Proc. Indian Acad. Sci. (Math. Sci.) Vol. 112, No. 3, August 2002, pp. 399–414.

Gao's conjecture on zero-sum sequences

B SURY and R THANGADURAI*

Indian Statistical Institute, 8th Mile Mysore Road, Bangalore 560 059, India
* Indian Statistical Institute, 203, B.T. Road, Kolkata 700 108, India
E-mail: sury@isibang.ac.in; thanga_v@isical.ac.in

MS received 28 January 2002; revised 9 May 2002

Abstract. In this paper, we shall address three closely-related conjectures due to van Emde Boas, W D Gao and Kemnitz on zero-sum problems on $\mathbf{Z}_p \oplus \mathbf{Z}_p$. We prove a number of results including a proof of the conjecture of Gao for the prime $p = 7$ (Theorem 3.1). The conjecture of Kemnitz is also proved (Propositions 4.6, 4.9, 4.10) for many classes of sequences.

Keywords. Zero-sum sequences; Chevally–Warning Theorm; Gao's conjecture.

1. Introduction and notations

Davenport [5] raised the following question for any finite Abelian group G. *What is the smallest constant $D(G)$ for which given an arbitrary sequence $a_1, a_2, \ldots, a_t$ in G with $t \geq D(G)$, there exists a subsequence whose sum is zero in G*? Evidently, we have $D(\mathbf{Z}_n) = n$. Davenport's constant is connected with algebraic number theory as follows. Let K be a number field (i.e., a finite extension of $\mathbf{Q}$) and $\mathcal{O}_K$ be its ring of integers. Let $\mathcal{C}(K)$ be its class group. Let $x \in \mathcal{O}_K$ be an irreducible element. As $\mathcal{O}_K$ is a Dedekind domain, the ideal

$$x\mathcal{O}_K = \prod_{i=1}^{r} \mathcal{P}_i$$

where $\mathcal{P}_i$ are prime ideals in $\mathcal{O}_K$ not necessarily distinct. $\mathcal{C}(K)$ is a finite Abelian group and if D is its Davenport constant, then in the prime ideal factorization of the integral ideal $x\mathcal{O}_K$ at most D prime ideals can occur. The precise value of $D(G)$ is known only in very special cases (see [10]).

To describe various conjectures and results pertaining to $D(G)$ and other problems, we need to recall the following precise definitions.

Let G be a finite Abelian group. Then $G = \mathbf{Z}_{n_1} \oplus \cdots \oplus \mathbf{Z}_{n_r}$ with $1 < n_1 | n_2 | \cdots | n_r$, where $n_r = \exp(G)$ is the exponent of G and r is the rank of G. Most of our discussion will be centered around the group $G = \mathbf{Z}_n \oplus \mathbf{Z}_n$.

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

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

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

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

where $\nu_g(S)$ is the number of times g appears in S and $|S| = \sum_{g \in G} v_g(S) = \ell \in N$ 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 $T|S$, the element $R = ST^{-1} \in \mathcal{F}(G)$ denotes 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 $1 \leq |S| \leq \exp(G)$.

The set of all zero sequences is a submonoid of $\mathcal{F}(G)$. Its irreducible elements are the minimal zero sequences (see [2–4]).

We study the following constants associated with a finite Abelian group G. Let $\eta(G)$ (respectively $f(G)$) denote the least positive integer r such that any sequence $S \in \mathcal{F}(G)$ with $|S| \geq r$ contains a nonempty zero subsequence T of S of length at most (respectively equal to) $\exp(G)$. Evidently, $\eta(G) \leq f(G)$. Typically, there are two types of conjectures in this subject – one predicts the value of $\eta(G)$ or $f(G)$ and, the other asserts that a sequence of length one less than the (predicted) value of $\eta(G)$ or $f(G)$ must have a certain very restricted form.

The main results of this paper are Theorem 3.1 which proves Gao's Conjecture on $\mathbf{Z}_p \oplus \mathbf{Z}_p$ *for* $p = 7$ *and Theorem 2.5 which addresses Emde Boas's Conjecture. Several partial results related to Kemnitz's Conjecture are obtained in* §4 *(Propositions 4.6, 4.9 and 4.10).*

2. Sequences of length at most $\eta(G)$

The results of this section will be used in the next one as well. In this section, we study sequences of length at most $\eta(G)$ for $G = \mathbf{Z}_n \oplus \mathbf{Z}_n$. We obtain results related to a conjecture of Emde Boas which addresses the structure of sequences of length $\eta(G) - 1$. These methods also yield new proofs of certain results of Davenport, Olson, Alon and Dubiner. Our proofs are based on the well-known:

Chevalley–Warning Theorem. *Let* $f_1, f_2 \ldots, f_r$ *be homogeneous polynomials in* n *variables over* $\mathbf{Z}_p$ *such that sum of their degrees is strictly less than the number* n *of variables. Then, all the* f_i *have a nonzero simultaneous solution over* $\mathbf{Z}_p$.

We start with the following general result.

Theorem 2.1.

(a) *If* $G \cong \mathbf{Z}_p^d$, *then* $D(G) = d(p-1) + 1$.

(b) *Let* $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_p^d)$ *with* $|S| = (d+1)(p-1)+1$. *Then, there exists a zero subsequence* T *of* S *such that* $|T| \equiv 0 \pmod{p}$.

(c) *Let* $2 \le d < p$. *Let* $S \in \mathcal{F}(\mathbf{Z}_p^d)$ *with* $S = (d+1)(p-1)+1$. *Then there exists a zero subsequence* T *of* S *such that* $1 \le |T| \le (d-1)p$.

A result stronger than (a) was proved already in 1969 by Olson [15] but this version is sufficient for our purpose.

Proof of (a). For $i \le d$, the set of elements

$$e_i = (\underbrace{0, 0, \dots, 0}_{i-1 \text{ times}}, 1, \underbrace{0, \dots, 0}_{d-i+1 \text{ times}})$$

of G, each repeated $p-1$ times, shows that $D(G) > d(p-1)$.

Let $a_i = (a_{i1}, a_{i2}, \dots, a_{id})$; $1 \le i \le d(p-1)+1$ be elements of G. Consider the polynomials

$$f_j(X_1, \dots, X_{d(p-1)+1}) = \sum_{i=1}^{d(p-1)+1} a_{ij} X_i^{p-1} \quad \text{for } j \le d.$$

The Chevalley–Warning Theorem ensures that there is a nontrivial common solution $x_1, x_2, \dots, x_{d(p-1)+1} \bmod p$. Evidently, one has therefore $\sum_{i \in I} a_i = 0$ where $I = \{i : x_i \neq 0\}$. Thus, $D(G) = d(p-1)+1$.

