CAMBRIDGE
UNIVERSITY PRESS

RESEARCH ARTICLE

On the structure of spectral and tiling subsets of cyclic groups

Romanos Diogenes Malikiosis

Aristotle University of Thessaloniki, Department of Mathematics, 541 24 Thessaloniki, Greece; E-mail: rwmanos@gmail.com.

Abstract

The purpose of this paper is to investigate the properties of spectral and tiling subsets of cyclic groups, with an eye towards the spectral set conjecture [9] in one dimension, which states that a bounded measurable subset of $\mathbb{R}$ accepts an orthogonal basis of exponentials if and only if it tiles $\mathbb{R}$ by translations. This conjecture is strongly connected to its discrete counterpart, namely that, in every finite cyclic group, a subset is spectral if and only if it is a tile. The tools presented herein are refinements of recent ones used in the setting of cyclic groups; the structure of vanishing sums of roots of unity [20] is a prevalent notion throughout the text, as well as the structure of tiling subsets of integers [1]. We manage to prove the conjecture for cyclic groups of order $p^m q^n$, when one of the exponents is ≤ 6 or when $p^{m-2} < q^4$, and also prove that a tiling subset of a cyclic group of order $p_1^m p_2 \cdots p_n$ is spectral.

Contents

1. Introduction

A basic fact in Fourier analysis is the decomposition of a periodic function into a series of orthogonal exponential functions. A natural question that arises is whether this concept can be generalized for functions defined not necessarily on intervals $[0, T]$, where T is the period, but on more general domains with some weaker conditions (for example, measurability or boundedness). This is the definition of a *spectral set*. This, of course, can be generalized to higher dimensions as well, where periodic functions have a similar decomposition.

Definition 1.1. Let μ denote the Lebesgue measure on $\mathbb{R}$. A bounded, measurable set $\Omega \subseteq \mathbb{R}^d$ with $\mu(\Omega) > 0$ is called *spectral* if there is a discrete set $\Lambda \subseteq \mathbb{R}^d$ such that the set of exponential functions $\{e_\lambda(x)\}_{\lambda \in \Lambda}$, where $e_\lambda(x) = e^{2\pi i \lambda \cdot x}$, is a complete orthogonal set, that is,

$$\langle e_\lambda, e_{\lambda'} \rangle_\Omega = \int_\Omega e_{\lambda - \lambda'}(x) dx = \delta_{\lambda \lambda'} \mu(\Omega),$$

and every $f \in L^2(\Omega)$ can be expressed as a Fourier series,

$$f(x) = \sum_{\lambda \in \Lambda} a_\lambda e_\lambda(x),$$

for some $a_\lambda \in \mathbb{C}$ (*Fourier coefficients*).

Usually, we restrict periodic functions on a fundamental domain with respect to the period lattice, so $[0, 1]^d$ is the standard case, when the period lattice is $\mathbb{Z}^d$. In general, functions defined on fundamental parallelepipeds of a lattice $\Lambda \subseteq \mathbb{R}^d$ have the same property; the exponentials then correspond to $e_\lambda(x)$, where λ ranges through the dual lattice $\Lambda^\star$. We note that fundamental parallelepipeds are *tiles* of $\mathbb{R}^d$ with respect to the period lattice, say Λ.

Definition 1.2. A subset $A \subseteq \mathbb{R}^d$ *tiles* $\mathbb{R}^d$ by translations if there is a translation set $T \subseteq \mathbb{R}^d$ such that almost all elements of $\mathbb{R}^d$ have a unique representation as a sum $a + t$, where $a \in A$, $t \in T$. We will denote this by $A \oplus T = \mathbb{R}^d$. T is called the *tiling complement* of A, and (A, T) is called a *tiling pair*.

Given the premise in the standard periodic case, i.e., functions defined on $[0, 1]^d$, it might be tempting to generalize this situation. This was first attempted in 1974 when Fuglede [9] stated the following conjecture, connecting spectral subsets and tiles of $\mathbb{R}^d$.

Conjecture 1.3. *Let $\Omega \subseteq \mathbb{R}^d$ be a bounded measurable set. Ω accepts a complete orthonormal basis of exponentials if and only if Ω tiles $\mathbb{R}^d$ by translations.*

Fuglede proved this conjecture when either a spectrum or a tiling complement of Ω is a lattice. All results proven in the next 30 years were in the positive direction until Tao [35] disproved this conjecture by constructing spectral subsets of $\mathbb{R}^5$ that do not tile the space. Shortly thereafter, tiles with no spectra in $\mathbb{R}^5$ were found by Kolountzakis and Matolcsi [15]. The current state of art on Euclidean spaces is the failure of Fuglede's conjecture on dimensions 3 and above in both directions [6, 7, 14, 24]. The noteworthy aspect of the construction of counterexamples is the passage to the setting of finite abelian groups, which is also the setting of the present article. To be more precise, an example of a spectral subset of $\mathbb{Z}_8^3$ that does not tile is lifted to a counterexample in $\mathbb{R}^3$ [14], and similarly, an example of a tile with no spectra in $\mathbb{Z}_{24}^3$ is lifted to a counterexample in $\mathbb{R}^3$ [6]. The conjecture is still open in $\mathbb{R}$ and $\mathbb{R}^2$. In the one-dimensional case, this is best summarized as follows ([3] and the references therein):

$$\textbf{T-S}(\mathbb{R}) \Longleftrightarrow \textbf{T-S}(\mathbb{Z}) \Longleftrightarrow \forall N \textbf{T-S}(\mathbb{Z}_N)$$

and

$$\textbf{S-T}(\mathbb{R}) \Longrightarrow \textbf{S-T}(\mathbb{Z}) \Longrightarrow \forall N \textbf{S-T}(\mathbb{Z}_N),$$

where **S-T**(G) denotes the fact that the Spectral $\Rightarrow$Tiling direction holds in G, while **T-S**(G) denotes that fact that the reverse implication is true.

We emphasize that the equivalence of the Spectral $\Rightarrow$Tiling direction between the 'continuous' and the 'discrete' settings depends on *rationality of spectrum*: the claim that every spectral subset of $\mathbb{R}$ of measure 1 has a spectrum in $\mathbb{Q}$, which is a difficult problem in its own right. Another important ingredient for this yet unproved equivalence is the periodicity of spectrum [10].

This conjecture has a renewed interest in the setting of finite abelian groups during the last few years, mostly due to the counterexamples mentioned above. In the cyclic case, Łaba first connected [17] the work of Coven and Meyerowitz [1] on tiling subsets of integers to Fuglede's conjecture and proved subsequently that tiles of $\mathbb{Z}$ of cardinality p^m or $p^m q^r$, where p, q primes, are also spectral; the reverse direction holds when the cardinality is p^m. These arguments can be adapted to the finite cyclic group setting, proving that the Tiling $\Rightarrow$ Spectral direction is true for finite cyclic groups of order $p^m q^n$. For a self-contained account, we refer the reader to [23]. Moreover, both directions of Fuglede's conjecture hold for cyclic groups of order p^m; again, self-contained proofs can be found in [5] and [23].

We mention in passing two another recent breakthroughs in Fuglede's conjecture. This conjecture has also been confirmed for the field of p-adic rational numbers $\mathbb{Q}_p$ [4, 5] and for convex bodies in $\mathbb{R}^d$ [21]. We return to the setting of this paper, namely finite abelian groups. For finite abelian groups with two generators, it has been shown that Fuglede's conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_p$ [11], a result later extended to $\mathbb{Z}_p \times \mathbb{Z}_{p^2}$ [32] and very recently to $\mathbb{Z}_p \times \mathbb{Z}_{p^n}$ [37]. When the generators are at least four, the Spectral $\Rightarrow$ Tiling direction fails when the cardinality of the group is odd [8].

The goal of the present article is to develop tools and prove facts about spectral subsets of $\mathbb{Z}_N$, especially when N has at most two distinct prime factors. We note that the conjecture is known to be true when $N = p^n q$ [23] or $N = p^n q^2$ [13], i.e., when one of the exponents is ≤ 2. The methods and techniques developed herein extend these results, thus 'raising' the exponent of q:

Theorem 1.4. *Let $A \subseteq \mathbb{Z}_N$ be a spectral set, where $N = p^m q^n$, with p, q distinct primes. Then A tiles $\mathbb{Z}_N$ if one of the following holds:*

1. $p < q$ and $m \leq 9$ or $n \leq 6$.
2. $p^{m-2} < q^4$.

Fuglede's conjecture in $\mathbb{Z}_N$ when $N = p^m q^n$ seems within reach. It is the hope of the author that the methods developed here to 'raise' the exponent, combined with the recent proofs of Fuglede's conjecture in the groups $\mathbb{Z}_{pqr}$ [31], $\mathbb{Z}_{p^2 qr}$ [33], and $\mathbb{Z}_{pqrs}$ [12], where the number of primes dividing N is increased, will provide the groundwork towards a more effective attack on the one-dimensional Fuglede conjecture.

Regarding the Tiling $\Rightarrow$ Spectral direction, we will provide a proof in cyclic groups of order $p_1^n p_2 \cdots p_k$; this direction was previously known for groups of order $p^m q^n$ [17] (see also [23]) or of square-free order (proven in Terence Tao's blog[1] by Łaba and Meyerowitz; see also [31]). Very recently, it was also proved for groups of order $(pqr)^2$ [18, 19].

Theorem 1.5. *Let $N = p_1^n p_2 \cdots p_k$, where $p_1, \ldots, p_k$ are distinct primes. If $A \subseteq \mathbb{Z}_N$ tiles, then A is spectral.*

Even if Fuglede's conjecture is proven for $\mathbb{Z}_{p^m q^n}$, one should be cautious before conjecturing further that this might be true in all cyclic groups. For example, several strengthened versions of the Tiling $\Rightarrow$ Spectral directions, such as the conjectures of Sands [28] and Tijdeman [36], are known to hold when N has the form $p^m q^n$, but they break down when N has at least three distinct prime factors due to counterexamples given by Szabo [34]. Furthermore, the main tools used here, such as the structure of vanishing sums of Nth roots of unity [20] and primitive subsets of $\mathbb{Z}_N$, are much stronger when N has at most two distinct prime factors.

The different tools needed for the proofs of the above theorems are laid out in Sections 2 and 3. In Section 4, we prove 1.5, which is based on an inductive approach and is relatively easy to follow. The remaining sections are exclusively devoted to the two-prime case, $N = p^m q^n$, and they are much more technical and demanding. Theorem 1.4 is eventually proven in Section 11.

2. Multisets and mask polynomials

We denote by $\mathbb{Z}_N$ the cyclic additive group of N elements. A multiset A in $\mathbb{Z}_N$ is a collection of elements of $\mathbb{Z}_N$ along with some multiplicities: Any element $a \in A$ appears $m_a \in \mathbb{N}$ times in A. The characteristic

---

function of A is denoted by $\mathbf{1}_A$, and is defined by $\mathbf{1}_A(a) = m_a$. It is understood that, if A is a proper set, this function takes only the values 0 and 1. The support of the multiset A, denoted by supp A, is simply the subset of $\mathbb{Z}_N$ of elements that appear at least once in A; in other words, supp A = supp($\mathbf{1}_A$).

Definition 2.1. Let A be a multiset of elements in $\mathbb{Z}_N$. The *mask polynomial* of A is defined by $A(X) = \sum_{a \in A} m_a X^a$ and is considered as an element in $\mathbb{Z}[X]/(X^N - 1)$. As such, the values of $A(X)$ on the Nth roots of unity ζ_N^d, $1 \le d \le N$, (here $\zeta_N = e^{2\pi i/N}$) are well-defined, i.e., independent of the representative of their class mod$(X^N - 1)$. Also, for every $d \in \mathbb{Z}$ define the multiset $d \cdot A$ whose characteristic function is

$$\mathbf{1}_{d \cdot A}(x) = \sum_{a \in \mathbb{Z}_N, da=x} \mathbf{1}_A(a).$$

The support of $d \cdot A$ will simply be denoted by dA. Finally, the multiset of elements of A that are congruent to j mod m for $m \mid N$ will be denoted as $A_{j \bmod m}$.

Example. If $A = \{0, 3\} \subseteq \mathbb{Z}_6$, then $2A = \{0\}$, while $2 \cdot A = \{0, 0\}$; moreover, $A(X) \equiv 1 + X^3$ mod $(X^6 - 1)$, $(2A)(X) \equiv 1$, $(2 \cdot A)(X) \equiv 2$. Also, $A_{0 \bmod 3} = A$, while $A_{1 \bmod 3} = A_{2 \bmod 3} = \varnothing$.

In general, the following holds for the mask polynomial of $m \cdot A$:

Proposition 2.2. *Let A be a multiset with elements from $\mathbb{Z}_N$. Then $A(X^m) \equiv (m \cdot A)(X) \bmod (X^N - 1)$ for every $m \in \mathbb{N}$. If $m \mid N$, then*

$$A(X^m) \equiv \sum_{j=0}^{N/m-1} |A_{j \bmod N/m}| X^{jm} \bmod (X^N - 1).$$

Proof. We have

$$A(X^m) \equiv \sum_{j \in A} X^{jm} \equiv \sum_{\substack{j \in A \\ jm \equiv g \bmod N}} X^g \bmod (X^N - 1),$$

and the last one is precisely the definition of the mask polynomial of the multiset $m \cdot A$. If $m \mid N$, then

$$\sum_{\substack{j \in A \\ jm \equiv g \bmod N}} X^g \equiv \sum_{\substack{j \in A \\ j \equiv gm^{-1} \bmod N/m}} X^g \equiv \sum_{j=0}^{N/m-1} |A_{j \bmod N/m}| X^{jm} \bmod (X^N - 1),$$

as desired. □

The Fourier transform of functions on $\mathbb{Z}_N$ is defined as

$$\hat{f}(x) = \sum_{d \in \mathbb{Z}_N} f(d) \zeta_N^{-dx}.$$

The values of mask polynomials $A(X)$ on Nth roots of unity have the following relation with those of the Fourier transform of $\mathbf{1}_A$:

$$\widehat{\mathbf{1}}_A(d) = A(\zeta_N^{-d}).$$

The reduced residues mod$N$ will be denoted as usual by $\mathbb{Z}_N^\star$. The group $\mathbb{Z}_N$ is partitioned into the subsets

$$d\mathbb{Z}_N^\star = \{x \in \mathbb{Z}_N : \gcd(x, N) = d\} = \{x \in \mathbb{Z}_N : \mathrm{ord}(x) = N/d\}, \tag{2.1}$$

called *divisor classes*, where d runs through the divisors of N. Since we will evaluate polynomials on Nth roots of unity, we unavoidably have to use the cyclotomic polynomials $\Phi_d(X)$ for $d \mid N$, which is the irreducible polynomial of ζ_d over $\mathbb{Q}$, and is factored as

$$\Phi_d(X) = \prod_{g \in \mathbb{Z}_d^\star} (X - \zeta_d^g).$$

Therefore, divisibility of $A(X) \bmod (X^N - 1)$ by cyclotomic polynomials of degree $d \mid N$, denoted by $\Phi_d(X)$, also makes sense as $X^N - 1 = \prod_{d \mid N} \Phi_d(X)$. $\Phi_d(X) \mid A(X)$ would then hold precisely when $A(\zeta_d) = 0$, which would also imply that $A(\zeta_d^g) = 0$ for every $g \in \mathbb{Z}_N$ with $\gcd(d, g) = 1$. From this, we readily deduce that the zero set

$$Z(A) := Z(\widehat{\mathbf{1}}_A) = \left\{ x \in \mathbb{Z}_N : A(\zeta_N^{-x}) = 0 \right\}$$

is a union of divisor classes.

3. Tiles and spectral subsets

These notions are similarly defined when we work on a finite cyclic group.

Definition 3.1. Let $A \subseteq \mathbb{Z}_N$. We say that A *tiles* $\mathbb{Z}_N$ by translations if there is some $T \subseteq \mathbb{Z}_N$ such that any element of $\mathbb{Z}_N$ can be written uniquely as a sum of an element of A and an element of T. T is called the *tiling complement* of A, and we write $A \oplus T = \mathbb{Z}_N$; we will also call (A, T) a *tiling pair*. We call A *spectral* if there is some $B \subseteq \mathbb{Z}_N$ with $|A| = |B|$ and the exponential functions

$$e_b(x) = \zeta_N^{bx}$$

are pairwise orthogonal on A, that is,

$$\langle e_b, e_{b'} \rangle_A = \sum_{a \in A} \zeta_N^{a(b-b')} = 0, \tag{3.1}$$

for every $b, b' \in B$, $b \neq b'$, or equivalently, the matrix

$$\frac{1}{\sqrt{|A|}} \left(\zeta_N^{ab} \right)_{a \in A, b \in B}$$

is unitary. In this case, B is called a *spectrum* of A, and (A, B) a *spectral pair* of $\mathbb{Z}_N$.

Using mask polynomials is very useful when describing tiling properties. The following was proven in [1] (Lemmata 1.3 and 3.1).

Lemma 3.2. *Let A, T be multisets in $\mathbb{Z}_N$. Then A and T are proper sets and form a tiling pair if and only if*

$$A(X)T(X) \equiv 1 + X + \cdots + X^{N-1} \bmod (X^N - 1).$$

Furthermore, if m is prime to $|A|$, the above equation also implies

$$A(X^m)T(X) \equiv 1 + X + \cdots + X^{N-1} \bmod (X^N - 1),$$

i.e., $m \cdot A$ is also a tiling complement of T.

Remark. Lemma 3.1 in [1] actually proves the second part when $m = p$ a prime; however, one could use this repetitively for all primes dividing m and obtain the above result.

Spectrality and the tiling property impose some structural properties on the difference set $A - A$.

Theorem 3.3. *Let $A \subseteq \mathbb{Z}_N$.*

(i) *$B \subseteq \mathbb{Z}_N$ is a spectrum of A if and only if $|A| = |B|$ and $B - B \subseteq \{0\} \cup Z(A)$.*
(ii) *A tiles $\mathbb{Z}_N$ by $T \subseteq \mathbb{Z}_N$, if and only if $N = |A||T|$ and $(A - A) \cap (T - T) = \{0\}$.*
(iii) *If (A, B) is a spectral pair of $\mathbb{Z}_N$ and $m \in \mathbb{Z}_N^{\star}$, then (A, mB) is also a spectral pair.*

Proof.

(i) This almost follows by definition. The space of functions $f : A \to \mathbb{C}$ has dimension $|A|$; therefore, a spectrum must have the same cardinality. Furthermore, by equation (3.1), we get that any $b, b' \in B$ with $b \neq b'$ must satisfy $b - b' \in Z(A)$.

(ii) Since every element of $\mathbb{Z}_N$ can be expressed uniquely as $a + t$ with $a \in A$, $t \in T$, we get a bijection between $\mathbb{Z}_N$ and $A \times T$, proving $N = |A||T|$. Furthermore, suppose that $a, a' \in A$ and $t, t' \in T$ satisfy $a - a' = t - t'$. Then $a + t' = a' + t$, so by uniqueness of representation of $a + t'$ as an element of A and an element of T, we must have $a = a'$ and $t = t'$, proving the desired fact.

(iii) We will show that $m(b - b') \in Z(A)$ for every $m \in \mathbb{Z}_N^{\star}$ and $b, b' \in B$ with $b \neq b'$. Assume that $b - b' \in d\mathbb{Z}_N^{\star}$; hence, by equation (3.1), we get $A(\zeta_N^{dg}) = 0$, where $b - b' \equiv dg \bmod N$, with $g \in \mathbb{Z}_N^{\star}$. Then $\Phi_{N/d}(X) \mid A(X)$; thus,

$$0 = A(\zeta_N^{dgm}) = A(\zeta_N^{m(b-b')}),$$

completing the proof.

$\square$

Another way to express Theorem 3.3(i) is the following.

Corollary 3.4. *Let (A, B) be a spectral pair in $\mathbb{Z}_N$. Then $A(\zeta_{\mathrm{ord}(b-b')}) = 0$, for all $b, b' \in B$ with $b \neq b'$.*

Proof. This follows from Theorem 3.3(i) as $Z(A)$ contains all divisor classes $d\mathbb{Z}_N^{\star}$ for which there are $b, b' \in B$ satisfying $b - b' \in d\mathbb{Z}_N^{\star}$, so by equation (2.1) $\mathrm{ord}(b - b') = N/d$, or equivalently, $\zeta_N^{b-b'}$ is a primitive N/d-th root of unity, yielding

$$A(\zeta_{N/d}) = A(\zeta_{\mathrm{ord}(b-b')}) = 0,$$

as desired.

