J. Aust. Math. Soc. **100** (2016), 289–302
doi:10.1017/S1446788715000439

SETS WITH EVEN PARTITION FUNCTIONS AND CYCLOTOMIC NUMBERS

N. BACCAR

(Received 14 April 2015; accepted 4 August 2015; first published online 14 March 2016)

Communicated by I. E. Shparlinski

Abstract

Let $P \in \mathbb{F}_2[z]$ be such that $P(0) = 1$ and degree $(P) \geq 1$. Nicolas *et al.* ['On the parity of additive representation functions', *J. Number Theory* **73** (1998), 292–317] proved that there exists a unique subset $\mathcal{A} = \mathcal{A}(P)$ of $\mathbb{N}$ such that $\sum_{n\geq 0} p(\mathcal{A}, n)z^n \equiv P(z) \bmod 2$, where $p(\mathcal{A}, n)$ is the number of partitions of n with parts in $\mathcal{A}$. Let m be an odd positive integer and let $\chi(\mathcal{A}, .)$ be the characteristic function of the set $\mathcal{A}$. Finding the elements of the set $\mathcal{A}$ of the form $2^k m$, $k \geq 0$, is closely related to the 2-adic integer $S(\mathcal{A}, m) = \chi(\mathcal{A}, m) + 2\chi(\mathcal{A}, 2m) + 4\chi(\mathcal{A}, 4m) + \cdots = \sum_{k=0}^{\infty} 2^k \chi(\mathcal{A}, 2^k m)$, which has been shown to be an algebraic number. Let G_m be the minimal polynomial of $S(\mathcal{A}, m)$. In precedent works there were treated the case P irreducible of odd prime order p. In this setting, taking $p = 1 + ef$, where f is the order of 2 modulo p, explicit determinations of the coefficients of G_m have been made for $e = 2$ and 3. In this paper, we treat the case $e = 4$ and use the cyclotomic numbers to make explicit G_m.

2010 *Mathematics subject classification*: primary 11P83; secondary 11B50, 11D88, 12F10.

Keywords and phrases: partitions, periodic sequences, order of a polynomial, cyclotomic polynomials, resultant, 2-adic integers, cyclotomic numbers, Gaussian periods.

1. Introduction

Let $\mathbb{N}$ and $\mathbb{Q}$ denote the sets of the integers and the rational numbers, respectively. For $\mathcal{A} = \{a_1 < a_2 < \cdots\}$ a nonempty subset of positive integers and for $n \in \mathbb{N}$, $p(\mathcal{A}, n)$ denotes the number of partitions of n into parts from $\mathcal{A}$; that is, the number of solutions of the diophantine equation

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

in nonnegative integers $x_1, \ x_2, \ldots.$

We set $p(\mathcal{A}, 0) = 1$ and let $F_{\mathcal{A}}$ denote the generating series of $p(\mathcal{A}, n)$, which is known to equal the following product:

$$F_{\mathcal{A}}(z) = \prod_{a\in\mathcal{A}} \frac{1}{1 - z^a}.$$

The set $\mathcal{A}$ is called an even partition set if the sequence $(p(\mathcal{A}, n))_{n\geq 0}$ is even from a certain point on.

Let N be a positive integer and let $\mathbb{F}_2$ be the field with two elements. In [10], Nicolas *et al.* proved that there exist 2^{N-1} even partition sets $\mathcal{A}$ such that $p(\mathcal{A}, N)$ is odd and $p(\mathcal{A}, n)$ is even for all $n \geq N+1$. More precisely, for each of these sets there exists a unique polynomial $P(z) = P_{\mathcal{A}}(z) \in \mathbb{F}_2[z]$ of degree N satisfying

$$F_{\mathcal{A}}(z) \equiv P(z) \bmod 2. \tag{1.1}$$

We shall also denote the set $\mathcal{A}$ by $\mathcal{A}(P)$. As an example, take $P(z) = 1 + z^q$; then $\mathcal{A}(P) = \{q, 2q, 4q, \ldots\}$, since

$$1 + z^q \equiv \prod_{j\geq 0} \frac{1}{1 - z^{2^j q}} \bmod 2.$$

Let $\mathcal{A}$ be an even partition set and let m be an odd positive integer. To get a complete description of the elements of the set $\mathcal{A}$ of the form $2^k m$, it is convenient to consider the 2-adic integer $S(\mathcal{A}, m)$ defined by

$$S(\mathcal{A}, m) = \chi(\mathcal{A}, m) + 2\chi(\mathcal{A}, 2m) + 4\chi(\mathcal{A}, 4m) + \cdots = \sum_{k=0}^{\infty} 2^k \chi(\mathcal{A}, 2^k m), \tag{1.2}$$

where $\chi(\mathcal{A}, d)$ is the characteristic function of the set $\mathcal{A}$,

$$\chi(\mathcal{A}, d) = \begin{cases} 1 & \text{if } d \in \mathcal{A}, \\ 0 & \text{otherwise.} \end{cases}$$

In [2] (see also [1]), it is proved that $S(\mathcal{A}, m)$ is an algebraic number. Moreover, if P and Q are two polynomials of $\mathbb{F}_2[z]$, we have (cf. [2, Section 3.2])

$$S(\mathcal{A}(PQ), m) = S(\mathcal{A}(P), m) + S(\mathcal{A}(Q), m),$$

which implies that

$$\begin{aligned} S(\mathcal{A}(P^{2^t}), m) &= \chi(\mathcal{A}(P^{2^t}), m) + 2\chi(\mathcal{A}(P^{2^t}), 2m) + 4\chi(\mathcal{A}(P^{2^t}), 4m) + \cdots \\ &= 2^t\chi(\mathcal{A}(P), m) + 2^{t+1}\chi(\mathcal{A}(P), 2m) + 2^{t+2}\chi(\mathcal{A}(P), 4m) + \cdots. \end{aligned}$$

This means that

$$\mathcal{A}(P^{2^t}) = 2^t \cdot \mathcal{A}(P) := \{2^t n,\ n \in \mathcal{A}(P)\}.$$

This formula follows easily from (1.1).

