FORMAL DUALITY IN FINITE CYCLIC GROUPS

ROMANOS DIOGENES MALIKIOSIS

Abstract. The notion of formal duality in finite Abelian groups appeared recently in relation to spherical designs, tight sphere packings, and energy minimizing configurations in Euclidean spaces. For finite cyclic groups it is conjectured that there are no primitive formally dual pairs besides the trivial one and the TITO configuration. This conjecture has been verified for cyclic groups of prime power order, as well as of square-free order. In this paper, we will confirm the conjecture for other classes of cyclic groups, namely almost all cyclic groups of order a product of two prime powers, with finitely many exceptions for each pair of primes, or whose order N satisfies $p \parallel N$, where p a prime satisfying the so-called self-conjugacy property with respect to N. For the above proofs, various tools were needed: the *field descent method*, used chiefly for the circulant Hadamard conjecture, the techniques of Coven & Meyerowitz for sets that tile $\mathbb{Z}$ or $\mathbb{Z}_N$ by translations, dubbed herein as *the polynomial method*, as well as basic number theory of cyclotomic fields, especially the splitting of primes in a given cyclotomic extension.

1. Introduction

A fundamental problem in physics is the determination of ground states in a given space, with a fixed density of particles and a pair potential. These ground states are also called *minimal energy configurations*. A typical example is the equilibrium state of electrons in a shell of an atom. Problems of this sort are extremely difficult to solve rigorously; the minimal energy configuration of five points on a sphere is a notoriously difficult problem, having been determined for certain special cases for the potential function [22].

In the Euclidean space $\mathbb{R}^n$ periodic configurations of fixed density are studied, say $\rho = 1$; a set $\Lambda \subseteq \mathbb{R}^n$ is called *periodic* if it satisfies $\Lambda + L = \Lambda$ for some lattice L, and its period is $\rho(\Lambda) = N/\det(L)$, where $\det(L)$ is the volume of a fundamental parallelepiped of L. The lattice L is called the *period lattice* of Λ, and there always exists a maximal such lattice. The Gaussian potential function is considered in this case [2, 1], defined by $G_c(r) = e^{-\pi c r^2}$, $c \in \mathbb{R}$; this is the *Gaussian core model*. For a potential function f and a periodic set $\Lambda = \bigcup_{j=1}^{N}(t_j + L)$, the total energy of the system is

$$E_f(\Lambda) = \frac{1}{N}\sum_{i,j=1}^{N}\sum_{\substack{v\in L\\ v\neq 0 \text{ if } i=j}} f(|v + t_i - t_j|). \tag{1.1}$$

When the density ρ is very small, or when $f = G_c$ with $c \to \infty$, the optimal configuration approaches the optimal sphere packing [2, 1].

Apart from the 1-dimensional case, where the energy minimizing configuration of density 1 is $\mathbb{Z}$, there are no proofs that certain structured configurations minimize energy, however, there is strong numerical evidence towards certain patterns. In the study conducted in [2] for the Gaussian core model and varying densities, a remarkable sort of symmetry was revealed between optimal configurations in densities ρ and $1/\rho$, the so-called *formal duality*. In particular, when $n \leq 9$, the optimal configurations for densities ρ and $1/\rho$ are either dual lattices, or when they are not lattices, they are formally dual periodic sets. Formally dual sets satisfy a very strong property, namely a generalization of the Poisson summation formula. We note that in all of the above situations, the density is considered fixed. For systems in equilibrium without the fixed density restriction this task is even more difficult; we refer the reader to [6].

We remind that for a Schwartz function $f : \mathbb{R}^n \to \mathbb{C}$, and a lattice $\Lambda \subseteq \mathbb{R}^n$, the Poisson summation formula states that

$$\sum_{x\in\Lambda} f(x) = \frac{1}{\det(\Lambda)}\sum_{y\in\Lambda^\star}\hat{f}(y) \tag{1.2}$$

This research project is supported by Alexander von Humboldt Foundation.

where $\hat{f}$ denotes the Fourier transform of f, defined by

$$\hat{f}(y) = \int f(x) e^{-2\pi i \langle x,y \rangle} dx, \tag{1.3}$$

and $\Lambda^\star := \{x \in \mathbb{R}^n : \langle x, y\rangle \in \mathbb{Z}, \forall y \in \Lambda\}$ is the dual lattice of Λ; finally, $\det(\Lambda)$ is the volume of any fundamental parallelepiped of Λ, also known as the covolume of Λ. A consequence of this formula is the fact that a lattice Λ minimizes E_f among periodic configurations of density $\rho = 1/\det(\Lambda)$ if and only if $\Lambda^\star$ minimizes $E_{\hat{f}}$ among periodic configurations of density $1/\rho$. The significance of the Gaussian core model is then justified by the relation $\widehat{G}_c = c^{-n/2} G_{1/c}$ (in particular, $\widehat{G}_1 = G_1$).

It is known that (1.2) characterizes dual pairs of lattices [3] among discrete subsets of $\mathbb{R}^n$; consider the *average pair sum* for the periodic configuration $\Lambda = \bigcup_{j=1}^N (t_j + L)$

$$\Sigma_f(\Lambda) = \frac{1}{N} \sum_{i,j=1}^{N} \sum_{v \in L} f(|v + t_i - t_j|), \tag{1.4}$$

or simply put, $\sum_f(\Lambda) = f(0) + E_f(\Lambda)$. Another consequence of (1.2) is $\sum_f(\Lambda) = \rho(\Lambda) \sum_{\hat{f}}(\Lambda^\star)$ when Λ is a lattice (i.e. $N = 1$). Minimal energy periodic configurations for the Gaussian core model found in [2] at densities ρ and $1/\rho$, say Λ and Γ respectively, were proven to satisfy

$$\Sigma_f(\Lambda) = \rho(\Lambda) \Sigma_{\hat{f}}(\Gamma). \tag{1.5}$$

Definition 1.1. Two periodic sets $\Lambda, \Gamma \subseteq \mathbb{R}^n$ are called formally dual if they satisfy (1.5) for every Schwartz function f.

Formally dual pairs that are not lattices seem to appear in a great scarcity in the 1-dimensional case; the only known example is $2\mathbb{Z} \cup (2\mathbb{Z} + \frac{1}{2})$ (or a scaled version thereof), the so-called *TITO configuration*[1]. While there are more high dimensional examples of formal duality, they do not seem to appear yet in numerical computations; in the computations performed in [2] and Coulangeon-Schürmann[2] for $n \leq 9$, all optimal configurations are linear images of $\mathbb{Z}^n$, TITO$\times\mathbb{Z}^{n-1}$, or TITO$^2 \times \mathbb{Z}^{n-2}$. Thus, the characterization of all 1-dimensional formally dual sets is in order; it was conjectured in [1], that $\mathbb{Z}$ and TITO are the only discrete periodic subsets of $\mathbb{R}$ with density 1, possessing a formal dual set.

The above can be rephrased in terms of cyclic groups (for more details, see [1]). Let $\mathbb{Z}_N$ denote the cyclic groups of N elements, and call a subset $T \subseteq \mathbb{Z}_N$ *primitive*, if it is not contained in any proper coset of $\mathbb{Z}_N$. Then the aforementioned conjecture is equivalent to the following:

Conjecture 1.2. *The only primitive subsets of $\mathbb{Z}_N$ possessing a formal dual subset are $\{0\} \subseteq \mathbb{Z}/\mathbb{Z}$ and $\{0, 1\} \subseteq \mathbb{Z}_4$.*

This conjecture has been verified when N is a prime power, by Schüler [21] for p odd or when N an even power of 2, and by Xia, Park, and Cohn [27] in the remaining cases, as well as when N is square-free.

We briefly mention that there is an infinite family of primitive formally dual sets in non–cyclic groups, the *Gauss sum configurations*. The set $T = \left\{(n, n^2) : n \in \mathbb{Z}_p\right\} \subseteq \mathbb{Z}_p \times \mathbb{Z}_p$ is primitive formally self-dual [1]. This example has been generalized to the groups $\mathbb{Z}_{p^k} \times \mathbb{Z}_{p^k}$ [27]. It might not be coincidental that this is a *Sidon set* (see Exercise 2.2.7 in [23]); as we will see in the cyclic case, it seems that such sets can only exist if their sizes both equal $\sqrt{N}$, where N is the order of the group, and their sets of differences spread out in the group G. We prove in particular that when N is divisible by at most two primes, then every element in $\mathbb{Z}_N^\star$ (which consists of a large part of the group $\mathbb{Z}_N$) appears exactly once as difference of the form $t - t'$, where $t, t' \in T$ and $T \subseteq \mathbb{Z}_N$ primitive, possessing a formally dual set.

In this paper, we provide ample evidence towards the veracity of Conjecture 1.2. In particular, we prove that the conjecture is true when:

(1) $N = p^2 q^2$, for p, q distinct primes.
(2) $N = p^m q^n$, for p, q distinct primes, with possibly finitely many exceptions for each pair (p, q).
(3) A prime p divides *exactly* N, that is, $p \mid N$, but $p^2 \nmid N$, and p is *self-conjugate* mod$N$, i.e. there exists $j \in \mathbb{Z}$ such that $p^j \equiv -1 \bmod N$.

[1]TITO stands for two in-two out.

[2]Private communication.

We should note that tools from different areas were introduced in order to tackle these cases; for case (1), the ideas of Coven-Meyerowitz [4] for sets that tile $\mathbb{Z}$ by translations were used; for (2), the so-called *field descent method* was used, that was developed by Schmidt [18, 19] chiefly for the circulant Hadamard conjecture, as well as for applications in combinatorial designs and coding theory; for (3), the arithmetic of cyclotomic fields, especially the splitting of primes in cyclotomic extensions.

We will try to keep this paper as self-contained as possible; it is organized as follows: in Section 2, we provide the necessary number theoretic background to the problem. In Section 3, we develop the "polynomial method", and in Section 4 we prove basic results with respect to formal duality in cyclic groups. The field descent method is introduced in Section 5, and in Section 6, we re-prove the prime power case, showcasing the importance of the new ideas involved. In Section 7, we apply the field descent method, as well as the polynomial method and use them to prove the conjecture for products of two prime powers, except for finitely many cases for every pair (p, q). In Section 8, we prove the conjecture when $p \parallel N$ and p self–conjugate $\bmod N$. In the appendix we provide some numerical data for case (2) above that indicate how few exceptions for each pair (p, q) exist.

2. Basic number theoretic background

2.1. **Notation.** Throughout this paper, we will denote by $\mathbb{Z}_N$ the ring of integers modulo N, which as an additive group is cyclic of order N. We also denote $\zeta_N = e^{2\pi i/N}$, a primitive Nth root of unity. For a function $f : \mathbb{Z}_N \to \mathbb{C}$, the Fourier transform is defined as

$$\mathbf{F}f(y) = \hat{f}(y) = \sum_{x \in \mathbb{Z}_N} f(x)\zeta_N^{xy}.$$

For a set $T \subseteq \mathbb{Z}_N$ we denote by $\mathbf{1}_T$ its indicator function. Some usual arithmetic functions will be needed here: the number of distinct prime factors of N will be denoted by $\omega(N)$ and the product of the distinct prime factors of N as $\mathrm{rad}(N)$, which is also known as the *radical* of N. Then, we have the Möbius function $\mu(n)$, defined as

$$\mu(n) = \begin{cases} (-1)^{\omega(N)}, & \text{if } N \text{ is square–free} \\ 0, & \text{otherwise.} \end{cases}$$

We also set $\mathrm{Id}(N) = N$ and $\mathbf{1}(N) = 1$ for all N, and $e(N) = 1$ if $N = 1$, while $e(N) = 0$ otherwise. $\varphi(N)$ is the usual *Euler totient function*, which enumerates the positive integers prime to N that are $\leq N$. The following well-known formula holds

$$\varphi(N) = N \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right).$$

Finally, for a prime p we define $\nu_p(N)$ by $p^{\nu_p(N)} \parallel N$. The symbol $*$ will denote convolution, either additive or multiplicative (i.e. *Dirichlet convolution*), depending on the context. For the classical arithmetic functions, it will always be multiplicative; for example, the following formulae hold

$$\varphi = \mu * \mathrm{Id}, \quad \mathrm{Id} = \varphi * \mathbf{1},$$

an example of *Möbius inversion*. We also have $f * e = f$ for all f, that is e is the identity element with respect to the Dirichlet convolution, and $\mathbf{1} * \mu = e$, that is, μ is the inverse of $\mathbf{1}$. For these basic facts on arithmetic functions we refer the reader to [16], or any other book on basic number theory.

2.2. **Cyclotomic fields.** We list some of the basic results on cyclotomic fields, mainly the splitting of primes in cyclotomic extensions of $\mathbb{Q}$. For these basic facts we refer the reader to any of [11, 12, 25].

Cyclotomic fields have the form $\mathbb{Q}(\zeta_N)$; we remind that if $N \equiv 2 \bmod 4$ then $\mathbb{Q}(\zeta_N) = \mathbb{Q}(\zeta_{2N})$, which is also recovered from the fact that the degreee of the extension satisfies $[\mathbb{Q}(\zeta_N) : \mathbb{Q})] = \varphi(N)$. This extension is always an Abelian extension, that is, it is Galois with Abelian Galois group. In particular,

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong \mathbb{Z}_N^\star,$$

and the canonical group isomorphism is defined by $g \mapsto \sigma_g$ for every $g \in \mathbb{Z}_N^\star$, where $\sigma_g(\zeta_N) = \zeta_N^g$. The ring of integers of the field $\mathbb{Q}(\zeta_N)$ is $\mathbb{Z}[\zeta_N]$, and every ideal can be factorized uniquely into a product of prime ideals (which are also maximal, as algebraic number rings are Dedekind domains). The most

important fact for our purposes is the splitting of the ideal $p\mathbb{Z}[\zeta_N]$ into primes, where p is a (rational) prime.

Theorem 2.1. *Let N be a positive integer, p be a prime and m the p-free part of N, i.e. $N = p^a m$, where $p \nmid m$. Then*

$$p\mathbb{Z}[\zeta_N] = (\mathfrak{P}_1\mathfrak{P}_2\cdots\mathfrak{P}_r)^e,$$

where $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ distinct prime ideals of $\mathbb{Z}[\zeta_N]$, $e = \varphi(p^a)$ the ramification index, and $r = \varphi(m)/f$, where f is the multiplicative order of $p \bmod m$, that is, $p^f \equiv 1 \bmod m$ and f is the smallest positive integer with this property (also called the inertia degree). Furthermore, if we define $\kappa(\mathfrak{P}) = \mathbb{Z}[\zeta_N]/\mathfrak{P}$ (the residue field), so that $\kappa(p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$, we have $f = [\kappa(\mathfrak{P}_i) : \mathbb{Z}/p\mathbb{Z}]$, in other words, the inertia degree is the degree of the residue field extension.

Corollary 2.2. *With the previous notation, if $N = p^a$ (i.e. $m = 1$), then $r = f = 1$, and*

$$p\mathbb{Z}[\zeta_N] = \mathfrak{P}^{\varphi(N)}.$$

The ideal $\mathfrak{P}$ is principal, and is generated by $1 - \zeta$, where ζ is any primitive Nth root of unity.

The prime ideals $\mathfrak{P}_i$ are said to lie above p; the Galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ acts transitively on those. For $\mathfrak{P} \mid p$, the subgroup

$$G_{\mathfrak{P}} = \{\sigma \in G : \sigma\mathfrak{P} = \mathfrak{P}\}$$

is called the *decomposition group* of $\mathfrak{P}$. Since G is Abelian, $G_{\mathfrak{P}}$ is the same for all $\mathfrak{P} \mid p$ (in general, these groups are conjugate with each other).

Corollary 2.2 shows that $1 - \zeta$ is not a unit in $\mathbb{Z}[\zeta_N]$, when N is a power of a prime and ζ is a primitive Nth root of unity, otherwise $(1 - \zeta)\mathbb{Z}[\zeta_N] = \mathbb{Z}[\zeta_N]$. This can be seen by taking the value of the cyclotomic polynomial $\Phi_N(X)$ at $X = 1$:

$$\Phi_N(1) = \prod_{\gcd(g,N)=1} (1 - \zeta_N^g).$$

As

$$\Phi_N(1) = \begin{cases} p, & \text{if } N \text{ is a power of } p \\ 1, & \text{otherwise,} \end{cases} \tag{2.1}$$

we obtain the following Lemma.