$\square$

Denote by S^N be the set of prime powers dividing N, and let $S_A^N = \{s \in S^N : A(\zeta_s) = 0\}$. We define the following properties:

(T1) $A(1) = \prod_{s \in S_A^N} \Phi_s(1)$

(T2) Let $s_1, s_2, \ldots, s_k \in S_A^N$ be powers of different primes. Then $\Phi_s(X) \mid A(X)$, where $s = s_1 \cdots s_k$.

These properties implicitly assume that the cyclic group under question has order N (see also [16]). Sometimes, a set $A \subseteq \mathbb{Z}_N$ might be reduced $\bmod M$, for some $M \mid N$, $M < N$, when no two elements of A are congruent $\bmod M$. In this case, we will explicitly mention the underlying group and say, for example, that 'A satisfies (T1) and (T2) in $\mathbb{Z}_M$'. For subsets of $\mathbb{Z}$, these properties were first defined by Coven and Meyerowitz [1] to study tiling subsets of integers. They proved that (T1) and (T2) (for integers) imply that A tiles $\mathbb{Z}$; furthermore, if $|A|$ is divided by at most two distinct primes, then (T1) and (T2) are equivalent to tiling. On the other hand, Łaba [17] proved that it also implies that A is spectral. Here, we will show that the same situation carries to the finite cyclic case.[2]

---

[2]Although (I) and (II) can easily be proven using the arguments for subsets of integers, we provide a self-contained proof here. In particular, the spectrum constructed in equation (3.2) is very similar to the one constructed in the proof of Theorem 1.5 in [17].

Theorem 3.5. *Let $A \subseteq \mathbb{Z}_N$.*

(I) *If A satisfies (T1) and (T2), then it tiles $\mathbb{Z}_N$.*

(II) *If A satisfies (T1) and (T2), then it has a spectrum.*

(III) *If N is divisible by at most two distinct primes, then A tiles $\mathbb{Z}_N$ if and only if it satisfies (T1) and (T2).*

Proof. Suppose that $A \subseteq \mathbb{Z}_N$ satisfies (T1) and (T2). Denote by N_s the maximal divisor of N that is prime to s. For example, if

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

then

$$N_{p_1^m} = p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad \forall m \text{ with } 1 \le m \le \alpha_1.$$

Consider the polynomial

$$T(X) = \prod_{s \in S^N \setminus S_A^N} \Phi_s(X^{N_s}).$$

By construction, $S_T^N = S^N \setminus S_A^N$ and $|A||T| = N$. Next, we will show that $A(X)T(X)$ vanishes on any Nth root of unity. Let $X = \zeta_d$, $d \mid N$. We write

$$d = p_1^{\beta_1} \cdots p_k^{\beta_k},$$

with $0 \le \beta_j \le \alpha_j$, $1 \le j \le k$. If $s = p_j^{\beta_j} \in S_T^N$ for some j so that $d = s \cdot d_s$, then $\Phi_s(X^{N_s})$ divides $T(X)$ and d_s divides N_s; therefore,

$$\Phi_s(\zeta_d^{N_s}) = \Phi_s(\zeta_s^g) = 0,$$

for $g = N_s/d_s$, which is prime to s, yielding $T(\zeta_d) = 0$. Otherwise, every $p_j^{\beta_j} \in S_A^N$, and since A satisfies (T2), we get $\Phi_d(X) \mid A(X)$ or, equivalently $A(\zeta_d) = 0$. Combined with $|A||T| = N$, this implies

$$A(X)T(X) \equiv 1 + X + \cdots + X^{N-1} \bmod (X^N - 1);$$

thus, $T(X)$ is the mask polynomial of a set $T \subseteq \mathbb{Z}_N$, which is a tiling complement of A, proving (I).

For (II), we define the set $B \subseteq \mathbb{Z}_N$ consisting of all elements of the form

$$\sum_{s \in S_A^N} k_s \frac{N}{s}, \tag{3.2}$$

where for each $s \in S_A^N$, k_s ranges through the set $\{0, 1, \ldots, p - 1\}$, where $p = \Phi_s(1)$ is the prime dividing s. Different choices of k_s, $s \in S_A^N$ give different elements, yielding $|A| = |B|$ since A satisfies (T1). Moreover, an element in $B - B$ has the form (3.2), with the difference that $|k_s| < \Phi_s(1)$ holds instead of $0 \le k_s \le \Phi_s(1) - 1$. The order of $k_s \frac{N}{s}$ with $|k_s| < \Phi_s(1)$ is exactly s. Based on this simple fact, the order of a nonzero element of $B - B$ is $s_1 s_2 \cdots s_\ell$, where $s_1, \ldots, s_\ell \in S_A^N$ powers of distinct primes. Since A satisfies (T2), we will then have $A(\zeta_{\mathrm{ord}(b-b')}) = 0$ for every $b, b' \in B$, $b \ne b'$, so B is the spectrum of A by Theorem 3.3(i) and Corollary 3.4.

A proof for part (III) is in [23]. □

Using (II) and (III) we can easily deduce:

Theorem 3.6. *If A tiles $\mathbb{Z}_N$, where N is divisible by at most two distinct primes, then A has a spectrum.*

4. Proof of Theorem 1.5

Here, we will test the tools of the previous section to prove the Tiling $\Rightarrow$ Spectral direction in $\mathbb{Z}_N$, where $N = p_1^m p_2 p_3 \cdots p_n$, where $p_1, \ldots, p_n$ are distinct primes and $m, n \geq 2$ are integers. We will do so by proving that (T1) and (T2) always hold for a tiling subset of $\mathbb{Z}_N$.

Suppose that $A \subseteq \mathbb{Z}_N$ tiles $\mathbb{Z}_N$ by translations so that $A \oplus T = \mathbb{Z}_N$. If $\gcd(|A|, |T|) = 1$, then Lemma 3.2 implies that

$$A(X)T(X^M) \equiv 1 + X + \cdots + X^{N-1} \mod (X^N - 1), \qquad (4.1)$$

where $M = |A|$. Therefore, $M \cdot T$ is a proper set; moreover, $|M \cdot T| = |T| = N/M$ and $M \cdot T \subseteq M\mathbb{Z}_N$, which yield $M \cdot T = M\mathbb{Z}_N$, i.e., A tiles by the subgroup $M\mathbb{Z}_N$ or, equivalently,

$$A(X) \equiv 1 + X + \cdots + X^{M-1} = \prod_{1 < d \mid M} \Phi_d(X) \mod (X^M - 1).$$

From the last representation of $A(X)$ as a product of cyclotomic polynomials mod $(X^M - 1)$, it is evident that A satisfies (T1) and (T2) in $\mathbb{Z}_N$ and hence is a spectral subset of $\mathbb{Z}_N$. We remark that the direction Tiling $\Rightarrow$ Spectral holds for every tiling subset $A \subseteq \mathbb{Z}_N$ satisfying $\gcd(|A|, N/|A|) = 1$, regardless of the primes dividing N, using the same argument.

We proceed to the difficult case, where $\gcd(|A|, |T|) > 1$, and hence, $\gcd(|A|, |T|)$ is a power of p_1. Let M be the maximal divisor of $|A|$ that is prime to p_1; in particular, $\gcd(M, |T|) = 1$. Hence, as before, $M \cdot T$ is a proper set and also a tiling complement of A by Lemma 3.2 so that equation (4.1) holds. Next, suppose that

$$S_A^N = \left\{ p_1^{\ell_1}, \ldots, p_1^{\ell_r}, p_2, \ldots, p_k \right\}$$

so that

$$S_{M \cdot T}^N = S^N \setminus S_A^N = \{ p^{m_1}, \ldots, p^{m_s}, p_{k+1}, \ldots \},$$

where the sets of exponents $\{\ell_1, \ldots \ell_r\}$ and $\{m_1, \ldots, m_s\}$ form a partition of $\{1, 2, \ldots, m\}$ by equation (4.1). It is clear that A satisfies **(T1)** as

$$|A| \cdot |T| = N, \quad p_1^r p_2 \cdots p_k \mid |A|, \quad p_1^s p_{k+1} \cdots p_n \mid |T|$$

imply that $|A| = p_1^r p_2 \cdots p_k$ (besides, it is already known that tiling always implies (T1) in every $\mathbb{Z}_N$ or in $\mathbb{Z}$ [1]). For the property (T2), consider first d to be a composite divisor of $p_2 \cdots p_k = M$. Then $T(\zeta_d^M) = T(1) \neq 0$; hence, $A(\zeta_d) = 0$ by (4.1), verifying **(T2)** when we consider primes among $p_2, \ldots, p_k$. Next, consider a root of unity of order $p_1^{\ell_j} d$ ($d \mid M$ as before); we get

$$T(\zeta_{p_1^{\ell_j} d}^M) = T(\zeta_{p_1^{\ell_j}}^{M/d}) = \sigma(T(\zeta_{p_1^{\ell_j}})) \neq 0,$$

for some $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p_1^{\ell_j}})/\mathbb{Q})$, since $p_1 \nmid \frac{M}{d}$, whence

$$\Phi_{p_1^{\ell_j} d}(X) \mid A(X),$$

confirming (T2) completely for A. By Theorem 3.5(II), A is spectral, completing the proof of Theorem 1.5.

5. Vanishing sums of roots of unity

Let $G = \langle \zeta_N \rangle$, the cyclic group generated by the standard Nth root of unity. Consider the group ring $\mathbb{Z}[G]$, the ring of all formal integer linear combinations of Nth roots of unity. It is known that $\mathbb{Z}[G] \cong \mathbb{Z}[X]/(X^N - 1)$, so we may represent an element of $\mathbb{Z}[G]$ by a polynomial with integer coefficients modulo $X^N - 1$. $\mathbb{Z}[G]$ is equipped with a natural evaluation map, say v, which simply evaluates the given sum. Considered as an element of $\mathbb{Z}[X]/(X^N - 1)$, say $F(X)$, the effect of the evaluation map is $v(F) = F(\zeta_N)$, as expected.

When this sum vanishes, we obtain some information on the structure of $F(X)$. We note that $\Phi_p(\zeta_p) = 0$ for p prime implies that

$$1 + \zeta_p + \cdots + \zeta_p^{p-1}$$

is a vanishing sum of roots of unity. The same holds true for any integer linear combination of sums of this form, multiplied by roots of unity. The following theorem, attributed to Rédei [26, 27], de Bruijn [2] and Schoenberg [30], shows that the converse is true as well. We will express it in polynomial notation.

Theorem 5.1. *Let* $F(X) \in \mathbb{Z}[X]$ *with* $F(\zeta_N) = 0$. *Then*

$$F(X) \equiv \sum_{p \mid N, \, p \text{ prime}} F_p(X) \Phi_p(X^{N/p}) \bmod (X^N - 1),$$

where $F_p(X) \in \mathbb{Z}[X]$.

When N is divisible by at most two primes and $F(X)$ has nonnegative coefficients, we obtain something stronger. This is due to Lam and Leung [20].

Theorem 5.2. *Let* $F(X) \in \mathbb{Z}_{\geq 0}[X]$. *Then* $F(\zeta_N) = 0$, *where* $N = p^m q^n$ *and* p, q *primes if and only if*

$$F(X) \equiv P(X) \Phi_p(X^{N/p}) + Q(X) \Phi_q(X^{N/q}) \bmod (X^N - 1)$$

for some $P(X), Q(X) \in \mathbb{Z}_{\geq 0}[X]$. *If* $F(\zeta_N^{p^k}) \neq 0$ *(respectively,* $F(\zeta_N^{q^\ell}) \neq 0$*) for some* $1 \leq k \leq m$ *(resp.,* $1 \leq \ell \leq n$*), then we cannot have* $P(X) \equiv 0 \bmod (X^N - 1)$ *(resp.,* $Q(X) \equiv 0 \bmod (X^N - 1)$*).*

This is no longer true if N has at least three distinct prime factors, say p, q, r, as the polynomial

$$F(X) = (\Phi_p(X^{N/p}) - 1)(\Phi_q(X^{N/q}) - 1) + (\Phi_r(X^{N/r}) - 1)$$

satisfies $F(\zeta_N) = 0$ but has no such representation.

We observe that

$$\Phi_p(X^{N/p}) = 1 + X^{N/p} + X^{2N/p} + \cdots + X^{(p-1)N/p}$$

is the mask polynomial of the subgroup of $\mathbb{Z}_N$ of order p. In general, for $d \mid N$, the cosets of the subgroup of order d, $\frac{N}{d}\mathbb{Z}_N$, will be called d-cycles. So, Theorem 5.2 asserts that a vanishing sum of roots of unity of order $N = p^m q^n$ can be expressed as a *disjoint* union (i.e., as multisets, counting multiplicities) of p- and q-cycles. This is very important when we consider the difference set $A - A$ of a spectral set $A \subseteq \mathbb{Z}_N$ with $A(\zeta_N) = 0$ as it yields both $\frac{N}{p}\mathbb{Z}_N, \frac{N}{q}\mathbb{Z}_N \subseteq A - A$ under certain mild conditions, which in turn gives roots for the mask polynomial of the spectrum B due to Theorem 3.3(i).

The condition $A(\zeta_N) = 0$ is satisfied when a spectrum B is *primitive*. We will subsequently focus on spectral pairs (A, B) of primitive sets. Otherwise, we may consider A and B (after an appropriate translation) as subsets of a proper subgroup.

Definition 5.3. Let G be a finite abelian group and T a subset. We call T primitive if it is not contained in a coset of a proper subgroup of G.

Lemma 5.4. *Let $G = \mathbb{Z}_N$ with $N = p^m q^n$. A subset $T \subseteq G$ is primitive if and only if $(T - T) \cap \mathbb{Z}_N^\star \neq \varnothing$.*

Proof. Since T is primitive, for a given $t \in T$ it would hold $t - T \nsubseteq p\mathbb{Z}_N$ and $t - T \nsubseteq q\mathbb{Z}_N$, yielding $t', t'' \in T$ such that $t - t' \notin p\mathbb{Z}_N$, $t - t'' \notin q\mathbb{Z}_N$. If either $t - t' \notin q\mathbb{Z}_N$ or $t - t'' \notin p\mathbb{Z}_N$, then we get $t - t' \in \mathbb{Z}_N^\star$ or $t - t'' \in \mathbb{Z}_N^\star$, respectively. Otherwise, $t - t' \in q\mathbb{Z}_N$ and $t - t'' \in p\mathbb{Z}_N$; therefore, $t' - t'' \notin p\mathbb{Z}_N \cup q\mathbb{Z}_N$, giving $t' - t'' \in \mathbb{Z}_N^\star$, thus $(T - T) \cap \mathbb{Z}_N^\star \neq \varnothing$. The converse is trivial. $\square$

Proposition 5.5. *Let $A \subseteq \mathbb{Z}_N$. Suppose that there is j such that $A \cap (j + \frac{N}{pq}\mathbb{Z}_N) = A_{j \bmod \frac{N}{pq}}$ is not supported on a p- or q-cycle. Then $(A - A) \cap \frac{N}{pq}\mathbb{Z}_N^\star \neq \varnothing$.*

Proof. Let j be as in the hypothesis, and without loss of generality assume that $A \subseteq j + \frac{N}{pq}\mathbb{Z}_N$ or, equivalently, $A = A_{j \bmod \frac{N}{pq}}$. Translating A does not affect the conclusion, so we may further assume that $j = 0$. This confines A in the subgroup of order pq. Dividing every element by $\frac{N}{pq}$, we can assume that $N = pq$. The problem has thus been reduced to the following: Assume that $A \subseteq \mathbb{Z}_{pq}$ is not a subset of a p- or a q-cycle, then $(A - A) \cap \mathbb{Z}_{pq}^\star \neq \varnothing$. Indeed, this is the case, since A is primitive, so the conlcusion of the reduced problem follows from Lemma 5.4 with $m = n = 1$. $\square$

Lemma 5.6. *Let $A \subseteq \mathbb{Z}_N$ with $N = p^m q^n$. Suppose that there is $d \mid \frac{N}{q}$ such that $(qd) \cdot A$ is a union of p-cycles, but $A(\zeta_N^d) \neq 0$. Then*

$$(A - A) \cap \frac{N}{pqd}\mathbb{Z}_N^\star \neq \varnothing.$$

If, in addition, A is spectral, then $B(\zeta_{pqd}) = 0$ for any spectrum B of A.

Proof. By hypothesis and Proposition 2.2, we have

$$A(X^{qd}) \equiv P(X)\Phi_p(X^{N/p}) \bmod (X^N - 1).$$

Consider the intersections of dA with the cosets of the subgroup of index pq, namely

$$dA \cap (j + \frac{N}{pq}\mathbb{Z}_N) = (dA)_{j \bmod \frac{N}{pq}},$$

where $0 \leq j \leq \frac{N}{pq} - 1$. If $(dA)_{j \bmod \frac{N}{pq}} \neq \varnothing$, then it intersects every coset of the subgroup $\frac{N}{q}\mathbb{Z}_N$ contained in $j + \frac{N}{pq}\mathbb{Z}_N$. Indeed, if $da \in (dA)_{j \bmod \frac{N}{pq}}$, then

$$qda + i\frac{N}{p} \in qdA$$

for $0 \leq i \leq p - 1$ by hypothesis, so, for each i, there is $a' \in A$ such that $qda' \equiv qda + i\frac{N}{p} \bmod N$; therefore,

$$da' \equiv da + i\frac{N}{pq} + k\frac{N}{q} \bmod N$$

for some k. Each element of the form $da + i\frac{N}{pq} + k\frac{N}{q}$ belongs to a different q-cycle of $j + \frac{N}{pq}\mathbb{Z}_N$, and since there are exactly p of them, dA intersects them all. If every pair of elements $da, da' \in (dA)_{j \bmod \frac{N}{pq}}$ lying on two different q-cycles belongs to the same p-cycle, then it is evident that $(dA)_{j \bmod \frac{N}{pq}}$ is a single p-cycle. By hypothesis, the multiset $(qd) \cdot A$ contains the entire p-cycle $qj + \frac{N}{p}\mathbb{Z}_N$ with some multiplicity (i.e., every element in this p-cycle appears with the same positive multiplicity in $(qd) \cdot A$), since $(dA)_{j \bmod \frac{N}{pq}} \neq \varnothing$. We have proven that the elements $d \cdot A$ restricted to $j + \frac{N}{pq}\mathbb{Z}_N$ (i.e. the inverse image of $qj + \frac{N}{p}\mathbb{Z}_N$ under the multiplication by q map) are supported on a single p-cycle; therefore,

this p-cycle must appear with the same multiplicity in $d \cdot A$ as $qj + \frac{N}{p}\mathbb{Z}_N$ appears in $(qd) \cdot A$. Thus, if every $(dA)_{j \bmod \frac{N}{pq}}$ is supported on a p-cycle, we conlcude that $d \cdot A$ is also a union of p-cycles as a multiset, giving $A(\zeta_N^d) = 0$, a contradiction.

This proves the existence of $da, da' \in (dA)_{j \bmod \frac{N}{pq}}$, lying on two different q-cycles, and two different p-cycles as well, for some j. Then $(dA)_{j \bmod \frac{N}{pq}}$ is not supported on a p- or q-cycle, so by Proposition 5.5

$$(dA - dA) \cap \frac{N}{pq}\mathbb{Z}_N^\star \neq \varnothing,$$

or equivalently, there are $a, a' \in A$ such that $d(a - a') \in \frac{N}{pq}\mathbb{Z}_N^\star$, which shows that $\mathrm{ord}(a - a') = pqd$; indeed, as $pqd(a - a') \equiv 0 \bmod N$, while $pd(a - a') \in \frac{N}{q}\mathbb{Z}_N^\star$ and $qd(a - a') \in \frac{N}{p}\mathbb{Z}_N^\star$. This implies that $(A - A) \cap \frac{N}{pqd}\mathbb{Z}_N^\star \neq \varnothing$, hence $B(\zeta_{pqd}) = 0$ for any spectrum B of A by Corollary 3.4, completing the proof. □

6. Some special cases

For the rest of this article, we restrict to $N = p^m q^n$, where p, q are distinct primes. There are some special cases that yield somewhat easily the Spectral $\Rightarrow$ Tile direction and serve as building blocks in more general cases.

Consider the natural map $\mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_q[X]$, which is just reduction of the coefficients $\bmod q$. The image of a polynomial $P(X) \in \mathbb{Z}[X]$ will be denoted simply by $\overline{P}(X)$. Reducing the coefficients modulo a prime dividing N seems very advantageous when a small power of said prime appears in the prime decomposition of N.

