Centro de Ciências Exatas
Universidade Estadual de Maringá
Programa de Pós-Graduação em Matemática
(Mestrado)

Representações Aditivas em Grupos Abelianos Finitos

Adriana Wagner

Orientador: Prof. Dr. Emerson Luiz do Monte Carmelo

Maringá - PR
2008

Aos meus pais, Dejaime e Elza, ao meu irmão Junior e ao meu namorado, José Luiz com imenso carinho.

Agradecimentos

Novamete agradeço a Deus por tudo. Aos meus pais e ao meu irmão pela confiança a mim depositada e ao meu namorado José Luiz.

Agradeço as pessoas que me proporcionaram esses momentos de alegria e também às pessoas que me ajudaram nas horas de fraqueza. Em especial aos amigos Luciemy, Frederico, Orlando e Cleverson.

Agradeço aos professores do Departamento de Matemática da UEM pelo auxílio na construção do meu conhecimento, em especial ao professor Emerson Luiz do Monte Carmelo, pela orientação, disponibilidade e paciência.

E finalmente aos programas da CAPES e Fundação Araucária pelo suporte financeiro.

Resumo

Nesse trabalho, apresentaremos algumas formas de expressar os elementos de um dado grupo abeliano G como elemento de conjuntos soma ou como soma de termos de uma dada sequência. Exibiremos diversos tipos de problemas diretos, como o Teorema de Cauchy-Davenport e o Teorema de Chowla e também problemas inversos, como o Teorema de Vosper. A representação de elemento como soma de termos de um sequência surge com o Teorema de Erdös-Ginzburg-Ziv. No teorema de Mann, uma sequência de comprimento $2p-1$ em $\mathbb{Z}_p$ representa pelo menos uma vez todos os elementos do grupo. No Teorema de Gao, temos um refinamento do Teorema de Mann. Através da constante de Davenport, um limite inferior para o comprimento de uma sequência de modo que esta represente o elemento neutro do grupo é estudado, principalmente no grupo formado por d cópias de $\mathbb{Z}_n$.

Abstract

In this work, we will present some forms to write the elements of a given abelian group G as element of sum sets or as element of sum of the terms of one given sequence. We will show several types of direct problems, for instance, the Theorem of Cauchy-Davenport and Theorem of Chowla, and inverse problems as the Theorem of Vosper. The representation of a element as sum of terms of a sequence appears with the Theorem of Erdös-Ginzburg-Ziv. From the theorem of Mann, a sequence of length $2p-1$ in $\mathbb{Z}_p$ represents at least one time every element of this group. Thus the Theorem of Gao, may be considered as a refinement of the Theorem of Mann. By using Davenport constant, lower bound on the length of a sequence such that it represents the identity element of the group is investigated, mainly it is studied in the group formed for d copies of $\mathbb{Z}_n$.

Índice de Notações

$\emptyset$	conjunto vazio.
(m, n)	máximo divisor comum entre m e n.
$[a, b]$	intervalo fechado de extremos a e b.
$\langle x \rangle$	subgrupo gerado por x.
$\lfloor x \rfloor$	função menor inteiro.
$\mathbb{Z}$	conjunto dos números inteiros.
$\mathbb{Z}_n$	conjunto das classes de congruência módulo n.
$\|A\|$	cardinalidade do conjunto A.
$S_h(A)$	todas as somas de h elementos distintos de A.
$S(A)$	todas as somas arbitrárias de A.
$s(A)$	soma de todos os elementos de A.
$max(A)$	máximo elemento de A.
$min(A)$	mínimo elemento de A.
$\bar{A}$	complementar de A.
$K \times H$	produto direto de K por H.
$K \oplus H$	soma direta de K por H.
$H \leq K$	H subgrupo de K.
$D(G)$	constante de Davenport de um grupo G.
$\|G : H\|$	índice do subgrupo H em G.
$\circ(x)$	ordem do elemento x.
$A \subset B$	A é um subconjunto próprio de B.
$A \subseteq B$	A é um subconjunto de B.

$a \mid b$	a divide b.
$a \nmid b$	a não divide b.
$A + B$	conjunto soma.
$r_{A+B}(g)$	número de representações de g em $A + B$.
$f_S(k)$	número mínimo de elementos representados por S.
$v_a(S)$	número de ocorrência de a na sequência S.
$\sigma(S)$	soma dos termos da sequência S.
$\mathbb{Z}(G)$	anel de grupo G sobre $\mathbb{Z}$.
$\frac{G}{H}, G/H$	grupo quociente de G por um subgrupo normal H.

Sumário

Introdução

Na Grécia Antiga, Pitágoras ilustrou a representação de quadrados como soma de 2 quadrados. A formulação desta representação baseada em soma de conjuntos deu origem a Teoria Aditiva dos Números, cujo objtetivo atualmente consiste no estudo de soma de conjuntos em certas estruturas algébricas. Dados $h \geq 2$ e $A_1, A_2, ..., A_h$ conjuntos de inteiros, $A_1 + A_2 + ... + A_h$ denota o *conjunto soma*, ou seja, o conjunto de todos os inteiros representados na forma $a_1+a_2+...+a_h$, onde $a_i \in A_i$ para todo $i = 1, ..., h$. Dessa forma, Pitágoras procurava a partir dos conjuntos $A = \{x^2 : x \in \mathbb{Z}\}$ e $B = \{y^2 : y \in \mathbb{Z}\}$ encontrar em $A + B = \{x^2 + y^2 : x^2 \in A,\ y^2 \in B\}$ os números quadrados, gerando os chamados números pitagóricos, ou seja, os números naturais que satisfazem $z^2 = x^2 + y^2$.

Os clássicos problemas nessa teoria só apareceram a partir do século XIX e foram classificados em duas classes:

(i) os *problemas diretos*, nos quais a partir dos conjuntos $A_1, ..., A_h$, buscamos informações sobre o conjunto soma $A_1 + ... + A_h$;

(ii) os *problemas inversos*, onde através de propriedades do conjunto soma, deduzimos informaçõs sobre $A_1, ..., A_h$.

Um exemplo clássico da Teoria Aditiva dos Números é o teorema dos quatro quadrados de Lagrange, onde todo número inteiro não negativo pode ser escrito como a soma de no máximo quatro quadrados. Os conjuntos somas também foram definidos em grupos abelianos e assim resultados precursores foram obtidos.

Em 1813, Augustin Louis Cauchy prova o Teorema de Cauchy-Davenport, no qual dados A e B conjuntos de classes de congruência módulo p, apresenta-se um limite in-

ferior para a cardinalidade do conjunto soma $A + B$. Esse teorema também foi provado por Harold Davenport, em 1935, sem o conhecimento da demonstração de Cauchy. Em 1956, Vosper caracteriza nesse mesmo ambiente, os pares de conjuntos críticos, ou seja, os conjuntos tais que a cardinalidade do conjunto soma é menor que a soma de suas cardinalidades. Em 1961, ainda no âmbito da aritmética modular, Paul Erdös numa parceria com Abraham Ginzburg e Abraham Ziv, demonstram um simples mas importante teorema, o Teorema de Erdös-Ginzburg-Ziv, no qual qualquer sequência de comprimento $2n - 1$ de números inteiros possui uma subsequência de comprimento n cuja soma dos seus termos é congruente a zero módulo n.

A partir do Teorema de Erdös-Ginzburg-Ziv [4], surge uma nova forma de representar os elementos de grupos abelianos, a saber, os elementos do grupo são representados como soma de termos de uma dada sequência. Ainda em 1961, Roger Eggleton juntamente com Paul Erdös no artigo [3], apresentam condições sobre grupos abelianos escritos aditivamente, de modo que estes possuam sequências que representem os elementos do grupo. Esses resultados serão apresentados no terceiro capítulo. Em 1967, Henry Mann no artigo [12], demonstra que dada uma sequência de comprimento $2p - 1$ em um grupo de cardinalidade prima p, todo elemento do grupo é representado como soma dos termos de uma subsequência de comprimento p. Assim Gao em [5], exibe um refinamento desse teorema, que também será apresentado no terceiro capítulo.

Alguns anos depois, Paul Erdös e Harold Davenport formularam o seguinte problema:

> dado um grupo abeliano finito G, determinar o menor inteiro positivo t tal que toda sequência em G de comprimento pelo menos t possua uma subsequência que represente o elemento neutro de G.

Esse inteiro ficou conhecido como a constante de Davenport de G. Embora bastante estudada, poucas classes exatas são conhecidas. Em 1968, J. Olson [17] calculou o valor exato para o p-grupo $\mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times ... \times \mathbb{Z}_{p^{e_r}}$, onde p é um inteiro primo.

Esse trabalho é uma coletânea de resultados já conhecidos e esta dividido em cinco capítulos. No primeiro capítulo, *Somas de Conjuntos de Inteiros*, apresentaremos alguns resultados do tipo direto e inverso sobre conjuntos de números inteiros. No segundo

capítulo, *Alguns Teoremas Clássicos*, apresentaremos os teoremas de Chowla, Cauchy-Davenport, Erdös-Ginzburg-Ziv e Vosper, onde os três primeiros são problemas diretos e o último um problema inverso, todos no ambiente da aritmética modular. No terceiro capítulo, *Sequências em Grupos Abelianos Finitos*, apresentaremos uma nova maneira de representar os elementos de um dado grupo abeliano finito, através de sequências e também um refinamento do Teorema de Mann. No quarto capítulo, *Sequências Soma-Zero*, vários resultados sobre a constante de Davenport de um dado grupo abeliano finito serão apresentados. No último capítulo, *Função* $s_k(G)$, continuaremos com o propósito de estimar o limite inferior t, de modo que toda sequência de um grupo abeliano finito de comprimento no mínimo t, possua uma subsequência soma-zero com propriedade adicional.

Capítulo 1

Somas de Conjuntos de Inteiros

Na Teoria Aditiva dos Números, busca-se o estudo de soma de conjuntos de inteiros. Dados $h \geq 2$ e $A_1, A_2, ..., A_h$ conjuntos de inteiros, $A_1 + A_2 + ... + A_h$ denota o *conjunto soma*, ou seja, o conjunto de todos os inteiros representados na forma $a_1+a_2+...+a_h$, onde $a_i \in A_i$ para todo $i = 1, ..., h$. Considerando A um conjunto de inteiros e $A_i = A$ para todo i, denotamos o conjunto soma $A_1+A_2+...+A_h$ simplesmente por hA, representando o conjunto de todas as somas de h elementos de A, com repetições permitidas. Nesse capítulo, estaremos interessados em investigar resultados entre o conjunto A e o conjunto hA, quando este não admite repetições.

Na primeira seção, apresentaremos problemas diretos e inversos entre um dado conjunto A e o conjunto de todas as somas de h elementos distintos de A. Na segunda seção, continuaremos com o mesmo propósito, apresentaremos problemas diretos e inversos, mas agora fazendo a relação entre um conjunto A e o conjunto de todas as somas arbitrárias de elementos distintos de A. Neste capítulo, convencionaremos que A sempre denotará um conjunto finito de números inteiros e a referência é o artigo de Nathanson [16].

1.1 Somas de h elementos distintos

Nessa seção, a partir de um conjunto A definiremos o conjunto de todas as somas de h elementos distintos de A e exibiremos no primeiro teorema um limite inferior para a cardinalidade desse conjunto. No segundo teorema temos uma natureza inversa. Sob certa condição sobre a cardinalidade do conjunto de todas as somas de h elementos distintos de A, mostraremos que A é uma progressão aritmética.

Definição 1.1. Seja $A = \{a_0, a_1, ..., a_{k-1}\}$ um conjunto finito de números inteiros com $|A| = k$. Para algum subconjunto não vazio $A^{'}$ de A, o *subconjunto soma de* $A^{'}$ é a soma de todos os seus elementos, simbolicamente

$$s(A^{'}) = \sum_{a \in A^{'}} a. \tag{1.1}$$

Convencionaremos que $s(\emptyset) = 0$.

Definição 1.2. Dado $A = \{a_0, a_1, ..., a_{k-1}\}$ um conjunto de inteiros. Fixado h, $0 \leq h \leq k$, o *conjunto de todas as somas de h elementos distintos de A* é denotado por

$$S_h(A) = \{s(A^{'}) : A^{'} \subseteq A, |A^{'}| = h\}. \tag{1.2}$$

Exemplo 1.3. Dados $h = 2$ e $A = \{0, 1, 2, 3\}$ vem que

$$\begin{aligned} S_2(A) &= \{0+1, 0+2, 0+3, 1+2, 1+3, 2+3\} \\ &= \{1, 2, 3, 4, 5\} \end{aligned}$$

Claramente dado $A = \{a_0, a_1, ..., a_{k-1}\}$, $h = 0$, $h = 1$ e $h = k$ vem que $S_0(A) = \{0\}$, $S_1(A) = A$ e $S_k(A) = \{a_0 + a_1 + ... + a_{k-1}\}$, respectivamente. Notemos também que se $A^{'} \subseteq A$, e considerando $\overline{A^{'}}$ o complementar de $A^{'}$ em relação a A, resulta que

$$s(\overline{A^{'}}) = s(A) - s(A^{'}). \tag{1.3}$$

Lema 1.4. *Dados A um conjunto com k inteiros e $h = 0, ..., k$. Temos a seguinte bijeção,*

$$\psi : S_h(A) \longrightarrow S_{k-h}(A)$$

$$s(A^{'}) \longmapsto s(\overline{A^{'}}) = s(A) - s(A^{'})$$

Demonstração: De fato, sejam $s(A^{'}),\ s(A^{''}) \in S_h(A)$. Suponhamos que $\psi(s(A^{'})) = \psi(s(A^{''}))$, assim $s(\overline{A'}) = s(\overline{A''})$, ou ainda, $s(A) - s(A^{'}) = s(A) - s(A^{''})$. Isso resulta que $s(A^{'}) = s(A^{''})$, logo ψ é uma função injetora. Agora mostremos que ψ é sobrejetora. De fato, dado $s(A^{'}) \in S_{k-h}(A)$, vem que $|\bar{A}'| = h$, assim $\psi(s(\overline{A'})) = s(A^{'})$. Completando a demonstração. □

Do Lema 1.4 decorre que

$$|S_h(A)| = |S_{k-h}(A)|. \tag{1.4}$$

Exemplo 1.5. Observemos alguns exemplos do Lema 1.4:

(i) Dado A um conjunto de k inteiros. Se $h = 0$ ou $h = k$ obtemos que $h(k-h)+1 = 1$ e $|S_0(A)| = |S_h(A)| = h(k-h)+1 = 1$.

(ii) Dado A um conjunto de k inteiros. Se $h = 1$ ou $h = k-1$ vem que $h(k-h)+1 = k$ e $|S_1(A)| = |S_{h-1}(A)| = h(k-h)+1 = k$.

(iii) Fixados $h = 2$ e $k = 4$ vem que $h(k-h)+1 = 5$. Considere $A = \{a_0, a_1, a_2, a_3\}$ um conjunto de inteiros tais que $a_0 < a_1 < a_2 < a_3$. Assim $S_2(A) = \{a_0+a_1, a_0+a_2, a_0+a_3, a_1+a_2, a_1+a_3, a_2+a_3\}$ e com isso $5 \leq |S_2(A)| \leq 6$. Visto que

$$a_0 + a_1 < a_0 + a_2 < a_0 + a_3 < a_1 + a_3 < a_2 + a_3$$

e

$$a_0 + a_2 < a_1 + a_2 < a_1 + a_3.$$

Segue que $|S_2(A)| = 5$ se, e somente se, $a_0+a_3 = a_1+a_2$. Assim $A = \{a_0, a_1, a_2, a_2+a_1-a_0\}$ para todo $a_0 < a_1 < a_2$.

Dados a e b números inteiros, $[a, b]$ denotará o conjunto de números inteiros x tais que $a \leq x \leq b$.

Teorema 1.6. *Fixados $h \in [0, k]$ e A um conjunto de k inteiros, temos*

$$|S_h(A)| \geq hk - h^2 + 1. \tag{1.5}$$

Demonstração: Considere $A = \{a_0, a_1, ..., a_{k-1}\}$ com $a_0 < a_1 < ... < a_{k-1}$. Para $i = 0, 1, ..., k-h-1$ e $j = 0, 1, ..., h$, definimos

$$s_{i,j} = \sum_{\substack{t=0 \\ t \neq h-j}}^{h} a_{i+t} \tag{1.6}$$

e

$$s_{k-h,0} = \sum_{t=0}^{h-1} a_{k-h+t} \tag{1.7}$$

Observemos que cada número acima é uma soma de h elementos distintos de A, ou seja, $s_{i,j} \in S_h(A)$ para todo i e j. Além disso, para $i = 0, 1, ..., k-h-1$ e $j = 0, 1, ..., h-1$, vem que

$$s_{i,j+1} - s_{i,j} = a_{i+h-j} - a_{i+h-j-1} > 0$$

e

$$s_{i,h} = \sum_{t=1}^{h} a_{i+t} = \sum_{t=0}^{h-1} a_{i+1+t} = s_{i+1,0}$$

Assim, para todo $i = 0, 1, ..., k-h-1$ a desigualdade abaixo segue

$$s_{i,0} < s_{i,1} < ... < s_{i,h-1} < s_{i,h} = s_{i+1,0}. \tag{1.8}$$

Para cada i obtemos h elementos na desigualdade (1.8) e como $i = 0, 1, ..., k-h-1$ teremos $h(k-h)+1$ elementos. Como $s_{i,j} \in S_h(A)$, resulta que

$$|S_h(A)| \geq h(k-h)+1 = hk - h^2 + 1.$$

□

Exemplo 1.7. O limite apresentado no Teorema 1.6 é o melhor possível no sentido de que há situações onde o limite é otimal. Para ilustrarmos a otimalidade tome $A = [0, k-1]$, então

$$S_h(A) = \left[\binom{h}{2},\ hk - \binom{h+1}{2} \right] = \binom{h}{2} + [0, hk - h^2].$$

Logo $|S_h(A)| = hk - h^2 + 1$.

Definição 1.8. Dados A um conjunto e d um inteiro qualquer, definimos os conjuntos

$$\begin{aligned} d + A &= \{d + a : a \in A\} \ \ e \\ d * A &= \{da : a \in A\}. \end{aligned}$$

Observemos que a função $|S_h(A)|$ é um invariante afim de A. De fato, dados a e d inteiros e $d \neq 0$, temos que $S_h(a + d*A) = ha + d*S_h(A)$. Assim $|S_h(a + d*A)| = |S_h(A)|$.

Definição 1.9. Dados a_0 e d inteiros tal que $d \geq 1$, uma progressão aritmética com k termos é um conjunto da forma

$$\{a_0, a_0 + d, a_0 + 2d, ..., a_0 + (k-1)d\} = a_0 + d * [0, k-1]. \tag{1.9}$$

Vimos no Exemplo 1.7, que todo intervalo de comprimento k satisfaz a igualdade na equação (1.5). Segue de (1.9) e do fato acima, que toda progressão aritmética com k termos também atinge o limite inferior no Teorema 1.6. Notemos que no Exemplo 1.5, obtemos a igualdade na equação (1.5), mesmo quando os conjuntos não são progressões aritméticas como no caso do Exemplo 1.7. Assim temos o resultado abaixo.

Teorema 1.10. *Fixe $k \geq 5$ e $2 \leq h \leq k-2$. Se A é um conjunto de k inteiros tais que $|S_h(A)| = hk - h^2 + 1$, então A é uma progressão aritmética.*

Demonstração: Seja $A = \{a_0, a_1, ..., a_{k-1}\}$, onde $a_0 < a_1 < ... < a_{k-1}$. Como vimos na demonstração do Teorema 1.6, os elementos em $S_h(A)$ são da forma $s_{i,j}$, definidos nas equações (1.6) e (1.7). Tomando $i = 0, 1, ..., k-h-2$ e $j = 2, 3, ..., h$, temos que

$$s_{i,j} = \sum_{\substack{t=0 \\ t \neq h-j}}^{h-1} a_{i+t} + a_{i+h} \quad e$$

$$s_{i,1} < s_{i,2} < s_{i,3} < ... < s_{i,h} = s_{i+1,0} < s_{i+1,1}.$$

Agora considere os inteiros $u_{i,j} \in S_h(A)$ da seguinte forma

$$u_{i,j} = \sum_{\substack{t=0 \\ t \neq h+1-j}}^{h-1} a_{i+t} + a_{i+h+1}.$$

Observemos que

$$s_{i,1} < u_{i,2} < u_{i,3} < ... < u_{i,h} < s_{i+1,1},$$

disso $s_{i,j} = u_{i,j}$ e logo $a_{i+h-j} + a_{i+h} = a_{i+h-j} + a_{i+h+1}$ para todo $i = 0, 1, ..., k-h-2$ e $j = 2, 3, ..., h$. Assim

$$a_{i+h-j+1} - a_{i+h-j} \quad = \quad a_{i+h+1} - a_{i+h}$$

e

$$\begin{aligned} a_{i+1} - a_i &= a_{i+2} - a_{i+1} = ... \\ &= a_{i+h-2} - a_{i+h-3} \\ &= a_{i+h-1} - a_{i+h-2} \\ &= a_{i+h+1} - a_{i+h} \end{aligned}$$

para $i = 0, 1, ..., k-h-2$. Afirmamos que $a_{i+h} - a_{i+h-1} = a_{i+1} - a_i$. De fato, para i tal que $i \geq 1$, temos

$$\begin{aligned} a_{i+h} - a_{i+h-1} &= a_{i-1+(h+1)} - a_{i-1+h} \\ &= a_{i-1+(h-1)} - a_{i-1+(h-2)} \\ &= a_{i+h-2} - a_{i+h-3} \\ &= a_{i+1} - a_i. \end{aligned}$$

Resta o caso $i = 0$. Devemos provar que $a_h - a_{h-1} = a_1 - a_0$. Se $h < k-2$, então $1 \leq k-h-2$ e

$$\begin{aligned} a_h - a_{h-1} &= a_{1+(h-1)} - a_{1+(h-2)} \\ &= a_{1+(h-2)} - a_{1+(h-3)} \\ &= a_{h-1} - a_{h-2} \\ &= a_1 - a_0. \end{aligned}$$

Disso vem que $a_i - a_{i-1} = a_1 - a_0$ para todo $i = 0, 1, ..., k-1$ e assim A é uma progressão aritmética. Agora se $h = k-2$, pela equação (1.4), $|S_{k-2}(A)| = |S_2(A)| = 2(k-2)+1$. Finalmente, como $2 < k-2$ quando $k \geq 5$, decorre que A é uma progressão aritmética.□

Observemos que o teorema anterior é um tipo de problema inverso. Note também que os únicos casos onde os conjuntos satisfazem a igualdade no Teorema 1.6, mas não são progressões aritméticas estão ilustrados no Exemplo 1.5.

1.2 Somas arbitrárias de elementos distintos

Nessa seção, continuaremos com o propósito de apresentar problemas diretos e inversos com relação ao conjunto de todas as somas arbitrárias de elementos distintos de A. Notemos que anteriormente, considerávamos apenas as somas de exatamente h elementos distintos. Aqui consideraremos todas as somas arbitrárias de elementos distintos de A, independente do valor de h. Assim através do conjunto A obteremos informações da cardinalidade do conjunto de todas as somas arbitrárias de elementos distintos de A, resultando num problema direto. Da mesma forma, no problema inverso caracterizaremos a estrutura do conjunto A munido da cardinalidade do conjunto de todas as somas arbitrárias de elementos distintos de A.

Definição 1.11. Dado A um conjunto de inteiros, definimos o *conjunto de todas as somas arbitrárias de elementos distintos de* A por

$$S(A) = \bigcup_{h=1}^{k} S_h(A) = \{s(A') : \emptyset \neq A' \subseteq A\}.$$

Exemplo 1.12. Retomando o Exemplo 1.3, obtemos que

$$\begin{aligned} S(A) &= \{0, 1, 2, 3, 0+1, 0+2, 0+3, 1+2, 1+3, 2+3, 0+1+2, 0+1+3, 0 \\ &+ 1+2, 1+2+3, 0+1+2+3\} \\ &= \{0, 1, 2, 3, 4, 5, 6\}. \end{aligned}$$

O resultado abaixo é um problema direto, onde através de um conjunto A estimaremos o limite inferior para a cardinalidade de $S(A)$.

