Journal of Integer Sequences, Vol. 13 (2010),
Article 10.1.3

Sets with Even Partition Functions and 2-adic Integers, II

N. Baccar[1]
Université de Sousse
ISITCOM Hammam Sousse
Dép. de Math Inf.
5 Bis Rue 1 Juin 1955
4011 Hammam Sousse
Tunisie
naceurbaccar@yahoo.fr

A. Zekraoui
Université de Monastir
F. S. M.
Dép. de Math.
Avenue de l'environnement
5000 Monastir
Tunisie
ahlemzekraoui@yahoo.fr

Abstract

For $P \in \mathbb{F}_2[z]$ with $P(0) = 1$ and $\deg(P) \geq 1$, let $\mathcal{A} = \mathcal{A}(P)$ be the unique subset of $\mathbb{N}$ such that $\sum_{n\geq 0} p(\mathcal{A}, n)z^n \equiv P(z) \pmod 2$, where $p(\mathcal{A}, n)$ is the number of partitions of n with parts in $\mathcal{A}$. Let p be an odd prime number, and let P be irreducible of order p ; i.e., p is the smallest positive integer such that P divides $1 + z^p$ in $\mathbb{F}_2[z]$. N. Baccar proved that the elements of $\mathcal{A}(P)$ of the form $2^k m$, where $k \geq 0$ and m is odd, are given by the 2-adic expansion of a zero of some polynomial R_m with integer coefficients. Let s_p be the order of 2 modulo p, i.e., the smallest positive integer such that $2^{s_p} \equiv 1 \pmod p$. Improving on the method with which R_m was obtained explicitly only when

[1]Research supported DGRST of Tunisia, UR 99/15-18, Faculté des Sciences de Tunis.

$s_p = \frac{p-1}{2}$, here we make explicit R_m when $s_p = \frac{p-1}{3}$. For that, we have used the number of points of the elliptic curve $x^3 + ay^3 = 1$ modulo p.

1 Introduction.

Let $\mathbb{N}$ denote the set of positive integers, and let $\mathcal{A} = \{a_1, a_2, \ldots\}$ be a non-empty subset of $\mathbb{N}$. For $n \in \mathbb{N}$, let $p(\mathcal{A}, n)$ be the number of partitions of n with parts in $\mathcal{A}$, i.e., the number of solutions of the diophantine equation

$$a_1x_1 + a_2x_2 + \cdots = n \tag{1}$$

in non-negative integers $x_1,\ x_2, \ldots$. By convention, $p(\mathcal{A}, 0) = 1$ and $p(\mathcal{A}, n) = 0$ for all $n < 0$. The generating series of $p(\mathcal{A}, n)$ is

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

Let $\mathbb{F}_2$ be the field with two elements and $P(z) = 1 + \epsilon_1 z + \cdots + \epsilon_N z^N \in \mathbb{F}_2[z]$, $N \geq 1$. J.-L. Nicolas, I. Z. Ruzsa and A. Sárközy [10] proved that there exists a unique set $\mathcal{A} = \mathcal{A}(P)$ satisfying

$$F_{\mathcal{A}}(z) \equiv P(z) \pmod 2, \tag{3}$$

which means that

$$p(\mathcal{A}, n) \equiv \epsilon_n \pmod 2 \text{ for } 1 \leq n \leq N \tag{4}$$

and $p(\mathcal{A}, n)$ is even for all $n > N$. Indeed, for $n = 1$,

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

and so, by (4),

$$1 \in \mathcal{A} \Leftrightarrow \epsilon_1 = 1.$$

Further, assume that we Know $\mathcal{A}_{n-1} = \mathcal{A} \cap \{1, \ldots, n-1\}$; since there exists only one partition of n containing the part n, then

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

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

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

which with (3) allow one to decide whether n belongs to $\mathcal{A}$.

Let p be an odd prime number, and let s_p be the order of 2 modulo p, i.e., s_p is the smallest positive integer such that p divides $2^{s_p} - 1$. Let $P \in \mathbb{F}_2[z]$ be irreducible of order p

(ord$(P)=p$); in other words, p is the smallest positive integer such that P divides $1+z^p$ in $\mathbb{F}_2[z]$. N. Baccar and F. Ben Saïd [2] determined the sets $\mathcal{A}(P)$ for all p such that $s_p=\frac{p-1}{2}$. Moreover, they proved that if $k\geq 0$ and m is an odd positive integer, then the elements of $\mathcal{A}(P)$ of the form $2^k m$ are given by the 2-adic expansion of some zero of a polynomial R_m with integer coefficients. N. Baccar [1] extended this last result to any odd prime number p. Unfortunately, the method used in that paper can make explicit R_m only when $s_p=\frac{p-1}{2}$. In this paper, we will improve on the method given by N. Baccar [1], by introducing elliptic curves, to make R_m explicit when $s_p=\frac{p-1}{3}$. In Section 2, some properties of the polynomial R_m are exposed. In Section 3, we introduce elliptic curves to compute some cardinalities used in Section 4 to make R_1 explicit, and in Section 5 to get R_m explicitly for any odd integer $m\geq 3$.

Throughout this paper, p is an odd prime number and P is some irreducible polynomial in $\mathbb{F}_2[z]$ of order p. We also denote by s_p the order of 2 modulo p. For $a\in\mathbb{Z}$ and $b\in\mathbb{N}$, we should write $a \bmod b$ for the remainder of the euclidean division of a by b.

2 Some results on the polynomial R_m

Let p be an odd prime. We denote by $(\mathbb{Z}/p\mathbb{Z})^*$ the group of invertible elements modulo p and by $<2>$ its subgroup generated by 2. We consider the action $\star$ of $<2>$ on the set $\mathbb{Z}/p\mathbb{Z}$ given by $a\star n=an$ for all $a\in<2>$ and all $n\in\mathbb{Z}/p\mathbb{Z}$. The quotient set will be denoted by $(\mathbb{Z}/p\mathbb{Z})/_{<2>}$ and the orbit of some $n\in\mathbb{Z}/p\mathbb{Z}$ by $O(n)$. So, we can write

$$\mathbb{Z}/p\mathbb{Z}=O(1)\cup O(g)\cup\cdots\cup O(g^{r-1})\cup O(p),$$

where g is some generator of $(\mathbb{Z}/p\mathbb{Z})^*$, $r=\frac{p-1}{s_p}$ is the number of invertible orbits of $\mathbb{Z}/p\mathbb{Z}$,

$$O(g^i)=\left\{2^j g^i \bmod p:\ 0\leq j\leq s_p-1\right\},\quad 0\leq i\leq r-1, \tag{5}$$

$$O(p)=\{0\}.$$

Note that for any integer t,

$$O(g^t)=O(g^{t \bmod r}). \tag{6}$$

The orbits $O(n)$ are defined as parts of $\mathbb{Z}/p\mathbb{Z}$; however, by extension, they are also considered as parts of $\mathbb{N}$.