Let p be an odd prime and let f be the order of 2 modulo p; that is, f is the smallest positive integer such that $2^f \equiv 1 \bmod p$. Hence, one can write

$$p = 1 + ef,$$

where e is a positive integer. Let $P(z) \in \mathbb{F}_2[z]$ be irreducible of order p (see [9, Definition 3.2]); that is, p is the smallest positive integer such that $P(z)$ divides $1 + z^p$ in $\mathbb{F}_2[z]$. Let G_m denote the minimal polynomial of the algebraic number $S(\mathcal{A}, m)$,

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

where $\mathcal{A} = \mathcal{A}(P)$ is the even partition set satisfying (1.1). In [1] (see also [3]), using Gauss sums, the polynomial G_m was obtained explicitly for the case $e = 2$. The case $e = 3$ was treated in [5], where the authors made explicit the polynomial G_m by using the number of points of the elliptic curve $x^3 + ay^3 = 1$ modulo p. In the present paper, we shall give explicitly the polynomial G_m in the case $e = 4$. For that, we will use cyclotomic numbers and the *Gaussian periods*.

In this paper, we first recall some properties of G_m. Thereafter, we give some background on cyclotomic numbers and Gaussian periods. Finally, we shall give our main result.

2. Properties of the polynomial G_m

Throughout this paper, we assume that p is an odd prime and g is a primitive root mod p. Let f be the order of 2 modulo p and write $p = 1 + ef$, where e is a positive integer. Then the cyclotomic classes of degree e and conductor p are given by

$$C_i^{(g)} = \{g^{i+ej} \bmod p,\ j = 0, \ldots, f-1\}, \quad i = 0, \ldots, e-1.$$

Such classes are defined as parts of $(\mathbb{Z}/p\mathbb{Z})^*$; however, by extension, they are also considered as parts of $\mathbb{N}$. Moreover, we can extend the definition of the $C_i^{(g)}$ to all values of $i \in \mathbb{Z}$ by

$$C_i^{(g)} = C_{i \bmod e}^{(g)}.$$

For $i \in \{0, 1, 2, \ldots, e-1\}$, we denote by $\omega_i(n)$ the arithmetic function which counts the number of distinct prime divisors of n belonging to $C_i^{(g)}$; that is,

$$\omega_i(n) = \sum_{\substack{q \text{ prime},\ q \mid n \\ q \in C_i^{(g)}}} 1. \tag{2.1}$$

Let $\mathcal{P}_0$ be the set of odd positive integers defined by

$$m \in \mathcal{P}_0 \iff \gcd(m, p) = 1 \quad \text{and} \quad \omega_0(m) = 0. \tag{2.2}$$

Let $\phi_p(z) = (1 - z^p)/(1 - z) = 1 + z + \cdots + z^{p-1}$ be the cyclotomic polynomial over $\mathbb{F}_2$ of index p. Using the elementary theory of finite fields, ϕ_p factors in $\mathbb{F}_2$ into e irreducible polynomials $P_1, P_2, \ldots, P_e$, each of degree f and of order p. For all ℓ, $1 \le \ell \le e$, let $\mathcal{A}_\ell = \mathcal{A}(P_\ell)$ be the even partition set obtained from (1.1).

A necessary condition (see [4, Theorem 1]) for an integer n to be in $\mathcal{A}_\ell$ is that

$$n = 2^k m p^c,$$

where k is a nonnegative integer, $c \in \{0, 1\}$ and $m \in \mathcal{P}_0$. From now on, we consider m to be in $\mathcal{P}_0$ and let

$$\delta = \delta(m) \tag{2.3}$$

be the unique integer in $\{0, 1, \ldots, e-1\}$ such that $m \in C_\delta^{(g)}$.

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

For all ℓ, $1 \le \ell \le e$, let $S(\mathcal{A}_\ell, m)$ be the 2-adic integer given by (1.2) and let $\mathcal{M}_m$ be the monic polynomial whose roots are the $S(\mathcal{A}_\ell, m)$:

$$\mathcal{M}_m(y) = (y - S(\mathcal{A}_1, m))(y - S(\mathcal{A}_2, m)) \cdots (y - S(\mathcal{A}_e, m)).$$

Let μ denote, as customary, the Möbius function and denote by $\widetilde{m}$ the squarefree kernel of m; that is, $\widetilde{m}$ is the product of the distinct primes dividing m. Let $R_m(y)$ be the polynomial with integer coefficients defined by the resultant,

$$R_m(y) = res_z\Big(\phi_p(z), my + \sum_{h=0}^{e-1} \alpha_h \sum_{j=0}^{f-1} z^{(2^j g^{(\delta-h)} \bmod e) \bmod p}\Big),$$

where, for all h, $0 \le h \le e-1$,

$$\alpha_h = \alpha_h(m) = \sum_{d \mid \widetilde{m}, d \in C_h^{(g)}} \mu(d). \tag{2.4}$$

In [1], it is proved that

$$R_m(y) = m^{p-1} \prod_{\ell=1}^{e} (y - S(\mathcal{A}_\ell, m))^f,$$

which means that

$$\mathcal{M}_m(y) = \frac{1}{m^e}(R_m(y))^{1/f} \in \mathbb{Q}[y].$$

Let G_m be the minimal polynomial of the algebraic number $S(\mathcal{A}_e, m)$. In fact, $\mathcal{M}_m$ is a multiple of the polynomial G_m and the $S(\mathcal{A}_\ell, m)$ could be conjugates.

