Some Zero Sum Problems in Combinatorial Number Theory

By

Bhavin K. Moriya

Harish-Chandra Research Institute, Allahabad

A Thesis submitted to the

Board of Studies in Mathematical Sciences

In partial fulfillment of the requirements

For the degree of

Doctor of Philosophy

of

Homi Bhabha National Institute, Mumbai

Certificate

This is to certify that the Ph.D. thesis titled "**Some Zero Sum Problems in Combinatorial Number Theory**" by **Bhavin K. Moriya** is a record of bona fide research work done under my supervision. It is further certified that the thesis represents independent work by the candidate and collaboration was necessitated by the nature and scope of the problems dealt with.

Thesis Supervisor: S. D. Adhikari

Place:_____

Date: _____

Declaration

The author hereby declares that the work in the thesis titled "**Some Zero Sum Problems in Combinatorial Number Theory**", submitted for Ph.D. degree to the **Homi Bhabha National Institute** has been carried out under the supervision of Professor S. D. Adhikari. Whenever contributions of others are involved, every effort is made to indicate that clearly, with due reference to the literature. The author attests that the work is original and has not been submitted in part or full by the author for any degree or diploma to any other institute or university.

Thesis Author: _____
Bhavin K. Moriya

Place:_____

Date: _____

"We may paint many pictures but there is nothing but paint.... The wise man should know what is at the root of everything."

Shri Sadguru Siddharameshwar Maharaj

Acknowledgements

First of all I would like to express my sincere thanks and gratitude to my supervisor, Prof. S. D. Adhikari, for his continual support and constant encouragement throughout my stay at Harish-Chandra Research Institute (HRI). Without his everlasting encouragement and affection, this thesis would not have possibly taken shape the way it has. I would also like to thank all my coauthors Prof. S. D. Adhikari, Dr. R. Thangadurai, Prof. W. D. Gao, M. N. Chintamani, Dr. P. Paul for some wonderful collaborations. I am very very grateful to Prof. Weidong Gao for suggesting the problem considered in chapter 3 of this thesis. I express my gratitude to the National Board of Higher Mathematics for funding in first three years and HRI for the same in subsequent years.

I am very grateful to all members of HRI for making my stay at HRI unforgettable. It has been a great pleasure discussing with Dr. R. Thangadurai. He was so very friendly everytime that I never felt hesitant in asking anything. I express my sincere thanks and gratitude to him. I would also like to thank Prof. S. D. Tripathi, Dr. Punita Batra, Dr. Manoj Yadav, Dr. D. S. Ramana, Dr. Kalyan Chakraborty, Prof. B. Ramakrishnan, Dr. P. K. Ratnakumar, Prof. R. S. Kulkarni for the courses they have given. Words are just not enough to thank my parents and brothers and a sister for their patience and belief in me.

The time I have had with scholars and post docs was splendid. I express my thanks to my friends Mahender, Kalpataru, Brundaban, Sanjoy, Jaban, Karam, Archana, Vikas, Pradeep, Pradip, Navin, Rangoli, Eshita, Sneh, Jay, Kashi et. al. With a less serious note, I enjoyed learning gym in the evening hours from Prof. S. D. Adhikari and Dr. Kalyan Chakraborty; this

too helped me with my study by improving my power of concentration.

Bhavin K. Moriya

HRI.

Abstract

This thesis comprises of three results each of which dealt in separate chapters. First chapter is of introductory nature, as the title suggest. And the other three chapters are devoted to three different problems. Following is a brief introduction to our results.

1. Let G be any finite abelian group of rank r with invariants $n_1, n_2, \cdots, n_r$. In other words, $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ where n_i's are integers satisfying $1 < n_1 | n_2 | \cdots | n_r$. The *Davenport constant* of a group G is defined as the smallest positive integer t such that every sequence of length t of elements of G has a non-empty zero-sum subsequence. It has been conjectured by Śliwa that, $D(G) \leq \sum_{i=1}^{r} n_i$. Thinking in the direction of this conjecture we have obtained the following upper bound on Davenport constant $D(G)$, of G,

   $$D(G) \leq n_r + n_{r-1} + (c(3)-1)n_{r-2} + (c(4)-1)n_{r-3} + \cdots + (c(r)-1)n_1 + 1,$$

   where $c(i)$'s are Alon-Dubiner constants [10] for respective i's. Also we shall give an application of Davenport's constant to Quadratic sieve.

2. Let G be a finite abelian group with $\exp(G) = e$. Let $s(G)$ (respectively, $\eta(G)$) be the minimal positive integer t with the property that any sequence S of length t of elements of G contains an e-term subsequence (respectively, a non-empty subsequence of length at most e) of S with sum zero. For the group of rank at most two this constant has been determined completely (see [45]). Looking at the problem for groups of rank greater that 2 gave rise to this result. Our problem is to determine value of $s(C_{nm}^r)$ under some constraints on $n, m,$ and r.

   Let n, m and r be positive integers and $m \geq 3$. Furthermore, $\eta(C_m^r) = a_r(m-1)+1$, for some constant a_r depending on r and n is a fixed

integer greater than or equal to,

$$\frac{m^r(c(r)m - a_r(m-r) + m - 3)(m-1) - (m+1) + (m+1)(a_r+1)}{m(m+1)(a_r+1)}$$

and $s(C_n^r) = (a_r+1)(n-1)+1$. In the above lower bound on $n, c(r)$ is the Alon-Dubiner constant. Then $s(C_{nm}^r) = (a_r+1)(nm-1)+1$.

3. Given an abelian group G of order n, and a finite non-empty subset A of integers, the *Davenport constant of G with weight A*, denoted by $D_A(G)$, is defined to be the least positive integer t such that every sequence $(x_1, \cdots, x_t)$ with $x_i \in G$ has a non-empty subsequence $(x_{j_1}, \cdots, x_{j_l})$ and $a_i \in A$ such that $\sum_{i=1}^{l} a_i x_{j_i} = 0$. Similarly, $E_A(G)$ is defined to be the least positive integer t such that every sequence $(x_1, \cdots, x_t)$ of length t of elements of G has a subsequence $(x_{j_1}, \cdots, x_{j_n})$ such that $\sum_{i=1}^{n} a_i x_{j_i} = 0$, for some $a_i \in A$. When G is of order n, one considers A to be a non-empty subset of $\{1, \cdots, n-1\}$. If G is the cyclic group $\mathbb{Z}/n\mathbb{Z}$ we denote $E_A(G)$ and $D_A(G)$ by $E_A(n)$ and $D_A(n)$ respectively.

   Here we extend some results in an article of Adhikari et al. [5] and determine bounds for $D_{R_n}(n)$ and $E_{R_n}(n)$, where $R_n = \{x^2 : x \in (\mathbb{Z}/n\mathbb{Z})^*\}$ and $(\mathbb{Z}/n\mathbb{Z})^*$ is a group of units modulo n. We follow some line of arguments in [5] and use a recent result of Yuan and Zeng [79], a theorem due to I. Chowla [24] and Kneser's theorem [52].

Synopsis

Thesis Title	**:**	Some Zero Sum Problems in Combinatorial Number Theory
Name	**:**	Bhavin K. Moriya
Supervisor	**:**	Prof. S. D. Adhikari
Affiliation	**:**	Harish-Chandra Research Institute, Allahabad

This thesis contains some of my work in zero-sum problems during my stay at Harish-Chandra Research Institute.

Let G be a finite abelian group, written additively. The *Davenport constant* of the finite abelian group G, denoted by $D(G)$, is defined to be the least positive integer t such that any sequence of t elements of G contains a subsequence whose sum is zero (the identity element of G). Such a subsequence is called a *zero-sum subsequence.* By the structure theorem, we know $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ where n_i's are integers satisfying $1 < n_1|n_2|\cdots|n_r$; n_r is the *exponent* (denoted by $\exp(G)$) of G and r is the *rank* of G. Also, $n_1, n_2, \cdots, n_r$ are called *invariants* of G. Let

$$M(G) = 1 + \sum_{i=1}^{r}(n_i - 1).$$

It is trivial to see that $M(G) \leq D(G) \leq |G|$. The equality holds if and only if $G = \mathbb{Z}_n$, the cyclic group of order n (See [6]). Olson (See [64] and [65], for instance) proved that $D(G) = M(G)$, for all finite abelian groups of rank 2 and for all finite abelian p-groups. It is also known that $D(G) > M(G)$, for infinitely many groups (See for instance, [46]). The best known upper bound is due to Emde Boas and Kruyswijk [78], Meshulam [59] and Alford, Granville and Pomerance [8], (see also, [13]):

$$D(G) \leq \exp(G)\left(1 + \log \frac{|G|}{\exp(G)}\right). \tag{1}$$

Some refinement of this bound was recently achieved by Rath, Srilakshmi and Thangadurai in [70]. Obtaining a good upper bound for the Davenport constant constitutes a very important question about which the current state of knowledge is rather limited. However, we do have the following conjectures.

Conjecture 1.

(i) $D(G) = M(G)$ *for all finite abelian groups* G *with rank* $r = 3$ *or* $G = \mathbb{Z}_n^r$ *(See [36], [37], for instance);*

(ii) For any finite abelian group G, $D(G) \leq \sum_{i=1}^{r} n_i$ *(See [61], for instance), where* n_i*'s are the invariants of* G.

Recently, G. Bhowmik and J-C. Schlage-Puchta [15], proved that 1*(i)* above is true whenever

$$G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{3a} \oplus \mathbb{Z}_{3ab}.$$

Let G be an abelian group of order n, written additively. The *Davenport constant* $D(G)$ has already been defined. Another combinatorial invariant $E(G)$ (known as *the EGZ constant*) is the smallest natural number t such that any sequence of length t of elements of G has a subsequence of length $|G|$ whose sum is zero. A classical theorem of Erdős, Ginzburg and Ziv [32] says that $E(\mathbb{Z}/n\mathbb{Z}) = 2n - 1$. These two constants are related by a theorem of Gao [35], which states that $E(G) = D(G) + n - 1$.

Definition. *The constant* $s(G)$ *is defined to be the least positive integer* t *such that any sequence of length* t *of elements of* G *has a zero-sum subsequence of length precisely the exponent of* G. *Another constant* $\rho(G)$ *is defined to be the least positive integer* t *such that any sequence of length*

t of elements of G has a zero-sum subsequence of length less than or equal to $\exp(G)$. *Sometimes the notation $\eta(G)$ is also used instead of $\rho(G)$ in the literature.*

When $G = \mathbb{Z}_n^r$, by the work of Alon and Dubiner [10], it is known that $s(G)$ is bounded above by a linear function in n and they showed that

$$s(\mathbb{Z}_n^r) \leq c(r)n, \tag{2}$$

where $c(r)$ is a constant which depends on r. It is known that $c(1)$ can be taken as 2 (due to Erdős, Ginzburg and Ziv [32]) and $c(2)$ can be taken as 4 (due to C. Reiher [71]). In general, in our current state of knowledge, $c(r)$ can be taken satisfying

$$c(r) \leq 256(r \log_2 r + 5)c(r-1) + (r+1) \tag{3}$$

for all $r \geq 3$.

One of our main result, is the following :

Theorem 1. *Let G be any finite abelian group of rank r with invariants $n_1, n_2, \cdots, n_r$. Then*

$$D(G) \leq n_r + n_{r-1} + (c(3)-1)n_{r-2} + (c(4)-1)n_{r-3} + \cdots + (c(r)-1)n_1 + 1.$$

where the constants $c(r)$ satisfy (2). Theorem 1 is an extension of the results proved by Dimitrov in [28] and Balasubramanian and Bhowmik in [14].

Definition. *A non-empty finite set of positive integers consisting of distinct primes $p_1, p_2, \cdots, p_d$ is called a factor base. An integer $n > 1$ is said to be smooth with respect to factor base $F = \{p_1, p_2, \cdots, p_d\}$ if all prime factors of n are in F.*

In quadratic sieve (see [69]), to factor a given integer N with a factor base F, one needs to know how many smooth integers that are required

to produce two distinct squares such that $x^2 \equiv y^2 \pmod{N}$. It is well-known that if we can find $|F| + 1 = d + 1$ number of smooth integers with respect to factor base F, then we can find two squares which are equivalent modulo N. Instead of squares, if we want to produce two cubes which are equivalent modulo N, then how many smooth numbers we need to produce? More generally, for any given integer $k \geq 2$, if we want to produce two kth powers which are equivalent modulo N, how many smooth integers we need to have?

Definition. *By $c(k, d)$, we denote the least positive integer t such that for any multiset U of smooth integers, with respect to F, of cardinality at least t, there is a non-empty multisubset T with the following property:*

$$\prod_{a \in T} a = b^k$$

for some integer b.

It is clear that often a good bound for $c(k, d)$ will supply us two distinct squares such that $x^2 \equiv y^2 \pmod{N}$.

Theorem 2. *For all positive integers n and d, we have $c(n, d) = D(\mathbb{Z}_n^d)$.*

Following are the few more results that we have obtained,

Theorem 3. *Let n be any integer and $\omega(n)$ denote the number of distinct prime factors of n. Then*

$$D(\mathbb{Z}_n^r) \leq r^{\omega(n)}(n-1) + 1.$$

Theorem 4. *Let $n = 3^\alpha p^\ell$ be any integer, where $p \geq 3$ be any prime number. Then*

$$3n - 2 \leq D(\mathbb{Z}_n^3) \leq 3n + 3^{\alpha+1} - 7.$$

In particular, when $\alpha = 1$, we get,

$$3n - 2 \leq D(\mathbb{Z}_n^3) \leq 3n + 2.$$

Theorem 5. *Let G be a finite abelian group of rank r with invariants $n_1, n_2, \cdots, n_r$. Then*

$$s(G) \leq c(1)n_r + c(2)n_{r-1} + \cdots + c(r)n_1.$$

Theorem 6. *Let G be a finite abelian group of rank r with invariants $n_1, n_2, \cdots, n_r$. Then*

$$\rho(G) \leq (c(1) - 1)n_r + (c(2) - 1)n_{r-1} + \cdots + (c(r) - 1)n_1 + 1.$$

Additive number theory, factorization theory and graph theory provide a good source for combinatorial problems in finite abelian groups (for instance, see [56, 57, 62, 27, 12]). Among them, zero-sum problems have been of growing interest. The corner-stone of almost all recent combinatorial research on zero-sum problems is the Erdős-Ginzburg-Ziv Theorem [32]. Then there is the important question of determining $D(G)$ for all finite abelian groups.

Let G be a finite abelian group. The investigation of invariants $s(G)$ and $\eta(G)$ has a long tradition, and in recent years the investigation of these invariants and of the related inverse problems, i.e., the investigation of the structure of extremal sequences with, and without, the respective properties, received a good deal of attention. Among others, this is due to applications in the theory of non-unique factorizations. We refer to the monograph of A. Geroldinger and F. Halter-Koch [45], in particular to Chapter 5, for a detailed account of results on these invariants and their applications in the theory of non-unique factorizations, and to the recent survey article of Gao and Geroldinger [39] for an exposition of the state of the knowledge and numerous references.

Still, many questions are wide open. The precise value of $s(G)$ for cyclic groups is known by the classical Erdős-Ginzburg-Ziv Theorem [32], but

$s(G)$ for groups of rank 2 has only recently been determined (see [71, 45]) and the precise value of $s(G)$ is unknown for most groups of rank greater than 2, as is the value of $\eta(G)$. One can see lower bounds on $s(G)$ and $\eta(G)$ in [49, 30, 31]. We will describe bounds and precise values of these constants in certain cases.

Conjecture 2 (Gao, Hou, Schmid and Thangadurai [41]). *Let $n \in \mathbb{N}$. Then*

$$s(\mathbb{Z}_n^3) = \begin{cases} 8n-7, & \text{if } n \text{ is even} \\ 9n-8, & \text{if } n \text{ is odd.} \end{cases}$$

Above conjecture had been established by Gao (see [41]) for $n = 3^a5^b$ and $n = 2^a3$, where $a, b \in \mathbb{N}$. Thinking in the direction of the above conjecture we got the desired value of $s(\mathbb{Z}_{nm}^r)$, under some assumptions on n, m and r. The precise statement of the theorem is as follows:

Theorem 7. *Assume that $m \geq 3$ is a fixed positive integer such that $\eta(\mathbb{Z}_m^r) = a_r(m-1)+1$, for some constant a_r depending on r. Further, assume that*

$$n \geq \frac{m^r(c(r)m - a_r(m-1) + m - 3)(m-1) - (m+1) + (m+1)(a_r+1)}{m(m+1)(a_r+1)}$$

is a fixed positive integer such that $s(\mathbb{Z}_n^r) = (a_r+1)(n-1)+1$. In the above lower bound on n, $c(r)$ is the Alon-Dubiner constant. Then, $s(\mathbb{Z}_{nm}^r) = (a_r+1)(nm-1)+1$.

Basically, the technique of proving this theorem is to extract zero-sum subsequences cleverly. After proving the theorem, we shall give some examples and observations, which will give us the exact value of $\eta(G)$ and $s(G)$ for few more groups.

Generalizations of the combinatorial invariants $E(G)$ and $D(G)$ with weights were considered in [4] and [7] for finite cyclic groups. Later in [3], generalizations for an arbitrary finite abelian group G were introduced. Given an abelian

group G of order n, and a finite non-empty subset A of integers, the *Davenport constant of G with weight A*, denoted by $D_A(G)$, is defined to be the least positive integer t such that for every sequence $(x_1, \cdots, x_t)$ with $x_i \in G$, there exists a non-empty subsequence $(x_{j_1}, \cdots, x_{j_l})$ such that $\sum_{i=1}^{l} a_i x_{j_i} = 0$, for some $a_i \in A$. Similarly, for an abelian group G of order n, $E_A(G)$ is defined to be the least positive integer t such that every sequence of length t of elements of G contains a subsequence $(x_{j_1}, \cdots, x_{j_n})$ such that $\sum_{i=1}^{n} a_i x_{j_i} = 0$, for some $a_i \in A$. When G is of order n, one may consider A to be a non-empty subset of $\{0, 1, \cdots, n-1\}$ and for the obvious reasons one assumes that $0 \notin A$. If G is the cyclic group $\mathbb{Z}/n\mathbb{Z}$ we denote $E_A(G)$ and $D_A(G)$ by $E_A(n)$ and $D_A(n)$ respectively.

S. D. Adhikari, C. David and J. Urroz (See [5]) considered the problem of determining values of $D_{R_n}(n)$ and $E_{R_n}(n)$, where $R_n = \{x^2 : x \in (\mathbb{Z}/n\mathbb{Z})^*\}$ and $(\mathbb{Z}/n\mathbb{Z})^*$ is group of units modulo n. The case $n = p$, a prime had already been dealt with by S. D. Adhikari and P. Rath in [7]. We have extended some results from [5]. In what follows, for a positive integer n, $\Omega(n)$ (resp. $\omega(n)$) denotes the number of prime factors of n counted with multiplicity (resp. without multiplicity).

We now state some results which are used in our proofs.

Theorem A (Yuan and Zeng [79]). *Let A be a finite non-empty subset of integers and n a positive integer. We have*

$$E_A(n) = D_A(n) + n - 1.$$

Theorem B (I. Chowla [24],[62]). *Let n be a natural number, and let A and B be two non-empty subsets of $\mathbb{Z}/n\mathbb{Z}$, such that $0 \in B$ and $A+B \neq \mathbb{Z}/n\mathbb{Z}$. If $\gcd(x, n) = 1$ for all $x \in B \setminus \{0\}$ then $|A + B| \geq |A| + |B| - 1$.*

Definition. *For a non-empty subset A of an abelian group G, the stabilizer*

of A, denoted by $Stab(A)$ is defined as follows,

$$Stab(A) = \{x \in G : x + A = A\}.$$

We shall also need the following generalization of Theorem B due to M. Kneser [52, 53, 54] (for the statement in the following form one may look into [62] or [45]).

