Combinatorica (2024) 44:393–416
https://doi.org/10.1007/s00493-023-00076-x

ORIGINAL PAPER

A Group Ring Approach to Fuglede's Conjecture in Cyclic Groups

Tao Zhang[1]

Received: 16 March 2023 / Revised: 8 October 2023 / Accepted: 29 October 2023 /
Published online: 27 November 2023

Abstract

Fuglede's conjecture states that a subset $\Omega \subseteq \mathbb{R}^n$ with positive and finite Lebesgue measure is a spectral set if and only if it tiles $\mathbb{R}^n$ by translation. However, this conjecture does not hold in both directions for $\mathbb{R}^n$, $n \geq 3$. While the conjecture remains unsolved in $\mathbb{R}$ and $\mathbb{R}^2$, cyclic groups are instrumental in its study within $\mathbb{R}$. This paper introduces a new tool to study spectral sets in cyclic groups and, in particular, proves that Fuglede's conjecture holds in $\mathbb{Z}_{p^n qr}$.

Keywords Fuglede's conjecture · Tile · Spectral set · Group ring

Mathematics Subject Classification 05B45 · 52C22 · 42B05 · 43A40

1 Introduction

A bounded measurable subset $\Omega \subseteq \mathbb{R}^n$ with $\mu(\Omega) > 0$ is called spectral, if there is a subset $\Lambda \subseteq \mathbb{R}^n$ such that the set of exponential functions $\{e_\lambda(x)\}_{\lambda \in \Lambda}$ is a complete orthogonal basis, where $e_\lambda(x) = e^{2\pi i \langle \lambda, x \rangle}$. In this case, Λ is called the spectrum of Ω, and (Ω, Λ) is called a spectral pair in $\mathbb{R}^n$.

A subset $A \subseteq \mathbb{R}^n$ tiles $\mathbb{R}^n$ by translation, if there is a set $T \subseteq \mathbb{R}^n$ such that almost all elements of $\mathbb{R}^n$ can be uniquely written as a sum $a + t$, where $a \in A$, $t \in T$. We will denote this by $A \oplus T = \mathbb{R}^n$. T is called the tiling complement of A, and (A, T) is called a tiling pair in $\mathbb{R}^n$.

In 1974, Fuglede [11] proposed the following conjecture, which connected these two notions.

✉ Tao Zhang
zhant220@163.com

1 Zhejiang Lab, Hangzhou 311100, China

Conjecture 1.1 *A subset $\Omega \subseteq \mathbb{R}^n$ of positive and finite Lebesgue measure is a spectral set if and only if it tiles $\mathbb{R}^n$ by translation.*

In the same paper, Fuglede proved this conjecture when the tiling complement or the spectrum is a lattice in $\mathbb{R}^n$. 30 years later, Tao [35] disproved this conjecture by constructing a non-tile spectral set in $\mathbb{R}^5$. Currently, the conjecture does not hold in both directions for $\mathbb{R}^n$, $n \geq 3$ [9, 18, 19, 27]. However, this conjecture remains open in $\mathbb{R}$ and $\mathbb{R}^2$.

Given the falsification of Fuglede's conjecture for $\mathbb{R}^n$, $n \geq 3$, researchers approached this problem from two perspectives. Firstly, under additional assumptions, Iosevich, Katz and Tao [13] showed that the conjecture holds for convex sets in $\mathbb{R}^2$ in 2003, and Greenfeld and Lev [12] later proved a similar result in dimension 3. Recently, Lev and Matolcsi [24] demonstrated that the conjecture holds for convex domains in $\mathbb{R}^n$ for all n. Secondly, researchers attempted to identify for which groups G, the conjecture holds. Fan et al. [7, 8] proved its validity in $\mathbb{Q}_p$, the field of p-adic numbers, and it is known to hold in various finite Abelian groups such as $\mathbb{Z}_p^d$ ($p = 2$ and $d \leq 6$; p is an odd prime and $d = 2$; $p = 3, 5, 7$ and $d = 3$) [1, 5, 10, 14], $\mathbb{Z}_p \times \mathbb{Z}_{p^n}$ [14, 31, 36], $\mathbb{Z}_p \times \mathbb{Z}_{pq}$ [15] and $\mathbb{Z}_{pq} \times \mathbb{Z}_{pq}$ [6], $\mathbb{Z}_{p^n}$ [20], $\mathbb{Z}_{p^n q^m}$ ($p < q$ and $m \leq 9$ or $n \leq 6$; $p^{m-2} < q^4$) [16, 25, 26], $\mathbb{Z}_{pqr}$ [30], $\mathbb{Z}_{p^2qr}$ [32] and $\mathbb{Z}_{pqrs}$ [17], where p, q, r, s are distinct primes.

In this paper, we focus on finite cyclic groups. Following the notations from [4], write $S - T(G)$ (respectively, $T - S(G)$), if the "Spectral $\Rightarrow$ Tile" (respectively, "Tile $\Rightarrow$ Spectral") direction of Fuglede's conjecture holds in G. Then we have the following relations [3, 4]:

$$T - S(\mathbb{R}) \Leftrightarrow T - S(\mathbb{Z}) \Leftrightarrow T - S(\mathbb{Z}_N) \text{ for all } N,$$

and

$$S - T(\mathbb{R}) \Rightarrow S - T(\mathbb{Z}) \Rightarrow S - T(\mathbb{Z}_N) \text{ for all } N.$$

The above relations show that finite cyclic groups play important roles in the study of Fuglede's conjecture in $\mathbb{R}$. As we have seen, Fuglede's conjecture holds in the following finite cyclic groups: $\mathbb{Z}_{p^n}$, $\mathbb{Z}_{p^n q^m}$ ($p < q$ and $m \leq 9$ or $n \leq 6$; $p^{m-2} < q^4$), $\mathbb{Z}_{pqr}$, $\mathbb{Z}_{p^2qr}$ and $\mathbb{Z}_{pqrs}$, where p, q, r, s are distinct primes. For the direction "Tile $\Rightarrow$ Spectral", Łaba [20] proved $T - S(\mathbb{Z}_{p^n q^m})$ for distinct primes p, q. Later, Łaba and Meyerowitz proved $T - S(\mathbb{Z}_n)$ in comments of Tao's blog [34] (see also [30]), where n is a squarefree integer. Recently, Malikiosis [25] proved $T - S(\mathbb{Z}_{p_1^n p_2 \cdots p_k})$, where $p_1, p_2, \ldots, p_k$ are distinct primes. In [21–23], the authors developed some new tools to study tiling sets in cyclic groups and proved $T - S(\mathbb{Z}_{p^2q^2r^2})$, where p, q, r are distinct primes.

Now we state our main result.

Theorem 1.2 *Let p, q, r be distinct primes and n be a positive integer. A subset in $\mathbb{Z}_{p^n qr}$ is a spectral set if and only if it is a tile of $\mathbb{Z}_{p^n qr}$.*

Note that the "Tile $\Rightarrow$ Spectral" direction follows from [25]. Hence, we only need to prove the "Spectral $\Rightarrow$ Tile" direction. When we consider Fuglede's conjecture in cyclic groups, one of the most important tools is the so-called (T1) and (T2) conditions, which was introduced by Coven and Meyerowitz [2]. In this paper, we introduce the group ring notation to study spectral sets in cyclic groups. In particular, we prove that Fuglede's conjecture holds in $\mathbb{Z}_{p^n qr}$. This paper is organized as follows. In Sect. 2, we recall some basics of spectral sets and tiles in cyclic groups. In Sect. 3, we prove some useful lemmas using the group ring notation. In Sect. 4, we prove Theorem 1.2.

2 Preliminaries

Let $\mathbb{Z}_n$ be a finite cyclic group with order n (written additively). For any $a, x \in \mathbb{Z}_n$, define

$$\chi_a(x) = e^{\frac{2\pi i \cdot ax}{n}}.$$

Then $\chi_a \chi_b = \chi_{a+b}$. Hence the set $\widehat{\mathbb{Z}_n} = \{\chi_a : a \in \mathbb{Z}_n\}$ forms a group which is isomorphic to $\mathbb{Z}_n$.

Now we restate the definition of spectral sets and tiles in cyclic groups.

Definition 2.1 A subset $A \subseteq \mathbb{Z}_N$ is said to be spectral if there is a subset $B \subseteq \mathbb{Z}_N$ such that

$$\{\chi_b : b \in B\}$$

forms an orthogonal basis in $L^2(A)$, the vector space of complex valued functions on A with Hermitian inner product $\langle f, g\rangle = \sum_{a\in A} f(a)\overline{g}(a)$. In such a case, the set B is called a spectrum of A, and (A, B) is called a spectral pair.

Since the dimension of $L^2(A)$ is $|A|$, the pair (A, B) being a spectral pair is equivalent to

$$|A| = |B| \text{ and } \sum_{a\in A} \chi_{b-b'}(a) = 0 \text{ for all } b \neq b' \in B.$$

The set of zeros of A is defined by

$$\mathcal{Z}_A = \{b \in \mathbb{Z}_n : \sum_{a\in A} \chi_b(a) = 0\}.$$

Then $\mathcal{Z}_A$ is precisely the zeros of the Fourier transform of the characteristic function of A.

The following equivalent conditions of a spectral pair can be found in [31, 36].

Lemma 2.2 *Let $A, B \subseteq \mathbb{Z}_N$. Then the following statements are equivalent.*

(a) (A, B) *is a spectral pair.*
(b) (B, A) *is a spectral pair.*
(c) $|A| = |B|$ *and* $(B - B)\backslash\{0\} \subseteq \mathcal{Z}_A$.

(d) *The pair* $(aA+g, bB+h)$ *is a spectral pair for all* $a, b \in \mathbb{Z}_N^*$ *and* $g, h \in \mathbb{Z}_N$.

Definition 2.3 A subset $A \subseteq \mathbb{Z}_N$ is said to be a tile if there is a subset $T \subseteq \mathbb{Z}_N$ such that each element $g \in \mathbb{Z}_N$ can be expressed uniquely in the form

$$g = a + t,\ a \in A,\ t \in T.$$

We will denote this by $\mathbb{Z}_N = A \oplus T$. The set T is called a tiling complement of A, and (A, T) is called a tiling pair.

We have the following equivalent conditions for a tiling pair [31], [33, Lemma 2.1].

Lemma 2.4 *Let* A, T *be subsets in* $\mathbb{Z}_N$. *Then the following statements are equivalent.*

(a) (A, T) *is a tiling pair.*
(b) (T, A) *is a tiling pair.*
(c) $(A+g, T+h)$ *is a tiling pair.*
(d) $|A| \cdot |T| = N$ *and* $(A-A) \cap (T-T) = \{0\}$.
(e) $|A| \cdot |T| = N$ *and* $\mathcal{Z}_A \cup \mathcal{Z}_T = \mathbb{Z}_N \backslash \{0\}$.

If $|A| = 1$ or $A = \mathbb{Z}_N$, then the set A is called trivial. It is easy to see that a trivial set is a spectral set and also a tiling set. In the following of this paper, we will only consider nontrivial sets. We also need the following lemmas, which will be useful in the following sections.