If ϕ_p is the cyclotomic polynomial over $\mathbb{F}_2$ of index p, then

$$1+z^p=(1+z)\phi_p(z).$$

Moreover, one has

$$\phi_p(z)=P_0(z)P_1(z)\cdots P_{r-1}(z),$$

where $P_0,P_1,\dots$ and P_{r-1} are the only distinct irreducible polynomials in $\mathbb{F}_2[z]$ of the same degree s_p and all of which are of order p. For all l, $0\leq l\leq r-1$, let $\mathcal{A}_l=\mathcal{A}(P_l)$ be the set obtained from (3). If m is an odd positive integer, we define the 2−adic integer $y_l(m)$ by

$$y_l(m) = \chi(\mathcal{A}_l, m) + 2\chi(\mathcal{A}_l, 2m) + 4\chi(\mathcal{A}_l, 4m) + \cdots = \sum_{k=0}^{\infty} \chi(\mathcal{A}_l, 2^k m) 2^k. \tag{7}$$

By computing $y_l(m) \bmod 2^{k+1}$, one can deduce $\chi(\mathcal{A}_l, 2^j m)$ for all j, $0 \leq j \leq k$, and obtain all the elements of $\mathcal{A}_l$ of the form $2^j m$. In [3], some necessary conditions on integers to be in $\mathcal{A}_l$ were given. For instance:

$$p^2 n \notin \mathcal{A}_l, \ \forall\, n \in \mathbb{N}, \tag{8}$$

$$\text{if } q \text{ is an odd prime in } O(1), \text{then } qn \notin \mathcal{A}_l, \ \forall n \in \mathbb{N}. \tag{9}$$

Let $\mathbb{K}$ be some field, and let $u(z) = \sum_{j=0}^{n} u_j z^j$ and $v(z) = \sum_{j=0}^{t} v_j z^j$ be polynomials in $\mathbb{K}[z]$. We denote the resultant of u and v with respect to z by $\mathrm{res}_z(u(z), v(z))$, and recall the following well known result

Lemma 1. *(i) The resultant $res_z(u(z), v(z))$ is a homogeneous multivariate polynomial with integer coefficients, of degree $n + t$ in the $n + t + 2$ variables u_i, v_j.*
(ii) If $u(z)$ is written as $u(z) = u_n(z - \alpha_1)(z - \alpha_2) \cdots (z - \alpha_n)$ in the splitting field of u over $\mathbb{K}$ then

$$res_z(u(z), v(z)) = u_n^t \prod_{i=1}^{n} v(\alpha_i). \tag{10}$$

N. Baccar proved [1] that, for all l, $0 \leq l \leq r - 1$, the 2-adic integers $y_l(m)$ defined by (7) are the zeros of some polynomial R_m with integer coefficients and which can be written as the resultant of two polynomials. We mention here that the expressions given in that paper to R_m, for $m = 1$ and $m \geq 3$, can be encoded in only one. So that we have

Theorem 2. *([1]) 1) Let m be an odd positive integer such that $m \notin O(p)$ (i.e., $\gcd(m, p) = 1$), and let $\delta = \delta(m)$ be the unique integer in $\{0, 1, \ldots, r - 1\}$ such that $m \in O(g^\delta)$. We define the polynomial A_m by*

$$A_m(z) = \sum_{h=0}^{r-1} \alpha_h(m) B_h(z), \tag{11}$$

where for all h, $0 \leq h \leq r - 1$,

$$\alpha_h(m) = \sum_{d \,|\, \widetilde{m},\ d \in O(g^h)} \mu(d), \tag{12}$$

$\widetilde{m} = \prod_{q \text{ prime } q|m} q$ is the radical of m with $\widetilde{1} = 1$, μ is the Möbius function and B_h is the polynomial

$$B_h(z) = B_{h,m}(z) = \sum_{j=0}^{s_p - 1} z^{\left(2^j g^{(\delta - h) \bmod r}\right) \bmod p}. \tag{13}$$

Then, the 2-adic integers $y_0(m), y_1(m), \ldots$ and $y_{r-1}(m)$ are the zeros of the polynomial $R_m(y)$ of $\mathbb{Z}[y]$ defined by the resultant

$$R_m(y) = res_z(\phi_p(z), my + A_m(z)) \tag{14}$$

and we have

$$R_m(y) = m^{p-1}\big((y - y_0(m))(y - y_1(m)) \cdots (y - y_{r-1}(m))\big)^{s_p}. \tag{15}$$

2) The 2-adic integers $y_0(p), y_1(p), \ldots$ and $y_{r-1}(p)$ are the zeros of the polynomial $R_1(-py - s_p)$; while if $m = pm'$, $m' \geq 3$ and $\gcd(m', p) = 1$, then $y_0(m), y_1(m), \ldots$ and $y_{r-1}(m)$ are the zeros of the polynomial $R_{m'}(-py)$ defined by (14).
3) If m is divisible by p^2 or by some prime q belonging to $O(1)$ then we extend the definition (14) to $R_m(y) = m^{p-1}y^{s_p}$; so that $y_0(m), y_1(m), \ldots$ and $y_{r-1}(m)$ remain zeros of R_m since, from (8) and (9), they all vanish.

Remark 3. Explicit formulas to the polynomials R_m defined by (14), when $s_p = \frac{p-1}{2}$, are given in [1]. Moreover in that paper, it is shown that if θ is a certain primitive p-th root of unity over the 2-adic field $\mathbb{Q}_2$, then for all l, $0 \leq l \leq r-1$,

$$y_l(1) = -T_l, \tag{16}$$

where, for all $l \in \mathbb{Z}$,

$$T_l = T_{l \bmod 3} = \sum_{k=0}^{s_p-1} \theta^{2^k g^l} = \sum_{j \in O(g^l)} \theta^j. \tag{17}$$

We also mention here that N. Baccar [1] proved that for all $m \in \mathbb{N}$,

$$R_m(y) = \prod_{l=0}^{r-1} \left(my + A_m(\theta^{g^l})\right)^{s_p}. \tag{18}$$

3 Orbits and elliptic curves.

From now on, we keep the above notation and assume that the prime number p is such that $s_p = \frac{p-1}{3}$ (the first ones up to 1000 are: $p = 43, 109, 157, 229, 277, 283, 307, 499, 643, 691, 733, 739, 811, 997$). So the number of invertible orbits is $r = 3$ and

$$\mathbb{Z}/p\mathbb{Z} = O(1) \cup O(g) \cup O(g^2) \cup O(p), \tag{19}$$

where g is some generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$. The order of 2 is $s_p = \frac{p-1}{3}$; if 2 were a square modulo p, its order should divide $\frac{p-1}{2}$, which is impossible. Hence 2 cannot be a square modulo p, and by Euler criterion, p has to satisfy $p \equiv \pm 3 \pmod 8$, and, as $p \equiv 1 \pmod 3$, $p \equiv 13,\ 19 \pmod{24}$.

Lemma 4. *For all i, $0 \le i \le 2$, let $O(g^i)$ be the orbit of g^i defined by (5). Then*

$$O(g^i) = \left\{-g^i, -2g^i, \dots, -2^{s_p-1}g^i\right\} = \left\{g^i, g^{i+3} \dots, g^{i+3(s_p-1)}\right\}. \tag{20}$$

In particular, 2 is a cube modulo p and the sub-group generated by 2 is the sub-group of cubes (generated by g^3) and contains -1.

Proof. To get the first equality of (20), it suffices to show that $-1 \in O(1)$. This follows from $-1 = (\frac{2}{p}) \equiv 2^{\frac{p-1}{2}} \pmod{p}$.
To prove the second equality of (20), one just use the fact that (cf. (6)) $g^3 \in O(1)$. □

Let us define the integers $\ell_{i,j},\ 0 \le i,\ j \le 2$, by

$$\ell_{i,j} = \left|\left\{t:\ 0 \le t \le s_p - 1,\ 1 + g^{j+3t} \in O(g^i)\right\}\right|. \tag{21}$$

Remark 5. As shown just above, $-1 \in O(1)$, so that there exists one and only one $t \in \{0, 1, \dots, s_p - 1\}$ such that $1 + g^{3t} \in O(p)$. Moreover, for all $t \in \{0, 1, \dots, s_p - 1\}$ and $j \in \{1, 2\}$, $1 + g^{j+3t} \notin O(p)$. Hence the integers $\ell_{i,j}$ defined by (21) satisfy

$$\sum_{i=0}^{2} \ell_{i,j} = s_p - \delta_{0,j}, \tag{22}$$

where $\delta_{i,j}$ is the Kronecker symbol given by

$$\delta_{i,j} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{otherwise.} \end{cases}$$

