Polyadic codes of prime power length II

Anuradha Sharma* and Gurmeet K. Bakshi†
Centre for Advanced Study in Mathematics
Panjab University, Chandigarh 160014, India

Abstract

Let $m \geq 2$ be an integer and let G be a finite Abelian group of order p^n, where p is an odd prime and n is a positive integer. In this paper, the necessary and sufficient conditions for the existence of an m-adic splitting of G, and hence for the existence of polyadic codes (as ideals in an Abelian group algebra) of length p^n, are derived. An algorithm to write down all the m-adic splittings of G is also given. This generalizes the results of Ling & Xing [9] and of Sharma, Bakshi & Raka [14].

Keywords : group algebra, Abelian group algebra codes, cyclotomic classes.
2000 Mathematics Subject Classification : 94B15.

1. Introduction

Let G be a finite Abelian group, written additively, of order $|G|$. Let F_q be the finite field of order q with $\gcd(q, |G|) = 1$. Let $\mathrm{F}_q[G]$ be the group algebra of G over F_q. The elements of $\mathrm{F}_q[G]$ are formal sums $\sum_{g\in G}\alpha_g Y^g$, $\alpha_g \in \mathrm{F}_q$, with addition and multiplication defined as follows :

$$\sum_{g\in G}\alpha_g Y^g + \sum_{g\in G}\beta_g Y^g = \sum_{g\in G}(\alpha_g + \beta_g)Y^g$$

and

$$(\sum_{g\in G}\alpha_g Y^g)(\sum_{h\in G}\beta_h Y^h) = \sum_{k\in G}(\sum_{\substack{g+h=k\\ g,h\in G}}\alpha_g\beta_h)Y^k.$$

Abelian group algebra codes are ideals in the group algebra $\mathrm{F}_q[G]$, which are natural generalizations of cyclic codes and have good error-correcting

*e-mail address: asharma@pu.ac.in
†Corresponding author, e-mail address: gkbakshi@yahoo.com

properties. The motivation behind the study of non-cyclic group algebra codes relies on the fact that many important codes can be realized as ideals of a non-cyclic group algebra. For reference, see [2, 5, 7 & 11].

Quadratic residue codes is a classical family of cyclic codes, which exist for prime lengths only. Quadratic residue codes have been generalized in two directions. Duadic codes defined by Leon, Masley & Pless [8] over binary fields and by Smid [15] over arbitrary fields, triadic codes defined by Pless & Rushanan [12], cyclic polyadic codes and cyclic m-adic residue codes by Brualdi & Pless [3] are generalizations of quadratic residue codes. All these generalizations belong to the family of cyclic codes. In another direction, quadratic residue codes have been generalized to generalized quadratic residue codes by Camion [4] and developed further by van Lint & MacWilliams [10]. They are defined as ideals in Abelian group algebras. Rushanan [13] defined duadic codes as ideals in an Abelian group algebra setting, which are generalized to split group codes by Ding, Kohel & Ling [6]. Analogous to cyclic m-adic residue codes, a generalization of duadic codes in an Abelian group algebra setting was given by Ward & Zhu [16]. The idea of polyadic codes was revisited by Ling & Xing [9] to include non-cyclic Abelian codes.

The necessary and sufficient conditions for the existence of polyadic codes of prime length p was given by Brualdi & Pless [3]. Ling & Xing [9] studied the necessary and sufficient conditions for the existence of polyadic codes, which arise from a restricted kind of splittings. The necessary and sufficient conditions for the existence of cyclic polyadic codes of prime power length was given by Sharma, Bakshi & Raka [14]. Extending [14], in this paper, we give the necessary and sufficient conditions for the existence of Abelian polyadic codes of prime power length p^n, where p is an odd prime and n is a positive integer.

The organization of this paper is as follows : In Section 2, we give a brief background of Abelian group algebra codes on the lines we shall follow. We also include the definition of polyadic codes (in terms of an m-adic splitting of G) as ideals in the Abelian group algebra $\mathrm{F}_q[G]$, which is given by Ling & Xing [9]. In Section 3, we compute q-cyclotomic classes in G when G is an Abelian group of order p^n, where p is an odd prime and n is a positive integer. In Section 4, we answer the following three natural questions:

Q 1: For what values of m, does G admit a non-trivial m-adic splitting?

Q 2: For a given value of m, what are the possible multipliers a_* w.r.t. which G admits a non-trivial m-adic splitting?

Q 3: For a given m and a given multiplier a_*, how to write down all possible non-trivial m-adic splittings of G w.r.t. a_*?

We give the necessary and sufficient conditions for the existence of Abelian polyadic codes of length p^n, where p is an odd prime and n is a positive integer (see Theorems 2 & 3). We also give an algorithm to write down all possible non-trivial m-adic splittings of G.

2. Some Preliminaries

Let $\mathrm{F}_q[G]$ be the group algebra of a finite Abelian group G over the field F_q with q elements. We assume that $\gcd(q, |G|) = 1$. Let the exponent of G be N and let E be an extension of F_q containing a primitive Nth root of unity ζ. Let $G^* = \mathrm{Hom}(G, E^*)$, where E^* is the multiplicative group of E. The set G^* of all the characters of G is an Abelian group under pointwise multiplication given by

$$(\chi_1\chi_2)(g) = \chi_1(g)\chi_2(g) \quad \text{for all} \quad g \in G, \ \chi_1, \chi_2 \in G^*.$$

It is well known that $G \overset{\phi}{\cong} G^*$. We see below little more explicitly, how the elements of G and G^* correspond under ϕ.

By the fundamental theorem of finite Abelian groups,

$$G \cong \mathrm{Z}/n_1\mathrm{Z} \oplus \mathrm{Z}/n_2\mathrm{Z} \oplus \cdots \oplus \mathrm{Z}/n_t\mathrm{Z}, \quad n_i \geq 2.$$

For $x = (x_1, x_2, \cdots, x_t) \in G$, define $\chi_x : G \to E^*$ by $(g_1, g_2, \cdots, g_t) \mapsto \zeta^{\sum_{i=1}^{t} \frac{g_i x_i N}{n_i}}$. One can check that $\chi_x \in G^*$ and the mapping $\phi : G \to G^*$ defined by $x \mapsto \chi_x$ is an isomorphism, and we say that the character χ_x corresponds to the element x in G. Further, any character $\chi \in G^*$ extends to an F_q-algebra homomorphism $\chi : \mathrm{F}_q[G] \to E$ given by

$$\chi(\sum_{g \in G} \alpha_g Y^g) = \sum_{g \in G} \alpha_g \chi(g).$$

By a q-cyclotomic class of $x \in G$, we mean the set $C_x = \{x, qx, q^2x, \cdots, q^{s-1}x\}$, where s is the least positive integer such that $q^s x = x$ in G. The q-cyclotomic class C_x in G corresponds to the q-cyclotomic class $C_{\chi_x} = \{\chi_x, \chi_{xq}, \chi_{xq^2}, \cdots, \chi_{xq^{s-1}}\}$ in G^* under ϕ. It is known that each ideal in $\mathrm{F}_q[G]$ corresponds uniquely to a union of q-cyclotomic classes in G^*, which is described as follows :

Given an ideal $\mathcal{C}$ in $\mathrm{F}_q[G]$, the set

$$R(\mathcal{C}) = \{\chi \in G^* : \chi(c) = 0 \quad \text{for all} \quad c \in \mathcal{C}\}$$

is called the root set of $\mathcal{C}$. It can be verified that $R(\mathcal{C})$ is a union of q-

cyclotomic classes in G^*. Conversely, given any union, say $\cup_{x\in I} C_{\chi_x}$, there is an ideal in $\mathrm{F}_q[G]$ whose root set is $\cup_{x\in I} C_{\chi_x}$. For reference, see [11, Ch. 9].

We next recall the definition of polyadic codes as given by Ling & Xing [9].

Under the componentwise multiplication, denoted by $*$, $G = \oplus_{i=1}^{t} \mathrm{Z}/n_i\mathrm{Z}$ is also a ring with unity. We denote this ring by R. Thus G is the underlying Abelian group of R.

For a unit $a \in R$, the map $a_* : R \to R$ defined as $a_*(x) = a * x$ for every $x \in R$, is called a multiplier.

For an integer $m \geq 2$ and a unit $a \in R$, an m-adic splitting of G w.r.t. the multiplier a_* is an $(m+1)$-tuple $(X_\infty, X_0, X_1, \cdots, X_{m-1})$ such that
(i) each of the sets $X_\infty, X_0, X_1, \cdots, X_{m-1}$ is a union of q-cyclotomic classes of G ;
(ii) $X_\infty, X_0, X_1, \cdots, X_{m-1}$ form a partition of G, i.e.,

$$G = X_\infty \cup X_0 \cup X_1 \cup \cdots \cup X_{m-1} \quad \text{(a disjoint union)};$$

(iii) $a_*(X_\infty) = X_\infty$ and $a_*(X_i) = X_{i+1}$ for $0 \leq i \leq m-1$, where the subscripts are taken modulo m.

We say that G admits an m-adic splitting if there exists an m-adic splitting of G w.r.t. some a_*.

Note that $0 \in G$ always lies in X_∞. Let $X'_\infty = X_\infty \setminus \{0\}$. Associated with an m-adic splitting of G, the four families of codes having root sets as $\{\chi_x : x \in X_\infty \cup X_i\}$, $\{\chi_x : x \in X'_\infty \cup X_i\}$, $\{\chi_x : x \in (X_\infty \cup X_i)^c\}$ and $\{\chi_x : x \in (X'_\infty \cup X_i)^c\}$ for $0 \leq i \leq m-1$, are called polyadic codes in $\mathrm{F}_q[G]$.

Since polyadic codes are defined in terms of an m-adic splitting of G, the problem of existence of polyadic codes in $\mathrm{F}_q[G]$ is equivalent to the existence of an m-adic splitting of G. In the following sections, we explore the existence of an m-adic splitting of G when G is a finite Abelian group of order p^n, where p is an odd prime and n is a positive integer.

3. q-cyclotomic classes in G

Let G be a finite Abelian group of order p^n, where p is an odd prime and n is a positive integer. G can be written as

$$G = \mathrm{Z}/p^{n_1}\mathrm{Z} \oplus \mathrm{Z}/p^{n_2}\mathrm{Z} \oplus \cdots \oplus \mathrm{Z}/p^{n_k}\mathrm{Z},$$

where $n = n_1 + n_2 + \cdots + n_k$ with $n_1 \geq n_2 \geq \cdots \geq n_k \geq 1$.

