Universidade Federal de Goiás

Instituto de Matemática e Estatística

Seqüências de Soma Zero em Grupos Abelianos Finitos

Kênio Alexsom de Almeida Silva

Orientador: Dr. Paulo Henrique de Azevedo Rodrigues

Dissertação de Mestrado em Matemática

Goiânia, Goiás

2007

Universidade Federal de Goiás

Instituto de Matemática e Estatística

Coordenação de Pós-Graduação em Matemática

Seqüências de Soma Zero em Grupos Abelianos Finitos

por

Kênio Alexsom de Almeida Silva

Área de concentração: Álgebra

Orientador: Dr. Paulo Henrique de Azevedo Rodrigues

Dissertação submetida à Banca Examinadora designada pelo Conselho Diretor do Instituto de Matemática e Estatística da Universidade Federal de Goiás, como parte dos requisitos necessários à obtenção do grau de Mestre em Matemática.

Goiânia, Goiás

2007

Sumário

Resumo

Dado um grupo abeliano finito $(G, +)$ consideramos os seguintes invariantes de G: $D(G)$, $s(G)$ e $s_0(G)$.

Neste trabalho estudamos $D(G)$ para G sendo um p-grupo e para o produto direto de dois grupos cíclicos onde a ordem de um deles divide a do outro. Estes resultados são de Olson [15] e [16]. Também estudamos a demonstração de Christian Reiher [17] para a Conjectura de Kemnitz, a qual declara que $s(C_n \times C_n) = 4n - 3$ para todo $n \in \mathbb{N}$, onde C_n é o grupo cíclico de ordem n.

Em outras palavras, esta Conjectura afirma que dadas quaisquer $4n - 3$ duplas de inteiros (não necessariamente distintas) sempre podemos escolher n delas de forma que a sua soma tenha as duas coordenadas divisíveis por n.

Além disso, vimos o seguinte resultado de Gao e Geroldinger [9]: $s_0(C_n \times C_n) = 3n - 2$ para todo $n \geq 2 \in \mathbb{N}$. Isto significa que dadas quaisquer $3n - 2$ duplas de inteiros (não necessariamente distintas) sempre existem m delas de forma que m e a soma destas duplas tenha as duas coordenadas divisíveis por n. Também obtivemos outros resultados relevantes como, por exemplo, que $s(C_{3^n}^3) = 9 \cdot 3^n - 8$, para todo $n \in \mathbb{N}$.

Abstract

Let $(G, +)$ an finite abelian group, we consider the following invariants of G: $D(G)$, $s(G)$ and $s_0(G)$.

In this work we study $D(G)$ for G being a $p-$group and the direct product of two cyclic groups where the order of one of them divides of another one. These results were obtained by Olson in [15] and [16]. Also, we study the proof of Christian Reiher in [17] for the Kemnitz'Conjecture, which declares that $s(C_n \times C_n) = 4n - 3$ for all $n \in \mathbb{N}$, where C_n is the cyclic group of order n.

In other words, this Conjecture affirms that given any $4n - 3$ double of integers (not necessarily distincts) we always can choose n of them of form that its sum has the two coordinates divisible for n.

Moreover, we saw the following result of Gao and Geroldinger [9]: $s_0(C_n \times C_n) = 3n-2$ for all $n \geq 2 \in \mathbb{N}$. This means that given any $3n - 2$ double of integers (not necessarily distincts), always exist m of them of form that m and the sum of these pairs has the two coordinates divisible for n. Also we got other excellent results as, for example, that $s(C_{3^n}^3) = 9 \cdot 3^n - 8$, for all $n \in \mathbb{N}$.

Introdução

Aspectos históricos

As pesquisas em Teoria dos Números relacionadas com seqüências em Grupos Abelianos Finitos surgiram com o trabalho conjunto de P. Erdös, A. Ginzburg e A. Ziv [5]. Neste artigo eles provaram o seguinte teorema:

Teorema de Erdös, Ginzburg e Ziv. *Dados quaisquer $2n-1$ inteiros sempre podemos achar n inteiros cuja soma seja divisível por n.*

Definimos para um grupo abeliano finito G o número $s(G)$ como sendo o menor inteiro positivo s tal que para qualquer seqüência de tamanho s exista uma subseqüência tendo soma zero e com tamanho igual a $exp(G)$. Sendo que $exp(G)$ é o expoente do grupo, ou seja, é o menor inteiro positivo l tal que para todo $g \in G$ tem-se $lg = 0$.

Uma afirmação equivalente ao Teorema acima é a seguinte: $s(C_n) = 2n - 1$ para o grupo cíclico C_n de ordem n.

Alguns anos depois, P. Erdös propôs a determinação de $s(C_p \times C_p)$ onde p é um inteiro primo.

Em abril de 1966, durante a *Midwestern Conference on Group Theory and Number Theory, Ohio State University*, H. Davenport propôs a seguinte questão:

Se R é o anel de inteiros de um corpo F de números algébricos, qual é o número maximal de classes de ideais primos (contando a multiplicidade) na decomposição em ideais primos de aR para um inteiro irredutível a em R?

Definindo para um grupo abeliano finito G o número $D(G)$ como sendo o menor inteiro positivo d tal que para qualquer seqüência de tamanho d exista uma subseqüência com soma zero. Agora tomando G como sendo o grupo de classes de ideais primos de R na questão anterior, Davenport mostrou que o número procurado é o $D(G)$, o qual é chamado a constante de Davenport de G.

Em 1969, J. Olson [15] provou que para o p-grupo, $G = C_{p^{e_1}} \times \cdots \times C_{p^{e_r}}$, onde p é um inteiro primo e r, e_i para todo $i \in \{1, \ldots, r\}$ são inteiros positivos, tem-se $D(G) = 1 + \sum_{i=1}^{r} (p^{e_i} - 1)$. Em [16], Olson mostrou que para o grupo $G = C_m \times C_n$ com m divisor de n tem-se $D(G) = m + n - 1$.

H. Harborth [10], em 1973, conseguiu as seguintes cotas inferior e superior para $s(C_n^d)$, onde C_n^d é o grupo formado por d cópias de C_n com $n,\ d$ inteiros positivos:

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

Neste mesmo artigo Harborth também obteve a seguinte cota superior para $s(C_{nm}^d)$ com $n,\ m,\ d$ inteiros positivos:

$$s(C_{nm}^d) \leq min\{s(C_n^d) + (s(C_m^d) - 1)n, s(C_m^d) + (s(C_n^d) - 1)m\}. \tag{2}$$

Para o grupo C_n^2 onde n é um inteiro positivo, A. Kemnitz [14], em 1983, conjecturou que $s(C_n^2) = 4n - 3$, ou seja, que a cota inferior dada em [10] é atingida, ele provou que basta considerarmos n primo.

L. Rónyai [19] provou que, para p primo, vale $s(C_p^2) \leq 4p - 2$. Depois W. Gao [7] estendeu isto para potências de primos, $s(C_{p^a}^2) \leq 4p^a - 2$ com a inteiro positivo.

Em 2003, C. Reiher anuncia a veracidade da conjectura de Kemnitz, este resultado será publicado em [17].

Também em 2003, W. Gao e A. Geroldinger [9], provam que $s_0(C_n^2) = 3n - 2$ se a conjectura de Kemnitz, $s(C_n^2) = 4n - 3$, para todo $n \in \mathbb{N}$, for verdadeira. Onde o invariante $s_0(G)$ é definido para um grupo abeliano finito G como sendo o menor inteiro positivo l tal que para qualquer seqüência de tamanho l exista uma subseqüência com soma zero e tamanho divisível por $exp(G)$.

Para o leitor interessado em saber um pouco mais a respeito da Teoria de soma zero em Grupos Abelianos Finitos recomendamos o artigo: Weidong Gao, Alfred Geroldinger, *Zero-sum problems in finite abelian groups: A survey*, Expo. Math. (2006), doi: 10.1016/j.exmath.2006.07.002. Neste os autores apresentam uma visão geral da teoria de soma zero para grupos abelianos finitos e dos problemas inversos relacionados.

Estrutura da dissertação

Esta dissertação está dividida em quatro capítulos da seguinte forma.

No primeiro capítulo, *Preliminares*, apresentaremos os conceitos e objetos matemáticos que nos servirão de base para obtermos os resultados mais importantes do trabalho. Neste capítulo descreveremos o monóide abeliano livre $\mathcal{F}(G)$ e o anel de grupo $\mathbb{Z}(G)$ de G sobre $\mathbb{Z}$, sendo que o primeiro será essencial ao longo do texto, e o último será útil apenas no Capítulo 2.

No segundo capítulo, *Um Problema Combinatório em Grupos Abelianos Finitos*, apresentaremos os principais resultados contidos nos artigos [15] e [16]. Na primeira seção determinaremos a constante de Davenport, $D(G)$ para um p-grupo abeliano finito. Na última seção determinaremos a constante de Davenport para o grupo $C_m \times C_n$ com m divisor de n, e veremos uma Conjectura de P. Erdös sobre inteiros gaussianos, assim como uma generalização do Teorema de Erdös, Ginzburg e Ziv.

No terceiro capítulo, *A Conjectura de Kemnitz*, apresentaremos o objetivo principal deste trabalho, o artigo [17], onde Christian Reiher faz uma demonstração elegante para a Conjectura de Kemnitz. Na primeira seção enunciaremos a Conjectura, juntamente com algumas observações pertinentes, entre elas está a inequação (1). Na segunda seção veremos o Teorema de Chevalley-Warning e alguns resultados que serão utilizados na conclusão da veracidade da Conjectura.

No último capítulo, *Subseqüências de soma zero e tamanho restrito em um grupo abeliano finito*, apresentaremos na primeira seção o seguinte resultado de Gao e Geroldinger [9], $s_0(C_n^2) = 3n-2$ para todo inteiro $n \geq 2$. Nas seções seguintes veremos dois resultados sobre o invariante $s(G)$ para um grupo G abeliano finito, os quais foram demonstrados em [3] por Gao e outros. Na segunda seção veremos uma generalização da desigualdade (2). Além disso, veremos que $s(C_n \times C_m) \leq 2(m+n) - 3$ sempre que n e m são inteiros satisfazendo $n, m \geq 2$ e n é um divisor de m.

Na última seção, veremos que $s(C_{3^n}^3) = 9 \cdot 3^n - 8$ e $s(C_{2^n}^d) = (2^n - 1)2^d + 1$ para todos $d, n \in \mathbb{N}$.

Finalmente, concluíremos o trabalho apresentando alguns resultados recentes que estão relacionados com a nossa proposta de estudo.

Capítulo 1

Preliminares

Neste capítulo descreveremos os objetos matemáticos a serem utilizados ao longo do trabalho.

Usaremos a notação aditiva para os grupos abelianos exceto no segundo capítulo, onde a notação será a multiplicativa. Para $n \in \mathbb{N}$, C_n denotará o grupo cíclico com n elementos, ou seja, o grupo aditivo formado pelas classes de congrüência módulo n.

Para $n, m \in \mathbb{N}, n < m$, denotaremos o conjunto $\{n, \ldots, m\}$ por $[n, m]$.

Nas seções seguintes descreveremos sucintamente o monóide abeliano livre com base G, onde G é um grupo abeliano finito, e o anel de grupo de G sobre o anel dos inteiros $\mathbb{Z}$. Estes objetos formarão o ambiente de trabalho da dissertação.