The integers $\ell_{i,j}$ defined above are cardinalities of some curves. Indeed, let us consider the curve over $\mathbb{F}_p$,

$$\mathcal{C}_{i,j}:\quad 1 + g^j X^3 = g^i Y^3$$

and denote by $c_{i,j}$ its cardinality, $c_{i,j} = \mid \mathcal{C}_{i,j} \mid$. Since -1 is a cube modulo p, it is clear that

$$c_{j,i} = c_{i,j}.$$

Using (21) it follows that

$$\ell_{i,j} = |\{(X^3, Y^3):\ X \neq 0,\ Y \neq 0 \text{ and } (X, Y) \in \mathcal{C}_{i,j}\}|.$$

Therefore,

$$\ell_{j,i} = \ell_{i,j}. \tag{23}$$

Note that, $(X^3, Y^3) = (X'^3, Y'^3)$ if and only if $X' = Xg^{vs_p}$ and $Y' = Yg^{ws_p}$ for some $v, w \in \{0, 1, 2\}$. Moreover, if $i \neq 0$ (resp. $j \neq 0$), no point on the curve $\mathcal{C}_{i,j}$ can be of the form $(0, Y)$ (resp. $(X, 0)$). But if $i = 0$ (resp. $j = 0$), we obtain three points on the curve $\mathcal{C}_{i,j}$ with $X = 0$ (resp. $Y = 0$). Consequently, we obtain the relation

$$c_{i,j} = 9\ell_{i,j} + 3\delta_{i,0} + 3\delta_{0,j}. \tag{24}$$

Now, let us consider the projective plane cubic curve

$$\mathcal{E}_{i,j}: \quad Z^3 + g^j X^3 = g^i Y^3$$

and $e_{i,j} = \mid \mathcal{E}_{i,j} \mid$ its cardinality. If $i \neq j$, $\mathcal{E}_{i,j}$ has no points at infinity; whereas if $i = j$, it has three points at infinity. Hence

$$e_{i,j} = c_{i,j} + 3\delta_{i,j}. \tag{25}$$

By multiplying the equation $Z^3 + gX^3 = gY^3$ by g^2, we get the curve $g^2Z^3 + X'^3 = Y'^3$. So, by permuting the variables, we deduce that $e_{1,1} = e_{2,0}$. Similarly, we obtain $e_{2,2} = e_{1,0}$. Hence, by (25) and (24) we find that

$$\ell_{1,1} = \ell_{2,0}, \tag{26}$$

$$\ell_{2,2} = \ell_{1,0}. \tag{27}$$

Therefore, from (22), it follows that

$$\ell_{2,1} = \ell_{0,0} + 1. \tag{28}$$

Furthermore, from (25) and (24) we have for all i, $0 \leq i \leq 2$,

$$\begin{aligned} 9\ell_{i,0} &= c_{i,0} - 3\delta_{i,0} - 3 \\ &= e_{i,0} - 6\delta_{i,0} - 3. \end{aligned} \tag{29}$$

Hence, to get all the numbers $\ell_{i,j}$, $0 \leq i, j \leq 2$, it suffices to know the values of $e_{i,0}$, $0 \leq i \leq 2$.

Computation of $e_{i,0}$, $i \in \{0, 1, 2\}$.

Here, we are interested with the curve $\mathcal{E}_{i,0}: \quad Z^3 + X^3 = g^i Y^3$. By setting $X = 9g^i z + 2y$, $Y = 6x$ and $Z = 9g^i z - 2y$, we get the Weierstrass's form

$$zy^2 = x^3 - (27/4)g^{2i}z^3,$$

which, when divided by z^3, gives the form

$$y^2 = x^3 - (27/4)g^{2i}.$$

Let

$$y^2 = x^3 + \alpha x + \beta$$

be the equation of an elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_p$. It is well known that the number of points of $\mathcal{E}$ is equal to

$$\mid \mathcal{E} \mid = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + \alpha x + \beta}{p} \right), \tag{30}$$

where $(\frac{\cdot}{p})$ is the Legendre's symbol. For $\alpha = 0$, the sum $\sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + \alpha x + \beta}{p} \right)$ was investigated by S. A. Katre [8]. He obtained:

Lemma 6. *Let p be a prime number such that $p \equiv 1 \pmod 3$. Then there exist a unique L, $L \equiv 1 \pmod 3$ and a unique M up to a sign such that $4p = L^2 + 27M^2$. Moreover, if β is an integer $\neq 0$ then*

$$\sum_{x\in\mathbb{F}_p} \left(\frac{x^3+\beta}{p}\right) = \begin{cases} (\frac{\beta}{p})L, & \text{if } 4\beta \text{ is a cube modulo } p; \\ -\frac{1}{2}(\frac{\beta}{p})(L+9M), & \text{otherwise, where } M \text{ is chosen uniquely} \\ & \text{by } (4\beta)^{\frac{p-1}{3}} \equiv \frac{L+9M}{L-9M} \pmod p \; . \end{cases}$$

Thanks to Lemma 6, we can give the values of $e_{i,0}$ for $0 \leq i \leq 2$.
Computation of $e_{0,0}$. From (30), since -27 is a cube , by using Lemma 6 with $\beta = -27/4$, we obtain

$$\begin{aligned} e_{0,0} &= p+1+\left(\frac{-27/4}{p}\right)L \\ &= p+1+\left(\frac{-27}{p}\right)L \\ &= p+1+\left(\frac{-3}{p}\right)^3 L. \end{aligned}$$

Since $p \equiv 1 \pmod 3$ then, by the quadratic reciprocity law, -3 is a quadratic residue modulo p. Hence,

$$e_{0,0} = p+1+L. \tag{31}$$

Computation of $e_{1,0}$. If $\beta = -27g^2/4$ then $4\beta = -27g^2$ is not a cube modulo p. Hence, by using Lemma 6 again, it follows that

$$\begin{aligned} e_{1,0} &= p+1-\frac{1}{2}\left(\frac{-27g^2/4}{p}\right)(L+9M) \\ &= p+1-\frac{1}{2}(L+9M), \end{aligned} \tag{32}$$

where the sign of M is given by

$$\begin{aligned} \left(-27g^2\right)^{(p-1)/3} &\equiv (g^2)^{(p-1)/3} \pmod p \\ &\equiv \frac{L+9M}{L-9M} \pmod p. \end{aligned}$$

Computation of $e_{2,0}$. Let M be fixed by last congruence, and let $\beta = -27g^4/4$. Since $(g^4)^{(p-1)/3} \not\equiv (g^2)^{(p-1)/3} \pmod p$, Lemma 6 implies that

$$e_{2,0} = p+1-\frac{1}{2}(L-9M). \tag{33}$$

4 The explicit form of R_1 when $s_p = \frac{p-1}{3}$.

First, we remark that the polynomial $R_1(y)$ given by (14) can also be defined (cf. (15), (16)) by

$$(R_1(y))^{1/s_p} = \prod_{i\in\{0,1,2\}} \Big(y + T_i\Big), \tag{34}$$

where $\theta \neq 1$ is some p-th root of unity.

Theorem 7. *Let p be an odd prime such that $s_p = \frac{p-1}{3}$. Then the polynomial R_1 given by (14) or (34) is equal to*

$$R_1(y) = \left(y^3 - y^2 - s_p y + \lambda_p\right)^{s_p},$$

with

$$\lambda_p = \frac{p(L+3)-1}{27},$$

where L is the unique integer satisfying $4p = L^2 + 27M^2$ and $L \equiv 1 \pmod 3$.

Remark 8. $p(L+3) \equiv 1 \pmod{27}$ follows easily from the congruences $L \equiv 1 \pmod 3$ and $p \equiv L^2 \pmod{27}$.