For a non-zero k-tuple $(\ell_1, \ell_2, \cdots, \ell_k)$, $0 \leq \ell_i \leq n_i$ $(1 \leq i \leq k)$, define

$$G_{\ell_1 \ell_2 \cdots \ell_k} = G_{\ell_1} \oplus G_{\ell_2} \oplus \cdots \oplus G_{\ell_k},$$

where G_{ℓ_i} is a reduced residue system modulo p^{ℓ_i}. It is clear that $G_{\ell_1\ell_2\cdots\ell_k}$ is a group under componentwise multiplication $*$. Since $\gcd(p,q)=1$, $q \in G_{\ell_i}$ for all i. Therefore the k-tuple $(q,q,\cdots,q) \in G_{\ell_1\ell_2\cdots\ell_k}$. Let $Q_{\ell_1\ell_2\cdots\ell_k}$ be the subgroup of $G_{\ell_1\ell_2\cdots\ell_k}$ generated by the k-tuple $(q,q,\cdots,q)$. Clearly $Q_{\ell_1\ell_2\cdots\ell_k}$ has order $O_{p^{\ell_t}}(q)$, where $O_{p^{\ell_t}}(q)$ denotes the multiplicative order of q modulo p^{ℓ_t} with $\ell_t = \max\{\ell_1,\ell_2,\cdots,\ell_k\}$.

For any $a \in G$ and a subset H of G, let

$$a * H = \{a * h : h \in H\}.$$

Let g be a primitive root modulo p^k for all positive integers k. Such a g always exists. For reference, see [1, Ch. 10].

Theorem 1. All the distinct non-zero q-cyclotomic classes in G are given by $a * Q_{\ell_1\ell_2\cdots\ell_k}$ for $0 \le \ell_i \le n_i$ $(1 \le i \le k)$, where for each non-zero k-tuple $(\ell_1,\ell_2,\cdots,\ell_k)$, a runs over the set $(p^{n_1-\ell_1},p^{n_2-\ell_2},\cdots,p^{n_k-\ell_k}) * S_{\ell_1\ell_2\cdots\ell_k}$ with $S_{\ell_1\ell_2\cdots\ell_k}$ defined as the following set :

$$\left\{ (g^{i_{\ell_1}},g^{i_{\ell_2}},\cdots,g^{i_{\ell_k}}) : \begin{array}{l} 0 \le i_{\ell_j} \le \phi(p^{\ell_j}) - 1 \text{ for } 1 \le j \le k,\ j \ne t \text{ and} \\ 0 \le i_{\ell_t} \le \frac{\phi(p^{\ell_t})}{O_{p^{\ell_t}}(q)} - 1,\ \ell_t = \max\{\ell_1,\ell_2,\cdots,\ell_k\} \end{array} \right\}.$$

This result follows as a consequence of the following two lemmas :

Lemma 1. For a non-zero k-tuple $(\ell_1,\ell_2,\cdots,\ell_k)$, let $S_{\ell_1\ell_2\cdots\ell_k}$ be a set of representatives of the distinct cosets of $Q_{\ell_1\ell_2\cdots\ell_k}$ in $G_{\ell_1\ell_2\cdots\ell_k}$. Then all the distinct non-zero q-cyclotomic classes in G are given by $a * Q_{\ell_1\ell_2\cdots\ell_k}$ for $0 \le \ell_i \le n_i$ $(1 \le i \le k)$, where for each non-zero k-tuple $(\ell_1,\ell_2,\cdots,\ell_k)$, a runs over the set $(p^{n_1-\ell_1},p^{n_2-\ell_2},\cdots,p^{n_k-\ell_k}) * S_{\ell_1\ell_2\cdots\ell_k}$.

Proof. Note that

$$G \setminus \{0\} = \bigcup (p^{n_1-\ell_1},p^{n_2-\ell_2},\cdots,p^{n_k-\ell_k}) * G_{\ell_1\ell_2\cdots\ell_k}, \tag{1}$$

where the union is over all the non-zero k-tuples $(\ell_1,\ell_2,\cdots,\ell_k)$, $0 \le \ell_i \le n_i$ $(1 \le i \le k)$. Further for each non-zero k-tuple $(\ell_1,\ell_2,\cdots,\ell_k)$, we have

$$G_{\ell_1\ell_2\cdots\ell_k} = \bigcup_{b \in S_{\ell_1\ell_2\cdots\ell_k}} b * Q_{\ell_1\ell_2\cdots\ell_k}, \tag{2}$$

as $S_{\ell_1\ell_2\cdots\ell_k}$ is a set of representatives of the distinct cosets of $Q_{\ell_1\ell_2\cdots\ell_k}$ in $G_{\ell_1\ell_2\cdots\ell_k}$. Observe that both the unions in (1) and (2) are disjoint and $(p^{n_1-\ell_1},p^{n_2-\ell_2},\cdots,p^{n_k-\ell_k}) * b * Q_{\ell_1\ell_2\cdots\ell_k}$ is a q-cyclotomic class in G containing $(p^{n_1-\ell_1},p^{n_2-\ell_2},\cdots,p^{n_k-\ell_k}) * b$. Therefore all the distinct non-zero q-cyclotomic classes in G are given by $(p^{n_1-\ell_1},p^{n_2-\ell_2},\cdots,p^{n_k-\ell_k}) * b *$

$Q_{\ell_1\ell_2\cdots\ell_k}$ for $0 \le \ell_i \le n_i$ $(1 \le i \le k)$, $(\ell_1, \ell_2, \cdots, \ell_k) \neq 0$, where b runs over the set $S_{\ell_1\ell_2\cdots\ell_k}$ for each non-zero k-tuple $(\ell_1, \ell_2, \cdots, \ell_k)$. This proves the lemma. □

Lemma 2. For a non-zero k-tuple $(\ell_1, \ell_2, \cdots, \ell_k)$ with $\ell_t = \max\{\ell_1, \ell_2, \cdots, \ell_k$ all the representatives of the distinct cosets of $Q_{\ell_1\ell_2\cdots\ell_k}$ in $G_{\ell_1\ell_2\cdots\ell_k}$ are given by

$$S_{\ell_1\ell_2\cdots\ell_k} = \left\{ (g^{i_{\ell_1}}, g^{i_{\ell_2}}, \cdots, g^{i_{\ell_k}}) : \begin{array}{l} 0 \le i_{\ell_j} \le \phi(p^{\ell_j}) - 1 \text{ for } 1 \le j \le k,\ j \neq t \\ \text{and } \ 0 \le i_{\ell_t} \le \frac{\phi(p^{\ell_t})}{O_{p^{\ell_t}}(q)} - 1 \end{array} \right.$$

Proof. To prove this lemma, it is enough to prove that $(g^{i_{\ell_1}}, g^{i_{\ell_2}}, \cdots, g^{i_{\ell_k}}) * Q_{\ell_1\ell_2\cdots\ell_k}$ with $0 \le i_{\ell_j} \le \phi(p^{\ell_j}) - 1$ for $1 \le j \le k$, $j \neq t$ and $0 \le i_{\ell_t} \le \frac{\phi(p^{\ell_t})}{O_{p^{\ell_t}}(q)} - 1$, are all the distinct cosets of $Q_{\ell_1\ell_2\cdots\ell_k}$ in $G_{\ell_1\ell_2\cdots\ell_k}$.

Suppose, if possible, that there exist i_{ℓ_j}, i'_{ℓ_j} $(1 \le j \le k)$ with $0 \le i_{\ell_j}, i'_{\ell_j} \le \phi(p^{\ell_j}) - 1$ $(1 \le j \le k,\ j \neq t)$ and $0 \le i_{\ell_t}, i'_{\ell_t} \le \frac{\phi(p^{\ell_t})}{O_{p^{\ell_t}}(q)} - 1$, satisfying

$$(g^{i_{\ell_1}}, g^{i_{\ell_2}}, \cdots, g^{i_{\ell_k}}) * Q_{\ell_1\ell_2\cdots\ell_k} = (g^{i'_{\ell_1}}, g^{i'_{\ell_2}}, \cdots, g^{i'_{\ell_k}}) * Q_{\ell_1\ell_2\cdots\ell_k}.$$

Then there exists an integer u such that $(g^{i_{\ell_1}}, g^{i_{\ell_2}}, \cdots, g^{i_{\ell_k}}) * (q^u, q^u, \cdots, q^u) = (g^{i'_{\ell_1}}, g^{i'_{\ell_2}}, \cdots, g^{i'_{\ell_k}})$, which gives

$$g^{i_{\ell_j} - i'_{\ell_j}} q^u \equiv 1 \pmod{p^{\ell_j}} \quad \text{for} \quad 1 \le j \le k. \tag{3}$$

For each j, $1 \le j \le k$, g is a primitive root modulo p^{ℓ_j}. Therefore there exists an integer r_j such that

$$q \equiv g^{r_j} \pmod{p^{\ell_j}} \quad \text{for} \quad 1 \le j \le k. \tag{4}$$

For $1 \le j \le k$, we note that

$$\frac{\phi(p^{\ell_j})}{O_{p^{\ell_j}}(q)} \quad \text{divides} \quad r_j \quad \text{and} \tag{5}$$

$$r_t \equiv r_j \pmod{\phi(p^{\ell_j})}. \tag{5}'$$

From (3) and (4), we have

$$g^{i_{\ell_j} - i'_{\ell_j} + ur_j} \equiv 1 (\text{mod } p^{\ell_j}),$$

which gives

$$i_{\ell_j} - i'_{\ell_j} + ur_j \equiv 0 \pmod{\phi(p^{\ell_j})} \quad \text{for} \quad 1 \le j \le k. \tag{6}$$

In particular, for $j = t$, we have

$$i_{\ell_t} - i'_{\ell_t} + ur_t \equiv 0 \pmod{\phi(p^{\ell_t})}.$$

From (5), we have $\frac{\phi(p^{\ell_t})}{O_{p^{\ell_t}}(q)}$ divides r_t, which implies that $\frac{\phi(p^{\ell_t})}{O_{p^{\ell_t}}(q)}$ divides $i_{\ell_t} - i'_{\ell_t}$. This gives $i_{\ell_t} = i'_{\ell_t}$, as $0 \le i_{\ell_t},\ i'_{\ell_t} \le \frac{\phi(p^{\ell_t})}{O_{p^{\ell_t}}(q)} - 1$. This further gives $ur_t \equiv 0 \pmod{\phi(p^{\ell_t})}$, which, by (5)', implies that $ur_j \equiv 0 \pmod{\phi(p^{\ell_j})}$ for $1 \le j \le k$. This gives, by (6), that $i_{\ell_j} - i'_{\ell_j} \equiv 0 \pmod{\phi(p^{\ell_j})}$ for $1 \le j \le k,\ j \ne t$. This implies that $i_{\ell_j} = i'_{\ell_j}$, as $0 \le i_{\ell_j}, i'_{\ell_j} \le \phi(p^{\ell_j}) - 1$ for every $j \ne t,\ 1 \le j \le k$.