Teorema 1.13. *Tome $k \geq 2$. Se A é um conjunto de k inteiros positivos, então*

$$|S(A)| \geq \binom{k+1}{2}.$$

Se A é um conjunto de k inteiros não negativos e $0 \in A$ então

$$|S(A)| \geq 1 + \binom{k}{2}.$$

Demonstração: Considere $A = \{a_0, a_1, ..., a_{k-1}\}$, com $a_0 < a_1 < ... < a_{k-1}$. Para $h = 1, ..., k$, definimos

$$B_h = \{a_i + a_{k-h+1} + a_{k-h+2} + ... + a_{k-1} : i = 0, 1, ..., k-h\}. \tag{1.10}$$

Assim $B_h \subseteq S_h(A) \subseteq S(A)$ e $|B_h| = k - h + 1$. Agora analisemos dois casos:

1° caso: A é um conjunto de inteiros positivos. Obrigatoriamente, $a_0 \geq 1$ e pela definição de B_h, vem que $max(B_h) < min(B_{h+1})$. Mais ainda, $B_1, B_2, ..., B_k$ são dois a dois disjuntos, então

$$|S(A)| \geq \left|\bigcup_{h=1}^{k} B_h\right| = \sum_{h=1}^{k} |B_h| = \sum_{h=1}^{k}(k-h+1) = \binom{k+1}{2}.$$

2° caso: A é um conjunto de inteiros não negativos e $a_0 = 0$. Assim $S(A) = \{0\} \cup S(A\backslash\{0\})$ e $A\backslash\{0\}$ é um conjunto de inteiros positivos. Pelo 1° caso,

$$|S(A)| \geq 1 + |S(A\backslash\{0\})| \geq 1 + \binom{k}{2}.$$

□

Observemos que no Teorema 1.13 a presença do 0 no conjunto A é decisiva no cálculo da $|S(A)|$.

Exemplo 1.14. Notemos que o limite apresentado no Teorema 1.13 pode ser otimal. De fato, dados $k \geq 2$, $A_0 = [0, k-1]$ e $A_1 = [1, k]$, vem que

$$S(A_0) = \left[0, \binom{k}{2}\right] \text{ e } S(A_1) = \left[1, \binom{k+1}{2}\right].$$

Embora o Teorema 1.13 possa ser otimal, como vimos no Exemplo 1.14, um refinamento do limite inferior segue abaixo. Observe que novamente o elemento 0 tem um papel decisivo no cálculo da cardinalidade de $S(A)$. Para tanto $\lfloor x \rfloor$, denotará a parte menor inteira de x.

Teorema 1.15. *Fixe $k \geq 2$ e tome A um conjunto de k inteiros. Se $0 \in A$, então*

$$|S(A)| \geq \lfloor k^2/4 \rfloor + 1.$$

Se $0 \notin A$, temos

$$|S(A)| \geq \lfloor (k+1)^2/4 \rfloor + 1.$$

Demonstração: Considere inicialmente $|A| = 2$. Note que $|S(A)| = 2$ se $0 \in A$ e $|S(A)| = 3$ se $0 \notin A$. Suponhamos $k \geq 3$, nesse caso podemos assumir que A contém p inteiros positivos e n inteiros negativos. Pelo Teorema 1.13, o conjunto $S(A)$ contém pelo menos $\binom{p+1}{2}$ inteiros positivos e pelo menos $\binom{n+1}{2}$ inteiros negativos. Analisemos dois casos:

$1^\circ : 0 \in A$. Como $A \subseteq S(A)$ decorre que $k = p + n + 1$ e

$$\begin{aligned} |S(A)| &\geq \binom{p+1}{2} + \binom{n+1}{2} + 1 \\ &= \binom{p+1}{2} + \binom{k-p}{2} + 1 \\ &= p(p+1)/2 + (k-p)(k-p-1)/2 + 1 \\ &= (2p^2 + 2p - 2kp + k^2 - k + 2)/2 = p^2 - (k-1)p + (k^2 - k + 2)/2 \\ &= (p - (k-1)/2)^2 + (k^2+3)/4 \\ &\geq (k^2+3)/4 \end{aligned}$$

e assim $|S(A)| \geq (k^2+3)/4$, como $|S(A)|$ é um número natural, obtemos

$$|S(A)| \geq \lfloor k^2/4 + 3/4 \rfloor + 1 = \lfloor k^2/4 \rfloor + 1.$$

$2^\circ : 0 \notin A$. Logo $k = p + n$ e consideremos p_0 o menor inteiro positivo em A e $-n_0$ o maior inteiro negativo em A. Novamente pelo Teorema 1.13, o conjunto $S(A)$ contém pelo menos $\binom{p+1}{2}$ inteiros positivos maiores do que ou iguais a p_0 e $\binom{n+1}{2}$ inteiros negativos menores do que ou iguais a $-n_0$. Mais ainda, o elemento $p_0 - n_0$ pertence a $S(A)$ e como $-n_0 < p_0 - n_0 < p_0$, vem que

$$\begin{aligned} |S(A)| &\geq \binom{p+1}{2} + \binom{n+1}{2} + 1 = \binom{p+1}{2} + \binom{k-p+1}{2} + 1 \\ &= (p(p+1))/2 + (k-p+1)(k-p)/2 + 1 = (2p^2 - 2kp + k^2 + k + 2)/2 \\ &= p^2 - kp + (k^2+k+2)/2 = (p - k/2)^2 - k^2/4 + (k^2+k+2)/2 \\ &= (p-k/2)^2 + (k^2+2k+4)/4 = (p-k/2)^2 + ((k+1)^2+3)/4 \\ &\geq ((k+1)^2+3)/4. \end{aligned}$$

Novamente como $|S(A)|$ é um número natural, obtemos $|S(A)| \geq \lfloor (k+1)^2/4 + 3/4 \rfloor + 1 = \lfloor (k+1)^2/4 \rfloor + 1$, como queríamos demonstrar. □

Exemplo 1.16. Os limites apresentados no Teorema 1.15 são atingidos por classes infinitas. De fato, primeiramente tome $k = 2m$ um inteiro par e $A = [-m, m-1]$, então $|A| = k$, $0 \in A$ e $S(A) = [-\binom{m+1}{2}, \binom{m}{2}]$. Assim

$$|S(A)| = \binom{m+1}{2} + \binom{m}{2} + 1 = m^2 + 1 = \lfloor k^2/4 \rfloor + 1.$$

Se $A = [-m, m]\backslash\{0\}$, então $|A| = k$, $0 \notin A$ e $S(A) = [-\binom{m+1}{2}, \binom{m+1}{2}]$. Logo

$$|S(A)| = 2\binom{m+1}{2} + 1 = m^2 + m + 1 = \lfloor (k+1)^2/4 \rfloor + 1.$$

Agora tomando $k = 2m+1$ um inteiro ímpar. Se $A = [-m, m]$, então $|A| = k$, $0 \in A$ e $S(A) = [-\binom{m+1}{2}, \binom{m+1}{2}]$. Assim

$$|S(A)| = 2\binom{m+1}{2} + 1 = m^2 + m + 1 = (k^2+3)/4 = \lfloor k^2/4 \rfloor + 1.$$

Finalmente, se $A = [-m, m+1]\backslash\{0\}$, então $|A| = k$, $0 \notin A$ e $S(A) = [\binom{m+1}{2}, \binom{m+2}{2}]$. Logo

$$\begin{aligned} |S(A)| &= \binom{m+1}{2} + \binom{m+2}{2} + 1 = m^2 + 2m + 2 \\ &= \lfloor (k+1)^2/4 \rfloor + 1. \end{aligned}$$

Ao contrário da função $|S_h(A)|$, $|S(A)|$ não é invariante por translação. Pois dados $k \geq 3$, $A_0 = [0, k-1]$ e $A_1 = 1 + A_0 = [1, k]$ temos

$$|S(A_0)| = 1 + \binom{k}{2} < \binom{k+1}{2} = |S(A_1)|.$$

No entanto, $|S(A)|$ é invariante sobre a multiplicação por escalar, pois para $d \neq 0$, $S(d * A) = d * S(A)$ e assim $|S(d * A)| = |S(A)|$.

Os últimos dois resultados dessa seção são problemas inversos para $S(A)$, ou seja, encontraremos os conjuntos A que satisfazem os limites inferiores dos Teoremas 1.13 e 1.15. Além disso, mostraremos que esses conjuntos são múltiplos escalares de intervalos.

Teorema 1.17. *Dados $k \geq 3$ e d um inteiro positivo. Se A é um conjunto de inteiros positivos com $|S(A)| = \binom{k+1}{2}$, então $A = d * [1, k]$. Se A é um conjunto de inteiros não negativos com $0 \in A$ e $|S(A)| = 1 + \binom{k}{2}$, vem que $A = d * [0, k-1]$.*

Demonstração: Considere $A = \{a_0, a_1, ..., a_{k-1}\}$, com $a_0 < ... < a_{k-1}$.

1° caso. Suponha A um conjunto de inteiros positivos. Claramente $a_0 \geq 1$, logo da demonstração do Teorema 1.13 seque que

$$S(A) = \bigcup_{i=1}^{h} B_h.$$

Para $h = 1, ..., k-1$, temos

$$\begin{aligned} a_{k-h-1} &+ a_{k-h+1} + a_{k-h+2} + ... + a_{k-1} \\ &< a_{k-h} + a_{k-h+1} + a_{k-h+2} + ... + a_{k-1} = max(B_h) \\ &< a_0 + a_{k-h} + a_{k-h+1} + a_{k-h+2} + ... + a_{k-1} = min(B_{h+1}) \end{aligned}$$

e

$$\begin{aligned} a_{k-h-1} &+ a_{k-h+1} + a_{k-h+2} + ... + a_{k-1} \\ &< a_0 + a_{k-h-1} + a_{k-h+1} + a_{k-h+2} + ... + a_{k-1} \\ &< a_0 + a_{k-h} + a_{k-h+1} + a_{k-h+2} + ... + a_{k-1}. \end{aligned}$$

Decorre que

$$\begin{aligned} a_{k-h} &+ a_{k-h+1} + a_{k-h+2} + ... + a_{k-1} \\ &= a_0 + a_{k-h-1} + a_{k-h+1} + a_{k-h+2} + ... + a_{k-1} \end{aligned}$$

e assim para $h = 1, ..., k-1$, obtemos $a_{k-h} = a_0 + a_{k-h-1}$. Logo

$$a_0 = a_1 - a_0 = a_2 - a_1 = ... = a_{k-1} - a_{k-2},$$

fazendo $d = a_0$ obtemos $A = d * [1, k]$.

2° caso. A é um conjunto de inteiros não negativos e $a_0 = 0$. Assim $A\backslash\{0\}$ é um conjunto de $k-1$ inteiros positivos e $S(A\backslash\{0\})$ é um conjunto de inteiros positivos. Como $S(A) = \{0\} \cup S(A\backslash\{0\})$, vem que

$$|S(A\backslash\{0\})| = \binom{k}{2},$$

tomando $d = a_1 \geq 1$, pelo caso anterior, $A\backslash\{0\} = d * [1, k-1]$. Portanto $A = d * [0, k-1]$, completando a demonstração. □

Teorema 1.18. *Fixado $k \geq 3$, considere A um conjunto de k inteiros. Se $0 \in A$ e $|S(A)| = \lfloor k^2/4 \rfloor + 1$, então existe um inteiro não nulo d tal que*

$$A = \begin{cases} d * [-m, m] & se \quad k = 2m+1, \\ d * [-m, m-1] & se \quad k = 2m. \end{cases}$$

Se por outro lado, $0 \notin A$ e $|S(A)| = \lfloor (k+1)^2/4 \rfloor + 1$, então existe um inteiro não nulo d tal que

$$A = \begin{cases} d * [-m, m] \backslash \{0\} & se \quad k = 2m, \\ d * [-m, m+1] \backslash \{0\} & se \quad k = 2m+1. \end{cases}$$

Demonstração: Como no Teorema 1.15 e pelas condições impostas sobre $|S(A)|$, vamos supor que A contém p inteiros positivos e n inteiros negativos, onde $p,\ n \geq 1$. Se $0 \in A$, então $k = p + n + 1$ e novamente pela demonstração do Teorema 1.15

$$\begin{aligned} \lfloor k^2/4 \rfloor + 1 &= |S(A)| \\ &\geq \binom{p+1}{2} + \binom{n+1}{2} + 1 \\ &= \binom{p+1}{2} + \binom{k-p}{2} + 1 \\ &= (p - (k-1)/2)^2 + (k^2+3)/4 \\ &\geq (k^2+3)/4. \end{aligned}$$

Disso segue $|S(A)| = 1 + \binom{p+1}{2} + \binom{n+1}{2}$ e

$$p - (k-1)/2 = \begin{cases} 0 & \text{se} \quad k = 2m+1, \\ \pm 1/2 & \text{se} \quad k = 2m. \end{cases}$$

isto é,

$$p = \begin{cases} m & \text{se} \quad k = 2m+1, \\ m \text{ ou } m-1 & \text{se} \quad k = 2m. \end{cases}$$

Vamos considerar todos os casos acima. Suponha que $k = 2m+1$, então $p = n = m$. Como $|S(A)|$ contém exatamente $\binom{m+1}{2}$ inteiros positivos e $\binom{m+1}{2}$ inteiros negativos, segue do Teorema 1.17 que existem inteiros positivos p_0 e n_0 tais que a parte positiva de A é $p_0 * [1, m]$ e a parte negativa de A é $-n_0 * [1, m]$. Visto que $0,\ p_0 - n_0 \in S(A)$ e $-n_0 < p_0 - n_0 < p_0$, vem que $p_0 - n_0 = 0$. Tomando $d = p_0$ temos $A = d * [-m, m]$.

O caso $k = 2m$ é similar à primeira parte da demostração. Por outro lado, se $0 \notin A$, então $k = p + n$ e pelo Teorema 1.15

$$\begin{aligned} \lfloor (k+1)^2/4 \rfloor + 1 &= |S(A)| \geq \binom{p+1}{2} + \binom{n+1}{2} + 1 \\ &= \binom{p+1}{2} + \binom{k-p+1}{2} + 1 \\ &= (p - (k/2))^2 + ((k+1)^2 + 3)/4 \geq ((k+1)^2 + 3)/4 \end{aligned}$$

e a demostração prossegue como na primeira parte. □

Notemos que nesses últimos dois resultados, o elemento 0 também teve um papel importante, como observado anteriormente.

Capítulo 2

Alguns Teoremas Clássicos

No capítulo anterior apresentamos problemas diretos e inversos em $\mathbb{Z}$. Nesse capítulo, abordaremos esses problemas no ambiente da aritmética modular. Dados A e B subconjuntos de um grupo abeliano escrito aditivamente G, $A + B$ denotará o *conjunto soma* formado por elementos de G que são representados como soma de elementos de A e B. Na primeira seção, abordaremos tipos de problemas diretos, como veremos nos teoremas de I. Chowla e Cauchy-Davenport. No Teorema de Cauchy-Davenport estimaremos a cardinalidade do conjunto soma $A + B$, munido das cardinalidades de A e B. Esse teorema foi provado primeiramente por Cauchy em 1813, Davenport também o demonstra em 1935, sem o conhecimento que Cauchy já havia provado. Imediatamente, Chowla extende o Teorema de Cauchy-Davenport. Na segunda seção apresentaremos tipos de problemas inversos, como exemplo principal temos o Teorema de Vosper. Esse teorema foi apresentado em 1956, quando Vosper caracteriza os pares de *conjuntos críticos*, ou seja, os conjuntos tais que a cardinalidade do conjunto soma é menor do que a soma de suas cardinalidades.

Agora, dada S uma sequência de números inteiros, algumas questões podem ser levantadas, como por exemplo:

qual seria o comprimento desta sequência de modo que possua uma subsequência de comprimento n, cuja soma de seus termos é congruente a zero módulo n?

Esse problema foi enunciado e demonstrado em 1961, numa parceria de Erdös, Ginzburg e Ziv. Após esse resultado muitas relações entre sequências e a Teoria Aditiva dos Números foram obtidas, como veremos com mais detalhes nos últimos capítulos desse trabalho. A referência aqui é o livro de Nathanson [15]. Convencionaremos que G sempre denotará um grupo abeliano escrito aditivamente, a menos que se mencione o contrário e assim o elemento neutro de G é denotado por 0.

2.1 Teorema de I. Chowla e Teorema de Cauchy-Davenport

Como mencionado, nessa seção apresentaremos problemas diretos sobre os conjuntos soma. Utilizando as cardinalidades dos conjuntos A e B de um grupo abeliano finito G, obteremos informações sobre a cardinalidade do conjunto soma $A+B$. Os resultados principais dessa seção são os teoremas de I. Chowla e o teorema de Cauchy-Davenport, sendo o último um resultado clássico no estudo de problemas diretos no grupo de classes de congruência módulo p, para p primo e de muita utilidade na demonstração de outros resultados. Primeiramente apresentaremos algumas definições e resultados prévios.

Definição 2.1. Dado G um grupo abeliano escrito aditivamente, sejam A e B subconjuntos de G. A *soma* $A+B$ é o conjunto de todos os elementos de G que podem ser representados na forma $a+b$, com a e b elementos de A e B, respectivamente . Simbolicamente,

$$A+B=\{a+b : a\in A \, e \, b\in B\}. \tag{2.1}$$

Considerando $A=\{\bar{1},\bar{2},\bar{3}\}$ e $B=\{\bar{1},\bar{2},\bar{3},\bar{4}\}$ subconjuntos do grupo $\mathbb{Z}_6$, vem que $A+B=\{\bar{0},\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$. Observemos que $\bar{5}$ em $A+B$ é escrito como $\bar{1}+\bar{4}$, $\bar{2}+\bar{3}$ e $\bar{3}+\bar{2}$ o que nós leva à próxima definição.

Definição 2.2. Para todo elemento g em G, o *número de representações de g como soma de elementos de A e B*, é denotado por

$$r_{A+B}(g) = |\{g = a + b : a \in A \, e \, b \in B\}|. \tag{2.2}$$

Observemos que no exemplo anterior a soma das cardinalidades de A e B supera a cardinalidade de $\mathbb{Z}_6$ em uma unidade, mais ainda, todo elemento de $\mathbb{Z}_6$ é representado em $A + B$ pelo menos uma vez. Esse fato não é isolado, conforme lema abaixo.

Lema 2.3. *Dados A e B subconjuntos em G. Se $|A| + |B| \geq |G| + t$ então $r_{A+B}(g) \geq t$ para todo $g \in G$. Em particular, se $|A| + |B| > |G|$ então $A + B = G$.*

Demonstração: Para a primeira parte, fixado $g \in G$ consideremos o subconjunto $g - B = \{g - b : \ b \in B\}$ de G. Com isso $|G| \geq |A \cup (g - B)|$. Por hipótese e do fato que $|g - B| = |B|$, obtemos

$$|A \cap (g - B)| \geq |A| + |B| - |G| \geq t. \tag{2.3}$$

Assim $A \cap (g - B)$ possui pelo menos t elementos, ou seja, existem $a_1, a_2, ..., a_t \in A$ e $b_1, b_2, ..., b_t \in B$, tais que $a_i = g - b_i$ para todo $i = 1, 2, ..., t$. Ou ainda, $g = a_i + b_i$, para todo $i = 1, 2, ..., t$ e assim $r_{A+B}(g) \geq t$.

Para a segunda parte, desde que $A + B \subset G$, resta mostrarmos que $G \subset A + B$. Por hipótese $|A| + |B| \geq G + 1$, logo decorre da primeira parte que $r_{A+B}(g) \geq 1$ para todo $g \in G$. Isto é, todo elemento de G é escrito como soma de elementos de A e B. Assim $G \subset A + B$. O que completa a demonstração. □

Definição 2.4. Dados $g \in G$ e (A, B) um par ordenado de conjuntos em G, a g-transformação de (A, B) é o par ordenado $(A(g), B(g))$ onde $A(g) = A \cup (B + g)$ e $B(g) = B \cap (A - g)$.

Exemplo 2.5. Consideremos $\bar{2}$, $A = \{\bar{1}, \bar{3}, \bar{5}\}$ e $B = \{\bar{1}, \bar{5}, \bar{7}\}$ em $\mathbb{Z}_9$. Assim a $\bar{2}$-transformação do par (A, B) é o par $(A(\bar{2}), B(\bar{2}))$ tais que $A(\bar{2}) = A \cup \{\bar{0}, \bar{3}, \bar{7}\}$ e $B(\bar{2}) = B \cap \{\bar{1}, \bar{3}, \bar{8}\}$, isto é, $A(\bar{2}) = \{\bar{0}, \bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ e $B(\bar{2}) = \{\bar{1}\}$.

A g-transformação é de grande utilidade nas demonstrações de muitos resultados na Teoria Aditiva, como logo podemos observar. Esta satisfaz algumas propriedades descritas abaixo.

Lema 2.6. *Sejam A e B conjuntos não vazios, $g \in G$ e $(A(g), B(g))$ a g-transformação do par (A, B). Então*

(i) $A(g) + B(g) \subseteq A + B$,

(ii) $A(g) \backslash A = g + (B \backslash B(g))$.

(iii) Se A e B são conjuntos finitos, então $|A(g)| + |B(g)| = |A| + |B|$. Além disso, se $g \in A$ e $0 \in B$, então $g \in A(g)$ e $0 \in B(g)$.

Demonstração: (i) Seja $x \in A(g) + B(g)$, logo existem $a_1 \in A(g)$ e $b_1 \in B(g)$ tais que $x = a_1 + b_1$. Pela Definição 2.4, $a_1 \in A$ ou $a_1 \in (B + g)$, $b_1 \in B$ e $b_1 \in (A - g)$. Se $a_1 \in A$ e como $b_1 \in B$ vem que $x = a_1 + b_1 \in A + B$. Agora se $a_1 \in B + g$, existe $b \in B$ tal que $a_1 = b + g$ e tomando $b_1 \in A - g$ temos que $b_1 = a - g$ onde $a \in A$, logo $x = a_1 + b_1 = b + g + a - g = a + b \in A + B$. Portanto $A(g) + B(g) \subseteq A + B$.

(ii) Temos que

$$\begin{aligned} A(g)\backslash A &= \{x \in A(g) : \ x \notin A\} = \{x \in (B + g) : \ x \notin A\} \\ &= (B + g)\backslash A = \{b + g : b \in B, \ b + g \notin A\} = g + \{b \in B : b \notin A - g\} \\ &= g + \{b \in B : \ b \notin B(g)\} = \ g + (B\backslash B(g)). \end{aligned}$$

(iii) Suponhamos que A e B são finitos. Através da Definição 2.4, $A \subseteq A(g)$ e $B(g) \subseteq B$. Por (ii), obtemos

$$|A(g)| - |A| = |A(g)\backslash A| = |g + (B\backslash B(g))| = |B\backslash B(g)| = |B| - |B(g)|.$$

Assim $|A(g)| + |B(g)| = |A| + |B|$. Finalmente, se $g \in A$, vem que $0 \in A - g$. Por hipótese, $0 \in B$, logo $0 \in B \cap (A - g)$. Completando a demonstração. □

Nós próximos resultados enfocaremos o grupo $G = \mathbb{Z}_m$. Iniciaremos com um problema direto, isto é, a partir de certas condições e das cardinalidades dos conjuntos A e B em G, estimaremos um limite inferior para a cardinalidade do conjunto $A + B$.

Teorema 2.7. (**I. Chowla**) *Sejam A e B conjuntos não vazios de $\mathbb{Z}_m$, com $m \geq 2$. Se $\bar{0} \in B$ e $(b, m) = 1$, para todo $\bar{b} \in B \backslash \{0\}$, então*

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

Demonstração: Pelo Lema 2.3, o resultado é verdadeiro sempre que $|A| + |B| > m$. Podemos assumir que $|A|+|B| \leq m$ e assim $min(m, |A|+|B|-1) = |A|+|B|-1 \leq m-1$. Se $|A| = 1$ ou $|B| = 1$, o teorema também é verdadeiro. De fato, com $|A| = 1$, teremos $|A + B| = |B| = 1 + |B| - 1 = |A| + |B| - 1$.