Proof of (b). Write $a_i = (a_{i1}, a_{i2}, \dots, a_{id})$ and put $r = (d+1)(p-1)$. Let a be a quadratic nonresidue modulo p. For $1 \le j < d$, consider the polynomials

$$f_j(X) = \sum_{i=1}^{r+1} a_{ij} X_i^{p-1} - \sum_{i=1}^{r+1} X_i^{p-1}$$

in $r+1$ variables $X = (X_1, X_2 \dots, X_{r+1})$ and

$$f_d(X) = \left(\sum_{i=1}^{r+1} a_{id} X_i^{p-1}\right)^2 - a\left(\sum_{i=1}^{r+1} X_i^{p-1}\right)^2.$$

These d homogeneous polynomials are considered over $\mathbf{Z}_p$. As the sum of their degrees is $(d+1)(p-1) = r$ which is less than the number of variables, the Chevalley–Warning Theorem implies that they have a common nontrivial zero over $\mathbf{Z}_p$. Let us fix such a solution $y_1, y_2, \dots, y_{r+1}$. If $I = \{i : 0 \neq y_i \in \mathbf{Z}_p\}$, then I is nonempty and the last equality $f_d(y_i) = 0$ gives $|I| \equiv 0 \pmod{p}$ as well as $\sum_{i \in I} a_{id} = 0$ in $\mathbf{Z}_p$. Therefore, we get $\sum_{i \in I} a_{ij} = 0$ in $\mathbf{Z}_p$ for each $j \le d$. This just means that $\sum_{i \in I} a_i = (\underbrace{0, 0, \dots, 0}_{d \text{ times}})$.

This completes this proof.

Proof of (c). Let $a_i = (a_{i1}, \dots, a_{id})$, $1 \le i \le (d+1)(p-1)+1$ be a sequence in $\mathbf{Z}_p^d$. Let us write $\ell = (d+1)(p-1)+1$ for simplicity of notation. Consider the $d+1$ homogeneous polynomials

$$f_j(X) = \sum_{i=1}^{\ell} a_{ij} X_i^{p-1}, \quad 1 \le j \le d$$

and

$$f_0(X) = \sum_{i=1}^{\ell} X_i^{p-1}, \quad 1 \leq j \leq d$$

in $X = (X_1, X_2, \ldots, X_\ell)$ ℓ variables.

By the Chevalley–Warning Theorem, there exists a zero subsequence of length rp for some $1 \leq r \leq d$. If the length is $\leq (d-1)p$, we are done. So, let us assume that $I \subset \{1, 2, \ldots, \ell\}$ such that $|I| = dp$ and $\sum_{i \in I} a_i = (\underbrace{0, 0, \ldots, 0}_{d \text{ times}})$ in $\mathbf{Z}_p^d$. By renaming, we may take $I = \{1, 2, \ldots, dp\}$. Let us now look at the $d+1$ polynomials

$$g_j(X) = \sum_{i=1}^{dp-1} a_{ij} X_i^{p-1}, \quad 1 \leq j \leq d$$

and

$$g_0(X) = \sum_{i=dp}^{\ell} X_i^{p-1}.$$

Again, by the Chevalley–Warning Theorem, there is a nontrivial solution x_i satisfied by all the g_j, $j \geq 0$. Writing $J = \{i : x_i \neq 0\}$, J is a nonempty subset of $\{1, 2, \ldots, \ell\}$. Since g_0 is a sum of less than p terms, $J \cap \{dp, dp+1, \ldots, \ell\}$ is empty. Thus, $J \subseteq \{1, 2, \ldots, dp-1\}$ and $\sum_{i \in J} a_i = 0$. If $|J| \leq (d-1)p$, we are done. If $|J| > (d-1)p$, then, clearly, $J_0 = I \setminus J$ has cardinality between 1 and $p-1$ and $\sum_{i \in J_0} a_i = (\underbrace{0, 0, \ldots, 0}_{d \text{ times}})$ in $\mathbf{Z}_p^d$. Thus, the theorem is proved.

COROLLARY 2.2

(a) (Erdős–Ginzburg–Ziv Theorem). *Let $S \in \mathcal{F}(\mathbf{Z}_n)$ with $|S| = 2n-1$. Then there exists a zero subsequence T of S of length n.*

(b) $\eta(\mathbf{Z}_n \oplus \mathbf{Z}_n) = 3n - 2$.

Proof. For (a), take $d = 1$ in Theorem 2.1(b) to obtain it for primes and then a trivial induction completes the proof.

Taking $d = 2$ in the above theorem gives $\eta(\mathbf{Z}_p \oplus \mathbf{Z}_p) \leq 3p - 2$ for a prime p. It is trivial to see that the upper bound for primes implies the upper bound for general n. If we consider $S = (0,1)^{n-1}(1,0)^{n-1}(1,1)^{n-1} \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$, then clearly S does not have any short zero subsequences. Therefore, $\eta(\mathbf{Z}_n \oplus \mathbf{Z}_n) \geq 3n - 2$.

Part (b) was first proved by Olson, [15] and Emde Boas [18]). A more general application analogous to the E–G–Z theorem for a finite group had been conjectured by Olson [15] and was obtained in [16].

Corollary 2.2(b) is actually equivalent to the, *a priori*, stronger:

PROPOSITION 2.3

Let k be a positive integer satisfying $0 \leq k \leq \lfloor n/2 \rfloor$. Let $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 3n - 2 + k$. Then there exists a short zero subsequence T of S such that $k + 1 \leq |T| \leq n$.

Proof. Let $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 3n - 2 + k$. By Corollary 2.2(b), there exists a short zero subsequence T such that $1 \leq |T| \leq n$. Choose T such that T has maximal length less than or equal to n. If $|T| \leq k$, consider the deleted sequence ST^{-1}. Then $|ST^{-1}| \geq 3n - 2 + k - |T| \geq 3n - 2$. Therefore, by Corollary 2.2(b), there exists a short zero subsequence T_1 of ST^{-1}. Note that, by maximality of $|T|$, we have $|T_1| \leq |T| \leq k \leq \lfloor n/2 \rfloor$. Note that $|T_1| + |T| \leq n$. This contradicts the maximality of $|T|$, since we would have chosen $T_1 \cup T$ as our T in the first step itself. Therefore $|T| \geq k + 1$.

The following proposition was suggested by the anonymous referee. It is proved completely similarly and will be used in the proof of Lemma 3.2.

