ON SOME PROBLEMS IN
ADDITIVE NUMBER THEORY

by

GYAN PRAKASH

A THESIS IN MATHEMATICS

Submitted to the Indian Statistical Institute in partial fulfillment of
the requirement for the degree of Doctor of Philosophy

OCTOBER 2005

THE INSTITUTE OF MATHEMATICAL SCIENCES
C.I.T. CAMPUS, THARAMANI
CHENNAI, TAMILNADU - 600 113, INDIA

Acknowledgment

I am indebted to my thesis supervisor Prof. R. Balasubramanian for his continuous encouragement and support.

I am grateful to Prof. S. D. Adhikari and Dr. D. Surya Ramana for their continuous encouragement and support. They also provided me their generous and extremely valuable help in the preparation of this thesis.

I thank the Director, Registrar, the staff of the administration and the library of The Institute of Mathematical Sciences, Chennai for their support and help during the period of my fellowship at that institute.

I am thankful to all the members of Harish-Chandra Research Institute, Allahabad for their support, during my frequent visits to that institute.

I express my gratitude to all my teachers of Indian Statistical Institute, Bangalore and Delhi centers for their encouragement, inspiration and excellent teaching during my post graduation. I am particularly thankful to Prof. Bhaskar Bagchi, Prof. Sunanda Bagchi, Prof. R. L. Karandikar, Prof. Gadadhar Mishra, Prof. P. L. Muthuramalingam, Prof. V. Pati, Prof. K. R. Parthasarthy, Prof. N. S. N. Sastry, Prof. K. B. Sinha, Prof. Cherian Verghese, and many others.

I have been blessed with many friends, who have been of help to me in every aspect of my life and in particular to this thesis. I am particularly grateful to Anirban-Chandi, Arijeet, Binu, Bobby, Golam, Indra, Jishnu, Kamil-Farzana, Madhu, Meenakshi, Maneesh, Nabeen Tiwari, Naru, Naveen, Shami-Paramita, Sreedhar, Srinivas-Jyoti, Srini-Padma, Suri-Aarti, Suresh, M. Rajesh, V. Rajesh, Ravindra-Sumithra, Ritumoni, Thanga-Anandi, Vibhu and Vinu.

To my teacher Dr. Arshad Majeed who not only taught me my basic mathematics but also has been always encouraging and inspiring. To Bagchi Sir, Sunanda Madam, Tintin and Tomtom for their affection. To my wife Janhavi, who joined me at the crucial phase of this thesis work and has been always supportive and understanding. To my father, Ram Swarup, for his support and affection.

Abstract

In this thesis we discuss some problems relating the properties of a set A and those of $A + A$, when A is a subset of an abelian group.

Given a finite abelian group G and $A \subset G$, we say A is **sum-free** if the sets $2A$ and A are disjoint.

In chapter 2 we discuss the problem of finding the structure of all large sum-free subsets of G. We obtain the **complete structure** of all **largest** sum-free subsets of G, provided all the divisors of order of G are congruent to 1 modulo 3. In the same chapter we also give **partial** results regarding structure of all large **maximal** sum-free subsets of G. We say a sum-free set A is maximal if it is not a proper subset of any sum-free set. If there is a divisor of order of G which is not congruent to 1 modulo 3 then structure of all largest sum-free subsets of G was known before. Our results are based on a recent result of Ben Green and Imre Ruzsa [GR05].

Let $SF(G)$ denote the set of all sum-free subsets of G and the symbol $\sigma(G)$ denotes the number $n^{-1}(\log_2 |SF(G)|)$. In chapter 3 we improve the **error term** in asymptotic formula of $\sigma(G)$ obtained by Ben Green and Imre Ruzsa [GR05]. The method used is a slight refinement of methods in [GR05].

In chapter 4 we discuss the following problem. Let A be an infinite subset of natural numbers. Suppose for all large natural numbers n the number of ways n can be written as a sum of two element (not necessarily distinct) of A is not equal to 1, then how "**thin**" can A be? The main result of this chapter is then an improvement of a result of Nicolas, Ruzsa, Sárközy [NRS98] and methods we use are refinement of methods developed in [NRS98]. A new ingredient used is an additive lemma proven by means of graph theory.

Contents

Chapter 1

Introduction

The theme of this thesis is the relation between the properties of a set A and those of the set $A + A$, when A is a subset of an abelian group G.

Throughout chapters 2 and 3, G will denote a *finite* abelian group of order n and exponent m. In these chapters we discuss some questions related to *sum-free* subsets of G. We say that a set $A \subset G$ is *sum-free* if the sets A and $A+A$ are disjoint. In other words, $A \subset G$ is sum-free if there is no triplet $(x, y, z) \in A \times A \times A$ with $x + y = z$.

We will presently describe the results of Chapter 2. To this end, we define the density of a subset B of G to be $\frac{|B|}{|G|}$ and denote it by $\alpha(B)$; write $\mu(G)$ to denote the density of a largest sum-free subset of G.

The fundamental observation on sum-free subsets of an abelian group is that the inverse image of a sum-free subset under a homomorphism is also sum-free. Moreover, if the homomorphism is surjective, then density of a sum-free subset and that of its inverse image are the same. In particular, if f is a surjective homomorphism from G onto $\mathbb{Z}/d\mathbb{Z}$, for some integer $d \geq 1$ and if B is a sum-free subset of $\mathbb{Z}/d\mathbb{Z}$ then $f^{-1}(B)$ is a sum-free subset of G and $\alpha\left(f^{-1}(B)\right) = \alpha(B)$. For any integer $d \geq 1$, the set B_d comprising all integers in the interval $(\frac{d}{3}, \frac{2d}{3})$ under the canonical homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}/d\mathbb{Z}$ is a sum-free subset of $\mathbb{Z}/d\mathbb{Z}$. The density of $B_d = \frac{[\frac{d-2}{3}]+1}{d}$. Consequently, for any finite abelian group G of exponent m, we have

$$\mu(G) \geq max_{d|m} \frac{[\frac{d-2}{3}]+1}{d}. \tag{1.1}$$

It is known that this inequality is equality for all finite abelian groups. More precisely, we have

Theorem 1.0.1. *([GR05]) Let G be a finite abelian group and m denote the exponent of G. Then*

$$\mu(G) = max_{d|m} \frac{[\frac{d-2}{3}]+1}{d}$$

This theorem was proven by Ben Green and Ruzsa [GR05] for groups G which are of type III. We say G is of type III if every divisor of the order of G is congruent to 1 modulo 3. For all other groups the above theorem was already obtained by P.H. Diananda and H. P. Yap [DY69]. Notice that, if G is of type III then it follows from above theorem that $\mu(G) = \frac{1}{3} - \frac{1}{3m}$.

The examples of sum-free sets given above and value of $\mu(G)$ suggest the following question regarding the structure of all large sum-free subsets of G.

Question 1.0.2. Given a "large" sum-free subset A of G does there exist a surjective homomorphism $f : G \to \mathbb{Z}/d\mathbb{Z}$, a sum-free set $B \subset \mathbb{Z}/d\mathbb{Z}$ such that A is a subset of $f^{-1}(B)$?

Notice that if the answer of above question is in the affirmative, then trivially Theorem 1.0.1 holds. The answer to this question is known to be in the affirmative when G is *not* of type III ([GR05], [oHP04]) and A is a *largest* sum-free set. *We determine the structure of all largest sum-free subsets of all groups G of type* III. When G is of type III, 2 does not divide the order of G. Thus every divisor d of m is congruent to 1 modulo 6 and $\frac{d-1}{6}$ is a non-negative integer. When G is of type III, Ben Green and Ruzsa [GR05] proved the following result.

Theorem 1.0.3. *([GR05]) Let A be a sum-free subset of an abelian group G of type III. Let $\eta = 2^{-23}$. Suppose that $\alpha(A) \geq \mu(G) - \eta$, then there exists a surjective homomorphism $\gamma : G \to \mathbb{Z}/q\mathbb{Z}$ with $q \neq 1$ such that the following holds.*

$$A \subset \gamma^{-1} p_q(\{l + j : 1 \leq j \leq 4l\}),$$

where $l = \frac{q-1}{6}$ and $p_q : \mathbb{Z} \to \mathbb{Z}/q\mathbb{Z}$ is the natural projection.

Let I_l denote the set $p_q(\{l+j : 1 \leq j \leq 4l\})$, where $l = \frac{q-1}{6}$. Let H_l, T_l denote the sets $p_q(\{l+j : 1 \leq j \leq l\})$ and $p_q(\{4l+j : 1 \leq j \leq l\})$ respectively. In case $q = m$ the symbols I, H, T denote the sets I_l, H_l, T_l respectively. Following the terminology of [GR05] we call γ the *special direction* of the set A and q the *order* of γ.

We say a sum-free set is *maximal* if it is not a proper subset of any sum-free set. In Chapter 2 we improve upon Theorem 1.0.3 and prove the following theorem.

Theorem 1.0.4. *Let G be a finite abelian group of type III. Let A be a sum-free subset of an abelian group G. Let n denote the order of G and m denote the exponent of G. Let $k = \frac{m-1}{6}$ and $\eta = 2^{-23}$. Suppose that $\alpha(A) > \mu(G) - min(\eta, \frac{5}{42m})$. Then there exists a surjective homomorphism*

$$f : G \to \mathbb{Z}/m\mathbb{Z}$$

such that the following holds.

$$A \subset f^{-1}p(\{2k+j : 0 \leq j \leq 2k+1\}),$$

where $p : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is the natural projection. In case A is a maximal sum-free set, then the following also holds.

$$f^{-1}p(\{2k+j : 2 \leq j \leq 2k-1\}) \subset A$$

Notice that $p(\{2k+j : 1 \leq j \leq 2k\})$ is a largest sum-free subset of $\mathbb{Z}/m\mathbb{Z}$. Let C denote the set $p(\{2k+j : 0 \leq j \leq 2k+1\}) \subset \mathbb{Z}/m\mathbb{Z}$. Then C is not sum-free. Therefore Theorem 1.0.4 does not answer Question 1.0.2 affirmatively. In fact we shall show that the answer of Question 1.0.2 is negative for all abelian groups G which are not cyclic and of type III. While the set C is not sum-free, it is "almost" sum-free and the triplets $(x, y, z) \subset C^3$ with $x+y = z$ are only $(p(2k), p(2k), p(4k))$, $(p(2k), p(2k+1), p(4k+1))$, $(p(4k), p(4k+1), p(2k))$, $(p(4k+1), p(4k+1), p(2k+1))$. The homomorphism f as required by Theorem 1.0.4 may be taken either γ or 2γ, where γ is a homomorphism as given by Theorem 1.0.3. The main result of chapter 2 isTheorem 1.0.4. Using this result we easily obtain the *complete structure of all largest sum-free subsets of all finite abelian groups G of type* III.

We now summarise the method of proof of Theorem 1.0.4. Indeed, we first verify

Theorem 1.0.4 when $G = \mathbb{Z}/m\mathbb{Z}$ and classify all largest sum-free subsets of $\mathbb{Z}/m\mathbb{Z}$. The proof of Theorem 1.0.4 is achieved by reducing the problem to classification of all largest sum-free subsets of $\mathbb{Z}/m\mathbb{Z}$. To each A as in Theorem 1.0.4 we associate a set $L \subset \mathbb{Z}/m\mathbb{Z}$ which we show is a largest sum-free subset of $\mathbb{Z}/m\mathbb{Z}$. The structure of L is determined by classification of all largest sum-free subsets of $\mathbb{Z}/m\mathbb{Z}$. Then Theorem 1.0.4 follows from relation between the properties of A and those of L.

We describe association of set $L \subset \mathbb{Z}/m\mathbb{Z}$ to a given "large" sum-free set $A \subset G$ and relation between properties of L and that of A. Let γ be the special direction of the set A, A_i denote the set $A \cap \gamma^{-1}\{i\}$ and $\alpha_i = \frac{q}{n}|A_i|$ where $i \in \mathbb{Z}/q\mathbb{Z}$. An idea that we repeatedly use from [GR05] is that for any $i, j \in \mathbb{Z}/q\mathbb{Z}$, the sets $A_i + A_j$ and A_{i+j} are disjoint. This is an easy consequence of the fact that A is sum-free and is very useful. This in particular implies that $\alpha_i + \alpha_{2i} \leq 1$. An *important property of set I_l we use is that it may be divided into $2l$ disjoint pairs* of the form $(i, 2i)$ with $i \in H_l \cup T_l$. This was exploited in [GR05] to prove Theorem 1.0.1 and also plays very important role in our proof of Theorem 1.0.4. For example, using this we immediately deduce that $\alpha(A) = \frac{1}{q}\sum_{i\in\mathbb{Z}/q\mathbb{Z}}\alpha_i = \frac{1}{q}\sum_{i\in H_l\cup T_l}(\alpha_i + \alpha_{2i}) \leq \frac{2l}{q}$. This implies Theorem 1.0.1 for groups of type III. It also implies that if density of A is "large" then *order of γ is same as the exponent* of G; that is $q = m$. To each A we *associate* the subset L of $\mathbb{Z}/m\mathbb{Z}$ comprising those $i \in \mathbb{Z}/m\mathbb{Z}$ such that $\alpha_i > \frac{1}{2}$. It is then easy to show that L is sum-free. In fact, for every $i, j \in L$ it follows that $A_i + A_j = \gamma^{-1}\{i + j\}$ and hence $\alpha_{i+j} = 0$. This is the *relation* between L and A which we use to prove Theorem 1.0.4. To determine the *cardinality* of L we show that for every $i_0 \in H \cup T$, exactly one of the element of the pair $(i_0, 2i_0)$ belong to L. We use the following argument. In case density of A is $\mu(G)$ then it follows easily that for every $i_0 \in H \cup T$ we have $\alpha_{i_0} + \alpha_{2i_0} = 1$. Since the order of G is odd, therefore for any $i \in \mathbb{Z}/m\mathbb{Z}$ we have that $\alpha_i \neq \frac{1}{2}$. Thus, in case density of A is $\mu(G)$, it follows that the cardinality of L is $2k$, where $k = \frac{m-1}{6}$. Using Kneser's theorem we show that the same conclusion holds for any sum-free set A with $\alpha(A) > \mu(G) - \frac{5}{42m}$.

We also exploit the properties of I frequently in classifying all largest sum-free subsets of $\mathbb{Z}/m\mathbb{Z}$. Let E be a largest sum-free subset of $\mathbb{Z}/m\mathbb{Z}$; that is cardinality of E is $2k$, where $k = \frac{m-1}{6}$. Further if we assume that $E \subset I$, then for any $i_0 \in H \cup T$, exactly one of the element of pair $(i_0, 2i_0)$ belong to E. Using this it follows easily that $E \cap H$ is an arithmetic progression. The same conclusion holds for $E \cap T$. After some calculations we determine that either $E = H \cup T$ or that E is a subset of C, where C is the subset of $\mathbb{Z}/m\mathbb{Z}$ as defined above. Using this the structure of L is obtained and the proof of Theorem 1.0.4 is completed.

In chapter 3 we consider the problem of counting the number of sum-free subsets of G. Let $SF(G)$ denote the set of all sum-free subsets of G and $\sigma(G)$ denote the number $n^{-1}(\log_2 |SF(G)|)$. We prove the following result.

Theorem 1.0.5. *Let G be a finite abelian group of order n. Then we have the following asymptotic formula.*

$$\sigma(G) = \mu(G) + O(\frac{1}{(\ln n)^{1/27}}).$$

Definition 1.0.6. Given a set $B \subset G$ we say that $(x, y, z) \in B^3$ is a Schur triple of the set B if $x + y = z$.

Theorem 1.0.5 follows immediately from the following result and results of [GR05].

Theorem 1.0.7. *There exist an absolute positive constant δ_0 such that if $F \subset G$ as at-most δn^2 Schur triples, where $\delta \leq \delta_0$. Then*

$$|F| \leq (\mu(G) + C\delta^{1/3})n \tag{1.2}$$

where C is an absolute positive constant.

The methods used are refinement of methods of [GR05] and an improvement of the following results of Ben Green and Imre Ruzsa [GR05].

Theorem 1.0.8. *([GR05], Theorem 1.8.) Let G be a finite abelian group of order n. Then we have the following asymptotic formula.*

$$\sigma(G) = \mu(G) + O(\frac{1}{(\ln n)^{1/2}}).$$

Theorem 1.0.9. *([GR05], Proposition 2.2) Let G be an abelian group, and suppose that $F \subseteq G$ has at-most δn^2 Schur triples. Then*

$$|F| \leq (\mu(G) + 2^{20}\delta^{1/5})n$$

Theorem 1.0.7 was proven in [GR05] if G is not of type III. More precisely,

Theorem 1.0.10. *([GR05], Corollary 4.3.) Let G be an abelian group, and suppose that $F \subseteq G$ has at-most δn^2 Schur triples. Then*

$$|F| \leq (max(\frac{1}{3}, \mu(G) + 3\delta^{1/3})n \tag{1.3}$$

In case G is not of type III then $\mu(G) \geq \frac{1}{3}$. Therefore Theorem 1.0.10 implies Theorem 1.0.7 immediately. In case G is of type III but exponent m of G is large, then too Theorem 1.0.7 follows.

We presently summarise the method used to prove Theorem 1.0.7. Given any F as in Theorem 1.0.9, Green and Ruzsa find a homomorphism $\gamma : G \to \mathbb{Z}/q\mathbb{Z}$ where $q \neq 1$ and such that for any $i \notin I_l$, cardinality of set $F \cap \gamma^{-1}\{i\}$ is extremely "small". Here I_l is a subset of $\mathbb{Z}/q\mathbb{Z}$ as defined above just after the statement of Theorem 1.0.3. Then the upper bound of $\sum_{i\in I_l} |A \cap \gamma^{-1}\{i\}|$ is obtained in [GR05] to prove Theorem 1.0.9. We use a refinement of arguments in [GR05] to improve upper bound of $\sum_{i\in I_l} |F \cap \gamma^{-1}\{i\}|$ and obtain Theorem 1.0.7.

