Fuglede's conjecture holds for cyclic groups of order $pqrs$

Gergely Kiss [*]   Romanos Diogenes Malikiosis [†]   Gábor Somlai [‡]   Máté Vizer [§]

Abstract

The tile-spectral direction of the discrete Fuglede-conjecture is well-known for cyclic groups of square-free order, initiated by Łaba and Meyerowitz, but the spectral-tile direction is far from being well-understood. The product of at most three primes as the order of the cyclic group was studied intensely in the last couple of years.

In this paper we study the case when the order of the cyclic group is the product of four different primes and prove that Fuglede's conjecture holds in this case.

1 Introduction

The conjecture of Fuglede [7] was originated from a problem posed to him by Segal on the restriction of the usual differential operators $\frac{\partial}{\partial x_i}$ (acting in the distribution sense) to commuting self-adjoint operators on $L^2(\Omega)$, where Ω is a bounded measurable subset of $\mathbb{R}^n$ with $0 < m(\Omega) < +\infty$. Fuglede showed that this happens if and only if Ω accepts an orthogonal basis of complex exponentials $e^{2\pi i \langle \lambda, x \rangle}$, which is the definition of a *spectral* set. The set of frequencies λ denoted by Λ, is called the *spectrum* of Ω.

We say that S is a *tile* of $\mathbb{R}^n$, if there is a set $T \subset \mathbb{R}^n$ such that almost every point of $\mathbb{R}^n$ can be uniquely written as $s + t$, where $s \in S$ and $t \in T$. In this case, we say that T is the *tiling complement of S*.

In the same paper, Fuglede proceeded to state the so-called Spectral Set Conjecture (that we will just call Fuglede's conjecture):

Conjecture 1. Ω is spectral if and only if Ω is a tile.

Fuglede proved this conjecture when the spectrum or the tiling complement is a lattice. However, this conjecture was largely proven to be false, initially by Tao [22] in 2004 for dimensions $n \geq 5$, and subsequently for $n \geq 3$ [5, 12]. In a recent paper [16] Fuglede's conjecture has verified for all convex bodies in all dimensions. The status of this conjecture remains open for $\mathbb{R}$ and $\mathbb{R}^2$. Recently, it was shown that a spectral subset of $\mathbb{R}$ of Lebesgue measure 1 has a spectrum that is periodic [8].

The notable feature of Tao's proof was the transition to the setting of finite abelian groups (although this had begun with Łaba [13], connecting Fuglede's conjecture with the tiling results of Coven and Meyerowitz [2]). Let us now state Fuglede's conjecture for abelian groups in a more precise way.

[*]Alfréd Rényi Institute of Mathematics. e-mail: kigergo57@gmail.com

[†]Aristotle University of Thessaloniki, Department of Mathematics. e-mail: rwmanos@gmail.com

[‡]Eötvös Loránd University, Faculty of Science, Institute of Mathematics. e-mail: gsomlai@cs.elte.hu

[§]Alfréd Rényi Institute of Mathematics. e-mail: vizermate@gmail.com

Definition 1.1. Let $\mathbb{Z}_N$ denote the cyclic group of order N.

• $S \subset \mathbb{Z}_N$ is called *spectral*, if there is some $\Lambda \subset \mathbb{Z}_N$ with $|S| = |\Lambda|$ and the exponential functions $e_\lambda(x) = \xi_N^{\lambda x}$ form an orthogonal basis over S, that is

$$\langle e_\lambda, e_{\lambda'} \rangle_S := \sum_{s \in S} e_\lambda(s)\overline{e_{\lambda'}(s)} = |S|\delta_{\lambda\lambda'} \tag{1}$$

for every $\lambda, \lambda' \in \Lambda$, where $\xi_N = \exp(2\pi i/N)$ a primitive N'th root of unity. We call Λ the *spectrum* and (S, Λ) is called a *spectral pair* of $\mathbb{Z}_N$.

• $S \subset \mathbb{Z}_N$ is called a *tile*, if there is another subset $T \subset \mathbb{Z}_N$ such that every element of $\mathbb{Z}_N$ can uniquely be written as $s + t$, where $s \in S$, $t \in T$. We call T the *tiling complement* of S, we write $S \oplus T$ [1] $= \mathbb{Z}_N$ and we call (S, T) a *tiling pair* of $\mathbb{Z}_N$.

Conjecture 2. For any N and $S \subset \mathbb{Z}_N$ we have that S is spectral if and only if S tiles $\mathbb{Z}_N$.

Borrowing the notation from [3] and [17], we write $\mathbf{S} - \mathbf{T}(G)$ (resp. $\mathbf{T} - \mathbf{S}(G)$), if the $Spectral \Rightarrow Tile$ (resp. $Tile \Rightarrow Spectral$) direction of Fuglede's conjecture holds in G. The above mentioned connection between the conjecture on $\mathbb{R}$, on $\mathbb{Z}$ and on finite cyclic groups is summarized below [3] (where $\mathbf{T} - \mathbf{S}(\mathbb{Z}_\mathbb{N})$ means that $\mathbf{T} - \mathbf{S}(\mathbb{Z}_n)$ holds for every $n \in \mathbb{N}$):

$$\mathbf{T} - \mathbf{S}(\mathbb{R}) \Longleftrightarrow \mathbf{T} - \mathbf{S}(\mathbb{Z}) \Longleftrightarrow \mathbf{T} - \mathbf{S}(\mathbb{Z}_\mathbb{N}),$$

$$\mathbf{S} - \mathbf{T}(\mathbb{R}) \Longrightarrow \mathbf{S} - \mathbf{T}(\mathbb{Z}) \Longrightarrow \mathbf{S} - \mathbf{T}(\mathbb{Z}_\mathbb{N}).$$

This close connection shows the importance of Fuglede's Conjecture for abelian groups. Since the result of Tao appeared, there have been many results on finite abelian groups by many authors, which we summarize below:

Theorem 1.2. *Let G be a finite abelian group and p, q, r different primes.*

(1) *If $G = \mathbb{Z}_p^d$ where p is an odd prime and $d \geq 4$, then there is a spectral subset of G that does not tile [1, 6].*

(2) *If $G = \mathbb{Z}_2^d$ where $d \geq 10$, then there is a spectral subset of G that does not tile [6].*

(3) *If $G = \mathbb{Z}_8^3$, then there is a spectral subset of G that does not tile [12].*

(4) *If $G = \mathbb{Z}_{24}^3$, then there is a tile of G that is not spectral [5].*

(5) *If $G = \mathbb{Z}_p^d$ where p is prime and $d \leq 3$, then any tile of G is spectral [1]. The converse holds if $d \leq 2$ [9] or $d = 3$ and $p \leq 7$.*

(6) *If $G = \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$ [20] or $G = \mathbb{Z}_p \oplus \mathbb{Z}_{pq}$ [11], where $p \neq q$ are primes, then a subset of G is spectral if and only if it is a tile.*

(7) *If $G = \mathbb{Z}_N$ and N is square-free or $N = p^m q^n$ or $N = p^n d$, where d is square-free, then any tile of G is spectral [14, 18, 19].*

---

[1]In general, we write $A \oplus B$ if every element in the sumset $A + B$ can be written uniquely as a sum of an element of A and an element of B.

(8) If $G = \mathbb{Z}_N$ and $N = p^n, p^n q, p^n q^2, pqr, p^2 qr$, then a subset of G is spectral if and only if it is a tile [10, 14, 17, 18, 19, 21].

Using the fundamental theorem of finite abelian groups, the following holds for G whose minimum number of generators is d:

$$G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_d},$$

where $n_i \mid n_{i+1}$ for $1 \le i \le d-1$. Thus, we obtain

Corollary 1.3. *Let G be a finite Abelian group, and d be the minimum number of generators of G.*

- *If $d \ge 4$ and $|G|$ is odd, then there is a spectral subset of G that does not tile.*

- *If $d \ge 10$, then there is a spectral subset of G that does not tile.*

In this article we investigate the discrete Fuglede's conjecture for cyclic groups of order of the product of 4 different primes. In particular we prove

Theorem 1.4. *Fuglede's conjecture is true for $\mathbb{Z}_{pqrs}$, where p, q, r, s are different primes.*

Combining the results in Theorem 1.2 (8) and Theorem 1.4 we obtain the following corollary.

Corollary 1.5. *Fuglede's conjecture is true for $\mathbb{Z}_{pqrs}$, where p, q, r, s are arbitrary primes.*

2 Preliminaries; Structures and tools

2.1 Basic properties of Spectral and Tiling pairs

In this section we list some properties of spectral pairs that we use during the proof. Our first remark is that we will always identify the dual group of a cyclic group $\mathbb{Z}_N$ with itself.

- First note that spectral pairs satisfy the following duality property.

Lemma 2.1. *Let G be a finite abelian group. Assume that $S \subset G$ is a spectral set having Λ as a spectrum. Then S is also a spectrum for Λ.*

- A trivial property of a tiling pair (T, S) is $(T - T) \cap (S - S) = \{0\}$. There is a similar property for spectral pairs involving the difference set of a spectrum that we introduce now. Let (S, Λ) be a spectral pair of $\mathbb{Z}_N$. Let us denote by $\mathbf{1}_S$ the characteristic function of S, and the Fourier transform of a function $f : \mathbb{Z}_N \to \mathbb{C}$ as

$$\hat{f}(y) = \sum_{x \in \mathbb{Z}_N} f(x) \xi_N^{-xy},$$

we have for any $\lambda, \lambda' \in \Lambda$, where $\lambda \ne \lambda'$,

$$0 = \sum_{s \in S} e_\lambda(s) \overline{e_{\lambda'}(s)} = \sum_{s \in S} \xi_N^{(\lambda - \lambda')s} = \hat{\mathbf{1}}_S(\lambda' - \lambda)$$

3

by (1), therefore

$$\Lambda - \Lambda \subset \{0\} \cup \big\{d \in \mathbb{Z}_N : \hat{\mathbf{1}}_S(d) = 0\big\}, \tag{2}$$

that is, the difference set of a spectrum is a subset of the zero set of the Fourier transform of $\mathbf{1}_S$ along with $\{0\}$.

- Relation (2) can also be expressed with the notion of the mask polynomial of a multiset.

Definition 2.2. For a cyclic group G, a field K and a function $f : G \to K$, we define the *mask polynomial of* f (in $K[x]$) by

$$m_f(x) = \sum_{g \in G} f(g)x^g.$$

For a (multi)set S on G we denote the multiplicity function of S by f_S (that is a function from G to $\mathbb{N}$) and we denote by m_S the mask polynomial of f_S.

