Universidade de Brasília

Instituto de Ciências Exatas

Departamento de Matemática

Contribuições sobre as Constantes EGZ Ponderada e de Davenport

por

Filipe Augusto Alves de Oliveira

Orientador: Hemar Teixeira Godinho

Brasília

2018

Contribuições sobre as Constantes EGZ Ponderada e de Davenport

Filipe Augusto Alves de Oliveira

Tese apresentada ao Programa de Pós-Graduação do Departamento de Matemática da Universidade de Brasília, como requisito parcial para obtenção do título de Doutor em Matemática.

Área de concentração: Teoria dos Números.

Orientador: Prof. Dr. Hemar Teixeira Godinho

Brasília

2018

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

O48c

Oliveira, Filipe Augusto Alves de
Contribuições sobre as Constantes EGZ Ponderada e de Davenport / Filipe Augusto Alves de Oliveira; orientador Hemar Teixeira Godinho. -- Brasília, 2018.
65 p.

Tese (Doutorado - Doutorado em Matemática) -- Universidade de Brasília, 2018.

1. Grupos abelianos finitos. 2. Problemas de soma-zero. 3. Soma-zero ponderada. 4. Constante de Davenport. 5. Polinômios Simétricos. I. Godinho, Hemar Teixeira, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Contribuições sobre as Constantes EGZ Ponderada e de Davenport

por

Filipe Augusto Alves de Oliveira

Tese apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática-UnB, como requisito parcial para obtenção do grau de

DOUTOR EM MATEMÁTICA*

Brasília, 23 de novembro de 2018.

Comissão Examinadora:

Prof. Dr. Hemar Teixeira Godinho – Orientador (MAT-UnB)

Prof. Dr. Diego Marques Ferreira (MAT-UnB)

Prof. Dr. Abílio Lemos Cardoso Júnior (UFV)

Prof. Dr. Paulo Henrique de Azevedo Rodrigues (UFG)

* O autor foi bolsista CAPES durante a elaboração desta tese.

Ao meu filho e à minha esposa,
Heitor Moura Alves de Oliveira e
Bárbara Moura de Oliveira.

Agradecimentos

Esta é uma das partes mais importantes da tese, uma vez que este é o espaço onde posso reconhecer e agradecer a todas as pessoas que fizeram parte desta trajetória.

Antes de tudo e todos, agradeço a Deus por ter me dado toda a força e a paciência necessárias para vencer todos os obstáculos desta caminhada e, principalmente, por ter colocado ao meu lado todos aqueles que agradecerei aqui, além daqueles não citados, mas que direta ou indiretamente contribuíram para esta conquista.

Sou grato a minha esposa Bárbara e a meu filho Heitor, por serem meu porto seguro, a minha base de sustentação. Agradeço por estarem sempre ao meu lado, suportando todos os momentos de dificuldades sem me deixar desanimar.

Agradeço as minhas duas mães, Efigênia e Maria (*in memoriam*), por todo o incentivo e pelas lições mais valiosas de minha vida.

A minha irmã Karla, por fazer parte de toda a minha história.

A minha "tia" Maninha e ao meu "primo" Werner por todo o suporte que nos deram em Brasília e que, mesmo não sendo meus parentes, fazem parte da minha família.

Aos amigos da MAT-UnB pelo companheirismo durante esta jornada. Agradeço em especial aos amigos Alessandra, Bruno, Carol, Daiane, Elaine, Gérsica, Jean, Josimar, Lais e Lucimeire.

Ao meu orientador, Hemar, por toda a confiança, a atenção e a compreensão durante este período.

Ao professor Abílio, por todos os ensinamentos e por sempre acreditar em meu potencial.

Ao professor Diego, por toda sua contribuição em minha formação.

Ao professor Paulo Henrique, por aceitar o convite de participar das minhas bancas de qualificação e de defesa.

A todos os professores e funcionários da MAT-UnB pela dedicação.

E finalmente, a CAPES, pelo suporte financeiro.

"Por vezes, sentimos que aquilo que fazemos não é, senão, uma gota de água no mar. Mas o mar seria menor se lhe faltasse uma gota."

Madre Teresa de Calcutá

Resumo

A Constante de Erdös-Ginzburg-Ziv (denotada por $s(G)$) de um grupo aditivo abeliano finito G é o menor inteiro ℓ tal que cada sequência sobre G de comprimento ℓ possui uma subsequência de comprimento $\exp(G) = n$ cuja soma dos elementos é igual ao zero do grupo. A constante com pesos coprimos análoga a esta constante (denotada por $s_A(G)$) é definida da mesma forma exceto que no lugar de considerar a soma de todos os elementos da subsequência pode-se optar por adicionar o elemento ou um múltiplo do elemento tal que os coeficientes da soma pertencem a $A = \{a \in \mathbb{Z}\,;\, \text{mdc}(a, n) = 1\}$. Determinamos o valor desta constante para p-grupos de posto 2, analisamos o problema inverso relacionado e obtivemos um limite superior para $s_A(G)$ em um caso mais geral.

Em uma análise distinta, sejam p um primo, $n \in \mathbb{N}$ e $\varphi \in \mathbb{Z}_p[x_1, \ldots, x_n]$ um polinômio simétrico sobre o corpo $\mathbb{Z}_p$. Considere que o polinômio é tal que podemos gerar o conjunto $\mathcal{F}_\varphi = \{\varphi_k\,;\, k \in \mathbb{N}\}$, onde cada $\varphi_k \in \mathbb{Z}_p[x_1, \ldots, x_k]$ representa o polinômio com o mesmo grau e os mesmos coeficientes de φ, alterando-se o número de variáveis. Uma sequência T sobre $\mathbb{Z}_p$ é uma *sequência $\mathcal{F}_\varphi$-zero* se $\varphi_k(T) = 0$, para algum $k \in \mathbb{N}$, e é chamada uma *$\mathcal{F}_\varphi$-zero livre* se não contém subsequências $\mathcal{F}_\varphi$-zero. Definimos a constante $D(\varphi, \mathbb{Z}_p)$ como sendo o menor inteiro ℓ tal que cada sequência de comprimento ℓ contém uma subsequência $\mathcal{F}_\varphi$-zero. Também definimos o conjunto $M(\mathcal{F}_\varphi, \mathbb{Z}_p)$ de todas as subsequências $\mathcal{F}_\varphi$-zero livres de comprimento $D(\varphi, \mathbb{Z}_p) - 1$. Além disso, analisamos $D(\varphi, \mathbb{Z}_p)$ e $M(\mathcal{F}_\varphi, \mathbb{Z}_p)$ no caso de polinômios simétricos quadráticos.

Palavras-chave: Grupos abelianos finitos; Problemas de soma-zero; Soma-zero ponderada; Constante de Davenport; Polinômios Simétricos.

Abstract

The Erdös-Ginzburg-Ziv constant (denoted by $s(G)$) of an additive finite abelian group G is the smallest integer ℓ such that each sequence over G of length ℓ has a subsequence of length $\exp(G) = n$ whose elements sum to zero of the group. The coprime weighted analogue of these constant (denoted by $s_A(G)$) is defined in the same way except that instead of considering the sum of all elements of the subsequence one can choose to add either the element or multiple of the element such that the coefficients of the sum belong to $A = \{x \in \mathbb{Z}\,;\, \gcd(x, n) = 1\}$. We determine this constant for p-groups of rank 2, we analyzed the related inverse problem and obtained an upper bound for $s_A(G)$ in a more general case.

In a separate analysis, let p be a prime, $n \in \mathbb{N}$ and $\varphi \in \mathbb{Z}_p[x_1, \ldots, x_n]$ a symmetric polynomial over the field $\mathbb{Z}_p$. Consider that the polynomial is such that we can generate the set $\mathcal{F}_\varphi = \{\varphi_k\,;\, k \in \mathbb{N}\}$, where each $\varphi_k \in \mathbb{Z}_p[x_1, \ldots, x_k]$ represents the polynomial with the same degree and the same coefficients of φ, changing the number of variables. A sequence T over $\mathbb{Z}_p$ is a *$\mathcal{F}_\varphi$-zero sequence* if $\varphi_k(T) = 0$, for some $k \in \mathbb{N}$, and is called a *$\mathcal{F}_\varphi$-zero free sequence* if contains no $\mathcal{F}_\varphi$-zero subsequence. We define the constant $D(\varphi, \mathbb{Z}_p)$ as being the smallest integer ℓ such that every sequence of length ℓ contains a $\mathcal{F}_\varphi$-zero subsequence. Also we define the set $M(\mathcal{F}_\varphi, \mathbb{Z}_p)$ of all the $\mathcal{F}_\varphi$-zero free sequences of length $D(\varphi, \mathbb{Z}_p) - 1$. In addition, we analyze $D(\varphi, \mathbb{Z}_p)$ and $M(\mathcal{F}_\varphi, \mathbb{Z}_p)$ in the case of quadratic symmetric polynomials.

Keywords: Finite abelian group; Zero-sum problem; Weighted zero-sum; Davenport constant; Symmetric polynomials.

Sumário

Introdução **1**

1 Constante EGZ para p-Grupos de Posto 2 **12**

1.1 Notações, Terminologias e Preliminares 12

1.2 Resultados Iniciais 14

1.3 O Valor Exato de $s_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta})$ 21

1.4 O Problema Inverso Relacionado 26

1.5 Um Limite Superior para um Caso Mais Geral 32

1.6 Considerações Adicionais 34

2 Uma Generalização para a Constante de Davenport **36**

2.1 Conceitos e Resultados Preliminares 36

2.2 A Constante de Davenport sob o ponto de vista dos Polinômios Simétricos 40

2.3 O Valor da Constante $D(\varphi, \mathbb{Z}_p)$ para Polinômios Simétricos Quadráticos . . 42

2.4 Observações Finais 47

Referências Bibliográficas **50**

Introdução

Seja G um grupo aditivo tal que G é abeliano e finito. Dado um número inteiro positivo t, definimos uma *sequência finita*

$$S = (x_1, x_2, \ldots, x_t) = x_1 x_2 \cdots x_t = \prod_{i=1}^{t} x_i$$

de elementos pertencentes a G, onde é permitida a repetição de elementos e podemos desconsiderar a ordem dos elementos em S (tornando coerente a notação multiplicativa). Diremos apenas que S é uma *sequência* sobre G de *comprimento* t. Definimos também uma *subsequência* $T = x_{i_1} x_{i_2} \cdots x_{i_k}$ de S de comprimento k ($\leq t$), com conjunto de índices $I_T = \{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, t\}$, onde escrevemos $T|S$. Além disso, chamamos S de *sequência de soma-zero* em G se

$$x_1 + x_2 + \cdots + x_t = 0,$$

onde 0 representa o elemento neutro (aditivo) de G.

Os *Problemas de Soma-Zero* são problemas combinatórios da Teoria Aditiva dos Números que estão relacionados com a estrutura de grupos abelianos finitos. De forma geral, um problema direto de soma-zero estuda condições que garantam que uma determinada sequência possua uma subsequência de soma-zero com propriedades pré-definidas. O problema inverso de soma-zero associado estuda a estrutura de sequências extremas que não possuem tais subsequências de soma-zero.

Muitas pesquisas se desenvolveram baseadas nestes problemas, uma vez que investigações desse tipo ocorrem naturalmente em vários ramos da análise combinatória, da

teoria dos números e da geometria. Os problemas de soma-zero também influenciaram o desenvolvimento de vários campos dentro destas áreas como a teoria de Ramsey de soma-zero, entre outros. Há, ainda, conexões intrínsecas com a teoria dos grafos, a teoria de Ramsey, a geometria e a teoria das fatorações não-singulares. Além de tudo isso, problemas de soma-zero aparecem em vários tópicos da teoria dos números como números de Carmichael, conjectura de Artin sobre formas aditivas, matrizes de permutação, entre outros.

Os problemas de soma-zero tiveram como ponto de partida um resultado de 1961, onde, dado um número inteiro positivo n, Paul Erdös, Abraham Ginzburg e Abraham Ziv mostraram (ver [18]) que toda sequência de números inteiros formada por $2n-1$ números possui uma subsequência de comprimento n cuja soma dos seus termos é um múltiplo de n. Este resultado é conhecido como o *Teorema de Erdös-Ginzburg-Ziv* (Teorema EGZ) e sua demonstração foi desenvolvida utilizando o *Princípio da Casa dos Pombos*.

Este resultado motivou a definição da seguinte constante: dado um grupo (aditivo) abeliano finito G arbitrário, definimos a constante $E(G)$ como sendo o menor inteiro positivo t tal que toda sequência de t elementos de G contém uma subsequência de comprimento igual a $o(G)$, onde $o(G)$ denota a ordem do grupo G, que é uma sequência de soma-zero sobre G. Observe o seguinte resultado:

Teorema 0.1. *Seja n um inteiro positivo e seja $\mathbb{Z}_n$ o grupo aditivo das classes de resíduos módulo n.*

(i) $E(\mathbb{Z}_n) = 2n-1$.

(ii) *As sequências de comprimento $2n-2$ em $\mathbb{Z}_n$ que não contém uma subsequência de soma-zero de comprimento n apresentam exatamente dois termos distintos de $\mathbb{Z}_n$, onde cada um se repete $n-1$ vezes.*

O ítem (i) do Teorema 0.1 é uma consequência direta do Teorema de Erdös-Ginzburg-Ziv. O item (ii) deste teorema corresponde ao problema inverso relativo ao item (i) e uma demonstração para esta parte pode ser encontrada em [45].

Constantes Associadas à Constante EGZ

Alguns anos após P. Erdös, A. Ginzburg e A. Ziv enunciarem o Teorema EGZ, P. C. Baayen, P. Erdös e H. Davenport propuseram (na *Mid-western Conference on Group Theory and Number Theory*, Ohio State University, em abril de 1966) um problema cuja resolução se resumia em determinar o valor do menor inteiro positivo ℓ tal que cada sequência S sobre um grupo (aditivo) abeliano finito G de comprimento $|S| \geq \ell$ contém uma subsequência de soma-zero em G (sem restrições para o comprimento da subsequência). Na literatura subsequente este inteiro ℓ passou a ser chamado *Constante de Davenport* de G e denotado por $D(G)$.

O primeiro e mais importante resultado sobre a Constante de Davenport para grupos cíclicos finitos será apresentado à seguir.

Teorema 0.2. *Sejam n um inteiro positivo e $\mathbb{Z}_n$ o grupo aditivo das classes residuais módulo n. Então $D(\mathbb{Z}_n) = n$ e, além disso, o conjunto de todas as sequências de comprimento $n-1$ livres de subsequências de soma-zero é formado apenas por sequências em que apenas um elemento, invertível em $\mathbb{Z}_n$, se repete $n-1$ vezes.*

Acrescentando uma quantidade adequada de zeros à sequência, vemos que a demonstração do Teorema 0.2 é uma consequência direta do Teorema 0.1.

Em 1973, Harborth (ver [30]) definiu dois invariantes e um deles formaliza o que foi feito no Teorema EGZ. A saber, dado o grupo $\mathbb{Z}_n^r$, onde n e r são inteiros positivos, a constante $f(n,r)$ é o menor inteiro ℓ tal que toda sequência S de elementos de $\mathbb{Z}_n^r$, de comprimento ℓ, possui uma subsequência de soma-zero de comprimento n; e a constante $g(n,r)$ é o menor inteiro t tal que toda sequência S de termos *distintos* de $\mathbb{Z}_n^r$, com comprimento t, possui uma subsequência de soma-zero de comprimento n. Neste mesmo artigo ele provou vários resultados para estas constantes para valores específicos de n e r.

Apresentaremos agora algumas constantes que serão objetos de nossos estudos. Dado um grupo (aditivo) abeliano finito G com ordem igual a $o(G) = t$ e *expoente* (definido como o menor inteiro positivo que, multiplicado por qualquer elemento do grupo, tem como resultado o zero do grupo) igual a $exp(G) = n$, definimos:

(i) $E(G)$ é o menor inteiro positivo ℓ tal que toda sequência sobre G de comprimento

ℓ contém uma subsequência de soma-zero de comprimento t.

(ii) $s(G)$ é o menor inteiro positivo ℓ tal que toda sequência sobre G de comprimento ℓ contém uma subsequência de soma-zero de comprimento n.

(iii) $D(G)$ é o menor inteiro positivo ℓ tal que toda sequência sobre G de comprimento ℓ contém uma subsequência de soma-zero sem restrições para o comprimento.

(iv) $\eta(G)$ é o menor inteiro positivo ℓ tal que toda sequência sobre G de comprimento ℓ contém uma subsequência de soma-zero de comprimento *menor ou igual a* n.

A constante $s(G)$ é chamada Constante de Erdös-Ginzburg-Ziv (ou Constante EGZ) e é uma generalização da constante $f(n,r)$. Note que, no caso de G ser um grupo cíclico, temos $s(G) = E(G)$. Além disso, podemos observar que as constantes $D(G)$ e $\eta(G)$ estão intrinsecamente ligadas.

Ainda não é possível calcular os valores exatos destas constantes para os grupos abelianos finitos de modo geral. Além disso existem muitas questões em aberto relacionadas a estas constantes. Apresentaremos agora alguns resultados conhecidos.

Logo depois da demonstração do Teorema de EGZ, Paul Erdös e outros autores passaram a buscar a determinação do valor exato de $s(\mathbb{Z}_p^2)$, onde p é um primo, $\mathbb{Z}_p$ é o grupo (aditivo) cíclico de ordem p e $\mathbb{Z}_p^2 = \mathbb{Z}_p \oplus \mathbb{Z}_p$.

Para o grupo $G = \bigoplus_{i=1}^{n} \mathbb{Z}_{p^{e_i}} = \mathbb{Z}_{p^{e_1}} \oplus \mathbb{Z}_{p^{e_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{e_n}}$, onde p é um número primo e os números n e e_i são inteiros positivos, para cada $i = 1, 2, \ldots, n$, J. Olson demonstrou em 1968 (ver [38]) que $D(G) = 1 + \sum_{i=1}^{n}(p^{e_i} - 1)$. Além disso, dados os inteiros positivos m e n tais que m divide n, Olson mostrou no mesmo ano (ver [39]) que, para o grupo $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$, temos $D(G) = m + n - 1$.

Em 1983, A. Kemnitz conjecturou (ver [31]) que $s(\mathbb{Z}_n^2) = 4n - 3$, onde n é um inteiro positivo. Este resultado foi demonstrado por C. Reiher em 2003 (mas o artigo [41] foi publicado apenas em 2007).

Em 2003, W. D. Gao (ver [20]) além de apresentar vários resultados sobre as constantes $s(G)$ e $\eta(G)$, conjecturou que, dado um grupo (aditivo) G abeliano finito arbitrário, a relação

$$s(G) = \eta(G) + \exp(G) - 1$$

é válida. Esta relação ficou conhecida como *Conjectura de Gao*.

Em 2007, Gao *et al* (ver [23]) provaram vários resultados para $s(\mathbb{Z}_n^3)$ e $\eta(\mathbb{Z}_n^3)$ para casos específicos do inteiro positivo n. Além disso provaram que a Conjectura de Gao é válida para alguns casos específicos.

Edel *et al* analisaram em [16] (2007) e em [17] (2008) cotas inferiores para $s(\mathbb{Z}_n^4)$, $s(\mathbb{Z}_n^5)$, $s(\mathbb{Z}_n^6)$ e $s(\mathbb{Z}_n^7)$.