1.1 O monóide abeliano livre $\mathcal{F}(G)$

Sejam G um grupo abeliano finito, $S = \prod_{g \in G} g^{v_g(S)}$ uma justaposição de elementos em G, onde a função v_g está definida para cada $g \in G$ por $v_g : \mathcal{F}(G) \to \mathbb{N} \cup \{0\}$, $v_g(S) = m$, com m sendo o número de vezes que o símbolo g aparece em S. Chamaremos S de seqüência, a qual também será denotada por $S = \prod_{i=1}^{l} g_i$. A seqüência onde ocorrer $v_g(S) = 0$ para todo $g \in G$ será denotada por 1 e será chamada de seqüência vazia.

O domínio da função v_g, $\mathcal{F}(G)$, é o conjunto formado pelos $S's$. Dadas S, $T \in \mathcal{F}(G)$ definimos uma seqüência justapondo os símbolos de T aos de S, a qual será denotada por $S \cdot T$. Com esta operação prova-se que o conjunto $\mathcal{F}(G)$ é um monóide abeliano, veja [12] pg 64.

Além disso, para a função $i : G \to \mathcal{F}(G)$ definida por $i(g) = g$ para todo $g \in G$, dada qualquer função de conjuntos $f : G \to H$, onde H é um monóide abeliano, pode-se provar que existe um único homomorfismo $\overline{f} : \mathcal{F}(G) \to H$ tal que $\overline{f} \circ i = f$. Isto significa que $\mathcal{F}(G)$ é um monóide abeliano livre com base G. Assim, usaremos o símbolo $\mathcal{F}(G)$ para denotar este monóide, para mais detalhes veja [12] ou [18] pg 44.

Uma seqüência S' será chamada uma subseqüência da seqüência $S \in \mathcal{F}(G)$, se existir alguma seqüência $S'' \in \mathcal{F}(G)$ tal que $S = S' \cdot S''$, ou seja, $v_g(S') \leq v_g(S)$ para todo $g \in G$. Neste caso, escreveremos $S' \mid S$ e $S'' = (S')^{-1} \cdot S$, onde S'' é a seqüência $S'' = \prod_{g \in G} g^{v_g(S) - v_g(S')}$.

Sejam $S_1, \ldots, S_k \in \mathcal{F}(G)$ subseqüências de S, diremos que elas são duas a duas disjuntas se sua justaposição $\prod_{i=1}^{k} S_i$ for uma subseqüência de S.

Dada uma seqüência $S = \prod_{g \in G} g^{v_g(S)} \in \mathcal{F}(G)$ definiremos sua soma por $\sigma(S) = \sum_{g \in G} v_g(S)g$ e seu tamanho por $|S| = \sum_{g \in G} v_g(S)$, notemos que a soma de S é a soma em G dos símbolos que aparecem em S. Diremos que a seqüência S tem soma zero quando $\sigma(S) = 0$. Agora se a operação do grupo G for a multiplicativa, para a seqüência S anterior definiremos o seu produto por $\pi(S) = \prod_{g \in G} g^{v_g(S)} \in G$, notemos que aqui estamos multiplicando os elementos $g^{v_g(S)}$ para todo $g \in G$. Quando o produto $\pi(S)$ for igual a $1 \in G$, diremos que a seqüência S tem produto 1.

Para grupos abelianos finitos aditivos H, G e uma função $f : G \to H$, definiremos uma função de $\mathcal{F}(G)$ em $\mathcal{F}(H)$ por $f(S) = \prod_{i=1}^{l} f(g_i)$ para toda seqüência $S = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)$, por abuso de notação usaremos o mesmo símbolo para denotar estas funções. Se f for um homomorfismo, então $f(S)$ tem soma zero se, e somente se, $\sigma(S) \in ker(f)$. Com efeito,

$$\begin{aligned}
\sigma(f(S)) &= \sum_{i=1}^{l} f(g_i) \\
&= f(\sum_{i=1}^{l} g_i) \\
&= f(\sigma(S)).
\end{aligned}$$

1.2 O anel de grupo $\mathbb{Z}(G)$ de G sobre $\mathbb{Z}$

Seja G um grupo abeliano, $\mathbb{Z}$ o anel dos inteiros, consideremos o conjunto $\mathbb{Z}(G)$ de todas as somas formais

$$\sum_{g \in G} r_g g$$

onde $r_g \in \mathbb{Z}$ e a quantidade de $r_g \neq 0$ é finita. Definimos neste conjunto as seguintes operações de adição e de multiplicação:

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

ii) $\displaystyle(\sum_{g \in G} r_g g) \cdot (\sum_{g \in G} s_g g) = \sum_{g \in G} (\sum_{yz = g} r_y \cdot s_z) g.$

Pode-se verificar que $(\mathbb{Z}(G), +, \cdot)$ é um anel com elemento identidade $1_{\mathbb{Z}} 0_G$, denotado por 1, chamamos este de o *anel de grupo de* G *sobre* $\mathbb{Z}$.

Como o grupo G é abeliano, e o anel $\mathbb{Z}$ é comutativo, então prova-se que o anel de grupo $\mathbb{Z}(G)$ é comutativo.

Para detalhes sobre este anel veja [12] pg 116, [18] pg 214.

Capítulo 2

Um Problema Combinatório em Grupos Abelianos Finitos

Neste capítulo veremos os principais resultados contidos nos artigos [15] e [16] de J. Olson. Na primeira seção determinaremos a constante de Davenport, $D(G)$ para um p-grupo abeliano finito com p inteiro positivo primo. Na segunda seção determinaremos a constante de Davenport para o grupo $C_m \times C_n$ com m divisor de n, e veremos uma Conjectura de P. Erdös sobre inteiros gaussianos, além disso veremos uma generalização do Teorema de Erdös, Ginzburg e Ziv, provado em [5].

Adotaremos, excepcionalmente neste capítulo, a notação multiplicativa para os grupos abelianos finitos.

2.1 A constante de Davenport de um p-grupo

A seguir definiremos formalmente o invariante $D(G)$ para um grupo abeliano G.

Definição 2.1. Seja G um grupo abeliano finito, definimos $D(G)$ como sendo o menor inteiro positivo d, tal que para toda seqüência $S \in \mathcal{F}(G)$ com tamanho $|S| \geq d$, existe uma subseqüência $T \in \mathcal{F}(G)$ com produto igual a 1, isto é, $\pi(T) = 1$. Chamamos o invariante $D(G)$ de constante de Davenport do grupo G.

Consideremos p um inteiro positivo primo, G o p-grupo abeliano finito $C_{p^{e_1}} \times \cdots \times C_{p^{e_r}}$, onde $r \in \mathbb{N}$, $e_i \in \mathbb{N}$ e $C_{p^{e_i}}$, $i \in [1, r]$, são grupos cíclicos isomorfos a subgrupos de G, ou seja, G é o produto interno de grupos cíclicos. Provaremos o seguinte resultado:

Teorema 2.2. *Nas condições acima temos que*

$$D(G) = 1 + \sum_{i=1}^{r} (p^{e_i} - 1). \tag{2.1}$$

Para tanto veremos um teorema declarado no contexto do anel de grupo de G sobre $\mathbb{Z}$, $\mathbb{Z}(G)$, definido no Capítulo 1 Seção 1.2.

Teorema 2.3. *Nas condições acima, sejam $g_1, \ldots, g_k \in G$, onde $k \geq 1 + \sum_{i=1}^{r} (p^{e_i} - 1)$, então*

$$(1 - g_1) \cdot \ldots \cdot (1 - g_k) \equiv 0 \,(mod\, p). \tag{2.2}$$

Demonstração. Consideremos $J = \prod_{i=1}^{k}(1 - g_i) \in \mathbb{Z}(G)$, $x_i \in G$, $C_{p^{e_i}} \cong \langle x_i \rangle$ para todo $i \in [1, r]$. Se $g_i = u \cdot v$, para algum $i \in [1, k]$, então podemos escrever J como sendo a soma

$$J = (\prod_{j=1}^{i-1}(1 - g_j)) \cdot (1 - u) \cdot \prod_{j=i+1}^{k} (1 - g_j) + u \cdot (\prod_{j=1}^{i-1}(1 - g_j)) \cdot (1 - v) \cdot \prod_{j=i+1}^{k} (1 - g_j).$$

Como cada g_i pode ser escrito na forma $g_i = x_1^{n_{i1}} \cdot \ldots \cdot x_r^{n_{ir}}$, $n_{ij} \in \mathbb{N}$, para todos $i \in [1, k]$, $j \in [1, r]$, podemos reduzir J para a expressão $J = \sum_{\sigma} g_\sigma J_\sigma$, onde $g_\sigma \in G$,

$$J_\sigma = \prod_{i=1}^{r}(1 - x_i)^{f_i},$$

$f_i \in \mathbb{N} \cup \{0\}$ dependem de $\sigma = (f_1, \ldots, f_r)$, $\sum_{i=1}^{r} f_i = k$.

Agora $\sum_{i=1}^{r} f_i = k > \sum_{i=1}^{r} (p^{e_i} - 1)$ então $f_i \geq p^{e_i}$ para algum $i \in [1, r]$. Mas

$$\begin{aligned}
(1 - x_i)^{p^{e_i}} &= 1 + \binom{p^{e_i}}{1}(-1)x_i + \cdots + \binom{p^{e_i}}{p^{e_i} - 1}(-1)^{p^{e_i}-1}x_i^{p^{e_i}-1} + (-1)^{p^{e_i}} x_i^{p^{e_i}} \\
&\equiv 1 + (-1)^{p^{e_i}} x_i^{p^{e_i}} \\
&\equiv 0 \,(\mathrm{mod}\, p),
\end{aligned}$$

pelo Teorema Binomial em anéis comutativos (veja [12] pg 118) e pelo fato de que $\binom{p^{e_i}}{k} \equiv 0 \,(\mathrm{mod}\, p)$ para todo $k \in [1, p^{e_i} - 1]$ e

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

Assim, $(1 - x_i)^{f_i} = (1 - x_i)^{f_i - p^{e_i}} \cdot (1 - x_i)^{p^{e_i}} \equiv 0 \,(\mathrm{mod}\, p)$ e $J_\sigma \equiv 0 \,(\mathrm{mod}\, p)$, para todo σ.

Portanto, $J \equiv 0 \,(\mathrm{mod}\, p)$. $\square$

A equação (2.1) será obtida como uma conseqüência deste teorema, a partir de duas proposições. A primeira delas afirma que o lado direito da equação (2.1) é uma cota inferior para a constante de Davenport, $D(G)$. A segunda proposição é uma interpretação da equação (2.2) por argumentos de combinatória.

Proposição 2.4. $D(G) \geq 1 + \sum_{i=1}^{r} (p^{e_i} - 1)$.

Demonstração. Basta provarmos que existe uma seqüência de tamanho $\sum_{i=1}^{r} (p^{e_i} - 1)$, a qual não possui subseqüência com produto 1. De fato, sejam $x_i \in G$, $C_{p^{e_i}} = \langle x_i \rangle$, para todo $i \in [1, r]$, e a seqüência

$$S = \prod_{i=1}^{p^{e_1}-1} x_1 \cdot \ldots \cdot \prod_{i=1}^{p^{e_r}-1} x_r \in \mathcal{F}(G),$$

formada pela repetição de x_i na quantidade $p^{e_i} - 1$. Suponha que existisse uma subseqüência com produto 1. Ela seria da forma

$$T = \prod_{j=1}^{n} x_{i_l} \cdot \prod_{j=n+1}^{t} x_{i_j}, \text{ com } n \leq p^{e_{i_l}} - 1, \ \pi(T) = 1,$$

então $1 = x_{i_l}^n \cdot x_{i_{n+1}} \cdot \ldots \cdot x_{i_t}$. Daí,

$$x_{i_l}^n = (x_{i_{n+1}} \cdot \ldots \cdot x_{i_t})^{-1} \in C_{p^{e_{i_l}}} \cap \langle x_{i_j} : j \in [n+1, t] \rangle = \{1\}.$$

Assim $p^{e_{i_l}} | n$, contradizendo o fato $n \leq p^{e_{i_l}} - 1$. □

Antes de vermos a próxima proposição vejamos uma definição.