Lemma 2.5 [16] *Let* A *be a spectral set in* $\mathbb{Z}_N$, *that does not generate* $\mathbb{Z}_N$. *Assume that for every proper subgroup* H *of* $\mathbb{Z}_N$ *we have* $S-T(H)$. *Then* A *tiles* $\mathbb{Z}_N$.

Lemma 2.6 [16] *Let* N *be a natural number and suppose that* $S-T(\mathbb{Z}_N/H)$ *holds for every* $\{0\} \neq H \leq \mathbb{Z}_N$. *Assume that* (A, B) *is a spectral pair and* B *does not generate* $\mathbb{Z}_N$. *Then* A *tiles* $\mathbb{Z}_N$.

Lemma 2.7 [16] *Let* N *be a natural number,* A *a spectral set in* $\mathbb{Z}_N$ *and* p *a prime divisor of* N. *Assume that* $S-T(\mathbb{Z}_{\frac{N}{p}})$. *If* A *is the union of* $\mathbb{Z}_p$*-cosets, then* A *tiles* $\mathbb{Z}_N$.

Lemma 2.8 [32] *Let* $0 \in T \subseteq \mathbb{Z}_N$ *be a generating set and assume that* p *and* q *are different prime divisors of* N. *Then there are elements* $t_1 \neq t_2 \in T$ *such that* $p \nmid (t_1 - t_2)$ *and* $q \nmid (t_1 - t_2)$.

Lemma 2.9 *Let* p *be a prime and set* $\zeta = \zeta_{p^n}$, *a primitive* p^n*-th root of unity. Let* $c = c_{p^n-1}\zeta^{p^n-1} + c_{p^n-2}\zeta^{p^n-2} + \cdots + c_1\zeta + c_0$, *where* $c_i \in \mathbb{Z}$, $0 \leq i \leq p^n - 1$. *Then* $c = 0$ *if and only if* $c_i = c_j$ *for any* i, j *with* $i \equiv j \pmod{p^{n-1}}$.

Proof Let $f(x) = c_{p^n-1}x^{p^n-1} + c_{p^n-2}x^{p^n-2} + \cdots + c_1x + c_0$, then $c = 0$ if and only if ζ is a root of $f(x)$. Since the minimal polynomial of ζ over $\mathbb{Z}$ is

$$\Phi_{p^n}(x) = x^{(p-1)p^{n-1}} + x^{(p-2)p^{n-1}} + \cdots + x^{p^{n-1}} + 1,$$

then $c = 0$ if and only if there exists a polynomial $g(x) \in \mathbb{Z}[x]$ such that

$$f(x) = \Phi_{p^n}(x)g(x).$$

Hence, the statement follows. □

Let $v_p(a)$ denote the p-adic valuation of a, i.e., $p^{v_p(a)} \| a$.

Lemma 2.10 *Let $V \subset \mathbb{Z}_{p^n}$ satisfy $|V| = p^t$, and $I \subset [0, n-1]$ satisfy $|I| = t$. If $v_p(v) \in I$ for all $v \in (V - V)\backslash\{0\}$, then the elements of V have the form $\alpha_0 + \alpha_1 p + \cdots + \alpha_{n-1}p^{n-1}$, where $\alpha_i \in [0, p-1]$ satisfy the following conditions:*

1. *if $i \in I$, then α_i can take every value from $[0, p-1]$;*
2. *if $j \notin I$, the value of α_j depends solely on $\alpha_0, \ldots, \alpha_{j-1}$.*

Proof We prove the lemma by induction. It is easy to see that the result is true for $|I| = 1$. Suppose that the statement holds for $|I| < t$.

Let $|I| = t$, $I = \{i_j : j \in [1, t]\}$, and $0 \le i_1 < i_2 < \cdots < i_t \le n-1$. For any $v \in V$, we can write v as $v = \sum_{i=0}^{n-1} v_i p^i$, where $v_i \in [0, p-1]$. Denote

$$V_k = \{v \in V : v_{i_1} = k\}.$$

Then $V = \cup_{k=0}^{p-1} V_k$. By the pigeonhole principle, there exists k such that $|V_k| \ge p^{t-1}$. Note that the p-adic valuations of the elements of $V_k - V_k$ are in $I\backslash\{i_1\}$. By the pigeonhole principle again, we have $|V_k| \le p^{t-1}$. Hence $|V_k| = p^{t-1}$ for all $k \in [0, p-1]$. By induction, the elements of V_k have the form $\alpha_0 + \alpha_1 p + \cdots + kp^{i_1} + \cdots + \alpha_{n-1}p^{n-1}$, where $\alpha_i \in [0, p-1]$ satisfy the following conditions:

1. if $i \in I\backslash\{i_1\}$, then α_i can take every value from $[0, p-1]$;
2. if $j \notin I$, the value of α_j depends solely on $\alpha_0, \ldots, \alpha_{j-1}$.

Then the statement follows from $V = \cup_{k=0}^{p-1} V_k$. □

3 Technique Tools

Throughout the following sections, the cyclic group $\mathbb{Z}_N$ will be written multiplicatively. Let $\mathbb{Z}_N = \langle u \rangle$, then all the statements in Sect. 2 still hold under the isomorphism map: $i \to u^i$.

Our main result will be demonstrated using the language of group rings, which is commonly employed in the investigation of combinatorial designs, finite geometry, and related fields. For further information, please refer to [28, 29] and their associated references.

Let $\mathbb{Z}[\mathbb{Z}_N]$ denote the group ring of $\mathbb{Z}_N$ over $\mathbb{Z}$. For any $X \in \mathbb{Z}[\mathbb{Z}_N]$, X can be written as formal sums $X = \sum_{g \in \mathbb{Z}_N} x_g g$, where $x_g \in \mathbb{Z}$. The addition and subtraction of elements in $\mathbb{Z}[\mathbb{Z}_N]$ is defined componentwise, i.e.,

$$\sum_{g \in \mathbb{Z}_N} x_g g \pm \sum_{g \in \mathbb{Z}_N} y_g g := \sum_{g \in \mathbb{Z}_N} (x_g \pm y_g) g.$$

The multiplication is defined by

$$\left(\sum_{g\in\mathbb{Z}_N} x_g g\right)\left(\sum_{g\in\mathbb{Z}_N} y_g g\right) := \sum_{g\in\mathbb{Z}_N}\left(\sum_{h\in\mathbb{Z}_N} x_h y_{h^{-1}g}\right) g.$$

For $X = \sum_{g\in\mathbb{Z}_N} x_g g$ and $t \in \mathbb{Z}$, we define

$$X^{(t)} := \sum_{g\in\mathbb{Z}_N} x_g g^t.$$

For any set X whose elements belong to $\mathbb{Z}_N$ (X may be a multiset), we can identify X with the group ring element $\sum_{g\in\mathbb{Z}_N} x_g g$, where x_g is the multiplicity of g appearing in X. The group ring notation is equivalent to the polynomial notation in cyclic groups. For example, the set $A \subset \mathbb{Z}_N$ corresponds to the polynomial $A(X) = \sum_{a\in A} X^a \pmod{X^N - 1}$.

For any $g = u^a, h = u^b \in \mathbb{Z}_N$, define

$$\chi_{g,N}(h) := e^{\frac{2\pi i\cdot ab}{N}}.$$

We will use $\chi_{a,N}$ instead of $\chi_{u^a,N} = \chi_{g,N}$ if there is no misunderstanding. For any $\chi \in \widehat{\mathbb{Z}_N}$ and $X = \sum_{g\in\mathbb{Z}_N} x_g g \in \mathbb{Z}[\mathbb{Z}_N]$, define

$$\chi(X) := \sum_{g\in\mathbb{Z}_N} x_g \chi(g).$$

Then the pair (A, B) forms a spectral pair if and only if

$$|A| = |B| \text{ and } \chi_{b-b',N}(A) = 0 \text{ for all } u^b \neq u^{b'} \in B.$$

Let $\mathbb{Z}_{p^n p_1\cdots p_k} = \langle a, a_1, \ldots, a_k\rangle$, where $o(a) = p^n$, $o(a_i) = p_i$ for $i = 1, \ldots, k$. Let A be a subset of $\mathbb{Z}_{p^n p_1\cdots p_k}$, then A can be written as $A = \sum_{i_1=0}^{p_1-1}\cdots\sum_{i_k=0}^{p_k-1} A_{i_1,\ldots,i_k} a_1^{i_1}\cdots a_k^{i_k}$, where $A_{i_1,\ldots,i_k} \in \mathbb{Z}_{\geq 0}[\langle a\rangle]$. For any $i'_{t+1} \in [0, p_{t+1}-1], \ldots, i'_k \in [0, p_k - 1]$, denote

$$\begin{aligned}\mathcal{I}_{t,s}(i'_{t+1}, \ldots, i'_k) :=\{&(i_1, i_2, \ldots, i_k) : \text{ there are exactly } s \text{ of } j \in [t+1, k] \text{ such that } i_j = 0\\ &\text{and for other } j \in [t+1, k], i_j = i'_j\}.\end{aligned}$$

Let $A_{\mathcal{I}_{t,s}(i'_{t+1},\ldots,i'_k)} := \sum_{I\in\mathcal{I}_{t,s}(i'_{t+1},\ldots,i'_k)} A_I$. Then we have the following lemma, which can transfer the problem from $\mathbb{Z}_{p^n p_1\cdots p_k}$ to $\mathbb{Z}_{p^n}$.

Lemma 3.1 *Let $0 \leq t \leq k$, $0 \leq i \leq n$, then $p^i p_1 \cdots p_t \in \mathcal{Z}_A$ if and only if*

$$\chi_{p^i,p^n}\left(\sum_{s=0}^{k-t}\sum_{i_1=0}^{p_1-1}\cdots\sum_{i_t=0}^{p_t-1}(-1)^s A_{\mathcal{I}_{t,s}(i'_{t+1},\ldots,i'_k)}\right) = 0$$

for all $i'_{t+1} \in [0, p_{t+1}-1], \ldots, i'_k \in [0, p_k - 1]$*, where* $p^i p_1 \cdots p_t := p^i$ *if* $t = 0$.