Outros resultados para estas constantes podem ser encontrados em [20], [25], [38] e [39].

Constante EGZ Ponderada e Algumas Constantes Associadas

No artigo [11] de 1996, Y. Caro conjecturou que, dados os inteiros n e m, com $n \geq 2$ e a sequência arbitrária de números inteiros $S = \prod_{i=1}^{m+n-1} x_i$, se $U = \prod_{i=1}^{n} u_i$ é uma sequência de inteiros tais que $u_1 + u_2 + \cdots + u_n \equiv 0 \pmod{m}$, então existe uma subsequência (rearranjada) $\prod_{i=1}^{n} x_{j_i}$ de S, ou seja, $\{j_1, j_2, \ldots, j_n\} \subset \{1, 2, \ldots, m+n-1\}$, tal que

$$u_1 x_{j_1} + u_2 x_{j_2} + \cdots + u_n x_{j_n} \equiv 0 \pmod{m}.$$

Supondo que $m = n$ e $u_i = 1$, para todo $i \in \{1, 2, \ldots, n\}$, obtemos exatamente o Teorema de Erdös-Ginzburg-Ziv na conjectura acima. Esta conjectura foi completamente demonstrada por D. J. Grynkiewicz em 2006 (ver [28]) e ela deu inicio ao estudo da Constante EGZ Ponderada e suas associadas.

Antes de prosseguirmos, faremos algumas observações. Seja G um grupo (aditivo) abeliano finito de ordem $o(G) = m$ e expoente $\exp(G) = n$, onde m e n são inteiros positivos. Como podemos considerar G como um $\mathbb{Z}$-módulo, dados um conjunto $A \subseteq \mathbb{Z}$ e uma sequência $S = x_1 x_2 \cdots x_t$ de elementos de G, se existe um conjunto $\{a_1, a_2, \ldots, a_t\} \subset A$ tal que

$$a_1 x_1 + a_2 x_2 + \cdots + a_t x_t = 0 \text{ (neutro aditivo de } G),$$

então diremos que S é uma *sequência de soma-zero A-ponderada* e o conjunto A é denominado o *conjunto dos pesos*. Desta forma podemos definir as seguintes constantes

ponderadas:

(i) $E_A(G)$ é o menor inteiro positivo ℓ tal que toda sequência sobre G de comprimento ℓ contém uma subsequência de soma-zero A-ponderada de comprimento m.

(ii) $s_A(G)$ é o menor inteiro positivo ℓ tal que toda sequência sobre G de comprimento ℓ contém uma subsequência de soma-zero A-ponderada de comprimento n.

(iii) $D_A(G)$ é o menor inteiro positivo ℓ tal que toda sequência sobre G de comprimento ℓ contém uma subsequência de soma-zero A-ponderada (sem restrições para o comprimento da subsequência).

(iv) $\eta_A(G)$ é o menor inteiro positivo ℓ tal que toda sequência sobre G de comprimento ℓ contém uma subsequência de soma-zero A-ponderada de comprimento *menor ou igual a* n.

Assim como nas constantes não ponderadas, ainda não se sabe os valores destas constantes de forma geral. Apresentaremos agora alguns resultados sobre estas constantes ponderadas.

Em 2006, S. D. Adhikari *et al* mostraram (ver [5]) que, dados um inteiro positivo n e o conjunto dos pesos $A = \{1, -1\}$, temos $E_A(\mathbb{Z}_n) = s_A(\mathbb{Z}_n) = n + \lfloor \log_2 n \rfloor$, onde, para um número real x, $\lfloor x \rfloor$ denota o maior inteiro menor ou igual a x. Este resultado é equivalente ao Teorema de Erdös-Ginzburg-Ziv para o conjunto de pesos $A = \{1, -1\}$. Além disso, em 2008, S. D. Adhikari *et al* provaram (ver [3]) que $s_A(\mathbb{Z}_n^2) = 2n - 1$ para o caso em que n é um inteiro positivo ímpar e $A = \{1, -1\}$ e, neste trabalho, também são demonstrados alguns resultados para a Constante de Davenport Ponderada $D_A(\mathbb{Z}_p)$, onde p é um número primo.

Em 2007, Thangadurai desenvolveu um trabalho (ver [43]) sobre a Constante de Davenport para o caso de um p-grupo (aditivo) abeliano finito. O principal resultado deste trabalho foi: dado o grupo $G = \bigoplus_{i=1}^{t} \mathbb{Z}_{p^{e_i}}$, onde t e $1 \leq e_1 \leq e_2 \leq \cdots \leq e_t$ são inteiros positivos, então

$$D_A(G) \leq \left\lceil \frac{1}{|A|} \left(1 + \sum_{i=1}^{t} (p^{e_1} - 1) \right) \right\rceil$$

para qualquer que seja o conjunto $A \subseteq \{1, 2, \ldots, p^{e_t}\}$ não vazio, onde os elementos de A são incongruentes entre si e não nulos módulo p. Como consequência desta cota superior, foram obtidos vários resultados para casos mais particulares.

Em 2009, Adhikari e Rath provaram (ver [9]) que $E_A(\mathbb{Z}_p) = p + 2$, com p sendo um número primo e A sendo o conjunto dos resíduos quadráticos módulo p.

Em 2010, Yuan e Zeng mostraram (ver [44]) que a relação $E_A(\mathbb{Z}_n) = D_A(\mathbb{Z}_n) + |\mathbb{Z}_n| - 1$ é válida para qualquer inteiro positivo n e qualquer $A \subseteq \mathbb{Z}$ não vazio. Em 2012, D. J. Grynkiewicz, L. E. Marchan e O. Ordaz generalizaram (ver [29]) este resultado mostrando que a relação $E_A(G) = D_A(G) + |G| - 1$ é válida para qualquer grupo (aditivo) G abeliano finito e qualquer $A \subseteq \mathbb{Z}$ não vazio.

A. Lemos apresentou em sua tese de doutorado (ver [32], 2010) vários resultados para os invariantes $\eta_A(G)$, $g_A(G)$ e $s_A(G)$, quando G é um grupo abeliano finito específico e $A = \{1, -1\}$. Já em 2013, A. Lemos, H. Godinho e D. Marques apresentaram (ver [26]) estimativas para $s_A(\mathbb{Z}_3^r)$ e provaram que $s_A(\mathbb{Z}_3^3) = 9$, $s_A(\mathbb{Z}_3^4) = 21$ e $41 \leq s_A(\mathbb{Z}_3^5) \leq 45$, onde $A = \{1, -1\}$.

Outros resultados sobre estas constantes podem ser encontrados em [2], [4], [6], [21], [46] e [47].

Deste momento em diante voltamos nossos interesses ao caso em que G é um grupo (aditivo) abeliano finito com $\exp(G) = n$ e $A = \{a \in \mathbb{Z}\,;\, \text{mdc}(a, n) = 1\}$ é o conjunto dos pesos. Neste sentido F. Luca mostrou em [34] (ver também [27]) que $s_A(\mathbb{Z}_n) = n + \Omega(n)$ e analisou o problema inverso relacionado classificando as sequências extremas livres de subsequências de soma-zero A-ponderada de comprimento n, para $n = p^k$, onde k é um inteiro positivo e $\Omega(n)$ denota o número total de divisores primos de n (contados com suas respectivas multiplicidades). Este resultado foi conjecturado por Adhikari *et al* (ver [5]).

O caso em que $G = \mathbb{Z}_p^r$, onde p é um primo e r um inteiro positivo, Adhikari *et al.* (ver [1]) provaram que $s_A(G) = p + r$, sempre que $p > r$.

Quando $G = \mathbb{Z}_2^r$, podemos considerar $A = \{1\}$ e quando $G = \mathbb{Z}_3^r$, $G = \mathbb{Z}_4^r$, $G = \mathbb{Z}_6^r$, $G = \mathbb{Z}_2^t \oplus \mathbb{Z}_4^r$ ou $G = \mathbb{Z}_2^t \oplus \mathbb{Z}_6^r$, usamos $A = \{\pm 1\}$. Para estes casos, temos:

(i) $s_A(\mathbb{Z}_2^r) = 2^r + 1$ (ver [30]);

(ii) $s_A(\mathbb{Z}_3) = 4$ (ver [5]), $s_A(\mathbb{Z}_3^2) = 5$ (ver [3]), $s_A(\mathbb{Z}_3^3) = 9$ (ver [26, 35]), $s_A(\mathbb{Z}_3^4) = 21$, $s_A(\mathbb{Z}_3^5) = 41$ e $s_A(\mathbb{Z}_3^6) = 113$ (ver [35]);

(iii) $s_A(\mathbb{Z}_4) = 6$ e $s_A(\mathbb{Z}_6) = 8$ (ver [5]);

(iv) $s_A(\mathbb{Z}_4^2) = 8$ (ver [7]);

(v) $s_A(\mathbb{Z}_2 \oplus \mathbb{Z}_4) = 7$ (ver [36, 37]), $s_A(\mathbb{Z}_2^2 \oplus \mathbb{Z}_4) = 8$ (ver [37]) e $s_A(\mathbb{Z}_2 \oplus \mathbb{Z}_6) = 9$ (ver [36]);

Alguns autores têm investigado uma relação análoga à Conjectura de Gao para as constantes ponderadas: dado um grupo (aditivo) G abeliano finito, então a relação $s_A(G) = \eta_A(G) + \exp(G) - 1$ é válida para o conjunto $A \subset \mathbb{Z}$ formado pelos inteiros coprimos com $\exp(G)$. Apresentamos alguns destes resultados:

(i) $s_A(\mathbb{Z}_2^r) = \eta_A(\mathbb{Z}_2^r) + 2 - 1$ (ver [30]);

(ii) $s_A(\mathbb{Z}_3) = \eta_A(\mathbb{Z}_3) + 3 - 1$ (ver [5]), $s_A(\mathbb{Z}_3^2) = \eta_A(\mathbb{Z}_3^2) + 3 - 1$ (ver [3, 37]);

(iii) $s_A(\mathbb{Z}_4) = \eta_A(\mathbb{Z}_4) + 4 - 1$ e $s_A(\mathbb{Z}_6) = \eta_A(\mathbb{Z}_6) + 6 - 1$ (ver [5]);

(iv) $s_A(\mathbb{Z}_4^2) = \eta_A(\mathbb{Z}_4^2) + 4 - 1$ (ver [7, 37]);

(v) $s_A(\mathbb{Z}_2 \oplus \mathbb{Z}_4) = \eta_A(\mathbb{Z}_2 \oplus \mathbb{Z}_4) + 4 - 1$ (ver [36, 37]), $s_A(\mathbb{Z}_2^2 \oplus \mathbb{Z}_4) = \eta_A(\mathbb{Z}_2^2 \oplus \mathbb{Z}_4) + 4 - 1$ (ver [37]) e $s_A(\mathbb{Z}_2 \oplus \mathbb{Z}_6) = \eta_A(\mathbb{Z}_2 \oplus \mathbb{Z}_6) + 6 - 1$ (ver [36]);

(vi) $s_A(\mathbb{Z}_{p^r} \oplus \mathbb{Z}_{p^s}) = \eta_A(\mathbb{Z}_{p^r} \oplus \mathbb{Z}_{p^s}) + p^r - 1$, onde p é um primo ímpar, $r \geq s$ e $s \in \{1, 2\}$ (ver [13, 14]);

A. Lemos, H. Godinho e D. Marques (ver [26]) provaram que $s_A(\mathbb{Z}_3^r) = 2\eta_A(\mathbb{Z}_3^r) - 1 > \eta_A(\mathbb{Z}_3^r) + 3 - 1$ para $r \geq 3$, ou seja, a conjectura é falsa para $A = \{a \in \mathbb{Z}\,;\, \text{mdc}(a, 3) = 1\}$ e o posto de G é maior ou igual a 3.

Recentemente, M. N. Chintamani e P. Paul (ver [13, 14]) provaram que se $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^s}$, onde $s \in \{1, 2\}$, $\alpha \geq s$ é um inteiro e p é um número primo ímpar, então $s_A(G) = p^\alpha + \alpha + s$ e eles classificaram as sequências extremas que são livres de subsequências de soma-zero A-ponderada de comprimento $\exp(G)$. Além disso, eles mostraram que se

$G = \mathbb{Z}_n \oplus \mathbb{Z}_{p^s}$, onde $s \in \{1, 2\}$ e $n > 1$ é um número inteiro ímpar tal que $p^s | n$, então $s_A(G) \leq n + \Omega(n) + 2s$. Um de nossos objetivos será fazer análises semelhantes às feitas por Chintamani e Paul para o grupo $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde $\alpha \geq \beta$ são inteiros positivos.

Constantes sobre Polinômios Simétricos

Dentre as várias generalizações do Teorema de Erdös-Ginzburg-Ziv enunciaremos agora um estudo feito por A. Bialostocki e T. D. Luong, no qual foi definida uma constante análoga à Constante EGZ com o auxílio de polinômios simétricos.

Sejam p um número primo e $S = (u_1, u_2, \ldots, u_p)$ uma sequência de elementos do corpo $\mathbb{Z}_p$ (com soma e multiplicação usuais). Dado um polinômio simétrico $\varphi \in \mathbb{Z}_p[x_1, x_2, \ldots, x_p]$, dizemos que S é uma *sequência φ-zero* se $\varphi(S) = \varphi(u_1, u_2, \ldots, u_p) = 0$ em $\mathbb{Z}_p$. Estendendo o conceito da Constante EGZ, Bialostocki e Luong definiram em [10] (2009) a nova constante $g(\varphi, \mathbb{Z}_p)$ como sendo o menor inteiro ℓ tal que cada sequência em $\mathbb{Z}_p$ de comprimento ℓ contém uma subsequência φ-zero e $g(\varphi, \mathbb{Z}_p) = \infty$, caso não exista tal ℓ. Definiram, também, o conjunto $M(\varphi, \mathbb{Z}_p)$ de todas as sequências de comprimento $g(\varphi, \mathbb{Z}_p) - 1$ livres de subsequências φ-zero, quando $g(\varphi, \mathbb{Z}_p)$ é finito.

Por simplicidade de notação usaremos que

$$[u_1]^{n_1}[u_2]^{n_2} \cdots [u_t]^{n_t} = (\underbrace{u_1, u_1, \ldots, u_1}_{n_1 \text{ vezes}}, \underbrace{u_2, u_2, \ldots, u_2}_{n_2 \text{ vezes}}, \ldots, \underbrace{u_t, u_t, \ldots, u_t}_{n_t \text{ vezes}}).$$

Além disso, dados os inteiros positivos n e k, considere em $\mathbb{Z}_p[x_1, x_2, \ldots, x_n]$ o polinômio simétrico $s_{n,k} = s_{n,k}(x_1, x_2, \ldots, x_n) = x_1^k + x_2^k + \cdots + x_n^k$.

Observe que o caso em que φ for um polinômio simétrico linear, ou seja, $\varphi = as_{n,1} \in \mathbb{Z}_p[x_1, x_2, \ldots, x_n]$, com $a \neq 0$, então o Teorema 0.1 garante que $g(\varphi, \mathbb{Z}_p) = 2p - 1$ e $M(\varphi, \mathbb{Z}_p)$ é o conjunto de todas as sequências de $\mathbb{Z}_p$ da forma $[u]^{p-1}[v]^{p-1}$, onde $u, v \in \mathbb{Z}_p$ e $u \neq v$.

No mesmo artigo [10], Bialostocki e Luong estudaram o caso em que o polinômio simétrico é quadrático e analisaram os valores de $g(\varphi, \mathbb{Z}_p)$ e $M(\varphi, \mathbb{Z}_p)$.

Usando o mesmo raciocínio definiremos uma nova constante que será uma generalização da Constante de Davenport para polinômios simétricos sobre $\mathbb{Z}_p$ que será denotada

por $D(\varphi, \mathbb{Z}_p)$. Além disso, analisaremos o problema inverso associado a esta constante denotando por $M(\mathcal{F}_\varphi, \mathbb{Z}_p)$ o conjunto de todas as sequências extremas.

Estrutura da Tese

Nesta tese apresentaremos alguns resultados relacionados à Constante EGZ Ponderada e à Constante de Davenport para Polinômios Simétricos.

No primeiro capítulo usaremos como base os resultados obtidos por F. Luca, M. N. Chintamani e P. Paul para provar os seguintes resultados:

Teorema 0.3 (Teorema 1.14)**.** *Sejam p um primo ímpar e $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ o grupo (aditivo) onde $\alpha \geq \beta$ são inteiros positivos. Então podemos afirmar que*

$$s_A(G) = p^\alpha + \alpha + \beta,$$

onde $A = \{a \in \mathbb{Z}\,;\, mdc(a, \exp(G)) = 1\}$.

Teorema 0.4 (Teorema 1.16)**.** *Sejam p um primo ímpar e S uma sequência sobre o grupo $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde $\alpha \geq \beta$ são inteiros positivos, com $|S| = p^\alpha + \alpha + \beta - 1$. Se S não possui subsequências de soma-zero A-ponderada de comprimento p^α, então S contém exatamente $p^\alpha - 1$ termos iguais a $(0, 0)$. Além disso, se $\delta_j(S)$ denota o número de termos (com multiplicidade) de S com ordem p^j, então $\delta_j(S) \geq 1$, para todo $j \in [1, \alpha]$, e $\sum_{j=1}^{\alpha} \delta_j(S) = \alpha + \beta$.*

Corolário 0.5 (Corolário 1.17)**.** *Sejam p um primo ímpar e S uma sequência sobre o grupo $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde $\alpha \geq \beta$ são inteiros positivos. Então:*

(i) $\eta_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}) = \alpha + \beta + 1$*;*

(ii) se $|S| = \alpha + \beta$ e S não possui subsequências de soma-zero A-ponderada de comprimento no máximo p^α, então $\delta_j(S) \geq 1$, para todo $j \in [1, \alpha]$;

(iii) a equação $s_A(G) = \eta_A(G) + \exp(G) - 1$ é válida para o grupo $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$.

Teorema 0.6 (Teorema 1.21)**.** *Sejam p um primo ímpar, β um inteiro positivo e $n \geq 1$ um inteiro ímpar tal que $n = p^{\beta}m$, para algum inteiro m. Então*

$$s_A(\mathbb{Z}_n \oplus \mathbb{Z}_{p^{\beta}}) \leq n + \Omega(n) + (2m-1)\beta,$$

para o caso em que $A = \{a \in \mathbb{Z}\,;\, mdc(a,n) = 1\}$.

No segundo capítulo formalizamos uma generalização para a *Constante de Davenport para Polinômios Simétricos* e provamos o seguinte resultado para polinômios simétricos quadráticos:

Teorema 0.7 (Teorema 2.9)**.** *Sejam p um primo, onde $p \geq 3$, $n \geq 2$ um inteiro positivo e seja $\varphi = as_{n,1}^2 + bs_{n,2} + cs_{n,1} \in \mathbb{Z}_p[x_1, x_2, \ldots, x_n]$, com $a \neq 0$ ou $b \neq 0$. Então são verdadeiras as seguintes afirmações:*

(i) Se $a = 0$ e $b \neq 0$, então $D(\varphi, \mathbb{Z}_p) = p$ e $M(\mathcal{F}_{\varphi}, \mathbb{Z}_p)$ é o conjunto de todas as sequências da forma $[u]^{\alpha}[-u-cb^{-1}]^{p-1-\alpha}$, onde $u \in \mathbb{Z}_p \setminus \{0, -cb^{-1}\}$ e $0 \leq \alpha \leq p-1$, ou da forma $[u]^{p-1}$, quando $u = -cb^{-1}$ e $c \neq 0$.