Moreover, these are all the distinct cosets of $Q_{\ell_1\ell_2\cdots\ell_k}$ in $G_{\ell_1\ell_2\cdots\ell_k}$. This is because

$$\begin{aligned} &\sum_{\substack{i_{\ell_j}=0 \\ 1\le j\le k,\ j\ne t}}^{\phi(p^{\ell_j})-1} \sum_{i_{\ell_t}=0}^{\frac{\phi(p^{\ell_t})}{O_{p^{\ell_t}}(q)}-1} |(g^{i_{\ell_1}}, g^{i_{\ell_2}}, \cdots, g^{i_{\ell_k}}) * Q_{\ell_1\ell_2\cdots\ell_k}| \\ &= \sum_{\substack{i_{\ell_j}=0 \\ 1\le j\le k,\ j\ne t}}^{\phi(p^{\ell_j})-1} \sum_{i_{\ell_t}=0}^{\frac{\phi(p^{\ell_t})}{O_{p^{\ell_t}}(q)}-1} |Q_{\ell_1\ell_2\cdots\ell_k}| = \prod_{j=1}^{k} \phi(p^{\ell_j}). \end{aligned}$$ □

4. Existence of an m-adic splitting of G

By a non-trivial m-adic splitting of G, we mean an m-adic splitting $(X_\infty, X_0, X_1, \cdots, X_{m-1})$ with $X_0 \ne \Phi$.

For $b \in G_{\ell_1\ell_2\cdots\ell_k}$, let $H_b^{(\ell_1\ell_2\cdots\ell_k)}$ be the subgroup of $G_{\ell_1\ell_2\cdots\ell_k}/Q_{\ell_1\ell_2\cdots\ell_k}$, generated by the coset $b * Q_{\ell_1\ell_2\cdots\ell_k}$, of order $|H_b^{(\ell_1\ell_2\cdots\ell_k)}|$.

For an integer $m \ge 2$ and a unit $a \in R$, we define an m-adic splitting of $G_{\ell_1\ell_2\cdots\ell_k}$ w.r.t. a_* to be an $(m+1)$-tuple $(Y_\infty, Y_0, Y_1, \cdots, Y_{m-1})$ such that
(i) each of the sets $Y_\infty, Y_0, Y_1, \cdots, Y_{m-1}$ is a union of cosets of $Q_{\ell_1\ell_2\cdots\ell_k}$ in $G_{\ell_1\ell_2\cdots\ell_k}$;
(ii) $G_{\ell_1\ell_2\cdots\ell_k} = Y_\infty \cup Y_0 \cup Y_1 \cup \cdots \cup Y_{m-1}$ as a disjoint union ;
(iii) $a_*(Y_\infty) = Y_\infty$ and $a_*(Y_i) = Y_{i+1}$ for $0 \le i \le m-1$, where the subscripts are taken modulo m.

The following proposition relates m-adic splitting of G w.r.t. a_* to those of $G_{\ell_1\ell_2\cdots\ell_k}$.

Proposition 1. G admits an m-adic splitting $(X_\infty, X_0, X_1, \cdots, X_{m-1})$ w.r.t a_* if and only if each $G_{\ell_1\ell_2\ldots\ell_k}$ admits an m-adic splitting $(X_\infty^{(\ell_1\ell_2\cdots\ell_k)}, X_0^{(\ell_1\ell_2\cdots\ell_k)}, X_1^{(\ell_1\ell_2\cdots\ell_k)}, \cdots, X_{m-1}^{(\ell_1\ell_2\cdots\ell_k)})$ w.r.t. a_*. Moreover,

$$X'_\infty = \bigcup_{\substack{0\le\ell_i\le n_i\ (1\le i\le k)\\(\ell_1,\ell_2,\cdots\ell_k)\neq 0}} (p^{n_1-\ell_1}, p^{n_2-\ell_2}, \cdots, p^{n_k-\ell_k}) * X_\infty^{(\ell_1\ell_2\cdots\ell_k)},$$

$$X_j = \bigcup_{\substack{0\le\ell_i\le n_i\ (1\le i\le k)\\(\ell_1,\ell_2,\cdots\ell_k)\neq 0}} (p^{n_1-\ell_1}, p^{n_2-\ell_2}, \cdots, p^{n_k-\ell_k}) * X_j^{(\ell_1\ell_2\cdots\ell_k)}$$

for $0 \le j \le m-1$.

Further if $(X_\infty, X_0, X_1, \cdots, X_{m-1})$ is non-trivial, then $(X_\infty^{(\ell_1\ell_2\cdots\ell_k)}, X_0^{(\ell_1\ell_2\cdots\ell_k)}, X_1^{(\ell_1\ell_2\cdots\ell_k)}, \cdots, X_{m-1}^{(\ell_1\ell_2\cdots\ell_k)})$ is non-trivial for some $(\ell_1, \ell_2, \cdots \ell_k)$ and vice versa.

Proof. Let $(X_\infty, X_0, X_1, \cdots, X_{m-1})$ be an m-adic splitting of G w.r.t. a_*. For a non-zero k-tuple $(\ell_1, \ell_2, \cdots, \ell_k)$, define $X_\infty^{(\ell_1\ell_2\cdots\ell_k)}$ as the union of all those $b*Q_{\ell_1\ell_2\cdots\ell_k} \in G_{\ell_1\ell_2\cdots\ell_k}/Q_{\ell_1\ell_2\cdots\ell_k}$ such that $(p^{n_1-\ell_1}, p^{n_2-\ell_2}, \cdots, p^{n_k-\ell_k})$, $b*Q_{\ell_1\ell_2\cdots\ell_k} \subseteq X'_\infty$ and for $0 \le j \le m-1$, define $X_j^{(\ell_1\ell_2\cdots\ell_k)}$ as the union of all those $b*Q_{\ell_1\ell_2\cdots\ell_k} \in G_{\ell_1\ell_2\cdots\ell_k}/Q_{\ell_1\ell_2\cdots\ell_k}$ such that $(p^{n_1-\ell_1}, p^{n_2-\ell_2}, \cdots, p^{n_k-$ $b*Q_{\ell_1\ell_2\cdots\ell_k} \subseteq X_j$.
It is clear that

$$\begin{aligned} X'_\infty &= \bigcup_{\substack{0\le\ell_i\le n_i\ (1\le i\le k)\\(\ell_1,\ell_2,\cdots\ell_k)\neq 0}} (p^{n_1-\ell_1}, p^{n_2-\ell_2}, \cdots, p^{n_k-\ell_k}) * X_\infty^{(\ell_1\ell_2\cdots\ell_k)}, \\ X_j &= \bigcup_{\substack{0\le\ell_i\le n_i\ (1\le i\le k)\\(\ell_1,\ell_2,\cdots\ell_k)\neq 0}} (p^{n_1-\ell_1}, p^{n_2-\ell_2}, \cdots, p^{n_k-\ell_k}) * X_j^{(\ell_1\ell_2\cdots\ell_k)} \end{aligned} \tag{7}$$

for $0 \le j \le m-1$.
We assert that $(X_\infty^{(\ell_1\ell_2\cdots\ell_k)}, X_0^{(\ell_1\ell_2\cdots\ell_k)}, X_1^{(\ell_1\ell_2\cdots\ell_k)}, \cdots, X_{m-1}^{(\ell_1\ell_2\cdots\ell_k)})$ is an m-adic splitting of $G_{\ell_1\ell_2\ldots\ell_k}$ w.r.t. a_* for each non-zero k-tuple $(\ell_1, \ell_2, \cdots \ell_k)$. We have

$$G \setminus \{0\} = \bigcup_{\substack{0\le\ell_i\le n_i\ (1\le i\le k)\\(\ell_1,\ell_2,\cdots\ell_k)\neq 0}} (p^{n_1-\ell_1}, p^{n_2-\ell_2}, \cdots, p^{n_k-\ell_k}) * G_{\ell_1\ell_2\cdots\ell_k}. \tag{8}$$

From (7) and (8), it follows that

$$\bigcup_{\substack{0\le\ell_i\le n_i(1\le i\le k)\\(\ell_1,\ell_2,\cdots\ell_k)\neq 0}} (p^{n_1-\ell_1}, p^{n_2-\ell_2}, \cdots, p^{n_k-\ell_k}) * (X_\infty^{(\ell_1\ell_2\cdots\ell_k)} \cup X_0^{(\ell_1\ell_2\cdots\ell_k)} \ldots \cup X_{m-1}^{(\ell_1\ell_2\cdots\ell_k}$$

$$= G \setminus \{0\} = \bigcup_{\substack{0 \le \ell_i \le n_i \ (1 \le i \le k) \\ (\ell_1, \ell_2, \cdots \ell_k) \neq 0}} (p^{n_1 - \ell_1}, p^{n_2 - \ell_2}, \cdots, p^{n_k - \ell_k}) * G_{\ell_1 \ell_2 \cdots \ell_k}. \qquad (9)$$

But for each non-zero k-tuple $(\ell_1, \ell_2, \cdots, \ell_k)$, the union $X_\infty^{(\ell_1 \ell_2 \cdots \ell_k)} \cup X_0^{(\ell_1 \ell_2 \cdots \ell_k)} \cup X_1^{(\ell_1 \ell_2 \cdots \ell_k)} \cup \cdots \cup X_{m-1}^{(\ell_1 \ell_2 \cdots \ell_k)}$ is contained in $G_{\ell_1 \ell_2 \cdots \ell_k}$ and the unions on both sides of (9) are disjoint. So we obtain $X_\infty^{(\ell_1 \ell_2 \cdots \ell_k)} \cup X_0^{(\ell_1 \ell_2 \cdots \ell_k)} \cup X_1^{(\ell_1 \ell_2 \cdots \ell_k)} \cdots \cup X_{m-1}^{(\ell_1 \ell_2 \cdots \ell_k)} = G_{\ell_1 \ell_2 \cdots \ell_k}$ for each non-zero k-tuple $(\ell_1, \ell_2, \cdots, \ell_k)$.
Now to prove the assertion, it remains to prove that $a_*(X_\infty^{(\ell_1 \ell_2 \cdots \ell_k)}) = X_\infty^{(\ell_1 \ell_2 \cdots \ell_k)}$ and $a_*(X_j^{(\ell_1 \ell_2 \cdots \ell_k)}) = X_{j+1}^{(\ell_1 \ell_2 \cdots \ell_k)}$ for $0 \le j \le m-1$, where the subscripts are taken modulo m.
For $0 \le j \le m-1$, we have $a_*(X_j) = X_{j+1}$. Using (7), we get

$$\bigcup_{\substack{0 \le \ell_i \le n_i \ (1 \le i \le k) \\ (\ell_1, \ell_2, \cdots \ell_k) \neq 0}} a * (p^{n_1 - \ell_1}, p^{n_2 - \ell_2}, \cdots, p^{n_k - \ell_k}) * X_j^{(\ell_1 \ell_2 \cdots \ell_k)}$$

$$= \bigcup_{\substack{0 \le \ell_i \le n_i \ (1 \le i \le k) \\ (\ell_1, \ell_2, \cdots \ell_k) \neq 0}} (p^{n_1 - \ell_1}, p^{n_2 - \ell_2}, \cdots, p^{n_k - \ell_k}) * X_{j+1}^{(\ell_1 \ell_2 \cdots \ell_k)}. \qquad (10)$$