Theorem 6.1. *Let p, q be distinct primes and $N = p^m q^n$, where m, n are positive integers. Suppose that $A \subseteq \mathbb{Z}_N$ is spectral such that $pq \nmid |A|$. Then A tiles $\mathbb{Z}_N$ by translations.*

Proof. Without loss of generality, we may assume that $q \nmid |A|$. It holds $A(\zeta) \neq 0$ when $\zeta^{q^n} = 1$; otherwise, $A(X)$ would be divided by some cyclotomic polynomial $\Phi_{q^k}(X)$ for some $1 \leq k \leq n$, and as a consequence, $q = \Phi_{q^k}(1)$ would divide $A(1) = |A|$, a contradiction. Next, consider the set

$$R = \left\{ r \in [1, m] : A(\zeta_{p^r}\zeta_{q^k}) = 0, \text{ for some } k, 0 \leq k \leq n \right\}.$$

Define the following polynomial

$$F(X) = A(X) \prod_{\substack{1 \leq r \leq m \\ r \notin R}} \Phi_{p^r}(X), \tag{6.1}$$

which has nonnegative integer coefficients. We will show that $F(1) \leq p^m$ or, equivalently, $A(1) \leq p^{|R|}$. To this end, consider the spectrum B of A, which satisfies $|A| = |B|$ and $B - B \subseteq \{0\} \cup Z(A)$ by Theorem 3.3(i). Since $A(\zeta) \neq 0$ when $\zeta^{q^n} = 1$, we obtain $(B - B) \cap p^m\mathbb{Z}_N = \{0\}$; therefore, any two distinct elements of B are not congruent modulo p^m (giving a first estimate of $|A| \leq p^m$). So, we may write for every $b \in B$

$$b \equiv b_0 + b_1 p + \cdots + b_{m-1}p^{m-1} \bmod p^m, \ 0 \leq b_j \leq p - 1, \ 0 \leq j \leq m - 1$$

and observe that no two elements of B correspond to the same m-tuple $(b_0, \ldots, b_{m-1})$. Moreover, no two elements of B can agree on all p-adic digits b_r for $m - r \in R$. If such elements existed, say $b \neq b'$, then $p^r \parallel b - b'$ for some $m - r \notin R$, and since (A, B) is a spectral pair, we should have $A(\zeta_{p^{m-r}}\zeta_{q^k}) = 0$ for some k by Corollary 3.4, contradicting the fact $m - r \notin R$. This clearly shows that $|A| \leq p^{|R|}$, and thus $F(1) \leq p^m$.

Next, we will show that $\overline{\Phi}_{p^r}(X) \mid \overline{F}(X)$ in $\mathbb{F}_q[X]$ for $1 \leq r \leq m$. If $r \notin R$, this follows immediately from equation (6.1). If $r \in R$, then by definition $\Phi_{p^r q^k}(X) \mid A(X)$ for some k, hence $\Phi_{p^r q^k}(X) \mid F(X)$, where $p^r q^k \mid N$. Using standard properties of cyclotomic polynomials, we get

$$\Phi_{p^r q^k}(X) = \Phi_{pq}(X^{p^{r-1}q^{k-1}}) = \frac{\Phi_p(X^{p^{r-1}q^k})}{\Phi_p(X^{p^{r-1}q^{k-1}})}.$$

Reducing coefficients $\mathrm{mod}\, q$, we obtain

$$\frac{\overline{\Phi}_p(X^{p^{r-1}})^{q^k}}{\overline{\Phi}_p(X^{p^{r-1}})^{q^{k-1}}} = \overline{\Phi}_p(X^{p^{r-1}})^{q^{k-1}(q-1)} = \overline{\Phi}_{p^r}(X)^{q^{k-1}(q-1)}.$$

Therefore,

$$\prod_{r=1}^{m} \overline{\Phi}_{p^r}(X) = X^{p^m-1} + \cdots + 1 \mid \overline{F}(X)$$

in $\mathbb{F}_q[X]$, say

$$\overline{F}(X) = (X^{p^m-1} + \cdots + 1)G(X).$$

Now, we reduce $\mathrm{mod}\,(X^{p^m} - 1)$. Since

$$X^\ell(X^{p^m-1} + \cdots + 1) \equiv X^{p^m-1} + \cdots + 1 \,\mathrm{mod}\,(X^{p^m} - 1)$$

for every ℓ, we get

$$\overline{F}(X) \equiv G(1)(X^{p^m-1} + \cdots + 1) \,\mathrm{mod}\,(X^{p^m} - 1), \tag{6.2}$$

where $G(1) \neq 0$ (in $\mathbb{F}_q$) by assumption. Consider the remainder of the Euclidean division $F(X)$: $X^{p^m} - 1$ in $\mathbb{Z}[X]$, say $R(X)$. It is not hard to show that R has also nonnegative coefficients; indeed, if $F(X) = \sum_{k=0}^{\deg F} f_k X^k \in \mathbb{Z}_{\geq 0}[X]$, then

$$R(X) = \sum_{k=0}^{p^m-1} \left(\sum_{\ell \equiv k \,\mathrm{mod}\,(p^m-1)} f_\ell \right) X^k \in \mathbb{Z}_{\geq 0}[X].$$

All coefficients of $R(X)$ must be congruent to $c \equiv G(1) \,\mathrm{mod}\, q$ due to equation (6.2). Without loss of generality, we may assume $0 < c < q$; hence, positivity of the coefficients of R implies

$$R(X) = c(X^{p^m-1} + \cdots + 1) + qQ(X),$$

where $Q(X) \in \mathbb{Z}_{\geq 0}[X]$. Therefore,

$$F(1) = R(1) = cp^m + qQ(1) \geq p^m,$$

implying $F(1) = p^m$ and $Q(X) \equiv 0$. From this we obtain

$$F(X) \equiv X^{p^m-1} + \cdots + 1 \,\mathrm{mod}\,(X^{p^m} - 1)$$

in $\mathbb{Z}[X]$. Clearly,

$$F(X) \sum_{s=0}^{q^n-1} X^{p^m s} \equiv X^{N-1} + \cdots + 1 \mod (X^N - 1),$$

so, for the polynomial $C(X) \in \mathbb{Z}[X]$ with nonnegative coefficients defined by

$$C(X) = \left(\sum_{s=0}^{q^n-1} X^{p^m s} \right) \prod_{\substack{1 \le r \le m \\ r \notin R}} \Phi_{p^r}(X),$$

we have

$$A(X)C(X) \equiv X^{N-1} + \cdots + 1 \mod (X^N - 1),$$

implying that $C(X)$ is the mask polynomial of a set C which is the tiling complement of A. This completes the proof. $\qquad \square$

Theorem 6.1 proves the Spectral $\Rightarrow$ Tiling direction for sets A whose cardinality is prime to either p or q. On the other extreme, the same holds when the cardinality is divisible by the maximal power of either p or q, dividing N.

Proposition 6.2. *Let $N = p^m q^n$ and $A \subseteq \mathbb{Z}_N$ spectral such that $p^m \mid |A|$ or $q^n \mid |A|$. Then A tiles $\mathbb{Z}_N$.*

Proof. Without loss of generality, $p^m \mid |A|$, and let B be a spectrum of A. Suppose that

$$S_B^N = \{p^{m_1}, \ldots, p^{m_\ell}, q^{n_1}, \ldots, q^{n_k}\},$$

where $1 \le m_1 < \cdots < m_\ell \le m$ and $1 \le n_1 < \cdots < n_k \le n$. Since

$$\Phi_{q^{n_1}}(X) \cdots \Phi_{q^{n_k}}(X) \mid B(X),$$

we obtain

$$p^m q^k \mid |B| = |A|$$

by putting $X = 1$, and using the hypothesis. For every j, consider $A_{j \bmod p^m}$. Since $A_{j \bmod p^m} - A_{j \bmod p^m} \subseteq p^m \mathbb{Z}_N$, we must have

$$A_{j \bmod p^m} - A_{j \bmod p^m} \subseteq \{0\} \cup p^m q^{n-n_1} \mathbb{Z}_N^\star \cup \cdots \cup p^m q^{n-n_k} \mathbb{Z}_N^\star \tag{6.3}$$

by Theorem 3.3(i). As usual, we consider the (finite) q-adic expansion of each $a \in \mathbb{Z}_N$ as

$$a \equiv a_0 + a_1 q + a_2 q^2 + \cdots + a_{n-1} q^{n-1} \mod q^n, \quad 0 \le a_i \le q - 1, 0 \le i \le n - 1.$$

Suppose that $|A_{j \bmod p^m}| > q^k$ for some j. This would imply the existence of $a, a' \in A_{j \bmod p^m}$ that would have the same q-adic digits at positions $n - n_1, \ldots, n - n_k$; hence, $a - a'$ would not belong to the above union, contradiction. Thus, $|A_{j \bmod p^m}| \le q^k$ for all j, and in light of $p^m q^k \mid |A|$, we must have

$$|A_{j \bmod p^m}| = q^k, \ \forall j.$$

This further implies $A(\zeta_{p^\ell}) = 0$, $1 \le \ell \le m$. Using the same argument as above, where we reverse the roles of A and B, we also obtain $B(\zeta_{p^\ell}) = 0$, for $1 \le \ell \le m$, whence

$$|B_{j \bmod p^m}| = q^k, \ \forall j.$$

Next, consider

$$S_A^N = \{p, p^2, \ldots, p^m, q^{s_1}, \ldots, q^{s_t}\},$$

where $1 \le s_1 < \cdots < s_t \le n$ so that

$$\Phi_{q^{s_1}}(X) \cdots \Phi_{q^{s_t}}(X) \mid A(X),$$

and putting $X = 1$, we get $q^t \mid |A|$, which yields $t \le k$. We actually have $t = k$ since

$$B_{j \bmod p^m} - B_{j \bmod p^m} = \{0\} \cup p^m q^{n-s_1} \mathbb{Z}_N^\star \cup \cdots \cup p^m q^{n-s_t} \mathbb{Z}_N^\star, \tag{6.4}$$

for every j, and $|B_{j \bmod p^m}| = q^k$. If $t < k$, then there would exist $b, b' \in B_{j \bmod p^m}$, $b \ne b'$ whose q-adic expansions $\bmod q^n$ agree on all q-adic digits corresponding to q^{n-s_i}, $1 \le i \le t$. But then

$$b - b' \notin \{0\} \cup p^m q^{n-s_1} \mathbb{Z}_N^\star \cup \cdots \cup p^m q^{n-s_t} \mathbb{Z}_N^\star,$$

contradiction. Thus, $t = k$ and in particular, A satisfies (T1).

Next, consider the polynomial

$$\Lambda(X) = \prod_{i=1}^k \Phi_{q^{n_i}}(X^{p^m}).$$

As the coefficients of $\Lambda(X)$ are 0 or 1, it is the mask polynomial of a set $\Lambda \subseteq \mathbb{Z}_N$ with cardinality $|\Lambda| = \Lambda(1) = q^k$. By equation (6.3), Λ is then the common spectrum of the sets $A_{j \bmod p^m}$. It holds

$$\bigcup_{i=1}^k p^m q^{n_i-1} \mathbb{Z}_N^\star \subseteq \Lambda - \Lambda \subseteq \{0\} \cup Z(A_{j \bmod p^m})$$

for every j by Theorem 3.3(i); therefore,

$$A_{j \bmod p^m}(\zeta_{q^{n-n_i+1}}) = 0, \ 1 \le i \le k, \ \forall j.$$

Thus, $A(\zeta_{q^{n-n_i+1}}) = 0$, $1 \le i \le k$, proving eventually that $n_i + s_i = n + 1$, and

$$S_A^N = \{p, p^2, \ldots, p^m, q^{n-n_1+1}, \ldots, q^{n-n_k+1}\}.$$

Next, we fix j and consider the polynomial $F(X)$ satisfying

$$A_{j \bmod p^m}(X) \equiv X^j F(X^{p^m}) \bmod (X^N - 1).$$

Since $\Phi_{q^{n-n_i+1}}(X) \mid F(X^{p^m})$ for $1 \le i \le k$ and p^m is prime to q^{n-n_i+1}, we also have $\Phi_{q^{n-n_i+1}}(X) \mid F(X)$. Therefore, for $1 \le \ell \le m$, we have

$$A_{j \bmod p^m}(\zeta_{p^\ell q^{n-n_i+1}}) = \zeta_{p^\ell q^{n-n_i+1}}^j F(\zeta_{p^\ell q^{n-n_i+1}}^{p^m}) = \zeta_{p^\ell q^{n-n_i+1}}^j F(\zeta_{q^{n-n_i+1}}^{p^{m-\ell}}) = 0,$$

proving

$$A(\zeta_{p^\ell q^{n-n_i+1}}) = 0, \ 1 \le i \le k, \ 1 \le \ell \le m;$$

thus, A satisfies (T2) as well, hence tiles $\mathbb{Z}_N$ by virtue of Theorem 3.5(I), as desired. $\square$

The techniques developed so far cover the result proven [23].

Corollary 6.3. *Let $N = p^n q$. Then $A \subseteq \mathbb{Z}_N$ is spectral if and only if it is a tile.*

Proof. If A tiles, then it is spectral by Theorem 3.6. Suppose that A is spectral. If $q \nmid |A|$, then A tiles by Theorem 6.1; if $q \mid |A|$, then A tiles by Proposition 6.2. □

7. Sketch of the proof of Theorem 1.4

Before proceeding to the most technical part of the proof of Theorem 1.4, we will describe the main ideas. First of all, the proof is inductive in nature. So far, there are some positive results involving products of two prime powers (for example, Corollary 6.3), so we may work in a group $\mathbb{Z}_N$ with $N = p^m q^n$ such that Fuglede's conjecture holds in all proper subgroups of $\mathbb{Z}_N$. In other words, it holds in all groups of the form $\mathbb{Z}_M$ with $M \mid N, M < N$.

If (A, B) is a spectral pair in such a group, we may easily make some reductions for both A and B. If either A or B is a subset of a coset of a proper subgroup, we reduce to a spectral pair in a subgroup of $\mathbb{Z}_N$. Hence, we obtain the tiling property in the smaller group, which in turn implies that A tiles $\mathbb{Z}_N$ (Proposition 8.2). Therefore, we reduce to the case where A and every spectrum B are primitive. Primitivity implies that both difference sets $A - A$ and $B - B$ intersect $\mathbb{Z}_N^\star$ by Lemma 5.4. Then Theorem 3.3(i) yields that ζ_N is a root of both $A(X)$ and $B(X)$ (Corollary 8.3). Hence, each of them is a disjoint union of p- and q-cycles by Theorem 5.2. We obtain thus a first strong information about the structure of both A and B, which in turn shows that $A - A$ and $B - B$ intersect other divisor classes, which provide more roots for $A(X)$ and $B(X)$, hence more information about A and B, and so on.

Further reductions are possible. If A is a union only of p-cycles (or only of q-cycles), then we can again reduce the problem to a smaller subgroup where Fuglede's conjecture holds, which yields that A tiles $\mathbb{Z}_N$. We can thus reduce to the case where A is not a union only of p-cycles or only of q-cycles (Proposition 8.4). The same fact applies for every spectrum B of A; however, it is more difficult to prove (Corollary 10.8).

Next, we consider subsets of a spectral set $A \subseteq \mathbb{Z}_N$, of the form $A_{j \bmod d} = A \cap (j + d\mathbb{Z}_N)$, where $d \mid N$. If, say, $pd \mid N$, we have the obvious partition of $A_{j \bmod d}$

$$A_{j \bmod d} = \bigsqcup_{k=0}^{p-1} A_{j+kd \bmod pd},$$

and a same partition holds when $qd \mid N$. If all sets in the above disjoint union have equal cardinalities, then we say that $A_{j \bmod d}$ is equidistributed $\bmod pd$, and on the other extreme, if only one of the above sets is nonempty, we say that $A_{j \bmod d}$ is absorbed $\bmod pd$. One or the other property holds when a certain combination of roots of $A(X)$ and $B(X)$ appears (Lemma 9.2). Taking into account how $A_{j \bmod d}$ distributes $\bmod pd$ or $\bmod qd$ and then taking the difference between sets in the union above, we obtain information not only about the roots of $B(X)$ (using Theorem 3.3(i)) but also of $A(X)$. This is the content of Section 9.

If there is some $d = p^k$ (respectively, $d = q^\ell$) such that either $A_{j \bmod d}$ or $B_{j \bmod d}$ is absorbed $\bmod pd$ (respectively, $\bmod qd$) for every j, then we can extend both sets so that we obtain a new spectral pair (A', B') (Lemma 9.3, Corollary 9.4, Lemma 9.6). Both A' and B' are absorption-free, and $A' = A \oplus S$, for some $S \subseteq \mathbb{Z}_N$ for which $0 \in S$. In particular, if A' tiles, then so does A. With this argument, we may further reduce the problem to those spectral sets A that are absorption-free as well. This certainly holds true when $A \in \mathscr{F}(N)$ has maximal size; we denote the set of all such spectral sets by $\mathscr{F}_{\max}(N)$.

The failure of Fuglede's conjecture in $\mathbb{Z}_N$, especially when it holds for all proper groups $\mathbb{Z}_N$, imposes some symmetry on the roots of the mask polynomials of the spectral pair (A, B) when $A \in \mathscr{F}(N)$ (Lemma 10.3 and Proposition 10.4). This result, along with subsequent ones, is obtained by checking how sets of the form $B_{j \bmod d}$ or $A_{j \bmod d}$ distribute $\bmod pd$ and $\bmod qd$ (i.e., especially when we have absorption or equidistribution) when d ranges through the powers $p, p^2, \ldots$ or $q, q^2 \ldots$. Arguments

of this type are used in the proofs of Lemma 10.5 and the more technical Lemmata 11.4 and 11.8 (in Lemma 11.4 we also examine the distribution of sets of the form $A_{j \bmod p^{m-r-1}q^{n-1}}$).

Lemma 10.5 is the first indication that, if $A \in \mathscr{F}_{\max}(N)$, then (T1) fails for every spectrum B so that $B \in \mathscr{F}_{\max}(N)$ (Corollary 10.7). We recall that every root of the form ζ_{p^x} contributes a factor of p in the cardinality of B; Lemma 10.5 states also that we get a contribution of a factor of p even when $B(\zeta_{p^x}) \neq 0 = B(\zeta_{p^x q})$. Lemma 11.4 estimates the number of such x, and then Lemma 11.8 estimates the number of x for which the symmetry of root patterns fails, called herein the root deficit. These estimates eventually lead to the desired result when one of the exponents m or n is small enough or when $p^{m-2} < q^4$.

8. Primitive subsets and an inductive approach

The existence of a spectral subset $A \subseteq \mathbb{Z}_N$ that does not tile imposes a very rigid structure on A that is impossible to appear in a subset of $\mathbb{Z}_N$ under certain conditions. This is the main argument for proving Fuglede's conjecture in certain cyclic groups of order $N = p^m q^n$. We will usually consider groups such that Fuglede's conjecture holds in all proper subgroups.

Definition 8.1. For two distinct primes p, q, define the following set:

$$\mathcal{S}_{p,q} = \{N = p^m q^n : \mathbb{Z}_N \text{ has spectral subsets that do not tile}\}.$$

We distinguish also the minimal elements in terms of division by defining the following subset of $\mathcal{S}_{p,q}$:

$$\mathcal{S}'_{p,q} = \{N \in \mathcal{S}_{p,q} : \forall M \mid N \text{ satisfying } M \neq N, \text{ it holds } M \notin \mathcal{S}_{p,q}\}$$

or, equivalently, $N \in \mathcal{S}'_{p,q}$ if Fuglede's conjecture is not true in $\mathbb{Z}_N$ but holds in every subgroup of $\mathbb{Z}_N$. Finally, for each $N \in \mathcal{S}_{p,q}$, we define

$$\mathscr{F}(N) = \{A \subseteq \mathbb{Z}_N : A \text{ is spectral but does not tile}\}.$$

Remark. Fuglede's conjecture holds in $\mathbb{Z}_{p^m q^n}$ for every $m, n \geq 1$ if and only if $\mathcal{S}_{p,q} = \varnothing$. Throughout this paper, we will usually show that Fuglede's conjecture holds for a specific $\mathbb{Z}_N$ (or a family of cyclic groups) by showing that N cannot belong to $\mathcal{S}_{p,q}$ or, equivalently, that $\mathscr{F}(N) = \varnothing$. We will do so by proving some properties of the sets belonging to $\mathscr{F}(N)$, which will be impossible to hold under some conditions, for example, if one of the exponents m, n is relatively small.