Definição 2.5. *Dados a seqüência* $S = \prod_{i=1}^{k} g_i \in \mathcal{F}(G)$, *e* $g \in G$, *definimos* $P(g)$ *(respectivamente* $I(g)$*) como sendo o número de subseqüências de* S *com tamanho par (resp. ímpar) e produto igual a* g.

Relembremos a definição do l-ésimo polinômio simétrico no anel de polinômios $\mathbb{Z}[x_1, \ldots, x_k]$. Para cada $l \in [1, k]$ definimos:

$$p_1(x_1, \ldots, x_k) = x_1 + \ldots + x_k$$

$$p_2(x_1, \ldots, x_k) = x_1 x_2 + \ldots + x_{k-1} x_k$$

$$\vdots$$

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

Agora seja $A(l)$ para cada $l \in [1,k]$ definido como sendo a soma formal dos produtos de todas as subseqüências de $S = \prod_{i=1}^{k} g_i \in \mathcal{F}(G)$ com tamanho igual a l. Com a notação anterior temos que $A(l) = p_l(g_1,\ldots,g_k) \in \mathbb{Z}(G)$.

Proposição 2.6. *Pela equação* (2.2) *obtemos que*

$$P(g) - I(g) \equiv \begin{cases} 0\,(mod\,p) & se\ g \neq 1 \\ -1\,(mod\,p) & se\ g = 1 \end{cases}. \tag{2.3}$$

Demonstração. De fato, consideremos $A(0) = 1 \in \mathbb{Z}(G)$, e para $l \in [1,k]$, seja $A(l) = p_l(g_1,\ldots,g_k) \in \mathbb{Z}(G)$. Então, temos

$$\begin{aligned} \prod_{i=1}^{k}(1-g_i) &= \sum_{l=0}^{k}(-1)^l A(l) \\ &= 1\cdot A(0) + \sum_{g\in G}(P(g)-I(g))g \\ &= (1+P(1)-I(1))\cdot 1 + \sum_{\substack{g\in G\\ g\neq 1}}(P(g)-I(g))g. \end{aligned}$$

Pela equação (2.2) segue o resultado da Proposição. □

Agora observamos que dada uma seqüência $S = \prod_{i=1}^{k} g_i \in \mathcal{F}(G)$, com $k = 1 + \sum_{i=1}^{r}(p^{e_i}-1)$, pela Proposição (2.6) segue que ela têm subseqüência de produto um. Do contrário, teríamos que S não possui subseqüência com tamanho par (ou ímpar) e produto igual a 1, ou seja, $P(1) = I(1) = 0$, $0 = P(1) - I(1) \equiv -1\,(\mathrm{mod}\,p)$, uma contradição. Portanto, acabamos de provar o Teorema 2.2.

2.2 A constante de Davenport do grupo $C_m \times C_n$ com m divisor de n

A seguir provaremos que para o grupo $G = C_m \times C_n$, com m divisor de n, temos $D(G) = m+n-1$, Corolário 2.9. Também veremos uma Conjectura de P. Erdös sobre inteiros gaussianos, e generalizaremos o Teorema de Erdös, Ginzburg e Ziv. Estes resultados serão conseqüências de um teorema que fornece uma cota superior para a constante de Davenport do produto direto de dois grupos abelianos onde a ordem de um deles divide à do outro.

Lema 2.7. *Seja $E = C_p^2$, p primo. Seja a seqüência $S = \prod_{i=1}^{s} g_i \in \mathcal{F}(E)$, onde $s \geq 3p-2$. Então S tem uma subseqüência com tamanho $t, 1 \leq t \leq p$ e produto igual a 1.*

Demonstração. Seja $F = C_p^3$ o produto cartesiano do grupo cíclico C_p três vezes, considerando $1 = (1,1,1)$ como sendo a identidade de F e (x,x,x) um gerador de F, tomamos $E = \langle (x,x,1) \rangle$ sendo um subgrupo de F.

Como $D(F) = 3p-2$, pelo Teorema 2.2, e $s \geq 3p-2$, então a seqüência $T = \prod_{i=1}^{s} (g_i, x) \in \mathcal{F}(F)$ tem uma subseqüência com tamanho $t \leq 3p-2$ e produto igual a 1, digamos que seja a seqüência $T_1 = \prod_{i=1}^{t} (g_i, x)$.

De $\pi(T_1) = 1$ segue que $(g_1, x) \cdot \ldots \cdot (g_t, x) = 1$, ou seja, $(g_1 \cdot \ldots \cdot g_t, x^t) = 1$. Então $p \mid t$, daí $|T_1| \in \{p, 2p\}$.

Se $|T_1| = p$, tomamos a subseqüência $U = \prod_{i=1}^{t} g_i$ e o lema está provado.

Se $|T_1| = 2p$, como $D(E) = 2p-1$ pelo Teorema 2.2, $U = \prod_{i=1}^{t} g_i$ tem uma subseqüência com tamanho $u \leq 2p-1$ e produto igual a 1, digamos que seja a seqüência $U_1 = \prod_{i=1}^{u} g_i$. Se $u \leq p$, então o lema está provado. Senão, temos $2p-u < p$ e a subseqüência $U_2 = \prod_{i=u+1}^{2p} g_i$ satisfaz o resultado do lema.

$\square$

Teorema 2.8. *Seja $G = H \times K$, sendo H, K grupos abelianos de ordens $|H| = h, |K| = k, h \mid k$ inteiros positivos. Então $D(G) \leq h + k - 1$.*

Demonstração. Seja a seqüência $S = \prod_{i=1}^{s} g_i \in \mathcal{F}(G)$, onde $s \geq h+k-1$. Aplicaremos o Princípio de Indução Finita sobre a ordem do grupo H.

Seja $h = 1$. Definimos os seguintes elementos de G, $\Pi_j = \prod_{i=1}^{j} g_i$, para todo $j \in [1, k]$. Se os Π_j são distintos, e como $G \cong K$, segue que $\Pi_j = 1$ para algum $j \in [1, k]$, o que prova o teorema. Senão temos $\Pi_i = \Pi_j$ para certos $i, j \in [1, k]$, com $i < j$, então a subseqüência $T = \prod_{l=i+1}^{j} g_l$ tem produto igual a 1.

Agora assumamos $h > 1$ e seja p um inteiro primo divisor de h. Pela recíproca do Teorema de Lagrange para grupos abelianos finitos (veja [12] pg 77), temos que existem os seguintes subgrupos, $H_1 \leqslant H, K_1 \leqslant K$ com índices $[H : H_1] = p = [K : K_1]$ e ordens, digamos $|H_1| = h_1$ e $|K_1| = k_1 \in \mathbb{N}$.

Seja o grupo $Q = H_1 \times K_1$ com $|Q| < |G|$, por hipótese de indução o teorema é válido para este grupo. Sabemos que $G/Q \cong C_p \times C_p$ 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 $D(G) = D(C_p^2) = 2p - 1$, pelo Teorema 2.2, e o teorema está provado.

Agora, suponhamos que $h_1 \geq 1$ e $k_1 \geq 2$. Consideremos a seguinte seqüência em $\mathcal{F}(G/Q)$, $T = \prod_{i=1}^{s} (g_i \cdot Q)$, como $s \geq p(h_1 + k_1 - 2) + 2p - 1 \geq 3p - 1$, pelo Lema 2.7 a seqüência T tem uma subseqüência T_1 com tamanho t, $1 \leq t \leq p$ e produto igual a identidade do grupo G/Q, isto é, igual a Q. Podemos aplicar o Lema 2.7 à seqüência $T_1^{-1} \cdot T$ para obtermos mais uma subseqüência T_2 com tamanho t, $1 \leq t \leq p$ e produto igual a Q. Continuando este processo, construimos $u - 1 = h_1 + k_1 - 2$ subseqüências duas a duas disjuntas, $T_1, \ldots, T_{u-1}$, com tamanhos $|T_j| \in [1, p]$, para todo $j \in [1, u - 1]$, e produtos iguais a Q, isto é, $\pi(S_j) = q_j \in Q$, sendo que S_j é a seqüência formada pelos g_i que aparecem em T_j. Resta uma seqüência de tamanho pelo menos $2p - 1$, logo ela possui uma subseqüência T_u disjuntas das anteriormente obtidas, com produto igual a Q, isto é, $\pi(S_u) = q_u \in Q$.

Como $D(Q) \leq h_1 + k_1 - 1$, por hipótese de indução, então a seqüência $\prod_{j=1}^{u} q_j \in \mathcal{F}(Q)$ tem uma subseqüência $\prod_{i \in I} q_i$, $I \subseteq [1, u]$ com produto igual a $1 \in Q$. Logo, S tem a subseqüência $\prod_{i \in I} \prod_{g \in S_i} g \in \mathcal{F}(G)$ com produto igual a 1.

Portanto, o teorema está provado. $\square$

Corolário 2.9. *Sejam $m, n \in \mathbb{N}$, m um divisor de n e o grupo $G = C_m \times C_n$. Então $D(G) = m + n - 1$.*

Demonstração. Pelo Teorema 2.8 temos que $D(G) \leq m + n - 1$.

Para provarmos que $D(G) \geq m + n - 1$ construíremos uma seqüência de tamanho $m + n - 2$ a qual não tem subseqüência com produto 1. Sejam $(x, 1), (1, y) \in G$ tais que

$C_m \cong \langle (x,1)\rangle, C_n \cong \langle (1,y)\rangle$. Seja a seqüência $S = \prod_{i=1}^{m-1}(x,1)\cdot\prod_{i=1}^{n-1}(1,y)$. Suponha que existisse uma subseqüência de S com produto 1. Ela seria da forma

$$U = \prod_{j=1}^{r}(x,1)\cdot\prod_{j=1}^{s}(1,y), \text{ com } r \leq m-1,\ s \leq n-1,\ \pi(U) = 1,$$

então $1 = (x^r, y^s)$. Daí $m|r$, uma contradição. Portanto, $D(G) = m+n-1$.

□

O próximo resultado confirma uma Conjectura de P. Erdös sobre inteiros gaussianos.

Corolário 2.10 (P. Erdös)**.** *Toda seqüência de tamanho $2n-1$ formada por inteiros gaussianos, possui uma subseqüência com soma divisível por n.*

Demonstração. Sejam $a_j + b_j \cdot i \in \mathbb{Z}[i]$ para todo $j \in [1, 2n-1]$, onde $\mathbb{Z}[i]$ é o anel dos inteiros gaussianos, e a seqüência $S = \prod_{j=1}^{2n-1}(a_j, b_j) \in \mathcal{F}(C_n^2)$, onde C_n^2 será considerado aditivo. Pelo Corolário 2.9 temos $D(C_n^2) = 2n-1$, então S possui uma subseqüência com soma 0 e tamanho $t \leq 2n-1$, isto é, entre os $2n-1$ inteiros gaussianos dados existem t deles, digamos $a_j + b_j \cdot i$, para todo $j \in [1,t]$ com $\sum_{j=1}^{t} a_j \equiv \sum_{j=1}^{t} b_j \equiv 0 (\operatorname{mod} n)$.

□

O seguinte Corolário generaliza o Teorema de Erdös, Ginzburg e Ziv, Corolário 2.12.