The basic connection between the mask polynomial and the Fourier transform of (the characteristic function of) a set S is

$$\hat{\mathbf{1}}_S(d) = m_S(\xi_N^{-d}),$$

so we may rewrite (2) as

$$\Lambda - \Lambda \subset \{0\} \cup \Big\{d \in \mathbb{Z}_N : m_S(\xi_N^{-d}) = 0\Big\}. \tag{3}$$

We define $Z(S) := \Big\{d \in \mathbb{Z}_N : m_S(\xi_N^{-d}) = 0\Big\}$. Since $m_S(x) \in \mathbb{Z}[x]$, the following holds: if $g \in \mathbb{Z}_N^\star$, then

$$m_S(\xi_N^d) = 0 \implies m_S(\xi_N^{dg}) = 0.$$

It is clear from (3) that $Z(S)$ is a union of subsets of the form $d\mathbb{Z}_N^\star = \{dg : g \in \mathbb{Z}_N^\star\}$, where $d \mid N$, in particular for a spectral pair (S, Λ) in $\mathbb{Z}_N$ we have

$$\Lambda - \Lambda \subseteq \{0\} \cup \bigcup_{d \mid N,\ m_S(\xi_N^d)=0} d\mathbb{Z}_N^\star. \tag{4}$$

2.2 Geometric interpretation of cyclic groups of square-free order and the cube rule

- For $m, n \in \mathbb{N}$ with $m \mid n$ let us define the *natural projection* of $\mathbb{Z}_n$ onto $\mathbb{Z}_m \leq \mathbb{Z}_n$, $\mathbb{Z}_m$ denotes the only subgroup of $\mathbb{Z}_n$ of order m. Let $k \in \mathbb{N}$ with $\frac{n}{m} \mid k$ and $k \equiv 1 \pmod{m}$. Then $x \to k \cdot x$ defines a surjective homomorphism from $\mathbb{Z}_n$ to $\mathbb{Z}_m$. Note that the function defined in this way is independent on the choice of k. If U is a subset of $\mathbb{Z}_n$, then its *projection* to $\mathbb{Z}_m$, which we denote by U_m, is a multiset defined as $\{k \cdot u \mid u \in U\}$.

In this subsection our goal will be to introduce a geometric interpretation of cyclic groups of square-free order and an important observation that we call the cube rule. We use the 'geometric language' introduced below throughout the proof.

• Note that the cyclic group $\mathbb{Z}_N$ with $N = p_1 p_2 \ldots p_k$ (p_i's are different prime numbers) can be written as the direct sum $\oplus_{i=1}^k \mathbb{Z}_{p_i}$, so its elements can also be considered as k-tuples. Let the *Hamming distance* of two elements $x, y \in \oplus_{i=1}^k \mathbb{Z}_{p_i}$ be the number of coordinates they differ. Let us denote by $d_H(x, y)$ the Hamming distance of x and y.

We consider $\oplus_{i=1}^k \mathbb{Z}_{p_i}$ as the subset of the k-dimensional integer grid, so we identify it with

$$\{x = (x_1, x_2, \ldots, x_k) \in \mathbb{Z}^k \mid 0 \le x_1 \le p_1 - 1, \ 0 \le x_2 \le p_2 - 1, \ \ldots, \ 0 \le x_k \le p_k - 1\}.$$

In this interpretation every coset of a subgroup of order $d = p_{i_1} \ldots p_{i_s}$ of $\mathbb{Z}_N$ can be identified with a proper s-dimensional affine subspace of $\oplus_{i=1}^k \mathbb{Z}_{p_i}$. For instance, $\mathbb{Z}_{p_1}$-cosets are lines that are the set of vertices with the same $\mathbb{Z}_{p_2}$-, $\ldots, \mathbb{Z}_{p_k}$-coordinates.

• Now we recall an important tool that was introduced in [10]. It describes a condition that a multiset $B \subseteq \mathbb{Z}_N$ should satisfy, in case N is square-free and $\Phi_N \mid m_B$. For an integer N we denote by $\omega(N)$ the number of (different) prime divisors of N. If N is square-free, then we can consider $\mathbb{Z}_N = \oplus_{i=1}^{\omega(N)} \mathbb{Z}_{p_i}$ as the direct sum of groups of different prime order. We call a subset C of $\mathbb{Z}_N$ an $\omega(N)$-*dimensional cube*, if $C = \oplus_{i=1}^{\omega(N)} A_i$, where $A_i \subset \mathbb{Z}_{p_i}$ are 2-element sets and let $c_0 \in C$.

Theorem 2.3. *(**Cube rule**; [10], Proposition 3.5.) Suppose that N is a square-free integer, $B \subseteq \mathbb{Z}_N$ is a multiset and $\Phi_N \mid m_B$. Then for every $\omega(N)$-dimensional cube C and $c_0 \in C$ the following holds*

$$\sum_{c \in C} (-1)^{d_H(c_0, c)} B(c) = 0, \tag{5}$$

where $B(c)$ denotes the multiplicity of c in B.

We say that B satisfies the $\omega(N)$-*dimensional cube rule*, if equation (5) holds for every $\omega(N)$-dimensional cube C. For shortening our notation a 2-, 3- or 4-dimensional cube (rule) will be denoted by 2D, 3D, 4D cube (rule), respectively.

• In general, for square-free $N = \prod_{i=1}^{\omega(N)} p_i$ we may introduce the d-dimensional cube $C_{p_{i_1} \ldots p_{i_d}} = \oplus_{j=1}^d A_{p_j}$, where $A_{p_j} \subset \mathbb{Z}_{p_j}$ are proper 2-element sets. If $x, y \in \mathbb{Z}_N$ with $d_H(x, y) = d$, then we denote by $C_{p_{i_1} \ldots p_{i_d}}(x, y)$ the unique d-dimensional cube determined by x, y, where x, y differ in $p_{i_1}, \ldots, p_{i_d}$-coordinates. If it is clear form the context, then we simply denote this cube by $C(x, y)$.

2.3 Preliminary statements

Let us start with some statements from [10].

Lemma 2.4. *Let G be a finite abelian group. It is enough to prove the Spectral $\Rightarrow$ Tile direction of Fuglede's conjecture for spectral pairs (S, Λ) with $0 \in S$ and $0 \in \Lambda$.*

Lemma 2.5. *Let G be a finite abelian group and S a spectral set in G, that does not generate G. Assume that for every proper subgroup H of G we have $\mathbf{S} - \mathbf{T}(H)$. Then S tiles G.*

Lemma 2.6. *Let N be a natural number and suppose that $\mathbf{S} - \mathbf{T}(\mathbb{Z}_N/H)$ holds for every $1 \ne H \le \mathbb{Z}_N$. Assume that (S, Λ) is a spectral pair and Λ is not primitive. Then S tiles $\mathbb{Z}_N$.*

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

Lemma 2.8. *Let (S, Λ) be a spectral pair in $\mathbb{Z}_N$, where $N = p \cdot p_1 \cdots p_k$ is a square-free integer and $\mathbf{S} - \mathbf{T}(\mathbb{Z}_{\frac{N}{p}})$ holds. Suppose that Λ is the union of $\mathbb{Z}_p$-cosets. Then S is a tile.*

Proof. Let $\Lambda' := \Lambda \cap \mathbb{Z}_{\frac{N}{p}}$. The mask polynomial $m_{\Lambda'}$ has degree at most $\frac{N}{p} - 1$ and $m_{\Lambda'}(1) = |\Lambda'| = \frac{|\Lambda|}{p}$ as Λ is the union of $\mathbb{Z}_p$-cosets. Note that the mask polynomial of the $\mathbb{Z}_p$-coset containing 0 is $\Phi_p(x^{\frac{N}{p}})$. Since Λ is the union of $\mathbb{Z}_p$-cosets we have $\Phi_p(x^{\frac{N}{p}}) \mid m_\Lambda$. Moreover $\Lambda = \Lambda' \oplus \mathbb{Z}_p$ implies

$$m_\Lambda = m_{\Lambda'} \Phi_p(x^{\frac{N}{p}}). \tag{6}$$

Since Λ is the union of $\mathbb{Z}_p$-cosets, we have $\Phi_p \mid m_S$, so S is equidistributed on the $\mathbb{Z}_{\frac{N}{p}}$-cosets. Note that, if $|S| = |\Lambda| = p$, then every $\mathbb{Z}_{\frac{N}{p}}$-coset contains exactly one element of S, hence S is a tile. Thus, we can assume that $|\Lambda| = |S| > p$. Let $S_i = \{x \in S \mid x \equiv i \pmod{p}\}$. Hence $|S_i| = \frac{|S|}{p} = \frac{|\Lambda|}{p} = |\Lambda'| > 2$ holds.

As (Λ, S) is a spectral pair this implies that for any $s_1, s_2 \in \mathbb{Z}_N$ we get that $\Phi_m \mid m_\Lambda$, where m is the order of $s_1 - s_2$. Since N is square-free, we have $p \nmid m$ for $s_1 - s_2 \in S_i$, $s_1 \neq s_2$ and $1 \leq i \leq n$. This implies that $\Phi_m \nmid \Phi_p(x^{\frac{N}{p}})$ hence, by (6), we obtain $\Phi_m \mid m_{\Lambda'}$. By $|S_i| = |\Lambda'|$, it follows that $S_i - i$ is a spectrum of Λ' for every $0 \leq i \leq p - 1$.

Then by assumption we have that $S_i - i$ is a tile on $\mathbb{Z}_{\frac{N}{p}}$. As N is square-free, by Proposition 4.1 of [19], we have that $S_i - i$ is a set of coset representatives of $\mathbb{Z}_{\frac{N}{p|S_i|}}$ in $\mathbb{Z}_{\frac{N}{p}}$. Therefore, the subgroup $T = \mathbb{Z}_{\frac{N}{|S|}}$ is a common tiling complement of $S_i - i$ in $\mathbb{Z}_{\frac{N}{p}}$ for each S_i, hence it is a tiling complement for S in $\mathbb{Z}_N$, finishing the proof of the lemma. $\qquad\square$

By [19], we have that $\mathbf{S} - \mathbf{T}(\mathbb{Z}_{pqr})$ holds, where p, q, r are different primes. Combining with Lemma 2.8 we get the following.