Now, we start proving properties for the sets defined above. We recall that a subset of $\mathbb{Z}_N$ is called primitive if it is not contained in a coset of a proper subgroup of $\mathbb{Z}_N$.

Proposition 8.2. *Let $A \subseteq \mathbb{Z}_N$ be a spectral set, $N \in \mathcal{S}'_{p,q}$, such that A is not primitive or possesses a nonprimitive spectrum, B. Then A satisfies (T1) and (T2) or, equivalently, $A \notin \mathscr{F}(N)$.*

Proof. Suppose that A has a spectrum B that is not primitive. Then a translate of B must be contained in a maximal subgroup of $\mathbb{Z}_N$, i.e., either $p\mathbb{Z}_N$ or $q\mathbb{Z}_N$. This translate is also a spectrum of A, so without loss of generality, we may assume $B \subseteq p\mathbb{Z}_N$. This shows the existence of $B' \subseteq \mathbb{Z}_N$ with $|B| = |B'|$ and $B = pB'$. The matrix

$$\frac{1}{\sqrt{|A|}} \left(\zeta_N^{ab}\right)_{a \in A, b \in B} = \frac{1}{\sqrt{|A|}} \left(\zeta_{N/p}^{ab'}\right)_{a \in A, b' \in B'}$$

is unitary by definition; hence, no two elements of A leave the same residue $\bmod N/p$ (as well as of B'). Hence, (A, B') can be considered as a spectral in $\mathbb{Z}_{N/p}$, so $A(X) \bmod (X^{N/p} - 1)$ satisfies (T1) and (T2) by definition of $\mathcal{S}'_{p,q}$. This in particular shows that $A(\zeta_{p^m}) \neq 0$. Otherwise, (T1) would fail $\bmod N/p$. Therefore, (T1) and (T2) are satisfied by $A(X) \bmod (X^N - 1)$ as well.

Next, suppose that A is not primitive so that $A \subseteq p\mathbb{Z}_N$ without loss of generality. As before, (A', B) would be a spectral pair in $\mathbb{Z}_{N/p}$, where $A = pA'$, so $A'(X)$ satisfies (T1) and (T2) by definition of $\mathcal{S}'_{p,q}$. We have $A(X) \equiv A'(X^p) \mod (X^N - 1)$, hence $A(\zeta_p) \neq 0$. The following show that A also satisfies (T1) and (T2):

$$A'(\zeta_{p^k q^\ell}) = 0 \implies A(\zeta_{p^{k+1} q^\ell}) = 0,$$

and

$$A'(\zeta_{q^k}) = 0 \implies A(\zeta_{pq^k}) = A(\zeta_{q^k}) = 0.$$

For the latter, consider t such that $pt \equiv 1 \mod q^k$. Then

$$A(\zeta_{q^k}^t) = A'(\zeta_{q^k}^{pt}) = A'(\zeta_{q^k}) = 0,$$

and by a Galois action, we get $A(\zeta_{q^k}) = 0$ as well. This completes the proof. $\qquad\square$

Corollary 8.3. *If $A \in \mathcal{F}(N)$, $N \in \mathcal{S}'_{p,q}$, then*

$$A(\zeta_N) = B(\zeta_N) = 0$$

for any spectrum $B \subseteq \mathbb{Z}_N$ of A.

Proof. By Proposition 8.2, A and every spectrum B are primitive. By Lemma 5.4, we get $(A - A) \cap \mathbb{Z}_N^\star \neq \varnothing \neq (B - B) \cap \mathbb{Z}_N^\star$, so by Theorem 3.3(i), we obtain $A(\zeta_N) = B(\zeta_N) = 0$. $\qquad\square$

Consider $A \in \mathcal{F}(N)$, $N \in \mathcal{S}'_{p,q}$, and B a spectrum of A. By Corollary 8.3 and Theorem 5.2, we may write

$$A(X) \equiv P(X)\Phi_p(X^{N/p}) + Q(X)\Phi_q(X^{N/q}) \mod (X^N - 1), \tag{8.1}$$

for $P(X), Q(X) \in \mathbb{Z}_{\geq 0}[X]$, and

$$B(X) \equiv R(X)\Phi_p(X^{N/p}) + S(X)\Phi_q(X^{N/q}) \mod (X^N - 1) \tag{8.2}$$

for $R(X), S(X) \in \mathbb{Z}_{\geq 0}[X]/(X^N - 1)$. Next, we will show that Fuglede's conjecture is satisfied if P or Q is identically zero.

Proposition 8.4. *Suppose that $A \in \mathcal{F}(N)$, $N \in \mathcal{S}'_{p,q}$. Then A cannot be expressed as a union of p- or q-cycles exclusively (i.e., $Q \equiv 0$ or $P \equiv 0$, respectively).*

Proof. Let B be a spectrum of A, and suppose that A is a union of p- or q-cycles exclusively. Without loss of generality, we may assume $Q \equiv 0$ so that

$$A(X) \equiv P(X)\Phi_p(X^{N/p}) \mod (X^N - 1). \tag{8.3}$$

For every $a \in A$, we have $a + \frac{N}{p}\mathbb{Z}_N \subseteq A$, hence $(A - A) \cap \frac{N}{p}\mathbb{Z}_N^\star \neq \varnothing$, implying $B(\zeta_p) = 0$ and

$$|B_{j \bmod p}| = \frac{1}{p}|B|, \ \forall j.$$

Since $P(X) \in \mathbb{Z}_{\geq 0}[X]$, the coefficients must be either 0 or 1; therefore, $P(X)$ is the mask polynomial of a set $P \subseteq \mathbb{Z}_N$. Furthermore, equation (8.3) shows that any element of P is unique $\bmod N/p$, so we may consider this as a subset in $\mathbb{Z}_{N/p}$.

Next, we will show that each $B_{j \bmod p}$ is a spectrum for P. Since

$$B_{j \bmod p} - B_{j \bmod p} \subseteq p\mathbb{Z}_N \cap (Z(A) \cup \{0\}),$$

by Theorem 3.3(i), it suffices to show that $A(\zeta_N^d) = 0$ implies $P(\zeta_N^d) = 0$ whenever $p \mid d$ and $d \mid N$, i.e., $A(X)$ and $P(X)$ have the same roots when we restrict to the $\frac{N}{p}$-roots of unity. But this is true since (8.3) implies

$$A(X) \equiv pP(X) \bmod (X^{N/p} - 1),$$

therefore, $A(\zeta_{N/p}^d) = pP(\zeta_{N/p}^d)$ for all d. We observe that each spectrum $-j + B_{j \bmod p}$ is a subset of the subgroup of $\mathbb{Z}_N$ of order N/p, which shows that $P \subseteq \mathbb{Z}_{N/p}$ is spectral since $|P| = |B_{j \bmod p}|$ for all j.

By definition of $\mathcal{S}'_{p,q}$, P satisfies (T1) and (T2). We remind that $A(X)$ and $P(X)$ have precisely the same roots when we restrict to the $\frac{N}{p}$-roots of unity. In addition, $A(X)$ vanishes for all other Nth roots of unity as $\Phi_p(X^{N/p}) \mid A(X)$, clearly showing that $A(X)$ satisfies (T1) and (T2) as well. □

One might expect that a similar proof applies when B is a union of p- or q-cycles exclusively. However, we didn't manage to find such a straightforward proof but rather a complicated one. The crucial ideas needed for this are examined in the next sections.

9. The absorption-equidistribution property

Definition 9.1. Let $A \subseteq \mathbb{Z}_N$, and let $pd \mid N$, where p is a prime. We call the set $A_{i \bmod d}$ *absorbed* $\bmod pd$ if there is k with $0 \le k \le p - 1$ such that $A_{i \bmod d} = A_{i+kd \bmod pd}$. We call it *equidistributed* $\bmod pd$ if $|A_{i+kd \bmod pd}| = \frac{1}{p}|A_{i \bmod d}|$ for every k with $0 \le k \le p - 1$.

A fundamental observation coming from the structure of the vanishing sums of roots of unity, i.e., Theorem 5.2, is the fact that $A(\zeta_{p^{k+1}}) = 0$ implies that each $A_{i \bmod p^k}$ is equidistributed $\bmod p^{k+1}$.

Lemma 9.2. *Let (A, B) be a spectral pair in $\mathbb{Z}_N$, $N = p^m q^n$ and d a divisor of $\frac{N}{pq}$ such that*

$$A(\zeta_N^d)B(\zeta_{pd}) \neq 0 = B(\zeta_{pqd}).$$

Then each subset $B_{i \bmod d}$ is either absorbed or equidistributed $\bmod pd$. Absorption occurs for at least one i.

Proof. By Theorem 5.2, the multiset $\frac{N}{pqd} \cdot B$ is a disjoint union of p- and q-cycles. Each such cycle is a subset of a unique pq-cycle (i.e., a coset of the subgroup $\frac{N}{pq}\mathbb{Z}_N$) as $j + \frac{N}{p}\mathbb{Z}_N \subseteq j + \frac{N}{pq}\mathbb{Z}_N$, for example. Therefore, the same conclusion holds for the elements of $\frac{N}{pqd} \cdot B$ (*counting multiplicities*) in an arbitrary pq-cycle. If $\frac{N}{pqd} \cdot B \cap (j + \frac{N}{pq}\mathbb{Z}_N)$ is not supported on a single p- or q-cycle, then there are $b, b' \in B$ such that $\frac{N}{pqd}(b - b') \in \frac{N}{pq}\mathbb{Z}_N^\star$ by virtue of Proposition 5.5. This yields $b - b' \in d\mathbb{Z}_N^\star$, contradicting the fact that $A(\zeta_N^d) \neq 0$, using Theorem 3.3(i). Now, every element of $\frac{N}{pqd} \cdot B_{i \bmod d}$ belongs to the pq-cycle $\frac{iN}{pqd} + \frac{N}{pq}\mathbb{Z}_N$; therefore, it must also be a disjoint union of p- and q-cycles. In our case, it must be a single p- or q-cycle with a certain multiplicity. If $\frac{N}{pqd} \cdot B_{i \bmod d}$ is a p-cycle with a multiplicity, then this p-cycle must be

$$\frac{iN}{pqd} + k\frac{N}{q} + \frac{N}{p}\mathbb{Z}_N = \frac{N}{pqd}B_{i \bmod d}$$

for some k, which clearly shows that $|B_{i+kpd+jqd \bmod pqd}|$ is constant in j, and

$$B_{i+k'pd+jqd \bmod pqd} = \varnothing,$$

for $k' \not\equiv k \bmod q$. This yields the absorption

$$B_{i+jqd \bmod pd} = B_{i+kpd+jqd \bmod pqd}$$

for all j, which shows that $B_{i \bmod d}$ is equidistributed $\bmod pd$. If on the other hand, $\frac{N}{pqd} \cdot B_{i \bmod d}$ is a q-cycle with a multiplicity, then this q-cycle must be

$$\frac{iN}{pqd} + j\frac{N}{p} + \frac{N}{q}\mathbb{Z}_N = \frac{N}{pqd}B_{i \bmod d}$$

for some j, which shows that $|B_{i+jqd+kpd \bmod pqd}|$ is constant in k, and

$$B_{i+j'qd+kpd \bmod pqd} = \varnothing,$$

for $j' \not\equiv j \bmod p$. This yields

$$|B_{i \bmod d}| = |B_{i+jqd \bmod pd}| = p|B_{i+jqd+kpd \bmod pqd}|$$

for this value of j and every k, which shows that $B_{i \bmod d}$ is absorbed $\bmod pd$. Absorption $\bmod pd$ must occur for at least one i. Otherwise, we would have $B(\zeta_{pd}) = 0$, contradiction. $\square$

Lemma 9.3. *Let (A, B) be a spectral pair in $\mathbb{Z}_N$, $N = p^m q^n$ such that $B_{i \bmod p^k}$ is absorbed $\bmod p^{k+1}$ for every i, where $0 \leq k < m$. Then*

$$\overline{A}(X) \equiv A(X)\Phi_{p^{m-k}}(X^{q^n}) \bmod (X^N - 1)$$

is the mask polynomial of a spectral set whose spectrum has the following mask polynomial:

$$\overline{B}(X) \equiv B(X)\Phi_{p^{k+1}}(X^{q^n}) \bmod (X^N - 1).$$

Moreover, $\overline{B}_{i \bmod p^k}$ is equidistributed $\bmod p^{k+1}$ for every i.

Proof. Denote by T the set whose mask polynomial is $\Phi_{p^{m-k}}(X^{q^n})$ so that

$$T = \left\{0, p^{m-k-1}q^n, 2p^{m-k-1}q^n, \ldots, (p-1)p^{m-k-1}q^n\right\}.$$

Since $B_{i \bmod p^k}$ is absorbed $\bmod p^{k+1}$ for every i, we have $B(\zeta_{p^{k+1}}) \neq 0$. Therefore, by Theorem 3.3(i), we get

$$(A - A) \cap \frac{N}{p^{k+1}}\mathbb{Z}_N^{\star} = \varnothing.$$

Moreover,

$$T - T = \left\{\ell p^{m-k-1}q^n : |\ell| < p\right\} \subseteq \{0\} \cup \frac{N}{p^{k+1}}\mathbb{Z}_N^{\star};$$

therefore, $(A - A) \cap (T - T) = \{0\}$. Hence, every element in $A + T$ has a unique representation as $a + t$ with $a \in A$, $t \in T$ (proof is similar to that of Theorem 3.3(ii)). This shows that $\overline{A}(X)$ is a mask polynomial of the set $\overline{A} = A \oplus T$. Furthermore, since each $B_{i \bmod p^k}$ is absorbed $\bmod p^{k+1}$, if $p^k \mid b - b'$ for some $b, b' \in B$, then $p^{k+1} \mid b - b'$ (definition of absorption). In other words,

$$(B - B) \cap (p^k \mathbb{Z}_N^{\star} \cup p^k q\mathbb{Z}_N^{\star} \cup \cdots \cup p^k q^n\mathbb{Z}_N^{\star}) = \varnothing. \tag{9.1}$$

The set

$$S = \{0, p^k q^n, 2p^k q^n, \ldots, (p-1)p^k q^n\} \tag{9.2}$$

has mask polynomial $\Phi_{p^{k+1}}(X^{q^n})$ and satisfies

$$S - S = \{\ell p^k q^n : |\ell| < p\} \subseteq \{0\} \cup p^k q^n \mathbb{Z}_N^\star; \tag{9.3}$$

therefore, $(B - B) \cap (S - S) = \{0\}$ and, similarly as before, we deduce that $\overline{B}(X)$ is the mask polynomial of the set $\overline{B} = B \oplus S$. We observe that $|\overline{A}| = |\overline{B}|$.

Next, we will show that $\overline{A}(\zeta_{\mathrm{ord}(\beta - \beta')}) = 0$ for every $\beta, \beta' \in \overline{B}$, $\beta \neq \beta'$. Every $\beta \in \overline{B}$ has a unique representation as $b + s$, where $b \in B$ and $s \in S$; we write also $\beta' = b' + s'$, $b' \in B$, $s' \in S$. By equation (9.3), $s - s' \in \{0\} \cup p^k q^n \mathbb{Z}_N^\star$, while $v_p(b - b') \neq k$ by (9.1). If $s = s'$, then $\beta - \beta' = b - b'$ and

$$\overline{A}(\zeta_{\mathrm{ord}(b-b')}) = A(\zeta_{\mathrm{ord}(b-b')}) \Phi_{p^{m-k}}(\zeta_{\mathrm{ord}(b-b')}^{q^n}) = 0$$

by Corollary 3.4 since B is a spectrum of A. So, assume $s \neq s'$ so that $s - s' \in p^k q^n \mathbb{Z}_N^\star$. Since $v_p(b - b') \neq k$, we will either have $p^{k+1} \mid b - b'$ or $p^k \nmid b - b'$. In the former case, $v_p(\beta - \beta') = k$, yielding $\mathrm{ord}(\beta - \beta') = p^{m-k} q^r$, where $0 \leq r \leq n$. Hence,

$$\overline{A}(\zeta_{\mathrm{ord}(\beta - \beta')}) = A(\zeta_{\mathrm{ord}(\beta - \beta')}) \Phi_{p^{m-k}}(\zeta_{p^{m-k}q^r}^{q^n}) = A(\zeta_{\mathrm{ord}(\beta - \beta')}) \Phi_{p^{m-k}}(\zeta_{p^{m-k}}^{q^{n-r}}) = 0.$$

In the latter case, $\mathrm{ord}(s - s') = p^{m-k} \mid \mathrm{ord}(b - b')$; therefore, $\mathrm{ord}(b - b') = \mathrm{ord}(b - b' + s - s') = \mathrm{ord}(\beta - \beta')$. Hence, again, Corollary 3.4 gives $\overline{A}(\zeta_{\mathrm{ord}(\beta - \beta')}) = 0$. One more application of Corollary 3.4 gives the desired conclusion as $\overline{A}(\zeta_{\mathrm{ord}(\beta - \beta')}) = 0$ for every $\beta, \beta' \in \overline{B}$, $\beta \neq \beta'$. The second part of the lemma follows from the fact that $\overline{B}(\zeta_{p^{k+1}}) = 0$. $\qquad \square$

Corollary 9.4. *Let (A, B) be a spectral pair in $\mathbb{Z}_N$, $N = p^m q^n$. Let $K_p(B) \subseteq [0, m-1]$ be the set of all k such that $B_{i \bmod p^k}$ is absorbed $\bmod\, p^{k+1}$ for all i. Then*

$$\overline{A}(X) \equiv A(X) \prod_{k \in K_p(B)} \Phi_{p^{m-k}}(X^{q^n}) \bmod (X^N - 1)$$

is the mask polynomial of a spectral set whose spectrum has the following mask polynomial:

$$\overline{B}(X) \equiv B(X) \prod_{k \in K_p(B)} \Phi_{p^{k+1}}(X^{q^n}) \bmod (X^N - 1).$$

Moreover, for every k with $p^{k+1} \mid N$, there is i such that $\overline{B}_{i \bmod p^k}$ is not absorbed $\bmod\, p^{k+1}$ (i.e., the set $K_p(\overline{B})$ is empty).

Proof. Induction on $|K_p(B)|$; the case $|K_p(B)| = 1$ is Lemma 9.3, and the proof for the induction step is almost identical. For the second part, we proceed by contradiction; suppose that $K_p(\overline{B}) \neq \varnothing$. By the second part of Lemma 9.3, we definitely have $K_p(B) \cap K_p(\overline{B}) = \varnothing$ as, for every $k \in K_p(B)$, it holds $\overline{B}(\zeta_{p^{k+1}}) = 0$; hence, each $\overline{B}_{i \bmod p^k}$ is equidistributed $\bmod\, p^{k+1}$ (and not absorbed). Consider next some arbitrary $\ell \notin K_p(B)$, $0 \leq \ell \leq m$. By definition, there is i such that $B_{i \bmod p^\ell}$ is not absorbed $\bmod\, p^{\ell+1}$. Then, as $B \subseteq \overline{B}$, it is obvious that $\overline{B}_{i \bmod p^k}$ is not absorbed $\bmod\, p^{k+1}$. $\qquad \square$

Definition 9.5. We call a set $A \subseteq \mathbb{Z}_N$ *absorption-free at p^k* if, for a prime p and $k \in \mathbb{N}$ with $p^{k+1} \mid N$, there is a class $A_{i \bmod p^k}$ that is not absorbed $\bmod\, p^{k+1}$ (i.e., $k \notin K_p(A)$). We call A *absorption-free* if it is absorption-free at every prime power p^k such that $p^{k+1} \mid N$ (i.e., $K_p(A) = \varnothing$ for every prime $p \mid N$).