We describe the method to estimate $\sum_{i\in I_l} |F \cap \gamma^{-1}\{i\}|$. Let F_i denote the set $F \cap \gamma^{-1}\{i\}$. Observe that $\sum_{i\in I_l} |F \cap \gamma^{-1}\{i\}| = \sum_{i\in H_l \cup T_l}(|F_i| + |F_{2i}|)$. Here H_l and T_l are subsets of $\mathbb{Z}/q\mathbb{Z}$ as defined above. Also observe that given any $x \in F_i$ and an element $z \in (x+F_i) \cap F_{2i}$ we have a Schur triplet (x, y, z) of set F. Now in case $|F_i|+|F_{2i}| \geq \frac{n}{q}(1+t)$, then cardinality of $(x + F_i) \cap F_{2i}$ is at-least $t\frac{n}{q}$ and we get at-least $\frac{n}{q}t|F_i|$ Schur triples of F. Also $|F_i| + |F_{2i}| \geq \frac{n}{q}(1 + t)$ trivially implies that cardinality of F_i is at-least $t\frac{n}{q}$. Therefore it follows that for any $i \in \mathbb{Z}/q\mathbb{Z}$ we have $|F_i| + |F_{2i}| \leq \frac{n}{q}(1 + (\delta)^{1/2}q)$ and $\sum_{i\in H_l \cup T_l}(|F_i| + |F_{2i}|) \leq \frac{n}{q}2l(1 + (\delta)^{1/2}q) \leq n(\mu(G) + (\delta)^{1/2}q)$. This bound was proven in [GR05] to prove Theorem 1.0.9. We improve this bound by observing that given any $t > 0$ if we consider the set $L(t) = \{i \in H_l \cup T_l : |F_i| + |F_{2i}| \geq \frac{n}{q}(1 + t)\}$, then for any $i \in L(t)$, there are at-least $\frac{n}{q}t|F_i|$ Schur triplets $(x, y, z) \subset F^3$ with $x \in F_i$. This follows from what we discussed above. The sets F_i and F_j are disjoint unless $i = j$. Therefore we get $\sum_{i\in L(t)} |F_i| \leq \frac{nq\delta}{t}$. This in turn implies that $\sum_{i\in I_l} |F_i| \leq \frac{n}{q}\left(|L(t)| + \frac{q^2\delta}{t} + (2l - |L(t)|)(1 + t)\right)$. Then choosing $t = (\delta q)^{1/2}$ we get that $\sum_{i\in I_l} |F_i| \leq n(\mu(G) + 2\delta^{1/2}q^{1/2})$.

Though the results of Chapter 2 and Chapter 3 are related to sum-free sets, these chapters can be read independently. There are some common definitions which are used in both chapters. However for the convenience of the reader, we repeat these definitions. Apart from these definitions, only the value of $\mu(G)$ is required in both chapters.

In Chapter 4, we discuss the following problem. In this chapter we set $G = \mathbb{Z}$ and A an infinite subset of $\mathbb{N}$, where $\mathbb{N}$ denote the set of all natural numbers. If A is an infinite subset of $\mathbb{N}$ then we set

$$A(x) = \{a \leq x : a \in A\}.$$

Let $r(A, n)$ denote the number of solutions of the equation

$$n = a_i + a_j, \quad \text{where } a_i \leq a_j, \quad a_i, a_j \in A.$$

Nicolas, Ruzsa, Sárközy [NRS98] asked if $r(A, n)$ is even for all sufficiently large natural numbers then what can be said about $|A(X)|$ as $X \to \infty$. They proved the following result.

Theorem 1.0.11. *[NRS98] If A is an infinite subset of $\mathbb{N}$ such that $r(A, n) \neq 1$ for all sufficiently large natural numbers n, then*

$$\limsup |A(x)| \left(\frac{\ln \ln x}{\ln x}\right)^{3/2} \geq \frac{1}{20}.$$

They also gave an example of a set A such that $r(A, n) \neq 1$ for all sufficiently large natural numbers n and $|A(x)| \ll (\ln x)^2$. We show the following:

Theorem 1.0.12. *There exists an absolute constant $c > 0$ with the following property: for any infinite subset A of $\mathbb{N}$ such that $r(A, n) \neq 1$ for all sufficiently large natural numbers n, we have*

$$|A(x)| \geq c \left(\frac{\ln x}{\ln \ln x}\right)^2 \text{ for all } x \text{ sufficiently large.}$$

Notice that the condition $r(A, n) \neq 1$ is much weaker condition than the condition $r(A, n)$ is even. Therefore, one will expect that one should be able to improve the above results considerably under the assumption $r(A, n)$ is even for all sufficiently large natural numbers. However no such result is known. There has been lot of progress in case $r(A, n)$ is replaced by $p(A, n)$ where $p(A, n)$ is the number of partition of n into parts from A.

The methods we use to prove Theorem 1.0.12 are refinements of methods used in [NRS98] to prove Theorem 1.0.11. Given a sufficiently large Y we may assume that $|A(Y)| \leq (\ln Y)^2$. Since otherwise the conclusion of Theorem 1.0.12 holds trivially. We show under this additional assumption, the number of elements of A contained in the interval $[b, b(\ln Y)^{11}) \subset (\sqrt{Y}, Y)$ is at-least $c\frac{\ln Y}{\ln\ln Y}$, where b is a real number and c is a positive absolute constant. Then Theorem 1.0.12 follows by noting that if Y is sufficiently large then for some positive absolute constant c the interval $[\sqrt{Y}, Y)$ contains at-least $c\frac{\ln Y}{\ln\ln Y}$ disjoint intervals of the form $[b, b(\ln Y)^{11})$.

Using ideas from [NRS98] we construct a sequence B_Y of elements of A not exceeding $\sqrt{Y}$ satisfying certain special properties. Moreover the number of terms in sequence B_Y is at-least $c\frac{\ln Y}{\ln\ln Y}$. We choose $a \in [b, b(\ln Y)^{10}) \cap A$ such that the interval $(a - b, a)$ does not contain any element of the set A. Let S denote the set of elements of A in the interval $[b, b(\in Y)^{11})$ and s denote the cardinality of S. Let S_1 and S_2 denote the sets of elements of A in the intervals $[b, a)$ and $[a, b(\ln Y)^{11})$ respectively and let s_1 and s_2 denote the cardinalities of S_1 and S_2 respectively. We then have $s = s_1 + s_2$. For each term $b_i \in B_Y$ let $n_i = a + b_i$. From the assumption that $r(A, n) \neq 1$ for all sufficiently large natural numbers, it follows that for each $b_i \in B_Y$ there are pairs (c_i, d_i) with $d_i \geq c_i$, of elements of A distinct from the pair (a, b_i) such that $n_i = c_i + d_i$. Let P_1 denote the set of those pairs (c_i, d_i) with $d_i < a$ and P_2 the set of those pairs (c_i, d_i) with $d_i > a$. Let p_1 and p_2 denote the cardinalities of P_1 and P_2 respectively. We then have $p_1 + p_2 = |B_Y|$. It is easy to see that $d_i \leq b(\in Y)^{11}$. It was shown in [NRS98] that the mapping ϕ that associates (c_i, d_i) to d_i maps P_2 into S_2 and is injective. Therefore we have that $s_2 \geq p_2$. It was also shown in [NRS98] that $P_1 \subset S_1 \times S_1$. From this it follows that $s_1 \geq p_1^{1/2}$. We show that $s_1 \geq cp_1$. For this we associate a graph G to P_1. The edges of G are in one-one correspondence with elements of P_1 and number of vertices of G is at-most $2s_1$. We observe another property of the sequence B_Y and show that G does not have any even closed trail. We show that number of edges in a graph G not having any even closed trail is at-most cn , where n is number of vertices of G. This shows that $s_1 \geq cp_1$. Therefore, $s = s_1 + s_2 \geq c(p_1 + p_2) \geq c\frac{\ln Y}{\ln\ln Y}$.

Theorem 1.0.12 is the main result in [BP04].

Chapter 2

Large Sum-free sets in abelian group

2.1 Introduction and statements of result

Throughout this chapter G will denote a finite abelian group of order n. If A is a subset of G then we say that A is sum-free if the equation $x + y = z$ has no solution with $(x, y, z) \in A \times A \times A$. We say that A is maximal sum-free if it is not a proper subset of any sum-free set. In this chapter we shall discuss the following question:

Question 2.1.1. Find a "*structure*" of all "*large*" maximal sum-free subsets of G.

In this regard we prove Theorem 2.1.10, Theorem 2.1.12 and Theorem 2.1.13. The results are based on Theorem 2.1.14 which is a recent result of Ben Green and Imre Ruzsa [GR05]. Our results give complete structure of all largest sum-free subsets of all finite abelian groups G, in case any divisor of order of G is congruent to 1 modulo 3.

Before stating our results and previously known results related to the above question, we shall explain what do we mean by "*large*" and what sort of '*structure*" does one may expect?

To understand the meaning of *large* in the above question, we need to understand the following question.

Question 2.1.2. What is the cardinality of a largest sum-free subset of G ?

Definition 2.1.3. (i) Given any finite abelian group K and a set $A \subset K$, we define the density of the set A to be $\frac{|A|}{|K|}$ and denote it by $\alpha(A)$.

(ii) We use $\mu(G)$ to denote the density of a largest sum-free subset of G.

We say a sum-free set $A \subset G$ is large if the density of the set A is close to $\mu(G)$; that is $\mu(G) - \alpha(A)$ is "*small*".
The value of $\mu(G)$ is now known for any finite abelian group G [GR05].

Theorem 2.1.4. ([GR05], Theorem 2) *Let G be a finite abelian group and m be its exponent. Then the value of $\mu(G)$ is given by the following formula.*

$$\mu(G) = max_{d|m} \frac{\left[\frac{d-2}{3}\right] + 1}{d}$$

The following facts are straightforward to check.

(i) For any positive integer d, we have the natural projection $p_d : \mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$. Let the set $B_d \subset \mathbb{Z}/d\mathbb{Z}$ be the image of integers in the interval $(\frac{d}{3}, \frac{2d}{3}]$ under the map p_d. Then it is straightforward to check that B_d is sum-free and density of the set B_d is given by
$$\alpha(B_d) = \frac{\left[\frac{d-2}{3}\right] + 1}{d}.$$

(ii) For any positive integer d, there is a surjective homomorphism $f : G \to \mathbb{Z}/d\mathbb{Z}$ if and only if d divides the exponent of the group G.

(iii) For any positive integer d and a surjective homomorphism $f : G \to \mathbb{Z}/d\mathbb{Z}$, the set $A = f^{-1}(B_d)$ is a sum-free subset of G and $\alpha(A) = \alpha(B_d)$.

Therefore, the following result follows.

Theorem 2.1.5. *([GR05]) Given any finite abelian group G, there exists a sum-free set $A \subset G$, a surjective homomorphism $f : G \to \mathbb{Z}/d\mathbb{Z}$ (where d is a positive integer), a sum-free set $B \subset \mathbb{Z}/d\mathbb{Z}$; such that the following hold.*

(i) $A = f^{-1}(B)$.

(ii) *The density of A is $\mu(G)$.*

Now, regarding the structure of *large* sum-free subsets of G we may ask the following question.

Question 2.1.6. Let A be a "large" sum-free subset of G. Then given any such set A, does there always exist a surjective homomorphism $f : G \to \mathbb{Z}/d\mathbb{Z}$ (where d is some positive integer) and a sum-free set $B \subset \mathbb{Z}/d\mathbb{Z}$, such that the set A is a subset of the set $f^{-1}(B)$?

Before discussing this question we describe the value of $\mu(G)$ more explicitly by dividing the finite abelian groups in the following three classes.

Definition 2.1.7. Suppose that G is a finite abelian group of order n.

(i) If n is divisible by any prime $p \equiv 2 (\text{mod } 3)$ then we say that G is type I. We say that G is type I(p) if it is type I and if p is the *least* prime factor of n of the form $3l + 2$. In this case the value of $\mu(G)$ is equal to $\frac{1}{3} + \frac{1}{3p}$.

(ii) If n is not divisible by any prime $p \equiv 2 (\text{mod } 3)$, but $3|n$, then we say that G is type II. In this case the value of $\mu(G)$ is equal to $\frac{1}{3}$.

(iii) The group G is said to be of type III if all the divisor of n (order of G) are congruent to 1 modulo 3. Let m be the exponent of G. In this case the value of $\mu(G)$ is equal to $\frac{1}{3} - \frac{1}{3m}$. We also note the fact that if G is a group of type III then any subgroup as well as quotient of G is also a type III group.

Remark 2.1.8. We note the fact that if G is a type III group and d is any divisor of m, then d is odd and congruent to 1 modulo 3. Therefore, d is congruent to 1 modulo 6 and $\frac{d-1}{6}$ is a non negative integer.

Theorem 2.1.4 was proven for type I and type II groups by Diananda and Yap [DY69]. For some special cases of type III groups it was proven by various authors (see [Yap72, Yap75, RS74]). For an arbitrary abelian groups of type III the proof of Theorem 2.1.4 is due to Ben Green and Ruzsa [GR05].

Hamidoune and Plagne [oHP04] answered the Question 2.1.6 affirmatively when

$|A| \geq \frac{|G|}{3}$, in the case $|G|$ is odd. In case $|G|$ is even they answered the Question 2.1.6 affirmatively if $|A| \geq \frac{|G|+1}{3}$. In case $G = (\mathbb{Z}/2\mathbb{Z})^r$ with $r \geq 4$ and $|A| \geq 5.2^{r-4}$ then Davydov and Tombak [DT89] showed that answer of this question is affirmative. Recently Lev [Lev05] answered this question affirmatively in the case when $G = (\mathbb{Z}/3\mathbb{Z})^r$ (with an integer $r \geq 3$) and $|A| > \frac{5}{27}3^r$. Lev [Lev] has also characterised the sum-free subsets A of $\mathbb{Z}/p\mathbb{Z}$ when p is prime and $|A| > 0.33p$.

Notice that none of the above mentioned results tells us anything related to the Question 2.1.6, in case G is a finite abelian group of type III and G is not cyclic. In case G is cyclic the answer of Question 2.1.6 is obviously affirmative. In case G is not cyclic and of type III, Theorem 2.1.10 shows that the answer of Question 2.1.6 is negative.

For the rest of this chapter unless specified differently, G shall denote a finite abelian group of type III and of order n. The symbol m shall denote the exponent of G and $k = \frac{m-1}{6}$.

Remark 2.1.9. If G is an abelian group of type III and m is exponent of G, there exist $S \subset G$ and $C \subset G$ such that S and C are subgroups of G, C is isomorphic to $\mathbb{Z}/m\mathbb{Z}$ and $G = S \oplus C$. In case G is not cyclic, S will be a nontrivial subgroup of G.

Let $p : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the natural projection from the group of integers to $\mathbb{Z}/m\mathbb{Z}$.

Theorem 2.1.10. *Let G be a finite abelian group of type III. Let m denote the exponent of G and $k = \frac{m-1}{6}$. Suppose G is not a cyclic group and S, C are nontrivial subgroups of G such that $G = S \oplus C$, and C is isomorphic to $\mathbb{Z}/m\mathbb{Z}$. Let $g : C \to \mathbb{Z}/mZ$ be an isomorphism. Let J be any proper subgroup of S and b is any element belonging to S. Then consider the following two examples:*

(i) *The set $A = ((J + b) \oplus g^{-1}p(\{2k\})) \cup (S \oplus g^{-1}p(\{2k + j : 1 \leq j \leq 2k - 1\}) \cup ((J + 2b)^c \oplus g^{-1}p(\{4k\}))$. (Here for any set $D \subset S$ the symbol D^c denotes the set $S \setminus D$.)*

(ii) *The set $A = ((J+b) \oplus g^{-1}p(\{2k\})) \cup ((J-2b)^c \oplus g^{-1}p(\{2k+1\}) \cup (S \oplus g^{-1}p(\{2k+j : 2 \leq j \leq 2k - 1\})) \cup ((J + 2b)^c \oplus g^{-1}p(\{4k\})) \cup ((J - b) \oplus g^{-1}p(\{4k + 1\}))$.*

Let A be any of the set as above. Then the following holds.

(i) *The set A is a sum-free subset of G and $\alpha(A) = \mu(G)$.*

(ii) *For any positive integer d, there does not exist any surjective homomorphism $f : G \to \mathbb{Z}/dZ$, a sum-free set $B \subset Z/d\mathbb{Z}$, such that the set A is a subset of the set $f^{-1}(B)$.*

We got to know the above examples from certain remarks made in [GR05] about the group $(\mathbb{Z}/7\mathbb{Z})^r$.

We prove that if G is a type III group and A is a sum-free subset of G of largest possible cardinality then either A is an inverse image of a sum-free subset of a cyclic quotient of G or A is one of the set as given in Theorem 2.1.10.

Definition 2.1.11. Given a sum-free set $A \subset G$, a surjective homomorphism $h : G \to \mathbb{Z}/dZ$ the following definition and notations are useful.

(i) For any $i \in \mathbb{Z}/d\mathbb{Z}$ the symbol $A(h, i)$ denote the set $A \cap h^{-1}\{i\}$.

(ii) For any $i \in \mathbb{Z}/d\mathbb{Z}$ we define $\alpha(h, i) = \frac{d}{n}|A(h, i)|$.

(iii) Let $l = \frac{d-1}{6}$ and $p_d : \mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ be the natural projection. The sets $H_d, T_d, M_d, I_d \subset \mathbb{Z}/d\mathbb{Z}$ denote the following sets.

$$\begin{aligned} H_d &= p_d\{l + j : 1 \leq j \leq l\} \\ M_d &= p_d\{2l + j : 1 \leq j \leq 2l\} \\ T_d &= p_d\{4l + j : 1 \leq j \leq l\} \\ I_d &= p_d\{l + j : 1 \leq j \leq 4l\} \end{aligned}$$

(iv) The symbol H, T, M, I denote the sets H_m, T_m, M_m, I_m respectively. The symbol p denotes the map p_m.

Theorem 2.1.12. *Let G be a finite abelian group of type III. Let A be a sum-free subset of an abelian group G. Let n denote the order of G and m denote the exponent of G. Let $k = \frac{m-1}{6}$ and $\eta = 2^{-23}$. Suppose that $\alpha(A) > \mu(G) - min(\eta, \frac{1}{9m})$. Then there exists a surjective homomorphism*

$$f : G \to \mathbb{Z}/m\mathbb{Z}$$

such that the following holds.

$$A \subset f^{-1}p(\{2k+j : 0 \leq j \leq 2k+1\}). \tag{2.1}$$

Further the following also holds.

(i) *For all* $i \in p(\{2k+j : 2 \leq j \leq 2k-1\})$ *the inequality* $\alpha(f,i) \geq 1 - m\,(\mu(G) - \alpha(A))$ *holds.*

(ii) $\alpha(f,2k) + \alpha(f,4k) \geq 1 - m\,(\mu(G) - \alpha(A))$.