Lemma 2.3. *Let ζ be a primitive Nth root of unity. $1 - \zeta$ is a unit in $\mathbb{Z}[\zeta_N]$ if and only if N is not a prime power.*

3. The polynomial method

With every multiset T with elements from G we associate an element of the group ring $\mathbb{Z}[G]$, namely $\sum_{g\in G} m_g g$, where m_g is the multiplicity of g in T. When G is cyclic, we can write instead $\sum_{g\in G} m_g X^g$, the so-called *mask polynomial*, which is an element of $\mathbb{Z}[X]/(X^N - 1) \cong \mathbb{Z}[G]$, where $N = |G|$. Both notations have appeared in bibliography before; see for example [9, 18, 19] for the group ring notation, or [4] for the mask polynomial. The former has been advantageous in algebraic coding theory, while the latter in tiling problems on $\mathbb{Z}$ or the finite cyclic groups, $\mathbb{Z}_N$ [10].

In this paper, we will adhere to the polynomial notation; the mask polynomial of the multiset T will be denoted simply by $T(X)$. Now let $d \mid n$, and define $d \cdot T$ to be the multiset of elements dt for $t \in T$, *counting multiplicities*. For example, if $T = \{0, 2\} \subseteq \mathbb{Z}_4$, then $2 \cdot T = \{0, 0\}$, i.e. 0 has multiplicity 2 in $2 \cdot T$. A fundamental observation is:

Proposition 3.1. *Let T be a multiset with elements from $\mathbb{Z}_N$ and $d \mid N$. Then, $T(X^d)$ is the mask polynomial of the multiset $d \cdot T$.*

Proof. Let $T(X) = \sum_{g\in\mathbb{Z}_N} m_g X^g$, where m_g is the multiplicity of g, as before. Then,

$$T(X^d) \equiv \sum_{g\in\mathbb{Z}_N} m_g X^{dg} \equiv \sum_{h\in\mathbb{Z}_N} \Bigg(\sum_{dg\equiv h \bmod N} m_g \Bigg) X^h \bmod (X^N - 1)$$

proving the desired fact. □

Formal duality induces polynomial congruences mod$X^N - 1$, as we will see in the next section. The following Lemma is then used to show that such a congruence cannot hold, as the values of the derivatives of the polynomials under question on roots of unity do not agree, thus proving the non-existence of primitive formally dual sets.

Lemma 3.2. *Let $P(X), Q(X) \in \mathbb{Z}[X]$ such that $P(X) \equiv Q(X) \bmod (X^N - 1)$, where N is a positive integer. Then, for every Nth root of unity ζ (not necessarily primitive) we have $P(\zeta) = Q(\zeta)$ and $P'(\zeta) \equiv Q'(\zeta) \bmod N\mathbb{Z}[\zeta_N]$.*

Proof. This almost follows from definition; let $R(X) \in \mathbb{Z}[X]$ be such that $P(X) - Q(X) = (X^N - 1)R(X)$. From this, we readily have $P(\zeta) = Q(\zeta)$, when $\zeta^N = 1$. Differentiating both sides, we obtain $P'(X) - Q'(X) = (X^N - 1)R(X) + NX^{N-1}R'(X)$, so substituting $X = \zeta$ gives $P'(\zeta) \equiv Q'(\zeta) \bmod N\mathbb{Z}[\zeta_N]$. □

The following polynomials will appear a lot in the sequel.

Proposition 3.3. *Let $d \mid N$ be positive integers. Consider the function*

$$F(X) = \sum_{k=0}^{N/d-1} X^{dk},$$

which we will also write formally as $\frac{X^N-1}{X^d-1}$, even at points where $X^d - 1 = 0$. Then,

$$F'(\zeta) \equiv \begin{cases} 0 \bmod N\mathbb{Z}[\zeta_N], & \text{if } \zeta^d = 1 \text{ and } N/d \text{ is odd,} \\ \frac{N}{2}\zeta^{-1} \bmod N\mathbb{Z}[\zeta_N], & \text{if } \zeta^d = 1 \text{ and } N/d \text{ is even} \\ \frac{N\zeta^{-1}}{\zeta^d-1} \bmod N\mathbb{Z}[\zeta_N], & \text{otherwise.} \end{cases}$$

Proof. Obviously

$$F'(X) = d \sum_{k=1}^{N/d-1} kX^{dk-1},$$

hence for $\zeta^d = 1$,

$$F'(\zeta) = d\zeta^{-1}\frac{1}{2} \cdot \frac{N}{d}\left(\frac{N}{d} - 1\right) = \zeta^{-1}\frac{N}{2}\left(\frac{N}{d} - 1\right),$$

and the result follows easily when $\zeta^d = 1$. In all other cases, we use

$$F'(X) = \left(\frac{X^N - 1}{X^d - 1}\right)' = -\frac{dX^{d-1}(X^N - 1)}{(X^d - 1)^2} + \frac{NX^{N-1}}{X^d - 1},$$

whence the case $\zeta^d \neq 1$, $\zeta^N = 1$, follows. □

The mask polynomial of $\mathbb{Z}_N^\star$ will be denoted by $R_N(X)$, and appears prominently in the polynomial congruences induced by formal duality. By definition,

$$R_N(X) = \sum_{\substack{1 \le g \le N \\ \gcd(g,N)=1}} X^g,$$

and the values of R_N at Nth roots of unity are the *Ramanujan sums*, denoted by

$$C_N(d) = R_N(\zeta_N^d).$$

As Ramanujan proved [13] (see also [7]), these sums are integers, and their values are given by the following formula

$$C_N(d) = \sum_{g \mid \gcd(d,N)} \mu(\frac{N}{g})g. \tag{3.1}$$

These sums will appear a lot when we apply Proposition 4.3, so we will also need the following [7] (d, N are integers).

$$C_N(d) = \mu\left(\frac{N}{\gcd(d,N)}\right)\frac{\varphi(N)}{\varphi\left(\frac{N}{\gcd(d,N)}\right)}. \tag{3.2}$$

Lemma 3.4. *Consider the polynomial $R_N(X)$, the mask polynomial of $\mathbb{Z}_N^\star$. Let $d \mid N$ and ζ a primitive dth root of unity. Then*

$$R'_N(\zeta) \equiv N\zeta^{-1} \sum_{g|N, d\nmid g} \frac{\mu(g)}{\zeta^g - 1} \bmod N\mathbb{Z}[\zeta_N], \tag{3.3}$$

unless $4 \mid N$ and $d = \mathrm{rad}(N)$ or $2 \parallel N$ and $d = \mathrm{rad}(\frac{N}{2})$, in which cases

$$R'_N(\zeta) \equiv N\zeta^{-1} \left[\frac{1}{2} + \sum_{g|N, d\nmid g} \frac{\mu(g)}{\zeta^g - 1} \right] \bmod N\mathbb{Z}[\zeta_N] \tag{3.4}$$

holds.

Proof. The polynomial $R_N(X)$ is a sum of polynomials of the same form as $F(X)$ in Proposition 3.3, for various $d \mid N$. In particular, we may formally write

$$R_N(X) = \sum_{g|N} \mu(g) \frac{X^N - 1}{X^g - 1}.$$

Let $d \mid N$ and $\zeta^d = 1$. Assume first that N is odd; if $d \mid g$, then also $\zeta^g = 1$ and the derivative of $\frac{X^N-1}{X^g-1}$ at $X = \zeta$ is 0 by Proposition 3.3, so the only terms that will appear in $R'_N(\zeta)$ are those satisfying $d \nmid g$, proving that (3.3) holds.

Next, assume that N is even. Again, by Proposition 3.3 the contribution of the terms satisfying $d \nmid g$ to $R'_N(\zeta)$ is precisely $\mu(g)\frac{N\zeta^{-1}}{X^g-1} \bmod N\mathbb{Z}[\zeta_N]$. So, assume that $d \mid g$, so that $\zeta^g = 1$; without loss of generality, both d and g are square–free, otherwise $\mu(g) = 0$ and the contribution is also 0 anyway. If $4|N$, then N/g is always even for every square–free g, so if $d \neq \mathrm{rad}(N)$ there is precisely an even number of square–free $g \mid N$ for which $d \mid g$ (equal to the number of divisors of $\frac{\mathrm{rad}(N)}{d}$ when $d \mid \mathrm{rad}(N)$ and 0 otherwise), hence their total contribution to $R'_N(\zeta)$ is 0 by Proposition 3.3 and (3.3) holds. If, on the other hand, $d = \mathrm{rad}(N)$, there is only one such contribution of the form $\frac{N}{2}\zeta^{-1} \bmod N\mathbb{Z}[\zeta_N]$ by Proposition 3.3 (namely, from $g = \mathrm{rad}(N)$), hence (3.4) holds. If $2 \mid N$ and the square–free $g \mid N$ is even, then the contribution is 0 to $R'_N(\zeta)$ by Proposition 3.3. So, let g be odd with $d \mid g$. Unless $d = \mathrm{rad}(\frac{N}{2})$, there is an even number of odd square–free divisors g divisible by d, so their total contribution is 0 and (3.3) holds. When $d = \mathrm{rad}(\frac{N}{2})$, the only contribution of $\frac{N}{2}\zeta^{-1} \bmod \mathbb{Z}[\zeta_N]$ comes from $g = d$, hence (3.4) holds, concluding the proof. □

Corollary 3.5. *Let $H(X) = R_{N/d}(X^d)$, where $d \mid N$. Then, if $\zeta^N = 1$*

$$H'(\zeta) \equiv N\zeta^{-1} \left[\frac{\varepsilon}{2} + \sum_{g|N, \delta\nmid g} \frac{\mu(g)}{\zeta^{dg-1}} \right] \bmod N\mathbb{Z}[\zeta_N]$$

holds, where ζ^d is a primitive δth root of unity, and

$$\varepsilon = \begin{cases} 1, & \text{if } 4 \mid \frac{N}{d} \text{ and } \delta = \mathrm{rad}(N/d) \text{ or } 2 \parallel \frac{N}{d} \text{ and } \delta = \mathrm{rad}(N/2d) \\ 0, & \text{otherwise.} \end{cases}$$

When $T(X)$ vanishes on a certain Nth root of unity, we get some information about the structure of $T \subseteq \mathbb{Z}_N$. This follows from a theorem on the vanishing sums of roots of unity, independently proven by Rédei [14, 15], de Bruijn [5] and Schoenberg [20]. When we consider vanishing sums of Nth roots of unity where N has at most two prime divisors (which are most of the cases that we consider in this paper), there is a stronger result by Lam and Leung [8]. We summarize this in the following theorem.

Theorem 3.6. *Suppose that $\sum_{j=0}^{N-1} c_j \zeta_N^j = 0$ for some integers c_j, $0 \leq j \leq N-1$. If we consider ζ_N formally as an element of $\mathbb{Z}[G]$, where $G = \langle \zeta_N \rangle$, then $\sum_{j=0}^{N-1} c_j \zeta_N^j$ is equal to an integer linear combination of terms of the form*

$$\zeta_N^k (1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1}), \tag{3.5}$$

for p prime divisor of N and k integer (these terms are called p-cycles). If N has at most two distinct prime divisors and $c_j \geq 0$ for all j, then we can write $\sum_{j=0}^{N-1} c_j \zeta_N^j$ as a nonnegative linear combination of terms such as the above.

The second part of this theorem does not hold when N has at least three distinct prime divisors, as is evident from the example

$$(\zeta_p + \cdots + \zeta_p^{p-1})(\zeta_q + \cdots + \zeta_q^{q-1}) + (\zeta_r + \cdots + \zeta_r^{r-1}) = (-1)(-1) + (-1) = 0,$$

which cannot be written as a nonnegative linear combination of p-, q- or r-cycles [8].

Expressed with the polynomial notation, Theorem 3.6 gives the results below; in the two prime case we include an additional fact that will be useful for our purposes (see also [10]):

Theorem 3.7. *Let $T \subseteq \mathbb{Z}_N$, such that $T(\zeta_N^d) = 0$ for some $d \mid N$, where $p_1, \ldots, p_k$ are the distinct prime divisors of N. Then*

$$T(X^d) \equiv \sum_{j=1}^{k} P_j(X^d)\Phi_N(X^{N/p_j}) \bmod (X^N - 1),$$

for some $P_j \in \mathbb{Z}[X]$.

Proof. We simply remark that $X^k\Phi_p(X^{N/p})$ is the mask polynomial that corresponds to the term in (3.5) under the canonical ring isomorphism $\mathbb{Z}[X]/(X^N - 1) \cong \mathbb{Z}[G]$ with $G = \langle \zeta_N \rangle$, which identifies X with ζ_N. The rest follows from Theorem 3.6. □

We emphasize that the polynomials P_j are not unique.list some basic facts about cyclotomic fields

Theorem 3.8. *Let $T \subseteq \mathbb{Z}_N$, such that $T(\zeta_N^d) = 0$ for some $d \mid N$, and N/d has at most two distinct prime divisors, say p, q. Then,*

$$T(X^d) \equiv P(X^d)\Phi_p(X^{N/p}) + Q(X^d)\Phi_q(X^{N/q}) \bmod (X^N - 1). \tag{3.6}$$

The polynomials $P, Q \in \mathbb{Z}[X]$ can be taken with nonnegative coefficients. If for some integer $a > 0$ we have $dp^a \mid N$ (resp. $dq^a \mid N$) and $T(\zeta_N^{dp^a}) \neq 0$ (resp. $T(\zeta_N^{dq^a}) \neq 0$), then $P \not\equiv 0$ (resp. $Q \not\equiv 0$) for any selection of Q (resp. P).

Proof. The nonnegativity of P and Q follows from the second part of Theorem 3.6. If $T(X^{dp^a}) \neq 0$, then replacing X by X^{p^a} we obtain

$$T(X^{dp^a}) \equiv pP(X^{dp^a}) + Q(X^{dp^a})\Phi_q(X^{N/q}) \bmod (X^N - 1),$$

and substituting X by ζ_N, $T(\zeta_N^{dp^a}) = pP(\zeta_N^{dp^a}) \neq 0$, therefore $P \not\equiv 0$, as desired. □

If N/d is only divided by one prime factor, p, it is understood $Q \equiv 0$ at (3.6).

4. Structural results on formal duality

Between G, a finite Abelian group, and its dual $\hat{G}$ there is a natural isomorphism; we will denote the image of $y \in G$ under this map by χ_y. With this notation, we have:

Definition 4.1. The sets $S, T \subseteq G$ are formally dual if they satisfy

$$\left| \frac{1}{|S|} \sum_{x \in S} \chi_y(x) \right|^2 = \frac{1}{|T|} \nu_T(y), \tag{4.1}$$

for every $y \in G$, where ν_T is the *weight enumerator* of T, defined by

$$\nu_T(y) = \#\big\{(t, t') \in T \times T : t - t' = y\big\}.$$

Under the notation introduced in Section 2, we observe that we can rewrite the weight enumerator function simply as a convolution:

$$\nu_T(y) = \mathbf{1}_T * \mathbf{1}_{-T}(y). \tag{4.2}$$

We will use the explicit isomorphism between $\mathbb{Z}_N$ and $\widehat{\mathbb{Z}}_N$ given by $\chi_y(x) = \zeta_N^{xy}$, for all $x, y, \in \mathbb{Z}_N$. Then, the left hand side of (4.1), can be written as

$$\frac{1}{|S|^2} \Big| \sum_{x \in S} \zeta_N^{xy} \Big|^2 = \frac{1}{|S|^2} |S(\zeta_N^y)|^2,$$

so we can rewrite (4.1) as

$$\frac{1}{|S|^2}|S(\zeta_N^y)|^2 = \frac{1}{|T|}\mathbf{1}_T * \mathbf{1}_{-T}(y). \tag{4.3}$$

Furthermore, there is an obvious connection between the mask polynomial of S and the Fourier transform of $\mathbf{1}_S$, namely

$$\hat{\mathbf{1}}_S(y) = S(\zeta_N^y).$$

The operator $\frac{1}{\sqrt{N}}\mathbf{F}$ is unitary, so Parseval's identity is

$$N\sum_{x=1}^{N}|f(x)|^2 = \sum_{y=1}^{N}|\hat{f}(y)|^2, \tag{4.4}$$

and we have $\widehat{f * g} = \hat{f}\hat{g}$, therefore,

$$|S(\zeta_N^y)|^2 = |\hat{\mathbf{1}}_S(y)|^2 = \hat{\mathbf{1}}_S(y)\hat{\mathbf{1}}_{-S}(y) = \widehat{\mathbf{1}_S * \mathbf{1}_{-S}}(y), \tag{4.5}$$

so (4.1) can be written as

$$\frac{1}{|S|^2}|\hat{\mathbf{1}}_S(y)|^2 = \frac{1}{|T|}\mathbf{1}_T * \mathbf{1}_{-T}(y). \tag{4.6}$$

Summing over $y \in \mathbb{Z}_N$ and applying (4.4), we obtain

$$\frac{N}{|S|^2}\sum_{y\in\mathbb{Z}_N}|\mathbf{1}_S(y)|^2 = \frac{N}{|S|} = |T|,$$

proving a fact already known [1, 21].