(ii) Se $a \neq 0$ e $b = c = 0$ então $D(\varphi, \mathbb{Z}_p) = p$ e $M(\mathcal{F}_{\varphi}, \mathbb{Z}_p)$ é o conjunto de todas as sequências da forma $[u]^{p-1}$, onde $u \in \mathbb{Z}_p \setminus \{0\}$.

(iii) Se $a \neq 0$, $b = 0$ e $c \neq 0$ então $D(\varphi, \mathbb{Z}_p) = p - 1$ e $M(\mathcal{F}_{\varphi}, \mathbb{Z}_p) = \{[ca^{-1}]^{p-2}\}$.

(iv) Se $a \cdot b \neq 0$, então $D(\varphi, \mathbb{Z}_p) \leq 2p - 1$ e:

(a) $D(\varphi, \mathbb{Z}_p) \geq p - 2$, para $c \neq 0$.

(b) $D(\varphi, \mathbb{Z}_p) \geq \overline{-ba^{-1}}$, para $c = 0$,

onde $\overline{x}$ representa o menor inteiro não negativo pertencente à classe $x \in \mathbb{Z}_p$.

Capítulo 1

Constante EGZ para p-Grupos de Posto 2

1.1 Notações, Terminologias e Preliminares

Começaremos por introduzir algumas notações, terminologias e algumas ferramentas importantes para obtermos nossos resultados. Seja $\mathbb{N}_0$ o *conjunto de inteiros não-negativos*. Para inteiros $a, b \in \mathbb{N}_0$, definimos $[a, b] = \{x \in \mathbb{N}_0 \,;\, a \leq x \leq b\}$. Dado um número inteiro positivo n, por abuso de notação, identificaremos por todo o capítulo o grupo aditivo $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ das classes residuais módulo n com o conjunto de números inteiros $\{0, 1, \ldots, n-1\}$. Além disso, fixado um grupo G com $\exp(G) = n$ usaremos por todo o capítulo que $A = \{a \in \mathbb{Z} \,;\, \text{mdc}(a, n) = 1\}$.

Como vimos anteriormente, dados um grupo (aditivo) G abeliano finito e uma sequência $S = x_1 x_2 \cdots x_t$ de elementos de G de comprimento t, então definimos uma subsequência $T = x_{i_1} x_{i_2} \ldots x_{i_k}$ de S, se o conjunto de índices de T é tal que $I_T = \{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, t\}$ e escrevemos $T|S$. Agora, diremos que duas subsequências T_1 e T_2 de S são iguais se $I_{T_1} = I_{T_2}$. Dadas as subsequências $T_1, T_2, \ldots, T_r$ de S, definimos $\text{mdc}(T_1, \ldots, T_r)$ como a subsequência indexada por $I = I_{T_1} \cap I_{T_2} \cap \cdots \cap I_{T_r}$, quando I é não vazio. Além disso, diremos que duas subsequências T_1 e T_2 de S são *disjuntas* se $I_{T_1} \cap I_{T_2} = \emptyset$, ou seja, $\text{mdc}(T_1, T_2) = \lambda$, onde λ denota a *sequência vazia*. Se T_1 e T_2 são disjuntas, então denotaremos por $T_1 T_2$ a subsequência com conjunto de índices dado por $I_{T_1} \cup I_{T_2}$. Se

$T_1|T_2$, então denotaremos por $T_2T_1^{-1}$ a subsequência de S com conjunto de índices dado por $I_{T_2} \setminus I_{T_1}$.

Consideremos $S = x_1x_2\cdots x_m$ uma sequência de elementos de um grupo G e vamos definir:

1. $|S| = m$ *o comprimento* S.
2. uma *soma A-ponderada* é uma soma da forma $\sigma^{\mathbf{a}}(S) = \sum_{i=1}^{m} a_ix_i$, para alguma sequência $\mathbf{a} = a_1a_2\cdots a_m$, onde $a_i \in A$ para cada $i \in [1,m]$.
3. $\sum_A(S) = \left\{\sum_{i\in I} a_ix_i : \emptyset \neq I \subseteq [1,m] \text{ e } a_i \in A\right\}$, um *conjunto não vazio de subsomas A-ponderadas de* S.

A sequência $S = x_1x_2\cdots x_m$ é chamada:

1. uma *sequência livre de somas-zero A-ponderadas* se $0 \notin \sum_A(S)$,
2. uma *sequência de soma-zero A-ponderada* se $\sigma^{\mathbf{a}}(S) = 0$ para alguma sequência $\mathbf{a} = a_1a_2\cdots a_m$, com $a_i \in A$ para $i \in [1,m]$.

O seguinte lema é um caso particular de um resultado provado por F. Luca (ver [34]) que será uma ferramenta chave para obter nossos resultados.

Lema 1.1. *Sejam $n \geq 2$ um inteiro ímpar, $m \geq 1$ um inteiro e $S = x_1x_2\cdots x_m$ uma sequência sobre $\mathbb{Z}_n$ de comprimento m. Para cada primo p dividindo n, escreveremos $S_p = \{i \in [1,m]\,;\, x_i \not\equiv 0 \pmod p\}$. Suponha que $|S_p| \geq 2$ para todo o primo p divisor de n. Então, para qualquer inteiro b dado, existe $\mathbf{a} = a_1a_2\cdots a_m$, com $a_i \in A = \{a \in \mathbb{Z}\,;\, mdc(a,n) = 1\}$ tal que*

$$\sigma^{\mathbf{a}}(S) \equiv b \pmod n.$$

A seguinte observação será frequentemente usada por todo o capítulo.

Observação 1.2. *Se $S = x_1x_2\cdots x_\ell$ é uma sequência de soma-zero A-ponderada de elementos de um grupo G, então a sequência $S' = (u_1x_1)(u_2x_2)\cdots(u_\ell x_\ell)$ continua sendo uma sequência de soma-zero A-ponderada, para qualquer escolha de $u_i \in A$, com $i \in [1,\ell]$. Além disso, se f é um automorfismo de G, então $f(S) = f(x_1)f(x_2)\cdots f(x_\ell)$ é também uma sequência de soma-zero A-ponderada.*

Sendo p um primo e $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ o grupo aditivo onde $\alpha \geq \beta$ são inteiros positivos, então $\exp(G) = p^\alpha$ e o conjunto A usado para calcular $s_A(G)$ será dado por

$$A = \{n \in \mathbb{Z}\,;\, \text{mdc}(n, p^\alpha) = 1\} = \{n \in \mathbb{Z}\,;\, \text{mdc}(n, p) = 1\}.$$

Agora, apresentaremos dois resultados obtidos por M. N. Chintamani e P. Paul em [14].

Teorema 1.3. *Seja p um primo ímpar e $\alpha \geq 2$ um inteiro. Então, temos*

$$s_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^2}) = p^\alpha + \alpha + 2.$$

Teorema 1.4. *Seja p um primo ímpar e $\alpha \geq 2$ um inteiro. Seja S uma sequência sobre o grupo $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^2}$ com $|S| = p^\alpha + \alpha + 1$. Suponha que S seja livre de subsequências de soma-zero A-ponderada de comprimento p^α. Então S contém exatamente $p^\alpha - 1$ zeros. Além disso, se $\delta_j(S)$ denota o número de termos (com multiplicidade) de S com ordem p^j, então $\delta_j(S) \geq 1$ para todo $j = 1, 2, \ldots, \alpha$ e $\sum_{j=1}^{\alpha} \delta_j(S) = \alpha + 2$.*

Nosso principal objetivo neste capítulo será generalizar os teoremas acima para o grupo aditivo $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde $\alpha \geq \beta$ são inteiros positivos arbitrários. Além disso, apresentaremos uma cota inferior e uma cota superior para $s_A(\mathbb{Z}_n \oplus \mathbb{Z}_{p^\beta})$, onde p é um primo ímpar, β é um inteiro positivo e n é inteiro positivo ímpar tal que $p^\beta | n$.

1.2 Resultados Iniciais

Inicialmente apresentaremos algumas ferramentas essenciais para os resultados deste capítulo.

Lema 1.5. *Sejam p um primo e o grupo (aditivo) $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde $\alpha \geq \beta$ são inteiros positivos. Dado um elemento $(a, b) \in G$ tal que $mdc(a, p) = 1$, então existe um automorfismo $\Theta \in Aut(G)$ tal que $\Theta(a, b) = (1, 0)$ e $\Theta(0, 1) = (0, 1)$.*

Demonstração. Começamos definindo $\overline{u}$ como sendo a classe em $\mathbb{Z}_{p^\beta}$ do menor inteiro positivo pertencente à classe u em $\mathbb{Z}_{p^\alpha}$. Note que, dados $u, v \in \mathbb{Z}_{p^\alpha}$, sempre teremos

$\overline{u+v} = \overline{u} + \overline{v}$. Além disso, $\overline{0_{\mathbb{Z}_{p^\alpha}}} = 0_{\mathbb{Z}_{p^\beta}}$ e $\overline{1_{\mathbb{Z}_{p^\alpha}}} = 1_{\mathbb{Z}_{p^\beta}}$. Como $\text{mdc}(a,p) = 1$, então existe $a^{-1} \in \mathbb{Z}_{p^\alpha}$ tal que $a \cdot a^{-1} = 1$ em $\mathbb{Z}_{p^\alpha}$.

Iremos mostrar que $\Theta : G \longrightarrow G$, tal que $\Theta(x,y) = (a^{-1}x, y - \overline{a^{-1}x}b)$, é um automorfismo de G da forma desejada. Dados $(x_1,y_1),(x_2,y_2) \in G$, temos

$$\begin{aligned}
\Theta[(x_1,y_1)+(x_2,y_2)] &= \Theta(x_1+x_2, y_1+y_2) \\
&= (a^{-1}(x_1+x_2), (y_1+y_2) - \overline{a^{-1}(x_1+x_2)}b) \\
&= (a^{-1}x_1, y_1 - \overline{a^{-1}x_1}b) + (a^{-1}x_2, y_2 - \overline{a^{-1}x_2}b) \\
&= \Theta(x_1,y_1) + \Theta(x_2,y_2).
\end{aligned}$$

Logo Θ é um homomorfismo. Além disso, é fácil verificar que $\Theta(x_1,y_1) = (0,0)$ se, e somente se, $(x_1,y_1) = (0,0)$, ou seja, Θ é um monomorfismo. Como G é um grupo finito, fica claro que Θ é também um epimorfismo e, portanto, um automorfismo. Por fim, $\Theta(a,b) = (1,0)$ e $\Theta(0,1) = (0,1)$ como queríamos. □

Lema 1.6. *Sejam p um primo e m um inteiro positivo. Dados os inteiros a_1, a_2, ... , a_m tais que $mdc(a_i,p) = 1$, para algum $i \in [1,m]$, então a equação*

$$a_1x_1 + a_2x_2 + \cdots + a_mx_m \equiv 0 \pmod{p} \tag{1.1}$$

possui no máximo $(p-1)^{m-1}$ soluções com $x_j \in [1,p-1]$, para todo $j \in [1,m]$.

Demonstração. Sem perda de generalidade, suponhamos que $\text{mdc}(a_1,p) = 1$. Sabemos que existem $(p-1)^{m-1}$ escolhas para a sequência $x_2x_3\cdots x_m$ onde $x_j \in [1,p-1]$, para todo $j \in [2,m]$. Fixemos uma destas escolhas como sendo $x_2^{(0)}x_3^{(0)}\cdots x_m^{(0)}$.

Tome $a_2x_2^{(0)} + \cdots + a_mx_m^{(0)} = -b$. Desta forma, resolver a equação (1.1) é equivalente a resolver a equação

$$a_1x_1 \equiv b \pmod{p}. \tag{1.2}$$

Como $\text{mdc}(a_1,p) = 1$, então é fácil ver que existe no máximo uma solução para a equação (1.2) com $x_1 \in [1,p-1]$ para cada escolha da sequência que fizermos. Portanto o resultado segue. □

Observação 1.7. *Na demonstração do lema anterior, se $b \equiv 0 \pmod{p}$ para uma determinada escolha da sequência $x_2x_3\cdots x_m$, então a equação (1.2) não possui solução*

da forma desejada para esta escolha. Portanto, se existem d escolhas para a sequência $x_2x_3\cdots x_m$ *tais que* $a_2x_2 + a_3x_3 + \cdots + a_mx_m \equiv 0 \pmod{p}$*, então o número de soluções para a equação* (1.1) *da forma requerida será no máximo* $(p-1)^{m-1} - d$*.*

Lema 1.8. *Sejam p um primo ímpar e* $m \geq 2$ *um inteiro. Dados os inteiros* a_1*,* a_2*,* ... *,* a_{m+1}*, existe um conjunto de índices* $I \subset [1, m+1]$*, de comprimento* $|I| = m$*, tal que* $\sum_{i\in I} u_ia_i \equiv 0 \pmod{p}$ *para alguma escolha de inteiros* $u_i \in [1, p-1]$*, para cada* $i \in I$*.*

Demonstração. Se existem dois índices $i, j \in [1, m+1]$ tais que $\text{mdc}(a_ia_j, p) = 1$ então é suficiente escolher qualquer conjunto de índices $I \subset [1, m+1]$, de comprimento $|I| = m$, contendo os índices i e j, onde o resultado é uma consequência direta do Lema 1.1.

Por outro lado, podemos assumir, sem perda de generalidade, que $a_i \equiv 0 \pmod{p}$ para todo $i \in [1, m]$. Assim fica claro que podemos escolher $I = [1, m]$ e o resultado segue. □

O próximo lema é um de nossos principais resultados deste capítulo.

Lema 1.9. *Sejam p um primo ímpar,* $m \geq 5$ *um inteiro e*

$$S = (1, 0)(a_2, b_2)(a_3, b_3)(a_4, b_4)\cdots(a_{m+1}, b_{m+1})$$

uma sequência de termos do grupo $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$*, onde* $\alpha \geq \beta$ *são inteiros positivos. Se* $mdc(b_2, p) = 1$*,* $p|a_2$ *e existem dois índices* $i, j \in [3, m+1]$ *(incluindo o caso* $i = j$*) tais que* $mdc(a_ib_j, p) = 1$*, então S possui uma subsequência de soma-zero A-ponderada de comprimento m.*

Demonstração. Vamos supor inicialmente que exista um termo (a_i, b_i), com $i \in [3, m+1]$ tal que $\text{mdc}(a_ib_i, p) = 1$. Sem perda de generalidade, vamos supor que $i = 3$. Pelo Lema 1.8, fazendo as mudanças necessárias nos índices, podemos supor que existe uma escolha de inteiros $u_4, u_5, \ldots, u_m \in [1, p-1]$ tais que $\sum_{i=4}^{m} u_ia_i \equiv 0 \pmod{p}$. Assim, podemos excluir o termo (a_{m+1}, b_{m+1}). Observe as seguintes equações:

$$a_3x_3 + a_4x_4 + \cdots + a_mx_m \equiv 0 \pmod{p} \tag{1.3}$$

$$b_3x_3 + b_4x_4 + \cdots + b_mx_m \equiv 0 \pmod{p} \tag{1.4}$$

Pelo Lema 1.6 e pela Observação 1.7, existem no máximo $(p-1)^{m-3}-1$ soluções para equação (1.3) e no máximo $(p-1)^{m-3}$ para a equação (1.4) tais que $x_k \in [1, p-1]$, para todo $k \in [3, m]$. Sabemos que existem $(p-1)^{m-2}$ escolhas para a sequência $x_3x_4\cdots x_m$ tais que $x_k \in [1, p-1]$, para todo $k \in [3, m]$. Como p é um primo ímpar, então $(p-1)^{m-2} = (p-1)(p-1)^{m-3} > 2(p-1)^{m-3} - 1$. Portanto, existe ao menos uma destas escolhas para a sequência que não é solução da equação (1.3) e também não é solução da equação (1.4). Tome uma destas escolhas como sendo $v_3v_4\cdots v_m$. Além disso, tome $a_3v_3 + a_4v_4 + \cdots + a_mv_m = a$ e $b_3v_3 + b_4v_4 + \cdots + b_mv_m = b$. Note que $\mathrm{mdc}(ab, p) = 1$. Desta forma, é fácil ver que

$$(-b_2a + ba_2)(1,0) + (-b)(a_2, b_2) + \sum_{i=3}^{m} b_2v_i(a_i, b_i) = (0,0)$$

onde $(-b_2a + ba_2)$,$(-b)$,$(b_2v_i) \in A$, pois $\mathrm{mdc}(abb_2v_i, p) = 1$ e $p|a_2$, como queríamos.

Por outro lado, vamos supor, sem perda de generalidade, que $\mathrm{mdc}(a_3b_4, p) = 1$, $p|a_4$ e $p|b_3$. Se observarmos o Lema 1.8, como $p|a_4$, podemos supor que que existe uma escolha de inteiros $u_4, u_5, \ldots, u_m \in [1, p-1]$ tais que $\sum_{i=4}^{m} u_ia_i \equiv 0 \pmod p$ (podemos fazer isso, pois se existe um único $i \in [5, m+1]$ tal que $\mathrm{mdc}(a_i, p) = 1$, então rearranjamos a sequência de forma que este termo apareça na posição $m+1$). Assim podemos excluir o termo (a_{m+1}, b_{m+1}) e seguir exatamente os mesmos passos do caso anterior. □

O próximo lema foi demonstrado por Chintamani e Paul em [13].

Lema 1.10. *Sejam $\ell \geq 2$ um inteiro e o grupo $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_p$, onde p é um primo ímpar e α é um inteiro positivo. Seja S uma sequência de termos em G de comprimento $\ell + 1$. Se S contém um termo de ordem p^α que se repete ao menos duas vezes, então S possui uma subsequência de soma-zero A-ponderada de comprimento ℓ.*

O lema acima não é verdadeiro para o caso onde $\ell = 3$. De fato, podemos observar que a sequência $(1,0)(1,0)(0,1)(0,1)$ sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_p$ satisfaz as hipóteses do Lema 1.10 e não possui subsequências de soma-zero A-ponderada de comprimento 3. Generalizando o Lema 1.10 para o caso geral e confirmando sua validade para $\ell \geq 4$, obtemos:

Lema 1.11. *Seja $\ell \geq 4$ um inteiro e o grupo $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde p é um primo ímpar e $\alpha \geq \beta$ são inteiros positivos. Seja $S = x_1x_2\cdots x_{\ell+\beta}$ uma sequência onde $x_i = (a_i, b_i) \in$*

$\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, para cada $i \in [1, \ell + \beta]$. Se S contém dois termos iguais cuja ordem da primeira coordenada é p^α, então S possui uma subsequência de soma-zero A-ponderada de comprimento ℓ que contém os dois termos em questão.