Suponhamos que o teorema é falso, então existem A e B conjuntos de $\mathbb{Z}_m$ tais que $|A|, |B| \geq 2$, e $|A + B| < |A| + |B| - 1$. Em particular $A \neq \mathbb{Z}_m$, pois caso contrário, teríamos a contradição $|A| + |B| > m$. Dessa maneira, escolha o par (A, B) tal que a cardinalidade de B é mínina. Desde que $|B| \geq 2$, existe $\bar{b}^* \in B$, $\bar{b}^* \neq 0$. Consideremos dois casos:

1° caso: Se $\bar{a} + \bar{b}^* \in A$, para todo $\bar{a} \in A$. Recursivamente, $\bar{a} + j\bar{b}^* \in A$, para todo $j = 0, 1, 2, \cdots$. Como por hipótese $(b^*, m) = 1$, vem que $\bar{b}^*$ é um elemento inversível em $\mathbb{Z}_m$, logo para todo $j = 0, 1, ..., m-1$, $\bar{a} + j\bar{b}^*$ gera todo o grupo $\mathbb{Z}_m$ disso resulta que

$$\mathbb{Z}_m = \{\bar{a} + j\bar{b}^* : j = 0, 1, .., , m-1\} \subseteq A.$$

Assim $A = \mathbb{Z}_m$, o que é falso.

2° caso: Caso contrário existe um elemento $\bar{g} \in A$ tal que $\bar{g} + \bar{b}^* \notin A$. Pelo Lema 2.6, $|A(\bar{g}) + B(\bar{g})| \leq |A + B| < |A| + |B| - 1 = |A(\bar{g})| + |B(\bar{g})| - 1$. Como $\bar{g} \in A$ e $\bar{0} \in B$, decorre que $\bar{g} \in A(\bar{g})$, $\bar{0} \in B(\bar{g}) \subseteq B$ e $(b, m) = 1$, para todo $\bar{b} \in B(\bar{g}) \backslash \{\bar{0}\}$. Pelo fato que $\bar{g} + \bar{b}^* \notin A$, ou ainda, $\bar{b}^* \notin A - \bar{g}$ obtemos que $\bar{b}^* \notin B(\bar{g}) = B \cap (A - \bar{g})$. Assim, $|B(\bar{g})| < |B|$, o que contradiz a minimalidade da cardinalidade de B. Portanto o teorema é verdadeiro. □

As condições do Teorema 2.7 são essenciais. Pois caso contrário não há garantias do limite inferior. De fato, consideremos $A = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ e $B = \{\bar{0}, \bar{2}, \bar{4}\}$ em $\mathbb{Z}_8$, logo $A + B = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ e assim $|A + B| = 4 < min(8, |A| + |B| - 1)$.

Restringindo o Teorema de Chowla para o caso de $m = p$, onde p é um número primo, obtemos o Teorema de Cauchy-Davenport, que primeiramente foi provado por Cauchy

em 1813 e depois em 1935 por Davenport. A demonstração de Davenport ocorreu de maneira independente à de Cauchy. Este teorema é de grande utilidade na demonstração dos resultados seguintes.

Teorema 2.8. (**Cauchy-Davenport**) *Fixado p um número primo, A e B conjuntos não vazios de $\mathbb{Z}_p$. Então*

$$|A+B| \geq min(p, |A|+|B|-1) \tag{2.4}$$

Demonstração: Dado $\bar{b}^* \in B$ e $B' = B - \bar{b}^*$. Assim $|B'| = |B|$ e $|A+B'| = |A+B-\bar{b}^*| = |A+B|$. Como $\bar{0} \in B'$ e $(b,p) = 1$ para todo $\bar{b} \in B'\backslash\{\bar{0}\}$, podemos aplicar o Teorema de *I. Chowla* no par (A, B'), obtendo $|A+B| = |A+B'| \geq min(p, |A|+|B'|-1) = min(p, |A|+|B|-1)$. Como queríamos demonstrar. □

Exemplo 2.9. Dados $A = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ e $B = \{\bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ em $\mathbb{Z}_{11}$, vem que $A+B = \{\bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}\}\}$ e assim $|A+B| = 8 = |A|+|B|-1$ satisfazendo o Teorema 2.8.

Notemos no exemplo anterior que para dois conjuntos em $\mathbb{Z}_p$ o Teorema de Cauchy-Davenport é sempre verdadeiro. Mas dispondo de h conjuntos não vazios em $\mathbb{Z}_p$ podemos nos perguntar se o teorema também é válido. Essa questão é respondida no teorema abaixo, onde apresentamos uma generalização do Teorema de *Cauchy-Davenport*.

Teorema 2.10. *Tome $h \geq 2$ e p um número primo. Para quaisquer conjuntos $A_1, A_2, ..., A_h$ não vazios de $\mathbb{Z}_p$, vale*

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

Demonstração: Procederemos a demonstração por indução sobre h. O caso $h = 2$ decorre do Teorema de *Cauchy-Davenport*. Suponhamos que $h \geq 3$ e que o teorema é válido para quaisquer $h-1$ conjuntos de $\mathbb{Z}_p$. Tomemos $B = A_1 + A_2 + ... + A_{h-1}$, pela hipótese indutiva,

$$|B| = |A_1 + A_2 + ... + A_{h-1}| \geq min\left(p, \sum_{i=1}^{h-1} |A_i| - (h-1) + 1\right) = min\left(p, \sum_{i=1}^{h-1} |A_i| - h + 2\right),$$

assim

$$\begin{aligned}
|A_1 + A_2 + ... + A_h| &= |(A_1 + A_2 + ... + A_{h-1}) + A_h| \\
&= |B + A_h| \geq min(p, |B| + |A_h| - 1) \\
&\geq min\left(p, \left(\sum_{i=1}^{h-1} |A_i| - h + 2\right) + |A_h| - 1\right) \\
&= min\left(p, \sum_{i=1}^{h} |A_i| - h + 1\right).
\end{aligned}$$

□

Exemplo 2.11. Dados $h \geq 2$ e $k_1, k_2, ..., k_h$ inteiros positivos tais que $k_1 + k_2 + ... + k_h \leq p + h - 1$, consideremos $A_i = \{0, 1, ..., k_i - 1\} \subseteq \mathbb{Z}_p$. Assim $|A_i| = k_i$, $A_1 + A_2 + ... + A_h = \{0, 1, ..., k_1 + ... + k_h - h\} \subseteq \mathbb{Z}_p$ e $|A_1 + A_2 + ... + A_h| = \sum_{i=1}^{h} |A_i| - h + 1$. Com esse exemplo vemos que o resultado do Teorema 2.10 é o melhor possível.

Recordemos que no capítulo anterior nos conjuntos somas as repetições não eram permitidades, já nesse capítulo as repetições nos elementos dos conjuntos somas são aceitas. Também observemos que se no teorema anterior considerarmos A um conjunto com k inteiros e $A_i = A$ para todo $i = 1, 2, ..., h$ vem que $|A+...+A| = |S_h(A)| \geq kh-h+1$, ou seja, um limite inferior maior do que o apresentado no Teorema 1.6.

2.2 Teorema de Vosper

Nessa seção estudaremos problemas inversos na Teoria Aditiva dos Números. O resultado principal desta seção é o Teorema de Vosper, onde munido da cardinalidade do conjunto soma $A+B$ em G, obteremos informações sobre as estruturas de A e B. Iniciaremos com algumas definições e lemas que utilizaremos na demonstração do Teorema de Vosper.

Definição 2.12. Dados A e B subconjuntos finitos em G, dizemos que o par (A,B) é *crítico* quando $A+B \neq G$ e $|A+B| \leq |A|+|B|-1$.

Definição 2.13. Fixados A e B subconjuntos em G e $d \neq 0$, dizemos que A e B são *progressões aritméticas com mesma diferença d*, quando

$$A = \{a+id : i = 0, 1..., s-1\} \;\; e \;\; B = \{b+id : 0, 1..., t-1\} \tag{2.5}$$

onde s e t são os comprimentos das progressões A e B, respectivamente.

Lema 2.14. *Fixado (A,B) um par crítico em $\mathbb{Z}_p$ tal que*

$$min(|A|,|B|) \geq 2 \;\; e \;\; |A+B| = |A|+|B|-1 < p-1.$$

Considere $D = \overline{A+B}$, então $(D,-A)$ é um par crítico.

Demonstração: Denote $s = |A|$ e $t = |B|$. Como $s+t-1 \leq p-2$, vem que $|D| = |\overline{A+B}| = p-(s+t-1) \geq 2$. Afirmamos que $|D-A| = |D|+|-A|-1 = p-t$. De fato, pelo Teorema de *Cauchy-Davenport*,

$$|D-A| \geq min(p, |D|+|-A|-1) = min(p, p-t) = p-t.$$

Por outro lado, como $(A+B)\cap D = \emptyset$, decorre que $B\cap(D-A) = \emptyset$ e assim $D-A \subseteq \overline{B}$. Logo, $|D-A| \leq |\overline{B}| = p-|B| = p-t$. Como queríamos demonstrar. □

Lema 2.15. *Seja (A,B) um par crítico de $\mathbb{Z}_p$ tal que $|A| = s \geq 2$, $|B| = t \geq 3$, $\bar{0} \in B$ e $|A+B| = |A|+|B|-1 < p-1$. Então existe uma classe de congruência $\bar{g} \in A$ tal que a $\bar{g}$-tranformação $(A(\bar{g}), B(\bar{g}))$ é um par crítico, $A(\bar{g})+B(\bar{g}) = A+B$ e $2 \leq |B(\bar{g})| < |B|$.*

Demonstração: Considere $(A(\bar{g}), B(\bar{g}))$ a $\bar{g}$-transformação do par crítico (A, B), segue do Lema 2.6 e do Teorema 2.8 que

$$|A| + |B| - 1 = |A(g)| + |B(g)| - 1 \leq |A(g) + B(g)| \leq |A + B| = |A| + |B| - 1.$$

Portanto, $|A(\bar{g}) + B(\bar{g})| = |A(\bar{g})| + |B(\bar{g})| - 1$, ou seja, $(A(\bar{g}), B(\bar{g}))$ é também um par crítico. Desde que $A(g) + B(g) \subseteq A + B$, vem que $A(g) + B(g) = A + B$. Defina

$$X = \{\bar{g} \in A : B(\bar{g}) \neq B\}. \tag{2.6}$$

Como $B(\bar{g}) \subseteq B$ para todo $\bar{g} \in \mathbb{Z}_p$, vem que $|B(\bar{g})| < |B|$ para todo $\bar{g} \in X$. Afirmamos que $|X| \geq 2$. De fato, considere

$$Y = A \backslash X = \{\bar{g} \in A : B(\bar{g}) = B\}. \tag{2.7}$$

Analisemos as condições sobre o conjunto Y. Se $Y = \emptyset$, então $X = A$ e $|X| = |A| \geq 2$. Se $Y \neq \emptyset$, selecione $\bar{g} \in Y$, assim $B = B(\bar{g}) = B \cap (A - \bar{g})$ e logo $B \subseteq A - \bar{g}$. Disso decorre que $\bar{g} + B \subseteq A$ para todo $\bar{g} \in Y$, então $Y + B \subseteq A$. Pelo Teorema 2.8,

$$s = |A| \geq |Y + B| \geq min(p, |Y| + t - 1) = |Y| + t - 1 = s - |X| + t - 1,$$

consequentemente $|X| \geq t - 1 \geq 2$.

Agora mostraremos que $|B(\bar{g})| \geq 2$ para algum $\bar{g} \in X$. Visto que $\bar{g} \in X$ e $\bar{0} \in B$, temos $\bar{0} \in B(\bar{g})$. Suponhamos que $B(\bar{g}) = B \cap (A - \bar{g}) = \{\bar{0}\}$ para todo $\bar{g} \in X$. Considere $B' = B \backslash \{\bar{0}\}$, então $B' \cap (A - \bar{g}) = \emptyset$ e assim $(\bar{g} + B') \cap A = \emptyset$ para todo $\bar{g} \in X$. Portanto, $(X + B') \cap A = \emptyset$. Desde que $X + B' \subseteq A + B$, segue que $X + B' \subseteq (A + B) \backslash A$ e novamente pelo Teorema 2.8,

$$|X| + t - 2 = |X| + (t - 1) - 1 \leq |X + B'| \leq |A + B| - |A| = t - 1,$$

ou ainda, $|X| \leq 1$ o que gera uma contradição. Logo $2 \leq |B(g)| < B$. Completando a demostração. □

Notemos que nos dois lemas anteriores, apresentamos condições para que específicos pares ordenados de conjuntos sejam críticos. Agora nos três últimos lemas, antes do Teorema de Vosper, apresentaremos condições suficientes para que os conjuntos do par crítico (A, B) sejam progressões aritméticas com mesma diferença.

Lema 2.16. *Sejam A e B subconjuntos de $\mathbb{Z}_p$ tais que $min(|A|,|B|) \geq 2$ e $|A+B| = |A|+|B|-1 < p-1$. Se A é uma progressão aritmética, então B é uma progressão aritmética com mesma diferença.*

Demonstração: Denote $s = |A|$ e $t = |B|$. Como A é uma progressão aritmética, existem $\bar{a}_0 \in A$ e $\bar{d} \in \mathbb{Z}_p$, com $\bar{d} \neq \bar{0}$ tal que $A = \{\bar{a}_0 + i\bar{d} : \ i = 0, 1, ..., s-1\}$. Tomando $\bar{b}_0 \in B$ considere os subconjuntos

$$\begin{aligned} A' &= \{(\bar{a} - \bar{a}_0)\bar{d}^{-1} : \bar{a} \in A\} = \{i + p\mathbb{Z} : i = 0, 1, ..., s-1\} \ e \\ B' &= \{(\bar{b} - \bar{b}_0)\bar{d}^{-1} : \bar{b} \in B\}, \end{aligned}$$

logo A' e $B' \subseteq \mathbb{Z}_p$. Assim $\bar{0} \in B'$, $|A'| = |A| = s$, $|B'| = |B| = t$ com $s, t \geq 2$ e $A'+B' = \{(\bar{c}-\bar{a}_0-\bar{b}_0)\bar{d}^{-1} : \bar{c} \in A+B\}$. Logo $|A'+B'| = |A+B| = |A'|+|B'|-1 < p-1$. Em virtude do argumento acima, podemos assumir sem perda de generalidade que $A = A'$ e $B = B'$. Mostraremos que $B = \{\bar{b}, \bar{b}+\bar{1}, \bar{b}+\bar{2}, ..., \bar{b}+\overline{t-1}\}$ para algum $\bar{b} \in B$.

Seja $B = \{\bar{b}_0, \bar{b}_1, ..., \bar{b}_{t-1}\}$. Para $j = 0, 1, ..., t-1$, escolha $r_j = 0, ..., p-1$ tal que $\bar{b}_j = r_j + p\mathbb{Z}$. Reenumerando as classes de congruência $\bar{b}_j$ de maneira adequada, podemos assumir que $0 = r_0 < r_1 < ... < r_{t-1} < p$ e supor que $r_t = p$. Como todo elemento de $A+B$ é da forma $\bar{b}_j + i = r_j + i + p\mathbb{Z}$, para algum $i = 0, ..., s-1$ e $j = 0, ..., t-1$, segue que

$$A + B = \bigcup_{j=0}^{t-1} [r_j, r_j + min(s-1, r_{j+1} - r_j - 1)] + p\mathbb{Z}.$$

Desse modo os t conjuntos nessa união são dois a dois disjuntos. De fato, dados $0 \leq i < j \leq t-1$ observemos que

$$[r_i, r_i + min(s-1, r_{i+1} - r_i - 1)] \ \subset \ [r_i, r_i + r_{i+1} - r_i - 1] = [r_i, r_{i+1} - 1].$$

Da mesma forma

$$[r_j, r_j + min(s-1, r_{j+1} - r_j - 1] \ \subset \ [r_j, r_{j+1} - 1].$$

Assim $[r_i, r_{i+1} - 1] \cap [r_j, r_{j+1} - 1] = \emptyset$. Logo

$$\begin{aligned} s + t - 1 &= |A+B| = \sum_{j=0}^{t-1} (1 + min(s-1, r_{j+1} - r_j - 1)) \\ &= t + \sum_{j=0}^{t-1} min(s-1, r_{j+1} - r_j - 1). \end{aligned}$$

Vamos analisar a minimalidade entre $s-1$ e $r_{j+1}-r_j-1$. Primeiramente se $r_{j+1}-r_j-1 \leq s-1$ para todo $j=0,1,...,t-1$ vem que,

$$s+t-1 = t+\sum_{j=0}^{t-1}(r_{j+1}-r_j-1) = r_t - r_0 = p,$$

mas isso contradiz o fato de que $|A|+|B|-1 < p-1$. Assim existe $j_0 \in [0,t-1]$ tal que $r_{j_0+1}-r_{j_0}-1 > s-1$ e assim

$$s+t-1 = |A+B| = s+t-1+\sum_{j=0, j\neq j_0}^{t-1} min(s-1, r_{j+1}-r_j-1).$$

Disso, decorre que $r_{j+1}-r_j = 1$ para todo $j=0,..,t-1$, $j \neq j_0$ e portanto B corresponde a progressão aritmética da forma, $[r_{j_0+1}, r_{j_0+1}+t-1]+p\mathbb{Z}$. □

Lema 2.17. *Sejam A e B subconjuntos de $\mathbb{Z}_p$ tais que*

$$min(|A|,|B|) = 2 \ \ e \ \ |A+B| = |A|+|B|-1 < p-1.$$

Então A e B são progressões aritméticas com a mesma diferença.

Demonstração: Decorre do Lema 2.16, observando que um conjunto com dois elementos é uma progressão aritmética. □

Lema 2.18. *Seja (A,B) um par crítico em $\mathbb{Z}_p$ tal que $min(|A|,|B|) \geq 2$ e $|A+B| = |A|+|B|-1 < p-1$. Se $A+B$ é uma progressão aritmética, então A e B são progressões aritméticas com mesma diferença.*

Demonstração: Sendo $A+B$ uma progressão aritmética, então $D = \overline{A+B}$ também é uma progressão aritmética. Pelo Lema 2.14, o par $(D,-A)$ é crítico, assim pelo Lema 2.16, o conjunto $-A$ é uma progressão aritmética. Desse fato decorre que A é uma progressão aritmética, e desde que o par (A,B) é crítico, os conjuntos A e B são progressões aritméticas com mesma diferença. □

No Exemplo (2.9) vemos que $|A+B| = |A|+|B|-1$, ou seja, o par (A,B) é crítico. Note que A e B são progressões aritméticas com mesma diferença. Dessa forma, podemos

nos perguntar: se o par (A, B) é crítico então A e B são progressões aritméticas? Essa questão é respondida no Teorema de Vosper, um problema inverso que possibilita a caracterização dos pares críticos (A, B) em $\mathbb{Z}_p$. Observemos que o Teorema de Vosper é um inverso ao Teorema de Cauchy-Davenport.

Teorema 2.19. (**Vosper**) *Fixado p um número primo, sejam A e B conjuntos não vazios do grupo $\mathbb{Z}_p$ tais que $A + B \neq \mathbb{Z}_p$. Então*

$$|A + B| = |A| + |B| - 1$$

se, e somente se, uma das seguintes condições é verificada:

(i) $min(|A|, |B|) = 1$

(ii) $|A + B| = p - 1$ e $B = \overline{c - A}$, onde $c = G\backslash(A + B)$

(iii) A e B são progressões aritméticas com mesma diferença.

Demonstração: Pelo Lema 2.3, se $A + B \neq \mathbb{Z}_p$, então $|A| + |B| \leq p$. Primeiramente assumiremos que (i), (ii) ou (iii) são válidas.

Suponhamos que (i) é válido, isto é, $min(|A|, |B|) = |B| = 1$, então $|A + B| = |A| = |A| + |B| - 1$ e assim (A, B) é um par crítico.

Se (ii) é válida, consideremos $c \in \mathbb{Z}_p$ e A um subconjunto de $\mathbb{Z}_p$ tal que $1 \leq |A| \leq p-1$. Definimos $B = \overline{c - A}$. Assim $c \notin A + B$, logo $|A + B| \leq p - 1$. Então $|B| = |\overline{c - A}| = p - |c - A| = p - |A|$, do Teorema de *Cauchy-Davenport* vem que $p - 1 = |A| + |B| - 1 \leq |A + B| \leq p - 1$, e assim $|A + B| = |A| + |B| - 1$, ou seja, (A, B) é crítico.

Agora se A e B são progressões aritméticas em $\mathbb{Z}_p$ com a mesma diferença, existem $\bar{a}, \bar{b} \in \mathbb{Z}_p$ e r, t inteiros positivos, com $r + t \leq p$ tais que $A = \{\bar{a} + i\bar{d} : i = 0, 1, ..., r - 1\}$ e $B = \{\bar{b} + i\bar{d} : i = 0, 1, ..., t - 1\}$. Como $\bar{d} \in \mathbb{Z}_p\backslash\{\bar{0}\}$ e $o(\bar{d})$ é um divisor de p, resulta que $o(\bar{d}) = p$. Então $A + B = \{\bar{a} + \bar{b} + i\bar{d} : i = 0, 1, ..., r + t - 2\}$, e assim $|A + B| = r + t - 1 = |A| + |B| - 1$. Portanto se (i), (ii) ou (iii) são válidas o par (A, B) é crítico.

Reciprocamente, é suficiente provar que uma das três condições ocorre. Seja (A, B) um par crítico, isto é, $|A + B| = |A| + |B| = 1$. Se $|A| = 1$ ou $|B| = 1$, o par é da forma (i). Se $|A + B| = p - 1$, então $\overline{A + B} = \{\bar{c}\}$ para qualquer $\bar{c} \in \mathbb{Z}_p$. Vamos provar que $B = \overline{\bar{c} - A}$. De fato, como $\bar{c} \notin A + B$, vem que $B \cap (\bar{c} - A) = \emptyset$ e assim $B \subseteq \overline{\bar{c} - A}$. Então

$|B| \leq |\overline{\bar{c} - A}| = p - |\bar{c} - A| = p - |A|$. Sendo $p - 1 = |A + B| = |A| + |B| - 1 \leq p - 1$, segue que $|B| = p - |A| = |\overline{\bar{c} - A}|$ e assim $B = \overline{\bar{c} - A}$. Logo o par (A, B) é da forma (ii).

Para finalizarmos a demonstração, assumiremos que (A, B) é um par crítico tal que, $min(|A|, |B|) \geq 2$ e $|A + B| < p - 1$. Pois caso contrário estaremos nas condições (i) e (ii). Seja (A, B) um par crítico com $|B| = t \geq 2$. Faremos a conclusão da demostração por indução sobre t. Se $t = 2$ o resultado segue do Lema 2.17. Suponha $t \geq 3$ e assuma que o teorema é válido para todo par crítico (A, B) com $|B| \geq t$. Pelo Lema 2.15, existe $\bar{g} \in A$ tal que $(A(\bar{g}), B(\bar{g}))$ é um par crítico com $A(\bar{g}) + B(\bar{g}) = A + B$ e $2 \leq |B(\bar{g})| < t$. Pela hipótese de indução, $A(\bar{g})$ e $B(\bar{g})$ são progressões aritméticas com mesma diferença. Portanto $A(\bar{g}) + B(\bar{g}) = A + B$ é uma progressão aritmética e do Lema 2.18 A e B são progressões aritméticas com mesma diferença. Completando a demonstração. □

2.3 Teorema de Erdös-Ginzburg-Ziv

Nessa seção apresentaremos o clássico Teorema de *Erdös-Ginzburg-Ziv*[4], um importante resultado sobre a adição de classes de congruência. Esse resultado foi um dos pontos de partida para as pesquisas sobre sequências em grupos abelianos finitos, a qual será apresentada com maiores detalhes nos últimos capítulos desse trabalho. O objetivo desse teorema é caracterizar o comprimento de sequências de números inteiros, munido de certas condições. O enunciado segue abaixo.