Theorem C. *Let G be an abelian group, and let A and B be finite, non-empty subsets of G. Let $H = Stab(A + B)$. Then*

$$|A + B| \geq |A + H| + |B + H| - |H|.$$

More precisely, we prove

Theorem 8. *Let $n = 3^\alpha$. Then we have*

(i) $D_{R_n}(n) = 2\Omega(n) + 1$, *and*

(ii) $E_{R_n}(n) = n + 2\Omega(n)$.

Theorem 9. Let $n = 2^\alpha$, $\alpha \geq 3$. Then we have $D_{R_n}(n) \leq 7\Omega(n) + 1$ and $E_{R_n}(n) \leq n + 7\Omega(n)$.

To prove the following theorem we have extended Lemma 9 and Lemma 10 of [5].

Theorem 10. *Let $n = 5^l \prod_{i=2}^{k} p_i^{\alpha_i}$, where $l, \alpha_i \geq 0$, primes $p_i \geq 7$, for each $i \in \{2, \cdots, k\}$. Let $m \geq 3\omega(n) + 1$ and $S = (x_1, x_2, \cdots, x_{m+2\Omega(n)+l})$ be a sequence of length $m+2\Omega(n)+l$ of integers. Then there exists a subsequence $(x_{i_1}, x_{i_2}, \cdots, x_{i_m})$ and $a_1, a_2, \cdots, a_m \in R_n$ such that $\sum_{j=1}^{m} a_j x_{i_j} \equiv 0 \pmod{n}$. In particular,*

$$E_{R_n}(n) \leq n + 2\Omega(n) + l.$$

This completes the sketch of my thesis.

After the brief introduction to my thesis, I would like to indicate how this thesis is organised in the rest. In the first chapter, we recall the important results about zero-sum problems and give some basic definitions. We shall also give proofs of certain important results. The second chapter (based on [22]) is on upper bound of Davenport constant of a finite abelian group. In the third chapter (based on [60]), we shall talk about higher dimensional analogue of Erdős-Ginzburg-Ziv Theorem. Finally, in the fourth chapter (based on [23]), we shall talk about weighted zero-sum problems with respect to the weight $A = \{1, -1\}$.

List of publications and preprints related to this thesis:

1. (with M. N. Chintamani, W. D. Gao, P. Paul, R. Thangadurai) *On Davenport's constant,* Preprint.
2. *On Zero Sum subsequences of restricted size,* Proc. Indian Acad. Sci. (Math. Sci.) Vol. 120, No. **4**, September 2010, pp. 395-402.
3. (with M. N. Chintamani) *Generalizations of some Zero Sum Theorems,* Preprint.

To my grandfather and other members of my family.

Table of Contents

Chapter 1

Introduction

Zero-sum additive theory is an area of mathematics whose oldest roots trace back to Cauchy, but which has only recently begun experiencing rapid growth and development. In this chapter we shall give proof of the some of the theorems that we are going to use in the subsequent chapters of this thesis. And we shall give the references to the theorems which we are not proving in this chapter.

1.1 The Erdős-Ginzburg-Ziv Theorem

A familiar high school problem says that given any sequence of n integers $a_1, a_2, \cdots, a_n$, there exists a non-empty subsequence, which sum up to 0 (mod n). In other words, $\exists$ nonempty $I \subset \{1, 2, \cdots, n\}$ such that

$$\sum_{i \in I} a_i \equiv 0 \pmod{n}. \tag{1}$$

Indeed, if one considers the sums $s_1 = a_1, s_2 = a_1 + a_2, \cdots, s_n = a_1 + \cdots + a_n$, then either some s_i is 0 (mod n) or by Pigeon Hole Principle at least two of the s_i's are equal modulo n.

Weighted generalization of the above problem is an interesting question. We do not take up this question in the present chapter, but shall be dealing with this problem

in the last chapter.

We [23] take up generalization of the problem in another direction, where one asks about prescribing the size of I (with introducing some weights) in (1). In this particular direction, a theorem of Erdős, Ginzburg and Ziv [32] (henceforth, referred to as the EGZ theorem) says the following,

Theorem 1.1.1 (EGZ Theorem)**.** *For any positive integer n, any sequence $a_1, a_2, \cdots, a_{2n-1}$ of $2n-1$ integers has a subsequence of n elements whose sum is 0 modulo n.*

A prototype of zero-sum theorems, the EGZ theorem continues to play a central role in the development of this area of combinatorics. In the chapter, we survey this area, give references to some related questions and try to summarize some of the recent developments including the result of C. Reiher [71]. We shall also give a proof of Rónyai's theorem at the end of Section 1.3.

Apart from the original paper of Erdős, Ginzburg and Ziv [32], there are many proofs of the above theorem available in the literature (see [1], [11], [17], [62], for instance). We shall present two proofs of EGZ theorem in this section.

The higher dimensional analogue of the EGZ theorem, which was considered initially by Harborth [49] and Kemnitz [51] has given rise to a very active area of combinatorics today. In Section 1.2, we shall take up this theme and mention some results of Alon, Dubiner [11], [10] and Reiher [71] in this direction along with other related questions. We shall end Section 1.3 with a Rónyai's [72] proof of $f(p,2) \leq 4p-2$, where p is a prime number. And in Chapter 3 we shall be dealing with results in this direction (see [60]).

Finally, in Section 1.4, we briefly describe the analogous questions related to general finite groups.

Proof of Theorem 1.1.1 We observe that the essence of the EGZ theorem lies in

the case when n is a prime. For the case $n = 1$, there is nothing to prove and let us assume the result is true in the case when n is a prime. Now, we proceed by induction on the number of prime factors (counted with multiplicity) of n. Therefore, if $n > 1$ is not a prime, we write $n = mp$, where p is prime. Since number of prime factors of m (counted with multiplicity) is less than that of n, by induction hypothesis theorem holds true for m. We shall use this fact later.

By our assumption, each subsequence of $2p-1$ members of the sequence $a_1, a_2, \cdots, a_{2n-1}$ has a subsequence of p elements whose sum is 0 modulo p. From the original sequence we go on repeatedly omitting such subsequences of p elements having sum equal to 0 modulo p. Even after $2m-2$ such sequences are omitted, we are left with $2pm - 1 - (2m-2)p = 2p - 1$ elements and so we can extract at least one more subsequence of p elements with the property that sum of its elements is equal to 0 modulo p.

Thus we have found $2m-1$ pairwise disjoint subsets $I_1, I_2, \cdots, I_{2m-1}$ of $\{1, 2, \cdots, 2mp-1\}$ with $|I_i| = p$ and $\sum_{j \in I_i} a_j \equiv 0 \pmod{p}$ for each $i \in \{1, 2, \cdots, 2m-1\}$. We now consider the sequence $b_1, b_2, \cdots, b_{2m-1}$ where for $i \in \{1, 2, \cdots, 2m-1\}$, b_i is the integer $\frac{1}{p}\sum_{j \in I_i} a_j$.

Now as we have just observed by the induction hypothesis, this new sequence has a subsequence of m elements whose sum is divisible by m. The union of the corresponding sets I_i will supply the desired subsequence of $mp = n$ elements of the original sequence such that the sum of the elements of this subsequence is divisible by n.

Let us now proceed to establish the result in the case $n = p$, a prime. For the first proof presented here, we shall need the following result (for a proof of which, one may look into [1] or [50], for instance).

Theorem 1.1.2 (Chevalley-Warning)**.** *Let $f_i(x_1, x_2, \cdots, x_n)$, $i = 1, \cdots, r$, be r polynomials in $\mathbb{F}_q[x_1, x_2, \cdots, x_n]$ such that the sum of the degrees of these polynomials is*

less than n and $f_i(0,0,\cdots,0)=0$, $i=1,\cdots,r$. Then there exists $(\alpha_1,\alpha_2,\cdots,\alpha_n)\in \mathbb{F}_q^n$ with not all α_i's zero, which is a common solution to the system $f_i(x_1,x_2,\cdots,x_n)=0$, $i=1,\cdots,r$.

Here and in what follows, for any prime power q, $\mathbb{F}_q$ will denote the finite field with q elements and the symbol $\mathbb{F}_q^*$ will denote the multiplicative group of non-zero elements of $\mathbb{F}_q$.

Now we proceed to prove Theorem 1.1.1 for the case $n=p$, a prime, which will finish the proof of Theorem 1.1.1. Given a sequence $a_1,a_2,\cdots,a_{2p-1}$ of elements of $\mathbb{F}_p$, we consider the following system of two equations in $(2p-1)$ variables over the finite field $\mathbb{F}_p$:

$$\sum_{i=1}^{2p-1} a_i x_i^{p-1}=0,$$
$$\sum_{i=1}^{2p-1} x_i^{p-1}=0.$$

Since $2(p-1)<2p-1$ and $x_1=x_2=\cdots=x_{2p-1}=0$ is a solution, by Theorem 1.1.2 above, there is a nontrivial solution $(y_1,\cdots,y_{2p-1})$ of the above system. By Fermat's little theorem, writing $I=\{i: y_i\neq 0\}$, from the first equation it follows that $\sum_{i\in I} a_i=0$ and from the second equation we have $|I|=p$.

For our second proof of the 'prime case' of EGZ theorem, we shall need the following generalized version of *Cauchy-Davenport inequality* ([20], [25], can also look into [58] or [62] for instance):

Theorem 1.1.3 (Cauchy-Davenport)**.** *Let $A_1,A_2,\cdots,A_h$ be non-empty subsets of $\mathbb{F}_p$. Then*

$$\left|\sum_{i=1}^{h} A_i\right| \geq min\left(p, \sum_{i=1}^{h}|A_i|-h+1\right).$$

(Here $\sum_{i=1}^{h} A_i$ is the set consisting of all elements of $\mathbb{F}_p$ of the form $\sum_{i=1}^{h} a_i$ where $a_i \in A_i$.)

Now, for a prime p, we consider representatives modulo p in the interval $0 \leq a_i \leq p-1$ for the given elements and rearranging, if necessary, we assume that

$$0 \leq a_1 \leq a_2 \leq \cdots \leq a_{2p-1} \leq p-1.$$

We can now assume that

$$a_j \neq a_{j+p-1}, \quad \text{for } j = 1, \cdots, p-1.$$

For otherwise, the p elements $a_j, a_{j+1}, \cdots, a_{j+p-1}$ being equal, the result holds trivially.

Now, applying Theorem 1.1.3 on the sets

$$A_i := \{a_j, a_{j+p-1}\}, \text{ for } \quad j = 1, \cdots, p-1,$$

so that

$$\left| \sum_{j=1}^{p-1} A_i \right| \geq min \left(p, \sum_{i=1}^{p-1} |A_i| - (p-1) + 1 \right) = p,$$

we have

$$-a_{2p-1} \in \sum_{j=1}^{p-1} A_i$$

and hence once again we have established EGZ theorem for the case when n is a prime. □

Remark 1.1.1. The EGZ theorem as well as many other zero-sum results can also find their place in a larger class of results in combinatorics. More precisely, a result saying that a substructure can not avoid certain regularity properties of the original structure because the 'size' of the substructure is 'large' enough, or a structure which sufficiently 'big' has certain unavoidable regularities, is termed as a *Ramsey-type theorem* in combinatorics.

Remark 1.1.2. Let us now observe that in Theorem 1.1.1, the number $2n-1$ is the smallest positive integer for which the theorem holds. In other words, if $f(n)$ denotes the smallest positive integer such that given a sequence $a_1, a_2, \cdots, a_{f(n)}$ of not necessarily distinct integers, there exists a set $I \subset \{1, 2, \cdots, f(n)\}$ with $|I| = n$ such that $\sum_{i\in I} a_i \equiv 0 (\text{mod } n)$, then $f(n) = 2n-1$. This can be seen as follows. From Theorem 1.1.1, it follows that $f(n) \leq 2n-1$. On the other hand, if we take a sequence of $2n-2$ integers such that $n-1$ among them are 0 modulo n and the remaining $n-1$ are 1 modulo n, then clearly, we do not have any subsequence of n elements, sum of whose elements is 0 modulo n. The idea we have used to prove EGZ theorem will be used many times in this thesis.

1.2 Higher dimensional analogue of EGZ theorem

As in Remark 1.1.2, for any positive integer d, we define $f(n,d)$ to be the smallest positive integer such that given a sequence of $f(n,d)$ number of not necessarily distinct elements of $\mathbb{Z}^d$, there exists a subsequence $x_{i_1}, x_{i_2}, \cdots, x_{i_n}$ of length n such that its centroid $(x_{i_1} + x_{i_2} + \cdots + x_{i_n})/n$ also belongs to $\mathbb{Z}^d$. In other words, $f(n,d)$ is the smallest positive integer N such that every sequence of N elements in $(\mathbb{Z}/n\mathbb{Z})^d$ has a subsequence of n elements which add up to $(\underbrace{0, 0, \cdots, 0}_{d\text{-times}})$. We observe that $f(n,1) = f(n)$ where $f(n)$ is as defined in Remark 1.1.2.

This higher dimensional analogue was first considered by Harborth [49]; he observed the following general bounds for $f(n,d)$.

Since the number of elements of $(\mathbb{Z}/n\mathbb{Z})^d$ having coordinates 0 or 1 is 2^d, considering a sequence where each of these elements are repeated $(n-1)$ times, one observes that

$$1 + 2^d(n-1) \leq f(n,d). \tag{2}$$

Again, observing that in any sequence of $1 + n^d(n-1)$ elements of $(\mathbb{Z}/n\mathbb{Z})^d$ there will

be at least one vector appearing at least n times, we have

$$f(n,d) \leq 1 + n^d(n-1). \tag{3}$$

For $d = 1$, the EGZ theorem gives the exact value

$$f(n,1) = 2n - 1.$$

For the case $d = 2$ also, the lower bound in (2) is expected to give the right magnitude of $f(n,2)$ and this expectation, which is known as *Kemnitz Conjecture* in the literature, has been recently established by Reiher (see [71]). In view of (2) and (4), to establish the Kemnitz's conjecture, it is enough to prove $f(p,2) = 4p - 3$, for all primes p, and that is what Reiher did. We shall state Reiher's result in the next section. Historically, the first result in this direction was contained in the above mentioned paper of Harborth [49] where he proved that $f(3,2) = 9$. Kemnitz [51] established this conjecture when n is of the form $2^e 3^f 5^g 7^h$. However, the lower bound given in (2) is known not to be tight in general. Harborth [49] proved that $f(3,3) = 19$; this is strictly greater than the lower bound 17 which one obtains from (2). Different proofs of the result $f(3,3) = 19$ appeared since then (see [18] and [2], for instance; see also [10] for some more references in this regard). However, Harborth's result on $f(3,3)$ did not rule out the possibility that for a fixed dimension d, for a sufficiently large prime p the lower bound in (2) might determine the exact value for $f(p,d)$. But a recent result of Elsholtz [31] in this direction, rules out such possibilities. We shall come back to this theme very shortly.

Another important observation made by Harborth [49] was the following:

$$f(mn,d) \leq \min(f(n,d) + n(f(m,d)-1), f(m,d) + m(f(n,d)-1)). \tag{4}$$

This result follows by an elementary argument of the same nature as was adopted in deriving Theorem 1.1.1 from the result in the 'prime case'.

Harborth [49] observed that from (2), (3) and (4), one can easily derive the exact value for $f(2^e, d)$ for any $d \geq 2$. More precisely, for $n = 2$ the lower and upper bounds for $f(2, d)$, given respectively by (2) and (3), are both $2^d + 1$ and assuming $f(2^r, d) = (2^r - 1)2^d + 1$, $f(2^s, d) = (2^s - 1)2^d + 1$ for some particular d, by (2) and (4), it follows that $f(2^{r+s}, d) = (2^{r+s} - 1)2^d + 1$.

However, for all odd primes p and $d \geq 3$, we have a long way to go regarding the exact values for $f(p, d)$.

Coming back to the cases $d \geq 3$, the lower bound in (2) is known not to be the exact value of $f(p, d)$ for all odd primes p. As mentioned earlier, a particular instance of this phenomenon was observed by Harborth [49] by proving that $f(3, 3) = 19$. The following general result in this direction was proved by Elsholtz [31].

Theorem 1.2.1. *For an odd integer $n \geq 3$, the following inequality holds:*

$$f(n, d) \geq \left(\frac{9}{8}\right)^{[\frac{d}{3}]} (n - 1)2^d + 1.$$

Thus the lower bound in (2) is not the correct value of $f(n, d)$ for $d \geq 3$.

Now, one observes that the gap is quite large between the lower and the upper bounds given respectively in (2) and (3). A very important result of Alon and Dubiner [10] says that the growth of $f(n, d)$ is linear in n; when d is fixed and n is increasing, this is much better as compared to the upper bound given by (3). More precisely, Alon and Dubiner [10] proved the following.

Theorem 1.2.2. *There is an absolute constant $c > 0$ so that for all n,*

$$f(n, d) \leq (cd \log_2 d)^d n.$$

The proof of Theorem 1.2.2 due to Alon and Dubiner combines techniques from additive number theory with results about the expansion properties of Cayley graphs with

given eigenvalues. In the same paper [10] the authors conjecture that the estimate in Theorem 1.2.2 can possibly be improved. More precisely, the existence of an absolute constant c is predicted such that

$$f(n,d) \leq c^d n, \text{ for all } n \text{ and } d.$$

1.3 The two dimensional case

As have been mentioned, with Reiher's [71] recent proof of Kemnitz's conjecture the problem has been solved in the two dimensional case. We go through the historical development to some extent.

In the two dimensional case, in a very significant paper [11], Alon and Dubiner proved that

Theorem 1.3.1. *We have*

$$f(n,2) \leq 6n - 5.$$

One can observe that by an argument similar to the one used in the proof of Theorem 1.1.1, the inequality $f(p,2) \leq 6p-5$, for every prime p, implies $f(n,2) \leq 6n-5$, for every n. The proof of the fact that $f(p,2) \leq 6p-5$, as given in this paper of Alon and Dubiner, is ingenious and uses algebraic tools such as the theorem of Chevalley and Warning (Theorem 1.1.2) and the algebra of permanents. It also uses the EGZ theorem, the result in the one dimensional case. It has been indicated in [11] that the proof can be modified to yield the stronger result that $f(p,2) \leq 5p-2$. A relatively simple proof of a slightly weaker version of Theorem 1.3.1 is also sketched in this paper.

We now state a sharper result due to Rónyai [72].

Theorem 1.3.2. *For a prime p, we have*

$$f(p,2) \leq 4p-2.$$

Remark 1.3.1. As we have mentioned before, from the inequality $f(p,2) \leq 6p-5$, for every prime p, by an argument similar to the one used in the proof of Theorem 1.1.1 one gets the result $f(n,2) \leq 6n-5$, for every n. Such would be the case for the bound $f(n,2) \leq 4n-3$ of Kemnitz's conjecture. However, this argument does not go through for the bound given by the above theorem. But, as mentioned in Rónyai [72], it is not difficult to observe that Theorem 1.3.2 along with (4) implies that

$$f(n,2) \leq \frac{41}{10}n.$$

Since Kemnitz proved $f(n,2) = 4n-3$, whenever n is of the form $2^e3^f5^g7^h$, and $4n-3 \leq \frac{41}{10}n$. So $f(n,2) \leq \frac{41}{10}n$ for all positive integers n which does not have a prime factor greater than 7.

