EXPOSITIONES MATHEMATICAE

Expo. Math. 20 (2002): 215–228

www.urbanfischer.de/journals/expomath

Interplay Between Four Conjectures on Certain Zero-Sum Problems

R. Thangadurai

The Institute of Mathematical Sciences, C.I.T. Campus, Taramani, Chennai 600113, India

Abstract. In this paper, we explore the interplay of four different conjectures on certain zero-sum problems in $\mathbf{Z}_p \oplus \mathbf{Z}_p$. This study of the inter-relations between these conjectures leads to the conclusion that determining the structure of minimal zero sequences (see below for the precise definition) is crucial. Also, we study the analogous situation in $\mathbf{Z}_n$.

1. Introduction and Notations

Additive number theory, factorization theory and graph theory provide a good source for combinatorial problems in finite abelian groups (for instance, see [17], [18], [7], [19] and [2]). Among them, zero sum problems have been of growing interest. The cornerstone of almost all recent combinatorial research on zero-sum problems is a 40-years old theorem of Erdős-Ginzburg-Ziv and a question of H. Davenport on an invariant of finite abelian groups.

Let G be a finite abelian group. We denote the cyclic group with n elements by $\mathbf{Z}_n$. Then $G = \mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_r}$ with $n_1 > 1$ and n_i dividing n_{i+1} for $1 \leq i < r$, where $n_r = \exp(G)$ is the exponent of G (exponent of G is the least common multiple of the orders of all the elements of G) and r is the rank of G. Most of our discussion will be centered around the group $G = \mathbf{Z}_n \oplus \mathbf{Z}_n$. Clearly, in this case, $\exp(G) = n$ and $r(G) = 2$. We denote an arbitrary prime number by p and an arbitrary natural number by n.

In general, our notations and terminology will be the same as the one in factorial theory (cf. survey articles by Chapman, Halter-Koch and Geroldinger in [2] and the paper of Gao and Geroldinger [14]). Let $\mathcal{F}(G)$ denote the free abelian monoid with basis G. The elements of $\mathcal{F}(G)$ will be called **sequences**. The monoid homomorphism

$$\sigma : \mathcal{F}(G) \longrightarrow G \text{ by } \sigma(S = \prod_{\nu=1}^{\ell} g_\nu) = \sum_{\nu=1}^{\ell} g_\nu$$

maps a sequence to the sum of its elements. Let $S = \prod_{\nu=1}^{\ell} g_\nu \in \mathcal{F}(G)$ be a sequence. Then S has a unique representation of the form

$$S = \prod_{g \in G} g^{v_g(S)} \in \mathcal{F}(G),$$

Current address: Stat-Math Division, Indian Statistical Institute, 203, B. T. Road, Kolkata 700035, India.
E-mail address: thanga_v@isical.ac.in

0732-0869/02/20/3-215 $15.00/0

where $v_g(S)$ is the number of times g appears in S and $|S| = \sum_{g \in G} v_g(S) = \ell \in \mathbb{N}$ is called the **length** of S. We say that $T \in \mathcal{F}(G)$ is a subsequence of S and we write $T|S$, if $v_g(T) \leq v_g(S)$ for every $g \in G$. As usual, we say that $T, T' \in \mathcal{F}(G)$ are disjoint subsequences of S if their product TT' is a subsequence of S. The identity element $1 \in \mathcal{F}(G)$ will be called the **empty sequence**, and we have $|1| = 0$. Whenever $T|S$, by the element $R = ST^{-1} \in \mathcal{F}(G)$ we mean the sequence with T deleted from S. Clearly, $RT = S$. We say that the sequence S is

a **zero sequence**, if $\sigma(S) = \sum_{k=1}^{\ell} g_k = 0$,

a **zero-free** sequence, if S does not have any zero subsequences,

a **minimal zero sequence**, if it is a zero sequence and each proper subsequence is zero-free,

a **short zero sequence**, if it is a zero sequence with $1 \leq |S| \leq \exp(G)$.

In factorization theory, the set of all zero-sequences is a submonoid of $\mathcal{F}(G)$. Its irreducible elements are the minimal zero sequences. For further reading, one may refer to [5], [2] and [6].

We denote $\eta(G)$ the least positive integer such that whenever $S \in \mathcal{F}(G)$ with $|S| \geq \eta(G)$ is given, then there exists a short zero subsequence T of S. Also, with these notations, the Davenport constant $D(G)$ is defined to be the maximum length of the minimal zero sequence in G. It is easy to see that $D(\mathbf{Z}_n) = \eta(\mathbf{Z}_n) = n$.

2. Four Conjectures and Their Interplay

2.1 Conjectures and Their Status

In 1969, Olson [21] proved that $D(\mathbf{Z}_p^d) = d(p-1)+1$ where $\mathbf{Z}_p^d := \underbrace{\mathbf{Z}_p \oplus \mathbf{Z}_p \oplus \cdots \mathbf{Z}_p}_{d \text{ times}}$. Using this, he proved the following theorem.

Theorem 2.1.1 (Olson, 1969, [21]) $\eta(\mathbf{Z}_p \oplus \mathbf{Z}_p) = 3p - 2$.

This theorem was extended to every natural number by van Emde Boas [28], who made the following conjecture.

Conjecture 1. (van Emde Boas, 1969, [28]) *Let $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 3n-3$. If S does not contain any short zero subsequences, then $S = a^{n-1}b^{n-1}c^{n-1}$, where $a, b, c \in \mathbf{Z}_n \oplus \mathbf{Z}_n$ are distinct elements.*

van Emde Boas [28] verified Conjecture 1 for primes $p = 2, 3, 5, 7$ using a computer. Recently, W. D. Gao [11] proved that if Conjecture 1 is true for $n = k$ and $n = m$, then it is true for $n = km$. Thus, it follows that if Conjecture 1 is true for all primes, then it is true for all natural numbers n.