Let ζ be a pth root of unity and define the *periods* η_i by

$$\eta_i = \sum_{u \in C_i^{(g)}} \zeta^u; \quad i \in \mathbb{Z}. \tag{2.5}$$

Since for all $i \in \mathbb{Z}$, $\eta_{i+e} = \eta_i$, one can consider the η_i to be indexed with $\mathbb{Z}/e\mathbb{Z}$. Here, $\eta_0, \eta_1, \ldots, \eta_{e-1}$ are the so-called Gaussian periods of degree e in the algebraic number fields $\mathbb{Q}(\zeta)$; they are known to be Galois conjugates and the *period polynomial*

$$F_e(y) = (y - \eta_0)(y - \eta_1) \cdots (y - \eta_{e-1}) \tag{2.6}$$

is their common minimal polynomial over $\mathbb{Q}$. One can also note (see [12]) that $\mathbb{Q}(\eta_0)$ is the unique subfield of $\mathbb{Q}(\zeta)$ of degree e over $\mathbb{Q}$ and the set $\{\eta_0, \eta_1, \ldots, \eta_{e-1}\}$ is an integral basis of $\mathbb{Q}(\eta_0)$.

For $i \in \{0, 1, \ldots, e-1\}$, we define $\theta_i = \theta_i(m)$ as follows:

$$\theta_i = \sum_{h=0}^{e-1} \alpha_h \eta_{\delta-h+i}, \tag{2.7}$$

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

where α_h has been defined in (2.4) and $\delta = \delta(m)$ in (2.3). In [1, formula (3.32)], it is shown that for all ℓ, $0 \le \ell \le e-1$, there exists some $i_\ell \in \{0, 1, \dots, e-1\}$ such that

$$mS(\mathcal{A}_\ell, m) = -\theta_{i_\ell}.$$

Moreover, it turns out that

$$\mathcal{M}_m(y) = \frac{1}{m^e}(my + \theta_0)(my + \theta_1)\cdots(my + \theta_{e-1}). \tag{2.8}$$

On the other hand, also in [1, page 188], it is shown that the elements of the form $2^k pm$ of the sets $\mathcal{A}_\ell$ are given by the 2-adic expansion of the roots of the polynomial $R_m(-py - \epsilon f)$, where $\epsilon = 1$ if $m = 1$, else $\epsilon = 0$. More precisely,

$$(y - S(\mathcal{A}_1, pm))(y - S(\mathcal{A}_2, pm))\cdots(y - S(\mathcal{A}_e, pm)) = \frac{1}{(-p)^e}\mathcal{M}_m(-py - \epsilon f).$$

In the cases $e = 2$ (see [1] or [3]) and $e = 3$ (see [5]), it turns out that $\mathcal{M}_m = G_m$. Moreover, we have the following explicit formulas:

$e = 2$ [1, formula (4.5)]:

$$G_1(y) = y^2 - y + \frac{1 - (-1)^f p}{4}$$

and, for $m \ge 3$,

$$G_m(y) = y^2 - \frac{(-1)^f 2^{2\omega_1 - 2} p}{m^2}. \tag{2.9}$$

$e = 3$ [5, Theorems 7 and 11]:

$$G_1(y) = y^3 - y^2 - fy + \frac{p(L+3) - 1}{27}$$

and, for $m \ge 3$,

$$G_m(y) = y^3 - \frac{\frac{3}{4}pu^2}{m^2}y + \frac{v}{m^3}, \tag{2.10}$$

with $u = u(m) = 2.3^{((\omega_1+\omega_2)/2)-1}$ and

$$v = v(m) = \begin{cases} \frac{1}{8}(-1)^{(\omega_2-\omega_1)/2} pu^3 L & \text{if } \omega_2 - \omega_1 \text{ is even,} \\ \frac{3\sqrt{3}}{8}(-1)^{(\omega_2-\omega_1-1)/2} pu^3 M & \text{if } \omega_2 - \omega_1 \text{ is odd,} \end{cases}$$

where L and M are the unique integers satisfying $4p = L^2 + 27M^2$, $L \equiv 1 \bmod 3$ and $(L + 9M)/(L - 9M) \equiv (g^2)^{(p-1)/3} \bmod p$.

3. Some results on cyclotomic numbers and Gaussian periods

Let p be an odd prime and let e and f be positive integers such that $p = 1 + ef$. Let g be a primitive root modulo p. Gauss introduced (see [6]) the cyclotomic numbers of order e given by

$$(i, j)_e = \#\{u \in (\mathbb{Z}/p\mathbb{Z})^*, u \in C_i^{(g)} \text{ and } 1 + u \in C_j^{(g)}\}, \quad 0 \le i, j \le e-1.$$

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

For $i, j \in \mathbb{Z}$, define $(i, j)_e$ by

$$(i, j)_e = (i \bmod e, j \bmod e)_e.$$

We start by listing some properties of the cyclotomic numbers (see [12]). For all $i, j \in \mathbb{Z}$,

$$\begin{aligned}
&(i, j)_e = \begin{cases} (j, i)_e & \text{if } f \text{ is even,} \\ (j + \frac{1}{2}e, i + \frac{1}{2}e)_e & \text{if } f \text{ is odd,} \end{cases} \\
&(i, j)_e = (-i, j - i)_e, \\
&\sum_{k=0}^{e-1} (i, k)_e = f - \delta_{i,s},
\end{aligned} \tag{3.1}$$

and

$$\sum_{k=0}^{e-1} (k, j)_e = f - \delta_{0,j},$$

where δ is Kronecker's delta and $s := s(f) = 0$ or $e/2$ according as f is even or odd.

Let $\eta_0, \eta_1, \ldots, \eta_{e-1}$ be the Gaussian periods of degree e as defined in (2.5) and let F_e (cf. (2.6)) be their common minimal polynomial. It is well known that determining the coefficients of the polynomial F_e is intimately connected to the cyclotomic numbers of order e. Here is a property that characterizes Gaussian periods and cyclotomic numbers (see [6, formula (7)]):

$$\eta_i \eta_{i+k} = \sum_{h=0}^{e-1} (k, h)_e \eta_{i+h} + f \delta_{k,s}. \tag{3.2}$$

In the sequel, we need the following lemma.