Corollary 2.9. *Let (S, Λ) be a spectral pair in $\mathbb{Z}_N$, where $N = pqrs$ with p, q, r, s different prime numbers. Suppose that Λ is the union of $\mathbb{Z}_p$-cosets. Then S is a tile.*

Lemma 2.10. *Let $N = p_1 p_2 \cdots p_k$ be a square-free integer, and let $S \subseteq \mathbb{Z}_N$ be a spectral set whose cardinality is divisible by at least $k - 1$ primes among $p_1, \ldots, p_k$. Then S tiles $\mathbb{Z}_N$.*

Proof. If $N \mid |S|$, then $S = \mathbb{Z}_N$ and there is nothing to prove. So, without loss of generality we can suppose that $p_1 \ldots p_{k-1} \mid |S|$ and $p_k \nmid |S|$. Let $\Lambda \subseteq \mathbb{Z}_N$ be a spectrum of S. Since $p_k \nmid |S| = |\Lambda|$, we must have $m_\Lambda(\zeta_{p_k}) \neq 0$, therefore (3) yields

$$(S - S) \cap \frac{N}{p_k}\mathbb{Z}_N = \{0\}.$$

Thus, every element of S is unique mod $\frac{N}{p_k}$, yielding $|S| \leq p_1 \cdots p_{k-1}$, and combined with $p_1 \cdots p_{k-1} \mid |S|$ we finally obtain

$$|S| = p_1 \cdots p_{k-1}.$$

Therefore, S consists of a complete set of coset representatives modulo the subgroup $\frac{N}{p_k}\mathbb{Z}_N$, and so this subgroup is exactly a tiling complement of S. $\qquad\square$

Lemma 2.10 immediately implies the following.

Corollary 2.11. *Let $N = pqrs$ with different primes p, q, r, s and (S, Λ) a spectral pair of $\mathbb{Z}_N$. Then, in order to prove $\mathbf{S} - \mathbf{T}(\mathbb{Z}_{pqrs})$, we can assume that $r \nmid |S|$ and $s \nmid |S|$ (otherwise we are done by Lemma 2.10). This automatically implies that $\Phi_r, \Phi_s \nmid m_S, m_\Lambda$.*

We also remind that if the spectral set is small, then it tiles.

Theorem 2.12 ([12], Theorem 2.1). *Let S be a spectral set in a finite abelian group G with $|S| \leq 5$. Then, S tiles G.*

Let us gather the information above in the following summary.

Summary 1. Let $N = p_1 \ldots p_k$ be a square-free integer and (S, Λ) a spectral pair of $\mathbb{Z}_N$. Any of the following assertions implies that S tiles $\mathbb{Z}_N$.

- S or Λ does not generate $\mathbb{Z}_N$.
- S or Λ is the union of $\mathbb{Z}_{p_i}$-cosets for some p_i.
- all p_i's except at most one divide the cardinality of S.
- $|S| \leq 5$.

We can also suppose that $0 \in S$ and $0 \in \Lambda$ to prove the Spectral $\Rightarrow$ Tile direction of Fuglede's conjecture.

2.4 Technical lemmata for the proof

- Let $N = p_1 \ldots p_k$ be a square-free natural number. For any primitive N'th root of unity ξ_N and for an integer t one can uniquely write the complex number ξ_N^t as $\xi_{p_1}^{a_1(t)} \cdot \xi_{p_2}^{a_2(t)} \cdot \ldots \cdot \xi_{p_k}^{a_k(t)}$, where $0 \leq a_i(t) \leq p_i - 1$, for $i = 1, \ldots, k$.

Lemma 2.13. *Let $N = p_1 \ldots p_k$ be a square-free integer and $B \subset \mathbb{Z}_N$ a multiset. Assume $\Phi_{\frac{N}{p_1}} \mid m_B$ and $\Phi_N \mid m_B$. Let us denote by $B_j = \{b \in B \mid b \equiv j \pmod{p_1}\}$. Consider B_j as a subset of $\mathbb{Z}_{\frac{N}{p_1}}$ by simply identifying B_j with $B_j - j$. Then $\Phi_{\frac{N}{p_1}} \mid m_{B_j}$ for every $j = 0, \ldots, p-1$.*

Proof. Note that $\Phi_N \mid m_B$ implies

$$0 = \sum_{t \in B} \xi_{p_1}^{a_1(t)} \cdots \xi_{p_k}^{a_k(t)}.$$

Let ℓ be an integer with $(\ell, p_1) = 1$ and $\ell p_1 \equiv 1 \pmod{\frac{N}{p_1}}$. Then $\xi_N^{\ell p_1}$ is a primitive $\frac{N}{p_1}$'th root of unity and

$$\xi_N^{(\ell p_1)t} = \xi_{p_1}^{(\ell p_1)a_1(t)} \xi_{p_2}^{(\ell p_1)a_2(t)} \cdots \xi_{p_k}^{(\ell p_1)a_k(t)} = \xi_{p_2}^{a_2(t)} \cdots \xi_{p_k}^{a_k(t)}. \tag{7}$$

Since $\xi_N^{\ell p_1}$ is a primitive $\frac{N}{p_1}$'th root of unity, by equation (7) we get that $\Phi_{\frac{N}{p_1}} \mid m_B$ is equivalent to

$$0 = \sum_{t \in B} \xi_{p_2}^{a_2(t)} \cdots \xi_{p_k}^{a_k(t)},$$

where $a_i(t) \equiv t \pmod{p_i}$, for $i = 2, \ldots, k$.

Using our notion B_j we can rewrite these equations as

$$0 = \sum_{j=0}^{p_1-1} \xi_{p_1}^j \sum_{t\in B_j} \xi_{p_2}^{a_2(t)}\dots\xi_{p_k}^{a_k(t)},$$

and

$$0 = \sum_{j=0}^{p_1-1} \sum_{t\in B_j} \xi_{p_2}^{a_2(t)}\dots\xi_{p_k}^{a_k(t)},$$

Let $t_j = \sum_{t\in B_j} \xi_{p_2}^{a_2(t)}\dots\xi_{p_k}^{a_k(t)}$. Thus $0 = \sum_{j=0}^{p_1-1} \xi_{p_1}^j t_j$ and $0 = \sum_{j=0}^{p_1-1} t_j$. Since $t_j \in \mathbb{Q}(\xi_{\frac{N}{p_1}})$ and the minimal polynomial of ξ_{p_1} over $\mathbb{Q}(\xi_{\frac{N}{p_1}})$ is $1 + x + \dots + x^{p_1-1}$, it follows that t_j's are constant. Using $\sum_{j=0}^{p_1-1} t_j = 0$ we obtain $t_j = 0$ for every $j = 0,\dots,p_1-1$. □

Note that Lemma 2.13 can be generalised as it is stated in Proposition B.1. As we do not use it in the proof of the main result we present it in Appendix B.

Lemma 2.14. *Let $N = pqrs$ for different prime numbers p,q,r,s and $S \subseteq \mathbb{Z}_N$ a set and assume $\Phi_N\Phi_{N/s} \mid m_S$ and $S \cap ((x+\mathbb{Z}_q) \cup (x+\mathbb{Z}_r)) = \{x\}$ for all $x \in S$. Then S is a union of $\mathbb{Z}_p$-cosets.*

Proof. By Lemma 2.13, the assumption $\Phi_N\Phi_{N/s} \mid m_S$ implies that S satisfies the 3D cube rule on every $\mathbb{Z}_{N/s}$-coset. By the way of contradiction, assume that S is not the union of $\mathbb{Z}_p$-cosets. Hence, there exists an $x \in S$ with $(x+\mathbb{Z}_p) \setminus S \neq \emptyset$. Let $x_p \in (x+\mathbb{Z}_p) \setminus S$. Then using our assumption $S \cap (x+\mathbb{Z}_q) = S \cap (x+\mathbb{Z}_r) = \{x\}$ we obtain that in every 3D cube containing x and x_p in $x + \mathbb{Z}_{N/s}$ there is no element $z \in S$ with $d_H(x,z) = 1$. Thus, for any $y \in x + \mathbb{Z}_{N/s}$ with $d_H(x,y) = 3$ and $x_p \in C(x,y)$ we have that $y \in S$, by applying the 3D cube rule on $C(x,y)$.

This implies that there are elements $y_1, y_2 \in S$ such that $y_1 - y_2 \in \mathbb{Z}_q$, if $q \geq 3$ (resp., $y_1 - y_2 \in \mathbb{Z}_r$, if $r \geq 3$), which contradicts the assumption $S \cap ((y_1+\mathbb{Z}_q)\cup(y_1+\mathbb{Z}_r)) = \{y_1\}$. □

Note that Lemma 2.14 holds verbatim for any permutation of the primes p,q,r,s.

Lemma 2.15. *Let $N = pqrs$ for different prime numbers p,q,r,s, (S,Λ) a spectral pair in $\mathbb{Z}_N$ and $r,s \nmid |S| = |\Lambda|$.*

1. *If $\Phi_N \mid m_S$, then $\Phi_{N/p} \nmid m_S$ (resp. $\Phi_{N/q} \nmid m_S$) or S is a tile.*

2. *If $\Phi_N \mid m_\Lambda$, then $\Phi_{N/p} \nmid m_\Lambda$ (resp. $\Phi_{N/q} \nmid m_\Lambda$) or S is tile.*

Proof.

1. By the way of contradiction, assume $\Phi_{N/p} \mid m_S$. By Lemma 2.13, $\Phi_N\Phi_{N/p} \mid m_S$ implies that the 3D cube rule holds for every $\mathbb{Z}_{N/p}$-coset. Since $r \nmid |S|$ and $s \nmid |S|$ we have $S \cap ((x+\mathbb{Z}_r) \cup (x+\mathbb{Z}_s)) = \{x\}$ for all $x \in S$. Applying Lemma 2.14 gives that S is a union of $\mathbb{Z}_q$-cosets and hence a tile by Summary 1. Similar argument applies if $\Phi_{N/q} \mid m_S$.

2. Assume $\Phi_{N/p} \mid m_\Lambda$ (resp. $\Phi_{N/q} \mid m_\Lambda$). Similar argument as in the previous case implies that Λ is a union of $\mathbb{Z}_q$-cosets (resp. $\mathbb{Z}_p$-cosets). Then, by Summary 1, S is a tile. □

2.5 Reduction mod p

• The lemma following below is due to Lam and Leung [15], written in polynomial notation.

Lemma 2.16. *If $\Phi_{pq}(x) \mid m_S(x)$, then the multiset S_{pq} is the sum of $\mathbb{Z}_p$- and $\mathbb{Z}_q$-cosets. In polynomial notation,*

$$m_S(x) \equiv P(x)\Phi(x^p) + Q(x)\Phi(x^q) \pmod{x^{pq} - 1},$$

where $P(x), Q(x) \in \mathbb{Z}_{\geq 0}[x]$. Then the cardinality of S satisfies $|S| = pk + q\ell$, for some $k, \ell \geq 0$. If $m_S(\xi_p)m_S(\xi_q) \neq 0$, then $k, \ell > 0$, and so $|S| \geq p + q$.

