

Fuglede's conjecture holds on cyclic groups

$$\mathbb{Z}_{pqr}$$

Ruxi Shi*

Received 24 July 2018; Revised 23 January 2019; Published 15 October 2019

Abstract: Fuglede's spectral set conjecture states that a subset Ω of a locally compact abelian group G tiles the group by translation if and only if there exists a subset of continuous group characters which is an orthogonal basis of $L^2(\Omega)$. We prove that Fuglede's conjecture holds on cyclic groups \mathbb{Z}_{pqr} with p, q, r distinct primes.

Key words and phrases: Spectral set, tiling, Fuglede's conjecture, vanishing sums of roots of unity

1 Introduction

Let G be a locally compact abelian group and let \widehat{G} be its dual group consisting of all continuous group characters. Let Ω be a Borel measurable subset in G with positive finite Haar measure. We say that the set Ω is a *spectral set* if there exists a subset $\Lambda \subset \widehat{G}$ which is an orthogonal basis of the Hilbert space $L^2(\Omega)$, and that Ω is a *tile* of G by translation if there exists a set $T \subset G$ of translates such that $\sum_{t \in T} 1_{\Omega}(x-t) = 1$ for almost all $x \in G$, where 1_A denotes the indicator function of a set A .

In the case where $G = \mathbb{R}^d$, Fuglede [7] formulated the following conjecture.

Conjecture 1.1. *A Borel set $\Omega \subset \mathbb{R}^d$ of positive and finite Lebesgue measure is a spectral set if and only if it is a tile.*

Fuglede's conjecture has attracted considerable attention over the last decades. Many positive results were obtained before Tao [19] disproved the conjecture by showing that the direction "Spectral \Rightarrow Tiling" does not hold when $d \geq 5$. Now it is known that the conjecture is false in both directions for $d \geq 3$ [6, 13, 14, 15]. However, the conjecture is still open in lower dimensions ($d = 1, 2$).

For any locally compact abelian group G , it is natural to formulate the following conjecture, also called Fuglede's conjecture (or spectral set conjecture) in G .

*Supported by the Centre of Excellence in Analysis and Dynamics Research funded by the Academy of Finland.

Conjecture 1.2. *A Borel set $\Omega \subset G$ of positive and finite Haar measure is a spectral set if and only if it is a tile.*

In its full generality, this conjecture is far from being proved and is false for some specific groups as Tao [19] showed. The question becomes for which group G , Fuglede's conjecture holds. For an integer $N \geq 1$, the ring of integers modulo N is denoted by $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$. We now know that Fuglede's conjecture holds on \mathbb{Z}_{p^n} [9, 5], $\mathbb{Z}_p \times \mathbb{Z}_p$ [8], p -adic field \mathbb{Q}_p [5, 4] and $\mathbb{Z}_{p^n q}$ with $n \geq 1$ [16].

Borrowing the notation from [3], write $S\text{-}T(G)$, respectively $T\text{-}S(G)$, if the direction "Bounded spectral sets \Rightarrow Tiles", respectively "Bounded tiles \Rightarrow Spectral sets", holds in G . The following relations are well established [11, 17, 10, 15, 6, 14, 2]:

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

and

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

We refer to [3] for an overview of the literature. From the above, we see that the cyclic groups play important roles in the study of the spectral set conjecture in \mathbb{R} . However, when we focus on this conjecture on cyclic groups, it is only known that this conjecture holds for \mathbb{Z}_{p^n} for p prime and very recently for $\mathbb{Z}_{p^n q}$ for p, q distinct primes. As for the direction $T\text{-}S$ alone, we know that Łaba [9] proved $T\text{-}S(\mathbb{Z}_{p^n q^m})$ for p, q distinct prime and that Łaba¹ and Meyerowitz² proved in comments on Tao's blog [20] that a tile in a cyclic group whose order is square-free always tiles by a subgroup.

In this paper, we prove that the spectral set conjecture holds in \mathbb{Z}_{pqr} with p, q, r distinct primes. This result relies heavily on the structure of vanishing sums of roots of unity, which was originally shown in [12] by Lam and Leung. Such structure is useful in the study of the zeros of the mask polynomials. Let A be a multi-set in \mathbb{Z}_N . Recall that the *mask polynomial* of A is defined to be

$$A(X) = \sum_{a \in A} m_a X^a,$$

where m_a is the multiplicity of a in A . It is clear that the degree of $A(X)$ is at most $N - 1$. Sometimes, the mask polynomial $A(X)$ is regarded as the polynomial in $\mathbb{Z}[X]/(X^N - 1)$. Actually, any integer polynomial of degree at most $N - 1$ with non-negative coefficients is a mask polynomial of some multi-set in \mathbb{Z}_N . Observe that A is a subset in \mathbb{Z}_N if and only if the coefficients of $A(X)$ are 0 or 1.

Let Φ_n be the cyclotomic polynomial of order n . Let S be the set of prime powers dividing N . Define

$$S_A = \{s \in S : \Phi_s(X) \mid A(X)\}.$$

Following Coven and Meyerowitz [1], we say that the set A satisfies the condition (T1) if

$$\#A = \prod_{s \in S_A} \Phi_s(1),$$

and that it satisfies the condition (T2) if $\Phi_{s_1 s_2 \dots s_m}(X)$ divides $A(X)$ whenever $s_1, s_2, \dots, s_m \in S_A$ are powers of distinct primes.

Now we state our main result.

¹<https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/> #comment-121464

²<https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/> #comment-112975

Theorem 1.3. *Let $A \subset \mathbb{Z}_{pqr}$ with p, q, r distinct primes. Then the following are equivalent.*

- (1) *The set A satisfies (T1) and (T2).*
- (2) *The set A is a spectral set.*
- (3) *The set A tiles \mathbb{Z}_{pqr} by translation.*

In fact, Coven and Meyerowitz [1] proved that the conditions (T1) + (T2) imply tiles, i.e. (1) \Rightarrow (3), and that tiles satisfy the condition (T1); Łaba [9] proved that conditions (T1) + (T2) imply spectral sets, i.e. (1) \Rightarrow (2); the implication (3) \Rightarrow (1) follows from Łaba and Meyerowitz's comments on Tao's blog [20]. Our novel contribution here is to prove that spectral sets satisfy the condition (T1) and (T2), i.e. (2) \Rightarrow (1). The method we used here is to analyse the structure of p -cycles, q -cycles and r -cycles by identifying the cyclic group \mathbb{Z}_{pqr} with the product space $\mathbb{Z}_p \times \mathbb{Z}_q \times \mathbb{Z}_r$.