Lemma 3.1. *For $i, j, k \in \mathbb{Z}$, let $\Theta_{i,j,k}$ be the quantity defined by*

$$\Theta_{i,j,k} = \sum_{\ell=0}^{e-1} \eta_\ell \eta_{\ell+i} \eta_{\ell+j} \eta_{\ell+k}.$$

Then

$$\Theta_{i,j,k} = \begin{cases} pf\delta_{k,s}\delta_{j-i,s} - f^3 + p \displaystyle\sum_{h=0}^{e-1} (k, h)_e (i - h, j - h)_e & \text{if } f \text{ is even,} \\ pf\delta_{k,s}\delta_{j-i,s} - f^3 + p \displaystyle\sum_{h=0}^{e-1} (k, h)_e (i - h, j - h + \tfrac{1}{2}e)_e & \text{if } f \text{ is odd.} \end{cases} \tag{3.3}$$

Proof. For $k, k' \in \mathbb{Z}$, we define Δ_k and $\Omega_{k,k'}$ as follows:

$$\Delta_k = \sum_{i=0}^{e-1} \eta_i \eta_{i+k} \tag{3.4}$$

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

and

$$\Omega_{k,k'} = \sum_{i=0}^{e-1} \eta_i \eta_{i+k} \eta_{i+k'}. \tag{3.5}$$

Hence (cf. [6, formula (20)]),

$$\Delta_k = p\delta_{k,s} - f \tag{3.6}$$

and (cf. [12, formula (15)])

$$\Omega_{k,k'} = \begin{cases} -f^2 + (k,k')_e p & \text{if } f \text{ is even,} \\ -f^2 + (k, k' + \frac{1}{2}e)_e p & \text{if } f \text{ is odd.} \end{cases} \tag{3.7}$$

In view of the fact that $\eta_d = \eta_{d \bmod e}$, it is clear that for all $u \in \mathbb{Z}$, $\sum_{i=u}^{u+e-1} \eta_i \eta_{i+k} \eta_{i+k'} = \sum_{i=0}^{e-1} \eta_i \eta_{i+k} \eta_{i+k'}$. Consequently,

$$\Omega_{k,k'} = \sum_{i=0}^{e-1} \eta_i \eta_{i-k} \eta_{i+k'-k} = \Omega_{-k,k'-k}. \tag{3.8}$$

For $v, k, k' \in \mathbb{Z}$, let $E_{v,k}$ and $H_{v,k,k'}$ be the quantities defined by

$$E_{v,k} = \sum_{i=0}^{e-1} \eta_{i+v} \eta_{i+k},$$

$$H_{v,k,k'} = \sum_{i=0}^{e-1} \eta_{i+v} \eta_{i+k} \eta_{i+k'}.$$

Arguing as in (3.8),

$$E_{v,k} = \Delta_{k-v}$$

and

$$H_{v,k,k'} = \Omega_{k-v,k'-v}.$$

Using (3.2),

$$\begin{aligned} \Theta_{i,j,k} &= \sum_{\ell=0}^{e-1} \eta_{\ell+i} \eta_{\ell+j} \Big(\sum_{h=0}^{e-1} (k,h)_e \eta_{\ell+h} + f\delta_{k,s} \Big) \\ &= \sum_{h=0}^{e-1} (k,h)_e H_{h,i,j} + f\delta_{k,s} E_{i,j} \\ &= \sum_{h=0}^{e-1} (k,h)_e \Omega_{i-h,j-h} + f\delta_{k,s} \Delta_{j-i}. \end{aligned}$$

Thus, to obtain (3.3), one just uses (3.7), (3.6) and (3.1). □

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

4. Computation of the polynomial $G_m(y)$ in the case $e = 4$

Let p be an odd prime, let f be the order of 2 modulo p and write $p = 1 + ef$, where e is a positive integer. Let $P_1, P_2, \ldots, P_e$ be all irreducible polynomials of order p and degree f over $\mathbb{F}_2$. For all ℓ, $1 \le \ell \le e$, let $\mathcal{A}_\ell$ be the even partition set satisfying (1.1) and $S(\mathcal{A}_\ell, m)$ be the 2-adic integer defined by (1.2). Recall that G_m (cf. Section 2) denotes the minimal polynomial of $S(\mathcal{A}_e, m)$. As will be seen, one of the key tools to get our main result is the classical theory of cyclotomy. In particular, one can wish to look at a special application of this theory with the intention of finding explicit formulas of the polynomial $G_m(y)$ for different values of e. Indeed, from (2.5)–(2.7) and (2.8), it is clear that

$$G_1(y) = (-1)^e F_e(-y).$$

For $m \ge 3$, as was already mentioned in (2.9) and (2.10), a formula was found for the polynomial $G_m(y)$ in the cases $e = 2$ and $e = 3$. In what follows, we assume that the prime p is such that $e = 4$ (for example, $p = 113, 281, 353, 577, 593, 617, 1033, \ldots$) and construct the polynomial $G_m(y)$. For that, we use cyclotomic numbers of order 4 and Gaussian periods.

Hence, by using the formula of $F_4(y)$ obtained by Gauss (see [8]),

$$G_1(y) = y^4 - y^3 - \tfrac{1}{8}(3p-3)y^2 - \tfrac{1}{16}[(2a-3)p+1]y + \tfrac{1}{256}[p^2 - (4a^2 - 8a + 6)p + 1],$$

where a is the unique integer such that

$$p = a^2 + 4b^2, \quad a \equiv 1 \bmod 4.$$

The last conditions determine a uniquely, and b up to sign. Note that the ambiguity of the sign b is solved in [7, Theorem 2] by

$$g^{(p-1)/4} \equiv \frac{a}{2b} \bmod p.$$

Let g be a primitive root modulo p and recall that

$$(\mathbb{Z}/p\mathbb{Z})^* = C_0^{(g)} \cup C_1^{(g)} \cup C_2^{(g)} \cup C_3^{(g)},$$

where the $C_i^{(g)}$ are the cyclotomic classes of degree 4 and conductor p. By observing that the class $C_0^{(g)}$ contains all the 4th-power residues and that $f = (p-1)/4$ is the order of 2 modulo p, one can conclude that 2 belongs to $C_0^{(g)}$, which leads to the fact that 2 is square modulo p. Since 2 is a quadratic residue of primes of the form $1 + 8k$ and $7 + 8k$, it follows that f must be even.