Proposition 4.2. *Let $T, S \subseteq \mathbb{Z}_N$ be formally dual. Then $N = |S| \cdot |T|$.*

(4.1) can also be written as

$$\frac{\widehat{\mathbf{1}_S * \mathbf{1}_{-S}}(y)}{|S|^2} = \frac{\mathbf{1}_T * \mathbf{1}_{-T}(y)}{|T|}. \tag{4.7}$$

$\frac{1}{N}\mathbf{F}^2$ fixes all even functions, therefore by Fourier inversion we get

$$\frac{N\mathbf{1}_S * \mathbf{1}_{-S}(y)}{|S|^2} = \frac{\widehat{\mathbf{1}_T * \mathbf{1}_{-T}}(y)}{|T|} \iff \frac{\mathbf{1}_S * \mathbf{1}_{-S}(y)}{|S|} = \frac{\widehat{\mathbf{1}_T * \mathbf{1}_{-T}}(y)}{|T|^2},$$

confirming that the definition of formal duality is indeed *dual* with respect to S, T, as expected.

Proposition 4.3. *Let $T, S \subseteq \mathbb{Z}_N$ be formally dual subsets. Then, the values of $\mathbf{1}_T * \mathbf{1}_{-T}$ are fixed within a divisor class, and $|T(\zeta_N^d)|^2 \in \mathbb{Z}$ for every integer d. Also, the mask polynomial of $T - T$ as a multiset is $\equiv T(X)T(X^{-1}) \bmod (X^N - 1)$, where it is understood that $X^{-1} \equiv X^{N-1} \bmod (X^N - 1)$, hence*

$$\begin{aligned} T(X)T(X^{-1}) &\equiv \sum_{d|N}\mathbf{1}_T * \mathbf{1}_{-T}(d)R_{N/d}(X^d) \bmod (X^N - 1) \\ &\equiv \frac{|T|}{|S|^2}\sum_{d|N}|S(\zeta_N^d)|^2 R_{N/d}(X^d) \bmod (X^N - 1). \end{aligned}$$

Proof. Let $y \in \mathbb{Z}_N$ be arbitrary, and let $g \in \mathbb{Z}_N^\star$. Consider $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ such that $\sigma(\zeta_N) = \zeta_N^g$. The right hand side of (4.3) is a rational number, hence invariant under the action of σ; the left hand side though, becomes

$$\frac{1}{|S|^2}|S(\zeta_N^{gy})|^2 = \frac{1}{|T|}\mathbf{1}_T * \mathbf{1}_{-T}(gy),$$

which gives

$$\mathbf{1}_T * \mathbf{1}_{-T}(y) = \mathbf{1}_T * \mathbf{1}_{-T}(gy),$$

for all $y \in \mathbb{Z}_N$, $g \in \mathbb{Z}_N^\star$, proving the first part. Next, by (4.3) we obtain

$$|T(\zeta_N^d)|^2 = \frac{|T|^2}{|S|}\mathbf{1}_S * \mathbf{1}_{-S}(d),$$

for every d. The left hand side is in $\mathbb{Z}[\zeta_N]$, while the right hand side in $\mathbb{Q}$, whence $|T(\zeta_N^d)|^2 \in \mathbb{Z}$ for all d (similarly for S).

The next part follows from the fact that $T(X^{-1})$ is the mask polynomial of $-T$, and if $A(X)$, $B(X)$ are the mask polynomials of the multisets A, B, then $A(X)B(X)$ is the mask polynomial of the sumset $A+B$ (*counting multiplicities*). Furthermore, the coefficients of the mask polynomial of the multiset $T-T$ are precisely the values of $\mathbf{1}_T * \mathbf{1}_{-T}$, which yields

$$\begin{aligned} T(X)T(X^{-1}) &\equiv \sum_{t=0}^{N-1} \mathbf{1}_T * \mathbf{1}_{-T}(t)X^t \equiv \sum_{d|N} \mathbf{1}_T * \mathbf{1}_{-T}(d)R_{N/d}(X^d) \equiv \\ &\equiv \frac{|T|}{|S|^2} \sum_{d|N} |S(\zeta_N^d)|^2 R_{N/d}(X^d) \bmod (X^N-1), \end{aligned}$$

completing the proof. □

For any $T \subseteq \mathbb{Z}_N$ and $d \mid N$, $0 \le j \le d-1$, we define

$$T_{j,d} := \{t \in T : t \equiv j \bmod d\}.$$

Proposition 4.4. *The following holds for a primitive $T \subseteq \mathbb{Z}_N$ possessing a formal dual:*

$$\mathbf{1}_T * \mathbf{1}_{-T}(1)R_N(X) \equiv \sum_{d|N} \mu(d) \sum_{j=0}^{d-1} T_{j,d}(X)T_{j,d}(X^{-1}) \bmod (X^N-1).$$

Proof. Consider the following union of *multisets*:

$$\bigcup_{\substack{0 \le i,j \le \mathrm{rad}(N)-1 \\ \gcd(N,i-j)=1}} (T_{i,\mathrm{rad}(N)} - T_{j,\mathrm{rad}(N)}).$$

By definition, this is precisely the set $\mathbb{Z}_N^\star$, where every element appears with the same multiplicity, i.e. $\mathbf{1}_T * \mathbf{1}_{-T}(1)$, hence its mask polynomial is

$$\mathbf{1}_T * \mathbf{1}_{-T}(1)R_N(X).$$

On the other hand, we have

$$\sum_{d|N} \mu(d) \sum_{j=0}^{d-1} T_{j,d}(X)T_{j,d}(X^{-1}) \equiv \sum_{n=0}^{N-1} \sum_{d|N} \mu(d) \sum_{j=0}^{d-1} \mathbf{1}_{T_{j,d}} * \mathbf{1}_{-T_{j,d}}(n)X^n \bmod (X^N-1),$$

so we will compare coefficients between the latter polynomial and $\mathbf{1}_T * \mathbf{1}_{-T}(1)R_N(X)$. The coefficient of X^n in $\sum_{n=0}^{N-1} \sum_{d|N} \mu(d) \sum_{j=0}^{d-1} \mathbf{1}_{T_{j,d}} * \mathbf{1}_{-T_{j,d}}(n)X^n$ is simply

$$\sum_{d|N} \mu(d) \sum_{j=0}^{d-1} \mathbf{1}_{T_{j,d}} * \mathbf{1}_{-T_{j,d}}(n). \tag{4.8}$$

The term $\mathbf{1}_{T_{j,d}} * \mathbf{1}_{-T_{j,d}}(n)$ counts the number of pairs $(t,t') \in T_{j,d} \times T_{j,d}$ that satisfy $t-t'=n$. If $\gcd(n,N)=1$, t and t' cannot belong to the same set $T_{j,d}$, for every $d>1$, $0 \le j \le d-1$; therefore the only contribution comes from the term $\mathbf{1}_T * \mathbf{1}_{-T}(n) = \mathbf{1}_T * \mathbf{1}_{-T}(1)$, which is the same as the coefficient of X^n in $\mathbf{1}_T * \mathbf{1}_{-T}(1)R_N(X)$. If $\gcd(n,N)>1$, then the contribution of a specific pair $(t,t') \in T \times T$ with $t-t'=n$ in (4.8) is $\sum_{d|t-t'} \mu(d) = 0$, which shows that both coefficients must be equal to 0 in this case, completing the proof. □

Lemma 4.5. *Let T, S be formally dual subsets of $\mathbb{Z}_N$. Then, for every $d \mid N$ we have*

$$\frac{1}{\sqrt{d}|T|^{3/2}} \sum_{e|d} \mu(\tfrac{d}{e})|T(\zeta_N^e)|^2 = \frac{1}{\sqrt{N/d}|S|^{3/2}} \sum_{\delta|\frac{N}{d}} \mu(\tfrac{N/d}{\delta})|S(\zeta_N^\delta)|^2.$$

Proof. By Proposition 4.3, we get

$$|T(\zeta_N^e)|^2 = \frac{|T|}{|S|^2} \sum_{\delta|N} |S(\zeta_N^\delta)|^2 C_{N/\delta}(e) = \frac{|T|}{|S|^2} \sum_{\delta|N} |S(\zeta_N^\delta)|^2 \sum_{g|\gcd(e,N/\delta)} g\mu(\frac{N/\delta}{g}).$$

Hence,

$$\sum_{e|d}\mu(\frac{d}{e})|T(\zeta_N^e)|^2=\frac{|T|}{|S|^2}\sum_{\delta|N}|S(\zeta_N^\delta)|^2\sum_{\substack{e|d\\ g|\gcd(e,N/\delta)}}g\mu(d/e)\mu(\frac{N/\delta}{g}). \tag{4.9}$$

The inner sum is equal to

$$\sum_{g|\gcd(d,N/\delta)}g\mu(\frac{N/\delta}{g})\sum_{g|e|d}\mu(d/e)=\sum_{g|\gcd(d,N/\delta)}g\mu(\frac{N/\delta}{g})\sum_{e'|\frac{d}{g}}\mu(\frac{d/g}{e'}).$$

The latter sum is nonzero, precisely when $g=d$ and $d\mid\frac{N}{\delta}$; in that case it's equal to $d\mu(\frac{N/d}{\delta})$. Substituting into (4.9) we obtain

$$\sum_{e|d}\mu(\frac{d}{e})|T(\zeta_N^e)|^2=\frac{d|T|}{|S|^2}\sum_{\delta|\frac{N}{\delta}}\mu(\frac{N/d}{\delta})|S(\zeta_N^\delta)|^2,$$

and the proof is completed by dividing both sides by $\sqrt{d}|T|^{3/2}$. □

Next, we restrict our attention to *primitive* subsets of $\mathbb{Z}_N$, that is, subsets that are not contained in a coset of a proper subgroup. We remark that if we remove this restriction, there are trivial pairs of formal duals given by $H<\mathbb{Z}_N$ and $H^\perp$, its orthogonal subgroup (which is isomorphic to the group of characters that vanish on H). However, these examples come from dual lattices in Euclidean spaces, so we gain no new information with regards to formal duality there. Furthermore, if T is not primitive, we can always reduce this situation to a primitive formally dual pair in $\mathbb{Z}_M$, where $M\mid N$ [1].

Proposition 4.6. *Let $T\subseteq\mathbb{Z}_N$ be primitive. Then, for every $\zeta\neq 1$, $\zeta^N=1$, we have*

$$|T(\zeta)|<|T|.$$

Proof. Assume otherwise, that $|T(\zeta)|^2=|T|^2$, where ζ is a primitive dth root of unity. As T is primitive, there are at least two integers j,k with $j\not\equiv k \bmod d$, such that $T_{j,d}$ and $T_{k,d}$ are nonempty. Then,

$$|T(\zeta)|=\left|\sum_{i=0}^{d-1}T_{i,d}\zeta^i\right|\leq|T_{j,d}\zeta^j+T_{k,d}\zeta^k|+\sum_{\substack{0\leq i\leq d-1\\ j,k\not\equiv i \bmod d}}|T_{i,d}|<\sum_{i=0}^{d-1}|T_{i,d}|=|T|,$$

as $|T_{j,d}\zeta^j+T_{k,d}\zeta^k|<|T_{j,d}|+|T_{k,d}|$; equality could only hold if $|T_{j,d}|\zeta^j=\lambda|T_{k,d}|\zeta^k$ for some $\lambda>0$, however, this is impossible. □

Lemma 4.5 provides the following estimate on $\mathbf{1}_T*\mathbf{1}_{-T}(1)$.

Corollary 4.7. *Let T, S be primitive formally dual subsets of $\mathbb{Z}_N$. Then,*

$$\mathbf{1}_T*\mathbf{1}_{-T}(1)\leq\frac{2^{\omega(N)-1}|T|^2}{N},$$

and similarly for S. Equality can only hold when $\omega(N)=1$ and $T(\zeta_p)=0$. Furthermore, if $|T|\leq|S|$ and $\mathbf{1}_T*\mathbf{1}_{-T}(1)\neq 0$ (or equivalently, $S(\zeta_N)\neq 0$), the following inequalities hold:

$$\sqrt{\frac{N}{2^{\omega(N)-1}}}\leq|T|\leq\sqrt{N}\leq|S|\leq\sqrt{2^{\omega(N)-1}N},$$

where again the leftmost and rightmost inequalities are equalities precisely when $\omega(N)=1$, $T(\zeta_p)=0$ and $\mathbf{1}_T*\mathbf{1}_{-T}(1)=1$.

Proof. We apply Lemma 4.5 for $d=N$:

$$\frac{1}{|S|^{3/2}}|S(\zeta_N)|^2=\frac{1}{\sqrt{N}|T|^{3/2}}\sum_{e|N}\mu(N/e)|T(\zeta_N^e)|^2\leq\frac{2^{\omega(N)-1}|T|^2}{\sqrt{N}|T|^{3/2}},$$

by Proposition 4.6, where equality could only hold if $\omega(N)=1$ and $T(\zeta_p)=0$. By (4.3), the left hand side is equal to

$$\frac{|S|^{3/2}}{N}\mathbf{1}_T*\mathbf{1}_{-T}(1),$$

whence

$$\mathbf{1}_T * \mathbf{1}_{-T}(1) \leq \frac{2^{\omega(N)-1}N|T|^2}{\sqrt{N}|S|^{3/2}|T|^{3/2}} = \frac{2^{\omega(N)-1}|T|^2}{N},$$

as desired. Solving this inequality for $|T|$ and then using $N = |S| \cdot |T|$ by Proposition 4.2, we get the final inequalities. □

The above estimate is not always the best we can achieve; we will close this section with another estimate which most of the times is better.

Lemma 4.8. *Let T, S be primitive formally dual subsets of $\mathbb{Z}_N$. Then*

$$\mathbf{1}_T * \mathbf{1}_{-T}(1) \leq \frac{|T|^2 - |T|}{\varphi(N)} < \frac{|T|^2}{\varphi(N)}, \tag{4.10}$$

and similarly for S. Furthermore, if $|T| \leq |S|$ and $\mathbf{1}_T * \mathbf{1}_{-T}(1) \neq 0$ (or equivalently, $S(\zeta_N) \neq 0$), the following inequalities hold:

$$\sqrt{\varphi(N)} < |T| \leq \sqrt{N} \leq |S| < \frac{N}{\sqrt{\varphi(N)}}. \tag{4.11}$$

The middle equalities can only hold when N is a square.

Proof. The number of nonzero differences between elements of T are precisely $|T|^2 - |T|$ (counting multiplicities). If $\mathbf{1}_T * \mathbf{1}_{-T}(1) \neq 0$, this means that every element of $\mathbb{Z}_N^\star$ appears at least once in $T - T$, yielding (4.10) (if $\mathbf{1}_T * \mathbf{1}_{-T}(1) = 0$, it is trivial). From $|T| \leq |S|$ and (4.10) we easily obtain (4.11). □

Now we compare the inequalities from Corollary 4.7 and Lemma 4.8. Suppose that $\omega(N) \geq 3$, that is N has at least three distinct prime factors. Then,

$$\frac{|T|^2}{\varphi(N)} = \frac{|T|^2}{N} \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)^{-1} \leq \frac{|T|^2}{N} \cdot 2 \cdot \frac{3}{2} \cdot \left(\frac{5}{4}\right)^{\omega(N)-2} < \frac{2^{\omega(N)-1}|T|^2}{N},$$

as $(8/5)^k > 3/2$ for all $k \geq 1$, so Lemma 4.8 provides a better bound. The same holds when $\omega(N) = 2$ and N is odd, as

$$\frac{|T|^2}{\varphi(N)} \leq \frac{|T|^2}{N}\frac{3 \cdot 5}{2 \cdot 4} < \frac{2|T|^2}{N},$$

but at all other cases, Corollary 4.7 gives better bounds. Indeed, if $\omega(N) = 1$, then obviously

$$\frac{|T|^2}{N} < \frac{|T|^2}{\varphi(N)},$$

while if $\omega(N) = 2$ and N even, we obtain

$$\frac{2|T|^2}{N} = \frac{2|T|^2}{\varphi(N)}\frac{p-1}{2p} < \frac{|T|^2}{\varphi(N)},$$

where p the unique odd prime dividing N.

5. The field descent method

We mention the main tools from the *field descent method*, developed in [9, 18, 19]. The question that was addressed by this method is the following: under which circumstances can we have $X \in \mathbb{Z}[\zeta_N]$, such that $|X|^2 = n \in \mathbb{Z}$? First, we need the definition below, before we pass to the main theorems of the field descent method.