We organize the paper as follows. In Section 2, we revisit the definitions of tiles and spectral sets in cyclic groups \mathbb{Z}_N and introduce prime-cycles in multi-sets. In Section 3, we give an equivalent description of prime-cycles by identifying $\mathbb{Z}_{p_1 p_2 \dots p_k}$ with $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \times \mathbb{Z}_{p_k}$. In Section 4, we prove that a tile in $\mathbb{Z}_{p_1 p_2 \dots p_k}$ satisfies (T1) and (T2). In Section 5, we prove that a spectral set in \mathbb{Z}_{pqr} satisfies (T1) and (T2).

2 Preliminaries

In this section, we first give some equivalent definitions of spectral sets and tiles in \mathbb{Z}_N . We then study the zeros of mask polynomials. At the end of this section, we study the structure of vanishing sums of roots of unity. Throughout this paper we denote by $\omega_N = e^{2\pi i/N}$, for $N \geq 1$, which is a primitive N -th root of unity.

2.1 Spectral sets in \mathbb{Z}_N

We recall that a subset $A \subset \mathbb{Z}_N$ is said to be *spectral* if there is a set $B \subset \mathbb{Z}_N$ such that

$$\{\omega_N^{bx} : b \in B\}$$

forms an orthogonal basis for $L^2(A)$. In such a case, the set B is called a *spectrum* of A and the pair (A, B) is called a *spectral pair*. Since the dimension of $L^2(A)$ is $\sharp A$, the pair (A, B) being a spectral pair is equivalent to that $\sharp A = \sharp B$ and $\{\omega_N^{bx} : b \in B\}$ is orthogonal on $L^2(A)$, that is to say,

$$\sharp A = \sharp B \text{ and } \sum_{a \in A} \omega_N^{(b-b')a} = 0, \forall b, b' \in B, b \neq b'. \tag{1}$$

This also means that the complex matrix $M = (\omega_N^{ba})_{b \in B, a \in A}$ is a complex Hadamard matrix, i.e. $M \overline{M}^T = (\sharp A)I$ where A^T is the transpose of A and I is the identity matrix. Since $\sharp A = \sharp B$, it follows that $\overline{M}^T M = (\sharp B)I$. This implies that B is also a spectral set and A is its spectrum.

Obviously, the mask polynomial of A is indeed the Fourier transform of the indicator function of A as follows

$$\widehat{1}_A(n) = \sum_{a \in A} \omega_N^{-an} = A(\omega_N^{-n}), \forall n \in \mathbb{Z}_N. \quad (2)$$

Denote the zeros of the mask polynomial $A(X)$ by

$$\mathcal{Z}_A = \{n \in \mathbb{Z}_N : A(\omega_N^n) = 0\}.$$

We restate the above equivalent definition of spectral sets as follows.

Proposition 2.1. *Let $A, B \subset \mathbb{Z}_N$. The following are equivalent.*

- (1) *The pair (A, B) is a spectral pair.*
- (2) *The pair (B, A) is a spectral pair.*
- (3) *$\sharp A = \sharp B$; $(B - B) \setminus \{0\} \subset \mathcal{Z}_A$.*

2.2 Tiles in \mathbb{Z}_N

Recall that a subset $A \subset \mathbb{Z}_N$ is said to be a *tile* if there is a set $T \subset \mathbb{Z}_N$ such that

$$\bigsqcup_{t \in T} (A + t) = \mathbb{Z}_N.$$

In such case, the set T is called a *tiling complement* of A and the pair (A, T) is called a *tiling pair*. Using the language of mask polynomials, we have the following equivalent definitions of tiles in \mathbb{Z}_N .

Lemma 2.2 (Lemma 1.3, [1]). *Let N be a positive integer. Let A, B be multi-sets in \mathbb{Z}_N . Then the following statements are equivalent. Each forces A and B to be sets such that $(\sharp A)(\sharp B) = N$.*

- (1) *(A, B) is a tiling pair.*
- (2) *$A \oplus B = \mathbb{Z}_N$.*
- (3) *$A(X)B(X) = 1 + X + X^2 + \dots + X^{N-1} \pmod{X^N - 1}$.*

As we have mentioned before, Coven and Meyerowitz proved that a set in \mathbb{Z}_N satisfying the conditions (T1) and (T2) is a tile, which shows (1) \Rightarrow (3) in Theorem 1.3.

Theorem 2.3 (Theorem A, [1]). *Let $A \subset \mathbb{Z}_N$. If A satisfies (T1) and (T2), then A is a tile of \mathbb{Z}_N .*

2.3 Zeros of mask polynomial

Let $N \geq 1$. Let \mathbb{Z}_N^* denote the group of all invertible elements in \mathbb{Z}_N . It is classical that the Galois group $\text{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q})$ is isomorphic to \mathbb{Z}_N^* and the isomorphism is induced by $\sigma(\omega_N) = \omega_N^g$ for $g \in \mathbb{Z}_N^*$. It follows that we have a natural action of $\text{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q})$ on the values of the mask polynomial of A , defined by

$$\sigma(A(X)) = A(X^g),$$

for $\sigma \in \text{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q})$ which is determined by $\sigma(\omega_N) = \omega_N^g$ for $g \in \mathbb{Z}_N^*$.

The following lemma shows that we only need to study the zeros of $A(\omega_N^d) = 0$ by restricting d as a divisor of N .