Demonstração. Para o caso em que $\beta = 1$ podemos assumir, sem perda de generalidade, que $x_1 = x_2$ em G com a_1 e a_2 de ordem p^α e, pela Observação 1.2 e pelo Lema 1.5, que $x_1 = x_2 = (1, 0)$. Suponha que $b_i \not\equiv 0 \pmod{p}$ para dois índices distintos $i_1, i_2 \in [3, \ell+1]$. Então existe um conjunto $I_1 \subset [3, \ell + 1]$, com $|I_1| = \ell - 2$ e $i_1,\ i_2 \in I_1$ (note que, para $\ell \geq 4$, isto é possível). Pelo Lema 1.1 com $n = p$, $a = 0$ e $m = \ell - 2$, obtemos

$$\sum_{i \in I_1} u_i b_i \equiv 0 \pmod{p},$$

onde $u_i \in A$, para todo $i \in I_1$. Novamente pelo Lema 1.1 com $n = p^\alpha$, $a = -\sum_{i \in I_1} u_i a_i$ e $m = 2$, obtemos $u_1,\ u_2 \in A$ tais que

$$u_1 a_1 + u_2 a_2 + \sum_{i \in I_1} u_i a_i \equiv 0 \pmod{p^\alpha}.$$

Portanto, temos

$$u_1 x_1 + u_2 x_2 + \sum_{i \in I_1} u_i x_i = (0, 0),$$

em G com $u_i \in A$. Assim obtemos uma subsequência de soma-zero A-ponderada de S de comprimento ℓ contendo x_1 e x_2. Por outro lado, vamos supor, sem perda de generalidade, que $b_i \equiv 0 \pmod{p}$ para cada índice $i \in [3, \ell]$. Assim, consideremos a sequência

$$S' = (1, 0)(1, 0)(a_3, 0)(a_4, 0) \cdots (a_\ell, 0) \text{ sobre } \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_p$$

de comprimento ℓ. Pelo Lema 1.1, vemos que S' é uma subsequência de soma-zero A-ponderada de S de comprimento ℓ contendo x_1 e x_2.

Vamos proceder por indução sobre β. Neste sentido, vamos considerar $\beta \geq 2$ e que o resultado é válido para todos os inteiros maiores ou iguais a 1 e menores que β.

Sem perda de generalidade, podemos assumir novamente que $x_1 = x_2$ em $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ com a_1 e a_2 sendo de ordem p^α em $\mathbb{Z}_{p^\alpha}$. Além disso, pela Observação 1.2 e pelo Lema 1.5, podemos considerar $x_1 = x_2 = (1, 0)$.

Suponha que $b_i \not\equiv 0 \pmod{p}$ para dois índices distintos $i_1, i_2 \in [3, \ell+\beta]$. Então existe um conjunto $I_2 \subset [3, \ell+\beta]$, com $|I_2| = \ell - 2$ e $i_1,\ i_2 \in I_2$ (note que $\ell \geq 4$ e $\beta \geq 2$). Pelo Lema 1.1 com $n = p^\beta$, $b = 0$ e $m = \ell - 2$, obtemos

$$\sum_{i \in I_2} u_i b_i \equiv 0 \pmod{p^\beta},$$

onde $u_i \in A$, para todo $i \in I_2$. Novamente aplicando o Lema 1.1 com $n = p^\alpha$, $b = -\sum_{i\in I_2} u_i a_i$ e $m = 2$ obtemos $u_1,\ u_2 \in A$ tais que

$$u_1 a_1 + u_2 a_2 + \sum_{i \in I_2} u_i a_i \equiv 0 \pmod{p^\alpha}.$$

Portanto

$$u_1 x_1 + u_2 x_2 + \sum_{i \in I_2} u_i x_i = (0,0),$$

em $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ com $u_i \in A$. Assim construimos uma subsequência de soma-zero A-ponderada de S de comprimento ℓ contendo x_1 e x_2.

Agora podemos supor, sem perda de generalidade, que $b_i \equiv 0 \pmod{p}$ para cada índice $i \in [3, \ell+\beta-1]$. Assim, $b_i = c_i p$, para todo $i \in [3, \ell+\beta-1]$, onde podemos tomar c_i como um elemento de $\mathbb{Z}_{p^{\beta-1}}$. Consideremos a sequência

$$S' = (1,0)(1,0)(a_3,c_3)(a_4,c_4)\cdots(a_{\ell+\beta-1}, c_{\ell+\beta-1}) \text{ sobre } \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}}$$

de comprimento $\ell + \beta - 1$. Pela hipótese de indução, S' contém uma subsequência de soma-zero A-ponderada T' de comprimento ℓ contendo os dois primeiros termos. Assim, vemos que existe um conjunto de índices $I_3 \subset [3, \ell+\beta-1]$ tal que $|I_3| = \ell - 2$,

$$T' = (1,0)(1,0)\prod_{i\in I_3}(a_i, c_i) \quad \text{e} \quad u_1(1,0) + u_2(1,0) + \sum_{i\in I_3} u_i(a_i,c_i) = (0,0),$$

sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}}$, para alguma escolha de inteiros u_i, onde $u_i \in A$ para todo $i \in I_3 \cup \{1,2\}$. Assim, temos

$$\sum_{i\in I_3} u_i c_i \equiv 0 \pmod{p^{\beta-1}} \quad \Rightarrow \quad \sum_{i\in I_3} u_i b_i = \sum_{i\in I_3} u_i (c_i p) \equiv 0 \pmod{p^\beta}.$$

Tomando a subsequência $T = (1,0)(1,0)\prod_{i\in I_3}(a_i, b_i)$ de S, temos $|T| = \ell$ e

$$u_1(1,0) + u_2(1,0) + \sum_{i\in I_3} u_i(a_i, b_i) = (0,0)$$

sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ como queríamos. □

Apresentamos um resultado que nos auxiliará na estimativa do valor de $s_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta})$ e ele é uma consequência imediata do Lema 1.11.

Lema 1.12. *Sejam $\ell \geq 4$ um inteiro e $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ um grupo aditivo, onde p é um primo ímpar e $\alpha \geq \beta$ são inteiros positivos. Seja $S = x_1 x_2 \cdots x_{\ell+\beta}$ uma sequência sobre G de comprimento $|S| = \ell + \beta$, onde $x_i = (a_i, b_i) \in \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, para cada $i \in [1, \ell + \beta]$. Suponha que a_i tem ordem p^α para algum índice $i \in [1, \ell + \beta]$ e existem $k \geq 1$ índices i_1, i_2, ... , $i_k \in \{1, 2, \ldots, \ell + \beta\} \setminus \{i\}$ tais que $k \leq \ell - 3$ e*

$$u_{i_1} x_{i_1} + u_{i_2} x_{i_2} + \cdots + u_{i_k} x_{i_k} = u x_i, \tag{1.5}$$

para alguma escolha de $u, u_{i_1}, u_{i_2}, \ldots, u_{i_k} \in A$. Então S possui uma subsequência de soma-zero A-ponderada de comprimento ℓ.

Demonstração. Consideremos a sequência S' dada por

$$S' = (u x_i) \cdot (u_{i_1} x_{i_1} + u_{i_2} x_{i_2} + \cdots + u_{i_k} x_{i_k}) \cdot S \cdot (x_i x_{i_1} x_{i_2} \cdots x_{i_k})^{-1}$$

de comprimento $(\ell - k + 1) + \beta$. Note que os primeiros dois termos que aparecem na descrição de S' são iguais e suas primeiras coordenadas possuem ordem igual a p^α. Como $k \leq \ell - 3$, então $\ell - k + 1 \geq 4$ e, pelo Lema 1.11, existe uma subsequência T' de soma-zero A-ponderada de S' de comprimento $\ell - k + 1$ que contém os dois primeiros termos de S', ou seja, existe um conjunto de índices $J \subset [1, \ell + \beta] \setminus \{i, i_1, i_2, \ldots, i_k\}$, tal que $|J| = \ell - k - 1$,

$$T' = (u x_i) \cdot (u_{i_1} x_{i_1} + u_{i_2} x_{i_2} + \cdots + u_{i_k} x_{i_k}) \cdot \prod_{j \in J} x_j$$

e T' é uma sequência de soma-zero A-ponderada de comprimento $\ell - k + 1$. Assim, a sequência

$$T = x_i \cdot \left(\prod_{t=1}^{k} x_{i_t} \right) \cdot \left(\prod_{j \in J} x_j \right)$$

é uma subsequência de soma-zero A-ponderada de S de comprimento ℓ, como queríamos.

□

Observação 1.13. *No lema anterior, a subsequência de soma-zero A-ponderada de S obtida contém todos os termos que aparecem na equação* (1.5).

1.3 O Valor Exato de $s_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta})$

O próximo teorema é o principal resultado deste capítulo.

Teorema 1.14. *Sejam p um primo ímpar e $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ o grupo (aditivo) onde $\alpha \geq \beta$ são inteiros positivos. Então podemos afirmar que*

$$s_A(G) = p^\alpha + \alpha + \beta,$$

onde $A = \{a \in \mathbb{Z}\,;\, mdc(a, \exp(G)) = 1\}$.

Demonstração. Seja $S = x_1 x_2 \cdots x_{p^\alpha+\alpha+\beta}$ uma sequência sobre G de comprimento $|S| = p^\alpha + \alpha + \beta$, onde $x_i = (a_i, b_i) \in G$, para todo $i \in [1, p^\alpha + \alpha + \beta]$. Inicialmente iremos mostrar que S possui uma subsequência de soma-zero A-ponderada de comprimento p^α.

O Teorema 1.3 nos garante que este resultado é válido para o caso em que $\beta = 2$ e $\alpha \geq 2$. Vamos proceder por indução sobre β. Portanto definimos a

Hipótese de Indução I: assumimos que $\beta \geq 3$ e que $s_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}}) \leq p^\alpha + \alpha + (\beta - 1)$, para qualquer escolha de $\alpha \geq \beta - 1$.

Para mostrar que o resultado é válido para β, usaremos o processo de indução novamente, mas agora sobre o inteiro positivo α. Como $\alpha \geq \beta$, nosso ponto de partida será:

O caso $\alpha = \beta$.

Neste caso, temos que $S = x_1 x_2 \cdots x_{p^\beta+2\beta}$ é uma sequência sobre $G = \mathbb{Z}_{p^\beta} \oplus \mathbb{Z}_{p^\beta}$.

Se $\mathrm{mdc}(b_i, p) = 1$ para no máximo um índice do conjunto $[1, p^\beta + 2\beta]$, então podemos encontrar a subsequência desejada de S. De fato, vamos considerar, sem perda de generalidade, que $p|b_i$ para todo $i \in [1, p^\beta + 2\beta - 1]$, ou seja, $b_i = b_i' p$ onde podemos assumir que $b_i' \in \mathbb{Z}_{p^{\beta-1}}$. Assim, a sequência

$$S' = (a_1, b_1')(a_2, b_2')(a_3, b_3') \cdots (a_{p^\beta+2\beta-1}, b_{p^\beta+2\beta-1}')$$

sobre $\mathbb{Z}_{p^\beta} \oplus \mathbb{Z}_{p^{\beta-1}}$ possui comprimento $p^\beta + \beta + (\beta - 1)$. Pela Hipótese de Indução I temos $s_A(\mathbb{Z}_{p^\beta} \oplus \mathbb{Z}_{p^{\beta-1}}) \leq p^\beta + \beta + (\beta - 1)$. Assim, S' contém uma subsequência de

soma-zero A-ponderada T' de comprimento p^β, ou seja, existe um conjunto de índices $I \subset [1, p^\beta + 2\beta - 1]$ tal que $|I| = p^\beta$,

$$T' = \prod_{i \in I}(a_i, b_i') \quad \text{e} \quad \sum_{i \in I} u_i(a_i, b_i') = (0,0) \quad \text{sobre } \mathbb{Z}_{p^\beta} \oplus \mathbb{Z}_{p^{\beta-1}},$$

para alguma escolha de inteiros u_i, onde $u_i \in A$ para todo $i \in I$. Assim, temos

$$\sum_{i \in I} u_i b_i' \equiv 0 \pmod{p^{\beta-1}} \quad \Rightarrow \quad \sum_{i \in I} u_i b_i = \sum_{i \in I} u_i (b_i' p) \equiv 0 \pmod{p^\beta}.$$

Tomando a subsequência $T = \prod_{i \in I}(a_i, b_i)$ de S, temos $|T| = p^\beta$ e $\sum_{i \in I} u_i(a_i, b_i) = (0,0)$ sobre $\mathbb{Z}_{p^\beta} \oplus \mathbb{Z}_{p^\beta}$ como queríamos.

De modo análogo (invertendo as coordenadas) podemos mostrar que, se $\text{mdc}(a_i, p) = 1$ para no máximo um índice do conjunto $[1, p^\beta + 2\beta]$, então obtemos a subsequência desejada de S.

Usando os dois parágrafos acima, vamos assumir, sem perda de generalidade, que $\text{mdc}(a_1, p) = 1$. Assim, aplicando o Lema 1.5 e a Observação 1.2, podemos reescrever S da seguinte maneira:

$$S = (1,0)(a_2, b_2)(a_3, b_3) \cdots (a_{p^\beta + 2\beta}, b_{p^\beta + 2\beta}).$$

Novamente sem perda de generalidade, vamos assumir que $\text{mdc}(b_2, p) = 1$. Invertendo as coordenadas e aplicando novamente o Lema 1.5, escrevemos

$$S = (1,0)(0,1)(a_3, b_3) \cdots (a_{p^\beta + 2\beta}, b_{p^\beta + 2\beta}).$$

Além disso, como vimos acima, podemos considerar que existem dois índices $i, j \in [3, p^\beta + 2\beta]$ (incluindo o caso onde $i = j$), tais que $\text{mdc}(a_i b_j, p) = 1$. Neste caso o Lema 1.9 nos assegura a existência de uma subsequência de soma-zero A-ponderada de S de comprimento p^β como queríamos.

Portanto, usando a Hipótese de Indução I, o resultado é válido para o caso $\alpha = \beta$. Usando o processo de indução novamente, vamos definir a

Hipótese de Indução II: assumimos que $\alpha > \beta$ e que $s_A(\mathbb{Z}_{p^{\alpha-1}} \oplus \mathbb{Z}_{p^\beta}) \leq p^{\alpha-1} + (\alpha - 1) + \beta$.

Afirmamos que, se $\text{mdc}(b_i, p) = 1$ para no máximo um índice do conjunto $[1, p^\alpha + \alpha + \beta]$, então podemos encontrar uma subsequência de soma-zero A-ponderada de S de

comprimento p^α. De fato, vamos considerar, sem perda de generalidade, que $b_i \equiv 0 \pmod{p}$ para todo $i \in [1, p^\alpha + \alpha + \beta - 1]$, ou seja, $b_i = b_i' p$, onde podemos assumir que $b_i' \in \mathbb{Z}_{p^{\beta-1}}$. Assim, a sequência

$$S' = (a_1, b_1')(a_2, b_2')(a_3, b_3') \cdots (a_{p^\alpha+\alpha+\beta-1}, b_{p^\alpha+\alpha+\beta-1}')$$

sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}}$ possui comprimento $p^\alpha + \alpha + \beta - 1$. Pela Hipótese de Indução I, temos $s_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}}) = p^\alpha + \alpha + (\beta - 1)$. Assim, S' contém uma subsequência de soma-zero A-ponderada T' de comprimento p^α, ou seja, existe um conjunto de índices $I \subset [1, p^\alpha + \alpha + \beta - 1]$ tal que $|I| = p^\alpha$,

$$T' = \prod_{i \in I} (a_i, b_i') \quad \text{e} \quad \sum_{i \in I} u_i (a_i, b_i') = (0, 0) \quad \text{sobre } \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}},$$

para alguma escolha de inteiros u_i, onde $u_i \in A$ para todo $i \in I$. Assim, temos

$$\sum_{i \in I} u_i b_i' \equiv 0 \pmod{p^{\beta-1}} \quad \Rightarrow \quad \sum_{i \in I} u_i b_i = \sum_{i \in I} u_i (b_i' p) \equiv 0 \pmod{p^\beta}.$$

Tomando a subsequência $T = \prod_{i \in I} (a_i, b_i)$ de S, temos $|T| = p^\alpha$ e $\sum_{i \in I} u_i (a_i, b_i) = (0, 0)$ sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ como queríamos.

Agora, vamos supor que $\text{mdc}(a_i, p) = 1$ para no máximo um índice do conjunto $[1, p^\alpha + \alpha + \beta]$. Sem perda de generalidade, consideremos que $a_i \equiv 0 \pmod{p}$ para todo $i \in [1, p^\alpha + \alpha + \beta - 1]$, ou seja, $a_i = a_i' p$, onde podemos assumir que $a_i' \in \mathbb{Z}_{p^{\alpha-1}}$. Assim, a sequência

$$S'' = (a_1', b_1)(a_2', b_2)(a_3', b_3) \cdots (a_{p^\alpha+\alpha+\beta-1}', b_{p^\alpha+\alpha+\beta-1})$$

sobre $\mathbb{Z}_{p^{\alpha-1}} \oplus \mathbb{Z}_{p^\beta}$ possui comprimento $p^\alpha + \alpha + \beta - 1 = pp^{\alpha-1} + (\alpha - 1) + \beta$. Pela Hipótese de Indução II, temos $s_A(\mathbb{Z}_{p^{\alpha-1}} \oplus \mathbb{Z}_{p^\beta}) \leq p^{\alpha-1} + (\alpha - 1) + \beta$. Assim fica claro que S'' contém p subsequências de comprimento $p^{\alpha-1}$ disjuntas duas a duas que são de soma-zero A-ponderada. Unindo todas estas p subsequências, obtemos T'' que é uma subsequência de soma-zero A-ponderada de S'' de comprimento $pp^{\alpha-1} = p^\alpha$. Desta forma existe um conjunto de índices $J \subset [1, p^\alpha + \alpha + \beta - 1]$ tal que $|J| = p^\alpha$,

$$T'' = \prod_{i \in J} (a_i', b_i) \quad \text{e} \quad \sum_{i \in J} u_i (a_i', b_i) = (0, 0) \quad \text{sobre } \mathbb{Z}_{p^{\alpha-1}} \oplus \mathbb{Z}_{p^\beta},$$

para alguma escolha de inteiros u_i, onde $u_i \in A$ para todo $i \in J$. Assim, temos

$$\sum_{i\in J} u_i a_i' \equiv 0 \pmod{p^{\alpha-1}} \quad \Rightarrow \quad \sum_{i\in J} u_i a_i = \sum_{i\in J} u_i (a_i' p) \equiv 0 \pmod{p^\alpha}.$$

Tomando a subsequência $T = \prod_{i\in J}(a_i, b_i)$ de S, temos $|T| = p^\alpha$ e $\sum_{i\in J} u_i(a_i, b_i) = (0, 0)$ sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ como queríamos.

Pelo que vimos acima, reordenando S para $\text{mdc}(a_1, p) = 1$ e aplicando o Lema 1.5 e a Observação 1.2, podemos reescrever S da seguinte forma:

$$S = (1, 0)(a_2, b_2)(a_3, b_3) \cdots (a_{p^\alpha+\alpha+\beta}, b_{p^\alpha+\alpha+\beta}).$$

Vamos supor que exista um índice $i \in [2, p^\alpha + \alpha + \beta]$ tal que $\text{mdc}(b_i, p) = 1$ e $p|a_i$. Pelo que vimos acima, podemos admitir que existem dois índices $j, k \in [2, p^\alpha + \alpha + \beta]$ diferentes de i (incluindo o caso onde $j = k$), tais que $\text{mdc}(a_j b_k, p) = 1$. Neste caso o resultado segue diretamente do Lema 1.9.