But for each $(\ell_1, \ell_2, \cdots, \ell_k)$, the set $a*(p^{n_1 - \ell_1}, p^{n_2 - \ell_2}, \cdots, p^{n_k - \ell_k}) * X_j^{(\ell_1 \ell_2 \cdots \ell_k)}$ is contained in $a_*(X_j) \cap \left((p^{n_1 - \ell_1}, p^{n_2 - \ell_2}, \cdots, p^{n_k - \ell_k}) * G_{\ell_1 \ell_2 \cdots \ell_k}\right)$, which is equal to the set $X_{j+1} \cap \left((p^{n_1 - \ell_1}, p^{n_2 - \ell_2}, \cdots, p^{n_k - \ell_k}) * G_{\ell_1 \ell_2 \cdots \ell_k}\right)$
$= (p^{n_1 - \ell_1}, p^{n_2 - \ell_2}, \cdots, p^{n_k - \ell_k}) * X_{j+1}^{(\ell_1 \ell_2 \cdots \ell_k)}$. Also the unions on both sides of (10) are disjoint, so it follows that $a_*(X_j^{(\ell_1 \ell_2 \cdots \ell_k)}) = X_{j+1}^{(\ell_1 \ell_2 \cdots \ell_k)}$ for $0 \le j \le m-1$.
Similarly, it can be seen that $a_*(X_\infty^{(\ell_1 \ell_2 \cdots \ell_k)}) = X_\infty^{(\ell_1 \ell_2 \cdots \ell_k)}$, which completes the proof of the assertion.
The converse is clear. □

In the next proposition, we give a method to write down all possible non-trivial m-adic splittings of $G_{\ell_1 \ell_2 \ldots \ell_k}$ w.r.t. a_*, provided they exist.

Proposition 2. Let $(Y_\infty, Y_0, Y_1, \cdots, Y_{m-1})$ be a non-trivial m-adic splitting of $G_{\ell_1 \ell_2 \ldots \ell_k}$ w.r.t. a_* and let C be a set of coset representatives of $H_a^{(\ell_1 \ell_2 \cdots \ell_k)}$ in $G_{\ell_1 \ell_2 \ldots \ell_k} / Q_{\ell_1 \ell_2 \ldots \ell_k}$. Then
(i) m divides $|H_a^{(\ell_1 \ell_2 \cdots \ell_k)}|$.
(ii) there exists a non-empty subset D of C and for each $b \in D$, there exists an integer t_b such that

$$
\begin{aligned}
Y_\infty &= \bigcup_{b\in C\setminus D} b * H_a^{(\ell_1\ell_2\cdots\ell_k)},\\
Y_0 &= \bigcup_{b\in D} a^{t_b} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)},\\
Y_1 &= \bigcup_{b\in D} a^{t_b+1} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)},\\
\cdots &\quad \cdots\cdots\\
Y_{m-1} &= \bigcup_{b\in D} a^{t_b+m-1} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)}
\end{aligned}
$$

and conversely.

Proof. Let $C = \{b_1, b_2, \cdots, b_u\}$. Then

$$G_{\ell_1\ell_2\ldots\ell_k}/Q_{\ell_1\ell_2\ldots\ell_k} = b_1 * H_a^{(\ell_1\ell_2\cdots\ell_k)} \cup b_2 * H_a^{(\ell_1\ell_2\cdots\ell_k)} \cup \cdots \cup b_u * H_a^{(\ell_1\ell_2\cdots\ell_k)}.$$

It is easy to see that each of the cosets $b_i * H_a^{(\ell_1\ell_2\cdots\ell_k)}$ is either contained in Y_∞ or is disjoint with Y_∞. Let $D = \{b_i \in C : b_i * H_a^{(\ell_1\ell_2\cdots\ell_k)}$ is disjoint with Y_∞ Since the splitting is non-trivial, $D \neq \Phi$. Now let $b \in D$. Then $b * H_a^{(\ell_1\ell_2\cdots\ell_k)} \subseteq Y_0 \cup Y_1 \cup \cdots \cup Y_{m-1}$. In particular, $b * Q_{\ell_1\ell_2\cdots\ell_k} \subseteq Y_j$ for some j, $0 \leq j \leq m-1$. Let $t_b = m - j$. Then we have

$$b * H_a^{(\ell_1\ell_2\cdots\ell_k)} = a^{t_b} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)} \cup a^{t_b+1} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)} \cup \cdots \cup a^{t_b+m-1} * b * H_{a^m}^{(\ell_1\ell_2\cdots}$$

where $a^{t_b+j} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)} \subseteq Y_j$ and $a_*(a^{t_b+j} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)}) = a^{t_b+j+1} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)}$ for all j, $0 \leq j \leq m-1$. So we obtain that if $b * H_a^{(\ell_1\ell_2\cdots\ell_k)}$ is disjoint with Y_∞, then it splits equally into m parts $a^{t_b} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)}$, $a^{t_b+1} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)}$, $\cdots$ $a^{t_b+m-1} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)}$ that lie in $Y_0, Y_1, \cdots, Y_{m-1}$ respectively, and that each of the parts satisfy $a_*(a^{t_b+j} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)}) = a^{t_b+j+1} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)}$ for all j, $0 \leq j \leq m-1$. Therefore m must divide the cardinality of $b_i * H_a^{(\ell_1\ell_2\cdots\ell_k)}$, which is equal to $|H_a^{(\ell_1\ell_2\cdots\ell_k)}|$. Also we have

$$
\begin{aligned}
Y_\infty &= \bigcup_{b\in C\setminus D} b * H_a^{(\ell_1\ell_2\cdots\ell_k)},\\
Y_0 &= \bigcup_{b\in D} a^{t_b} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)},\\
Y_1 &= \bigcup_{b\in D} a^{t_b+1} * b * H_{a^m}^{(\ell_1\ell_2\cdots\ell_k)},\\
\cdots &\quad \cdots\cdots
\end{aligned}
$$

$$Y_{m-1} = \bigcup_{b \in D} a^{t_b+m-1} * b * H_{a^m}^{(\ell_1 \ell_2 \cdots \ell_k)}.$$

Proof of the converse is an easy verification. This proves the proposition. □

In the next theorem, we find the necessary and sufficient conditions for the existence of a non-trivial m-adic splitting of G, which completely answers Q 1 posed in the introduction.

Theorem 2. G admits a non-trivial m-adic splitting if and only if m divides either $\dfrac{\phi(p^{n_1})}{O_{p^{n_1}}(q)}$ or $\phi(p^{n_2})$.

Proof. Suppose that G admits a non-trivial m-adic splitting w.r.t. a_*. By Proposition 1, there exist $\ell_1, \ell_2, \cdots, \ell_k$ for which $G_{\ell_1 \ell_2 \cdots \ell_k}$ admits a non-trivial m-adic splitting w.r.t. a_*. By Proposition 2, m must divide $|H_a^{(\ell_1 \ell_2 \cdots \ell_k)}|$. But $|H_a^{(\ell_1 \ell_2 \cdots \ell_k)}|$ divides $|H_a^{(n_1 n_2 \cdots n_k)}|$, which implies that m is a divisor of $|H_a^{(n_1 n_2 \cdots n_k)}|$.

To prove the theorem, it is enough to prove that $|H_a^{(n_1 n_2 \cdots n_k)}|$ divides either $\dfrac{\phi(p^{n_1})}{O_{p^{n_1}}(q)}$ or $\phi(p^{n_2})$.

Now $|H_a^{(n_1 n_2 \cdots n_k)}|$ is the least positive integer L satisfying

$$a^L * Q_{n_1 n_2 \cdots n_k} = Q_{n_1 n_2 \cdots n_k}. \tag{11}$$

As a is a unit in R, a is of the form $(g^{i_1}, g^{i_2}, \cdots, g^{i_k})$ for some non-negative integers $i_1, i_2, \cdots, i_k$. Thus (11) becomes

$$(g^{i_1}, g^{i_2}, \cdots, g^{i_k})^L * Q_{n_1 n_2 \cdots n_k} = Q_{n_1 n_2 \cdots n_k}.$$

That is, $|H_a^{(n_1 n_2 \cdots n_k)}|$ is the least positive integer L satisfying

$$(g^{i_1 L}, g^{i_2 L}, \cdots, g^{i_k L}) * (q^u, q^u, \cdots, q^u) = (1, 1, \cdots, 1) \text{ for some integer } u,$$

which is equivalent to saying that L is the least positive integer for which there exists an integer u satisfying

$$g^{i_j L} q^u \equiv 1 (\text{mod } p^{n_j}) \text{ for all } j,\ 1 \le j \le k. \tag{12}$$

Write $q \equiv g^{r_j} (\text{mod } p^{n_j})$ for $1 \le j \le k$. Then for $1 \le j \le k$, we note that

$$\frac{\phi(p^{n_j})}{O_{p^{n_j}}(q)} \text{ divides } r_j \text{ and} \tag{13}$$

$$r_j \equiv r_1 (\text{mod } \phi(p^{n_j})). \tag{13}'$$

And (12) can be rewritten as $g^{i_j L + r_j u} \equiv 1 (\text{mod } p^{n_j})$ for $1 \leq j \leq k$, which implies that

$$i_j L + r_j u \equiv 0 (\text{mod } \phi(p^{n_j})) \text{ for } 1 \leq j \leq k. \tag{14}$$

Now the following two cases arise :
I. $i_1 i_2 \cdots i_k \neq 0$ and
II. $i_1 i_2 \cdots i_k = 0$.