Teorema 2.20. (**Erdös-Ginzburg-Ziv**) *Dados $n \geq 1$ e $a_0, a_1, ..., a_{2n-2}$ uma sequência de 2n-1 inteiros não necessariamente distintos, então existe uma subsequência $a_{i_1}, ..., a_{i_n}$ tal que*

$$a_{i_1} + a_{i_2} + ... + a_{i_n} \equiv 0 \ (mod\ n) \tag{2.8}$$

Procedemos a demonstração do Teorema de Erdös-Ginzburg-Ziv de duas maneiras. A primeira atráves do *Teorema de Cauchy-Davenport* e a outra como corolário do *Teorema de Chevalley-Warning*.

1ª**Demonstração**: (Utilizando o *Teorema de Cauchy-Davenport*)

Primeiramente suponha que $n = p$, onde p é um número primo. Escolha $a_i^{'} \in \mathbb{Z}$ tal que $a_i^{'} \equiv a_i \ (mod\ p)$ e $0 \leq a_i^{'} < p$. Reenumere os inteiros a_i tais que

$$0 \leq a_0^{'} \leq a_1^{'} \leq ... \leq a_{2p-2}^{'} \leq p-1. \tag{2.9}$$

Analisemos dois casos:

1° caso: Existe $i = 1, ..., p-1$ tal que $a_i^{'} = a_{i+p-1}^{'}$. Assim da desigualdade (2.9) vem que $a_i^{'} = ... = a_{i+p-1}^{'}$ e como $a_i^{'} \equiv a_i$ decorre que $a_i \equiv a_{i+1} \equiv ... \equiv a_{i+p-1} \ (mod\ p)$ e

$$a_i + a_{i+1} + ... + a_{i+p-1} \equiv pa_i \equiv 0 \ (mod\ p).$$

2° caso: Para todo $i = 1, ..., p-1$, $a_i^{'} \neq a_{i+p-1}^{'}$. Com isso definimos em $\mathbb{Z}_p$ os subconjuntos de dois elementos

$$A_i = \{a_i + p\mathbb{Z}, a_{i+p-1} + p\mathbb{Z}\}.$$

Aplicando a generalização do Teorema de *Cauchy-Davenport*,

$$|A_1 + A_2 + ... + A_{p-1}| \geq min(p, 2(p-1) - (p-1) + 1) = p,$$

assim $A_1 + A_2 + ... + A_{p-1} = \mathbb{Z}_p$. Logo existem classes de congruência $a_{j_i} + p\mathbb{Z} \in A_i$ para todo $i = 1, ..., p-1$ tal que $j_i \in \{i, i+p-1\}$ e

$$-a_0 \equiv a_{j_1} + a_{j_2} + ... + a_{j_{p-1}} \ (mod\ p),$$

isto é, $a_0 + a_{j_1} + a_{j_2} + ... + a_{j_{p-1}} \equiv 0 \ (mod\ p)$. Assim o teorema é verdadeiro quando $n = p$ é primo.

Agora provaremos o teorema por indução sobre n. Se $n = 1$, nada temos a fazer. Suponha que $n > 1$ e que o teorema é válido para todo inteiro menor do que n. Se n é primo já provamos que o teorema vale. Assim considere n um número composto, logo $n = uv$, onde $1 < u \leq v < n$, então o resultado vale para u e v. Da sequência $a_0, ..., a_{2n-2}$ de comprimento $2n - 1 = 2uv - 1$ existe uma subsequência $a_{1,i_1}, ...a_{1,i_v}$ tal que

$$a_{1,i_1} + ... + a_{1,i_v} \equiv 0 \ (mod\ v).$$

Existem $2n-1-v = (2u-1)v-1$ inteiros na sequência original que não estão nessa subsequência. Como $2u - 1 \geq 2$, podemos encontrar uma subsequência disjunta $a_{2,i_1}, ...a_{2,i_v}$

de comprimento v tal que

$$a_{2,i_1} + ... + a_{2,i_v} \equiv 0 \ (mod\ v).$$

Existem $2n - 1 - 2v = (2u - 2)v - 1$ termos que não pertencem a nenhuma das duas subsequências já relacionadas. Agindo de maneira indutiva para $j = 1, ..., 2u-1$, obtemos $2u - 1$ subsequências distintas $a_{j,i_1}, ..., a_{j,i_v}$ de comprimento v tal que

$$a_{j,i_1} + ... + a_{j,i_v} \equiv 0 \ (mod\ v).$$

Então $a_{j,i_1} + ... + a_{j,i_v} = b_j v$, onde $b_j \in \mathbb{Z}$. Desde que o teorema é válido para u, existe uma subsequência $b_{j_1}, ...b_{j_u}$ da sequência $b_1, ..., b_{2u-1}$ tal que

$$b_{j_1} + ... + b_{j_u} \equiv 0 \ (mod\ u),$$

isto é, $b_{j_1} + ... + b_{j_u} = cu$ para algum $c \in \mathbb{Z}$. Então

$$\sum_{r=1}^{u} \sum_{s=1}^{v} a_{j_r,i_s} = \sum_{r=1}^{u} b_{j_r} v = cuv = cn \equiv 0 \ (mod\ p).$$

□

Para a segunda demonstração utilizaremos o Teorema de Chevalley-Warning, que será enunciado e demonstrado abaixo, antes apresentaremos um lema que será utilizado na demonstração do Teorema de Chevalley-Warning.

Lema 2.21. *Sejam $\mathbb{F}_q$ um corpo com q elementos e $0 \leq r < q - 1$. Convencionando que $0^0 = 1$ vem que*

$$\sum_{x \in \mathbb{F}_q} x^r = 0.$$

Demonstração: Para $r = 0$, o resultado é óbvio. Suponha que $0 < r < q - 1$ e considere α um gerador do grupo multiplicativo $\mathbb{F}_q^*$. Assim $\mathbb{F}_q^* = \{\alpha, \alpha^2, ..., \alpha^{(q-1)}\}$, logo

$$\begin{aligned} \sum_{x \in \mathbb{F}_q} x^r &= 0^r + \sum_{x \in \mathbb{F}_q^*} x^r \\ &= 0^0 + \alpha^r + \alpha^{2r} + ... + \alpha^{(q-1)r}. \end{aligned}$$

Observemos que $(\alpha^r, \alpha^{2r}, \alpha^{3r}, ..., \alpha^{(q-1)r})$ é uma progressão geométrica de razão α^r e como $x^{(q-1)} = 1$ para todo $x \in \mathbb{F}_q^*$ vem que

$$\begin{aligned}\sum_{x\in\mathbb{F}_q} x^r &= 0 + \frac{\alpha^r((\alpha^r)^{q-1}-1)}{\alpha^r - 1} \\ &= \frac{\alpha^r((\alpha^{q-1})^r - 1)}{\alpha^r - 1} = \frac{\alpha^r(1-1)}{\alpha^r - 1} = 0.\end{aligned}$$

□

Exemplo 2.22. Dado o grupo $\mathbb{Z}_2$, como 2 é um número primo temos que $\mathbb{Z}_2$ é um corpo. Considere os polinômios $f_1(x_1, x_2, x_3) = x_1 + x_2 + x_3$ e $f_2(x_1, x_2, x_3) = x_2 + x_3$ de graus 1 nas 3 variáveis com coeficientes em $\mathbb{Z}_2$. Por inspeção, vemos que as 3-uplas que são raízes dos polinômios f_1 e f_2 simultâneamente são $(\bar{0}, \bar{0}, \bar{0})$ e $(\bar{0}, \bar{1}, \bar{1})$. Observe que $2 \equiv 0\ (mod\ 2)$. Esse fato não é isolado, como veremos no teorema abaixo.

Teorema 2.23. (**Chevalley-Warning**) *Seja p um número primo e $\mathbb{F}_q$ o corpo finito com $q = p^t$ elementos. Para $i = 1, ..., m$, seja $f_i(x_1, x_2, ..., x_n)$ um polinômio de grau d_i em n variavéis com coeficientes em $\mathbb{F}_q$. Denotemos por N o número de n-uplas $(x_1, x_2, ..., x_n)$ de elementos de $\mathbb{F}_q$ tais que $f_i(x_1, x_2, ..., x_n) = 0$ para todo $i = 1, ..., m$. Se*

$$\sum_{i=1}^{m} d_i < n,$$

então

$$N \equiv 0\ (mod\ p).$$

Demonstração: Como o grupo multiplicativo $\mathbb{F}_q^*$ é cíclico, para qualquer $x \in \mathbb{F}_q$

$$x^{q-1} = \begin{cases} 1 & \text{se} \quad x \neq 0 \\ 0 & \text{se} \quad x = 0. \end{cases} \tag{2.10}$$

Além disso, convencionando que $0^0 = 1$ e considerando $0 \leq r < q - 1$, temos pelo Lema 2.21 que

$$\sum_{x\in\mathbb{F}_q} x^r = 0. \tag{2.11}$$

Sejam $x_1, ..., x_n \in \mathbb{F}_q$ note que

$$\prod_{i=1}^{m}(1 - f_i(x_1, ..., x_n)^{q-1}) = \begin{cases} 1 & \text{se} \quad f_i(x_1, ..., x_n) = 0 \textit{ para todo } i \\ 0 & \text{se} \quad f_i(x_1, ..., x_n) \neq 0. \end{cases}$$

e assim

$$N = \sum_{x_1,...,x_n \in \mathbb{F}_q} \prod_{i=1}^{m}(1 - f_i(x_1, ..., x_n)^{q-1}).$$

Como o grau de $f_i(x_1, ..., x_n)$ é d_i, vem que

$$\prod_{i=1}^{m}(1 - f_i(x_1, ..., x_n)^{q-1}) = \sum_{r_1,...,r_n} a_{r_1...r_n} x_1^{r_1} ... x_n^{r_n}$$

é um polinômio de grau no máximo $(q-1)\sum_{i=1}^{m} d_i$ com coeficientes $a_{r_1...r_n} \in \mathbb{F}_q$. Então

$$\begin{aligned} N &\equiv \sum_{x_1,...,x_n \in \mathbb{F}_q} \prod_{i=1}^{m}(1 - f_i(x_1, ..., x_n)^{q-1}) \ (mod\ p) \\ &\equiv \sum_{x_1,...,x_n \in \mathbb{F}_q} \sum_{r_1,...,r_n} a_{r_1,...,r_n} x_1^{r_1} ... x_n^{r_n} \ (mod\ p) \\ &\equiv \sum_{r_1,...r_n} a_{r_1,...r_n} \sum_{x_1,...,x_n \in \mathbb{F}_q} x_1^{r_1} ... x_n^{r_n} \ (mod\ p) \\ &\equiv \sum_{r_1,...,r_n} a_{r_1,...,r_n} \prod_{j=1}^{n} \sum_{x_j \in \mathbb{F}_q} x_j^{r_j} \ (mod\ p), \end{aligned}$$

onde a somatória percorre todas as n-uplas $r_1, ..., r_n$ de inteiros não negativos tais que

$$\sum_{j=1}^{n} r_j \leq (q-1)\sum_{j=1}^{n} d_j < n(q-1).$$

Isso implica que para algum j, $0 \leq r_j < q-1$, assim pela equação (2.11), $\sum_{x_j \in \mathbb{F}_q} x_j^{r_j} = 0$ e logo

$$\prod_{j=1}^{n} \sum_{x_j \in \mathbb{F}_q} x_j^{r_j} \equiv 0 \ (mod\ p).$$

Portanto, $N \equiv 0 \ (mod\ p)$. □

Observemos que no caso $n = p$, onde p é um número primo o Teorema de *Erdös-Ginzburg-Ziv* é um corolário do Teorema de *Chevalley-Warning*. Assim temos a segunda demostração.

2^a**Demonstração**: (Corolário do *Teorema de Chevalley-Warning*) Dada $a_1, ..., a_{2p-1}$ uma sequência de elementos no corpo finito $\mathbb{F}_p = \mathbb{Z}_p$. Considere os polinômios $f_1, f_2 \in \mathbb{F}_p[x_1, ..., x_{2p-1}]$ definidos por

$$f_1(x_1, ..., x_{2p-1}) = \sum_{j=1}^{2p-1} x_j^{p-1}$$

e

$$f_2(x_1, ..., x_{2p-1}) = \sum_{j=1}^{2p-1} a_j x_j^{p-1}.$$

Seja d_i o grau do polinômio f_i. Então $d_1 = d_2 = p - 1$. Denotemos por N o número das soluções simultâneas desses polinômios. Como $d_1 + d_2 = 2p - 2 < 2p - 1$, vem do Teorema 2.23 que $N \equiv 0 \ (mod\ p)$. Desde que $f_1(0, ..., 0) = f_2(0, ..., 0) = 0$, decorre que $N > 1$ e assim $N \geq p \geq 2$. Portanto, os polinômios f_1 e f_2 têm uma solução não trivial, isto é, existem $x_1, ..., x_{2p-1} \in \mathbb{Z}_p$ não todos nulos tais que

$$f_1(x_1, ..., x_{2p-1}) = \sum_{j=1}^{2p-1} x_j^{p-1} = 0 \tag{2.12}$$

e

$$f_2(x_1, ..., x_{2p-1}) = \sum_{j=1}^{2p-1} a_j x_j^{p-1} = 0. \tag{2.13}$$

Como $x^{p-1} = 1$ se, e somente se, $x \neq 0$, segue da equação (2.12) que $x_j \neq 0$ para exatamente p elementos $x_{j_1}, ..., x_{j_p} \in \mathbb{Z}_p$. Assim a equação (2.13) implica que $a_{j_1} + ... + a_{j_p} \equiv 0 \ (mod\ p)$. □

Capítulo 3

Sequências em Grupos Abelianos Finitos

Nos capítulos anteriores essencialmente, dados $A_1, ..., A_n$ conjuntos de um grupo abeliano escrito aditivamente G, representávamos os elementos de G como soma em $A_1 + ... + A_n$ e exibiamos resultados do tipo diretos e inversos. Nesse capítulo ilustraremos uma nova forma de representação para os elementos de G. Em 1961, com o Teorema de *Erdös-Ginzburg-Ziv*, os elementos de um grupo G passaram a ser representados como soma de termos de uma dada sequência.

Aprofundaremos os resultados neste capítulo envolvendo sequências em G. Dessa forma, dada S uma sequência em G, diversos problemas podem ser levantados, como por exemplo:

(i) determinar o total de elementos de G representados pela soma de termos de S;

(ii) estabelecer um limite para a cardinalidade de G de modo que a sequência S represente o elemento neutro de G.

Em 1972, esses problemas foram levantados e solucionados por Eggleton e Erdös [3], como veremos na primeira seção desse capítulo. Em 1962, Henry Mann nessa linha de pesquisa, demonstra que dada uma sequência de comprimento $2p - 1$ em um grupo de

cardinalidade prima p, todo elemento do grupo é representado como soma dos termos de uma subsequência de comprimento exatamente p. Através desse resultado em 1996, Gao [5] apresenta um refinamento do Teorema de Mann, como observaremos na segunda seção. Salvo mensão contrária, G sempre denotará um grupo abeliano finito escrito aditivamente. Assim o elemento neutro de G será denotado por 0.

3.1 Representação como soma de termos de sequência

Aprofundaremos o estudo de representações via sequências em G. Teremos como objetivos, reapresentar as soluções dos problemas levantados por Egglenton e Erdös em [3]. Estimaremos o total de elementos de um grupo G representado por uma dada sequência e também apresentaremos condições sobre a cardinalidade do grupo G de modo que possua sequências que representem o seu elemento neutro.

Definição 3.1. Dada $S = (a_i)_{i=1}^{n}$ uma sequência em G, diremos que S representa x se existe um conjunto $J \subseteq \{1, ..., n\}$ tal que

$$\sum_{j \in J} a_j = x.$$

Na próxima definição e nos dois resultados subsequentes estaremos considerando sequências em G de modo que essas não representam o elemento 0.

Definição 3.2. Seja $S = (a_i)_{i=1}^{k}$ uma sequência de k elementos distintos G, tal que S não represente 0. O *número de elementos representados por* S será denotado por $f_S(k)$. Simbolicamente,

$$f_S(k) = |\{x \in G : x = \sum_{j \in J} a_j;\ J \subseteq \{1, ..., k\}|.$$

Estaremos interessados em estabelecer um resultado sobre um limite inferior para a função $f_S(k)$. Para atingir esse objetivo, necessitamos do Teorema de *Moser-Scherk* [13].

Teorema 3.3. (Moser-Scherk) *Dados A e B conjuntos finitos de G, tais que*

(i) $0 \in A$

(ii) $0 \in B$

(iii) $a + b = 0$ *implica que* $a = 0 = b$.

Nessas condições $|A + B| \geq |A| + |B| - 1$.

Demonstração: Procederemos a demonstração por indução sobre a cardinalidade de B. Se $|B| = 1$ o resultado segue trivialmente. Suponhamos que o teorema vale para todo conjunto B' tal que $|B'| \leq n - 1$. Dado B tal que $0 \in B$ e $|B| = n > 1$, considere $b_1 \in B$ com $b_1 \neq 0$. Então $0 \notin A + b_1$. Desde que $|A + b_1| = |A|$, existem elementos em $A + b_1$ que não pertencem a A, assim existe $a_0 \in A$ tal que $a_1 = a_0 + b_1 \notin A$.

Tomemos $A_1 = \{a_1\}$ e $B_1 = \{b_1\}$, como $0 \notin B_1$ vem que

$$0 < |A_1| = |B_1| < |B|. \tag{3.1}$$

Agora consideremos os conjuntos $A_2 = A \cup A_1$ e $B_2 = B \backslash \{b_1\}$, logo $0 \in B_2 \subset B$ e $0 \in A \subset A_2$ e pela equação (3.1)

$$\begin{aligned} |A_2| + |B_2| &= |A| + |A_1| + |B_2| \\ &= |A| + |B_1| + |B_2| \\ &= |A| + |B|. \end{aligned} \tag{3.2}$$

Afirmamos que

$$A_2 + B_2 \subset A + B \tag{3.3}$$

e que dados $a_2 \in A_2, b_2 \in B_2$ com a condição que $a_2 + b_2 = 0$, temos que

$$a_2 = 0 = b_2. \tag{3.4}$$

Vamos provar as afirmações. Sejam $a_2 \in A_2$ e $b_2 \in B_2$. Consideraremos somente o caso em que $a_2 \notin A$, isto é, $a_2 = a_0 + b_1 \in A_1$, pois caso contrário o resultado segue. Assim

$$a_2 + b_2 = (a_0 + b_1) + b_2 = (a_0 + b_2) + b_1.$$

Como $b_2 \in B_2$, a definição de B_1 implica que $a_0 + b_2 \in A$, logo $(a_0 + b_2) + b_1 \in A + B_1$ e consequentemente em $A + B$. Também se $(a_0 + b_2) + b_1 = 0$ teríamos que $b_1 = 0$, o que

é impossível. O que prova as equações (3.3) e (3.4). Desde que $|B_2| < |B|$, pela hipótese de indução

$$|A_2 + B_2| \geq |A_2| + |B_2| - 1. \tag{3.5}$$

Finalmente pelas equações (3.3), (3.5) e (3.2) resulta que

$$|A + B| \geq |A_2 + B_2| \geq |A_2| + |B_2| - 1 = |A| + |B| - 1.$$

□

Notemos que o Teorema de Moser-Scherk é um tipo de problema direto.

Teorema 3.4. *Fixe $S = (a_i)_{i=1}^{k}$ uma sequência de k termos distintos em G. Se S não representa 0, então*

$$f_S(k) \geq 2k - 1.$$

Demonstração: Procederemos a demonstração por indução sobre k. Para $k = 1$, basta considerarmos a sequência formada por apenas um termo, logo $f_S(k) = 1$. Dado $k \geq 1$, para toda sequência S com k termos distintos, suponhamos que $f_S(k) \geq 2k - 1$. Seja $S' = (a_i)_{i=1}^{k+1}$ uma sequência de $k + 1$ termos distintos de G que não representa 0. Temos dois casos a considerar:

Caso (i): Existe um termo em S' que não é representado pelos k termos restantes. Suponhamos sem perda de generalidade que este termo seja a_{k+1}. Tome a subsequência $S = (a_i)_{i=1}^{k}$, pela hipótese indutiva, os $2k - 1$ elementos (ou mais) representados pelos k primeiros termos de S' não incluem a_{k+1}, nem $\sum_{i=1}^{k+1} a_i$. Caso contrário a diferença entre essa soma e algum elemento representado pelos k primeiros termos seria 0, o que não pode ocorrer. Assim S' representa pelo menos $2k + 1$ elementos.

Caso (ii): Todo termo de S' é representado pelos outros k termos. Considere $A = B = \{0, a_1, a_2, ..., a_{k+1}\}$, então pelo Teorema de Moser-Scherk, $|A+B| \geq 2k+3$. Pela condição desse caso, $2a_j = a_j + \sum_{i \in I} a_i$, com $I \subseteq \{1, ..., k + 1\}$. Isso mostra que todo elemento de $A + B$ diferente de 0 é representado por S', rendendo um total de pelo menos $2k + 2$ elementos representados por S', logo $f_{S'}(k + 1) \geq 2k + 2$. Portanto o teorema é válido.□

Exemplo 3.5. Observemos que a condição de S não representar 0 no Teorema 3.4 é de grande necessidade, pois caso contrário, o resultado do teorema não é válido. De fato, tome $k = 3$ e considere $S = (\bar{0}, \bar{1}, \bar{3})$ uma sequência em $\mathbb{Z}_7$, notemos que os elementos representados por S são $\{\bar{0}, \bar{1}, \bar{3}, \bar{4}\}$, ou seja, $f_S(3) < 2k - 1$.

Exemplo 3.6. Considere a sequência $S = (\bar{1}, \bar{1}, \bar{2}, \bar{3})$, observemos que essa sequência não representa $\bar{0} \in \mathbb{Z}_9$. Agora a sequência $S' = (\bar{1}, \bar{1}, \bar{1}, \bar{2}, \bar{2}, \bar{2}, \bar{3}, \bar{3}, \bar{3})$ representa $\bar{0}$ em $\mathbb{Z}_7$.

A partir do Exemplo (3.6), poderíamos pensar se a ordem do grupo G é um fator decisivo para garantir a representação de 0. Isso realmente é verdadeiro, como veremos nos resultados abaixo.

Teorema 3.7. *Dada $S = (a_i)_{i=1}^n$ uma sequência arbitrária de elementos de G, com exatamente k desses elementos distintos. Se o grupo tem ordem $|G| \leq n + \binom{k}{2}$ e $n \geq k\binom{k}{2}$, então S obrigatoriamente representa* 0.

Demonstração: Procederemos a demonstração por contradição. Suponhamos que S não representa o elemento 0. Em particular, nenhum das m primeiras somas $s_j = \sum_i^j a_i$ com $j = 1, 2, ..., m$ é 0. Mais ainda nenhuma dessas m primeiras somas são iguais a qualquer das $n - m$ somas da forma $\sum_{i=1}^{r} a_i$, com $m + 1 \leq r \leq n$, pois caso contrário a diferença entre as m primeiras e as $n - m$ somas seria igual a 0. Novamente, nenhuma dessas $n - m$ somas são iguais a 0, e todas são distintas entre si, pois de outra forma existiriam s, t com $m + 1 \leq s < t \leq n$ tais que $\sum_{i=s+1}^{t} a_i = 0$, ou seja, uma diferença igual a 0, contrariando a hipótese.

Pelas hipóteses do teorema, podemos supor que existem t termos iguais em S, digamos $a_i = a_1$ para $1 \leq i \leq t$, onde $kt \geq n$. Assim S representa os elementos xa_1 para $1 \leq x \leq t$, os quais são necessariamente distintos e diferentes de 0. Há dois casos a considerar.