(iii) $\alpha(f,4k+1) + \alpha(f,2k+1) \geq 1 - m\,(\mu(G) - \alpha(A))$

(iv) *If* A *is maximal then*

$$f^{-1}p(\{2k+j : 2 \leq j \leq 2k-1\}) \subset A$$

Using Theorem 2.1.12 the following theorem follows easily.

Theorem 2.1.13. *Let* A *be a sum-free subset of an abelian group* G *of type III. Let the symbol* m *denote the exponent of* G *and* $k = \frac{m-1}{6}$. *Let the density of the set* A *be equal to* $\mu(G)$ *and* $f : G \to \mathbb{Z}/m\mathbb{Z}$ *be a surjective homomorphism as given by Theorem 2.1.12. Let the set* S *denote the kernel of* f *and* C *be a subgroup of* G *such that* $G = S \oplus C$. *Let* $g : C \to \mathbb{Z}/m\mathbb{Z}$ *be an isomorphism obtained by restricting* f *to the subgroup* C. *Then there exist* J *a subgroup of* S *and* $b \in S$ *such that one of the following holds:*

(i) *The set* $A = f^{-1}p\,(\{2k+j : 1 \leq j \leq 2k\})$.

(ii) *One of the set* A *or* $-A$ *is equal to the following set*

$$\big((J+b) \oplus g^{-1}p(\{2k\})\big) \cup \big(f^{-1}p(\{2k+j : 1 \leq j \leq 2k-1\})\big) \cup ((J+2b)^c \oplus g^{-1}\{4k\}).$$

(Here and in the following for any set $D \subset S$ *the symbol* D^c *denotes the set* $S \setminus D$.*)*

(iii) *The set* A *is union of the sets* $f^{-1}p(\{2k+j : 2 \leq j \leq 2k-1\})$,

$$(J+b) \oplus g^{-1}p\{2k\}, \qquad (J+2b)^c \oplus g^{-1}p\{4k\},$$
$$(J-b) \oplus g^{-1}p\{4k+1\}, \qquad (J-2b)^c \oplus g^{-1}p\{2k+1\}.$$

The proof of Theorem 2.1.12 is based on the following result of Ben Green and Ruzsa [GR05].

Theorem 2.1.14. *([GR05], Proposition 7.2.) Let A be a sum-free subset of an abelian group G of type III. Let $\eta = 2^{-23}$. Suppose that $\alpha(A) \geq \mu(G) - \eta$, then there exists a surjective homomorphism $\gamma : G \to \mathbb{Z}/q\mathbb{Z}$ with $q \neq 1$ such that the following holds.*

$$A \subset \gamma^{-1} I_q.$$

We require the following definitions and notations.

Definition 2.1.15. Let A be a sum-free subset of G and $\alpha(A) \geq \mu(G) - \eta$, then we choose a γ a surjective homomorphism from Z to $\mathbb{Z}/q\mathbb{Z}$ with $q \neq 1$ and $A \subset \gamma^{-1} I_q$. Following the terminology of [GR05] we call γ the special direction of the set A and q the order of special direction. We use the symbols α_i and A_i to denote the number $\alpha(\gamma, i)$ and the set $A(\gamma, i)$ respectively. We use symbol S to denote the set $ker(\gamma)$ and S_i to denote $\gamma^{-1}\{i\}$.

Remark 2.1.16. Notice that in case $G = (\mathbb{Z}/7\mathbb{Z})^r$, Theorem 2.1.14 is equivalent to Theorem 2.1.12, as in this special case $l + 1 = 2l$.

2.2 Plan of the proof

Let $H(A)$ be the largest subset of G such that $H(A) + A = A$. The set $H(A)$ as defined is called period or stabiliser of the set A. For any set A as in Theorem 2.1.10 we prove that $H(A) = J$ where J is as in Theorem 2.1.10. Using this Theorem 2.1.10 is easy to prove.

Let A be as in Theorem 2.1.12 and γ be the special direction of A. The main difficulty in proving Theorem 2.1.12 is to prove the existence of a homomorphism f such that (2.1) holds. For this we show the following.

(i) The order of the special direction of A is m.

(ii) We define the set $L = \{i \in \mathbb{Z}/m\mathbb{Z} : \alpha_i > \frac{1}{2}\}$. We show that for any $i, j \in L$, $\alpha_{i+j=0}$. In particular the set L is a sum-free subset of $\mathbb{Z}/m\mathbb{Z}$. Moreover, the cardinality of L is $2k = 2\frac{m-1}{6}$; that is L is a largest sum-free subset of $\mathbb{Z}/m\mathbb{Z}$.

(iii) We describe all the largest sum-free subset of $\mathbb{Z}/m\mathbb{Z}$ which are subsets of I. Using Theorem 2.1.14 this characterises all the largest sum-free subsets of $\mathbb{Z}/m\mathbb{Z}$. This determines the structure of L and the proof of Theorem 2.1.12 is completed.

There are two facts which we use repeatedly. One is that for any $i, j \in Z/q\mathbb{Z}$ the sets $A(\gamma, i) + A(\gamma, j)$ and $A(\gamma, i + j)$ are disjoint. Another is that for any divisor d of m, the set I_d is divided into $2\frac{d-1}{6}$ disjoint pairs of the form $(i, 2i)$ with i belonging to the set $H_d \cup M_d$.

2.3 Stabiliser of largest sum-free subset

In this section we shall give the proof of Theorem 2.1.10. Any abelian group acts on itself by translation. Given any set $B \subset G$ we define the set $H(B)$ to be those elements of the group G such that the set B is stable under the translation by the elements of the set $H(B)$. In other words, the set $H(B) = \{g \in G : g + B = B\}$. For any set B the set $H(B)$ is a subgroup.

Let G be an abelian group of type III and let $A \subset G$ be as in Theorem 2.1.10. To prove Theorem 2.1.10 we shall prove the following

Lemma 2.3.1. *Let S and C be as in Theorem 2.1.10 and $\pi_C : G \to G/S = C$ be the natural projection. Then the set $\pi_C(H(A)) = \{0\}$.*

Proof. Since π_C is a homomorphism and $H(A)$ is a subgroup of G, the set $\pi_C(H(A))$ is a subgroup of M. Since $H(A) + A = A$ by the definition of $H(A)$, it follows that $\pi_C(H(A))+\pi_C(A) = \pi_C(A)$. Therefore, the set $\pi_C(A)$ is a union of cosets of $\pi_C\,(H(A))$. Therefore, the cardinality of the subgroup $\pi_C(H(A))$ divides the cardinality of the set $\pi_C(A)$. Since the set $\pi_C(H(A))$ is a subgroup of C, it is also true that $|\pi_C(H(A))|$ divides m. This implies that $|\pi_C(H(A))|$ divides $gcd(|\pi_C(A)|, m)$. Now if A is a set as in Theorem 2.1.10 (i) then the cardinality of the set $\pi_C(A)$ is equal to $2k + 1$ and if A is a set as in Theorem 2.1.10 (ii) then the cardinality of the set $\pi_C(A)$ is equal to $2k + 2$. Since $m = 6k + 1$ it follows that in first case the number $gcd(|\pi_C(A)|, m)$ divides 2 and in the second case it divides 5. But as G is type III group, any divisor of m which is not equal to 1 is greater than or equal to 7. Hence $gcd(|\pi_C(A)|, m) = 1$

for any of the set A as in Theorem 2.1.10. This forces $|\pi_C(H(A))| = 1$ and hence the lemma follows. □

Proposition 2.3.2. *Let A be any of the set as in Theorem 2.1.10 and S be a subgroup of G, J be a proper subgroup of S as in Theorem 2.1.10. Then the stabiliser of the set A is equal to the set J.*

Proof. Using the previous lemma it follows that $H(A) + ((J + b) \oplus g^{-1}\{2k\}) = (J + b) \oplus g^{-1}\{2k\}$. This implies that $H(A) + J + b = J + b$. This implies that $H(A) \subset J$. But it is straightforward to check that $J + A = A$. Therefore, it follows that $J = H(A)$, proving the claim. □

Proof. of Theorem 2.1.10:

(i) This is straightforward to check.

(ii) Suppose A is one of a set as in Theorem 2.1.10. Suppose the claim is not true for this set. Then there exist a positive integer q, a surjective homomorphism $f : G \to \mathbb{Z}/q\mathbb{Z}$, a sum-free set $B \subset \mathbb{Z}/q\mathbb{Z}$ such that the set A is a subset of $f^{-1}(B)$. Since from (i), the set A is a sum-free set of largest possible cardinality, it follows that the set $A = f^{-1}(B)$. Therefore, the kernel of f is a subset of $H(A)$. Therefore, we have the following inequality

$$|H(A)| \geq \frac{n}{q}. \tag{2.2}$$

But from Proposition 2.3.2 the stabiliser of the set A is J which is a proper subgroup of S. Since m is the exponent of G it follows that q is less than or equal to m. Therefore, we have the following inequality

$$|H(A)| < |S| = \frac{n}{m} \leq \frac{n}{q} \tag{2.3}$$

This contradiction proves the claim.

□

2.4 Order of the special direction

Let A be a sum-free subset of G and $\alpha(A) > min(\eta, \frac{5}{42m})$. Let γ be the special direction of the set A as given by Theorem 2.1.14. In this section, we shall show that the order of γ is equal to m. The proof of this result is inherent in [GR05]. We reproduce the proof here for the sake of completeness.

Lemma 2.4.1. *([GR05], Lemma 7.3. (ii)) Let A be a sum-free subset of the group G. Let g be any surjective homomorphism $g : G \to \mathbb{Z}/d\mathbb{Z}$, where d is a positive integer. Then for any $i \in \mathbb{Z}/d\mathbb{Z}$, the following inequality holds.*

$$\alpha(g, i) + \alpha(g, 2i) \leq 1 \tag{2.4}$$

Here $\alpha(g, i)$ is a number as defined in section 2.1.

Proof. For any $i \in \mathbb{Z}/d\mathbb{Z}$, let the set $A(g, i)$ be as defined in section 2.1. The fact that g is a homomorphism implies that the set $A(g, i)+A(g, i)$ is a subset of the set $g^{-1}\{2i\}$. The fact that the set A is sum-free implies that the set $A(g, i) + A(g, i)$ is disjoint from the set $A(g, 2i)$. Therefore, we have the following inequality.

$$|A(g, i) + A(g, i)| + |A(g, 2i)| \leq |g^{-1}\{2i\}| \tag{2.5}$$

The claim follows by observing that the set $A(g, i) + A(g, i)$ has cardinality at least $|A(g, i)|$. $\square$

The following lemma is straightforward to check, but is very useful.

Lemma 2.4.2. *Let d be a positive integer congruent to 1 modulo 6. Let $d = 6l+1$. Let the set I_d, H_d, M_d, T_d are subsets of the group $\mathbb{Z}/d\mathbb{Z}$ as defined in section 2.1. The set I_d is divided into $2l$ disjoint pairs of the form $(i, 2i)$ where i belongs to the set $H_d \cup T_d$ and $2i$ belongs to the set M_d.*

Proposition 2.4.3. *Let A be a sum-free subset of an abelian group G, of type III. Let m be the exponent of G and $\alpha(A) > min(\eta, \frac{5}{42m})$. Let $\gamma : G \to \mathbb{Z}/q\mathbb{Z}$ be the special direction of the set as given by Theorem 2.1.14. Then the order of $\gamma = q = m$.*

Proof. Since G is type III group, therefore any prime divisor of the order of G is greater than or equal to 7. Therefore, if q is not equal to m, then

$$q \leq \frac{m}{7}.$$

Using Theorem 2.1.14 we have the following equality for the density of the set A.

$$\alpha(A) = \frac{1}{q}\sum_{i\in\mathbb{Z}/q\mathbb{Z}} \alpha_i = \frac{1}{q}\sum_{i\in I_q} \alpha_i$$

Now, from Lemma 2.4.2, it follows that

$$\alpha(A) = \frac{1}{q}\sum_{i\in H_q\cup M_q} (\alpha_i + \alpha_{2i}) \leq \frac{1}{q}\sum_{i\in H_q\cup M_q} 1.$$

Since the cardinality of the set $H_q \cup M_q$ is equal to $\frac{q-1}{3}$, it follows that

$$\alpha(A) \leq \frac{1}{q}\frac{q-1}{3} \leq \frac{1}{3} - \frac{7}{3m}.$$

But the last inequality above is contrary to assumption that

$$\alpha(A) > \mu(G) - \frac{5}{42m} > \frac{1}{3} - \frac{7}{3m}.$$

Hence the lemma follows. $\square$

2.5 Element with large fibre

Given a set $A \subset G$ such that $\alpha(A) \geq \mu(G) - min(\eta, \frac{5}{42m})$, from Theorem 2.1.14 and Proposition 2.4.3 it follows that γ is a surjective homomorphism from G to $\mathbb{Z}/m\mathbb{Z}$ such that A is a subset of the set $\gamma^{-1}(I)$, where γ is the special direction of the set A and I is a subset of $\mathbb{Z}/m\mathbb{Z}$ as defined in section 2.1. Then we define $L \subset \mathbb{Z}/m\mathbb{Z}$ as follows.

$$L = \{i \in \mathbb{Z}/m\mathbb{Z} : \alpha_i > \frac{1}{2}\}$$

We say that the fibre of an element $i \in \mathbb{Z}/m\mathbb{Z}$ is large if i belong to the set L. It is clear that L is a subset of the set I. In this section, we shall show that the set L is a sum-free subset $\mathbb{Z}/m\mathbb{Z}$ and the cardinality of the set L is $2k$, where k is equal to $\frac{m-1}{6}$.

The fact that the set L is sum-free is a consequence of the following folklore in additive number theory. We give a proof of the following lemma for the sake of completeness.

Lemma 2.5.1. *(folklore) Let C and B be subsets of a finite abelian group K such that $min(|C|, |B|) > \frac{1}{2}|K|$. Then $C + B = K$.*

Proof. Suppose there exist $x \in K$ such that x does not belong to $C+B$. This is clearly equivalent to the fact that $C \cap (x-B) = \phi$. But this means that $|K| > |C|+|x-B| > |K|$. This is not possible. Hence the lemma is true. □

Lemma 2.5.2. *For any two elements $i, j \in L$, we have $\alpha_{i+j} = \alpha_{i-j} = 0$. In particular the set L is sum-free.*

Proof. The fact that γ is a homomorphism implies that the set $A_i + A_j$ is a subset of the set S_{i+j}. Take any $x \in S_i, y \in S_j$. Let $C = A_i - x$ and $B = A_j - y$ so that we have the sets C and B are subsets of group S. Then applying Lemma 2.5.1 it follows that $C + B = S$. Therefore, we have $A_i + A_j = S_{i+j}$. The fact that A is sum-free implies that $A_{i+j} \cap (A_i + A_j) = \phi$. Since we have shown that the set $A_i + A_j = S_{i+j}$, it follows that the set $A_{i+j} = \phi$. In other words it follows that $\alpha_{i+j} = 0$. From similar arguments it also follows that $\alpha_{i-j} = 0$. □

Now we shall show that the cardinality of the set L is equal to $2k$. For this we require the following Lemma.

Lemma 2.5.3. *Let A, G, be as in theorem 2.1.12. Let m be the exponent of the group G and I, H, T, M are the subsets of $\mathbb{Z}/m\mathbb{Z}$ as defined in section 2.1. Let $m = 6k+1$. Let g be a surjective homomorphism $g : G \to \mathbb{Z}/m\mathbb{Z}$ such that the following holds.*

$$A \subset g^{-1}(I).$$

Then we have the following inequality

$$\alpha(g,i) + \alpha(g,2i) \geq 1 - m(\mu(G) - \alpha(A)), \quad \forall i \in H \cup T. \tag{2.6}$$

Proof. From the assumption on the homomorphism g it follows that the density of the set A satisfy the following equality

$$\alpha(A) = \frac{1}{m} \sum_{i \in I} \alpha(g,i)$$

Now from Lemma 2.4.2, it follows that the set I is divided into $2k$ disjoint pairs of the form $(i, 2i)$ where i belongs to the set $H \cup T$. Therefore, it follows that

$$\alpha(A) = \frac{1}{m} \sum_{i \in I} \alpha(g,i) = \frac{1}{m} \sum_{i \in H \cup T} (\alpha(g,i) + \alpha(g,2i)).$$

Now using Lemma 2.4.1 it follows that for any $i_0 \in H \cup T$ the following inequality holds

$$m\alpha(A) \leq 2k - 1 + \alpha(g, i_0) + \alpha(g, 2i_0).$$

From this the required inequality follows for any i_0 belonging to the set $H \cup T$ after observing that $\mu(G) = \frac{2k}{m}$. $\square$

We need the following well known theorem due to Kneser.

Theorem 2.5.4. *(Kneser) Let C, B be subsets of a finite abelian group K such that $|C + B| < |C| + |B|$. Let $F = H(C + B) = \{g \in G : g + C + B = C + B\}$ be the stabiliser of the set $C + B$. Then the following holds*

$$|C + B| = |C + F| + |B + F| - |F|.$$

In particular the set F is a nontrivial subgroup of K and

$$|F| \geq |C| + |B| - |C + B|. \tag{2.7}$$

For the proof of this theorem one may see [Nat91].

Lemma 2.5.5. *Let A, G, be as in theorem 2.1.12, γ be as provided by Theorem 2.1.14 and H, T, M be as defined earlier. Then the following holds*

(i) *For any $i \in H \cup T$ if $\alpha_i \leq \frac{1}{2}$ then $\alpha_{2i} > \frac{1}{2}$.*

(ii) *The cardinality of the set L is equal to $2k$.*

Proof. (i) Suppose the claim is not true. Then there exist $i_0 \in H \cup T$ such that

$$\alpha_{i_0} \leq \frac{1}{2} \tag{2.8}$$
$$\alpha_{2i_0} \leq \frac{1}{2}. \tag{2.9}$$

Then from (2.6) it follows that

$$\alpha_{i_0} > \frac{1}{2} - \frac{5}{42} \tag{2.10}$$
$$\alpha_{2i_0} > \frac{1}{2} - \frac{5}{42}. \tag{2.11}$$

Take any $x \in S_{i_0}$ and consider the set $A_{i_0} - x$. Then invoking (2.5) and using (2.11), it follows that

$$|(A_{i_0} - x) + (A_{i_0} - x)| = |A_{i_0} + A_{i_0}| \leq |S| - |A_{2i_0}| < (\frac{1}{2} + \frac{5}{42})|S| \qquad (2.12)$$

Therefore, using (2.10) it follows that

$$2|A_{i_0} - x| = 2|A_{i_0}| > 2(\frac{1}{2} - \frac{5}{42})|S| > |(A_{i_0} - x) + (A_{i_0} - x)| \qquad (2.13)$$

Let F denote the stabiliser of the set $(A_{i_0} - x) + (A_{i_0} - x)$. We can apply Theorem 2.5.4 with $C = B = A_{i_0} - x$ and using (2.7), (2.12), (2.13) we have the following inequality

$$|F| > \left(\frac{1}{2} - \frac{15}{42}\right)|S| = \frac{1}{7}|S|. \qquad (2.14)$$

Therefore, the cardinality of the group S/F is strictly less than 7. But since S is a group of type III, the group S/F is also of type III. Hence it follows that $S = F$. Therefore, the stabiliser of the set $A_{i_0} - x$ is equal to the group S. This implies that the set $A_{i_0} = S_{i_0}$. This is in contradiction to the assumption that $\alpha_{i_0} \leq \frac{1}{2}$. Hence the claim follows.