Lemma 2.4. *Let A be a subset in \mathbb{Z}_N . Let p be a prime factor of N . Let $a \in \mathbb{Z}_N$. Then we have the following.*

(1) $A(\omega_N^a) = 0$ if and only if $A(\omega_N^{ag}) = 0$ for any $g \in \mathbb{Z}_N^*$.

(2) For any $d \mid N$, we have the equivalence

$$A(\omega_N^d) = 0 \iff \Phi_{N/d}(X) \mid A(X) \pmod{X^N - 1}.$$

(3) Suppose that $\#\{p^d \in \mathbb{Z}_N : A(\omega_N^{N/p^d}) = 0\} = k$. Then p^k divides $\#A$.

Proof. For $g \in \mathbb{Z}_N^*$, let $\sigma \in \text{Gal}(\mathbb{Q}(\omega_N)/\mathbb{Q})$ which is determined by g . It follows that $\sigma(A(\omega_N^a)) = A(\omega_N^{ag})$. Since $\sigma(0) = 0$, we deduce (1). Since the cyclotomic polynomial of order N/d is the monic minimal polynomial of ω_N^d , we obtain (2). By definition, $\prod_{s \in S_A} \Phi_s(X)$ divides $A(X)$ in $\mathbb{Z}[X]$. Putting $X = 1$, we get (3). \square

The above lemma shows that \mathcal{Z}_A is invariant by multiplying any element in \mathbb{Z}_N^* .

2.4 Vanishing sums of roots of unity

Let d be a factor of N . Following [16], a d -cycle is a coset of the cyclic subgroup of order N/d in \mathbb{Z}_N , that is, a set of the form

$$\{j, j + N/d, j + 2N/d, \dots, j + (d-1)N/d\},$$

for some $j \in \mathbb{Z}_N$. Moreover, we say that such d -cycle is a *prime-cycle* if d is a prime. For interpretation of cycles, one may refer to [18] where Steinberger used the tensor product representation (given here in Lemma 3.1) to provide a useful geometric interpretation of cycles.

Let A be a multi-set in \mathbb{Z}_N . Let $n \geq 1$. Denote by $n \cdot A$ (or sometimes nA) the multi-set consisting of elements $na \in \mathbb{Z}_N$ counting the multiplicity for all $a \in A$. We are concerned whether the multi-set $n \cdot A$ is a union of prime-cycles. If we assume that N/n has at most two prime divisors, say p and q , the following lemma tells us that $n \cdot A$ must be a union of p -cycles and q -cycles whenever $A(\omega_N^n) = 0$.

Proposition 2.5 (Lemma 2.5, Proposition 2.6, [16]). *Let n be a factor of N such that N/n has at most two prime divisors, say p and q . If $A(\omega_N^n) = 0$, then*

$$A(X^n) \equiv P(X^n)\Phi_p(X^{N/p}) + Q(X^n)\Phi_q(X^{N/q}) \pmod{X^N - 1},$$

where P and Q have nonnegative coefficients. Moreover, if N/n has only one prime divisor, say p , then $Q \equiv 0$; if $A(\omega_N^{nq^b}) \neq 0$ for some $b > 0$, then $Q \not\equiv 0$.

Obviously, the converse of the previous proposition also holds, even for N/n having more than two prime divisors. However, the previous proposition is not true when N/n has at least three prime divisors. For example, considering the multi-set A defined by the following mask polynomial in \mathbb{Z}_N where $N = pqr$ with p, q, r distinct primes,

$$A(X) = (X^{qr} + X^{2qr} + \dots + X^{(p-1)qr})(X^{pr} + X^{2pr} + \dots + X^{(q-1)pr}) \\ + (X^{pq} + X^{2pq} + \dots + X^{(r-1)pq}),$$

we have $A(\omega_N) = 0$ but A cannot be expressed as a union of p -, q - and r -cycles [12].

Nevertheless, for general $N > 1$, Lam and Leung [12] proved that if $A(\omega_N) = 0$, then $\sharp A$ is a nonnegative integer linear combination of the prime divisors of N .

Theorem 2.6 (Main theorem, [12]). *Let N be a positive integer. If $A(\omega_N) = 0$, then there exist integers $n_p \geq 0$ for all p prime with $p \mid N$ such that $\sharp A = \sum_{p \mid N} n_p p$.*

3 Prime-cycles in \mathbb{Z}_N for N square free

In this section, we identify the cyclic group \mathbb{Z}_N for $N = p_1 p_2 \cdots p_k$ square free, with the product space $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}$ and show the equivalent description of prime cycles in \mathbb{Z}_N by using their representations in $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}$.

The following lemma is classical and of independent interest. We provide the proof in order to make our paper self-contained.

Lemma 3.1. *Let $N = p_1 p_2 \cdots p_k$. Then there is a group isomorphism*

$$\phi : (\mathbb{Z}_N, +) \longrightarrow (\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}, +), \\ x \longmapsto (x_1, x_2, \dots, x_k),$$

where $x_j \equiv x \pmod{p_j}$ for all $1 \leq j \leq k$.

Proof. Let $x, y \in \mathbb{Z}_N$. Denote by $\phi(x) = (x_1, x_2, \dots, x_k)$ and $\phi(y) = (y_1, y_2, \dots, y_k)$. We observe that

$$x + y \equiv x_j + y_j \pmod{p_j}, \forall 1 \leq j \leq k,$$

which implies that $\phi(x + y) = \phi(x) + \phi(y)$. Thus ϕ is a group homomorphism. On the other hand, if $\phi(x) = (0, 0, \dots, 0)$ which means that

$$x \equiv 0 \pmod{p_j}, \forall 1 \leq j \leq k,$$

then $x = 0$. This implies that ϕ is injective. Due to the Chinese remainder theorem, it is also surjective. Therefore, we conclude that ϕ is an isomorphism. \square

For an element $x \in \mathbb{Z}_N$, we sometimes write (x_1, x_2, \dots, x_k) , which is actually $\phi(x)$, to represent x . In what follows, we identify \mathbb{Z}_N with the set $\{0, 1, \dots, N - 1\}$ whenever we do not concentrate on the addition on \mathbb{Z}_N . Now we study the equivalent definition of prime-cycles in \mathbb{Z}_N .