For a positive integer n and any integer r, let us define

$$J(n, r) = \sum_{\substack{k=0 \\ k \equiv r \bmod 4}}^{n} \binom{n}{k} (-1)^k. \tag{4.1}$$

Then we can state the following result.

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

LEMME 4.1. *For n fixed, the sequence $(J(n,r))_{r\geq 0}$ is periodic with period 4. Moreover,*

$$J(n,r) = 2^{n/2-1}\cos\Big(r\frac{\pi}{2} + n\frac{\pi}{4}\Big) + (-1)^r 2^{n-2}. \tag{4.2}$$

PROOF. The statement follows from the formula (see [11, page 41])

$$\sum_{\substack{k=0 \\ k\equiv r \bmod c}}^{n} \binom{n}{k} = \frac{1}{c}\sum_{j=0}^{c-1}\Big(2\cos\Big(j\frac{\pi}{c}\Big)\Big)^n \cos\Big(j(n-2r)\frac{\pi}{c}\Big)$$

applied for $c = 4$. □

Before giving the formula of G_m, we need the following result.

COROLLARY 4.2. *Let $\mathcal{P}_0$ be the set defined by (2.2), let $m \geq 3$ be an element of $\mathcal{P}_0$ and assume that $\widetilde{m}$ has the following complete factorization:*

$$\widetilde{m} = q_{1,1}q_{1,2}\cdots q_{1,\omega_1}q_{2,1}q_{2,2}\cdots q_{2,\omega_2}q_{3,1}q_{3,2}\cdots q_{3,\omega_3}, \tag{4.3}$$

where, for i, $1 \leq i \leq 3$, $\omega_i = \omega_i(m)$ is the integer defined by (2.1) and $q_{i,j} \in C_i^{(g)}$. Let α_h be the integer given by (2.4). Then, for all h, $0 \leq h \leq 3$,

$$\alpha_h = (-1)^h\rho + \gamma\cos\Big(\frac{\lambda\pi}{4} + h\frac{\pi}{2}\Big), \tag{4.4}$$

with

$$\lambda = \lambda(m) = \omega_1 - \omega_3, \tag{4.5}$$

$$\gamma = \gamma(m) = 2^{((\omega_1+\omega_3+2\omega_2)/2)-1} \tag{4.6}$$

and

$$\rho = \rho(m) = 2^{\omega_1+\omega_3-2}\kappa(\omega_2), \tag{4.7}$$

where

$$\kappa(\omega_2) = \begin{cases} 1 & \text{if } \omega_2 = 0, \\ 0 & \text{otherwise.} \end{cases}$$

PROOF. First let us suppose that $\omega_1 \neq 0$, $\omega_2 \neq 0$ and $\omega_3 \neq 0$. From (2.4), (4.3) and (4.1),

$$\begin{aligned}\alpha_h &= \sum_{i_1=0}^{\omega_1}(-1)^{i_1}\binom{\omega_1}{i_1}\sum_{i_2=0}^{\omega_2}(-1)^{i_2}\binom{\omega_2}{i_2}\sum_{\substack{i_3=0 \\ i_1+2i_2+3i_3\equiv h \bmod 4}}^{\omega_3}(-1)^{i_3}\binom{\omega_3}{i_3} \\ &= \sum_{i_1=0}^{\omega_1}(-1)^{i_1}\binom{\omega_1}{i_1}\sum_{i_2=0}^{\omega_2}(-1)^{i_2}\binom{\omega_2}{i_2}J(\omega_3, i_1+2i_2-h). \end{aligned}\tag{4.8}$$

Denote the inner sum in (4.8) by $K(i_1,\omega_2,\omega_3,h)$. Then

$$\begin{aligned}K(i_1,\omega_2,\omega_3,h) &= \sum_{r=0}^{3}\sum_{\substack{i_2=0 \\ i_2\equiv r \bmod 4}}^{\omega_2}(-1)^{i_2}\binom{\omega_2}{i_2}J(\omega_3, i_1+2i_2-h) \\ &= \sum_{r=0}^{3} J(\omega_2, r)J(\omega_3, i_1+2r-h).\end{aligned}$$

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

Using (4.2) and after simplifications,

$$K(i_1, \omega_2, \omega_3, h) = 2^{((\omega_3+2\omega_2)/2)-1} \cos\Big((i_1 - h)\frac{\pi}{2} + \omega_3\frac{\pi}{4}\Big). \tag{4.9}$$

Since

$$\alpha_h = \sum_{i_1=0}^{\omega_1}(-1)^{i_1}\binom{\omega_1}{i_1}K(i_1, \omega_2, \omega_3, h) = \sum_{r=0}^{3} K(r, \omega_2, \omega_3, h)J(\omega_1, r),$$

arguing as above and using (4.9),

$$\alpha_h = 2^{((\omega_1+2\omega_2+\omega_3)/2)-2} \sum_{r=0}^{3} \cos\Big((r - h)\frac{\pi}{2} + \omega_3\frac{\pi}{4}\Big)\cos\Big(r\frac{\pi}{2} + \omega_1\frac{\pi}{4}\Big).$$