Daqui por diante vamos assumir, sem perda de generalidade, que $x_2 = (1, b_2)$ e $x_3 = (1, b_3)$, onde $\text{mdc}(b_2 b_3, p) = 1$, pela Observação 1.2.

Se existe um índice $i \in [4, p^\alpha + \alpha + \beta]$ tal que $\text{mdc}(a_i, p) = 1$ e $p|b_i$, então observe que

$$(a_i b_3 - b_i)x_2 - a_i b_2 x_3 + b_2 x_i = (a_i b_3 - b_i)(1, 0)$$

e todos os termos $(a_i b_3 - b_i)$, $a_i b_2$ e b_2 pertencem a A. Tomando $\ell = p^\alpha$ e $k = 3$, o resultado segue do Lema 1.12, pois $k \leq \ell - 3$.

Por fim, nos falta apenas analisar a seguinte situação: dado um inteiro $3 \leq t \leq p^\alpha + \alpha + \beta$, a sequência

$$S = (1, 0)(1, b_2)(1, b_3) \cdots (1, b_t)(a_{t+1}, b_{t+1}) \cdots (a_{p^\alpha+\alpha+\beta}, b_{p^\alpha+\alpha+\beta})$$

é tal que $\text{mdc}(b_2 b_3 \cdots b_t, p) = 1$ e $a_i \equiv 0 \equiv b_i \pmod{p}$, para todo índice i pertencente ao conjunto $[t + 1, p^\alpha + \alpha + \beta]$.

Se existem $b_i \not\equiv b_j \pmod{p}$, para alguma escolha de índices $i, j \in \{2, 3, \ldots, t\}$ com $i \neq j$, então temos

$$b_i x_j - b_j x_i = (b_i - b_j)(1, 0),$$

onde $b_i - b_j \in A$. Neste caso basta tomar $\ell = p^\alpha$ e $k = 2$ onde o resultado segue pelo Lema 1.12, como fizemos anteriormente. Assim, podemos assumir que $b_2 \equiv b_3 \equiv \cdots \equiv b_t$

(mod p), ou seja, existe um inteiro k_i tal que $b_i = b_2 + k_i p$, para todo $i \in \{3, 4, \ldots, t\}$. Assim, podemos reescrever S como

$$S = (1,0)(1,b_2)(1,b_2+k_3p)\cdots(1,b_2+k_tp)(a_{t+1},b_{t+1})\cdots(a_{p^\alpha+\alpha+\beta},b_{p^\alpha+\alpha+\beta})$$

onde $\text{mdc}(b_2, p) = 1$, $p|a_i$ e $p|b_i$, para todo $i \geq t+1$.

Pelo Lema 1.5 existe um automorfismo sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ que leva $(1, b_2)$ em $(1, 0)$. Mais do que isso, na demonstração do Lema 1.5 construimos, para $a = 1$ e $b = b_2$, o automorfismo $\Theta : \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta} \longrightarrow \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, dado por $\Theta(x, y) = (x, y - \overline{x}b_2)$, tal que $\Theta(1, b_2) = (1, 0)$, onde $\overline{x}$ representa a classe em $\mathbb{Z}_{p^\beta}$ do menor inteiro positivo pertencente à classe x em $\mathbb{Z}_{p^\alpha}$. Note que:

(i) $\Theta(1,0) = (1,-b_2)$;

(ii) $\Theta(1, b_2 + k_i p) = (1, k_i p)$, para todo $i \in \{3, 4, \ldots, t\}$;

(iii) Como $p|a_i$ e $p|b_i$, então $\Theta(a_i, b_i) = (a_i, c_i)$, onde $p|c_i$, para todo $i \in [t+1, p^\alpha+\alpha+\beta]$.

Desta forma, temos a sequência

$$S_1 = \Theta(S) = (1,-b_2)(1,0)(1,k_3p)\cdots(1,k_tp)(a_{t+1},c_{t+1})\cdots(a_{p^\alpha+\alpha+\beta},c_{p^\alpha+\alpha+\beta})$$

onde $p|a_i$ e $p|c_i$, para todo $i \geq t+1$. Tomando $c_i = c_i' p$, para todo $i \geq t+1$, onde $c_i' \in \mathbb{Z}_{p^{\beta-1}}$, construimos a sequência

$$S_2 = (1,0)(1,k_3)(1,k_4)\cdots(1,k_t)(a_{t+1},c'_{t+1})\cdots(a_{p^\alpha+\alpha+\beta},c'_{p^\alpha+\alpha+\beta})$$

de comprimento $p^\alpha+\alpha+\beta-1$ sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}}$. Pela Hipótese de Indução I vemos que S_2 possui uma subsequência de soma-zero A-ponderada T de comprimento p^α. Multiplicando a segunda coordenada de cada termo de T por p e aplicando o automorfismo inverso de Θ, obtemos a subsequência desejada de S.

Portanto, dada uma sequência S sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ de comprimento $p^\alpha+\alpha+\beta$, mostramos que existe uma subsequência de soma-zero A-ponderada de S de comprimento p^α. Isto nos mostra que $s_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}) \leq p^\alpha + \alpha + \beta$.

Considere a seguinte sequência:

$$\underbrace{(0,0)(0,0)\cdots(0,0)}_{p^\alpha-1 \text{ termos}}(1,0)(p,0)(p^2,0)\cdots(p^{\alpha-1},0)(0,1)(0,p)\cdots(0,p^{\beta-1})$$

sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ de comprimento $p^\alpha + \alpha + \beta - 1$. É fácil observar que esta sequência não possui uma subsequência de soma-zero A-ponderada de comprimento p^α. Então vemos que $s_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}) \geq p^\alpha + \alpha + \beta$. Isto completa a demonstração do teorema. □

1.4 O Problema Inverso Relacionado

Sejam p um primo ímpar e S uma sequência sobre o grupo (aditivo) $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde $\alpha \geq \beta$ são inteiros positivos. Nesta seção, $\delta_j(S)$ denota o número de termos (com multiplicidade) de S com ordem p^j, para todo $j \in [1, \alpha]$.

O próximo resultado é uma consequência direta do Teorema 1.14.

Lema 1.15. *Sejam p um primo ímpar e S uma sequência de elementos de $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde $\alpha \geq \beta$ são inteiros positivos, com $|S| = p^\alpha + \alpha + \beta - 1$. Suponha que S não possua uma subsequência de soma-zero A-ponderada de comprimento p^α, então S contém ao menos um termo cuja primeira coordenada possui ordem p^α e ao menos um termo cuja segunda coordenada possui ordem p^β.*

Demonstração. Considere que $S = x_1 x_2 \cdots x_{p^\alpha+\alpha+\beta-1}$ é tal que $x_i = (a_i, b_i) \in \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, para todo $i \in [1, p^\alpha + \alpha + \beta - 1]$.

Suponha inicialmente que S não possui um termo tal que a_i é de ordem p^α. Assim, temos $a_i = c_i p$, para todo $i \in [1, p^\alpha + \alpha + \beta - 1]$, onde podemos assumir $c_i \in \mathbb{Z}_{p^{\alpha-1}}$. Considere a sequência

$$S_1 = (c_1, b_1)(c_2, b_2) \cdots (c_{p^\alpha+\alpha+\beta-1}, b_{p^\alpha+\alpha+\beta-1})$$

sobre $\mathbb{Z}_{p^{\alpha-1}} \oplus \mathbb{Z}_{p^\beta}$ de comprimento $p^\alpha + \alpha + \beta - 1 = pp^{\alpha-1} + (\alpha - 1) + \beta$. Portanto, podemos obter p subsequências T_1, T_2, ..., T_p de S_1, disjuntas duas a duas e de comprimento $p^{\alpha-1}$, que são de soma-zero A-ponderada em $\mathbb{Z}_{p^{\alpha-1}} \oplus \mathbb{Z}_{p^\beta}$, pelo Teorema 1.14. Unindo todas estas subsequências obtemos a sequência $T = \prod_{i=1}^{p} T_i$ de comprimento $pp^{\alpha-1} = p^\alpha$. Desta forma existe um conjunto de índices $I_1 \subset [1, p^\alpha + \alpha + \beta - 1]$ tal que $|I_1| = p^\alpha$,

$$T = \prod_{i \in I_1} (c_i, b_i) \quad \text{e} \quad \sum_{i \in I_1} u_i (c_i, b_i) = (0, 0) \quad \text{sobre } \mathbb{Z}_{p^{\alpha-1}} \oplus \mathbb{Z}_{p^\beta},$$

para alguma escolha de inteiros u_i, onde $u_i \in A$ para todo $i \in I_1$. Assim, temos

$$\sum_{i\in I_1} u_i c_i \equiv 0 \pmod{p^{\alpha-1}} \quad \Rightarrow \quad \sum_{i\in I_1} u_i a_i = \sum_{i\in I_1} u_i (c_i p) \equiv 0 \pmod{p^{\alpha}}.$$

Tomando a subsequência $U = \prod_{i\in I_1}(a_i, b_i)$ de S, temos $|U| = p^\alpha$ e $\sum_{i\in I_1} u_i(a_i, b_i) = (0, 0)$ sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, contrariando a hipótese do lema.

Agora, suponha que S não possua nenhum termo tal que b_i é de ordem p^β. Assim, temos $b_i = d_i p$, para todo $i \in [1, p^\alpha + \alpha + \beta - 1]$, onde podemos assumir $d_i \in \mathbb{Z}_{p^{\beta-1}}$. Considere a sequência

$$S_2 = (a_1, d_1)(a_2, d_2) \cdots (a_{p^\alpha+\alpha+\beta-1}, d_{p^\alpha+\alpha+\beta-1})$$

sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}}$ de comprimento $p^\alpha+\alpha+(\beta-1)$. Portanto, S_2 possui uma subsequência de soma-zero A-ponderada T' de comprimento p^α em $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}}$, pelo Teorema 1.14. Assim existe um conjunto de índices $I_2 \subset [1, p^\alpha + \alpha + \beta - 1]$ tal que $|I_2| = p^\alpha$,

$$T' = \prod_{i\in I_2}(a_i, d_i) \quad \text{e} \quad \sum_{i\in I_2} u_i(a_i, d_i) = (0, 0) \quad \text{sobre } \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}},$$

para alguma escolha de inteiros u_i, onde $u_i \in A$ para todo $i \in I_2$. Assim, temos

$$\sum_{i\in I_2} u_i d_i \equiv 0 \pmod{p^{\beta-1}} \quad \Rightarrow \quad \sum_{i\in I_2} u_i b_i = \sum_{i\in I_2} u_i (d_i p) \equiv 0 \pmod{p^{\beta}}.$$

Tomando a subsequência $U' = \prod_{i\in I_2}(a_i, b_i)$ de S, temos $|U'| = p^\alpha$ e $\sum_{i\in I_2} u_i(a_i, b_i) = (0, 0)$ sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, que contraria novamente a hipótese do lema, completando sua demonstração. □

O próximo teorema fornece uma caracterização para todas as sequências extremas sobre o grupo (aditivo) $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$ que são livres de subsequências de soma-zero A-ponderada de comprimento p^α.

Teorema 1.16. *Sejam p um primo ímpar e S uma sequência sobre o grupo $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde $\alpha \geq \beta$ são inteiros positivos, com $|S| = p^\alpha+\alpha+\beta-1$. Se S não possui subsequências de soma-zero A-ponderada de comprimento p^α, então S contém exatamente $p^\alpha - 1$ termos iguais a $(0, 0)$, $\delta_j(S) \geq 1$, para todo $j \in [1, \alpha]$, e $\sum_{j=1}^{\alpha} \delta_j(S) = \alpha + \beta$.*

Demonstração. Vamos considerar que a sequência $S = x_1x_2, \cdots x_{p^\alpha+\alpha+\beta-1}$ é tal que $x_i = (a_i, b_i) \in \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, para todo $i \in [1, p^\alpha + \alpha + \beta - 1]$, e que S não contém subsequências de soma-zero A-ponderada de comprimento p^α.

Pelo Teorema 1.4, este resultado é válido para o caso em que $\beta = 2$. Vamos proceder por indução sobre β. Assim, definimos a

Hipótese de Indução I: vamos assumir que $\beta > 2$ e que o resultado é válido para $\beta - 1$, para qualquer que seja $\alpha \geq \beta - 1$.

Para mostrar que o resultado é válido para β, usaremos o processo de indução novamente, mas agora sobre α. Como $\alpha \geq \beta$, nosso ponto de partida será:

O caso $\alpha = \beta$.

Neste caso, consideremos que $S = x_1x_2 \cdots x_{p^\beta+2\beta-1}$ é uma sequência sobre $\mathbb{Z}_{p^\beta} \oplus \mathbb{Z}_{p^\beta}$. Pelo Lema 1.15 vamos assumir, sem perda de generalidade, que $\text{mdc}(b_1, p) = 1$. Se $p|b_i$ para todo $i \in [2, p^\beta + 2\beta - 1]$, ou seja, $b_i = b_i'p$ com $b_i' \in \mathbb{Z}_{p^{\beta-1}}$, então a sequência

$$S' = (a_2, b_2')(a_3, b_3')(a_4, b_4') \cdots (a_{p^\beta+2\beta-1}, b_{p^\beta+2\beta-1}')$$

sobre $\mathbb{Z}_{p^\beta} \oplus \mathbb{Z}_{p^{\beta-1}}$ possui comprimento $p^\beta + \beta + (\beta - 1) - 1$ e, como S não possui sequências de soma-zero A-ponderada de comprimento p^α, então o mesmo acontece com S'. Pela Hipótese de Indução I, S' contém $p^\beta - 1$ termos iguais a $(0, 0)$, $\delta_j(S') \geq 1$, para todo $j \in [1, \beta]$, e $\sum_{j=1}^{\beta} \delta_j(S') = \beta + (\beta - 1)$. Podemos observar facilmente que, se (a_i, b_i') tem ordem t sobre $\mathbb{Z}_{p^\beta} \oplus \mathbb{Z}_{p^{\beta-1}}$, para algum inteiro t, então $(a_i, b_i) = (a_i, b_i'p)$ tem ordem t sobre $\mathbb{Z}_{p^\beta} \oplus \mathbb{Z}_{p^\beta}$, para todo $i \in [2, p^\beta + 2\beta - 1]$. Retornando para S, o resultado segue, pois (a_1, b_1) é não nulo.

De forma análoga (invertendo as coordenadas) podemos mostrar que, se $\text{mdc}(a_i, p) = 1$ para exatamente um índice no conjunto $[1, p^\beta + 2\beta - 1]$, o resultado segue.

Com estas considerações podemos assumir, sem perda de generalidade, que $\text{mdc}(a_1, p) = 1$. Assim, aplicando o Lema 1.5 e a Observação 1.2, podemos reescrever S da seguinte maneira:

$$S = (1, 0)(a_2, b_2)(a_3, b_3) \cdots (a_{p^\beta+2\beta-1}, b_{p^\beta+2\beta-1}).$$

Novamente sem perda de generalidade, vamos assumir que $\text{mdc}(b_2, p) = 1$. Invertendo as

coordenadas e aplicando novamente o Lema 1.5, escrevemos

$$S = (1,0)(0,1)(a_3,b_3)\cdots(a_{p^\beta+2\beta-1}, b_{p^\beta+2\beta-1}).$$

Além disso, como vimos acima, podemos considerar que existem dois índices $i, j \in [3, p^\beta + 2\beta - 1]$ (incluindo o caso onde $i = j$), tais que $\text{mdc}(a_i b_j, p) = 1$. Neste caso, o Lema 1.9 nos assegura a existência de uma subsequência de soma-zero A-ponderada de S de comprimento p^β, contrariando a hipótese do teorema.

Portanto, usando a Hipótese de Indução I, o resultado é válido para o caso $\alpha = \beta$. Usaremos o processo de indução novamente, mas agora sobre o inteiro α. Vamos definir a:

Hipótese de Indução II: vamos considerar que $\alpha > \beta$ e que o resultado é válido para todo inteiro maior ou igual a β e menor que α.

Agora, seja $S = x_1 x_2 \cdots x_{p^\alpha+\alpha+\beta-1}$ uma sequência sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$.

Pelo Lema 1.15 vamos considerar, sem perda de generalidade, que $\text{mdc}(a_1, p) = 1$. Se $a_i \equiv 0 \pmod{p}$ para todo $i \in [2, p^\alpha + \alpha + \beta - 1]$, ou seja, $a_i = a_i' p$ com $a_i' \in \mathbb{Z}_{p^{\alpha-1}}$, então a sequência

$$S_1 = (a_2', b_2)(a_3', b_3)(a_4', b_4)\cdots(a'_{p^\alpha+\alpha+\beta-1}, b_{p^\alpha+\alpha+\beta-1})$$

sobre $\mathbb{Z}_{p^{\alpha-1}} \oplus \mathbb{Z}_{p^\beta}$ possui comprimento $p^\alpha + \alpha + \beta - 2 = pp^{\alpha-1} + (\alpha-1) + \beta - 1$. Aplicando o Teorema 1.14, vemos que S_1 possui $p-1$ subsequências T_i, $i \in [1, p-1]$, disjuntas duas a duas e de comprimento $p^{\alpha-1}$ tais que cada uma dela é de soma-zero A-ponderada. Considere a sequência $S_2 = S_1(T_1 \cdots T_{p-1})^{-1}$. Note que $|S_2| = p^{\alpha-1} + (\alpha-1) + \beta - 1$. Como S é livre de subsequências de soma-zero A-ponderada de comprimento p^α, então S_2 é livre de subsequências de soma-zero A-ponderada de comprimento $p^{\alpha-1}$. Aplicando a Hipótese de Indução II vemos que S_2 possui $p^{\alpha-1} - 1$ termos iguais a $(0,0)$, $\delta_j(S_2) \geq 1$, para todo $j \in [1, \alpha-1]$, e $\sum_{j=1}^{\alpha-1} \delta_j(S_2) = (\alpha-1) + \beta$. Retornando para S, precisamos apenas mostrar que todos os termos da sequência $T_1 T_2 \cdots T_{p-1}$ são iguais a $(0,0)$, pois o termo (a_1, b_1) possui ordem p^α. Seja x um termo da sequência T_i, para algum índice $i \in [1, p-1]$. Pelo Teorema 1.14, a sequência xS_2 possui uma subsequência de soma-zero A-ponderada S_3 de comprimento $p^{\alpha-1}$, contendo x. Note que a sequência $S_2 T_i S_3^{-1}$ possui exatamente $\alpha + 2$ termos não nulos, da mesma forma que S_2. Como $p^{\alpha-1} > \alpha + \beta$, então

S_3 possui ao menos um termo igual a $(0,0)$ e o mesmo acontece com T_i. Agora, como a sequência S não possui uma subsequência de soma-zero A-ponderada, então a sequência

$$S_2 \cdot T_i \cdot [\underbrace{(0,0)(0,0)\cdots(0,0)}_{p^{\alpha-1} \text{ termos}}]^{-1}$$

possui exatamente $\alpha+\beta-1$ termos não nulos (todos pertencentes a S_2), pela Hipótese de Indução II novamente, ou seja, todos os termos de T_i são iguais a $(0,0)$ como queríamos. Como o índice i é arbitrário, então todos os termos de $T_1T_2\cdots T_{p-1}$ são nulos e S possui a forma desejada.