Case I. Let $i_1 i_2 \cdots i_k \neq 0$.
From (13) and (14), we have $\dfrac{\phi(p^{n_j})}{O_{p^{n_j}}(q)}$ divides $i_j L$ for all j, $1 \leq j \leq k$. This gives L is divisible by $\text{lcm}_{1 \leq j \leq k} \left[\dfrac{\phi(p^{n_j})/O_{p^{n_j}}(q)}{\gcd\left(i_j, \phi(p^{n_j})/O_{p^{n_j}}(q)\right)} \right] = L'$(say). Also note that

$$(g^{i_1 L'}, g^{i_2 L'}, \cdots, g^{i_k L'}) * Q_{n_1 n_2 \cdots n_k} = Q_{n_1 n_2 \cdots n_k},$$

which implies that L divides L'. Therefore we get

$$|H_a^{(n_1 n_2 \cdots n_k)}| = L = L' = \text{lcm}_{1 \leq j \leq k} \left[\frac{\phi(p^{n_j})/O_{p^{n_j}}(q)}{\gcd\left(i_j, \phi(p^{n_j})/O_{p^{n_j}}(q)\right)} \right], \tag{15}$$

which clearly divides $\dfrac{\phi(p^{n_1})}{O_{p^{n_1}}(q)}$.

Case II. Let $i_1 i_2 \cdots i_k = 0$. Let $S = \{j : 1 \leq j \leq k, i_j \neq 0\}$.
Here (14) becomes

$$\begin{aligned} i_j L + r_j u &\equiv 0 (\text{mod } \phi(p^{n_j})) \text{ for all } j \in S \text{ and} \\ r_\theta u &\equiv 0 (\text{mod } \phi(p^{n_\theta})) \text{ for all } \theta \in S^c, \end{aligned} \tag{14}'$$

(where S^c denotes the complement of S w.r.t. the set $\{1, 2, \cdots, k\}$).
Further, in view of (13)', (14)' implies that

$$\begin{aligned} i_j L + r_1 u &\equiv 0 (\text{mod } \phi(p^{n_j})) \text{ for all } j \in S \text{ and} \\ r_1 u &\equiv 0 (\text{mod } \phi(p^{n_\theta})) \text{ for all } \theta \in S^c, \end{aligned}$$

which further implies that $\gcd\left(\phi(p^{n_j}), \text{lcm}_{\theta \in S^c}[\phi(p^{n_\theta})]\right)$ divides $i_j L$ for all $j \in S$. This gives L is divisible by $\text{lcm}_{j \in S} \left[\dfrac{\gcd\left(\phi(p^{n_j}), \text{lcm}_{\theta \in S^c}[\phi(p^{n_\theta})]\right)}{\gcd\left(i_j, \phi(p^{n_j}), \text{lcm}_{\theta \in S^c}[\phi(p^{n_\theta})]\right)} \right] = L''$(say). Also note that

$$(g^{i_1 L''}, g^{i_2 L''}, \cdots, g^{i_k L''}) * Q_{n_1 n_2 \cdots n_k} = Q_{n_1 n_2 \cdots n_k},$$

which implies that L divides L''. Therefore we get

$$|H_a^{(n_1 n_2 \cdots n_k)}| = L = L'' = \mathrm{lcm}_{j \in S} \left[\frac{\gcd\left(\phi(p^{n_j}), \mathrm{lcm}_{\theta \in S^c}\left[\phi(p^{n_\theta})\right]\right)}{\gcd\left(i_j, \phi(p^{n_j}), \mathrm{lcm}_{\theta \in S^c}\left[\phi(p^{n_\theta})\right]\right)} \right], \quad (16)$$

which is clearly a divisor of $\phi(p^{n_2})$.

Conversely, suppose that m divides either $\dfrac{\phi(p^{n_1})}{O_{p^{n_1}}(q)}$ or $\phi(p^{n_2})$. In view of Propositions 1 & 2, it is enough to produce a unit $a \in R$ and a non-zero k-tuple $(\ell_1, \ell_2, \cdots, \ell_k)$ for which m divides $|H_a^{(\ell_1 \ell_2 \cdots \ell_k)}|$. We shall consider the following two cases separately :

I. m divides $\dfrac{\phi(p^{n_1})}{O_{p^{n_1}}(q)}$ and

II. m divides $\phi(p^{n_2})$.

Case I. Let m divide $\dfrac{\phi(p^{n_1})}{O_{p^{n_1}}(q)}$.

Take $\ell_j = n_j$ $(1 \le j \le k)$ and $a = (g^{i_1}, g^{i_2}, \cdots, g^{i_k})$, where $i_1 = \dfrac{\phi(p^{n_1})}{m O_{p^{n_1}}(q)}$, $i_j = \dfrac{\phi(p^{n_j})}{O_{p^{n_j}}(q)}$ for $2 \le j \le k$. By (15), we get $|H_a^{(n_1 n_2 \cdots n_k)}| = m$.

Case II. Let m divide $\phi(p^{n_2})$.
Take $\ell_j = n_j$ $(1 \le j \le k)$ and $a = (g^{i_1}, g^{i_2}, \cdots, g^{i_k})$, where $i_1 = 0$, $i_2 = \dfrac{\phi(p^{n_2})}{m}$, $i_j = \phi(p^{n_j})$ for $3 \le j \le k$. By (16), we get $|H_a^{(n_1 n_2 \cdots n_k)}| = m$.
This completes the proof. □

Let $e = \frac{p-1}{O_p(q)}$ and write $q^{\frac{p-1}{e}} = 1 + p^d c$, where $p \nmid c$, $d \ge 1$. It is clear that $O_{p^{n_1}}(q) = \left(\frac{p-1}{e}\right) p^{\max\{0,\ n_1 - d\}}$, which gives $\dfrac{\phi(p^{n_1})}{O_{p^{n_1}}(q)} = e p^{\min\{n_1 - 1,\ d-1\}}$.

Remark 1. It is clear from the proof of Theorem 2 that
(i) when the multiplier is of the kind a_*, where $a = (g^{i_1}, g^{i_2}, \cdots, g^{i_k})$ with $i_1 i_2 \cdots i_k \neq 0$, then m must be a divisor of $\dfrac{\phi(p^{n_1})}{O_{p^{n_1}}(q)} = e p^{\min\{n_1 - 1,\ d-1\}}$.
(ii) when the multiplier is of the kind a_*, where $a = (g^{i_1}, g^{i_2}, \cdots, g^{i_k})$ with $i_1 i_2 \cdots i_k = 0$, then m must be a divisor of $\phi(p^{n_2})$.

Remark 2. Since $G_{n_1 n_2 \cdots n_k}$ is the unit group of R, so by Lemma 2, it is enough to consider m-adic splittings w.r.t. the multipliers $(g^{i_1}, g^{i_2}, \cdots, g^{i_k})_*$, where $0 \le i_1 \le \dfrac{\phi(p^{n_1})}{O_{p^{n_1}}(q)} - 1 = e p^{\min\{n_1 - 1,\ d-1\}} - 1$, $0 \le i_j \le \phi(p^{n_j}) - 1$

for $2 \leq j \leq k$.

Definition. Let $m \geq 2$ be an integer and let $a \in G_{n_1 n_2 \cdots n_k}$. Write $m = m' p^{\lambda}$, where $p \nmid m'$ and λ is a non-negative integer, and also write $a = (g^{i_1}, g^{i_2}, \cdots, g^{i_k})$ for some non-negative integers $i_1, i_2, \cdots, i_k$. Let β_j be the highest power of p dividing i_j for $1 \leq j \leq k$. We say that m and a are compatible if either the conditions

(i) $i_1 i_2 \cdots i_k \neq 0$,

(ii) $\gcd(i_1, i_2, \cdots, i_k, e)$ divides $\frac{e}{m'}$ and

(iii) in case $\lambda \geq 1$, $\beta_j \leq \min\{n_j - 1,\ d - 1\} - \lambda$ for some j $(1 \leq j \leq k$

hold, or the conditions

(i)$'$ $i_1 i_2 \cdots i_k = 0$,

(ii)$'$ $\gcd_{j \in S} (\gcd (i_j, p-1))$ divides $\frac{p-1}{m'}$ and

(iii)$'$ in case $\lambda \geq 1$, $\beta_j \leq \min\{n_j - 1, \max_{\theta \in S^c}\{n_\theta - 1\}\} - \lambda$ for some $j \in S$

hold, where $S = \{j : 1 \leq j \leq k, i_j \neq 0\}$ and S^c denotes the complement of S w.r.t. $\{1, 2, \cdots, k\}$.

Remark 3. If m and a are compatible, it can be easily seen that m divides $ep^{\min\{n_1 - 1,\ d-1\}}$ in the case when (i), (ii) and (iii) hold, or m divides $\phi(p^{n_2})$ in the case when (i)$'$, (ii)$'$ and (iii)$'$ hold.

In the next theorem, we give the necessary and sufficient conditions for the existence of a non-trivial m-adic splitting of G w.r.t. a_*, which completely answers Q 2 posed in the introduction.

Theorem 3. *G admits a non-trivial m-adic splitting w.r.t. the multiplier a_* if and only if m and a are compatible.*

Proof. First suppose that G admits a non-trivial m-adic splitting w.r.t. a_*. Write $a = (g^{i_1}, g^{i_2}, \cdots, g^{i_k})$ for some non-negative integers $i_1, i_2, \cdots, i_k$. Working as in Theorem 2, we see that m must divide $|H^{(n_1 n_2 \cdots n_k)}_{(g^{i_1}, g^{i_2}, \cdots, g^{i_k})}|$.

Now the following two cases arise :

I. $i_1 i_2 \cdots i_k \neq 0$ and

II. $i_1 i_2 \cdots i_k = 0$.

To show that m and a are compatible, it is enough to show that (ii) and (iii) hold in the case when $i_1 i_2 \cdots i_k \neq 0$, and that (ii)$'$ and (iii)$'$ hold in

the case when $i_1 i_2 \cdots i_k = 0$.