Definition 5.1 (Definition 2.6 [9])**.** Let $m, n > 1$ integers. $\mathscr{D}(t)$ denotes the set of prime divisors of an integer t. For $q \in \mathscr{D}(n)$ let

$$m_q := \begin{cases} \prod_{p \in \mathscr{D}(m) \setminus \{q\}} p, & \text{if } m \text{ is odd or } q = 2 \\ 4\prod_{p \in \mathscr{D}(m) \setminus \{2,q\}} p, & \text{otherwise.} \end{cases}$$

Set

$$\begin{aligned} b(2,m,n) = &\quad \max_{q\in\mathscr{D}(n)\setminus\{2\}}\left\{\nu_2(q^2-1)+\nu_2(\mathrm{ord}_{m_q}(q))-1\right\}\\ b(r,m,n) = &\quad \max_{q\in\mathscr{D}(n)\setminus\{r\}}\left\{\nu_r(q^{r-1}-1)+\nu_r(\mathrm{ord}_{m_q}(q))\right\}\end{aligned}$$

for any prime $r>2$ with the convention that $b(2,m,n)=2$ if $\mathscr{D}(n)=\{2\}$ and $b(r,m,n)=1$ if $\mathscr{D}(n)=\{r\}$. We define

$$F(m,n):=\gcd(m,\prod_{p\in\mathscr{D}(m)}p^{b(p,m,n)}).$$

Theorem 5.2 ([18, 19])**.** *Let $A\in\mathbb{Z}[\zeta_m]$, such that $|A|^2=n$. Then, A belongs to a smaller cyclotomic field up to multiplication by a root of unity, that is*

$$A\in\zeta_m^j\mathbb{Z}[\zeta_{F(m,n)}].$$

Theorem 5.3 ([19])**.** *Let $X\in\mathbb{Z}[\zeta_m]$ be of the form*

$$X=\sum_{i=0}^{m-1}a_i\zeta_m^i$$

with $0\le a_i\le C$ for some constant C and assume that $n=|X|^2$ is an integer. Then

$$n\le\frac{C^2F(m,n)^2}{4\varphi(F(m,n))}.$$

The definition of $F(m,n)$ seems technical, so we need the Proposition below in order to shed some light on it; see also [9].

Proposition 5.4. *The number $F(m,n)$ has the following properties.*

(1) $F(m,n)$ divides m.
(2) $\mathrm{rad}(m)=\mathrm{rad}(F(m,n))$.
(3) $F(m,n)=F(m,\mathrm{rad}(n))$, i.e., if we fix m, $F(m,n)$ depends only on the prime divisors of n.
(4) For every finite set of primes P, there is an explicitly computable constant $C(P)$, such that $F(m,n)\le C(P)$ whenever $\mathscr{D}(m),\mathscr{D}(n)\subseteq P$ (Proposition 2.2.7 [19]).

The case $\omega(m)\le 2$ and $\mathscr{D}(n)\subseteq\mathscr{D}(m)$ $(n>1)$ will be particularly useful in the next two sections, so we will provide formulae for $F(m,n)$ in this case. By Proposition 5.4(3), $F(m,n)=F(m,p)$ if $\mathscr{D}(m)=\{p\}$, and $F(m,n)$ is equal to $F(m,pq)$, $F(m,p)$, or $F(m,q)$, if $\mathscr{D}(m)=\{p,q\}$.

Proposition 5.5. *Let p, q be distinct primes. We have*

$$F(p^k,p)=\begin{cases}p, & \text{if } p>2\\ \gcd(2^k,4), & \text{if } p=2.\end{cases}$$

Next, let $m=p^kq^l$ and $k,l>0$. If m is odd we have

$$F(m,pq) = \gcd(m,(p^{q-1}-1)(q^{p-1}-1)) \tag{5.1}$$

$$F(m,p) = p\gcd(q^l,p^{q-1}-1) \tag{5.2}$$

$$F(m,q) = q\gcd(p^k,q^{p-1}-1), \tag{5.3}$$

and if m is even (without loss of generality, $p=2$) we have

$$F(m,2q) = \begin{cases}\gcd(m,\frac{1}{2}(q^2-1)(2^{q-1}-1)), & \text{if } q\equiv 1 \bmod 4\\ \gcd(m,(q^2-1)(2^{q-1}-1)), & \text{if } q\equiv 3 \bmod 4\end{cases} \tag{5.4}$$

$$F(m,2) = \begin{cases}2\gcd(q^l,2^{q-1}-1), & \text{if } 4\nmid m\\ 4\gcd(q^l,2^{q-1}-1), & \text{if } 4\mid m\end{cases} \tag{5.5}$$

$$F(m,q) = \begin{cases}q\gcd(2^k,\frac{1}{2}(q^2-1)), & \text{if } q\equiv 1 \bmod 4\\ q\gcd(2^k,q^2-1), & \text{if } q\equiv 3 \bmod 4\end{cases}. \tag{5.6}$$

At all cases,

$$F(m,p),F(m,q)\le F(m,pq)\le p^aq^b, \tag{5.7}$$

where

$$a = \begin{cases} \nu_p(q^{p-1}-1), & \text{if } p > 2 \\ \nu_2(q^2-1), & \text{otherwise,} \end{cases}$$

$b = \nu_q(p^{q-1}-1)$.

Proof. By Definition 5.1, $b(2, 2^k, 2) = 2$ and $b(p, p^k, p) = 1$ for $p > 2$, so $F(2^k, 2) = \gcd(2^k, 2^2)$, while $F(p^k, p) = \gcd(p^k, p) = p$, proving the first part.

Next, let $m = p^k q^l$. First we assume that m is odd. Then, according to Definition 5.1, $m_q = p$ and $m_p = q$, therefore $b(p, m, pq) = b(p, m, q) = \nu_p(q^{p-1}-1)$ while $b(p, m, p) = 1$, and similarly $b(q, m, pq) = b(q, m, p) = \nu_q(p^{q-1}-1)$ and $b(q, m, q) = 1$, since $p \nmid \operatorname{ord}_p(q)$ and $q \nmid \operatorname{ord}_q(p)$. This shows that

$$F(m, pq) = \gcd(m, p^{b(p,m,pq)} q^{b(q,m,pq)}) = \gcd(m, (p^{q-1}-1)(q^{p-1}-1)),$$

since

$$\nu_p((p^{q-1}-1)(q^{p-1}-1)) = \nu_p(p^{q-1}-1) + \nu_p(q^{p-1}-1) = b(p, m, pq),$$

and similarly for $b(q, m, pq)$. Moreover,

$$F(m, p) = \gcd(m, pq^{b(q,m,p)}) = p \gcd(q^l, q^{p-1}-1),$$

and the formula for $F(m, q)$ is recovered in the same manner.

Next, assume that m is even, so that $p = 2$ without loss of generality. Then, $m_2 = q$ and $m_q = 4$, therefore $b(2, m, 2q) = b(2, m, q) = \nu_2(q^2-1) + \nu_2(\operatorname{ord}_4(q)) - 1$ and $b(2, m, 2) = 2$; similarly $b(q, m, 2q) = b(q, m, 2) = \nu_q(2^{q-1}-1)$, as $q \nmid \operatorname{ord}_q(2)$, and $b(q, m, q) = 1$, as before. Hence,

$$F(m, 2q) = \gcd(m, 2^{b(2,m,2q)} q^{b(q,m,2q)}) = \gcd(m, \frac{1}{2} \operatorname{ord}_4(q)(q^2-1)(2^{q-1}-1))$$

yielding (5.4). Also

$$F(m, 2) = \gcd(m, 4q^{b(q,m,2)}) = 2 \gcd(\frac{m}{2}, 2^q - 2),$$

and

$$F(m, q) = \gcd(m, 2^{b(2,m,q)} q) = q \gcd(2^k, \frac{1}{2} \operatorname{ord}_4(q)(q^2-1)),$$

giving us (5.5) and (5.6). Equation (5.7) follows easily. □

6. The prime power case, revisited

Now we are ready to apply the methods already introduced; we will begin by providing two different proofs for the prime power case, one using the field descent method and one using the polynomial method. We emphasize that the polynomial method comprises of similar arguments as in [21], albeit with a different language.

Theorem 6.1. *Let $N = p^k$, where p prime. Then, $\mathbb{Z}_N$ cannot have primitive formally dual sets, unless $N = 4$*

Let $N = p^m$, and let T, S be a pair of primitive formally dual subsets of $\mathbb{Z}_N$. We have (see also Lemma 7.1)

$$(T - T) \cap \mathbb{Z}_N^\star \neq \varnothing \neq (S - S) \cap \mathbb{Z}_N^\star,$$

otherwise $T - T \subseteq p\mathbb{Z}_N$ or $S - S \subseteq p\mathbb{Z}_N$, a possibility excluded due to the fact that T, S are primitive. Thsi is equivalent to $\mathbf{1}_T * \mathbf{1}_{-T}(1)\mathbf{1}_S * \mathbf{1}_{-S}(1) \neq 0$ or $T(\zeta_N)S(\zeta_N) \neq 0$. Without loss of generality, we suppose $|T| \leq |S|$, so that $|T| \leq \sqrt{N}$. If N is not a square, then $m = 2k+1$, and

$$|T| \leq p^k < p^{k+1} \leq |S|.$$

But then, the differences between unequal elements of T are

$$|T|^2 - |T| \leq p^{2k} - p^k < p^{2k}(p-1) = \varphi(N),$$

contradicting Lemma 4.8. Hence, N must be a square, so that $m = 2k$. If $|T| < |S|$, then $|T| \leq p^{k-1}$, and we are led again to a contradiction, as

$$|T|(|T|-1) \leq p^{2k-2} - p^{k-1} < p^{2k-1}(p-1) = \varphi(N).$$

Therefore, $|T| = |S| = \sqrt{N} = p^k$.

Proof of Theorem 6.1 via the field descent method. By Lemma 4.8 we have

$$0 < \mathbf{1}_T * \mathbf{1}_{-T}(1) < \frac{|T|^2}{N} = \frac{N}{\varphi(N)} = \frac{p}{p-1} \leq 2,$$

hence $\mathbf{1}_T * \mathbf{1}_{-T}(1) = 1$ and by (4.3) we get

$$n = |S(\zeta_N)|^2 = \frac{|S|^2}{|T|} \geq \sqrt{N} = p^k,$$

and $\mathscr{D}(n) = \{p\}$. Furthermore, $S(\zeta_N) = \sum_{s\in S} \zeta_N^s$, therefore applying Theorem 5.3 with $C = 1$ and Propositions 5.4 and 5.5 we get for p odd

$$p^k \leq \frac{F(p^{2k}, p)^2}{4\varphi(F(p^k, p))} = \frac{p^2}{4(p-1)} < p,$$

a contradiction, while for $p = 2$,

$$2^k \leq \frac{F(2^{2k}, 2)^2}{4\varphi(F(2^{2k}, 2))} = 2,$$

yielding $k = 1$, as desired. □

Proof of Theorem 6.1 via the polynomial method. Define $T_j := \{t \in T : t \equiv j \bmod p\}$. Since

$$\mathbf{1}_T * \mathbf{1}_{-T}(1) = 1,$$

Proposition 4.4 gives

$$R_N(X) \equiv T(X)T(X^{-1}) - \sum_{j=0}^{p-1} T_j(X)T_j(X^{-1}) \bmod X^N - 1,$$

so that

$$R_N(\zeta) = |T(\zeta)|^2 - \sum_{j=0}^{p-1} |T_j(\zeta)|^2,$$

for every Nth root of unity ζ. Putting $\zeta = 1$ we get

$$\varphi(N) = N - \sum_{j=0}^{p-1} |T_j|^2 \iff \sum_{j=0}^{p-1} |T_j|^2 = N/p \iff N = p\sum_{j=0}^{p-1} |T_j|^2 \geq |T|^2$$

by Cauchy-Schwarz inequality, where equality holds precisely when all $|T_j|$ are the same; equality indeed holds[3], since $|T| = \sqrt{N}$, hence $|T_j| = p^{k-1}$, for all j. This implies that

$$T(\zeta_p) = \sum_{j=0}^{p-1} \zeta_p^j |T_j| = 0,$$

and similarly $S(\zeta_p) = 0$. The case $N = p^2$ has already been tackled in [1], where primitive formally dual subsets exist only for $p = 2$, so we may assume that $m = 2k$ with $k \geq 2$.

If $T(\zeta) \neq 0$ for any other Nth root of unity besides ζ_p and its conjugates, then $S - S$ intersects all divisor classes except for $\frac{N}{p}\mathbb{Z}_N^\star$, yielding

$$|S|^2 - |S| \geq \sum_{i=0}^{m-2} \varphi(N/p^i) = N - p,$$

while on the other hand

$$|S|^2 - |S| = N - \sqrt{N} < N - p,$$

a contradiction. So, there is some Nth root of unity ζ with $\zeta^p \neq 1$, such that $T(\zeta) = 0$, hence by (3.2)

$$0 = R_N(\zeta) = -\sum_{j=0}^{p-1} |T_j(\zeta)|^2,$$

[3]In [1, 21], this argument was attributed to Gregory Minton.

implying that $T_j(\zeta) = 0$ for all j. This leads to a contradiction, when we take derivatives; by Lemma 3.4 we have

$$R'(\zeta) \equiv N\zeta^{-1}\left[\frac{1}{\zeta-1} - \frac{1}{\zeta^p-1}\right] \equiv \frac{N(1+\zeta+\ldots+\zeta^{p-2})}{\zeta^p-1} \equiv \frac{N}{\zeta^p-1}\frac{\zeta^{p-1}-1}{\zeta-1} \not\equiv 0 \bmod N\mathbb{Z}[\zeta_N],$$

since $\frac{\zeta^{p-1}-1}{\zeta-1}$ is a unit in $\mathbb{Z}[\zeta_N]$, while $\zeta^p - 1$ is not. On the other hand, we obtain

$$\left[T(X)T(X^{-1}) - \textstyle\sum_{j=0}^{p-1} T_j(X)T_j(X^{-1})\right]' =$$
$$T'(X)T(X^{-1}) - T(X)T'(X^{-1})X^{-2} - \textstyle\sum_{j=0}^{p-1}(T_j'(X)T_j(X^{-1}) - T_j(X)T_j'(X^{-1})X^{-2}),$$

and keeping in mind that we have $T(\zeta) = T(\zeta^{-1}) = T_j(\zeta) = T_j(\zeta^{-1}) = 0$ for all j, we get

$$\frac{d}{dX}\left[T(X)T(X^{-1}) - \sum_{j=0}^{p-1} T_j(X)T_j(X^{-1})\right]_{X=\zeta} = 0,$$

a contradiction. Thus, if N is a prime power with $N \neq 4$, there are no primitive formally dual pairs in $\mathbb{Z}_N$. □

7. Products of two prime powers

In this section, we will address the case $\mathscr{D}(N) = \{p, q\}$.

Lemma 7.1. *Let $T \subseteq \mathbb{Z}_N$ be primitive and N is divisible by at most two primes. Then $(T-T)\cap\mathbb{Z}_N^\star \neq \varnothing$.*

Proof. If $\mathrm{rad}(N) = p$, then T is not a subset of any coset of the subgroup $p\mathbb{Z}_N$. In particular, there are two elements of T that are not congruent mod$p$; hence, their difference is also prime to N, which yields the desired conclusion.

Let $\mathrm{rad}(N) = pq$, and define $T_j = \{t \in T : t \equiv j \bmod p\}$. Since T is primitive, at least two of the sets T_j are nonempty. Let T_a and T_b be two arbitrary nonempty sets of this family. Suppose that T_a has at least two elements, say t, t', and take $t'' \in T_b$. Assume that $(T-T)\cap\mathbb{Z}_N^\star = \varnothing$. Since $p \nmid t - t''$, we must certainly have $q \mid t - t''$, otherwise $\gcd(t-t'', N) = 1$. The same holds for the difference between elements of T_a and T_b, so

$$T_a - T_b \subseteq q\mathbb{Z}_N.$$

On the other hand, $t - t' = (t - t'') - (t' - t'') \in q\mathbb{Z}_N$, and since $t, t' \in T_a$ were arbitrary, we obtain

$$T_a - T_a \subseteq q\mathbb{Z}_N,$$

therefore,

$$T - T = \bigcup_{a,b=0}^{p-1} (T_a - T_b) \subseteq q\mathbb{Z}_N,$$

a contradiction. Thus, $(T-T)\cap\mathbb{Z}_N^\star \neq \varnothing$. □

Remark. The above does not necessarily hold when n is divisible by at least three primes. For example, take $\mathrm{rad}(N) = pqr$, and

$$T = pq\mathbb{Z}_N \cup qr\mathbb{Z}_N \cup pr\mathbb{Z}_N.$$

T is indeed a primitive set, but $(T-T)\cap\mathbb{Z}_N^\star = \varnothing$.