Como $\text{mdc}(a_1,p)=1$, então, aplicando o Lema 1.5 e a Observação 1.2, podemos reescrever S da seguinte forma:

$$S=(1,0)(a_2,b_2)(a_3,b_3)\cdots(a_{p^\alpha+\alpha+\beta-1},b_{p^\alpha+\alpha+\beta-1}).$$

Pelo Lema 1.15 vamos considerar, sem perda de generalidade, que $\text{mdc}(b_2,p)=1$. Se $b_i\equiv 0 \pmod p$ para todo $i\in[3,p^\alpha+\alpha+\beta-1]$, ou seja, $b_i=b_i'p$ com $b_i'\in\mathbb{Z}_{p^{\beta-1}}$, então a sequência

$$S'=(1,0)(a_3,b_3')(a_4,b_4')\cdots(a_{p^\alpha+\alpha+\beta-1},b'_{p^\alpha+\alpha+\beta-1})$$

sobre $\mathbb{Z}_{p^\alpha}\oplus\mathbb{Z}_{p^{\beta-1}}$ possui comprimento $p^\alpha+\alpha+(\beta-1)-1$. Como S não possui subsequências de soma-zero A-ponderada de comprimento p^α, então o mesmo acontece com S'. Pela Hipótese de Indução I, vemos que S' possui $p^\alpha-1$ termos iguais a $(0,0)$, $\delta_j(S')\geq 1$, para todo $j\in[1,\alpha]$, e $\sum_{j=1}^{\alpha}\delta_j(S')=\alpha+(\beta-1)$. Retornando para S, o resultado segue, pois o termo (a_2,b_2) é não nulo.

Agora, vamos supor que exista um índice $i\in[2,p^\alpha+\alpha+\beta-1]$ tal que $\text{mdc}(b_i,p)=1$ e $p|a_i$. Pelo que vimos acima, existem dois índices $j,k\in[2,p^\alpha+\alpha+\beta-1]$ diferentes de i (incluindo o caso onde $j=k$), tais que $\text{mdc}(a_jb_k,p)=1$. Neste caso, o Lema 1.9 garante que S contém uma subsequência de soma-zero A-ponderada de comprimento p^α, contrariando a hipótese do teorema.

Daqui por diante podemos assumir, sem perda de generalidade, que $x_2=(1,b_2)$ e $x_3=(1,b_3)$, onde $\text{mdc}(b_2b_3,p)=1$, pela Observação 1.2.

Suponhamos que exista um índice $i\in[4,p^\alpha+\alpha+\beta-1]$ tal que $\text{mdc}(a_i,p)=1$ e $p|b_i$.

Desta forma, temos

$$(a_ib_3 - b_i)x_2 - a_ib_2x_3 + b_2x_i = (a_ib_3 - b_i)(1, 0),$$

com $a_ib_3 - b_i$, a_ib_2 e b_2 pertencentes ao conjunto A. Portanto, S contém uma subsequência de soma-zero A-ponderada de comprimento p^α, pelo Lema 1.12. Isto contradiz a hipótese do teorema.

Neste momento nos falta analisar o seguinte caso: dado o inteiro $3 \leq t \leq p^\alpha + \alpha + \beta - 1$, temos

$$S = (1, 0)(1, b_2)(1, b_3) \cdots (1, b_t)(a_{t+1}, b_{t+1}) \cdots (a_{p^\alpha+\alpha+\beta-1}, b_{p^\alpha+\alpha+\beta-1})$$

onde $\text{mdc}(b_2b_3 \cdots b_t, p) = 1$ e $a_i \equiv 0 \equiv b_i \pmod{p}$, para todo $i \in [t + 1, p^\alpha + \alpha + \beta - 1]$.

Se existem $b_i \not\equiv b_j \pmod{p}$, para alguma escolha de índices $i, j \in \{2, 3, \ldots, t\}$ com $i \neq j$, então

$$b_ix_j - b_jx_i = (b_i - b_j)(1, 0),$$

onde $b_i, b_j, (b_i - b_j) \in A$. Neste caso, S contém uma subsequência de soma-zero A-ponderada de comprimento p^α, pelo Lema 1.12, contrariando a hipótese do teorema. Assim, podemos assumir que $b_2 \equiv b_3 \equiv \cdots \equiv b_t \pmod{p}$, ou seja, existe um inteiro k_i tal que $b_i = b_2 + k_ip$, para todo $i \in \{3, 4, \ldots, t\}$. Com isso, podemos reescrever S da seguinte forma:

$$S = (1, 0)(1, b_2)(1, b_2 + k_3p) \cdots (1, b_2 + k_tp)(a_{t+1}, b_{t+1}) \cdots (a_{p^\alpha+\alpha+\beta-1}, b_{p^\alpha+\alpha+\beta-1})$$

onde $\text{mdc}(b_2, p) = 1$ e $a_i \equiv 0 \equiv b_i \pmod{p}$, para todo $i \in [t + 1, p^\alpha + \alpha + \beta - 1]$.

Como fizemos na demonstração do Teorema 1.14, o Lema 1.5 garante que podemos aplicar o automorfismo $\Theta : \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta} \longrightarrow \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, dado por $\Theta(x, y) = (x, y - \overline{x}b_2)$, onde $\overline{x}$ representa a classe em $\mathbb{Z}_{p^\beta}$ do menor inteiro positivo pertencente à classe x em $\mathbb{Z}_{p^\alpha}$. Relembre que $\Theta(1, b_2) = (1, 0)$, $\Theta(1, 0) = (1, -b_2)$, $\Theta(1, b_2 + k_ip) = (1, k_ip)$, para todo $i \in \{3, 4, \ldots, t\}$ e, como $p|a_i$ e $p|b_i$, então $\Theta(a_i, b_i) = (a_i, c_i)$, onde $p|c_i$, para todo $i \in [t + 1, p^\alpha + \alpha + \beta - 1]$.

Desta forma, consideremos a sequência

$$S' = \Theta(S) = (1, -b_2)(1, 0)(1, k_3p) \cdots (1, k_tp)(a_{t+1}, c_{t+1}) \cdots (a_{p^\alpha+\alpha+\beta-1}, c_{p^\alpha+\alpha+\beta-1}),$$

onde $p|a_i$ e $p|c_i$, para todo $i \geq t+1$. Tomando $c_i = c_i' p$, para todo $i \geq t+1$, onde $c_i' \in \mathbb{Z}_{p^{\beta-1}}$, construimos a sequência

$$S'' = (1,0)(1,k_3)(1,k_4)\cdots(1,k_t)(a_{t+1},c_{t+1}')\cdots(a_{p^\alpha+\alpha+\beta-1},c_{p^\alpha+\alpha+\beta-1}')$$

de comprimento $p^\alpha + \alpha + (\beta-1) - 1$ sobre $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^{\beta-1}}$. Pela Hipótese de Indução I vemos que S'' contém $p^\alpha - 1$ termos iguais a $(0,0)$, $\delta_j(S'') \geq 1$, para todo $j \in [1,\alpha]$, e $\sum_{j=1}^{\alpha} \delta_j(S'') = \alpha + (\beta-1)$. Como $(1,-b_2)$ é não nulo e um automorfismo preserva a ordem dos elementos de um grupo, então podemos aplicar o automorfismo inverso de Θ em S' fazendo com que S tenha a forma desejada. Isto completa a demonstração do teorema. □

Como uma consequência direta dos Teoremas 1.14 e 1.16, obtemos o seguinte resultado:

Corolário 1.17. *Sejam p um primo ímpar e S uma sequência sobre o grupo $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde $\alpha \geq \beta$ são inteiros positivos. Então:*

(i) $\eta_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}) = \alpha + \beta + 1$;

(ii) se $|S| = \alpha + \beta$ e S não possui subsequências de soma-zero A-ponderada de comprimento no máximo p^α, então $\delta_j(S) \geq 1$, para todo $j \in [1,\alpha]$;

(iii) a equação $s_A(G) = \eta_A(G) + \exp(G) - 1$ é válida para o grupo $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$.

A demonstração deste corolário é obtida acrescentando uma quantidade adequada de termos iguais a $(0,0)$ às sequências e aplicando os Teoremas 1.14 e 1.16.

1.5 Um Limite Superior para um Caso Mais Geral

Nesta seção estamos interessados em analisar o valor da constante s_A para o grupo abeliano aditivo $\mathbb{Z}_n \oplus \mathbb{Z}_{p^\beta}$, onde β é um inteiro positivo e n é um inteiro ímpar tal que $p^\beta | n$. Note que, neste caso, $A = \{a \in \mathbb{Z}\,;\, \text{mdc}(a,n) = 1\}$.

Chintamani e Paul demonstraram em [13] e em [14] os seguintes resultados:

Teorema 1.18. *Seja p um primo ímpar e $n \geq 1$ um inteiro ímpar tal que $p|n$. Então*

$$s_A(\mathbb{Z}_n \oplus \mathbb{Z}_p) \leq n + \Omega(n) + 2.$$

Teorema 1.19. *Seja p um primo ímpar e $n \geq 1$ um inteiro ímpar tal que $p^2|n$. Então*

$$s_A(\mathbb{Z}_n \oplus \mathbb{Z}_{p^2}) \leq n + \Omega(n) + 4.$$

Usando uma abordagem diferente da utilizada por Chintamani e Paul, faremos estimativas para o valor de $s_A(\mathbb{Z}_n \oplus \mathbb{Z}_{p^\beta})$.

Inicialmente vamos escrever $n = p^\alpha q_1 q_2 \cdots q_t$, onde $q_1, \ldots, q_t$ são primos (não necessariamente distintos dois a dois) com $p \neq q_i$ para qualquer $i \in [1, t]$, e $\alpha \geq \beta$. Considere a sequência

$$\underbrace{(0,0)(0,0)\cdots(0,0)}_{n-1 \text{ termos}}\left(\prod_{k=0}^{\beta-1}(0,p^k)\right)\left(\prod_{k=0}^{\alpha-1}(p^k,0)\right)(p^{\alpha-1}q_1,0)(p^{\alpha-1}q_1q_2,0)\cdots(p^{\alpha-1}q_1q_2\cdots q_t,0)$$

de comprimento $n + \Omega(n) + \beta - 1$. É fácil observar que esta sequência não possui uma soma-zero A-ponderada de comprimento n, então temos que

$$s_A(Z_n \oplus \mathbb{Z}_{p^\beta}) \geq n + \Omega(n) + \beta.$$

Em sua Tese de Doutorado, A. Lemos demonstrou o seguinte resultado (ver [32], Proposição 1.6):

Proposição 1.20. *Sejam G um grupo abeliano finito, $A = \{1\}$ ou $A = \{1, -1\}$, H um subgrupo de G e S uma sequência de termos de G tal que $|S| \geq (s_A(H) - 1)\exp(G/H) + s_A(G/H)$. Então S possui uma subsequência de soma-zero A-ponderada de comprimento $\exp(H)\exp(G/H)$. Em particular, se $\exp(G) = \exp(H)\exp(G/H)$, então*

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

Esta proposição é uma generalização de um resultado de Gao (ver [15], Proposição 3.1), que é exatamente o caso $A = \{1\}$. Além disso, seguindo o mesmo procedimento usado por Lemos, a Proposição 1.20 continua válida para o caso em que A é um subgrupo multiplicativo de $\mathbb{Z}_n^* = \{a \in \mathbb{Z}\,;\, 1 \leq a \leq n \text{ e } \text{mdc}(a, n) = 1\}$, onde $n = \exp(G)$.

Agora vamos estabelecer uma cota superior para $s_A(Z_n \oplus \mathbb{Z}_{p^\beta})$.

Teorema 1.21. *Sejam p um primo ímpar, β um inteiro positivo e $n \geq 1$ um inteiro ímpar tal que $n = p^\beta m$, para algum inteiro m. Então*

$$s_A(\mathbb{Z}_n \oplus \mathbb{Z}_{p^\beta}) \leq n + \Omega(n) + (2m - 1)\beta,$$

para o caso em que $A = \{a \in \mathbb{Z}\,;\, mdc(a,n) = 1\}$.

Demonstração. Tome $G = \mathbb{Z}_n \oplus \mathbb{Z}_{p^\beta}$ e o conjunto $H = \{(a,b) \in G\,;\, m|a\}$. É fácil observar que H é um subgrupo de G e que $H \cong \mathbb{Z}_{p^\beta} \oplus \mathbb{Z}_{p^\beta}$. Portanto $\exp(H) = p^\beta$ e, pelo Teorema 1.14,

$$s_A(H) = p^\beta + 2\beta.$$

Por outro lado, podemos observar que $G/H \cong \mathbb{Z}_m$. Assim, $\exp(G/H) = m$ e obtemos a relação

$$\exp(G) = \exp(H)\exp(G/H).$$

Já nos referimos a um resultado de F. Luca (ver [34]) que nos diz que $s_A(G/H) = s_A(\mathbb{Z}_m) = m + \Omega(m)$. Além disso, note que $\Omega(n) = \Omega(m) + \beta$.

Usando a Proposição 1.20 para $A = \{a \in \mathbb{Z}\,;\, \mathrm{mdc}(a,n) = 1\}$, temos

$$\begin{aligned} s_A(\mathbb{Z}_n \oplus \mathbb{Z}_{p^\beta}) &\leq (s_A(H) - 1)\exp(G/H) + s_A(G/H) \\ &= (p^\beta + 2\beta - 1)m + (m + \Omega(m)) \\ &= mp^\beta + 2m\beta + \Omega(n) - \beta \\ &= n + \Omega(n) + (2m-1)\beta \end{aligned}$$

como queríamos. □

Observando as cotas superiores obtidas por Chintamani e Paul nos Teoremas 1.18 e 1.19, fica claro que a cota que obtivemos no Teorema 1.21 não é muito boa e está muito distante da cota inferior que apresentamos. Como sugestão para novos estudos neste sentido, o próximo passo deverá ser reduzir esta cota superior.

1.6 Considerações Adicionais

Para um primo ímpar p os Teoremas 1.14 e 1.16 calculam o valor exato de s_A para o grupo abeliano aditivo finito $\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$, onde $\alpha \geq \beta$ são inteiros positivos, e classificam as sequências de comprimento $s_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}) - 1$ que são livres de subsequências de soma-zero A-ponderada de comprimento p^α. Além disso, como vimos no Corolário 1.17, sabemos que $\eta_A(\mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}) = \alpha + \beta + 1$, temos uma caracterização da sequências de comprimento $\alpha + \beta$

que são livres de subsequências de soma-zero A-ponderada de comprimento no máximo p^α e a equação

$$s_A(G) = \eta_A(G) + \exp(G) - 1 \tag{1.6}$$

é válida para o grupo $G = \mathbb{Z}_{p^\alpha} \oplus \mathbb{Z}_{p^\beta}$.

Já vimos que $s_A(\mathbb{Z}_3^r) = 2\eta_A(\mathbb{Z}_3^r) - 1 > \eta_A(\mathbb{Z}_3^r) + 3 - 1$, para $A = \{a \in \mathbb{Z}\,;\, \text{mdc}(a, n) = 1\}$ e $r \geq 3$ (ver [26]), ou seja, a equação (1.6) é falsa para este caso. Note que, neste caso, o posto de $G = \mathbb{Z}_3^r$ é maior ou igual a $\exp(G) = 3$.

Dados um primo ímpar p e os inteiros positivos t e $n_1 \geq n_2 \geq \cdots \geq n_t$, considere o grupo aditivo $G = \mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_t}}$, onde vemos que $\exp(G) = p^{n_1}$. Observe a seguinte sequência sobre G:

$$S = \underbrace{(0, \ldots, 0) \cdots (0, \ldots, 0)}_{p^{n_1} - 1 \text{ termos}} \prod_{k=0}^{n_1 - 1} (p^k, 0, 0, \ldots, 0) \prod_{k=0}^{n_2 - 1} (0, p^k, 0, \ldots, 0) \cdots \prod_{k=0}^{n_t - 1} (0, 0, 0, \ldots, p^k).$$

É fácil observar que S tem comprimento $|S| = p^{n_1} - 1 + \sum_{i=1}^{t} n_i$ e não possui subsequências de soma-zero A-ponderada de comprimento p^{n_1}. No entanto, supondo que $t \geq p^{n_1}$ (o posto de G é maior ou igual a $\exp(G)$), podemos considerar a sequência

$$T = S \cdot (1, 1, \ldots, 1)$$

de comprimento $|T| = p^{n_1} + \sum_{i=1}^{t} n_i$ e não possui subsequências de soma-zero A-ponderada de comprimento p^{n_1} (note que ela possui subsequências de soma-zero A-ponderada de comprimento maior ou menor que p^{n_1}, mas nunca igual).

Estas observações somadas aos nossos estudos nos levam a acreditar que a seguinte conjectura seja verdadeira:

Conjectura 1.22. *Sejam p um primo ímpar e o grupo (aditivo) $G = \bigoplus_{i=1}^{t} \mathbb{Z}_{p^{n_i}}$, onde t e $n_1 \geq n_2 \geq \cdots \geq n_t$ são inteiros positivos, com $t < p^{n_1}$. Então*

(i) $s_A(G) = p^{n_1} + \sum_{i=1}^{t} n_i$;

(ii) $s_A(G) = \eta_A(G) + \exp(G) - 1$.

Esta conjectura propõe uma generalização para o resultado obtido por J. Olson em 1968 (ver [38]) que calcula o valor da Constante de Davenport para este grupo, a saber $D(G) = 1 + \sum_{i=1}^{t} (p^{n_i} - 1)$.

Capítulo 2

Uma Generalização para a Constante de Davenport

2.1 Conceitos e Resultados Preliminares

Como já vimos anteriormente, usaremos sempre $[u_1]^{n_1}[u_2]^{n_2}\cdots[u_t]^{n_t}$ para denotar a sequência

$$(\underbrace{u_1, u_1, \ldots, u_1}_{n_1 \text{ vezes}}, \underbrace{u_2, u_2, \ldots, u_2}_{n_2 \text{ vezes}}, \ldots, \underbrace{u_t, u_t, \ldots, u_t}_{n_t \text{ vezes}})$$

em $\mathbb{Z}_p$ de comprimento $n = n_1 + n_2 + \cdots + n_t$. Dada esta notação é importante observar que podemos considerar que duas sequências em $\mathbb{Z}_p$ são iguais se elas diferem somente na ordem de seus elementos.

Usando [19] como referência, começaremos introduzindo mais algumas definições e notações.

Definição 2.1. *Seja n um inteiro positivo e K um corpo. O polinômio $f(x_1, x_2, \ldots, x_n) \in K[x_1, x_2, \ldots, x_n]$ é dito simétrico se*

$$f(x_1, x_2, \ldots, x_n) = f(x_{\alpha(1)}, x_{\alpha(2)}, \ldots, x_{\alpha(n)}),$$

para qualquer que seja a permutação α sobre o conjunto $\{1, 2, \ldots, n\}$.

Abaixo definimos os polinômios simétricos mais simples.