Caso (i): Se S não possui um termo no conjunto gerado por a_1. Suponhamos que $a_{t+1} \notin < a_1 >$. Fazendo $m = t + 1$, os primeiros m termos de S devem representar $2t + 1$ elementos distintos. Pois caso contrário, existiriam x, y com $1 \leq x < y \leq t$ tais que $a_{t+1} + (y - x)a_1 = 0$. Como $n \geq k\binom{k}{2}$, pelo menos $m + \binom{k}{2}$ elementos distintos são

representados por S. Assim com as $m-n$ somas restantes e com o elemento 0 temos um total de $n+\binom{k}{2}+1$ elementos distintos em G. Contrariando o fato de que $|G| \leq n+\binom{k}{2}$.

Caso (ii): Todos os termos de S são gerados por a_1. Denote $a_i = r_i a_1$ para $1 \leq i \leq n$ e defina a sequência auxiliar $S' = (r_i)_{i=1}^n$ que compreende inteiros positivos, com exatamente k desses distintos e $r_i = 1$ para $1 \leq i \leq t$. Como S não representa o 0, claramente S' não tem termos iguais a 0. Se nenhum termo de S' excede t, então S' representa todos os inteiros positivos até t, incluindo $\sum_{i-1}^{n} r_i$ e essa soma é tão grande quanto a soma dos primeiros k inteiros positivos junto com uma das $n-k$ somas. Assim S' certamente representa $|G|$ se $|G| \leq n+\binom{k}{2}$, logo S representa $|G|.a_1$, o qual é 0. O que é uma contradição, assim S' deve conter um termo que excede t, digamos $r_{i+1} > t$. Novamente tomando $m = t+1$ e repetindo o argumento do caso (i), obteremos que a $|G| \geq n+\binom{k}{2}$, o que é uma contradição. □

Exemplo 3.8. Notemos que o Teorema 3.7 é o melhor possível no sentido que o limite sobre $|G|$ não pode ser melhorado em geral. De fato, considere $S = (a_i)_{i=1}^n$ a sequência no grupo $\mathbb{Z}_t$ com $t = n+\binom{k}{2}+1$, dada por $a_i = i$ se $1 \leq i \leq k$ e $a_i = 1$ se $k+1 \leq i \leq n$. Observemos que S representa todo o elemento em $\mathbb{Z}_t \backslash \{0\}$.

Exemplo 3.9. De maneira analóga, o Teorema 3.7 é o melhor possível em relação a n, no sentido que n não pode ser reduzido. De fato, considere $S = (a_i)_{i=1}^n$ uma sequência no grupo $\mathbb{Z}_{2s^2+4s}$ tal que $a_i = i$ se $1 \leq i \leq s$, $a_i = 1$ se $s+1 \leq i \leq 2s-1$ e $a_i = s^2+i$ quando $2s \leq i \leq 3s$. Tomando $k = 2s+1$, temos que S não representa $\bar{0}$. Desde que $|\mathbb{Z}_{2s^2+4s}| = 2s^2+4s = n+\binom{k}{2}+1$, o limite apresentado no Teorema 3.7 sobre n não pode ser reduzido até $3/2(k-1)$ em geral.

Teorema 3.10. *Seja $S = (a_i)_{i=1}^n$ uma sequência arbitrária em G, com pelo menos k desses elementos distintos. Se $|G| \leq n+k-1$, então S representa* 0.

Demonstração: Procedemos a demonstração por contradição. Suponhamos que S não represente 0, assim podemos tomar os k primeiros termos distintos de S. Nenhum dos elementos que esses k termos representam, podem ser iguais a qualquer das $n-k$ somas $\sum_{i=1}^{r} a_i$, onde $k+1 \leq r \leq n$, pois caso contrário a diferença correspondente seria igual a 0

e S poderia representar o 0. Similarmente, nenhum par das $n-k$ somas podem ser iguais. Pelo Teorema 3.4, os k primeiros termos representam pelo menos $2k-1$ elementos e com as $n-k$ somas temos um total de pelo menos $n+k-1$ elementos distintos representados por S. Como S não representa 0, teríamos $|G| \geq n+k$ o que contraria a hipótese, logo o teorema é válido. □

3.2 Refinamento do Teorema de Mann

Recordemos que o Teorema de *Erdös-Ginzburg-Ziv*, foi aplicado no conjunto de número inteiros. Dada S uma sequência de comprimento $2n-1$, tal teorema afirmava que existe uma subsequência de comprimento n cuja soma dos termos é congruente a 0 módulo n. Uma questão natural é investigar quantas subsequências desse tipo podem ser encontradas.

Podemos transformar este problema de existência em um problema combinatório, ou seja, buscar quantas subsequências deste tipo existem. Mais geralmente, quantas subsequências de comprimento n representam determinado elemento? Em uma situação mais restrita, essa questão é respondida por Mann em 1967, onde a cardinalidade do grupo G é prima p e a sequência tem comprimento $2p-1$. Também veremos um refinamento do Teorema de Mann, apresentado por Gao em 1996. Para tanto precisaremos de alguns conceitos prévios.

Definição 3.11. Considere $S = (a_1, a_2, ..., a_{2n-1})$ uma sequência de $2n-1$ elementos em G. Para todo $g \in G$ denotemos por $r(S,g)$ o número de subsequências $S' = (a_{i_1}, a_{i_2}, ..., a_{i_n})$ de comprimento exatamente n tal que a soma de todos os termos de S' é igual a g. Simbolicamente,

$$r(S,g) = |\{S' = (a_{i_j})_{j=1}^{n} : \sum_{j=1}^{n} a_{i_j} = g\}| \tag{3.6}$$

Exemplo 3.12. Consideremos a sequência $S = (a_i)_{i=1}^{7} = (\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7})$ em $\mathbb{Z}_9$. Por simples inspeção, as subsequências $(a_3, a_4, a_5, a_6) = (\bar{3}, \bar{4}, \bar{5}, \bar{6})$ e $(a_2, a_4, a_5, a_7) = (\bar{2}, \bar{4}, \bar{5}, \bar{7})$ de comprimento 4 representam $\bar{0}$ e assim $r(S, \bar{0}) = 2$. De maneira análoga o

elemento $\bar{2}$ é representado por três subsequências de comprimento 4, a saber (a_1, a_2, a_3, a_5), (a_3, a_4, a_6, a_7), (a_2, a_5, a_6, a_7) e assim $r(S, \bar{2}) = 3$.

O Teorema de Mann é enunciado precisamente abaixo, o leitor poderá consultar a demonstração em [12]. A seguir apresentaremos um resultado que também será utilizado na demonstração do refinamento do Teorema de Mann.

Teorema 3.13. (**Mann**) *Dada S uma sequência de comprimento $2p-1$ no grupo abeliano G de cardinalidade prima p. Se os elementos de G ocorrem no máximo p vezes em S, então $r(S, g) \geq 1$ para todo $g \in G$. Em outras palavras, existe pelo menos uma subsequência de tamanho exatamente p tal que a soma de seus termos é g.*

Exemplo 3.14. Notemos que a condição de que os elementos de G ocorrem no máximo p vezes em S no Teorema de Mann é de grande necessidade, pois caso contrário não obteremos o resultado. De fato, considerando $S = (\bar{2}, \bar{2}, \bar{2}, \bar{2}, \bar{2}, \bar{2}, \bar{2}, \bar{1}, \bar{1})$ uma sequência em $\mathbb{Z}_5$, observamos que não existe $I \subseteq \{1, ..., 9\}$ tal que $\sum_{i \in I}(a_i) = \bar{1}$, ou seja, $r(S, \bar{1}) = 0$.

Os próximos resultados foram obtidos por Gao, conforme a referência [5].

Teorema 3.15. (**Gao**) *Dada $S = (a_1, a_2, ..., a_{2p-1})$ uma sequência de $2p-1$ elementos em um grupo G de ordem prima p. Então*

$$r(S, a) = \begin{cases} 0 \ (mod\ p) & se \quad a \neq 0 \\ 1 \ (mod\ p) & se \quad a = 0 \end{cases} \tag{3.7}$$

Demonstração: Como G é um grupo abeliano de ordem prima p, vem que G é isomorfo ao grupo cíclico $\mathbb{Z}_p$. Dado m um inteiro qualquer positivo, temos a seguinte identidade combinatória

$$\sum_{a=0}^{p-1} a^m r(S, a) = \sum_{1 \leq i_1 < ... < ip \leq 2p-1} (a_{i_1} + a_{i_2} + ... + a_{i_p})^m. \tag{3.8}$$

De fato, contaremos essa identidade de duas maneiras distintas. No lado direito da equação (3.8) estamos somando a m-ésima potência das somas dos termos de subsequências de comprimento exatamente p, tal que $\sum_{j=1}^{p} a_{i_j} = a$ para todo $a \in G$. Desse argumento e da Definição 3.11 decorre o lado esquerdo da equação (3.8).

Sabemos do teorema multinomial que

$$(a_{i_1} + a_{i_2} + ... + a_{i_p})^m = \sum \frac{m!}{\beta_1!\beta_2!...\beta_p!} a_{i_1}^{\beta_1} a_{i_2}^{\beta_2} ... a_{i_p}^{\beta_p}$$

assim a parte direita da equação (3.8) pode ser escrita da seguinte maneira

$$\sum_{1 \leq i_1 < ... < ip \leq 2p-1} (a_{i_1} + a_{i_2} + ... + a_{i_p})^m$$

$$= \sum_{\beta_1 + ... + \beta_k = m} \binom{2p-1-k}{p-k} \frac{m!}{\beta_1!...\beta_k!} a_{i_1}^{\beta_1} ... a_{i_k}^{\beta_k}. \tag{3.9}$$

Assumindo $1 \leq k \leq p-1$ e observando que

$$\binom{2p-1-k}{p-k} = \frac{(2p-1-k)...(p+1)p(p-1)!}{(p-k)!(p-1)!} = \frac{(2p-1-k)...p}{(p-k)!}$$

decorre que p divide $(2p-1-k)...(p+1)p$ e p não divide $(p-k)!$, logo

$$\binom{2p-1-k}{p-k} \equiv 0 \ (mod\ p).$$

Assim das igualdades (3.8) e (3.9) obtemos

$$\sum_{0 \neq a \in G} a^m r(S, a) = 0 \tag{3.10}$$

onde $m = 1, 2, ..., p-1$.

Através da equação (3.10) obtemos o seguinte sistema

$$\begin{cases} 1r(S,1) + 2r(S,2) + ... + (p-1)r(S,p-1) = 0 \\ 1r(S,1) + 2^2 r(S,2) + ... + (p-1)^2 r(S,p-1) = 0 \\ \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \quad . \\ 1r(S,1) + 2^{p-1} r(S,2) + ... + (p-1)^{p-1} r(S,p-1) = 0 \end{cases} \tag{3.11}$$

o qual nos fornece a seguinte matriz dos coeficientes

$$\begin{vmatrix} 1 & 2 & \cdots & p-1 \\ 1 & 2^2 & \cdots & (p-1)^2 \\ \vdots & \vdots & \cdots & \vdots \\ 1 & 2^{p-1} & \cdots & (p-1)^{p-1} \end{vmatrix}. \tag{3.12}$$

Observemos que essa é uma matriz de Vandermonde e assim possui determinante não nulo em $\mathbb{Z}_p$. Desde que $\mathbb{Z}_p$ é corpo, o sistema (3.11) admite solução trivial. Assim $r(S,a) \equiv 0 \ (mod\ p)$ para todo $0 \neq a \in G$. Observemos que a quantidade de subsequências de comprimento extamente p é $\binom{2p-1}{p}$, isto é,

$$\sum_{a \in G} r(S,a) = \binom{2p-1}{p}$$

Portanto

$$r(S,0) = \binom{2p-1}{p} - \sum_{0 \neq a \in G} r(S,a).$$

Pela Igualdade (3.10) e do fato que $\binom{2p-1}{p} \equiv 1 \ (mod\ p)$, vem que

$$r(S,0) \equiv 1 \ (mod\ p).$$

□

Teorema 3.16. (**Refinamento do Teorema de Mann**) *Seja* $S = (a_1, a_2, ..., a_{2p-1})$ *uma sequência de* $2p-1$ *elementos de um grupo* G *de ordem prima* p*, então*

(i) $r(S,a) \geq p$ *para todo* $a \in G$, $a \neq 0$*, com a condição que nenhum elemento da sequência* S *ocorra mais que* p *vezes,*

(ii) $r(S,0) \geq p+1$*, a não ser que apenas dois elementos* x *e* y *ocorram em* S*,* x *aparecendo* p *vezes e* y *p-1 vezes.*

Demonstração: (i) Como $0 \neq a \in G$, vem do Teorema 3.15 que $r(S,a) \equiv 0 \ (mod\ p)$, isto é, $r(S,a) = bp$, $b \in \mathbb{Z}$. Pelo Teorema de *Mann*, $r(S,a) \geq 1$ para todo $a \in G$, então $r(S,a) \geq p$.

(ii) Por absurdo, suponha que $r(S,0) < p+1$, logo $1 \leq r(S,0) \leq p$. Novamente do Teorema 3.15, $r(S,0) \equiv 1 \ (mod\ p)$ e assim

$$r(S,0) = 1. \tag{3.13}$$

Reenumerando os elementos na sequência se necessário, podemos assumir sem perda de generalidade que

$$\sum_{i=p}^{2p-1} a_i = 0. \tag{3.14}$$

Seja $\{i_1, i_2, ..., i_{p-1}\}$ uma permutação arbitrária de $1, 2, ..., p-1$. Definamos $b_k = a_{i_k} - a_{p+k}$ para $k = 1, ..., p-1$. Das equações (3.13) e (3.14) decorre que não existe subconjunto não vazio I de $\{1, 2, ..., p-1\}$ tal que $\sum_{k \in I} b_k = 0$. Pois caso contrário, obtemos duas subsequências cuja soma é 0, contrariando a equação (3.13). Assim pelo Teorema 3.10, $b_1 = b_2 = ... = b_{p-1}$. Logo

$$a_{i_1} - a_{p+1} = a_{i_2} - a_{p+2} = ... = a_{i_{p-1}} - a_{2p-1} \tag{3.15}$$

para qualquer permutação $i_1, i_2, ..., i_{p-1}$ do conjunto $\{1, 2, ..., p-1\}$.

Fazendo $i_j = j$ para $j = 1, ..., p-1$ na equação (3.15) temos $a_1 - a_{p+1} = a_2 - a_{p+2} = a_3 - a_{p+3} = ... = a_{p-1} - a_{2p-1}$. Agora tomando $i_1 = 2$, $i_2 = 1$ e $i_j = j$ para $j = 3, 4, ..., p-1$ na equação (3.15), vem que $a_2 - a_{p+1} = a_1 - a_{p+2} = ... = a_{p-1} - a_{2p-1}$. Assim $a_1 = a_2$. Procedendo dessa maneira até $i_{p-2} = p-1$ e $i_{p-1} = p-2$, obtemos $a_1 = a_2 = ... = a_{p-1} \neq a_{p+1} = ...a_{2p-1}$. Deste argumento e da equação (3.14), vem que $a_1 = a_2 = ... = a_{p-1} \neq a_p = a_{p-1} = ... = a_{2p-1}$. Mas isso contraria a restrição sobre S em (ii) e a prova está completa. □

Capítulo 4

Sequências Soma-Zero

Neste capítulo, continuaremos com os estudos de sequências em grupos abelianos finitos. Dada uma sequência em G, outras questões podem ser levantadas, como por exemplo:

> determinar condições para que essa sequência possua uma subsequência que represente o elemento neutro de G.

Esse problema foi primeiramente apresentado a partir de 1961, por Paul Edös e Harold Davenport onde estipularam a função, atualmente conhecida como a constante de Davenport. Embora tenha sido bastante estudada, poucos valores precisos são conhecidos para a constante de Davenport. Em 1968, J. Olson [17] calculou o valor exato para a constante de Davenport do p-grupo $\mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times ... \times \mathbb{Z}_{p^{e_r}}$, onde p é um inteiro primo, r e e_i inteiros positivos para todo $i \in 1, 2, ..., r$. Para certas classes de grupos apresentaremos valores precisos para a constante de Davenport, para outros casos somente aproximações.

4.1 Constante de Davenport

Nessa seção, a partir de um grupo G, teremos como objetivo definir a constante de Davenport. Apresentaremos em alguns casos, valores exatos para a constante, em outros apenas aproximações, pois seu cálculo não é uma tarefa fácil. Nos preocupares em estudar as sequências principalmente em $\mathbb{Z}_n^d$, o grupo formado por d cópias de $\mathbb{Z}_n$ com n e d inteiros positivos. Antes precisaremos de alguns conceitos prévios.

Definição 4.1. Seja $S = (a_i)_{i=1}^k$ uma sequência do grupo G, denotaremos o número de elementos de S por $|S|$. O número de vezes que o elemento a ocorre em S por $v_a(S)$ e a soma dos termos de S por $\sigma(S) = \sum_{i=1}^{k} a_i$.

Definição 4.2. Fixada S uma sequência de comprimento k em G. Dadas T_1 e T_2 subsequências de S, diremos que essas *subsequências são disjuntas* se existem subconjuntos disjuntos de índices $I, J \subseteq \{1, 2, ..., k\}$ tais que $T_1 = (a_i)_{i\in I}$ e $T_2 = (a_j)_{j\in J}$.

Definição 4.3. Dada $S = (a_i)_{i=1}^k$ uma sequência em G. Considere $I, J \subseteq \{1, 2, ..., k\}$ tais que $T_1 = (a_i)_{i\in I}$ e $T_2 = (a_j)_{j\in J}$ são subsequências de S. Assim duas operações podem ser definidas:

(i) $ST_1^{-1} = (a_t)_{t\in\{1,...,k\}\setminus I}$, sequência obtida pela remoção dos elementos de T_1 em S;

(ii) $T_1T_2 = (a_t)_{t\in I\cup J}$, a sequência obtida pela concatenação de T_1 e T_2.

Como ilustração, consideremos $S = (\bar{1}, \bar{2}, \bar{1}, \bar{2}, \bar{1}, \bar{3}, \bar{3}, \bar{3}, \bar{1}, \bar{2}, \bar{1})$ uma sequência em $\mathbb{Z}_5$, vemos que $|S| = 11$, $v_{\bar{1}}(S) = 5$. Tomando $T_1 = (a_i)_{i\in I}$ e $T_2 = (a_j)_{j\in J}$ subsequências de S tais que $I = \{1, 2, 4, 5\}$ e $J = \{4, 6, 7, 8\}$, temos que $ST_1^{-1} = (\bar{1}, \bar{3}, \bar{3}, \bar{3}, \bar{1}, \bar{2}, \bar{1})$ e $T_1T_2 = (\bar{1}, \bar{2}, \bar{2}, \bar{1}, \bar{3}, \bar{3}, \bar{3})$. Observemos também que $\sigma(S) = 0$. Isso nos leva a seguinte definição.

Definição 4.4. Dada S é uma sequência em G, diremos que S é uma *sequência soma-zero* se a soma de S é igual ao elemento neutro de G, isto é, $\sigma(S) = 0$.

Alguns anos depois do Teorema de Erdös-Ginzburg-Ziv, Erdös, Davenport e Baayen formularam o seguinte problema:

Para um grupo abeliano finito G, determinar o menor inteiro positivo t tal que toda sequência S em G com comprimento pelo menos t contém uma subsequência soma-zero.

Esse inteiro positivo t ficou conhecido como a constante de Davenport, o qual tem a seguinte definição.

Definição 4.5. O menor inteiro positivo t tal que toda sequência S em um grupo abeliano finito G de comprimento pelo menos t possua uma subsequência soma-zero, é definido como a *constante de Davenport* e denotado por $D(G)$.

Podemos nos perguntar se esse inteiro t sempre existe. A próxima proposição justifica que a constante de Davenport está bem definida.

Proposição 4.6. *Dado o grupo G de ordem n, então*

$$D(G) \leq n.$$

Demonstração: Seja $S = (a_i)_{i=1}^{n}$ uma sequência em G de comprimento n. Primeiramente observemos que se $a_i = 0$ para algum $i = 1, ..., n$, S terá uma subsequência soma-zero e o resultado segue. Com isso, podemos assumir que $0 \notin S$. Consideremos $\lambda_j = \sum_{i=1}^{j} a_i$ para todo $j = 1, ..., n$. Se todos os λ_j são distintos, obtemos n elementos distintos, logo $\lambda_j = 0$ para algum $j = 1, 2, ..., n$. Agora se $\lambda_i = \lambda_j$ para certos i, j com $i < j$, a sequência $T = (a_k)_{k=i+1}^{j}$ é soma-zero. Portanto $D(G) \leq n$, para qualquer grupo abelino finito G. □

Dado um grupo qualquer G, encontrar o valor exato para a constante de Davenport, em geral, não é uma tarefa fácil. No próximo resultado, mostraremos que o limite superior apresentado no Teorema 4.6 é atingido.

Proposição 4.7. *Sejam n um inteiro positivo e o grupo $\mathbb{Z}_n$, então*

$$D(\mathbb{Z}_n) = n.$$

Demonstração: Mostraremos que o limite inferior e superior da constante de Davenport para $\mathbb{Z}_n$ são iguais a n. De fato, pela Proposição 4.6, basta mostrarmos o limite inferior.

Para tanto, consideremos a sequência S de comprimento $n-1$ em $\mathbb{Z}_n$, onde o elemento $\bar{1}$ ocorra $n-1$ vezes. Observemos que S não possui subsequência soma-zero, logo $D(\mathbb{Z}_n) \geq n$. Este argumento completa a demonstração. □

4.1.1 Constante de Davenport para um p-grupo

Nessa subseção, consideraremos G um grupo abeliano finito com notação multiplicativa e assim denotaremos o elemento identidade de G por 1. As definições apresentadas anteriormente também são válidas, notando que ao invés de soma-zero as subsequências terão produto igual a 1. Calcularemos o valor exato da constante de Davenport para um p-grupo G. Para tanto, precisaremos de alguns resultados no contexto do anel de grupo G sobre o anel dos inteiros.

Definição 4.8. Dados G um grupo qualquer e $\mathbb{Z}$ o anel dos inteiros. O conjunto $(\mathbb{Z}(G), \oplus, \odot)$ formado de todas as somas formais $\sum_{g\in G} r_g(g)$ onde $r_g \in \mathbb{Z}$ e $r_g \neq 0$ para uma quantidade finita, com as seguintes operações de adição e multiplicação :

$$(i) \sum_{g\in G} r_g(g) \oplus \sum_{g\in G} s_g(g) = \sum_{g\in G} (r_g + s_g)(g)$$

$$(ii)(\sum_{g\in G} r_g(g)) \odot (\sum_{h\in G} s_h(h)) = \sum_{g,h\in G} r_g s_h(g.h),$$

é denominado o *anel de grupo de G sobre $\mathbb{Z}$*.