Indeed, if we write $n = mp$, where $p \geq 11$ is a prime and assume $f(m,2) \leq \frac{41}{10}m$, then using $f(p,2) \leq 4p-2$ and (4), we get $f(mp,2) \leq (f(p,2)-1)m + f(m,2) \leq (4p-3)m + \frac{41}{10}m \leq \frac{11}{10}m + 4mp \leq \frac{mp}{10} + 4mp = \frac{41}{10}n$.

Gao [34] obtained the following generalization of the result (Theorem 1.3.2) of Rónyai [72] mentioned before.

Theorem 1.3.3. *For an odd prime p and a positive integer r, we have*

$$f(p^r,2) \leq 4p^r-2.$$

Following Gao [34], we now sketch a proof of Theorem 1.3.3. We note that this proof proceeds along a line which is quite different from the proof of Theorem 1.3.2 as given by Rónyai [72].

The proof uses the following special case of a very elegant result of Olson [64]. Apart from being interesting in its own right, it has several important results as its immediate corollaries.

Lemma 1.3.4 (Olson)**.** *For a prime p, let $s_1, s_2, \cdots, s_k$ be a sequence S of elements of $(\mathbb{Z}/p^r\mathbb{Z})^d$ such that $k \geq 1 + d(p^r - 1)$. Then, writing $f_e(S)$ for the number of subsequences of even length of S which sum up to zero and $f_o(S)$ for the number of subsequences of odd length which sum up to zero, we have*

$$f_e(S) - f_o(S) \equiv -1 \pmod{p}.$$

First we note the following two corollaries to Lemma 1.3.4; these will be used to prove Theorem 1.3.3. Later we shall remark about few more consequences of the above lemma of Olson.

Lemma 1.3.5. *If S is a zero-sum sequence of $3p^r$ elements in $(\mathbb{Z}/p^r\mathbb{Z})^2$, then S contains a zero-sum subsequence of length p^r.*

For any sequence S of elements of $(\mathbb{Z}/p^r\mathbb{Z})^2$, if $r(S)$ denotes the number of zero-sum subsequences W of S with $|W| = 2p^r$, one has the following.

Lemma 1.3.6. *Let T be a sequence of elements of $(\mathbb{Z}/p^r\mathbb{Z})^2$ with $3p^r - 2 \leq |T| \leq 4p^r - 1$. Suppose that T contains no zero-sum subsequence of length p^r. Then*

$$r(T) \equiv -1 \pmod{p}.$$

Both the above lemmas follow easily from Lemma 1.3.4 by appending 1 as the third coordinate to each of the elements in S and T respectively. For instance, if S in Lemma 1.3.5 is $(a_1, b_1), (a_2, b_2), \cdots, (a_m, b_m)$, where $m = 3p^r$, one considers the sequence

$S' = (a_1, b_1, 1), (a_2, b_2, 1), \cdots, (a_l, b_l, 1)$ with $l = 3p^r - 2$. Now, by Lemma 1.3.4, S' and hence $S_1 = (a_1, b_1), (a_2, b_2), \cdots, (a_l, b_l)$ must have a zero-sum subsequence, length of which must be p^r or $2p^r$. If there is a zero-sum subsequence S_2 of S_1 of length $2p^r$, then its complement in S provides us with one such with length p^r. Hence Lemma 1.3.5 follows. Let T' be the sequence corresponding to T with the length same as that of T. Since T does not have a zero sum subsequence of length p^r, by Lemma 1.3.5 it does not have a zero sum subsequence of length $3p^r$. So $f_e(T') - f_o(T') = r(T') = r(T)$. Therefore, by Lemma 1.3.4, we get Lemma 1.3.6.

Proof of Theorem 1.3.3. If possible, suppose that there is a sequence S of elements of $(\mathbb{Z}/p^r\mathbb{Z})^2$ such that S is of length $4p^r - 2$ and S has no zero-sum subsequence of length p^r.

By Lemma 1.3.6,

$$r(T) \equiv -1 \pmod{p},$$

for every subsequence T of S with $|T| \geq 3p^r - 2$.

We have

$$\sum_{T \subset S,\ |T| = 3p^r - 2} r(T) = \binom{4p^r - 2 - 2p^r}{3p^r - 2 - 2p^r} r(S).$$

Hence

$$\sum_{T \subset S,\ |T| = 3p^r - 2} (-1) \equiv \binom{2p^r - 2}{p^r - 2} (-1) \pmod{p}.$$

Thus

$$\binom{4p^r - 2}{3p^r - 2} \equiv \binom{2p^r - 2}{p^r - 2} \pmod{p},$$

which would imply that

$$3 \equiv \binom{4p^r - 2}{3p^r - 2} \equiv \binom{2p^r - 2}{p^r - 2} \equiv 1 \pmod{p}$$

- a contradiction. □

Remark 1.3.2. As was observed by Alon and Dubiner [11], the EGZ theorem follows almost immediately from Lemma 1.3.4. More precisely, for any prime p, given any

sequence $a_1, a_2, \cdots, a_{2p-1}$ of elements of $(\mathbb{Z}/p\mathbb{Z})$, we just consider the sequence

$$(a_1, 1), (a_2, 1), \cdots, (a_{2p-1}, 1)$$

in $(\mathbb{Z}/p\mathbb{Z})^2$.

Remark 1.3.3. Regarding implications of Lemma 1.3.4 we must mention that in the original paper of Olson [64], the lemma was used to find the value of Davenport's constant $D(G)$ for a finite abelian p-group G. For any finite abelian group G, the important combinatorial invariant *Davenport's constant* $D(G)$ is defined to be the smallest positive integer s such that for any sequence $g_1, g_2, \cdots, g_s$ of (not necessarily distinct) elements of G, there is a nonempty $I \subset \{1, \cdots, s\}$ such that $\sum_{\in I} g_i = 0$. For relations between Kemnitz's conjecture and a conjecture involving the Davenport's constant and some other conjectures related to zero-sum problems, one may look into some papers of Thangadurai [77] and Gao and Geroldinger [40]. In Section 1.4, we shall have an occasion to state an important relation (due to Gao [35]) between the Davenport's constant and another constant emerging out from a natural generalization of the EGZ theorem for finite abelian groups.

Theorem 1.3.7 (Reiher)**.** *For an odd prime p, we have*

$$f(p, 2) = 4p - 3.$$

We now consider a generalization of $f(n, d)$ as defined in the beginning of Section 1.2. Let $f_r(n, d)$ denote the smallest positive integer such that given any sequence of $f_r(n, d)$ elements in $(\mathbb{Z}/n\mathbb{Z})^d$, there exists a subsequence of (rn) elements whose sum is zero in $(\mathbb{Z}/n\mathbb{Z})^d$. Thus $f_1(n, d) = f(n, d)$.

As has been mentioned in a paper of Gao and Thangadurai [43], one can derive (as in [40]) that

$$f_r(n, 2) = (r + 2)n - 2, \text{ for integers } r \geq 2 \tag{5}$$

from the known results about the Davenport's constant for finite abelian p-groups and by using Reiher's result on the exact value of $f_1(n,2)$. Indeed we shall use following result of Gao [34] and Reiher's Theorem [71] to conclude (5).

Theorem 1.3.8. *Let q be a prime power. Then we have $f(q,2) \leq 4q-2$ and $f_2(q,2) \leq 4q-2$.*

Exact values of $f_r(n,1)$ for $r \geq 1$ can be easily obtained from the EGZ theorem. We shall be dealing with case $r = 1$ in Chapter 3 (See [60]).

As had been mentioned in the introduction, we shall conclude this section with a sketch of Rónyai's recent proof of Kemnitz's conjecture. We mention that some interesting partial results towards the conjecture of Kemnitz and some related results had been obtained by Gao [41], Thangadurai [76] and Sury and Thangadurai [74]. We shall need following lemma before giving the proof of Rónyai's theorem [72] (see also [1]).

Lemma 1.3.9. *Let F be a field and m a positive integer. Then the (multilinear) monomials $\prod_{i\in I} x_i,\ I \subset \{1,2,\cdots,m\}$ constitute a basis of the F-linear space of all functions from $\{0,1\}^m$ to F (Here 0 and 1 are viewed as elements of F).*

Proof. The monomials $\prod_{i\in I} x_i,\ I \subset \{1,2,\cdots,m\}$ span a linear space of dimension 2^m over F. This is also the dimension of the space of functions from $\{0,1\}^m$ to F, therefore it suffices to verify that every function from the latter set can be expressed as an F-linear combination of the monomials $\prod_{i\in I} x_i$. The space of functions is clearly spanned by the characteristic functions $\chi_u,\ u \in \{0,1\}^m$, where $\chi_u(u) = 1$ and $\chi_u(v) = o$ if $v \neq u$, hence it is enough to establish the required representation for characteristic functions. Write $u = (u_1, u_2, \cdots, u_m)$ and let $U \subset \{1,2,\cdots,m\}$ be the set of coordinate positions j where $u_j = 1$ and U' be the set of indices j with $u_j = 0$. Then we have

$$\chi_u(x_1, x_2, \cdots, x_m) = \prod_{i\in U} x_i \prod_{i\in U'} (1 - x_i)$$

as functions on $\{0,1\}^m$. By expanding the right hand side we obtain an expression of the desired form. This proves the lemma. □

Now, we shall give the proof of the Rónyai's theorem.

Proof of Theorem 1.3.2. The assertion is obvious for $p = 2$, hence we may assume that p is an odd prime. Put $m = 4p - 2$.

Let

$$v_1 = (a_1, b_1), v_2 = (a_2, b_2), \cdots, v_m = (a_m, b_m)$$

be a sequence of terms from $\mathbb{Z}_p \oplus \mathbb{Z}_p$. We have to prove that there exists an $I \subset \{1, 2, \cdots, m\}$, $|I| = p$ such that $\sum_{i\in I} v_i = (0, 0)$.

Let $\sigma(x_1, x_2, \cdots, x_m) := \sum_{I\subset\{1,2,\cdots,m\},\ |I|=p} \prod_{i\in I} x_i$ denote the p-th elementary symmetric polynomial of the variable $x_1, x_2, \cdots, x_m$. By Lemma 1.3.5 it is enough to prove that there is a subset J of $\{1, 2, \cdots, m\}$, with $|J| = p$ or $|J| = 3p$ such that $\sum_{i\in J} v_i = (0, 0)$. Assume on the contrary that, there does not exist such J. Consider the polynomial P over the prime field $\mathbb{F}_p$,

$$P := \left(\left(\sum_{i=1}^{m} a_i x_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^{m} b_i x_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^{m} x_i\right)^{p-1} - 1\right)\mathcal{A},$$

where $\mathcal{A} = (\sigma(x_1, x_2, \cdots, x_m) - 2)$. We claim that P vanishes on all vectors $u \in \{0,1\}^m$, except on the all 0 vector $\mathbf{0}$, where $P(\mathbf{0}) = 2$. Indeed, the third factor vanishes on u unless it has Hamming weight (the number of ones) multiple of p. If the Hamming weight of u is $2p$ then one can easily see that, $\sigma(u) = \binom{2p}{p} = 2$ in $\mathbb{F}_p$, hence the last factor vanishes on u. Finally if the Hamming weight of u is p or $3p$ then

$$\left(\left(\sum_{i=1}^{m} a_i x_i\right)^{p-1} - 1\right)\left(\left(\sum_{i=1}^{m} b_i x_i\right)^{p-1} - 1\right)$$

is 0 on u by the indirect hypothesis. We obtained that $P = 2\chi_0$ as function on $\{0,1\}^m$. Note also that $\deg P \leq 3(p-1)+p = 4p-3$. Now, reduce P into a linear combination of multilinear monomials by using the relations $x_i^2 = x_i$ (which are valid on $\{0,1\}^m$)

and let Q denote the resulting expression. Clearly, we have $Q = 2\chi_0$ as a function on $\{0,1\}^m$ and $\deg Q \leq 4p-3$, because reduction can not increase the degree. But this is in contradiction with the uniqueness part of Lemma 1.3.9, form the multilinear representative of $2\chi_0 = 2(1-x_1)(1-x_2)\cdots(1-x_m)$ has degree $m = 4p-2$. Hence theorem is proved. □

1.4 EGZ theorem for finite groups

It is not difficult to see that following the method employed in deriving Theorem 1.1.1 from the 'prime case', and appealing to the structure theorem for finite abelian groups, one can derive Theorem 1.4.1 from the EGZ theorem.

Theorem 1.4.1. *Let G be an abelian group of order n. Then given any sequence $g_1, g_2, \cdots, g_{2n-1}$ of $2n-1$ elements of G, there exists a subsequence of n elements whose sum is the identity element 0 of G.*

We note that for the cyclic group of order n, $2n-1$ is the smallest number satisfying the above property. That is, if for any abelian group G of order n, if $\mathrm{Z}S(G)$ is the smallest integer t such that for any sequence of t elements of G, there exists a subsequence of n elements whose sum is the identity element 0 of G, then we have

$$\mathrm{Z}S(\mathbb{Z}/n\mathbb{Z}) = 2n-1.$$

Sometimes the notation $E(G)$ is also used instead of $\mathrm{Z}S(G)$ in the literature. By Theorem 1.4.1, $\mathrm{Z}S(G) \leq 2n-1$, for any abelian group G of order n. However, for a non-cyclic abelian group G of order n, $\mathrm{Z}S(G)$ need not be equal to $2n-1$. In this direction, a result of Alon, Bialostocki and Caro [9] says that for a non-cyclic abelian group G of order n, $\mathrm{Z}S(G) \leq \frac{3n}{2}$ and the bound $\frac{3n}{2}$ is realized only by groups of the form $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$. Subsequently, Caro [19] showed that if a non-cyclic abelian group G of order n is not of the form $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$, then $\mathrm{Z}S(G) \leq \frac{4n}{3} + 1$ and this

bound is realized only by groups of the form $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3m\mathbb{Z}$. Further generalization of the same nature have been obtained by Ordaz and Quiroz [68] rather recently stating that apart from the groups $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2m\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3m\mathbb{Z}$ which appear in the last statement, for any non-cyclic abelian group G of order n, $\mathrm{Z}S(G) \leq \frac{5n}{4}+2$ and equality holds only for groups of the form $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4m\mathbb{Z}$. Further generalization of these results describing the situation with abelian groups G having smaller values of $\mathrm{Z}S(G)$ may involve groups other than $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z}$, $\cdots$, $\mathbb{Z}/r\mathbb{Z} \oplus \mathbb{Z}/rm\mathbb{Z}$, for positive integers r. One should mention that the method of Ordaz and Quiroz [68] involves obtaining an upper bound for the Davenport's constant $D(G)$ (as defined in Remark 1.3.3) of the relevant groups G and using the following beautiful result of Gao [35] which links $\mathrm{Z}S(G)$ with $D(G)$.

Theorem 1.4.2. *If G is a finite abelian group of order n, then $ZS(G) = D(G)+n-1$.*

One would also like to know the validity of the statement of Theorem 1.4.1 for general finite groups.

For a finite solvable group G, by induction on the length k of a minimal abelian tower $(0) = G_k \subset G_{k-1} \subset \cdots \subset G_0 = G$ and using the result in Theorem 1.4.1, one can easily derive (see [67],[73], for instance) the following result employing the same argument as employed in the proof of Theorem 1.1.1 in deriving the general case from the 'prime case'.

Theorem 1.4.3. *Let G be a finite solvable group (written additively) of order n. Then given any sequence $g_1, g_2, \cdots, g_{2n-1}$ of $2n-1$ elements of G, there exist n distinct indices $i_1, \cdots, i_n$ such that*

$$g_{i_1} + g_{i_2} + \cdots + g_{i_n} = 0.$$

The above result holds without the assumption that the group G is solvable. This follows from the following general result of Olson [66].

Theorem 1.4.4. *Let G be a finite group (written additively) of order $n > 1$. Let S be a sequence $g_1, g_2, \cdots, g_{2n-1}$ of elements of G in which no element appears more than n times. Then G has a subgroup K of order $k > 1$ and S has a subsequence $T = a_1, \cdots, a_{n+k-1}$ such that*

i) K is a normal subgroup of the subgroup H of G generated by the elements $\{a_1, a_2, \cdots, a_{n+k-1}\}$,

ii) there exists an $a \in H$ such that $a_i \in a + K = K + a$ for $1 \leq i \leq n + k - 1$, and

iii) K is the set of all sums $a_{i_1} + \cdots + a_{i_n}$ where $i_1, \cdots, i_n$ are n distinct indices (in any order) in $\{1, \cdots, n + k - 1\}$.

We note that for a non-abelian group G of order n, given a sequence of $2n-1$ elements of G, we are not ensured that there is a subsequence of n elements which adds up to the identity, rather a permutation of a subsequence of length n will do so. However, it is conjectured [66] that there must be a subsequence of n elements which adds up to the identity. This is not known even for solvable groups.

1.5 Kneser's Addition Theorem

A beautiful theorem of Kneser is about sums of finite subsets of an abelian group G. We need the following definitions to state the theorem.

For a non-empty subset A of an abelian group G. The *stabilizer* of A, denoted by $Stab(A)$, is defined as the following set,

$$Stab(A) = \{x \in G : x + A = A\}.$$

One can easily see that $0 \in Stab(A)$ and $Stab(A)$ is a subgroup of G. Moreover, $Stab(A)$ is a largest subgroup of G such that,

$$Stab(A) + A = A.$$

In particular, $Stab(A) = G$ if and only if $A = G$. An element $g \in Stab(A)$ is called a *period* of A, and A is called a *periodic set* if $Stab(A) \neq \{0\}$ and A is called an *aperiodic*

set if $Stab(A) = 0$. For example, if A is an infinite arithmetic progression in $\mathbb{Z}$ with difference d, then $Stab(A) = d\mathbb{Z}$.

Kneser proved that if A and B are non-empty, finite subsets of an abelian group G, then either $|A + B| \geq |A| + |B|$ or

$$|A + B| = |A + H| + |B + H| - |H|,$$

where $H = Stab(A + B)$ is the stabilizer of $A + B$.

Note that, if $\phi : G \to G/H$ is the natural group homomorphism, where $H = Stab(A)$, then $Stab(\phi(A)) = \{H\} \subset G/H$. In other words, $\phi(A)$ is an aperiodic subset of G/H.

Next, we shall state Kneser's Theorem.

Theorem 1.5.1 (Kneser's Addition Theorem)**.** *Let G be an abelian group, and let A and B be finite, non-empty subsets of G. Let $H = Stab(A + B)$. Then*

$$|A + B| \geq |A + H| + |B + H| - |H|.$$

Following theorem is a consequence of the above theorem, which is also referred as Kneser's Addition Theorem sometimes.