By Theorem 2.1.1, we know that there exists a short zero subsequence. In 1973, Harborth [15] considered the existence problem of a zero subsequence of prescribed length p. More precisely, $f(p)$ is the least positive integer such that, given any arbitrary element $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$, with $|S| \geq f(p)$, S contains a zero subsequence of length p. He proved that $f(2) = 5$ and $f(3) = 9$. Later, Kemnitz [16] proved that $f(5) = 17$ and $f(7) = 25$. Also, he conjectured the following.

Conjecture 2. (Kemnitz, 1983, [16]) *For every prime p, we have $f(p) = 4p - 3$.*

This conjecture was first made by Kemnitz and was suggested, independently, by N. Zimmerman and Y. Peres. It is trivial to see that if the conjecture holds for two integers m and n, it is also true for mn. So, if one proves it for all primes, then it holds for all natural numbers.

In 1996, W. D. Gao [9] proved that if $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 4n - 3$ and $T = a^{n-1}$ as its subsequence for some $a \in \mathbf{Z}_n \oplus \mathbf{Z}_n$, then S satisfies Conjecture 2. Moreover, he proved that if $f(n) = 4n-3$ and $n \geq ((3m-4)(m-1)m^2+3)/4m$ with $m \geq 2$, then $f(nm) = 4nm - 3$. These results were improved upon by the author in [26] where it has, in fact, been proved that if $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 4n - 3$ and $T = a^s$ as its subsequence with $s \geq \lfloor \frac{n}{2} \rfloor$, then S satisfies Conjecture 2 and that if $f(n) = 4n - 3$ and $n > (2m^3 - 3m^2 + 3)/4m$, with $m \geq 2$, then $f(nm) = 4nm - 3$.

In another direction, in 1995, Alon and Dubiner [1] gave the upper bound $f(n) \leq 6n - 5$ for all $n \in \mathbf{N}$. Later, this was improved to $f(p) \leq 5p - 1$ for all prime p by W. D. Gao [10]. In 2000, L. Rónyai [20] proved that $f(p) \leq 4p - 2$ for all primes p. From this bound, he concluded that $f(n) \leq (41/10)n$. Recently, W. D. Gao [12] proved that $f(p^k) \leq 4p^k - 2$ for all primes p and $k \geq 1$.

Clearly, $f(n) \geq 4n - 3$, as the example $S = (0,0)^{n-1}(0,1)^{n-1}(1,0)^{n-1}(1,1)^{n-1}$ in $\mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ shows. W. D. Gao,[11] conjectured the following.

Conjecture 3 (W. D. Gao, 2000, [11]) *If $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 4p-4$ is such that S does not contain any zero subsequences of length p, then $S = a^{p-1}b^{p-1}c^{p-1}d^{p-1}$, where $a, b, c, d \in \mathbf{Z}_p \oplus \mathbf{Z}_p$ are all distinct elements.*

In the same paper, Gao proved that if Conjecture 3 is true for all primes, then it is true for all natural numbers. He also verified this conjecture for $p = 2, 3$ and 5. Recently, it has been proved in [25] that Conjecture 3 is true for $p = 7$.

In 1998, Gao and Geroldinger [14] studied the structure of long minimal zero sequences in G. There they conjectured the following.

Conjecture 4. (Gao and Geroldinger, 1998, [14]) *If $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 2p-1$ is a minimal zero sequence, then there exists a subsequence $T = a^{p-1}$ of S for some $a \in \mathbf{Z}_p \oplus \mathbf{Z}_p$.*

They verified Conjecture 4 for primes $p = 2, 3, 5$ and 7.

2.2 Inter-Relationships

In this subsection, we shall explore the inter-relations between these four conjectures.

Theorem 2.2.1 (W. D. Gao, 2000, [11]) *Conjecture 3 implies Conjecture 2.*

Proof. Suppose not. Let $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 4n-3$, which admits no zero subsequence of length n. Then no subsequence can admit a zero sum of length n. Fix $x \in S$ and $T = Sx^{-1}$. Then by Conjecture 3, T is of the form $a^{n-1}b^{n-1}c^{n-1}d^{n-1}$. Let $T_1 = Sa^{-1} = xa^{n-2}b^{n-1}c^{n-1}d^{n-1}$. Once again by Conjecture 3, $x = a$. Then a^n is a subsequence of S of length n having zero sum. This contradiction proves the Theorem. □

Theorem 2.2.2 *Conjecture 3 implies Conjecture 1.*

Proof. Let $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 3n-3$ such that S does not have any short zero subsequences. Therefore, every element appearing in S is non-zero in $\mathbf{Z}_n \oplus \mathbf{Z}_n$. Consider $S_1 := (0,0)^{n-1}S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S_1| = 4n-4$. Note that S cannot have a zero subsequence of length n. Hence S_1 does not have a zero subsequence of length n. By Conjecture 3, $S_1 = (0,0)^{n-1}a^{n-1}b^{n-1}c^{n-1}$, where $a, b, c \in \mathbf{Z}_n \oplus \mathbf{Z}_n$ are distinct elements. That is, Conjecture 1 is true. □

Remark. Assume Conjecture 1. If $S = a^{n-1}\prod_{i=1}^{3n-3} b_i \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 4n-4$ such that S doesn't have any zero subsequences of length n. Let $S_1 = S - a$ be the translation of S by a. Then S_1 does not have a zero subsequence of length n. Hence by Conjecture 1, $S_1 = (0,0)^{n-1}b_1^{n-1}c_1^{n-1}d_1^{n-1}$. Therefore $S = a^{n-1}b^{n-1}c^{n-1}d^{n-1}$, where $b = b_1 + a$, $c = c_1 + a$ and $d = d_1 + a$. We improve this observation further in the following theorem.