PROPOSITION 2.3′

Let k be an integer satisfying $0 \leq k \leq [n/2]$. Let $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 3n - 3 + k$. Then, either there exists a short zero subsequence T of S with $k + 1 \leq |T| \leq n$, or there is a subsequence W of S of length $3n - 3$ which does not contain any short zero-sum subsequence.

Using the above methods, we have a new and short proof of the following result due to Alon and Dubiner [1]:

PROPOSITION 2.4

If $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ is a zero sequence with $|S| = 3p$, then S contains a zero subsequence T with $|T| = p$.

Proof. If $S = \{s_i = (a_i, b_i) : 1 \leq i \leq 3p\}$ with $\sum_{i=1}^{3p} s_i = (0, 0)$, then the Chevalley–Warning Theorem ensures the existence of a nontrivial common zero for $\sum_{i=1}^{3p-2} a_i X_i^{p-1}$, $\sum_{i=1}^{3p-2} b_i X_i^{p-1}$, and $\sum_{i=1}^{3p-2} X_i^{p-1}$. This gives $I \subset \{1, 2, \ldots, 3p\}$ with $|I| = p$ or $|I| = 2p$ such that $\sum_I s_i = (0, 0)$. In the latter case, the complement $J = \{1, 2, \ldots, 3p\} \setminus I$ has cardinality p and gives again a zero subsequence of S.

As we noticed earlier, $S = (0, 1)^{n-1}\,(1, 0)^{n-1}\,(1, 1)^{n-1} \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ does not have any short zero subsequences. One may wonder if the same kind of structure must prevail for any sequence of length $3n - 3$ which does not have short zero subsequences. This has been conjectured to be so by van Emde Boas.

Conjecture 1 [18]. 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 himself [18] verified the conjecture for the primes 2, 3, 5 and 7 using a computer. Later, Gao [9] proved that the conjecture is 'multiplicative', i.e., if it is true for $n = k$ and $n = m$, then it is true for $n = km$. Thus, it suffices to prove this conjecture for all primes. The following theorem proves some properties that a sequence $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 3p - 3$ must possess if it does not contain any short zero subsequence.

Theorem 2.5. *Let $S = \prod_i x_i \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 3p - 3$ and suppose S does not contain any short zero subsequence. Then*
(a) *there exists a minimal zero subsequence T_1 of S with $|T_1| = 2p - 2$,*
(b) *there exists a minimal zero subsequence T_2 of S with $|T_2| = 2p - 1$,*
(c) *there is no zero subsequence of cardinality at least $2p$.*

Proof. Write $x_i = (a_i, b_i) \in \mathbf{Z}_p \oplus \mathbf{Z}_p$. We shall start by proving (c). We divide into two parts – first, we prove the nonexistence of zero subsequences of any length $\geq 2p+1$ and then do the $2p$ case.

Suppose K is a subset of $\{1, 2, \ldots, 3p-3\}$ such that $\sum_{i\in K} x_i = (0,0)$ and $|K| \geq 2p+1$. Consider the $3p$ elements y_i; $1 \leq i \leq 3p$ where

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

As $\sum_{i=1}^{3p} y_i = (0,0)$, by Proposition 2.4, there is a zero subsequence T with $|T| = p$ and the index set I of T is a subset of $\{1, 2, \ldots, 3p\}$. As $|K| \geq 2p+1$, we have $3p - |K| \leq p-1$. 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 $2p+1$.

Suppose now that there is a zero subsequence of length $2p$. Rename and assume that $\sum_{i=1}^{2p} x_i = (0,0)$. Consider the three polynomials in $3p-2$ variables $X := (X_1, X_2, \ldots, X_{3p-2})$ defined by

$$f(X) = \sum_{i=1}^{3p-3} a_i X_i^{p-1}, \quad g(X) = \sum_{i=1}^{3p-3} b_i X_i^{p-1}, \quad h(X) = \sum_{i=2p}^{3p-2} X_i^{p-1}.$$

Note that h involves only X_{2p} onwards. By the Chevalley–Warning Theorem, there is a common nontrivial zero, say $t_1, t_2, \ldots, t_{3p-2}$. The last polynomial shows that $t_i = 0$ for $i \geq 2p$. In other words, there is a nonempty subset I_1 of $\{1, 2, \ldots, 2p-1\}$ with $\sum_{i\in I_1} a_i = 0 = \sum_{i\in I_1} b_i$, i.e., $\sum_{i\in I_1} x_i = (0,0)$. Note that $J = \{1, 2, \ldots, 2p\} \setminus I_1$ is nonempty (as $2p \notin I_1$) and $\sum_J x_i = (0,0)$. By hypothesis, both I_1 and J must have cardinality more than p, which is an impossibility. Hence (c) is proved for $2p$ also.

We shall prove (b) now. Put $x_0 = (0,0)$ and applying Proposition 2.4 to the $3p-2$ elements x_i; $0 \leq i \leq 3p-3$, one has a zero subsequence T_0 of length p or $2p$. Let the index set of T_0 be I_0. Take $I = I_0 \setminus \{0\}$; then $|I| = p$ or $p-1$ or $2p$ or $2p-1$. The first two have been ruled out by hypothesis and the third one has been ruled out by part (*c*). Therefore $|I| = 2p-1$. This proves (b).

Let us prove (a) now. Take $x_{3p-2} = -\sum_{i=1}^{3p-3} x_i$. We know already that $x_{3p-2} \neq (0,0)$ from (c); here a separate argument needs to be given for $p = 3$, since (c) does not apply here as $3p-3 < 2p+1$.

Let $p \geq 5$ be any odd prime and we can take $x_{3p-2} = -\sum_{i=1}^{3p-3} x_i \neq (0,0)$. Write $x_i = (a_i, b_i)$ for $1 \leq i \leq 3p-2$. Consider the three polynomials in $3p-2$ variables $X := (X_1, X_2, \ldots, X_{3p-2})$ defined by

$$F(X) = \sum_{i=1}^{3p-2} a_i X_i^{p-1}, \quad G(X) = \sum_{i=1}^{3p-2} b_i X_i^{p-1}, \quad H(X) = \sum_{i=1}^{3p-2} X_i^{p-1}.$$

By Proposition 2.4, there is a subset $I_1 \subset \{1, 2, \ldots, 3p-2\}$ such that $|I_1| = p$ or $2p$ and $\sum_{i\in I_1} x_i = (0,0)$.