Theorem 1.5.2. *Let G be an abelian group, and let $A_1, A_2, \cdots, A_k$ be k finite, non-empty subsets of G. Let $H = Stab(A_1 + A_2 + \cdots + A_k)$. Then*

$$|A_1 + A_2 + \cdots + A_k| \geq |A_1 + H| + |A_2 + H| + \cdots + |A_k + H| - (k - 1)|H|.$$

Theorem 1.5.3 (I. Chowla)**.** *Let $m \geq 2$, and let A and B be non-empty subsets of $\mathbb{Z}/m\mathbb{Z}$. If $0 \in B$ and $\gcd(b, m) = 1$ for all $b \in B \setminus \{0\}$, then*

$$|A + B| \geq \min(m, |A| + |B| - 1).$$

In the special case when G is a finite cyclic group, Kneser's theorem implies the theorems of Cauchy-Davenport (Theorem 1.1.3) and I. Chowla (Theorem 1.5.3). Theorem 1.5.3 follows from Kneser's theorem in following way,

Let A and B be non-empty subsets of $\mathbb{Z}/m\mathbb{Z}$ such that $0 \in B$ and $\gcd(n, m) = 1$, for any $n \in B \setminus \{0\}$. If $A + B = \mathbb{Z}/m\mathbb{Z}$, then we are through. Suppose $A + B \neq \mathbb{Z}/m\mathbb{Z}$. Kneser's Theorem implies $|A+B| \geq |A+H|+|B+H|-|H|$, where $H = Stab(A+B)$. Since $\gcd(n, m) = 1$, for any $n \in B \setminus \{0\}$, $H \neq n+H$. Therefore $|B+H| = |B'+H|+|H|$, where $B' = B \setminus \{0\}$. So $|A+B| \geq |A+H|+|B'+H| \geq |A|+|B'| = |A|+|B|-1$. So we have Chowla's theorem. Clearly Cauchy-Davenport theorem (Theorem 1.1.3) follows from Chowla's theorem.

1.6 Weighted EGZ Theorem

If n is a positive integer, we will identify $\mathbb{Z}_n$ with the set of integers $\{0, 1, 2, \cdots, n-1\}$. Adhikari et. al. [3, 7, 4, 5] generalized well known constants $\mathrm{Z}S(G)$ and $D(G)$ to $E_A(G)$ and $D_A(G)$ respectively. Sometimes the notation $E(G)$ is used instead of $\mathrm{Z}S(G)$, in literature. Let G be an additive finite abelian group of order n with additive identity 0. Let A be a non-empty subset of integers. The weighted EGZ constant, denoted by $E_A(G)$, is defined as the least $t \in \mathbb{N}$ such that for every sequences $x_1, x_2, \cdots, x_t$ of elements of G, there exist indices $j_1, j_2, \cdots, j_n \in \mathbb{N}$, $1 \leq j_1 < j_2 < \cdots < j_n \leq t$ and $(a_1, a_2, \cdots, a_n) \in A^n$ with $\sum_{i=1}^{n} a_i x_{j_i} = 0$. And the weighted Davenport's constant $D_A(G)$, is defined as the least $t \in \mathbb{N}$ such that for all sequences $x_1, x_2, \cdots, x_t$ of elements of G, there exist indices $j_1, j_2, \cdots, j_k \in \mathbb{N}$, $1 \leq j_1 < j_2 < \cdots < j_k \leq t$ and $(a_1, a_2, \cdots, a_k) \in A^k$ with $\sum_{i=1}^{k} a_i x_{j_i} = 0$. For obvious reasons we take $A \subset \{1, 2, \cdots, \exp(G) - 1\}$. When G is a cyclic group $\mathbb{Z}_n$, we denote $E_A(G)$ and $D_A(G)$ by $E_A(n)$ and $D_A(n)$ respectively.

For several sets $A \subset \mathbb{Z}_n \setminus \{0\}$ of weights, exact value of $E_A(n)$ and $D_A(n)$ have been determined (see [4, 5, 7]. The case $A = \{1\}$ is covered by the well known EGZ theorem. In [23] we shall be extending the results of [5]. And in [22] we shall be giving an upper bound on the Davenport constant $D(G)$. The case $A = \{\pm 1\} = \{1, -1\}$ was done in [4], where it has been shown that, $E_A(n) = n + \lfloor \log_2 n \rfloor$. Moreover, by the

pigeonhole principle one can easily see, $D_A(n) \leq \lfloor \log_2 n \rfloor + 1$ (See [4]). And by considering the sequence $1, 2, 2^2, \cdots, 2^r$, where r is defined by $2^{r+1} \leq n < 2^{r+2}$, it follows that, $D_A(n) \geq \lfloor \log_2 n \rfloor + 1$. Hence, $D_A(n) = \lfloor \log_2 n \rfloor + 1$. It has also been observed in [4] that for $A = \{1, 2, 3, \cdots, n-1\}$, we have $E_A(n) = n+1$. In this case it is very clear that, $D_A(n) = 2$. So for $A = \{1, 2, 3, \cdots, n-1\}$ and $A = \{\pm 1\}$ we have $E_A(n) = D_A(n) + n - 1$. In [4] it has been conjectured that $E_A(n) = n + \Omega(n)$, where $A = \{a \in \{1, 2, 3, \cdots, n-1\} : \gcd(a, n) = 1\}$ and $\Omega(n)$ is the number of prime factors of n, counted with multiplicity. This conjecture was independently established by F. Luca [55] and S. Griffiths [47]. It has been expected by Adhikari and conjectured by R. Thangadurai [75] that, $E_A(G) = D_A(G) + |G| - 1$. This conjecture has been established recently by Grynkiewicz, Marchan and Ordaz [48]. Before this the following partial results had been obtained by Adhikari and Chen [3], Yuan and Zeng [79].

Theorem 1.6.1 (Adhikari, Chen)**.** *Let G be a finite abelian group of order n and $A = \{a_1, a_2, \cdots, a_r\}$ be a non-empty subset of $\mathbb{Z}$ and $r \geq 2$. If $\gcd(a_2 - a_1, a_3 - a_1, \cdots, a_r - a_1, n) = 1$, then $E_A(G) = D_A(G) + n - 1$.*

Theorem 1.6.2 (Yuan, Zeng)**.** *Let A be any non-empty subset of $\mathbb{Z}$. Then $E_A(n) = D_A(n) + n - 1$.*

Now we give the plan of the remaining chapters. In Chapter 2 we shall be giving an upper bound on a Davenport constant of a finite abelian group of rank r. In Chapter 3 we shall give a conditional result in the direction of higher dimensional analogue of Erdős-Ginzburg-Ziv Theorem. In Chapter 4 we shall be giving an upper bound on weighted Erdős-Ginzburg-Ziv constant for one particular weight, $A = \{\pm 1\}$.

Chapter 2

On Davenport's constant

2.1 Introduction

Let G be a finite abelian group. By the structure theorem, we know $G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ where n_i's are integers satisfying $1 < n_1 | n_2 | \cdots | n_r$; n_r is the *exponent* (denoted by $\exp(G)$) of G and r is the *rank* of G. Also, $n_1, n_2, \cdots, n_r$ are called *invariants* of G. Let

$$M(G) = 1 + \sum_{i=1}^{r} (n_i - 1).$$

As had been mentioned in Remark 1.3.3, **Davenport constant** (respectively, **Olson constant**) of a finite abelian group G denoted by $D(G)$ (respectively, $Ol(G)$) is defined to be the least positive integer t such that any sequence (respectively, set) of t elements in G contains a subsequence (respectively, subset) whose sum is zero in G. Such a subsequence (respectively, subset) is called **zero-sum subsequence (respectively, zero-sum subset)**.

It is trivial to see that $M(G) \leq D(G) \leq |G|$. The equality holds if and only if $G = \mathbb{Z}_n$, the cyclic group of order n (See [6]). Olson [64] and [65] proved that $D(G) = M(G)$ for all finite abelian groups of rank 2 and for all finite abelian p-groups. It is also known that $D(G) > M(G)$, for infinitely many groups (See [46], for instance). The

best known upper bound is due to Emde Boas and Kruyswijk [78], Meshulam [59] and Alford, Granville and Pomerance [8], (see also, [13]) and they proved that

$$D(G) \leq \exp(G)\left(1 + \log \frac{|G|}{\exp(G)}\right). \tag{1}$$

Some refinement of this bound was recently achieved by Rath, Srilakshmi and Thangadurai in [70]. Their theorem is as follows:

Let G be a finite abelian group of rank m and of exponent n. Let $\ell_1, \ell_2, \cdots, \ell_{d-1}$ and r be integers such that $1 \leq \ell_i \leq n-1$ for all $i = 1, 2, \cdots, d-1$ and the positive integer

$$r := \begin{cases} n + \left[n\left(\sum_{i=1}^{d-1} \log \ell_i - \log \frac{n^d}{|G|} \right) \right] & \text{if } \prod_{i=1}^{d-1} \ell_i > \frac{n^d}{|G|} \\ n & \text{otherwise} \end{cases}$$

Let

$$S = (\underbrace{g_1, \cdots, g_1}_{(n-\ell_1) \text{ times}}, \cdots, \underbrace{g_{d-1}, \cdots, g_{d-1}}_{(n-\ell_{d-1}) \text{ times}}, c_1, c_2, \cdots, c_r)$$

be a sequence in G of length $\rho = \sum_{i=1}^{d-1}(n - \ell_i) + r$. Then S has a subsequence whose product is identity in G.

Obtaining a good upper bound for the Davenport constant constitutes a very important question about which the current state of knowledge is rather limited. However, we do have the following conjectures.

Conjecture 2.1.1. *(i) $D(G) = M(G)$ for all finite abelian groups G with rank $r = 3$ or $G = \mathbb{Z}_n^r$ (See [36], [37], for instance);*

(ii) For any finite abelian group G, $D(G) \leq \sum_{i=1}^{r} n_i$ (See [61], for instance), where n_i's are invariants of G.

Concerning Conjecture 2.1.1*(i)*, recently, G. Bhowmik and J-C. Schlage-Puchta [15], proved that 2.1.1*(i)* above is true whenever

$$G \cong \mathbb{Z}_3 \oplus \mathbb{Z}_{3a} \oplus \mathbb{Z}_{3ab}.$$

We have been thinking in direction of getting an upper bound on Davenport's constant of an abelian group of rank r. And we ended up with the upper bound given in Theorem 2.1.1. Before introducing this theorem we need to define certain constants.

For a subset S of natural numbers and a finite abelian group G, we define **the generalized davenport constant** (denoted by $D^S(G)$) to be the least integer t such that every sequence of length t of elements of G has a zero-sum subsequence of length ℓ for some $\ell \in S$. Dimitrov [28] defined this constant and studied its properties.

When $S = \mathbb{N}$, then we see that $D^{\mathbb{N}}(G) = D(G)$. When $S = \{1, 2, \cdots, m\}$, then we denote $D^S(G)$ by $D^m(G)$. Also, when $S = \{\exp(G)\}$, then the constant $D^{\{\exp(G)\}}(G)$ is nothing but the well-known constant $s(G)$ which is defined to be the least positive integer t such that given any sequence of G of length t has a zero-sum subsequence of length precisely the exponent of G.

Also, in the literature $D^{\exp(G)}(G)$ is known as $\rho(G)$ which is defined to be the least positive integer t such that any sequence of G of length t has a zero-sum subsequence of length less than or equal to the exponent of G. Both of these constants $\rho(G)$ and $s(G)$ will be explored in the chapter on higher dimensional analogue of Erdős-Ginzburg-Ziv Theorem. Sometimes in literature, the notation $\eta(G)$ is used in place of $\rho(G)$.

By definition of $\rho(G)$, there exists a sequence of length $\rho(G)-1$ of elements of G which does not contain a zero sum subsequence of length at most $\exp(G)$. Considering this sequence together with sequence of $\exp(G) - 1$ many 0 (identity element of G), we shall get a sequence of length $\rho(G) + \exp(G) - 2$, which does not have a zero sum subsequence of length $\exp(G)$. And one can easily see by definition, $D(G) \leq \rho(G)$. Therefore we have,

$$D(G) \leq \rho(G) \leq s(G) - \exp(G) + 1.$$

Indeed, $D(G)$ and $s(G)$ are the corner-stones of these type of 'zero-sum problems'. When $G = \mathbb{Z}_n^r$, by the work of Alon and Dubiner [10], it is known that $s(G)$ is bounded

above by a linear function in n and they showed that

$$s(\mathbb{Z}_n^r) \leq c(r)n, \tag{2}$$

where $c(r)$ is a constant which depends on r. It is known that $c(1)$ can be taken as 2 (due to Erdős, Ginzburg and Ziv [32]) and $c(2)$ can be taken as 4 (due to C. Reiher [71]). In general, in our current state of knowledge, $c(r)$ can be taken satisfying

$$c(r) \leq 256(r \log_2 r + 5)c(r-1) + (r+1) \tag{3}$$

for all $r \geq 3$. In particular,

$$c(3) \leq 9994. \tag{4}$$

Also, from (3), one can arrive at the following general bound;

$$c(r) \leq (cr \log_2 r)^r, \tag{5}$$

for an absolute constant c.
Also, it is clear that

$$\rho(\mathbb{Z}_n^r) \leq s(\mathbb{Z}_n^r) - n + 1 \leq (c(r) - 1)n + 1. \tag{6}$$

Conjecture 2.1.2 (Gao [39])**.** *We have,* $c(3) \leq 9$.

The following is the main theorem in this chapter, which is in the direction of Conjecture 2.1.1*(ii)*.

Theorem 2.1.1. *Let G be any finite abelian group of rank r with invariants $n_1, n_2, \cdots, n_r$. Then*

$$D(G) \leq n_r + n_{r-1} + (c(3) - 1)n_{r-2} + (c(4) - 1)n_{r-3} + \cdots + (c(r) - 1)n_1 + 1,$$

where the constants $c(r)$ satisfy (2).

Corollary 2.1.2. *If Conjecture 2.1.2 is true, then, we have*

$$D(G) \leq n_3 + n_2 + 8n_1 + 1$$

for all finite abelian groups G of rank 3.

Corollary 2.1.3. *Let $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ be the finite abelian group of rank r If Conjecture 2.1.1(i) is true for $\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k}$ for some positive integer $3 \leq k \leq r-1$, then, we have,*

$$D(G) \leq n_r + n_{r-1} + \cdots + n_{r-k+1} + (c(k+1)-1)n_{r-k+2} + \cdots + (c(r)-1)n_1 + 1.$$

Theorem 2.1.1 is the extension of the results proved by Dimitrov in [28] and Balasubramanian and Bhowmik in [14]. Dimitrov used Alon Dubiner constant to prove that $D(G) \leq M(G)(Kr\log r)^r$, where K is an absolute constant.

Theorem (Balasubramanian and Bhowmik). *Let G be a finite abelian group of order n and exponent m, then for $k \leq 7$, its Davenport constant $D(G) \leq \frac{n}{k} + k - 1$, whenever $\frac{n}{m} \geq k$.*

Note that Theorem 2.1.1 asserts that for all finite abelian group G of rank $r \geq 3$, we have

$$D(G) \leq rd(r)\exp(G) \tag{7}$$

where $d(r)$ is a constant depends only on the rank r. Whereas (1) implies

$$D(G) \leq r\exp(G)\log\exp(G). \tag{8}$$

This is because, (1) and $|G| \leq (\exp(G))^r$ together implies

$$\begin{aligned} D(G) &\leq \exp(G) + \exp(G)\log\frac{|G|}{\exp(G)} \\ &\leq \exp(G) + (r-1)\exp(G)\log\exp(G) \\ &\leq r\exp(G)\log\exp(G). \end{aligned}$$

Note that when $\exp(G) < e^{d(r)}$, then (8) is better bound than the bound in (7).

Before giving the proof of Theorem 2.1.1, we shall provide an application of Davenport's constant to factor integers using smooth numbers. To state the precise result, we need the following.

A non-empty finite set of positive integers consisting of distinct primes $p_1, p_2, \cdots, p_d$ is called a *factor base*. An integer $n > 1$ is said to be *smooth* with respect to factor base $F = \{p_1, p_2, \cdots, p_d\}$ if all prime factors of n are in F.

In quadratic sieve (see [69]), to factor a given integer N with a factor base F, one needs to know how many smooth integers that are required to produce two distinct squares such that $x^2 \equiv y^2 \pmod{N}$. It is well-known that if we can find $|F|+1 = d+1$ number of smooth integers with respect to factor base F, then we can find two squares which are equivalent modulo N.

Instead of squares, if we want to produce two cubes which are equivalent modulo N, then how many smooth numbers we need to produce? More generally, for any given integer $k \geq 2$, if we want to produce two k-th powers which are equivalent modulo N, how many smooth integers we need to have?

By $c(k, d)$, we denote the least positive integer t such that for any multiset U of smooth integers, with respect to F, of cardinality at least t has a non-empty multisubset T with the following property:

$$\prod_{a \in T} a = b^k$$

for some integer b.

It is clear that often a good bound for $c(k, d)$ will supply us two distinct squares such that $x^2 \equiv y^2 \pmod{N}$. When $k = 2$, it is well-known that $c(2, d) = d + 1$.

Question. What is the exact value of $c(k, d)$ for each $k, d \geq 2$?

Theorem 2.1.4. *For all positive integers n and d, we have $c(n,d) = D(\mathbb{Z}_n^d)$.*

Proof. We shall first prove that $c(n,d) \leq D(\mathbb{Z}_n^d)$. Let $\ell = D(\mathbb{Z}_n^d)$ and let $U = \{m_1, m_2, \cdots, m_\ell\}$, be a multiset, where each m_i is smooth number with respect to F. Hence we can write

$$m_i = p_1^{e_{1i}} p_2^{e_{2i}} \cdots p_d^{e_{di}},$$

for each $i = 1, 2, \cdots, \ell$ where $e_{ij} \geq 0$ integers.

We associate each m_i to $a_i \in \mathbb{Z}_n^d$ as follows;

$$m_i \mapsto a_i := (e_{1i}, e_{2i}, \cdots, e_{di}) \pmod{n}$$

for all $i = 1, 2, \cdots, \ell$. Let $S = (a_1, a_2, \cdots, a_\ell)$ be the sequence in $\mathbb{Z}_n^d$ of length $\ell = D(\mathbb{Z}_n^d)$. Therefore, by the definition, we can find a non-empty subsequence T' whose sum is identity in $\mathbb{Z}_n^d$. Let $T' = (a_{j_1}, a_{j_2}, \cdots, a_{j_t})$ be the subsequence of S whose sum is the zero element of $\mathbb{Z}_n^d$. Hence, we get,

$$\sum_{i=1}^{t} e_{kj_i} \equiv 0 \pmod{n} \text{ for all } k = 1, 2, \cdots, d. \tag{9}$$

Consider the multisubset T of U which is corresponding T'. Clearly, $T = \{m_{j_1}, m_{j_2}, \cdots, m_{j_t}\}$ and by equation (9), we get

$$\prod_{m \in T} m = \prod_{i=1}^{d} p_i^{\sum_{k=1}^{t} e_{ij_k}} = \left(\prod_{i=1}^{d} p_i^{k_i} \right)^n$$

for some integers $k_i \geq 0$ for all $i = 1, 2, \cdots, d$. Thus, by the definition of $c(n,d)$, it is clear that $c(n,d) \leq D(\mathbb{Z}_n^d)$.