Lemma 3.2. *Let L be a multi-set in \mathbb{Z}_N . Then L is a p_1 -cycle if and only if it has the form*

$$\{(\ell, x_2, \dots, x_k) : 0 \leq \ell \leq p_1 - 1\}, \tag{3}$$

for some $x_j \in \mathbb{Z}_{p_j}$, for $2 \leq j \leq k$. Moreover, if L is a p_1 -cycle, then for any $y \in \mathbb{Z}_N$ with $p_1 \nmid y$, yL is also a p_1 -cycle.

Proof. By definition, L is a p_1 -cycle if and only if L has the form $\{x, x + N/p_1, x + 2N/p_1, \dots, x + (p_1 - 1)N/p_1\}$ for some $x \in \mathbb{Z}_N$. We observe that

$$\ell N/p_1 \equiv 0 \pmod{p_j}, \forall 2 \leq j \leq k, 0 \leq \ell \leq p_1,$$

and that $\{\ell N/p_1 : 0 \leq \ell \leq p_1\}$ forms a complete set of residues modulo p_1 . Thus for $x = (x_1, x_2, \dots, x_k) \in \mathbb{Z}_N$, we deduce that the set $\{x, x + N/p_1, x + 2N/p_1, \dots, x + (p_1 - 1)N/p_1\}$ is exactly of the form (3).

On the other hand, it is not hard to check that if L has the form (3), then yL also has the form (3) for any $y \in \mathbb{Z}_N$ with $p_1 \nmid y$. This completes the proof. \square

Now we prove a criterion for a multi-set in \mathbb{Z}_N having prime-cycles.

Lemma 3.3. *Let A be a multi-set in \mathbb{Z}_N . Let $2 \leq m \leq k$. Then $p_m p_{m+1} \cdots p_k A$ has a p_1 -cycle if and only if the multi-set A contains a subset*

$$\{(\ell, x_2, \dots, x_{m-1}, x_m^{(\ell)}, \dots, x_k^{(\ell)}) : 0 \leq \ell \leq p_1 - 1\}.$$

Proof. Observe that $p_m p_{m+1} \cdots p_k \mathbb{Z}_N$ is the set

$$\{(x_1, x_2, \dots, x_{m-1}, 0, 0, \dots, 0) : x_j \in \mathbb{Z}_{p_j} \text{ for } 1 \leq j \leq m - 1\}.$$

By Lemma 3.2, we complete the proof. \square

The above lemma is useful to analyse the structure of multi-sets when it has some zeros. Moreover, it is the crucial technique in the proof of Theorem 1.3.

4 Tiles in $\mathbb{Z}_{p_1 p_2 \dots p_k} \Rightarrow (T1) + (T2)$

In this section, we show that tiles in $\mathbb{Z}_{p_1 p_2 \dots p_k}$ satisfy the conditions (T1) and (T2). After we obtained this result, we are informed by Romanos-Diogenes Malikiosis that the result is not new and is a consequence of the argument [20]: a tile in a cyclic group whose order is square-free always tiles by a subgroup. We give the proof here for completeness. Actually, we prove the following proposition.

Proposition 4.1. *Let A be a subset in $\mathbb{Z}_{p_1 p_2 \dots p_k}$ with p_1, p_2, \dots, p_k distinct primes. Then the following are equivalent.*

- (i) The set A is a tile of $\mathbb{Z}_{p_1 p_2 \dots p_k}$ by translation.
- (ii) The set A satisfies the conditions (T1) and (T2).
- (iii) The set A has the form

$$\{(\vec{n}, \vec{y}_{\vec{n}}) : \vec{n} \in \mathbb{Z}_{p'_1 p'_2 \dots p'_\ell}\}.$$

where $1 \leq \ell \leq k$, $(p'_1, p'_2, \dots, p'_\ell)$ is a permutation of (p_1, p_2, \dots, p_k) and $\vec{y}_{\vec{n}} \in \mathbb{Z}_{p'_{\ell+1} p'_{\ell+2} \dots p'_k}$ for all $\vec{n} \in \mathbb{Z}_{p'_1 p'_2 \dots p'_\ell}$.

We will need the following lemma which is due to Tijdeman [21] and is also included in [1]. We review the proof for completeness.

Lemma 4.2. *Let N be a positive integer. Let (A, B) be a tiling pair in \mathbb{Z}_N . Then for any positive integer n with $(n, \sharp A) = 1$, nA is a subset in \mathbb{Z}_N and (nA, B) is also a tiling pair in \mathbb{Z}_N .*

Proof. Since (A, B) is a tiling pair in \mathbb{Z}_N , by Lemma 2.2, we have

$$A(X)B(X) = 1 + X + X^2 + \dots + X^{N-1} \pmod{X^N - 1}. \tag{4}$$

We write $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ where $\alpha_1, \alpha_2, \dots, \alpha_k \geq 1$ and p_1, p_2, \dots, p_k are distinct primes. By Lemma 3.1 [1], we have

$$A(X^{p_1})B(X) = 1 + X + X^2 + \dots + X^{N-1} \pmod{X^N - 1}.$$

Observing that the mask polynomial of $p_1 A$ is $A(X^{p_1}) \pmod{X^N - 1}$, by Lemma 2.2, we obtain that $(p_1 A, B)$ is a tiling pair. It follows that $\sharp(p_1 A) = \sharp A$. Since p_j do not divide $\sharp A$ for all $1 \leq j \leq k$, repeating the same reason, we get that (nA, B) is a tiling pair and consequently nA is a subset in \mathbb{Z}_N . \square

Proof of Proposition 4.1. Denote by $N = p_1 p_2 \dots p_k$. Since it is proved that (ii) \Rightarrow (i) by Theorem 2.3, it remains to prove here that (i) \Rightarrow (iii) and (iii) \Rightarrow (ii).