By transforming the cosine product in the sum, we get (4.4). This proves Lemma 4.2 when $\omega_1\omega_2\omega_3 \neq 0$. Now, when $\omega_1\omega_2\omega_3 = 0$, by following exactly the same arguments as above with suitable modifications, we obtain (4.4). □

Theorem 4.3. *Let $m \geq 3$ be an element of $\mathcal{P}_0$ and let $G_m(y)$ be the minimal polynomial of $S(\mathcal{A}_4, m)$. Let λ, ρ and γ be the quantities, respectively, defined by (4.5), (4.7) and (4.6). Then*

$$G_m(y) = \frac{1}{m^4}(m^4y^4 + m^2\nu_2y^2 + m\nu_3y + \nu_4),$$

with

$$\nu_2 = -(2\rho^2 + \gamma^2)p, \tag{4.10}$$

$$\nu_3 = \begin{cases} (-1)^{(\lambda/2)+1}2\rho\gamma^2pa & \text{if } \lambda \text{ is even,} \\ (-1)^{(\lambda-1)/2}4\rho\gamma^2pb & \text{if } \lambda \text{ is odd,} \end{cases} \tag{4.11}$$

$$\nu_4 = \begin{cases} p^2\rho^2(\rho^2 - \gamma^2) + pb^2\gamma^4 & \text{if } \lambda \text{ is even,} \\ p^2\rho^2(\rho^2 - \gamma^2) + \frac{1}{4}pa^2\gamma^4 & \text{if } \lambda \text{ is odd,} \end{cases} \tag{4.12}$$

where the integers a and b are given by

$$p = a^2 + 4b^2, \quad a \equiv 1 \bmod 4 \quad \text{and} \quad g^{(p-1)/4} \equiv \frac{a}{2b} \bmod p.$$

Moreover, $S(\mathcal{A}_1, m), S(\mathcal{A}_2, m), S(\mathcal{A}_3, m)$ and $S(\mathcal{A}_4, m)$ are the roots of the polynomial $G_m(y)$.

Proof. Recall that $\mathcal{M}_m(y)$ is the polynomial of $\mathbb{Q}[y]$ whose roots are $S(\mathcal{A}_1, m)$, $S(\mathcal{A}_2, m), S(\mathcal{A}_3, m)$ and $S(\mathcal{A}_4, m)$. We claim that $G_m(y) = \mathcal{M}_m(y)$. For that, let σ be the automorphism of $\mathbb{Q}(\eta_0)$ over $\mathbb{Q}$ given by $\sigma(\eta_i) = \eta_{i+1}$. Then σ maps θ_0 onto θ_1, θ_1 onto θ_2, θ_2 onto θ_3 and θ_3 onto θ_0, which means that the θ_i $(0 \leq i \leq 3)$ are conjugates. Furthermore, to prove that $\mathcal{M}_m(y)$ is the minimal polynomial of $S(\mathcal{A}_e, m)$, it suffices to prove that the θ_i $(0 \leq i \leq 3)$ are distinct. For that, first note that $\theta_0 \neq \theta_1$, since otherwise $\sigma(\theta_0) = \theta_0$, which is impossible because of the fact that $\theta_0 \notin \mathbb{Q}$. Now suppose that $\theta_0 = \theta_2$. Using the fact that η_0, η_1, η_2 and η_3 are linearly independent, it follows that

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

$\alpha_0 = \alpha_2$ and $\alpha_1 = \alpha_3$, which is impossible (this can be easily seen by observing the formula giving α_h (cf. (2.4))). Finally, the equality $\theta_0 = \theta_3$ is also impossible, since, by applying σ, we obtain $\theta_0 = \theta_1$.

We denote by σ_k, $1 \le k \le 4$, the elementary symmetric polynomials in four variables of degree k. Now, using (2.8), we can write

$$G_m(y) = \frac{1}{m^4}\prod_{i=0}^{3}(my+\theta_i) = \frac{1}{m^4}(m^4y^4 + m^3\nu_1y^3 + m^2\nu_2y^2 + m\nu_3y + \nu_4),$$

with

$$\nu_k = \sigma_k(\theta_0,\theta_1,\theta_2,\theta_3); \quad 1 \le k \le 4 \tag{4.13}$$

and (cf. (2.7))

$$\theta_i = \sum_{h=0}^{3}\alpha_h\eta_{\delta-h+i}; \quad 0 \le i \le 3. \tag{4.14}$$

Computation of ν_1: from (4.13) and (4.14),

$$\nu_1 = \sum_{h=0}^{3}\alpha_h\sum_{i=0}^{3}\eta_{\delta-h+i}.$$

Since $\eta_{\delta-h+i} = \eta_{\delta-h+i \bmod 4}$, it follows that for a fixed h, $\sum_{i=0}^{3}\eta_{\delta-h+i} = \sum_{i=0}^{3}\eta_i$. On the other hand from (2.4), $\sum_{h=0}^{3}\alpha_h = \sum_{d|\widetilde{m},}\mu(d)$. Hence,

$$\nu_1 = \Big(\sum_{d|\widetilde{m}}\mu(d)\Big)\Big(\sum_{i=0}^{3}\eta_i\Big) = 0,$$

since the first sum vanishes for $\widetilde{m} \ne 1$.

Computation of ν_2: using (4.14) and (4.4), expanding in (4.13) and by grouping the product of the form $\eta_i\eta_{i+k}$,

$$\nu_2 = \sum_{k=0}^{2}V_k\Delta_k,$$

where the Δ_k are defined by (3.4), $V_0 = -2\rho^2 - \gamma^2$, $V_1 = 4\rho^2$ and $V_2 = -V_0 - V_1 = -2\rho^2 + \gamma^2$. Hence, by using (3.6), we get (4.10).