Now, let us prove $D(\mathbb{Z}_n^d) \leq c(n,d)$. Let $\ell = c(n,d)$ and let $S = (a_1, a_2, \cdots, a_\ell)$ be a sequence in $\mathbb{Z}_n^d$ of length ℓ where for each $i = 1, 2, \cdots, \ell$ we have

$$a_i = (e_{1i}, e_{2i}, \cdots, e_{di}) \in \mathbb{Z}_n^d.$$

Let

$$m_i = p_1^{e_{1i}} p_2^{e_{2i}} \cdots p_d^{e_{di}}$$

for all $i = 1, 2, \cdots, \ell$. Clearly, if we let $U = \{m_1, m_2, \cdots, m_\ell\}$, then U is a multiset of smooth numbers with respect to F. Since $\ell = c(n, d)$, by definition, there exists a non-empty subset T of U such that

$$\prod_{a \in T} a = b^n \text{ where } b = p_1^{k_1} p_2^{k_2} \cdots p_d^{k_d}$$

for some integers $k_i \geq 0$. If we let $T = \{m_{j_1}, m_{j_2}, \cdots, m_{j_t}\}$, then a subsequence T' of S corresponding to T, will sum up to identity in $\mathbb{Z}_n^d$. Hence $D(\mathbb{Z}_n^d) \leq c(n, d)$ and the theorem follows. □

Corollary 2.1.5. *We have $c(p^\ell, d) = d(p^\ell - 1) + 1$ where p is any prime number and $\ell \geq 1$ is an integer.*

Proof. As we have mentioned in Section 2.1, $D(G) = M(G)$ for $G = \mathbb{Z}_{p^\ell}^d$, the corollary follows from above theorem. □

Theorem 2.1.6. *Let n be any integer and $\omega(n)$ denote the number of distinct prime factors of n. Then*

$$D(\mathbb{Z}_n^r) \leq r^{\omega(n)}(n-1) + 1.$$

For any rank $r \geq 3$, Theorem 2.1.6 asserts that $D(\mathbb{Z}_n^r) \leq r^2(n-1) + 1$ for every $n = p_1^{a_1} p_2^{a_2}$ for two distinct primes $p_1 \neq p_2$. This bound cannot come from Theorem 2.1.1, as the constant involved in Theorem 2.1.1 is $\sim (r \log_2 r)^r$. Also, for rank 3 case we have the following better bound for specific values of n's.

Theorem 2.1.7. *Let $n = 3^\alpha p^\ell$ be any integers such that $p \geq 3$ be any prime number. Then*

$$3n - 2 \leq D(\mathbb{Z}_n^3) \leq 3n + 3^{\alpha+1} - 7.$$

In particular, when $\alpha = 1$, then we get,

$$3n - 2 \leq D(\mathbb{Z}_n^3) \leq 3n + 2.$$

Along the same lines of the proof of Theorem 2.1.1, we can prove the following theorem for $s(G)$.

Theorem 2.1.8. *Let G be a finite abelian group of rank r with invariants $n_1, n_2, \cdots, n_r$. Then*

$$s(G) \leq c(1)n_r + c(2)n_{r-1} + \cdots + c(r)n_1.$$

Theorem 2.1.9. *Let G be a finite abelian group of rank r with invariants $n_1, n_2, \cdots, n_r$. Then*

$$\rho(G) \leq (c(1) - 1)n_r + (c(2) - 1)n_{r-1} + \cdots + (c(r) - 1)n_1 + 1.$$

2.2 Preliminaries

We shall start with some basic propositions which will be useful to conclude theorems. Throughout this section, we assume that the given finite abelian group G, unless otherwise specified, is not a p-group.

Proposition 2.2.1. *Let p be a prime number and let $n_1, n_2, \cdots, n_r > 1$ be integers such that $p^k | n_1 | n_2 | \cdots | n_r$. Let $m > 1$ be the unique integer such that*

$$(m - 1)D(\mathbb{Z}_{p^k}^r) \leq D^{p^k}(\mathbb{Z}_{p^k}^r) < mD(\mathbb{Z}_{p^k}^r).$$

Let

$$h := \begin{cases} D(\mathbb{Z}_{\frac{n_1}{p^k}} \oplus \cdots \oplus \mathbb{Z}_{\frac{n_r}{p^k}}) & \text{if } n_1 \neq p^k \\ D(\mathbb{Z}_{\frac{n_2}{p^k}} \oplus \cdots \oplus \mathbb{Z}_{\frac{n_r}{p^k}}) & \text{if } n_1 = p^k, n_2 \neq p^k \\ \cdots & \cdots \\ D(\mathbb{Z}_{\frac{n_r}{p^k}}) & \text{if } n_1 = n_2 = \cdots = n_{r-1} = p^k, n_r \neq p^k \end{cases}$$

Then we have,

$$D(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}) \leq \begin{cases} (h-m+1)p^k + D^{p^k}(\mathbb{Z}_{p^k}^r) & \text{if } h \geq m-1 \\ D^{p^k}(\mathbb{Z}_{p^k}^r) & \text{otherwise.} \end{cases}$$

Furthermore, if $D^{p^k}(\mathbb{Z}_{p^k}^r) - (m-1)D(\mathbb{Z}_{p^k}^r) \geq p^k$, *then we have*

$$D(\mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}) \leq (h-m)p^k + D^{p^k}(\mathbb{Z}_{p^k}^r),$$

provided $h \geq m-1$.

Proof. If $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_r}$ is a p-group, then we know exact value of $D(G)$. Hence we can always assume that G is not a p-group and so $n_i \neq p^k$ for some $i \leq r$.

Let

$$\ell = \begin{cases} (h-m+1)p^k + D^{p^k}(\mathbb{Z}_{p^k}^r) & \text{if } h \geq m-1 \\ D^{p^k}(\mathbb{Z}_{p^k}^r) & \text{if } h < m-1. \end{cases}$$

Let $\Phi : G \longrightarrow \mathbb{Z}_{p^k}^r$ be the natural homomorphism. Let $S = (a_1, a_2, \cdots, a_\ell)$ be a sequence of length ℓ of elements of G. To end the proof, it is enough to produce a zero-sum subsequence T of S.

Assume that $h < m-1$. Then, clearly,

$$hD(\mathbb{Z}_{p^k}^r) < (m-1)D(\mathbb{Z}_{p^k}^r) \leq D^{p^k}(\mathbb{Z}_{p^k}^r).$$

Therefore, there are pairwise disjoint subsets $A_1, A_2, \cdots, A_h$ of $\{1, 2, \cdots, \ell\}$ such that

$$\sum_{i \in A_j} \Phi(a_i) = 0,$$

for each $j = 1, 2, \cdots, h$. As Φ is a homomorphism, we get

$$\Phi\left(\sum_{i\in A_j} a_i\right) = 0,$$

for each $j = 1, 2, \cdots, h$. That is, for each j, $\sum_{i\in A_j} a_i \in \mathrm{Ker}(\Phi)$. By the definition, $h = D(\mathrm{Ker}(\Phi))$, there exists a subset $A \subset \{1, 2, \cdots, h\}$ such that

$$\sum_{j\in A}\sum_{f\in A_{i_j}} a_f = 0 \text{ in } G.$$

Now, we assume that $h \geq m-1$. Since $\ell \geq D^{p^k}(\mathbb{Z}^r_{p^k})$, then by the definition, we can extract $h-m+1$ disjoint zero-sum subsequences $\Phi(B_1), \Phi(B_2), \cdots, \Phi(B_{h-m+1})$ of $\Phi(S)$ such that the length of each B_i is at most p^k. The length of the remaining sequence S', which is obtained by deleting all the elements of $\Phi(B_i)$ from $\Phi(S)$, is at least

$$\ell - (h-m+1)p^k \geq D^{p^k}(\mathbb{Z}^r_{p^k}) \geq (m-1)D(\mathbb{Z}^r_{p^k}).$$

By the definition of $D(\mathbb{Z}^r_{p^k})$, we can extract $m-1$ disjoint zero-sum subsequence say $\Phi(B_{h-m+2}), \cdots, \Phi(B_h)$ of $\Phi(S)$. Clearly, the sums of B_i lie in the kernel of Φ which is a proper subgroup H with $D(H) = h$. Therefore, by the definition of h, we have a zero-sum subsequence of S and hence the result. □

When $r = 3$, we can improve Proposition 2.2.1 as follows;

Corollary 2.2.2. *Let $p \geq 3$ be a prime number and let n_1, n_2 and n_3 be integers such that $p^k | n_1 | n_2 | n_3$. Let*

$$h := \begin{cases} D(\mathbb{Z}_{\frac{n_1}{p^k}} \oplus \mathbb{Z}_{\frac{n_2}{p^k}} \oplus \mathbb{Z}_{\frac{n_3}{p^k}}) & \text{if } n_1 \neq p^k \\ D(\mathbb{Z}_{\frac{n_2}{p^k}} \oplus \mathbb{Z}_{\frac{n_3}{p^k}}) & \text{if } n_1 = p^k, n_2 \neq p^k \\ D(\mathbb{Z}_{\frac{n_3}{p^k}}) & \text{if } n_1 = n_2 = p^k, n_3 \neq p^k. \end{cases}$$

Then we have,

$$D(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3}) \leq (h-3)p^k + D^{p^k}(\mathbb{Z}^3_{p^k}).$$

Proof. By the result (due to Edel, Elsholtz, Geroldinger, Kubertin and Rackham in [30]), we know that $D^n(\mathbb{Z}_n^3) \geq 8n-7$ for all odd integer n. Therefore, the integer m is ≥ 3 in Proposition 2.2.1. Suppose $m = 3$. Since Davenport constant of p-group is known we can assume that G is not a p-group. So $h \geq 2 = 3-1 = m-1$. Also $8p^k - 7 - 2D(\mathbb{Z}_{p^k}^3) = 8p^k - 7 - 2(3p^k - 2) = 2p^k - 3 \geq p^k$. Hence by Proposition 2.2.1, we get the desired result. Suppose $m \geq 4$. If $h \geq m-1$ than by Proposition 2.2.1, $D(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3}) \leq (h-m+1)p^k + D^{p^k}(\mathbb{Z}_{p^k}^3) \leq (h-3)p^k + D^{p^k}(\mathbb{Z}_{p^k}^3)$. Hence we are through in this case also. If $h < m-1$, then we get $D(\mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \mathbb{Z}_{n_3}) \leq D^{p^k}(\mathbb{Z}_{p^k}^3)$. If $h \geq 3$ then $D^{p^k}(\mathbb{Z}_{p^k}^3) \leq (h-3)p^k + D^{p^k}(\mathbb{Z}_{p^k}^3)$. Hence we are through in this case. Since $h \geq 2$, only case we need to take care of is $h = 2$. If $h = 2$, we can clearly see that $G = \mathbb{Z}_{p^k} \oplus \mathbb{Z}_{p^k} \oplus \mathbb{Z}_{2p^k}$. We shall see in the Proposition 2.2.3 that, taking $H = \mathbb{Z}_2$, we get $D(G) \leq (D(\mathbb{Z}_{p^k}^3) - 1)D(H) + 2 \leq 6(p^k - 1) + 2 \leq 7p^k - 7$, since $p \geq 3$. And $7p^k - 7 \leq D^{p^k}(\mathbb{Z}_{p^k}^3) - p^k = D^{p^k}(\mathbb{Z}_{p^k}^3) + (h-3)p^k$. Hence we are through in every case. Hence the corollary is proved. □

Proposition 2.2.3. *If H be any subgroup of G, then*

$$D(G) \leq (D(G/H) - 1)D(H) + 2.$$

Proof. We know from [28] that for any integer $m > 1$, we have

$$D(G) \leq D^m(G/H) + m(D(H) - 1).$$

By choosing $m = D(G/H) - 1$ and by noting that $D^{D(G)-1}(G) = D(G) + 1$, we get the desired result. □

2.3 Proof of Theorems

Proof of Theorem 2.1.1. Given that G is a finite abelian group of rank r. We shall prove that

$$D(G) \leq n_r + n_{r-1} + (c(3)-1)n_{r-2} + (c(4)-1)n_{r-3} + \cdots + (c(r)-1)n_1 + 1$$

by the induction on r. Since $D(\mathbb{Z}_n) = n$, result follows when G is a finite cyclic group. When $r = 2$, a result of Olson implies that

$$D(G) = M(G) \leq n_2 + n_1$$

and hence the theorem follows for groups of rank 2. So we assume the result for some $k \geq 3$ and we shall prove the result for $r = k + 1$.

If $n_1 = n_2 = \cdots = n_r$, then, by (6),

$$D(G) \leq \rho(G) = \rho(\mathbb{Z}_{n_1}^r) \leq (c(r)-1)n_1 + 1.$$

Therefore, the result is true. Hence we assume that $n_r > n_1$. Let

$$H = \mathbb{Z}_{n_1}^r \text{ and } K \cong G/H \cong \mathbb{Z}_{\frac{n_r}{n_1}} \oplus \cdots \oplus \mathbb{Z}_{\frac{n_2}{n_1}}.$$

Let $\varphi : G \to H$ be a canonical homomorphism from G onto H. Then, $\mathrm{Ker}(\varphi) = K$. Let S be a sequence in G of length

$$|S| = n_r + n_{r-1} + (c(3)-1)n_{r-2} + \cdots + (c(r)-1)n_1 + 1.$$

Since $\rho(H) \leq (c(r)-1)n_1 + 1$, we can find disjoint subsequences $S_1, S_2, \cdots, S_\ell$ where

$$\ell = \frac{n_r}{n_1} + \frac{n_{r-1}}{n_1} + (c(3)-1)\frac{n_{r-2}}{n_1} + \cdots + (c(r-1)-1)\frac{n_2}{n_1} + 1$$

of S such that $1 \leq |S_i| \leq n_1$ for every $i = 1, 2, \cdots, \ell$ and $\sigma(\varphi(S_i)) := \varphi(\sum_{a \in S_i} a) = 0$ in H. Therefore, $\sigma(S_1), \sigma(S_2), \cdots, \sigma(S_\ell) \in \mathrm{Ker}(\varphi) = K$. Since the rank of K is $r-1$, by the induction hypothesis, we have

$$D(K) \leq \frac{n_r}{n_1} + \frac{n_{r-1}}{n_1} + (c(3)-1)\frac{n_{r-2}}{n_1} + \cdots + (c(r-1)-1)\frac{n_2}{n_1} + 1 = \ell$$

and hence, we can find a subsequence T of the sequence $\sigma(S_1), \sigma(S_2), \cdots, \sigma(S_r)$ such that whose sum is zero in K. That in turn produces a zero-sum subsequence of S in G. Therefore the result follows. □

Proof of Corollary 2.1.2 and Corollary 2.1.3 are straightforward from the proof of Theorem 2.1.1 and hence we omit their proofs.

To prove Theorem 2.1.6, we need the Proposition 2.2.3.

Proof of Theorem 2.1.6. We shall prove this result by induction on $\omega(n)$, the number of distinct prime factors of n. When $\omega(n) = 1$, then $n = p^\alpha$ and hence result is true, by Olson's result. We shall assume that the result is true for integers m satisfying $\omega(m) < k$. Let $\omega(n) = k$ and $n = p^\alpha p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where $\alpha, \alpha_i > 0$ are integers.

Set $H = \mathbb{Z}^r_{n/p^\alpha}$. Since p^α divides n, clearly H is a subgroup of $\mathbb{Z}^r_n$. Therefore we have $G/H = \mathbb{Z}^r_{p^\alpha}$. Hence by Proposition 2.2.3, we get,

$$\begin{aligned} D(\mathbb{Z}^r_n) &\leq (D(\mathbb{Z}^r_{p^\alpha}) - 1)D(H) + 2 = r(p^\alpha - 1)D(H) + 2 \\ &\leq r(p^\alpha - 1)\left(r^{\omega(n/p^\alpha)}\left(\frac{n}{p^\alpha} - 1\right) + 1\right) + 2. \\ &= r^{\omega(n)}\frac{(p^\alpha - 1)}{p^\alpha}n - (p^\alpha - 1)(r^{\omega(n)} - r) + 2. \end{aligned}$$

To prove the theorem, it is enough to prove that

$$r^{\omega(n)}\frac{(p^\alpha - 1)}{p^\alpha}n - (p^\alpha - 1)(r^{\omega(n)} - r) + 2 \leq r^{\omega(n)}(n-1) + 1.$$

That is to prove that,

$$\frac{r^{\omega(n)}n}{p^\alpha} = r^{\omega(n)}n\left(1 - \frac{(p^\alpha - 1)}{p^\alpha}\right) > r^{\omega(n)} - (p^\alpha - 1)(r^{\omega(n)} - r).$$

If $(p^\alpha - 1)(r^{\omega(n)} - r) \geq r^{\omega(n)}$, then the above inequality obviously holds. So we can assume that $(p^\alpha - 1)(r^{\omega(n)} - r) < r^{\omega(n)}$. Since $\omega(n) \geq 2$, we get $p^\alpha \leq 2$. Since $\alpha > 0,\ p^\alpha = 2$. Hence it is enough to prove that,

$$\frac{r^{\omega(n)}n}{p^\alpha} > r^{\omega(n)} - (r^{\omega(n)} - r) = r,$$

which is true. Hence the theorem. □

Remark 2.3.1. (a) Let $n \geq \exp\left(\prod_{\ell|\omega(n),\ell\neq 1} \Phi_\ell(r)\right)$ where $\Phi_k(X)$ denote the k-th cyclotomic polynomial. Then the above bound improves the bound (1). For, since

$$n \;\geq\; \exp\left(\prod_{\ell|\omega(n),\ell\neq 1} \Phi_\ell(r)\right) = \exp\left(\frac{r^{\omega(n)}-1}{r-1}\right)$$

This implies,

$$(r-1)\log n \geq r^{\omega(n)} - 1.$$

Therefore,

$$n\,(1+(r-1)\log n) \geq r^{\omega(n)} n > r^{\omega(n)}(n-1)+1.$$

In particular, for all integers $n = p^\ell q^m \geq \exp(r+1)$ where $p \neq q$ primes, Theorem 2.1.6 does improve the known bound (1).

(b) When $r = 3$ and $n = q^k p^\ell$ for any primes $p \neq q$ in Theorem 2.1.6, we get $D(\mathbb{Z}_n^3) \leq 9n - 8$. Theorem 2.1.7 improves this result, when $n = 3^\alpha p^\ell$ where $p \neq 3$.

Proof of Theorem 2.1.7. We shall prove the upper bound. First note that $D^3(\mathbb{Z}_3^3) = 17 = 8\times 3 - 7$ (see [31, 49, 18]). Second, observe that if $f(p) = D^p(\mathbb{Z}_p^3) = 8p-7$, then $f(p^\alpha) \leq 8p^\alpha - 7$.

To show this, it is enough prove that

$$f(p^\alpha) \leq (f(p^{\alpha-1})-1)p + f(p).$$

For, let $\ell = (f(p^{\alpha-1})-1)p + f(p)$. Consider a sequence S in $\mathbb{Z}_{p^\alpha}^r$ of length ℓ. Consider an endomorphism $\Phi : \mathbb{Z}_{p^\alpha}^r \longrightarrow \mathbb{Z}_p^r$. Look at the image sequence $\Phi(S)$ and apply the definition of $f(p)$. We get disjoint zero-sum subsequences $\Phi(A_1), \cdots, \Phi(A_k)$ of $\Phi(S)$ each of whose length is at most p where $k = f(p^{\alpha-1})$. Look at the kernel of Φ which

is $\mathbb{Z}^r_{p^{\alpha-1}}$. Then by induction, we can get the desired zero-sum sequence of length at most p^α in S.

Put $p = 3$ in $f(p^\alpha)$. We get $f(3^\alpha) \leq 8 \times 3^\alpha - 7$. But we know that $D^n(\mathbb{Z}^3_n) \geq 8n - 7$ *for all odd integer* n (see [30]). So $f(3^\alpha) \geq 8 \times 3^\alpha - 7$ and hence we get $f(3^\alpha) = 8 \times 3^\alpha - 7$. Now, apply Corollary 2.2.2, by putting $n = 3^\alpha p^\ell$ for all prime $p > 3$. We get

$$\begin{aligned} D(\mathbb{Z}^3_n) &\leq (D(\mathbb{Z}^3_{p^\ell}) - 3)3^\alpha + D^{3^\alpha}(\mathbb{Z}^3_{3^\alpha}) = (3p^\ell - 5)3^\alpha + 8 \times 3^\alpha - 7 \\ &\leq 3n + 3^{\alpha+1} - 7. \end{aligned}$$

Hence the theorem. □

Next we shall give proof of Theorem 2.1.8 and 2.1.9 which is similar to the proof of Theorem 2.1.1.