Case 1. (When $|I_1| = 2p$)

If $3p-2 \in I_1$, look at $I = I_1 \setminus \{3p-2\}$. Then, $I \subset \{1, 2, \ldots, 3p-3\}$, $|I| = 2p-1$ and $\sum_{i\in I} x_i = -x_{3p-2} = \sum_{i=1}^{3p-3} x_i$. Then, $J = \{1, 2, \ldots, 3p-3\} \setminus I$ has cardinality

$p-2$ and satisfies $\sum_{i\in J} x_i = (0,0)$. This contradicts the hypothesis. Thus, $3p-2 \notin I_1$. But, then $x_i; i \in I_1$ is a zero subsequence of $x_i; i \le 3p-3$ of length $2p$. We have ruled it out already by part (c). Thus, Case 1 cannot occur.

Case 2. (When $|I_1| = p$)

Then $3p-2$ must belong to I_1 by hypothesis. Consider $I = I_1 \setminus \{3p-2\}$. Then, $I \subset \{1, 2, \ldots, 3p-3\}$, $|I| = p-1$ and $\sum_{i\in I} x_i = -x_{3p-2} = \sum_{i=1}^{3p-3} x_i$. Then, $J = \{1, 2, \ldots, 3p-3\} \setminus I$ has cardinality $2p-2$ and satisfies $\sum_{i\in J} x_i = (0,0)$.

For $p = 3$, do separately as follows. We have $x_1, x_2, \ldots, x_6$. If they sum to $(0, 0)$, take $y_6 = y_7 = (0,0)$ and look at the elements $x_1, \ldots, x_5, y_6, y_7$. Since they are $3p-2 = 7$ elements, by Proposition 2.4, there is a zero subsequence which has length either 3 or 6. So, there is a zero subsequence of $x_1, \ldots, x_5$ of length either 1 or 2 or 3 or 4 or 5. The first three are ruled out by hypothesis. In the last two cases, look at their complements in $\{x_1, \ldots, x_6\}$. These are zero subsequences of length either 1 or 2 which once again contradicts the hypothesis. If $\sum_{i=1}^{6} x_i \neq (0,0)$, then proceed as in the general case.

3. Gao's conjecture

Consider the least number $f(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ such that any $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = f(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ has a zero subsequence T whose $|T| = p$. Its value is predicted by the following conjecture first made by Kemnitz [13] and suggested, independently, by N. Zimmerman and Y. Peres:

Conjecture 2. $f(\mathbf{Z}_p \oplus \mathbf{Z}_p) = 4p-3$.

One can easily see that $f(\mathbf{Z}_p \oplus \mathbf{Z}_p) \ge 4p-3$. For, consider

$$S = (0,0)^{p-1}(0,1)^{p-1}(1,0)^{p-1}(1,1)^{p-1} \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p).$$

Clearly, S does not contain a zero subsequence of length p. The results known about Conjecture 2 and our results on it will be discussed in the next section.

This section deals with the following conjecture due to Gao [9] which predicts that a sequence of length $4p-4$ which does not contain a zero sequence of length p in $\mathbf{Z}_p \oplus \mathbf{Z}_p$ must look like the above example.

Conjecture 3. If $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ with $|S| = 4p-4$ 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.

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. We shall prove this conjecture for the prime $p = 7$ now.

Theorem 3.1. *Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_7 \oplus \mathbf{Z}_7)$ with $|S| = 24$. Suppose S does not contain a zero subsequence of length 7. Then $S = a^6b^6c^6d^6$ where $a, b, c, d \in \mathbf{Z}_7 \oplus \mathbf{Z}_7$ are distinct elements. In other words, Conjecture 3 is true when $p = 7$.*

For the proof of Theorem 3.1, we need the following lemma.

Lemma 3.2. *Let $S \in \mathcal{F}(\mathbf{Z}_7 \oplus \mathbf{Z}_7)$ with $|S| = 24$ such that S does not contain any zero subsequence of length 7. Suppose $a \in \mathbf{Z}_7 \oplus \mathbf{Z}_7$ with $v_a(S) \ge 3$. Then S satisfies Conjecture 3.*

Proof. Suppose $a \in Z_7 \oplus Z_7$ with $v_a(S) = s$. We may assume that s is the maximum number of times that some element occurs. Without loss of generality, we may also assume that $a = (0,0)$ (otherwise we consider $S - a$ instead of S). Set $R = S((0,0)^{-s})$. Then, $|R| = 24 - s$. It follows from Proposition 2.3′ that either R contains a short zero-sum subsequence T of length $7 - s \leq |T| \leq 7$, or R contains a subsequence W of length 18 which does not contain any short zero-sum subsequence. If the first option holds, then S contains a zero-sum subsequence of length 7 of the form $T(0,0)^*$, a contradiction. Thus, the second option holds and, applying (for W) the fact that Conjecture 1 is true for $p = 7$, we get that W contains three distinct elements each appearing six times. This forces (by maximality of s) that $s = 6$ and the proof is complete.

Proof of Theorem 3.1. If some element of S is repeated at least $(7-1)/2 = 3$ times, then the result holds by Lemma 3.2.

If the sequence $S \in \mathcal{F}(\mathbf{Z}_7 \oplus \mathbf{Z}_7)$ has at least 13 distinct elements modulo 7, then, by Kemnitz [13], it follows that S contains a zero subsequence of length 7 which leads to a contradiction of our assumption. Therefore at most 12 distinct elements of $\mathbf{Z}_7 \oplus \mathbf{Z}_7$ can appear in S.

Assume that at least one of the elements of S is repeated exactly twice (we have covered all the other cases already). Once again by the same result of Kemnitz, it will imply that S contains 12 distinct elements of $\mathbf{Z}_7 \oplus \mathbf{Z}_7$ each of them repeated exactly twice. Hence we can assume that $S = (0,0)^2 \prod_{i=1}^{11} a_i^2 \in \mathcal{F}(\mathbf{Z}_7 \oplus \mathbf{Z}_7)$.

Set $S^* = \prod_{i=1}^{11} a_i^2$. By Corollary 2.2(b), there exists a short zero-sum subsequence T_1 of S^*. We assert that we must have

$$|T_1| = 4. \tag{1}$$

Since $S = S^*(0,0)^2$, and S contains no zero-sum subsequence of length 7, $|T_1| \leq 4$. But S^* does not contain $(0,0)$. Therefore, $2 \leq |T_1| \leq 4$. If $|T_1| = 2$ or 3, then $|S^* T_1^{-1}| = 20$ or 19. Since Conjecture 1 is true for $p = 7$, Proposition 2.3′ implies that $S^* T_1^{-1}$ contains a short zero-sum subsequence T_2 with $3 \leq |T_2| \leq 7$. Once again, (since $(0,0)^2$ occurs in S), we get $3 \leq |T_2| \leq 4$. Therefore, $T = T_1 T_2$ is a zero-sum subsequence of S^* with $5 \leq |T| \leq 7$, and similarly above one can derive a contradiction. Therefore, $|T_1| = 4$. This proves the assertion.