Lemma 9.6. *Let (A, B) be a spectral pair in $\mathbb{Z}_N$, $N = p^m q^n$. Then, there are $S, T \subseteq \mathbb{Z}_N$ such that $(A \oplus S, B \oplus T)$ is a spectral pair in $\mathbb{Z}_N$, with the additional property that $A \oplus S$ and $B \oplus T$ are absorption-free.*

Proof. If both A and B are absorption-free, there is nothing to prove as we can just take $S = T = \{0\}$. So, suppose first that B is not absorption-free. The process described in Lemma 9.3 and subsequently in Corollary 9.4 'kills' all absorption in the following sense: If $B_{i \bmod p^k}$ is absorbed $\bmod p^{k+1}$ for all i, then $\overline{B}_{i \bmod p^k}$ is equidistributed $\bmod p^{k+1}$ for all i since $\overline{B}(\zeta_{p^{k+1}}) = 0$, and thus, $\overline{B}$ is absorption-free at p^k. Moreover, for every $k \in [0, m-1]$, there is i such that $\overline{B}_{i \bmod p^k}$ is not absorbed $\bmod p^{k+1}$. With the goal to eliminate all absorption from A and B, we successively multiply $B(X)$ by polynomials of the form $\Phi_{p^{k+1}}(X^{q^n})$ or $\Phi_{q^{\ell+1}}(X^{p^m})$, whose product is a mask polynomial of a set S, and, respectively, $A(X)$ by polynomials of the form $\Phi_{p^{m-k}}(X^{q^n})$ or $\Phi_{q^{n-\ell}}(X^{p^m})$, whose product is a mask polynomial of a set T. We thus obtain a pair of absorption-free sets $(A \oplus S, B \oplus T)$, which is also spectral, by virtue of Lemma 9.3 or Corollary 9.4. □

Corollary 9.7. *Suppose that every absorption-free spectral subset of $\mathbb{Z}_N$ tiles $\mathbb{Z}_N$. Then, every spectral subset of $\mathbb{Z}_N$ tiles $\mathbb{Z}_N$.*

Proof. Let (A, B) be a spectral pair in $\mathbb{Z}_N$. If A is absorption-free, then it tiles $\mathbb{Z}_N$ by hypothesis. If not, there are $S, T \subseteq \mathbb{Z}_N$ by Lemma 9.6 such that $(A \oplus T, B \oplus S)$ is an absorption-free spectral pair. By hypothesis, this shows the existence of $R \subseteq \mathbb{Z}_N$ such that $(A \oplus T) \oplus R = \mathbb{Z}_N$ or, alternatively, $A \oplus (T \oplus R) = \mathbb{Z}_N$, that is, A tiles $\mathbb{Z}_N$. □

All the above motivate the following definition.

Definition 9.8. Let $N \in \mathbb{N}$. Define the following subset of $\mathscr{F}(N)$

$$\mathscr{F}_{\max}(N) = \{A \subseteq \mathbb{Z}_N : A \in \mathscr{F}(N), \text{ and } A \text{ has maximal size}\}.$$

Lemma 9.6 and Corollary 9.7 imply that every $A \in \mathscr{F}_{\max}(N)$ is absorption-free, as well as every spectrum B of A. Hence, Corollary 9.7 implies

$$N \in \mathcal{S}_{p,q} \iff \mathscr{F}_{\max}(N) \neq \varnothing. \tag{9.4}$$

10. Symmetry of root patterns

We consider again $N \in \mathcal{S}'_{p,q}$, $A \in \mathscr{F}(N)$ and B a spectrum of A. We recall Propositions 8.2, 8.4 and Corollary 8.3, which imply that A and B are both primitive; they satisfy equations (8.1) and (8.2) such that the polynomials P, Q in (8.1) are nonzero. Therefore, A contains a coset from each of the subgroups $\frac{N}{p}\mathbb{Z}_N$ and $\frac{N}{q}\mathbb{Z}_N$, so using Theorem 3.3(i) we obtain

$$\frac{N}{p}\mathbb{Z}_N \cup \frac{N}{q}\mathbb{Z}_N \subseteq A - A \subseteq \{0\} \cup Z(B),$$

and then Corollary 3.4 gives

$$B(\zeta_p) = B(\zeta_q) = 0 \tag{10.1}$$

for any spectrum B of A. If in addition $A \in \mathscr{F}_{\max}(N)$ holds, then A and every spectrum B are absorption-free by Lemma 9.6.

Definition 10.1. For $A \subseteq \mathbb{Z}_N$, we define

$$S_A^N(p) := \{\log_p s : s \in S_A^N, p \mid s\} = \{x \in [1, m] : A(\zeta_{p^x}) = 0\},$$

and the definition of $S_A^N(q)$ is similar. Also, denote by $m_p(A)$ the maximal exponent $x \le m$ such that $A(\zeta_N^{p^x}) \ne 0$, and similarly define $m_q(A)$ to be the maximal exponent $y \le n$ such that $A(\zeta_N^{q^y}) \ne 0$. If such exponents do not exist, we put $m_p(A) = -1$, $m_q(A) = -1$, respectively. Lastly, define the following set

$$R_A^N(p) := \left\{ x \in [0, m] : A(\zeta_N^{p^x}) = 0 \right\}$$

and, similarly, $R_A^N(q)$. The sets thus defined will be called *root patterns* of A.

We remark that, if the sets below are nonempty, then

$$m_p(A) = \max\left([0, m] \setminus R_A^N(p)\right), \quad m_q(A) = \max\left([0, m] \setminus R_A^N(q)\right).$$

For $A \in \mathcal{F}(N)$, the above sets are always nonempty, i.e., $m_p(A), n_p(A) \ge 0$. This is a consequence of Ma's lemma for the cyclic case [22] (see also Lemma 1.5.1 [29], or Corollary 1.2.14 [25]), using the polynomial notation.

Lemma 10.2. *Suppose that $A(X) \in \mathbb{Z}[X]$, and let $\mathbb{Z}_N$ be a cyclic group such that $p^m \parallel N$ for p prime. If $A(\zeta_d) = 0$, for every $p^m \mid d \mid N$, then*

$$A(X) \equiv P(X)\Phi_p(X^{N/P}) \bmod (x^N - 1).$$

If the coefficients of A are nonnegative, then P can be taken with nonnegative coefficients as well. In particular, if $A \subseteq \mathbb{Z}_N$ satisfies $A(\zeta_d) = 0$ for every $p^m \mid d \mid N$, then A is a union of p-cycles.

Therefore, if $A \subseteq \mathbb{Z}_N$ satisfies $m_p(A) = -1$ (resp., $m_q(A) = -1$), then it is a union of q-cycles (resp., p-cycles), so if $N \in \mathcal{S}_{p,q}'$ and A are spectral, then A is also a tile by Proposition 8.4.

Lemma 10.3. *Let $N \in \mathcal{S}_{p,q}'$, $A \in \mathcal{F}(N)$ and B any spectrum of A. Then, we have the following relation between the root patterns of A and B:*

$$(S_B^N(p) - 1) \cap [0, m_p(A)] = R_A^N(p) \cap [0, m_p(A)] \tag{10.2}$$

$$(S_B^N(q) - 1) \cap [0, m_q(A)] = R_A^N(q) \cap [0, m_q(A)]. \tag{10.3}$$

Equations (10.2) and (10.3) are also equivalent to the statements

$$\text{If } x \le m_p(A), \text{ then it holds } A(\zeta_N^{p^x}) = 0 \iff B(\zeta_{p^{x+1}}) = 0 \tag{10.4}$$

$$\text{If } x \le m_q(A), \text{ then it holds } A(\zeta_N^{q^x}) = 0 \iff B(\zeta_{q^{x+1}}) = 0. \tag{10.5}$$

Proof. Since $A \in \mathcal{F}(N)$ and $N \in \mathcal{S}_{p,q}'$, we obtain that A cannot be expressed as a union of p- or q-cycles exclusively by virtue of Theorem 5.2, Corollary 8.3 and Proposition 8.4. Thus, $m_p(A), m_q(A) \ge 0$. Let $x < m_p(A)$ and $A(\zeta_N^{p^x}) = 0$. Then $p^x \cdot A$ is a union of p- and q-cycles, not exclusively of q-cycles by Theorem 5.2 (second part) because $A(\zeta_N^{p^{m_p(A)}}) \ne 0$. So, there are $a, a' \in A$ such that

$$p^x(a - a') \equiv \frac{N}{p} \bmod N$$

or, equivalently,

$$a - a' \equiv \frac{N}{p^{x+1}} \bmod \frac{N}{p^x},$$

which in turn implies $a - a' \in \frac{N}{p^{x+1}}\mathbb{Z}_N^\star$, whence $B(\zeta_{p^{x+1}}) = 0$ by Theorem 3.3. This proves one direction of equation (10.4).

Next, suppose that the reverse implication of equation (10.4) does not hold, and let y be the smallest exponent such that $A(\zeta_N^{p^y}) \neq 0 = B(\zeta_{p^{y+1}})$. For every $x \leq y$ and every i, we have the obvious partition

$$B_{i \bmod p^x} = \bigcup_{k=1}^{p} B_{i+kp^x \bmod p^{x+1}}.$$

If $A(\zeta_N^{p^x}) = 0$ so that $B(\zeta_{p^{x+1}}) = 0$, the above partition is an equidistribution $\bmod\, p^{x+1}$, that is,

$$|B_{i \bmod p^x}| = p|B_{i+kp^x \bmod p^{x+1}}|$$

for every k. If $A(\zeta_N^{p^x}) \neq 0 \neq B(\zeta_{p^{x+1}})$, we certainly do not have equidistribution for at least one choice of j; if we do not have absorption $\bmod\, p^{x+1}$, i.e., $B_{i \bmod p^x} = B_{i+kp^x \bmod p^{x+1}}$, then there are k, k' with $k \not\equiv k' \bmod p$ such that $B_{i+kp^x \bmod p^{x+1}}$ and $B_{i+k'p^x \bmod p^{x+1}}$ are nonempty. Let

$$b \in B_{i+kp^x \bmod p^{x+1}}, b' \in B_{i+k'p^x \bmod p^{x+1}}$$

be arbitrary. It holds $p^x \parallel b - b'$ by assumption, and $b - b' \notin p^x \mathbb{Z}_N^{\star}$ due to $A(\zeta_N^{p^x}) \neq 0$. This shows $q \mid b - b'$; therefore, all elements of $B_{i+kp^x \bmod p^{x+1}}$ and $B_{i+k'p^x \bmod p^{x+1}}$ have the same residue $\bmod\, q$. The same holds for all other elements of $B_{i \bmod p^x}$, establishing

$$B_{i \bmod p^x} \subseteq B_{j \bmod q}$$

for some j. Now, for each $i \in [0, p^y - 1]$, define $x(i)$ to be the smallest exponent x such that $B_{i \bmod p^x}$ is neither absorbed nor equidistributed $\bmod\, p^{x+1}$, and then define $j(i)$ such that

$$B_{i \bmod p^{x(i)}} \subseteq B_{j(i) \bmod q}. \tag{10.6}$$

If for every $x \leq y$, $B_{i \bmod p^x}$ is either absorbed or equidistributed $\bmod\, p^{x+1}$, define $x(i) = y$; since $B_{i \bmod p^y}$ is equidistributed $\bmod\, p^{y+1}$ and $A(\zeta_N^{p^y}) \neq 0$, we conclude that there is again some $j(i)$ such that equation (10.6) still holds. On $[0, p^y - 1]$, we define an equivalence relation: It holds $i \sim i'$ if and only if $i \equiv i' \bmod p^{x(i)}$ (it is not hard to show that this satisfies the properties of an equivalence relation as $i \equiv i' \bmod p^{x(i)}$ implies $x(i) = x(i')$). Let $I \subseteq [0, p^y - 1]$ be a complete system of representatives; it holds

$$B = \bigsqcup_{i \in I} B_{i \bmod p^{x(i)}}.$$

The important fact about the above partition is that each $B_{i \bmod p^{x(i)}}$ has cardinality $\frac{|B|}{p^{k(i)}}$ for some positive integer $k(i)$. Indeed, as for every $x < x(i)$, we have either $|B_{i \bmod p^x}| = |B_{i \bmod p^{x+1}}|$ (absorption) or $|B_{i \bmod p^x}| = p|B_{i \bmod p^{x+1}}|$ (equidistribution). Then, by equation (10.6), we have

$$B_{0 \bmod q} = \bigsqcup_{i \in I, j(i)=0} B_{i \bmod p^{x(i)}},$$

and taking cardinalities on both sides, we obtain

$$\frac{|B|}{q} = \sum_{i \in I, j(i)=0} \frac{|B|}{p^{k(i)}},$$

which then leads to an equation of the form $1/q = s/p^t$, which has no solutions in integers, contradicting the fact that $A(\zeta_N^{p^y}) \neq 0 = B(\zeta_{p^{y+1}})$. This completes the proof. $\qquad\square$

Proposition 10.4. *Let $N \in \mathcal{S}'_{p,q}$, $A \in \mathcal{F}(N)$ and B be any spectrum of A. Then*

$$A(\zeta_{q^n}) = A(\zeta_{p^m}) = 0$$

and

$$B(\zeta_{p^{m_p(A)+1}q}) = B(\zeta_{pq^{m_q(A)+1}}) = 0.$$

Proof. We will show first that $A(\zeta_{q^n}) = A(\zeta_{p^m}) = 0$. Suppose that it doesn't hold, say $A(\zeta_{q^n}) \neq 0$, so that $m_p(A) = m$. By equation (10.2), we get

$$S_B^N(p) - 1 = R_A^N(p).$$

Using the same argument as in the proof of Lemma 10.3, replacing y by m, we get

$$B = \bigsqcup_{i \in I} B_{i \bmod p^{x(i)}},$$

where each $B_{i \bmod p^{x(i)}}$ has cardinality $\frac{|B|}{p^{k(i)}}$ and is contained in $B_{j(i) \bmod q}$; this is also true if $x(i) = m$ as $A(\zeta_N^{p^m}) \neq 0$. We establish a contradiction in the same way.

This shows $m_p(A) < m$ and $m_q(A) < n$. Since $B(\zeta_{p^{m_p(A)+1}}) \neq 0$ by (10.4), the polynomial

$$\overline{A}(X) \equiv A(X)\Phi_p(X^{p^{m-m_p(A)-1}q^n}) \bmod (X^N - 1)$$

is the mask polynomial of a set, say $\overline{A}$; this follows from the fact that $(A - A) \cap \frac{N}{p^{m_p(A)+1}}\mathbb{Z}_N^\star = \emptyset$, which implies that $A - A$ and the difference set whose mask polynomial is $\Phi_p(X^{p^{m-m_p(A)-1}q^n})$ intersect trivially. Consider now the multiset $p^{m_p(A)} \cdot A$. By definition, its mask polynomial does not vanish on ζ_N, while on the other hand, $p^{m_p(A)+1} \cdot A$ is a disjoint union of q-cycles by Lemma 10.2. By Lemma 5.6 and Theorem 3.3(i), we obtain $B(\zeta_{p^{m_p(A)+1}q}) = 0$ and, similarly, $B(\zeta_{pq^{m_q(A)+1}}) = 0$, as desired.   □

Using the above notation, condition (T1) can be rewritten as

$$|A| = p^{|S_A^N(p)|}q^{|S_A^N(q)|}.$$

At any rate, regardless whether A is spectral or not, it holds

$$p^{|S_A^N(p)|}q^{|S_A^N(q)|} \mid |A|.$$

We restrict now to $A \in \mathcal{F}_{\max}(N)$, $N \in \mathcal{S}'_{p,q}$ due to equation (9.4). In this case, we will show that (T1) fails for B when the multiset $\frac{N}{p^{m_p(A)+1}q} \cdot B$ is not a union of q-cycles only; in particular, the power of p is higher than it is supposed to be.

Lemma 10.5. *Let $N \in \mathcal{S}'_{p,q}$, $A \in \mathcal{F}_{\max}(N)$, and B any spectrum of A so that $m_p(A), m_q(A) \geq 0$. Consider the set*

$$U_B^N(p) = \{x : B(\zeta_{p^x}) \neq 0 = B(\zeta_{p^x q})\}.$$

Then

$$p^{|S_B^N(p)|+|U_B^N(p)|} \mid |B|.$$

Moreover, for every j, every $x \in [1, m_p(A) + 1] \setminus S_B^N(p)$ and every $y \in [1, m_q(A) + 1] \setminus S_B^N(q)$, each of the sets

$$\left(\frac{N}{p^x q}B\right)_{j \bmod \frac{N}{pq}} = \frac{N}{p^x q}B \cap \left(j + \frac{N}{pq}\mathbb{Z}_N\right), \quad \left(\frac{N}{pq^y}B\right)_{j \bmod \frac{N}{pq}} = \frac{N}{pq^y}B \cap \left(j + \frac{N}{pq}\mathbb{Z}_N\right),$$

is supported either on a p- or a q-cycle.

Proof. We first note, that $x = m_p(A) + 1$ satisfies $B(\zeta_{p^x}) \neq 0 = B(\zeta_{p^x q})$ by Lemma 10.3 and Proposition 10.4, therefore $U_B^N(p) \neq \varnothing$. By (10.1), we have $B(\zeta_p) = 0$ or, equivalently, $|B_{i \bmod p}| = \frac{1}{p}|B|$ for all i. At every step, we will estimate

$$\min \left\{i : v_p(|B_{i \bmod p^x}|)\right\}$$

or, in other words, how much the power of p drops from $|B|$ down to one of the subsets $|B_{i \bmod p^x}|$. If $x \in S_B^N(p)$, then each $B_{i \bmod p^{x-1}}$ is equidistributed $\bmod p^x$, therefore

$$v_p(|B_{i \bmod p^{x-1}}|) - 1 = v_p(|B_{i \bmod p^x}|),$$

for all i. If $x \notin S_B^N(p)$, we have in general

$$v_p(|B_{i \bmod p^{x-1}}|) \geq \min \left\{v_p(|B_{i+kp^{x-1} \bmod p^x}|) : 0 \leq k \leq p - 1\right\}.$$

Next, consider the minimum element of $U_B^N(p)$, say x, and suppose that $B_{i \bmod p^{x-1}}$ is not absorbed $\bmod p^x$; such an i exists due to hypothesis and equation (9.4) since B is absorption-free. Each nonempty class $B_{i+kp^{x-1} \bmod p^x}$ would then be absorbed $\bmod p^x q$. Otherwise, $\frac{N}{p^x q}B \cap (j + \frac{N}{pq}\mathbb{Z}_N)$ would neither be supported on a p-cycle nor on a q-cycle for some j. For the same reason, each element in $B_{i+kp^{x-1} \bmod p^x}$ must have the same residue $\bmod q$ for all k, showing that $B_{i \bmod p^{x-1}}$ is absorbed $\bmod p^{x-1}q$; furthermore, since $B(\zeta_{p^x q}) = 0$, $B_{i \bmod p^{x-1}}$ and $B_{i \bmod p^{x-1}q}$ are equidistributed $\bmod p^x$ and $\bmod p^x q$, respectively. Therefore,

$$v_p(|B_{i \bmod p^{x-1}}|) - 1 = v_p(|B_{i \bmod p^x}|).$$

Next, let x be the minimum element not belonging to $S_B^N(p)$, that is,

$$B(\zeta_p) = \cdots = B(\zeta_{p^{x-1}}) = 0 \neq B(\zeta_{p^x}).$$

Suppose that $B_{i \bmod p^{x-1}}$ is not absorbed $\bmod p^x$; such an i exists due to hypothesis and equation (9.4). Let then $B_{i+kp^{x-1} \bmod p^x}$ and $B_{i+k'p^{x-1} \bmod p^x}$ be nonempty with $p \nmid k - k'$. If there are $b \in B_{i+kp^{x-1} \bmod p^x}$ and $b' \in B_{i+k'p^{x-1} \bmod p^x}$ with $q \nmid b - b'$, then $b - b' \in p^{x-1}\mathbb{Z}_N^\star$, yielding $A(\zeta_N^{p^{x-1}}) = 0$ by Theorem 3.3(i), and then $B(\zeta_{p^x}) = 0$ by Lemma 10.3, contradicting the definition of x. Thus, we must have $q \mid b - b'$ for every such selection of b, b', implying eventually that every element of $B_{i \bmod p^{x-1}}$ has the same residue $\bmod q$.

For every $y \geq x$, we choose an integer $i_y \equiv i \bmod p^{x-1}$ as follows (we denote $i_j = i$ for $1 \leq j \leq x-1$):

○ If $y \notin S_B^N(p) \cup U_B^N(p)$, choose i_y satisfying

$$v_p(|B_{i_{y-1} \bmod p^{y-1}}|) \geq v_p(|B_{i_y \bmod p^y}|).$$

○ If $y \in S_B^N(p) \cup U_B^N(p)$, then $i_y = i_{y-1}$.