Proof By the definition of zeros of a set, we have $p^i p_1 \cdots p_t \in \mathcal{Z}_A$ if and only if

$$\begin{aligned}
0 &= \chi_{p^i p_1\cdots p_t, p^n p_1\cdots p_k}(A) \\
&= \chi_{p^i p_1\cdots p_t, p^n p_1\cdots p_k}\left(\sum_{i_1=0}^{p_1-1}\cdots\sum_{i_k=0}^{p_k-1} A_{i_1,\ldots,i_k} a_1^{i_1}\cdots a_k^{i_k}\right) \\
&= \sum_{i_1=0}^{p_1-1}\cdots\sum_{i_k=0}^{p_k-1} \chi_{p^i,p^n}(A_{i_1,\ldots,i_k})\zeta_{p_{t+1}}^{i_{t+1}}\cdots\zeta_{p_k}^{i_k} \\
&= \sum_{i_k=0}^{p_k-1}\left(\sum_{i_{t+1}=0}^{p_{t+1}-1}\cdots\sum_{i_{k-1}=0}^{p_{k-1}-1}\chi_{p^i,p^n}\left(\sum_{i_1=0}^{p_1-1}\cdots\sum_{i_t=0}^{p_t-1} A_{i_1,\ldots,i_k}\right)\zeta_{p_{t+1}}^{i_{t+1}}\cdots\zeta_{p_{k-1}}^{i_{k-1}}\right)\zeta_{p_k}^{i_k} \\
&= \sum_{i_k=1}^{p_k-1}\left(\sum_{i_{t+1}=0}^{p_{t+1}-1}\cdots\sum_{i_{k-1}=0}^{p_{k-1}-1}\chi_{p^i,p^n}\left(\sum_{i_1=0}^{p_1-1}\cdots\sum_{i_t=0}^{p_t-1}(A_{i_1,\ldots,i_k} - A_{i_1,\ldots,i_{k-1},0})\right)\zeta_{p_{t+1}}^{i_{t+1}}\cdots\zeta_{p_{k-1}}^{i_{k-1}}\right)\zeta_{p_k}^{i_k},
\end{aligned}$$

where the last equation follows from $1 = -\sum_{i_k=1}^{p_k-1}\zeta_{p_k}^{i_k}$. Since $\zeta_{p_k}, \zeta_{p_k}^2, \ldots, \zeta_{p_k}^{p_k-1}$ forms a basis of $\mathbb{Q}(\zeta_{p^n p_1\cdots p_k})/\mathbb{Q}(\zeta_{p^n p_1\cdots p_{k-1}})$, then $\chi_{p^i p_1\cdots p_t, p^n p_1\cdots p_k}(A) = 0$ is equivalent to

$$\sum_{i_{t+1}=0}^{p_{t+1}-1}\cdots\sum_{i_{k-1}=0}^{p_{k-1}-1}\chi_{p^i,p^n}\left(\sum_{i_1=0}^{p_1-1}\cdots\sum_{i_t=0}^{p_t-1}(A_{i_1,\ldots,i_k} - A_{i_1,\ldots,i_{k-1},0})\right)\zeta_{p_{t+1}}^{i_{t+1}}\cdots\zeta_{p_{k-1}}^{i_{k-1}} = 0$$

for all $i_k \in [0, p_k - 1]$. Repeating above arguments, we have the statement. □

In particular, let $\mathbb{Z}_{p^n qr} = \langle a, b, c\rangle$, where $o(a) = p^n$, $o(b) = q$ and $o(c) = r$, and write $A = \sum_{j=0}^{q-1}\sum_{k=0}^{r-1} A_{j,k} b^j c^k$, where $A_{j,k} \in \mathbb{Z}_{\geq 0}[\langle a\rangle]$. Then we have the following corollary.

Corollary 3.2 (1) $p^i \in \mathcal{Z}_A$ *if and only if* $\chi_{p^i,p^n}(A_{j,k} - A_{j,0} - A_{0,k} + A_{0,0}) = 0$ *for all* $j \in [0, q-1], k \in [0, r-1]$.

(2) $p^i q \in \mathcal{Z}_A$ *if and only if* $\chi_{p^i,p^n}(\sum_{j=0}^{q-1}(A_{j,k} - A_{j,0})) = 0$ *for all* $k \in [0, r-1]$.

(3) $p^i r \in \mathcal{Z}_A$ *if and only if* $\chi_{p^i,p^n}(\sum_{k=0}^{r-1}(A_{j,k} - A_{0,k})) = 0$ *for all* $j \in [0, q-1]$.

(4) $p^i qr \in \mathcal{Z}_A$ *if and only if* $\chi_{p^i,p^n}(\sum_{j=0}^{q-1}\sum_{k=0}^{r-1} A_{j,k}) = 0$.

If A has many zeros, then we can get more information about the sets $A_{j,k}$, $j \in [0, q-1], k \in [0, r-1]$.

Lemma 3.3 (1) $p^i, p^i q \in \mathcal{Z}_A$ *if and only if* $\chi_{p^i,p^n}(A_{j,k} - A_{j,0}) = 0$ *for all* $j \in [0, q-1], k \in [0, r-1]$.

(2) $p^i, p^i r \in \mathcal{Z}_A$ *if and only if* $\chi_{p^i,p^n}(A_{j,k} - A_{0,k}) = 0$ *for all* $j \in [0, q-1], k \in [0, r-1]$.

(3) $p^i q, p^i r \in \mathcal{Z}_A$ *if and only if* $r\chi_{p^i,p^n}(\sum_{j=0}^{q-1} A_{j,k'}) = q\chi_{p^i,p^n}(\sum_{k=0}^{r-1} A_{j',k})$ *for all* $j' \in [0, q-1], k' \in [0, r-1]$.
(4) $p^i q, p^i qr \in \mathcal{Z}_A$ *if and only if* $\chi_{p^i,p^n}(\sum_{j=0}^{q-1} A_{j,k}) = 0$ *for all* $k \in [0, r-1]$.
(5) $p^i r, p^i qr \in \mathcal{Z}_A$ *if and only if* $\chi_{p^i,p^n}(\sum_{k=0}^{r-1} A_{j,k}) = 0$ *for all* $j \in [0, q-1]$.
(6) $p^i, p^i q, p^i r \in \mathcal{Z}_A$ *if and only if* $\chi_{p^i,p^n}(A_{j,k} - A_{0,0}) = 0$ *for all* $j \in [0, q-1], k \in [0, r-1]$.
(7) $p^i, p^i r, p^i q, p^i qr \in \mathcal{Z}_A$ *if and only if* $\chi_{p^i,p^n}(A_{j,k}) = 0$ *for all* $j \in [0, q-1], k \in [0, r-1]$.

Proof We will only prove (1) and (3). For other statements, the proofs are similar.

(1). If $p^i, p^i q \in \mathcal{Z}_A$, by Corollary 3.2 (1) and (2), we have

$$\chi_{p^i,p^n}(A_{j,k} - A_{j,0} - A_{0,k} + A_{0,0}) = 0,$$
$$\chi_{p^i,p^n}\left(\sum_{j=0}^{q-1}(A_{j,k} - A_{j,0})\right) = 0.$$

Then we can compute to get that

$$\begin{aligned} 0 &= \sum_{j=0}^{q-1} \chi_{p^i,p^n}(A_{j,k} - A_{j,0} - A_{0,k} + A_{0,0}) \\ &= \chi_{p^i,p^n}\left(\sum_{j=0}^{q-1}(A_{j,k} - A_{j,0} - A_{0,k} + A_{0,0})\right) \\ &= \chi_{p^i,p^n}\left(\sum_{j=0}^{q-1}(-A_{0,k} + A_{0,0})\right) \\ &= q\chi_{p^i,p^n}(-A_{0,k} + A_{0,0}) \\ &= q\chi_{p^i,p^n}(-A_{j,k} + A_{j,0}). \end{aligned}$$

Hence $\chi_{p^i,p^n}(A_{j,k} - A_{j,0}) = 0$ for all $j \in [0, q-1], k \in [0, r-1]$. For the converse, the result directly follows from Corollary 3.2 (1) and (2).

(3) If $p^i q, p^i r \in \mathcal{Z}_A$, by Corollary 3.2 (2) and (3), we have

$$\chi_{p^i,p^n}\left(\sum_{j=0}^{q-1}(A_{j,k'} - A_{j,0})\right) = 0,$$
$$\chi_{p^i,p^n}\left(\sum_{k=0}^{r-1}(A_{j',k} - A_{0,k})\right) = 0.$$

Then we can compute to get that

$$
\begin{aligned}
r\chi_{p^i,p^n}\left(\sum_{j=0}^{q-1}A_{j,k'}\right) &= r\chi_{p^i,p^n}\left(\sum_{j=0}^{q-1}A_{j,0}\right) = \chi_{p^i,p^n}\left(\sum_{j=0}^{q-1}\sum_{k=0}^{r-1}A_{j,0}\right)\\
&= \chi_{p^i,p^n}\left(\sum_{j=0}^{q-1}\sum_{k=0}^{r-1}A_{j,k}\right)\\
&= \chi_{p^i,p^n}\left(\sum_{j=0}^{q-1}\sum_{k=0}^{r-1}A_{0,k}\right) = q\chi_{p^i,p^n}\left(\sum_{k=0}^{r-1}A_{0,k}\right) = q\chi_{p^i,p^n}\left(\sum_{k=0}^{r-1}A_{j',k}\right).
\end{aligned}
$$

For the converse, the result directly follows from Corollary 3.2 (2) and (3). □

4 Proof of Theorem 1.2

Let (A, B) be a nontrivial spectral pair in $\mathbb{Z}_{p^n qr}$. Assuming further that A is not a tiling set, we will establish a contradiction.

Let $\mathbb{Z}_{p^n qr} = \langle a, b, c\rangle$, where $o(a) = p^n$, $o(b) = q$ and $o(c) = r$, and write $A = \sum_{j=0}^{q-1}\sum_{k=0}^{r-1} A_{j,k} b^j c^k$ and $B = \sum_{j=0}^{q-1}\sum_{k=0}^{r-1} B_{j,k} b^j c^k$, where $A_{j,k}, B_{j,k} \in \mathbb{Z}_{\geq 0}[\langle a\rangle]$. Let e be the identity element of group $\mathbb{Z}_{p^n qr}$.

Remark 4.1 (1) If $a^{i_0}, a^{i_0+up^{i_1}} \in A_{j,k}$ for some $j \in [0, q-1], k \in [0, r-1]$ and $u \not\equiv 0 \pmod p$, then $p^{i_1}qr \in \mathcal{Z}_B$.

(2) If $a^{i_0} \in A_{j_0,k}, a^{i_0+up^{i_1}} \in A_{j_1,k}$ for some $j_0, j_1 \in [0, q-1], k \in [0, r-1]$ with $j_0 \neq j_1$, then $p^{i_1}r \in \mathcal{Z}_B$ when $u \not\equiv 0 \pmod p$, and $p^n r \in \mathcal{Z}_B$ when $u = 0$.

(3) If $a^{i_0} \in A_{j,k_0}, a^{i_0+up^{i_1}} \in A_{j,k_1}$ for some $j \in [0, q-1], k_0, k_1 \in [0, r-1]$ with $k_0 \neq k_1$, then $p^{i_1}q \in \mathcal{Z}_B$ when $u \not\equiv 0 \pmod p$, and $p^n q \in \mathcal{Z}_B$ when $u = 0$.

(4) If $a^{i_0} \in A_{j_0,k_0}, a^{i_0+up^{i_1}} \in A_{j_1,k_1}$ for some $j_0, j_1 \in [0, q-1], k_0, k_1 \in [0, r-1]$ with $j_0 \neq j_1$ and $k_0 \neq k_1$, then $p^{i_1} \in \mathcal{Z}_B$ when $u \not\equiv 0 \pmod p$, and $p^n \in \mathcal{Z}_B$ when $u = 0$.

Note that Fuglede's conjecture holds in $\mathbb{Z}_{p^n q}$ [26], $\mathbb{Z}_{pqr}$ [30] and $\mathbb{Z}_{p^2 qr}$ [32], where p, q, r are distinct primes. By Lemmas 2.2, 2.4, 2.5, 2.6 and 2.7, we also assume that

(1) $e \in A, e \in B$;
(2) A generates group $\mathbb{Z}_{p^n qr}$;
(3) B generates group $\mathbb{Z}_{p^n qr}$;
(4) A is not a union of $\mathbb{Z}_p$- or $\mathbb{Z}_q$- or $\mathbb{Z}_r$-cosets exclusively.