(ii) The set I is divided into $2k$ disjoint pairs of the form $(i, 2i)$ with $i \in H \cup T$. From (i) it follows that at-least one element of any such pair belongs to the set L. The claim follows since we have shown that the set L is sum-free and is a subset of the set I.

□

From Lemma 2.5.2 and Lemma 2.5.5 the following proposition follows

Proposition 2.5.6. (i) *The set L is a sum-free subset of $\mathbb{Z}/m\mathbb{Z}$ of cardinality $2k$. The set L is a subset of the set I.*

(ii) *For any two elements $i, j \in L$, we have $\alpha_{i+j} = \alpha_{i-j} = 0$.*

2.6 Sum-free subset of cyclic group

Let the group $\mathbb{Z}/m\mathbb{Z}$ be of type III group and $m = 6k + 1$. In this section we shall characterise all the sets $E \subset \mathbb{Z}/m\mathbb{Z}$ such that the set E is sum-free and $|E| = 2k$. From

Theorem 2.1.14 it is sufficient to characterise those sets E which are subset of the set I.

Lemma 2.6.1. *Let $E \subset \mathbb{Z}/m\mathbb{Z}$ be a sum-free set. Let the group $\mathbb{Z}/m\mathbb{Z}$ be of type III and the cardinality of the set E be $2k$, where k is equal to $\frac{m-1}{6}$. Let H, T, M, I be subsets of $\mathbb{Z}/m\mathbb{Z}$ as defined in section 2.1 and the set E is a subset of the set I. Then for any element y belonging to the set M exactly one of the element of the pair $(\frac{y}{2}, y)$ belongs to the set E.*

Proof. This is straightforward from the fact that the set I is divided into $2k$ disjoint pairs of the form $(\frac{y}{2}, y)$ with y belonging to the set M and the assumption that the set E is a sum-free set and a subset of the set I. □

We have the natural projection p from the set of integers to $\mathbb{Z}/m\mathbb{Z}$.

$$p : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$$

Since the restriction of map p to the set $\{0, 1, 2, \cdots, m-2, m-1\} \subset \mathbb{Z}$ is a bijection to the group $\mathbb{Z}/m\mathbb{Z}$ (as a map of the sets) we can define

$$p^{-1} : \mathbb{Z}/m\mathbb{Z} \to \{0, 1, 2, \cdots m-1\}$$

in an obvious way.
The following lemma is straightforward to check.

Lemma 2.6.2. (i) *The set H is equal to the set $-T$.*

(ii) *The set M is equal to the set $-M$.*

(iii) *The set I is equal to the set $-I$.*

(iv) *For any set $B \subset \mathbb{Z}/m\mathbb{Z}$ the set $B \cap T$ is same as the set $-((-B) \cap H)$. Also the set $p^{-1}(B \cap T) = m - p^{-1}((-B) \cap H)$.*

(v) *The set $H + H$ as well as the set $T + T$ are subsets of the set M.*

(vi) *Given any even element y belonging to the set $p^{-1}(M)$ the element $\frac{p(y)}{2}$ belong to the set H. Also the element $p^{-1}(\frac{p(y)}{2})$ is equal to the element $\frac{y}{2}$.*

(vii) *Given any odd element y belonging to the set $p^{-1}(M)$ the element $\frac{p(y)}{2}$ belong to the set T. Also the element $p^{-1}(\frac{p(y)}{2})$ is equal to the element $\frac{y+6k+1}{2}$.*

(viii) *Given any two elements x, y belonging to the set $\in p^{-1}(H)$ which are of same parity, the element $p^{-1}(\frac{p(x+y)}{2}) = \frac{x+y}{2}$ and the element $\frac{x+y}{2}$ belongs to the set $p^{-1}(H)$. Moreover if x is strictly less than y then the following inequality holds.*

$$x < \frac{x+y}{2} < y$$

Lemma 2.6.3. *Let E be a set as above. Then the following holds.*

(i) *Given any two elements x, y which belong to the set $p^{-1}(E \cap H)$ and are of same parity, the element $\frac{x+y}{2}$ belong to the set $p^{-1}(E \cap H)$.*

(ii) *Given any two elements x, y which belong to the set $p^{-1}(E \cap H)$ and are of different parity, the element $\frac{x+y+6k+1}{2}$ belong to the set $p^{-1}(E \cap T)$.*

(iii) *Given an element x belonging to the set $p^{-1}(E \cap H)$ and an element y belonging to the set $p^{-1}(E \cap T)$, the element $\frac{p(x)-p(y)}{2}$ belong to the set $p^{-1}(E \cap (H \cup T))$.*

(iv) *Any two consecutive element of the set $p^{-1}(E \cap H)$ (or of the set $p^{-1}(E \cap T)$)are of different parity.*

Proof. Since the set E is sum-free, it follows that given any two elements x, y belonging to the set $p^{-1}(E)$, neither the element $p(x) + p(y)$ nor the element $p(x) - p(y)$ belong to the set E. Using this we prove all the claims.

(i) Under the assumption, the element $p(x) + p(y)$ belong to the set M. From Lemma 2.6.1 it follows that the element $\frac{p(x) + p(y)}{2}$ belong to the set E. Also the element $p^{-1}(p(x) + p(y))$ is equal to $x + y$ and is even. Therefore, invoking Lemma 2.6.2 it follows that the element $p^{-1}\left(\frac{p(x) + p(y)}{2}\right)$ is equal to $\frac{x+y}{2}$ and belong to the set $p^{-1}(H)$. Hence the claim follows.

(ii) Under the assumption, the element $p(x) + p(y)$ belong to the set M. From Lemma 2.6.1 it follows that the element $\frac{p(x) + p(y)}{2}$ belong to the set E. In this case the element $p^{-1}p(x+y)$ is equal to the element $x+y$ and is odd. Therefore, invoking Lemma 2.6.2 it follows that the element $p^{-1}\left(\frac{p(x) + p(y)}{2}\right)$ is equal to the element $\frac{x+y+6k+1}{2}$ and belongs to the set $p^{-1}(T)$. Hence the claim follows.

(iii) Under the assumption, the element $p(x) - p(y)$ belong to the set M. Therefore, the claim follows invoking Lemma 2.6.1.

(iv) Let the set $p^{-1}(E\cap H) = \{x_1 < x_2 < \cdots < x_h\}$. Suppose there exist $1 \leq i_0 \leq h-1$ such that the element x_{i_0} and the element x_{i_0+1} have same parity. Then from (i) it follows that the element $\frac{x_{i_0}+x_{i_0+1}}{2}$ belong to the set $p^{-1}(E\cap H)$. From Lemma 2.6.2 the following inequality also follows.

$$x_{i_o} < \frac{x_{i_o}+x_{i_o+1}}{2} < x_{i_o+1}$$

But this contradicts the fact that the elements x_{i_o} and x_{i_o+1} are consecutive elements of the set $p^{-1}(E\cap H)$. Therefore, the claim follows for the set $p^{-1}(E\cap H)$. Replacing the set E by the set $-E$, it follows that any two consecutive element of the set $p^{-1}((-E)\cap H)$ are also of different parity. Noticing that the set $p^{-1}(E\cap T) = m - p^{-1}((-E)\cap H)$, the claim follows for the set $p^{-1}(E\cap T)$ also.

□

Proposition 2.6.4. *Let E be a set as above then the following holds.*

(i) *The set $p^{-1}(E\cap H)$ as well as the set $p^{-1}(E\cap T)$ is an arithmetic progression with an odd common difference.*

(ii) *The following inequality holds.*

$$|E\cap T| - 1 \leq |E\cap H| \leq |E\cap T| + 1 \tag{2.15}$$

Proof. Let the set $p^{-1}(E\cap H) = \{x_1 < x_2 < \cdots < x_h\}$.

(i) In case the cardinality of the set $E\cap H$ is less than or equal to 2, the claim is trivial for the set $p^{-1}(E\cap H)$. Otherwise for any $1 \leq i \leq h-2$, consider the elements x_i, x_{i+1}, x_{i+2}, then from Lemma 2.6.3 it follows that the parity of elements x_i and x_{i+1} are different. For the same reason the parity of elements x_{i+1} and x_{i+2} are different. Therefore, the parity of elements x_i and x_{i+2} are same. Therefore, from Lemma 2.6.3 it follows that the element $\frac{x_i+x_{i+2}}{2}$ belong to the set $p^{-1}(E\cap H)$. But from Lemma 2.6.2 the following inequality follows.

$$x_i < \frac{x_i+x_{i+2}}{2} < x_{i+1}$$

Hence it follows that for any $1 \leq i \leq h-2$

$$\frac{x_i+x_{i+2}}{2} = x_{i+1}.$$

This is equivalent to the fact that the set $p^{-1}(E \cap H)$ is an arithmetic progression. It also follows that the common difference is odd. The claim for the set $p^{-1}(E \cap T)$ follows by replacing the set E by the set $-E$.

(ii) From Lemma 2.6.3 it follows that the set

$$\{\frac{x_1 + x_2 + 6k + 1}{2} < \frac{x_2 + x_3 + 6k + 1}{2} < \cdots < \frac{x_{h-1} + x_h + 6k + 1}{2}\} \subset p^{-1}(E \cap T). \tag{2.16}$$

Therefore, it follows that

$$|E \cap T| \geq |E \cap H| - 1.$$

Replacing the set E by the set $-E$, it also follows that

$$|E \cap H| \geq |E \cap T| - 1.$$

Hence the claim follows.

□

2.6.1 $max(|E \cap H|, |E \cap T|) \geq 2$

Proposition 2.6.5. *Let E be a set as above and H, T, M as defined above.*

(i) *Suppose the inequality $min(|E \cap H|, |E \cap T|) \geq 2$ is satisfied. Then the set $p^{-1}(E \cap H)$ and the set $E \cap T$ are arithmetic progression with same common difference $d(H, E) = d(T, E) = d(E)($ say $)$.*

(ii) *Suppose the inequality $min(|E \cap H|, |E \cap T|) \geq 2$ is satisfied. The set $p^{-1}(E^c \cap M)$ is an arithmetic progression with common difference $d(E)$, where $d(E)$ is a positive integer given by (i).*

(iii) *Suppose the cardinality of the set $p^{-1}(E \cap H)$ (resp. $p^{-1}(E \cap T)$) is equal to 2 and the cardinality of the set $p^{-1}(E \cap H)$ (resp. $p^{-1}(E \cap T)$) equal to 1, then the set $p^{-1}(E^c \cap M)$ is an arithmetic progression with common difference $d(H, E)$ (resp. $d(T, E)$) which is equal to 1.*

(iv) *Let the inequality $max(|E \cap H|, |E \cap T|) \geq 2$ be satisfied. Then the set $p^{-1}(E^c \cap M)$ is an arithmetic progression with common difference equal to 1.*

Proof. (i) We discuss the two cases.

Case 1: $max((|E \cap H|, |E \cap T|) \geq 3$.

Under the assumption, either the inequality $|E \cap H| \geq 3$ holds or the inequality $|E \cap T| \geq 3$ holds (both the inequalities may also hold). Since the claim holds for the set E if and only if it holds for the set $-E$, it is sufficient to prove the assertion under the assumption that the inequality $|E \cap H| \geq 3$ holds.

Now from Proposition 2.6.4 it follows that the sets $p^{-1}(E \cap H)$ and $E \cap T$ are arithmetic progression. Let the set

$$p^{-1}(E \cap H) = \{x_1 < x_1 + d(H,E) < x_2 + 2d(H,E) < \cdots < x_1 + (h-1)d(H,E)\}.$$

Then from (2.16) it follows that the following set

$$\{x_1 + \frac{d(H,E) + 6K + 1}{2}, x_1 + \frac{d(H,E) + 6K + 1}{2} + d(H,E)\}$$

is a subset of the set $p^{-1}(E \cap T)$. From this the following inequality follows immediately

$$d(H,E) \leq d(T,E).$$

In the case the cardinality of the set $E \cap T$ is equal to 2 it also follows that the set

$$\{x_1 + \frac{d(H,E) + 6K + 1}{2}, x_1 + \frac{d(H,E) + 6K + 1}{2} + d(H,E)\}$$

is equal to the set $p^{-1}(E \cap T)$. Hence the claim follows in case the cardinality of the set $E \cap T$ is equal to 2. Suppose the cardinality of the set $E \cap T$ is also greater than or equal to 3, then replacing the set E by the set $-E$, it follows that

$$d(H,-E) \leq d(T,-E).$$

Since the numbers $d(H,-E)$ and $d(T,-E)$ are equal to the numbers $d(T,E)$ and $d(H,E)$ respectively, the claim follows.

Case 2: $|E \cap H| = |E \cap T| = 2$.

Let the set $p^{-1}(E \cap H) = \{x, y\}$ and the set $p^{-1}(E \cap T) = \{z, w\}$. Then from Lemma 2.6.3, it follows that the parity of the elements x and y are different and the element $\frac{x+y+6k+1}{2}$ belong to the set $p^{-1}(E \cap T)$. Since we are not assuming that $z < w$, we can assume without any loss of generality that the element

$$\frac{x + y + 6k + 1}{2} = z.$$

For the similar reason the element $\frac{z+w-6k-1}{2}$ belong to the set $p^{-1}(E \cap T)$ and we can assume without any loss of generality that the element

$$\frac{z+w-6k-1}{2} = x.$$

Therefore, it follows that

$$w - z = x - y.$$

This proves the claim.

(ii) First we notice that the claim is true for the set E if and only if it is true for the set $-E$. This is because the sets $(-E)^c$ and M are equal to the sets $-(E)^c$ and $-M$ respectively. Therefore, the set $p^{-1}(E^c \cap M)$ is same as the set $6k + 1 - p^{-1}((-E)^c \cap M)$. Therefore, replacing the set E by the set $-E$ if necessary we may assume that the following inequality holds.

$$|E \cap H| \geq |E \cap T|.$$

Let the smallest member of $p^{-1}(E \cap H)$ be x so that $p^{-1}(E \cap H) = \{x + jd(E) : 0 \leq j \leq h - 1\}$. Using (2.16) it follows that the set

$$\{a + jd(E) : 0 \leq j \leq h-2\} \qquad \text{where} \quad a = x + 3k + \frac{d(E)+1}{2}, \tag{2.17}$$

is a subset of $p^{-1}(E \cap T)$ and its cardinality is $h - 1$. Since the cardinality of $p^{-1}(E \cap T)$ is at-most h and since $p^{-1}(E \cap T)$ is in arithmetic progression with common difference $d(E)$, it follows that it is a subset of $\{a + jd(E) : -1 \leq j \leq h - 1\}$. On the other hand, $p^{-1}(E^c \cap M)$ is the disjoint union of $\{2x : x \in p^{-1}(E \cap H)\}$ and $\{2x - 6k - 1 : x \in p^{-1}(E \cap T)\}$. Therefore, we have $\{2x + jd(E) : 0 \leq j \leq 2h-2\} \subset p^{-1}(E^c \cap M) \subset \{2x + jd(E) : -1 \leq j \leq 2h-1\}$. From this the claim is immediate.

(iii) It is sufficient to prove the assertion in the case the cardinality of the sets $p^{-1}(E \cap H)$ and $p^{-1}(E \cap T)$ are equal to 2 and 1 respectively. In the other case then the assertion follows by replacing the set E by the set $-E$. Suppose the set $p^{-1}(E \cap H)$ is $\{x, y\}$ and $p^{-1}(E \cap T)$ is $\{z\}$. Then it follows that the element $2z - 6k - 1$ is equal to the element $x + y$. It also follows that the set $p^{-1}(E^c \cap M)$ is $\{x, x+y, 2y\}$. Hence the assertion follows.

(iv) Replacing the set E by the set $-E$ we may assume $|E \cap H| \geq 2$. From $(i), (ii)$ and (iii) we know that the set $p^{-1}(E^c \cap M)$ is an arithmetic progression with common difference equal to $d(H.E)$ which is an odd positive integer. Suppose the assertion is not true, then it means that $d(H, E) \geq 3$. Then the smallest element of the set $p^{-1}(E \cap H)$ (let say x) is less than or equal to $2k-3$. This implies that k is at-least 3. It also follows that the cardinality of the set $\{2k+1, 2k+2, 2k+3\} \cap (E \cap M) \geq 2$. But since $x \leq 2k - 3$, the set $\{x + 2k + 1, x + 2k + 2, x + 2k + 3\}$ is a subset of the set $p^{-1}(M)$ and contains at-least 2 elements of the set $p^{-1}(E^c \cap M)$. But this contradicts the fact that the set $p^{-1}(E^c \cap M)$ is in arithmetic progression of common difference $d(H, E)$ which is at-least 3. Hence the claim follows.

□

Definition 2.6.6. We shall say that a set $B \subset Z$ is an interval if either it is an arithmetic progression with common difference equal to 1 or the cardinality of the set B is equal to 1.

Proposition 2.6.7. *Let E be a set as above. Suppose $max(|E \cap H|, |E \cap T|) \geq 2$ then $E = H \cup T$.*

Proof. From Lemma 2.6.1, the conclusion of proposition is equivalent of the assertion that $p^{-1}(E^c \cap M) = p^{-1}(M)$. Let y be the smallest member of $p^{-1}(E^c \cap M)$ and it's cardinality is s. Then using Proposition 2.6.5 it follows $p^{-1}(E^c \cap M)$ is equal to $\{y + j : 0 \leq j \leq s - 1\}$. Suppose the claim is not true. Therefore, at least one of the element of the set $\{2k + 1, 4k\}$ belong to the set $p^{-1}(E)$. The assumption of the proposition is satisfied for the set $-E$ as well and the conclusion is true for the set E if and only if it is true for the set $-E$. Therefore, replacing the set E by the set $-E$ if necessary we may assume that the element $2k + 1$ belong to the set $p^{-1}(E)$. Using this we prove the following.