Theorem 2.2.3 *Assume Conjecture 1. Let $S = a^s \prod_j a_j \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $s > [\frac{n-3}{2}]$ and $|S| = 4n-4$. Suppose S does not contain a zero subsequence of length n. Then S is of the form $a^{n-1}b^{n-1}c^{n-1}d^{n-1}$ for some $a, b, c, d \in \mathbf{Z}_n \oplus \mathbf{Z}_n$.*

Proof. Let $S = a^s \prod_{i=1}^{4n-4-s} a_i \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 4n-4$ and $s > [\frac{n-3}{2}]$. Translate the given $4n-4$ elements by a. We get $S - a = (0,0)^s \prod_{i=1}^{4n-4-s} b_i$, where $b_i = a_i - a \neq (0,0) \in \mathbf{Z}_n \oplus \mathbf{Z}_n$. Let $S^* = \prod_{i=1}^{4n-4-s} b_i$.

In order to prove this theorem, we shall prove that when $s = n-1$, the sequence $S-a$ will be of the form $(0,0)^{n-1}x^{n-1}y^{n-1}z^{n-1} \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$, where $x, y, z \in \mathbf{Z}_n \oplus \mathbf{Z}_n$ are distinct elements. When $s < n-1$, we produce a zero subsequence of $S - a$ of length n so that we get a contradiction and hence the case $s < n-1$ cannot happen.

Case (i) $(s = n-1)$

This is same as the above remark.

Case (ii) ($[\frac{n-3}{2}] < s \leq n-2$)
In this case, $|S^*| = 4n - 4 - s \geq 3n - 2$. Therefore, S^* contains a short zero subsequence T, by Theorem 2.1.1 In fact, $|T| < n - s$. That is,

$$|T| + s \leq n - 1. \tag{1}$$

Otherwise, T together with $n - |T|$ zeros will produce a zero subsequence of length n, which is a contradiction of the assumption.

Since $|S^*| \geq 3n - 2$, while choosing the above T, we may choose maximal T with respect to its length. In case if we have many maximal short zero sequences, we choose one among them and fix as T. Now, the deleted sequence S^*T^{-1} has length $4n-4-(s+t) \geq 3n-3$. Since there is no subsequence $R = a^{n-1}$ of S^*T^{-1} for every $a \in \mathbf{Z}_n \oplus \mathbf{Z}_n$, by Conjecture 1, there exists a short zero subsequence D of S^*T^{-1} (in fact, if $|S^*T^{-1}| \geq 3n-2$, we can use Theorem 2.1.1). Because of maximality of $|T|$, we have

$$|D| \leq |T|. \tag{2}$$

Also, if $|T| + |D| \leq n$, then TD is a short zero subsequence of S^* with $|T| < |TD|$, contradicting to the choice of T. Thus

$$n + 1 \leq |T| + |D|. \tag{3}$$

Now, multiplying the equation (1) by 2, we get $2s \leq 2n - 2 - 2|T|$. If we add the equations (2) and (3), we get, $2|T| \geq n+1$. Combaining these two informations, we get $2s \leq 2n - 2 - 2|T| \leq n - 3$, which is a contradiction. Hence the theorem. □

Theorem 2.2.4 (Gao and Geroldniger, 1998, [14]) *Conjecture 4 implies Conjecture 1 for all primes.*

Corollary 2.2.5 *Assume Conjecture 4. Let $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 4p - 4$ such that S does not have a zero subsequence of length p. Also assume that S has a minimal zero subsequence of length $2p - 1$. Then S is of the form $a^{p-1}b^{p-1}c^{p-1}d^{p-1}$ for some $a, b, c, d \in \mathbf{Z}_p \oplus \mathbf{Z}_p$.*

Proof. Let $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 4p - 4$ such that S doesn't have a zero sequence of length p. Also we have by assumption S has a minimal zero subsequence of length $2p - 1$. By Conjecture 4, we have $S = a^{p-1}\prod_{i=1}^{3p-3} a_i \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$. Since by Theorem 2.2.4, Conjecture 1 is true and $v_a(S) = p-1$, by Theorem 2.2.3, we get the required structure of the sequence S. □

Theorem 2.2.6 *Assume Conjecture 2. Let $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 4p - 4$. Suppose S does not have a zero-sum of length p. Then S does have a zero-sum of length $p - 1$ and a zero-sum of length $3p - 3$.*

Proof. Let the sequences S_1 and S_2 be such that $S_1 := S(0,0)$ and $S_2 := Sx_{4p-3}$, where $x_{4p-3} = -\sum_{i=1}^{4p-4} x_i$. Since $|S_1| = |S_2| = 4p-3$, by the Conjecture 2, S_1, S_2 have zero subsequences, say T_1 and T_2 of length p, respectively. Clearly, by the assumption, neither T_1 nor T_2 can be subsequence of S. Therefore $(0,0)$ is in T_1 and x_{4p-3} is in T_2. Hence there exist a common subsequences I of T_1 and S and J of T_2 and S of length $p-1$ such that $\sum_I x = (0,0)$ and $\sum_J x = -x_{4p-3} = \sum_{i=1}^{4p-4} x_i$. Then taking J_0 after omitting J from $x_1, \cdots, x_{4p-4}$ will produce a zero sequence with $|J_0| = 3p-3$. □

Remark. The sequence $S = (1,0)^{p-1}(0,1)^{p-1}(1,1)^{p-1} \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ has no short zero subsequence in it. But S has minimal zero subsequence of length t for every t in the range $p+1 \leq t \leq 2p-1$. For, $T_i = (1,1)^i(0,1)^{p-i}(1,0)^{p-i}$ is a minimal zero subsequence of S with $|T_i| = 2p-i$ for all i in the range $1 \leq i \leq p-1$.