Claim. If a appears in S^* then $-a, a/2, -a/2, 2a, -2a$ cannot appear in S^*. It follows assertion (1) that $-a$ cannot appear in S^*. If $a/2$ appears in S^*, then $S - a/2 = ((0,0), (0,0), a/2, a/2, -a/2, -a/2)S_1$ for some S_1. The proof of assertion (1) shows also that $(S - a/2)((0,0)^{-2})$ contains no zero-sum subsequence of length 2 or 3. But $(S - a/2)((0,0)^2)^{-1}$ contains the subsequence $(a/2, -a/2)$, a contradiction. If $-a/2$ appears in S^*, then S^* contains subsequence $(a, -a/2, -a/2)$, a contradiction of assertion (1) again. If $2a$ appears in S^*, then $S - a = ((0,0), (0,0), a, a, -a, -a)S_1$. Exactly, as in the case of $a/2$ one can derive a contradiction. If $-2a$ appears in S^*, then S^* contains the subsequence $(a, a, -2a)$, a contradiction of assertion (1). This proves the claim. As $a, -a, a/2, -a/2, 2a, -2a$ are the nonzero multiples of an element a in $\mathcal{F}(\mathbf{Z}_7 \oplus \mathbf{Z}_7)$, a simple counting gives us $|S^*| \leq 2 \times (7^2 - 1)/(7-1) = 16$, a contradiction. This completes the proof of the theorem.

Since Conjecture 3 is ‘multiplicative’ [9], it follows immediately that:

COROLLARY 3.3

Conjecture 3 is true for all positive integer n of the form $n = 2^a 3^b 5^c 7^d$ *for all* $(a, b, c, d) \in \mathbf{N}^4 \backslash \{(0, 0, 0, 0)\}$.

Remark 3.4. It must be noted that there are sequences of length $4n - 4$ in $\mathbf{Z}_n \oplus \mathbf{Z}_n$ which are made up of four distinct elements repeated $n - 1$ times each which may contain a zero-sum subsequence of length n. In other words, the candidates appearing in the conclusion of Conjecture 3 are somewhat restricted. For example, if $(0, 0)$, (a, b), $(-a, -b)$ are three of the four elements, there is always a zero-sum sequence of length n. Similarly, if $n = 5$, the elements $(0, 2)$, $(2, 0)$, $(1, 1)$ occurring four times each gives a zero-sum subsequence of length 5.

4. Zero subsequences of length n in $\mathbf{Z}_n \oplus \mathbf{Z}_n$

In this section, we shall prove results about sequences in $\mathbf{Z}_n \oplus \mathbf{Z}_n$ which must contain a zero subsequence of length n. In particular, we obtain some results pertaining to Conjecture 2 of Kemnitz for the group $\mathbf{Z}_p \oplus \mathbf{Z}_p$.

It is trivial to see that if the conjecture holds good for two integers m and n, it is also true for mn. So, if one proves it for all primes, then it holds good for all natural numbers. For our convenience, instead of writing $f(\mathbf{Z}_p \oplus \mathbf{Z}_p)$, we write simply $f(p)$.

Harborth [12] considered a function $g(n)$ which is related to $f(n)$. To define $g(n)$, let us define an element $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ to be square-free, if a_i's are pairwise distinct in $\mathbf{Z}_n \oplus \mathbf{Z}_n$. Then $g(n)$ is defined to be the least positive integer such that given any square-free $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ contains a zero subsequence of length n. Harborth proved that $g(3) = 5$ and used this to prove $f(3) = 9$. Then Kemnitz [13] utilized the special values of $g(p) = 2p - 1$ for $p = 5, 7$ to prove $f(p) = 4p - 3$ for $p = 5, 7$. A bound known for all primes p is, due to Kemnitz [13]:

$$2p - 1 \leq g(p) \leq 4p - 3.$$

We shall prove on the one hand that the lower bound $2p - 1$ is tight for many classes of sequences and, on the other hand, we improve the upper bound for many classes of sequences. In 1996, Gao [7] 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 second author of this paper in [17] 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 $s \geq \lfloor n/2 \rfloor$, 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 1995, Alon and Dubiner [1] gave the upper bound $f(n) \leq 6n - 5$ for all $n \in \mathbf{N}$. Later this was improved upon for all primes to $f(p) \leq 5p - 1$ by Gao [8]. In 2000, Rónyai [14] proved that $f(p) \leq 4p - 2$ for all primes p. From this bound, he concluded that $f(n) \leq (41/10)n$. Recently, Gao [11] has proved that $f(p^k) \leq 4p^k - 2$ for all primes p and $k \geq 1$. Many of these proofs use graph theory and are quite different from our methods.

We start with the observation:

Lemma 4.1. *If* $S \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ *with* $|S| = 4p - 3$ *such that there is no zero subsequence* T *of* S *with* $|T| = 2p$, *then S must contain a zero subsequence of length p, i.e., S satisfies Conjecture 2.*

Proof. The proof follows by putting $d = 2$ in Theorem 2.1(b) and applying Proposition 2.4.

PROPOSITION 4.2

(a) *Let k be an integer such that* $0 \leq k \leq \lfloor n/2 \rfloor$. *Let* $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ *with* $|S| = 4n - 3$. *Suppose* $T = a^{n-1-k}$ *is a subsequence of S for some* $a \in \mathbf{Z}_n \oplus \mathbf{Z}_n$. *Then there exists a zero subsequence R of S with* $|R| = n$.

(b) *Let* ℓ *and k be two integers such that* $0 \leq \ell < k \leq \lfloor n/2 \rfloor$. *Let* $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ *with* $|S| = 4n - 3 - \ell$. *Suppose* $T = (0, 0)^{n-k}$ *is a subsequence of S. Then S contains a zero subsequence R with* $n - \ell \leq |R| \leq n$.

Proof of (a). Without loss of generality we can assume that $T = (0, 0)^{n-1-k}$. Let $S^* = ST^{-1}$ be the subsequence of S. Clearly $|S^*| = 4n - 3 - n + 1 + k = 3n - 2 + k$. By Proposition 2.3, there exists a zero subsequence U of S^* with $k + 1 \leq |U| \leq n$. Thus there exists a zero subsequence R of TU with $|R| = n$.