(i) \Rightarrow (iii) : Suppose that A is a tile in \mathbb{Z}_N . Then there is $1 \leq \ell \leq k$ and a permutation $(p'_1, p'_2, \dots, p'_\ell)$ of (p_1, p_2, \dots, p_k) such that $\sharp A = p'_1 p'_2 \dots p'_\ell$. By Lemma 4.2, $p'_{\ell+1} p'_{\ell+2} \dots p'_k A$ is a subset in \mathbb{Z}_N . Observe that the set $p'_{\ell+1} p'_{\ell+2} \dots p'_k A$ has the form

$$\left\{ (x, \vec{0}_{\mathbb{Z}_{p'_{\ell+1} p'_{\ell+2} \dots p'_k}}) : x \in S \right\}, \text{ for some } S \subset \mathbb{Z}_{p'_1 p'_2 \dots p'_\ell},$$

where $\vec{0}_{\mathbb{Z}_{p'_{\ell+1} p'_{\ell+2} \dots p'_k}}$ stands for $(0, 0, \dots, 0) \in \mathbb{Z}_{p'_{\ell+1}} \times \mathbb{Z}_{p'_{\ell+2}} \times \dots \times \mathbb{Z}_{p'_k}$. Since $\sharp A = p'_1 p'_2 \dots p'_\ell$, it follows that S has to be $\mathbb{Z}_{p'_1 p'_2 \dots p'_\ell}$. Thus A has the form

$$A = \{(\vec{n}, \vec{y}_{\vec{n}}) : \vec{n} \in \mathbb{Z}_{p'_1 p'_2 \dots p'_\ell}\},$$

where $\vec{y}_{\vec{n}} \in \mathbb{Z}_{p'_{\ell+1} p'_{\ell+2} \dots p'_k}$ for all $\vec{n} \in \mathbb{Z}_{p'_1 p'_2 \dots p'_\ell}$.

(iii) \Rightarrow (ii) : Let $N' = p'_1 p'_2 \dots p'_\ell$. It is not hard to see that $\sharp A = N'$ and for any $1 \leq j \leq \ell$,

$$(N/p'_j) \cdot A = (N'/p'_j) \left\{ \left(\vec{0}_{\mathbb{Z}_{p'_1 p'_2 \dots p'_{j-1}}}, i, \vec{0}_{\mathbb{Z}_{p'_{j+1} p'_{\ell+2} \dots p'_k}} \right) : 0 \leq i \leq p'_j - 1 \right\}.$$

It follows that $(N/p'_j) \cdot A$ is a union of p'_j -cycles. By Proposition 2.5, $N/p'_j \in \mathcal{Z}_A$ for all $1 \leq j \leq \ell$. It follows that A satisfies (T1). It remains to prove that A satisfies the condition (T2). In fact, it is sufficient to prove that $p'_1 p'_2 \cdots p'_j p'_{\ell+1} p'_{\ell+2} \cdots p'_k \in \mathcal{Z}_A$ for any $0 \leq j \leq \ell - 1$. Actually, we observe that $p'_1 p'_2 \cdots p'_j p'_{\ell+1} p'_{\ell+2} \cdots p'_k A$ has the form

$$p'_1 p'_2 \cdots p'_j \{ (\vec{0}_{\mathbb{Z}_{p'_1 p'_2 \cdots p'_j}}, \vec{n}, \vec{0}_{\mathbb{Z}_{p'_{\ell+1} p'_{\ell+2} \cdots p'_k}}) : \vec{n} \in \mathbb{Z}_{p'_{j+1} p'_{j+2} \cdots p'_\ell} \}.$$

It is easy to see that $p'_1 p'_2 \cdots p'_j p'_{\ell+1} p'_{\ell+2} \cdots p'_k A$ is a union of p'_ℓ -cycles. It follows that

$$p'_1 p'_2 \cdots p'_j p'_{\ell+1} p'_{\ell+2} \cdots p'_k \in \mathcal{Z}_A.$$

We conclude that A satisfies the condition (T2). □

5 Spectral sets in $\mathbb{Z}_{pqr} \Rightarrow (T1) + (T2)$

In this section, we prove that spectral sets in \mathbb{Z}_{pqr} satisfies the conditions (T1) + (T2). This completes the proof of Theorem 1.3.

We first prove several technical lemmas. These lemmas which may also be of independent interest will be useful in the proof of Theorem 1.3.

Lemma 5.1. *Let (A, B) be a spectral pair in \mathbb{Z}_{pqr} . If $pq \notin \mathcal{Z}_B$, then there exist a subset $S \subset \mathbb{Z}_p \times \mathbb{Z}_q$ and a function $f : \mathbb{Z}_p \times \mathbb{Z}_q \rightarrow \mathbb{Z}_r$ such that*

$$A = \{ (x, y, f(x, y)) : (x, y) \in S \}. \tag{5}$$

Moreover, we have $\sharp A \leq pq$, and equality holds if and only if $S = \mathbb{Z}_p \times \mathbb{Z}_q$.

Proof. If the set A has two elements (x, y, z) and (x, y, z') with $z \neq z'$, then we have

$$(x, y, z) - (x, y, z') = (0, 0, z - z') \in pq\mathbb{Z}_{pqr}^*.$$

By Proposition 2.1, we have $pq \in \mathcal{Z}_B$, which is a contradiction. It follows that for any $(x, y, z) \in A$, the value of z is decided by the values x and y together. Thus A has the form (5). Moreover, it is easy to see that $\sharp A = \sharp S$. Since S is a subset of $\mathbb{Z}_p \times \mathbb{Z}_q$, we conclude that $\sharp A = pq$ if and only if $S = \mathbb{Z}_p \times \mathbb{Z}_q$. □

The general case of the following lemma has been already proved by the implication (iii) \Rightarrow (ii) in Proposition 4.1. Here, we use mask polynomials to give a different proof of this special case. We remark that the general case can also be proved by this method.