Claim: $p^{-1}(E \cap H) = p^{-1}(H)$.

Let x be the smallest member of $p^{-1}(E^c \cap M)$ and it's cardinality is h. Then using Proposition 2.6.5 it follows $p^{-1}(E \cap H)$ is equal to $\{x + j : 0 \leq j \leq h - 1\}$. Therefore, it is sufficient to show that $x + h - 1$ is $2k$ and x is $k + 1$.

Claim The largest element of $p^{-1}(E \cap H)$ is $2k$.

Suppose $x + h - 1$ is not equal to $2k$. Since the set E is sum-free, it follows that $\{2x + j : 0 \leq j \leq 2h - 2\}$ is a subset of $p^{-1}(E^c \cap M)$. As $x + h - 1$ is not $2k$, therefore $2x + 2h$ belong to $p^{-1}(E \cap M)$. Therefore, $y + s - 1 \leq 2x + 2h - 1$. Since $2k + 1$ belong to the set $p^{-1}(E)$ it also follows that $x + h - 1 + 2k + 1$ belong to the set $p^{-1}(E^c)$. Since $x + h - 1 < 2K$, we have $x + h - 1 + 2k + 1$ belong to the set $p^{-1}(E^c \cap M)$. Therefore, it follows that $x + h - 1 + 2k + 1 \leq 2x + 2h - 1$ which implies $x + h - 1 \geq 2k$. Since $x + h - 1$ belong to the set $p^{-1}(H)$, it follows that $x + h - 1 = 2k$. This is contradictory to the assumption $x + h - 1 \neq 2k$. Therefore, $x + h - 1$ is $2k$.

Claim The smallest element of $p^{-1}(E \cap H)$ is $k + 1$.

Now, we will show that x is $k + 1$. Since we have shown that $p^{-1}(E \cap H) = \{x + j : 0 \leq j \leq 2k - x\}$, using Lemma 2.6.3 it follows that $\{x + j : 3k + 1 \leq j \leq 5k - x\}$ is a subset of $p^{-1}(E \cap T)$ and it's cardinality is $h - 1 = 2k - x$. The set $p^{-1}(E \cap T)$ is an interval and it's cardinality is at most $h + 1$. Therefore, we have that $p^{-1}(E \cap T)$ is a subset of $\{x + j : 3k - 1 \leq j \leq 5k - x\}$. But in case $\{x + 3k - 1, x + 3k + 1\}$ is a subset of $p^{-1}(E \cap T)$, from Lemma 2.6.3 it follows that $x - 1$ belong to $p^{-1}(E \cap T)$. This contradicts that x is the smallest element of $p^{-1}(E \cap H)$. Therefore, $p^{-1}(E \cap T)$ is a subset of $\{x + j : 3k \leq j \leq 5k - x\}$. Therefore, the least element of $p^{-1}(E \cap T)$ is either $x + 3k$ or $x + 3k + 1$.

Case The least element of $p^{-1}(E \cap T)$ is $x + 3k$.

In this case the element $x + 3k - 2k = x + k$ does not belong to the set $p^{-1}(E)$. Since x belong to $p^{-1}(H)$, the element $x + k$ belong to $p^{-1}(M)$. Therefore, in case $x + k$ is even, the element $\frac{x+k}{2}$ belong to the set $p^{-1}(E \cap H)$. But if $x + k$ is even, then $\frac{x+k}{2} < x$. This contradicts the assumption that the element x is the least element of $p^{-1}(E \cap H)$. In case $x + k$ is odd, then the element $\frac{x+k+6k+1}{2}$ belong to the set $p^{-1}(E \cap T)$. Now in case x is not $k + 1$ then $x \geq k + 2$ and the inequality $\frac{x+k+6k+1}{2} < x + 3k$ is satisfied. This contradicts that $x + 3k$ is the least element of $p^{-1}(E \cap T)$. Therefore, x has to be $k + 1$ in this case.

Case The least element of $p^{-1}(E \cap T)$ is $x + 3k + 1$.

In this case the element $x + k + 1$ belong to the set $p^{-1}(E^c \cap M)$. Then again if x is not $k + 1$, this leads to a contradiction.

Therefore, $p^{-1}(E \cap H) = H$. The assumption of proposition can hold only in case $k \geq 2$. In that case $k + 1$ and the element $k + 2$ belong to $p^{-1}(H) = p^{-1}(E \cap H)$. Therefore, the element $2k+3$ does not belong to $p^{-1}(E)$ and invoking Lemma 2.6.1 the element $p^{-1}p\left(\frac{2k+3}{2}\right) = 4k + 2$ belong to $p^{-1}(E \cap T)$. But since by assumption $2k + 1$ belong to the set $p^{-1}(E)$, this contradicts that the set E is sum-free. Therefore, finally it follows that the set $p^{-1}(E^c \cap M) = M$ and hence the proposition follows. $\square$

2.6.2 $max(|E \cap H|, |E \cap T|) \leq 1$

Replacing the set E by the set $-E$ if necessary we may assume that the following inequality holds.

$$|E \cap H| \geq |E \cap T|$$

Then we have the following three possible cases.

(i) The equality $|E \cap H| = |E \cap T| = 1$ holds.

(ii) The cardinality of the sets $E \cap H$ and $E \cap T$ are 1 and 0 respectively.

(iii) The equality $|E \cap H| = |E \cap T| = 0$.

Proposition 2.6.8. *Let E, H, T, M be as above. If $|E \cap H| = |E \cap T| = 1$, then the set $p^{-1}(E) = \{2k\} \cup \{2k + 2, 2k + 3, \cdots, 4k - 2, 4k - 1\} \cup \{4k + 1\}$.*

Proof. Let the set $(E \cap H) = \{x\}$ and the set $(E \cap T) = \{y\}$. From Proposition 2.6.1 the set $E^c \cap M = \{2x, 2y\}$ and the set $p^{-1}(E^c \cap M) = \{p^{-1}(2x), p^{-1}(2y)\}$. We claim that

Claim : x = -y.

Proof of claim: From Proposition 2.6.1 it follows that the element $\frac{-y+x}{2}$ belongs to the set $E \cap (H \cup T)$. Now if $p^{-1}(-y)$ and $p^{-1}(x)$ have same parity then the element $p^{-1}(\frac{-y+x}{2})$ belongs to the set $p^{-1}(E \cap H)$. But as the element $p^{-1}(x)$ is the only element belonging to the set $E \cap H$, in this case the claim follows. Otherwise the element

$\frac{-y+x}{2}$ belongs to the set $E \cap T$ and hence is equal to y. Also then $p^{-1}(-x)$ and $p^{-1}(y)$ have different parity and the element $\frac{-x+y}{2}$ is equal to x. But this implies after simple calculation that $x = 9x$. As m is odd this is not possible. Hence the claim follows.

Next claim is
Claim: $p^{-1}(x) = 2k$
Proof of claim: Suppose not, then $p^{-1}(y)$ is also not equal to $4k+1$. Therefore, the element $2k+1$ belong to the set $p^{-1}(E)$. This implies that the element $p^{-1}(x)+2k+1$ belongs to the set $p^{-1}(E^c \cap M)$. The element $p^{-1}(x)+2k+1$ also satisfy the inequality $p^{-1}(x)+2k+1 > 2p^{-1}(x)$. Therefore, the element $p^{-1}(x)+2k+1 = p^{-1}(2y)$. Since $y = -x$, it follows that $p^{-1}(2y) = 6k+1-2p^{-1}(x)$. Therefore, we have $3p^{-1}(x) = 4k$. This is possible only if k is divisible by 3. It is easy to check that case $k = 3$ is not possible. So we may assume that k is greater than 3 and is divisible by 3. As k is strictly greater than 3 therefore $p^{-1}(x) = \frac{4k}{3} \neq k+1$ and hence $2k+2$ belong to the set E. Also we have the inequality $\frac{4k}{3} \leq 2k-2$. Therefore, the element $p^{-1}(x)+2k+2$ belong to the set $E^c \cap M$. Therefore, the elements $p^{-1}(x)+2k+1$ as well as $p^{-1}(x)+2k+2$ belong to the set $p^{-1}(E^c \cap M)$ and neither of these elements are same as $2p^{-1}(x)$. This implies that the cardinality of the set $p^{-1}(E^c \cap M)$ is greater than or equal to 3. This is not possible. Hence the claim follows.
Now the proposition follows immediately. □

Proposition 2.6.9. *Let E be a set as above, then following holds. If $|E \cap H| = 1$ and $|E \cap T| = 0$ then we have the set $p^{-1}(E) = \{2k, 2k+1, \cdots, 4k-2, 4k-1\}$.*

Proof. Suppose the set $\{x\}$ is $p^{-1}(E \cap H)$. The claim is immediate from the assertion $x = \{2k\}$. Suppose the assertion is not true. Since we have assumed $|E \cap T| = 0$, using Lemma 2.6.1 it follows that $2k+1$ belong to the set $p^{-1}(E)$. Therefore, if $x \neq \{2k\}$, then $x+2k+1$ belong to the set $p^{-1}(M)$ and actually belong to $p^{-1}(E^c \cap M)$. But trivially $p^{-1}(E^c \cap M) = \{2x\}$ and the element $x+2k+1$ is not equal to $2x$. Hence there is a contradiction and the claim follows. □

The following proposition is trivial.

Proposition 2.6.10. *Let E be a set as above. In the case $|E \cap H| = |E \cap M| = 0$, then $E = M$*

Therefore, from Proposition 2.6.7, 2.6.8, 2.6.9 the proof of Theorem 2.1.13 in case G is cyclic follows. That is the following result follows.

Theorem 2.6.11. *Let G be a cyclic abelian group of type III. That is $G = \mathbb{Z}/m\mathbb{Z}$. Let $k = \frac{m-1}{6}$. Let E be a sum-free subset of G of density $\mu(G)$. Then there exist a surjective homomorphism $f : G \to \mathbb{Z}/m\mathbb{Z}$ such that one of the following holds.*

(i) *The set $E = f^{-1}(M)$.*

(ii) *The set E is equal to $f^{-1}p(\{2k\} \cup \{2k + j : 2 \leq j \leq 2k - 1\} \cup \{4k + 1\})$.*

(iii) *The set E or the set $-E$ is equal to $f^{-1}p(\{2k\} \cup \{2k + j : 1 \leq j \leq 2k - 1\})$.*

Proof. From Theorem 2.1.14, it follows that there exist a surjective homomorphism $g : G \to \mathbb{Z}/m\mathbb{Z}$ such that the set E is a subset of the set $g^{-1}(I)$. Then in case $max(|g(E) \cap H|, |g(E) \cap T|) \geq 2$, from Proposition 2.6.7 we have $g(E) = H \cup T$. Therefore, taking $f = 2g$ it follows $E = f^{-1}(M)$. In the other cases taking $f = g$, the claim follows from Proposition 2.6.8, 2.6.9, 2.6.10. □

2.7 Sum-free subsets of general abelian group of type III

Proof. of Theorem 2.1.12: Let γ be a special direction of the set A. Then from Proposition 2.4.3 it follows that order of γ is equal to m. We have also from Theorem 2.1.14 it follows that A is a subset of $\gamma^{-1}(I)$. Let $L \subset \mathbb{Z}/m\mathbb{Z}$ as defined in section 2.5. Then from Proposition 2.5.6 we have that L is a sum-free subset of $\mathbb{Z}/m\mathbb{Z}$ and it's cardinality is $2k$. Then from propositions 2.6.7, 2.6.8, 2.6.9, 2.6.10 it follows that $p^{-1}(L)$ is one of the following set.

Case 1: $p^{-1}(L) = p^{-1}(H \cup T)$.

In this case, we easily check that given any element $i \in \mathbb{Z}/m\mathbb{Z}$ such that i does not belong to the set L, there exist $x, y \in L$ such that either $i = x + y$ or $i = x - y$. Therefore, invoking Proposition 2.5.6, it follows that for any $i \in \mathbb{Z}/m\mathbb{Z}$ which does not belong to L, the number $\alpha_i = 0$. Therefore, A is a subset of $\gamma^{-1}(I)$. Hence $f = 2\gamma$ is a surjective homomorphism from G to $\mathbb{Z}/m\mathbb{Z}$ and moreover

$$A \subset f^{-1}\{M\}.$$

Case 2: $p^{-1}(L) = \{2k\} \cup \{2k + j : 2 \leq j \leq 2k - 1\} \cup \{4k + 1\}$.
In this case again, given any element $i \in \mathbb{Z}/m\mathbb{Z}$ such that i does not belong to the set L, there exist $x, y \in L$ such that either $i = x + y$ or $i = x - y$. Therefore, taking $f = \gamma$ we have

$$A \subset f^{-1}p(2k) \cup f^{-1}p(\{2k + j : 2 \leq j \leq 2k - 1\}) \cup f^{-1}p(4k + 1).$$

Case 3: Either $p^{-1}(L)$ or $p^{-1}(-L)$ is $\{2k\} \cup \{2k + j : 1 \leq j \leq 2k - 1\}$.
In both these cases, given any element $i \in \mathbb{Z}/m\mathbb{Z}$ such that i does not belong to the set L, there exist $x, y \in L$ such that either $i = x + y$ or $i = x - y$. Therefore, taking $f = \gamma$ the claims follows.

$$A \subset f^{-1}p(2k) \cup f^{-1}p(\{2k + j : 2 \leq j \leq 2k - 1\}) \cup f^{-1}p(4k + 1).$$

Case 4:$p^{-1}(L) = p^{-1}(M)$.
In this case, given any $i \in \mathbb{Z}/m\mathbb{Z}$ which does not belong to $\{2k + j : 0 \leq\leq 2k + 1\}$ there exist $x, y \in L$ such that either $i = x + y$ or $i = x - y$. Therefore, taking $f = \gamma$ we have

$$A \subset f^{-1}p(\{2k + j : 0 \leq j \leq 2k + 1\})$$

Therefore, in all the cases there exist a homomorphism $f : G \to \mathbb{Z}/m\mathbb{Z}$ such that

$$A \subset f^{-1}p(\{2k + j : 0 \leq j \leq 2k + 1\}).$$

Now the claims $(i), (ii), (iii)$ follows invoking Lemma 2.5.3. The claim (iv) follows observing that the set $A \cup f^{-1}p(\{2k + j : 0 \leq j \leq 2k + 1\}$ is also a sum-free set. □

Now we prove Theorem 2.1.13.

Proof. of Theorem 2.1.13: Let f be a surjective homomorphism from G to $\mathbb{Z}/m\mathbb{Z}$ given by Theorem 2.1.12. Since m is the exponent of group G and f is a surjective homomorphism to $\mathbb{Z}/m\mathbb{Z}$ there exist a subgroup C of G such that $G = S \oplus C$ where S is a kernel of f. Therefore, f restricted to C is an isomorphism from C to $\mathbb{Z}/m\mathbb{Z}$. We denote this restriction by g. Since $\alpha(A) = \mu(G)$ it follows from Theorem 2.1.12 we have

$$f^{-1}p(\{2k + j : 0 \leq j \leq 2k + 1\}) \subset A.$$

Also the following equalities hold.

$$|A(f,2k)| + |A(f,4k)| = \frac{n}{m} \tag{2.18}$$

$$|A(f,4k+1)| + |A(f,2k+1)| = \frac{n}{m} \tag{2.19}$$

Now $A(f,2k) + A(f,2k)$ is a subset of $f^{-1}\{4k\}$ and it is disjoint from $A(f,4k)$. Therefore, the following inequality follows.

$$|A(f,4k)| \leq \frac{n}{m} - |A(f,2k) + A(f,2k)| = |A(f,4k)| + |A(f,2k)| - |A(f,2k) + A(f,2k)|$$

Hence we have

$$|A(f,2k) + A(f,2k)| = |A(f,2k)|. \tag{2.20}$$

For any $i \in \mathbb{Z}/m\mathbb{Z}$ there exist $X_i \subset S$ such that $A(f,i) = X_i \oplus g^{-1}\{i\}$. Then from (2.20) it follows that $|X_{2k} + X_{2k}| = |X_{2k}|$. Therefore, either $X_{2k} = \phi$ or there exist J_1 a subgroup of S and an element $b_1 \in S$ such that $X_{2k} = J_1 + b_1$. Similar arguments implies that either $X_{4k+1} = \phi$ or there exist J_2 a subgroup of S and an element $b_2 \in S$ such that $X_{4k+1} = J_2 + b_1$. Then there are three possibilities.

Case 1: Both the sets X_{2k} and X_{4k+1} are empty sets.
In this case from (2.18) and (2.19) it follows $X_{2k+1} = S$ and $X_{4k} = S$. Hence A is $f^{-1}(M)$.

Case 2: Exactly one of the sets X_{2k} and X_{4k+1} is an empty set.
Replacing the set A by $-A$ if necessary we may assume that X_{4k+1} is an empty set. Since the set A is sum-free it follows that X_{4k} is a subset of $(J_1 + 2b_1)^c$. From (2.18) it follows trivially that $X_{4k}$is $(J_1 + 2b_1)^c$.
Case 3: Both the sets X_{2k} and X_{4k+1} are not empty sets.
Then arguing as in case 2 it follows that X_{4k} is $(J_1 + 2b_1)^c$ and X_{4k+1} is $(J_2 + 2b_2)^c$. The assumption that A is sum-free implies that X_{4k+1} is a subset of $(X_{2k} + X_{2k+1})^c$. This means

$$J_2 + b_2 \subset (J_1 + b_1 + (J_2 + 2b_2)^c)^c.$$

This implies,

$$(J_2 + b_2)^c = J_1 + b_1 + (J_2 + 2b_2)^c.$$

Therefore, we have

$$J_1 + b_1 \subset J_2 - b_2. \tag{2.21}$$

Since X_{2k} is a subset of $(X_{2k} + X_{2k+1})^c$, same argument implies that

$$J_2 + b_2 \subset J_1 - b_1. \tag{2.22}$$

From (2.21) and (2.22) we have $J_1 + b_1 = J_2 - b_2$. Hence $J_1 = J_2$. This proves the theorem. □

2.8 Remarks

In case G is of type I(p) group and A is a maximal sum-free subset of G such that $\alpha(A) > \frac{1}{3} + \frac{1}{3(p+1)}$ then $\alpha(A) = \mu(G)$. For the proof of this one may see [GR05]. But in case G is of type III, there exist A such that A is a maximal sum-free set of cardinality $\mu(G)n - 1$. For this consider the following example.