Proof of (b). Let $S^* = ST^{-1}$ be the subsequence of S with $|S^*| = 4n - 3 - \ell - n + k = 3n - 2 + (k - \ell - 1)$. Therefore by Proposition 2.3, there exists a zero subsequence T_1 of S^* with $k - \ell \leq |T_1| \leq n$. Therefore there exists a zero subsequence R of TT_1 with $n - \ell \leq |R| \leq n$.

Remark 4.3. One can prove that if $f(n) = 4n - 3$ and $n \geq (3m^3 - m^2 + 6)/8m$ for some positive integer m, then $f(nm) = 4nm - 3$. The proof of this is quite similar to the corresponding result proved in [17], except that one uses $f(n) \leq (41/10)n$ instead of $f(n) \leq 5n - 4$.

Here is a result about the group $\mathbf{Z}_m \oplus \mathbf{Z}_n$.

PROPOSITION 4.4

Let $S \in \mathcal{F}(\mathbf{Z}_m \oplus \mathbf{Z}_n)$ *with* $|S| = 2n + (21/10)m$ *where* $m|n$. *Then S contains a zero subsequence of length n.*

Proof. Since $2n + (21/10)m = (2n/m - 2)m + (41/10)m$ and we know $f(m) \leq (41/10)m$, we can extract $2n/m - 1$ disjoint subsequences $S_1, S_2, \ldots, S_{2n/m-1}$ of S with length m whose sum is zero in $\mathbf{Z}_m \oplus \mathbf{Z}_m$. Since we have the following exact sequence

$$0 \longrightarrow \mathbf{Z}_{n/m} \longrightarrow \mathbf{Z}_m \oplus \mathbf{Z}_n \longrightarrow \mathbf{Z}_m \oplus \mathbf{Z}_m \longrightarrow 0$$

and by the E–G–Z theorem (Corollary 2.2(a) here), we know there is a subsequence of the sequence $\{s_i\}_{i=1}^{2n/m-1}$ of length n/m where $s_i \in \mathbf{Z}_{n/m}$ such that $s_i := 1/m \sum_{j=1, a_{ij} \in S_i}^{m} a_{ij}$ under the exact sequence. Let $s_1, s_2, \ldots, s_{n/m}$ be the zero subsequence of $\{s_i\}_{i=1}^{2n/m-1}$ of length n/m. This means

$$\sum_{i=1}^{n} s_i = \sum_{i=1}^{n} \sum_{j=1}^{m} a_{ij} = 0$$

in $\mathbf{Z}_m \oplus \mathbf{Z}_n$ where $a_{ij} \in S_i$ for $j = 1, 2, \ldots, m$ and for $i = 1, 2, \ldots, n/m$.

Remark 4.5. If $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ is square free with $|S| = 2n - 1$, then all the first (or second) co-ordinates of the a_j's cannot be distinct in $\mathbf{Z}_n$. Also, none of the first (second) co-ordinates can be repeated more than n times, since the corresponding second (first) co-ordinates run through 0 to $n - 1$. If n is odd and, one of the first (second) co-ordinate repeats exactly n times, then the corresponding second (first) co-ordinate runs through 0 to $n-1$ and we pick up those a_j in S to produce a zero subsequence of length n. Hence we can always assume that if n is odd, then, in any such sequence, a single residue class modulo n is repeated at most $n - 1$ times among the first (second) co-ordinates.

Now, we can prove two qualitative results both of which exemplify the tightness of the lower bound $g(p) \geq 2p - 1$.

PROPOSITION 4.6

(a) *Let n be a prime and let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ be a square-free element with $|S| = 2n - 1$. Suppose the first co-ordinates of the a_j's run through all the different n residue classes modulo n such that $n - 1$ different residue classes modulo n are repeated exactly twice. Then there exists a zero subsequence T of S with $|T| = n$.*

(b) *Let n be a prime and let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ be a square-free element with $|S| = 2n - 1$. Suppose the first co-ordinates of the a_j run through three distinct residue classes modulo n such that two of the residue classes repeat $n - 1$ times. Then there exists a zero subsequence T of S with $|T| = n$.*

The following lemma will be used in the proof of (a) as well as later in the proof of Proposition 4.9.

Lemma 4.7. *Let n be a prime and let $S = \prod_i a_j \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ be a square-free element with $|S| = 2n - 1$. Let $a_i = (x_i, y_i)$ and $a_{i+n-1} = (x_i, z_i)$ for $i = 1, 2, \ldots n - 1$ where $y_i \not\equiv z_i \pmod{n}$ for all i and $a_{2n-1} = (b, c)$. If $x_1 + x_2 + \cdots + x_{n-1} + b \equiv 0 \pmod{n}$, then, there exists a zero subsequence T of S with $|T| = n$.*

Proof. Let $K \equiv y_1 + y_2 + \cdots + y_{n-1} + c \pmod{n}$ and $e_\ell = z_\ell - y_\ell \pmod{n}$ for all $\ell = 1, 2, \ldots, n - 1$. Clearly, $e_\ell \not\equiv 0 \pmod{n}$ because $y_i \not\equiv z_i \pmod{n}$ for all i. If we form all the partial sums of e_ℓ's we get all the distinct residue classes modulo n (This can be done by simple induction, see for instance [6]). Therefore, there exists a positive integer m such that $K + e_{i_1} + e_{i_2} + \cdots + e_{i_m} \equiv 0 \pmod{n}$ which implies

$$\begin{aligned} &y_1 + \cdots + y_{i_1-1} + z_{i_1} + y_{i_1+1} + \cdots + y_{i_m-1} + z_{i_m} \\ &\quad + y_{i_m+1} + \cdots + y_{n-1} + c \equiv 0 \pmod{n}. \end{aligned}$$

Then, the following subsequence of S

$$(x_1, y_1), \ldots, (x_{i_1-1}, y_{i_1-1}), (x_{i_1}, z_{i_1}), (x_{i_1+1}, y_{i_1+1}), \ldots, (x_{n-1}, y_{n-1}), (b, c)$$

produces the required zero subsequence of length n

Proof of Proposition 4.6(a). Let $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ be the given square-free element satisfying the hypothesis. Let us list the elements of S as follows:

$$a_i = (x_i, y_i) \quad \text{for all } i = 1, 2, \ldots, n - 1$$

and

$$a_{i+n-1} = (x_i, z_i) \quad \text{for all } i = 1, 2, \ldots, n-1$$

where $z_i \not\equiv y_i \pmod{n}$ for all $i = 1, 2, \ldots, n-1$ and $x_i \not\equiv x_j \pmod{n}$ for every $i \neq j$. Also, let $a_{2n-1} = (b, c)$ such that $b \not\equiv x_i \pmod{n}$ for every $i = 1, 2, \ldots, n-1$. Clearly, we have a zero-sum of length n as follows:

$$x_1 + x_2 + \cdots + x_{n-1} + b \equiv 0 \pmod{n}.$$

Now, the result follows from lemma 4.7.