Corolário 2.11. *Sejam K um grupo abeliano finito de ordem $|K| = k$, e $h \in \mathbb{N}$, $h \mid k$, $S = \prod_{i=1}^{h+k-1} g_i \in \mathcal{F}(K)$, então S tem uma subseqüência de produto igual a 1 e tamanho $t \equiv 0 (mod\, h)$.*

Demonstração. Sejam os grupos $H = C_h$ e $K \cong \{1\} \times K \leqslant H \times K$. Consideremos $C_h = \langle x \rangle$ e $U = \prod_{i=1}^{h+k-1}(x, g_i) \in \mathcal{F}(H \times K)$. Segue do Teorema 2.8 que U possui uma subseqüência $W = \prod_{i \in I}(x, g_i)$ de tamanho $|I| = t \leq h+k-1$ e produto 1, então $1 = (x^t, \prod_{i \in I} g_i)$ implica que $t \equiv 0 (\operatorname{mod} h)$. Logo, $\prod_{i \in I} g_i$ tem produto igual a 1 e tamanho $t \equiv 0 (\operatorname{mod} h)$.

□

Corolário 2.12 (Erdös, Ginzburg e Ziv). *Toda seqüência de tamanho $2n-1$ formada por inteiros, possui uma subseqüência de tamanho n e soma divisível por n.*

Demonstração. Pelo Corolário 2.11 toda seqüência de $2n-1$ inteiros, isto é, de tamanho $2n-1$ em $\mathcal{F}(C_n^2)$,onde C_n^2 é aditivo, possui uma subseqüência de tamanho $t \equiv 0 (\bmod n)$ e soma zero, ou seja, existem $t = n$ inteiros na seqüência dada com soma divisível por n.

$\square$

Capítulo 3

A Conjectura de Kemnitz

Neste capítulo estudaremos o resultado principal deste trabalho, o artigo [17], onde Christian Reiher faz uma demonstração elegante para a Conjectura de Kemnitz. Na primeira seção enunciaremos a Conjectura, juntamente com algumas observações pertinentes. Na seção 2 veremos o Teorema de Chevalley-Warning e alguns resultados técnicos que serão utilizados na conclusão da veracidade da Conjectura.

3.1 Apresentação da Conjectura de Kemnitz

Faremos agora uma definição formal do invariante $s(G)$ para um grupo abeliano aditivo G.

Definição 3.1. Seja G um grupo abeliano finito, definimos $s(G)$ como sendo o menor inteiro positivo s, tal que para toda seqüência S em $\mathcal{F}(G)$ com tamanho $|S| \geq s$, existe uma subseqüência $T \mid S$ com $\sigma(T) = 0$ e tamanho $|T| = exp(G)$. Onde o símbolo $exp(G)$ denota o expoente do grupo, ou seja, é o menor inteiro positivo l tal que para todo $g \in G$ tem-se $lg = 0$.

Conjectura 3.2 (Conjectura de Kemnitz)**.** $s(C_n^2) = 4n - 3$ *para todo* $n \in \mathbb{N}$.

Veremos algumas proposições que nos darão condições de concluir que basta provarmos a Conjectura 3.2 para n sendo um inteiro primo ímpar. A primeira delas nos fornece cotas inferior e superior para a constante $s(C_n^d)$ para todos $n,\ d\ \in \mathbb{N}$. A segunda proposição é um resultado elementar sobre o endomorfismo multiplicação por $n \in \mathbb{N}$ em um grupo abeliano. A última proposição afirma que o conjunto dos inteiros positivos que satisfazem a Conjectura 3.2 é fechado sob a multiplicação de inteiros.

Proposição 3.3. *[H. Harborth, [10]]. Temos que* $(n-1)2^d+1 \leq s(C_n^d) \leq (n-1)n^d+1$ *para todos* $n,\ d\ \in \mathbb{N}$. *Em particular,* $s(C_2^2) = 4 \cdot 2 - 3$.

Demonstração. Tomando a seqüência S em $\mathcal{F}(C_n^d)$ de tamanho $(n-1)2^d$ formada por todos os $\{0,1\}$-elementos de C_n^d, isto é, os elementos que têm 0 ou 1 como coordenadas, onde cada um destes elementos aparecem repetidos $n-1$ vezes em S, vemos que esta seqüência não possui subseqüência com soma zero e tamanho n, pois para cada subseqüência com tamanho n temos que a soma de cada coordenada vista como números inteiros é sempre menor do que n, logo é incongruente a 0 módulo n. Assim, o número $(n-1)2^d+1$ é uma cota inferior para $s(C_n^d)$.

Agora, o número $(n-1)n^d+1$ é uma cota superior para $s(C_n^d)$, pois em qualquer seqüência $S \in \mathcal{F}(C_n^d)$ de tamanho $(n-1)n^d+1$, temos que $v_g(S) \geq n$ para algum $g \in C_n^d$, pelo Princípio da Casa dos Pombos (ver [11] pg 127). Logo a subseqüência $T = \prod_{i=1}^{n} g$ tem tamanho n e soma zero.

$\square$

Proposição 3.4. *Sejam os seguintes grupos* C_{mn}, $G = C_{mn}^k$ *e* $H = C_{mn}^{k+1}$, *onde* $m,\ n,\ k \in \mathbb{N}$. *Seja o homomorfismo multiplicação por* n, $\varphi : H \to H$ *definido por* $\varphi(h) = nh$, *então* $\varphi(G) \cong C_m^k$, $\varphi(H) \cong C_m^{k+1}$, $ker(\varphi) \cong C_n^{k+1}$.

Demonstração. Primeiro verifiquemos que $ker(\varphi) \cong C_n^{k+1}$.

Sejam $C_{mn} = \langle a \rangle$ e $h = (n_1 a, \ldots, n_{k+1} a) \in ker(\varphi)$ com $n_i \in \mathbb{Z}$, para todo $i \in [1, k+1]$. Então $0 = \varphi(h) = (nn_1 a, \ldots, nn_{k+1} a)$. Daí $nn_i \equiv 0 \pmod{mn}$, para todo $i \in [1, k+1]$, ou seja, $n_i \equiv 0 \pmod{m}$ para todo $i \in [1, k+1]$. Assim, $h \in \langle ma \rangle^{k+1} \cong C_n^{k+1}$.

Agora, se $h = (r_1 ma, \ldots, r_{k+1} ma) \in \langle ma \rangle^{k+1}$, com $r_i \in \mathbb{Z}$, para todo $i \in [1, k+1]$, então $\varphi(h) = (r_1 mna, \ldots, r_{k+1} mna) = 0$. Logo $h \in ker(\varphi)$.

Considerando a restrição do homomorfismo φ ao subgrupo $G \leqslant H$, $\overline{\varphi} = \varphi | G$, obtemos que $ker(\overline{\varphi}) \cong C_n^k$.

Pelo Primeiro Teorema de Isomorfismo para homomorfismo de grupos (veja [12] pg 44) segue que $\varphi(H) \cong H/ker(\varphi)$, ou seja, $\varphi(H) \cong C_{mn}^{k+1}/C_n^{k+1} \cong C_m^{k+1}$. Analogamente, prova-se $\varphi(G) \cong C_m^k$.

$\square$

Agora veremos que o conjunto dos inteiros positivos que verificam a Conjectura 3.2 é fechado para a multiplicação. Daí, concluíremos que dado $n \in \mathbb{N}$, é suficiente provarmos a Conjectura 3.2 para os fatores primos de n.

Proposição 3.5. *Seja $E = \{n \in \mathbb{N} : s(C_n^2) = 4n - 3\}$. Este conjunto é fechado para a multiplicação de inteiros.*

Demonstração. Pela Proposição 3.3 temos que $s(C_2^2) = 4 \cdot 2 - 3$. Logo, $2 \in E$. Agora provemos que $mn \in E$ sempre que $m, n \in E$. Sejam o grupo $G \cong C_{mn}^2$ e $\varphi : G \to G$ o endomorfismo dado por $\varphi(g) = ng$. Então pela Proposição 3.4 temos que $\varphi(G) \cong C_m^2$ e $ker(\varphi) \cong C_n^2$. Agora seja S uma seqüência em $\mathcal{F}(G)$ com tamanho $|S| = 4mn - 3$.

Como $\varphi(G) \cong C_m^2$ e $s(C_m^2) = 4m - 3$, por hipótese, então $s(\varphi(G)) = 4m - 3$.

De $4mn-3 = (4n-4)m+4m-3$ segue que a seqüência $\varphi(S)$ possui uma subseqüência $\varphi(S_1)$ com tamanho $|\varphi(S_1)| = m$ e $\sigma(\varphi(S_1)) = 0$. Repetindo este processo $4n - 4$ vezes obteremos $4n - 4$ subseqüências disjuntas $S_1, \ldots, S_{4n-4}$ com tamanhos $|S_i| = m$ e $\sigma(\varphi(S_i)) = 0$ para todo $i \in [1, 4n - 4]$, e restará uma subseqüência de S de tamanho $4m - 3$. Desta seqüência obtemos mais uma subseqüência S_t, disjunta das anteriormente obtidas, com tamanho $|S_t| = m$ e $\sigma(\varphi(S_t)) = 0$ onde $t = 4n - 3$.

Agora seja $T = \prod_{i=1}^{t} \sigma(S_i)$, esta é uma seqüência em $\mathcal{F}(ker(\varphi))$, pois $\varphi(\sigma(S_i)) = \sigma(\varphi(S_i)) = 0$ para todo $i \in [1, 4n - 3]$.

Como $|T| = 4n-3$ e, por hipótese, $s(ker(\varphi)) = s(C_n^2)$, de $|T| = s(C_n^2)$ segue que existe algum $I \subseteq [1, t]$, $|I| = n$ tal que $\prod_{i \in I} \sigma(S_i) \mid T$ tem soma zero.

Daí, $S' = \prod_{i \in I} S_i$ é uma subseqüência de soma zero de S com $|S'| = \sum_{i \in I} |S_i| = nm$. $\square$

3.2 A prova da Conjectura de Kemnitz

A bela demonstração de C. Reiher foi construída a partir do Teorema de Chevalley-Warning. Ele obteve cinco corolários deste Teorema, um Lema e finalmente o Teorema que declara que a Conjectura de Kemnitz é verdadeira.

O Teorema de Chevalley-Warning (veja [13]) afirma que o número de soluções de um sistema de equações polinomiais com muitas variáveis, sobre um corpo finito de característica prima, é múltiplo da característica quando a soma dos graus dos polinômios for menor do que o número de variáveis envolvidas. Por questão de zelo, enunciaremos e provaremos este teorema clássico, o leitor mais experiente pode ir direto para a Definição 3.7.

Teorema 3.6 (Chevalley-Warning)**.** *Seja p um inteiro primo, $\mathbb{F}_q$ o corpo finito com $q = p^n$ elementos. Para $i \in [1, m]$ sejam $f_i(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n]$ de graus $gr(f_i) = d_i$. Seja N o número de soluções em $\mathbb{F}_q^n$ do seguinte sistema de equações polinomiais*

$$f_i(x_1, \ldots, x_n) = 0 \text{ para todo } i \in [1, m].$$

Se $\sum_{i=1}^{m} d_i < n$, então $N \equiv 0\,(mod\, p)$.

Demonstração. Seja $\mathbb{F}_q^* = \langle a \rangle$ o grupo cíclico multiplicativo do corpo $\mathbb{F}_q$, então

$$x^{q-1} = \begin{cases} 1 & \text{se } x \neq 0 \\ 0 & \text{caso contrário} \end{cases}.$$

Convencionando que $0^0 = 1$, temos $\sum_{x \in \mathbb{F}_q} x^r = 0$ se $0 \leq r < q-1$. De fato, para $r = 0$ a prova é trivial, e para $0 < r < q-1$ temos

$$\sum_{x \in \mathbb{F}_q} x^r = \sum_{x \in \mathbb{F}_q^*} x^r = \sum_{i=0}^{q-2} (a^i)^r = (a^r - 1)^{-1}(a^{r(q-1)} - 1) = 0.$$

Seja $g(x_1, \ldots, x_n) = \prod_{i=1}^{m} \left(1 - f_i(x_1, \ldots, x_n)^{q-1}\right) \in \mathbb{F}_q[x_1, \ldots, x_n]$,

$c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$, então $g(c) = \begin{cases} 1 & \text{se } f_i(c) = 0 \text{ para todo } i \in [1, m] \\ 0 & \text{caso contrário} \end{cases}$.