• In what follows, it will be very useful to reduce the coefficients of mask polynomials mod p, for some primes $p \mid N$ (i.e., we will consider them as polynomials in $\mathbb{F}_p[x]$). For square-free integer m not divisible by p the following equation holds.

$$\Phi_{pm}(x) = \frac{\Phi_m(x^p)}{\Phi_m(x)} = \frac{\Phi_m(x)^p}{\Phi_m(x)} = \Phi_m(x)^{p-1} \text{ in } \mathbb{F}_p[x], \tag{8}$$

hence

$$\Phi_{pm}(x) \mid m_S(x) \implies \Phi_m(x) \mid m_S(x) \text{ in } \mathbb{F}_p[x]. \tag{9}$$

Lemma 2.17. *Assume that*

$$\Phi_{p_2 p_3}\Phi_{p_2}\Phi_{p_3} \mid m_S$$

in $\mathbb{F}_{p_1}[x]$. Then at least one of the following conditions holds:

(i) $\Phi_{p_1} \mid m_S$.

(ii) $\Phi_{p_2}\Phi_{p_3}\Phi_{p_2 p_3} \mid m_S$.

(iii) $\Phi_{p_4} \mid m_\Lambda$ *for every spectrum Λ of S.*

If in addition,

$$m_S(\xi_{p_1})m_S(\xi_{p_4})m_S(\xi_{p_1 p_4}) \neq 0,$$

then either **(ii)** *holds or* **(iii)** *holds along with $p_1 \mid |S|$.*

Proof. It follows from our condition that

$$m_S(x) \equiv \sum_{j=0}^{p_2 p_3 - 1} |S_{j \bmod p_2 p_3}| x^j \equiv c(1 + x + \cdots + x^{p_2 p_3 - 1}) + p_1 P(x) \mod (x^{p_2 p_3} - 1)$$

for some $0 \leq c < p_1$ and $P(x) \in \mathbb{Z}_{\geq 0}[x]$, where

$$S_{j \bmod p_2 p_3} = \{x \in S_{p_2 p_3} \mid x \equiv j \pmod{p_2 p_3}\}.$$

Thus

$$m_S(x) \equiv c(1 + x + \cdots + x^{p_2 p_3 - 1}) \mod (p_1, x^{p_2 p_3} - 1),$$

If the polynomial P is identically zero, then obviously **(ii)** holds. If **(ii)** fails, there is some j with $|S_{j \bmod p_2 p_3}| \geq c + p_1 \geq p_1$. If there is some j such that $|S_{j \bmod p_2 p_3}| > p_1$, then there are two distinct elements of $S_{j \bmod p_2 p_3}$ having the same remainder modulo p_1, hence

$(S - S) \cap \frac{N}{p_4}\mathbb{Z}_N^\star \neq \varnothing$ and **(iii)** holds by (4). If both **(ii)** and **(iii)** fail, then we must have $|S_{j \bmod p_2 p_3}| \leq p_1$ for every j, i.e., $c = 0$ and

$$|S_{j \bmod p_2 p_3}| = 0 \text{ or } p_1$$

for every j. Moreover, $(S - S) \cap \frac{N}{p_4}\mathbb{Z}_N^\star = \varnothing$ by (4), so $S_{\frac{N}{p_4}}$ is a proper set, which implies that $|S_{j+kp_2 p_3 \bmod \frac{N}{p_4}}| \leq 1$, for every j and k. For those j that $|S_{j \bmod p_2 p_3}| = p_1$ holds, we must have

$$|S_{j+kp_2 p_3 \bmod \frac{N}{p_4}}| = 1$$

for all k, which in polynomial form is written as

$$m_S(x) \equiv Q(x)\Phi_{p_1}(x^{\frac{N}{p_1 p_4}}) \bmod (x^{N/p_4} - 1),$$

which easily yields **(i)**.

Next, suppose that $m_S(\xi_{p_4})m_S(\xi_{p_1})m_S(\xi_{p_1 p_4}) \neq 0$, so that **(i)** fails. By the previous discussion, either **(ii)** or **(iii)** holds. Assume that **(ii)** fails, so that **(iii)** holds true. We only need to show that $p_1 \mid |S|$. By (4) we obtain

$$(\Lambda - \Lambda) \cap p_2 p_3 \mathbb{Z}_N = \{0\},$$

for every Λ spectrum of S, so that $|\Lambda| \leq p_2 p_3$. On the other hand,

$$|S| = m_S(1) = cp_2 p_3 + p_1 P(1).$$

The latter is greater than $p_2 p_3$ when $c \geq 1$, since P is not identically zero, otherwise **(ii)** holds. Hence $c = 0$, and obviously $p_1 \mid |S|$, as desired. $\square$

3 The main result and the structure of the proof

Theorem 3.1. *Fuglede's conjecture is true for $\mathbb{Z}_{pqrs}$, where p, q, r, s are different primes.*

Proof. Note that the *Tile $\Rightarrow$ Spectral* direction follows from an argument of Meyerowitz and Łaba written on Tao's blog[2] and also by Ruxi Shi [19].

Now we consider the *Spectral $\Rightarrow$ Tile* direction. Let (S, Λ) be a spectral pair of $\mathbb{Z}_{pqrs}$. Let m_S and m_Λ denote their mask polynomials. In the proof we distinguish the following cases.

(I) $\Phi_N \mid m_S$ or $\Phi_N \mid m_\Lambda$,

(II) $\Phi_N \nmid m_S$ and $\Phi_N \nmid m_\Lambda$.

3.1 Proof of Case (I): $\Phi_N \mid m_S$ or $\Phi_N \mid m_\Lambda$

We also assume that $r, s \nmid |S| = |\Lambda|$ hence, by Corollary 2.11, $\Phi_r, \Phi_s \nmid m_S, m_\Lambda$.

Lemma 3.2. *Let (S, Λ) be a spectral pair of $\mathbb{Z}_N$. Assume that for every $x \in S$ we have $x + \mathbb{Z}_p \subseteq S$ or $x + \mathbb{Z}_q \subseteq S$. Then S is a tile.*

---
[2] https://terrytao.wordpress.com/2011/11/19/some-notes-on-the-coven-meyerowitz-conjecture/#comment-121464

Proof. By Summary 1, if S is the union of $\mathbb{Z}_p$-cosets (or $\mathbb{Z}_q$-cosets), then S is a tile. Since S is primitive, S contains $x + \mathbb{Z}_p$ and $y + \mathbb{Z}_q$ with $(x + \mathbb{Z}_p) \cap (y + \mathbb{Z}_q) = \emptyset$.

First, assume that $(x + \mathbb{Z}_p) \cup (y + \mathbb{Z}_q)$ is contained in a $\mathbb{Z}_{N/s}$-coset. Then it is easy to find $x_1 \in (x + \mathbb{Z}_p)$, $x_2 \in (y + \mathbb{Z}_q)$ with $x_1 - x_2 \in \mathbb{Z}_r$, implying $r \mid |\Lambda|$, a contradiction. Note that a similar argument works if $(x + \mathbb{Z}_p) \cup (y + \mathbb{Z}_q)$ is contained in a $\mathbb{Z}_{N/r}$-coset.

Now assume that $(x + \mathbb{Z}_p) \cup (y + \mathbb{Z}_q)$ is not contained in any proper coset of $\mathbb{Z}_N$. Then we may write $(x + \mathbb{Z}_p) = \{(a, b_1, c_1, d_1) \mid a \in \mathbb{Z}_p\}$ and $(y + \mathbb{Z}_q) = \{(a_2, b, c_2, d_2) \mid b \in \mathbb{Z}_q\}$, where $c_1 \neq c_2$ and $d_1 \neq d_2$. Then by suitable choice of a and b we obtain that $\Phi_N \mid m_\Lambda$ and $\Phi_{\frac{N}{p}} \mid m_\Lambda$. Using Lemma 2.15.2 we obtain that S is a tile. $\qquad\square$

Lemma 3.3. *Let (S, Λ) be a spectral pair of $\mathbb{Z}_N$. If $\Phi_N \mid m_S$ and there exists an $x \in S$ such that $x + \mathbb{Z}_p \not\subseteq S$ and $x + \mathbb{Z}_q \not\subseteq S$, then S is tile.*

Proof. Let us assume that there are $x, y, z \in \mathbb{Z}_N$ such that $x \in S$, $y, z \notin S$ and $y \in x + \mathbb{Z}_p$, $z \in x + \mathbb{Z}_q$. As $\Phi_N \mid m_S$, the 4D cube rule holds for S. Then, by taking any 4D cube C having vertices x, y and z, we obtain that S contains at least one element of C of Hamming distance 3 from x. Indeed, points of Hamming distance 1 are excluded by $y, z \notin S$ and $r \nmid |S|$, $s \nmid |S|$. Without loss of generality we may assume $r > s$.

Fix a 4D cube C containing x, y, z. Let $u = u(x, y, z)$ be the point of C such that $d_H(u, x) = 3$ and u and x have the same r-coordinate. Let o be the point opposite to x on C.

Case 1. $s \geq 3$ (hence $r \geq 5$).

Case 1.1. If $u \notin S$, then one of the other 3 points of distance 3 from x is in S. (These are the ones that differ from x in their r-coordinate.) Since $r \geq 5$, modifying only the r-coordinate of o we may build up 3 more 4D cubes having vertices x, y, z, u. Applying the previous argument using $y, z, u \notin S$ we obtain that S contains a pair of points of Hamming distance 3 from x differing only in their r-coordinate, which contradicts the fact that $r \nmid |S|$.

Case 1.2. If $u \in S$, then let u' be a point which only differs in its s-coordinate from u and have different s-coordinate from x. Such u' exists since $s \geq 3$. Then $u' \notin S$ since $s \nmid |S|$. Hence we may apply the previous argument by exchanging the role of u and u'.

Note that similar argument works if $p \nmid |S|$ (resp. $q \nmid |S|$) by changing the role of p (resp. q) and s. Therefore we can assume that $pq \mid |S|$.

Case 2. $s = 2$ (and $pq \mid |S|$).

Note that the projection S_{pqs} is a set in $\mathbb{Z}_{pqs}$ as $r \nmid |S|$. Therefore $|S|$ can be either pq or $spq = 2pq$. The latter case is not possible since $s \nmid |S|$, thus $|S| = |\Lambda| = pq$. Now we project Λ on $\mathbb{Z}_{2pq}$ and so at least half of the elements of Λ project on the same $\mathbb{Z}_{pq}$-coset. Easy calculation shows if $\min\{p, q\} \geq 3$ (which clearly holds), then there are three pairs of elements of Λ_{2pq} having only different p-, q-, pq-coordinates, respectively.