Lemma 7.1 shows that $S(\zeta_N)T(\zeta_N) \neq 0$ when $\mathrm{rad}(N) = pq$ and S, T are primitive formally dual, or equivalently, $\mathbf{1}_T * \mathbf{1}_{-T}(1), \mathbf{1}_S * \mathbf{1}_{-S}(1) \geq 1$. Upper bounds are given by the following:

Proposition 7.2. *Let N be a positive integer with $\mathrm{rad}(N) = pq$, and T, S primitive formally dual subsets of $\mathbb{Z}_N$ with $|T| \leq |S|$. Then*

$$|S(\zeta_N)|^2 = \frac{|S|^3}{N}. \tag{7.1}$$

Furthermore, $\mathbf{1}_S * \mathbf{1}_{-S}(1) \leq 3$*, so that*

$$|T(\zeta_N)|^2 = \frac{K|T|^3}{N},$$

where $1 \leq K \leq 3$*.*

Proof. By Corollary 4.7 we obtain

$$\mathbf{1}_T * \mathbf{1}_{-T}(1) < \frac{2|T|^2}{N} \leq 2,$$

whence $\mathbf{1}_T * \mathbf{1}_{-T}(1) = 1$, due to Lemma 7.1, yielding (7.1). Furthermore,

$$\mathbf{1}_S * \mathbf{1}_{-S}(1) < \frac{2|S|^2}{N} < \frac{2 \cdot 2N}{N} = 4,$$

concluding the proof. □

Since $|S| \mid N$ and $|S(\zeta_N)|^2 \in \mathbb{Z}$, Proposition 7.2 implies that $|S(\zeta_N)|^2$ is not divisible by primes other than p and q, and $|S| \geq \sqrt{N}$ yields

$$|S(\zeta_N)|^2 \geq \sqrt{N},$$

that is, the squared modulus of the algebraic integer $S(\zeta_N) \in \mathbb{Z}[\zeta_N]$ is a relatively large integer with respect to the order of ζ_N, i.e. N. This leads to the main result of this section.

Theorem 7.3. *Fix* p*,* q*, two distinct primes. Then, possibly with finitely many exceptions, no group* $\mathbb{Z}_N$ *with* $\mathrm{rad}(N) = pq$ *possesses primitive formally dual subsets.*

Proof. Let $P = \{p, q\}$ and put a, b, exactly as in Proposition 5.5, hence $F(m, n) \leq p^a q^b$, whenever $\mathscr{D}(n) \subseteq \mathscr{D}(m) = P$. Now let $N = p^k q^l$, and $T, S \subseteq \mathbb{Z}_N$ be primitive formally dual, with $|T| \leq |S|$, so that $|S| \geq \sqrt{N}$; also, put $n = |S(\zeta_N)|^2$, where $\zeta_N = e^{2\pi i/N}$. Then, by Proposition 7.2 we get

$$n = \frac{|S|^3}{N} \geq \sqrt{N}. \tag{7.2}$$

On the other hand, we observe that $S(\zeta_N) = \sum_{j \in S} \zeta_N^j$, so if we put $X = S(\zeta_N)$ as in Theorem 5.3, the constant C can be taken equal to 1. Applying this Theorem we obtain

$$n \leq \frac{F(N,n)^2}{4\varphi(F(N,n))} = \frac{F(N,n)}{4(1-\frac{1}{p})(1-\frac{1}{q})} \leq \frac{p^a q^b}{4(1-\frac{1}{p})(1-\frac{1}{q})}. \tag{7.3}$$

Combining equations (7.2) and (7.3), we get

$$N \leq \frac{p^{2a} q^{2b}}{16(1-\frac{1}{p})^2(1-\frac{1}{q})^2},$$

hence at most finitely many groups $\mathbb{Z}_N$ with $\mathrm{rad}(N) = pq$ possess primitive formally dual subsets. □

Theorem 7.3 tackles the Conjecture when the sum of the exponents of p and q is sufficiently high. Next, we will tackle some cases where one or both of the exponents are small.

Proposition 7.4. *Let* $N = p^a q$*, where* p*,* q *distinct primes. Then* $\mathbb{Z}_N$ *does not have primitive formally dual subsets.*

Proof. We remind that if $a = 1$ then N is square–free, so this is already proven by [27]; we may assume that $a > 1$. Suppose on the contrary that T, S are such subsets, with $|T| < |S|$ as usual (equality cannot occur in this case, as N is not a square), therefore

$$\sqrt{\varphi(N)} < |T| < \sqrt{N} < |S| < \frac{N}{\sqrt{\varphi(N)}}. \tag{7.4}$$

By Proposition 7.2 we get

$$|S(\zeta_N)|^2 = \frac{|S|^3}{N},$$

hence $q \mid |S|$ and $q \nmid |T|$, so $|T| = p^b$ and $|S| = p^{a-b}q$ for some integer b. We recall that

$$|T(\zeta_N)|^2 = \frac{|T|^3}{N} \mathbf{1}_S * \mathbf{1}_{-S}(1). \tag{7.5}$$

Since the latter is an integer, $q \mid N$ and $q \nmid |T|$, we must have

$$q \mid \mathbf{1}_S * \mathbf{1}_{-S}(1). \tag{7.6}$$

Suppose first that q is odd; then by Proposition 7.2 we must have $q = \mathbf{1}_S * \mathbf{1}_{-S}(1) = 3$ so that $N = 3p^a$ and $\varphi(N) = 2(p-1)p^{a-1}$. By virtue of Lemma 4.8 we obtain

$$\sqrt{2(p-1)}p^{\frac{a-1}{2}} < p^b < \sqrt{3}p^{\frac{a}{2}}.$$

If N is odd, then $p > 3$, so we have $\sqrt{2(p-1)} > \sqrt{p}$, so the above inequalities lead to

$$p^{\frac{a}{2}} < p^b < p^{\frac{a+1}{2}}$$

which is a contradiction, as there is no such integer b.

Now suppose that $p = 2$, so that $N = 2^a 3$. Then $|T| = 2^b$ and by (7.4) we get

$$2^{\frac{a}{2}} < 2^b < 2^{\frac{a}{2}}\sqrt{3},$$

yielding $|T| = 2^{\frac{a+1}{2}}$ and $|S| = 2^{\frac{a-1}{2}}3$; also, a must be odd. Equations (7.5) and (7.6) yield

$$|T(\zeta_N)|^2 = 2^{\frac{a+3}{2}}.$$

Applying Theorem 5.3 and equation (5.4), we get

$$|T(\zeta_N)|^2 \leq \frac{F(2^a 3, 2)}{4\varphi(F(2^a 3, 2))} = \frac{12^2}{4\varphi(12)} = 9,$$

and since a is odd, the only solution we get from $2^{\frac{a+3}{2}} \leq 9$ is $a = 3$. Hence, $N = 24$, $|T| = 4$, $|S| = 6$, and $|T(\zeta_N)|^2 = 8$. Now we will try to determine $T - T$ as a multi-set. Since $12 = |T|^2 - |T| < 2\varphi(24) = 16$ it only contains $\mathbb{Z}_{24}^\star$ with multiplicity one. The rest of the $4 = |T|^2 - |T| - \varphi(24)$ differences between different elements of T must belong to other divisor classes. Two of these classes must necessarily be from

$$12\mathbb{Z}_{24}^\star = \{12\},\ 6\mathbb{Z}_{24}^\star = \{6, 18\},\ 3\mathbb{Z}_{24}^\star = \{3, 9, 15, 21\},$$

otherwise $4 \mid |S|$, a contradiction. Thus, the only possibility is for $12\mathbb{Z}_{24}^\star$ to appear with multiplicity 2 and $6\mathbb{Z}_{24}^\star$ with multiplicity 1. This means, that there is some $t \in T$, such that $t + 12 \in T$, say $T = \{u, v, t, t + 12\}$. But then,

$$|T(\zeta_N)|^2 = |\zeta_N^u + \zeta_N^v + \zeta_N^t - \zeta_N^t|^2 = |\zeta_N^u + \zeta_N^v|^2 \leq 4 < 8,$$

a contradiction. Therefore, neither in this case do exist primitive formally dual subsets.

Finally, suppose that $q = 2$, so that $N = 2p^a$, $|T| = p^b$, $|S| = 2p^{a-b}$. By (7.4) we have the bounds

$$\sqrt{2}p^{\frac{a}{2}} < 2p^{a-b} < \frac{2p^{\frac{a+1}{2}}}{\sqrt{p-1}},$$

or equivalently,

$$\frac{1}{\sqrt{2}}p^{\frac{a}{2}} < p^{a-b} < \frac{p^{\frac{a+1}{2}}}{\sqrt{p-1}},$$

which can only happen if a is even and $a = 2b$. Hence, $|S| = 2p^{\frac{a}{2}}$ and $|T| = p^{\frac{a}{2}}$; however, this contradicts Corollary 4.7 and Lemma 7.1, as

$$\mathbf{1}_T * \mathbf{1}_{-T}(1) < \frac{2|T|^2}{N} = 1,$$

completing the proof. □

Proposition 7.5. *Let $N = p^a q^2$, where p, q distinct primes and a is odd. Then $\mathbb{Z}_N$ does not have primitive formally dual subsets.*

Proof. Throughout the proof we assume that $a \geq 3$, as the case $a = 1$ is covered by Proposition 7.4. As before, we assume that T, S are primitive formally dual subsets of $\mathbb{Z}_N$, with $|T| < |S|$, as N is not a square, hence

$$\sqrt{\varphi(N)} < |T| < \sqrt{N} < |S| < \frac{N}{\sqrt{\varphi(N)}}.$$

Proposition 7.2 implies that $q \mid |S|$. We will also show that $q \mid |T|$; suppose on the contrary that $q \nmid |T|$. Then $q^2 \mid \mathbf{1}_S * \mathbf{1}_{-S}(1)$, since

$$|T(\zeta_N)|^2 = \frac{|T|^3}{N}\mathbf{1}_S * \mathbf{1}_{-S}(1),$$

contradicting Proposition 7.2.

Thus, q divides both $|T|$ and $|S|$, hence $|T| \leq p^k q$, where $a = 2k+1$. This leads to $|T|^2 - |T| \leq p^k q(p^k q - 1)$, while $\varphi(N) = p^{2k}q(p-1)(q-1)$. Since $|T|^2 - |T| \geq \varphi(N)$, we get $p^k q - 1 \geq p^k(p-1)(q-1)$; when p is odd, the latter is $\geq 2p^k(q-1) \geq p^k q$, a contradiction. Hence, $p = 2$, and applying Corollary 4.7 we obtain

$$\mathbf{1}_T * \mathbf{1}_{-T}(1) < \frac{2|T|^2}{N} \leq \frac{2 \cdot 2^{2k} q^2}{2^{2k+1} q^2} = 1,$$

contradicting Lemma 7.1, as desired. □

Lastly, we prove the following:

Proposition 7.6. *Let $N = p^2 q^2$, for p, q distinct primes. Then, $\mathbb{Z}_N$ does not have primitive formally dual subsets.*

Proof. As usual, suppose that such subsets exists, with $|T| \leq |S|$. Without loss of generality assume $p < q$; then $|T| \in \{p, q, p^2, pq\}$. If $|T| = p$ or $|T| = q$, then $\varphi(N) = pq(p-1)(q-1) \geq 2q(q-1) > q^2 \geq |T|^2$, contradicting Lemma 4.8 and Lemma 7.1. If $|T| = p^2$, then $\varphi(N) = pq(p-1)(q-1) \geq (p+2)(p+1)p(p-1) = p^4 + 2p^3 - p^2 - 2p > p^4$, contradicting again Lemma 4.8. Thus, $|T| = |S| = pq$, and Proposition 7.2 applies to T as well, that is

$$|S(\zeta_N)|^2 = |T(\zeta_N)|^2 = pq,$$

or equivalently, $\mathbf{1}_T * \mathbf{1}_{-T}(1) = \mathbf{1}_S * \mathbf{1}_{-S}(1) = 1$. Applying Lemma 4.5 for $d = N$ we obtain

$$\frac{pq}{(pq)^{3/2}} = \frac{1}{pq(pq)^{3/2}}\Big[|T(1)|^2 - |T(\zeta_p)|^2 - |T(\zeta_q)|^2 + |T(\zeta_{pq})|^2\Big],$$

or equivalently,

$$|T(\zeta_{pq})|^2 = |T(\zeta_p)|^2 + |T(\zeta_q)|^2, \tag{7.7}$$

and similarly for S,

$$|S(\zeta_{pq})|^2 = |S(\zeta_p)|^2 + |S(\zeta_q)|^2. \tag{7.8}$$

Suppose first that $T(\zeta_{pq}) = 0$; from (7.7) we also get $T(\zeta_p) = T(\zeta_q) = 0$, hence $T(X)$ is divided by $\frac{X^{pq}-1}{X-1} = 1 + X + \cdots + X^{pq-1}$. Since $T(1) = |T| = pq$, we have

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

This implies that $|T_{j,pq}| = 1$, for all $0 \leq j \leq pq - 1$, therefore

$$\mathbf{1}_T * \mathbf{1}_{-T}(pq) = \mathbf{1}_T * \mathbf{1}_{-T}(p^2 q) = \mathbf{1}_T * \mathbf{1}_{-T}(pq^2) = 0,$$

or $S(\zeta_{pq}) = S(\zeta_p) = S(\zeta_q) = 0$. Moreover, $T_{j,pq}(X)$ are monomials with coefficient 1; since $\mathbf{1}_T * \mathbf{1}_{-T}(1) = 1$, we have

$$\bigcup_{j \in \mathbb{Z}_{pq}} (T_{j,pq} - T_{j-1,pq}) = 1 + pq\mathbb{Z}_N.$$

Taking mask polynomials on both sides we obtain

$$X(1 + X^{pq} + \cdots + X^{pq(pq-1)}) \equiv \sum_{j \in \mathbb{Z}_{pq}} T_{j,pq}(X) T_{j-1,pq}(X^{-1}) \bmod (X^N - 1).$$

Differentiating both sides with respect to X and then setting $X = 1$ we get

$$\begin{aligned} pq + pq\frac{pq(pq-1)}{2} &\equiv \sum_{j \in \mathbb{Z}_{pq}} T'_{j,pq}(1) T_{j-1,pq}(1) - T_{j,pq}(1) T'_{j-1,pq}(1) \bmod N \\ &\equiv \sum_{j \in \mathbb{Z}_{pq}} T'_{j,pq}(1) - T'_{j-1,pq}(1) \equiv 0 \bmod N, \end{aligned}$$

a contradiction, since the left hand side can never be divisible by N; if N is odd, it is $pq \bmod N$, otherwise, we have (say) $p = 2$, and it is $2q \bmod 2q^2$.

Therefore, we assume that $T(\zeta_{pq})S(\zeta_{pq}) \neq 0$. If $T(\zeta_N^p) = 0$, then

$$T(X^p) \equiv P_p(X^p)\Phi_p(X^{N/p}) + Q_p(X^p)\Phi_q(X^{N/q}) \bmod (X^N - 1),$$

for some $P_p, Q_p \in \mathbb{Z}[X]$ with nonnegative coefficients. Since

$$pq = T(1) = pP_p(1) + qQ_p(1),$$

we have either $P_p(1) = q$ and $Q_p \equiv 0$ or $P_p \equiv 0$ and $Q_p(1) = p$. The former case implies

$$T(X^{pq}) \equiv P_p(X^{pq})\Phi_p(X^{N/p}) \bmod (X^N - 1),$$

contradicting $T(\zeta_{pq}) \neq 0$. Thus, $P_p \equiv 0$, establishing

$$T(X^p) \equiv Q_p(X^p)\Phi_q(X^{N/q}) \bmod (X^N - 1),$$

whence $T(\zeta_N^{p^2}) = 0$. Applying Lemma 4.5 for $d = p^2$ we get

$$|S(\zeta_N^{q^2})|^2 = |S(\zeta_N^q)|^2,$$

and another application for $d = p$ yields

$$-\frac{1}{\sqrt{p}}|T(\zeta_N)|^2 = -\frac{1}{q\sqrt{p}}|S(\zeta_q)|^2,$$

or equivalently, $|S(\zeta_q)|^2 = pq^2$.