Lemma 5.2. *Suppose that a set A has the form (5) with $S = \mathbb{Z}_p \times \mathbb{Z}_q$. Then A satisfies the conditions (T1) and (T2).*

Proof. We observe that prA is a multi-set in \mathbb{Z}_{pqr} and its mask polynomial is

$$(prA)(X) = A(X^{pr}) = \sum_{j \in \mathbb{Z}_q} pX^{jpr}. \quad (6)$$

It follows that $(prA)(\omega_{pqr}) = 0$. Thus $pr \in \mathcal{Z}_A$. Similarly, we have $qr \in \mathcal{Z}_A$. Since $r \nmid \#A = pq$, we have $pq \notin \mathcal{Z}_A$. Therefore, we obtain that A satisfies the condition (T1). On the other hand, it is easy to see that

$$rA = \{(x, y, 0) : (x, y) \in \mathbb{Z}_p \times \mathbb{Z}_q\}. \quad (7)$$

It follows that rA is a union of p -cycles. Thus we obtain that $r \in \mathcal{Z}_A$ and conclude that A satisfies the condition (T2). □

The following result is crucial for our proof of Theorem 1.3.

Lemma 5.3. *Let A be a multi-set in \mathbb{Z}_{pqr} . If $(A - A) \cap pq\mathbb{Z}_{pqr}^* \neq \emptyset$ and there exists a r -cycle in pA , then $p > r$ and $(A - A) \cap q\mathbb{Z}_{pqr}^* \neq \emptyset$.*

Proof. Since pA has a r -cycle, by Lemma 3.3, we obtain that the multi-set A has a subset L which has the form

$$\{(f(j), y, j) : 0 \leq j \leq r - 1\}$$

for some $y \in \mathbb{Z}_q$ and some function $f : \mathbb{Z}_r \rightarrow \mathbb{Z}_p$. Since $(A - A) \cap pq\mathbb{Z}_{pqr}^* \neq \emptyset$, we obtain that for $(x, y, z), (x', y, z') \in A$, if $z \neq z'$, then $x \neq x'$. It follows that the function f is injective and that $(A - A) \cap q\mathbb{Z}_{pqr}^* \neq \emptyset$. By the fact that p, r are distinct primes, we have $p > r$. □

By Proposition 2.5, if $p \in \mathcal{Z}_A$ and $pr \notin \mathcal{Z}_A$, then pA must have a r -cycle. Thus, the following lemma is a direct consequence of Lemma 5.3.

Lemma 5.4. *Let (A, B) be a spectral pair in \mathbb{Z}_{pqr} . Suppose that $p \in \mathcal{Z}_A$, $pr \notin \mathcal{Z}_A$ and $pq \notin \mathcal{Z}_B$. Then $p > r$ and $q \in \mathcal{Z}_B$.*

Now we begin to prove Theorem 1.3 (3) \Rightarrow (1). If $\{pq, pr, qr\} \subset \mathcal{Z}_A$, then by Lemma 2.4, the set A has to be \mathbb{Z}_{pqr} , which satisfies the conditions (T1) and (T2). It remains to consider the case where $\#(\mathcal{Z}_A \cap \{pq, pr, qr\}) \leq 2$. We then decompose the proof of Theorem 1.3 (3) \Rightarrow (1) into three situation: $\#(\mathcal{Z}_A \cap \{pq, pr, qr\}) = 2$; $\mathcal{Z}_A \cap \{pq, pr, qr\} = \emptyset$; $\#(\mathcal{Z}_A \cap \{pq, pr, qr\}) = 1$. We will prove that A satisfies the conditions (T1) and (T2) in each situation.

5.1 Case 1: $\#(\mathcal{Z}_A \cap \{pq, pr, qr\}) = 2$

Without loss of generality, we suppose that $qr, pr \in \mathcal{Z}_A$ and $pq \notin \mathcal{Z}_A$. It follows that $pq \mid \#A = \#B$. If $pq \in \mathcal{Z}_B$, then by Lemma 2.4, we have that r divides $\#B$ and consequently $\#A = \#B = pqr$. This implies that $A = \mathbb{Z}_{pqr}$ and as a result $\{pq, pr, qr\} \subset \mathcal{Z}_A$, which is impossible. Thus $pq \notin \mathcal{Z}_B$. By Lemma 5.1 and the fact that pq divides $\#A$, we have $\#A = pq$ and there exists a function $f : \mathbb{Z}_p \times \mathbb{Z}_q \rightarrow \mathbb{Z}_r$ such that

$$A = \{(x, y, f(x, y)) : (x, y) \in \mathbb{Z}_p \times \mathbb{Z}_q\}. \quad (8)$$

By Lemma 5.2, we conclude that A satisfies the conditions (T1) and (T2).

Remark 5.1. In this case, by the fact that $pq \notin \mathcal{Z}_A$ and $\sharp B = \sharp A = pq$, we deduce by Lemma 5.1 that there exists a function $g : \mathbb{Z}_p \times \mathbb{Z}_q \rightarrow \mathbb{Z}_r$ such that

$$B = \{(x, y, g(x, y)) : (x, y) \in \mathbb{Z}_p \times \mathbb{Z}_q\}. \quad (9)$$

Hence, by Lemma 5.2, we obtain that $\sharp(\mathcal{Z}_B \cap \{pq, pr, qr\}) = 2$ and the spectrum B also satisfies the conditions (T1) and (T2).

5.2 Case 2: $\mathcal{Z}_A \cap \{pq, pr, qr\} = \emptyset$

It follows from Lemma 5.1 that $\sharp B = \sharp A \leq \min\{pq, pr, qr\}$. We first show that $\mathcal{Z}_B \cap \{pq, pr, qr\} = \emptyset$.

Lemma 5.5. $\mathcal{Z}_B \cap \{pq, pr, qr\} = \emptyset$.