Since (S, Λ) is a spectral pair, these conditions imply that $\Phi_p \Phi_q \Phi_{pq} \mid m_S$ over $\mathbb{F}_r[x]$. Applying Lemma 2.17 and $rs \nmid |S|$ which gives $\Phi_r, \Phi_s \nmid m_S, m_\Lambda$, we conclude that (**ii**) holds, i.e., $\Phi_p \Phi_q \Phi_{pq} \mid m_S$. This means that $S_{pq} = c\mathbb{Z}_{pq}$, for some $c \in \mathbb{N}$. As $|S| = pq$, we have that $c = 1$ and plainly, S tiles $\mathbb{Z}_N$. $\qquad\square$

Lemma 3.4. *Let $N = pqrs$ and let (Λ, S) be a spectral pair. Assume that $r, s \nmid |S| = |\Lambda|$, $\phi_N \nmid m_S$ and $\phi_N \mid m_\Lambda$. Then S is a tile.*

Proof. By applying Lemmata 3.2 and 3.3 to the spectral pair (Λ, S), we obtain that Λ is a tile. Thus $|\Lambda| \in \{1, p, q, pq\}$ and by [19] we have $\Lambda_{|\Lambda|} = \mathbb{Z}_{|\Lambda|}$. Note that one element subsets are tiles, thus we assume $|\Lambda| \neq 1$.

We distinguish two cases according to the conditions of the previous two Lemmata.

Case 1. Assume that for every $x \in \Lambda$ we have $x + \mathbb{Z}_p \subseteq \Lambda$ or $x + \mathbb{Z}_q \subseteq \Lambda$.

If $q \nmid |\Lambda|$ (i.e. $|\Lambda| = p$), then there is no point x in Λ such that $x + \mathbb{Z}_q \subset \Lambda$. Thus Λ is a $\mathbb{Z}_p$-coset, hence $\Lambda - \Lambda \in \mathbb{Z}_p$. Therefore, by spectrality, S intersects every $\mathbb{Z}_{qrs}$-coset once, when S is a tile. A similar argument works if $|\Lambda| = q$.

It remains to handle the case $|S| = |\Lambda| = pq$. Assume first that $(x + \mathbb{Z}_p) \cup (x + \mathbb{Z}_q) \subset \Lambda$. Then $\Phi_p \Phi_q \Phi_{pq} \mid m_S$. Thus $S_{pq} = \mathbb{Z}_{pq}$ and since $|S| = pq$ we obtain that S is a tile.

Assume now that there are x and y such that $x + \mathbb{Z}_p$ and $y + \mathbb{Z}_q$ are disjoint subsets of Λ. Then $\Lambda_{pq} \neq \mathbb{Z}_{pq}$, a contraction.

Finally, if Λ is the union of $\mathbb{Z}_p$-cosets or $\mathbb{Z}_q$-cosets only, then S is a tile by Summary 1.

Case 2. There exists an $x \in \Lambda$ such that $x + \mathbb{Z}_p \not\subseteq \Lambda$ and $x + \mathbb{Z}_q \not\subseteq \Lambda$

Note that the proof of Lemma 3.3 shows that there is no such spectral set except if $|\Lambda| = pq$ and $s = 2$. Since Λ is tile we have $\Lambda_{pq} = \mathbb{Z}_{pq}$. Since $p \geq 3$, there are at least 3 elements of Λ_{pq} in each $\mathbb{Z}_p$-cosets. Two of them have the same s-coordinate as well since $s = 2$. Thus $\Phi_p \mid m_S$ or $\Phi_{pr} \mid m_S$. Similarly we obtain $\Phi_q \mid m_S$ or $\Phi_{qr} \mid m_S$. There are 3 elements of Λ_{pq} such that the Hamming distance of any two of them is 2. Thus again two of them have the same s-coordinate. This implies that $\Phi_{pq} \mid m_S$ or $\Phi_{pqr} \mid m_S$. Thus $\Phi_p \Phi_q \Phi_{pq} \mid m_S$ in $\mathbb{F}_r[x]$.

By applying Lemma 2.17 we obtain $\Phi_p \Phi_q \Phi_{pq} \mid m_S$ since $r \nmid |S|$ and $s \nmid |S|$ (so cases **(i)** and **(iii)** are excluded). Thus $S_{pq} = \mathbb{Z}_{pq}$ and since $|S| = pq$, we obtain that S is a tile. $\square$

3.2 Proof of Case (II): $\Phi_{pqrs} \nmid m_S$ and $\Phi_{pqrs} \nmid m_\Lambda$

We start with a technical lemma as follows.

Lemma 3.5. *Let $N = p'p''q'q''$ and let $B \subseteq \mathbb{Z}_N$ be primitive. Then, for every pair p', p'' of distinct primes with $p'p'' \mid N$ we have*

$$(B - B) \cap \left(\mathbb{Z}_N^\star \cup p'\mathbb{Z}_N^\star \cup p''\mathbb{Z}_N^\star \cup p'p''\mathbb{Z}_N^\star\right) \neq \varnothing.$$

Proof. Let $b \in B$; since B is not primitive, $b - B$ is not contained in either $q'\mathbb{Z}_N$ or $q''\mathbb{Z}_N$, where $P = \{p', p'', q', q''\}$. So, let $b - b' \notin q'\mathbb{Z}_N$ and $b - b'' \notin q''\mathbb{Z}_N$. If either $b - b' \notin q''\mathbb{Z}_N$ or $b - b'' \notin q'\mathbb{Z}_N$ then either $b - b'$ or $b - b''$ belongs to

$$\mathbb{Z}_N^\star \cup p'\mathbb{Z}_N^\star \cup p''\mathbb{Z}_N^\star \cup p'p''\mathbb{Z}_N^\star$$

as desired. On the other hand, if $b - b' \in q''\mathbb{Z}_N$ and $b - b'' \in q'\mathbb{Z}_N$, then $b' - b''$ belongs to the aforementioned union, completing the proof. $\square$

Corollary 3.6. *Let $N = pqrs$ and let (S, Λ) be a spectral pair in $\mathbb{Z}_N$ such that S is primitive. Then there exist x and y in S such that they have different p- and q-coordinates. With other words $\Phi_N \mid m_\Lambda$ or $\Phi_{\frac{N}{r}} \mid m_\Lambda$ or $\Phi_{\frac{N}{s}} \mid m_\Lambda$ or $\Phi_{\frac{N}{rs}} \mid m_\Lambda$.*

Note that if S is a spectral set, then the previous corollary can be applied to both S and Λ since Λ is also spectral in this case.

Now, we handle a special case which will be crucial in the sequel.

Proposition 3.7. *Let $S \subset \mathbb{Z}_{pqrs}$ be a spectral set that is primitive and suppose $\Phi_p \Phi_q \mid m_S$ and $\Phi_N \nmid m_S$. Then S is a tile.*

Proof. We prove this statement in two steps.

Lemma 3.8. *Under the assumptions of Proposition 3.7 we have $S_{pq} = c\mathbb{Z}_{pq}$ for some $c \in \mathbb{N}$.*

Proof. By Corollary 3.6, if $\Phi_N \nmid m_S$, then either $\Phi_{pq} \mid m_S$, or $\Phi_{pqr} \mid m_S$ or $\Phi_{pqs} \mid m_S$. If $\Phi_p \Phi_q \Phi_{pq} \mid m_S$, then we are done. Thus, by contradiction, let us assume $\Phi_{pq} \nmid m_S$. By the symmetry of the role of r and s we can assume that $\Phi_{pqr} \mid m_S$. Thus

$$\Phi_p(x)\Phi_q(x)\Phi_{N/s}(x) = \Phi_p(x)\Phi_q(x)\Phi_{pq}(x)^{r-1} \mid m_S(x) \text{ in } \mathbb{Z}_r[x].$$

We may apply Lemma 2.17. Since $r \nmid |S| = |\Lambda|$ and $s \nmid |S| = |\Lambda|$ we obtain $\Phi_p \Phi_q \Phi_{pq} \mid m_S$. □

Lemma 3.9. *Under the assumptions of Proposition 3.7 if $S_{pq} = c\mathbb{Z}_{pq}$ for some $0 < c \in \mathbb{N}$, then $c = 1$.*

Proof. We proceed by contradiction. Take two elements $t_1, t_2 \in S$ with the same p- and q-coordinates. Their r- or s-coordinates must be different since otherwise we have $\Phi_s \mid m_\Lambda$ or $\Phi_r \mid m_\Lambda$, which was excluded. So let $t_1 = (a_1, a_2, a_3, a_4)$ and $t_2 = (a_1, a_2, a_3', a_4') \in S$, where $a_3 \neq a_3'$ and $a_4 \neq a_4'$.

As $p, q \geq 2$ and $c > 1$, clearly there are elements t_3, t_4 having a_1' in the first and a_2' in their second coordinate, where $a_1 \neq a_1'$ and $a_2 \neq a_2'$. Since $\Phi_N \nmid m_\Lambda$, it implies that there are no points of Hamming-distance 4 in S. Thus, we may assume that $t_3 = (a_1', a_2', a_3, a_4'), t_4 = (a_1', a_2', a_3', a_4)$, since t_3 and t_4 cannot differ only in their r- or s-coordinate.

If $p, q \geq 3$, then there are $a_1'' \notin \{a_1, a_1'\}$ and $a_2'' \notin \{a_2, a_2'\}$. Then in the $\mathbb{Z}_{rs}$-coset $(a_1'', a_2'', *, *)$ every element is of Hamming distance 4 from one of t_1, t_2, t_3, t_4, a contradiction.

If $c \geq 3$, then we also get a contradiction, as there is an element $t = (a_1, a_2, a_3'', a_4'')$ with $a_3'' \notin \{a_3, a_3'\}$ and $a_4'' \notin \{a_4, a_4'\}$ and so $d_H(t, t_4) = 4$.

Hence we can assume without loss of generality that $c = 2$ and $p = 2$. So every element has either a_1 or a_1' in its first coordinate. Iterating the argument as above, we get that for every element having a_1 in its first coordinate is of the form $(a_1, *, a_3, a_4)$ or $(a_1, *, a_3', a_4')$. Similarly, every element having a_1' in its first coordinate is of the form $(a_1', *, a_3, a_4')$ or $(a_1', *, a_3', a_4)$. Moreover all of these elements are in S. This implies that $|S| = 4q$. Thus S is not a tile. Therefore we have to show that S is not a spectral set.