Example. Let $G = (\mathbb{Z}/7\mathbb{Z})^2$ and $\pi_2 : G \to \mathbb{Z}/7\mathbb{Z}$ be a natural projection to second co-ordinate. Then let

$$A = \pi_2^{-1}\{3\} \cup (0,2) \cup (1,2) \cup (\pi_2^{-1}\{4\} \setminus \{(0,4),(1,4),(2,4)\}).$$

If A is as in the above example, then A is a maximal sum-free subset of cardinality $\mu(G)n - 1$. Therefore, Theorem 2.1.12 does not give complete characterisation of all large maximal sum-free subsets of G.

In general Hamidoune and Plagne [oHP04] have studied (k,l) free subsets of finite abelian groups. For any positive integer t we define tA by

$$tA = \{x \in G : x = \sum_{i=1}^{t} a_i, \quad a_i \in A \quad \forall i\}.$$

Given any two positive integers we say A is (k,l) free if $kA \cap lA = \phi$. In case $k - l \equiv 0(\text{mod m})$, where m is the exponent of G, then it is easy to check that there is no set apart from empty set which is (k,l) free. To rule out such cases, one assume that $gcd(|G|, k-l) = 1$. We denote the density of the largest (k,l) free set by $\lambda_{k,l}$. Hamidoune and Plagne [oHP04] conjectured the following.

Conjecture. Let G be a finite abelian group and m is the exponent of G. Let k,l be positive integers such that $gcd(|G|, k-l) = 1$. Then the density of largest (k,l) free set is given by the following formula.

$$\lambda_{k,l} = max_{d|m} \frac{[\frac{d-2}{k+l}] + 1}{d}$$

They [oHP04] proved the above conjecture in case when there exist a divisor d_0 of m such that d_0 is not congruent to 1 modulo $k + l$. In this situation they also showed that given any (k, l) free set of density $\lambda_{k,l}$, there exist a positive integer d, a surjective homomorphism $f : G \to \mathbb{Z}/d\mathbb{Z}$, a set $B \subset \mathbb{Z}/d\mathbb{Z}$ such that B is (k, l) free and $A = f^{-1}(B)$. That is any (k, l) free set of density $\lambda_{k,l}$ is an inverse image of a (k, l) free subset of a cyclic group. One may ask the following question:

Question 2.8.1. Let G be a finite abelian group and m is the exponent of G. Suppose k, l are positive integers such that all the divisors of m are congruent to 1 modulo $k+l$ and $gcd(k - l, |G|) = 1$. Is it true that any (k, l) free set of density $\lambda_{k,l}$ is an inverse image of a (k, l) free set of a cyclic group?

We have already seen that the answer of the above question is negative in case $k = 2$ and $l = 1$. The following arguments show that the answer of the above question is negative for an arbitrary value of k provided $l = 1$.
In case all the divisors of m are congruent to 1 modulo $k + l$, it is easy to check that

$$max_{d|m} \frac{[\frac{d-2}{k+l}] + 1}{d} = \frac{[\frac{m-2}{k+l}] + 1}{m}.$$

Now consider the following example.

Example. Let G be a finite abelian group and m is the exponent of G. We further assume that G is not cyclic. Let k be a positive integer such that $gcd(|G|, k - 1) = 1$ and all the divisors of m are congruent to 1 modulo $k + 1$. Then $G = S \oplus \mathbb{Z}/m\mathbb{Z}$ with $S \neq \{0\}$. Let $q = [\frac{m-2}{k+1}]$. Let $x \in \mathbb{Z}/m\mathbb{Z}$ such that $(k - 1)x \equiv 1 + q (\text{mod m})$. Let J be any proper subgroup of S and

$$A = (J \oplus \{x\}) \cup (S \oplus \{x + 1, x + 2, \cdots, x + q\}) \cup (J^c \oplus \{x + q + 1\}).$$

If A is as in the above example then it is easy to check that A is $(k, 1)$ free and density of A is $\frac{\frac{m-2}{k+1}+1}{m}$. Hamidoune and Plagne [oHP04] also proved the above conjecture for all cyclic groups. Using this and following the arguments as in section 2.3 it follows that stabiliser of A is J. This shows that if A is the set as in above example then A is not an inverse image of any $(k, 1)$ free subset of a cyclic group.

Chapter 3

Asymptotic formula for number of sum-free subsets

3.1 Introduction

Let G be a finite abelian group of order n. A subset A of G is said to be sum-free if there is no solution of the equation $x + y = z$, with x, y, z belonging to the set A. Let $SF(G)$ denotes the set of all sum-free subsets of G. In this chapter, we discuss the question of determining the cardinality of $SF(G)$.

Definition 3.1.1. (i) Let $\mu(G)$ denote the density of a largest sum-free subset of G, so that any such subset has size $\mu(G)n$.

(ii) Given a set $B \subset G$ we say that $(x, y, z) \in B^3$ is a Schur triple of the set B if $x + y = z$.

Observing that all subsets of a sum-free set are sum-free we have the obvious inequality

$$|SF(G)| \geq 2^{\mu(G)n} \tag{3.1}$$

Let the symbol $\sigma(G)$ denote the number $n^{-1}(\log_2 |SF(G)|)$. Then from (3.1) it follows trivially that $\sigma(G) \geq \mu(G)$.

In this chapter we prove the following two results. Theorem 3.1.2 follows immediately from Theorem 3.1.3 and a result from [GR05], namely Theorem 3.1.7. The methods used to prove Theorem 3.1.3 are a slight refinements of methods in [GR05].

Theorem 3.1.2. *Let G be a finite abelian group of order n. Then we have the following asymptotic formula*

$$\sigma(G) = \mu(G) + O(\frac{1}{(\ln n)^{1/27}}).$$

Theorem 3.1.3. *There exist an absolute positive constant δ_0 such that if $F \subset G$ as at-most δn^2 Schur triples, where $\delta \leq \delta_0$, then*

$$|F| \leq (\mu(G) + C\delta^{1/3})n, \tag{3.2}$$

where C is an absolute positive constant.

Earlier Ben Green and Ruzsa [GR05] proved the following:

Theorem 3.1.4. *([GR05], Theorem 1.8.) Let G be a finite abelian group of order n. Then we have the following asymptotic formula*

$$\sigma(G) = \mu(G) + O(\frac{1}{(\ln n)^{1/45}}).$$

Theorem 3.1.5. *([GR05], Proposition 2.2) Let G be an abelian group, and suppose that $F \subseteq G$ has at-most δn^2 Schur triples. Then*

$$|F| \leq (\mu(G) + 2^{20}\delta^{1/5})n. \tag{3.3}$$

The following theorem is also proven in [GR05].

Theorem 3.1.6. *([GR05], Corollary 4.3.) Let G be an abelian group, and suppose that $F \subseteq G$ has at-most δn^2 Schur triples. Then*

$$|F| \leq (max(\frac{1}{3}, \mu(G) + 3\delta^{1/3})n. \tag{3.4}$$

Theorem 3.1.3 follows immediately from Theorem 3.1.6 in the case $\mu(G) \geq \frac{1}{3}$. In the case $\mu(G) < \frac{1}{3}$, Theorem 3.1.3 again follows immediately from Theorem 3.1.6 in the case δ is not very "small". In the case δ is small we require Lemma 3.2.3 where an estimate is done differently than in [GR05]. For the rest of results we require to prove Theorem 3.1.3, the methods used are completely identical as in [GR05], but the results used are not identical.

For proving Theorem 3.1.2 we use the following result from [GR05].

Theorem 3.1.7. *([GR05], Proposition 2.1') Let G be an abelian group of cardinality n, where n is sufficiently large. Then there is a family $\mathcal{F}$ of subsets of G with the following properties*

(i) $\log_2 |\mathcal{F}| \leq n(\ln n)^{-1/18}$*;*

(ii) *Every $A \in SF(G)$ is contained in some $F \in \mathcal{F}$;*

(iii) *If $F \in \mathcal{F}$ then F has at-most $n^2(\ln n)^{-1/9}$ Schur triples.*

Theorem 3.1.2 follows immediately from Theorem 3.1.7 and Theorem 3.1.3. We shall reproduce the proof given in [GR05]. If n is sufficiently large as required by Theorem 3.1.7 then associated to each $A \in SF(G)$ there is an $F \in \mathcal{F}$ for which $A \subset F$. For a given F, the number of A which can arise in this way is at most $2^{|F|}$. Thus we have the bound

$$|SF(G)| \leq \sum_{F \in \mathcal{F}} 2^{|F|} \leq |\mathcal{F}| max_{F \in \mathcal{F}} |F|$$

Hence it follows that

$$\sigma(G) \leq \mu(G) + C\frac{1}{(\ln n)^{1/27}} + \frac{1}{\ln n^{1/18}}. \tag{3.5}$$

But from (3.1) we have the inequality $\sigma(G) \geq \mu(G)$. Hence Theorem 3.1.2 follows.

In order to prove Theorem 3.1.3 we shall require the value of $\mu(G)$, which is now known for all finite abelian groups. In order to explain the results we need the following definition.

Definition 3.1.8. Suppose that G is a finite abelian group of order n. If n is divisible by any prime $p \equiv 2 (\text{mod } 3)$ then we say that G is type I. We say that G is type I(p) if it is type I and if p is the *least* prime factor of n of the form $3l + 2$. If n is not divisible by any prime $p \equiv 2 (\text{mod } 3)$, but $3|n$, then we say that G is type II. Otherwise G is said to be type III. That is the group G is said to be of type III if and only all the divisors of n are congruent to 1 modulo 3.

The following theorem is due to P. H. Diananda and H. P. Yap [DY69] for type I and type II groups and due to Green and Ruzsa [GR05] for type III groups.

Theorem 3.1.9. *([GR05], Theorem 1.5.) Let G be a finite abelian group of order n. Then the following holds.*

(i) *If G is of type I(p) then $\mu(G) = \frac{1}{3} + \frac{1}{3p}$.*

(ii) *If G is of type II then $\mu(G) = \frac{1}{3}$.*

(iii) *If G is of type III then $\mu(G) = \frac{1}{3} - \frac{1}{3m}$, where m is the exponent of G.*

3.2 Cardinality of almost sum-free set

In case the group G is not of type III it follows from Theorem 3.1.9 that $\mu(G) \geq \frac{1}{3}$ and hence Theorem 3.1.3 follows immediate using Theorem 3.1.6. Therefore we are required to prove Theorem 3.1.3 for type III groups only.

For the rest of this chapter G will be a finite abelian group of type III and m shall denote the exponent of G. The following proposition is an immediate corollary of Theorem 3.1.9 and Theorem 3.1.6.

Proposition 3.2.1. *Let G be an abelian group of type III. Let the order of G be n and the exponent of G be m. If $F \subset G$ as at-most δn^2 Schur triples then*

(i) $|F| \leq (\mu(G) + \frac{1}{3m} + 3\delta^{1/3})n$.

(ii) *In the case $\delta^{1/3}m \geq 1$ then $|F| \leq (\mu(G) + 4\delta^{1/3})n$, that is Theorem 3.1.3 holds in this case.*

Therefore to prove Theorem 3.1.3 we are left with the following case.
Case: The group G is an abelian group of type III, order n and exponent m. The subset $F \subset G$ has at most δn^2 Schur triples and $\delta^{1/3}m < 1$.

Let γ be a character of G and q denote the order of γ. Given such γ we define $H_j = \gamma^{-1}(e^{2\pi i j/q})$. We also denote the set $H_0 = ker(\gamma)$ by just H. Notice that H is a subgroup of G and H_j are cosets of H. The cardinality of the coset $|H_j| = |H| = \frac{n}{q}$. The indices is to be considered as residues modulo q, reflecting the isomorphism $G/H \equiv \mathbb{Z}/q\mathbb{Z}$. For any set $F \subset G$ we also define $F_j = F \cap H_j$ and $\alpha_j = |F_j|/|H_j|$.

Proposition 3.2.2. *Let G be a finite abelian group of order n. Let F be a subset of G having at most δn^2 Schur triples where $\delta \geq 0$. Let γ be any character of G and q be its order. Also let F_i and α_i be as defined above. Then the following holds.*

(i) *If x belongs to F_i and y belongs to F_j then $x+y$ belongs to H_{i+j}.*

(ii) *The number of Schur triples $\{x, y, z\}$ of the set A with x belongs to F_l, y belongs to F_j and z belongs to F_{j+l} is at least $|F_l|(|F_j| + |F_{j+l}| - |H|)$. In other words there are at least $\alpha_l(\alpha_j + \alpha_{j+l} - 1)(\frac{n}{q})^2$ Schur triples $\{x, y, z\}$ of the set F with x belongs to the set F_l.*

(iii) *Given any $l \in \mathbb{Z}/q\mathbb{Z}$ such that $\alpha_i > 0$, it follows that for any $j \in \mathbb{Z}/q\mathbb{Z}$ the inequality*
$$\alpha_j + \alpha_{j+l} \leq 1 + \frac{\delta q^2}{\alpha_l} \tag{3.6}$$
holds.

(iv) *Given any $t > 0$, we define the set $L(t) \subset \mathbb{Z}/q\mathbb{Z}$ as follows. The set*
$$L(t) = \{i \in \mathbb{Z}/q\mathbb{Z} : \alpha_i + \alpha_{2i} \geq 1 + t\}.$$
Then it follows that
$$\sum_{i \in L(t)} \alpha_i \leq \frac{\delta q^2}{t} \tag{3.7}$$

Proof. (i) This follows immediately from the fact that γ is an homomorphism.

(ii) In the case $|F_l|(|F_j| + |F_{j+l}| - |H|) \leq 0$, there is nothing to prove. Hence we can assume that the set $F_l \neq \phi$. Then for any x which belongs to the set F_l, the sets $x+F_j \subset H_{j+l}$. Since the set F_{j+l} is also a subset of H_{j+l} and $|F_j|+|F_{j+l}|-|H| > 0$, it follows that
$$|(x + F_j) \cap F_{j+l}| = ||F_j| + |F_{j+l}| - |(x + F_j) \cup F_{j+l}| \geq |F_j| + |F_{j+l}| - |H|.$$
Now, for any z belonging to the set $(x + F_j) \cap F_{j+l}$ there exist y belonging to F_j such that $x + y = z$. Hence the claim follows.

(iii) From (ii) there are at least $\alpha_l(\alpha_j + \alpha_{j+l} - 1)(\frac{n}{q})^2$ Schur triples of the set F. Hence the claim follows by the assumed upper bound on the number of Schur triples of the set F.

(iv) For any fixed $i \in L(t)$, taking $j = l = i$ in (ii), we get there are at least $\alpha_i t(\frac{n}{q})^2$ Schur triples $\{x, y, z\}$ of the set F with x belonging to the set F_i. Now for given any two $i_1, i_2 \in L(t)$ such that $i_1 \neq i_2$,the sets F_{i_1} and F_{i_2} have no element in common. Therefore there are at least $t(\frac{n}{q})^2 \sum_{i\in L(t)} \alpha_i$ Schur triples of the set F. Hence the claim follows.

□

Since the order of any character of an abelian group G divides the order of group and G is of type III, the order q of any character γ of G is odd and congruent to 1 modulo 3. Therefore $q = 6k + 1$ for some $k \in \mathbb{N}$. Let $I, H, M, T \subset \mathbb{Z}/q\mathbb{Z}$ denote the image of natural projection of the intervals $\{k + 1, k + 2, \cdots, 5k - 1, 5k\}, \{k + 1, k + 2, \cdots, 2k - 1, 2k\}, \{2k + 1, 2k + 2, \cdots, 4k - 1, 4k\}, \{4k + 1, 4k + 2, \cdots, 5k - 1, 5k\} \subset \mathbb{Z}$ to $\mathbb{Z}/q\mathbb{Z}$. Then the set I is divided into $2k$ disjoint pairs of the form $(i, 2i)$ where i belongs to the set $H \cup T$.

Lemma 3.2.3. *Let G be a finite abelian group of type III and order n. Suppose that $F \subset G$ has at-most δn^2 Schur triples. Let γ be a character of G. Let the order of γ be equal to $q = 6k + 1$. Then the following inequality holds.*

$$\sum_{i=k+1}^{5k} \alpha_i \leq 2k + 2\delta^{1/2} q^{3/2} \tag{3.8}$$

Proof. The set $I = \{k + 1, k + 2, \cdots, 5k\}$ is divided into $2k$ disjoint pairs of the form $(i, 2i)$ where i belongs to the set $H \cup T$. Therefore it follows that

$$\sum_{i=k+1}^{5k} \alpha_i = \sum_{i\in H\cup T} (\alpha_i + \alpha_{2i}) \tag{3.9}$$

Given a $t > 0$ we divide the set $H \cup T$ into two disjoint sets as follows. We define the set

$$S = \{i \in H \cup T : \alpha_i + \alpha_{2i} \leq 1 + t\}$$

and

$$L = \{i \in H \cup T : \alpha_i + \alpha_{2i} > 1 + t\}.$$

Therefore the sets S and L are disjoint and the set $H \cup T = S \cup L$. Therefore it follows that

$$\sum_{i\in H\cup T} (\alpha_i + \alpha_{2i}) = \sum_{i\in S} (\alpha_i + \alpha_{2i}) + \sum_{i\in L} (\alpha_i + \alpha_{2i}). \tag{3.10}$$

From (3.7) we have the following inequality

$$\sum_{i\in L}\alpha_i \leq \frac{\delta q^2}{t}.$$

Since for any $l \in \mathbb{Z}/q\mathbb{Z}$, the inequality $\alpha_l \leq 1$ holds trivially. It follows that

$$\sum_{i\in L}(\alpha_i+\alpha_{2i}) \leq |L| + \frac{\delta q^2}{t}. \tag{3.11}$$

Also the following inequality

$$\sum_{i\in S}(\alpha_i+\alpha_{2i}) \leq |S| + |S|t \tag{3.12}$$

holds just by the definition of the set S. Therefore from (3.9), (3.10), (3.12), (3.11) it follows that

$$\sum_{i=k+1}^{5k}\alpha_i \leq |L| + \frac{\delta q^2}{t} + |S| + |S|t \leq 2k + qt + \frac{\delta q^2}{t}. \tag{3.13}$$

Now choosing $t = (\delta q)^{1/2}$ the lemma follows. □

Remark 3.2.4. The sum appearing in last lemma was estimated as $2k + (\delta)^{1/2}q^2$ in [GR05]. There the estimate $\alpha_i + \alpha_{2i} \leq (\delta)^{1/2}q$ is used to estimate the right hand side of (3.9).