Proof of (b). Let $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ be a square-free element with $|S| = 2n-1$ satisfying the hypothesis. We shall list the elements of S in the following manner. Let

$$a_i = (x, y_i) \quad \text{for } i = 1, 2, \ldots, n-1 \quad \text{where } y_i \not\equiv y_j \pmod{n}$$

and

$$a_{i+n-1} = (y, z_i) \quad \text{for } i = 1, 2, \cdots, n-1 \quad \text{where } z_i \not\equiv z_j \pmod{n}$$

and $x \not\equiv y \pmod{n}$. Also, we let $a_{2n-1} = (b, c)$ where $b \not\equiv x \pmod{n}$ and $b \not\equiv y \pmod{n}$. Consider $R = x^{n-1}y^{n-1}b \in \mathcal{F}(\mathbf{Z}_n)$ with $|R| = 2n-1$. Therefore, by the Erdős–Ginzburg–Ziv theorem, there exists a zero subsequence T_1 of R with $|T_1| = n$. Clearly, b appears in T_1. Thus, we have, $T_1 = x^m y^\ell b \in \mathcal{F}(\mathbf{Z}_n)$ such that $\ell + m + 1 = n$ where $\ell, m \geq 1$.

Suppose $\{y_i\}_{i=1}^{n-1}$ and $\{z_i\}_{i=1}^{n-1}$ miss r and s residue classes modulo n respectively. If $r \equiv s \equiv c \pmod{n}$, then we can choose, by relabeling indices, $y_1, y_2, \ldots, y_\ell, z_1, z_2, \ldots, z_m$ such that $y_i \not\equiv z_j \pmod{n}$ for all $i = 1, 2, \ldots, \ell$ and $j = 1, 2, \ldots, m$. We are in the following situation:

$$(x, y_1), \ldots, (x, y_\ell), (y, z_1), \ldots, (y, z_m), (b, c)$$

such that its sum is zero modulo n, since $y_1, \ldots, y_\ell, z_1, \ldots z_m, c$ runs through all distinct residue modulo n.

If $r \not\equiv s \pmod{n}$, then we can choose $y_1, \ldots, y_\ell, z_1, \ldots z_m, c$ runs through all distinct residue modulo n. Therefore again we can produce a zero-sum subsequence of S of length n.

If $r \equiv s \not\equiv c \pmod{n}$, then we do the following. Let $r \equiv s \equiv a \pmod{n}$. Let us take

$$\mathbf{Z}_n = \{0, 1, 2, \ldots, a-1, a, a+1, \ldots, \ell, \ell+1, \ldots, c-1, c, \ldots, n-1\}.$$

Then we choose the sequences

$$\{y_i\}_{i=1}^{\ell} : 0, 2, 3, \ldots, a-1, a+1, a+2, \ldots, \ell+1$$

and

$$\{z_j\}_{j=1}^{m} : a+1, \ell+2, \ell+3, \ldots, c-1, c+1, \ldots, n-2, n-1.$$

Then we see that

$$y_1 + y_2 + \cdots + y_\ell + z_1 + z_2 + \cdots + z_m + c \equiv 0 \pmod{n}.$$

Thus, we have the following zero subsequence T of S of length n

$$(x, y_1), (x, y_2), \dots, (x, y_\ell), (y, z_1), \dots, (y, z_m), (b, c)$$

in $\mathbf{Z}_n \oplus \mathbf{Z}_n$.

Our last two results go to indicate that the upper bound $g(p) \le 4p - 3$ can be strengthened in some cases. In the proof, we shall need to use the so-called:

Cauchy–Davenport Inequality. Let A and B be two nonempty subsets of $\mathbf{Z}_p$. If we denote the cardinality of A by $|A|$ and of B by $|B|$, then

$$|A + B| \ge \min\{p, |A| + |B| - 1\},$$

where $A + B$ stands for the sum-set of these two subsets.

An induction argument easily gives: *If $A_1, A_2, \dots, A_h$ are nonempty subsets of $\mathbf{Z}_p$, then*

$$|A_1 + A_2 + \cdots + A_h| \ge \min(p, \sum_{i=1}^{h} |A_i| - h + 1).$$

Remark 4.8. Let $S \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ be a square-free element with $|S| > 3n - 3$. We know that if n is odd and S does not contain a zero subsequence of length n, then no single residue class can occur as the first co-ordinate more than $n - 1$ times. Therefore, the first co-ordinates of the elements of S run through at least four distinct residue classes modulo n in such a case.

PROPOSITION 4.9

Let s be an integer such that $4 \le s \le p$. Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ be a square-free element with $|S| = 4p - 2 - s$. Assume that the first co-ordinates of the a_j's run through exactly s different residue classes modulo p and that each different residue class modulo p repeats an odd number of times. Then there is a zero subsequence T of S with $|T| = p$.

Proof. Let $S = \prod_j a_j \in \mathcal{F}(\mathbf{Z}_p \oplus \mathbf{Z}_p)$ be the given element satisfying the hypothesis. By hypothesis, the first co-ordinates of the elements a_j run through s different residue classes modulo p and each of these residue classes repeats an odd number of times. Some of the residues may appear only once. The number of such residues is at most s. Now, let us list the elements of S as follows if necessary by relabeling the indices

$$a_i = (b_i, c_i) \quad \text{for } i = 1, 2, \dots, s$$

where $b_i \not\equiv b_j \pmod p$ for $i \ne j$. Also among the b_i's we put those residues which appear only once in S. Therefore the remaining residues will be appearing as pairs. So, let

$$a_{i+s} = (x_i, y_i) \quad \text{for } i = 1, 2, \dots, 2p - 1 - s$$

and

$$a_{i+2p-1} = (x_i, z_i) \quad \text{for } i = 1, 2, \dots, 2p - 1 - s$$

where $y_i \not\equiv z_i \pmod p$ for all $i = 1, 2, \dots, 2p - 1 - s$. This kind of listing is possible because of the assumption on the first co-ordinates of the elements $a_i \in \mathbf{Z}_p \oplus \mathbf{Z}_p$.