Computation of ν_3: the same calculation as in ν_2 gives

$$\nu_3 = \sum_{k=0}^{3}U_k\Omega_{0,k} + U\Omega_{1,2},$$

where the $\Omega_{\ell,k}$ are defined by (3.5) and U_0, U_1, U_2, U_3, U are quantities depending solely upon the α_h, which can be simplified by (4.4) to find that

$$U_0 = \begin{cases}(-1)^{\lambda/2}2\rho\gamma^2 & \text{if } \lambda \text{ is even,}\\ 0 & \text{if } \lambda \text{ is odd,}\end{cases}$$

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

$$U_1 = \begin{cases} -(-1)^{\lambda/2} 2\rho\gamma^2 & \text{if } \lambda \text{ is even,} \\ (-1)^{(\lambda-1)/2} 4\rho\gamma^2 & \text{if } \lambda \text{ is odd,} \end{cases}$$
$$U_2 = \begin{cases} -(-1)^{\lambda/2} 2\rho\gamma^2 & \text{if } \lambda \text{ is even,} \\ 0 & \text{if } \lambda \text{ is odd,} \end{cases}$$
$$U_3 = \begin{cases} -(-1)^{\lambda/2} 2\rho\gamma^2 & \text{if } \lambda \text{ is even,} \\ -(-1)^{(\lambda-1)/2} 4\rho\gamma^2 & \text{if } \lambda \text{ is odd,} \end{cases}$$
$$U = \begin{cases} (-1)^{\lambda/2} 4\rho\gamma^2 & \text{if } \lambda \text{ is even,} \\ 0 & \text{if } \lambda \text{ is odd.} \end{cases}$$

Hence, (4.11) follows from (3.7) and the fact that for f even (cf. [6] and [7]),

$$(1,3)_4 = (2,3)_4 = (1,2)_4, \quad (1,1)_4 = (0,3)_4,$$
$$(2,2)_4 = (0,2)_4, \quad (3,3)_4 = (0,1)_4,$$
$$16(0,0)_4 = p - 11 - 6a, \quad 16(0,1)_4 = p - 3 + 2a + 8b, \quad 16(0,2)_4 = p - 3 + 2a,$$
$$16(0,3)_4 = p - 3 + 2a - 8b, \quad 16(1,2)_4 = p + 1 - 2a.$$

Computation of ν_4: doing as above, the calculation yields

$$\nu_4 = \sum_{j=0}^{2} \sum_{k=j}^{3} U_{j,k}\Theta_{0,j,k} + V\Theta_{1,2,3},$$

where the $U_{j,k}$ and V are quantities depending solely upon the α_h, which, with the use of (4.4), can be written as follows:

$$U_{0,0} = \begin{cases} \rho^4 - \rho^2\gamma^2 & \text{if } \lambda \text{ is even,} \\ \rho^4 - \rho^2\gamma^2 + \frac{1}{4}\gamma^4 & \text{if } \lambda \text{ is odd,} \end{cases}$$
$$U_{0,1} = -4\rho^4 + 2\rho^2\gamma^2$$
$$U_{0,2} = \begin{cases} 4\rho^4 & \text{if } \lambda \text{ is even,} \\ 4\rho^4 - \gamma^4 & \text{if } \lambda \text{ is odd,} \end{cases}$$
$$U_{0,3} = -4\rho^4 + 2\rho^2\gamma^2,$$
$$U_{1,1} = \begin{cases} 6\rho^4 - 2\rho^2\gamma^2 + \gamma^4 & \text{if } \lambda \text{ is even,} \\ 6\rho^4 - 2\rho^2\gamma^2 - \frac{1}{2}\gamma^4 & \text{if } \lambda \text{ is odd,} \end{cases}$$
$$U_{1,2} = -12\rho^4 - 2\rho^2\gamma^2,$$
$$U_{1,3} = \begin{cases} 12\rho^4 - 2\gamma^4 & \text{if } \lambda \text{ is even,} \\ 12\rho^4 + \gamma^4 & \text{if } \lambda \text{ is odd,} \end{cases}$$
$$U_{2,2} = \begin{cases} 3\rho^4 + \rho^2\gamma^2 & \text{if } \lambda \text{ is even,} \\ 3\rho^4 + \rho^2\gamma^2 + \frac{3}{4}\gamma^4 & \text{if } \lambda \text{ is odd,} \end{cases}$$
$$U_{2,3} = -12\rho^4 - 2\rho^2\gamma^2,$$
$$V = \begin{cases} 6\rho^4 + 2\rho^2\gamma^2 + \gamma^4 & \text{if } \lambda \text{ is even,} \\ 6\rho^4 + 2\rho^2\gamma^2 - \frac{1}{2}\gamma^4 & \text{if } \lambda \text{ is odd.} \end{cases}$$

Hence, from (3.3),

$$\nu_4 = \begin{cases} (-\frac{3}{8}p - \frac{5}{2}b^2 - \frac{5}{8}a^2)p\rho^2\gamma^2 \\ \quad + (\frac{3}{8}p + \frac{5}{2}b^2 + \frac{5}{8}a^2)p\rho^4 + pb^2\gamma^4 & \text{if } \lambda \text{ is even,} \\ (-\frac{3}{8}p - \frac{5}{2}b^2 - \frac{5}{8}a^2)p\rho^2\gamma^2 + (\frac{3}{8}p + \frac{5}{2}b^2 + \frac{5}{8}a^2)p\rho^4 \\ \quad + (\frac{3}{32}p - \frac{3}{8}b^2 + \frac{5}{32}a^2)p\gamma^4 & \text{if } \lambda \text{ is odd,} \end{cases}$$

which, by using the fact that $p = a^2 + 4b^2$, gives (4.12). □

Remark 4.4. To show the irreducibility over $\mathbb{Q}$ of the polynomial $\mathcal{M}_m(y)$, one also could simply use Eisenstein's criterion, since in

$$m^4\mathcal{M}_m(y) = m^4y^4 + m^3\nu_1y^3 + m^2\nu_2y^2 + m\nu_3y + \nu_4 \in \mathbb{Z}[y]$$

all of the coefficients except m^4 are divisible by the prime p, but ν_4 is not divisible by p^2.