We distinguish two cases; first, $T(\zeta_p) = 0$. By (7.7) we have $|T(\zeta_{pq})|^2 = |T(\zeta_q)|^2$, so Lemma 4.5 for $d = p^2q$ gives $|S(\zeta_N^q)|^2 = |S(\zeta_N)|^2$, and thence

$$|S(\zeta_N^{q^2})|^2 = |S(\zeta_N^q)|^2 = |S(\zeta_N)|^2 = pq.$$

Also, by $|S(\zeta_q)|^2 = pq^2$ and (7.8) we get $|S(\zeta_{pq})|^2 \geq pq^2$, so by Proposition 4.3 for $X = 1$ we get

$$p^2q^2 = \frac{1}{pq}\sum_{d|N}|S(\zeta_N^d)|^2\varphi(N/d) \geq \varphi(p^2q^2) + \varphi(p^2q) + \varphi(p^2) + q(\varphi(pq) + \varphi(q)) + pq = p^2q^2,$$

therefore, since the inequality in the middle is actually an equality, we obtain

$$S(\zeta_N^p) = S(\zeta_N^{p^2}) = S(\zeta_p) = 0,$$

and utilizing the same arguments as before (interchanging T by S) we obtain

$$|T(\zeta_N^d)|^2 = |S(\zeta_N^d)|^2$$

for all integers d. This also yields

$$\begin{aligned}\mathbf{1}_T * \mathbf{1}_{-T}(1) = \mathbf{1}_T * \mathbf{1}_{-T}(q) = \mathbf{1}_T * \mathbf{1}_{-T}(q^2) = 1,\\ \mathbf{1}_T * \mathbf{1}_{-T}(pq) = \mathbf{1}_T * \mathbf{1}_{-T}(p^2q) = q,\\ \mathbf{1}_T * \mathbf{1}_{-T}(p) = \mathbf{1}_T * \mathbf{1}_{-T}(p^2) = \mathbf{1}_T * \mathbf{1}_{-T}(pq^2) = 0.\end{aligned}$$

For every $j \in \mathbb{Z}_p$, the difference sets $T_{j,p} - T_{j-1,p}$ are subsets of $1 + p\mathbb{Z}_N$; furthermore, from the equations above, every element of $1 + p\mathbb{Z}_N$ occurs exactly once as difference $t - t'$, where $t, t' \in T$. Hence, the following equality between multisets holds:

$$\bigcup_{j\in\mathbb{Z}_p}(T_{j,p} - T_{j-1,p}) = 1 + p\mathbb{Z}_N,$$

and taking mask polynomials on both sides we obtain

$$\sum_{j\in\mathbb{Z}_p} T_{j,p}(X)T_{j-1,p}(X^{-1}) \equiv X\sum_{k=0}^{pq^2-1} X^{pk} \bmod (X^N - 1). \tag{7.9}$$

A consequence of $T(\zeta_p) = 0$ is $|T_{j,p}| = q$ for all j; indeed, as

$$T(\zeta_p) = \sum_{j\in\mathbb{Z}_p}\zeta_p^j|T_{j,p}| = 0.$$

Differentiating the left hand side side of (7.9) at $X = 1$, we get

$$\sum_{j\in\mathbb{Z}_p} T'_{j,p}(1)T_{j-1,p}(1) - T_{j,p}(1)T'_{j-1,p}(1) = q\sum_{j\in\mathbb{Z}_p} T'_{j,p}(1) - T'_{j-1,p}(1) = 0,$$

and differentiating the right hand side of (7.9) at $X = 1$,

$$pq^2 + p\frac{pq^2(pq^2-1)}{2} = \frac{N}{p} + N\frac{N/p-1}{2}.$$

Next, we apply Lemma 3.2; if N is odd, then the above derivative is $\equiv \frac{N}{p} \bmod N$, a contradiction. So, N must be even and $p = 2$, because this derivative is $\equiv \frac{N}{p} \bmod \frac{N}{2}$. Furthermore, $T(\zeta_{q^2}) = 0$ implies

$$\sum_{j\in\mathbb{Z}_{q^2}} \zeta_{q^2}^j |T_{j,q^2}| = 0.$$

This implies that for every j,

$$|T_{j,q^2}| = |T_{j+q,q^2}| = |T_{j+2q,q^2}| = \cdots = |T_{j+(q^2-q),q^2}|,$$

or, simply put, $|T_{j,q}| = q|T_{j,q^2}|$. Since $|T| = 2q$ and $T \neq T_{j,q}$ for any j, due to the primitivity of T, there must be $j, k \in \mathbb{Z}_q$, $j \neq k$, such that $T = T_{j,q} \cup T_{k,q}$; moreover, $|T_{j,q}| = |T_{k,q}| = q$. The differences $T - T$ taken mod$q$ would then be only 0 and $\pm(j-k)$, which shows that $q = 3$, since all possible residues mod$q$ appear in $\mathbb{Z}_{4q^2}^\star \subseteq T - T$. Possibly after translating T, we may assume that $T = T_{0,3} \cup T_{1,3}$. As multisets, we would have the following equality

$$(T_{0,3} - T_{1,3}) \cup (T_{1,3} - T_{0,3}) = \mathbb{Z}_{36}^\star.$$

But this leads to a contradiction, as the possible differences in the left hand side are 18, while $\mathbb{Z}_{36}^\star = 12$.

The next case is $T(\zeta_p) \neq 0$. Applying Lemma 4.5 for $d = p^2q$ and (7.7) we obtain

$$-\frac{1}{p\sqrt{q}}|T(\zeta_p)|^2 = \frac{1}{\sqrt{q}}\Big[|S(\zeta_N^q)|^2 - |S(\zeta_N)|^2\Big],$$

hence $|S(\zeta_N^q)|^2 < |S(\zeta_N)|^2$ or equivalently, $\mathbf{1}_T * \mathbf{1}_{-T}(q) < 1$. Therefore, $S(\zeta_N^q) = 0$, and by Lemma 4.5 for $d = p^2$ we also get

$$S(\zeta_N^q) = S(\zeta_N^{q^2}) = 0.$$

Applying Lemma 4.5 for $d = pq^2$ and $d = q^2$, we obtain the formulae

$$\frac{1}{q}\Big[-|T(\zeta_q)|^2 - |T(\zeta_N^{q^2})|^2 + |T(\zeta_N^q)|^2\Big] = |S(\zeta_N^p)|^2 - |S(\zeta_N)|^2$$

and

$$\frac{1}{q}\Big[|T(\zeta_N^{q^2})|^2 - |T(\zeta_N^q)|^2\Big] = \frac{1}{p}\Big[|S(\zeta_N^{p^2})|^2 - |S(\zeta_N^p)|^2\Big].$$

Adding these equations by parts yields

$$\begin{aligned} -\frac{1}{q}|T(\zeta_q)|^2 &= \frac{1}{p}\Big[|S(\zeta_N^{p^2})|^2 - |S(\zeta_n^p)|^2\Big] + \Big[|S(\zeta_N^p)|^2 - |S(\zeta_N)|^2\Big] \\ &= \frac{1}{p}\Big[|S(\zeta_N^{p^2})|^2 - |S(\zeta_n)|^2\Big] + \left(1-\frac{1}{p}\right)\Big[|S(\zeta_N^p)|^2 - |S(\zeta_N)|^2\Big]. \end{aligned}$$

Since the left hand side is negative, either one of $|S(\zeta_N^p)|^2$ and $|S(\zeta_N^{p^2})|^2$ must be less than $|S(\zeta_N)|^2$; but this means that one of them is zero, as it would imply that either $\mathbf{1}_T * \mathbf{1}_{-T}(p) < 1$ or $\mathbf{1}_T * \mathbf{1}_{-T}(p^2) < 1$. If $S(\zeta_N^p) = 0$, then $S(\zeta_N^{p^2}) = 0$ as well, since $S(\zeta_{pq}) \neq 0$, so at any rate, $S(\zeta_N^{p^2}) = 0$. Hence,

$$-\frac{1}{q}|T(\zeta_q)|^2 = \left(1-\frac{1}{p}\right)|S(\zeta_N^p)|^2 - |S(\zeta_N)|^2.$$

If $\mathbf{1}_T * \mathbf{1}_{-T}(p) \geq 2$, then $|S(\zeta_N^p)|^2 \geq 2pq$ and the right hand side would be $\geq 2(p-1)q - pq = (p-2)q \geq 0$, while the left hand side is negative. so, either $\mathbf{1}_T * \mathbf{1}_{-T}(p) = 0$ or 1. If $\mathbf{1}_T * \mathbf{1}_{-T} = 1$, then $|T(\zeta_q)|^2 = q^2$, an absurdity as $pq \mid |T(\zeta_N^d)|^2$ for all $d \in \mathbb{Z}$. This shows that $S(\zeta_N^p) = 0$ as well; a symmetric argument also yields $T(\zeta_N^q) = T(\zeta_N^{q^2}) = 0$. Now consider the difference sets $T_{j,p} - T_{k,p}$, for $j \not\equiv k \bmod p$; all differences are prime to p, and since $\mathbf{1}_T * \mathbf{1}_{-T}(q) = \mathbf{1}_T * \mathbf{1}_{-T}(q^2) = 0$, we must have the following equality of multisets:

$$\bigcup_{\substack{j,k\in\mathbb{Z}_p \\ j\not\equiv k \bmod p}} (T_{j,p} - T_{k,p}) = \mathbb{Z}_N^\star.$$

Taking mask polynomials, we get

$$\sum_{\substack{j,k\in\mathbb{Z}_p\\ j\not\equiv k \bmod p}} T_{j,p}(X)T_{k,p}(X^{-1}) \equiv R_N(X) \bmod (X^N-1),$$

whence for $X=1$,

$$\sum_{\substack{j,k\in\mathbb{Z}_p\\ j\not\equiv k \bmod p}} |T_{j,p}||T_{k,p}| = pq(p-1)(q-1).$$

The left hand side is also equal to

$$\left[\sum_{j\in\mathbb{Z}_p}|T_{j,p}|\right]^2 - \sum_{j\in\mathbb{Z}_p}|T_{j,p}|^2 = p^2q^2 - \sum_{j\in\mathbb{Z}_p}|T_{j,p}|^2.$$

therefore,

$$\sum_{j\in\mathbb{Z}_p}|T_{j,p}|^2 = pq(p+q-1).$$

On the other hand, using a simliar argument as before, the fact that $T(\zeta_N^{q^2})=0$ implies $p \mid |T_{j,p}|$ for all p, whence $p^2 \mid \sum_{j\in\mathbb{Z}_p}|T_{j,p}|^2$; we should also have $q^2 \mid \sum_{j\in\mathbb{Z}_p}|T_{j,p}|^2$, as $T(\zeta_N^{p^2})=0$ as well, which is clearly an absurdity as $p^2q^2 \nmid pq(p+q-1)$.

Thus, we may assume that

$$T(\zeta_N^p)T(\zeta_N^q)T(\zeta_{pq})S(\zeta_N^p)S(\zeta_N^q)S(\zeta_{pq}) \neq 0,$$

otherwise we would revisit one of the previous cases, possibly by interchanging S by T and p by q. We will show that

$$q\mathbf{1}_T * \mathbf{1}_{-T}(p^2) + \mathbf{1}_T * \mathbf{1}_{-T}(p^2q) \geq q, \tag{7.10}$$

and similarly,

$$p\mathbf{1}_T * \mathbf{1}_{-T}(q^2) + \mathbf{1}_T * \mathbf{1}_{-T}(pq^2) \geq p. \tag{7.11}$$

If $\mathbf{1}_T * \mathbf{1}_{-T}(p^2) \geq 1$, (7.10) is trivially satisfied, so assume $\mathbf{1}_T * \mathbf{1}_{-T}(p^2) = 0$, or equivalently, $S(\zeta_N^{p^2})=0$. Then,

$$S(X^{p^2}) \equiv Q(X^{p^2})\Phi_q(X^{N/q}) \bmod (X^N-1),$$

for some $Q(X)\in\mathbb{Z}[X]$ with nonnegative coefficients. Therefore,

$$S(X^{p^2q}) \equiv qQ(X^{p^2q}) \bmod (X^N-1),$$

whence

$$|S(\zeta_q)|^2 = q^2|Q(\zeta_q)|^2.$$

The term $|Q(\zeta_q)|^2$ is simultaneously an algebraic integer by definition and a rational number due to the above equation, hence an integer. This implies $q^2 \mid |S(\zeta_q)|^2$, hence $q \mid \mathbf{1}_T * \mathbf{1}_{-T}(p^2q)$; we note that $\mathbf{1}_T * \mathbf{1}_{-T}(p^2q)$ and $\mathbf{1}_T * \mathbf{1}_{-T}(p^2)$ cannot be both zero, otherwise $q^2 \mid |S|$, a contradiction. Thus, $\mathbf{1}_T * \mathbf{1}_{-T}(p^2q) \geq q$ in this case, proving (7.10) and (7.11) at all cases. Now apply Proposition 4.3 for $X=1$, along with (7.10) and (7.11) we get

$$\begin{aligned}
|T|^2 &= \sum_{d|N} \mathbf{1}_T * \mathbf{1}_{-T}(d)\varphi(N/d)\\
&\geq pq + \varphi(p^2q^2) + \varphi(p^2q) + \varphi(pq^2) + \varphi(pq) +\\
&+ \mathbf{1}_T * \mathbf{1}_{-T}(p^2)\varphi(q^2) + \mathbf{1}_T * \mathbf{1}_{-T}(p^2q)\varphi(q) + \mathbf{1}_T * \mathbf{1}_{-T}(q^2)\varphi(p^2) + \mathbf{1}_T * \mathbf{1}_{-T}(pq^2)\varphi(p)\\
&\geq pq + pq(p-1)(q-1) + q(p-1)(q-1) + p(p-1)(q-1) + (p-1)(q-1) + q(q-1) + p(p-1)\\
&= p^2q^2 + (p-1)(q-1) > p^2q^2,
\end{aligned}$$

which is clearly a contradiction, concluding the proof. □

Summarizing the results of this section, we conclude that the field descent method tackles the cases $p^k q^l$ with both exponents relatively high, while the polynomial method tackles the cases where one exponent is small. Combining these methods, we see that for most pairs of primes the conjecture is settled; of course, this needs to be properly quantified. In the Appendix, we find the number of exceptions among all N with $\mathrm{rad}(N) = pq$ and $p, q < 10^3$, just to get an idea. This number is significantly lower if we use the polynomial method to prove the $N = p^4 q^2$ case.

8. Beyond two prime factors

The main obstruction to apply the field descent method when $\omega(N) > 2$ is the fact that primitivity of $T \subseteq \mathbb{Z}_N$ does not imply $(T-T) \cap \mathbb{Z}_N^\star \neq \varnothing$, as can be seen from the Remark immediately after Lemma 7.1. However, it needs to be emphasized that so far this method was only applied to the condition $|S(\zeta_N)|^2 \in \mathbb{Z}$, and not $|S(\zeta_N^d)|^2 \in \mathbb{Z}$ in general. For $S(\zeta_N^d)$, the constant C in Theorem 5.3 can be as large as d, so it might suffice to show that there always exists some $d \mid N$, say $d \leq N^{1/5}$, satisfying $S(\zeta_N^d) \neq 0$. Moreover, Lemma 7.1 was proven for primitive sets, without any other condition. It is possible that this can be extended to other cases with conditions such as $|T| \mid N$, or the requirement that the differences $t - t'$ with $t, t' \in T$ are equidistributed in every divisor class $d\mathbb{Z}_N^\star$.

Besides the case for square–free N where Conjecture 1.2 has been confirmed [27], we will show that 1.2 is also true for another family of orders N that satisfy the so–called *self conjugacy* property with respect to a prime factor p (there is no restriction on the number of distinct prime factors for such N). This notion was first used by Turyn [24] to attack the circulant Hadamard conjecture stated by Ryser [17].

Definition 8.1. A prime p is called self–conjugate mod$N$ if every ideal $\mathfrak{P} \subseteq \mathbb{Z}[\zeta_N]$ dividing $p\mathbb{Z}[\zeta_N]$ is invariant under complex conjugation, i.e. $\overline{\mathfrak{P}} = \mathfrak{P}$.

In other words, the complex conjugation belongs to the decomposition group of any prime ideal $\mathfrak{P} \mid p$. A characterization of the decomposition group (cf. Theorem 1.4.3 [19]) shows that $\sigma \in G_{\mathfrak{P}}$ if and only if $\sigma(\zeta_m) = \zeta_m^{p^j}$ for some $j \in \mathbb{Z}$, where $N = p^a m$, $p \nmid m$ (i.e. m is the p–free part of N). From this follows the result of Turyn [24] (see also Corollary 1.4.5 [19]), a weaker version of which we state below.

Theorem 8.2. *Let $A \in \mathbb{Z}[\zeta_N]$ such that $|A|^2 \equiv 0 \bmod p^{2b}$, where p is self–conjugate* mod$N$. *Then $A \equiv 0 \bmod p^b \mathbb{Z}[\zeta_N]$.*

This the main result of this section.