We have $|B_{i \bmod p^{x-1}}| = \frac{1}{p^{x-1}}|B|$. If $y \in S_B^N(p)$, then $B_{i_{y-1} \bmod p^{y-1}}$ is equidistributed $\bmod\, p^y$, so

$$|B_{i_y \bmod p^y}| = \frac{1}{p}|B_{i_{y-1} \bmod p^{y-1}}|. \tag{10.7}$$

If $y \in U_B^N(p)$, we have $B(\zeta_{p^y q}) = 0$. Therefore, the multiset $\frac{N}{p^y q} \cdot B$ is a disjoint union of p- and q-cycles by Theorem 5.2. Every such cycle consists of elements $p^y q b$ for $b \in B$ that have the same residue $\bmod\, p^{y-1}$; indeed, if $\frac{N}{p^y q}(b - b') \in \frac{N}{p}\mathbb{Z}_N$, then $b - b' \equiv k p^{y-1} q \bmod p^y q$ for some k, and if $\frac{N}{p^y q}(b - b') \in \frac{N}{q}\mathbb{Z}_N$, then $b - b' \equiv k p^y \bmod p^y q$ for some k, proving our claim. This shows that $\frac{N}{p^y q} \cdot B_{i_{y-1} \bmod p^{y-1}}$ is a disjoint union of p- and q-cycles; however, a q-cycle in $\frac{N}{p^y q} \cdot B_{i_{y-1} \bmod p^{y-1}} \subseteq \frac{N}{p^y q} B$ consists of elements having all possible residues $\bmod\, q$, a contradiction, since every element of $B_{i \bmod p^{x-1}}$ has the same residue $\bmod\, q$. This shows that $\frac{N}{p^y q} \cdot B_{i_{y-1} \bmod p^{y-1}}$ is a union of p-cycles, yielding the equidistribution of $B_{i_{y-1} \bmod p^{y-1}}$ modulo p^y. Thus, (10.7) holds in this case as well.

Summarizing, we obtain the following: If $y \in S_B^N(p) \cup U_B^N(p)$, then (10.7) is valid; otherwise,

$$v_p(|B_{i_{y-1} \bmod p^{y-1}}|) \geq v_p(|B_{i_y \bmod p^y}|)$$

holds. This obviously yields that

$$0 \leq v_p(|B_{i_m \bmod p^m}|) \leq v_p(|B|) - |S_B^N(p)| - |U_B^N(p)|,$$

proving the first part.

For the second part of the lemma, we proceed by contradiction. If there is some j and $x \in U_B^N(p)$ with $x \leq m_p(A) + 1$ such that $\frac{N}{p^x q} B \cap (j + \frac{N}{pq}\mathbb{Z}_N)$ is supported neither on a p- nor on a q-cycle, then by Proposition 5.5 we get that

$$\left(\frac{N}{p^x q}B - \frac{N}{p^x q}B\right) \cap \frac{N}{pq}\mathbb{Z}_N^\star \neq \emptyset.$$

This shows the existence of $b, b' \in B$ such that

$$\frac{N}{p^x q}(b - b') \in \frac{N}{pq}\mathbb{Z}_N^\star$$

or, equivalently,

$$\mathrm{ord}(b - b') = pq\frac{N}{p^x q} = \frac{N}{p^{x-1}}.$$

Hence, by Theorem 3.3(i), we obtain

$$A(\zeta_{N/p^{x-1}}) = A(\zeta_N^{p^{x-1}}) = 0,$$

contradicting the definition of x. This completes the proof. $\qquad\qquad\square$

Definition 10.6. Let $A \subseteq \mathbb{Z}_N$. We define

(wT1) $p^{|S_A^N(p)|} \,\|\, |A|$, for some $p \mid |A|$.

Obviously, when (T1) holds for A, then **(wT1)** holds for *every* $p \mid A$. An immediate consequence of this definition and Lemma 10.5 is the following.

Corollary 10.7. *Let* $N \in \mathscr{S}'_{p,q}$, $A \in \mathscr{F}_{\max}(N)$. *Then, no spectrum B of A satisfies* **(wT1)**. *In particular, every spectrum B of A satisfies* $B \in \mathscr{F}_{\max}(N)$.

Proof. This is obvious by Lemma 10.5 since the sets $U_B^N(p)$ and $U_B^N(q)$ are nonempty.   □

Corollary 10.8. *Let* $N \in \mathcal{S}'_{p,q}$, $A \in \mathcal{F}_{\max}(N)$. *Then no spectrum B of A is a disjoint union either of p- or q-cycles exclusively.*

Proof. If B was a union of (say) p-cycles only, then by Proposition 8.4, B satisfies (T1) and (T2). On the other hand, Corollary 10.7 gives us that **(wT1)** fails for B, a contradiction, as (T1) implies **(wT1)**.   □

This corollary complements Proposition 8.4. We summarize below all the reductions made so far:

Theorem 10.9. *Let* $N \in \mathcal{S}'_{p,q}$, $A \in \mathcal{F}_{\max}(N)$. *Then the following hold:*

1. *A and any spectrum B are primitive.*
2. *A, as well as any spectrum B, can be expressed as disjoint unions of p- and q-cycles; not exclusively of p- or q-cycles (i.e., none of the polynomials P, Q, R, S in both equation (8.1) and equation (8.2) can be identically zero).*
3. *If $N = p^m q^n$, it holds*

$$A(\zeta_N) = A(\zeta_p) = A(\zeta_q) = A(\zeta_{p^m}) = A(\zeta_{q^n}) =$$
$$= B(\zeta_N) = B(\zeta_p) = B(\zeta_q) = B(\zeta_{p^m}) = B(\zeta_{q^n}) = 0 \tag{10.8}$$

   for any spectrum B of A. This also implies that both A and B are equidistributed both $\mathrm{mod}\, p$ and $\mathrm{mod}\, q$.
4. *A as well as any spectrum B are absorption-free.*
5. *Every spectrum B of A satisfies $B \in \mathcal{F}_{\max}(N)$.*

We have established enough tools to extend the results of [13] related to Fuglede's conjecture.

Corollary 10.10. *Let* $N = p^m q^n$, $n \leq 3$ *and* (A, B) *be a spectral pair in* $\mathbb{Z}_N$. *Then A tiles* $\mathbb{Z}_N$.

Proof. Suppose on the contrary that there is such an N with $\mathcal{F}(N) \neq \varnothing$, $A \in \mathcal{F}_{\max}(N)$ and B a spectrum. Corollary 6.3 implies that $n \geq 2$. By Theorem 10.9, we obtain $A(\zeta_q) = A(\zeta_{q^n}) = 0$, so if $n = 2$ we have $q^n \mid |A|$, and so by Proposition 6.2 we get that A tiles, contradiction. If $n = 3$, we have $B(\zeta_q) = B(\zeta_{q^3}) = 0$ again by Theorem 10.9 so that $|S_B^N(q)| \geq 2$. Since $U_B^N(q)$ is nonempty, by Lemma 10.5 we obtain $q^3 \mid |B|$, and then Proposition 6.2 gives us again that A tiles $\mathbb{Z}_N$, a contradiction. Thus, $\mathcal{S}_{p,q}$ cannot have elements of the form $p^m q^n$ with $n \leq 3$, proving the desired result.   □

Proposition 10.11. *Let* $N = p^m q^n \in \mathcal{S}'_{p,q}$, $A \in \mathcal{F}_{\max}(N)$ *and B any spectrum of A. Then*

$$A(\zeta_{p^m q}) = A(\zeta_{p q^n}) = B(\zeta_{p^m q}) = B(\zeta_{p q^n}) = A(\zeta_{pq}) = B(\zeta_{pq}) = 0.$$

Proof. By Theorem 10.9, we also have $B \in \mathcal{F}_{\max}(N)$, so we may use Lemma 10.3 with the roles of A and B reversed. If $A(\zeta_{p q^n}) = A(\zeta_N^{p^{m-1}}) \neq 0 = A(\zeta_N^{p^m}) = A(\zeta_{q^n})$, we would have $m_p(A) = m - 1$, so by virtue of Lemma 10.3 we would have $B(\zeta_{p^m}) \neq 0$, contradicting equations 10.2. Reversing the roles of p, q, and A, B, we obtain with the same reasoning

$$A(\zeta_{p^m q}) = A(\zeta_{p q^n}) = B(\zeta_{p^m q}) = B(\zeta_{p q^n}) = 0.$$

Next, consider the minimal element of $U_B^N(p)$, say x so that $B(\zeta_{p^x}) \neq 0 = B(\zeta_{p^x q})$. By Proposition 10.4, we have $x \leq m_p(A) + 1$; hence, by Lemma 10.3 we get $A(\zeta_N^{p^{x-1}}) \neq 0$. Applying Lemma 9.2 for $d = p^{x-1}$, we get that each $B_{i \bmod p^{x-1}}$ is either absorbed or equidistributed $\mathrm{mod}\, p^x$. Since $B(\zeta_{p^x}) \neq 0$, there is some i such that $B_{i \bmod p^{x-1}}$ is absorbed $\mathrm{mod}\, p^x$; without loss of generality we put $B_{i \bmod p^{x-1}} = B_{i \bmod p^x}$. This also shows that $B_{i \bmod p^x q}$ is supported on a q-cycle. In fact, $B_{i \bmod p^x}$ must

be equidistributed mod $p^x q$, hence

$$|B_{i+kp^x \bmod p^x q}| = \frac{1}{q}|B_{i \bmod p^x}|, \quad 0 \le k \le q - 1. \tag{10.9}$$

For $y \le x - 1$, we then claim the following: $B_{i \bmod p^y}$ is either absorbed or equidistributed mod p^{y+1}. Indeed, if $y + 1 \in S_B^N(p)$, then $B(\zeta_{p^{y+1}}) = 0$ and $B_{i \bmod p^y}$ is equidistributed mod p^{y+1}. If $B(\zeta_{p^{y+1}}) \ne 0$, then $A(\zeta_N^{p^y}) \ne 0$ by Lemma 10.3. If $B_{i \bmod p^y}$ is not absorbed mod p^{y+1}, then there are $k \not\equiv k' \bmod p$ such that

$$B_{i+kp^y \bmod p^{y+1}} \ne \emptyset, B_{i+k'p^y \bmod p^{y+1}} \ne \emptyset.$$

This means that the multiset $\frac{N}{p^{y+1}q} \cdot B_{i \bmod p^y}$ (which is supported in a pq-cycle) intersects nontrivially at least two q-cycles, namely

$$\frac{iN}{p^{y+1}q} + k\frac{N}{pq} + \frac{N}{q}\mathbb{Z}_N, \quad \frac{iN}{p^{y+1}q} + k'\frac{N}{pq} + \frac{N}{q}\mathbb{Z}_N.$$

By the second part of Lemma 10.5, $\frac{N}{p^{y+1}q} \cdot B_{i \bmod p^y}$ must be supported on a p-cycle, in particular,

$$\frac{iN}{p^{y+1}q} + \ell\frac{N}{q} + \frac{N}{p}\mathbb{Z}_N,$$

for some ℓ. But the latter implies that $B_{i \bmod p^y}$ is absorbed mod $p^y q$:

$$B_{i \bmod p^y} = B_{i+\ell'p^y \bmod p^y q},$$

where

$$\ell' \equiv p\ell \bmod q.$$

But this leads to a contradiction since (10.9) implies that $B_{i+kp^x \bmod p^x q} \ne \emptyset$ for every k, while

$$B_{i+kp^x \bmod p^x q} \subseteq B_{i+(kp^{x-y})p^y \bmod p^y q} = \emptyset$$

when $kp^{x-y} \not\equiv \ell' \bmod q$, contradiction.

Therefore, if $B_{i \bmod p^{x-1}}$ is absorbed mod p^x, then $B_{i \bmod p^y}$ is either absorbed of equidistributed mod p^{y+1} for every $y < x$; this implies

$$|B_{i+kp^x \bmod p^x q}| = \frac{1}{q}|B_{i \bmod p^x}| = \frac{|B|}{p^t q}$$

for some $t \in \mathbb{N}$. With the same arguments as above, if $B_{i \bmod p^{x-1}}$ is equidistributed mod p^x, we deduce that if $y \le x - 1$ is the smallest exponent such that $B_{i \bmod p^y}$ is neither absorbed nor equidistributed mod p^{y+1} (assuming there exists one), then $B_{i \bmod p^y}$ is absorbed mod $p^y q$, which means that every element in $B_{i \bmod p^y}$ has the same residue mod q, again by the second part of Lemma 10.5. In this case, there is some k such that

$$|B_{i+kp^y \bmod p^y q}| = |B_{i \bmod p^y}| = \frac{|B|}{p^s}$$

for some $s \in \mathbb{N}$. We write

$$B_{i \bmod pq} = \bigsqcup_{k=1}^{p^{x-1}} B_{i+kpq \bmod p^x q},$$

and we define $y(k) \leq x - 1$ to be the smallest exponent such that $B_{i+kpq \bmod p^{y(k)}}$ is neither absorbed nor equidistributed $\bmod p^{y(k)+1}$; if such an exponent does not exist, define $y(k) = x - 1$. We define the relation $k \sim k'$ to denote $y(k) = y(k')$ and $k \equiv k' \bmod p^{y(k)-1}$. It is not hard to see that this is an equivalence relation and

$$B_{i \bmod pq} = \bigsqcup_{k \in K} B_{i+kpq \bmod p^{y(k)-1} q}.$$

As we have seen, though, the cardinality of each set in the union above is divisible by $\frac{|B|}{p^r q}$ for some $r \in \mathbb{N}$. Reversing the roles of p and q, we obtain that

$$\frac{|B|}{pq} \mid |B_{i \bmod pq}| \tag{10.10}$$

for every i. If B were not equidistributed $\bmod pq$, there would exist some i such that

$$|B_{i \bmod pq}| \geq \frac{2|B|}{pq}.$$

By equation (10.10) and the trivial partition

$$B_{i \bmod q} = \bigsqcup_{j=1}^{p} B_{i+jq \bmod pq},$$

we obtain the existence of a j such that $B_{i+jq \bmod pq} = \varnothing$. Similarly, there is some ℓ such that $B_{i+\ell p \bmod pq} = \varnothing$. If $B_{i+kpq \bmod p^{x-1}}$ is absorbed $\bmod p^x$, then it is equidistributed $\bmod p^{x-1}q$, as we've shown above. But then, $B_{i+kpq+up^{x-1} \bmod p^{x-1}q}$ is nonempty for every u, however,

$$B_{i+kpq+up^{x-1} \bmod p^{x-1}q} \subseteq B_{i+\ell p \bmod pq} = \varnothing$$

for $up^{x-1} \equiv \ell p \bmod pq$, contradiction. This shows that $B_{i+kpq \bmod p^{x-1}}$ is equidistributed $\bmod p^x$ for every k, showing that $\frac{|B|}{p^t}$ divides $|B_{i \bmod pq}|$. Similarly, we obtain that $\frac{|B|}{q^s}$ divides $|B_{i \bmod pq}|$, showing thus $|B| \mid |B_{i \bmod pq}|$, contradiction. Thus, B is equidistributed $\bmod pq$, and the same holds for A by reversing the roles of A and B. This eventually shows

$$A(\zeta_{pq}) = B(\zeta_{pq}) = 0,$$

as desired. □

Remark. The above verifies property (T2) for the pairs of prime powers (p^m, q), (p, q^n) and (p, q).

11. Root deficit

We continue to assume that $N \in \mathscr{S}'_{p,q}$ and (A, B) is a spectral pair with $A \in \mathscr{F}_{\max}(N)$ so that $B \in \mathscr{F}_{\max}(N)$ as well.

Definition 11.1. Let $A \subseteq \mathbb{Z}_N$ satisfy $A(\zeta_q) = A(\zeta_p) = \cdots = A(\zeta_{p^k}) = 0 \neq A(\zeta_{p^{k+1}})$. We define the following property:

(wT2) It holds $A(\zeta_{pq}) = \cdots = A(\zeta_{p^k q}) = 0$.

It should be emphasized that, when **(wT2)** holds, then A is equidistributed mod $p^k q$ (and in particular, every $A_{j \bmod p^k}$ is equidistributed mod $p^k q$). Indeed, the hypothesis of the definition and **(wT2)** imply that $\Phi_d(X) \mid A(X)$ for every $d \mid p^k q$, $d \neq 1$. Therefore,

$$X^{p^k q - 1} + \cdots + 1 \mid A(X)$$

or, equivalently, $A(X) = G(X)(X^{p^k q - 1} + \cdots + 1)$ for some $G(X) \in \mathbb{Z}[X]$. When we reduce $\mathrm{mod}(X^{p^k q} - 1)$, we obtain

$$
\begin{aligned}
A(X) &\equiv G(X)(X^{p^k q - 1} + \cdots + 1) \bmod (X^{p^k q} - 1) \\
&\equiv G(1)(X^{p^k q - 1} + \cdots + 1) \bmod (X^{p^k q} - 1),
\end{aligned}
$$

which clearly shows that

$$|A_{j \bmod p^k}| = \frac{|A|}{p^k}, \quad |A_{j \bmod p^k q}| = \frac{|A|}{p^k q}, \quad \forall j. \tag{11.1}$$

Proposition 11.2. *Let* $N \in \mathcal{S}'_{p,q}$, $A \in \mathcal{F}_{\max}(N)$, *satisfying*

$$A(\zeta_q) = A(\zeta_p) = \cdots = A(\zeta_{p^k}) = 0 \neq A(\zeta_{p^{k+1}}).$$

Then there is some j such that $A_{j \bmod p^k}$ is absorbed $\mathrm{mod}\, p^k q$. In particular, (wT2) fails for A.

Proof. By definition, A is absorption-free; therefore, there is some j such that $A_{j \bmod p^k}$ is not absorbed $\mathrm{mod}\, p^{k+1}$. Hence,

$$A_{j \bmod p^k} = \bigcup_{i=1}^{r} A_{j + (\ell_i q) p^k \bmod p^{k+1}},$$

where $r \geq 2$, the ℓ_i are pairwise distinct mod p and all sets in the above union are nonempty. This shows that the multiset $\frac{N}{p^{k+1} q} \cdot A_{j \bmod p^k}$ has elements on r distinct q-cycles, namely

$$\frac{jN}{p^{k+1} q} + \ell_i \frac{N}{p} + \frac{N}{q} \mathbb{Z}_N, \quad 1 \leq i \leq r.$$

Consider two arbitrary elements from two different q-cycles (relabeling the ℓ_i if necessary), say

$$\frac{a_1 N}{p^{k+1} q} = \frac{jN}{p^{k+1} q} + \ell_1 \frac{N}{p} + m_1 \frac{N}{q} \quad \text{and} \quad \frac{a_2 N}{p^{k+1} q} = \frac{jN}{p^{k+1} q} + \ell_2 \frac{N}{p} + m_2 \frac{N}{q},$$

where $a_1, a_2 \in A_{j \bmod p^k}$. We will show that $m_1 \equiv m_2 \bmod q$; if not, then

$$\frac{N}{p^{k+1} q}(a_2 - a_1) = (\ell_2 - \ell_1)\frac{N}{p} + (m_2 - m_1)\frac{N}{q} \in \frac{N}{pq}\mathbb{Z}_N^\star$$

or, equivalently $a_2 - a_1 \in p^k \mathbb{Z}_N^\star$ or $\mathrm{ord}(a_2 - a_1) = \frac{N}{p^k}$, which by Corollary 3.4 gives $B(\zeta_N^{p^k}) = 0$, contradicting the hypothesis $A(\zeta_{p^{k+1}}) \neq 0$ due to Lemma 10.3 (especially equation (10.4)), with the

roles of A and B reversed). Thus, $m_1 \equiv m_2 \bmod q$, and considering any other pair of elements of $\frac{N}{p^{k+1}q} \cdot A_{j \bmod p^k}$ on two different q-cycles, where one element is either $\frac{a_1 N}{p^{k+1}q}$ or $\frac{a_2 N}{p^{k+1}q}$, we obtain

$$\frac{N}{p^{k+1}q} A_{j \bmod p^k} \subseteq \frac{jN}{p^{k+1}q} + \frac{N}{p}\mathbb{Z}_N + m_1 \frac{N}{q},$$

by repeating the above argument. This shows that $\frac{N}{p^{k+1}q} \cdot A_{j \bmod p^k}$ is supported on a p-cycle; thus, $A_{j \bmod p^k}$ is absorbed $\bmod p^k q$, as desired. The fact that **(wT2)** fails follows easily from equation (11.1). □

Corollary 11.3. *Let $N \in \mathcal{S}'_{p,q}$, (A, B) a spectral pair in $\mathbb{Z}_N$ with $A \in \mathcal{F}_{\max}(N)$. It holds*

$$A(\zeta_{q^2}) = B(\zeta_{q^2}) = A(\zeta_{p^2}) = B(\zeta_{p^2}) = 0.$$

If $p < q$, then

$$A(\zeta_{p^3}) = \cdots = A(\zeta_{p^{\lceil \log_p q \rceil + 1}}) = B(\zeta_{p^3}) = \cdots = B(\zeta_{p^{\lceil \log_p q \rceil + 1}}) = 0,$$

as well. Moreover,

$$A(\zeta_N^q) = B(\zeta_N^q) = A(\zeta_N^p) = \cdots = A(\zeta_N^{p^{\lceil \log_p q \rceil}}) = B(\zeta_N^p) = \cdots = B(\zeta_N^{p^{\lceil \log_p q \rceil}}) = 0.$$