Proof of Theorem 7. From (34), we have

$$R_1(y) = \Big((y+T_0)(y+T_1)(y+T_2)\Big)^{s_p}.$$

This can be written as

$$R_1(y) = \Big(y^3 + \lambda_p'' y^2 + \lambda_p' y + \lambda_p\Big)^{s_p},$$

with

$$\lambda_p = T_0T_1T_2, \tag{35}$$

$$\lambda_p' = T_0T_1 + T_0T_2 + T_1T_2, \tag{36}$$
$$\lambda_p'' = T_0 + T_1 + T_2.$$

We begin by calculating λ_p''. It follows immediately from (17) and (19) that

$$\begin{aligned} \lambda_p'' &= T_0 + T_1 + T_2 \\ &= \sum_{i=0}^{2} \sum_{k=0}^{s_p-1} \theta^{2^k g^i} \\ &= \sum_{j=1}^{p-1} \theta^j \\ &= -1, \end{aligned} \tag{37}$$

since cf. Remark 3, θ is a primitive p-th root of unity.

Now, let us prove that $\lambda'_p = -s_p$. From (36) and (17), we have

$$\lambda'_p = \sum_{0\le k,k'\le s_p-1} \theta^{2^k g + 2^{k'} g^2} + \sum_{0\le k,k'\le s_p-1} \theta^{2^k g^2 + 2^{k'}} + \sum_{0\le k,k'\le s_p-1} \theta^{2^k g + 2^{k'}}. \tag{38}$$

To treat the last sum in (38), let us fix k and k' in $\{0, 1, \ldots, s_p - 1\}$. We have $\theta^{2^k g + 2^{k'}} = \theta^{2^{k'}(1+2^{k-k'} g)}$. Since $2^{k-k'} g \in O(g)$ then, from the second equality in (20), there exists a unique $t \in \{0, 1, \ldots, s_p - 1\}$ such that $2^{k-k'} g = g^{1+3t}$. Hence, the last sum in (38) becomes

$$\sum_{0\le k,k'\le s_p-1} \theta^{2^k g + 2^{k'}} = \sum_{0\le k',t\le s_p-1} \theta^{2^{k'}(1+g^{1+3t})}. \tag{39}$$

For the first and second sums in (38), arguing as above, we get

$$\begin{aligned} \sum_{0\le k,k'\le s_p-1} \theta^{2^k g^2 + 2^{k'}} &= \sum_{0\le k,k'\le s_p-1} \theta^{2^{k'}(1+2^{k-k'} g^2)} \\ &= \sum_{0\le k',t\le s_p-1} \theta^{2^{k'}(1+g^{2+3t})} \end{aligned} \tag{40}$$

and

$$\begin{aligned} \sum_{0\le k,k'\le s_p-1} \theta^{2^k g + 2^{k'} g^2} &= \sum_{0\le k,k'\le s_p-1} \theta^{2^k(g+2^{k'-k} g^2)} \\ &= \sum_{0\le k,t\le s_p-1} \theta^{2^k(g+g^{2+3t})}. \end{aligned} \tag{41}$$

Now, from (21), (26), (27), (17) and Remark 5, we obtain

$$\begin{aligned} \sum_{0\le k',t\le s_p-1} \theta^{2^{k'}(1+g^{1+3t})} &= \sum_{i=0}^{2} \ell_{i,1} T_i \\ &= \ell_{1,0} T_0 + \ell_{2,0} T_1 + \ell_{2,1} T_2 \end{aligned} \tag{42}$$

and

$$\begin{aligned} \sum_{0\le k',t\le s_p-1} \theta^{2^{k'}(1+g^{2+3t})} &= \sum_{i=0}^{2} \ell_{i,2} T_i \\ &= \ell_{2,0} T_0 + \ell_{2,1} T_1 + \ell_{1,0} T_2. \end{aligned} \tag{43}$$

On the other hand, since for all $v \ge 0$, $0 \le i, j \le 2$,

$$1 + g^{j+3t} \in O(g^i) \Longleftrightarrow g^v + g^{v+j+3t} \in O(g^{v+i}),$$

again by (21), (26), (17) and Remark 5, we get

$$\begin{aligned}\sum_{0\le k,t\le s_p-1}\theta^{2^k(g+g^{2+3t})} &= \sum_{i=0}^{2}\ell_{i,1}T_{1+i}\\ &= \ell_{2,1}T_0+\ell_{1,0}T_1+\ell_{2,0}T_2. \qquad (44)\end{aligned}$$

Clearly, from (22) and (28), one can deduce that

$$\ell_{1,0}+\ell_{2,0}+\ell_{2,1}=s_p, \qquad (45)$$

which, by (38)-(44) and (37), gives

$$\begin{aligned}\lambda'_p &= s_p\,(T_0+T_1+T_2)\\ &= s_p\sum_{j=1}^{p-1}\theta^j\\ &= -s_p. \qquad (46)\end{aligned}$$

Finally, let us calculate λ_p. From (35) and (17), we have

$$\begin{aligned}\lambda_p &= \sum_{0\le k,k',k"\le s_p-1}\theta^{2^k+2^{k'}g+2^{k"}g^2}\\ &= \sum_{0\le k\le s_p-1}\theta^{2^k}\left(\sum_{0\le k',k"\le s_p-1}\theta^{2^{k'}g+2^{k"}g^2}\right). \qquad (47)\end{aligned}$$

Hence, by (41), (44) and (17), we get

$$\begin{aligned}\lambda_p &= \sum_{0\le k\le s_p-1}\theta^{2^k}\left(\ell_{2,1}\sum_{j\in O(1)}\theta^j+\ell_{1,0}\sum_{j\in O(g)}\theta^j+\ell_{2,0}\sum_{j\in O(g^2)}\theta^j\right)\\ &= \ell_{2,1}\sum_{0\le k,k'\le s_p-1}\theta^{2^k+2^{k'}}+\ell_{1,0}\sum_{0\le k,k'\le s_p-1}\theta^{2^k+2^{k'}g}+\ell_{2,0}\sum_{0\le k,k'\le s_p-1}\theta^{2^k+2^{k'}g^2}.\end{aligned}$$

Consequently, from (39), (42), (40) and (43), it happens that

$$\begin{aligned}\lambda_p &= \ell_{2,1}\sum_{0\le k,k'\le s_p-1}\theta^{2^k+2^{k'}}+(\ell_{1,0}^2+\ell_{2,0}^2)T_0+(\ell_{1,0}\ell_{2,0}+\ell_{2,0}\ell_{2,1})T_1\\ &\quad+(\ell_{1,0}\ell_{2,1}+\ell_{1,0}\ell_{2,0})T_2. \qquad (48)\end{aligned}$$

Since $2^{k'-k}\in O(1)=O(g^3)$ then, cf. (20), there exists a unique $t\in\{0,1,\ldots,s_p-1\}$ such that $2^{k'-k}=g^{3t}$. Hence

$$\begin{aligned}\sum_{0\le k,k'\le s_p-1}\theta^{2^k+2^{k'}} &= \sum_{0\le k,k'\le s_p-1}\theta^{2^k(1+2^{k'-k})}\\ &= \sum_{0\le k,t\le s_p-1}\theta^{2^k(1+g^{3t})}.\end{aligned}$$

Now, we recall that cf. Remark 5 there exists one and only one $t \in \{0, 1, \ldots, s_p - 1\}$ satisfying $1 + g^{3t} \in O(p)$. Consequently, by (21) and (17), we get

$$\begin{aligned} \sum_{0 \le k, k' \le s_p - 1} \theta^{2^k + 2^{k'}} &= \sum_{0 \le k, t \le s_p - 1} \theta^{2^k (1 + g^{3t})} \\ &= \ell_{0,0} T_0 + \ell_{1,0} T_1 + \ell_{2,0} T_2 + s_p. \end{aligned} \tag{49}$$