We shall prove the above remark in generality as follows.

Theorem 2.2.7 *Let $S = a^{p-1}b^{p-1}c^{p-1}$ be a sequence in $\mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 3p-3$. Assume that S does not have any short zero subsequences in it. Then, S has minimal zero subsequence T of length r for every $p+1 \leq r \leq 2p-1$.*

To prove the above theorem, we first prove a sequence of lemmas as follows.

Lemma 2.2.8 *Let $S = \prod_i x_i \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ be a sequence of length $3p-3$. Assume that S does not have any short zero subsequences. Then, S does not have any zero subsequence of length at least $2p$.*

Proof. First we shall prove that S does not have any zero subsequence of length at least $2p+1$. Suppose not. That is, there exists a zero subsequence $T = \prod_{i \in K} x_i \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ of S of length $\ell \geq 2p+1$ where K is a subset of $\{1, 2, \cdots, 3p-3\}$ and $|K| = \ell$. Consider the $3p$ elements y_i; $1 \leq i \leq 3p$ where

$$y_i = \begin{cases} x_i, & \text{if } i \in K \\ (0,0), & \text{otherwise} \end{cases}$$

It is clear that $\sum_{i=1}^{3p} y_i = \sum_{i \in K} x_i = (0,0)$. We invoke a theorem of Alon and Dubiner [1] which says that if a sequence $a_1, a_2, \cdots, a_{3p}$ where $a_i \in \mathbf{Z}_p \oplus \mathbf{Z}_p$ such that $\sum_{i=1}^{3p} a_i = (0,0)$, then there exists a zero subsequence of length p in the given sequence. Therefore, there is a zero subsequence T' with $|T'| = p$ and the index set I of T' is a subset of $\{1, 2, \cdots, 3p\}$. As $\ell \geq 2p+1$, we have $3p - \ell \leq p-1$. Then, $J = I \cap K$ has cardinality between 1 and p. Thus $\sum_{i \in J} y_i = \sum_{i \in J} x_i = (0,0)$ which contradicts the hypothesis. Hence there is no zero subsequence of length at least $2p+1$.

Now we assume that there is a zero subsequence T'' of S of length $2p$. Since the Davenport constant $D(\mathbf{Z}_p \oplus \mathbf{Z}_p) = 2p-1$, it is clear that T'' has a zero subsequence, say T'''. This means, the length of T''' or the length of the complement subsequence T''' of T'' is less than or equal to p which contradicts the hypothesis. Thus S does not have any zero subsequence of length at least $2p$. Hence the lemma. □

Lemma 2.2.9 *Let $S = (1,0)^{p-1}(0,1)^{p-1}(e,f)^{p-1}$ in $\mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ be a sequence of length $3p-3$. Assume that S does not have any short zero subsequences in it. Then, S has minimal zero subsequence T of length r for every r in the range $p+1 \leq r \leq 2p-1$.*

Proof. Given that $S = (1,0)^{p-1}(0,1)^{p-1}(e,f)^{p-1}$ in $\mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 3p-3$ such that S does not have any short zero subsequences in it. We shall produce minimal zero subsequence T of S of length r for every r in the range $p+1 \leq r \leq 2p-1$.

First note that any zero subsequence $T = (1,0)^k(0,1)^\ell(e,f)^m$ of S of length r will be $k(1,0)+\ell(0,1)+m(e,f) = (0,0)$ in $\mathbf{Z}_p \oplus \mathbf{Z}_p$ for some $k, \ell, m \in \mathbf{Z}_p$ and $k+\ell+m = r$. Thus, we get the following equations over $\mathbf{Z}_p$ as follows;

$$\begin{aligned} k + me &= 0 \\ \ell + mf &= 0 \\ k + \ell + m &= r \end{aligned} \tag{4}$$

Therefore if we treat k, ℓ, m are unknown variables, then to prove the theorem it is enough to prove that for every $p+1 \leq r \leq 2p-1$, there is a simultaneous solution for the system of equations (4) over $\mathbf{Z}_p$. This system of equations has solution over $\mathbf{Z}_p$ if and only if the determinant of the following matrix

$$\begin{pmatrix} 1 & 0 & e \\ 0 & 1 & f \\ 1 & 1 & 1 \end{pmatrix}$$

is non-zero over $\mathbf{Z}_p$. So, whenever the determinant of this matrix is non-zero, for any given r modulo p, there exists k, ℓ and m such that $k(1,0) + \ell(0,1) + m(e,f) = 0$ in $\mathbf{Z}_p \oplus \mathbf{Z}_p$ with $k + \ell + m = r$. Clearly, by the assumption that S does not have any short zero subsequence, r cannot be less than or equal to p. Therefore, r is either $p + r'$ or $2p + r'$ where $1 \leq r' \leq p-1$. Lemma 2.2.8 assures that $r \neq 2p + r'$. Therefore, $r = p + r'$ where $1 \leq r' \leq p-1$.