Proof. Observe that $\sharp(\mathcal{Z}_B \cap \{pq, pr, qr\})$ takes the value 0, 1, 2 or 3. If $\sharp(\mathcal{Z}_B \cap \{pq, pr, qr\}) = 3$, then $\sharp B = pqr$. This means $A = B = \mathbb{Z}_{pqr}$, which contradicts $\mathcal{Z}_A \cap \{pq, pr, qr\} = \emptyset$. If $\sharp(\mathcal{Z}_B \cap \{pq, pr, qr\}) = 2$, then due to Remark 5.1, we have $\sharp(\mathcal{Z}_A \cap \{pq, pr, qr\}) = 2$ which is a contradiction. It suffices to show $\sharp(\mathcal{Z}_B \cap \{pq, pr, qr\}) \neq 1$. We will prove it by contradiction. Assume that $\sharp(\mathcal{Z}_B \cap \{pq, pr, qr\}) = 1$. Without loss of generality, we suppose that $pq \in \mathcal{Z}_B$ and $pr, qr \notin \mathcal{Z}_B$. It follows that r divides $\sharp B$, implying $\sharp B \geq r$. We thus consider two cases: $\sharp B > r$ and $\sharp B = r$, and prove that such a set B does not exist in each of these two cases.

If $\sharp B > r$, then by pigeonhole principle, there exist two different elements $b, b' \in B$ such that $r \mid b - b'$. It follows that

$$(B - B) \cap (r\mathbb{Z}_{pqr}^* \cup pr\mathbb{Z}_{pqr}^* \cup qr\mathbb{Z}_{pqr}^*) \neq \emptyset.$$

Since $pr, qr \notin \mathcal{Z}_A$ and (A, B) is a spectral pair, we have that

$$(B - B) \cap r\mathbb{Z}_{pqr}^* \neq \emptyset$$

and consequently $r \in \mathcal{Z}_A$. It follows from Lemma 5.4 that $r > p$, $r > q$ and $p, q \in \mathcal{Z}_B$. Since $p \in \mathcal{Z}_B$, $pr \notin \mathcal{Z}_B$ and $pq \notin \mathcal{Z}_A$, by Lemma 5.4, we have $p > r$ which is impossible.

Now suppose that $\sharp B = r$. If A has the form

$$A = \{(x_j, y_j, j) : 0 \leq j \leq r - 1\},$$

for some $x_j \in \mathbb{Z}_p$ and some $y_j \in \mathbb{Z}_q$ for all $0 \leq j \leq r - 1$, then by Lemma 3.3, we have that pqA is a r -cycle which implies that $pq \in \mathcal{Z}_A$. This is impossible. Thus there exist two different elements $a, a' \in A$ such that $r \mid a - a'$. It follows that

$$(A - A) \cap (r\mathbb{Z}_{pqr}^* \cup pr\mathbb{Z}_{pqr}^* \cup qr\mathbb{Z}_{pqr}^*) \neq \emptyset.$$

Since $pr, qr \notin \mathcal{Z}_B$, we have $r \in \mathcal{Z}_B$. By the fact that $pr, qr \notin \mathcal{Z}_A$, $pr, qr \notin \mathcal{Z}_B$ and Lemma 5.4, we have $r > p$, $r > q$ and $p, q \in \mathcal{Z}_A$. Since $p \in \mathcal{Z}_A$, $pq \notin \mathcal{Z}_A$ and $pr \notin \mathcal{Z}_B$, we have $p > q$. Similarly, since $q \in \mathcal{Z}_A$, $pq \notin \mathcal{Z}_A$ and $qr \notin \mathcal{Z}_B$, we have $q > p$ which is a contradiction.

We conclude that $\mathcal{Z}_B \cap \{pq, pr, qr\}$ must be empty. □

Now we claim that $p, q, r \notin \mathcal{Z}_A$. In fact, if $p \in \mathcal{Z}_A$, then it follows from Lemma 5.4 that $p > q$ and $q \in \mathcal{Z}_B$. By Lemma 5.4 again, we have $q > p$ which is a contradiction. This completes the proof of our claim. Similarly, we have $p, q, r \notin \mathcal{Z}_B$.

Now we prove that $\#A = 1$. If $\#A > 1$, then B has two different elements. By the fact that $\mathcal{Z}_A \cap \{p, q, r, pq, pr, qr\} = \emptyset$ and that $(B - B) \setminus \{0\} \subset \mathcal{Z}_A$, we have $1 \in \mathcal{Z}_A$. Similarly, we have $1 \in \mathcal{Z}_B$. This implies that for any two different elements $(x, y, z), (x', y', z') \in A$, we must have $x \neq x', y \neq y'$ and $z \neq z'$. It follows that $\#A \leq \min\{p, q, r\}$. Without loss of generality, we assume $p < q < r$. Then have $\#A \leq p$. If $\#A = p$, then qrA has the form

$$\{(j, 0, 0) : 0 \leq j \leq p - 1\}.$$

It is easy to see that qrA is a p -cycle and consequently $qr \in \mathcal{Z}_A$. This is impossible. Thus $\#A < p$. However, by Theorem 2.6, $\#A$ is a nonnegative integer combination of p, q and r , that is, $\#A \geq \min\{p, q, r\} = p$. This is a contradiction. Thus we have $\#A = 1$. Obviously, the set A satisfies the conditions (T1) and (T2).

5.3 Case 3: $\#(\mathcal{Z}_A \cap \{pq, pr, qr\}) = 1$

Obviously, the condition (T2) holds for A vacuously. It remains to prove that A satisfies the condition (T1). Without loss of generality, we suppose that $qr \in \mathcal{Z}_A$ and $pq, pr \notin \mathcal{Z}_A$. Then the prime number p divides $\#A$. We claim that $pq, pr \notin \mathcal{Z}_B$. In fact, if $pr \in \mathcal{Z}_B$, then $\#B$ is divided by q and consequently $\#B \geq pq$. Since $pq \notin \mathcal{Z}_A$, by Lemma 5.1, B has the form (5) with $S = \mathbb{Z}_p \times \mathbb{Z}_q$. By Lemma 5.2, we have $\#(\mathcal{Z}_B \cap \{pq, pr, qr\}) = 2$. But by Remark 5.1, we have $\#(\mathcal{Z}_A \cap \{pq, pr, qr\}) = 2$ which is a contradiction. Thus $pr \notin \mathcal{Z}_B$. Similarly, we have $pq \notin \mathcal{Z}_B$. On the other hand, by Lemma 5.5 that $\mathcal{Z}_B \cap \{pq, pr, qr\} = \emptyset$ implying $\mathcal{Z}_A \cap \{pq, pr, qr\} = \emptyset$, we have $\mathcal{Z}_B \cap \{pq, pr, qr\} \neq \emptyset$. Since $pq, pr \notin \mathcal{Z}_B$, we obtain $qr \in \mathcal{Z}_B$.