Then $e \in A_{0,0}$ and $e \in B_{0,0}$. Denote

$$
\begin{aligned}
I_1 &= \{i : i \in [0, n-1], p^i qr \in \mathcal{Z}_A\},\\
I_2 &= \mathcal{Z}_A \cap \{p^n q, p^n r\},\\
J_1 &= \{i : i \in [0, n-1], p^i qr \in \mathcal{Z}_B\},\\
J_2 &= \mathcal{Z}_B \cap \{p^n q, p^n r\}.
\end{aligned}
$$

Then $0 \le |I_1|, |J_1| \le n$ and $0 \le |I_2|, |J_2| \le 2$. Now we first prove some lemmas.

Lemma 4.2 (1) *If $q, r \in \mathcal{Z}_A$ and $qr \notin \mathcal{Z}_A$, then $p^n q, p^n r \in \mathcal{Z}_B$.*
(2) *If $q, r \in \mathcal{Z}_B$ and $qr \notin \mathcal{Z}_B$, then $p^n q, p^n r \in \mathcal{Z}_A$.*

Proof We will only prove the first statement, the proof of the second statement is similar. Note that $qr \notin \mathcal{Z}_A$. By Lemma 3.3 (3), (4) and (5), we have

$$r\chi_{1,p^n}\left(\sum_{j=0}^{q-1} A_{j,k'}\right) = q\chi_{1,p^n}\left(\sum_{k=0}^{r-1} A_{j',k}\right) \neq 0,$$

for any $j' \in [0, q-1]$ and $k' \in [0, r-1]$. Let $\sum_{j=0}^{q-1} A_{j,k'} = \sum_{i=0}^{p^n-1} x_i a^i$, and $\sum_{k=0}^{r-1} A_{j',k} = \sum_{i=0}^{p^n-1} y_i a^i$, where $x_i, y_i \in \mathbb{Z}_{\ge 0}$. Then, the above inequations show that

$$\sum_{i=0}^{p^n-1} x_i \zeta_{p^n}^i \neq 0, \tag{1}$$

$$\sum_{i=0}^{p^n-1} y_i \zeta_{p^n}^i \neq 0, \tag{2}$$

$$\sum_{i=0}^{p^n-1} (rx_i - qy_i)\zeta_{p^n}^i = 0. \tag{3}$$

By Lemma 2.9, Equation (1) implies that there exist i_1, i_2 with $i_1 \equiv i_2 \pmod{p^{n-1}}$ such that $x_{i_1} \neq x_{i_2}$. By Equation (3), we have $rx_{i_1} - qy_{i_1} = rx_{i_2} - qy_{i_2}$, which leads to $r(x_{i_1} - x_{i_2}) = q(y_{i_1} - y_{i_2})$. Hence, we have $|x_{i_1} - x_{i_2}| \ge q$ and $|y_{i_1} - y_{i_2}| \ge r$. Therefore, $\max\{x_{i_1}, x_{i_2}\} \ge q$ and $\max\{y_{i_1}, y_{i_2}\} \ge r$. In other words, there exists $a^{i_0} \in \sum_{j=0}^{q-1} A_{j,k'}$ such that a^{i_0} appears q times in $\sum_{j=0}^{q-1} A_{j,k'}$. By Remark 4.1 (2), we have $p^n r \in \mathcal{Z}_B$. Similarly, $p^n q \in \mathcal{Z}_B$. □

Lemma 4.3 (1) *If $|J_2| \le 1$, then $1 \in \mathcal{Z}_A$.*
(2) *If $|I_2| \le 1$, then $1 \in \mathcal{Z}_B$.*

Proof We will only prove the first statement, the proof of the second statement is similar.

Assume to the contrary, $1 \notin \mathcal{Z}_A$. By Lemma 2.8, there exist $x, y \in B$ such that $p \nmid (x-y)$ and $q \nmid (x-y)$. Since $1 \notin \mathcal{Z}_A$, then $r \mid (x-y)$, and so $r \in \mathcal{Z}_A$. Similarly, we have $q \in \mathcal{Z}_A$.

By Lemma 4.2 (1), we have $qr \in \mathcal{Z}_A$. By Lemma 3.3 (4) and (5), we get

$$\chi_{1,p^n}\left(\sum_{j=0}^{q-1} A_{j,k'}\right) = \chi_{1,p^n}\left(\sum_{k=0}^{r-1} A_{j',k}\right) = 0 \text{ for all } j' \in [0, q-1], k' \in [0, r-1].$$

In other words, $\sum_{j=0}^{q-1} A_{j,k'}$ and $\sum_{k=0}^{r-1} A_{j',k}$ are unions of some $\mathbb{Z}_p$-cosets. Since $1 \notin \mathcal{Z}_A$, then there exist j_1, k_1 such that $\chi_{1,p^n}(A_{j_1,k_1}) \neq 0$. Hence, there exists $a^{i_0} \in A_{j_1,k_1}$ such that $a^{i_0+up^{n-1}} \notin A_{j_1,k_1}$ for some $u \in [1, p-1]$. Moreover, $a^{i_0+up^{n-1}} \in A_{j_2,k_1}$ and $a^{i_0+up^{n-1}} \in A_{j_1,k_2}$ for some j_2, k_2 with $j_2 \neq j_1$ and $k_2 \neq k_1$. This shows that $p^{n-1}q, p^{n-1}r, p^n \in \mathcal{Z}_B$. By Lemma 3.3 (3) and $p^{n-1}q, p^{n-1}r \in \mathcal{Z}_B$, we have

$$r\chi_{p^{n-1},p^n}\left(\sum_{j=0}^{q-1} B_{j,k'}\right) = q\chi_{p^{n-1},p^n}\left(\sum_{k=0}^{r-1} B_{j',k}\right) \text{ for all } j' \in [0, q-1], k' \in [0, r-1]. \tag{4}$$

By Corollary 3.2 (1) and $p^n \in \mathcal{Z}_B$, we have

$$|B_{j,k}| - |B_{j,0}| - |B_{0,k}| + |B_{0,0}| = 0 \text{ for all } j \in [0, q-1], k \in [0, r-1]. \tag{5}$$

Claim: $p^{n-1} \notin \mathcal{Z}_B$.

Assume to the contrary, $p^{n-1} \in \mathcal{Z}_B$.

If $p^{n-1}qr \in \mathcal{Z}_B$, by Lemma 3.3 (7), we have $\chi_{p^{n-1},p^n}(B_{j,k}) = 0$. Noting that $e \in B_{0,0}$, then

$$\{i \pmod p : a^i \in B_{0,0}\} = \{0, 1, \ldots, p-1\}.$$

Since $1 \notin \mathcal{Z}_A$, then $B_{j,k} = \emptyset$ for $j \in [1, q-1]$ and $k \in [1, r-1]$. If $B_{j,0} \neq \emptyset$ for some $j \in [1, q-1]$, similarly as before,

$$\{i \pmod p : a^i \in B_{j,0}\} = \{0, 1, \ldots, p-1\},$$
$$B_{0,k} = \emptyset \text{ for } k \in [1, r-1].$$

Thus $B = \sum_{j=0}^{q-1} B_{j,0}b^j$, which contradicts the fact that B generates $\mathbb{Z}_{p^nqr}$. Hence $B_{j,0} = \emptyset$ for all $j \in [1, q-1]$ and so $B = \sum_{k=0}^{r-1} B_{0,k}c^k$, which also contradicts the fact that B generates $\mathbb{Z}_{p^nqr}$. Therefore, $p^{n-1}qr \notin \mathcal{Z}_B$.

By Lemma 3.3 (6), (7) and $p^{n-1}, p^{n-1}q, p^{n-1}r \in \mathcal{Z}_B$, $p^{n-1}qr \notin \mathcal{Z}_B$, we have

$$\chi_{p^{n-1},p^n}(B_{j,k}) = \chi_{p^{n-1},p^n}(B_{0,0}) \neq 0 \text{ for all } j, k. \tag{6}$$

If there exists $j \in [0, q-1], k \in [0, r-1]$ such that $|\{i \pmod p : a^i \in B_{j,k}\}| \geq 2$, WLOG, assume that $|\{i \pmod p : a^i \in B_{0,0}\}| \geq 2$. Equation (6) implies that $|B_{j,k}| \geq 1$ for all j, k. Then we have $1 \in \mathcal{Z}_A$, which is a contradiction. Hence $|\{i \pmod p : a^i \in B_{j,k}\}| = 1$ for all $j \in [0, q-1], k \in [0, r-1]$, and

$$\{i \pmod p : a^i \in B_{j,k}\} = \{i \pmod p : a^i \in B_{0,0}\}.$$

This implies that $B \subset i + p\mathbb{Z}_{p^nqr}$, so it does not generate $\mathbb{Z}_{p^nqr}$, which is a contradiction. This ends the proof of claim.

Now we divide our discussion into two cases.

Case 1: p **is an odd prime.**

Since $q, r, qr \in \mathcal{Z}_A$, by Lemma 3.3 (4) and (5),

$$\chi_{1,p^n}\left(\sum_{j=0}^{q-1} A_{j,k'}\right) = \chi_{1,p^n}\left(\sum_{k=0}^{r-1} A_{j',k}\right) = 0 \text{ for all } j' \in [0, q-1], k' \in [0, r-1].$$

In other words, $\sum_{j=0}^{q-1} A_{j,k'}$ and $\sum_{k=0}^{r-1} A_{j',k}$ are unions of some $\mathbb{Z}_p$-cosets. Note that $1 \notin \mathcal{Z}_A$. There exist j_1, k_1 such that $\chi_{1,p^n}(A_{j_1,k_1}) \neq 0$. Hence, there exists $a^{i_0} \in A_{j_1,k_1}$ such that at least 2 of $a^{i_0+tp^{n-1}}, t = 1, \ldots, p-1$ do not belong to A_{j_1,k_1}, say $a^{i_0+p^{n-1}}$ and $a^{i_0+2p^{n-1}}$ (if there are $p-1$ of $a^{i_0+tp^{n-1}}$, $t = 0, \ldots, p-1$ belong to A_{j_1,k_1} and the remaining one belong to $A_{j_1,k_1'}$, then change A_{j_1,k_1} to $A_{j_1,k_1'}$). Moreover, $a^{i_0+p^{n-1}} \in A_{j_2,k_1}$ and $a^{i_0+2p^{n-1}} \in A_{j_1,k_2}$ for some j_2, k_2 with $j_2 \neq j_1$ and $k_2 \neq k_1$. Therefore, $p^{n-1} \in \mathcal{Z}_B$, which is a contradiction.

Case 2: $p = 2$.

We divide our discussion into two subcases.

Subcase 2.1: For all j, k, $|\{i \pmod 2 : a^i \in B_{j,k}\}| \leq 1$.

Claim: $B_{j,k} = \emptyset$ **for all** $j \in [1, q-1], k \in [1, r-1]$.