Theorem 8.3. *Let p be a prime such that $p \parallel N$ and $p^j \equiv -1 \bmod \frac{N}{p}$ for some integer j. Then $\mathbb{Z}_N$ does not have any pair of primitive formally dual subsets.*

Proof. The hypothesis clearly shows that p is self–conjugate mod$N$. Let T, S be a pair of primitive formally dual subsets of $\mathbb{Z}_N$. Without loss of generality, we assume $p \mid |T|$, so that $p \nmid |S|$. For every $d \mid N$ we have

$$|T(\zeta_N^d)|^2 = \mathbf{1}_S * \mathbf{1}_{-S}(d) \frac{|T|^2}{|S|},$$

hence $p^2 \mid |T(\zeta_N^d)|^2$. We consider the mask polynomial $T(X) \bmod (p, X^{N/p} - 1)$, and let $\mathfrak{P}$ be any prime ideal in $\mathbb{Q}(\zeta_N^p)$ that is above p. The degree of the residue field extension

$$f = [\mathbb{Z}[\zeta_N^p]/\mathfrak{P} : \mathbb{Z}/p\mathbb{Z}]$$

is also equal to the multiplicative order of $p \bmod \frac{N}{p}$. In particular, the ring epimorphism

$$\mathbb{Z}[\zeta_N^p] \twoheadrightarrow \kappa(\mathfrak{P}) := \mathbb{Z}[\zeta_N^p]/\mathfrak{P}$$

sends all $\frac{N}{p}$th roots of unity of $\mathbb{C}$ to the $\frac{N}{p}$th roots of unity of $\kappa(\mathfrak{P})$. Let $\overline{T}(X)$ be the image of $T(X)$ under the projection

$$\mathbb{Z}[X] \twoheadrightarrow \mathbb{F}_p[X].$$

Since $p^2 \mid |T(\zeta_N^d)|^2$ for every $d \mid N$, we must have

$$T(\zeta_N^d) \equiv 0 \bmod \mathfrak{P},$$

for every $d \mid N$ by Theorem 8.2; restricting to $p \mid d$, we observe that $\overline{T}(X)$ accepts as roots all $\frac{N}{p}$th roots of unity of $\kappa(\mathfrak{P}) \cong \mathbb{F}_{p^f}$, which yields

$$\overline{T}(X) \equiv 0 \bmod (X^{N/p} - 1).$$

Lifting up to $\mathbb{Z}[X]$, we obtain

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

or equivalently,

$$T(X^p) \equiv pQ(X^p) \bmod X^N - 1, \tag{8.1}$$

where we can take $Q(X) \in \mathbb{Z}_{\geq 0}[X]$. But $T(X^p) \bmod X^N - 1$ is also the mask polynomial of the multi-set $p \cdot T$; the multiplicities that appear in this multi-set are at most p, since T is a proper set. On the other hand, (8.1) shows that all multiplicities are at least p. This can only occur when $t \in T$ implies $t + jN/p \in T$ for all j, as these elements exactly have the same image under multiplication by p. Therefore, T is a union of p-cycles, in particular,

$$T(X) \equiv \Phi_p(X^{N/p})R(X) \bmod X^N - 1,$$

for some $R(X) \in \mathbb{Z}_{\geq 0}[X]$. Then, for every $t \in T$, $t - N/p \in T$, which shows that

$$\mathbf{1}_T * \mathbf{1}_{-T}(\tfrac{N}{p}) = |T|,$$

hence by (4.3), $|S(\zeta_p)| = |S|$, contradicting Proposition 4.6. □

Appendix A. Products of two powers of small primes

We will focus on $N = p^k q^l$, where $p, q < 10^3$. As mentioned at the end of Section 7, the field descent method tackles the cases where $k + l$ is large, and the polynomial method tackles those where $k + l$ is small, roughly speaking. Most of the times there is no gap, and when there is, it usually consists of a single exception. This search for exceptions is assisted by simple computer programs on wxMaxima[4]. In particular, for every pair (p, q) with $p < q < 10^3$ these programs compute $\nu_p(q^{p-1} - 1)$ and $\nu_q(p^{q-1} - 1)$ when $p > 2$; when $p = 2$ they compute $\nu_2(\frac{1}{2}\operatorname{ord}_4(q)(q^2 - 1))$, as well the number of possible exceptions from each pair of the form $(2, q)$.

Before proceeding, we will need two useful propositions for small primes, as well as the notions of a *Wieferich prime* and a *Wieferich pair* [26]:

Definition A.1. A prime p is called Wieferich, if $p^2 \mid 2^{p-1} - 1$. A pair of primes (p, q) is called a Wieferich pair, if $p^2 \mid q^{p-1} - 1$ and $q^2 \mid p^{q-1} - 1$.

There are only two known Wieferich primes, namely 1193 and 3511, and only 7 known Wieferich pairs (sequences A124121 and A124122 from OEIS[5]):

$(2, 1093), (3, 1006003), (5, 1645333507), (5, 188748146801), (83, 4871), (911, 318917), (2903, 18787)$.

Proposition A.2. *Let $N = p^3q^3$. If $\mathbb{Z}_N$ has a pair of primitive formally dual subsets, then p and q are simultaneously twin primes and a Wieferich pair.*

Proof. Let $T, S \subseteq \mathbb{Z}_N$ be such a pair with $|T| < |S|$. Since $|S(\zeta_N)|^2 \in \mathbb{Z}$, Proposition 7.2 implies that $pq \mid |S|$. Furthermore, since $\mathbf{1}_S * \mathbf{1}_{-S}(1)$ cannot be divisible by the cube of any integer > 1 by Proposition 7.2, we must also have $pq \mid |T|$. Without loss of generality, we consider $p < q$, so by Proposition 4.2 the only possibility for $|T|$ and $|S|$ is

$$|T| = p^2q, \ |S| = pq^2.$$

If N is even, then $p = 2$, hence by Corollary 4.7 we get $32q^2 = 2|T|^2 > N = 8q^3$, hence $q = 3$, and $|S(\zeta_N)|^2 = 27$ by Proposition 7.2. Applying Theorem 5.3 and Propositions 5.4 and 5.5, we obtain

$$27 \leq \frac{F(216, 27)^2}{4\varphi(F(216, 27))} = 18,$$

a contradiction by Proposition 5.5.

[4]Available at `https://sites.google.com/site/romanosdiogenesmalikiosis/computational-data`

[5]`http://oeis.org/A124121` and `http://oeis.org/A124122`

So, N must be odd. By Lemma 4.8, we get

$$pq\sqrt{(p-1)(q-1)} < p^2q,$$

or equivalently, $(p-1)(q-1) < p^2$, which cannot hold true unless $q = p+2$, i.e. p and q are twin primes. Since $|S| = pq^2$, we will have $|S(\zeta_N)|^2 = q^3$, so applying again Theorem 5.3 and Propositions 5.4 and 5.5 we get

$$q^3 \leq \frac{F(p^3q^3, q^3)^2}{4\varphi(F(p^3q^3, q^3))} = \frac{F(p^3q^3, q)}{4(1-\frac{1}{p})(1-\frac{1}{q})} = \frac{q\gcd(p^3, q^{p-1}-1)}{4(1-\frac{1}{p})(1-\frac{1}{q})},$$

or equivalently, $4(p-1)(q-1)q \leq p\gcd(p^3, q^{p-1}-1)$. This inequality can only hold when $p^3 \mid q^{p-1}-1$. We note that this cannot happen when $(p,q) = (3,5)$ or $(5,7)$, so we may assume that $p \geq 7$. Next, we examine

$$|T(\zeta_N)|^2 = \frac{|T|^3}{N}\mathbf{1}_S * \mathbf{1}_{-S}(1) = p^3\mathbf{1}_S * \mathbf{1}_{-S}(1).$$

By Lemma 4.8 we get

$$\mathbf{1}_S * \mathbf{1}_{-S}(1) < \frac{|S|^2}{\varphi(N)} = \frac{q^2}{(p-1)(q-1)} = 1 + \frac{4p+5}{p^2-1} \leq 1 + \frac{p(p-2)}{(p-1)(p+1)} < 2,$$

since $q = p+2$, so $\mathbf{1}_S * \mathbf{1}_{-S}(1) = 1$ and $|T(\zeta_N)|^2 = p^3$. Applying the field descent method, as was done with $|S(\zeta_N)|^2$, we also get $q^3 \mid p^{q-1}-1$, thus p and q form a Wieferich pair. □

We remark that p and q satisfy a stronger condition than the one given in Definition A.1; at any rate, these conditions never hold when $p, q < 10^3$. It is possible, however, that an application of the polynomial method (that was left out from the proof) would eventually show that no such $\mathbb{Z}_N$ has a primitive formal dual pair.

Proposition A.3. *Let $N = p^4q^3$. Then $\mathbb{Z}_N$ has no primitive formally dual subsets.*

Proof. Let $T, S \subseteq \mathbb{Z}_N$ be such a pair with $|T| < |S|$. Since $|S(\zeta_N)|^2 \in \mathbb{Z}$, Proposition 7.2 implies that $p^2q \mid |S|$. Furthermore, $pq \mid |T|$, since $\mathbf{1}_S * \mathbf{1}_{-S}(1)$ cannot be divided by a cube of an integer > 1. If $p \parallel |T|$, then we must necessarily have $p \mid \mathbf{1}_S * \mathbf{1}_{-S}(1)$, which can only happen if $p = 2$ or $p = 3$. If $p = 2$, so that $N = 16q^3$, then $|T| = 2q^2$; the only other possibility would be $|T| = 2q$, but this contradicts Corollary 4.7, as $2|T|^2 = 8q^2 < N$ in this case. Hence, $|S| = 8q$, and since $|S| > |T|$, we must have $q = 3$ and $|S(\zeta_N)|^2 = 32$ by Proposition 7.2. Applying Theorem 5.3 and Propositions 5.4 and 5.5 we get

$$32 \leq \frac{F(N,32)^2}{4\varphi(F(N,32))} = \frac{F(2^4 3^3, 2)}{4/3} = \frac{4\gcd(3^3, 2^2-1)}{4/3} = 9,$$

a contradiction. Assume next that $p = 3$. If $|T| = 3q$, then $|T|^2 < \varphi(N)$, hence the only possibility that remains by Lemma 4.8 is $|T| = 3q^2$ and $|S| = 27q$. Since $|S| > |T|$, we must have $q < 9$. Furthermore, since $|T|^2 > \varphi(N)$ by Lemma 4.8, we should have

$$9q^4 > 27q^2 \cdot 2(q-1) \Leftrightarrow q^2 > 6(q-1),$$

which yields $q > 4$. Lastly, since $3 \mid \mathbf{1}_S * \mathbf{1}_{-S}(1)$, we must have $\mathbf{1}_S * \mathbf{1}_{-S}(1) = 3$ by Proposition 7.2, which implies $3\varphi(N) < |S|^2$ by Lemma 4.8. Hence,

$$3^4q^2 \cdot 2(q-1) < 3^6q^2 \Leftrightarrow 2(q-1) < 9,$$

yielding $q \leq 5$, thus $q = 5$, and $|S(\zeta_N)|^2 = 3^5$ by Proposition 7.2. Applying Theorem 5.3 and Propositions 5.4 and 5.5 we get

$$3^5 \leq \frac{F(N,3^5)^2}{4\varphi(F(N,3^5))} = \frac{F(N,3)}{4 \cdot \frac{2}{3} \cdot \frac{4}{5}} < \frac{1}{2} \cdot 3\gcd(5^3, 3^4-1) = \frac{15}{2},$$

a contradiction.

Therefore, $p \parallel |T|$ cannot hold; p^2q divides both $|T|$ and $|S|$. The only possibility is $|T| = p^2q$ and $|S| = p^2q^2$. The inequality $\varphi(N) < |T|^2$ would then imply $(p-1)(q-1) < p$, which only holds when $q = 2$. Applying Corollary 4.7 we establish a contradiction, as $2|T|^2 = 8p^4 = N$, completing the proof. □

Proposition A.4. *Let $N = p^m q^3$, with $m \geq 5$ and $p, q < 10^3$. Then $\mathbb{Z}_N$ has no primitive formally dual subsets.*

Proof. Let $T, S \subseteq \mathbb{Z}_N$ be such a pair of subsets with $|S| > |T|$. As before, Proposition 7.2 yields $q \mid |S|$ and $q \mid |T|$. We distinguish two cases.

$\boxed{q \parallel |S|}$ As $|S(\zeta_N)|^2 = \frac{|S|^3}{N}$, this must be equal to a power of p; furthermore, $|S(\zeta_N)|^2 > \sqrt{N} \geq p^{5/2}q^{3/2}$. Applying Theorem 5.3 and Proposition 5.4, we get

$$p^{5/2}q^{3/2} < \frac{F(N, |S(\zeta_N)|^2)^2}{4\varphi(F(N, |S(\zeta_N)|^2))} = \frac{F(N,p)}{4(1-\frac{1}{p})(1-\frac{1}{q})}. \tag{A.1}$$

If $p = 2$, then $F(N,2) \leq 4\gcd(q^3, 2^{q-1}-1) = 4q$, by Proposition 5.5 and the fact that no prime $q < 10^3$ is Wieferich. Therefore, (A.1) gives $2\sqrt{2}(q-1) < \sqrt{q}$, which never holds. If $q = 2$, then $F(N,p) \leq p\gcd(8, p^2-1) = 8p$, by Proposition 5.5, since p is odd. In this case, (A.1) gives $\sqrt{p}(p-1) < \sqrt{2}$, which again never holds. So, we assume that N is odd. Then, (A.1) becomes

$$p^{5/2}q^{3/2} < \frac{p\gcd(q^3, p^{q-1}-1)}{4(1-\frac{1}{p})(1-\frac{1}{q})} < \frac{1}{2}pq^a,$$

where $a \leq 3$. This in turn yields

$$2p^{3/2} < q^{a-3/2}, \tag{A.2}$$

and as the right hand side is $< q^{3/2}$, we must certainly have $p < q$. A simple search for primes $p < q < 10^3$ reveals that we never have $q^3 \mid p^{q-1}-1$, so $a \leq 2$. If $a = 1$, (A.2) cannot hold; the only pairs of primes (p,q) with $p < q < 10^3$ and $q^2 \mid p^{q-1}-1$ are

$$(3,11), (11,71), (13,863), (19,137), (71,331), (127,907). \tag{A.3}$$

However, none of them satisfies $2p\sqrt{p} < \sqrt{q}$, therefore we cannot have $q \parallel |S|$.

$\boxed{q \parallel |T|}$ Then $\frac{|T|^3}{N}$ is a power of p. For $p, q \geq 7$, we have

$$\mathbf{1}_S * \mathbf{1}_{-S}(1) < \frac{|S|^2}{\varphi(N)} < \frac{N^2}{\varphi(N)^2} = \left(\frac{pq}{(p-1)(q-1)}\right)^2 \leq \left(\frac{77}{60}\right)^2 < 2,$$

and if $p, q \geq 5$ with $p, q \neq 7$, then

$$\mathbf{1}_S * \mathbf{1}_{-S}(1) < \left(\frac{pq}{(p-1)(q-1)}\right)^2 \leq \left(\frac{55}{40}\right)^2 < 2,$$

so in both cases,

$$|T(\zeta_N)|^2 = \frac{|T|^3}{N}.$$

In these cases, we get

$$\frac{|T|^3}{N} \leq \frac{F(N, |T(\zeta_N)|^2)^2}{4\varphi(F(N, |T(\zeta_N)|^2))} = \frac{F(N,p)}{4(1-\frac{1}{p})(1-\frac{1}{q})} = \frac{p\gcd(q^3, p^{q-1}-1)}{4(1-\frac{1}{p})(1-\frac{1}{q})}.$$

By Lemma 4.8, we get

$$\frac{|T|^3}{N} > \frac{\varphi(N)^{3/2}}{N} = \sqrt{N}\Big[(1-\tfrac{1}{p})(1-\tfrac{1}{q})\Big]^{\frac{3}{2}}.$$

Combining the above, we get

$$p^{5/2}q^{3/2} \leq \sqrt{N} < pq^a,$$

since $4[(1-\frac{1}{p})(1-\frac{1}{q})]^{5/2} > 1$ when $p, q \geq 5$, where $q^a = \gcd(q^3, p^{q-1}, 1)$. The above is equivalent to $p\sqrt{p} < q^{a-3/2}$, and as the latter is $\leq q\sqrt{q}$, we must have $p < q$. Again, with a simple computer search we find that we cannot have $a = 3$ for such primes with $p < q < 10^3$; moreover, if $a = 1$, $p\sqrt{p} < q^{a-3/2}$ cannot hold, so we must have $a = 2$ and $p^3 < q$. We are led again to the pairs in (A.3), but none satisfies $p^3 < q$. The only case that is not tackled for $p, q \geq 5$ is when we have the pair $(5,7)$, or equivalently, $35 \mid N$. In that case, by Theorem 5.3 and Propositions 5.4 and 5.5 we get

$$5^{5/2}7^{3/2} \leq \sqrt{N} < |S(\zeta_N)|^2 \leq \frac{F(N, |S(\zeta_N)|^2)^2}{4\varphi(F(N, |S(\zeta_N)|^2))} \leq \frac{F(N,35)}{4 \cdot \frac{24}{35}} = \frac{5^3 7^2}{96},$$

since $5^2 \parallel 7^4 - 1$ and $7 \parallel 5^6 - 1$. But this leads to $96 < \sqrt{35}$ a contradiction.