Now we partition the x_i; $i = 1, 2, \ldots, 2p - 1 - s$ into nonempty classes $A_1, A_2, \ldots, A_{p-1}$ such that each A_i consists of different residues modulo p. This is possible because no single residue class can be repeated more than $p - 1$ times. Set

$$A_p = \{b_1, b_2, \ldots, b_s\}.$$

Clearly $A_i \subset \mathbf{Z}_p$ for $i = 1, 2, \ldots, p$. Consider the sum $A_1 + A_2 + \cdots + A_p$. Cauchy–Davenport inequality implies now that

$$|A_1 + \cdots + A_p| \geq \min\left(p, \sum_{i=1}^{p} |A_i| - p + 1\right) = \min(p, (2p - 1 - s + s - p + 1)) = p.$$

This means, $0 \in \mathbf{Z}_p$ can be written as sum of p elements, i.e., $x_1 + x_2 + \cdots + x_{p-1} + b_r = 0$ where $x_i \in A_i$ for $i = 1, 2, \ldots, p - 1$ and $b_r \in A_p$ (Here we have relabeled the indices of x_i.)

Now we have the following situation.

$$(x_1, y_1), (x_2, y_2), \ldots, (x_{p-1}, y_{p-1}), (b_r, c_r)$$

and

$$(x_1, z_1), (x_2, z_2), \ldots, (x_{p-1}, z_{p-1})$$

where $x_1 + x_2 + \cdots + x_{p-1} + b_r \equiv 0 \pmod{p}$ and $y_i \not\equiv z_i$ for all $i = 1, 2, \ldots, p - 1$. An application of Lemma 4.7 now yields the result.

For general n, with an additional assumption on the first co-ordinates, we prove:

PROPOSITION 4.10

Let $0 \leq s \leq [(n-1)/2]$ be an integer. Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ with $|S| = 3n - 2 + s$ be a square-free element. Assume that the first co-ordinates of the a_j's run through $n - s$ different residue classes modulo n and each residue class occurs an odd number of times with at least $s + 1$ different residue classes modulo n which are repeated at least three times. Then there exists a zero subsequence T of S with $|T| = n$.

Proof. Let $S = \prod_j a_j \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ be the given square-free element satisfying the hypothesis. By our assumption, all the first co-ordinates of the a_j's appear an odd number of times as different residues modulo n. It is clear that the number of residues which appear exactly once cannot exceed n-s-3, since any residue modulo n can be repeated at most $n - 1$ times. Therefore other than these residues, every other residue is repeated at least three times.

Now, let us list the elements of the given sequence S as follows, if necessary by relabeling the indices

$$a_i = (x_i, y_i) \quad \text{for } i = 1, 2, \ldots, n - 1 + s$$

and

$$a_{i+n-s} = (x_i, z_i) \quad \text{for } i = 1, 2, \ldots, n - 1 + s$$

where $y_i \not\equiv z_i \pmod{n}$ for all $i = 1, 2, \ldots, n - 1 + s$. Also,

$$a_{i+2(n-1+s)} = (b_i, c_i) \quad \text{for } i = 1, 2, \ldots, n - s$$

where $b_i \not\equiv b_j \pmod{n}$ for $i \neq j$. Any residue that is repeated only once has been put in the class of the b_i's. This kind of listing is possible because of the assumption over the first co-ordinates of the elements $a_i \in \mathbf{Z}_n \oplus \mathbf{Z}_n$.

Since $s+1$ distinct residue classes modulo n repeat at least three times, we can take them to be $x_{n-1}, x_n, \ldots, x_{n-1+s}$. Other than these x_i's for $i = 1, 2, \ldots, n-1+s$, we have b_i's which run through $n-s$ different residue classes modulo n.

Let $\sum_{i=1}^{n-2} x_i + x_j = d_j$ for $j = n-1, n, \ldots, n-1+s$. Since the sequence $\{-d_j\}$ of length $s+1$ is such that $d_j \not\equiv d_k \pmod{n}$ for $j \neq k$, there exists one b_r among the b_i's such that $-d_j = b_r$ for some j, since the sequence $\{b_j\}$ cannot miss $s+1$ different residue class modulo n. Hence we have

$$x_1 + x_2 + \cdots + x_{n-2} + x_j + b_r \equiv 0 \pmod{n}.$$

Suppose, by relabeling, we let $x_j = x_{n-1}$ for our convenience. Now we have the following situation:

$$(x_1, y_1), (x_2, y_2), \ldots, (x_{n-1}, y_{n-1}), (b_r, c_r)$$

and

$$(x_1, z_1), (x_2, z_2), \ldots, (x_{n-1}, z_{n-1})$$

where $x_1 + x_2 + \cdots + x_{n-1} + b_r \equiv 0 \pmod{n}$ and $y_i \not\equiv z_i \pmod{n}$ for all $i = 1, 2, \ldots, n-1$. Once again, an application of Lemma 4.7 proves the result.

COROLLARY 4.11

Let r be an integer such that $0 \leq r \leq 3$. Let $S = \prod_i a_i \in \mathcal{F}(\mathbf{Z}_n \oplus \mathbf{Z}_n)$ be a square-free element with $|S| = 3n - 2 + r$. Suppose the first co-ordinates of a_j's run through $n - r$ different residue classes modulo n such that each residue class is repeated an odd number of times. Then there exists a zero subsequence T of S with $|T| = n$.

Proof. It is enough to prove that there exist $r+1$ different residue classes modulo n which are repeated at least three times. Then, the corollary follows from the theorem. Since we have totally $n-r$ different residue classes modulo n, at least four different residue classes modulo n have to repeat a minimum of three times. Hence the corollary is proved.

Acknowledgements

It is a pleasure to thank Professor R. Balasubramanian for some fruitful discussions. It is a delight to note the insightful and detailed comments of the anonymous referee which simplified the proof of the main result. In particular, the statement of Proposition 2.3′ has been suggested by him. We thank the referee heartily.

References

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

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

[3] Chapman S, 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) (1995) vol. 171, pp. 167–190

[4] Chapman S and Geroldinger A, 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) (1997) vol. 189, pp. 73–112

[5] Davenport H, On the addition of residue classes, *J. London Math. Soc.* **22** (1947) 100–101

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

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

[8] Gao W D, Addition theorems and group rings, *J. Comb. Theory Ser. A* (1997) 98–109

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

[10] Gao W D, On Davenport's constant of finite abelian groups with rank three, *Discrete Math.* **222** (2000) 111–124

[11] Gao W D, A note on a zero-sum problem, *J. Comb. Theory Ser. A*, **95** (2001) 387–389

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

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

[14] Rónyai L, On a conjecture of Kemnitz, *Combinatorica* **20(4)** (2000) 569–573

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

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

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

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