Assume to the contrary, there exist $j_0 \in [1, q-1]$, $k_0 \in [1, r-1]$ such that $B_{j_0,k_0} \neq \emptyset$. Note that $e \in B_{0,0}$ and $1 \notin \mathcal{Z}_A$. We can get that

$$\{i \pmod 2 : a^i \in B_{j_0,k_0}\} = \{0\},$$
$$1 \notin \{i \pmod 2 : a^i \in \cup_{j\in[0,q-1],k\in[0,r-1]} B_{j,k} \backslash (B_{j_0,0} \cup B_{0,k_0})\}.$$

Since B generates $\mathbb{Z}_{p^n qr}$, then $1 \in \{i \pmod 2 : a^i \in \cup_{j\in[0,q-1],k\in[0,r-1]} B_{j,k}\}$. Hence $1 \in \{i \pmod 2 : a^i \in B_{j_0,0} \cup B_{0,k_0}\}$.

If both $B_{j_0,0}$ and B_{0,k_0} are nonempty, then $\{i \pmod 2 : a^i \in B_{0,k_0}\} = \{i \pmod 2 : a^i \in B_{j_0,0}\} = \{1\}$ and

$$B_{j,k} = \emptyset \text{ for all } (j,k) \neq (0,0), (j_0,k_0), (j_0,0), (0,k_0).$$

For any $j_1 \neq j_0, k_1 \neq k_0$, by Equation (5), we have $|B_{j_1,k_1}| - |B_{j_1,0}| - |B_{0,k_1}| + |B_{0,0}| = 0$. Then $|B_{0,0}| = 0$, which is a contradiction.

If only one of $B_{j_0,0}$ and B_{0,k_0} is nonempty, say B_{0,k_0}, then $\{i \pmod 2 : a^i \in B_{0,k_0}\} = \{1\}$, $B_{j_0,0} = \emptyset$ and

$$\{i \pmod 2 : a^i \in \cup_{j\in[1,q-1]} B_{j,k_0}\} = \{i \pmod 2 : a^i \in \cup_{k\in[0,r-1]\backslash\{k_0\}} B_{0,k}\} = \{0\}.$$

By Equation (5), we have

$$|B_{0,k_1}| = |B_{0,k_2}| \text{ for all } k_1, k_2 \in [0, r-1]\backslash\{k_0\},$$

$$|B_{j_1,k_0}| = |B_{j_2,k_0}| \text{ for all } j_1, j_2 \in [1, q-1],$$
$$|B_{0,k_0}| = |B_{0,k_1}| + |B_{j_1,k_0}| \text{ for all } k_1 \in [0, r-1]\backslash\{k_0\}, j_1 \in [1, q-1].$$

Since $p^{n-1}q, p^{n-1}r \in \mathcal{Z}_B$, by Corollary 3.2 (2) and (3),

$$\chi_{p^{n-1},p^n}\left(\sum_{j=0}^{q-1}(B_{j,k_0} - B_{j,0})\right) = 0,$$
$$\chi_{p^{n-1},p^n}\left(\sum_{k=0}^{r-1}(B_{j_0,k} - B_{0,k})\right) = 0.$$

From above equations, we can get

$$|B_{0,0}| = \sum_{j=1}^{q-1}|B_{j,k_0}| - |B_{0,k_0}| = (q-1)|B_{j_0,k_0}| - |B_{0,k_0}|,$$
$$|B_{j_0,k_0}| = \sum_{k\in[0,r-1]\backslash\{k_0\}}|B_{0,k}| - |B_{0,k_0}| = (r-1)|B_{0,0}| - |B_{0,k_0}|,$$

which contradicts $|B_{0,k_0}| = |B_{0,0}| + |B_{j_0,k_0}|$. This ends the proof of claim.

Since B generates $\mathbb{Z}_{p^n qr}$, then $\cup_{j=1}^{q-1} B_{j,0} \neq \emptyset$ and $\cup_{k=1}^{r-1} B_{0,k} \neq \emptyset$. Note that $1 \notin \mathcal{Z}_A$. We can get that

$$\{i \pmod 2 : a^i \in \cup_{j=1}^{q-1} B_{j,0}\} = \{i \pmod 2 : a^i \in \cup_{k=1}^{r-1} B_{0,k}\} = \{1\}.$$

By Equation (5), we have

$$|B_{0,0}| = |B_{0,k}| + |B_{j,0}| \text{ for } j \in [1, q-1], k \in [1, r-1],$$

which leads to

$$|B_{0,k_1}| = |B_{0,k_2}| \text{ for } k_1, k_2 \in [1, r-1],$$
$$|B_{j_1,0}| = |B_{j_2,0}| \text{ for } j_1, j_2 \in [1, q-1].$$

Since $p^{n-1}q, p^{n-1}r \in \mathcal{Z}_B$, by Corollary 3.2 (2) and (3),

$$\chi_{p^{n-1},p^n}\left(\sum_{j=0}^{q-1}(B_{j,k} - B_{j,0})\right) = 0,$$
$$\chi_{p^{n-1},p^n}\left(\sum_{k=0}^{r-1}(B_{j,k} - B_{0,k})\right) = 0.$$

In other words,

$$|B_{0,0}| - (q-1)|B_{1,0}| = |B_{0,0}| - \sum_{j=1}^{q-1} |B_{j,0}| = -\sum_{j=0}^{q-1} |B_{j,1}| = -|B_{0,1}|, \quad (7)$$

$$|B_{0,0}| - (r-1)|B_{0,1}| = |B_{0,0}| - \sum_{k=1}^{r-1} |B_{0,k}| = -\sum_{k=0}^{r-1} |B_{1,k}| = -|B_{1,0}|. \quad (8)$$

Combining above two equations, we have $q|B_{1,0}| = r|B_{0,1}|$. Assume that $|B_{1,0}| = rm$ for some $m \in \mathbb{Z}_{>0}$, then $|B_{0,1}| = qm$ and $|B_{0,0}| = (q+r)m$. By Equation (7), we have $(q+r)m - (q-1)rm = -qm$, that is $(qr - 2q - 2r)m = 0$, which contradicts $2 \nmid qr$.

Subcase 2.2: There exist j, k such that $\{i \pmod 2 : a^i \in B_{j,k}\} = \{0, 1\}$.

WLOG, assume that $\{i \pmod 2 : a^i \in B_{0,0}\} = \{0, 1\}$. Since $1 \notin \mathcal{Z}_A$, then

$$B_{j,k} = \emptyset \text{ for all } j \in [1, q-1], k \in [1, r-1].$$

Since B generates $\mathbb{Z}_{p^n qr}$, then $\cup_{j=1}^{q-1} B_{j,0} \neq \emptyset$ and $\cup_{k=1}^{r-1} B_{0,k} \neq \emptyset$. Note that $1 \notin \mathcal{Z}_A$. We can get that

$$|\{i \pmod 2 : a^i \in \cup_{j=1}^{q-1} B_{j,0}\}| = |\{i \pmod 2 : a^i \in \cup_{k=1}^{r-1} B_{0,k}\}| = 1,$$
$$\text{and } \{i \pmod 2 : a^i \in \cup_{j=1}^{q-1} B_{j,0}\} = \{i \pmod 2 : a^i \in \cup_{k=1}^{r-1} B_{0,k}\}.$$

WLOG, assume that $\{i \pmod 2 : a^i \in \cup_{j=1}^{q-1} B_{j,0}\} = \{i \pmod 2 : a^i \in \cup_{k=1}^{r-1} B_{0,k}\} = \{0\}$. By Equation (5),

$$|B_{0,0}| = |B_{0,k}| + |B_{j,0}| \text{ for } j \in [1, q-1], k \in [1, r-1],$$

which leads to

$$|B_{0,k_1}| = |B_{0,k_2}| \text{ for } k_1, k_2 \in [1, r-1],$$
$$|B_{j_1,0}| = |B_{j_2,0}| \text{ for } j_1, j_2 \in [1, q-1].$$

Since $p^{n-1}q, p^{n-1}r \in \mathcal{Z}_B$, by Corollary 3.2 (2) and (3),

$$\chi_{p^{n-1},p^n}\left(\sum_{j=0}^{q-1}(B_{j,k} - B_{j,0})\right) = 0,$$

$$\chi_{p^{n-1},p^n}\left(\sum_{k=0}^{r-1}(B_{j,k} - B_{0,k})\right) = 0.$$

Let $u = |\{b \in B_{0,0} : b \pmod 2 = 0\}|$ and $v = |\{b \in B_{0,0} : b \pmod 2 = 1\}|$, then we have

$$u + v = |B_{0,0}| = |B_{1,0}| + |B_{0,1}|, \tag{9}$$

$$(u - v) + (q - 1)|B_{1,0}| = \chi_{p^{n-1},p^n}(B_{0,0}) + \sum_{j=1}^{q-1} |B_{j,0}| = \sum_{j=0}^{q-1} |B_{j,1}| = |B_{0,1}|, \tag{10}$$

$$(u - v) + (r - 1)|B_{0,1}| = \chi_{p^{n-1},p^n}(B_{0,0}) + \sum_{k=1}^{r-1} |B_{0,k}| = \sum_{k=0}^{r-1} |B_{1,k}| = |B_{1,0}|. \tag{11}$$

By Equations (10) and (11), we have $r|B_{0,1}| = q|B_{1,0}|$. Assume that $|B_{1,0}| = rm$ for some $m \in \mathbb{Z}_{>0}$, then $|B_{0,1}| = qm$ and $|B_{0,0}| = (q + r)m$. By Equations (9) and (10), we get

$$u - v = (q + r - qr)m,$$
$$u + v = (q + r)m.$$

Combining above two equations, we obtain $2u = (2q + 2r - qr)m \geq 0$. Since q, r are distinct odd primes, then $(q, r) = (3, 5)$ or $(5, 3)$. WLOG, assume that $q = 3$ and $r = 5$. Then we can get that $|B_{0,0}| = 8m$, $|B_{j,0}| = 5m$, $|B_{0,k}| = 3m$ and $|A| = |B| = 30m$. By the pigeonhole principle, we have $|I_1| \geq \log_2(8m)$, that is $2^{|I_1|} \geq 8m$. On the other hand, by the definition of I_1, we have $2^{|I_1|} \mid |A|$, and then $2^{|I_1|} \mid 2m$, which is a contradiction. □

Lemma 4.4 $|J_2| \geq 1$.

Proof If $|J_2| = 0$, then $1 \in \mathcal{Z}_A$ by Lemma 4.3 (1). By Corollary 3.2 (1), we have

$$\chi_{1,p^n}(A_{j,k} - A_{j,0} - A_{0,k} + A_{0,0}) = 0 \text{ for all } j \in [0, q-1], k \in [0, r-1].$$

Since $p^n q \notin \mathcal{Z}_B$, by Remark 4.1 (3), we have $A_{j,k} \cap A_{j,0} = \emptyset$ and $A_{0,k} \cap A_{0,0} = \emptyset$. Similarly, we can prove that

$$(A_{j,k} \cup A_{0,0}) \cap (A_{j,0} \cup A_{0,k}) = \emptyset. \tag{12}$$

Let $A_{j,k} + A_{0,0} = \sum_{i=0}^{p^n-1} x_i a^i$ and $A_{j,0} + A_{0,k} = \sum_{i=0}^{p^n-1} y_i a^i$, where $x_i, y_i \in \{0, 1, 2\}$. By Equation (12), we have $x_i y_i = 0$ for all $i \in [0, p^n - 1]$. Since $\chi_{1,p^n}(A_{j,k} - A_{j,0} - A_{0,k} + A_{0,0}) = \sum_{i=0}^{p^n-1} (x_i - y_i)\zeta_{p^n}^i = 0$, and $x_i - y_i = x_i$ or $-y_i$, by Lemma 2.9, we have $\chi_{1,p^n}(A_{j,k} + A_{0,0}) = 0$.