Assim, $N \cdot 1 = \sum_{c \in \mathbb{F}_q^n} g(c)$, notemos que $g(c) \in \mathbb{F}_q$.

Como $g(x_1, \ldots, x_n) = \sum_{r_1, \ldots, r_n} a_{r_1, \ldots, r_n} x_1^{r_1} \cdots x_n^{r_n}$, onde $r_1, \ldots, r_n \in \mathbb{Z}^+ \cup \{0\}$, $a_{r_1, \ldots, r_n} \in \mathbb{F}_q$, e $gr(f_i) = d_i$, então

$$\text{máx}\{\sum_{j=1}^{n} r_j : \ a_{r_1, \ldots, r_n} \text{ é um coeficiente de g}\} \leq (q-1) \sum_{i=1}^{m} d_i < (q-1)n,$$

$\sum_{(c_1, \ldots, c_n) \in \mathbb{F}_q^n} c_1^{r_1} \cdots c_n^{r_n} = \prod_{i=1}^{n} \sum_{c_i \in \mathbb{F}_q} c_i^{r_i} = 0$. Como isso acontece em cada monômio de g, então $N \cdot 1 = \sum_{c \in \mathbb{F}_q^n} g(c) = 0$. Portanto, $N \equiv 0\,(\text{mod}\, p)$. $\square$

A seguir definiremos um subconjunto de $\mathcal{F}(C_p^2)$, depois provaremos seis resultados envolvendo este subconjunto, os quais fornecerão a prova da Conjectura 3.2. De agora diante, nesta seção, p denotará um inteiro primo ímpar.

Definição 3.7. Seja $S \in \mathcal{F}(C_p^2)$, $S = \prod_{i=1}^{m}(a_i, b_i)$, $\sigma(S) = \sum_{i=1}^{m}(a_i, b_i)$, definimos o seguinte conjunto $S(n) = \{T \mid S : |T| = n,\ \sigma(T) = 0\}$.

Corolário 3.8. *Seja $S \in \mathcal{F}(C_p^2)$ tal que $|S| = 3p - 3$, então*

$$1 - |S(p-1)| - |S(p)| + |S(2p-1)| + |S(2p)| \equiv 0\,(mod\,p).$$

Demonstração. Sejam $S = \prod_{i=1}^{3p-3}(a_i, b_i)$, e consideremos o seguinte sistema de polinômios em $\mathbb{F}_p[x_1, \ldots, x_{3p-2}]$,

$$\begin{cases} x_1^{p-1} + \cdots + x_{3p-3}^{p-1} + x_{3p-2}^{p-1} = 0 \\ a_1 x_1^{p-1} + \cdots + a_{3p-3}x_{3p-3}^{p-1} = 0 \\ b_1 x_1^{p-1} + \cdots + b_{3p-3}x_{3p-3}^{p-1} = 0 \end{cases}.$$

Como a soma dos graus dos polinômios no sistema é menor do que o número de variáveis, então pelo Teorema de Chevalley-Warning, o número N de soluções do sistema satisfaz $N \equiv 0\,(\mathrm{mod}\,p)$.

Sejam Ω o conjunto de soluções do sistema, $\Omega_1 \subseteq \Omega$ o conjunto das soluções $(c_1, \ldots, c_{3p-2})$, com $c_{3p-2} = 0$ e $\Omega_2 = \Omega \setminus \Omega_1$ (este é o complementar de Ω_1).

Seja $c \in \Omega_1$. Pela primeira equação polinomial temos que c possui kp coordenadas não nulas onde $k \in [0, 2]$; como c satisfaz as outras duas equações polinomiais então ele determina uma subseqüência $A_k \in S(kp)$. Por sua vez, cada elemento de $S(kp)$ determina $(p-1)^{kp}$ elementos de Ω_1, pois para $T = \prod_{i \in I}(a_i, b_i) \in S(kp)$, $I \subseteq [1, 3p-3]$, $|I| = kp$ e para cada par (a_i, b_i) podemos formar uma solução para o sistema, digamos a solução $c = (c_1, \ldots, c_{3p-2}) \in \mathbb{F}_p^{3p-2}$, com $c_i \neq 0$ para todo $i \in I$ e $c_i = 0$ para todo $i \in [1, 3p-3] \setminus I$, além disso, cada $c_i \neq 0$ pode ser escolhido entre $p-1$ elementos de $\mathbb{F}_p^*$.

Assim,

$$|\Omega_1| = 1 + (p-1)^p|S(p)| + (p-1)^{2p}|S(2p)| \equiv 1 - |S(p)| + |S(2p)|\,(\mathrm{mod}\,p).$$

Agora seja $c \in \Omega_2$, então temos que c possui kp coordenadas não nulas, e pelas últimas equações do sistema, c determina uma subseqüência $A_k \in S(kp-1)$. Por sua vez, cada elemento de $S(kp-1)$ determina $(p-1)^{kp}$ elementos de Ω_2.

Logo,

$$|\Omega_2| = (p-1)^p|S(p-1)| + (p-1)^{2p}|S(2p-1)| \equiv -|S(p-1)| + |S(2p-1)|\,(\mathrm{mod}\,p).$$

De $N \equiv 0 \pmod p$ e de $N = |\Omega| = |\Omega_1| + |\Omega_2|$ vem que

$$1 - |S(p-1)| - |S(p)| + |S(2p-1)| + |S(2p)| \equiv 0 \pmod p.$$

$\square$

Corolário 3.9. *Seja $S \in \mathcal{F}(C_p^2)$ tal que $|S| = 3p-2$ ou $|S| = 3p-1$, então $1 - |S(p)| + |S(2p)| \equiv 0 \,(mod\, p)$.*

Demonstração. Consideremos $S = \prod_{i=1}^{l}(a_i, b_i)$, $l \in [3p-2, 3p-1]$, e o seguinte sistema de polinômios em $\mathbb{F}_p[x_1, \ldots, x_l]$,

$$\begin{cases} x_1^{p-1} + & \cdots & + x_l^{p-1} & = 0 \\ a_1 x_1^{p-1} + & \cdots & + a_l x_l^{p-1} & = 0 \\ b_1 x_1^{p-1} + & \cdots & + b_l x_l^{p-1} & = 0 \end{cases}.$$

Como a soma dos graus dos polinômios no sistema é menor do que o número de variáveis, então pelo Teorema de Chevalley-Warning, o número N de soluções do sistema satisfaz $N \equiv 0 \pmod p$. Seja Ω o conjunto de soluções do sistema.

Como cada elemento de $S(kp)$ determina $(p-1)^{kp}$ elementos de Ω, então

$$|\Omega| = 1 + (p-1)^p |S(p)| + (p-1)^{2p} |S(2p)| \equiv 1 - |S(p)| + |S(2p)| \pmod p.$$

Portanto,

$$1 - |S(p)| + |S(2p)| \equiv 0 \pmod p.$$

$\square$

Corolário 3.10 (Alon-Dubiner). *Seja S uma seqüência em $\mathcal{F}(C_p^2)$ satisfazendo $|S| = 3p$ e $\sigma(S) = 0$. Então $S(p)$ é não vazio.*

Demonstração. Consideremos $S = \prod_{i=1}^{3p}(a_i, b_i)$, e o seguinte sistema de polinômios em $\mathbb{F}_p[x_1, \ldots, x_{3p-1}]$,

$$\begin{cases} x_1^{p-1} + & \cdots & + x_{3p-1}^{p-1} & = 0 \\ a_1 x_1^{p-1} + & \cdots & + a_{3p-1} x_{3p-1}^{p-1} & = 0 \\ b_1 x_1^{p-1} + & \cdots & + b_{3p-1} x_{3p-1}^{p-1} & = 0 \end{cases}.$$

Aplicando o Teorema de Chevalley-Warning obtemos que o número N de soluções do sistema é tal que $N \equiv 0 \pmod p$, como o sistema admite a solução trivial então $N \geq p$.

Logo existe uma solução não trivial $c = (c_1, \ldots, c_{3p-1}) \in \mathbb{F}_p^{3p-1}$. Seja $I \subseteq [1, 3p-1]$ tal que $c_i \neq 0$ para todo $i \in I$, então $|I| \in \{p, 2p\}$. Se $|I| = p$, então $\prod_{i \in I}(a_i, b_i) \in S(p)$. Agora se $|I| = 2p$, de $\sigma(S) = 0$ segue que $\prod_{i \in [1,3p] \setminus I} (a_i, b_i) \in S(p)$. □

Corolário 3.11. *Seja $S \in \mathcal{F}(C_p^2)$ tal que $|S| = 4p-3$. Então*

a) $-1 + |S(p)| - |S(2p)| + |S(3p)| \equiv 0 \,(mod\, p)$;

b) $|S(p-1)| - |S(2p-1)| + |S(3p-1)| \equiv 0 \,(mod\, p)$.

Demonstração. a) Sejam $S = \prod_{i=1}^{4p-3} (a_i, b_i)$, e consideremos o seguinte sistema de polinômios em $\mathbb{F}_p[x_1, \ldots, x_{4p-3}]$,

$$\begin{cases} x_1^{p-1} + & \cdots & + \, x_{4p-3}^{p-1} & = 0 \\ a_1 x_1^{p-1} + & \cdots & + \, a_{4p-3} x_{4p-3}^{p-1} & = 0 \\ b_1 x_1^{p-1} + & \cdots & + \, b_{4p-3} x_{4p-3}^{p-1} & = 0 \end{cases}.$$

Aplicando o Teorema de Chevalley-Warning vemos que o número N de soluções do sistema é tal que $N \equiv 0 \,(\mathrm{mod}\, p)$.

Sejam Ω o conjunto de soluções do sistema. Seja $c \in \Omega$, pela primeira equação polinomial temos que c possui kp coordenadas não nulas onde $k \in [0, 3]$. Como c satisfaz as outras duas equações polinomiais então ele determina uma subseqüência $A_k \in S(kp)$.

Para $T = \prod_{i \in I}(a_i, b_i) \in S(kp)$, $I \subseteq [1, 4p-3]$, $|I| = kp$ e para cada par (a_i, b_i) podemos formar uma solução , digamos $c = (c_1, \ldots, c_{4p-3}) \in \mathbb{F}_p^{4p-3}$ para o sistema, com $c_i \neq 0$ para todo $i \in I$ e $c_i = 0$ para todo $i \in [1, 4p-3] \setminus I$, onde cada $c_i \neq 0$ pode ser escolhido entre $p-1$ elementos de $\mathbb{F}_p^*$. Logo cada elemento de $S(kp)$ determina $(p-1)^{kp}$ elementos de Ω. Assim,

$$|\Omega| = 1 + (p-1)^p |S(p)| + (p-1)^{2p} |S(2p)| + (p-1)^{3p} |S(3p)|.$$

De $N = |\Omega|$ e de $N \equiv 0 \,(\mathrm{mod}\, p)$ segue que $1 - |S(p)| + |S(2p)| - |S(3p)| \equiv 0 \,(\mathrm{mod}\, p)$.

b) Consideremos o seguinte sistema de polinômios

$$\begin{cases} x_1^{p-1} + & \cdots & + \, x_{4p-3}^{p-1} & +1 & = 0 \\ a_1 x_1^{p-1} + & \cdots & + \, a_{4p-3} x_{4p-3}^{p-1} & & = 0 \\ b_1 x_1^{p-1} + & \cdots & + \, b_{4p-3} x_{4p-3}^{p-1} & & = 0 \end{cases}.$$

Seja $c \in \Omega$ o conjunto das soluções do sistema, então pela primeira equação polinomial temos que c determina uma subseqüência $A_k \in S(kp-1)$. Agora cada elemento de $S(kp-1)$ determina $(p-1)^{kp-1}$ elementos de Ω.