Now, to end the proof of the lemma, it is enough to check the case when the determinant of the matrix vanishes modulo p. The determinant of this matrix is zero if and only if $e + f \equiv 1 \pmod p$. But if we consider the sequence $S^* = (1,0)^{p-1}(0,1)^{p-1}(e,1-e)^{p-1}$ in $\mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$, then we see that the subsequence

$$T = (1,0)^{p-e}(0,1)^{e-1}(e,1-e)$$

of S^* is a zero subsequence of length p. Since, by assumption, S does not have short zero subsequence, this case never arises. □

Proof of Theorem 2.2.7 Given that $S = a^{p-1}b^{p-1}c^{p-1}$ is a sequence in $\mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 3p-3$ such that S doesn't have any short zero subsequences in it. It is clear that any two elements among $a, b, c \in \mathbf{Z}_p \oplus \mathbf{Z}_p$ is linearly independent over $\mathbf{Z}_p$. That is, there does not exist $\lambda, \mu, \gamma \in \mathbf{Z}_p$ such that either $a = \lambda b$ or $b = \mu c$ or $c = \gamma a$. If not, then we can produce a short zero subsequence in S which would contradict to the assumption. Without loss of generality, we can assume that a and b constiute a basis for $\mathbf{Z}_p \oplus \mathbf{Z}_p$ over $\mathbf{Z}_p$. Therefore $c = \lambda a + \mu b$ for some $\lambda, \mu \in \mathbf{Z}_p$.

To end the proof of Theorem 2.2.7, we shall prove that it is enough to assume $a = (1,0)$ and $b = (0,1)$. Then by Lemma 2.2.9, the proof of the theorem follows immediately.

Claim. If the sequence $S^* = (1,0)^{p-1}(0,1)^{p-1}(\lambda,\mu)^{p-1}$ has a zero subsequence of length r, then the sequence S also has a zero subsequence of length r.

For, if S^* has a zero subsequence of length r, then there exist integers $0 \le k, \ell, m \le p-1$ such that $k + \ell + m = r$ and $k(1,0) + \ell(0,1) + m(\lambda,\mu) = (0,0)$ in $\mathbf{Z}_p \oplus \mathbf{Z}_p$. That is,

$$k + m\lambda = 0 \text{ and } \ell + m\mu = 0 \tag{5}$$

in $\mathbf{Z}_p$. Consider the following subsequence T' of S where $T' = a^k b^\ell c^m$, where $a = (a_1, a_2), b = (b_1, b_2), c = (c_1, c_2) \in \mathbf{Z}_p \oplus \mathbf{Z}_p$. Since $c = \lambda a + \mu b = (\lambda a_1 + \mu b_1, \lambda a_2 + \mu b_2)$, we get $c_1 = \lambda a_1 + \mu b_1$ and $c_2 = \lambda a_2 + \mu b_2$. With these in hand, we see that

$$\begin{aligned} ka + mb + \ell c &= k(a_1, a_2) + m(b_1, b_2) + \ell(c_1, c_2) \\ &= (ka_1 + \ell b_1 + mc_1, ka_2 + \ell b_2 + mc_2) \\ &= ((k + m\lambda)a_1 + (\ell + m\mu)b_1, (k + m\lambda)a_2 + (\ell + m\mu)b_2) \\ &= (0,0) \end{aligned}$$

(using the equation (5)) in $\mathbf{Z}_p \oplus \mathbf{Z}_p$.

Now, it is clear from the above claim that S^* does not have any short zero subsequence in it. Therefore by Lemma 2.2.8, S^* contains a minimal zero subsequence T^* of length r for every $p+1 \le r \le 2p-1$. Once again appealing to the above observation, we conclude that S does have minimal zero subsequence of length r for every $p+1 \le r \le 2p-1$ (the minimality follows because S does not have any short zero subsequences). Hence the theroem. □

Corollary 2.2.10. *Assume Conjecture 1. Let $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ be a sequence of length $3p-3$. Also, assume that S does not have any short zero subsequences. Then S has minimal zero subsequence T of length r for every r in the range $p+1 \le r \le 2p-1$.*

Proof. Since, by assumption, Conjecture 1 is true, S is of the form as in Theorem 2.2.7. Hence the conclusion of Theorem 2.2.7 holds. □

Corollary 2.2.11. *Assume Conjecture 1. Let $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ be a sequence of length $3p-3$. Also, assume that S does not have any short zero subsequences. Then any minimal zero subsequence of S of length $2p-1$ has an element $a \in \mathbf{Z}_p \oplus \mathbf{Z}_p$ which is repeated at least $(2p-1)/3$ times.*

3. Analogous Problems in $\mathbf{Z}_n$

Since $D(\mathbf{Z}_n) = \eta(\mathbf{Z}_n) = n$, the analogue to Conjecture 1 will be: If $S \in \mathcal{F}(\mathbf{Z}_n)$ with $|S| = n-1$ and S is zero-free, then $S = a^{n-1}$ for some $a \in \mathbf{Z}_n$. Indeed, this is known in great generality as follows.

Theorem 3.1 (Bovey, Erdős and Niven, 1975, [4]) *Let $n, k \in \mathbf{N}$ with $n - 2k \geq 1$. Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n)$ be a zero-free sequence with $|S| = n-k$. Then there exists $a \in \mathbf{Z}_n$ such that $v_a(S) \geq n - 2k + 1$.*

Corollary 3.2 *Let k be an integer such that $1 \leq k < (n+2)/4$. Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n)$ with $|S| = n-k$ be a zero-free element. Then S is of the following form:*

$$S = a^{n-2k+1+\ell} \prod_{i=1}^{k-1-\ell} b_i \quad \text{where } b_i = e_i a, \ 0 \leq \ell \leq k-1,$$

and $2 \leq e_1 \leq e_2 \leq \cdots \leq e_{k-1-\ell}$ with $e_1 + e_2 + \cdots + e_{k-1-\ell} \leq 2k - 1 - \ell$.