If there exist j, k such that $\chi_{1,p^n}(A_{j,k}) \neq 0$, then $\chi_{1,p^n}(A_{0,0}) \neq 0$. Hence, there exists $a^{i_0} \in A_{0,0}$ such that $a^{i_0 + tp^{n-1}} \notin A_{0,0}$ for some $t \in [1, p-1]$, hence $a^{i_0 + tp^{n-1}} \in A_{j,k}$. If $r \geq 3$, a similar discussion as above, we can get that $a^{i_0 + tp^{n-1}} \in A_{j,k'}$ for some $k' \neq k$. Hence, $p^n q \in \mathcal{Z}_B$, which is a contradiction. If $r = 2$ and $q \geq 3$, we have

$a^{i_0+tp^{n-1}} \in A_{j',k}$ for some $j' \neq j$. Hence, $p^n r \in \mathcal{Z}_B$, which is also a contradiction. Therefore, $\chi_{1,p^n}(A_{j,k}) = 0$ for all $j \in [0, q-1], k \in [0, r-1]$. This shows that A is a union of $\mathbb{Z}_p$-cosets, which is a contradiction. □

Lemma 4.5 (1) *$p^n r \in \mathcal{Z}_A$ or $p^n r \in \mathcal{Z}_B$;*
(2) *$p^n q \in \mathcal{Z}_A$ or $p^n q \in \mathcal{Z}_B$.*

Proof We will only prove the first statement, the proof of the second statement is similar. Assume to the contrary, $p^n r \notin \mathcal{Z}_A$ and $p^n r \notin \mathcal{Z}_B$. By Lemmas 4.3 and 4.4, $1 \in \mathcal{Z}_A$ and $1, p^n q \in \mathcal{Z}_B$. Then $r \mid |A|$, we may assume that $|A| = p^t rm$, where $\gcd(p, m) = 1$.

If $r \in \mathcal{Z}_A$, by Lemma 3.3 (2), $\chi_{1,p^n}(A_{j,k} - A_{0,k}) = 0$. Since $p^n r \notin \mathcal{Z}_B$, then $A_{j,k} \cap A_{0,k} = \emptyset$. Hence, $\chi_{1,p^n}(A_{j,k}) = 0$ for all $j \in [0, q-1], k \in [0, r-1]$. This shows that A is a union of $\mathbb{Z}_p$-cosets, which is a contradiction. Therefore $r \notin \mathcal{Z}_A$.

Claim: $p^{n-1}qr \in \mathcal{Z}_B$.

Assume to the contrary, $p^{n-1}qr \notin \mathcal{Z}_B$. Since $1 \in \mathcal{Z}_A$, by Corollary 3.2 (1),

$$\chi_{1,p^n}(A_{j,k} - A_{j,0} - A_{0,k} + A_{0,0}) = 0.$$

Then for any $a^{i_0} \in A_{0,0}$, we have $a^{i_0+up^{n-1}} \notin A_{0,0}$ for $u \in [1, p-1]$. Note that $p^n r \notin \mathcal{Z}_B$. We can get that $A_{j,0} \cap A_{0,0} = \emptyset$, and then $a^{i_0} \notin A_{j,0}$.

If $a^{i_0} \notin A_{0,k}$, then $a^{i_0+up^{n-1}} \in A_{j,k}$. This leads to $p = 2$, since every $A_{j,k}$ contains at most one element from every $\mathbb{Z}_p$-coset, hence $q > 2$. Considering $\chi_{1,p^n}(A_{j',k} - A_{j',0} - A_{0,k} + A_{0,0}) = 0$ for some $j' \neq j$, similarly as before, we can get $a^{i_0+up^{n-1}} \in A_{j',k}$. This shows that $p^n r \in \mathcal{Z}_B$, which is a contradiction. Hence, $a^{i_0} \in A_{0,k}$.

Then we have $A_{0,k} - A_{0,0} = 0$. Therefore, $A_{j,k} = A_{j,0}$ for all j, k, and then $A = \sum_{j=0}^{q-1} A_{j,0} b^j \sum_{k=0}^{r-1} c^k$, which contradicts the fact that A is not a union of $\mathbb{Z}_r$-cosets. This ends the proof of claim.

Claim: $qr \in \mathcal{Z}_A$.

Assume to the contrary, $qr \notin \mathcal{Z}_A$. Since $p^{n-1}qr, p^n q \in \mathcal{Z}_B$, by Corollary 3.2 (2) and (4), we have

$$\sum_{j=0}^{q-1} |B_{j,k}| = p^t m,$$

$$\chi_{p^{n-1},p^n}\left(\sum_{j=0}^{q-1}\sum_{k=0}^{r-1} B_{j,k}\right) = 0.$$

Note that $r, qr \notin \mathcal{Z}_A$. We have $\{i \pmod p) : a^i \in \cup_{j=0}^{q-1} B_{j,k}\} = \{i_k\}$ for some $i_k \in [0, p-1]$. Then we can compute to get that

$$0 = \chi_{p^{n-1},p^n}\left(\sum_{j=0}^{q-1}\sum_{k=0}^{r-1} B_{j,k}\right)$$

$$
\begin{aligned}
&= \sum_{k=0}^{r-1} \chi_{p^{n-1},p^n} \left(\sum_{j=0}^{q-1} B_{j,k} \right) \\
&= \sum_{k=0}^{r-1} \sum_{j=0}^{q-1} |B_{j,k}| e^{\frac{2\pi i \cdot i_k}{p}} \\
&= p^t m \sum_{k=0}^{r-1} e^{\frac{2\pi i \cdot i_k}{p}},
\end{aligned}
$$

which contradicts $p \nmid r$. This ends the proof of claim.

Since $r \notin \mathcal{Z}_A$, WLOG, the nonempty sets $B_{j,k}$ are as follows (after permuting the rows and columns of $(B_{j,k})_{j\in[0,q-1],k\in[0,r-1]}$)

$$
\begin{array}{ccccccccccccc}
B_{0,0} \cdots B_{0,s_0-1} & & & B_{0,s_u} & \cdots & B_{0,s_{u+1}-1} & \cdots & B_{0,s_{u+p-1}} & & B_{0,s_{u+p}-1} \\
 & \ddots & & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
 & & B_{u,s_{u-1}} \cdots B_{u,s_u-1} & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
 & & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
 & & & B_{q-1,s_u} & \cdots & B_{q-1,s_{u+1}-1} & \cdots & B_{q-1,s_{u+p-1}} & & B_{q-1,s_{u+p}-1}
\end{array},
$$

where $0 =: s_{-1} \le s_0 \le s_1 \le \cdots \le s_{u+p} := r$, $|\{i \pmod p) : a^i \in B_{j,k}\}| \ge 2$ for $j \in [0,u]$, $k \in [s_{j-1}, s_j - 1]$, and $\{l \pmod p) : a^l \in \cup_{j=0}^{q-1} B_{j,k}\} = \{i\}$ for $k \in [s_{u+i}, s_{u+i+1} - 1]$, $i \in [0, p-1]$. Since $p^n q \in \mathcal{Z}_B$, we have

$$
\begin{aligned}
&|B_{j,k}| = p^t m \text{ for } j \in [0,u], k \in [s_{j-1}, s_j - 1], \\
&\sum_{j=0}^{q-1} |B_{j,k}| = p^t m \text{ for } k \in [s_u, s_{u+p} - 1].
\end{aligned}
$$

Case 1: $0 < s_u < r$.

For this case, $|I_1| \le t$. By the pigeonhole principle, we have $|I_1| \ge \log_p(p^t m)$. Then $m = 1$.

If $q \in \mathcal{Z}_A$, note that $1, qr \in \mathcal{Z}_A$, by Lemma 3.3 (1) and (4), we have

$$
\begin{aligned}
&\chi_{1,p^n}(A_{j,k} - A_{j,0}) = 0 \text{ for all } j \in [0, q-1], k \in [0, r-1], \\
&\chi_{1,p^n} \left(\sum_{j=0}^{q-1} A_{j,k} \right) = 0 \text{ for all } k \in [0, r-1].
\end{aligned}
$$

Since $r \notin \mathcal{Z}_A$, then there exists j, k such that $\chi_{1,p^n}(A_{j,k}) \neq 0$. Hence, there exists $a^{i_0} \in A_{j,k}$ but $a^{i_0 + up^{n-1}} \notin A_{j,k}$ for some $u \in [1, p-1]$. Moreover, $a^{i_0} \in A_{j,0}$ and $a^{i_0+up^{n-1}} \in A_{j',k}$ for some $j' \neq j$. This shows that $p^{n-1}, p^{n-1} r \in \mathcal{Z}_B$. By

Lemma 3.3 (2), we have

$$\chi_{p^{n-1},p^n}(B_{j,k} - B_{0,k}) = 0 \text{ for all } j \in [0, q-1], k \in [0, r-1].$$

Then we deduce that $|B_{j,k}| = |B_{0,k}|$ for $j \in [0, q-1], k \in [s_u, s_{u+p} - 1]$, which contradicts $\sum_{j=0}^{q-1} |B_{j,k}| = p^t$ for $k \in [s_u, s_{u+p} - 1]$. Hence $q \notin \mathcal{Z}_A$.

Now the nonempty sets $B_{j,k}$ are as follows

$$\begin{array}{llllll}
B_{0,0} & & & & & \\
\ddots & & & & & \\
& B_{u,u} & & & & \\
& & B_{u+1,s_u} \ \cdots \ B_{u+1,s_{u+1}-1} & & & \\
& & \vdots \quad\ \ddots \quad\ \vdots & & & \\
& & B_{u+j_1,s_u} \ \cdots \ B_{u+j_1,s_{u+1}-1} & & & \\
& & & \ddots & & \\
& & & & B_{u+j_{p-1}+1,s_{u+p-1}} \ \cdots \ B_{u+j_{p-1}+1,s_{u+p}-1} & \\
& & & & \vdots \quad\ \ddots \quad\ \vdots & \\
& & & & B_{u+j_p,s_{u+p-1}} \ \cdots \ B_{u+j_p,s_{u+p}-1} &
\end{array}.$$

Since $\cup_{l=0}^{q-1}\{l \pmod p) : a^l \in B_{j,k}\} = \{i\}$ for $k \in [s_{u+i}, s_{u+i+1} - 1], i \in [0, p-1]$, then p^{n-1}, $p^{n-1}q$, $p^{n-1}r \notin \mathcal{Z}_B$. Hence, for any $j_1 \in [0, q-1]$, $k_1 \in [0, r-1]$ and $a^{i_0} \in A_{j_1,k_1}$, we have $a^{i_0+up^{n-1}} \notin A_{j,k}$ for all $u \in [1, p-1]$, $(j, k) \neq (j_1, k_1)$. Note that $qr \in \mathcal{Z}_A$. By Corollary 3.2 (4), $\chi_{1,p^n}(\sum_{j=0}^{q-1}\sum_{k=0}^{r-1} A_{j,k}) = 0$. Then we have $\chi_{1,p^n}(A_{j,k}) = 0$ for all $j \in [0, q-1], k \in [0, r-1]$. This implies A is a union of $\mathbb{Z}_p$-cosets, which is a contradiction.