Proof. By Proposition 11.2, property **(wT2)** fails for both A and B. Combined with Proposition 10.11, this shows that

$$A(\zeta_{p^2}) = B(\zeta_{p^2}) = A(\zeta_{q^2}) = B(\zeta_{q^2}) = 0,$$

and then Lemma 10.3 implies

$$A(\zeta_N^p) = B(\zeta_N^p) = A(\zeta_N^q) = B(\zeta_N^q) = 0.$$

Next, assume $p < q$, and suppose

$$A(\zeta_p) = \cdots = A(\zeta_{p^k}) = 0 \neq A(\zeta_{p^{k+1}}).$$

By Proposition 11.2, there is some j such that $A_{j \bmod p^k}$ is absorbed $\bmod p^k q$, that is,

$$A_{j \bmod p^k} = A_{j + \ell p^k \bmod p^k q}$$

for some ℓ. But then,

$$A_{j \bmod p^k} \subseteq A_{j + \ell p^k \bmod pq};$$

therefore,

$$\frac{|A|}{p^k} = |A_{j \bmod p^k}| \leq |A_{j + \ell p^k \bmod pq}| = \frac{|A|}{pq},$$

which yields $p^{k-1} > q$ or, equivalently, $k > \log_p q + 1$, so finally

$$k \geq \lceil \log_p q \rceil + 1.$$

Reversing the roles of A and B, we obtain the same result for B. The final part then follows directly from Lemma 10.3. □

Lemma 11.4. *Let (A, B) be a spectral pair in $\mathbb{Z}_N$, where $N \in \mathcal{S}'_{p,q}$ and $A \in \mathcal{F}_{\max}(N)$. Then neither A nor B satisfy (wT1) as*

$$|U_A^N(p)|, |U_B^N(p)| \geq \lceil \log_p q \rceil$$

and

$$|U_A^N(q)|, |U_B^N(q)| \geq \lceil \log_q p \rceil.$$

Proof. Without loss of generality, we may assume $p < q$ so that the second inequality becomes $|U_A^N(q)|, |U_B^N(q)| \geq 1$, which easily follows from Proposition 10.4. We remind that $m_p(A)$ denotes as usual the maximal exponent x such that $A(\zeta_N^{p^x}) \neq 0$. We will show

$$|U_B^N(p)| \geq \lceil \log_p q \rceil,$$

and the inequality $|U_A^N(p)| \geq \lceil \log_p q \rceil$ has similar proof. Denote

$$s = |[0, m_p(A)] \cap R_A^N(p)|.$$

We will show the existence of j satisfying

$$|A_{j \bmod p^{m-m_p(A)-1}q^{n-1}}| = p^s q$$

and $A_{j \bmod p^{m-m_p(A)-1}q^{n-1}}$ is not absorbed $\bmod p^{m-m_p(A)}q^{n-1}$. For convenience, we will put $d = p^{m-m_p(A)-1}q^{n-1}$. Suppose that

$$A(\zeta_N) = A(\zeta_N^p) = \cdots = A(\zeta_N^{p^k}) = 0 \neq A(\zeta_N^{p^{k+1}})$$

so that

$$B(\zeta_p) = B(\zeta_{p^2}) = \cdots = B(\zeta_{p^{k+1}}) = 0 \neq B(\zeta_{p^{k+2}})$$

by Lemma 10.3. It holds

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

for some $P(X), Q(X) \in \mathbb{Z}_{\geq 0}[X]$ by Theorem 5.2, and $P \not\equiv 0$ by Theorem 10.9(2). Replacing X by X^p and observing that $\Phi_q(X^{N/q}) \equiv \Phi_q(X^{pN/q}) \bmod (X^N - 1)$, we obtain

$$A(X^p) \equiv pP(X^p) + Q(X^p)\Phi_q(X^{N/q}) \bmod (X^N - 1).$$

Since $A(\zeta_N^p) = 0$, we must have

$$pP(\zeta_N^p) = A(\zeta_N^p) - Q(\zeta_N^p)\Phi_q(\zeta_q^p) = 0,$$

therefore

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

where $\widetilde{P}(X), \widetilde{Q}(X) \in \mathbb{Z}_{\geq 0}[X]$, hence

$$A(X^p) \equiv pP_1(X^p)\Phi_p(X^{N/p}) + Q_1(X^p)\Phi_q(X^{N/q}) \bmod (X^N - 1),$$

where $P_1(X^p) = \widetilde{P}(X^p)$ and $Q_1(X^p) = Q(X^p) + p\widetilde{Q}(X^p)$. The polynomial P_1 is not identically zero since $A(\zeta_N^{p^{k+1}}) \neq 0$ (see Theorem 5.2). Repeating this process for the roots

$$\zeta_N^{p^2}, \ldots, \zeta_N^{p^k},$$

we obtain

$$A(X^{p^k}) \equiv p^k P_k(X^{p^k})\Phi_p(X^{N/p}) + Q_k(X^{p^k})\Phi_q(X^{N/q}) \bmod (X^N - 1), \tag{11.2}$$

where $P_k(X), Q_k(X) \in \mathbb{Z}_{\geq 0}[X]$, and P_k is not identically zero since $A(\zeta_N^{p^{k+1}}) \neq 0$. As

$$A(X^{p^{k+1}}) \equiv p^{k+1} P_k(X^{p^{k+1}}) + Q_k(X^{p^{k+1}})\Phi_q(X^{N/q}) \bmod (X^N - 1) \tag{11.3}$$

is the mask polynomial of the mutliset $p^{k+1} \cdot A$, we deduce that there are elements in $p^{k+1} \cdot A$ whose multiplicity is exactly p^{k+1} (in general, since A is a proper set, the multiplicity of any element in $d \cdot A$ cannot exceed d). The element $p^{k+1}a$ can only have multiplicity p^{k+1} in A if

$$a + \frac{N}{p^{k+1}}\mathbb{Z}_N \subseteq A,$$

i.e., a is an element of a p^{k+1}-cycle contained in A or, equivalently, $|A_{a \bmod p^{m-k-1}q^n}| = p^{k+1}$. A cannot have two p^{k+1}-cycles of the form

$$a + \frac{N}{p^{k+1}}\mathbb{Z}_N, \quad a + \ell\frac{N}{p^{k+1}q} + \frac{N}{p^{k+1}}\mathbb{Z}_N,$$

for $\ell \not\equiv 0 \bmod q$ because, in that case, we would have

$$\ell p^{m-k-1}q^{n-1} + p^{m-k-1}q^n\mathbb{Z}_N \subseteq A - A,$$

which implies that

$$(A - A) \cap d\mathbb{Z}_N^\star \neq 0, \quad \forall d \in \{p^{m-k-1}q^{n-1}, p^{m-k}q^{n-1}, \ldots, p^{m-2}q^{n-1}, p^{m-1}q^{n-1}\},$$

whence

$$B(\zeta_{pq}) = B(\zeta_{p^2q}) = \cdots = B(\zeta_{p^{k+1}q}) = 0$$

by Theorem 3.3(i), which means that B satisfies (wT2), contradicting Proposition 11.2. The above show that

$$|A_{a \bmod p^{m-k-1}q^n}| = p^{k+1} \implies A_{a \bmod p^{m-k-1}q^{n-1}} \text{ is absorbed } \bmod p^{m-k-1}q^n. \tag{11.4}$$

Now let

$$R_A^N(p) \cap [0, m_p(A)] = \{r_0, r_1, \ldots, r_{s-1}\},$$

where the r_i are in increasing order. We know already that $r_i = i$ for $0 \leq i \leq k$. Continuing from equation (11.2), we obtain

$$A(X^{p^{r_{k+1}}}) \equiv p^{k+1} P_k(X^{p^{r_{k+1}}}) + Q_k(X^{p^{r_{k+1}}})\Phi_q(X^{N/q}) \bmod (X^N - 1).$$

Since $A(\zeta_N^{p^{r_{k+1}}}) = 0 \neq A(\zeta_N^{p^{m_p(A)}})$, we get that $P_k(\zeta_N^{p^{r_{k+1}}}) = 0 \neq P_k(\zeta_N^{p^{m_p(A)}})$, whence by Theorem 3.3(i) we obtain

$$P_k(X^{p^{r_{k+1}}}) \equiv \widetilde{P}_k(X^{p^{r_{k+1}})\Phi_p(X^{N/p}) + \widetilde{Q}_k(X^{p^{r_{k+1}}})\Phi_q(X^{N/q}) \bmod (X^N - 1)$$

for some $\widetilde{P}_k(X), \widetilde{Q}_k(X) \in \mathbb{Z}_{\geq 0}[X]$, with $\widetilde{P}_k$ not identically zero. This gives

$$A(X^{p^{r_{k+1}}}) \equiv p^{k+1}P_{k+1}(X^{p^{r_{k+1}}})\Phi_p(X^{N/p}) + Q_{k+1}(X^{p^{r_{k+1}}})\Phi_q(X^{N/q}) \bmod (X^N - 1),$$

where $P_{k+1}(X) = \widetilde{P}_k(X)$ and $Q_{k+1}(X) = Q_k(X) + p^{k+1}\widetilde{Q}_k(X)$. Repeating this process for the roots

$$\zeta_N^{p^{r_{k+2}}}, \dots, \zeta_N^{p^{r_{s-1}}},$$

we obtain

$$A(X^{p^{r_{s-1}}}) \equiv p^{s-1}P_{s-1}(X^{p^{r_{s-1}}})\Phi_p(X^{N/p}) + Q_{s-1}(X^{p^{r_{s-1}}})\Phi_q(X^{N/q}) \bmod (X^N - 1)$$

for some $P_{s-1}(X), Q_{s-1}(X) \in \mathbb{Z}_{\geq 0}[X]$, where P_{s-1} is not identically zero since $r_{s-1} < m_p(A)$ and $A(\zeta_N^{p^{m_p(A)}}) \neq 0$; this is achieved by repeated use of Theorem 5.2. Therefore, it holds

$$A(X^{p^{m_p(A)+1}}) \equiv p^s P_{s-1}(X^{p^{m_p(A)+1}}) + Q_{s-1}(X^{p^{m_p(A)+1}})\Phi_q(X^{N/q}) \bmod (X^N - 1).$$

By definition of $m_p(A)$, we have

$$A(\zeta_N^{p^{m_p(A)+1}}) = A(\zeta_N^{p^{m_p(A)+2}}) = \cdots = A(\zeta_N^{p^m}) = 0,$$

hence

$$P_{s-1}(\zeta_N^{p^{m_p(A)+1}}) = P_{s-1}(\zeta_N^{p^{m_p(A)+2}}) = \cdots = P_{s-1}(\zeta_N^{p^m}) = 0,$$

so by Lemma 10.2 we get

$$P_{s-1}(X^{p^{m_p(A)+1}}) \equiv P_s(X^{p^{m_p(A)+1}})\Phi_q(X^{N/q}) \bmod (X^N - 1),$$

where $P_s(X) \in \mathbb{Z}_{\geq 0}[X]$, hence

$$A(X^{p^{m_p(A)+1}}) \equiv (p^s P_s(X^{p^{m_p(A)+1}}) + Q_{s-1}(X^{p^{m_p(A)+1}}))\Phi_q(X^{N/q}) \bmod (X^N - 1) \qquad (11.5)$$

so that the multiset $p^{m_p(A)+1} \cdot A$ is a disjoint union of q-cycles. It is clear from equation (11.5) that there is some j with $|A_{j \bmod p^{m-m_p(A)-1}q^n}| \geq p^s$. However, we will show that

$$|A_{j \bmod p^{m-m_p(A)-1}q^n}| \leq p^s$$

for every j. For this purpose, consider the p-adic expansion of $a - j$, where a is an arbitrary element of $A_{j \bmod p^{m-m_p(A)-1}q^n}$

$$a - j \equiv a_{m-m_p(A)-1}p^{m-m_p(A)-1} + \cdots + a_{m-1}p^{m-1} \bmod p^m,$$

where, as usual, $0 \leq a_i \leq p - 1$, $m - m_p(A) - 1 \leq i \leq m - 1$. Now, if $|A_{j \bmod p^{m-m_p(A)-1}q^n}| > p^s$, then there would exist two elements $a, a' \in A_{j \bmod p^{m-m_p(A)-1}q^n}$ such that the p-adic expansions of $a - j$ and $a' - j$ would have the same digits at all places $m - r$ for $r - 1 \in R_A^N(p)$. Therefore, $a - a' = (a - j) - (a' - j) \in d\mathbb{Z}_N^\star$, where $d = p^{m-r}q^n$, with $r - 1 \leq m_p(A)$ and $r - 1 \notin R_A^N(p)$. By

Lemma 10.3, we would have $r \notin S_B^N(p)$, whence $B(\zeta_{p^r}) \neq 0$, contradicting Theorem 3.3(i) or Corollary 3.4, which yield $B(\zeta_{p^r}) = 0$ due to $a - a' \in p^{m-r}q^n\mathbb{Z}_N^\star$.

To summarize, we have $|A_{j \bmod p^{m-m_p(A)-1}q^n}| \leq p^s$ for every j, and equality occurs for some j. Using the same arguments as above, we deduce that, if $|A_{j \bmod p^{m-m_p(A)-1}q^n}| = p^s$, then the elements of $A_{j \bmod p^{m-m_p(A)-1}q^n} - j$ obtain all possible arrangements of p-adic digits at the places $m - r$, where $r - 1 \in R_A^N(p)$; in particular, $A_{j \bmod p^{m-m_p(A)-1}q^n}$ must be a disjoint union of p^{k+1}-cycles. So, let $|A_{j \bmod p^{m-m_p(A)-1}q^n}| = p^s$. By equations (11.4) and (11.5), we obtain

$$|A_{j \bmod p^{m-k-1}q^{n-1}}| = p^{k+1}, \qquad |A_{j \bmod p^{m-m_p(A)-1}q^{n-1}}| = p^s q.$$

We observe that $A_{j \bmod p^{m-m_p(A)-1}q^{n-1}}$ is equidistributed mod $p^{m-m_p(A)-1}q^n$, while $A_{j \bmod p^{m-k-1}q^{n-1}}$ is absorbed mod $p^{m-k-1}q^n$. For every $r \in [k, m_p(A)]$, we will take into account the number of nonempty sets in the partition

$$A_{j \bmod p^{m-r-1}q^{n-1}} = \bigsqcup_{u=0}^{q-1} A_{j+up^{m-r-1}q^{n-1} \bmod p^{m-r-1}q^n},$$

denoted by $f_j(r)$, so that $1 \leq f_j(r) \leq q$ for all $r \in [k, m_p(A)]$ and $f_j(m_p(A)) = q$, $f_j(k) = 1$. Now, pick j' such that $j' \equiv j \bmod p^{m-m_p(A)-1}q^n$ and

$$f_{j'}(r-1) = \max_{0 \leq \ell \leq p-1} f_{j'+\ell p^{m-r-1}q^{n-1}}(r-1).$$

Without loss of generality, we may simply have $j' = j$, and it holds

$$f_j(r-1) \geq \frac{1}{p} f_j(r), \qquad r \in [k+1, m_p(A)].$$

We observe that, if $f_j(r-1) < f_j(r)$, then $r + 1 \in U_B^N(p)$. Indeed, consider the multiset $p^r \cdot A_{j \bmod p^{m-r-1}q^{n-1}}$, which is supported at the pq-cycle $p^r j + \frac{N}{pq}\mathbb{Z}_N$. We will show that $A(\zeta_N^{p^r}) \neq 0$, which implies $B(\zeta_{p^{r+1}}) \neq 0$ by Lemma 10.3. Assume otherwise, that $A(\zeta_N^{p^r}) = 0$; hence, $p^r \cdot A_{j \bmod p^{m-r-1}q^{n-1}}$ must be a disjoint union of p- and q-cycles. Since $f_j(r-1) < f_j(r)$, we cannot have any q-cycles because

$$f_{j+\ell p^{m-r-1}q^{n-1}}(r-1) \leq f_j(r-1) < f_j(r) \leq f_j(m_p(A)) = q, \qquad 0 \leq \ell \leq p-1,$$

which means that, for every $0 \leq \ell \leq p-1$, there is $0 \leq u \leq q-1$ such that

$$A_{j+\ell p^{m-r-1}q^{n-1}+up^{m-r}q^{n-1} \bmod p^{m-r}q^n} = \varnothing.$$

But $p^r \cdot A_{j \bmod p^{m-r-1}q^{n-1}}$ cannot be a disjoint union of p-cycles either because in this case $A_{j \bmod p^{m-r-1}q^{n-1}}$ would be equidistributed mod $p^{m-r}q^{n-1}$, whence $f_j(r-1) = f_j(r)$, contradiction. Hence, $A(\zeta_N^{p^r})B(\zeta_{p^{r+1}}) \neq 0$. Moreover, $p^r \cdot A_{j \bmod p^{m-r-1}q^{n-1}}$ can be supported neither on a q-cycle, because in this case $f_j(r-1) = f_j(r)$ and

$$f_{j+\ell p^{m-r-1}q^{n-1}}(r-1) = 0, \qquad 1 \leq \ell \leq p-1,$$

nor on a p-cycle because it would hold

$$f_{j+\ell p^{m-r-1}q^{n-1}}(r-1) = f_j(r) = 1, \qquad 0 \leq \ell \leq p-1,$$

contradiction. Hence, by Proposition 5.5, we obtain

$$(p^r A - p^r A) \cap \frac{N}{pq} \mathbb{Z}_N^\star \neq \varnothing,$$

so there are $a, a' \in A$ such that $a - a' \in \frac{N}{p^{r+1}q}$, whence $B(\zeta_{p^{r+1}q}) = 0$ by Theorem 3.3(i), and $r + 1 \in U_B^N(p)$, as desired.

For the last part of our proof, we will just show that we have $f_j(r-1) < f_j(r)$ for at least $\lceil \log_p q \rceil$ values of r. Indeed, let

$$\{r_1, \ldots, r_t\} = \left\{ r \in [k, m_p(A)] : f_j(r-1) < f_j(r) \right\}.$$

By definition and the property $f_j(r-1) \geq \frac{1}{p} f_j(r)$ for all r, we obtain

$$q = f_j(r_t) \leq p f_j(r_t - 1) = p f_j(r_{t-1}) \leq p^2 f_j(r_{t-1} - 1) = p^2 f_j(r_{t-2}) \leq \cdots$$
$$\cdots \leq p^{t-1} f_j(r_1) \leq p^t f_j(r_1 - 1) = p^t f_j(k) = p^t,$$

which clearly implies $t \geq \lceil \log_p q \rceil$, finally showing

$$|U_B^N(p) \cap [1, m_p(A) + 1]| \geq \lceil \log_p q \rceil,$$

as desired. □

Corollary 11.5. *Let (A, B) be a spectral pair in $\mathbb{Z}_N$, where $N \in \mathcal{S}'_{p,q}$ and $A \in \mathcal{F}_{\max}(N)$. Then*

$$p^{|S_B^N(p)| + \lceil \log_p q \rceil} q^{|S_B^N(q)| + \lceil \log_q p \rceil} \mid |B|$$

and

$$p^{|S_A^N(p)| + \lceil \log_p q \rceil} q^{|S_A^N(q)| + \lceil \log_q p \rceil} \mid |A|.$$

Proof. By Lemmata 10.5 and 11.4 we obtain

$$p^{|S_B^N(p)| + \lceil \log_p q \rceil} \mid |B|.$$

Reversing the roles of A and B and of p and q, we obtain the desired result. □

If $p < q$, we observe that the power of p dividing $|A|$ with $A \in \mathcal{F}_{\max}(N)$ is at least

$$|S_A^N(p)| + \lceil \log_p q \rceil \geq 2 \lceil \log_p q \rceil + 2 \geq 6,$$

which can be seen by Theorem 10.9 and Corollary 11.3. Moreover, the power of q dividing $|A|$ is at least

$$|S_A^N(q)| + 1 \geq 4,$$

again by Theorem 10.9 and Corollary 11.3. We have thus proven:

Corollary 11.6. *Let $N = p^m q^n$, with $p < q$, and let $A \subseteq \mathbb{Z}_N$ be spectral. If either $m \leq 6$ or $n \leq 4$, then A tiles. The same conclusion holds if $p^{m-4} < q^2$.*

Proof. Assume otherwise, that $N \in \mathcal{S}_{p,q}$; without loss of generality, we may assume $N \in \mathcal{S}'_{p,q}$. Let $A \in \mathcal{F}_{\max}(N)$ so that $p^6 q^4 \mid |A|$, as shown above. By Proposition 6.2, this would mean that A tiles if

either $m \leq 6$ or $n \leq 4$, contradiction. For the second part, we observe that $p^{m-4} < q^2$ is equivalent to $p^{\frac{m}{2}-2} < q$ or, equivalently,

$$\frac{m}{2} - 1 \leq \lceil \log_p q \rceil \Leftrightarrow m \leq 2\lceil \log_p q \rceil + 2 \leq |S_A^N(p)| + \lceil \log_p q \rceil,$$

which again implies that $p^m \mid |A|$; hence, A tiles by Proposition 6.2, contradiction. This completes the proof. □

We may assume henceforth that both exponents are at least 5, and that of the smallest prime is at least 7. We will refine the above bound by introducing a new concept.