Daí, $N = (p-1)^{p-1}|S(p-1)| + (p-1)^{2p-1}|S(2p-1)| + (p-1)^{3p-1}|S(3p-1)|$.

Pelo Pequeno Teorema de Fermat (veja [12] pg 40), $N \equiv |S(p-1)| - |S(2p-1)| + |S(3p-1)| \pmod{p}$.

Portanto, $|S(p-1)| - |S(2p-1)| + |S(3p-1)| \equiv 0 \pmod{p}$. $\square$

A seguinte proposição será útil na demonstração do próximo Corolário.

Proposição 3.12. *Dados $t, r \in \mathbb{N}$, $p \in \mathbb{N}$ primo, com $t \geq 2$ e $p \geq r$ temos que*

$$\binom{tp-r}{(t-1)p-r} \equiv \begin{cases} (1-t) \, (mod\, p) & se\ p = 2 \\ (t-1) \, (mod\, p) & se\ p > 2 \end{cases}.$$

Demonstração. Seja $L = \binom{tp-r}{(t-1)p-r}$, então

$$(p-1)! \cdot L = ((t-1)p - r + 1) \ldots ((t-1)p-1)(t-1)((t-1)p+1) \ldots (tp-r).$$

Assim,

$$\begin{aligned} (p-1)!L &= ((t-1)p-(r-1)) \ldots ((t-1)p-1)(t-1)((t-1)p+1) \ldots (tp-r) \pmod{p} \\ &\equiv (p-(r-1)) \ldots (p-1)(t-1)(p-(p-1)) \ldots (p-r) \pmod{p} \\ &\equiv (-1)^{(p-1)}(p-1)! \cdot (t-1) \pmod{p}. \end{aligned}$$

Logo, $L \equiv (-1)^{(p-1)}(t-1) \pmod{p}$.

$\square$

Corolário 3.13. *Seja $S \in \mathcal{F}(C_p^2)$ tal que $|S| = 4p-3$, então*

$$3 - 2|S(p-1)| - 2|S(p)| + |S(2p-1)| + |S(2p)| \equiv 0 \, (mod\, p).$$

Demonstração. Seja A uma seqüência em $\mathcal{F}(C_p^2)$ com $|A| = 3p-3$, pelo Corolário 3.8 temos que

$$1 - |A(p-1)| - |A(p)| + |A(2p-1)| + |A(2p)| \equiv 0 \pmod{p}.$$

Seja

$$L = \sum_{\substack{A|S \\ |A|=3p-3}} \{1 - |A(p-1)| - |A(p)| + |A(2p-1)| + |A(2p)|\}.$$

Então $L \equiv 0 \,(\mathrm{mod}\, p)$.

Dado $B \mid S$, $|B| = t$, o número de subseqüências A, com $A \mid S$ e $B \mid A$, é igual a $\binom{|S|-|B|}{|A|-|B|} = \binom{4p-3-t}{3p-3-t}$.

Assim,

$$\begin{aligned} L &= \binom{4p-3}{3p-3} - \binom{3p-2}{2p-2}|S(p-1)| - \binom{3p-3}{2p-3}|S(p)| + \\ &+ \binom{2p-2}{p-2}|S(2p-1)| + \binom{2p-3}{p-3}|S(2p)| \end{aligned}$$

Pela Proposição 3.12 segue que $L \equiv 3-2|S(p-1)|-2|S(p)|+|S(2p-1)|+|S(2p)| \,(\mathrm{mod}\, p)$.

Portanto, segue o resultado do Corolário. $\square$

Lema 3.14. *Seja $S \in \mathcal{F}(C_p^2)$ tal que $|S| = 4p-3$ e $S(p)$ é um conjunto vazio. Então*

$$|S(p-1)| \equiv |S(3p-1)| \,(mod\, p).$$

Demonstração. Seja r o número de partições de S na forma $S = A \cdot B \cdot C$, com $|A| = p-1$, $|B| = p-2$, $|C| = 2p$, $\sigma(A) = 0$, $\sigma(B) = \sigma(S)$ e $\sigma(C) = 0$. Nesta situação, diremos que A, B e C são subseqüências admissíveis para S. Calcularemos $r \,(\mathrm{mod}\, p)$.

Primeiro, consideramos todas as subseqüências A admissíveis e contamos para cada A quantas possíveis subseqüências B existem em $A^{-1} \cdot S$. Notemos que ao contarmos as subseqüências B estamos contando os pares B e C pois $A^{-1} \cdot S = B \cdot C$. Então obtemos

$$r = \sum_{A\ adm.} |(A^{-1} \cdot S)(2p)|.$$

Como $|A^{-1} \cdot S| = 3p-2$ e $(A^{-1} \cdot S)(p) = S(p) = \varnothing$, o Corolário 3.9 implica que $|(A^{-1} \cdot S)(2p)| \equiv -1 \,(\mathrm{mod}\, p)$. Assim,

$$r \equiv \sum_{A\ adm.} -1 \equiv -|S(p-1)| \,(\mathrm{mod}\, p).$$

Agora consideramos todas as subseqüências B admissíveis e contamos para cada B quantas possíveis subseqüências A existem em $B^{-1} \cdot S$, notemos que estamos contando os pares A e C pois $B^{-1} \cdot S = A \cdot C$. Então temos

$$r = \sum_{B\ adm.} |(B^{-1} \cdot S)(2p)|.$$

Como $|B^{-1} \cdot S| = 3p-1$ e $(B^{-1} \cdot S)(p) = S(p) = \varnothing$, o Corolário 3.9 implica que $|(B^{-1} \cdot S)(2p)| \equiv -1 \,(\mathrm{mod}\, p)$, e como o número de subseqüências B admissíveis é igual ao número de subseqüências $B^{-1} \cdot S$ admissíveis, o qual é igual a $|S(3p-1)|$, então

$$r \equiv \sum_{B \ adm.} -1 \equiv -|S(3p-1)| \pmod{p}.$$

Igualando estas duas congrüências para r, obtemos o resultado desejado. □

Teorema 3.15. *A Conjectura de Kemnitz é verdadeira, isto é,* $s(C_n^2) = 4n - 3$ *para todo* $n \in \mathbb{N}$.

Demonstração. Conforme vimos na seção 3.1 é suficiente provarmos a Conjectura para $n = p$ primo ímpar.

Seja S uma seqüência em $\mathcal{F}(C_p^2)$ com $|S| = 4p - 3$.

Pelos Corolários 3.11 e 3.13 temos as seguintes congruências:

$$\begin{array}{lcl} -1 + |S(p)| - |S(2p)| + |S(3p)| & \equiv & 0 \pmod{p} \\ |S(p-1)| - |S(2p-1)| + |S(3p-1)| & \equiv & 0 \pmod{p} \\ 3 - 2|S(p-1)| - 2|S(p)| + |S(2p-1)| + |S(2p)| & \equiv & 0 \pmod{p} \end{array}.$$

Adicionando estas congrüências obtemos o seguinte

$$2 - |S(p-1)| - |S(p)| + |S(3p-1)| + |S(3p)| \equiv 0 \pmod{p}.$$

Suponhamos, por absurdo, que fosse $S(p) = \varnothing$, então pelo Corolário 3.10 teríamos que $S(3p) = \varnothing$ e do Lema 3.14 seguiria que $|S(p-1)| \equiv |S(3p-1)| \pmod{p}$. Daí, a congrüência acima seria $2 \equiv 0 \pmod{p}$, uma contradição com o fato de p ser um primo ímpar.

Portanto, $S(p) \neq \varnothing$, ou seja, toda seqüência em $\mathcal{F}(C_p^2)$ com tamanho pelo menos $4p - 3$ possui uma subseqüência de tamanho $p = exp(C_p^2)$ e soma zero.

□

Capítulo 4

Subseqüências de soma zero e tamanho restrito em um grupo abeliano finito

Neste último capítulo veremos na primeira seção que $s_0(C_n^2) = 3n - 2$ para todo $n \geq 2 \in \mathbb{N}$. Este resultado foi demonstrado por Gao e Geroldinger em [9]. Afim de obter isto provaremos dois lemas e um teorema.

Na segunda seção veremos dois resultados sobre o invariante $s(G)$ para um grupo G abeliano finito, os quais foram demonstrados por Gao e outros em [3].

O primeiro deles é uma generalização da seguinte desigualdade que aparece em Harborth [10]:

$$s(C_{nm}^d) \leq min\{s(C_n^d) + (s(C_m^d) - 1)n, s(C_m^d) + (s(C_n^d) - 1)m\} \tag{4.1}$$

para todos n, m e $d \in \mathbb{N}$.

O outro é o seguinte: $s(C_n \times C_m) \leq 2(m + n) - 3$ sempre que $n, m \in \mathbb{N}$, $n, m \geq 2$ com n divisor de m.

Na última seção, veremos como conseqüências dos resultados obtidos nesta dissertação que $s(C_{3^n}^3) = 9 \cdot 3^n - 8$ e $s(C_{2^n}^d) = (2^n - 1)2^d + 1$, para todos $d, n \in \mathbb{N}$.

4.1 Subseqüências de soma zero e tamanho restrito em C_n^2

Vejamos a definição formal do invariante $s_0(G)$ para um grupo abeliano aditivo G.

Definição 4.1. Seja G um grupo abeliano finito. Definimos $s_0(G)$ como sendo o menor inteiro positivo l, tal que para toda seqüência S em $\mathcal{F}(G)$ com tamanho $|S| \geq l$, existe uma subseqüência T de S com $\sigma(T) = 0$ e tamanho $|T|$ divisível por $exp(G)$.

Lema 4.2. *Seja G um grupo abeliano finito com $exp(G) = n \geq 2$. Então*

$$D(G) + n - 1 \leq s_0(G) \leq min\{s(G), D(G \times C_n)\}.$$

Demonstração. Seja $S \in \mathcal{F}(G)$, com $|S| = D(G) - 1$, uma seqüência que não possui subseqüência com soma zero. Logo a seqüência $S \cdot \prod_{i=1}^{n-1} 0$ não tem subseqüência com soma zero e tamanho divisível por n. Portanto, $D(G) + n - 2 = |S \cdot \prod_{i=1}^{n-1} 0| < s_0(G)$.

Das definições 3.1 e 4.1 segue que $s_0(G) \leq s(G)$, logo basta verificarmos que $s_0(G) \leq D(G \times C_n)$.

Suponhamos que $C_n = \langle (0, x) \rangle$ sendo 0 a identidade de G, e seja a seqüência $U = \prod_{i=1}^{l} g_i \in \mathcal{F}(G)$, sendo
$l = D(G \times \langle x \rangle)$.

Então a seqüência $\prod_{i=1}^{l}(g_i, x) \in \mathcal{F}(G \times \langle x \rangle)$ contém uma subseqüência $T = \prod_{i \in I}(g_i, x)$, $I \subset [1, l]$, com soma zero pela definição 2.1. De $\sigma(\prod_{i \in I} x) = 0$, isto é, $|I|x = 0$ segue que $|I| \equiv 0 (\bmod n)$. Assim U tem uma subseqüência, $\prod_{i \in I} g_i$, com soma zero e tamanho $|I| \equiv 0 (\bmod n)$.