By contradiction, assume that (S, Λ) is a spectral pair for some $|S| = |\Lambda| = 4q$. Then there is a $\mathbb{Z}_{pq}$-coset which contains at least 2 elements of Λ, i.e., these elements have the same p- and q-coordinates. Then their r- and s- coordinate should be different, otherwise $\Phi_r \mid m_S$ or $\Phi_s \mid m_S$, which is excluded. This implies that $\Phi_{rs} \mid m_S$. Hence the 2D cube rule holds for S_{rs} on $\mathbb{Z}_{rs}$, i.e., S_{rs} is the sum of $\mathbb{Z}_r$- and $\mathbb{Z}_s$-cosets. All the elements of S can have only 2 different r-coordinates and 2 different s-coordinates, thus S_{rs} does not contain either a $\mathbb{Z}_r$-coset or a $\mathbb{Z}_s$-coset. This contradiction shows that S is not a spectral set. □

By Lemma 3.8, $S_{pq} = c\mathbb{Z}_{pq}$ for some $0 < c \in \mathbb{N}$. By Lemma 3.9, $c = 1$, and then S is a tile, finishing the proof of Proposition 3.7. □

Lemma 3.10. *Let (S, Λ) be a spectral pair of $\mathbb{Z}_{pqrs}$. Assume $\Phi_N \nmid m_S$ and $\Phi_N \nmid m_\Lambda$. Then*

$$\Phi_{pqr} \mid m_S \iff \Phi_{pqr} \mid m_\Lambda.$$

$$\Phi_{pqs} \mid m_S \iff \Phi_{pqs} \mid m_\Lambda.$$

Proof. The proof is the same for the two statements and by duality it is enough to show that if $\Phi_{pqr} \mid m_S$, then there is a pair of points in S_{pqr} of Hamming distance 3. This implies that the preimage of these points are of distance 3 in S as $\Phi_N \nmid m_S$, which implies $\Phi_{pqr} \mid m_\Lambda$.

We prove it by contradiction. If there is no pair of points of Hamming distance 3 in S_{pqr}, then either all of the points are of distance 1 from each other, but then one can easily see that S is not primitive or there is a pair of points $x, y \in S_{pqr}$ of Hamming distance 2. Since the 3D cube rule holds on S_{pqr} and S_{pqr} is a set (as $\Phi_s \nmid m_S$), there are at least two other points in any 3D cube containing both x and y of odd distance from x. There are 4 points of odd Hamming distance from x on each of these 3D cubes. Two of them are excluded, since each of them are of Hamming distance 3 from either x or y. The remaining two points that are on the 2D cube spanned by x and y must be in the set S_{pqr} (by 3D cube rule). Then all of the points of $\mathbb{Z}_{pqr}$ which is not in the plane determined by x, y is of Hamming distance 3 from one of these 4 points, so none of them can be in S_{pqr}. By Summary 1, S is primitive, thus S_{pqr} should also be primitive, a contradiction. $\square$

Lemma 3.11. *Let (S, Λ) be a spectral pair of $\mathbb{Z}_N$. Assume $\Phi_N \nmid m_S$ and $\Phi_N \nmid m_\Lambda$. If $\Phi_{pqr} \mid m_\Lambda$ (resp. $\Phi_{pqs} \mid m_\Lambda$), then every pair of points in Λ having different p- and q-coordinates must have different r-coordinate (resp. s-coordinate) as well or S is a tile.*

Proof. Suppose there are points $x, y \in \Lambda$ with different p- and q-coordinates and with the same r-coordinate. Then their projection $x', y' \in \Lambda_{pqr}$ is of Hamming distance 2. By assumption the 3D cube rule holds for Λ_{pqr}, thus there are at least two more points z', w' in every 3D cube containing x' and y'.

We have two cases. If one of these additional points are in 2D cube determined by x', y', then this implies that $\Phi_p \Phi_q \Phi_{pq} \mid m_S$ over $\mathbb{F}_s$. Thus by Lemma 2.17 we have that either $\Phi_p \Phi_q \mid m_S$ and $\Phi_{pq} \mid m_S$, then S is a tile and we are done by Proposition 3.7; or $\Phi_r \mid m_S$ or $\Phi_s \mid m_\Lambda$, which cases were excluded. Otherwise both of the additional points z', w' differ in their r-coordinates from x', y', respectively. Without loss of generality we can assume that $d_H(x', w') = d_H(y', z') = 3$. Hence, the preimage z of z' has the same s-coordinate as y; and the preimage w of w' have the s-coordinate as x, because their distance in $\mathbb{Z}_{pqrs}$ is at least 3 and it cannot be 4, since $\Phi_s \nmid m_S$. Thus $d_H(x, w) = d_H(y, z) = 3$.

If $r \geq 3$, then taking another cube containing x' and y' we get z'' and w'' similarly as above and then z' and z'' differ only in their r-coordinates, thus $\Phi_r \mid m_S$, which was excluded and we are done.

If $r = 2$, then we have two cases whether x and y have the same or different s-coordinates. If they have the same s-coordinates, then so do z and w. By the first part of the proof, there is no more points of the 3D cube $C(x', w')$ in Λ_{pqr}. On the other hand, using the fact that $r = 2$, one can see that every point of $\mathbb{Z}_{pqr} \setminus C(x', w')$ is of Hamming distance 3 from at least one of x', y', z', w'. Hence, every point of S has the same s-coordinate thus Λ is not primitive so S is a tile, by Summary 1. Assume now that x' and y' have different s-coordinates. This implies that $\Phi_{pqs} \mid m_S$. By Lemma 3.10, it implies that $\Phi_{pqs} \mid m_\Lambda$ and the projection of x and w in Λ_{pqs} is of distance 2. Repeating the argument above for these case and using $s > 2$ we get a contradiction. $\square$

Proposition 3.12. *Let (S, Λ) be a spectral pair. Assume that $\Phi_N \nmid m_S$, $\Phi_N \nmid m_\Lambda$ and Λ is a tile. Then S is a tile.*

Proof. We may assume $|S| = |\Lambda| = 1$ or p or pq. The $|S| = 1$ case is trivial.

If $|\Lambda| = pq$, then $\Lambda_{pq} = \mathbb{Z}_{pq}$ by [19]. Since $\Phi_N \nmid m_S$ we have that for every pair of elements x, y of Λ if the p-coordinate and q-coordinate of x and y are different, then their r- or s-coordinate is the same.

If $\Lambda_{pq} = \mathbb{Z}_{pq}$, then there is a pair of points having different p- and q- that have different r-coordinate as well. Otherwise, Λ is not primitive, and then S is a tile by Summary 1. Let x_1 and y_1 be such a pair in Λ, so their p-, q- and r-coordinates are different. So the s-coordinate of x_1 and y_1 is the same since $\Phi_N \nmid m_S$. Thus $\Phi_{pqr} \mid m_S$, which implies $\Phi_{pqr} \mid m_\Lambda$ by Lemma 3.10. Thus by Lemma 3.11 if the p- and q-coordinates of a pair of points of Λ are different, then so do their r-coordinates. Again, we obtain that the s-coordinate of these points is the same. Then it is easy to see from $\Lambda_{pq} = \mathbb{Z}_{pq}$ that the s-coordinate of every point of Λ is the same. Thus Λ is not primitive, and then S is a tile.

Finally, assume $|\Lambda| = p$. Suppose by contradiction that S is not a tile. Then there is a pair x and y in S such that $p \mid x - y$. Then by our assumptions we have $\Phi_{qr} \mid m_\Lambda$ or $\Phi_{qs} \mid m_\Lambda$ or $\Phi_{rs} \mid m_\Lambda$ or $\Phi_{qrs} \mid m_\Lambda$. We may assume without loss of generality that $\Phi_{rs} \mid m_\Lambda$ or $\Phi_{qrs} \mid m_\Lambda$.

If $\Phi_{rs} \mid m_\Lambda$, then Λ_{rs} is the sum of $\mathbb{Z}_r$-cosets and $\mathbb{Z}_s$-cosets by Lemma 2.16. Since $r \nmid |\Lambda|$ and $s \nmid |\Lambda|$ both types appear in the sum. Thus we have $\Phi_{pq} \mid m_S$ or $\Phi_q \mid m_S$ or $\Phi_p \mid m_S$.

The last option would imply that S is equidistributed $\bmod\, p$ and since $|S| = p$, it is a tile, which contradicts our assumption. $\Phi_q \mid m_S$ is excluded since $q \nmid |S|$. Finally, one can see that $\Phi_{pq} \mid m_S$ and $|S| = p$ also implies that S_{pq} is a $\mathbb{Z}_p$-coset by Lemma 2.16, and hence S is a tile, a contradiction.

Assume $\Phi_{qrs} \mid m_\Lambda$. Then the 3D cube rule holds for Λ_{qrs}. We claim that in this case there is a pair of points in Λ_{qrs} of Hamming distance 1. This follows simply from the fact that if $z \in \Lambda_{qrs}$ such that none of the point of Hamming distance 1 from z is in Λ_{qrs}, then every point z' with $d_H(z, z') = 3$ is in Λ_{qrs} by the 3D cube rule.

We obtain that $\Phi_{up} \mid m_S$ or $\Phi_u \mid m_S$, where $u \in \{q, r, s\}$. The latter is excluded by $u \nmid |S|$. If $\Phi_{up} \mid m_S$ and $|S| = p$, then by Lemma 2.16, S_{up} is a $\mathbb{Z}_p$-coset so S is a tile, which is a contradiction. $\qquad\square$

Corollary 3.13. *Let (S, Λ) be a spectral pair of $\mathbb{Z}_N$. Assume $\Phi_N \nmid m_S$ and $\Phi_N \nmid m_\Lambda$. If $\Phi_{pqr} \mid m_S$ (resp. $\Phi_{pqs} \mid m_S$), then every pair of points in Λ having different p- and q-coordinates must have different r-coordinate (resp. s-coordinate) as well or S is a tile.*

Proof. Applying Lemma 3.10, either the statement follows directly from Lemma 3.11 or Λ is a tile. Then by Proposition 3.12, S is a tile. $\qquad\square$

Lemma 3.14. *If $\Phi_{pqr} \mid m_S$, then $\Phi_{pqs} \nmid m_S$, and also if $\Phi_{pqs} \mid m_S$, then $\Phi_{pqr} \nmid m_S$. The same holds for Λ.*

Proof. We take x and y obtained from Corollary 3.6, i.e., they have different p- and q-coordinates. By Corollary 3.13, if $\Phi_{pqr} \mid m_S$ holds, then their r-coordinates are different, as well. Similarly, if $\Phi_{pqs} \mid m_S$ holds, then so their s-coordinates. If both $\Phi_{pqr}\Phi_{pqs} \mid m_S$ holds, then $d_H(x, y) = 4$, which is a contradiction. The statement for Λ directly follows by applying Lemma 3.10. $\qquad\square$

By Lemma 3.14, without loss of generality, we can assume that $\Phi_{pqs} \nmid m_S$, and thus $\Phi_{pqs} \nmid m_\Lambda$ by Lemma 3.10.