Hence, (48) gives

$$\begin{aligned} \lambda_p &= (\ell_{1,0}^2 + \ell_{2,0}^2 + \ell_{0,0}\ell_{2,1}) T_0 + (\ell_{1,0}\ell_{2,0} + \ell_{2,0}\ell_{2,1} + \ell_{1,0}\ell_{2,1}) T_1 \\ &\quad + (\ell_{1,0}\ell_{2,0} + \ell_{1,0}\ell_{2,1} + \ell_{2,0}\ell_{2,1}) T_2 + \ell_{2,1} s_p. \end{aligned} \tag{50}$$

On the other hand, from (47), by changing the order of summation, λ_p can be written as

$$\lambda_p = \sum_{0 \le k' \le s_p - 1} \theta^{2^{k'} g} \left(\sum_{0 \le k, k" \le s_p - 1} \theta^{2^k + 2^{k"} g^2} \right)$$

and we get in the way as above

$$\begin{aligned} \lambda_p &= (\ell_{1,0}\ell_{2,0} + \ell_{1,0}\ell_{2,1} + \ell_{2,0}\ell_{2,1}) T_0 + (\ell_{1,0}^2 + \ell_{2,0}^2 + \ell_{0,0}\ell_{2,1}) T_1 \\ &\quad + (\ell_{1,0}\ell_{2,0} + \ell_{2,0}\ell_{2,1} + \ell_{1,0}\ell_{2,1}) T_2 + \ell_{2,1} s_p \end{aligned} \tag{51}$$

Whereas, if we write λ_p in the form

$$\lambda_p = \sum_{0 \le k" \le s_p - 1} \theta^{2^{k"} g^2} \left(\sum_{0 \le k, k' \le s_p - 1} \theta^{2^k + 2^{k'} g} \right),$$

we get

$$\begin{aligned} \lambda_p &= (\ell_{1,0}\ell_{2,0} + \ell_{2,0}\ell_{2,1} + \ell_{1,0}\ell_{2,1}) T_0 + (\ell_{1,0}\ell_{2,0} + \ell_{1,0}\ell_{2,1} + \ell_{2,0}\ell_{2,1}) T_1 \\ &\quad + (\ell_{1,0}^2 + \ell_{2,0}^2 + \ell_{0,0}\ell_{2,1}) T_2 + \ell_{2,1} s_p. \end{aligned} \tag{52}$$

By summing (50), (51) and (52), we obtain

$$\begin{aligned} 3\lambda_p &= (\ell_{1,0}^2 + \ell_{2,0}^2 + 2\ell_{1,0}\ell_{2,0} + 2\ell_{1,0}\ell_{2,1} + 2\ell_{2,0}\ell_{2,1} + \ell_{0,0}\ell_{2,1}) \times \\ &\quad (T_0 + T_1 + T_2) + 3\ell_{2,1} s_p. \end{aligned}$$

But, according to (37), $T_0 + T_1 + T_2 = -1$. Hence,

$$\begin{aligned} 3\lambda_p &= -(\ell_{1,0}^2 + \ell_{2,0}^2 + 2\ell_{1,0}\ell_{2,0} + 2\ell_{1,0}\ell_{2,1} + 2\ell_{2,0}\ell_{2,1} + \ell_{0,0}\ell_{2,1}) + 3\ell_{2,1} s_p \\ &= -\big((\ell_{1,0} + \ell_{2,0})^2 + \ell_{1,0}\ell_{2,1} + \ell_{2,0}\ell_{2,1} + \ell_{2,1}(\ell_{0,0} + \ell_{1,0} + \ell_{2,0})\big) + 3\ell_{2,1} s_p. \end{aligned}$$

So that, from (45) and (22), we obtain

$$3\lambda_p = -(s_p - \ell_{2,1})^2 - \ell_{2,1}(s_p - \ell_{2,1}) - \ell_{2,1}(s_p - 1) + 3\ell_{2,1} s_p,$$

which gives $\lambda_p = \frac{(3s_p + 1)\ell_{2,1} - s_p^2}{3} = \frac{p\ell_{2,1} - s_p^2}{3}$. Finally, using the value of $\ell_{2,1}$:

$$\ell_{2,1} = \frac{1}{9}(p + 1 + L) \tag{53}$$

which follows from (28), (29) and (31), we complete the proof of Theorem 7. □

In the following table we give L, g, M and $R_1(y)$ when $p \leq 1000$.

p	L	g	M	$R_1(y)$
43	-8	3	-2	$(y^3 - y^2 - 14y - 8)^{14}$
109	-2	6	4	$(y^3 - y^2 - 36y + 4)^{36}$
157	-14	5	4	$(y^3 - y^2 - 52y - 64)^{52}$
229	22	6	4	$(y^3 - y^2 - 76y + 212)^{76}$
277	-26	5	-4	$(y^3 - y^2 - 92y - 236)^{92}$
283	-32	3	-2	$(y^3 - y^2 - 94y - 304)^{94}$
307	16	5	-6	$(y^3 - y^2 - 102y + 216)^{102}$
499	-32	7	-6	$(y^3 - y^2 - 166y - 536)^{166}$
643	40	11	6	$(y^3 - y^2 - 214y + 1024)^{214}$
691	-8	3	10	$(y^3 - y^2 - 230y - 128)^{230}$
733	-50	6	4	$(y^3 - y^2 - 244y - 1276)^{244}$
739	16	3	10	$(y^3 - y^2 - 246y + 520)^{246}$
811	-56	3	-2	$(y^3 - y^2 - 270y - 1592)^{270}$
997	10	7	-12	$(y^3 - y^2 - 332y + 480)^{332}$

xxxx

5 The explicit form of R_m when $s_p = \frac{p-1}{3}$ and $m \geq 3$.

We remind that if $m \in O(p)$ or m is divisible by some prime q belonging to $O(1)$, then the polynomial R_m is given by Theorem 2, 2) and 3). Let m be an odd integer ≥ 3 such that all its prime divisors are in $O(g) \cup O(g^2)$. For $i \in \{1, 2\}$, we denote by ω_i the arithmetic function which counts the number of distinct prime divisors belonging to $O(g^i)$ of an integer, i.e.,

$$\omega_i(n) = \sum_{q \text{ prime},\ q \in O(g^i),\ q \mid n} 1. \tag{54}$$

Let the decomposition of m into irreducible factors be

$$m = q_{1,1}^{\gamma_{1,1}} q_{1,2}^{\gamma_{1,2}} \cdots q_{1,\omega_1}^{\gamma_{1,\omega_1}} q_{2,1}^{\gamma_{2,2}} q_{2,2}^{\gamma_{2,2}} \cdots q_{2,\omega_2}^{\gamma_{2,\omega_2}}, \tag{55}$$

where $\omega_i = \omega_i(m)$, $\omega = \omega(m) = \omega_1 + \omega_2$ and $q_{i,j} \in O(g^i)$.

We shall begin with some result concerning binomial coefficients:

Lemma 9. *For all $n \in \mathbb{N}$ and all j , $0 \leq j \leq 2$,*

$$\sum_{k \geq 0} \binom{n}{3k+j} (-1)^{k+j} = 2.3^{\frac{n}{2}-1} \cos(\frac{n\pi}{6} + \frac{2j\pi}{3}). \tag{56}$$

Proof. Let $z_1 = e^{(2i\pi)/3}$ and $z_2 = e^{(4i\pi)/3}$ be the two cubic primitive roots of unity, and let $f(z) = \sum_{k \geq 0} a_k z^k$ be some convergent power series. Since for all j, $0 \leq j \leq 2$,

$$\frac{1 + z_1^{n-j} + z_2^{n-j}}{3} = \begin{cases} 1, & \text{if } n \equiv j \pmod 3; \\ 0, & \text{otherwise}, \end{cases}$$

it follows that

$$\frac{f(z) + \frac{1}{z_1^j} f(z_1 z) + \frac{1}{z_2^j} f(z_2 z)}{3} = \sum_{k \geq 0} a_{3k+j} z^{3k+j}.$$