Definition 11.7. Let (A, B) be a primitive spectral pair in $\mathbb{Z}_N$. Define the *p-root deficit* of A as

$$\mathrm{def}_p(A) = \left| \left\{ x : A(\zeta_{p^{x+1}}) \neq 0 = B(\zeta_N^{p^x}) \right\} \right|,$$

and similarly define $\mathrm{def}_q(A)$, $\mathrm{def}_p(B)$, $\mathrm{def}_q(B)$.

Remark. We should note that the root deficits of a spectral set A always depend on the choice of the spectrum B.

Lemma 11.8. *Let (A, B) be a primitive spectral pair in $\mathbb{Z}_N$, $N \in \mathcal{S}'_{p,q}$, $A \in \mathcal{F}_{\max}(N)$. Then, the following inequalities hold:*

$$|A| = |B| \leq \min\{ p^{|S_B^N(p)|+\mathrm{def}_p(B)} q^{|S_A^N(q)|}, p^{|S_A^N(p)|+\mathrm{def}_p(A)} q^{|S_B^N(q)|},$$
$$p^{|S_B^N(p)|} q^{|S_A^N(q)|+\mathrm{def}_q(A)}, p^{|S_A^N(p)|} q^{|S_B^N(q)|+\mathrm{def}_q(B)} \}$$

Proof. We will show that

$$|A| \leq p^{|S_B^N(p)|} q^{|S_A^N(q)|+\mathrm{def}_q(A)}.$$

All the other inequalities are obtained by reversing the roles of p, q and of A, B. First, we will prove that

$$|A_{j \bmod q^n}| \leq p^{|S_B^N(p)|} \tag{11.6}$$

for all j. Let

$$S_B^N(p) = \{x_1, \ldots, x_t\} \subseteq \{1, 2, \ldots, m\},$$

where $t = |S_B^N(p)|$ and the x_i are in increasing order. We will write every element of $a \in A_{j \bmod q^n}$ in p-adic representation, that is,

$$a \equiv a_0 + a_1 p + \cdots + a_{m-1} p^{m-1} \bmod p^m,$$

where, as usual, $0 \leq a_i \leq p - 1$, $0 \leq i \leq m - 1$. No two elements of $A_{j \bmod q^n}$ have the same p-adic digits; otherwise, $N = p^m q^n$ would divide their difference, i.e., they would be equal. Moreover, two distinct elements $a, a' \in A_{j \bmod q^n}$ cannot have the same p-adic digits at the places

$$m - x_t, \ldots, m - x_1,$$

otherwise, $a - a' \in p^{m-x} q^n \mathbb{Z}_N^\star$ where $x \notin S_B^N(p)$, and as a consequence,

$$B(\zeta_{\mathrm{ord}(a-a')}) = B(\zeta_{p^x}) \neq 0,$$

contradicting Corollary 3.4. Thus, the elements of $A_{j \bmod q^n}$ have distinct digits at one of the places $m - x_i$. This clearly shows that

$$|A_{j \bmod q^n}| \le p^t = p^{|S_B^N(p)|},$$

proving our claim. Next, we will show that there is some j such that

$$|A_{j \bmod q^n}| \ge \frac{|A|}{q^{|S_A^N(q)| + \mathrm{def}_q(A)}}.$$

Recall that $m_q(B)$ is the maximal integer $x \in [0, n-1]$ for which

$$B(\zeta_N^{q^x}) \ne 0.$$

Since $B \in \mathscr{F}_{\max}(N)$, such an exponent exists, as we have already seen. Furthermore, Lemma 10.3 and Proposition 10.4 imply that

$$A(\zeta_{q^{m_q(B)+1}}) \ne 0 = A(\zeta_{pq^{m_q(B)+1}}).$$

Applying Lemma 9.2 for $d = q^{m_q(B)}$, with the roles of p, q and A, B reversed, we obtain that $A_{j \bmod q^{m_q(B)}}$ is either absorbed or equidistributed $\mathrm{mod}q^{m_q(B)+1}$ for every j. Since $A(\zeta_{q^{m_q(B)+1}}) \ne 0$, there must exist some j such that $A_{j \bmod q^{m_q(B)}}$ is absorbed $\mathrm{mod}q^{m_q(B)+1}$. Without loss of generality, we put

$$A_{j \bmod q^{m_q(B)}} = A_{j \bmod q^{m_q(B)+1}}.$$

The set $A_{j \bmod q^{m_q(B)+1}}$ is in turn equidistributed $\mathrm{mod}pq^{m_q(B)+1}$ since the multiset $\frac{N}{pq^{m_q(B)+1}} \cdot A_{j \bmod q^{m_q(B)}}$ is contained in a pq-cycle for every j, and for this specific value of j, it is supported on a p-cycle. In particular,

$$\left|A_{j + \ell q^{m_q(B)+1} \bmod pq^{m_q(B)+1}}\right| = \frac{1}{p}\left|A_{j \bmod q^{m_q(B)+1}}\right|$$

for every ℓ. For any $y \le m_q(B)$ with $y + 1 \in S_A^N(q)$, it holds

$$|A_{j \bmod q^{y+1}}| = \frac{1}{q}|A_{j \bmod q^y}|, \tag{11.7}$$

while if $y \le m_q(B)$ and $y + 1 \notin S_A^N(q)$, it holds

$$|A_{j \bmod q^{y+1}}| = |A_{j \bmod q^y}|. \tag{11.8}$$

Indeed, since $B(\zeta_N^{q^y}) \ne 0$ by Lemma 10.3, we must have $a - a' \notin q^y \mathbb{Z}_N^\star$ for every $a, a' \in A$, $a \ne a'$ due to Theorem 3.3(i) (or Corollary 3.4). If $A_{j \bmod q^y}$ were not absorbed $\mathrm{mod}q^{y+1}$, there would exist some $u \not\equiv 0 \bmod q$ such that $A_{j + uq^y \bmod q^{y+1}} \ne \varnothing$; hence, for some $0 \le \ell \le p - 1$ satisfying

$$\ell q^{m_q(B)+1-y} \not\equiv u \bmod p,$$

and $a \in A_{j + \ell q^{m_q(B)+1} \bmod pq^{m_q(B)+1}}$, $a' \in A_{j + uq^y \bmod q^{y+1}}$, we obtain

$$a - a' \equiv q^y(\ell q^{m_q(B)+1-y} - u) \bmod pq^{m_q(B)+1},$$

hence $a - a' \in q^y \mathbb{Z}_N^\star$, contradiction. Thus, combining equations (11.7) and (11.8), we get

$$\left|A_{j \bmod q^{m_q(B)+1}}\right| = \frac{|A|}{q^{|S_A^N(q) \cap [1, m_q(B)+1]|}}.$$

Next, we recall

$$\mathrm{def}_q(A) = \left|\left\{y \in [1, n] : A(\zeta_{p^y}) \neq 0 = B(\zeta_N^{p^{y-1}})\right\}\right|,$$

where the set of y in the description above must satisfy $y > m_q(B) + 1$. In other words, every $y \in [m_q(B) + 2, n]$ either satisfies $A(\zeta_{q^y}) = 0$ or $A(\zeta_{p^y}) \neq 0 = B(\zeta_N^{p^{y-1}})$, hence

$$n - m_q(B) - 1 = |S_A^N(q) \cap [m_q(B) + 2, n]| + \mathrm{def}_q(A).$$

Therefore, by equation (11.6), we get

$$\begin{aligned} p^{|S_B^N(p)|} &\geq \max_\ell |A_{j+\ell q^{m_q(B)+1} \bmod q^n}| \\ &\geq \frac{1}{q^{n - m_q(B) - 1}} |A_{j \bmod q^n}| \\ &= \frac{|A|}{q^{|S_A^N(q) \cap [m_q(B)+2, n]| + \mathrm{def}_q(A)} q^{|S_A^N(q) \cap [1, m_q(B)+1]|}}, \end{aligned}$$

whence we finally obtain

$$|A| \leq p^{|S_B^N(p)|} q^{|S_A^N(q)| + \mathrm{def}_q(A)},$$

as desired. $\qquad\square$

Corollary 11.9. *Let (A, B) be a spectral pair in $\mathbb{Z}_N$, where $N \in \mathscr{S}'_{p,q}$, $A \in \mathscr{F}_{\max}(N)$. Then*

$$p^{\lceil \log_p q \rceil} q^{\lceil \log_q p \rceil} < \min\left\{p^{\mathrm{def}_p(A)}, p^{\mathrm{def}_p(B)}, q^{\mathrm{def}_q(A)}, q^{\mathrm{def}_q(B)}\right\}.$$

If in addition $p < q$, we get

$$\mathrm{def}_q(A), \mathrm{def}_q(B) \geq 3,$$

and

$$\mathrm{def}_p(A), \mathrm{def}_p(B) \geq 2\lceil \log_p q \rceil \geq 4.$$

Proof. Denote

$$s_p = \max\left\{|S_A^N(p)|, |S_B^N(p)|\right\}, \quad s_q = \max\left\{|S_A^N(q)|, |S_B^N(q)|\right\}.$$

By Corollary 11.5, we obtain

$$p^{s_p + \lceil \log_p q \rceil} q^{s_q + \lceil \log_q p \rceil} \mid |A|,$$

whence by Lemma 11.8 it follows

$$\begin{aligned} p^{s_p + \lceil \log_p q \rceil} q^{s_q + \lceil \log_q p \rceil} \leq \min\{&p^{|S_B^N(p)| + \mathrm{def}_p(B)} q^{|S_A^N(q)|}, p^{|S_A^N(p)| + \mathrm{def}_p(A)} q^{|S_B^N(q)|}, \\ &p^{|S_B^N(p)|} q^{|S_A^N(q)| + \mathrm{def}_q(A)}, p^{|S_A^N(p)|} q^{|S_B^N(q)| + \mathrm{def}_q(B)}\}, \end{aligned}$$

which easily yields the inequality

$$p^{\lceil \log_p q \rceil} q^{\lceil \log_q p \rceil} < \min \left\{ p^{\operatorname{def}_p(A)}, p^{\operatorname{def}_p(B)}, q^{\operatorname{def}_q(A)}, q^{\operatorname{def}_q(B)} \right\}.$$

Next, suppose $p < q$ so that the above inequality becomes

$$p^{\lceil \log_p q \rceil} q < \min \left\{ p^{\operatorname{def}_p(A)}, p^{\operatorname{def}_p(B)}, q^{\operatorname{def}_q(A)}, q^{\operatorname{def}_q(B)} \right\}.$$

Since $q^2 < p^{\lceil \log_p q \rceil} q$, the above yields

$$\operatorname{def}_q(A), \operatorname{def}_q(B) \geq 3$$

and

$$p^{2 \lceil \log_p q \rceil} \leq \min \left\{ p^{\operatorname{def}_p(A)}, p^{\operatorname{def}_p(B)} \right\}$$

or, equivalently,

$$\operatorname{def}_p(A), \operatorname{def}_p(B) \geq 2 \lceil \log_p q \rceil \geq 4,$$

as desired.   □

Proposition 11.10. *Let (A, B) be a spectral pair in $\mathbb{Z}_N$ such that $N \in \mathcal{S}'_{p,q}$, $A \in \mathcal{F}_{\max}(N)$ and $p < q$. Then*

$$\operatorname{def}_p(A), \operatorname{def}_p(B) \leq m - 2 - 2 \lceil \log_p q \rceil$$

and

$$\operatorname{def}_q(A), \operatorname{def}_q(B) \leq n - 4.$$

Proof. We remind that $|S_A^N(p) - 1|$, $|U_A^N(p) - 1|$ and $\operatorname{def}_p(A)$ are cardinalities of pairwise disjoint subsets of $\{0, 1, \ldots, m-1\}$ by definition. The bounds given by Proposition 10.11, Corollary 11.3, Lemma 11.4 and Corollary 11.9 yield

$$m \geq |S_A^N(p)| + |U_A^N(p)| + \operatorname{def}_p(A) \geq 2 \lceil \log_p q \rceil + 2 + \operatorname{def}_p(A),$$

which easily gives the first estimate (the same holds for $\operatorname{def}_p(B)$). For the second inequality, we obtain similarly

$$n \geq |S_A^N(q)| + |U_A^N(q)| + \operatorname{def}_q(A) \geq 4 + \operatorname{def}_q(A),$$

which gives the second inequality (the same inequality also holds for $\operatorname{def}_q(B)$).   □

12. Proof of Theorem 1.4

From Corollary 11.9 and Proposition 11.10, we obtain that $\mathcal{F}(N)$, and hence, $\mathcal{F}_{\max}(N)$ is nonempty with $N \in \mathcal{S}'_{p,q}$ only if

$$4 \leq 2 \lceil \log_p q \rceil \leq m - 2 - 2 \lceil \log_p q \rceil \leq m - 6,$$

and $3 \leq n - 4$. This proves that, if $N = p^m q^n$ with $p < q$, and either $m \leq 9$ or $n \leq 6$ holds, then every spectral subset of $\mathbb{Z}_N$ tiles, i.e., Fuglede's conjecture holds for cyclic groups of order N with the

given conditions. For the second part of the theorem, we invoke the inequalities involving $\mathrm{def}_p(A)$ and $\mathrm{def}_p(B)$ in Corollary 11.9 and Proposition 11.10 to obtain

$$4\lceil \log_p q \rceil + 2 \le m,$$

which implies

$$q^4 < p^{4\lceil \log_p q \rceil} \le p^{m-2}.$$

Thus, if $p^{m-2} < q^4$ holds, then $\mathscr{F}_{\max}(N)$ must be necessarily empty, or in other words, $N \notin \mathcal{S}_{p,q}$, which by definition means that Fuglede's conjecture holds for cyclic groups of order $p^m q^n$, where $p^{m-2} < q^4$.

Conflict of Interest. None.

References

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

[2] N. G. de Bruijn, 'On the factorization of cyclic groups', *Nederl. Akad. Wetensch. Proc. Ser. A. 56 = Indagationes Math.* **15** (1953), 370–377.

[3] D. E. Dutkay and C.-K. Lai, 'Some reductions of the spectral set conjecture to integers', *Math. Proc. Cambridge Philos. Soc.* **156**(1) (2014), 123–135.

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

[5] A. Fan, S. Fan and R. Shi, 'Compact open spectral sets in $\mathbb{Q}_p$', *J. Funct. Anal.* **271**(12) (2016), 3628–3661.

[6] B. Farkas, M. Matolcsi and P. Móra, 'On Fuglede's conjecture and the existence of universal spectra', *J. Fourier Anal. Appl.* **12**(5) (2006), 483–494.

[7] B. Farkas and S. G. Révész, 'Tiles with no spectra in dimension 4', *Math. Scand.* **98**(1) (2006), 44–52.

[8] S. J. Ferguson and N. Sothanaphan, 'Fuglede's conjecture fails in 4 dimensions over odd prime fields', *Discrete Math.* **343**(1) (2020), 111507.

[9] B. Fuglede, 'Commuting self-adjoint partial differential operators and a group theoretic problem', *J. Funct, Anal.* **16** (1974), 101–121.

[10] A. Iosevich and M. N. Kolountzakis, 'Periodicity of the spectrum in dimension one', *Anal. PDE* **6**(4) (2013), 819–827.

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

[12] G. Kiss, R. D. Malikiosis, G. Somlai and M. Vizer, 'Fuglede's conjecture holds for cyclic groups of order *pqrs*', Preprint, 2020, arXiv:2011.09578.

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

[14] M. N. Kolountzakis and M. Matolcsi, 'Complex Hadamard matrices and the spectral set conjecture', *Collect. Math.* (2006), 281–291.

[15] M. N. Kolountzakis and M. Matolcsi, 'Tiles with no spectra', *Forum Math.* **18**(3) (2006), 519–528.

[16] M. N. Kolountzakis and M. Matolcsi, 'Algorithms for translational tiling', *J. Math. Music* **3**(2) (2009), 85–97.

[17] I. Łaba, 'The spectral set conjecture and multiplicative properties of roots of polynomials', *J. London Math. Soc. (2)* **65**(3) (2002), 661–671.

[18] I. Łaba and I. Londner, 'Combinatorial and harmonic-analytic methods for integer tilings', Preprint, 2021, arXiv:2106.14042.

[19] I. Łaba and I. Londner, 'The Coven-Meyerowitz tiling conditions for 3 odd prime factors', Preprint, 2021, arXiv:2106.14044.

[20] T. Y. Lam and K. H. Leung, 'On vanishing sums of roots of unity', *J. Algebra* **224**(1) (2000), 91–109.

[21] N. Lev and M. Matolcsi, 'The Fuglede conjecture for convex domains is true in all dimensions', *to appear in Acta Mathematica*, Preprint, 2019, arXiv:1904.12262.

[22] S. L. Ma, 'Polynomial addition sets', Ph.D. thesis, University of Hong Kong, 1985.

[23] R. D. Malikosis and M. N. Kolountzakis, 'Fuglede's conjecture on cyclic groups of order $p^n q$', *Discrete Anal.* (2017), Paper No. 12.

[24] M. Matolcsi, 'Fuglede's conjecture fails in dimension 4', *Proc. Amer. Math. Soc.* **133**(10) (2005), 3021–3026.

[25] A. Pott, *Finite Geometry and Character Theory*, Lecture Notes in Mathematics, Vol. **1601** (Springer-Verlag, Berlin, 1995).

[26] L. Rédei, 'Ein Beitrag zum Problem der Faktorisation von endlichen Abelschen Gruppen', *Acta Math. Acad. Sci. Hungar.* **1** (1950), 197–207.

[27] L. Rédei, 'Über das Kreisteilungspolynom', *Acta Math. Acad. Sci. Hungar.* **5** (1954), 27–28.

[28] A. D. Sands, 'On Keller's conjecture for certain cyclic groups', *Proc. Edinburgh Math. Soc. (2)* **22**(1) (1979), 17–21.

[29] B. Schmidt, *Characters and Cyclotomic Fields in Finite Geometry*, Lecture Notes in Mathematics, Vol. **1797** (Springer-Verlag, Berlin, 2002).

[30] I. J. Schoenberg, 'A note on the cyclotomic polynomial', *Mathematika* **11** (1964), 131–136.

[31] R. Shi, 'Fuglede's conjecture holds on cyclic groups $\mathbb{Z}_{pqr}$', *Discrete Anal.* (2019), Paper No. 14.

[32] R. Shi, 'Equi-distributed property and spectral set conjecture on $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$', *J. Lond. Math. Soc. (2)* **102**(3) (2020), 1030–1046.

[33] G. Somlai, 'Spectral sets in $\mathbb{Z}_{p^2qr}$ tile', Preprint, 2019, arXiv:1907.04398.

[34] S. Szabó, 'A type of factorization of finite abelian groups', *Discrete Math.* **54**(1) (1985), 121–124.

[35] T. Tao, 'Fuglede's conjecture is false in 5 and higher dimensions', *Math. Res. Lett.* **11**(2–3) (2004), 251–258.

[36] R. Tijdeman, *Decomposition of the Integers as a Direct Sum of Two Subsets*, Number theory (Paris, 1992–1993), London Math. Soc. Lecture Note Ser., Vol. **215**, (Cambridge Univ. Press, Cambridge, 1995), 261–276.

[37] T. Zhang, 'Fuglede's conjecture holds in $\mathbb{Z}_p \times \mathbb{Z}_{p^n}$', Preprint, 2021, arXiv:2109.08400.