Proof. By Theorem 3.1, there is an element $a \in \mathbf{Z}_n$ which is repeated in S at least $n-2k+1$ times. Since $1 \leq k < (n+2)/4$, it is clear that $v_a(S) \geq n/2+1$. Therefore, the order of a in $\mathbf{Z}_n$ is n. Then any element $b \in \mathbf{Z}_n$ is $b = ea$ with $1 \leq e \leq n-1$. If $v_a(S) = n - 2k + 1 + \ell < n - k$, then there exist $b_1, b_2, \cdots, b_{k-1-\ell}$ not necessarily distinct, but not equal to a in $\mathbf{Z}_n$ such that $v_{b_i}(S) > 0$. Clearly, since S is zero-free and $b_i = e_i a$, we have $e_1 + e_2 + \cdots + e_{k-1-\ell} < 2k - 1 - \ell$. □

Corollary 3.3 *Let $S \in \mathcal{F}(\mathbf{Z}_n)$ be a zero-free element of length $n-1$. Then there exists $a \in \mathbf{Z}_n$ such that $v_a(S) = n-1$.*

Proof. Put $k = 1$ in Theorem 3.1, to get the result. □

Corollary 3.4 *Let $S \in \mathcal{F}(\mathbf{Z}_n)$ be a zero-free element of length $n-2$. Then S consists of either only one element a such that $v_a(S) = n-2$ or two distinct elements a and b such that $v_a(S) = n-3$ and $b = 2a$ with $v_{2a}(S) = 1$.*

Proof. Put $k = 2$ in Theorem 3.1, we get S contains an element a which is repeated at least $n-3$ times. If $v_a(S) = n-2$, then there is nothing to prove. If not, then $v_a(S) = n-3$. Therefore the cyclic subgroup generated by a in $\mathbf{Z}_n$ is the whole group, since S is zero-free. In other words, the order of a is n. Since $|S| = n-2$, S has to have another element $b \in \mathbf{Z}_n$ such that $v_b(S) = 1$. Clearly $b = a\ell$ for some $2 \leq \ell \leq n-1$. As b is different from a, it is clear that $\ell \neq 1$. If $\ell > 2$, then we have a zero subsequence $b, \underbrace{a, a, \cdots, a}_{n-\ell \text{ times}}$ of S, which is impossible. Therefore $\ell = 2$. □

The following theorem is a generalisation of the analogue of Conjecture 4 in $\mathbf{Z}_n$.

Theorem 3.5 *Let $n, k \in \mathbf{N}$ with $n - 2k \geq 1$. Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n)$ be a minimal zero sequence with $|S| = n - k + 1$. Then*

(i) whenever $1 \leq k < (n+2)/3$, there exists $a \in \mathbf{Z}_n$ such that $v_a(S) \geq n - 2k + 2$.

(ii) whenever $(n+2)/3 \leq k \leq (n-1)/2$, there exists $a \in \mathbf{Z}_n$ such that $v_a(S) \geq n - 2k + 1$.

In particular, in both the cases, we have $v_a(S) \geq n - 2k + 1$.

Proof. Let S be a minimal zero sequence with $|S| = n - k + 1$. Let $a \in \mathbf{Z}_n$ be appearing in S a maximum number of times. Since S is a minimal zero sequence, the subsequence $R = Sa^{-1}$ is zero-free and $|R| = n - k$. Therefore by Theorem 3.1, there exists an element $b \in \mathbf{Z}_n$ such that $v_b(R) \geq n - 2k + 1$.

(i) Let $1 \leq k < (n+2)/3$. Suppose $b \neq a$. Since $v_a(S) \geq v_b(R) \geq n - 2k + 1$, $|S| \geq 2n - 4k + 2$. Since $|S| = n - k$, it is clear that $2n - 4k + 2 \leq n - k$, which implies $k \geq (n+2)/3$. But this not true. Therefore $a = b$ and hence $v_a(S) \geq n - 2k + 2$.

(ii) Let $(n+2)/3 \leq k \leq (n-1)/2$. In this case, b can be different from a and also, $v_a(S) \geq v_b(S) \geq n - 2k + 1$. Therefore, $v_a(S) \geq n - 2k + 1$. □

Corollary 3.6 *Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n)$ be a minimal zero sequence with $|S| = n$. Then $S = a^n$ for some $a \in \mathbf{Z}_n$ with order n.*

Proof. Put $k = 1$ in Theorem 3.5 to get $S = a^n$ for some $a \in \mathbf{Z}_n$. □

Corollary 3.7 *Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n)$ be a minimal zero sequence with $|S| = n - 1$. Then $S = a^{n-2}b$ for some $a \in \mathbf{Z}_n$ whose order is n, and $b = 2a$.*

Proof. Put $k = 2$ in Theorem 3.5. We get that there is an element $a \in \mathbf{Z}_n$ which is repeated at least $n - 2$ times. The sequence S cannot be of the form $S = a^{n-1}$, since it is not even a zero sequence. Therefore, $S = a^{n-2}b$ where $b \neq a \in \mathbf{Z}_n$. Since S is a zero sequence, it is clear that $b = 2a$. □