Lemma 3.15. *If $\Phi_{pqs} \nmid m_S$, then S is not primitive.*

Proof. Let $x, y \in S_{pqs}$ be the projection of the points getting from Corollary 3.6, i.e., their p- and q-coordinates are different. Then their s-coordinate is the same, otherwise $\Phi_{pqs} \mid m_\Lambda$. Now we take those points that have different s-coordinate than x (and y). These points must have the same p-coordinate as x has and the same q-coordinate as y has or vica-versa. Thus, there are two $\mathbb{Z}_s$-cosets in S_{pqs} that contain all of the points having different s-coordinate than x has. We can distinguish three cases:

Case 1. Every point have the same s-coordinates as x has. Then, clearly, S is not primitive.

Case 2. There are points on both $\mathbb{Z}_s$-cosets. Then taking one point from each coset, they differ in their p- and q- coordinates and since $\Phi_{pqs} \nmid m_\Lambda$ and $\Phi_N \nmid m_\Lambda$, their s-coordinates must be the same. Let z and w denote this pair of points. By the same reasoning it follows that every point having different s-coordinate than z (and w) are in two $\mathbb{Z}_s$-cosets containing x and y, respectively.

Observe that if $a \in S$ and $b \in S$ have different p- and q-coordinates, then the $\mathbb{Z}_s$-cosets containing them do not contain any other element of S.

Therefore it immediately follows that $S_{pqs} = \{x, y, z, w\}$, thus $|S| = 4$ and by Summary 1, $|S|$ is not spectral.

Case 3. One $\mathbb{Z}_s$-coset contains all points of S having different s-coordinate than x.

Now our strategy is that under the conditions $\phi_N \nmid m_S$ and $\phi_{pqs} \nmid m_S$ and the assumption of Case 3 we prove that $\phi_{pqr} \nmid m_S$ also holds. Thus, it is enough to exclude that $\phi_{pq} \mid m_S$, by Corollary 3.6.

We denote one of the points of S from this $\mathbb{Z}_s$-coset by z. Without loss of generality we can assume that z has the same q-coordinate as x and p-coordinate as y.

It is easy to see that if $\Phi_{pqs} \nmid m_\Lambda$ and $x, y, z \in S_{pqs}$, then every point of S_{pqs} are in $(x + \mathbb{Z}_p) \cup (y + \mathbb{Z}_q) \cup (z + \mathbb{Z}_s)$. Hence every point having the same q-coordinate as x and different from y has the same s-coordinate as x, and the every point having the same p-coordinate as y and different from x has the same s-coordinate as y.

Since S_{pqs} is a set, every element in $S_{pqs} \cap (x + \mathbb{Z}_p)$ has multiplicity 1. As y and z have the same p-coordinates, it implies that S is not equidistributed by p, and hence $\Phi_p \nmid m_S$. Similar argument shows that $\Phi_q \nmid m_S$. Furthermore, S_{pq} is in the projection of $(x + \mathbb{Z}_p) \cup (y + \mathbb{Z}_q)$, where their intersection may have higher multiplicity.

As $\Phi_{pqs} \nmid m_\Lambda$ holds, by Lemma 3.10, the same argument shows that $\Lambda_{pqs} \subset (u + \mathbb{Z}_p) \cup (v + \mathbb{Z}_q) \cup (w + \mathbb{Z}_s)$ for some $u, v, w \in \Lambda_{pqs}$ (otherwise Λ is primitive and by Summary 1 we are done). In particular, $\Phi_p \nmid m_\Lambda$ and $\Phi_q \nmid m_\Lambda$ hold, as well.

Now we show that $\Phi_{pqr} \nmid m_S$. By contradiction we assume that $\Phi_{pqr} \mid m_S$. In this case the 3D cube rule holds. Now we take the preimages of x, y and project it to S_{pqr} which is also a set by $s \nmid |S|$. Denote these projections by $x', y' \in S_{pqr}$. As their p-, q-coordinates are different, by Corollary 3.13, their r-coordinates are also different. Let us write $x' = (a_1, b_1, c_1)$ and $y' = (a_2, b_2, c_2)$, where $a_i \in \mathbb{Z}_p$, $b_i \in \mathbb{Z}_q$ and $c_i \in \mathbb{Z}_r$ are pairwise different for $i = 1, 2$. It is clear that $p \geq 3$ or $q \geq 3$.

Without loss of generality, we can assume that $p \geq 3$. Thus there exists an $a_3 \in \mathbb{Z}_p \setminus \{a_1, a_2\}$. Clearly, $z_1 = (a_3, b_2, c_1)$ and $z_2 = (a_3, b_1, c_2)$ are not in S_{pqr} since x' and z_1 (resp., y' and z_2) differ in their p- and q-coordinates and coincide in their r-coordinate, which is impossible by Corollary 3.13. On the other hand, $z_3 = (a_3, b_1, c_1)$ cannot be in S_{pqr}, since z_3 has the same q-coordinate as x' and different from y', which implies that the preimage of z_3 in $\mathbb{Z}_N$ and x' have the same s-coordinate. Thus x' and z_3 are in the same $\mathbb{Z}_p$-coset, which implies

that $\Phi_p \mid m_\Lambda$ which was excluded. Similar argument shows that $z_4 = (a_3, b_2, c_2) \notin S_{pqr}$ since $y' \in S_{pqr}$, by changing the role of x' and y'.
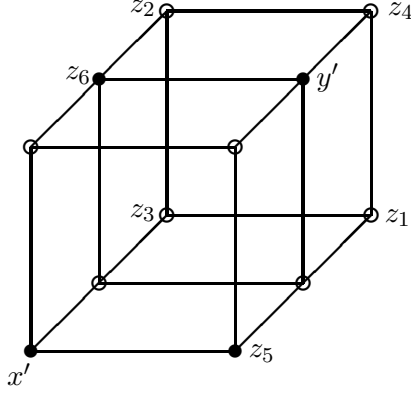
As (a_2, b_2, c_1) and (a_1, b_1, c_2) are not in S_{pqr} by Corollary 3.13, applying the 3D cube rule for $C(x', z_4)$ and $C(y', z_3)$ we get that $z_5 = (a_1, b_2, c_1)$ and $z_6 = (a_2, b_1, c_2)$ are in S_{pqr}. Then the projection of these 4 points $\{x', y', z_5, z_6\}$ in S_{pq} is a 2D cube, although it is known that S_{pq} is in $(x + \mathbb{Z}_p) \cup (y + \mathbb{Z}_q)$. This contradiction shows that $\Phi_{pqr} \nmid m_S$.

By Corollary 3.6, if $\Phi_N \nmid m_S$ and $\Phi_{pqr} \nmid m_S$ and $\Phi_{pqs} \nmid m_S$, then $\Phi_{pq} \mid m_S$. In this case, the projection S_{pq} is the sum of $\mathbb{Z}_p$- and $\mathbb{Z}_q$-cosets. As $S_{pqs} \subset (x + \mathbb{Z}_p) \cup (y + \mathbb{Z}_q) \cup (z + \mathbb{Z}_s)$, it follows that S_{pq} is the sum of a $\mathbb{Z}_p$- and a $\mathbb{Z}_q$-coset. Let x'', y'', and z'' denote the projection of x, y and z on $\mathbb{Z}_{pq}$, respectively. Clearly, $z'' = (x'' + \mathbb{Z}_p) \cap (y'' + \mathbb{Z}_q)$. Since all elements of $(x'' + \mathbb{Z}_p) \setminus \{z''\}$ have different p- and q-coordinates from any elements of $(y'' + \mathbb{Z}_q) \setminus \{z''\}$ and $\Phi_{pqr}, \Phi_{pqs} \nmid m_S$, the preimages of the elements $(x'' + \mathbb{Z}_p) \setminus \{z''\}$ has the same r- and s-coordinate. Since the elements of $(x'' + \mathbb{Z}_p)$ have also the same q-coordinate, it follows that their preimages differ only in their p-coordinates. As $p \geq 3$ (by our assumption), we have $|(x'' + \mathbb{Z}_p) \setminus \{z''\}| \geq 2$, and hence $\Phi_p \mid m_\Lambda$, which was excluded. This contradiction shows the statement. $\qquad\square$

Acknowledgement

References

[1] C. Aten, B. Ayachi, E. Bau, D. FitzPatrick, A. Iosevich, H. Liu, A. Lott, I. MacKinnon, S. Maimon, S. Nan, J. Pakianathan, G. Petridis, C. Rojas Mena, A. Sheikh, T. Tribone, J. Weill, C. Yu. "Tiling sets and spectral sets over finite fields". *J. Funct. Anal.* **273**, 8: 2547–2577, 2017.

[2] E. M. Coven, A. Meyerowitz. "Tiling the integers with translates of one finite set". *Journal of Algebra*, **212**(1), 161–174, 1999.

[3] D. E. Dutkay, C. K. Lai. "Some reductions of the spectral set conjecture to integers". *Mathematical Proceedings of the Cambridge Philosophical Society*, **156**(1), 123–135, 2014.

[4] A. Fan, S. Fan, L. Liao, R. Shi. "Fuglede's conjecture holds in $\mathbb{Q}_p$". *Math. Annalen*, Vol. **375**, Issue 1–2, 315–341, 2019.

[5] B. Farkas, M. Matolcsi, P. Móra. "On Fuglede's conjecture and the existence of universal spectra". *Journal of Fourier Analysis and Applications*, **12**(5), 483–494, 2006.

[6] S. J. Ferguson, N. Sothanaphan. "Fuglede's conjecture fails in 4 dimensions over odd prime fields". *Discrete Mathematics*, Vol. **343**, Issue 1, 111507, 2020.

[7] B. Fuglede. "Commuting self-adjoint partial differential operators and a group theoretic problem". *Journal of Functional Analysis*, **16**(1), 101–121, 1974.

[8] A. Iosevich, M. N. Kolountzakis. "Periodicity of the spectrum in dimension one". *Analysis & PDE* **6**(4), 819–827, 2013.

[9] A. Iosevich, A. Mayeli, J. Pakianathan. "The Fuglede conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$". *Analysis & PDE*, **10**(4), 757–764, 2017.

[10] G. Kiss, R. D. Malikiosis, G. Somlai, M. Vizer. "On the discrete Fuglede and Pompeiu problems". *Analysis & PDE*, **13**(3), 765–788, 2020.