Hence, defining $g_j(z)$, $0 \leq j \leq 2$, by

$$g_j(z) = \sum_{k \geq 0} \binom{n}{3k+j} z^{3k+j},$$

and taking $f(z) = (1+z)^n$, we get

$$g_j(z) = \frac{f(z) + \frac{1}{z_1^j} f(z_1 z) + \frac{1}{z_2^j} f(z_2 z)}{3}.$$

By making the substitution $z = -1$, we obtain

$$\begin{aligned} g_j(-1) &= \sum_{k \geq 0} \binom{n}{3k+j} (-1)^{k+j} \\ &= \frac{\frac{1}{z_1^j}(1-z_1)^n + \frac{1}{z_2^j}(1-z_2)^n}{3} \\ &= \frac{1}{3} \left\{ \frac{1}{z_1^j} \left(\frac{3 - i\sqrt{3}}{2} \right)^n + \frac{1}{z_2^j} \left(\frac{3 + i\sqrt{3}}{2} \right)^n \right\}. \end{aligned}$$

To get (56), we need only transform the right hand-side of the last equality. □

Corollary 10. *Let m be an odd integer ≥ 3 of the form (55), and let $\alpha_h(m)$ be the quantity defined by (12). For all h, $0 \leq h \leq 2$, we have*

$$\alpha_h(m) = \eta(m) \cos\left((\omega_2 - \omega_1)\frac{\pi}{6} + 4h\frac{\pi}{3} \right) \tag{57}$$

where

$$\eta(m) = 2.3^{\frac{\omega}{2}-1}. \tag{58}$$

Proof. From (12), for all h, $0 \leq h \leq 2$, we have

$$\alpha_h(m) = \sum_{d \,|\, \widetilde{m},\ d \in O(g^h)} \mu(d).$$

First, let us suppose that $\omega_1 \neq 0$ and $\omega_2 \neq 0$. By (54) and (55), we obtain that for all h, $0 \leq h \leq 2$,

$$\alpha_h(m) = \sum_{i_1=0}^{\omega_1} (-1)^{i_1} \binom{\omega_1}{i_1} \sum_{\substack{i_2=0 \\ i_2 \equiv i_1 + 2h \pmod 3}}^{\omega_2} (-1)^{i_2} \binom{\omega_2}{i_2}.$$

So that, by (56), we get

$$\begin{aligned}\alpha_h(m) &= \sum_{i_1=0}^{\omega_1}(-1)^{i_1}\binom{\omega_1}{i_1}2.3^{\frac{\omega_2}{2}-1}\cos\left(\frac{\omega_2\pi}{6}+\frac{2(i_1+2h)\pi}{3}\right)\\ &= 2.3^{\frac{\omega_2}{2}-1}\sum_{j=0}^{2}\cos\left(\frac{\omega_2\pi}{6}+\frac{2(j+2h)\pi}{3}\right)\sum_{\substack{i_1=0\\ i_1\equiv j \pmod 3}}^{\omega_1}(-1)^{i_1}\binom{\omega_1}{i_1},\end{aligned}$$

which, by (56) again, gives

$$\alpha_h(m) = 4.3^{\frac{\omega}{2}-2}\sum_{j=0}^{2}\cos\left(\frac{\omega_2\pi}{6}+\frac{2(j+2h)\pi}{3}\right)\cos\left(\frac{\omega_1\pi}{6}+\frac{2j\pi}{3}\right).$$

Consequently, to get (57), one need only use the elementary trigonometric formulas

$$\cos a\cos b = \frac{1}{2}\left(\cos(a+b)+\cos(a-b)\right) \text{ for all } a \text{ and } b \text{ in } \mathbb{R}$$

and

$$\cos c+\cos(c+\frac{2\pi}{3})+\cos(c+\frac{4\pi}{3}) = 0, \text{ for all } c\in\mathbb{R}.$$

In case $\omega_1 =$ or $\omega_2 = 0$, (57) follows immediately from (56). □

Theorem 11. *Let m be an odd integer ≥ 3 of the form (55). Let $\eta(m)$ be as defined in (58), and let R_m be the polynomial given by (14). Then*

$$R_m(y) = \left(m^3y^3 - \frac{3}{4}pm\eta^2(m)y + \nu_p\right)^{s_p}, \tag{59}$$

with

$$\nu_p = \begin{cases} \frac{1}{8}(-1)^{\frac{\omega_2-\omega_1}{2}}p\eta^3(m)L, & \text{if } \omega_2-\omega_1 \text{ is even };\\ \frac{3\sqrt{3}}{8}(-1)^{\frac{\omega_2-\omega_1-1}{2}}p\eta^3(m)M, & \text{if } \omega_2-\omega_1 \text{ is odd,}\end{cases} \tag{60}$$

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

Proof. From (18), we have

$$\begin{aligned} R_m(y) &= \prod_{l=0}^{2}\left(my+A_m(\theta^{g^l})\right)^{s_p}\\ &= \left(m^3y^3+m^2\nu_p''y^2+m\nu_p'y+\nu_p\right)^{s_p}, \end{aligned} \tag{61}$$

where

$$\nu_p'' = A_m(\theta)+A_m(\theta^g)+A_m(\theta^{g^2}), \tag{62}$$

$$\nu'_p = A_m(\theta)A_m(\theta^g) + A_m(\theta)A_m(\theta^{g^2}) + A_m(\theta^g)A_m(\theta^{g^2}) \tag{63}$$

and

$$\nu_p = A_m(\theta)A_m(\theta^g)A_m(\theta^{g^2}). \tag{64}$$

Recall that cf. Theorem 2, δ is the unique integer in $\{0,1,2\}$ such that $m \in O(g^\delta)$. So that from (11)-(13) and (17), we get for $i \in \{0,1,2\}$

$$A_m(\theta^{g^i}) = \sum_{h=0}^{2} \alpha_h(m) T_{\delta-h+i}. \tag{65}$$

Computation of ν''_p.
From (65) and (62) we deduce that

$$\nu''_p = \Big(\alpha_0(m) + \alpha_1(m) + \alpha_2(m)\Big)\Big(T_0 + T_1 + T_2\Big).$$

Since $\gcd(m,p) = 1$ and $m \neq 1$, it follows immediately from (12) and (19) that

$$\alpha_0(m) + \alpha_1(m) + \alpha_2(m) = \sum_{d \,|\, \widetilde{m}} \mu(d) = 0 \tag{66}$$

and thus $\nu''_p = 0$.
Computation of ν'_p.
From (61), to prove (59) it suffices to show (60) and that $\nu'_p = \frac{-3}{4}p\eta^2(m)$. By (63) and (65), we have

$$\nu'_p = \sum_{k=0}^{2}\sum_{h=0}^{k} \alpha_h(m)\alpha_k(m) U(h,k)$$

with

$$U(h,h) = \sum_{(i,j)\in\{(0,1),(0,2),(1,2)\}} T_{\delta-h+i}T_{\delta-h+j}$$

and, for $h < k$,

$$U(h,k) = \sum_{(i,j)\in\{(0,1),(0,2),(1,2)\}} \left(T_{\delta-h+i}T_{\delta-k+j} + T_{\delta-k+i}T_{\delta-h+j}\right).$$

Observing that, for $0 \leq \delta, h, k \leq 2$, $U(h,k)$ does not depend on δ and is equal to $T_0T_1 + T_0T_2 + T_1T_2$ when $h = k$ and to $T_0T_1 + T_0T_2 + T_1T_2 + T_0^2 + T_1^2 + T_2^2$ when $h < k$, we obtain

$$\nu'_p = \beta(m)\Big(T_0^2 + T_1^2 + T_2^2\Big) + \beta'(m)\Big(T_0T_1 + T_0T_2 + T_1T_2\Big), \tag{67}$$

where

$$\beta(m) = \alpha_0(m)\alpha_1(m) + \alpha_0(m)\alpha_2(m) + \alpha_1(m)\alpha_2(m)$$

and

$$\beta'(m) = \alpha_0^2(m) + \alpha_1^2(m) + \alpha_2^2(m) + \beta(m).$$

From (57), it is easy to check that

$$\beta(m) = -\frac{3}{4}\eta^2(m).$$

By (66), we find that

$$\begin{aligned}\beta'(m) &= \left(\sum_{i=0}^{2} \alpha_i(m)\right)^2 - 2\beta(m) + \beta(m)\\ &= -\beta(m)\\ &= \frac{3}{4}\eta^2(m).\end{aligned}$$

