• $\mathcal{A}(P)^{<3.5.7>} = 3\cdot\mathcal{A}^{<35>}$ and $\mathcal{A}(Q)^{<3.5.7>} = 3\cdot\mathcal{A}'^{<35>}$
$\mathcal{A}(P)^{<105>} = \{105, 420, 840, 3360, 26880, 2^9\times 105, 2^{10}\times 105, 2^{14}\times 105, 2^{19}\times 105, \ldots\}$
$\mathcal{A}(Q)^{<105>} = \{105, 210, 1680, 6720, 13440, 2^{11}\times 105, 2^{12}\times 105, 2^{13}\times 105, 2^{15}\times 105, \ldots\}$

• $\mathcal{A}(P)^{<63>} = 3\cdot\mathcal{A}^{<21>}$ and $\mathcal{A}(Q)^{<63>} = 3\cdot\mathcal{A}'^{<21>}$

$\mathcal{A}(P)^{<63>} = \{63, 126, 504, 4032, 2^8 \times 63, 2^{13} \times 63, 2^{16} \times 63, 2^{17} \times 63, 2^{20} \times 63, \ldots\}$
$\mathcal{A}(Q)^{<63>} = \{63, 252, 1008, 2016, 2^7 \times 63, 2^9 \times 63, 2^{10} \times 63, 2^{11} \times 63, 2^{12} \times 63, \ldots\}$

• $\mathcal{A}(P)^{<315>} = 3 \cdot \mathcal{A}^{<105>}$ and $\mathcal{A}(Q)^{<315>} = 3 \cdot \mathcal{A}'^{<105>}$.
$\mathcal{A}(P)^{<315>} = \{315, 5040, 10080, 2^6 \times 315, 2^7 \times 105, 2^9 \times 315, 2^{12} \times 315, 2^{15} \times 315, \ldots\}$
$\mathcal{A}(Q)^{<315>} = \{315, 630, 1260, 2520, 2^8 \times 315, 2^{10} \times 315, 2^{11} \times 315, 2^{13} \times 315, \ldots\}$.

Conclusion Let $\beta \geq 3$ be an odd positive integer and let $P(z) \in \mathbb{F}_2[z]$ be irreducible of order β. It can now be stated that the problem of determining the elements of the set $\mathcal{A}^{<m>}$ is solved for the case $s(\beta) = \varphi(\beta)/2$ and it will be interesting to envisage extending the cases $\beta = p$ a prime with $s(p) = (p-1)/3$ or $(p-1)/4$ to all β such that $s(\beta) = \varphi(\beta)/3$ or $\varphi(\beta)/4$.
In the following table we give $s(\beta)$ for all values of $\beta < 100$.

β	$s(\beta)$	35	$12 = \varphi(35)/2$	69	$22 = \varphi(69)/2$
3	$2 = \varphi(3)$	37	$36 = \varphi(37)$	71	$35 = \varphi(71)/2$
5	$4 = \varphi(5)$	39	$12 = \varphi(39)/2$	73	$9 = \varphi(73)/8$
7	$3 = \varphi(7)/2$	41	$20 = \varphi(41)/2$	75	$20 = \varphi(75)/2$
9	$6 = \varphi(9)$	43	$14 = \varphi(43)/3$	77	$30 = \varphi(77)/2$
11	$10 = \varphi(11)$	45	$12 = \varphi(45)/2$	79	$39 = \varphi(79)/2$
13	$12 = \varphi(13)$	47	$23 = \varphi(47)/2$	81	$54 = \varphi(81)$
15	$4 = \varphi(15)/2$	49	$21 = \varphi(49)/2$	83	$82 = \varphi(83)$
17	$8 = \varphi(17)/2$	51	$8 = \varphi(51)/4$	85	$8 = \varphi(85)/8$
19	$18 = \varphi(19)$	53	$52 = \varphi(53)$	87	$28 = \varphi(87)/2$
21	$6 = \varphi(21)/2$	55	$20 = \varphi(55)/2$	89	$11 = \varphi(89)/8$
23	$11 = \varphi(23)/2$	57	$18 = \varphi(57)/2$	91	$12 = \varphi(91)/6$
25	$20 = \varphi(25)$	59	$58 = \varphi(59)$	93	$10 = \varphi(93)/6$
27	$18 = \varphi(27)$	61	$60 = \varphi(61)$	95	$36 = \varphi(95)/2$
29	$28 = \varphi(29)$	63	$6 = \varphi(63)/6$	97	$48 = \varphi(97)/2$
31	$5 = \varphi(31)/6$	65	$12 = \varphi(65)/4$	99	$30 = \varphi(99)/2$
33	$10 = \varphi(33)/2$	67	$66 = \varphi(67)$		

The values of $\beta < 100$ for which the problem of determining the elements of the set $\mathcal{A}^{<m>}$ is solved by Theorem 5.1 are

$$\beta = 15, 21, 33, 35, 39, 45, 55, 57, 69, 75, 77, 87, 95, 99.$$

On the other hand the values of $\beta < 100$ for which the problem remains unresolved are

$$\beta = 51, 63, 65, 73, 85, 89, 91, 93;$$

it should be noted that the case $\beta = 31$ has been treated in [7].

References

[1] N. Baccar, Sets with even partition function and 2-adic integers, Periodica Math. Hungar 55 (2) (2007), 177-193.

[2] N. Baccar, On the elements of sets with even partition function, Ramanujan J 38 (2015), 561-577.

[3] N. Baccar, Sets with even partition function and cyclotomic numbers, Journal of the Australian Mathematical Society 100 (2016), 289-302.

[4] N. Baccar and A. Zekraoui, Sets with even partition function and 2-adic integers II, Journal of Integer Sequences 13 (2010), Article 10.1.3.

[5] N. Baccar and F. Ben Saïd, On sets such that the partition function is even from a certain point on, International Journal of Number Theory 5 (3) (2009), 1-22.

[6] N. Baccar, F. Ben Saïd and A. Zekraoui, On the divisor function of sets with even partition functions, Acta Math. Hungar 112 (1-2) (2006), 25-37.

[7] F. Ben Saïd, J.-L. Nicolas and A. Zekraoui, On the parity of generalised partition function III, Journal de Th´eorie des Nombres de Bordeaux 22 (2010), 51-78

[8] Z. I. Borevitch and I. R. Chafarevitch, Théorie des Nombres (Gauthiers-Villars, Paris, 1967).

[9] H. L. Montgomery and R. C. Vaughan, Multiplicative Number Theory I. Classical Theory, Cambridge University Press 2006.

[10] R. Lidl and H. Niederreiter, Introduction to Finite Fields and their Applications, Cambridge University Press, (1986).

[11] J.-L. Nicolas and A. Sárközy, On the parity of partition functions, Illinois J. Math. 39 (1995), 586-597.

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

[13] J.-L. Nicolas, A. Sárközy,On the parity of generalized partition functions, in: Proceedings of the Millennium Conference, Urbana, IL, May 2000.