[11] G. Kiss, G. Somlai. "Fuglede's conjecture holds on $\mathbb{Z}_p^2 \times \mathbb{Z}_q$". *ArXiv preprint*, 2019: https://arxiv.org/abs/1912.07114.

[12] M. N. Kolountzakis, M. Matolcsi. "Complex Hadamard matrices and the spectral set conjecture". *Collectanea Mathematica*, Vol. Extra, 281–291, 2006.

[13] I. Łaba. "Fuglede's conjecture for a union of two intervals". *Proceedings of the American Mathematical Society*, **129**(10), 2965–2972, 2001.

[14] I. Łaba. "The spectral set conjecture and multiplicative properties of roots of polynomials". *Journal of the London Mathematical Society*, **65**(3), 661–671, 2002.

[15] T. Y. Lam, K. H. Leung. " On Vanishing Sums of Roots of Unity". *Journal of Algebra* **224**, 91–109, 2000.

[16] N. Lev, M. Matolcsi. "The Fuglede conjecture for convex domains is true in all dimensions". *ArXiv preprint*, 2019: https://arxiv.org/abs/1904.12262

[17] R. D. Malikiosis, M. N. Kolountzakis. "Fuglede's conjecture on cyclic groups of order $p^n q$". *Discrete Analysis*, 2017:12, 16pp.

[18] R. D. Malikiosis "On the structure of spectral and tiling subsets of cyclic groups". *ArXiv preprint*, 2020: `https://arxiv.org/abs/2005.05800`.

[19] R. Shi. "Fuglede's conjecture holds on cyclic groups $\mathbb{Z}_{p_1 p_2 p_3}$". *Discrete Analysis*, 2019:14, 14pp.

[20] R. Shi. "Equi-distributed property and spectral set conjecture on $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$". *Journal of the London Mathematical Society*, to appear.

[21] G. Somlai. "Spectral sets in $\mathbb{Z}_{p^2 qr}$ tile". *ArXiv preprint*, 2019: `https://arxiv.org/abs/1907.04398`

[22] T. Tao. "Fuglede's conjecture is false in 5 and higher dimensions". *Mathematical Research Letters*, **11**(2), 251–258, 2004.

A   Appendix

Let $N = pqr$, where p, q, r are different primes and (A, B) a spectral pair. By Lemma 2.10, we can assume that at least two primes does not divide the cardinality of S. Without loss of generality we may assume $q \nmid |S|$ and $r \nmid |S|$ and $q > r \geq 2$.

Lemma A.1. *Let (S, Λ) be a spectral pair. If $\Phi_N \mid m_S$ and $gcd(|S|, N) \mid p$, then S is the union of $\mathbb{Z}_p$-cosets.*

Proof. It follows from $q \nmid |S|$ and $r \nmid |S|$ that $S \cap ((x + \mathbb{Z}_q) \cup (x + \mathbb{Z}_r)) = \{x\}$ for every $x \in \mathbb{Z}_N$. We proceed indirectly. Assume there is $y \in (x + \mathbb{Z}_p) \setminus S$. Let H denote the set of points z of Hamming distance 3 from x such that $y \in C(x, z)$. Clearly, q or r is at least 3 so there are point in H, which differ only in their q- or r-coordinate.

Note that by the 3D cube-rule $H \subseteq S$ which implies $q \mid |S|$ and $r \mid |S|$, a contradiction. $\square$

Thus if $\Phi_N \mid m_S$, then by Lemma A.1 and Summary 1, it follows that S is a tile. Similar argument shows the same if $\Phi_N \mid m_\Lambda$. Therefore we get the following statement.

Lemma A.2. *Let (S, Λ) be a spectral pair of Z_N. If either $\Phi_N \mid m_S$ or $\Phi_N \mid m_\Lambda$, then S is a tile.*

Now suppose that (S, Λ) is a spectral pair such that $\Phi_N \nmid m_S$ and $\Phi_N \nmid m_\Lambda$ and $q, r \nmid |S|$. If $\Phi_{pq} \mid m_S$, then S_{pq} satisfies the 2D cube rule, thus by Lemma 2.16, S_{pq} is the union of $\mathbb{Z}_p$-cosets and $\mathbb{Z}_q$-cosets. Now we show that it is only the sum of $\mathbb{Z}_p$-cosets. Indeed, if S_{pq} is the union of Z_q-cosets, then $q \mid |S|$, which is a contradiction. If two elements of S having the same projection in S_{pq}, $\Phi_r \mid m_\Lambda$ and hence $r \mid |\Lambda| = |S|$. Hence there is no pair of points in S having the same projection. This implies S_{pq} can only be the union of $\mathbb{Z}_p$-cosets that are not coincide, so it is the sum of $\mathbb{Z}_p$-cosets.

If S_{pq} is a $\mathbb{Z}_p$-coset, then clearly S_{pq} is a tile of $\mathbb{Z}_{pq}$ and hence S tiles $\mathbb{Z}_N$. Now we assume that $|S| > p$. Since $\Phi_{pqr} \nmid m_\Lambda$, there are no elements of S of Hamming-distance 3. Thus, if either $|S| \geq 3p$ or $p > 2$ and $|S| \geq 2p$, then every element of S have the same r-coordinate. Indeed, every element of S can be reached by a path in S_{pq} of length at most 3, where each

consecutive elements are of Hamming-distance 2, hence their r-coordinate is the same. Thus S is not primitive and by Summary 1 we are done. If $p = 2$ and $|S| = 2p = 4 < 5$, then by Summary 1, S is not a spectral. Thus, as $\mathbf{T} - \mathbf{S}(\mathbb{Z}_N)$ holds by [20], if N is square-free, we proved the following, which was first proved in [20].

Theorem A.3. *Fuglede's conjecture holds on $\mathbb{Z}_{pqr}$, where p, q, r are different primes.*

B   Appendix

Now we state and prove the generalisation of Lemma 2.13 as follows. We show it when $m = \frac{N}{p_i p_j}$, one can plainly modify it for other cases along the same line.

Proposition B.1. *Suppose $N = p_1 p_2 \ldots p_k$ is a square-free integer, $m \mid N$ and let $B \subseteq \mathbb{Z}_N$. Suppose also that for every l with $m \mid l \mid N$ we have $\Phi_l \mid m_B$. Then for every $\mathbb{Z}_m$-coset $\mathbb{Z}_m + a$ we have $\Phi_m \mid m_{(B \cap (\mathbb{Z}_m + a)) - a}$.*

Proof. Lemma 2.13 handles the case $m = \frac{N}{p_i}$ so we may assume $k \geq 2$ and $m \mid \frac{N}{p_i p_j}$, where $i \neq j$.

We prove the statement for $m = \frac{N}{p_1 p_2}$. More general situation can be proved analogously. We prove that if $\Phi_N \Phi_{\frac{N}{p_1}} \Phi_{\frac{N}{p_2}} \Phi_{\frac{N}{p_1 p_2}} \mid m_B$, then $\Phi_{\frac{N}{p_1 p_2}} \mid m_{(B_{i,j} - b_{i,j})}$, where $B_{i,j} = \{b \in B \mid b \equiv i \pmod{p_1}, b \equiv j \pmod{p_2}\}$ and $b_{i,j}$ is a coset representative from $B_{i,j}$. For the sake of simplicity, from now on we identify $B_{i,j} - b_{i,j}$ with $B_{i,j}$. As in the proof of Lemma 2.13, $\Phi_N \mid m_B$, $\Phi_{\frac{N}{p_1}} \mid m_B$, $\Phi_{\frac{N}{p_2}} \mid m_B$, $\Phi_{\frac{N}{p_1 p_2}} \mid m_B$ is equivalent to

$$0 = \sum_{i=0}^{p_1-1} \sum_{j=0}^{p_2-1} \xi_{p_1}^i \xi_{p_2}^j \sum_{t \in B_{i,j}} \xi_{p_3}^{a_3(t)} \ldots \xi_{p_k}^{a_k(t)},$$

$$0 = \sum_{i=0}^{p_1-1} \sum_{j=0}^{p_2-1} \xi_{p_2}^j \sum_{t \in B_{i,j}} \xi_{p_3}^{a_3(t)} \ldots \xi_{p_k}^{a_k(t)},$$

$$0 = \sum_{i=0}^{p_1-1} \sum_{j=0}^{p_2-1} \xi_{p_1}^i \sum_{t \in B_{i,j}} \xi_{p_3}^{a_3(t)} \ldots \xi_{p_k}^{a_k(t)},$$

$$0 = \sum_{i=0}^{p_1-1} \sum_{j=0}^{p_2-1} \sum_{t \in B_{i,j}} \xi_{p_3}^{a_3(t)} \ldots \xi_{p_k}^{a_k(t)},$$

where $a_h(t) \equiv t \pmod{p_h}$, for $h = 3, \ldots, k$, respectively. Let $t_{i,j} = \sum_{t \in B_{i,j}} \xi_{p_3}^{a_3(t)} \ldots \xi_{p_k}^{a_k(t)}$. Then we have that

$$0 = \sum_{i=0}^{p_1-1} \sum_{j=0}^{p_2-1} t_{i,j} \xi_{p_1}^i \xi_{p_2}^j, \; 0 = \sum_{i=0}^{p_1-1} \sum_{j=0}^{p_2-1} t_{i,j} \xi_{p_2}^j, \; 0 = \sum_{i=0}^{p_1-1} \sum_{j=0}^{p_2-1} t_{i,j} \xi_{p_1}^i, \; 0 = \sum_{i=0}^{p_1-1} \sum_{j=0}^{p_2-1} t_{i,j}.$$

Let U be a function from $\mathbb{Z}_{p_1 p_2}$ to $\mathbb{Q}(\xi_{p_3}, \ldots, \xi_{p_k})$ defined as $U(b_{i,j}) = t_{i,j}$. Note that the minimal polynomial of ξ_{p_1}, ξ_{p_2} and $\xi_{p_1 p_2}$ over $\mathbb{Q}(\xi_{p_3}, \ldots, \xi_{p_k})$ are Φ_{p_1}, Φ_{p_2} and $\Phi_{p_1 p_2}$, respectively. Then the first three equations imply that $\Phi_{p_1 p_2} \Phi_{p_1} \Phi_{p_2} \mid m_U$. Since $\Phi_{p_1 p_2} \Phi_{p_1} \Phi_{p_2} = \sum_{i=0}^{p_1 p_2 - 1} x^i$ we have U is constant. Using the last equation we obtain $t_{i,j} = 0$ for every $i \in \mathbb{Z}_{p_1}, j \in \mathbb{Z}_{p_2}$. $\square$