Corollary 3.8 *Let k be an integer such that $1 \leq k \leq (n+2)/4$. Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n)$ with $|S| = n - k + 1$ be a minimal zero sequence. Then S is of the following form:*

$$S = ca^{n-2k+1+\ell} \prod_{i=1}^{k-1-\ell} b_i \quad \text{where } b_i = e_i a, \ 0 \leq \ell \leq k - 1,$$

and $2 \leq e_1 \leq e_2 \leq \cdots \leq e_{k-1-\ell}$ with $e_1 + e_2 + \cdots + e_{k-1-\ell} \leq 2k - 1 - \ell$ and $c = -ha + \sum_{i=1}^{k-1-\ell} b_i$

Proof. Let S be a given minimal zero sequence with $|S| = n - k + 1$. Let $c \in \mathbf{Z}_n$ such that $v_c(S) > 0$. Let $R = c^{-1}S$ be a subsequence of length $n - k$. Since S is minimal zero sequence, R is a zero-free subsequence of length $n - k$. Therefore by Corollary 3.2, the result follows. □

We move on to a 40 year old classical theorem, known as the EGZ theorem, which is analogous to Conjecture 2 in $\mathbf{Z}_n$ and is stated as follows.

Theorem 3.9 (Erdős, Ginzburg and Ziv, 1961, [8]) *If $S \in \mathcal{F}(\mathbf{Z}_n)$ with $|S| = 2n-1$, then there exists a zero subsequence T of S with $|T| = n$.*

It is easy to see that if $S = 0^{n-1}1^{n-1} \in \mathcal{F}(\mathbf{Z}_n)$, then there doesn't exist a zero subsequence of length n in S.

Recently, the author [27] proved the following theorem, which is a generalization analogue of Conjecture 3 in $\mathbf{Z}_n$.

Theorem 3.10 *Let n, k be positive integers such that $n - 2k \geq 1$. Let $S \in \mathcal{F}(\mathbf{Z}_n)$ with $|S| = 2n - k - 1$. Suppose S does not have a zero subsequence of length n. Then there exist $a \neq b \in \mathbf{Z}_n$ such that $v_a(S) \geq v_b(S) \geq n - 2k + 1$.*

Corollary 3.11 *If $S \in \mathcal{F}(\mathbf{Z}_n)$ with $|S| = 2n - 2$ is such that S does not contain any zero subsequence of length n, then $S = a^{n-1}b^{n-1}$, where $a \neq b \in \mathbf{Z}_n$.*

Proof. Put $k = 1$ in Theorem 3.10 to get the result. □

Remark. The result in Corollary 3.11 is analogous to Conjecture 3. This was proved by Peterson and Yuster [23] and Bialostocki and Dierker [3].

It has been observed in [27] that Theorem 3.10 can be easily deduced from Theorem 3.1, and conversely, Theorem 3.1 also can be proved as a consequence of Theorem 3.10.

We shall give a different proof of Theorem 3.9, starting from Corollary 3.11 as follows.

Alternative proof of Theorem 3.9. Let $S \in \mathcal{F}(\mathbf{Z}_n)$ with $|S| = 2n - 1$. Suppose $T = a^{-1}S$ is a subsequence of S with $|T| = 2n - 2$ such that T does not have any zero subsequences of length n. By Corollary 3.11, we know, $T = x^{n-1}y^{n-1} \in \mathcal{F}(\mathbf{Z}_n)$. Now, consider $T_1 = x^{-1}S$. Clearly, $|T_1| = 2n - 2$. If T_1 has a zero subsequence of length n, then there is nothing to prove. If not, again by Corollary 3.11, we get $a = x$ or $a = y$. In any case, we have an element of $\mathbf{Z}_n$ which is repeated n times. Thus Theorem 3.9 is true. □

Theorem 3.12. *Let k be an integer such that $1 \leq k \leq n/4$. Then Theorem 3.1 implies and is implied by Theorem 3.5*

Proof. Theorem 3.1 $\Longrightarrow$ Theorem 3.5 is clear from the proof of Theorem 3.5. Now we shall prove the converse implication.

Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n)$ with $|S| = n - k$ and S be a zero-free element of $\mathcal{F}(\mathbf{Z}_n)$. Let $a = \sum_{i=1}^{n-k} a_i \neq 0$ in $\mathbf{Z}_n$, by assumption. Consider $S_1 = (-a)S \in \mathcal{F}(\mathbf{Z}_n)$. Clearly

$|S_1| = n - k + 1$ and S_1 is a minimal zero sequence, as S is zero-free. Therefore, there is an element $b \in \mathbf{Z}_n$ such that $v_b(S_1) \geq n - 2k + 1$. If $b \neq -a$, then we are done. Suppose $b = -a$ and $-a$ is repeated exactly $n - 2k$ times in S. Let us rename the indices of the elements a_i's and assume that $a_1, a_2, \cdots, a_k$ are different from b. Then none of the a_i is equal to any of the elements from the subset $A \subseteq \mathbf{Z}_n$ where $A := \{a, 2a, \cdots, (n-2k)a\}$. This is because if $a_i = \ell a$ for some $\ell \in A$, then $a_i + \underbrace{b + b + \cdots + b}_{\ell \text{ times}} = 0 \in \mathbf{Z}_n$ which is a contradiction. Also note that $2n - 4k \geq n$, we conclude that $a_i = b\ell_i$ for all $i = 1, 2, \cdots, k$ and since $a_i \neq a$, $\ell_i \geq 2$ for every i. Hence $\sum_{i=1}^{k} \ell_i \geq 2k$. Therefore, we can find (by renaming the indices) $\ell_1, \ell_2, \cdots, \ell_r$ where $1 \leq r \leq k$ such that $2k \leq \sum_{i=1}^{r} \ell_i \leq n$. Writting $\sum_{i=1}^{r} \ell_i = 2k + m$ with $0 \leq m \leq n - 2k$, then we have the following zero subsequence $T = b^m \prod_{i=1}^{r} a_i$ of S which is a contradiction. Therefore $v_b(S) \geq n - 2k + 1$. Thus Theorem 3.1 is true. □

Remark. (i) If $1 \leq k \leq n/4$, then we have the following implications:

$$\text{Theorem 3.5} \iff \text{Theorem 3.1} \iff \text{Theorem 3.10} \Longrightarrow \text{Theorem 3.9}.$$

(ii) In the range $1 \leq k \leq n/4$, the desired sequence has one element which is repeated at least $n/2$ times.