Example $p = 113$. In this case $e = 4$, $f = 28$ and we can take $g = 3$. The four irreducible polynomials over $\mathbb{F}_2[z]$ of order 113 are

$$P_1(z) = z^{28} + z^{25} + z^{24} + z^{22} + z^{21} + z^{15} + z^{14} + z^{13} + z^7 + z^6 + z^4 + z^3 + 1,$$
$$P_2(z) = z^{28} + z^{26} + z^{22} + z^{20} + z^{19} + z^{18} + z^{14} + z^{10} + z^9 + z^8 + z^6 + z^2 + 1,$$
$$P_3(z) = z^{28} + z^{23} + z^{22} + z^{20} + z^{17} + z^{16} + z^{15} + z^{14} + z^{13} + z^{12} + z^{11} + z^8 + z^6 + z^5 + 1,$$
$$P_4(z) = z^{28} + z^{27} + z^{25} + z^{24} + z^{23} + z^{22} + z^{20} + z^{19} + z^{18} + z^{15} + z^{14} + z^{13} + z^{10} + z^9 + z^8 + z^6 + z^5 + z^4 + z^3 + z + 1.$$

For ℓ, $1 \le \ell \le 3$, let $\mathcal{A}_\ell = \mathcal{A}(P_\ell)$ be the set defined by (1.1). Since $p = a^2 + 4b^2$, $a \equiv 1 \bmod 4$, where the sign of b is chosen so that $g^{(p-1)/4} \equiv a/2b \bmod p$, we find that $a = -7$ and $b = 4$.

- $m = 1$

$G_m(y)$	$y^4 - y^3 - 42y^2 + 120y - 64$
The elements of the form 2^km of $\mathcal{A}_1$	$4, 8, \ldots, 2^{998}, 2^{999}, \ldots$
The elements of the form 2^km of $\mathcal{A}_2$	$2, 4, 8, 32 \ldots, 2^{996}, \ldots$
The elements of the form 2^km of $\mathcal{A}_3$	$8, 32, \ldots, 2^{996}, \ldots$
The elements of the form 2^km of $\mathcal{A}_4$	$1, 2, 4, 8, 16 \ldots, 2^{998}, 2^{999}, \ldots$

- $m = 11$

$G_m(y)$	$\frac{1}{14\,641}(14\,641y^4 - 13\,673y^2 + 1808)$
The elements of the form 2^km of $\mathcal{A}_1$	$44, 176, 1408, \ldots, 2^{997} \cdot 11, 2^{998} \cdot 11, 2^{999} \cdot 11, \ldots$
The elements of the form 2^km of $\mathcal{A}_2$	$11, 22, 176, 352, \ldots, 2^{998} \cdot 11, \ldots$
The elements of the form 2^km of $\mathcal{A}_3$	$44, 88, 352, 704, \ldots, 2^{996} \cdot 11, \ldots$
The elements of the form 2^km of $\mathcal{A}_4$	$11, 44, 88, 704, 1408, \ldots, 2^{997} \cdot 11, 2 \cdot 11^{999} \cdot 11, \ldots$

https://doi.org/10.1017/S1446788715000439 Published online by Cambridge University Press

- $m = 165 = 3 \cdot 5 \cdot 11$

$G_m(y)$	$\frac{1}{741\,200\,625}(741\,200\,625y^4 - 12\,305\,700y^2 + 28\,928)$
The elements of the form $2^k m$ of $\mathcal{A}_1$	$1320, 2640, 10\,560, \ldots, 2^{997} \cdot 165, 2^{998} \cdot 165, \ldots$
The elements of the form $2^k m$ of $\mathcal{A}_2$	$330, 1320, 2640, 5280, \ldots, 2^{997} \cdot 165,$ $2^{998} \cdot 165, 2^{999} \cdot 165, \ldots$
The elements of the form $2^k m$ of $\mathcal{A}_3$	$1320, 5280, \ldots, 2^{999} \cdot 165, \ldots$
The elements of the form $2^k m$ of $\mathcal{A}_4$	$330, 660, 10\,560, \ldots, 2^{996} \cdot 165, \ldots$

Acknowledgements

I am pleased to thank J.-L. Nicolas for helpful discussions. I would also like to thank the referee for his valuable remarks.

References

[1] N. Baccar, 'Sets with even partition function and 2-adic integers', *Period. 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 and F. Ben Saïd, 'On sets such that the partition function is even from a certain point on', *Int. J. Number Theory* **5**(3) (2009), 1–22.
[4] 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.
[5] N. Baccar and A. Zekraoui, 'Sets with even partition function and 2-adic integers II', *J. Integer Seq.* **13** (2010), Article 10.1.3.
[6] L. E. Dickson, 'Cyclotomy, higher congruences and Waring's problem', *Amer. J. Math.* **57** (1935), 391–424.
[7] S. A. Katre and A. R. Rajwade, 'Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum', *Math. Scand.* **60** (1987), 52–62.
[8] E. Lehmer, 'Connection between Gaussian periods and cyclic units', *Math. Comp.* **50**(182) (1988), 535–541.
[9] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and their Applications* (Cambridge University Press, New York, 1986).
[10] J.-L. Nicolas, I. Z. Ruzsa and A. Sárközy, 'On the parity of additive representation functions', *J. Number Theory* **73** (1998), 292–317.
[11] J. Riordan, *Introduction to Combinatorial Analysis* (Dover, Mineola, NY, 2002).
[12] F. Thaine, 'Properties that characterize Gaussian periods and cyclotomic numbers', *Proc. Amer. Math. Soc.* **124** (1996), 35–45.

N. BACCAR, Université de Sousse, ISITCOM Hammam Sousse,
Dép. de Math Inf., 5 Bis, Rue 1 Juin 1955, 4011 Hammam Sousse, Tunisie
e-mail: naceurbaccar@yahoo.fr