Como ilustração, dado o grupo multiplicativo $\mathbb{C}_3 = \{1, \beta, \beta^2\}$, onde $\beta^3 = 1$, considere o anel de grupo de $\mathbb{C}_3$ sobre $\mathbb{Z}$, $(\mathbb{Z}(\mathbb{C}_3), \oplus, \odot)$. Sejam α_1 e α_2 elementos em $(\mathbb{Z}(\mathbb{C}_3), \oplus, \odot)$ tais que $\alpha_1 = (1 \cdot \beta + 2 \cdot \beta^2)$ e $\alpha_2 = (1 \cdot 1 + 1 \cdot \beta^2)$. Assim

$$\begin{aligned} \alpha_1 \oplus \alpha_2 &= [1 \cdot \beta + 2 \cdot \beta^2] \oplus [1 \cdot 1 + 1 \cdot \beta^2] \\ &= 1 \cdot 1 + 1 \cdot \beta + (2+1) \cdot \beta^2 = 1 \cdot 1 + 1 \cdot \beta + 3 \cdot \beta^2. \end{aligned}$$

e

$$\begin{aligned}\alpha_1 \odot \alpha_2 &= [1\cdot\beta + 2\cdot\beta^2] \odot [1\cdot 1 + 1\cdot\beta^2] \\ &= [(1.1)\cdot(\beta\cdot 1)] + [(1.1)\cdot(\beta\cdot\beta^2)] + [(2.1)\cdot(\beta^2\cdot 1)] + [(2.1)\cdot(\beta^2\cdot\beta^2)] \\ &= 1\cdot\beta + 1\cdot 1 + 2\cdot\beta^2 + 2\cdot\beta = 1\cdot 1 + 3\cdot\beta + 2\cdot\beta^2.\end{aligned}$$

Observação 4.9. Sendo G um grupo abeliano e o anel dos inteiros $\mathbb{Z}$ comutativo, então prova-se que o anel de grupo $\mathbb{Z}(G)$ é comutativo. Para mais detalhes deste anel o leitor pode recorrer a [14]

Proposição 4.10. *Dados p um primo e G o p-grupo abeliano finito $\mathbb{Z}_{p^{e_1}} \times \mathbb{Z}_{p^{e_2}} \times ... \times \mathbb{Z}_{p^{e_r}}$, onde $r \in \mathbb{N}$, $e_i \in \mathbb{N}$ e $\mathbb{Z}_{p^{e_i}}$ grupo cíclico isomorfo a subgrupo de G com $1 \leq i \leq r$. Dada $S = (a_i)_{i=1}^k$ uma sequência em G, onde $k \geq 1 + \sum_{i=1}^{r}(p^{e_i} - 1)$ temos*

$$(1 - a_1)(1 - a_2)...(1 - a_k) \equiv 0 \ (mod\ p). \tag{4.1}$$

Demonstração: Consideremos $J = (1 - a_1)(1 - a_2)...(1 - a_k) \in \mathbb{Z}(G)$ e $x_i \in G$ tal que $\mathbb{Z}_{p^{e_i}} \cong < x_i >$ para todo $1 \leq i \leq r$, onde $< x_i >$ denota o subgrupo gerado por x_i. Se $a_i = u.v$ para algum $1 \leq i \leq k$, escreva J como

$$J = (1 - a_1)(1 - a_2)...(1 - a_{i-1})(1 - u)(1 - a_{i+1})...(1 - a_k) +$$

$$u(1 - a_1)...(1 - a_{i-1})(1 - v)(1 - a_{i+1})...(1 - a_k).$$

Como cada a_i é fatorado na forma $a_i = x_1^{n_{i_1}} \cdot ... \cdot x_r^{n_{i_r}}$, com $n_{i_j} \in \mathbb{N}$ para todos $1 \leq i \leq k$ e $1 \leq j \leq r$, reduzimos J a seguinte expressão

$$J = \sum_{\gamma} J_\gamma g_\gamma,$$

onde $g_\gamma \in G$ e $J_\gamma = (1 - x_1)^{f_1}(1 - x_2)^{f_2}...(1 - x_r)^{f_r}$. Os f_i's são inteiros não negativos que dependem de γ, com $\sum_{i=1}^{r} f_i = k$.

Como $\sum_{i=1}^{r} f_i = k > \sum_{i=1}^{r}(p^{e_i} - 1)$ então $f_i \geq p_{e_i}$ para todo $1 \leq i \leq r$. Mas pela expansão binomial neste anel, pelo fato que $\binom{p^{e_i}}{k} \equiv 0 \ (mod\ p)$ para todo $1 \leq k \leq p^{e_i - 1}$ e

$$(-1)^{p^{e_i}} x_i^{p^{e_i}} = \begin{cases} 1.1 & \text{se } p \text{ é par} \\ (-1).1 & \text{se } p \text{ é ímpar} \end{cases}$$

vem que

$$\begin{aligned}(1-x_i)^{p^{e_i}} &= \binom{p^{e_i}}{0} + \sum_{j=1}^{k-1}\binom{p^{e_i}}{j}(1)^{p^{e_i}-j}(-x_i)^j + (-1)^{p^{e_i}}(x_i)^{p^{e_i}} \\ &\equiv 1 + (-1)^{p^{e_i}}x_i^{p^{e_i}} \\ &\equiv 0\ (mod\ p).\end{aligned}$$

Assim $(1-x_i)^{f_i} = (1-x_i)^{f_i-p^{e_i}}(1-x_i)^{p^{e_i}} \equiv 0\ (mod\ p)$, logo como todos os coeficientes são congruentes a 0 módulo p, obtemos que $J_\gamma \equiv 0\ (mod\ p)$ para todo γ. Portanto $J \equiv 0\ (mod\ p)$. Como queríamos demonstrar. □

Notemos que no teorema anterior, quando afirmamos que o produto J em $\mathbb{Z}(G)$ é congruente a 0 módulo p, estamos querendo dizer que os coeficientes de cada fator do produto J, os quais são números inteiros, são congruente a 0 módulo p.

Definição 4.11. Dada $S = (a_i)_{i=1}^k$ uma sequência no p-grupo G. Defina

$$P_g(S) = \left|\left\{J \subset \{1,2,...,k\} | \prod_{j\in J} a_j = g,\ |J|\ par\right\}\right| e$$

$$I_g(S) = \left|\left\{J \subset \{1,2,...,k\} | \prod_{j\in J} a_j = g,\ |J|\ \text{ímpar}\right\}\right|.$$

Como ilustração, consideremos $S = ((\bar{0},\bar{0}),(\bar{1},\bar{0}),(\bar{1},\bar{1}),(\bar{2},\bar{2}))$ uma sequência em $\mathbb{Z}_3^2$. Assim $P_{\bar{0}}(S) = |\{J_1 = \{1,2\}, J_2 = \{1,3\}, J_3 = \{1,4\}, J_4 = \{1,2,3,4\}\}|$ e $I_{\bar{0}}(S) = |\{J_5 = \{1\}, J_6 = \{1,2,3\}, J_7 = \{1,2,4\}, J_8 = \{1,3,4\}|$. Logo $P_{\bar{0}}(S) = 4$ e $I_{\bar{0}}(S) = 4$.

Observação 4.12. Recordemos a definição do l-ésimo polinômio simétrico no anel de polinômios $\mathbb{Z}[x_1, x_2, ..., x_k]$, ou seja, para cada $l \in [1,k]$, temos que

$$p_l(x_1,...,x_k) = \sum_{1\le i_1<...<i_l\le k}\prod_{j=1}^{l} x_{i_j}.$$

Definição 4.13. Sejam $S = (a_i)_{i=1}^k$ uma sequência no p-grupo G. Para todo $1 \le l \le k$ definimos $A(l)$ como a soma formal dos produtos de todas as subsequências de S com tamanho l. Com a notação do l-ésimo polinômio simétrico em $\mathbb{Z}[x_1, x_2, ..., x_k]$ decorre que $A(l) = p_l(a_1,...,a_k) \in \mathbb{Z}(G)$.

Na próxima proposição onde S é uma sequência em G, estabeleceremos uma relação entre todas as subsequências de comprimentos pares e ímpares de modo que tenham produto igual a $g \in G$.

Proposição 4.14. *Para a sequência S, obtemos que*

$$P_g(S) - I_g(S) \equiv \begin{cases} 0 \ (mod\ p) & se \quad g \neq 1 \\ -1 \ (mod\ p) & se \quad g = 1 \end{cases}$$

Demonstração: De fato, consideremos $A(0) = 1 \in \mathbb{Z}(G)$ e $A(l) = p_l(a_1, ...a_k) \in \mathbb{Z}(G)$ para todo $l \in [1, k]$. Assim,

$$\begin{aligned} \prod_{i=1}^{k}(1 - a_i) &= \sum_{l=0}^{k}(-1)^l A(l) \\ &= (-1)^0 A(0) + \sum_{l=1}^{k}(-1)^l A(l) \\ &= 1.A(0) + \sum_{g\in G}(P_g(S) - I_g(S)).g \\ &= 1.A(0) + (P_1(S) - I_1(S)).1 + \sum_{\substack{g\in G \\ g\neq 1}}(P_g(S) - I_g(S)).g \\ &= (1 + P_1(S) - I_1(S)).1 + \sum_{\substack{g\in G \\ g\neq 1}}(P_g(S) - I_g(S)).g \end{aligned}$$

Pela equação (4.1) vem que $(1 + P_1(S) - I_1(S)) \equiv 0 \ (mod\ p)$ e $P_g(S) - I_g(S) \equiv 0 \ (mod\ p)$ para todo $g \in G$ com $g \neq 1$, completando a demonstração. □

Estamos prontos para calcular o valor exato da constante de Davenport para um p-grupo G.

Teorema 4.15. *Seja G um p-grupo abeliano finito como no Teorema 4.10. Então*

$$D(G) = 1 + \sum_{i=1}^{r}(p^{e_i} - 1).$$

Demonstração: Tomemos $k = 1 + \sum_{i=1}^{r}(p^{e_i} - 1)$. Primeiramente mostraremos que k é um limite inferior para $D(G)$, ou seja, provaremos que existe uma sequência de comprimento $k - 1$ a qual não possui subsequência de produto 1. De fato, sejam $x_i \in G$

com $1 \leq i \leq r$ uma base para G onde cada x_i tem ordem p^{e_i}. Consideremos S uma sequência de comprimento $k-1$ na qual cada x_i ocorre $p^{e_i}-1$ vezes para todo $i = 1, ..., r$. Suponhamos que exista um subsequência com produto 1, $T = T_1T_2$ de S com $|T| = t$ tal que T_1 é a subsequência onde o elemento x_{i_k} ocorre m vezes com $m \leq p^{e_i} - 1$ e $T_2 = (x_{i_j})_{j=m+1}^{t}$ onde os termos de T_2 são distintos entre si e dos termos de T_1. Como estamos na notação multiplicativa

$$1 = x_{i_k}^m \cdot x_{i_{m+1}} \cdot ... \cdot x_t.$$

Isso resulta que $x_{i_k}^m = (x_{i_{m+1}} \cdot ... \cdot x_{i_t})^{-1}$. Pela definição de produto direto de grupos [8], $\mathbb{Z}_{p^{e_i}} \cap (\mathbb{Z}_{p^{e_1}}...\mathbb{Z}_{p^{e_i-1}}\mathbb{Z}_{p^{e_i+1}}...\mathbb{Z}_{p^{e_r}}) = \{1\}$, ou seja, $x_{i_k}^m = 1$. Logo p^{e_i} é um divisor de m, mas isso é contrário ao fato de que $m \leq p^{e_i} - 1$.

Analisemos o limite superior, dada uma sequência $S' = (a_i)_{i=1}^{k}$ em G, afirmamos que S' possui subsequência de produto 1. Pois caso contrário, teríamos que S' não contém subsequência com tamanho par ou ímpar de produto 1, ou seja, $P_1(S') = I_1(S') = 0$. Logo aplicando a Proposição 4.14, vem que $0 = P_1(S') - I_1(S') \equiv -1 \ (mod\ p)$, gerando uma contradição. □

4.1.2 Mais resultados sobre $D(G)$

Novamente retornemos à notação aditiva. Nos anos de 1968 e 1969, após o Teorema 4.15, Olson e Baayen em [17] e [1] conjecturaram que para todo grupo G, $G = \mathbb{Z}_{n_1} \oplus ... \oplus \mathbb{Z}_{n_r}$, onde $n_1|n_2|...|n_r$, $D(G) = 1+\sum_{i=1}^{r}(n_i-1)$. Mas ainda em 1969, Van Emde Boas e Kruyswijk no artigo [20] refutaram essa conjectura, como observaremos no contra-exemplo abaixo, para tanto denotaremos $M(G) = 1 + \sum_{i=1}^{r}(n_i - 1)$. Para mais contra-exemplos o leitor poderá recorrer a [9] e [20].

Proposição 4.16. *Dados m, n inteiros positivos ímpares com $m \geq 3$, m um divisor de n e $G = (\mathbb{Z}_m \oplus \mathbb{Z}_n \oplus \mathbb{Z}_n \oplus \mathbb{Z}_{2n})$. Então $D(\mathbb{Z}_m \oplus \mathbb{Z}_n \oplus \mathbb{Z}_n \oplus \mathbb{Z}_{2n}) > M(\mathbb{Z}_m \oplus \mathbb{Z}_n \oplus \mathbb{Z}_n \oplus \mathbb{Z}_{2n})$.*

Demonstração: Sejam m, n inteiros positivos ímpares com $m \geq 3$ e $m \mid n$. Consideremos $\{e_1, e_2, e_3, e_4\}$ um sistema de geradores de G com as ordens de $e_1,\ e_2,\ e_3$ e e_4 iguais a

m, n, n e $2n$ respectivamente. Façamos $a_1 = -e_1+e_2+e_3+e_4$; $a_2 = e_1-e_2+e_3+e_4$; $a_3 = e_1+e_2-e_3+e_4$; $a_4 = -e_1+e_2+e_3-e_4$; $a_5 = e_1+e_2+e_3+e_4$; $a_6 = e_2+(2-m)e_3+(2-m)e_4$ e $a_7 = (2-m)e_2 + e_3 + (2-m)e_4$.

Considere a sequência onde $v_{a_1}(S) = m-1$, $v_{a_i}(S) = (n-1)$ para $2 \leq i \leq 5$ e $v_{a_6}(S) = v_{a_7}(S) = 1$. Assim $|S| = (m-1)+4(n-1)+2 = m+4n-3 = M(G)$. Afirmamos que S não possui subsequência soma-zero. Suponhamos o contrário que existem $I_1 \in \{0, ..., m-1\}$, $I_2, ..., I_5 \in \{0, ..., n-1\}$ e $I_6, I_7 \in \{0, 1\}$ tais que $\sum_{i=1}^{7} I_i > 0$ e $\sum_{i=1}^{7} I_i a_i = 0$. Assim obtemos o seguinte sistema de congruência,

$$
\begin{aligned}
&(i) \quad -I_1 + I_2 + I_3 - I_4 + I_5 \equiv 0 \ (mod\ m)\\
&(ii) \quad I_1 - I_2 + I_3 + I_4 + I_5 + I_6 + (2-m)I_7 \equiv 0 \ (mod\ n)\\
&(iii) \quad I_1 + I_2 - I_3 + I_4 + I_5 + (2-m)I_6 + I_7 \equiv 0 \ (mod\ n)\\
&(iv) \quad I_1 + I_2 + I_3 - I_4 + I_5 + (2-m)I_6 + (2-m)I_7 \equiv 0 \ (mod\ 2n).
\end{aligned}
$$

Analisemos dois casos:

Caso 1 : $I_6 = I_7$. Subtraindo (iii) de (ii) nós obtemos $-2I_2+2I_3 \equiv 0 \ (mod\ n)$ e assim $I_2 = I_3$, pois $I_2, I_3 \in \{0, ..., n-1\}$ e $I_2 \equiv I_3$. Agora fazendo $(iv) - (i)$ vem que $2I_1 + 4I_6 \equiv 0 \ (mod\ m)$ e portanto $I_1 = I_6(m-2)$. De (ii) concluimos que $I_4+I_5+I_6 \equiv 0 \ (mod\ n)$. Se $I_4 + I_5 + I_6 = 0$, então $I_4 = I_5 = I_6 = 0 = I_7$, logo (iv) implica que $I_2 + I_3 \equiv 0 \ (mod\ 2n)$, com isso $I_2 = I_3 = 0$ e então $\sum_{i=1}^{7} I_i = 0$, o que é uma contradição. Se $I_4+I_5+I_6 = n$, então $I_4+I_5+I_6 \equiv n \ (mod\ 2n)$. Adicionando (iv) obtemos $2I_3+2I_5+3I_6-mI_6 \equiv n \ (mod\ 2n)$. Desde que $2 \mid 3I_6 - mI_6$, segue que $2 \mid n$, uma contradição.

Caso 2 : $I_6 \neq I_7$. Sem perda de generalidade, assumimos que $I_6 = 1$ e $I_7 = 0$. Subtraindo (i) de (iv) segue que $2I_1 + 2 \equiv 0 \ (mod\ m)$ e assim $I_1 = m - 1$. Agora subtraindo (iii) de (iv) decorre que $2I_3 - 2I_4 \equiv 0 \ (mod\ n)$ implicando que $I_3 = I_4$. Então de (iv) temos $I_2 + I_5 + 1 \equiv 0 \ (mod\ 2n)$ uma contradição, pois se $I_2 = I_5 = 0$ teriamos que $1 \equiv 0 \ (mod\ 2n)$ o que é um absurdo. Portanto a proposição é válida. □

Proposição 4.17. *Fixe p primo e $S = (a_i)_{i=1}^{s}$ uma sequência em $\mathbb{Z}_p^2$, com $s \geq 3p-2$. Então S possui uma subsequência soma-zero de comprimento t com $1 \leq t \leq p$.*

Demonstração: Seja $S = (a_i)_{i=1}^{s}$ uma sequência em $\mathbb{Z}_p^2$ de comprimento $s \geq 3p-2$. Para todo $i = 1, 2, ..., s$, consideremos $b_i = (\bar{1}, a_i)$ elementos em $\mathbb{Z}_p^3$. Dessa maneira, $W = (b_i)_{i=1}^{s}$ é uma subsequência em $\mathbb{Z}_p^3$ de comprimento s. Pelo Teorema 4.15, $D(\mathbb{Z}_p^3) = 3p-2$, assim W contém uma subsequência soma-zero $T' = (\bar{1}, a_i)_{i=1}^{t}$ de comprimento $1 \leq t \leq s$, ou seja,

$$(0, \overline{0}) = \sigma(T') = \sum_{i=1}^{t} b_i = \left(\sum_{i=1}^{t} 1, \sum_{i=1}^{t} a_i \right).$$

Logo p é um divisor de t e $T = (a_i)_{i=1}^{t}$ é uma sequência soma-zero de S, assim $|T| = p$ ou $2p$. Se $|T| = p$ temos o desejado. Assumimos $|T| = 2p$, aplicando o Teorema 4.15 no grupo $\mathbb{Z}_p^2$ resulta que T possui uma subsequência soma-zero de comprimento $u \leq 2p-1$, digamos $U = (a_i)_{i=1}^{u}$. Se $u \leq p$, então o teorema esta provado. Caso contrário, temos que $2p - u < p$ e a subsequência TU^{-1} é soma-zero e de comprimento menor que p. □

No resultado seguinte, também exibiremos uma classe de valor exato para $D(G)$.

Teorema 4.18. *Dado $G = H \oplus K$, onde H, K são grupos abelianos de ordens $|H| = h$, $|K| = k$ com $h \mid k$. Então $D(G) \leq h + k - 1$.*

Demonstração: Seja $S = (a_i)_{i=1}^{s}$ uma sequência em G, onde $s \geq h+k-1$. Procederemos a demonstração por indução sobre a ordem do grupo H. Suponhamos $h = 1$, para todo $j = 1, ..., k$ definimos as seguintes somas parciais $\lambda_j = \sum_{i=1}^{j} a_i$. Se os λ_j são todos distintos e como $G \cong K$, segue que $\lambda_j = 0$ para algum $j \in [1, k]$, o que prova o teorema. Caso contrário, temos $\lambda_i = \lambda_j$ para certos $i, j \in [1, k]$, com $i < j$, então a subsequência $T = (a_l)_{l=i+1}^{j}$ é soma-zero.

Com isso, podemos supor que $h > 1$ e considere p um inteiro primo divisor de h, que por consequência divide k. Pela recíproca do Teorema de Lagrange para grupos abelianos finitos, existem os subgrupos $H_1 \leq H$ e $K_1 \leq K$ com índices p e ordens digamos h_1, k_1 respectivamente. Seja $Q = H_1 \oplus K_1$ com $|Q| < |G|$, pela hipótese de indução o teorema é válido para esse grupo. Sabemos que $G/Q \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$ e $s \geq h + k - 1$, ou seja, $s \geq p(h_1 + k_1 - 2) + 2p - 1$. Se $h_1 = k_1 = 1$, então $D(G) = D(\mathbb{Z}_p^2) = 2p - 1$ e o teorema está provado. Assim suponhamos que $h_1 \geq 1$ e $k_1 \geq 2$. Consideremos a sequência $T = (g_i + Q)_{i=1}^{s}$ em G/Q, como $s \geq p(h_1 + k_1 - 2) + 2p - 1 \geq 3p - 1$, pela Proposição 4.17

a sequência T possui uma subsequência soma-zero T_1 de comprimento t, com $1 \leq t \leq p$. Podemos novamente aplicar a Proposição 4.17 na sequência TT_1^{-1} para obtermos mais uma subsequência soma-zero T_2 de comprimento $t^{'}$ com $1 \leq t^{'} \leq p$.

Continuando esse processo, construimos $u-1 = h_1 + k_1 - 2$ subsequências soma-zero duas a duas disjuntas, $T_1, T_2, ..., T_{u-1}$, com comprimentos $|T_j| \in [1, p]$, para todo $j \in [1, u-1]$, ou seja $\sigma(S_j) = q_j \in Q$, sendo que S_j é a sequência formada pelos a_i que aparecem em T_j. Resta uma sequência de comprimento pelo menos $2p-1$, logo essa possui uma subsequência T_u disjunta das obtidas anteriormente, com soma igual a Q, isto é, $\sigma(S_u) = q_u \in Q$. Como $D(Q) \leq h_1 + k_1 - 1$, pela hipótese de indução, então a sequência $(q_j)_{j=1}^{u}$ em Q possui uma subsequência soma-zero $(q_i)_{i \in I}$, onde $I \subseteq [1, u]$. Logo S possui uma subsequência soma-zero $(a)_{i \in I; a \in S}$ em G. □

Lema 4.19. *Sejam $m,\ n \in \mathbb{N}$, m um divisor de n. Então $D(\mathbb{Z}_m \oplus \mathbb{Z}_n) = m + n - 1$.*

Demonstração: Pelo Teorema 4.18 obtemos que $m + n - 1$ é um limite superior para $D(\mathbb{Z}_m \oplus \mathbb{Z}_n)$. Para o limite inferior, construíremos uma sequência de comprimento $m+n-2$ e provaremos que essa sequência não possui uma subsequência soma-zero. Para isso, sejam $(x, 0), (0, y) \in G$ tais que $\mathbb{Z}_m \cong < (x, 0) >$ e $\mathbb{Z}_n \cong < (0, y) >$. Consideremos a sequência S em G formada por $m-1$ repetições do elemento $(x, 0)$ e $n-1$ repetições de $(0, y)$, ou seja, $S = (x, 0)_{i=1}^{m-1}(0, y)_{i=1}^{n-1}$. Suponhamos que exista uma subsequência T soma-zero de S. Então essa seria da forma $T = (x, 0)_{i=1}^{r}(0, y)_{i=1}^{s}$, com $r \leq m-1$, $s \leq n-1$. Como $\sigma(T) = 0$ vem que $0 = (rx, sy)$. Assim $m \mid r$, o que é uma contradição. Portanto S não possui subsequência soma-zero e o lema segue. □

Na demonstração do próximo resultado, utilizaremos novamente o recurso de através de sequências no grupo $\mathbb{Z}_n^{d+1}$, obter informações das sequências com soma-zero em $\mathbb{Z}_n^d$.

Lema 4.20. *Dados n e d inteiros positivos com $n \geq 2$ e $d \geq 1$, suponha que $D(\mathbb{Z}_n^{d+1}) = (d+1)(n-1)+1$. Qualquer sequência S em $\mathbb{Z}_n^d$ tal que $|S| = (d+1)(n-1)+1$ possui uma subsequência soma-zero T com $|T| = k.n$ para algum inteiro k satisfazendo $1 \leq k \leq d$.*

Demonstração: Seja $S = (a_i)_i^s$ uma sequência em $\mathbb{Z}_n^d$ tal que $s = (d+1)(n-1)+1$. Para todo $i = 1, 2, ..., (d+1)(n-1)+1$, consideremos $b_i = (\bar{1}, a_i)$ elementos em $\mathbb{Z}_n^{d+1}$. Com isso,

$W = (b_i)$ é uma sequência em $\mathbb{Z}_n^{d+1}$ de comprimento $(d+1)(n-1)+1$. Pela hipótese, W possui um subsequência T' soma-zero de comprimento t, com $1 \leq t \leq (d+1)(n-1)+1$, ou seja,

$$(0, \overline{0}) = \sigma(T') = \sum_{i=1}^{t} b_i = \left(\sum_{i=1}^{t} \overline{1}, \sum_{i=1}^{t} a_i\right) = \left(t, \sum_{i=1}^{t} a_i\right).$$

Assim, $t = kn$ e $T = (a_i)_{i=1}^{kn}$ é uma subsequência soma-zero de S em $\mathbb{Z}_p^n$ tal que $|T| = kn$ com $1 \leq k \leq d$. □

Do teorema anterior temos o seguinte corolário.