Case I. Let $i_1 i_2 \cdots i_k \neq 0$. Here, by Remark 1(i), m must be of the type $m'p^\lambda$, where $m' | e$ and $0 \leq \lambda \leq \min\{n_1 - 1, d - 1\}$.
Using (15) and after a little simplification, we see that $|H^{(n_1 n_2 \cdots n_k)}_{(g^{i_1}, g^{i_2}, \cdots, g^{i_k})}|$ is equal to $\frac{e}{\gcd(i_1, i_2, \cdots, i_k, e)} p^{\max_{1 \leq j \leq k}\{\min\{n_j - 1, d-1\} - \min\{\beta_j, \min\{n_j - 1, d-1\}\}\}}$. Thus $m = m'p^\lambda$ divides $|H^{(n_1 n_2 \cdots n_k)}_{(g^{i_1}, g^{i_2}, \cdots, g^{i_k})}|$ if and only if

$$m' \text{ divides } \frac{e}{\gcd(i_1, i_2, \cdots, i_k, e)} \quad \text{and} \tag{17}$$

$$\lambda \leq \max_{1 \leq j \leq k} \{\min\{n_j - 1, d - 1\} - \min\{\beta_j, \min\{n_j - 1, d - 1\}\}\}. \tag{18}$$

But (17) holds if and only if $\gcd(i_1, i_2, \cdots, i_k, e)$ divides $\frac{e}{m'}$, which proves condition (ii).
For $\lambda = 0$, (18) always holds.
Now let $\lambda \geq 1$. We assert that not all $\beta_j' s$ are greater than or equal to $\min\{n_j - 1, d - 1\}$. For if, this is so, then (18) implies that $\lambda \leq 0$, which contradicts our assumption that $\lambda \geq 1$. Thus $\beta_j < \min\{n_j - 1, d - 1\}$ for some j, $1 \leq j \leq k$.
Let $U = \{j : 1 \leq j \leq k, \beta_j < \min\{n_j - 1, d - 1\}\}$. Then (18) becomes

$$1 \leq \lambda \leq \max_{j \in U} \{\min\{n_j - 1, d - 1\} - \beta_j\},$$

which implies that $\beta_j \leq \min\{n_j - 1, d - 1\} - \lambda$ for some $j \in U$. That is, $\beta_j \leq \min\{n_j - 1, d - 1\} - \lambda$ for some j, $1 \leq j \leq k$. This proves condition (iii).

Case II. Let $i_1 i_2 \cdots i_k = 0$. Let $S = \{j : 1 \leq j \leq k, i_j \neq 0\}$. Here, by Remark 1(ii), m must be of the type $m'p^\lambda$, where m' divides $p - 1$ and $0 \leq \lambda \leq n_2 - 1$.
Using (16) and after a little simplification, we get

$$|H^{(n_1 n_2 \cdots n_k)}_{(g^{i_1}, g^{i_2}, \cdots, g^{i_k})}| = \text{lcm}_{j \in S} \left[\frac{p - 1}{\gcd(i_j, p - 1)}\right] p^\mu,$$

where $\mu = \max_{j \in S}\{\min\{n_j - 1, \max_{\theta \in S^c}\{n_\theta - 1\}\} - \min\{\beta_j, \min\{n_j - 1, \max_{\theta \in S^c}\{n_\theta - 1\}\}\}\}$.
Thus $m = m'p^\lambda$ divides $|H^{(n_1 n_2 \cdots n_k)}_{(g^{i_1}, g^{i_2}, \cdots, g^{i_k})}|$ if and only if

$$m' \text{ divides } \text{lcm}_{j \in S} \left[\frac{p - 1}{\gcd(i_j, p - 1)}\right] \quad \text{and} \tag{19}$$

$$\lambda \leq \max_{j\in S}\{\min\{n_j-1, \max_{\theta\in S^c}\{n_\theta-1\}\} - \min\{\beta_j, \min\{n_j-1, \max_{\theta\in S^c}\{n_\theta-1\}\}\}\}.$$

But (19) holds if and only if $\gcd_{j\in S}(\gcd(i_j, p-1))$ divides $\frac{p-1}{m'}$, which proves condition (ii)'.

For $\lambda = 0$, (20) always holds.

Now let $\lambda \geq 1$. We assert that not all β_j's are greater than or equal to $\min\{n_j - 1, \max_{\theta\in S^c}\{n_\theta - 1\}\}$.

For if, this is so, then (20) implies that $\lambda \leq 0$, which contradicts our assumption that $\lambda \geq 1$. Thus $\beta_j < \min\{n_j - 1, \max_{\theta\in S^c}\{n_\theta - 1\}\}$ for some $j \in S$.

Let $T = \{j \in S : \beta_j < \min\{n_j - 1, \max_{\theta\in S^c}\{n_\theta - 1\}\}\}$. Thus (20) can be rewritten as

$$\lambda \leq \max_{j\in T}\{\min\{n_j - 1, \max_{\theta\in S^c}\{n_\theta - 1\}\} - \beta_j\},$$

which implies $\beta_j \leq \min\{n_j - 1, \max_{\theta\in S^c}\{n_\theta - 1\}\} - \lambda$ for some $j \in T$. This gives $\beta_j \leq \min\{n_j - 1, \max_{\theta\in S^c}\{n_\theta - 1\}\} - \lambda$ for some $j \in S$, which proves condition (iii)'.

Conversely, let m and a be compatible. Here, in view of Proposition 1, one needs to produce a non-zero k-tuple $(\ell_1, \ell_2, \cdots, \ell_k)$ such that $G_{\ell_1\ell_2\cdots\ell_k}$ admits a non-trivial m-adic splitting w.r.t. a_*. In fact, in the next theorem, we produce all non-zero k-tuples $(\ell_1, \ell_2, \cdots, \ell_k)$, $0 \leq \ell_i \leq n_i$ $(1 \leq i \leq k)$, such that $G_{\ell_1\ell_2\cdots\ell_k}$ admits a non-trivial m-adic splitting w.r.t. a_*, provided m and a are compatible. □

From now onwards, we assume that $m = m'p^\lambda$ and $a = (g^{i_1}, g^{i_2}, \cdots, g^{i_k})$ are compatible, and we proceed to find all non-zero k-tuples $(\ell_1, \ell_2, \cdots, \ell_k)$, $0 \leq \ell_i \leq n_i$ $(1 \leq i \leq k)$, for which $G_{\ell_1\ell_2\cdots\ell_k}$ admits a non-trivial m-adic splitting w.r.t. a_*.

For a k-tuple $(\ell_1, \ell_2, \cdots, \ell_k)$, define $R_{\ell_1\ell_2\cdots\ell_k} = \{j : 1 \leq j \leq k,\ \ell_j \neq 0\}$.

We fix some notations for the two different cases, $i_1 i_2 \cdots i_k \neq 0$ and $i_1 i_2 \cdots i_k = 0$, separately.

Case I. For $i_1 i_2 \cdots i_k \neq 0$, define

$$B = \{j : 1 \leq j \leq k,\ \beta_j \leq \min\{n_j - 1, d-1\} - \lambda\}.$$

Further, in case $\lambda = 0$, define W as

$$\left\{(\ell_1, \ell_2, \cdots, \ell_k) \neq 0 : \begin{array}{l} 0 \leq \ell_i \leq n_i \ \text{ for } \ 1 \leq i \leq k \ \text{ and} \\ \gcd_{j\in R_{\ell_1\ell_2\cdots\ell_k}} (\gcd(i_j, e)) \ \text{ divides } \ \dfrac{e}{m'}, \end{array}\right\} \qquad (21)$$

and in case $\lambda \geq 1$, define W as

$$\left\{ (\ell_1, \ell_2, \cdots, \ell_k) \neq 0 : \begin{array}{c} 0 \leq \ell_i \leq n_i \ \text{ for } \ 1 \leq i \leq k, \\ \gcd\limits_{j \in R_{\ell_1 \ell_2 \cdots \ell_k}} (\gcd(i_j, e)) \ \text{ divides } \ \dfrac{e}{m'} \\ \text{and } \ \ell_j \geq \lambda + \beta_j + 1 \ \text{ for some } j \in B \end{array} \right\}. \quad (22)$$

Case II. For $i_1 i_2 \cdots i_k = 0$, define

$$B = \{j \in S : \beta_j \leq \min\{n_j - 1, \max_{\theta \in S^c}\{n_\theta - 1\}\} - \lambda\}.$$

Further in case $\lambda = 0$, define W as

$$\left\{ (\ell_1, \ell_2, \cdots, \ell_k) \neq 0 : \begin{array}{c} 0 \leq \ell_i \leq n_i \ (1 \leq i \leq k), \ V_{\ell_1 \ell_2 \cdots \ell_k} \neq \phi, \\ \gcd\limits_{j \in V_{\ell_1 \ell_2 \cdots \ell_k}} (\gcd(i_j, p-1)) \ \text{ divides } \ \dfrac{p-1}{m'} \end{array} \right\} \quad (23)$$

and in case $\lambda \geq 1$, define W as

$$\left\{ (\ell_1, \ell_2, \cdots, \ell_k) \neq 0 : \begin{array}{l} 0 \leq \ell_i \leq n_i \ (1 \leq i \leq k), \ V_{\ell_1 \ell_2 \cdots \ell_k} \neq \phi, \\ \gcd\limits_{j \in V_{\ell_1 \ell_2 \cdots \ell_k}} (\gcd(i_j, p-1)) \ \text{ divides } \ \dfrac{p-1}{m'}, \\ \text{and for some } j \in S \cap B, \\ \beta_j + \lambda \leq \min\{\ell_j - 1, \max\limits_{\theta \in U_{\ell_1 \ell_2 \cdots \ell_k}} \{\ell_\theta - 1\}\} \end{array} \right\}, \quad (24)$$

where $V_{\ell_1 \ell_2 \cdots \ell_k} = S \cap R_{\ell_1 \ell_2 \cdots \ell_k}$ and $U_{\ell_1 \ell_2 \cdots \ell_k} = R_{\ell_1 \ell_2 \cdots \ell_k} \setminus V_{\ell_1 \ell_2 \cdots \ell_k}$ for each $\ell_1, \ell_2, \cdots, \ell_k$.

Note that since m and a are compatible, the sets B and W are non-empty.

Theorem 4. Let m and a be compatible. Then $G_{\ell_1 \ell_2 \cdots \ell_k}$ for $0 \leq \ell_i \leq n_i$ $(1 \leq i \leq k)$, admits a non-trivial m-adic splitting w.r.t. a_* if and only if $(\ell_1, \ell_2, \cdots, \ell_k) \in W$, (where W is as defined by (21),(22), (23) and (24)).