Definição 2.2. *Sejam K um corpo e os inteiros n e k, tais que $1 \leq k \leq n$. Definimos o polinômio simétrico elementar de ordem k em $K[x_1, x_2, \ldots, x_n]$ como sendo*

$$\sigma_{n,k}(x_1, x_2, \ldots, x_n) = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} x_{i_1} x_{i_2} \cdots x_{i_k}.$$

Por simplicidade de notação, escreveremos $\sigma_{n,k}$ no lugar de $\sigma_{n,k}(x_1, \ldots, x_n)$. Assim,

$$\sigma_{n,1} = \sum_{i=1}^{n} x_i \ , \quad \sigma_{n,2} = \sum_{1 \leq i < j \leq n} x_i x_j \ , \ \ldots \ , \quad \sigma_{n,n} = x_1 x_2 \ldots x_n.$$

Enunciaremos um importante resultado que resume o estudo a respeito de polinômios simétricos ao estudo dos polinômios simétricos elementares.

Teorema 2.3 (Teorema Fundamental dos Polinômios Simétricos)**.** *Se n é um inteiro positivo e f é um polinômio simétrico nas indeterminadas x_1, x_2, ... , x_n sobre um corpo K, então existe um único polinômio $g \in K[x_l, x_2, \ldots, x_n]$ tal que*

$$f(x_l, x_2, \ldots, x_n) = g(\sigma_{n,1}, \sigma_{n,2}, \ldots, \sigma_{n,n}).$$

O Teorema 2.3 nos diz que qualquer polinômio simétrico nas indeterminadas x_1, x_2, ..., x_n é, na verdade, uma expressão polinomial sobre os polinômios simétricos elementares $\sigma_{n,1}$, $\sigma_{n,2}$, ..., $\sigma_{n,n}$. A demonstração deste teorema também se encontra em [19] (Teorema 6.4.2).

Ao longo deste capítulo denotaremos por $s_{n,k}(x_1, x_2, \ldots, x_n)$, para n e k inteiros positivos e K um corpo, o polinômio das somas de potências de grau k em $K[x_1, x_2, \ldots, x_n]$, que é definido por

$$s_{n,k}(x_1, x_2, \ldots, x_n) = x_1^k + x_2^k + \cdots + x_n^k.$$

Observe que os polinômios $s_{n,k}(x_1, x_2, \ldots, x_n)$ são simétricos e, por simplicidade de notação, escreveremos $s_{n,k}$ no lugar de $s_{n,k}(x_1, x_2, \ldots, x_n)$. Agora vamos apresentar um resultado que relaciona os polinômios das somas de potências com os polinômios simétricos elementares.

Teorema 2.4 (Fórmula de Newton)**.** *Sejam n um inteiro positivo e $\sigma_{n,1}, \sigma_{n,2}, \ldots, \sigma_{n,n}$ os polinômios simétricos elementares nas indeterminadas x_1, x_2, ... , x_n sobre um corpo K. Se assumirmos $s_{n,0} = n$, então a fórmula*

$$s_{n,k} - s_{n,k-1}\sigma_{n,1} + s_{n,k-2}\sigma_{n,2} + \ldots + (-1)^{m-1} s_{n,k-m+1}\sigma_{n,m-1} + (-1)^m \frac{m}{n} s_{n,k-m}\sigma_{n,m} = 0$$

é válida para todo inteiro $k \geq 1$, onde $m = \min(n, k)$.

Este resultado foi citado em [33] (Teorema 1.75). Agora observe algumas relações obtidas da Fórmula de Newton (com as condições de que $n \geq k$ e a ordem do corpo K é maior que k):

$$s_{n,1} - \sigma_{n,1} = 0 \ , \quad s_{n,2} - s_{n,1}\sigma_{n,1} + 2\sigma_{n,2} = 0 \ , \quad s_{n,3} - s_{n,2}\sigma_{n,1} + s_{n,1}\sigma_{n,2} - 3\sigma_{n,3} = 0 \ , \quad \ldots$$

De outra forma:

$$\sigma_{n,1} = s_{n,1} \ , \quad \sigma_{n,2} = \frac{1}{2}(s_{n,1}^2 - s_{n,2}) \ , \quad \sigma_{n,3} = \frac{1}{6}(s_{n,1}^3 - 3s_{n,1}s_{n,2} + 2s_{n,3}) \ , \quad \ldots$$

Observação 2.5. *Note que, pelas relações acima, podemos escrever os polinômios simétricos elementares como expressão polinomial dos polinômios das somas de potências sempre que $n \geq k$. Pelo Teorema 2.4, o mesmo não ocorre quando $n < k$. Além disso, para escrever esta expressão polinomial precisamos que a ordem do corpo K seja maior que k, para que o último termo da Fórmula de Newton seja não nulo. Para esta última afirmação, como exemplo, podemos ver que a relação envolvendo o termo $\sigma_{n,3}$ acima não faria sentido no corpo $\mathbb{Z}_3$.*

Agora, reescrevendo o Teorema 0.1, temos o seguinte resultado:

Teorema 2.6. *Se p é um primo, então toda sequência de elementos em $\mathbb{Z}_p$ de comprimento $2p-1$ contém uma subsequência de soma-zero de comprimento p. Além disso, o conjunto de todas as sequências de comprimento $2p-2$ sobre $\mathbb{Z}_p$ livres de subsequências de soma-zero de comprimento p é dado por*

$$\left\{ [u]^{p-1}[v]^{p-1} \ / \ u, v \in \mathbb{Z}_p, \ \ e \ u \neq v \right\}.$$

Dados um primo p, o corpo $\mathbb{Z}_p$ (com a adição e a multiplicação usuais), um inteiro positivo n e um polinômio simétrico φ em $\mathbb{Z}_p[x_1, x_2, \ldots, x_n]$, dizemos que uma sequência de n elementos $S = (u_1, u_2, \ldots, u_n)$ sobre $\mathbb{Z}_p$ será chamada um *sequência φ-zero* se

$$\varphi(S) = \varphi(u_1, u_2, \ldots, u_n) = 0.$$

Além disso, chamaremos uma sequência em $\mathbb{Z}_p$ de sequência φ-zero livre se ela não contém nenhuma subsequência φ-zero.

Seja φ um polinômio simétrico em $\mathbb{Z}_p[x_1, x_2, \ldots, x_p]$, onde p é um primo. Estendendo o conceito do invariante $E(G)$ obtido do Teorema 2.6, A. Bialostocki e T. D. Luong definiram em [10] (2009) um novo invariante $g(\varphi, \mathbb{Z}_p)$ definido como sendo o menor inteiro ℓ tal que cada sequência em $\mathbb{Z}_p$ de comprimento ℓ contém uma subsequência φ-zero e $g(\varphi, \mathbb{Z}_p) = \infty$, caso não exista tal ℓ. Definiram, também, o conjunto $M(\varphi, \mathbb{Z}_p)$ de todas as sequências de comprimento $g(\varphi, \mathbb{Z}_p) - 1$ que são φ-zero livres, para $g(\varphi, \mathbb{Z}_p)$ finito. Observe que, se $\varphi(0, 0, \ldots, 0) \neq 0$, então a sequência $[0]^m$ é livre de subsequências φ-zero, para todo inteiro $m \geq p$, ou seja, $g(\varphi, \mathbb{Z}_p) = \infty$.

Observe que o caso em que φ for um polinômio simétrico linear, ou seja, $\varphi = as_{p,1} \in \mathbb{Z}_p[x_1, x_2, \ldots, x_p]$, com $a \neq 0$, então o Teorema 2.6 garante que $g(\varphi, \mathbb{Z}_p) = 2p - 1$ e $M(\varphi, \mathbb{Z}_p)$ é o conjunto de todas as sequências de $\mathbb{Z}_p$ da forma $[u]^{p-1}[v]^{p-1}$, onde $u, v \in \mathbb{Z}_p$ e $u \neq v$.

Além disso, no mesmo artigo ([10]), Bialostocki e Luong estudaram o caso em que φ é um polinômio simétrico quadrático e analisaram o valor de $g(\varphi, \mathbb{Z}_p)$ e a descrição do conjunto $M(\varphi, \mathbb{Z}_p)$ provando o seguinte resultado:

Teorema 2.7. *Sejam $p \geq 3$ um primo e $\varphi = as_{p,1}^2 + bs_{p,2} + cs_{p,1} \in \mathbb{Z}_p[x_1, x_2, \ldots, x_p]$ um polinômio simétrico quadrático, onde $a, b, c \in \mathbb{Z}_p$ e $a \neq 0$, ou $b \neq 0$. Então são verdadeiras as seguintes afirmações:*

(i) Se $a = 0$ e $b \neq 0$, então $g(\varphi, \mathbb{Z}_p) = 2p-1$ e as sequências de $M(\varphi, \mathbb{Z}_p)$ são da forma

$$[u]^{\alpha}[-u - cb^{-1}]^{p-1-\alpha}[v]^{\beta}[-v - cb^{-1}]^{p-1-\beta},$$

onde $u, v \in \mathbb{Z}_p$, $u \neq v$, $u + v \neq -cb^{-1}$ e $0 \leq \alpha \leq p-1$, $0 \leq \beta \leq p-1$.

(ii) Se $a \neq 0$ e $b = c = 0$, então $g(\varphi, \mathbb{Z}_p) = 2p - 1$ e as sequências de $M(\varphi, \mathbb{Z}_p)$ são da forma

$$[u]^{p-1}[v]^{p-1},$$

onde $u, v \in \mathbb{Z}_p$ e $u \neq v$.

(iii) Se $a \cdot c \neq 0$ e $b = 0$, então $g(\varphi, \mathbb{Z}_p) = 2p - 2$ e as sequências de $M(\varphi, \mathbb{Z}_p)$ são da forma

$$[u]^{p-1}[u + ca^{-1}]^{p-2},$$

onde $u \in \mathbb{Z}_p$.

(iv) Se $a \cdot b \neq 0$ *e* $p \geq 5$, *então*

$$2(p-1) + n(p) \leq g(\varphi, \mathbb{Z}_p) \leq 4p - 3,$$

onde $n(p)$ *denota o menor resíduo não quadrático módulo* p.

Nosso objetivo será similar ao de Bialostocki e Luong, pois queremos definir um invariante que consistirá numa generalização da Constante de Davenport sobre os polinômios simétricos e fazer análises semelhantes às feitas por eles.

2.2 A Constante de Davenport sob o ponto de vista dos Polinômios Simétricos

Inicialmente vamos reescrever o primeiro resultado relacionado à Constante de Davenport (Teorema 0.2):

Teorema 2.8. *Sendo* p *um primo, então toda sequência sobre* $\mathbb{Z}_p$ *de comprimento* p *possui uma sequência de soma-zero e, além disso, o conjunto* $\{[u]^{p-1} \,/\, u \in \mathbb{Z}_p, u \neq 0\}$ *é formado por todas as sequências de comprimento* $p-1$ *que são livres de soma-zero.*

Neste momento iremos fornecer as ferramentas necessárias para generalizar o conceito da Constante de Davenport para polinômios simétricos.

Dados n um inteiro positivo, K um corpo e $\varphi \in K[x_1, x_2, \ldots, x_n]$ um polinômio simétrico. É perfeitamente possível aplicar este polinômio nos termos de uma sequência $S = (u_1, u_2, \ldots, u_n)$ de termos em K da sequinte forma:

$$\varphi(S) = \varphi(u_1, u_2, \ldots, u_n).$$

Observe que, se φ puder ser escrito como uma expressão polinomial dos polinômios somas de potências $s_{n,t}$, para $t \in \mathbb{N}$, ou seja,

$$\varphi = g(s_{n,1}, s_{n,2}, \ldots, s_{n,t}),$$

então podemos definir o conjunto $\mathcal{F}_\varphi$ dos polinômios simétricos que possuem os mesmos coeficientes e o mesmo grau do polinômio φ, alterando-se apenas o número de variáveis. De fato,

$$\mathcal{F}_\varphi = \{\varphi_k = g(s_{k,1}, s_{k,2}, \ldots, s_{k,t}) \ / \ k \in \mathbb{N}\}.$$

Observe que $\varphi_n \in \mathcal{F}_\varphi$ é o próprio polinômio φ. Agora, com o conjunto $\mathcal{F}_\varphi$ definido, podemos calcular o valor de um polinômio com características muito semelhantes aos de φ em subsequências de S. A sequência $T = (u_1, u_2, u_3)$, por exemplo, é uma subsequência de S e, para $n > 3$, não podemos calcular $\varphi(T)$, mas podemos calcular $\varphi_3(T)$, onde $\varphi_3 \in \mathcal{F}_\varphi$.

Como vimos na Observação 2.5, nem todos os polinômios podem ser escritos como expressão polinomial dos polinômios somas de potências sobre determinados corpos. Por exemplo: o polinômio $\sigma_{n,2}$ sobre o corpo $\mathbb{Z}_3$ em n indeterminadas pode ser escrito como

$$\sigma_{n,2} = 2^{-1}(s_{n,1}^2 - s_{n,2}) = -s_{n,1}^2 + s_{n,2}.$$

No entanto é impossível descrever desta forma o mesmo polinômio $\sigma_{n,2}$ sobre o corpo $\mathbb{Z}_2$. O mesmo acontece com o polinômio $\sigma_{n,3}$ sobre o corpo $\mathbb{Z}_3$, pois nestes casos as relações dadas pela Fórmula de Newton (Teorema 2.4) não são suficientes.

Dados $t, n \in \mathbb{N}$, p um primo e φ um polinômio simétrico sobre $\mathbb{Z}_p$ de grau t em n indeterminadas, o Teorema Fundamental dos Polinômios Simétricos (Teorema 2.3) garante a existência de um polinômio $g \in \mathbb{Z}_p[x_1, x_2, \ldots, x_n]$ tal que

$$\varphi(x_1, x_2, \ldots, x_n) = g(\sigma_{n,1}, \sigma_{n,2}, \ldots, \sigma_{n,n}).$$

Agora, tendo em vista a Observação 2.5, podemos concluir que, sob algumas condições para os valores de p, n e t, existe um polinômio $f \in \mathbb{Z}_p[x_1, x_2, \ldots, x_n]$ tal que

$$\varphi(x_1, x_2, \ldots, x_n) = g(\sigma_{n,1}, \sigma_{n,2}, \ldots, \sigma_{n,n}) = f(s_{n,1}, s_{n,2}, \ldots, s_{n,n}).$$

Sendo assim, vamos definir o conjunto $\mathcal{F}_\varphi = \{\varphi_k = f(s_{k,1}, s_{k,2}, \ldots, s_{k,n}) \, ; \, k \in \mathbb{N}\}$ de todos os polinômios de mesmo grau e com os mesmos coeficientes de φ. Como exemplo, considere o polinômio $\varphi \in \mathbb{Z}_7[x_1, x_2, x_3]$ simétrico de grau 2 dado por

$$\begin{aligned} \varphi(x_1, x_2, x_3) &= s_{3,1}^2 + 2s_{3,1} - s_{3,2} + 3 \\ &= (x_1 + x_2 + x_3)^2 + 2(x_1 + x_2 + x_3) - (x_1^2 + x_2^2 + x_3^2) + 3. \end{aligned}$$

Assim, para todo $k \in \mathbb{N}$, definimos

$$\begin{aligned}\varphi_k(x_1, x_2, \ldots, x_k) &= s_{k,1}^2 + 2s_{k,1} - s_{k,2} + 3 \\ &= (x_1 + \ldots + x_k)^2 + 2(x_1 + \ldots + x_k) - (x_1^2 + \ldots + x_k^2) + 3\end{aligned}$$

e, com isso, $\mathcal{F}_\varphi = \left\{ s_{k,1}^2 + 2s_{k,1} - s_{k,2} + 3 \ ; \ k \in \mathbb{N} \right\}$.

Dizemos que uma sequência S em $\mathbb{Z}_p$ é uma *sequência $\mathcal{F}_\varphi$-zero* se existe $k \in \mathbb{N}$ tal que S é uma sequência φ_k-zero. Defina $D(\varphi, \mathbb{Z}_p)$ como sendo o menor inteiro ℓ tal que cada sequência de comprimento ℓ em $\mathbb{Z}_p$ contém uma subsequência $\mathcal{F}_\varphi$-zero e, no caso em que ℓ não exista, escrevemos $D(\varphi, \mathbb{Z}_p) = \infty$. Defina $M(\mathcal{F}_\varphi, \mathbb{Z}_p)$ como sendo o conjunto de todas as sequências de comprimento $D(\varphi, \mathbb{Z}_p) - 1$ livres de subsequências $\mathcal{F}_\varphi$-zero, quando $D(\varphi, \mathbb{Z}_p)$ é finito. Observe que, se $\varphi([0]^n) \neq 0$, então para cada natural k, a sequência $[0]^k$ é livre de subsequências $\mathcal{F}_\varphi$-zero, implicando em $D(\varphi, \mathbb{Z}_p) = \infty$. Se φ é um polinômio simétrico *linear* tal que $\varphi([0]^n) = 0$, então o Teorema 2.8 garante que

$$D(\varphi, \mathbb{Z}_p) = p \quad \text{e} \quad M(\mathcal{F}_\varphi, \mathbb{Z}_p) = \{[u]^{p-1} \,/\, u \in \mathbb{Z}_p, u \neq 0\}.$$

Nosso principal objetivo neste capítulo consiste em determinar o valor de $D(\varphi, \mathbb{Z}_p)$ e descrever o conjunto $M(\mathcal{F}_\varphi, \mathbb{Z}_p)$ para o caso em que φ é um polinômio simétrico quadrático com coeficientes em $\mathbb{Z}_p$, onde p é um primo.

2.3 O Valor da Constante $D(\varphi, \mathbb{Z}_p)$ para Polinômios Simétricos Quadráticos

Sejam n um inteiro maior ou igual a 2, p um primo ímpar e $\varphi \in \mathbb{Z}_p[x_1, x_2, \ldots, x_n]$ um polinômio quadrático com $\varphi([0]^n) = 0$. Então φ pode ser escrito da seguinte forma

$$\varphi(x_1, x_2, \ldots, x_n) = as_{n,1}^2 + bs_{n,2} + cs_{n,1},$$

onde $a, b, c \in \mathbb{Z}_p$. Agora, considere a família $\mathcal{F}_\varphi$ de todos os polinômios de mesmo grau e mesmos coeficientes que φ.

Para cada $k \in \mathbb{N}$, tome

$$\varphi_k = as_{k,1}^2 + bs_{k,2} + cs_{k,1} \in \mathbb{Z}_p[x_1, x_2, \ldots, x_k].$$

Observe que os únicos casos especiais em que φ_k não pertence a $\mathcal{F}_\varphi$ ocorrem quando $a = b = 0$, pois o grau de φ_k é menor que dois. Portanto, sendo $a \neq 0$ ou $b \neq 0$, temos que

$$\mathcal{F}_\varphi = \{as_{k,1}^2 + bs_{k,2} + cs_{k,1} \in \mathbb{Z}_p[x_1, x_2, \ldots, x_k] \ ; \ k \in \mathbb{N}\} = \{\varphi_k \ ; \ 1 \leq k \in \mathbb{Z}\}.$$

Observe que o caso em que $a = b = 0$ e $c \neq 0$ é consequência direta do Teorema 2.8, pois, neste caso, φ é um polinômio linear dependendo somente dos valores dos polinômios $s_{k,1}$, para $k \in \mathbb{N}$.