Corolário 4.21. *Fixemos p um primo e r um inteiro positivo. Seja S uma sequência em $\mathbb{Z}_{p^r}^d$ de comprimento $(d+1)(p^r-1)+1$. Então S possui uma subsequência soma-zero de comprimento kp^r, com $1 \leq k \leq d$.*

Demonstração: Pelo Teorema 4.15, $D(\mathbb{Z}_{p^r}^{d+1}) = (d+1)(p^r-1)+1$. Assim pelo Lema 4.20, a sequência S em $\mathbb{Z}_{p^r}^d$ de comprimento $(d+1)(p^r-1)+1$ possui uma subsequência soma-zero T de comprimento $k.p^r$, com $1 \leq k \leq d$. □

A partir desse momento, extrairemos resultados no grupo $\mathbb{Z}_p^d$, onde p é um primo. Antes precisaremos da seguinte definição.

Definição 4.22. Seja $S = (a_i)_{i=1}^{l}$ uma sequência em $\mathbb{Z}_p^d$. Defina

$$r(S;q) = \left|\left\{I \subset \{1,2,...,l\} | \sum_{i \in I} a_i = 0,\ |I| = qp\right\}\right|$$

Lema 4.23. *Dados d, q inteiros positivos e p um número primo com $d \geq 2$, $1 \leq q \leq d$ e $p \geq d+2$. Considere T uma sequência em $\mathbb{Z}_p^d$ com $(d+1)(p-1)+1 \leq |T| \leq (d+2)p-1$. Suponha que T não possui subsequência soma-zero de comprimento kp, para todo $k \in \{1,2,...,d+1\} \backslash q$. Então*

$$r(T;q) \equiv (-1)^{q+1} \ (mod\ p).$$

Demonstração: Seja $T = (a_i)_{i=1}^{t}$ uma sequência em $\mathbb{Z}_p^d$ tal que $|T| = t$, com $(d+1)(p-1)+1 \leq t \leq (d+2)p+1$. Para todo $i = 1,2,...,t$, considere $b_i = (\overline{1}, a_i) \in \mathbb{Z}_p^{d+1}$. Dessa maneira, $W = (b_i)_{i=1}^{t}$ é uma sequência em $\mathbb{Z}_p^{d+1}$. Como $t \geq D(\mathbb{Z}_p^{d+1})$, W possui uma subsequência soma-zero V' com $|V'| = r$. Assim $\sum_{i=1}^{r} b_i = \sum_{i=1}^{r} (\overline{1}, a_i) = \left(\sum_{i=1}^{r} 1, \sum_{i=1}^{r} a_i\right) =$

$(0, \bar{0})$, logo $r = \bar{0}$ em $\mathbb{Z}_p$, ou seja, $p \mid r = |V^{'}|$. Seja V a subsequência soma-zero em T correspondente a $V^{'}$, então $p \mid |V|$ e assim $|V| = kp$ para algum $k \in \{1, 2, ..., d+1\}$. Por hipótese, T não contém subsequência soma-zero de comprimento kp com $k \in \{1, 2, ..., d+1\}\backslash\{q\}$, com isso $|V| = qp$. Portanto, da Definição 4.22, ou $r(T, q) = P_0(W) - 1$, se $2 \mid q$ ou $r(T, q) = I_0(W)$, se $2 \nmid q$.

Analisemos esses dois casos. No primeiro caso, $r(T, q) + 1 = P_0(W)$, como $2 \mid q$ temos que $|V^{'}| = |V|$ é par, logo $I_0(W) \equiv 0 \ (mod\ p)$, pois $\sigma(V^{'}) = 0$ em $\mathbb{Z}_p^{d+1}$. Pelo Proposição 4.14, $P_0(W) \equiv I_0(W) \ (mod\ p)$, assim $r(T, q) + 1 \equiv 0 \ (mod\ p)$. Sabemos que $-1 \equiv -1 \ (mod\ p)$, disso decorre que $r(T, q) + 1 - 1 \equiv 0 - 1 \ (mod\ p)$ ou ainda $r(T, q) \equiv -1$.

No segundo caso, $r(T, q) = I_0(W)$, como $2 \nmid q$ temos que $|V^{'}|$ é ímpar, logo $P_0(W) = 1$. Novamente pelo Proposição 4.14, $r(T, q) = I_0(W) \equiv P_0(W) = 1 \ (mod\ p)$. Assim $r(T, q) \equiv 1 \ (mod\ p)$. Portanto $r(T, q) \equiv (-1)^{q+1}$. □

Observação 4.24. No Lema 4.23, assumimos um limite superior para $|T|$, com o objetivo de assegurar que $|V| \neq (d+2)p$.

Teorema 4.25. *Fixados d, q inteiros e p um primo com $d \geq 2$, $1 \leq q \leq d$ e $p \geq d+2$. Seja S uma sequência em $\mathbb{Z}_p^d$ de comprimento pelo menos $(d+2)(p-1)+2$. Então S contém uma subsequência soma-zero de comprimento kp para algum inteiro $k \in \{1, 2, ..., d+1\}\backslash q$. Além disso, para todo $q \in \{1, 2, ..., d\}\backslash\{\frac{d+1}{2}\}$, S contém uma subsequência soma-zero de comprimento kp com $k \in \{1, 2, ..., d\}\backslash\{l\}$.*

Demonstração: Suponhamos o contrário, que existe uma sequência S em $\mathbb{Z}_p^d$ com $|S| = (d+2)(p-1)+2$ tal que S não possui subsequência soma-zero de comprimento kp para todo $k \in \{1, 2, ..., d+1\}\backslash\{q\}$. Pelo Lema 4.23, temos que $r(T, q) \equiv (-1)^{q+1} \ (mod\ p)$ é verdadeiro para toda subsequência T de S com $|T| \geq (d+1)(p-1)+1$. Consideremos os seguintes conjuntos:

$$A = \left\{ I : \ I \subset \{1, 2, ..., |S|\}, \ \sum_{i \in I} a_i = 0, \ |I| = qp \right\}$$

e

$$B = \left\{ T : \ T \subset \{1, 2, ..., |S|\}, \ |T| = (d+1)(p-1)+1 \right\},$$

onde $(a_t)_{t\in T}$ é uma subsequência de S. Criemos uma relação R de A em B dada por $I\ R\ T$ se, e somente se, $I \subset T$. Consideremos o conjunto $R = \{(I,T) \in A \times B : I \subseteq T\}$. Assim contaremos a cardinalidade do conjunto R de duas maneiras distintas. Primeiramente fixado T, vemos que o total de pares ordenados (I,T) em R é exatamente $r(T,q)$. Logo $|U| = \sum_{|T|=(d+1)(p-1)+1} r(T,q)$, com $(a_t)_{t\in T}$ uma subsequência de S. Agora fixado I, temos que o total de pares ordenados (I,T) em R é $\binom{(d+2)(p-1)+2-qp}{(d+1)(p-1)+1-qp}$ e um total de $r(S,q)$ elementos em A, ou seja, $|R| = \binom{(d+2)(p-1)+2-qp}{(d+1)(p-1)+1-qp} r(S,q)$. Portanto temos a seguinte igualdade,

$$\sum_{|T|=(d+1)(p-1)+1} r(T,q) = \binom{(d+2)(p-1)+2-qp}{(d+1)(p-1)+1-qp} r(S,q).$$

Novamente pelo Lema 4.23, vem que

$$\sum_{|T|=(d+1)(p-1)+1} (-1)^{q+1} \equiv \binom{(d+2-q)p-d}{(d+1-q)p-d} (-1)^{q+1}\ (mod\ p).$$

Isso resulta que

$$\binom{(d+2)(p-1)+2}{(d+1)(p-1)+1} \equiv \binom{(d+2-q)p-d}{(d+1-q)-d}\ (mod\ p).$$

Lembrando a identidade binomial $\binom{n}{m} = \binom{n}{n-m}$ com $n \geq m$, vem que

$$\begin{aligned} d+1 &\equiv \binom{(d+2)(p-1)+2}{p} \equiv \binom{(d+2)(p-1)+2}{(d+1)(p-1)+1} \\ &\equiv \binom{(d+2-q)p-d}{(d+1-q)p-d} \equiv \binom{(d+2-q)p-d}{p} \\ &\equiv d+1-q\ (mod\ p), \end{aligned}$$

o qual é uma contradição. Isso prova a primeira parte do teorema. Para mostrarmos a segunda parte, suponhamos que $q \neq \frac{d+1}{2}$. Pela primeira parte, existe uma subsequência soma-zero V tal que $|V| = kp$ com $k \in \{1,2,...,d+1\}\backslash\{q\}$. Se $k \leq d$, então já temos feito. Por outro lado, $|V| = (d+1)p$ e pelo Corolário 4.21 a sequência V possui uma subsequência soma-zero W com $|W| = hp$ e $1 \leq h \leq d$. Assim, VW^{-1} é também uma subsequência soma-zero de V com $|VW^{-1}| = (d+1-h)p$. Assumindo $h = q$ e $d+1-h = q$, nós obtemos $q = \frac{d+1}{2}$, uma contradição. □

Com a próxima definição introduziremos uma nova função, $E_k(G)$, que foi apresentada em 2000 por Gao no artigo [7].

Definição 4.26. Seja k um inteiro positivo qualquer. Denotaremos por $E_k(G)$ o menor inteiro positivo t tal que toda sequência em G de comprimento pelo menos t contém uma subsequência T soma-zero com $k \nmid |T|$.

No próximo teorema estimaremos um valor exato para a $E_k(\mathbb{Z}_p^d)$.

Teorema 4.27. *Se p é um primo ímpar e k um inteiro positivo tal que $(k,p)=1$, então*

$$E_k(\mathbb{Z}_p^d) = \left\lfloor \frac{k}{k-1} d(p-1) \right\rfloor + 1.$$

Demonstração: O leitor poderá consultar a demonstração em [7] para o caso de $k=1$ e em [18] para o caso geral. □

Teorema 4.28. *Sejam p um primo ímpar e k um inteiro positivo tal que $(k,p)=1$, então toda sequência de comprimento $\left\lfloor \frac{k}{k-1}(d+1)(p-1) \right\rfloor + 1$ em $\mathbb{Z}_p^d$ possui uma subsequência soma-zero de comprimento rp com $k \nmid r$.*

Demonstração: Seja $l = \left\lfloor \frac{k}{k-1}(d+1)(p-1) \right\rfloor + 1$ e $S = (a_i)_{i=1}^{l}$ uma sequência em $\mathbb{Z}_p^d$ tal que $|S| = l$. Para $i = 1, 2, ..., l$ considere $b_i = (\overline{1}, a_i) \in \mathbb{Z}_p^{d+1}$. Dessa maneira $W = (b_i)_{i=1}^{l}$ é uma sequência em $\mathbb{Z}_p^{d+1}$ de comprimento l. Pelo Teorema 4.27, W possui uma subsequência T soma-zero com $k \nmid |T|$. Tome $|T| = t$, se necessário fazendo uma reenumeração de índices, temos

$$(0, \overline{0}) = \sigma(T) = \sum_{i=1}^{t} b_i = \left(t, \sum_{i=1}^{t} a_i \right).$$

Assim p divide t e $T' = (a_i)_{i=1}^{t}$ é uma subsequência soma-zero de S. Portanto, $|T'| = rp$ para algum inteiro r com $k \nmid r$ (pois como $k \nmid t$, $k \nmid p$ e $t = rp$, temos que $k \nmid r$). □

Novamente na demonstração do resultado acima, utilizamos o grupo $\mathbb{Z}_p^{d+1}$, ou seja, aumentamos uma dimensão para obtermos resultado em $\mathbb{Z}_p^d$.

Lema 4.29. *Seja S uma sequência em $\mathbb{Z}_3^3$ de comprimento 12. Suponha que S não é uma sequência soma-zero. Então S contém uma subsequência soma-zero de comprimento 6.*

Demonstração: Seja $S = (a_i)_{i=1}^{12}$ uma sequência em $\mathbb{Z}_3^3$ de comprimento 12, onde $a_i = (a_i^1, a_i^2, a_i^3)$ para todo $i = 1, ..., 12$. Vamos assumir que $v_g(S) \leq 5$ para todo $g \in \mathbb{Z}_3^3$,

pois caso contrário $U = (g)_{i=1}^{6}$ seria a subsequência desejada. Afirmamos que existe uma subsequência T de S de comprimento 9 tal que T não é soma-zero. De fato, suponhamos que toda subsequência de S de comprimento 9 é soma-zero. Dividimos S em quatro subsequências de comprimento 3, digamos $I_1 = (a_1, a_2, a_3)$, $I_2 = (a_4, a_5, a_6)$, $I_3 = (a_7, a_8, a_9)$ e $I_4 = (a_{10}, a_{11}, a_{12})$.

Com isso escrevemos as seguintes subsequências de comprimento 9, digamos $T_1 = I_1I_2I_3$, $T_2 = I_1I_2I_4$, $T_3 = I_1I_3I_4$ e $T_4 = I_2I_3I_4$. Agora consideremos $\pi^j(\sigma(T_i))$ com $j = 1, 2, 3$ e $i = 1, 2, 3, 4$, as projeções de $\sigma(T_i)$ com relação as três coordenadas e escrevemos os seguintes números em $\mathbb{Z}_3$:

$$\begin{aligned}
x_1 &= a_1^1 + a_2^1 + a_3^1; x_2 = a_1^2 + a_2^2 + a_3^2; x_3 = a_1^3 + a_2^3 + a_3^3; \\
x_4 &= a_4^1 + a_5^1 + a_6^1; x_5 = a_4^2 + a_5^2 + a_6^2; x_6 = a_4^3 + a_5^3 + a_6^3; \\
x_7 &= a_7^1 + a_8^1 + a_9^1; x_8 = a_7^2 + a_8^2 + a_9^2; x_9 = a_7^3 + a_8^3 + a_9^3; \\
x_{10} &= a_{10}^1 + a_{11}^1 + a_{12}^1; x_{11} = a_{10}^2 + a_{11}^2 + a_{12}^2; x_{12} = a_{10}^3 + a_{11}^3 + a_{12}^3.
\end{aligned}$$

Como por hipótese $\sigma(T_i) = (\bar{0}, \bar{0}, \bar{0})$ para todo $i = 1, 2, 3, 4$, obtemos o seguinte sistema em $\mathbb{Z}_3$,

$$\begin{cases}
x_1 + x_4 + x_7 = \bar{0} \\
x_2 + x_5 + x_8 = \bar{0} \\
x_3 + x_6 + x_9 = \bar{0} \\
x_1 + x_4 + x_{10} = \bar{0} \\
x_2 + x_5 + x_{11} = \bar{0} \\
x_3 + x_6 + x_{12} = \bar{0} \\
x_1 + x_7 + x_{10} = \bar{0} \\
x_2 + x_8 + x_{11} = \bar{0} \\
x_3 + x_9 + x_{12} = \bar{0} \\
x_4 + x_7 + x_{10} = \bar{0} \\
x_5 + x_8 + x_{11} = \bar{0} \\
x_6 + x_9 + x_{12} = \bar{0}
\end{cases} \tag{4.2}$$

O sistema é homogêneo e admite apenas solução trivial, isto é, $x_1 = x_2 = x_3 = x_4 = ... = x_{12} = \bar{0}$ em $\mathbb{Z}_3$. Então

$$\sigma(S) = \sum_{i=1}^{12} a_i = (x_1 + x_4 + x_7 + x_{10}, x_2 + x_5 + x_8 + x_{11}, x_3 + x_6 + x_9 + x_{12}) = (\bar{0}, \bar{0}, \bar{0})$$

contradizendo o fato de que S não é soma-zero. Agora pelo Corolário 4.21, T possui uma subsequência T_1 soma-zero de comprimento 3 ou 6. Se $|T_1| = 6$ temos o desejado. Assuma que $|T_1| = 3$, logo a subsequência ST^{-1} é de comprimento 9. Desde que S não é soma-zero, ST^{-1} também não é uma subsequência soma-zero de S. Novamente pelo Corolário 4.21, existe uma subsequência T_2 soma-zero de ST^{-1} de comprimento 3 ou 6. Se $|T_2| = 3$, então T_1T_2 é a subsequência soma-zero desejada. Por outro lado, T_2 faz esse papel. □

Capítulo 5

Função $s_k(G)$

Naturalmente, surgem outros questionamentos quando estabelecemos propriedades adicionais para a subsequência soma-zero de uma dada sequência. Assim para um grupo abeliano finito G, $s_k(G)$ denotará o menor inteiro positivo t tal que toda sequência de comprimento pelo menos t, possui uma subsequência soma-zero de comprimento $k.exp(G)$. Neste capítulo, abordaremos o estudo dessa função. Para algumas classes particulares, como veremos na última seção desse capítulo, valores exatos são conhecidos, mas na maioria dos casos, como na constante de Davenport, apenas conseguimos aproximações. Salvo mensão contrária, G sempre denotará um grupo abeliano finito escrito aditivamente e consequentemente o elemento neutro de G será denotado por 0.

Definição 5.1. Definimos o *exponente de* G, denotado por exp(G), como o menor inteiro positivo tal que $exp(G).g = 0$ para todo $g \in G$.

Exemplo 5.2. Dados n um inteiro positivo e o grupo $G = \mathbb{Z}_n$, vemos que n é o menor inteiro positivo tal que $n.g = \bar{0}$ para todo $g \in \mathbb{Z}_n$ e assim $exp(\mathbb{Z}_n) = n$.

Definição 5.3. Fixado k um inteiro positivo, $s_k(G)$ denota o menor inteiro positivo t tal que toda sequência S em G de comprimento pelo menos t possui uma subsequência soma-zero de comprimento $k.exp(G)$.

Ressaltamos que encontrar valores exatos para a função $s_k(G)$ também não é uma tarefa fácil. Abaixo apresentaremos alguns resultados para o caso de $k = 1$.

Proposição 5.4. *Dado n um inteiro positivo, $s_1(\mathbb{Z}_n) = 2n - 1$.*

Demonstração: Seja S uma sequência em $\mathbb{Z}_n$ de comprimento $2n - 1$. Pelo Teorema de Erdos-Ginzburd-Ziv, S possui uma subsequência soma-zero de comprimento $1.n = 1.exp(\mathbb{Z}_n)$, visto que $exp(\mathbb{Z}_n) = n$, conforme o Exemplo 5.2. Assim $s_1(\mathbb{Z}_n) \leq 2n - 1$. Agora defina $S_1 = (\bar{0}, \bar{0}, \bar{0}, ..., \bar{0}, \bar{1}, \bar{1}, \bar{1}, ..., \bar{1})$ uma sequência em $\mathbb{Z}_n$ com $v_0(S_1) = v_1(S_1) = n-1$ tal que $|S_1| = 2n-2$. Assim S_1 não possui subsequência soma-zero de comprimento $1.exp(\mathbb{Z}_n)$. Logo $s_1(\mathbb{Z}_n) > 2n - 2$, completando a demonstração. □

Notemos que o limite superior da proposição anterior segue diretamento do Teorema de Erdös-Ginzburg-Ziv. Abaixo apresentamos uma generalização da proposição acima.

Teorema 5.5. *Dados n e k inteiros positivos,*

$$s_k(\mathbb{Z}_n) = kn + n - 1.$$

Demonstração: Procederemos a demostração por indução sobre k. O caso $k = 1$ segue da Proposição 5.4. Suponhamos que $s_k(\mathbb{Z}_n) = k.n + n - 1$ e provaremos que $s_{k+1}(\mathbb{Z}_n) = (k+1).n+n-1$. Considere S uma sequência em $\mathbb{Z}_n$ com $|S| = (k+1)n+n-1$, mostraremos que S possui uma subsequência soma-zero de comprimento $(k + 1).n$. De fato, como $|S| > s_k(\mathbb{Z}_n)$ então S possui uma subsequência T soma-zero de comprimento kn. Assim a sequência ST^{-1} tem comprimento $2n - 1$ e, pela Proposição 5.4, contém uma subsequência T_1 soma-zero de comprimento n. Por conseguinte, a subsequência TT_1 soma-zero tem comprimento $kn+n = (k+1)n$. Agora para o limite inferior consideremos a sequência $S_1 = (0)_{i=1}^{kn}(1)_{i=1}^{2n-2}$ de comprimento $(k + 1)n + n - 2$ com $v_0(S) = kn$ e $v_1(S) = 2n - 2$. Notemos que S não possui subsequência soma-zero de comprimento $(k + 1)n$. □

Como comentado anteriormente, a busca de um valor exato da função $s_k(\mathbb{Z}_n^d)$ para o caso $k = 1$ também não é uma tarefa fácil. Para o caso geral, são conhecidos limites inferior e superior para $s_1(\mathbb{Z}_n^d)$.

Teorema 5.6. *Fixados n e d inteiros positivos,*

$$(n-1)2^d + 1 \leq s_1(\mathbb{Z}_n^d) \leq (n-1)n^d + 1. \tag{5.1}$$

Demonstração: Para o limite inferior, considere S uma sequência em $\mathbb{Z}_n^d$ de comprimento $(n-1)2^d$ tal que os termos de S sejam $(n-1)$ cópias de cada um dos 2^d vetores com entradas 0 ou 1. Assim não conseguimos extrair de S uma subsequência soma-zero de comprimento n, pois para cada subsequência com tamanho n temos que a soma de cada coordenada vista como números inteiros é sempre menor do que n, logo não é congruente a 0 módulo n, satisfazendo o limite inferior. Para o limite superior, notemos que em qualquer sequência S de comprimento $(n-1)n^d + 1$ em $\mathbb{Z}_n^d$, $v_g(S) \geq n$ para algum $g \in \mathbb{Z}_n^d$, pelo Princípio da Casa dos Pombos. Logo a subsequência $T = (g)_{i=1}^n$ é soma-zero e de comprimento n, completando a demonstração. □

No teorema abaixo, estimaremos um limite inferior de $s_k(G)$ em função da constante de Davenport, mais precisamente,

Teorema 5.7. *Dados $exp(G) = n$ e k inteiro positivo. Valem as estimativas*

1. $s_k(G) \geq kn + D(G) - 1$.
2. *Se* $k < \frac{D(G)}{n}$ *então* $s_k(G) > kn + D(G)$.

Demonstração: 1. Seja $S = (a_1, a_2, ..., a_{D(G)-1})$ uma sequência de comprimento $|S| = D(G) - 1$ e $\sigma(S) \neq 0$. Considere a sequência $T = (0)_{i=1}^{kn-1}(a_i)_{i=1}^{D(G)}$ em G, onde $kn - 1$ primeiros termos são iguais a 0 e os outros $D(G)-1$ termos são os termos da sequência S. Assim T não possui subsequência soma-zero de comprimento kn e $|T| = kn + D(G) - 2$. Portanto $D(G) \geq kn + D(G) - 1$.

2. Para $kn < D(G)$, seja $S = (a_1, a_2, ..., a_{D(G)})$ uma sequência minimal soma-zero em G de comprimento $D(G)$. Considere $T = (0)_{i=1}^{kn-1}(a_i)_{i=1}^{D(G)}$, logo T não contém subsequência soma-zero de comprimento kn e $|T| = kn + D(G) - 1$. Portanto $s_k(G) > kn + D(G) - 1$. □

Um limite inferior para $s_k(\mathbb{Z}_n^d)$ é estimado abaixo.