Portanto, $s_0(G) \leq D(G \times C_n)$. □

Proposição 4.3. *Seja G o p-grupo abeliano finito $C_{p^{e_1}} \times \cdots \times C_{p^{e_r}}$, onde $p \in \mathbb{N}$ é primo, $r, e_i \in \mathbb{N}$ e $e_1 \leq \cdots \leq e_r$. Então $s_0(G) = D(G) + exp(G) - 1$.*

Demonstração. Como $exp(G) = p^{e_r}$ e $D(G \times C_{p^{e_r}}) = D(G) + p^{e_r} - 1$ pelo Teorema 2.2, então do Lema 4.2 segue que $s_0(G) = D(G) + exp(G) - 1$. □

Lema 4.4. *Sejam $m, n \geq 2$ inteiros satisfazendo $s_0(C_m^2) = 3m - 2$ e $D(C_n^3) = 3n - 2$. Então $s_0(C_{mn}^2) = 3mn - 2$.*

Demonstração. Como $D(C_{mn}^2) = 2mn-1$, pelo Corolário 2.9, então $s_0(C_{mn}^2) \geq 3mn-2$ pelo Lema 4.2. Logo é suficiente provarmos que $s_0(C_{mn}^2) \leq 3mn-2$.

Sejam $G = C_{mn}^2$ e $S = \prod_{i=1}^{l} g_i$ uma seqüência em $\mathcal{F}(G)$ com $l = 3mn-2$. Consideremos $H = G \times C_{mn}$, $C_{mn} = \langle x \rangle$ e $U = \prod_{i=1}^{l}(g_i, x) \in \mathcal{F}(H)$. Provaremos que S possui as seguintes subseqüências $S_i = \prod_{j \in I(i)} g_j$ onde $I(i) \subseteq [1, 3mn-2]$, $|I(i)| = m$ para todo $i \in [1, 3n-3]$ e $|I(3n-2)| \in \{m, 2m\}$. Também mostraremos que U tem uma subseqüência $W = \prod_{i \in J} U_i$, $\varnothing \neq J \subseteq [1, 3n-2]$, com $\sigma(W) = 0$ e $U_i = \prod_{j \in I(i)}(g_j, x)$. Assim, teremos $T = \prod_{i \in J} S_i \mid S$ com $\sigma(T) = 0$ e $|T| \equiv 0 (\operatorname{mod} mn)$.

Seja $\phi : H \to H$, dada por $\phi(h) = nh$ para todo $h \in H$, então, pela Proposição 3.4, temos que $ker(\phi) \cong C_n^3$ e $\phi(G) \cong C_m^2$.

Como $3nm - 2 = (3n-4)m + (4m-2)$ e $s(C_m^2) < 4m-2$ pelo Teorema 3.15, então para a seqüência $S = \prod_{i=1}^{l} g_i$ temos que $\phi(S) = \prod_{i=1}^{l} ng_i \in \mathcal{F}(\phi(G))$ tem uma subseqüência $\phi(S_1)$ com $|\phi(S_1)| = m$ e $\sigma(\phi(S_1)) = 0$. Podemos repetir este procedimento $3n-4$ vezes para obtermos esta quantidade de subseqüências disjuntas aos pares, $\phi(S_i)$, para todo $i \in [1, 3n-4]$, com $|\phi(S_i)| = m$ e $\sigma(\phi(S_i)) = 0$. Além disso, restará uma subseqüência com tamanho $4m-2$, esta por sua vez possuirá uma subseqüência $\phi(S_{3n-3})$ com tamanho $|\phi(S_{3n-3})| = m$ e $\sigma(\phi(S_{3n-3})) = 0$.

De $|S \cdot \prod_{i=1}^{3n-3} S_i^{-1}| = 3m-2$ e pela hipótese de que $s_0(C_m^2) = 3m-2$ segue que existe uma subseqüência $\phi(S_{3n-2})$, com $\sigma(\phi(S_{3n-2})) = 0$ e tamanho divisível por m, isto é, $|\phi(S_{3n-2})| \in \{m, 2m\}$.

Para $i \in [1, 3n-2]$ seja $U_i \mid U$ a subseqüência de U correspondente à $S_i = \prod_{j \in I(i)} g_j$ onde $I(i) \subseteq [1, 3mn-2]$. De $\phi(\sigma(U_i)) = \sigma(\phi(U_i))$ e $\sigma(\phi(U_i)) = (\sigma(\phi(S_i)), mnx) = 0$ para todo $i \in [1, 3n-2]$ temos que $\sigma(U_i) \in ker(\phi)$ e $V = \prod_{i=1}^{3n-2} \sigma(U_i)$ é uma seqüência em $\mathcal{F}(ker(\phi))$ com tamanho $3n-2$.

Como por hipótese $3n-2 = D(C_n^3)$, então existe $\varnothing \neq J \subseteq [1, 3n-2]$ tal que $V_1 = \prod_{i \in J} \sigma(U_i)$ é uma subseqüência de V com soma zero. Daí, $W = \prod_{i \in J} U_i$ é uma subseqüência de U com soma zero pois $\sigma(W) = \sum_{i \in J} \sigma(U_i) = \sigma(V_1)$. De $0 = \sigma(W) = \sum_{i \in J} \sum_{j \in I(i)} (g_j, x) =$

$\sum_{i\in J}(\sigma(S_i), |I(i)|x)$ segue que $|W| = \sum_{i\in J} |I(i)| \equiv 0 (\mathrm{mod}\, mn)$.

Portanto, $T = \prod_{i\in J} S_i$ é tal que $\sigma(T) = 0$ e tamanho $|T| = |W| \equiv 0 (\mathrm{mod}\, mn)$.

$\square$

Teorema 4.5. *Seja $n \geq 2$ um inteiro, então $s_0(C_n^2) = 3n - 2$.*

Demonstração. Seja $n = \prod_{i=1}^{l} {p_i}^{k_i}$ com p_i primos, $l, k_i \in \mathbb{N}$, a fatoração canônica de n. Provaremos o Teorema aplicando o Princípio de Indução Finita sobre l.

Para $l = 1$, n é uma potência de um inteiro primo, $n = p^k$, então o resultado segue do Lema 4.4 observando que $D(C_{p^r}^2) = 2p^r - 1$ e $D(C_{p^r}^3) = 3p^r - 2$, devido ao Teorema 2.2.

Suponhamos que o resultado vale para $l \geq 1$.

Consideremos $m = \prod_{i=1}^{l} {p_i}^{k_i}$, $n = m{p_{l+1}}^{k_{l+1}}$. Pela hipótese de indução temos que $s_0(C_m^2) = 3m - 2$, $D(C^3_{{p_{l+1}}^{k_{l+1}}}) = 3{p_{l+1}}^{k_{l+1}} - 2$ pelo Teorema 2.2. Então o Lema 4.4 implica que $s_0(C_n^2) = 3n - 2$.

$\square$

4.2 Uma cota superior para $s(G)$

Nesta seção veremos uma generalização da desigualdade (4.1).

Teorema 4.6. *Sejam G um grupo abeliano finito, $H \leqslant G$ um subgrupo de G e S uma seqüência em $\mathcal{F}(G)$ com $|S| \geq (s(H) - 1)exp(G/H) + s(G/H)$. Então S tem uma subseqüência de soma zero e tamanho $exp(H)exp(G/H)$. Em particular, se $exp(G) = exp(H)exp(G/H)$, então*

$$s(G) \leq (s(H) - 1)exp(G/H) + s(G/H).$$

Demonstração. Seja $\phi : G \to G/H$, o epimorfismo canônico, dado por $\phi(g) = g+H$ para cada $g \in G$. De $|\phi(S)| = |S|$ e de $|S| \geq s(G/H)$ segue que $\phi(S)$ possui uma subseqüência $\phi(S_1)$ com $|S_1| = exp(G/H)$, $\sigma(\phi(S_1)) = 0$, e resta uma subseqüência com tamanho maior ou igual a $(s(H) - 2)exp(G/H) + s(G/H)$. De novo, repetimos este procedimento para obtermos mais uma subseqüência $\phi(S_2)$ com $|S_2| = exp(G/H)$, $\sigma(\phi(S_2)) = 0$, e uma subseqüência com tamanho maior ou igual a $(s(H) - 3)exp(G/H) + s(G/H)$.

Após repetirmos este procedimento $s(H) - 1$ vezes obteremos esta quantidade de subseqüências disjuntas aos pares, $\phi(S_i)$, para todo $i \in [1, s(H)-1]$, com $|S_i| = exp(G/H)$,

$\sigma(\phi(S_i)) = 0$, e restará uma subseqüência com tamanho maior ou igual a $s(G/H)$. Mais uma vez aplicamos o procedimento anterior para obtermos uma subseqüência $\phi(S_{s(H)})$ com $|S_{s(H)}| = exp(G/H)$, $\sigma(\phi(S_{s(H)})) = 0$, a qual é disjunta das anteriormente obtidas.

Seja $T = \prod_{i=1}^{s(H)} \sigma(S_i)$, de $\phi(\sigma(S_i)) = \sigma(\phi(S_i)) = 0$ segue que $T \in \mathcal{F}(ker(\phi))$. Como $ker(\phi) = H$, então T tem uma subseqüência $T' = \prod_{j\in I} \sigma(S_j)$, $I \subseteq [1, s(H)]$, com soma zero e tamanho $|I| = exp(H)$.

Logo, a seqüência $S' = \prod_{j\in I} S_j$ tem tamanho $|S'| = exp(H)exp(G/H)$ e soma zero.

Em particular, se $exp(G) = exp(H)exp(G/H)$ então $s(G) \leq (s(H) - 1)exp(G/H) + s(G/H)$, pela definição do invariante $s(G)$.

□

Proposição 4.7 (Harborth [10])**.** *Seja o grupo $G = C^d_{nm}$ com $n, m, d \in \mathbb{N}$, então*

$$s(C^d_{nm}) \leq min\{s(C^d_n) + (s(C^d_m) - 1)n, s(C^d_m) + (s(C^d_n) - 1)m\}.$$

Demonstração. Sejam $C^d_n \cong H \leqslant G$ e $C^d_m \cong K \leqslant G$. Como $G/H \cong K$, $G/K \cong H$, $exp(H) = n$ e $exp(K) = m$, então $exp(G) = exp(H)exp(K)$. Pelo Teorema 4.6 segue que $s(G) \leq s(C^d_n) + (s(C^d_m) - 1)n$ e $s(G) \leq s(C^d_m) + (s(C^d_n) - 1)m$. □

Corolário 4.8. *Sejam $n, m \in \mathbb{N}, n, m \geq 2$, com $n \mid m$ e o grupo $G = C_n \times C_m$. Então*

$$s(G) \leq 2(m + n) - 3.$$

Demonstração. Seja $l \in \mathbb{N}$, $n = \prod_{i=1}^{l} q_i$, $q_i \in \mathbb{N}, q_i \geq 2$ para todo $i \in [1, l]$ uma fatoração qualquer de n. Sejam $\varphi_1 : C_n \to C_n$ e $\varphi_2 : C_m \to C_m$ endomorfismos multiplicação por q_1. Pela Proposição 3.4 segue que $\varphi_1(C_n) \cong C_{n/q_1}$ e $\varphi_2(C_m) \cong C_{m/q_1}$.

Seja $H = \varphi_1(C_n) \times \varphi_2(C_m) \leqslant G$, então $G/H \cong C_n/C_{n/q_1} \times C_m/C_{m/q_1} \cong C_{q_1} \times C_{q_1}$.

Provaremos o Corolário aplicando o Princípio de Indução Finita sobre l.