Proof. In view of Proposition 2, we see that $G_{\ell_1 \ell_2 \cdots \ell_k}$ admits a non-trivial m-adic splitting w.r.t. a_* if and only if m divides $|H_a^{(\ell_1 \ell_2 \cdots \ell_k)}|$. We have $a = (g^{i_1}, g^{i_2}, \cdots, g^{i_k})$. Working as in Theorem 2, we find that $|H_{(g^{i_1}, g^{i_2}, \cdots, g^{i_k})}^{(\ell_1 \ell_2 \cdots \ell_k)}|$

is equal to

$$\begin{cases} \operatorname{lcm}_{j\in R_{\ell_1\ell_2\cdots\ell_k}} \left[\dfrac{\phi(p^{\ell_j})/O_{p^{\ell_j}}(q)}{\gcd\left(i_j, \phi(p^{\ell_j})/O_{p^{\ell_j}}(q)\right)}\right] & \text{if } i_1i_2\cdots i_k \neq 0\ ; \\ \operatorname{lcm}_{j\in V_{\ell_1\ell_2\cdots\ell_k}} \left[\dfrac{\gcd\left(\phi(p^{\ell_j}), \operatorname{lcm}_{\theta\in U_{\ell_1\ell_2\cdots\ell_k}}\left[\phi(p^{\ell_\theta})\right]\right)}{\gcd\left(i_j, \phi(p^{\ell_j}), \operatorname{lcm}_{\theta\in U_{\ell_1\ell_2\cdots\ell_k}}\left[\phi(p^{\ell_\theta})\right]\right)}\right] & \text{if } i_1i_2\cdots i_k = 0, \end{cases}$$

which, after a little simplification, gives

$$|H^{(\ell_1\ell_2\cdots\ell_k)}_{(g^{i_1}, g^{i_2}, \cdots, g^{i_k})}| = \begin{cases} \operatorname{lcm}_{j\in R_{\ell_1\ell_2\cdots\ell_k}} \left[\frac{e}{\gcd(i_j,e)}\right] p^{\mu_{\ell_1\ell_2\cdots\ell_k}} & \text{if } i_1i_2\cdots i_k \neq 0\ ; \\ \operatorname{lcm}_{j\in V_{\ell_1\ell_2\cdots\ell_k}} \left[\frac{p-1}{\gcd(i_j,p-1)}\right] p^{\omega_{\ell_1\ell_2\cdots\ell_k}} & \text{if } i_1i_2\cdots i_k = 0, \end{cases}$$

where $\mu_{\ell_1\ell_2\cdots\ell_k}$ is given by

$$\max_{j\in R_{\ell_1\ell_2\cdots\ell_k}} [\min\{\ell_j - 1, d-1\} - \min\{\beta_j, \min\{\ell_j - 1, d-1\}\}]$$

and $\omega_{\ell_1\ell_2\cdots\ell_k}$ is given by

$$\max_{j\in V_{\ell_1\ell_2\cdots\ell_k}} \left[\min\{\ell_j - 1, \max_{\theta\in U_{\ell_1\ell_2\cdots\ell_k}} \{\ell_\theta - 1\}\} - \min\{\beta_j, \min\{\ell_j - 1, \max_{\theta\in U_{\ell_1\ell_2\cdots\ell_k}} \{\ell_\theta -$$

We consider the two cases, $i_1i_2\cdots i_k \neq 0$ and $i_1i_2\cdots i_k = 0$, separately as follows :

Case I. Let $i_1i_2\cdots i_k \neq 0$.

Now $m = m'p^\lambda$ divides $|H^{(\ell_1\ell_2\cdots\ell_k)}_{(g^{i_1}, g^{i_2}, \cdots, g^{i_k})}|$ if and only if m' divides $\operatorname{lcm}_{j\in R_{\ell_1\ell_2\cdots\ell_k}} \left[\frac{e}{\gcd(i_j,e)}\right]$ and $\lambda \leq \mu_{\ell_1\ell_2\cdots\ell_k}$ by (25). Arguing as in Theorem 3, we obtain that this holds if and only if $(\ell_1, \ell_2, \cdots, \ell_k) \in W$.

Case II. Let $i_1i_2\cdots i_k = 0$.
Now $m = m'p^\lambda$ divides $|H^{(\ell_1\ell_2\cdots\ell_k)}_{(g^{i_1}, g^{i_2}, \cdots, g^{i_k})}|$ if and only if m' divides $\operatorname{lcm}_{j\in V_{\ell_1\ell_2\cdots\ell_k}} \left[\frac{p-1}{\gcd(i_j,p-1)}\right]$ and $\lambda \leq \omega_{\ell_1\ell_2\cdots\ell_k}$ by (25). Again arguing as in Theorem 3, we obtain that this holds if and only if $(\ell_1, \ell_2, \cdots, \ell_k) \in W$. □

Using Propositions 1 & 2 and Theorem 4, we get an algorithm to write down all non-trivial m-adic splittings of G w.r.t. a_*.

An algorithm to write down all non-trivial m-adic splittings of G.

Step I. Choose an integer $m \geq 2$ dividing either $\frac{\phi(p^{n_1})}{O_{p^{n_1}}(q)}$ or $\phi(p^{n_2})$.

Step II. Choose $a \in G_{n_1 n_2 \cdots n_k}$ such that m and a are compatible.

Step III. Given m and a, compute the set W in the respective case, as defined by (21) and (22).

Step IV. Using Proposition 2, write all m-adic splittings $(X_\infty^{(\ell_1\ell_2\cdots\ell_k)}, X_0^{(\ell_1\ell_2\cdots\ell_k)}, X_1^{(\ell_1\ell_2\cdots\ell_k)}, \cdots, X_{m-1}^{(\ell_1\ell_2\cdots\ell_k)})$ of $G_{\ell_1\ell_2\cdots\ell_k}$ w.r.t. the multiplier a_* for all $(\ell_1, \ell_2, \cdots, \ell_k) \in W$.

Step V. By Proposition 1, all the non-trivial m-adic splittings of G w.r.t. the multiplier a_* are given by

$$X'_\infty = \bigcup_{\substack{0 \leq \ell_i \leq n_i \ (1 \leq i \leq k) \\ (\ell_1, \ell_2, \cdots \ell_k) \neq 0}} (p^{n_1-\ell_1}, p^{n_2-\ell_2}, \cdots, p^{n_k-\ell_k}) * X_\infty^{(\ell_1\ell_2\cdots\ell_k)},$$

$$X_j = \bigcup_{\substack{0 \leq \ell_i \leq n_i \ (1 \leq i \leq k) \\ (\ell_1, \ell_2, \cdots \ell_k) \neq 0}} (p^{n_1-\ell_1}, p^{n_2-\ell_2}, \cdots, p^{n_k-\ell_k}) * X_j^{(\ell_1\ell_2\cdots\ell_k)}$$

for $0 \leq j \leq m-1$, where $X_\infty^{(\ell_1\ell_2\cdots\ell_k)} = G_{\ell_1\ell_2\cdots\ell_k}$, $X_0^{(\ell_1\ell_2\cdots\ell_k)} = X_1^{(\ell_1\ell_2\cdots\ell_k)} = \cdots = X_{m-1}^{(\ell_1\ell_2\cdots\ell_k)} = \Phi$ for all $(\ell_1, \ell_2, \cdots, \ell_k) \notin W$ and the m-adic splitting $(X_\infty^{(\ell_1\ell_2\cdots\ell_k)}, X_0^{(\ell_1\ell_2\cdots\ell_k)}, X_1^{(\ell_1\ell_2\cdots\ell_k)}, \cdots, X_{m-1}^{(\ell_1\ell_2\cdots\ell_k)})$ is non-trivial for some $(\ell_1, \ell_2, \cdots, \ell_k) \in W$.

To illustrate the algorithm, we give below an example :

An example

Let $G = \mathbb{Z}/7\mathbb{Z} \oplus \mathbb{Z}/7\mathbb{Z}$ and $q = 2$. Here $p = 7$, $n_1 = n_2 = d = 1$, $e = 2$ and $g = 3$. Define $T_{X_0} = \{b \in G_{11} : b * Q_{11} \subseteq X_0\}$. Then we have $X_0 = \bigcup_{b \in T_{X_0}} b * Q_{11}$. Note that an m-adic splitting of G w.r.t. a_* is completely determined by X_0 or T_{X_0}. This is because $X_1 = a_*(X_0)$, $X_2 = a_*^2(X_0)$, $\cdots$ $X_{m-1} = a_*^{m-1}(X_0)$ and $X_\infty = G \setminus (X_0 \cup X_1 \cup \cdots \cup X_{m-1})$. Also the splitting is non-trivial if and only if $T_{X_0} \neq \Phi$.

By Theorem 2, m has exactly three choices, viz 2, 3 and 6. And by Remark 2, it is enough to consider m-adic splittings w.r.t. the multipliers a_*, where a is of the type (g^{i_1}, g^{i_2}), $0 \leq i_1 \leq 1$ and $0 \leq i_2 \leq 5$.

I. Let $m = 2$. Now $m = 2$ and $a = (g^{i_1}, g^{i_2})$ are compatible if and only if either (i) $i_1 i_2 \neq 0$ and $\gcd(i_1, i_2, 2) = 1$
or (ii) $i_1 = 0$ and $\gcd(i_2, 6) = 1$
or (iii) $i_1 = 0$ and $i_2 = 3$

or (iv) $i_1 = 1$ and $i_2 = 0$.

(i) When $m = 2$, $i_1 i_2 \neq 0$ and $\gcd(i_1, i_2, 2) = 1$, we always have $i_1 = 1$ in this case and we need to consider the following sub-cases separately :
(a) Let $i_2 = 1$. Here T_{X_0} equals any non-empty subset of the following set :

$$\{C_1, C_2, C_3, C_4, C_5, C_6, C_7, C_8\},$$

where $C_1 \in \{(1,1),(g,g)\}$, $C_2 \in \{(1,g),(g,g^2)\}$, $C_3 \in \{(1,g^2),(g,g^3)\}$, $C_4 \in \{(1,g^3),(g,g^4)\}$, $C_5 \in \{(1,g^4),(g,g^5)\}$, $C_6 \in \{(1,g^5),(g,1)\}$, $C_7 \in \{(1,0),(g,0)\}$ and $C_8 \in \{(0,1),(0,g)\}$.
(b) Let $i_2 = 2$. Here T_{X_0} equals any non-empty subset of the following set:

$$\{C_1, C_2, C_3\},$$

where $C_1 \in \{\{(1,1),(1,g^2),(1,g^4)\},\{(g,g^2),(g,g^4),(g,1)\}\}$, $C_2 \in \{\{(1,g),(1,g^3),(1,g^5)\},\{(g,g^3),(g,g^5),(g,g)\}\}$ and $C_3 \in \{(1,0),(g,0)\}$.
(c) Let $i_2 = 3$ or 5. Here T_{X_0} equals any non-empty subset of the following set :

$$\{C_1, C_2, C_3, C_4\},$$

where $C_1 \in \{\{(1,1),(1,g^2),(1,g^4)\},\{(g,g),(g,g^3),(g,g^5)\}\}$, $C_2 \in \{\{(1,g),(1,g^3),(1,g^5)\},\{(g,1),(g,g^2),(g,g^4)\}\}$, $C_3 \in \{(1,0),(g,0)\}$ and $C_4 \in \{(0,1),(0,g)\}$.
(d) Let $i_4 = 4$. Here T_{X_0} equals any non-empty subset of the following set :

$$\{C_1, C_2, C_3, C_4, C_5, C_6, C_7\},$$

where $C_1 \in \{(1,1),(g,g^4)\}$, $C_2 \in \{(1,g),(g,g^5)\}$, $C_3 \in \{(1,g^2),(g,1)\}$, $C_4 \in \{(1,g^3),(g,g)\}$, $C_5 \in \{(1,g^4),(g,g^2)\}$, $C_6 \in \{(1,g^5),(g,g^3)\}$ and $C_7 \in \{(1,0),(g,0)\}$.