Proof of Theorem 2.1.8. Given that G is a finite abelian group of rank r. We shall prove that

$$s(G) \leq c(1)n_r + c(2)n_{r-1} + \cdots + c(r)n_1$$

by the induction on r. Since $c(1)$ can be taken as 2 (see [32]), result follows from EGZ theorem, when G is a finite cyclic group. Also we know that $c(2)$ can be taken as 4 (see [71]). It has been proved that, $s(\mathbb{Z}_m \oplus \mathbb{Z}_n) = 2m + 2n - 3$, where $m|n$ (see [45]). Hence for $r = 2$, the theorem follows. So we assume the result for some $k \geq 3$ and we shall prove the result for $r = k + 1$.

If $n_1 = n_2 = \cdots = n_r$, then, by (2),

$$s(G) \leq c(r)n_r.$$

Therefore, the result is true. Hence we assume that $n_r > n_1$. Let

$$H = \mathbb{Z}^r_{n_1} \text{ and } K \cong G/H \cong \mathbb{Z}_{\frac{n_r}{n_1}} \oplus \cdots \oplus \mathbb{Z}_{\frac{n_2}{n_1}}.$$

Let $\varphi : G \to H$ be a canonical homomorphism from G onto H. Then, $\mathrm{Ker}(\varphi) = K$. Let S be a sequence in G of length

$$|S| = c(1)n_r + c(2)n_{r-1} + \cdots + c(r)n_1.$$

Since $s(H) \leq c(r)n_1$, we can find pairwise disjoint subsequences $S_1, S_2, \cdots, S_\ell$, where

$$\ell = c(1)\frac{n_r}{n_1} + c(2)\frac{n_{r-1}}{n_1} + c(3)\frac{n_{r-2}}{n_1} + \cdots + c(r-1)\frac{n_2}{n_1} + 1$$

of S such that $|S_i| = n_1$ for every $i = 1, 2, \cdots, \ell$ and $\sigma(\varphi(S_i)) := \varphi(\sum_{a \in S_i} a) = 0$ in H. Therefore, $\sigma(S_1), \sigma(S_2), \cdots, \sigma(S_\ell) \in \text{Ker}(\varphi) = K$. Since the rank of K is $r-1$, by the induction hypothesis, we have

$$s(K) \leq c(1)\frac{n_r}{n_1} + c(2)\frac{n_{r-1}}{n_1} + c(3)\frac{n_{r-2}}{n_1} + \cdots + c(r-1)\frac{n_2}{n_1} = \ell$$

and hence, we can find a subsequence T of length n_r/n_1 of the sequence $\sigma(S_1), \sigma(S_2)$, $\sigma(S_3)$ $, \cdots, \sigma(S_\ell)$ whose sum is zero in K. That in turn produces a zero-sum subsequence of S of length n_r. Therefore the result follows. □

Proof of Theorem 2.1.9. Given that G is a finite abelian group of rank r. We shall prove that

$$\rho(G) \leq (c(1)-1)n_r + (c(2)-1)n_{r-1} + \cdots + (c(r)-1)n_1 + 1$$

by the induction on r. It has been proved that, $s(\mathbb{Z}_m \oplus \mathbb{Z}_n) = 2m + n - 2$, where $m|n$ (see [45]). As we mentioned in the proof of Theorem 2.1.8, $c(1)$ can be taken as 2 and $c(2)$ can be taken as 4. Hence for $r \leq 2$, the theorem follows. So we assume the result for some $k \geq 3$ and we shall prove the result for $r = k + 1$.

If $n_1 = n_2 = \cdots = n_r$, then, since $\rho(G) \leq (c(r)-1)n_r + 1$, we are done. Hence we may assume that $n_r > n_1$. Let

$$H = \mathbb{Z}_{n_1}^r \text{ and } K \cong G/H \cong \mathbb{Z}_{\frac{n_r}{n_1}} \oplus \cdots \oplus \mathbb{Z}_{\frac{n_2}{n_1}}.$$

Let $\varphi : G \to H$ be a canonical homomorphism from G onto H. Then, $\text{Ker}(\varphi) = K$. Let S be a sequence in G of length

$$|S| = (c(1)-1)n_r + (c(2)-1)n_{r-1} + \cdots + (c(r)-1)n_1 + 1.$$

Since $\rho(H) \leq (c(r)-1)n_1+1$, we can find pairwise disjoint subsequences $S_1, S_2, \cdots, S_\ell$, where

$$\ell = (c(1)-1)\frac{n_r}{n_1} + (c(2)-1)\frac{n_{r-1}}{n_1} + (c(3)-1)\frac{n_{r-2}}{n_1} + \cdots + (c(r-1)-1)\frac{n_2}{n_1} + 1$$

of S such that $1 \leq |S_i| \leq n_1$ for every $i = 1, 2, \cdots, \ell$ and $\sigma(\varphi(S_i)) := \varphi(\sum_{a \in S_i} a) = 0$ in H. Therefore, $\sigma(S_1), \sigma(S_2), \cdots, \sigma(S_\ell) \in \text{Ker}(\varphi) = K$. Since the rank of K is $r-1$, by the induction hypothesis, we have

$$\rho(K) \leq (c(1)-1)\frac{n_r}{n_1} + (c(2)-1)\frac{n_{r-1}}{n_1} + (c(3)-1)\frac{n_{r-2}}{n_1} + \cdots + (c(r-1)-1)\frac{n_2}{n_1} + 1 = \ell$$

and hence, we can find a subsequence T of length at most n_r/n_1 of the sequence $\sigma(S_1), \sigma(S_2), \cdots, \sigma(S_\ell)$ whose sum is zero in K. That in turn produces a zero-sum subsequence of S of length at most n_r. Therefore the result follows. □

2.4 Concluding remarks

It is clear from the definition of Olson's constant that $Ol(G) \leq D(G)$. This constant came from a question of P. Erdős and Heilbronn [33]. For early history, we refer to an article [42]. P. Erdős conjectured the following.

Conjecture 2.4.1 (P. Erdős)**.** *For all finite abelian group G, we have*

$$Ol(G) \leq \sqrt{2|G|}.$$

From the upper bound (1) for $D(G)$, we can see that the Conjecture 2.4.1 is true for all G satisfying

$$|G| \geq (r \exp(G) \log \exp(G))^2. \tag{7}$$

However, Theorem 2.1.1 implies that Conjecture 2.4.1 is true for all G satisfying,

$$|G| \geq \frac{(C(r)r)^2}{2} \exp(G)^2.$$

In particular, (7) implies that Conjecture 2.4.1 is true when $G \cong \mathbb{Z}_n^r$ for all $r \geq 4$ and for all $n \geq 5$ and when $G \cong \mathbb{Z}_n^3$, the Conjecture 2.4.1 is true for all $n \geq 290$. This can be improved for all odd $n \geq 85$ using Corollary 2.1.3.

The above relation does not imply Conjecture 2.4.1 for all groups G with rank ≤ 2, as for these groups $|G| \leq \exp(G)^2$. However, we know that when $r \leq 2$, $D(G) = M(G)$. When $G \cong \mathbb{Z}_n^2$, we know that $Ol(G) \leq D(G) = 2n - 1 < 2\sqrt{|G|}$ for all $n > 1$. It will be interesting to prove that $Ol(\mathbb{Z}_n^2) \leq \sqrt{2}\ n$ for all $n > 1$.

Recently, Nguyen, Szemerédi and Vu [63] and Deshouillers and Prakash [26] independently proved that

$$Ol(\mathbb{Z}_p) \leq \sqrt{2p} + \epsilon$$

for all large enough primes p. In 2004, Gao, Ruzsa and Thangadurai [42] proved that

$$Ol(\mathbb{Z}_p^2) = Ol(\mathbb{Z}_p) + p - 1$$

for all primes $p \geq 4.67 \times 10^{34}$. Recently, Bhowmik and Schlage-Puchta [16] have proved that the above relation is true for all primes $p > 6000$. Therefore, Conjecture 2.4.1 is open for $G \cong \mathbb{Z}_n^2$ for all composite numbers $n > 1$ and for all primes $p < 6000$.

It is also known (see [38]) that $Ol(\mathbb{Z}_n^r) \geq r(n-1) + 1$ for any odd integer $n > 1$ and for any $r \geq 2n + 1$. By Conjecture 2.1.1 *(i)*, we have $D(\mathbb{Z}_n^r) = r(n-1) + 1$. Hence together with the above result, we get, $Ol(\mathbb{Z}_n^r) = D(\mathbb{Z}_n^r)$ for every odd integer n and for any $r \geq 2n + 1$.

Chapter 3

Higher dimensional analogue of Erdős-Ginzburg-Ziv Theorem

3.1 Introduction

Additive number theory, factorization theory and graph theory provide a good source for combinatorial problems in finite abelian groups (See [56, 57, 62, 27, 12], for instance). Among them, zero sum problems have been of growing interest. The cornerstone of almost all recent combinatorial research on zero-sum problems is a theorem of Erdős-Ginzburg-Ziv [32] and a question of H. Davenport on an invariant of finite abelian groups.

In general, our notations and terminology will be the same as the one in factorization theory (cf. survey articles by Chapman, Halter-Koch and Geroldinger in [12] and the paper of Gao and Geroldinger [38]). Here for a finite sequence $S = \{g_1, g_2, \cdots, g_l\} = g_1 g_2 \cdots g_l$ of elements of G, repetitions are allowed and the order is disregarded. If $S = \{a_1, a_2, \cdots, a_k\},\ T = \{b_1, b_2, \cdots, b_k\}$ are two sequences of elements of group G then ST will denote the sequence $\{a_1, a_2, \cdots, a_k, b_1, b_2, \cdots, b_k\}$. In an analogous way one defines the sequence $\prod_{i=1}^{k} A_i$ for given sequences $A_1, A_2, \cdots, A_k$. A sequence T is

called a subsequence of S if there exists a sequence T' such that $TT' = S$; clearly the sequence T' is uniquely determined by S and T and we denote it by ST^{-1}.

Let G be a finite abelian group. We denote a cyclic group of order n by C_n. As defined in Section 2.1, by $s(G)$ (or $\eta(G)$ respectively) we denote the smallest integer $\ell \in \mathbb{N}$ such that every sequence S of length $|S| \geq \ell$ of elements of G has a zero-sum subsequence T of length $|T| = \exp(G)$ (or $1 \leq |T| \leq \exp(G)$ respectively). The investigation of these invariants has a long tradition, and in recent years the investigation of these invariants and of the related inverse problems, i.e., the investigation of the structure of extremal sequences with, and without, the respective properties, received a good deal of attention. Among others, this is due to applications in the theory of non-unique factorizations. We refer to the monograph of Geroldinger and F. Halter-Koch [45], in particular to Chapter 5, for a detailed account of results on these invariants and their applications in the theory of non-unique factorizations, and to the recent survey article of Gao and Geroldinger [39] for an exposition of the state of the knowledge and numerous references.

Still, many questions are wide open. The precise value of $s(G)$ for cyclic groups is known by the classical Erdős-Ginzburg-Ziv Theorem [32], but $s(G)$ for groups of rank 2 has only recently been determined (see [71, 45]) and the precise value of $s(G)$ is unknown for most groups of rank greater than 2, as is the value of $\eta(G)$. We will describe the bounds and precise value in certain cases.

Lemma 3.1.1 (Chi, Ding, Gao et. al. [21])**.** *Let G be a finite abelian group and let $H \subset G$ be a subgroup such that $\exp(G) = \exp(H)\exp(G/H)$. Then*

$$s(G) \leq \exp(G/H)s(H) + s(G/H) - \exp(G/H).$$

Theorem 3.1.2. *Let $m, n, r \in \mathbb{N}$ with $m|n$.*

(i) $\eta(C_m \oplus C_n) = 2m + n - 2$ and $s(C_m \oplus C_n) = 2m + 2n - 3$ (See [71], [45]).

(ii) $\eta(C_n^r) \geq (2^r - 1)(n-1) + 1$ *and* $s(C_n^r) \geq 2^r(n-1) + 1$. *If* n *is a power of 2, then equality holds (See [49], [30]).*

(iii) If n *is odd, then* $\eta(C_n^3) \geq 8n - 7$ *and* $s(C_n^3) \geq 9n - 8$. *If* n *is a power of 3, then equality holds (See [31]).*

In order to prove the main theorem of this paper we will need following upper bound obtained by Alon and Dubiner [10] :

When $G = C_n^r$ then $s(G)$ is bounded above by a linear function of n and they showed that,

$$s(C_n^r) \leq c(r)n, \tag{1}$$

where $c(r)$ is a constant which depends on r. It is known that $c(1)$ can be taken as 2 (due to Erdős, Ginzburg and Ziv [32]), and $c(2)$ can be taken as 4 (due to C. Reiher [71]). In general, in our current state of knowledge $c(r)$ can be taken satisfying,

$$c(r) \leq 256(r \log_2 r + 5)c(r-1) + r + 1, \ for \ r \geq 3.$$

.

Remark 3.1.1. From above expression $c(3)$ turns out to be approximately 9994. So

$$s(C_n^3) \leq 9994n.$$

Conjecture 3.1.1 (Gao, Hou, Schmid, Thangadurai [41])**.** *Let* $n \in \mathbb{N}$. *Then*

$$s(C_n^3) = \begin{cases} 8n - 7, & \text{if } n \text{ is even} \\ 9n - 8, & \text{if } n \text{ is odd.} \end{cases}$$

Remark 3.1.2. If one assumes Conjecture 3.1.1 then from the fact that $s(G) \geq \eta(G) + \exp(G) - 1$ and Theorem 3.1.2*(iii)* it follows that,

$$\eta(C_n^3) = 8n - 7, \text{ if } n \text{ is an odd integer.}$$

Remark 3.1.3. If one assumes Conjecture 3.1.1 then from the fact that $s(G) \geq \eta(G) + \exp(G) - 1$ and $\eta(\mathbb{Z}_n^3) \geq 7n - 6$, for n an even integer, it follows that

$$\eta(C_n^3) = 7n - 6, \text{ if } n \text{ is an even integer.}$$

Remark 3.1.4. It can be easily proved that for n, m both positive integers if $s(C_n^r) = a_r(n-1)+1$ and $s(C_m^r) = a_r(m-1)+1$, then $s(C_{nm}^r) \leq a_r(nm-1)+1$. According to Dr. Wolfgang Schmid, there doesn't seem to be a general process available to get the lower bound on $s(C_{nm}^r)$ in this situation. For example note, $s(C_3^5) = 45(3-1)+1$ is known, but as per him nobody knows $s(C_9^5)$ and there are reasons to believe that they are not related in the form one might expect; for $s(C_3^5) = 45(3-1)+1$ is known but the best lower bound for $s(C_9^5)$ is $42(9-1)+1$ and the upper bound is $45(9-1)+1$. One can see the paper by Y. Edel [29, Theorem 1] for the information on this. Also it has been proved that, $s(C_3^3) = 9(3) - 8 = 19$ (see [49, Satz 4]); also cf. [30, Corollary 4.5]. So in view of Theorem 3.1.2*(iii)*, $s(C_{3^k}^3) = 9(3^k) - 8$, for $k \in \mathbb{N}$.

We prove the following Theorem :

Theorem 3.1.3. *Assume that $m \geq 3$ is a fixed positive integer such that $\eta(C_m^r) = a_r(m-1)+1$, for some constant a_r depending on r. Further, assume that*

$$n \geq \frac{m^r(c(r)m - a_r(m-1) + m - 3)(m-1) - (m+1) + (m+1)(a_r+1)}{m(m+1)(a_r+1)}$$

is a fixed positive integer such that $s(C_n^r) = (a_r+1)(n-1)+1$. In the above lower bound on n, $c(r)$ is the Alon-Dubiner constant. Then, $s(C_{nm}^r) = (a_r+1)(nm-1)+1$.

3.2 Proof of the Main Theorem

Proof of Theorem 3.1.3. Let S is a sequence in C_{nm}^r, $|S| = (a_r + 1)(nm - 1) + 1$. Let S_m be the sequence of all elements of S modulo m. Then, we see that there exists an element $x \in S_m$ which is repeated maximum number of times. We can assume x to be the zero element of S_m, if necessary by translating the elements of S. Note that in S_m at least $\left\lceil \frac{(a_r+1)(nm-1)+1}{m^r} \right\rceil$ zeros are available. (For a real number x by $\lceil x \rceil$ we mean, the least integer $\geq x$).

Let S_m^* be the sequence of all non-zero elements of S_m. From S_m^* take out all possible $k \geq 0$ disjoint non-empty subsequences $R_1, R_2, \cdots, R_k$ with $|R_i| = m$ such that $\sum_{a \in R_i} a = 0 \in C_m^r, \quad \forall\ i = 1, 2, \cdots, k$. Hence, $W := S_m^* \left(\prod_{i=1}^{k} R_i \right)^{-1}$ contains no m-element subsequence whose sum is zero in C_m^r. Hence by a theorem of Alon and Dubiner [10], we have $|W| \leq c(r)m - 1$.

If $|W| \leq a_r(m-1)$ then we shall show that there exist a subsequence of S of length nm which sum up to zero in C_{nm}^r. Let us count all the disjoint m-element subsequences of S_m whose sum is zero in C_m^r . First remove all possible disjoint m-element zero sum subsequences from $S_m(S_m^*)^{-1}$ and say the remaining sequence be A (It may happen that there is no such subsequence. In this case take $A = S_m(S_m^*)^{-1}$). Let the number of all possible disjoint m-element subsequences from $S_m(S_m^*)^{-1}$ be t. Clearly, $0 \leq |A| \leq m - 1$. Then,

$$tm + km = (a_r + 1)(nm - 1) + 1 - |W| - |A|.$$

Hence,

$$t + k \geq \frac{1}{m}((a_r + 1)(nm - 1) + 1 - a_r(m - 1) - m + 1) = (a_r + 1)(n - 1) + \frac{1}{m}.$$

Since $(t+k)$ is an integer, $(t+k) \geq (a_r+1)(n-1)+1$. Hence we have pairwise disjoint m-element subsequences, $I_1, I_2, \cdots, I_{(a_r+1)(n-1)+1}$ of S such that $\sum_{b \in I_j} b = 0 \in C_m^r$ for

every $j = 1, 2, \cdots, (a_r+1)(n-1)+1$. Write $c_j = \frac{1}{m}\sum_{b\in I_j} b$, for every $j = 1, 2, \cdots, (a_r+1)(n-1)+1$. Since $s(C_n^r) = (a_r+1)(n-1)+1$ and we have $(a_r+1)(n-1)+1$ number of integer lattice points $c_1, c_2, \cdots, c_{(a_r+1)(n-1)+1}$, there exist n element subsequence $c_{i_1}, c_{i_2}, \cdots, c_{i_n}$ such that its sum is zero in C_n^r. Thus we get,

$$\sum_{j=1}^{n} c_{i_j} = 0 \in C_n^r \Longrightarrow \sum_{j=1}^{n}\sum_{b\in I_{i_j}} b = 0 \in C_{nm}^r.$$

Hence we are done in this case.

Now we assume that $|W| > a_r(m-1)$ and we show that

1. There are disjoint subsequences $B_1, B_2, \cdots, B_\ell$ of W of length $< m$ with zero sum in C_m^r and with $|B_i| + |B_j| > m$ for $i \neq j$,
2. There are at least $\dfrac{(c(r)m - a_r(m-1) + m - 3)(m-1)}{m+1}$ zeroes in $S_m(S_m^*)^{-1}$, and
3. $\left| W\left(\prod_{i=1}^{\ell} B_i\right)^{-1} \right| \leq a_r(m-1)$.