On the other hand, using (17), we get

$$T_0^2 + T_1^2 + T_2^2 = \left(\sum_{k=0}^{s_p-1} \theta^{2^k}\right)^2 + \left(\sum_{k=0}^{s_p-1} \theta^{2^k g}\right)^2 + \left(\sum_{k=0}^{s_p-1} \theta^{2^k g^2}\right)^2.$$

The first sum in the last equality is, by (49), equal to

$$\begin{aligned}T_0^2 &= \sum_{0\le k,k'\le s_p-1} \theta^{2^k+2^{k'}}\\ &= \ell_{0,0}T_0 + \ell_{1,0}T_1 + \ell_{2,0}T_2 + s_p. \qquad (68)\end{aligned}$$

Similarly, for the second and third sums, we obtain

$$\begin{aligned}T_1^2 &= \sum_{0\le k,k'\le s_p-1} \theta^{2^k g+2^{k'} g}\\ &= \ell_{0,0}T_1 + \ell_{1,0}T_2 + \ell_{2,0}T_0 + s_p \qquad (69)\end{aligned}$$

and

$$\begin{aligned}T_2^2 &= \sum_{0\le k,k'\le s_p-1} \theta^{2^k g^2+2^{k'} g^2}\\ &= \ell_{0,0}T_2 + \ell_{1,0}T_0 + \ell_{2,0}T_1 + s_p. \qquad (70)\end{aligned}$$

Consequently,

$$T_0^2 + T_1^2 + T_2^2 = 3s_p + (\ell_{0,0} + \ell_{1,0} + \ell_{2,0})(T_0 + T_1 + T_2).$$

So that, by (22) and (37), we get

$$\begin{aligned}T_0^2 + T_1^2 + T_2^2 &= 3s_p - (s_p - 1)\\ &= 2s_p + 1. \qquad (71)\end{aligned}$$

Therefore, with the use of (67), (36) and the fact that $s_p = \frac{p-1}{3}$, we obtain

$$\nu'_p = -\frac{3}{4}p\eta^2(m).$$

Computation of ν_p.
By (64) and (65), we obtain

$$\nu_p = \sum_{h,k,t\in\{0,1,2\}} \alpha_h(m)\alpha_k(m)\alpha_t(m)T_{\delta-h}T_{\delta-k+1}T_{\delta-t+2}$$

and by observing the 27 terms of the expansion of the above sum, we find that

$$\begin{aligned}\nu_p &= \gamma_1(m)\Big(T_0T_1^2 + T_1T_2^2 + T_2T_0^2\Big) + \gamma_2(m)\Big(T_0T_2^2 + T_1T_0^2 + T_2T_1^2\Big)\\ &\quad +\gamma_3(m)\Big(T_0^3 + T_1^3 + T_2^3\Big) + \gamma_4(m)T_0T_1T_2, \qquad (72)\end{aligned}$$

where

$$\gamma_1(m) = \alpha_0^2(m)\alpha_1(m) + \alpha_0(m)\alpha_2^2(m) + \alpha_1^2(m)\alpha_2(m), \qquad (73)$$

$$\gamma_2(m) = \alpha_0^2(m)\alpha_2(m) + \alpha_0(m)\alpha_1^2(m) + \alpha_1(m)\alpha_2^2(m), \qquad (74)$$

$$\gamma_3(m) = \alpha_0(m)\alpha_1(m)\alpha_2(m) \qquad (75)$$

and

$$\gamma_4(m) = \alpha_0^3(m) + \alpha_1^3(m) + \alpha_2^3(m) + 3\gamma_3(m). \qquad (76)$$

Using (68)-(70), we get

$$T_0^3 = \ell_{0,0}T_0^2 + \ell_{1,0}T_0T_1 + \ell_{2,0}T_0T_2 + s_pT_0,$$

$$T_1^3 = \ell_{0,0}T_1^2 + \ell_{1,0}T_1T_2 + \ell_{2,0}T_0T_1 + s_pT_1$$

and

$$T_2^3 = \ell_{0,0}T_2^2 + \ell_{1,0}T_0T_2 + \ell_{2,0}T_1T_2 + s_pT_2.$$

Therefore,

$$\begin{aligned}T_0^3 + T_1^3 + T_2^3 &= s_p\Big(T_0 + T_1 + T_2\Big) + \ell_{0,0}\Big(T_0^2 + T_1^2 + T_2^2\Big)\\ &\quad +(\ell_{1,0} + \ell_{2,0})\Big(T_0T_1 + T_0T_2 + T_1T_2\Big).\end{aligned}$$

So that, from (37), (71) and (36) , we get

$$T_0^3 + T_1^3 + T_2^3 = -s_p + \ell_{0,0}(2s_p + 1) - (\ell_{1,0} + \ell_{2,0})s_p,$$

which, by (22), gives

$$\begin{aligned} T_0^3+T_1^3+T_2^3 &= \ell_{0,0}(3s_p+1)-s_p^2 \\ &= p\ell_{0,0}-s_p^2. \end{aligned} \tag{77}$$

Similarly, by again using (68)-(70), we obtain

$$T_0^2T_1+T_0T_2^2+T_1^2T_2 = p\ell_{1,0}-s_p^2 \tag{78}$$

and

$$T_0^2T_2+T_0T_1^2+T_1T_2^2 = p\ell_{2,0}-s_p^2. \tag{79}$$

Using (73)-(75) and (57), it is easy to show that

$$\gamma_1(m) = \frac{3}{4}\eta^3(m)\cos\left((\omega_2-\omega_1)\frac{\pi}{2}+\frac{4\pi}{3}\right),$$

$$\gamma_2(m) = \frac{3}{4}\eta^3(m)\cos\left((\omega_2-\omega_1)\frac{\pi}{2}+\frac{2\pi}{3}\right)$$

and

$$\gamma_3(m) = \frac{1}{4}\eta^3(m)\cos\left((\omega_2-\omega_1)\frac{\pi}{2}\right).$$

Since, cf. (66), $\alpha_0(m)+\alpha_1(m)+\alpha_2(m)=0$, from (76) we find that

$$\gamma_4(m) = -\gamma_1(m)-\gamma_2(m)+3\gamma_3(m).$$

Therefore,

$$\gamma_4(m) = \frac{3}{2}\eta^3(m)\cos\left((\omega_2-\omega_1)\frac{\pi}{2}\right).$$

Note that if w_2-w_1 is even then

$$\gamma_1(m)=\gamma_2(m)=-\frac{3}{2}\gamma_3(m)=-\frac{1}{4}\gamma_4(m)=-\frac{3}{8}\eta^3(m)\,(-1)^{\frac{w_2-w_1}{2}};$$

while if w_2-w_1 is odd then

$$\gamma_1(m)=-\gamma_2(m)=-\frac{3\sqrt{3}}{8}\eta^3(m)(-1)^{\frac{w_2-w_1+1}{2}},\quad \gamma_3(m)=0,\quad \gamma_4(m)=0.$$

For w_2-w_1 even, from (72), (77)-(79) and (28), we get

$$\nu_p = \frac{1}{8}(-1)^{\frac{\omega_2-\omega_1}{2}}p\eta^3(m)\left(9\ell_{2,1}-p-1\right).$$