Acknowledgements. I am thankful to Professors R. Balasubramanian and B. Sury for carefully going through the manuscript and for their encouragements. Also, I am greatful to the referee for patiently correcting all the typographical errors. I take this oppurtunity to thank Harish-Chandra Research Insitute, Allahabad, where I was able to complete this work.

References

[1] N. Alon and M. Dubiner, Zero-sum sets of prescribed size, *Combinatorics: Paul Erdös is Eighty*,Colloq. Math. Soc. Jànos Bolyai,(1993), North-Holland Publishing Co., Amsterdam, 33-50.

[2] D. D. Anderson, *Factorization in integral domains*, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, **189**, 1997.

[3] A. Bialostocki and P. Dierker, On Erdős-Ginzburg-Ziv theorem and the Ramsey numbers for stars and matchings, *Discrete Mathematics*, **110** (1992), 1-8.

[4] J. D. Bovey, P. Erdős and I. Niven, Conditions for zero-sum modulo n, *Canad. Math. Bull.*, **18** (1975) 27-29.

[5] S. Chapman, On the Davenport's constant, the cross number and their application in factorization theory, in: *Zero-dimensional commutative rings*, Lecture Notes in Pure Appl. Math., Marcel Dekker, **171**, (1995) 167-190.

[6] S. Chapman and A. Geroldinger, Krull domains and moniods, their sets of lengths and associated combinatorial problems, in: *Factorization in integeral domains*, Lecture Notes in Pure Appl. Math., Marcel Dekker, **189**, (1997) 73-112.

[7] G. T. Diderrich and H. B. Mann, Combinatorial problems in finite abelian groups, in: *A survey of combinatorial theory*, edited by J. N. Srivastava, North-Holland, 1973.

[8] P. Erdös, A. Ginzburg and A. Ziv, Theorem in the additive number theory, *Bull. Res. Council Israel*, **10 F**(1961), 41-43.

[9] W. D. Gao, On zero-sum subsequences of restricted size, *J. Number Theory*, **61**(1996), 97-102.

[10] W. D. Gao, Addition Theorems and Group Rings, *J. Comb. Theory, Series A*, (1997), 98-109.

[11] W. D. Gao, Two zero-sum problems and multiple properties, *J. Number Theory*, **81**(2000), 254-265.

[12] W. D. Gao, A note on a zero-sum problem, *J. Combin. Theory Ser. A* **95** (2001), no. 2, 387–389.

[13] W. D. Gao and A. Geroldinger, On the structure of zero-free sequences, *Combinatorica*, **18** (1998), 519-527.

[14] W. D. Gao and A. Geroldinger, On long minimal zero sequences in finite abelian groups, *Periodica Mathematica Hungarica*, Vol. 38 (3)(1999), 179-211.

[15] H. Harborth, Ein Extremalproblem Für Gitterpunkte, *J. Reine Angew. Math.*, **262/263** (1973), 356-360.

[16] A. Kemnitz, On a lattice point problem, *Ars Combinatorica*, **16b**(1983), 151-160.

[17] H. B. Mann, *Addition theorems: the addition theorems of group theory and number theory*, Interscience Publishers, J. Wiley & Sons, 1965.

[18] H. B. Mann, Additive group theory- a progress report, *Bull. Amer. Math. Soc.*, **79** (1973), 1069-1075.

[19] M. B. Nathanson, *Additive Number Theory*, GTM **165**, Springer, 1996.

[20] L. Rónyai, On a conjecture of Kemnitz, *Combinatorica* 20 (2000), no. 4, 569-573.

[21] J. E. Olson, On a combinatorial problem of Erdös, Ginzburg and Ziv, *J. Number Theory*, **8**(1976), 52-57.

[22] J. E. Olson, On a combinatorial problem of finite Abelian groups I and II, *J. Number Theory*, **1**(1969), 8-10, 195-199.

[23] B. Peterson and T. Yuster, A generalization of an addition theorem for solvable groups, *Can. J. Math.*, vol XXXVI, No. 3 (1984) 529-536.

[24] B. Sury, The Chevalley-Warning theorem and a combinatorial question on finite groups, *Proc. Amer. Math. Soc.*, **127** (1999), 4, 951-953.

[25] B. Sury and R. Thangadurai, On zero-sums sequences in finite Abelian groups, *Preprint* (2001).

[26] R. Thangadurai, On a conjecture of Kemnitz, *C. R. Math. Rep. Acad. Sci. Canada*, Vol. **23** (2) (2001), 39-45.

[27] R. Thangadurai, Non-canonical extensions of Erdős-Ginzburg-Ziv theorem, *Preprint* (2001).

[28] P. van Emde Boas, A combinatorial problem on finite Abelian groups II, Z. W. (1969-007) Math. Centrum-Amsterdam.

[29] P. van Emde Boas and D. Kruyswijk, A combinatorial problem on finite Abelian groups III, Z. W. (1969-008) Math. Centrum-Amsterdam.

Received: 13.06.2001
Revised: 24.01.2002