(ii) When $m = 2$, $i_1 = 0$ and $\gcd(i_2, 6) = 1$, all the non-trivial m-adic splittings of G w.r.t. $(g^{i_1}, g^{i_2})_*$ are given, for $0 \leq i, j, k, \ell \leq 1$, by the following possible choices for T_{X_0} :

$\{(1,g^i),(1,g^{i+2i_2}),(1,g^{i+4i_2}),(g,g^j),(g,g^{j+2i_2}),(g,g^{j+4i_2}),(g^\ell,0),(0,g^k)\}$,
$\{(1,g^i),(1,g^{i+2i_2}),(1,g^{i+4i_2}),(g,g^j),(g,g^{j+2i_2}),(g,g^{j+4i_2}),(g^\ell,0)\}$,
$\{(g,g^j),(g,g^{j+2i_2}),(g,g^{j+4i_2}),(g^\ell,0),(0,g^k)\}$,
$\{(g^\ell,0),(0,g^k),(1,g^i),(1,g^{i+2i_2}),(1,g^{i+4i_2})\}$,
$\{(0,g^k),(1,g^i),(1,g^{i+2i_2}),(1,g^{i+4i_2}),(g,g^j),(g,g^{j+2i_2}),(g,g^{j+4i_2})\}$,
$\{(1,g^i),(1,g^{i+2i_2}),(1,g^{i+4i_2}),(g,g^j),(g,g^{j+2i_2}),(g,g^{j+4i_2})\}$,
$\{(g,g^j),(g,g^{j+2i_2}),(g,g^{j+4i_2}),(g^\ell,0)\}$,
$\{(g^\ell,0),(0,g^k)\}$,
$\{(0,g^k),(1,g^i),(1,g^{i+2i_2}),(1,g^{i+4i_2})\}$,
$\{(1,g^i),(1,g^{i+2i_2}),(1,g^{i+4i_2}),(g^\ell,0)\}$,

$\{(g, g^j), (g, g^{j+2i_2}), (g, g^{j+4i_2}), (0, g^k)\}$,
$\{(1, g^i), (1, g^{i+2i_2}), (1, g^{i+4i_2})\}$,
$\{(g, g^j), (g, g^{j+2i_2}), (g, g^{j+4i_2})\}$,
$\{(g^\ell, 0)\}$,
$\{(0, g^k)\}$.

(iii) When $m = 2$, $i_1 = 1$ and $i_2 = 0$, all the non-trivial m-adic splittings of G w.r.t. $(g^{i_1}, g^{i_2})_*$ are given, for $0 \leq i, j, \ell \leq 1$, by the following possible choices for T_{X_0} :

$\{(g^i, 1), (g^{i+2}, 1), (g^{i+4}, 1), (g^j, g), (g^{j+2}, g), (g^{j+4}, g), (g^\ell, 0)\}$,
$\{(g^i, 1), (g^{i+2}, 1), (g^{i+4}, 1), (g^j, g), (g^{j+2}, g), (g^{j+4}, g)\}$,
$\{(g^j, g), (g^{j+2}, g), (g^{j+4}, g), (g^\ell, 0)\}$,
$\{(g^\ell, 0), (g^i, 1), (g^{i+2}, 1), (g^{i+4}, 1)\}$,
$\{(g^i, 1), (g^{i+2}, 1), (g^{i+4}, 1)\}$,
$\{(g^j, g), (g^{j+2}, g), (g^{j+4}, g)\}$,
$\{(g^\ell, 0)\}$.

(iv) When $m = 2$, $i_1 = 0$ and $i_2 = 3$, T_{X_0} equals any non-empty subset of the following set :

$$\{C_1, C_2, C_3, C_4, C_5, C_6, C_7, \},$$

where $C_1 \in \{(1,1), (1, g^3)\}$, $C_2 \in \{(1, g), (1, g^4)\}$, $C_3 \in \{(1, g^2), (1, g^5)\}$, $C_4 \in \{(g, 1), (g, g^3)\}$, $C_5 \in \{(g, g), (g, g^4)\}$, $C_6 \in \{(g, g^2), (g, g^5)\}$ and $C_7 \in \{(0, 1), (0, g)\}$.

II. Let $m = 3$. Now $m = 3$ and $a = (g^{i_1}, g^{i_2})$ are compatible if and only if either (i) $i_1 = 0$ and $\gcd(i_2, 6) = 1$
or (ii) $i_1 = 0$ and $\gcd(i_2, 6) = 2$
or (iii) $i_1 = 1$ and $i_2 = 0$.

(i) When $m = 3$, $i_1 = 0$ and $\gcd(i_2, 6) = 1$, all the non-trivial m-adic splittings of G w.r.t. $(g^{i_1}, g^{i_2})_*$ are given, for $0 \leq i, j \leq 2$, by the following possible choices for T_{X_0} :

$\{(1, g^i), (1, g^{i+3i_2}), (g, g^j), (g, g^{j+3i_2})\}$,
$\{(1, g^i), (1, g^{i+3i_2})\}$,
$\{(g, g^j), (g, g^{j+3i_2})\}$.

(ii) When $m = 3$, $i_1 = 0$ and $\gcd(i_2, 6) = 2$, all the non-trivial m-adic splittings of G w.r.t. $(g^{i_1}, g^{i_2})_*$ are given, for $0 \leq i, j \leq 2$ and $k, \ell \equiv 1 \pmod 2$, by the following possible choices for T_{X_0} :

$$\{(1, g^{2i}), (1, g^{2i+\ell}), (g, g^{2j}), (g, g^{2j+k})\},$$

$$\{(1,g^{2i}),(1,g^{2i+\ell}),(g,g^{2j})\},$$
$$\{(1,g^{2i+\ell}),(g,g^{2j}),(g,g^{2j+k})\},$$
$$\{(g,g^{2j}),(g,g^{2j+k}),(1,g^{2i})\},$$
$$\{(g,g^{2j+k}),(1,g^{2i}),(1,g^{2i+\ell})\},$$
$$\{(1,g^{2i}),(1,g^{2i+\ell})\},$$
$$\{(1,g^{2i+\ell}),(g,g^{2j})\},$$
$$\{(g,g^{2j}),(g,g^{2j+k})\},$$
$$\{(g,g^{2j+k}),(1,g^{2i})\},$$
$$\{(1,g^{2i}),(g,g^{2j})\},$$
$$\{(1,g^{2i+\ell}),(g,g^{2j+k})\},$$
$$\{(1,g^{2i})\},$$
$$\{(1,g^{2i+\ell})\},$$
$$\{(g,g^{2j})\},$$
$$\{(g,g^{2j+k})\}.$$

(iii) When $m=3$, $i_1=1$ and $i_2=0$, all the non-trivial m-adic splittings of G w.r.t. $(g^{i_1},g^{i_2})_*$ are given, for $0\le i,j\le 2$, by the following possible choices for T_{X_0} :

$$\{(g^i,1),(g^{i+3},1),(g^j,g),(g^{j+3},g)\},$$
$$\{(g^i,1),(g^{i+3},1)\},$$
$$\{(g^j,g),(g^{j+3},g)\}.$$

III. Let $m=6$. Now $m=6$ and $a=(g^{i_1},g^{i_2})$ are compatible if and only if
either (i) $i_1=0$ and $\gcd(i_2,6)=1$
or (ii)$i_1=1$ and $i_2=0$.
(i) When $m=6$, $i_1=0$ and $\gcd(i_2,6)=1$, all the non-trivial m-adic splittings of G w.r.t. $(g^{i_1},g^{i_2})_*$ are given, for $0\le i,j\le 5$, by the following possible choices for T_{X_0} :

$$\{(1,g^i),(g,g^j)\},$$
$$\{(1,g^i)\},$$
$$\{(g,g^j)\}.$$

(ii) When $m=6$, $i_1=1$ and $i_2=0$, all the non-trivial m-adic splittings of G w.r.t. $(g^{i_1},g^{i_2})_*$ are given, for $0\le i,j\le 5$, by the following possible choices for T_{X_0} :

$$\{(g^i,1),(g^j,g)\},$$
$$\{(g^i,1)\},$$
$$\{(g^j,g)\}.$$

References

1. T. M. Apostol, Introduction to analytic number theory, Undergraduate Texts in Mathematics. Springer-Verlag, New York-Heidelberg (1976).

2. S. D. Berman, On the theory of group codes, Cybernatics 3 (1967) 25-31.

3. R. A. Brualdi & V. S. Pless, Polyadic codes, Discrete Appl. Math. 25 (1989) no. 1-2, 3–17.

4. P. Camion, Global quadratic Abelian codes, Information Theory CISM Courses and Lectures no. 219, G. Longo, ed., Springer, Vienna (1975) 293-310.

5. P. Charpin, The Reed-Solomon code as ideals in a modular algebra, C. R. Acad. Sci. Paris, Ser. I. Math. 294 (1982) 597-600.

6. C. Ding, D. R. Kohel & S. Ling, Split group codes, IEEE Trans. Inform. Theory 46 (2000) no. 2, 485–495.

7. R. E. Evans & S. J. Lomonaco, Metacyclic error-correcting codes, AAECC6 (1995) 191-210.

8. J. S. Leon, J. M. Masley & V. Pless, Duadic codes, IEEE Trans. Inform. Theory 30 (1984) no. 5, 709–714.

9. S. Ling & C. Xing, Polyadic codes revisited, IEEE Trans. Inform. Theory 50 (2004) no. 1, 200–207.

10. J. H. van Lint & F. J. MacWilliams, Generalized quadratic residue codes, IEEE Trans. Inform. Theory 24 (1978) no. 6, 730–737.

11. V. S. Pless & W. C. Huffman, Handbook of Coding Theory, Volume I, Elsevier North-Holland (1998).

12. V. Pless & J. J. Rushanan, Triadic codes, Linear Algebra Appl. 98 (1988) 415–433.

13. J. J. Rushanan, Duadic codes and difference sets, J. Combin. Theory Ser A 57 (1991) 254-261.

14. A. Sharma, G. K. Bakshi & M. Raka, Polyadic codes of prime power length, Finite Fields and their Appl. 13 (2007) 1071- 1085.

15. M. H. M. Smid, Duadic codes, IEEE Trans. Inform. Theory 33 (1987) no. 3, 432–433.

16. H. N. Ward & L. Zhu, Existence of abelian group code partitions, J. Combin. Theory Ser. A 67 (1994) no. 2, 276–281.