Since $|W| > a_r(m-1)$ we can find a natural number t, $2 \leq t \leq m-1$ such that one finds such a t-element subsequence of W sums to zero in C_m^r. Let B_1 be a maximal subsequence of W such that $|B_1| = t_1$ with $2 \leq t_1 \leq m-1$ and its sum is zero in C_m^r. Then we can take a subsequence A_1 of S_m which contains $m - t_1$ zeros and together with B_1 we get an m-element subsequence whose sum is zero in C_m^r.

If $|W(B_1)^{-1}| \geq a_r(m-1)+1$, we can find B_2 which is the maximal subsequence of $W(B_1)^{-1}$ with $|B_2| = t_2$ with $2 \leq t_2 \leq m-1$, whose sum is zero in C_m^r. Note that $t_1 \geq t_2$ and $|B_1B_2| > m$. If not, we would have chosen B_1B_2 in the first step and it would have contradicted the maximality. Once we have chosen B_2, take A_2, a subsequence of S_m of all zeros disjoint from A_1 and having cardinality $m - t_2$. Then, A_2B_2 produces an m-element subsequence of S_m whose sum is zero in C_m^r.

Continue this process, until we arrive at $|W(\prod_{i=1}^{\ell} B_i)^{-1}| \leq a_r(m-1)$, where ℓ is a positive integer. We will calculate upper bound of ℓ now. By definition of ℓ, we have

$$a_r(m-1)+1+\sum_{i=1}^{\ell-1}|B_i| \leq |W| \leq a_r(m-1)+\sum_{i=1}^{\ell}|B_i| \tag{2}$$

Case 1. $\ell = 2k$, $k \in \mathbb{N}$.

Since $|B_i| \geq 2, \ \forall i \in \{1,2,\cdots,\ell\}$ and $|B_i|+|B_j| \geq m+1, \ \forall i,j \in \{1,2,\cdots,\ell\}, \ i \neq j$, we have

$$(k-1)(m+1)+2 \leq \sum_{i=1}^{\ell-1}|B_i| \leq |W| - a_r(m-1) - 1$$

Hence,

$$\begin{aligned}
(k-1)(m+1)+2 &\leq c(r)m - a_r(m-1) - 2 \\
\Rightarrow (k-1) &\leq \frac{c(r)m - a_r(m-1) - 4}{m+1} \\
\Rightarrow k &\leq \frac{c(r)m - a_r(m-1) - 4 + m + 1}{m+1} \\
&= \frac{c(r)m - a_r(m-1) + m - 3}{m+1}
\end{aligned}$$

Hence at most $X = \dfrac{(c(r)m - a_r(m-1) + m - 3)(m-1)}{m+1}$ zeros are required in this case.

Case 2. $\ell = 2k+1$, $k \in \mathbb{N} \cup \{0\}$.

Sub-case (I) : $k = 0$. Clearly, number of zeros required is at most $m-2$.

Sub-case (II) : $k \in \mathbb{N}$. Then from (2), we have

$$k(m+1) \leq \sum_{i=1}^{\ell-1}|B_i| \leq |W| - a_r(m-1) - 1$$

$$\Rightarrow k \leq \frac{c(r)m - a_r(m-1) - 2}{m+1}$$

For this sub-case $\ell \geq 3$. Observe that there exists B_i such that $|B_i| \geq \frac{m+1}{2}$. Hence the number of zeros required in this sub-case is at most,

$$Y = \frac{(c(r)m - a_r(m-1) - 2)(m-1)}{m+1} + \frac{m-1}{2}$$

Since $m \geq 3$, $X = \max\{X, Y, m-2\}$. Hence the number of zeros needed in any case is at most, $X = \dfrac{(c(r)m - a_r(m-1) + m - 3)(m-1)}{m+1}$.

Hence in order to make sure that there are at least X zeros in S_m, we need the following condition,

$$|S_m(S_m^*)^{-1}| \geq \left\lceil \frac{(a_r+1)(nm-1)+1}{m^r} \right\rceil \geq X.$$

This holds because

$$n \geq \frac{m^r(c(r)m - a_r(m-1) + m - 3)(m-1) - (m+1) + (m+1)(a_r+1)}{m(m+1)(a_r+1)}$$

by hypothesis.

If $\left| S_m(S_m^*)^{-1} \left(\prod_{i=1}^{\ell} A_i \right)^{-1} \right| \geq m$, remove all possible disjoint m-element subsequences and say the remaining sequence be A. Let us say these subsequences are t in number. Clearly, $0 \leq |A| \leq m-1$. Then,

$$\begin{aligned}
tm + |A| &= (a_r+1)(nm-1) + 1 - |S_m^*| - \sum_{i=1}^{\ell} |A_i|. \\
\Rightarrow tm + \ell m + |A| &= (a_r+1)(nm-1) + 1 - |S_m^*| + \sum_{i=1}^{\ell} |B_i|. \\
&= (a_r+1)(nm-1) + 1 - |W| - km + \sum_{i=1}^{\ell} |B_i|. \\
\Rightarrow (t+\ell+k)m &= (a_r+1)(nm-1) + 1 - |W| + \sum_{i=1}^{\ell} |B_i| - |A|.
\end{aligned}$$

Hence,

$$(t+\ell+k) \geq \frac{1}{m}((a_r+1)(nm-1) + 1 - a_r(m-1) - m + 1) = (a_r+1)(n-1) + \frac{1}{m}.$$

Since $(t+\ell+k)$ is an integer, $(t+\ell+k) \geq (a_r+1)(n-1)+1$. Hence as in the case $|W| \leq a_r(m-1)$ we can extract a zero sum subsequence of S of length nm. Hence the theorem is proved. □

Following are some observations in rank 3 case.

Observations :

1. Take $r = 3,\ a_r = 8$ and n, m odd in the Theorem 3.1.3. Then by Remark 3.1.1 the lower bound on n becomes $\dfrac{(9987m+5)(m-1)m^3+8(m+1)}{9m(m+1)}$.

2. Take $r = 3,\ a_r = 7$ and n, m even in the Theorem 3.1.3. Then by Remark 3.1.1 the lower bound on n becomes $\dfrac{(9988m+4)(m-1)m^3+7(m+1)}{8m(m+1)}$.

3. There is one more bound on $s(G)$ which was given by W. D. Gao et al. [44] (see also [45, Theorem 5.7.4]), which says that for a finite abelian group G of exponent m, $s(G) \leq |G|+m-1$. For those m for which this bound is lesser than that comes from Alon and Dubiner, we can get a better bound on n following same procedure as in the main theorem apart from replacing Alon Dubiner bound by this particular bound. We will get to see the difference between two bounds when we see some examples at the end of this chapter. Following are the bounds that one will get in this situation,

   (i) Assume $\eta(C_m^3) = 8m-7$, m-odd and $m \geq 3$. If $s(C_n^3) = 9n-8$, n-odd and if $n \geq \dfrac{m^3(m^3-6m+4)(m-1)+8(m+1)}{9m(m+1)}$, then $s(C_{nm}^3) = 9nm-8$.

   (ii) Assume $\eta(C_m^3) = 7m-6$, m is an even integer and $m \geq 4$. For n even integer if $s(C_n^3) = 8n-7$, and if $n \geq \dfrac{m^3(m^3-5m+3)(m-1)+7(m+1)}{8m(m+1)}$ then $s(C_{nm}^3) = 8nm-7$.

Now, we will see that using condition on n *and* m in above Observations and following Theorem one can get conjectured bound for few more groups.

Theorem 3.2.1 (Gao [41])**.** *(i) Let $n = 3^a5^b$ for $a, b \in \mathbb{N} \cup \{0\}$. Then*

$$s(C_n^3) = \eta(C_n^3) + n - 1 = 9n - 8.$$

(ii) Let $n = 2^a 3$ for $a \in \mathbb{N}$. Then

$$s(C_n^3) = \eta(C_n^3) + n - 1 = 8n - 7.$$

Examples : (1) Let $n = 3^{12},\ m \in \{3, 5, 7\}$ (using Observation 1). Then

$$s(C_{nm}^3) = \eta(C_{nm}^3) + nm - 1 = 9nm - 8.$$

By using Observation 3(i) we can see that these holds true for $m \in \{3, 5, 7, 9,$ $11, 13, 15, 17, 19, 21\}$.

(2) Let $n = 2^{20}3,\ m \in \{4, 6, 8, 10, 12, 14\}$ (using Observation 2). Then

$$s(C_{nm}^3) = \eta(C_{nm}^3) + nm - 1 = 8nm - 7.$$

By using Observation 3(ii) and Remark 3.1.4 we can see that relation holds true for $m \in \{2n : n \in [1, 15]\}$.

(3) Let $n = 2^{16}$, $m = 4$ (using Observation 2). Then

$$s(C_{nm}^3) = \eta(C_{nm}^3) + nm - 1 = 8nm - 7.$$

By using Observation 3(ii) and Remark 3.1.4 we can see that relation holds true for $m \in \{2, 4, 6, 8, 10, 12, 14\}$.

Chapter 4

Weighted Zero Sum Theorems

4.1 Introduction

Let G be an abelian group of order n, written additively. The *Davenport constant* $D(G)$ is as it had been defined in Remark 1.3.3. And as it had been mentioned in Section 1.4 another combinatorial invariant $E(G)$ (known as the *EGZ constant*) is the smallest natural number t such that any sequence of length t of elements of G has a subsequence of length $|G|$ whose sum is zero. A classical theorem of Erdős, Ginzburg and Ziv [32] says that $E(\mathbb{Z}/n\mathbb{Z}) = 2n - 1$. These two constants are related by a theorem of Gao [35], which states that $E(G) = D(G) + n - 1$.

Generalizations of the constants $E(G)$ and $D(G)$ with weights were considered in [4] and [7] for finite cyclic groups. Later in [3], generalizations for an arbitrary finite abelian group G were introduced. Let us recall definitions of weighted *Davenport constant* and *EGZ constant* given in Section 1.6. Given an abelian group G of order n, and a finite non-empty subset A of integers, the *Davenport constant of G with weight A*, denoted by $D_A(G)$, is defined to be the least positive integer t such that for every sequence $(x_1, \cdots, x_t)$ with $x_i \in G$, there exists a non-empty subsequence $(x_{j_1}, \cdots, x_{j_l})$ such that $\sum_{i=1}^{l} a_i x_{j_i} = 0$, for some $a_i \in A$. Similarly, for an abelian

group G of order n, $E_A(G)$ is defined to be the least positive integer t such that every sequence $(x_1, x_2, \cdots, x_t)$ of length t of elements of G contains a subsequence $(x_{j_1}, \cdots, x_{j_n})$ such that $\sum_{i=1}^{n} a_i x_{j_i} = 0$, for some $a_i \in A$. When G is of order n, one may consider A to be a non-empty subset of $\{0, 1, \cdots, n-1\}$ and for the obvious reasons one assumes that $0 \notin A$. If G is the cyclic group $\mathbb{Z}/n\mathbb{Z}$ we denote $E_A(G)$ and $D_A(G)$ by $E_A(n)$ and $D_A(n)$ respectively.

S. D. Adhikari, C. David, J. Urroz (See [5]) considered the problem of determining values of $D_{R_n}(n)$ and $E_{R_n}(n)$, where $R_n = \{x^2 : x \in (\mathbb{Z}/n\mathbb{Z})^*\}$, where $(\mathbb{Z}/n\mathbb{Z})^*$ is group of units modulo n. The case $n = p$, a prime had already been dealt with by S. D. Adhikari and P. Rath in [7]. In this chapter we will be extending some results from [5].

In what follows, for a positive integer n, $\Omega(n)$ (resp. $\omega(n)$), denotes the number of prime factors of n counted with multiplicity (resp. without multiplicity).

We shall prove the following theorems.

Theorem 4.1.1. *Let $n = 3^\alpha$. Then we have*

(i) $D_{R_n}(n) = 2\Omega(n) + 1$, *and*

(ii) $E_{R_n}(n) = n + 2\Omega(n)$.

Theorem 4.1.2. *Let $n = 2^\alpha$, $\alpha \geq 3$. Then we have $D_{R_n}(n) \leq 7\Omega(n) + 1$ and $E_{R_n}(n) \leq n + 7\Omega(n)$.*

Theorem 4.1.3. *Let $n = 5^l \prod_{i=2}^{k} p_i^{\alpha_i}$, where $l, \alpha_i \geq 0$, primes $p_i \geq 7$, for each $i \in \{2, \cdots, k\}$. Let $m \geq 3\omega(n) + 1$ and $S = (x_1, x_2, \cdots, x_{m+2\Omega(n)+l})$ be a sequence of length $m + 2\Omega(n) + l$ of integers. Then there exists a subsequence $(x_{i_1}, x_{i_2}, \cdots, x_{i_m})$ and $a_1, a_2, \cdots, a_m \in R_n$ such that $\sum_{j=1}^{m} a_j x_{i_j} \equiv 0 \pmod{n}$. In particular,*

$$E_{R_n}(n) \leq n + 2\Omega(n) + l.$$

As a consequence of above theorem we have the following :

Remark 4.1.1. Let n be an integer such that $\gcd(30, n) = 1$ then combining Theorem 4.1.3 with Theorem 1 from [5] we get $E_{R_n}(n) = n + 2\Omega(n)$. Then using Theorem A (which will be stated in the next section) we get $D_{R_n}(n) = 2\Omega(n) + 1$.

4.2 Notations and Preliminaries

First, we shall recall some results stated in Section 1.5 and 1.6, which we shall be using in this chapter.

As conjectured in [7], a result similar to the result of Gao [35], the link between the constants $E_A(n)$ and $D_A(n)$ was established by Yuan and Zeng [79] :

Theorem A (Yuan and Zeng). *Let A be a finite non-empty subset of integers and n a positive integer. We have*

$$E_A(n) = D_A(n) + n - 1.$$

It should be remarked that the corresponding generalization of the above result for arbitrary finite abelian groups has been established by Grynkiewicz, Marchan and Ordaz [48].

We shall need following theorem due to I. Chowla (See [24] and [62]).

Theorem B. *Let n be a natural number, and let A and B be two non-empty subsets of $\mathbb{Z}/n\mathbb{Z}$, such that $0 \in B$ and $A + B \neq \mathbb{Z}/n\mathbb{Z}$. If $\gcd(x, n) = 1$ for all $x \in B \setminus \{0\}$ then $|A + B| \geq |A| + |B| - 1$.*

For a non-empty subset A of an abelian group G, the *stabilizer* of A, denoted by $Stab(A)$ is defined as follows,

$$Stab(A) = \{x \in G : x + A = A\}.$$

We shall also need the following generalization of Theorem B due to M. Kneser [52, 53, 54] (for the statement in the following form one may look in [62] or [45]).

Theorem C. *Let G be an abelian group, and let A and B be finite, non-empty subsets of G. Let $H = Stab(A + B)$. Then*

$$|A + B| \geq |A + H| + |B + H| - |H|.$$

From Theorem C, the following can be easily deduced.

Theorem D. *Let G be an abelian group, and let $A_1, A_2, \cdots, A_k$ be k finite, non-empty subsets of G. Let $H = Stab(A_1 + A_2 + \cdots + A_k)$. Then*

$$|A_1 + A_2 + \cdots + A_k| \geq |A_1 + H| + |A_2 + H| + \cdots + |A_k + H| - (k-1)|H|.$$

In what follows, for a positive integer n, we shall denote the set $\{1, 2, 3, \cdots, n\}$ by the symbol $[n]$.

If $n = p^a$, p an odd prime number and $a \in \mathbb{N}$ then $(\mathbb{Z}/n\mathbb{Z})^*$ is a (multiplicative) cyclic group (see [50]). Let x be a generator. Then clearly $R_n = \langle x^2 \rangle$. Hence $|R_n| = ord(x^2) = \phi(n)/2$.

If $n = 2^a$, $a \in \mathbb{N}$, $a \geq 3$, then $(\mathbb{Z}/n\mathbb{Z})^*$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{a-2}\mathbb{Z}$ (see [50]). Let x be a generator of $\mathbb{Z}/2^{a-2}\mathbb{Z}$. Then clearly $(0, 2x)$ is a generator of R_n. So $|R_n| = ord((0, 2x)) = 2^{a-3}$.

We will be using the following remark several times in this note.

Remark 4.2.1. Let $m, n \in \mathbb{N}$, with $m|n$. Let $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be a surjective ring homomorphism. Then $(\mathbb{Z}/m\mathbb{Z})^* = \phi((\mathbb{Z}/n\mathbb{Z})^*)$ and $R_m = \phi(R_n)$.

Above remark can be observed as follows.

Since ϕ is an abelian group homomorphism, it is completely determined by where it maps an additive generator, say identity 1_n. On the other hand, ϕ being a surjective

ring homomorphism it must take the multiplicative identity to the multiplicative identity. Thus we have $\phi(1_n) = 1_m$, where 1_m is the multiplicative identity of $\mathbb{Z}/m\mathbb{Z}$. Since $(\mathbb{Z}/n\mathbb{Z})^*$ is precisely the subset of all the generators of $\mathbb{Z}/n\mathbb{Z}$ (as an abelian group), we have $\phi((\mathbb{Z}/n\mathbb{Z})^*) \subset (\mathbb{Z}/m\mathbb{Z})^*$. Now it remains to show that for any $\alpha \cdot 1_m \in (\mathbb{Z}/m\mathbb{Z})^*$ there exists some $\beta \cdot 1_n \in (\mathbb{Z}/n\mathbb{Z})^*$ with $\alpha \cdot 1_m = \phi(\beta \cdot 1_n) = \beta \cdot 1_m$. This is equivalent to showing that, for any number $\alpha \in \mathbb{Z}$ that is relatively prime to m there must be some $\alpha + mx$, where $x \in \mathbb{Z}$, that is relatively prime to n. If the prime divisors of m and n are the same, then $\gcd(m, \alpha) = 1$, implies $\gcd(n, \alpha) = 1$, as needed. Let p be a prime divisor of n, not dividing m. If $\alpha + xm \equiv 0 \pmod{p}$, for all $x \in \mathbb{Z}$, then $\alpha + xm \equiv \alpha + (x+1)m \pmod{p}$, which implies $m \equiv 0 \pmod{p}$, contradicting that p does not divide m. Thus we can find $x \in \mathbb{Z}$ such that $\alpha + xm$ is not divisible by p. Iterating this procedure for remaining prime divisors of n but not m (replacing α by $\alpha + xm$ and m by pm each time) yields the integer with the needed properties. Thus $\phi((\mathbb{Z}/n\mathbb{Z})^*) = (\mathbb{Z}/m\mathbb{Z})^*$. Now one can easily observe that, $\phi(R_n) = R_m$.

4.3 Proof of our Theorems

Lemma 4.3.1. *Let $p \geq 7$ be any prime number and $n = p^\alpha$. Then, given $x_1,\ x_2,\ x_3 \in (\mathbb{Z}/n\mathbb{Z})^*$ we have,*

$$R_n x_1 + R_n x_2 + R_n x_3 = \mathbb{Z}/n\mathbb{Z}.$$

Proof. Let $H = Stab\ (R_n x_1 + R_n x_2 + R_n x_3)$. Clearly, the quotient group $(\mathbb{Z}/n\mathbb{Z})/H$ is cyclic, say $\mathbb{Z}/m\mathbb{Z}$, where $m = p^\beta,\ \beta \leq \alpha$. Consider $\phi : (\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z})$ to be the natural homomorphism with kernel H. Since $\phi(R_n) = R_m$, we have

$$\phi\left(\sum_{i=1}^{3} R_n x_i\right) = \sum_{i=1}^{3} R_m \phi(x_i).$$

Since H is the $Stab\ (R_nx_1 + R_nx_2 + R_nx_3)$ and $\phi : (\mathbb{Z}/n\mathbb{Z}) \to (\mathbb{Z}/m\mathbb{Z})$, we get $Stab\left(\sum_{i=1}^{3} R_m\phi(x_i)\right) = \{\phi(0)\}$.