If $\#A = p$, then both A and B satisfy (T1). Assume that $\#A > p$. By the pigeonhole principle, there exist two different elements $b, b' \in B$ such that $p \mid b - b'$. It follows that

$$\mathcal{Z}_A \cap \{p, pq, pr\} \neq \emptyset.$$

Since $pq, pr \notin \mathcal{Z}_A$, we have $p \in \mathcal{Z}_A$. Applying Lemma 5.4 by the fact that $p \in \mathcal{Z}_A$, $pq \notin \mathcal{Z}_A$ and $pr \notin \mathcal{Z}_B$, we have $p > q$ and $r \in \mathcal{Z}_B$. Similarly, we have $p > r$ and $q \in \mathcal{Z}_B$. Moreover, since $r \in \mathcal{Z}_B$ and $pr \notin \mathcal{Z}_B$, we obtain that rB has a p -cycle. By Lemma 5.3, we have $r > p$, which is a contradiction. Thus, we have $\#A = p$ which completes the proof.

Acknowledgments

We would like to thank Romanos-Diogenes Malikiosis for bringing our attention to Tao's blog [20]. We are also grateful to the anonymous reviewer's valuable remarks.

References

- [1] Ethan M. Coven and Aaron Meyerowitz. Tiling the integers with translates of one finite set. *J. Algebra*, 212 (1999), no. 1, 161-174. [2](#), [3](#), [4](#), [8](#)

- [2] Dorin Ervin Dutkay and Palle E.T. Jorgensen. On the universal tiling conjecture in dimension one. *J. Fourier Anal. Appl.*, 2013, 19(3): 467-477. [2](#)
- [3] Dorin Ervin Dutkay and Chun-Kit Lai. Some reductions of the spectral set conjecture to integers. *Math. Proc. Cambridge Philos. Soc.*, 156 (2014), no. 1, 123-135. [2](#)
- [4] Aihua Fan, Shilei Fan, Lingmin Liao, and Ruxi Shi. Fuglede's conjecture holds in \mathbb{Q}_p . 2015, arXiv:1512.08904. [2](#)
- [5] Aihua Fan, Shilei Fan, and Ruxi Shi. Characterization of compact open spectral sets in \mathbb{Q}_p . *J. Functional Analysis*, 2016, 271(12): 3628-3661. [2](#)
- [6] Bálint Farkas, Máté Matolcsi, and Péter Móra. On Fuglede's conjecture and the existence of universal spectra. *J. Fourier Anal. Appl.*, 12 (2006), no. 5, 483-494. [1](#), [2](#)
- [7] Bent Fuglede. Commuting self-adjoint partial differential operators and a group theoretic problem. *J. Functional Analysis*, 16 (1974), 101-121. [1](#)
- [8] Alex Iosevich, Azita Mayeli, and Jonathan Pakianathan. The Fuglede conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$. *Anal. PDE*, 10 (2017), no. 4, 757-764. [2](#)
- [9] Izabella Łaba. The spectral set conjecture and multiplicative properties of roots of polynomials. *J. London Math. Soc.*, (2) 65 (2002), no. 3, 661-671. [2](#), [3](#)
- [10] Jeffrey C. Lagarias and Sándor Szabó. Universal spectra and Tijdeman's conjecture on factorization of cyclic groups. *J. Fourier Anal. Appl.*, 7:63-70, 2001 [2](#)
- [11] Jeffrey C. Lagarias and Yang Wang. Spectral sets and factorizations of finite abelian groups. *J. Functional Analysis*, 145(1):73-98, 1997. [2](#)
- [12] Tsit Yuen Lam and Ka Hin Leung. On vanishing sums of roots of unity. *J. Algebra*, 224 (2000), no. 1, 91-109. [2](#), [6](#)
- [13] Mihail N. Kolountzakis. Non-symmetric convex domains have no basis of exponentials. *Illinois Journal of Mathematics*, 44.3 (2000), 542-550. [1](#)
- [14] Mihail N. Kolountzakis and Máté Matolcsi. Tiles with no spectra. *Forum Mathematicum*, 18 (2006), 519-528. [1](#), [2](#)
- [15] Máté Matolcsi. Fuglede conjecture fails in dimension 4. *Proceedings of the American Mathematical Society*, 133(2005), 3021-3026. [1](#), [2](#)
- [16] Romanos-Diogenes Malikiosis and Mihail N. Kolountzakis. Fuglede's conjecture on cyclic groups of order $p^n q$. *Discrete Analysis*, 2017:12. [2](#), [5](#), [6](#)
- [17] Steen Pedersen and Yang Wang. Universal spectra, universal tiling sets and the spectral set conjecture. *Math. Scand.*, 88(2):246-256, 2001. [2](#)

RUXI SHI

- [18] John P. Steinberger. Minimal vanishing sums of roots of unity with large coefficients. *Proceedings of the London Mathematical Society*, 2008, 97(3): 689-717. [5](#)
- [19] Terence Tao. Fuglede's conjecture is false in 5 and higher dimensions. *Math. Research Letters*, 11 (2004), 251-258. [1](#), [2](#)
- [20] Terence Tao. Some notes on the Coven-Meyerowitz conjecture. <https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/>. [2](#), [3](#), [7](#), [12](#)
- [21] Robert Tijdeman. Decomposition of the integers as a direct sum of two subsets. Number theory (Paris, 1992-1993), 261-276. *London Math. Soc. Lecture Note Ser.*, 215. [8](#)

AUTHOR

Ruxi Shi
Department of Mathematical sciences, University of Oulu
Oulu, Finland
ruxi.shi@oulu.fi
Current address:
Institute of Mathematics, Polish Academy of Sciences
ul. Śniadeckich 8, 00-656 Warszawa, Poland
rshi@impan.pl
<https://sites.google.com/view/ruxishi>