Next, assume that N is odd and $p = 3$. Then $\sqrt{N} \geq 3^{5/2} q^{3/2}$ and

$$\sqrt{N} < |S(\zeta_N)|^2 \leq \frac{F(N, |S(\zeta_N)|^2)^2}{4\varphi(F(N, |S(\zeta_N)|^2))} \leq \frac{F(N, 3q)}{\frac{8}{3}(1 - \frac{1}{q})},$$

yielding

$$8 \cdot 3^{3/2} \sqrt{q}(q-1) < \gcd(3^m q^3, (3^{q-1} - 1)(q^2 - 1)), \tag{A.4}$$

by Theorem 5.3 and Propositions 5.4 and 5.5. If $q \neq 11$ and $q < 10^3$, then the right hand side is $q \gcd(3^m, q^2 - 1) \leq 3^{\nu_3(q^2-1)}$. The left hand side is $> 3^3$, as $8 > 3^{3/2}$ and $q - 1 > \sqrt{q}$ for all odd primes q; hence, $\nu_3(q^2 - 1) \geq 4$, therefore $q \geq 163$. At any rate, $\nu_3(q^2 - 1) \leq 5$ for $q < 10^3$, yielding

$$\frac{q-1}{\sqrt{q}} < \frac{3^{7/2}}{8},$$

which is a contradiction, as $6 > \frac{3^{7/2}}{8}$ and $\frac{q-1}{\sqrt{q}} > 12$ for $q \geq 163$. If $q = 11$, (A.4) becomes

$$8 \cdot 3^{3/2} \frac{10}{\sqrt{11}} < 3 \cdot 11^2,$$

which holds. Applying Theorem 5.3 and Propositions 5.4 and 5.5 on $|S(\zeta_N)|^2 > \sqrt{N}$ gives

$$3^{5/2} 11^{3/2} \leq \sqrt{N} < \frac{F(N, 33)^2}{4\varphi(F(N, 33))} = \frac{3 \cdot 11^2}{\frac{80}{33}}$$

or $80\sqrt{3} < 11\sqrt{11}$, a contradiction.

If N is odd and $q = 3$, then applying Theorem 5.3 and Propositions 5.4 and 5.5 for $|S(\zeta_N)|^2 > \sqrt{N} \geq 3^{3/2} p^{5/2}$,

$$3^{3/2} p^{5/2} < \frac{F(N, 3p)^2}{4\varphi(F(N, 3p))}$$

holds, or equivalently,

$$8\sqrt{3} p^{3/2}(p-1) < \gcd(p^m 3^3, (p^2 - 1)(3^{p-1} - 1)).$$

If $p \neq 11$ and $p < 10^3$, then the right hand side is $p \gcd(27, p^2 - 1) \leq 27p$, so we must have

$$8\sqrt{p}(p-1) < 9\sqrt{3} < 16,$$

whence $\sqrt{p}(p-1) < 2$, a contradiction, as $p \geq 3$ does not satisfy this inequality. If $p = 11$, then we get $8 \cdot 11^{3/2}\sqrt{3} \cdot 10 < 3 \cdot 11^2$ or $80 < \sqrt{33}$, a contradiction.

Lastly, suppose that N is even. Assume first that $p = 2$, so that $|S(\zeta_N)|^2 > \sqrt{N} = 2^{m/2} q^{3/2}$. By Theorem 5.3 and Propositions 5.4 and 5.5 we get

$$2^{m/2} q^{3/2} < \frac{F(N, |S(\zeta_N)|^2)}{4\varphi(F(N, |S(\zeta_N)|^2))} \leq \frac{F(N, 2q)}{2(1 - \frac{1}{q})},$$

yielding

$$2^{\frac{m}{2}+1} \sqrt{q}(q-1) < \gcd(2^m q^3, (2^{q-1} - 1)(\tfrac{1}{2} \operatorname{ord}_4(q)(q^2 - 1))) = q \gcd(2^m, \tfrac{1}{2} \operatorname{ord}_4(q)(q^2 - 1)),$$

as no prime $q < 10^3$ is Wieferich. We put $2^a = \gcd(2^m, \frac{1}{2} \operatorname{ord}_4(q)(q^2 - 1))$; for $q < 10^3$, $a \leq 8$ holds. Furthermore, the above inequality yields

$$q - 1 < 2^{a - \frac{m}{2} - 1} \sqrt{q}. \tag{A.5}$$

By definition, $a \leq m$, so the right hand side is $\leq 2^{\frac{a}{2}-1}\sqrt{q} \leq 8\sqrt{q}$, as

$$\nu_2(\tfrac{1}{2} \operatorname{ord}_4(q)(q^2 - 1)) \leq 8$$

when $q < 10^3$. The inequality $q - 1 < 8\sqrt{q}$ further yields $q \leq 67$; for these primes,

$$\nu_2(\tfrac{1}{2} \operatorname{ord}_4(q)(q^2 - 1)) \leq 6,$$

which in turn implies $q - 1 < 4\sqrt{q}$, therefore $q \leq 17$. Repeating this argument once again, we deduce

$$\nu_2(\tfrac{1}{2} \operatorname{ord}_4(q)(q^2 - 1)) \leq 4.$$

Since $m \geq 5$, (A.5) gives

$$q - 1 < \sqrt{2q},$$

which can only hold for $q = 3$. However, $\nu_2(\frac{1}{2}\operatorname{ord}_4(3)(3^2-1)) = \nu_2(8) = 3$, so substituting at (A.5) we obtain $q - 1 < \sqrt{\frac{q}{2}}$, a contradiction. The last case is N even and $q = 2$. As before, we apply Theorem 5.3 and Propositions 5.4 and 5.5 on $|S(\zeta_N)|^2$, getting

$$p^{m/2}2^{3/2} = \sqrt{N} < |S(\zeta_N)|^2 \leq \frac{F(N, |S(\zeta_N)|^2)^2}{4\varphi(F(N, |S(\zeta_N)|^2))} \leq \frac{F(N, 2p)}{2(1-\frac{1}{p})},$$

or equivalently,

$$p^{\frac{m}{2}-1}2^{5/2}(p-1) < \gcd(2^3p^m, \tfrac{1}{2}\operatorname{ord}_4(p)(p^2-1)(2^{p-1}-1)) = p\gcd(8, \tfrac{1}{2}\operatorname{ord}_4(p)(p^2-1)) \leq 8p,$$

as no prime $p < 10^3$ is Wieferich. The above gives

$$p^{\frac{m}{2}-2}(p-1) < \sqrt{2},$$

a contradiction, wince the left hand side is $\geq \sqrt{p}(p-1) > 2$, concluding the proof. □

Proposition A.5. *Let $N = p^m q^n$, with $m, n \geq 4$ and $p, q < 10^3$. Then $\mathbb{Z}_N$ has no primitive formally dual subsets.*

Proof. Without loss of generality, we assume $p < q$. Also, we suppose that $T, S \subseteq \mathbb{Z}_N$ is a primitive pair of formally dual sets with $|S| \geq |T|$. Then by Proposition 7.2,

$$|S(\zeta_N)|^2 = \frac{|S|^3}{N} \geq \sqrt{N} \geq p^2q^2.$$

Applying Theorem 5.3 and Propositions 5.4 and 5.5 we obtain

$$p^2q^2 \leq \frac{F(N, |S(\zeta_N)|^2)^2}{4\varphi(F(N, |S(\zeta_N)|^2))} \leq \frac{F(N, pq)}{4(1-\frac{1}{p})(1-\frac{1}{q})}. \tag{A.6}$$

Suppose first that N is odd; for $p, q < 10^3$, we have either $F(N, pq) = p^a q$ for some $a \leq 5$ or $F(N, pq) = pq^2$. In the latter case, (A.6) yields

$$4(1-\tfrac{1}{p})(1-\tfrac{1}{q})p < 1,$$

a contradiction, as the left hand side is $> 2p$. In the former case, we get

$$4(1-\tfrac{1}{p})(1-\tfrac{1}{q})q < p^{a-2}$$

which implies

$$2q < p^{a-2}, \tag{A.7}$$

since $4(1-\frac{1}{p})(1-\frac{1}{q}) \geq 4 \cdot \frac{8}{15} > 2$ when p, q are odd primes. Therefore, either $a = 4$ or $a = 5$; both cases occur only when $q \geq 163$. The case $a = 5$ happens only for $p = 3$; (A.7) cannot hold, as $326 \leq 2q < 27$ is false. Moreover, $a = 4$ happens for $p \leq 13$, but again (A.7) fails, as $p^2 \leq 169 < 326 \leq 2q$.

Next, suppose that N is even, that is $p = 2$. (A.6) gives

$$8q(q-1) \leq F(N, 2q) = \gcd(2^m q^n, \tfrac{1}{2}\operatorname{ord}_4(q)(q^2-1)(2^{q-1}-1)) = 2^a q, \tag{A.8}$$

since no prime $q < 10^3$ is Wieferich; here, $a = \min(m, \nu_2(\frac{1}{2}\operatorname{ord}_4(q)(q^2-1)))$. (A.8) is equivalent to

$$q - 1 < 2^{a-3}. \tag{A.9}$$

For $q < 10^3$, $\nu_2(\frac{1}{2}\operatorname{ord}_4(q)(q^2-1)) \leq 8$ holds, so (A.9) implies $q - 1 < 32$ or $q \leq 31$. For this range of primes, $\nu_2(\frac{1}{2}\operatorname{ord}_4(q)(q^2-1)) \leq 6$, so (A.9) further gives $q - 1 < 8$ or $q \leq 7$. This argument once again gives $\nu_2(\frac{1}{2}\operatorname{ord}_4(q)(q^2-1)) \leq 4$, so (A.9) implies $q - 1 < 2$, a contradiction, concluding the proof. □

The number of prime pairs (p, q) with $p < q < 10^3$ is 14028. Propositions 7.4, 7.5, 7.6, A.2, A.3, A.4, A.5 show that the only possible exceptions come from orders N of the form $p^{2k}q^2$. The number of pairs with possible exceptions is only 162, and the total number of exceptions (that cannot be solved with the methods developed here) is 290.

Indeed, we consider first the case $p = 2$; then, either $N = 2^{2k}q^2$ or $4q^{2k}$. Applying (7.2) and (7.3) in the latter case, we obtain

$$2q^2 \leq \sqrt{N} \leq \frac{4q}{2(1-\frac{1}{q})}.$$

We remark that $b = 1$ in (7.3), as no prime $q < 10^3$ is Wieferich; furthermore, the quantity $F(N, n)$ in (7.3) is $\leq F(N, 2q) = 4q$ due to Proposition 5.5. The above gives $q - 1 \leq 1$ a contradiction. Thus, all such exceptions are of the form $2^{2k}q^2$, $k \geq 2$, hence applying (7.2) and (7.3) we obtain

$$2^k q \leq \frac{2^a q}{2(1-\frac{1}{q})},$$

which is equivalent to $2 \leq k \leq a - 1$, giving $a - 2$ exceptions. We can easily calculate a for every $q < 10^3$ and verify[6] that the number of such exceptions for N even are 240.

If N is odd, we have possible exceptions of the form $p^{2k}q^2$ or p^2q^{2k}, for $p < q < 10^3$. Inequalities (7.2) and (7.3) give in the former case

$$p^k q \leq \frac{p^a q^b}{4(1-\frac{1}{p})(1-\frac{1}{q})} < \frac{1}{2}p^a q^b.$$

We either have $a = 1$ or $b = 1$ when $p, q < 10^3$. For $a = 1$ the above inequality can only hold for $b > 1$, however, since $b \leq 2$ if $a = 1$, we get the pairs from (A.3). The previous inequality becomes $2p^{k-1} < q$, and we have a total of 7 exceptions; every pair has an exception of the form p^4q^2 and there is also the additional exception 13^6863^2. When $b = 1$, the inequality becomes $2p^k < p^a$ or $k < a$, or $a - 2$ exceptions for every such pair as $k \geq 2$. We can calculate all such exceptions[7]; they are another 42 in total which come from 32 pairs, and this tackles the case $N = p^{2k}q^2$ with $p < q < 10^3$, which gives a total of 49 cases. When $N = p^2q^{2k}$, we have only one other possible exception, namely 13^2239^4; indeed, (7.2) and (7.3) give

$$pq^k \leq \frac{p^a q^b}{4(1-\frac{1}{p})(1-\frac{1}{q})} < \frac{1}{2}p^a q^b.$$

If $a = 1$ we would have $b \leq 2$ and $pq^k < pq^2$, a contradiction, as $k \geq 2$. So $b = 1$, so the above inequality becomes $2q^{k-1} < p^{a-1}$, which is only satisfied for $p = 13$, $q = 239$, $k = 2$, thus obtaining a total of 50 possible exceptions when N is odd. Therefore, the total number of possible exceptions is 290.

References

1. H. Cohn, A. Kumar, C. Reiher, and A. Schürmann, *Formal duality and generalizations of the Poisson summation formula*, Discrete geometry and algebraic combinatorics, Contemp. Math., vol. 625, Amer. Math. Soc., Providence, RI, 2014, pp. 123–140.
2. H. Cohn, A. Kumar, and A. Schürmann, *Ground states and formal duality relations in the gaussian core model*, Phys. Rev. E **80** (2009), 061116.
3. A. Córdoba, *La formule sommatoire de Poisson*, C. R. Acad. Sci. Paris Sér. I Math. **306** (1988), no. 8, 373–376. MR 934622
4. Ethan M. Coven and Aaron Meyerowitz, *Tiling the integers with translates of one finite set*, J. Algebra **212** (1999), no. 1, 161–174.
5. N. G. de Bruijn, *On the factorization of cyclic groups*, Nederl. Akad. Wetensch. Proc. Ser. A. **56** = Indagationes Math. **15** (1953), 370–377.
6. A. Georgakopoulos and M. N. Kolountzakis, *On particles in equilibrium on the real line*, To appear in Proc. AMS.
7. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008, Revised by D. R. Heath-Brown and J. H. Silverman, With a foreword by Andrew Wiles.
8. T. Y. Lam and K. H. Leung, *On vanishing sums of roots of unity*, J. Algebra **224** (2000), no. 1, 91–109.
9. K. H. Leung and B. Schmidt, *The field descent method*, Des. Codes Cryptogr. **36** (2005), no. 2, 171–188.
10. R. D. Malikiosis and M N. Kolountzakis, *Fuglede's conjecture on cyclic groups of order p^nq*, 11pp., `https://arxiv.org/abs/1612.01328`.
11. D. A. Marcus, *Number fields*, Springer-Verlag, New York-Heidelberg, 1977, Universitext.

[6] Check `orders2.wxmx` at `https://sites.google.com/site/romanosdiogenesmalikiosis/computational-data`

[7] Check `orders.wxm` at `https://sites.google.com/site/romanosdiogenesmalikiosis/computational-data`

12. J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
13. S. Ramanujan, *On certain trigonometrical sums and their applications in the theory of numbers [Trans. Cambridge Philos. Soc.* **22** *(1918), no. 13, 259–276]*, Collected papers of Srinivasa Ramanujan, AMS Chelsea Publ., Providence, RI, 2000, pp. 179–199.
14. L. Rédei, *Ein Beitrag zum Problem der Faktorisation von endlichen Abelschen Gruppen*, Acta Math. Acad. Sci. Hungar. **1** (1950), 197–207. MR 0045729
15. ———, *Über das Kreisteilungspolynom*, Acta Math. Acad. Sci. Hungar. **5** (1954), 27–28.
16. H. E. Rose, *A course in number theory*, second ed., Oxford Science Publications, The Clarendon Press, Oxford University Press, New York, 1994.
17. H. J. Ryser, *Combinatorial mathematics*, The Carus Mathematical Monographs, No. 14, Published by The Mathematical Association of America; distributed by John Wiley and Sons, Inc., New York, 1963.
18. B. Schmidt, *Cyclotomic integers and finite geometry*, J. Amer. Math. Soc. **12** (1999), no. 4, 929–952.
19. ———, *Characters and cyclotomic fields in finite geometry*, Lecture Notes in Mathematics, vol. 1797, Springer-Verlag, Berlin, 2002.
20. I. J. Schoenberg, *A note on the cyclotomic polynomial*, Mathematika **11** (1964), 131–136.
21. R. Schüler, *Formal-dual subsets of cyclic groups of prime power order*, 13pp., `https://arxiv.org/abs/1605.05939`.
22. R. E. Schwartz, *The Five-Electron Case of Thomson's Problem*, Experimental Mathematics **22** (2013), no. 2, 157–186.
23. Terence Tao and Van Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, vol. 105, Cambridge University Press, Cambridge, 2006.
24. R. J. Turyn, *Character sums and difference sets*, Pacific J. Math. **15** (1965), 319–346.
25. L. C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.
26. A. Wieferich, *Zum letzten Fermatschen Theorem*, J. Reine Angew. Math. **136** (1909), 293–302.
27. J. Xia, S. Park, and H. Cohn, *Classification of formal duality with an example in sphere packing*, 21pp., `https://math.mit.edu/research/undergraduate/urop-plus/documents/2016/Xia.pdf`.

Technische Universität Berlin, Institut für Mathematik, Sekretariat MA 4-1, Strasse des 17. Juni 136,I D-10623 Berlin, Germany

E-mail address: `malikios@math.tu-berlin.de`