Observe that, as each of the x_i's generate $\mathbb{Z}/n\mathbb{Z}$, we have $\langle\phi(x_i)\rangle = \mathbb{Z}/m\mathbb{Z}$, for each $i = 1, 2, 3$. Applying Kneser's theorem (Theorem D) we get,

$$\begin{aligned}\left|\sum_{i=1}^{3} R_m\phi(x_i)\right| &\geq 3|R_m| - 2\\ &= \frac{3(p^\beta - p^{\beta-1})}{2} - 2\\ &\geq p^\beta.\end{aligned}$$

Thus, $\sum_{i=1}^{3} R_{p^\beta}\phi(x_i) = \mathbb{Z}/p^\beta\mathbb{Z}$. Therefore, $Stab\ (\sum_{i=1}^{3} R_{p^\beta}\phi(x_i)) = \mathbb{Z}/p^\beta\mathbb{Z}$. Since $H = Stab\ (R_nx_1 + R_nx_2 + R_nx_3)$, we get $Stab\ (\phi(R_nx_1 + R_nx_2 + R_nx_3)) = \{0\}$. That is, $\mathbb{Z}/p^\beta\mathbb{Z} = \{0\}$. Therefore, $H = \mathbb{Z}/p^\alpha\mathbb{Z}$. Hence $R_nx_1 + R_nx_2 + R_nx_3 = \mathbb{Z}/n\mathbb{Z}$. □

The proof of the following lemma is similar to that of the above.

Lemma 4.3.2. *Let $n = 5^\alpha$. Given $x_1,\ x_2,\ x_3,\ x_4 \in (\mathbb{Z}/n\mathbb{Z})^*$, we have*

$$R_nx_1 + R_nx_2 + R_nx_3 + R_nx_4 = \mathbb{Z}/n\mathbb{Z}.$$

Proof of Theorem 4.1.1. In view of Theorem 1 of [5], for part (i) of the theorem we have only to prove that $D_{R_n}(n) \leq 2\Omega(n) + 1$.

Consider a sequence $x_1, x_2, \cdots, x_{2\Omega(n)+1}$ of elements of $(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$. Observe that there are three elements, say $x_1,\ x_2$ and x_3, such that $3^r||x_i$ for $i = 1, 2, 3$ and some $r \in \{0, 1, \cdots, \alpha - 1\}$. Put $y_i = x_i/3^r$. By repeated application of Theorem B of Chowla, we see that

$$
\begin{aligned}
&|(R_n y_1 + R_n y_2 \cup \{0\}) + R_n y_3 \cup \{0\}| \\
&\qquad \geq \min\{n, |R_n y_1 + R_n y_2 \cup \{0\}| + |R_n y_3 \cup \{0\}| - 1\} \\
&\qquad \geq \min\{n, \min\{n, 2|R_n|\} + |R_n y_3 \cup \{0\}| - 1\} \\
&\qquad = \min\{n, 3|R_n|\} \\
&\qquad = \min\left\{n, \frac{3(3^\alpha - 3^{\alpha-1})}{2}\right\} \\
&\qquad = n.
\end{aligned}
$$

Looking at the set $(R_n y_1 + R_n y_2 \cup \{0\}) + R_n y_3 \cup \{0\}$ and Theorem B of Chowla, one sees that the reason behind including 0 to $R_n y_2$ and $R_n y_3$ is just to get the setting in which we can apply Theorem B. Since y_2, y_3 are coprime to n, $0 \notin R_n y_2 \cup R_n y_3$. So including 0 increases the cardinality of both the sets $R_n y_2$ and $R_n y_3$ by 1.
From the above inequality, it follows that $0 \in (R_n y_1 + R_n y_2 \cup \{0\}) + R_n y_3 \cup \{0\}$. Hence, $D_{R_n}(n) \leq 2\Omega(n) + 1$, as desired. Part (ii) follows from part (i) and Theorem A. □

Proof of Theorem 4.1.2. Observe that by the structure of $(\mathbb{Z}/n\mathbb{Z})^*$ we get $|R_n| = 2^{\alpha-3}$. Observe that any sequence of length $7\Omega(n) + 1$ of elements of $(\mathbb{Z}/n\mathbb{Z}) \setminus \{0\}$ contains 8 terms such that k is the largest power of 2 dividing these 8 terms for some $k \in \{0, 1, 2, \cdots, \alpha - 1\}$. Now we get the result by arguments similar to that employed in the above theorem. □

Proof of Theorem 4.1.3. We shall prove the theorem by induction on $\Omega(n)$.

Suppose $\Omega(n) = 1$. Therefore, $n = p$, a prime.

First, suppose that $p = 5$. In this case, $m \geq 3(1) + 1 = 4$ and $S = (x_1, x_2, \cdots, x_{m+3})$. If there are at least four non-zero terms modulo 5 in the given sequence, then by Lemma 4.3.2 we shall get an R_n-weighted zero sum subsequence modulo 5 of length m. If the sequence does not have more than three non-zero terms modulo 5, then the sequence has at least m terms which are zero modulo 5 and so we are through.

Suppose $p \neq 5$. If the sequence contains at least three non-zero terms modulo p,

then by Lemma 4.3.1 we shall get an R_n-weighted zero sum subsequence modulo p of length m. Otherwise, at most two terms of the sequence are units modulo p which implies that at least m terms are divisible by p and we are through.

Thus the result is established for the case $\Omega(n) = 1$.

Now, assume that $\Omega(n) > 1$ and that the result holds for all N with $\Omega(N) < \Omega(n)$.

Case 1. Suppose there exists a prime divisor $p_t \neq 5$ of n such that number of terms in S which are coprime to p_t is at most 2. Let S_1 be the subsequence of S obtained by removing these terms. Clearly, the length of S_1 is at least $m + 2\Omega(n/p_t) + l$. Since $m \geq 3\omega(n/p_t)+1$, by the induction hypothesis, we get a subsequence $(x_{i_1}, x_{i_2}, \cdots, x_{i_m})$ of S_1 such that

$$\sum_{j=1}^{m} a_j \ \frac{x_{i_j}}{p_t} \equiv 0 \pmod{n/p_t}, \quad with \ \ a_j \in R_{n/p_t}.$$

Since n/p_t divides n by Remark 4.2.1, we can see that $\phi(R_n) = R_{n/p_t}$. In fact, map ϕ is just reducing an element of R_n modulo n/p_t. Therefore, for each $j \in \{1, 2, \cdots, m\}$, there exists $a'_j \in R_n$ such that $a'_j \equiv a_j \pmod{n/p_t}$. So

$$\sum_{j=1}^{m} a'_j \ \frac{x_{i_j}}{p_t} \equiv 0 \pmod{n/p_t}, \quad with \ \ a'_j \in R_n.$$

Therefore,

$$\sum_{j=1}^{m} a'_j x_{i_j} \equiv 0 \pmod{n}.$$

Case 2. Suppose the sequence contains at most three units modulo 5. Let S_1 be the sequence obtained by removing these terms from S. Clearly, the length of S_1 is at least $m + 2\Omega(n/5) + l - 1$. Since $m \geq 3\omega(n/5) + 1$, by applying the induction hypothesis, we get $\sum_{j=1}^{m} a_j \ \frac{x_{i_j}}{5} \equiv 0 \pmod{n/5}$, where $a_j \in R_{n/5}$. As in Case 1, using Remark 4.2.1, we get $b_j \in R_n$ such that $\sum_{j=1}^{m} b_j x_{i_j} \equiv 0 \pmod{n}$.

Case 3. Suppose the sequence contains at least four units modulo 5 and at least three units modulo p_t for each $t \in \{2, 3, \cdots, k\}$. Then by Lemma 4.3.1 and Lemma 4.3.2, we get a subsequence $(x_{i_1}, x_{i_2}, \cdots, x_{i_m})$ of S such that, $\sum_{j=1}^{m} a_j^{(1)} x_{i_j} \equiv 0 \pmod{5^l}$

and $\sum_{j=1}^{m} a_j^{(i)} x_{i_j} \equiv 0 \pmod{p_i^{\alpha_i}}$, for some $a_j^{(i)} \in R_{p_i^{\alpha_i}}$ and $a_j^{(1)} \in R_{5^l}$. Now the result follows by the Chinese Remainder Theorem. □

Bibliography

[1] S. D. Adhikari, *Aspects of combinatorics and combinatorial number theory,* Narosa Publishing House, New Delhi, 2002.

[2] S. D. Adhikari, S. Baier and P. Rath, *An extremal problem in lattice point combinatorics*, Diophantine equations, 19-32, Tata Inst. Fund. Res. Stud. Math., **20**, Tata Inst. Fund. Res., Mumbai, 2008.

[3] S. D. Adhikari and Y. G. Chen, *Davenport constant with weights and some related questions II*, J. Combin. Theory Ser. A **115** (2008), no. 1, 178-184.

[4] S. D. Adhikari, Y. G. Chen, J. B. Friedlander, S. V. Konyagin and F. Pappalardi, *Contributions to zero-sum problems*, Discrete Math., **306** (2006), no. 1, 1-10.

[5] S. D. Adhikari, C. David and J. Urroz, *Generalizations of Some Zero-Sum Theorems*, Integers, **8** (2008) Article A52.

[6] S. D. Adhikari and P. Rath, *Zero-sum problems in Combinatorial Number Theory*, The Riemann zeta function and related themes: papers in honour of Professor K. Ramachandra, 1-14, Ramanujan Math. Soc. Lect. Notes Ser., **2**, Ramanujan Math. Soc., Mysore, 2006.

[7] S.D. Adhikari and P. Rath, *Davenport Constant with weights and some related questions*, Integers, **6** (2006), Article A30.

[8] W. R. Alford, A. Granville and C. Pomerance, *There are infinitely many Carmichael numbers*, Annals of Math., **139** (2) (1994), no. 3, 703-722.

[9] N. Alon, A. Bialostocki and Y. Caro, *Extremal zero-sum problems*, manuscript.

[10] N. Alon and M. Dubiner, *A lattice point problem and additive number theory*, Combinatorica, **15** (1995), no. 3, 301-309.

[11] N. Alon and M. Dubiner, *Zero-sum sets of prescribed size*, Combinatorics, Paul Erdős is eighty (Volume **1**), Keszthely (Hungary), 33-50 (1993).

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

[13] R. C. Baker and W. Schmidt, *Diophantine problems in variables restricted to the values of* 0 *and* 1, J. Number Theory, **12** (1980), 460-486.

[14] R. Balasubramanian and G. Bhowmik, *Upper bounds for the Davenport constant*, Combinatorial number theory, 61-69, de Gruyter, Berlin, 2007.

[15] G. Bhowmik and J-C. Schlage-Puchta, *Davenport's constant for groups of the form* $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3d}$, Additive combinatorics, 307-326, CRM Proc. Lecture Notes, **43**, Amer. Math. Soc., Providence, RI, 2007.

[16] G. Bhowmik and J-C. Schlage-Puchta, *An Improvement on Olson's Constant for* $\mathbb{Z}_p \oplus \mathbb{Z}_p$, Acta Arith. **141** (2010), no. 4, 311-319.

[17] B. Bollobás and I. Leader, *The number of k-sums modulo k*, J. Number Theory, **78**, no. 1, 27–35 (1999).

[18] J. L. Brenner, *Problem 6298*, Amer. Math. Monthly, **89**, 279-280 (1982).

[19] Y. Caro, *Zero-sum subsequences in abelian non-cyclic groups*, Israel Journal of Mathematics, **92**, 221–233 (1995).

[20] A. L. Cauchy, *Recherches sur les nombres*, J. École polytech., **9**, 99-116 (1813).

[21] R. Chi, S. Ding, W. Gao, A. Geroldinger and W. A. Schmid, *On zero-sum subsequences of restricted size IV*, Acta Math. Hungar., **107(4)** (2005), 337-344.

[22] M. N. Chintamani, W. D. Gao, B. K. Moriya, P. Paul and R. Thangadurai, *On Davenport's constant,* Preprint.

[23] M. N. Chintamani and B. K. Moriya, *Generalizations of some Zero Sum Theorems,* Preprint.

[24] I. Chowla, *A Theorem on the Addition of Residue Classes: Application to the number F(k) in Waring's Problem*, Proc. Indian Acad. Sci. **2**, 242-243 (1935).

[25] H. Davenport, *On the addition of residue classes*, J. London Math. Soc., **10**, 30-32, (1935).

[26] J-M. Deshouillers and G. Prakash *Large zero free subsets of* $\mathbb{Z}/p\mathbb{Z}$, Preprint, 2009.

[27] G. T. Diderrich and H. B. Mann, *Combinatorial problems in finite Abelian groups. Survey of combinatorial theory*, (Proc. Internat. Sympos., Colorado State Univ., Fort Collins, Colo., 1971), 75-100. North-Holland, Amsterdam, 1973.

[28] V. Dimitrov, *Zero-sum problems in finite groups*, Research Science Institute Students Reports, 2003, The center for excellence in education, Vienna, pg. 9-18.

[29] Y. Edel, *Sequences in abelian groups G of odd order without zero-sum subsequences of length exp(G),* Des. Codes Cryptogr. **47** (2008), no. 1-3, 125-134.

[30] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin and L. Rackham, *Zero-sum problems in finite abelian groups and affine caps*, Q. J. Math., **58** (2007), no. 2, 159-186.

[31] C. Elsholtz, *Lower bounds for multidimensional zero sums*, Combinatorica, **24 (3)** (2004), 351-358.

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

[33] P. Erdős and H. Heilbronn, *On the addition of residue classes mod p*, Acta Arith., **9** (1964), 149-159.

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

[35] W. D. Gao, *A combinatorial problem on finite abelian groups,* J. Number Theory, **58**, (1996), 100-103.

[36] W. D. Gao, *On Davenport's constant of finite abelian groups with rank three*, Discrete Math., **222** (2000), no. 1-3, 111-124.

[37] W. D. Gao and A. Geroldinger, *Zero-sum problems and coverings by proper cosets*, European J. Combinatorics, **24** (2003), 531-549.

[38] W. D. Gao and A. Geroldinger, *On long minimal zero sequences in finite abelian groups*, Period. Math. Hungar., **38** (3) (1999), 179-211.

[39] W. D. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups; a survey*, Expo. Math., **24** (2006), no. 4, 337-369.

[40] W. D. Gao and A. Geroldinger, *On zero-sum sequences in* $\mathbb{Z}/n\mathbb{Z}\oplus\mathbb{Z}/n\mathbb{Z}$, Integers: Electronic Journal of Combinatorial Number Theory, **3**, #A8, 45 pp. (2003).

[41] W. D. Gao, Q. H. Hou, W. A. Schmid and R. Thangadurai, *On short zero-sum subsequences II*, Integers **7** (2007), A21, 22 pp.

[42] W. D. Gao, I. Z. Ruzsa and R. Thangadurai, *Olson's constant for the group* $\mathbb{Z}_p \oplus \mathbb{Z}_p$, J. Combin. Theory, Ser. A, **107** (2004), 49-67.

[43] W. D. Gao and R. Thangadurai, *On zero-sum sequences of prescribed length*, Aequationes Math., **72** (2006), no. 3, 201-212.

[44] W. D. Gao and Y. X. Yang, *Note on a combinatorial constant*, J. Math. Res. Exposition **17** (1997) 139-140.

[45] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Pure and Applied Mathematics (Boca Raton), **278**, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[46] A. Geroldinger and R. Schneider, *On Davenport's constant*, J. Combin. Theory, Ser. A, **61** (1992), no. 1, 147-152.

[47] S. Griffiths, *The Erdős-Ginzberg-Ziv theorem with units,* Discrete Math., **308** (2008), no. **23**, 5473-5484.

[48] D. J. Grynkiewicz, L. E. Marchan and O. Ordaz, *A Weighted generalization of Two Theorems of Gao*, Preprint.

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

[50] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, GTM, **84**, Springer-Verlag, New York-Berlin, 1982.

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

[52] M. Kneser, *Abschätzung der asymptotischen Dichte von Summenmengen,* Math. Z., **58**, (1953), 459-484.

[53] M. Kneser, *Summenmengen in lokalkompakten abelschen Gruppen,* (German) Math. Z., **66** (1956), 88-110.

[54] M. Kneser, *Ein Satz überabelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen,* (German) Math. Z., **61**, (1955). 429-434.

[55] F. Luca, *A generalization of a classical zero-sum problem,* Discrete Math., **307** (2007), no. 13, 1672-1678.

[56] H. B. Mann, *Addition theorems: The addition theorems of group theory and number theory*, Interscience Publishers John Wiley & Sons, New York-London-Sydney, 1965.

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

[58] H. B. Mann, *Addition Theorems in Group Theory and Number Theory*, R. E. Krieger Publishing Company, Huntington, New York, 1976.

[59] R. Meshulam, *An uncertainty inequality and zero subsums*, Discrete Math., **84** (1990), no. 2, 197-200.

[60] B. K. Moriya, *On Zero Sum subsequences of restricted size,* Proc. Indian Acad. Sci. (Math. Sci.) Vol. **120**, No. 4, September 2010, pp. 395-402.

[61] W. Narkiewicz and J. Śliwa, *Finite abelian groups and factorization problems II*, Colloq. Math., **46** (1982), 115-122.

[62] M. B. Nathanson, *Additive Number Theory : Inverse Problems and the Geometry of Sumsets*, GTM, Vol. **165**, Springer, New York, 1996.

[63] H. Nguyen, E. Szemerédi and V. H. Vu, *Subset sums modulo a prime*, Acta Arith, **131** (2008), no. 4, 303-316.

[64] J. E. Olson, *A combinatorial problem in finite abelian groups I*, J. Number Theory, **1** (1969), 8-10.

[65] J. E. Olson, *A combinatorial problem in finite abelian groups II*, J. Number Theory, **1** (1969), 195-199.

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

[67] J. E. Olson, *An addition theorem for finite abelian groups*, J. Number Theory, **9**, 63-70 (1977).

[68] O. Ordaz and D. Quiroz, *The Erdős-Ginzburg-Ziv theorem in abelian non-cyclic groups*, Divulg. Mat. **8** (2), 113-119 (2000).

[69] C. Pomerance, *A tale of two sieves,* Notices Amer. Math. Soc. **43** (1996), no. 12, 1473-1485.

[70] P. Rath, K. Srilakshmi and R. Thangadurai, *On Davenport's constant*, Int. J. Number Theory, **4** (2008), no. 1, 107-115.

[71] C. Reiher, *On Kemnitz' conjecture concerning lattice-points in the plane*, Ramanujan J., **13** (2007), no. 1-3, 333-337.

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

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

[74] B. Sury and R. Thangadurai, *Gao's conjecture on zero-sum sequences*, Proc. Indian Acad. Sci. (math. Sci.), **112** (3), 399-414 (2002).

[75] R. Thangadurai, *A variant of Davenport's constant,* Proc. Indian Acad. Sci. Math. Sci. **117** (2007), no. 2, 147-158.

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

[77] R. Thangadurai, *Interplay between four conjectures on certain zero-sum problems*, Expo. Math., **20**, no. 3, 215-228 (2002).

[78] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite abelian group III*, Z. W. 1969-008 (Math. Centrum, Amsterdam).

[79] P. Yuan and X. Zeng, *Davenport constant with weights*, European Journal of Combinatorics, **31** (2010), 677-680.