Se $l = 1$ obtemos $H \cong \{1\} \times C_{m/q_1}$ e pelo Teorema 4.6 vem que

$$\begin{aligned} s(G) &\leq (s(H) - 1)exp(G/H) + s(G/H) \\ &\leq (s(C_{\frac{m}{q_1}}) - 1)q_1 + s(C_{q_1} \times C_{q_1}) \\ &\leq ((2\frac{m}{q_1} - 1) - 1)q_1 + 4q_1 - 3 \\ &\leq 2m + 2q_1 - 3. \end{aligned}$$

Onde na terceira desigualdade usamos o Teorema de Erdös, Ginzburg e Ziv, Corolário 2.12 e o Teorema 3.15.

Se $l \geq 2$, por hipótese de indução temos que $s(H) \leq 2(\frac{m}{q_1} + \frac{n}{q_1}) - 3$, o Teorema 4.6 implica que

$$\begin{aligned} s(G) &\leq (s(H)-1)exp(G/H) + s(G/H) \\ &\leq (s(H)-1)q_1 + s(C_{q_1} \times C_{q_1}) \\ &\leq (2(\frac{m}{q_1} + \frac{n}{q_1}) - 3 - 1)q_1 + 4q_1 - 3 \\ &\leq 2(m+n) - 3. \end{aligned}$$

De novo, na terceira desigualdade usamos o Teorema 3.15.

Portanto, o Corolário está provado.

□

4.3 A determinação de $s(C_{3^n}^3)$ e de $s(C_{2^n}^d)$

A seguir provaremos que $s(C_{3^n}^3) = 9 \cdot 3^n - 8$. Além disso, veremos o seguinte resultado de Harborth [10], $s(C_{2^n}^d) = (2^n - 1)2^d + 1$.

Proposição 4.9. *Temos que* $s(C_{3^n}^3) = 9 \cdot 3^n - 8$*, para todo* $n \in \mathbb{N}$.

Demonstração. Em [4], Elsholtz prova que

$$s(C_n^d) \geq 1,125^{\lfloor d/3 \rfloor}(n-1)2^d + 1,$$

para todos $n \geq 3$ ímpar e $d \geq 3$ inteiros.

Então, segue que $s(C_{3^n}^3) \geq 9 \cdot 3^n - 8$.

Provaremos, pelo Princípio de Indução Finita sobre $n \in \mathbb{N}$, que $s(C_{3^n}^3) \leq 9 \cdot 3^n - 8$.

O caso $n = 1$ segue de que $s(C_3^3) = 9 \cdot 3 - 8$ por Harborth [10].

Suponhamos, por hipótese de indução, que $s(C_{3^{(n-1)}}^3) = 9 \cdot 3^{(n-1)} - 8$ para todo $n \geq 2$.

Sejam $G = C_{3^n}^3$ e $H \leqslant G$ um subgrupo de G tal que $H \cong C_{3^{(n-1)}}^3$, então $G/H \cong C_3^3$, $s(H) = 9 \cdot 3^{(n-1)} - 8$, $s(G/H) = 9 \cdot 3 - 8$, $exp(H) = 3^{(n-1)}$ e $exp(G/H) = 3$.

Como $exp(G) = 3^n = exp(H)exp(G/H)$, segue do Teorema 4.6 que

$$\begin{aligned} s(G) &\leq (9 \cdot 3^{(n-1)} - 8 - 1)3 + (9 \cdot 3 - 8) \\ &\leq 9 \cdot 3^n - 8. \end{aligned}$$

Portanto, $s(C_{3^n}^3) = 9 \cdot 3^n - 8$, para todo $n \in \mathbb{N}$. □

Proposição 4.10. *[Harborth [10].] Temos que* $s(C_{2^n}^d) = (2^n - 1)2^d + 1$, *para todos* $d, n \in \mathbb{N}$.

Demonstração. Da Proposição 3.3 segue que $(2^n - 1)2^d + 1 \leq s(C_{2^n}^d)$, para todos $d, n \in \mathbb{N}$.

Provaremos aplicando o Princípio de Indução Finita sobre $n \in \mathbb{N}$, que $s(C_{2^n}^d) \leq (2^n - 1)2^d + 1$.

Seja $n = 1$, segue da Proposição 3.3, que $s(C_2^d) = 2^d + 1$.

Suponhamos, por hipótese de indução, que $s(C_{2^{(n-1)}}^d) = (2^{(n-1)} - 1)2^d + 1$, para todo $n \geq 2$.

Sejam $G = C_{2^n}^d$ e $H \leqslant G$ um subgrupo de G tal que $H \cong C_{2^{(n-1)}}^d$, então $G/H \cong C_2^d$, $s(H) = (2^{(n-1)} - 1)2^d + 1$, $s(G/H) = 2^d + 1$, $exp(H) = 2^{(n-1)}$ e $exp(G/H) = 2$.

Como $exp(G) = exp(H)exp(G/H)$, segue do Teorema 4.6 que

$$\begin{aligned} s(G) &\leq (s(H) - 1)exp(G/H) + s(G/H) \\ &\leq ((2^{(n-1)} - 1)2^d + 1 - 1)2 + (2^d + 1) \\ &\leq (2^n - 1)2^d + 1. \end{aligned}$$

Portanto, $s(C_{2^n}^d) = (2^n - 1)2^d + 1$, para todo $n \in \mathbb{N}$. $\square$

Conclusão

Nosso objetivo foi estudar os invariantes $D(G), s(G)$ e $s_0(G)$ para um grupo abeliano finito G, mais especificamente vimos:

1) $D(G) = 1 + \sum_{i=1}^{r} (p^{e_i} - 1)$ para o p-grupo abeliano finito $G = C_{p^{e_1}} \times \cdots \times C_{p^{e_r}}$, p primo;

2) Sejam $m, n \in \mathbb{N}$, $m \mid n$ e o grupo $G = C_m \times C_n$, obtivemos que $D(G) = m + n - 1$, em particular, obtivemos o Teorema de Erdös, Ginzburg e Ziv:

$$s(C_n) = 2n - 1 \text{ para todo } n \in \mathbb{N};$$

3) A Conjectura de Kemnitz: $s(C_n^2) = 4n - 3$, para todo $n \in \mathbb{N}$;

4) Para todo G grupo abeliano finito com $exp(G) = n \geq 2$ tem-se

$$D(G) + n - 1 \leq s_0(G) \leq min\{s(G), D(G \times C_n)\};$$

5) $s_0(C_n^2) = 3n - 2$ para todo $n \geq 2 \ \in \mathbb{N}$;

6) Para todo G, grupo abeliano finito, $H \leqslant G$, se $S \in \mathcal{F}(G)$ com $|S| \geq (s(H) - 1)exp(G/H) + s(G/H)$, então $S(m) \neq \varnothing$ para $m = exp(H)exp(G/H)$, em particular, se $exp(G) = m$, então $s(G) \leq (s(H) - 1)exp(G/H) + s(G/H)$;

7) $s(C_n \times C_m) \leq 2(m + n) - 3$, para todos $n, m \in \mathbb{N}, n, m \geq 2$ e $n \mid m$;

8) Como uma aplicação da desigualdade obtida por Elsholtz [4]:

$$s(C_n^d) \geq 1,125^{\lfloor d/3 \rfloor}(n-1)2^d + 1, \text{para todos } n \geq 3, \text{ímpar e } d \geq 3$$

e do resultado do item 6) obtivemos $s(C_{3^n}^3) = 9 \cdot 3^n - 8$, para todo $n \in \mathbb{N}$.

O resultado do item 8) nos sugere uma expressão geral para o invariante $s(C_{p^n}^3)$ sendo p um primo ímpar.

Em [15] Olson faz a seguinte conjectura: para o grupo abeliano $G = C_{n_1} \times \cdots \times C_{n_r}$ onde $n_i \mid n_{i+1}$ tem-se $D(G) = 1 + \sum_{i=1}^{r} (n_i - 1)$.

Como vimos a igualdade é válida se G é um p-grupo ou se $r \leq 2$, e quando $r \geq 2$ sabemos, até o momento, apenas que $D(G) \leq 1 + \sum_{i=1}^{r} (n_i - 1)$, resultado que foi provado por Gao e Geroldinger em [6]. Recentemente G. Bhowmik e J. Schlage-Puchta [2] provaram que a conjectura de Olson é verdadeira para o grupo $G = C_3 \times C_3 \times C_{3r}$.

Em [1] Alon e Dubiner provam que $s(G \times H) \leq 6n - 5$ para G, H grupos abelianos finitos com $|G| = |H| = n$.

Referências Bibliográficas

[1] Alon, N. and Dubiner, M., *Zero-sum sets of prescribed size.* In Combinatorics, Paul Erdos is Eighty, J. Bolyai Math. Soc. 1 1993, 33-50.

[2] Bhowmik, G., Schlage-Puchta, J., *Davenport's constant for groups of the form* $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{3d}$. arXiv:math.NT/0610416 v1 12 Oct 2006.

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

[4] Elsholtz, C., *Lower bounds for multidimensional zero sums.* Combinatorica. 24 2004, 351-358.

[5] Erdös, P., Ginzburg, A., and Ziv,A., *Theorem in the additive number theory.* Bulletim Research Council Israel. 1961, 41-43.

[6] Gao, W., Geroldinger A., *On long minimal zero sequences in finite abelian groups.* Periodica Math. Hungar., 38 1999, 179-211.

[7] Gao, W., *Note on a zero-sum problem.* Journal Combinatorial Theory. Series A 95 2001, 387-389.

[8] Gao, W., *On zero-sum subsequences of restricted size II.* Discrete Mathematics. 271 2003, 51-59.

[9] Gao, W., Geroldinger A., *On zero sum sequences in* $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$. Integers: Eletronic Journal of Combinatorial Number Theory. 3 A8 2003, 45 pp.

[10] Harborth, H., *Ein Extremalproblem für Gitterpunkte.* J. Reine Angew. Math. 262 1973, 356-360.

[11] Herstein, I. N., *Topics in Algebra.* John Wiley and Sons, 2nd edition, (1975).

[12] Hungerford, T. W., *Algebra*. Holt, Rinehart and Winston Inc. (1974).

[13] Nathanson, M. B., *Additive number theory: inverse problems and the geometry of sumsets*. Springer-Verlag New York Inc. (1996).

[14] Kemnitz, A., *On a lattice point problem*. Ars Combinatoria, 16 1983, 151-160.

[15] Olson, J. E., *A combinatorial problem on finite abelian groups I*. Journal of Number Theory. 1 1969, 8-10.

[16] Olson, J. E., *A combinatorial problem on finite abelian groups II*. Journal of Number Theory. 1 1969, 195-199.

[17] Reiher, C., *On Kemnitz' Conjecture concerning lattice-points in the plane*. The Ramanujan Journal, Vol. 13, No. 1-3 (2007), 333-337 to appear.

[18] Robinson, D. J. S., *A course in the theory of groups*. Springer-Verlag New York Inc, 2nd edition. (1996).

[19] Rónyai, L., *On a conjecture of Kemnitz*. Combinatorica. 20 2000, 569-573.

[Baixar livros de Literatura](#)
[Baixar livros de Literatura de Cordel](#)
[Baixar livros de Literatura Infantil](#)
[Baixar livros de Matemática](#)
[Baixar livros de Medicina](#)
[Baixar livros de Medicina Veterinária](#)
[Baixar livros de Meio Ambiente](#)
[Baixar livros de Meteorologia](#)
[Baixar Monografias e TCC](#)
[Baixar livros Multidisciplinar](#)
[Baixar livros de Música](#)
[Baixar livros de Psicologia](#)
[Baixar livros de Química](#)
[Baixar livros de Saúde Coletiva](#)
[Baixar livros de Serviço Social](#)
[Baixar livros de Sociologia](#)
[Baixar livros de Teologia](#)
[Baixar livros de Trabalho](#)
[Baixar livros de Turismo](#)