Notice that Lemma 3.2.3 holds for any character γ of a group G of type III. We would like to show that given $F \subset G$ having at most δn^2 Schur triples and also assuming that $(\delta)^{1/3}m < 1$ where m is the exponent of G, there is a character γ such that $\alpha_l \leq C(\delta q)^{1/2}$ $i \in \{0,1,2,\cdots k\} \cup \{5k+1, 5k+2, \cdots, 6k\}$ where C is an absolute positive constant, q is the order of γ and $k = \frac{q-1}{6}$. To be able to do this we recall the concept of special direction as defined in [GR05]. The method of proof of this part is completely identical as in [GR05], though the results are not.

Given any set $B \subset G$, and a character γ of G we define $\widehat{B}(\gamma) = \sum_{b\in B}\gamma(b)$. Given a set $B \subset G$ fix a character γ_s such that $Re\widehat{B}(\gamma)$ is minimal. We follow the terminology in [GR05] and call γ_s to be the special direction of the set B.
The following Lemma is proven in [GR05].

Lemma 3.2.5. *([GR05], Lemma 7.1, Lemma 7.3. (iv)) Let G be an abelian group of type III. Let $F \subset G$ has at most δn^2 Schur triples. Let γ_s be a special direction of the set F. Let α denotes the number $\frac{|F|}{|G|}$. Then the following holds.*

(i) $Re\widehat{F}(\gamma_s) \leq \left(\frac{\delta}{\alpha(1-\alpha)} - \frac{\alpha^2}{\alpha(1-\alpha)}\right) n.$

(ii) *In case $\delta \leq \eta/5$, then either $|F| \leq (\mu(G))n$ or the following inequality holds.*

$$q^{-1}\sum_{j=0}^{q-1} \alpha_j \cos(\frac{2\pi j}{q}) + \frac{\mu(\mathbb{Z}/q\mathbb{Z})^2}{1-\mu(\mathbb{Z}/q\mathbb{Z})} < 6\delta. \tag{3.14}$$

Proof. (i) The number of Schur triples in the set F is exactly $n^{-1}\sum_\gamma (\widehat{F}(\gamma))^2\widehat{F}(\gamma)$. This follows after the straightforward calculation, using the fact that

$$\sum_\gamma \gamma(b) = 0 \quad if \quad b \neq 1, \tag{3.15}$$

and is equal to n if $b = 1$ where 1 here denotes the identity element of the group G. Therefore using the assumed upper bound on the number of Schur triples in the set F it follows that

$$n^{-1}\sum_\gamma (\widehat{F}(\gamma))^2\widehat{F}(\gamma) = n^{-1}\sum_{\gamma\neq 1} (\widehat{F}(\gamma))^2\widehat{F}(\gamma) + n^{-1}\widehat{F}(1))^2\widehat{F}(1) \leq \delta n^2,$$

Where $\gamma = 1$ is the trivial character of the group G. Since $n^{-1}(\widehat{F}(1))^2\widehat{F}(1) = (\alpha)^3 n^2$, it follows that

$$n^{-1}Re\widehat{F}(\gamma_s)\sum_{\gamma\neq 1}(\widehat{F}(\gamma))^2 \leq n^{-1}\sum_{\gamma\neq 1}(\widehat{F}(\gamma))^2\widehat{F}(\gamma) \leq (\delta - \alpha^3)n^2$$

Since using (3.15) it follows that $\sum_{\gamma\neq 1}(\widehat{F}(\gamma))^2 = \alpha(1-\alpha^2)n^2$, the claim follows.

(ii) We have $Re\widehat{F}(\gamma_s) = |H|\sum_j \alpha_j \cos(\frac{2\pi j}{q})$. Therefore in the case $|F| \geq \mu(G)$, then from (i) it follows that

$$q^{-1}\sum_{j=0}^{q-1} \alpha_j \cos(\frac{2\pi j}{q}) \leq \frac{\delta}{\alpha(1-\alpha)} - \frac{\alpha^2}{\alpha(1-\alpha)} \tag{3.16}$$

$$q^{-1}\sum_{j=0}^{q-1} \alpha_j \cos(\frac{2\pi j}{q}) + \frac{\mu(G)^2}{1-\mu(G)} \leq \frac{\delta}{\alpha(1-\alpha)} \tag{3.17}$$

Since from Theorem 3.1.9 that $\mu(G) \geq \mu(\mathbb{Z}/q\mathbb{Z})$ it follows that

$$\frac{\mu(G)^2}{1-\mu(G)} \geq \frac{(\mu(\mathbb{Z}/q\mathbb{Z}))^2}{1-\mu(\mathbb{Z}/q\mathbb{Z})}.$$

The claim follows using this and the fact that $\mu(G) \geq \frac{1}{4}$, which implies that $\frac{\delta}{\alpha(1-\alpha)} \leq 6\delta$.

□

Proposition 3.2.6. *Let G be an abelian group of type III. Let n and m denote the order and exponent of G respectively. Let $F \subset G$ has at most δn^2 Schur triples and $\delta^{1/3} m \leq 1$. Let $|F| \geq \mu(G)n$. Let γ_s be a special direction of the set F and q be the order of γ_s. Let $q = 6k+1$ and α_i be as defined above. There exist an positive absolute constants q_0 and δ_1 such that if $q \geq q_0$ and $\delta \leq \delta_1$, then the following holds*

$$\alpha_i \leq c(\delta q)^{1/2} \textit{ for all } i \in \{0, 1, \cdots, k-1, k\} \cup \{5k+1, 5k+2, \cdots 6k-1\}, \tag{3.18}$$

where c is a positive absolute constant.

Proof. If $F \subset G$ be the set as given, then $-F \subset G$ is also a set which satisfies the same hypothesis as required in the statement of proposition. It follows from definition of special direction that if γ is a special direction of F then γ is also a special direction of $-F$. It is also the case that $|F_j| = |(-F)_{-j}|$. Therefore to prove the proposition it is sufficient to show that

$$\alpha_i \leq c(\delta q)^{1/2} \text{ for all } i \in \{0, 1, \cdots, k-1, k\}$$

for some positive absolute constant c.
Let $S = q^{-1} \sum_{j=0}^{q-1} \alpha_j \cos(\frac{2\pi j}{q}) + \frac{\mu(\mathbb{Z}/q\mathbb{Z})^2}{1-\mu(\mathbb{Z}/q\mathbb{Z})}$. Then from Lemma 3.2.5 we have that

$$S \leq 6\delta. \tag{3.19}$$

Let for some $l \in \{0, 1, \cdots, k-1, k\}$, $\alpha_l > c(\delta q)^{1/2}$ (where c is a positive number which we shall choose later), then we shall show that this violates (3.19), provided q and c are sufficiently large and δ is sufficiently small. For this we shall find the lower bound of $M = q^{-1} \sum_{j=0}^{q-1} \alpha_j \cos(\frac{2\pi j}{q})$.
Let γ_j denote $\frac{(\alpha_j + \alpha_{j+l})}{2}$. Then we have

$$M = \frac{1}{q 2\cos(\frac{\pi l}{q})} \sum_{j=0}^{q-1} \alpha_j \left(\cos\frac{(2j+l)\pi}{q} + \cos\frac{(2j-l)\pi}{q} \right).$$

That is we have

$$M = \frac{1}{q\cos(\frac{\pi l}{q})} \sum_{j=0}^{q-1} \gamma_j \cos\frac{(2j+l)\pi}{q} \tag{3.20}$$

Notice that $\cos(\frac{\pi l}{q})$ is not well defined if we consider l as an element of $\mathbb{Z}/q\mathbb{Z}$. This is because the function $\cos(\frac{\pi t}{q})$ as a function of t is not periodic with period q but is periodic with period $2q$. But we have assumed that $l \in \{0, 1, \cdots, k-1, k\}$, therefore the above computation is valid.

Since $\delta^{1/2}q^{3/2} \le \delta^{1/2}m^{3/2} < 1$ is true by assumption, recalling Lemma 3.2.2 it follows that

$$\begin{aligned} 2\gamma_j &= \alpha_j + \alpha_{j+l} \le 1 + \frac{1}{c}\delta^{1/2}q^{3/2} \le 1 + \frac{1}{c}, \text{ for any } j \in \mathbb{Z}/q\mathbb{Z} \quad (3.21) \\ \text{and} \sum_j \gamma_j &= \sum_j \alpha_j \ge \mu(G)n \ge 2k. \quad (3.22) \end{aligned}$$

The inequality (3.22) follows from the assumption that $|F| \ge \mu(G)n$.

Let t_c denote the number $1 + 1/c$. Let $E(c, q)$ denote the minimum value of $\sum_{j=0}^{q-1} \gamma_j \cos\frac{(2j+l)\pi}{q}$ subject to the constraints that $0 \le \gamma_j \le \frac{t_c}{2}$ and $\sum_j \gamma_j \ge 2k$.
The function $f : \mathbb{Z} \to \mathbb{R}$ given by $f(x) = \cos(\frac{(q+x)\pi}{q})$ is an even function with period $2q$. Also for $0 \le x \le q$ we have the following

$$f(0) < f(1) < f(2) < f(3) < \cdots < f(q-1) < f(q) \quad (3.23)$$

Now to determine the minimum value of $E(c, q)$, we should choose γ_j to be as large as we can when the function $\cos\frac{2j+l}{q}$ takes the small value. Now we have the two cases to discuss, the one when l is even and when l is odd. Now the image of function $g : \mathbb{Z}/qZ \to \mathbb{R}$ given by $g(j) = cos\frac{(2j+l)\pi}{q}$ is equal to $\{f(x) : x \text{ is even }\}$ in case l is odd and is equal to $\{f(x) : x \text{ is odd }\}$ in case l is even. From this it is also easy to observe that the number of $j \in \mathbb{Z}/q\mathbb{Z}$ such that the function $\cos\frac{2j+l}{q}$ is negative is at most $\frac{q+1}{2}$.
Now let $-\frac{q-1}{2} - l \le j \le \frac{q-1}{2} - l$ so that $-q \le 2j + l \le q$. Now in case l is odd then consider the case when $\gamma_j = \frac{t_c}{2}$ if

$$2j + l = q - [\frac{k}{t_c}\frac{1}{2}], \dots, q-2, q, q+1, \dots, q + [\frac{k}{t_c} - \frac{1}{2}] \text{ and } \gamma_j = 0 \text{ otherwise.} \quad (3.24)$$

The condition $2[\frac{k}{t_c} - 1/2] + 1 \ge \frac{q+1}{2}$ ensures that in the above configuration for all possible negative values of $cos\frac{(2j+l)\pi}{q}$ the maximum possible weight $\frac{t_c}{2}$ is chosen. This condition can be ensured if $q \ge 11$ by choosing $c \ge c_1$ where c_1 is sufficiently large positive absolute constant. Therefore after doing a small calculation one may check that for $c \ge c_1$ the following inequality

$$E(c, q) \ge -t_c \frac{\sin\frac{2\pi[\frac{k}{t_c} - \frac{1}{2}]}{q}}{2q \sin\pi/q \cos\pi l/q} - \frac{1}{q} \quad (3.25)$$

holds. In case l is even and $c \geq c_1$ then choosing $\gamma_j = \frac{t_c}{2}$ if

$$2j + l = q - [\frac{k}{t_c}], \ldots, q-1, q+1, \ldots, q + [\frac{k}{t_c}] \text{ and weights 0 otherwise,} \tag{3.26}$$

we get that the following inequality

$$E(c) \geq -t_c \frac{\sin \frac{2\pi[\frac{k}{t_c}]+1}{q}}{2q \sin \pi/q \cos \pi l/q} - \frac{t_c}{q} \tag{3.27}$$

holds. Using this we get

$$\begin{aligned} S &\geq -t_c \frac{\sin \frac{2\pi[\frac{k}{t_c}]}{q}}{2q \sin \pi/q \cos \pi l/q} + \frac{\mu(\mathbb{Z}/q\mathbb{Z})^2}{1 - \mu(\mathbb{Z}/q\mathbb{Z})} \text{ when l is even and} && (3.28) \\ S &\geq t_c \frac{\sin \frac{2\pi[\frac{k}{t_c} - \frac{1}{2}]}{q}}{2q \sin \pi/q \cos \pi l/q} - \frac{1}{q} + \frac{\mu(\mathbb{Z}/q\mathbb{Z})^2}{1 - \mu(\mathbb{Z}/q\mathbb{Z})} \text{ when l is odd.} && (3.29) \\ & && (3.30) \end{aligned}$$

Now as $q \to \infty$ right hand side of (3.28) as well as (3.29) converges to the

$$-t_c \frac{\sin \frac{2\pi}{3t_c}}{2\pi \cos \frac{\pi l}{q}} + \frac{1}{6}$$

Then let $\eta = 2^{-20}$, then there exist positive absolute constants c_2 and q_0 such that for all $c \geq c_2$ and $q \geq q_0$ we get that

$$S \geq -\frac{1}{2\pi} + \frac{1}{6} - \eta = 8\delta_1 \text{ say .} \tag{3.31}$$

The above quantity is strictly positive absolute constant. Then if $\delta < \delta_1$, this contradicts (3.19). Hence the lemma follows. □

To complete the proof of Theorem 3.1.3, we require the following result from [GR05].

Lemma 3.2.7. *([GR05], Proposition 7.2) Let G be an abelian group of type III and n , m be its order and exponent respectively. Let $F \subset G$ has at most δn^2 Schur triples, with $\delta^{1/3} m < 1$. Let q be the order of special direction such that $q \leq q_0$, where q_0 is a positive absolute constant as in Lemma 3.2.6. Also assume that $\delta \leq \frac{\eta}{q^5} = \delta_2$, where $\eta = 2^{-50}$, then either $|F| \leq \mu(G)n$ or $\alpha_i \leq 64\delta^{1/3} q^{2/3}$.*

Let δ_1 and δ_2 be as in Lemma 3.2.6 and Lemma 3.2.7 respectively. Then we take $\delta_0 = min(\delta_1, \delta_2)$ in Theorem 3.1.3. As we remarked above that in case G is not of type

III, Theorem 3.1.3 follows immediately from Theorem 3.1.6. Combining Lemma 3.2.3, Lemma 3.2.6 and Lemma 3.2.7, Theorem 3.1.3 follows in the case G is of type III and $\delta^{1/3}m < 1$. In case G is of type III and $\delta^{1/3}m > 1$, Theorem 3.1.3 follows from Proposition 3.2.1.

Chapter 4

On an additive representation function

Let $\mathbb{N}$ denote the set of all natural numbers. If A is an infinite subset of $\mathbb{N}$ then we set

$$A(x) = \{a \leq x : a \in A\}.$$

Let $r(A, n)$ denote the number of solutions of the equation

$$n = a_i + a_j, \quad \text{where } a_i \leq a_j, \quad a_i, a_j \in A.$$

Here and in what follows A will always denote an infinite subset of $\mathbb{N}$ such that there exists a natural number $n_0(A)$ such that

$$r(A, n) \neq 1 \text{ for } n \geq n_0(A).$$

Also $a_0(A)$ shall denote the least natural number such that $a_0(A) \in A$ and $a_0(A) \geq n_0(A)$. Regarding such sets, Nicolas, Ruzsa, Sárközy [NRS98] proved the following theorem.

Theorem. *If A is an infinite subset of $\mathbb{N}$ such that $r(A, n) \neq 1$ for all sufficiently large natural numbers n, then*

$$\limsup |A(x)| \left(\frac{\ln \ln x}{\ln x} \right)^{3/2} \geq \frac{1}{20}.$$

They also gave an example of a set A such that $r(A, n) \neq 1$ for all sufficiently large natural numbers n and $|A(x)| \ll (\ln x)^2$. In this chapter we shall show the following:

Theorem 4.0.8. *There exists an absolute constant $c > 0$ with the following property: for any infinite subset A of $\mathbb{N}$ such that $r(A,n) \neq 1$ for all sufficiently large natural numbers n, then*

$$|A(x)| \geq c\left(\frac{\ln x}{\ln\ln x}\right)^2 \text{ for all } x \text{ sufficiently large.}$$

Theorem 4.0.8 follows from Proposition 4.0.14 by noting that if Y is sufficiently large then for some positive absolute constant c the interval $[(Y)^{\frac{1}{2}}, Y)$ contains at least $c\left(\frac{\ln Y}{\ln\ln Y}\right)$ disjoint intervals of the form $[b, b(\ln Y)^{11})$.

Apart from the arguments used in proving Lemma 4.0.13, the rest of arguments used in this chapter are as in [NRS98]. Lemma 4.0.13 improves inequality (4.1) of Proposition 4.0.12 and this improves result of Proposition 4.0.12 and gives Proposition 4.0.14. As remarked above Theorem 4.0.8 is an immediate corollary of Proposition 4.0.14. The sequence B_Y constructed in Lemma 4.0.11 is a slight modification of analogous sequence constructed in [NRS98] (see page number 304 of [NRS98]).

Lemma 4.0.9. *For all real numbers $x > a_0(A)$ the interval $(x, 2x]$ contains an element of the set A.*

Proof. Let a be the largest element of A not exceeding x. Then $a \geq a_0(A)$ so that the integer $n = a + a$ is $> n_0(A)$. It now follows that there is a pair (c,d), with $c \leq d$, of elements of A distinct from the pair (a,a) such that $n = c+d$. Since $d \geq c$ this implies that $d > a$ whence $d > x$ by the choice of a. Clearly we have $d \leq n = a + a \leq 2x$. In summary, we have verified that the element d of A lies in $(x, 2x]$. □

l-good interval: An interval $I = [k, k+l]$ is defined to be l-good if $I \cap A = \{k+l\}$; that is, it is of length l, the last element is in A and no other element is in A.