Case 2: $s_u = 0$.

For this case, the nonempty sets $B_{j,k}$ are as follows

$$\begin{array}{ccccccc}
B_{0,s_u} & \cdots & B_{0,s_{u+1}-1} & \cdots & B_{0,s_{u+p-1}} & & B_{0,s_{u+p}-1} \\
\vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\
\cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
B_{q-1,s_u} & \cdots & B_{q-1,s_{u+1}-1} & \cdots & B_{q-1,s_{u+p-1}} & & B_{q-1,s_{u+p}-1}
\end{array},$$

where $0 = s_u \leq \cdots \leq s_{u+p} = r$, and $\{l \pmod p) : a^l \in \cup_{j=0}^{q-1} B_{j,k}\} = \{i\}$ for $k \in [s_{u+i}, s_{u+i+1} - 1], i \in [0, p-1]$.

If $q \in \mathcal{Z}_A$, note that $1, qr \in \mathcal{Z}_A$, by Lemma 3.3 (1) and (4), we have

$$\chi_{1,p^n}(A_{j,k} - A_{j,0}) = 0 \text{ for all } j \in [0, q-1], k \in [0, r-1],$$
$$\chi_{1,p^n}\left(\sum_{j=0}^{q-1} A_{j,k}\right) = 0 \text{ for all } k \in [0, r-1].$$

Since $r \notin \mathcal{Z}_A$, then there exist j, k such that $\chi_{1,p^n}(A_{j,k}) \neq 0$. Hence, there exists $a^{i_0} \in A_{j,k}$ but $a^{i_0+up^{n-1}} \notin A_{j,k}$ for some $u \in [1, p-1]$. Moreover, $a^{i_0} \in A_{j,0}$ and $a^{i_0+up^{n-1}} \in A_{j',k}$. This shows that p^{n-1}, $p^{n-1}r \in \mathcal{Z}_B$. By Lemma 3.3 (2), we have

$$\chi_{p^{n-1},p^n}(B_{j,k} - B_{0,k}) = 0.$$

Thus $|B_{j,k}| = |B_{0,k}|$ for $k \in [s_u, s_{u+p} - 1]$. Therefore, $|B| = \sum_{j,k} |B_{j,k}| = p^t qrm'$, and $|B_{j,k}| = p^t m'$ for all $j \in [0, q-1]$, $k \in [0, r-1]$, which contradicts $p^n r \notin \mathcal{Z}_B$. Hence, $q \notin \mathcal{Z}_A$.

Now the nonempty sets $B_{j,k}$ are as follows

$$\begin{array}{cccccc}
B_{0,s_u} & \cdots & B_{0,s_{u+1}-1} & & & \\
\vdots & \ddots & \vdots & & & \\
B_{j_1,s_u} & \cdots & B_{j_1,s_{u+1}-1} & & & \\
 & & & \ddots & & \\
 & & & B_{j_{p-1}+1,s_{u+p-1}} & \cdots & B_{j_{p-1}+1,s_{u+p}-1} \\
 & & & \vdots & \ddots & \vdots \\
 & & & B_{j_p,s_{u+p-1}} & \cdots & B_{j_p,s_{u+p}-1}
\end{array}.$$

Since $\{l \pmod p : a^l \in \cup_{i=0}^{q-1} B_{j,k}\} = \{i\}$ for $k \in [s_{u+i}, s_{u+i+1} - 1]$, $i \in [0, p-1]$, then $p^{n-1}q$, $p^{n-1}r \notin \mathcal{Z}_B$.

If $p^{n-1} \in \mathcal{Z}_B$, by Corollary 3.2 (1), we have

$$\chi_{p^{n-1},p^n}(B_{j_{p-1}+1,s_{u+p-1}} - B_{j_{p-1}+1,0} - B_{0,s_{u+p-1}} + B_{0,0}) = 0.$$

That is $\chi_{p^{n-1},p^n}(B_{j_{p-1}+1,s_{u+p-1}} + B_{0,0}) = 0$. Note that $\{i \pmod p : a^i \in B_{0,0}\} = \{0\}$ and $\{i \pmod p : a^i \in B_{j_{p-1}+1,s_{u+p-1}}\} = \{p-1\}$. We deduce that $p = 2$ and $|B_{j_{p-1}+1,s_{u+p-1}}| = |B_{0,0}|$. A similar discussion as above, we can get that all nonempty $B_{j,k}$ have the same size. Hence $j_p < q - 1$. By Corollary 3.2 (1), we have

$$\chi_{p^{n-1},p^n}(B_{q-1,r-1} - B_{q-1,0} - B_{0,r-1} + B_{0,0}) = 0.$$

This shows that $\chi_{p^{n-1},p^n}(B_{0,0}) = 0$. This contradicts $\{i \pmod p : a^i \in B_{0,0}\} = \{0\}$. Hence $p^{n-1} \notin \mathcal{Z}_B$.

Note that $p^{n-1}q$, $p^{n-1}r \notin \mathcal{Z}_B$. Then for any $j_1 \in [0, q-1]$, $k_1 \in [0, r-1]$, $a^{i_0} \in A_{j_1,k_1}$, we have $a^{i_0+up^{n-1}} \notin A_{j,k}$ for all $u \in [1, p-1]$ and $(j,k) \neq (j_1, k_1)$. Since $qr \in \mathcal{Z}_A$, by Corollary 3.2 (4),

$$\chi_{1,p^n}\left(\sum_{j=0}^{q-1}\sum_{k=0}^{r-1} A_{j,k}\right) = 0.$$

Then we have $\chi_{1,p^n}(A_{j,k}) = 0$ for all $j \in [0, q-1]$, $k \in [0, r-1]$. This implies A is a union of $\mathbb{Z}_p$-cosets, which is a contradiction.

Case 3: $s_u = r$.

For this case, the nonempty sets $B_{j,k}$ are as follows

$$\begin{matrix} B_{0,0} \cdots B_{0,s_0-1} & & \\ & \ddots & \\ & & B_{u,s_{u-1}} \cdots B_{u,s_u-1} \end{matrix},$$

where $s_u = r$ and $u \le q-1$. Then $|B_{j,k}| = p^t m$ for $j \in [0, u]$ and $k \in [s_{j-1}, s_j - 1]$. By the pigeonhole principle, we have $m = 1$, $|I_1| = t$, and $|B_{j,k}| = p^t$ for $j \in [0, u]$, $k \in [s_{j-1}, s_j - 1]$. Hence $|A| = |B| = p^t r$.

By Lemma 2.10, for all $j \in [0, u]$ and $k \in [s_{j-1}, s_j - 1]$, the elements of $B_{j,k}$ have the form $a^{\alpha_0+\alpha_1 p+\cdots+\alpha_{n-1}p^{n-1}}$, where $\alpha_i \in [0, p-1]$ satisfy the following conditions:

1. if $i \in I_1$, then α_i can take every value from $[0, p-1]$;
2. if $j \notin I_1$, the value of α_j depends solely on $\alpha_0, \ldots, \alpha_{j-1}$.

For any $i \in I_1$, let $s = \{l \in I_1 : l \ge i\}$, we can partition $B_{j,k}$ into p^{t-s} parts, say $P_1, P_2, \ldots, P_{p^{t-s}}$, such that for any $a^u, a^v \in P_x$, we have $v_p(u-v) \ge i$. Then $|P_x| = p^s$, $x \in [1, p^{t-s}]$. Fix an element $a^{u_0} \in P_x$, for each $w \in [0, p-1]$, there are exactly p^{s-1}'s $a^v \in P_x$ such that $u_0 - v$ has the form $wp^i + \alpha_{i+1}p^{i+1} + \cdots + \alpha_{n-1}p^{n-1}$. Then we can compute to get that $\chi_{p^{n-1-i},p^n}(B_{j,k}) = \chi_{p^{n-1-i},p^n}(\sum_{x=1}^{p^{t-s}} P_x) = 0$ for any $i \in I_1$, $j \in [0, q-1]$, $k \in [0, r-1]$. Hence $J_1 = \{n-1-i : i \in I_1\}$.

Claim: $p^n \notin \mathcal{Z}_B$.

If $p^n \in \mathcal{Z}_B$, then by Corollary 3.2 (1),

$$|B_{u,s_{u-1}}| - |B_{0,s_{u-1}}| - |B_{u,0}| + |B_{0,0}| = 0.$$

We have $|B_{u,s_{u-1}}| + |B_{0,0}| = 0$, which is a contradiction. Hence $p^n \notin \mathcal{Z}_B$. This ends the proof of claim.

Claim: For $i \in [0, n-1]$, $p^i \in \mathcal{Z}_B$ **if and only if** $p^i qr \in \mathcal{Z}_B$.

If $p^i qr \in \mathcal{Z}_B$, that is $i \in J_1$, from above discussion, we have $\chi_{p^i,p^n}(B_{j,k}) = 0$ for any $j \in [0, q-1]$, $k \in [0, r-1]$, and so $p^i \in \mathcal{Z}_B$. Now we assume that $p^i \in \mathcal{Z}_B$.

If $u < q-1$, by Corollary 3.2 (1),

$$\chi_{p^i,p^n}(B_{u,s_{u-1}} - B_{u,0} - B_{q-1,s_{u-1}} + B_{q-1,0}) = 0.$$

Then we get $\chi_{p^i,p^n}(B_{u,s_{u-1}}) = 0$. Similarly, we can get that $\chi_{p^i,p^n}(B_{j,k}) = 0$ for all $j \in [0, q-1]$, $k \in [0, r-1]$. Hence $p^i qr \in \mathcal{Z}_B$.

If $u = q-1$ and $q \ge 3$, by Corollary 3.2 (1),

$$\chi_{p^i,p^n}(B_{u,s_{u-1}} - B_{u,0} - B_{u-1,s_{u-1}} + B_{u-1,0}) = 0.$$

Then we get $\chi_{p^i,p^n}(B_{u,s_{u-1}})=0$. Similarly, we can get that $\chi_{p^i,p^n}(B_{j,k})=0$ for all $j\in[0,q-1]$, $k\in[0,r-1]$. Hence $p^iqr\in\mathcal{Z}_B$.

If $u=q-1$ and $q=2$, by Corollary 3.2 (1),

$$\chi_{p^i,p^n}(B_{1,s_0}-B_{1,0}-B_{0,s_0}+B_{0,0})=0.$$

That is

$$\chi_{p^i,p^n}(B_{1,s_0}+B_{0,0})=0.$$

Then for any $a^u\in B_{0,0}$, there exist at least two elements among $a^u, a^{u+p^{n-1-i}+f(u,1)p^j}, a^{u+2p^{n-1-i}+f(u,2)p^j}$ that belong to $B_{0,0}$ or B_{1,s_0}, where $f(u,1)$, $f(u,2)$ are certain integers and $j>n-1-i$. This implies $n-1-i\in I_1$, which in turn implies $i\in J_1$. That is $p^iqr\in\mathcal{Z}_B$. This ends the proof of claim.

Subcase 3.1: $r>q$.