For w_2-w_1 odd, from (72) and (77)-(79), we get

$$\nu_p = \frac{3\sqrt{3}}{8}(-1)^{\frac{\omega_2-\omega_1+1}{2}}p\eta^3(m)(\ell_{1,0}-\ell_{2,0}).$$

By (29), (32) and (33), we have

$$\ell_{1,0}-\ell_{2,0}=-M.$$

Lastly, for w_2-w_1 even (resp. odd), (60) follows from (53) (resp. the last equality). □

Example: $p = 43$**.**
As an explicit example, let us consider the case $p = 43$. Then

$$1 + z^{43} = (1 + z)P_1(z)P_2(z)P_3(z),$$

where $P_1(z) = z^{14} + z^{12} + z^{10} + z^7 + z^4 + z^2 + 1$, $P_2(z) = z^{14} + z^{11} + z^{10} + z^9 + z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + 1$ and $P_3(z) = z^{14} + z^{13} + z^{11} + z^7 + z^3 + z + 1$ are the only irreducible polynomials over $\mathbb{F}_2[z]$ of order 43. For $1 \leq l \leq 3$, let $\mathcal{A}(P_l)$ be the unique set defined by (3). For $m \geq 1$, let $\mathcal{A}(P_l)_m$ denote the set of the elements of $\mathcal{A}(P_l)$ of the form $2^k m$. We give bellow the description of the sets $\mathcal{A}(P_l)_1$ and $\mathcal{A}(P_l)_3$; $1 \leq l \leq 3$.
Since $p = 43$ then $g = 3$ is a generator of the cyclic group $(\mathbb{Z}/43\mathbb{Z})^*$. Let L and M be the unique integers satisfying $4p = 172 = L^2 + 27M^2$, $L \equiv 1 \pmod 3$ and $(g^2)^{(p-1)/3} = (3^2)^{14} \equiv \frac{L+9M}{L-9M} \pmod{43}$. Hence, $L = -8$, $M = -2$, $R_1(y) = (y^3 - y^2 - 14y - 8)^{14}$ and $R_3(y) = (27y^3 - 129y + 86)^{14}$.
By using the function polrootspadic of PARI, the 2−adic expansions of the zeros of the polynomial $R_1(y)$ are
$2^2 + 2^3 + 2^6 + 2^{10} + 2^{13} + 2^{17} + 2^{18} + 2^{20} + 2^{22} + 2^{25} + 2^{27} + 2^{29} + 2^{30} + 2^{32} + 2^{33} + 2^{36} + \cdots$
$2 + 2^4 + 2^6 + 2^7 + 2^{10} + 2^{15} + 2^{16} + 2^{19} + 2^{20} + 2^{23} + 2^{26} + 2^{27} + 2^{31} + 2^{34} + 2^{35} + \cdots$
$1 + 2 + 2^5 + 2^6 + 2^7 + 2^9 + 2^{10} + 2^{12} + 2^{14} + 2^{20} + 2^{24} + 2^{27} + \cdots$
and the 2−adic expansions of the zeros of the polynomial $R_3(y)$ are
$1+2^2+2^3+2^4+2^6+2^7+2^{12}+2^{17}+2^{18}+2^{19}+2^{20}+2^{21}+2^{25}+2^{27}+2^{31}+2^{32}+2^{35}+2^{36}+\cdots$
$1 + 2^2 + 2^5 + 2^7 + 2^{10} + 2^{13} + 2^{14} + 2^{19} + 2^{20} + 2^{22} + 2^{23} + 2^{24} + 2^{25} + 2^{27} + 2^{29} + 2^{34} + \cdots$
$2+2^2+2^3+2^4+2^5+2^6+2^9+2^{11}+2^{15}+2^{16}+2^{19}+2^{21}+2^{22}+2^{23}+2^{24}+2^{27}+2^{30}+2^{33}+\cdots$.
After computing some first few elements of the sets $\mathcal{A}(P_l)$, we deduce that
$\mathcal{A}(P_1)_1 = \{2, 2^4, 2^6, 2^7, 2^{10}, 2^{15}, 2^{16}, 2^{19}, 2^{20}, 2^{23}, 2^{26}, 2^{27}, 2^{31}, 2^{34}, 2^{35}, \ldots\}$
$\mathcal{A}(P_2)_1 = \{2^2, 2^3, 2^6, 2^{10}, 2^{13}, 2^{17}, 2^{18}, 2^{20}, 2^{22}, 2^{25}, 2^{27}, 2^{29}, 2^{30}, 2^{32}, 2^{33}, 2^{36}, \ldots\}$
$\mathcal{A}(P_3)_1 = \{1, 2, 2^5, 2^6, 2^7, 2^9, 2^{10}, 2^{12}, 2^{14}, 2^{20}, 2^{24}, 2^{27}, \ldots\}$.
$\mathcal{A}(P_1)_3 = \{2.3, 2^2.3, 2^3.3, 2^4.3, 2^5.3, 2^6.3, 2^9.3, 2^{11}.3, 2^{15}.3, 2^{16}.3, 2^{19}.3, 2^{21}.3, 2^{22}.3, 2^{23}.3, 2^{24}.3, \ldots\}$
$\mathcal{A}(P_2)_3 = \{3, 2^2.3, 2^3.3, 2^4.3, 2^6.3, 2^7.3, 2^{12}.3, 2^{17}.3, 2^{18}.3, 2^{19}.3, 2^{20}.3, 2^{21}.3, 2^{25}.3, 2^{27}.3, 2^{31}.3, \ldots\}$
$\mathcal{A}(P_3)_3 = \{3, 2^2.3, 2^5.3, 2^7.3, 2^{10}.3, 2^{13}.3, 2^{14}.3, 2^{19}.3, 2^{20}.3, 2^{22}.3, 2^{23}.3, 2^{24}.3, 2^{25}.3, 2^{27}.3, 2^{29}.3, \ldots\}$.

6 Acknowledgments

We are pleased to thank professors F. Ben Saïd, F. Morain, C. Delaunay and J.- L. Nicolas for valuable comments and helpful discussions. We also would like to thank the referees for their valuable remarks that help to improve the initial version of this paper.

References

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

[2] N. Baccar and F. Ben Saïd, On sets such that the partition function is even from a certain point on, *Internat. J. Number Theory* **5** (2009), 1–22.

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

[4] F. Ben Saïd, On some sets with even valued partition function, *Ramanujan J.* **9** (2005), 63–75.

[5] F. Ben Saïd and J.-L. Nicolas, Even partition functions, *Séminaire Lotharingien de Combinatoire* (http//www.mat.univie.ac.at/ slc/), **46** (2002), B 46i.

[6] F. Ben Saïd, J.-L. Nicolas and A. Zekraoui, On the parity of generalised partition function III, to appear in *J. Théorie Nombres Bordeaux*.

[7] F. Ben Saïd, H. Lahouar and J.-L. Nicolas, On the counting function of the sets of parts such that the partition function takes even values for n large enough, *Discrete Math.* **306** (2006), 1115–1125.

[8] S. A. Katre, Jacobsthal sums in terms of quadratic partitions of a prime. In K. Alladi, editor, *Number Theory*, volume 1122 of *Lecture Notes in Math.*, Springer-Verlag, 1985, pp. 153–162.

[9] M. Mignotte, *Mathématiques pour le Calcul Formel,* Presses Universitaires de France, 1989.

[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] H. S. Wilf, *Generatingfunctionology*, Academic Press, Second Edition, 1994.

2000 *Mathematics Subject Classification*: Primary 11P83; Secondary 11B50, 11D88, 11G20.
Keywords: Partitions, periodic sequences, order of a polynomial, cyclotomic polynomials, resultant, 2-adic integers, elliptic curves.

Received July 16 2009; revised version received December 23 2009. Published in *Journal of Integer Sequences*, December 31 2009.

Return to Journal of Integer Sequences home page.