Lemma 4.0.10. *Let Y be a sufficiently large real number and $|A(Y)| \leq (\ln Y)^2$. Then for any real number b such that $1 \leq b \leq \frac{Y}{2(\ln Y)^{10}}$ there exists b-good interval in $[b(\ln Y)^5, 2b(\ln Y)^{10}]$.*

Proof. We consider interval $C = [b(\ln Y)^5, b(\ln Y)^{10}]$. Then the length of C is at least $\frac{1}{2}b(\ln Y)^{10}$ for all Y sufficiently large, but

$$|C \cap A| \leq |A(Y)| \leq (\ln Y)^2 < \frac{1}{2}(\ln Y)^{10}.$$

Therefore there exists in C a closed interval I of length b and void of A. Moving I to right till it hits A, we get a b-good interval I'. Using Lemma 4.0.9 it follows that $I' \subset [b(\ln Y)^5, 2b(\ln Y)^{10}]$.

□

Lemma 4.0.11. *Let Y be a sufficiently large real number and $|A(Y)| \leq (\ln Y)^2$. Then there exists an increasing sequence $\{b_1, b_2, \ldots, b_m\} = B_Y$ of elements of A not exceeding $\sqrt{Y}$ and satisfying the following properties:*

(i) *For each $1 \leq i \leq m-1, b_{i+1} \geq b_i(\ln Y)^5$.*

(ii) *For each $1 \leq i \leq m-1, [b_{i+1} - b_i, b_{i+1})$ does not contain an element of the set A.*

(iii) *The number of terms m of sequence B_Y is at least $c\frac{\ln Y}{\ln \ln Y}$ where c is a positive absolute constant.*

Proof. We shall define $B_Y = \{b_1, b_2, \ldots, b_i, \ldots\}$ recursively. We set $b_1 = a_0(A)$. Suppose $b_1, b_2, \ldots, b_i$ have been determined and $b_i \leq \frac{1}{2}\frac{\sqrt{Y}}{(\ln Y)^{10}}$ then applying Lemma 4.0.10 we choose the smallest $a \in [b_i(\ln Y)^5, 2b_i(\ln Y)^{10}]$ such that $[a - b_i, a)$ does not contain any element of A. We set b_{i+1} to be a. The recursion is terminated if $b_i > \frac{1}{2}\frac{\sqrt{Y}}{(\ln Y)^{10}}$.

Let B_Y be a sequence constructed in manner described above. Clearly, (i) and (ii) hold for each $1 \leq i \leq m-1$. Further for each i we have that

$$b_{i+1} \leq 2b_i(\ln Y)^{10} < b_i(\ln Y)^{11}$$

whence by induction $b_m < a_0(A)(\ln Y)^{11m}$. Since recursion terminates at b_m we have $b_m > \frac{1}{2}\frac{\sqrt{Y}}{(\ln Y)^{10}}$. These remarks imply (iii).

□

In what follows, B_Y will denote the sequence constructed as in the proof of Lemma 4.0.11.

Proposition 4.0.12. *Let Y be a sufficiently large real number and $|A(Y)| \leq (\ln Y)^2$. Let b be any real number such that $[b, b(\ln Y)^{11}) \subset (\sqrt{Y}, Y)$. Then the number of elements of A contained in the interval $[b, b(\ln Y)^{11})$ is $> c(\frac{\ln Y}{\ln \ln Y})^{\frac{1}{2}}$ where c is a positive absolute constant.*

Proof. Lemma 4.0.10 implies that there is an element a of the set A lying in the interval $[b, 3b(\ln Y)^{10})$ such that the interval $[a-b, a)$ does not contain any element of A. We choose one such a.

Let S denote the set of elements of A in the interval $[b, b(\ln Y)^{11})$ and s denote the cardinality of S. Let S_1 and S_2 denote the sets of elements of A in the intervals $[b, a)$ and $[a, b(\ln Y)^{11})$ respectively and let s_1 and s_2 denote the cardinalities of S_1 and S_2 respectively. We then have $s = s_1 + s_2$.

For each i, $1 \le i \le m$, let $n_i = a + b_i$, where B_Y is a sequence supplied by Lemma 4.0.11. Since each $n_i \ge Y^{1/2}$, we see that when Y is sufficiently large, each n_i is $\ge n_0(A)$. For each i we then choose a pair (c_i, d_i), with $d_i \ge c_i$, of elements of A distinct from the pair (a, b_i) such that $n_i = c_i + d_i$. For each i we then have either $d_i < a$ or $d_i > a$. Let P_1 denote the set of those pairs (c_i, d_i) with $d_i < a$ and P_2 the set of those pairs (c_i, d_i) with $d_i > a$. Let p_1 and p_2 denote the cardinalities of P_1 and P_2 respectively. We then have $p_1 + p_2 = m$.

If (c_i, d_i) is in P_1 we have $c_i \le d_i < a - b$ and hence that $d_i \ge c_i = a + b_i - d_i \ge a - (a - b) = b$. In other words, c_i and d_i are elements of S_1. It follows that $S_1 \times S_1$ contains P_1. Consequently, we have that $s_1^2 \ge p_1$ or that

$$s_1 \ge p_1^{1/2}. \tag{4.1}$$

If (c_i, d_i) is in P_2 we have $a < d_i$. Further, we have that

$$c_i + d_i = a + b_i \le 3b(\ln Y)^{10} + Y^{\frac{1}{2}} \le 3b(\ln Y)^{10} + b \le b(\ln Y)^{11}, \tag{4.2}$$

and hence that $d_i \le b(\ln Y)^{11}$. It follows that the mapping ϕ that associates (c_i, d_i) to d_i maps P_2 into S_2. Let us verify that ϕ is injective. Suppose to the contrary that (c_i, d_i) and (c_j, d_j) are elements of P_2 such that $d_i = d_j$ and $i < j$. Then

$$c_j \ge c_j - c_i = b_j - b_i \ge b_j - b_{j-1}\ . \tag{4.3}$$

Also $c_j < b_j$ because $c_j + d_j = a + b_j$ and $d_j > a$. It follows that the element c_j of A lies in the interval $[b_j - b_{j-1}, b_j)$ contradicting *(ii)* of Lemma 4.0.11. The injectivity of ϕ implies that $s_2 \ge p_2$.

In summary we have verified that

$$s = s_1 + s_2 \ge p_1^{1/2} + p_2 \ge p_1^{1/2} + p_2^{1/2} \ge (p_1 + p_2)^{1/2} \ge m^{1/2} \tag{4.4}$$

from which the proposition follows on recalling (iii) of Lemma 4.0.11. □

Corollary. *There exists an absolute constant $c > 0$ with the following property: For any infinite subset A of $\mathbb{N}$ such that $r(A, n) \neq 1$ for all sufficiently large natural numbers n , we have:*

$$|A(Y)| \geq c\,(\frac{\ln Y}{\ln\ln Y})^{\frac{3}{2}}.$$

Proof. The corollary follows from Proposition 4.0.12 on noting that if Y is sufficiently large then for some positive absolute constant c the interval $[(Y)^{\frac{1}{2}}, Y]$ contains at-least $c\frac{\ln Y}{\ln\ln Y}$ disjoint intervals of the form $[b, b(\ln Y)^{11})$.

□

Result in Proposition 4.0.12 can be improved and we have Proposition 4.0.14. Rest of arguments being the same, Proposition 4.0.14 follows by improving inequality 4.1 in Proposition 4.0.12 using Lemma 4.0.13. We shall first just state Lemma 4.0.13 and deduce Proposition 4.0.14. Later we shall prove Lemma 4.0.13 which require a few other Lemmas.

Lemma 4.0.13. *With notations and assumptions as in Proposition 4.0.12 we have $|[b, a) \cap A| \geq\ c\ |P_1|$, where c is a positive absolute constant.*

Proposition 4.0.14. *Let Y be a sufficiently large real number and $|A(Y)| \leq (\ln Y)^2$. Let b be any real number ≥ 1 such that $[b, b(\ln Y)^{11}) \subset (\sqrt{Y}, Y)$. Then the number of elements of A contained in the interval $[b, b(\ln Y)^{11})$ is $> c(\frac{\ln Y}{\ln\ln Y})$ where c is an positive absolute constant.*

Proof. Notice that assumptions of Propositions 4.0.12 are satisfied here. Then arguing as in proof of Proposition 4.0.12 and using Lemma 4.0.13 in place of inequality 4.1 Proposition 4.0.14 follows. □

Lemma 4.0.15 and 4.0.17 are required for proving Lemma 4.0.13.

Lemma 4.0.15. *Let $B_Y = \{b_1, b_2, \ldots, b_m\}$ be a sequence as constructed in Lemma 4.0.11. Suppose $\sum_{i=1}^{n} x_i b_i = 0$ where $1 \leq n \leq m$ and $x_i \in \{1, -1, 0, 2, -2\}$ for all $1 \leq i \leq n$. Then $x_i = 0$ for all i.*

Proof. Suppose it is not true and there exist sequence $\{x_i\}$ such that $\sum_{i=1}^{n} x_i b_i = 0$ where $1 \leq n \leq m$ and x_i is not zero for some i. Without loss of generality we may assume that $x_n \neq 0$. Then

$$x_n b_n = \sum_{i=1}^{n-1} -x_i b_i.$$

As $n < m < |A(Y)| < (\ln Y)^2$ so $b_n \leq |x_n b_n| < 2(\ln Y)^2 b_{n-1}$. But by construction of B_Y, $b_n \geq (\ln Y)^5 b_{n-1}$. Hence there is a contradiction. □

Let us recall some definitions from graph theory which we need for our purpose. A graph G consists of a finite nonempty set $V = V(G)$ of vertices together with a prescribed set X of unordered pairs of elements of V. Each pair $x = \{u, v\}$ is an edge of G and is said to join u and v. Notice that a graph thus defined is a finite undirected graph without multiple edges but may have loops. A walk of a graph G is an alternating sequence of vertices and edges $v_1, x_1, v_2, \ldots, v_{n-1}, x_{n-1}, v_n$, beginning and ending with vertices, in which each edge joins two vertices immediately preceding and following it. It is closed if $v_1 = v_n$. It is a trail if all the edges are distinct. By an *even closed trail* we shall mean a trail which is closed and have even number of edges. A cycle is a closed trail in which all the vertices are distinct. Two trails which define the same subgraph are considered equivalent and are not distinguished.

Lemma 4.0.16. *Let G be a graph with no loops and no even closed trails. Then any two distinct closed trails in G are disjoint, that is, if T_1, T_2 are two distinct closed trails in G and $V(T_1)$, $V(T_2)$ denote the set of vertices in T_1, T_2 respectively then $V(T_1) \cap V(T_2) = \emptyset$.*

Proof. Suppose it is not true. Then there exist two distinct closed trails T_1, T_2 in G such that $V(T_1) \cap V(T_2) = V_c$ (say) $\neq \emptyset$. As T_1, T_2 are two distinct trails so there is an edge in at-least one of them which is not common to both of them. Say x is one such edge and without loss of generality we may assume it is in T_1. Suppose $T_1 = v_1, x_1, v_2, x_2, v_3, \ldots, v_i, x_i, v_{i+1}, \ldots, v_{n-1}, x_n, v_n$. As $V_c \neq \emptyset$ so we may assume that $v_1 = v_n \in V_c$. Then if we choose $v_l \in V(T_2)$ nearest to left of x and $v_r \in V(T_2)$ nearest to right, in sequence for T_1 thus considered, then only vertices which $T = v_l, x_l, v_{l+1}, \ldots, v_{r-1}, x_{r-1}, v_r$ share with T_2 are v_l and v_r. (It is possible that v_l is same as v_r.) Also then by choice of x, v_l, v_r the trail T doesn't have any common edge with T_2. As $v_l, v_r \in V(T_2)$ so there is a trail T'' in T_2 starting from v_l and ending with v_r.

Now by choice of T we have that $T_u = T \cup T''$ is a closed trail. Also again by choice of T we have that $T_r = (T_2 \setminus T'') \cup T$ is another closed trail. (Notice that it may be so that $(T_2 \setminus T'')$ is empty but that doesn't affect our arguments.) Now it's clear that either T_u or T_r has an even number of edges depending on whether number of edges of T and T'' have same parity or different parity. But this is contrary to assumption that G has no even-closed trail. $\square$

Lemma 4.0.17. *Let G be a graph with n vertices and having no loops. Further assume that G has no even closed trail. Then number of edges in G, say $e(G)$, is at most $2n$.*

Proof. It is clearly enough to prove lemma in case when G is connected. From previous lemma no closed trail in G has a proper closed sub-trail. This implies that any closed trail is a cycle and any two cycles are disjoint. So G can't have more than n cycles. Now we shall show that $d(G) = e(G)-$ number of vertices is at most n and this proves the lemma. If we shrink all cycles in G to get new graph G' then G' has no cycle and is connected. So G' is a tree. But then $d(G') = -1$. Also as cycles in G are disjoint so $d(G) = d(G')$ + number of cycles in G. This implies that $d(G) \leq n - 1$. $\square$

Lemma 4.0.13. With notations and assumptions as in Proposition 4.0.12 we have

$$|[b, a) \ \cap \ A| \ \geq \ c \ |P_1|,$$

where c is a positive absolute constant.

Proof. From Proposition 4.0.12 we recall that the set P_1 consists of pairs (c_j, d_j) of elements of the set A such that $c_j \leq d_j < a$. Also for each pair (c_j, d_j) belonging to the set P_1 there is exactly one term b_j of the sequence B_Y such that $c_j + d_j = a + b_j$. Let S_1 denote the set of elements of A lying in interval $[b, a)$, that is, $S_1 = [b, a) \ \cap \ A$. Then it was shown in Proposition 4.0.12 that $P_1 \subset S_1 \times S_1$.

We shall construct a graph G associated to the set P_1. As $P_1 \subset S_1 \times S_1$ we define $f_1 : \ P_1 \to S_1$ and $f_2 : \ P_1 \to S_1$ by $f_1(c_i, d_i) = c_i$, $f_2(c_i, d_i) = d_i$. The set of vertices of graph G, let say V, consists of those elements v of S_1 such that either v belongs to image of f_1 or of f_2. Then we have following upper bound on number of vertices of G.

$$|V| = n \leq |\text{Image of } f_1| + |\text{Image of } f_2| \leq 2|S_1| = 2|[b, a) \cap A|. \tag{4.5}$$

The set of edges of G (say X) consists of those unordered pair $\{v_1, v_2\}$ of V such that either (v_1, v_2) or $(v_2, v_1) \in P_1$. In other words two vertices v_1 and v_2 are joined by an edge if and only if either (v_1, v_2) or $(v_2, v_1) \in P_1$. The graph G thus constructed satisfy following properties:

(i) There is a natural one-one correspondence between edges of G and elements of P_1.

(ii) If x is an edge in G joining vertices v_1 and v_2 then there is a term b_x in the sequence B_Y such that $v_1 + v_2 = a + b_x$.

(iii) For two distinct edges x and y, the corresponding b_x and b_y given as above are distinct.

All these properties are easily verified using definition of G and P_1. So (i) in particular implies that number of edges in G is same as number of elements in P_1. Then to prove the Lemma it is enough to show that

$$\text{number of edges in } G = e(G) \leq cn \text{ for some positive absolute constant c.} \tag{4.6}$$

Now G can have at most n loops. So if we remove all loops from G to get another graph G_1 then to show (4.6) it is enough to show that

$$e(G_1) \leq cn \text{ for some positive absolute constant c .}$$

We claim that G_1 doesn't have any even closed trail. Then using claim and Lemma 4.0.17 we have (4.6).

Suppose claim is not true and G_1 has an even closed trail

$$T = v_1, x_1, v_2, x_2, v_3, \ldots, v_i, x_i, v_{i+1}, \ldots, v_{2m-1}, x_{2m-1}, v_{2m}, x_{2m}, v_1$$

where v_i is a vertex of G and x_i is an edge joining vertices immediately preceding and following it. Also by definition of trail we have, for $1 \leq i, j \leq 2m$ and $i \neq j$, $x_i \neq x_j$. Then using property (ii) of G we have

$$\begin{aligned} v_i + v_{i+1} &= a + b_i, \text{ where } 1 \leq i \leq 2m - 1 \\ v_{2m} + v_1 &= a + b_{2m}, \end{aligned}$$

where $b_i \in \{b_i\}$ for all $1 \leq i \leq 2m$. Further using property (iii) of G it follows that for $1 \leq i, j \leq 2m$ and $i \neq j$ we have $b_i \neq b_j$. Now we have

$$\sum_{i=1}^{2m-1} (-1)^i (v_i + v_{i+1}) = \sum_{i=1}^{2m-1} (-1)^i (a + b_i) \tag{4.7}$$

$$v_{2m} + v_1 = a + b_{2m} \tag{4.8}$$

Adding (4.7) and (4.8) we get

$$0 = \sum_{i=1}^{2m} (-1)^i b_i$$

which is a contradiction to Lemma 4.0.15. $\square$

Bibliography

[BP04] R. Balasubramanian and Gyan Prakash. On an additve representation function. *Journal of Number theory*, 104:327–334, 2004.

[DT89] A. Davydov and L. Tombak. Quasi-perfect linear binary codes with distance 4 and complete caps in projective geometry. *Problemy Peredachi Informatzii*, 25(4):11–23, 1989.

[DY69] P.H. Diananda and H.P. Yap. Maximal sum-free sets of elements of finite abelian groups. *Proc. Japan Acad*, 45:1–5, 1969.

[GR05] B.J. Green and I. Z. Ruzsa. Sum-free sets in abelian groups. *Israel J. Math*, 147:157–189, 2005.

[Lev] V. F. Lev. Large sum-free sets in $\mathbb{Z}/p\mathbb{Z}$. *Israel J. Math.* to appear.

[Lev05] V.F. Lev. Large sum-free sets in ternary spaces. *Journal of Combinatorial Theory, Series A,*, 111(2):337–346, 2005.

[Nat91] Melvyn B. Nathanson. *Additive number theory Inverse problems and the geometry of sumsets*. Springer GTM, 165, 1991.

[NRS98] J.-L. Nicolas, I. Z. Ruzsa, and A. Sárközy. On the parity of additive representation functions. *Journal of Number Theory*, 73(292-317), 1998.

[oHP04] Yahya ould Hamidoune and Alain Plagne. A new critical pair theorem applied to sum-free sets in abelian groups. *Comment. Math. Helv.*, 79:183–207, 2004.

[RS74] A.H. Rhemtualla and A.P. Street. Maximal sum-free sets in finite abelian groups. *Bull. Austral. Math. Soc.*, 2:289–267, 1974.

[Yap72] H.P. Yap. Maximal sum-free sets in finite abelian groups iv. *Nanta. Math.*, 5(3):70–75, 1972.

[Yap75] H.P. Yap. Maximal sum-free sets in finite abelian groups v. *Bull. Austral. Math. Soc.*, 13(3):337–342, 1975.