Define

$$T=\{a^{\sum_{i\in[0,n-1]\setminus J_1}a_ip^i}(bc)^j : a_i\in[0,p-1], j\in[0,q-1]\}.$$

Note that the elements of $TT^{(-1)}$ have the form $(bc)^j$ or $a^l(bc)^j$, where $v_p(l)\in[0,n-1]\setminus J_1$, $j\in[0,q-1]$. On the other hand, from above claims, $p^n\notin\mathcal{Z}_B$ and $p^i, p^iqr\notin\mathcal{Z}_B$ for all $i\in[0,n-1]\setminus J_1$. This implies $AA^{(-1)}\cap TT^{(-1)}=\{e\}$ (note that the group is written multiplicatively, and this is the multiplicative version of Lemma 2.4 (d)). Since $|A||T|=p^nqr$, by Lemma 2.4 (d), (A,T) forms a tiling pair in $\mathbb{Z}_{p^nqr}$, which is a contradiction.

Subcase 3.2: $q>r$.

For this case, we have $B_{q-1,k}=\emptyset$ for all $k\in[0,r-1]$.

If $p^ir\in\mathcal{Z}_B$, by Corollary 3.2 (3), we have

$$\chi_{p^i,p^n}\left(\sum_{k=0}^{r-1}(B_{j,k}-B_{q-1,k})\right)=0.$$

that is $\chi_{p^i,p^n}(\sum_{k=0}^{r-1}B_{j,k})=0$. Then we have $\chi_{p^i,p^n}(\sum_{j=0}^{q-1}\sum_{k=0}^{r-1}B_{j,k})=0$. By Corollary 3.2 (4), $p^iqr\in\mathcal{Z}_B$. Hence, we have proved that $p^ir\notin\mathcal{Z}_B$ for all $i\in[0,n-1]\setminus J_1$.

Define

$$T=\{a^{\sum_{i\in[0,n-1]\setminus J_1}a_ip^i}b^j : a_i\in[0,p-1], j\in[0,q-1]\}.$$

Note that the elements of $TT^{(-1)}$ have the form b^j or a^lb^j, where $v_p(l)\in[0,n-1]\setminus J_1$, $j\in[0,q-1]$. On the other hand, $p^nr\notin\mathcal{Z}_B$ and $p^ir, p^iqr\notin\mathcal{Z}_B$ for all $i\in[0,n-1]\setminus J_1$. This implies $AA^{(-1)}\cap TT^{(-1)}=\{e\}$. Since $|A||T|=p^nqr$, by Lemma 2.4 (d), (A,T) forms a tiling pair in $\mathbb{Z}_{p^nqr}$, which is a contradiction. □

By Lemma 4.5, we have the following corollary.

Corollary 4.6 $|I_2| + |J_2| \geq 2$.

Now we divide our discussion into 2 cases according to the size of I_2, J_2.

4.1 $|I_2| = 2$ or $|J_2| = 2$

Assume that $|I_1| = t$, then we have $p^t qr \mid |A|$. If $|A| = |B| > p^t qr$, then there exist $j \in [0, q-1]$, $k \in [0, r-1]$ such that $|B_{j,k}| > p^t$. By the pigeonhole principle, we have $|I_1| \geq t+1$, which is a contradiction.

Now we assume that $|A| = p^t qr$, then $|J_1| \leq t$. By the pigeonhole principle again, we have $|A_{j,k}| = p^t$ for any $j \in [0, q-1]$, $k \in [0, r-1]$. Then $|J_1| = t$. Denote

$$T := \{a^{\sum_{i \in [0,n-1] \setminus J_1} x_i p^i} : x_i \in [0, p-1]\}.$$

If $(AA^{(-1)}) \cap (TT^{(-1)}) \neq \{e\}$, then there exists $i \in [0, n-1] \setminus J_1$, such that $p^i qr \in \mathcal{Z}_B$, which is a contradiction. Hence $(AA^{(-1)}) \cap (TT^{(-1)}) = \{e\}$. By Lemma 2.4 (d), (A, T) forms a tiling pair in $\mathbb{Z}_{p^n qr}$, which contradicts the fact that A is not a tiling set.

4.2 $|I_2| = |J_2| = 1$

By Lemma 4.5, WLOG, we assume that $p^n q \in \mathcal{Z}_A$, $p^n r \notin \mathcal{Z}_A$, $p^n r \in \mathcal{Z}_B$ and $p^n q \notin \mathcal{Z}_B$. Then $qr \mid |A|$. Assume that $|A| = p^t qrm$. A similar discussion as Sect. 4.1, we can get that $m = 1$, $|A| = p^t qr$ and $|A_{j,k}| = p^t$ for $j \in [0, q-1]$, $k \in [0, r-1]$. This shows that $p^n q, p^n r \in \mathcal{Z}_A$, which is a contradiction.

Now we have proved that if (A, B) is a spectral pair in $\mathbb{Z}_{p^n qr}$, then A is a tiling set in $\mathbb{Z}_{p^n qr}$.

Acknowledgements The author expresses his gratitude to the anonymous reviewers for their detailed and constructive comments which are very helpful to the improvement of the presentation of this paper.

Data Availability Data sharing is not applicable to this article as no new data were created or analyzed in this study.

References

1. Aten, C., Ayachi, B., Bau, E., FitzPatrick, D., Iosevich, A., Liu, H., Lott, A., MacKinnon, I., Maimon, S., Nan, S., Pakianathan, J., Petridis, G., Rojas Mena, C., Sheikh, A., Tribone, T., Weill, J., Yu, C.: Tiling sets and spectral sets over finite fields. J. Funct. Anal. **273**(8), 2547–2577 (2017)
2. Coven, E.M., Meyerowitz, A.: Tiling the integers with translates of one finite set. J. Algebra **212**(1), 161–174 (1999)
3. Dutkay, D.E., Jorgensen, P.E.T.: On the universal tiling conjecture in dimension one. J. Fourier Anal. Appl. **19**(3), 467–477 (2013)
4. Dutkay, D.E., Lai, C.-K.: Some reductions of the spectral set conjecture to integers. Math. Proc. Camb. Philos. Soc. **156**(1), 123–135 (2014)
5. Fallon, T., Mayeli, A., Villano, D.: The fuglede's conjecture holds in $\mathbb{F}_p^3$ for $p = 5, 7$. Proc. Am. Math. Soc. To appear

6. Fallon, T., Kiss, G., Somlai, G.: Spectral sets and tiles in $\mathbb{Z}_p^2 \times \mathbb{Z}_q^2$. J. Funct. Anal. **282**(12), 109472 (2022)
7. Fan, A., Fan, S., Shi, R.: Compact open spectral sets in $\mathbb{Q}_p$. J. Funct. Anal. **271**(12), 3628–3661 (2016)
8. Fan, A., Fan, S., Liao, L., Shi, R.: Fuglede's conjecture holds in $\mathbb{Q}_p$. Math. Ann. **375**(1–2), 315–341 (2019)
9. Farkas, B., Matolcsi, M., Móra, P.: On Fuglede's conjecture and the existence of universal spectra. J. Fourier Anal. Appl. **12**(5), 483–494 (2006)
10. Ferguson, S.J., Sothanaphan, N.: Fuglede's conjecture fails in 4 dimensions over odd prime fields. Discret. Math. **343**(1), 111507, 7 (2020)
11. Fuglede, B.: Commuting self-adjoint partial differential operators and a group theoretic problem. J. Funct. Anal. **16**, 101–121 (1974)
12. Greenfeld, R., Lev, N.: Fuglede's spectral set conjecture for convex polytopes. Anal. PDE **10**(6), 1497–1538 (2017)
13. Iosevich, A., Katz, N., Tao, T.: The Fuglede spectral conjecture holds for convex planar domains. Math. Res. Lett. **10**(5–6), 559–569 (2003)
14. Iosevich, A., Mayeli, A., Pakianathan, J.: The Fuglede conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$. Anal. PDE **10**(4), 757–764 (2017)
15. Kiss, G., Somlai, G.: Fuglede's conjecture holds on $\mathbb{Z}_p^2 \times \mathbb{Z}_q$. Proc. Am. Math. Soc. **149**(10), 4181–4188 (2021)
16. Kiss, G., Malikiosis, R.D., Somlai, G., Vizer, M.: On the discrete Fuglede and Pompeiu problems. Anal. PDE **13**(3), 765–788 (2020)
17. Kiss, G., Malikiosis, R.D., Somlai, G., Vizer, M.: Fuglede's conjecture holds for cyclic groups of order $pqrs$. J. Fourier Anal. Appl. **28**, 79 (2022)
18. Kolountzakis, M.N., Matolcsi, M.: Complex Hadamard matrices and the spectral set conjecture. Collect. Math. (Vol. Extra), 281–291 (2006)
19. Kolountzakis, M.N., Matolcsi, M.: Tiles with no spectra. Forum Math. **18**(3), 519–528 (2006)
20. Łaba, I.: The spectral set conjecture and multiplicative properties of roots of polynomials. J. Lond. Math. Soc. (2) **65**(3), 661–671 (2002)
21. Łaba, I., Londner, I.: Splitting for integer tilings and the Coven-Meyerowitz tiling conditions. arXiv:2207.11809
22. Łaba, I., Londner, I.: Combinatorial and harmonic-analytic methods for integer tilings. Forum Math. Pi **10**, e8 1-46 (2022)
23. Łaba, I., Londner, I.: The Coven-Meyerowitz tiling conditions for 3 odd prime factors. Invent. Math. **232**, 365–470 (2023)
24. Lev, N., Matolcsi, M.: The Fuglede conjecture for convex domains is true in all dimensions. Acta Math. **228**(2), 385–420 (2022)
25. Malikiosis, R.D.: On the structure of spectral and tiling subsets of cyclic groups. Forum Math. Sigma **10**, e23 1-42 (2022)
26. Malikiosis, R.D., Kolountzakis, M.N.: Fuglede's conjecture on cyclic groups of order $p^n q$. Discret. Anal., Paper No. 12, 16 (2017)
27. Matolcsi, M.: Fuglede's conjecture fails in dimension 4. Proc. Am. Math. Soc. **133**(10), 3021–3026 (2005)
28. Pott, A.: Finite Geometry and Character Theory, vol. 1601. Springer, Berlin (1995)
29. Schmidt, B.: Characters and Cyclotomic Fields in Finite Geometry. Lecture Notes in Mathematics, vol. 1797. Springer, Berlin (2002)
30. Shi, R.: Fuglede's conjecture holds on cyclic groups $\mathbb{Z}_{pqr}$. Discret. Anal., Paper No. 14, 14 (2019)
31. Shi, R.: Equi-distributed property and spectral set conjecture on $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$. J. Lond. Math. Soc. (2) **102**(3), 1030–1046 (2020)
32. Somlai, G.: Spectral sets in $\mathbb{Z}_{p^2qr}$ tile. Discret. Anal., Paper No. 5, 10, (2023)
33. Szabó, S., Sands, A.D.: Factoring Groups into Subsets. Lecture Notes in Pure and Applied Mathematics, vol. 257. CRC Press, Boca Raton, FL (2009)
34. Tao, T.: Some notes on the coven-meyerowitz conjecture. https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/
35. Tao, T.: Fuglede's conjecture is false in 5 and higher dimensions. Math. Res. Lett. **11**(2–3), 251–258 (2004)
36. Zhang, T.: Fuglede's conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_{p^n}$. SIAM J. Discret. Math. **37**(2), 1180–1197 (2023)