Lema 5.8. *Dados d e k inteiros tais que $1 \leq k \leq d-1$. Para qualquer inteiro positivo n, vale*

$$s_k(\mathbb{Z}_n^d) \geq n(d+k) + \left\lfloor \frac{(d-k)n-1}{d-1} \right\rfloor - d.$$

Demonstração: Seja $T = (1)_{t=1}^{s}(e_i^{n-1})_{t=1}^{d}$, onde $e_i = (0,0,...,1,...,0)$ para todo $i = 1,2,...,d$ e $s = \left\lfloor \frac{(d-k)n-1}{d-1} \right\rfloor$. Notemos que qualquer subsequência W soma-zero será da forma $W = (1)_{t=1}^{i}(e_j^{n-i})_{j=1}^{d}$ e portanto $|W| = d(n-i)+i = dn-(d-1)i$. Como $i \leq s$ e $s = \left\lfloor \frac{(d-k)n-1}{d-1} \right\rfloor$, vem que $i \leq \left\lfloor \frac{(d-k)n-1}{d-1} \right\rfloor$, ou ainda, $(d-1)i \leq dn-kn-1$. Logo $kn+1 \leq dn-(d-1)i = |W|$, com isso $|W| > kn$. Agora considere $S = T(0)_{t=1}^{kn-1}$ uma sequência em Z_n^d cujo comprimento é $|T|+kn-1 = d(n-1)+s+kn-1 = dn-d+s+kn-1 = (d+k).n+s-d-1$. Claramente, pela construção de S, decorre que S não tem subsequência soma-zero de comprimento kn, completando a demonstração. □

No próximo resultado, estimaremos um limite superior para a função $s_{kl}(G)$, com k, l inteiros positivos.

Lema 5.9. *Consideremos os inteiros $k,l \geq 1$. Então*

$$s_{kl}(G) \leq (l-1)k.exp(G) + s_k(G).$$

Demonstração: Definamos $m = (l-1)k.exp(G) + s_k(G) + s_k(G)$ e $S = (a_i)_{i=1}^{m}$ uma sequência em G de comprimento m. Mostraremos que S possui uma subsequência soma-zero de comprimento $kl.exp(G)$. Pela definição de m, podemos extrair l subsequências soma-zero disjuntas, digamos $T_1, T_2, ..., T_l$ de S tal que $|T_i| = k.exp(G)$ para cada i. Portanto a sequência $T_1T_2...T_l$ é a subsequência soma-zero de S desejada. □

5.1 Estimativas sobre s_k para alguns grupos

A partir dos resultados anteriores e do quarto capítulo, apresentaremos estimativas inferiores e superiores para s_k sobre alguns grupos. No primeiro teorema apresentaremos estimativas para a função $s_k(\mathbb{Z}_p^3)$, onde p é primo e $k \geq 4$.

Teorema 5.10. *Seja p um número primo, $p \geq 5$, vale*

(i) $5p + \frac{p-1}{2} - 3 \leq s_2(\mathbb{Z}_p^3) \leq 6p - 3$;

(ii) $6p - 3 \leq s_3(\mathbb{Z}_p^3) \leq 8p - 7$;

(iii) $s_k(\mathbb{Z}_p^3) = kp + 3p - 3$, *para todo* $k \geq 4$.

Demonstração: (i) O limite inferior segue do Lema 5.8, tomando $d = 3,\ l = 2$ *e* $n = p$. Para o limite superior, consideremos S uma sequência em $\mathbb{Z}_p^3$ de comprimento $6p - 3$, mostraremos que S contém uma subsequência de comprimento $2p$. Da segunda parte do Teorema 4.25, fazendo $d = q = 3$, decorre que S possui uma subsequência T de comprimento p ou $2p$. Assumimos que $|T| = p$, pois caso contrário teremos o desejado. Agora considere a subsequência ST^{-1} de comprimento $5p-3$, novamente pela segunda parte do Teorema 4.25 com $q = 3$, obtemos uma subsequência T_1 soma-zero de comprimento p ou $2p$. Suponhamos que $|T_1| = p$, pois caso contrário o resultado segue, assim a subsequência TT_1 é a desejada.

(ii) O limite inferior decorre do Teorema 5.7 e do Teorema 4.15. Para o limite superior, seja S uma sequência em $\mathbb{Z}_p^3$ de comprimento $8p - 7$, provaremos que S contém uma subsequência de comprimento $3p$. Pelo Teorema 4.28 com $k = 2$, S possui uma subsequência T tal que $|T| = p,\ 3p,\ 5p$ ou $7p$. Suponhamos $|T| = p$, logo a sequência ST^{-1} tem comprimento $7p - 7$. Assim por (i), a sequência ST^{-1} possui uma subsequência T_1 soma-zero com $|T_1| = 2p$. Então TT_1 é uma subsequência de S de comprimento $3p$. Se $|T| = 3p$, o resultado segue. Agora suponhamos que $|T| = 5p$, pela segunda parte do Teorema 4.25 com $d = 3$ e $q = 1$, a sequência T possui uma subsequência T_2 de comprimento $2p$ ou $3p$. Assumimos que $|T_2| = 2p$, pois caso contrário obtemos o desejado. Assim a subsequência TT_2^{-1} soma-zero de S tem comprimento $3p$. Finalmente consideremos que $|T| = 7p$ por (i) existe uma subsequência T_3 soma-zero de comprimento $2p$. Logo a subsequência TT_3^{-1} soma-zero tem comprimento $5p$. Desde que $|TT_3^{-1}| = 5p$, pelo argumento do caso anterior, obteremos uma subsequência soma-zero de S de comprimento $3p$.

(iii) Primeiramente provaremos que $s_k(\mathbb{Z}_p^3) = 2kp + 3p - 3$ e assim mostraremos que $S_{2(k+1)}(\mathbb{Z}_p^3) = 2(k+1)p + 3p - 3$ para todo inteiro $k \geq 2$. Seja S uma sequência em $\mathbb{Z}_p^3$ de comprimento $2kp + 3p - 3$. Suponhamos que $k = 2$, logo $|S| = 7p - 3$ mostraremos que S contém uma subsequência soma-zero de comprimento $4p$. Por (ii), S possui uma sub-

sequência T_1 soma-zero de comprimento $2p$. Observamos que $|ST_1^{-1}| = 5p-3$. Aplicando o Teorema 4.25 com $q = 3$, vemos que ST_1^{-1} contém uma subsequência T_2 soma-zero de comprimento p ou $2p$. Se $|T_2| = 2p$, então T_1T_2 é a subsequência soma-zero procurada. Assim podemos assumir que $|T_2| = p$. Como $|ST_1^{-1}T_2^{-1}| = 4p-3$, pelo Corolário 4.21, $ST_1^{-1}T_2^{-1}$ possui uma subsequência T_3 soma-zero de comprimento p, $2p$ ou $3p$. Assim $T_1T_2T_3$, T_1T_3 ou T_2T_3 é uma subsequência soma-zero de S de comprimento $4p$, para $|T_3| = p$ $2p$ ou $3p$, respectivamente. Logo $s_4(\mathbb{Z}_p^3) \leq 7p-3$. Contudo, pelo Teorema 5.7, $s_4(\mathbb{Z}_p^3) \geq 4p + D(\mathbb{Z}_p^3) - 1 = 4p + (3(p-1)+1) - 1 = 7p-3$, disso decorre que $S_4(\mathbb{Z}_p^3) = 4p + 3p - 3$.

Assumindo que o resultado é válido para $k \geq 2$, provaremos para $k+1$. Através do Teorema 5.7, basta provarmos que $s_{2(k+1)}(\mathbb{Z}_p^3) \leq 2(k+1)p+3p-3$. Seja S_1 uma sequência em $\mathbb{Z}_p^3$ com $|S_1| = 2(k+1)p + 3p - 3$. Sendo $k \geq 2$ e $s_2(\mathbb{Z}_p^3) \leq 6p-3$, S_1 possui uma subsequência T_4 soma-zero de comprimento $2p$. Assim, $|S_1T_4^{-1}| = 2kp + 5p - 3 - 2p = 2kp + 3p - 3$, logo pela hipótese de indução $S_1T_4^{-1}$ possui uma subsequência T_5 soma-zero com $|T_5| = 2kp$. Logo T_4T_5 é uma subsequência soma-zero de S_1 de comprimento $2(k+1)p$. Portanto $s_{2k}(\mathbb{Z}_p^3) = 2kp + 3p - 3$ para todo inteiro $k \geq 2$.

Agora mostraremos que $s_5(\mathbb{Z}_p^3) = 8p-3$. Novamente pelo Teorema 5.7, basta provarmos que $s_5(\mathbb{Z}_p^3) \leq 8p-3$. Seja S uma sequência em $\mathbb{Z}_p^3$ de comprimento $8p-3$, mostraremos que S contém uma subsequência soma-zero de comprimento $5p$. Do Teorema 4.28 com $k = 2$, S possui uma subsequência T soma-zero de comprimento rp com $r \in \{1,3,5,7\}$. Analisemos os quatro casos. Se $|T| = 5p$ temos o desejado. Se $|T| = p$ e como $s_4(\mathbb{Z}_p^3) = 7p-3$ obtemos uma subsequência T_1 de ST^{-1} de comprimento $4p$, logo TT_1 é a subsequência desejada. Se $|T| = 7p$, novamente usando o fato que $s_4(\mathbb{Z}_p^3) = 7p-3$, obtemos uma subsequência T_2 soma-zero de T de comprimento $4p$, logo TT_2^{-1} tem comprimento $3p$. Assim podemos assumir que S contém uma subsequência T soma-zero de comprimento $3p$, observemos que $|ST^{-1}| = 5p-3$. Pelo Teorema 4.25, fazendo $d = q = 3$, ST^{-1} possui uma subsequência T_2 tal que $|T_2| = mp$ com $m \in \{1,2\}$. Se $|T_2| = 2p$, então $|TT_2| = 5p$. Por outro lado, se $|T_2| = p$, segue do caso acima. Se $|T| = 5p$ o resultado segue. Portanto $s_5(\mathbb{Z}_p^3) = 8p-3$. Finalmente, para provarmos que $s_k(\mathbb{Z}_p^3) = kp + 3p - 3$ para todo inteiro ímpar $k \geq 7$, consideremos S uma sequência em $\mathbb{Z}_p^3$ de comprimento

$kp+3p-3$. Mostraremos que S possui uma subsequência de comprimento kp. Desde que $k \geq 7$, como $S_2(\mathbb{Z}_p^3) \leq 6p-3$, S contém uma subsequência T soma-zero de comprimento $2p$. Vemos que a sequência ST^{-1} tem comprimento $(k-2)p+3p-3$, pela hipótese de indução, ST^{-1} possui uma subsequência T_1 soma-zero de comprimento $(k-2)p$, sendo $k-2 \geq 5$ e ímpar. Assim TT_1 é a subsequência desejada. □

No próximo teorema encontraremos estimativas $s_k(\mathbb{Z}_3^3)$ onde p é um primo e $k \geq 4$.

Teorema 5.11. *Dado $k \geq 2$ um inteiro positivo, valem as estimativas.*

(i) $s_2(\mathbb{Z}_3^3) = 13$;

$(ii) 15 \leq s_3(\mathbb{Z}_3^3) \leq 17$;

(iii) $s_k(\mathbb{Z}_p^3) = 3k+6$, *para todo* $k \geq 4$.

Demonstração: (i) Do Teorema 5.7 vem que $s_2(\mathbb{Z}_3^3) \geq 13$. Logo resta provarmos que $S_2(\mathbb{Z}_3^3) \leq 13$. Seja S uma sequência em $\mathbb{Z}_3^3$ tal que $|S| = 13$, mostraremos que S possui uma subsequência soma-zero de comprimento 6. Se $v_g(S) \geq 6$ para todo $g \in \mathbb{Z}_3^3$, obteremos uma subsequência $(a_i)_{i=1}^6$ com $a_i = g$ para todo i, tal que $\sum_{i=1}^{6} a_i = 6g = 0$, isto é, uma subsequência soma-zero de comprimento 6. Assim assumiremos que $v_g(S) \leq 5$ para todo $g \in \mathbb{Z}_3^3$. Logo podemos encontrar uma subsequência T de S tal que $|T| = 12$ e T não é subsequência soma-zero (mesmo argumento da demonstração do Lema 4.29). Portanto pelo Lema 4.29 existe uma subsequência T_2 soma-zero de T, consequentemente de S, de comprimento 6.

(ii) Pelo Teorema 5.7 obtemos o limite inferior. Resta mostrarmos o superior. Seja S uma sequência em $\mathbb{Z}_3^3$ de comprimento 17, provaremos que S tem uma subsequência de comprimento 9. Fazendo $k = 2$ no Teorema 4.28, vem que S tem uma subsequência T de comprimento 3, 9 ou 15. Logo basta analisarmos $|T| = 3$ ou 15, pois caso contrário obtemos a subsequência desejada. Se $|T| = 3$, logo $|ST^{-1}| = 14$ e por (ii) existe uma subsequência T_1 soma-zero de comprimento 6 em ST^{-1}, assim TT_1 é a subsequência desejada. Agora se $|T| = 15$, novamente por (i), T possui uma subsequência T_2 soma-zero de comprimento 6, assim TT_2^{-1} é uma subsequência soma-zero de comprimento 9.

(iii) Provaremos por indução sobre k que $s_k(\mathbb{Z}_3^3) = 3k+6$, para $k \geq 4$. Então para $k = 4$ temos pelo Teorema 5.7 que $s_4(\mathbb{Z}_3^3) \geq 18$. Resta mostrarmos que $s_4(\mathbb{Z}_3^3) \leq 18$. Seja

S uma sequência em $\mathbb{Z}_3^3$ tal que $|S| = 18$, provaremos que S contém uma subsequência soma-zero de comprimento 12. Por (ii), S possui uma subsequência T soma-zero de comprimento 6. Logo $|ST^{-1}| = 12$, se ST^{-1} é soma-zero temos o desejado. Caso contrário, pelo Lema 4.29 obtemos uma subsequência T_1 soma-zero de ST^{-1}. Assim TT_1 é a subsequência desejada.

Assumindo que $s_k(\mathbb{Z}_3^3) = 3k+6$ é válido para algum $k \geq 4$, faremos para $k+1$. Seja S uma sequência em $\mathbb{Z}_3^3$ de comprimento $3(k+1)+6$. Visto em [10] e [11] que $s_1(\mathbb{Z}_3^3) = 19$, S contém uma subsequência soma-zero T de comprimento 3. Como a sequência ST^{-1} tem comprimento $3k+6$, pela hipótese de indução, existe uma subsequência T_1 soma-zero de ST^{-1} com $|T_1| = 3k$. Logo TT_1 é uma subsequência soma-zero de S de comprimento $3k+3 = 3(k+1)$. Portanto, $s_k(\mathbb{Z}_3^3) = 3k+6$ para todo $k \geq 4$. □

No teorema seguinte estimamos valores exatos para a função $s_k(\mathbb{Z}_2^3)$ com $k \geq 2$.

Teorema 5.12. *Seja k inteiro positivo, então $s_k(\mathbb{Z}_2^3) = 2k+3$ para todo $k \geq 2$.*

Demonstração: Provaremos por indução sobre $k \geq 2$. Pelo Teorema 5.7, temos $s_2(\mathbb{Z}_2^3) \geq 7$. Resta mostrarmos que $s_2(\mathbb{Z}_2^3) \leq 7$, considere S uma sequência em $\mathbb{Z}_2^3$ com $|S| = 7$. Provaremos que S contém uma subsequência soma-zero de comprimento 4. Pelo Corolário 4.21, S possui uma subsequência soma-zero T_1 de comprimento 2 ou 4. Assuma que $|T| = 2$, pois caso contrário temos o desejado. Como $|ST^{-1}| = 5$, novamente pelo Corolário 4.21 obtemos uma subsequência T_1 soma-zero de ST^{-1} tal que $|T_1| = 2$ ou 4. Suponha que $|T_1| = 2$, pois caso contrário temos o desejado. Assim TT_1 é a subsequência almejada. Portanto $s_2(\mathbb{Z}_2^3) = 7$.

Agora suponhamos que $s_k(\mathbb{Z}_2^3) = 2k+3$ é válido para algum $k \geq 2$, faremos para $k+1$. Pelo Teorema 5.7, $s_{k+1}(\mathbb{Z}_2^3) \geq 2(k+1)+3$. Resta mostrarmos que $s_{k+1}(\mathbb{Z}_2^3) \leq 2(k+1)+3$. Considere S uma sequência em $\mathbb{Z}_2^3$ de comprimento $2(k+1)+3$. Como $s_k(\mathbb{Z}_2^3) = 2k+3$, S possui uma subsequência T soma-zero de comprimento $2k$. Logo $|ST^{-1}| = 5$, então pelo Corolário 4.21, ST^{-1} possui uma subsequência T_1 soma-zero de comprimento 2. Nesse caso TT_1 é uma subsequência soma-zero de comprimento $2(k+1)$. Portanto $s_k(\mathbb{Z}_2^3) = 2k+3$ para todo $k \geq 2$. □

No próximo teorema estimaremos um limite inferior para $s_{6k}(\mathbb{Z}_p^4)$ com $p \geq 7$.

Teorema 5.13. *Para todo inteiro $k \geq 1$ e todo primo $p \geq 7$, temos*

$$s_{6k}(\mathbb{Z}_p^4) \leq 6(k+1)p - 4 \tag{5.2}$$

Demonstração: Considere p um primo com $p \geq 7$. Tomando $k = 1$ e $l = 6$ no Lema 5.9, obtemos que $s_6(\mathbb{Z}_p^4) \leq 12p-4$. Considere S uma sequência em $\mathbb{Z}_p^4$ de comprimento $12p-4$. Pelo Teorema 4.25, sabemos que todo sequência em $\mathbb{Z}_p^4$ de comprimento $6p-4$ possui uma subsequência de comprimento qp com $q \in \{1,2,3,4\}\backslash r$ para todo $r \in \{1,2,3,4\}$. Analisemos alguns casos:

Caso (i): S tem duas subsequências soma-zero disjuntas T_1 e T_2 de comprimento $3p$. Nesse caso, temos que T_1T_2 é a subsequência soma-zero de comprimento $6p$ desejada.

Caso (ii): Caso (i) não acontece, mas S possui uma subsequência T de comprimento $3p$. Nesse caso, consideremos a sequência ST^{-1} a qual tem comprimento $9p-4$. Claramente, ST^{-1} não tem uma subsequência soma-zero de comprimento $3p$. Fazendo $q = 4 = d$ no Teorema 4.25, ST^{-1} possui subsequências soma-zero disjuntas T_1, T_2, T_3 ou T_4, T_5 ou T_6, T_7 com comprimentos $p,\ p,\ p$ ou $p,\ 2p$ ou $2p,\ 2p$, respectivamente. Nos dois primeiros casos, $TT_1T_2T_3$ ou TT_4T_5 são as subsequências soma-zero de comprimento $6p$ desejadas. Dessa maneira, assumimos que ST^{-1} tem duas subsequências soma-zero disjuntas de comprimentos $2p$. Notemos que $|ST^{-1}T_6^{-1}T_7^{-1}| = 5p-4$, logo pelo Corolário 4.21, possui uma subsequência soma-zero de comprimento rp com $r \in \{1,2,3,4\}$. Assim para qualquer valor de r obteremos uma subsequência soma-zero de S de comprimento $6p$.

Caso (iii): S não tem nenhuma subsequência soma-zero de comprimento $3p$. Dessa maneira, pelo Teorema 4.25 com $q = 4 = d$, as possíveis subsequências soma-zero disjuntas de S terão comprimentos $2p$, $2p$, $2p$. Portanto S possui uma subsequência soma-zero de comprimento $6p$. □

No último teorema dessa seção, sendo S uma sequência em $\mathbb{Z}_p^3$ com $p \geq 5$ contendo duas subsequências soma-zero de comprimento $2p$, ainda conseguimos encontrar uma subsequência soma-zero em S de comprimento p.

Teorema 5.14. *Sejam $p \geq 5$ um número primo e S uma sequência em $\mathbb{Z}_p^3$ de comprimento $9p-3$. Suponhamos que S possui no máximo duas subsequências soma-zero*

disjuntas de comprimento $2p$. *Então* S *contém uma subsequência soma-zero de comprimento* p.

Demonstração: Pelo Teorema 5.10-(*iii*), $s_6(\mathbb{Z}_p^3) = 9p - 3$, então S possui uma subsequência de soma-zero T de comprimento $6p$. Usando o fato de que $s_2(\mathbb{Z}_p^3) \leq 6p - 3$, existe uma subsequência soma-zero T_1 de T de comprimento $2p$. Assim TT_1^{-1} é uma subsequência soma-zero de comprimento $4p$. Pelo Corolário 4.21, TT_1^{-1} possui uma subsequência soma-zero T_2 tal que $|T_2| = p,\ 2p$ *ou* $3p$. Se $|T_2| = p$ temos o desejado. Se $|T_2| = 2p$, então $TT_1^{-1}T_2^{-1}$ é também uma subsequência soma-zero de S de comprimento $2p$. Dessa maneira, T_1,$TT_1^{-1}T_2^{-1}$ e T_2 são subsequências soma-zero disjuntas de comprimento $2p$, o que contraria a hipótese. Agora se $|T_2| = 3p$, $TT_1^{-1}T_2^{-1}$ é uma subsequência soma-zero de S de comprimento p. □

Bibliografia

[1] BAAYEN, P. C., *Een Combinatorisch Probleem Voor Eindige Abelse Groepen*. Math. Centrum Syllabus 5, Colloq Wiskunde Caput 3, Math. Centre, Amsterdam, 1968.

[2] DAVENPORT, H.,*On the Addition of Residue Classes*. Journal London Mathematical Society. 10, 30-32, 1935.

[3] EGGLETON, R.B. and ERDÖS, P.*Two Combinatoriol Problems in Group Theory*. Acta Arithmetica, 21, 111-116, 1972.

[4] ERDÖS, P., GINZBURG, A. and ZIV, A., *A theorem in Additive Number Theory* Bull. Research Council, Israel 10F, 41-43, 1961.

[5] GAO, W.D., *Two Addition Theorems on Groups of Prime Order*. Journal of Number Theory 56, 211-213, 1996.

[6] GAO, W. D. and RAVINDRANATHAN, T., *On Zero-Sum Sequences of Prescribe Length*. Aequations Mathematical, 72, 201-212, 2006.

[7] GAO, W. D., *On Zero-Sum Subsequences of Restricted Size III*. Ars Combinatoria, 61, 65-72, 2001.

[8] GARCIA, A. e LEQUAIN, Y., *Elementos de Álgebra*, 4 ed. Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2006.

[9] GEROLDINGER, A. and SCHINEIDER, R., *On Davenport's Constant*. Journal of Combinatorial Theory, Series A 61, 147-152, 1992.

[10] HARBORTH, H., *Ein Extremslproblem für Gitterpunkte*. Journal Reine Angrewandte Mathematik. 262/263, 356-360, 1973.

[11] KEMNITZ, A., *On a Lattice Point Problem*. Ars Combinatorica. 16 b, 151-160, 1983.

[12] MANN, H. B., *Two Addition Theorems*. Journal Combinatorial Theory 3, 233-235, 1967.

[13] MOSER, L., SCHERK, P., *Distinct Elements in a Set of Sums*. American Math. Monthly, 46-47, 1955.

[14] MILIES, C. P., Anéis e Módulos. IME-USP, São Paulo, 1972.

[15] NATHANSON, M. B., *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*. New York, Springer-Verlag, 1996.

[16] NATHANSON, M. B., *Inverse Theorems for Subset Sums*. Transactions of the American Mathematical Society 347, 1409-1418, 1995.

[17] OLSON, J. E., *A Combinatorial Problem on Finite Abelian Groups I and II*. Journal Number Theory 1, 8-11, 195-199, 1968.

[18] SCHMID, W. A., *On Zero-Sum Subsequences in Finite Abelian Groups*. Integers 1, A1, 8 pp, 2001.

[19] SILVA, K. A. A., *Sequências de Soma Zero em Grupos Abelianos Finitos*. Dissertação de Mestrado, UFG, 2007.

[20] VAN EMDE BOAS, P., KRUYSWIJK, D., *A Combinatorial Problem on Finite Abelian Groups III*. Math. Centre, Amsterdam. Report ZW-008-1969.

Índice