Agora, vamos estabelecer o resultado cuja demonstração é o objetivo desta seção:

Teorema 2.9. *Sejam $n \geq 2$ um inteiro, p um primo ímpar e seja $\varphi = as_{n,1}^2 + bs_{n,2} + cs_{n,1}$, onde $a, b, c \in \mathbb{Z}_p$, e $a \neq 0$ ou $b \neq 0$, um polinômio simétrico quadrático em $\mathbb{Z}_p[x_1, x_2, \ldots, x_n]$. Então são verdadeiras as seguintes afirmações:*

(i) Se $a = 0$ e $b \neq 0$, então $D(\varphi, \mathbb{Z}_p) = p$ e $M(\mathcal{F}_\varphi, \mathbb{Z}_p)$ é o conjunto de todas as sequências da forma

$$[u]^\alpha[-u - cb^{-1}]^{p-1-\alpha}, \text{ onde } u \in \mathbb{Z}_p \setminus \{0, -cb^{-1}\} \text{ e } 0 \leq \alpha \leq p-1,$$

ou da forma

$$[u]^{p-1}, \text{ quando } u = -cb^{-1} \text{ e } c \neq 0.$$

(ii) Se $a \neq 0$ e $b = c = 0$ então $D(\varphi, \mathbb{Z}_p) = p$ e $M(\mathcal{F}_\varphi, \mathbb{Z}_p)$ é o conjunto de todas as sequências da forma $[u]^{p-1}$, onde $u \in \mathbb{Z}_p \setminus \{0\}$.

(iii) Se $a \neq 0$, $b = 0$ e $c \neq 0$ então $D(\varphi, \mathbb{Z}_p) = p - 1$ e $M(\mathcal{F}_\varphi, \mathbb{Z}_p) = \{[ca^{-1}]^{p-2}\}$.

(iv) Se $a \cdot b \neq 0$, então $D(\varphi, \mathbb{Z}_p) \leq 2p - 1$ e:

(a) $D(\varphi, \mathbb{Z}_p) \geq p - 2$, para $c \neq 0$.

(b) $D(\varphi, \mathbb{Z}_p) \geq \overline{-ba^{-1}}$, para $c = 0$, onde $\overline{x}$ representa o menor inteiro não negativo pertencente à classe $x \in \mathbb{Z}_p$.

Para demonstrar este teorema serão necessários os seguintes resultados auxiliares:

Proposição 2.10. *Sejam p um primo e o inteiro ℓ satisfazendo $p/2 < \ell < p$. Se T é uma sequência de comprimento ℓ que é livre de subsequências de soma-zero em $\mathbb{Z}_p$, então T contém um elemento não nulo de multiplicidade no mínimo*

$$2\ell - p + 1, \quad se \quad (2p-2)/3 \leq \ell < p,$$

e no mínimo

$$\ell - \lfloor (p-1)/3 \rfloor, \quad se \quad p/2 < \ell \leq (2p-2)/3,$$

onde $\lfloor x \rfloor$ indica o maior inteiro menor que x.

Esta proposição foi demonstrada em 2007 por Savchev e Chen em [42] (Proposição 12). Além desta proposição, precisaremos também do teorema:

Teorema 2.11. *Sejam os inteiros positivos m e n tais que m divide n. Então, dado o grupo $G = \mathbb{Z}_m \oplus \mathbb{Z}_n$, temos*

$$D(G) = m + n - 1.$$

Já vimos que, em 1968, J. Olson demosntrou o teorema anterior em [39], entre outros resultados para a Constante de Davenport para p-grupos (ver também [38]).

Dada uma sequência T de elementos de $\mathbb{Z}_p$, em todo o nosso estudo usaremos que $\Sigma(T)$ representa o conjunto de todas as possíveis somas das subsequências de T. Por exemplo, seja $T = (u, v, w)$ em $\mathbb{Z}_p$, então

$$\Sigma(T) = \{u\,,\, v\,,\, w\,,\, (u+v)\,,\, (u+w)\,,\, (v+w)\,,\, (u+v+w)\}.$$

Agora vamos à demonstração do nosso resultado principal.

Demonstração. (Teorema 2.9)

(i) Como $a = 0$ e $b \neq 0$, então os polinômios pertencentes à $\mathcal{F}_\varphi$ são da forma $\varphi_k = bs_{k,2} + cs_{k,1}$, onde $k \in \mathbb{N}$, ou seja,

$$\varphi_k(x_1, x_2, \ldots, x_k) = \sum_{i=1}^{k} (bx_i^2 + cx_i),$$

para todo $k \in \mathbb{N}$.

Dada a sequência $T = (u_1, u_2, \ldots, u_k)$, é claro que $\varphi_k(T) = 0$ se, e somente se, a sequência

$$V = (f(u_1), f(u_2), \ldots, f(u_k))$$

tem soma zero, onde $f(x) = bx^2 + cx$, para todo $x \in \mathbb{Z}_p$. Logo, o Teorema 2.8 nos garante que $D(\varphi, \mathbb{Z}_p) = p$. Além disso, juntamente com a afirmação de que

$$f(u) = f(v) \quad \Leftrightarrow \quad v = u \quad \text{ou} \quad v = -u - cb^{-1},$$

para quaisquer $u, v \in \mathbb{Z}_p$, o teorema também garante que o conjunto $M(\mathcal{F}_\varphi, \mathbb{Z}_p)$ tem a forma desejada.

(ii) Para $a \neq 0$ e $b = c = 0$, então os polinômios de $\mathcal{F}_\varphi$ possuem a forma $\varphi_k = as_{k,1}^2$, onde $k \in \mathbb{N}$. Pelo Teorema 2.8, é fácil concluirmos que $D(\varphi, \mathbb{Z}_p) = p$ e $M(\mathcal{F}_\varphi, \mathbb{Z}_p) = \{[u]^{p-1} \ ; \ u \in \mathbb{Z}_p \setminus \{0\}\}$.

(iii) Neste caso, sendo $a \cdot c \neq 0$ e $b = 0$, então os polinômios de $\mathcal{F}_\varphi$ possuem a forma

$$\varphi_k = as_{k,1}^2 + cs_{k,1} = s_{k,1}(as_{k,1} + c),$$

para todo $k \in \mathbb{N}$. Logo φ_k só é zero quando $s_{k,1} \in \{0, -ca^{-1}\}$. O Teorema 2.8 nos diz que $D(\varphi, \mathbb{Z}_p) \leq p$ e que as sequências de tamanho $p-1$ livres de subsequências $\mathcal{F}_\varphi$-zero são da forma $S = [s]^{p-1}$, para $s \in \mathbb{Z}_p \setminus \{0\}$. Por outro lado, o conjunto de todas as possíveis somas de uma subsequência de S é dado por

$$\Sigma(S) = \{s, 2s, 3s, \ldots, (p-1)s\} = \mathbb{Z}_p \setminus \{0\},$$

ou seja, $-ca^{-1} \in \Sigma(S)$. Portanto, $D(\varphi, \mathbb{Z}_p) \leq p - 1$.

Vamos agora construir o conjunto M de todas as sequências em $\mathbb{Z}_p$ de tamanho $p-2$ e livres de subsequências cujas somas sejam iguais a zero ou a $-ca^{-1}$. Observe que, neste ponto, ainda não sabemos se este conjunto não é vazio. Para $p = 3$ fica fácil verificar que M não é vazio, logo $M = \{[ca^{-1}]\}$ e o teorema segue.

Se $p \geq 5$, pela Proposição 2.10 sabemos que, se a sequência U pertence ao conjunto M, então existe $u \in \mathbb{Z}_p$ não nulo tal que $U' = [u]^{p-3}$ é uma subsequência de U. Portanto,

$$0, (-ca^{-1}) \notin \Sigma(U') = \{u, 2u, 3u, \ldots, (p-3)u\},$$

pois U' é subsequência de $U \in M$. Com isso, sendo os elementos u e $-ca^{-1}$ não nulos, temos que

$$(p-1)u = -ca^{-1} \text{ ou } (p-2)u = -ca^{-1},$$

ou, equivalentemente,

$$u = ca^{-1} \quad \text{ou} \quad u = c(2a)^{-1}.$$

A sequência U é formada pela sequência U' acrescida de um único termo, ou seja, $U = [u]^{p-3}[v]$ para algum $v \in \mathbb{Z}_p$, $v \neq 0$. Como $\mathbb{Z}_p = \langle u \rangle$ (subgrupo aditivo cíclico), então $v = ku$, com $1 \leq k \leq p-1$, e temos

$$\Sigma(U) = \{u, 2u, \ldots, (p-3)u\} \cup \{(k+1)u, (k+2)u, \ldots, (k+p-3)u\},$$

Como nem 0 nem $-ca^{-1}$ são elementos de $\Sigma(U)$, então temos $k = 1$, ou seja, $U = [u]^{p-2}$, e

$$\Sigma(U) = \{u, 2u, \ldots, (p-2)u\}.$$

Além disso, se $u = c(2a)^{-1}$, então vemos que $(p-2)c(2a)^{-1} = -ca^{-1} \in \Sigma(U)$, contrariando a definição do conjunto M. Assim, a única possibilidade para U é a sequência $[ca^{-1}]^{p-2}$. Portanto, concluímos que $D(\varphi, \mathbb{Z}_p) = p-1$ and $M(\mathcal{F}_\varphi, \mathbb{Z}_p) = M = \{[ca^{-1}]^{p-2}\}$.

(iv) Vamos analisar inicialmente o limite superior para $D(\varphi, \mathbb{Z}_p)$. Tendo em vista o Teorema 2.11, vemos que $D(\mathbb{Z}_p \oplus \mathbb{Z}_p) = 2p-1$. Isto nos faz concluir que, dado uma sequência $T = (u_1, u_2, \ldots, u_{2p-1})$ em $\mathbb{Z}_p$, a sequência

$$T' = ((u_1, u_1^2), (u_2, u_2^2), \ldots, (u_{2p-1}, u_{2p-1}^2)) \text{ em } \mathbb{Z}_p \oplus \mathbb{Z}_p$$

possui uma subsequência

$$U = ((u_{i_1}, u_{i_1}^2), (u_{i_2}, u_{i_2}^2), \ldots, (u_{i_k}, u_{i_k}^2))$$

de comprimento k e $1 \leq i_1 < i_2 < \ldots < i_k \leq 2p-1$, tal que a soma dos elementos de U é igual ao elemento $(0,0) \in \mathbb{Z}_p \oplus \mathbb{Z}_p$. Com isso,

$$s_{k,1}(u_{i_1}, u_{i_2}, \ldots, u_{i_k}) = s_{k,2}(u_{i_1}, u_{i_2}, \ldots, u_{i_k}) = 0,$$

ou seja, a sequência T possui uma subsequência $\mathcal{F}_\varphi$-zero. Portanto, $D(\varphi, \mathbb{Z}_p) \leq 2p-1$.

(a) Para verificar este limite inferior basta encontrar uma sequência de tamanho no mínimo $p-3$ que seja livre de subsequências $\mathcal{F}_\varphi$-zero. Se $b \neq a$, tomamos a sequência $[u]^{p-2}$, onde $u = c(a-b)^{-1}$. Assim

$$\varphi_t([u]^t) = at^2u^2 + btu^2 + ctu = \frac{tac^2}{(a-b)^2}(t+1) \neq 0,$$

para qualquer $1 \leq t \leq p-2$. Se $b = a$, tomamos a sequência $[v]^{p-3}$, onde $v = ca^{-1}$. Assim

$$\varphi_k([v]^k) = ak^2v^2 + akv^2 + ckv = \frac{kc^2}{a}(k+2) \neq 0,$$

para qualquer $1 \leq k \leq p-3$. Estas sequências são da forma que queríamos.

(b) Seja $t = \overline{-ba^{-1}}$. Como $a \cdot b \neq 0$, então $1 \leq t \leq p-1$. No caso em que $b = -a$ e $c = 0$, observe que $\varphi_1 \notin \mathcal{F}_\varphi$, pois ele é o polinômio nulo. Então tome a sequência $[u]^{p-1}$, para $u \in \mathbb{Z}_p \setminus \{0\}$. Assim

$$\varphi_k([u]^k) = ak^2u^2 - aku^2 = aku^2(k-1) \neq 0,$$

para qualquer $2 \leq k \leq p-1$. Além disso, $p-1 \geq t-1$ como queríamos. Por fim, para o caso onde $b \neq -a$, então $t \geq 2$ e podemos tomar a sequência $[u]^{t-1}$, para $u \in \mathbb{Z}_p \setminus \{0\}$. Assim

$$\varphi_k([u]^k) = ak^2u^2 + bku^2 = aku^2(ak+b) \neq 0,$$

para qualquer $1 \leq k \leq t-1$. Estas sequências são livres de subsequências $\mathcal{F}_\varphi$-zero como queríamos.

Isto conclui a demonstração. □

Podemos observar que, acrescentando uma quantidade adequada de termos nulos às sequências, também podemos obter as cotas superiores para $D(\varphi, \mathbb{Z}_p)$ para os casos (i), (ii) e (iii) do Teorema 2.9 usando o Teorema 2.7 de Bialostocki e Luong.

2.4 Observações Finais

No item (ii)(b) do Teorema 2.9, o limitante inferior para $D(\varphi, \mathbb{Z}_p)$ pode ser muito bom, no caso em que $\overline{-ba^{-1}} = p-1$, mas pode, também, ser muito ruim, no caso em que

$\overline{-ba^{-1}} = 1$. Para que este limitante seja melhorado, deve-se analisar cada caso particular em separado.

Por outro lado, analisando o limitante superior para $D(\varphi, \mathbb{Z}_p)$, tivemos a falsa impressão de que ele fosse menor ou igual p. Neste processo, observamos algumas pequenas propriedades sobre os polinômios da família $\mathcal{F}_\varphi$, onde $\varphi \in \mathbb{Z}_p[x_1, x_2, \ldots, x_n]$ é um polinômio simétrico de grau dois, como, por exemplo,

$$\varphi_{k+1}(x_1, x_2, \ldots, x_k, x_{k+1}) = \varphi_k(x_1, x_2, \ldots, x_k) + \varphi_1(x_{k+1}) + 2x_{k+1}(x_1 + x_2 + \ldots + x_k).$$

No entanto, estas propriedades não foram suficientes para garantir que $D(\varphi, \mathbb{Z}_p) \leq p$. Com isso, passamos a procurar contra-exemplos para esta afirmação e conseguimos encontrá-los.

Considere o polinômio

$$\varphi = s_{n,1}^2 + s_{n,2} - s_{n,1} \in \mathbb{Z}_p[x_1, x_2, \ldots, x_n],$$

onde $n \geq 2$ é um inteiro e p é um primo tal que $p \equiv 7 \pmod 8$. Se $\mathcal{F}_\varphi$ é a familia dos polinômios da forma

$$\varphi_k = s_{k,1}^2 + s_{k,2} - s_{k,1} \in \mathbb{Z}_p[x_1, x_2, \ldots, x_k],$$

para todo $k \in \mathbb{N}$, então a sequência $[1]^{p-1}[-1][2]$ é livre de subsequências φ_k-zero para qualquer que seja $k \in \mathbb{N}$. De fato, observe que

$$\varphi_1(-1) = 3\,, \;\; \varphi_1(2) = 6 \;\text{ e }\; \varphi_2(2, -1) = 5$$

que são diferentes de zero, pois p é primo e $p \equiv 7 \pmod 8$. Para todo inteiro t tal que $1 \leq t \leq p - 1$, temos

$$\varphi_t([1]^t) = t^2 + t - t = t^2 \neq 0.$$

Além disso,

$$\varphi_{t+1}([1]^t[-1]) = (t-1)^2 + 2,$$

$$\varphi_{t+1}([1]^t[2]) = (t+2)^2 + 2,$$

$$\varphi_{t+2}([1]^t[-1][2]) = (t+1)^2 + 4.$$

Se algum destes valores pudesse ser nulo, deveríamos ter

$$\left(\frac{-2}{p}\right) = 1 \quad \text{ou} \quad \left(\frac{-4}{p}\right) = 1,$$

onde $\left(\frac{x}{p}\right)$ indica o Símbolo de Legendre de x módulo p. Mas, sendo $p \equiv 7 \pmod 8$, temos

$$\left(\frac{-1}{p}\right) = -1 \quad \text{e} \quad \left(\frac{2}{p}\right) = 1,$$

o que torna impossível a afirmação inicial. Por tudo isso, concluímos que a sequência $[1]^{p-1}[-1][2]$ é livre de subsequências φ_k-zero, para qualquer que seja $k \in \mathbb{N}$, ou seja, $D(\varphi, \mathbb{Z}_p) \geq p + 2$.

Referências Bibliográficas

[1] S. D. Adhikari, A. A. Ambily and B. Sury, *Zero-sum problems with subgroup weights*, Proc. Indian Acad. Sci. Math. Sci. **120** (3) (2010), 259–266.

[2] S.D. Adhikari, R. Balasubramanian, P. Rath, *Some combinatorial group invariants and their generalizations with weights*, Additive combinatorics, (Eds. Granville, Nathanson, Solymosi), 327–335, CRM, Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, (2007).

[3] S.D. Adhikari, R. Balasubramanian, F. Pappalardi, P. Rath, *Some zero-sum constants with weights*, Proc. Indian Acad. Sci. (Math. Sci.) **118** (2008), 183–188.

[4] S.D. Adhikari, Y. G. Chen, *Davenport constant with weights and some related questions II*, J. Combin. Theory, Ser. A115(1) (2008), 178–184.

[5] S.D. Adhikari, Y. G. Chen, J.B. Friedlander, S.V. Konyagin, F. Pappalardi, *Contributions to zero-sum problems*, Discrete Math. **306** (2006), 1–10.

[6] S.D. Adhikari, C. David, J. J. Urroz, *Generalizations of some zero-sum theorems*, Integers Electron Comb. Number Theory **8** (2008), A52.

[7] S. D. Adhikari, D. J. Grynkiewicz and Z.-W. Sun, *On weighted zero-sum sequences*, Adv. in Appl. Math. **48** (2012), 506–527.

[8] S.D. Adhikari, P. Rath, *Davenport constant with weights and some related questions*, Integers **6** (2006), A30, 6 pp.

[9] S.D. Adhikari, P. Rath, *Remarks on some zero-sum theorems*, Proc. Indian Acad. Sci. (Math. Sci.), **119** (3) (2009), 275–281.

[10] A. Bialostocki and T. Luong, *An Analogue of the Erdös-Ginzburg-Ziv Theorem for Quadratic Symmetric Polynomials,* Integers **9** (2009), Paper A36, 459-465.

[11] Y. Caro, *Zero-sum problems - a survey*, Discrete Math. **152** (1-3) (1996), 93–113.

[12] M.N. Chintamani, B.K. Moriya, W.D. Gao, P. Paul, R. Thangadurai, *New upper bounds for the Davenport and for the Erdős–Ginzburg–Ziv constants*, Arch. Math. (Basel) **98** (2012), 133–142.

[13] M. N. Chintamani and P. Paul, *On some weighted zero-sum constants*, Int. J. Number Theory **13**(2) (2017), 301–308.

[14] M. N. Chintamani and P. Paul, *On some weighted zero-sum constants II*, Int. J. Number Theory **14**(2) (2018), 383–397.

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

[16] Y. Edel, C. Elsholtz, A. Geroldinger, S. Kubertin, L. Rackham, *Zero-sum problems in finite abelian groups and affine caps*, Quart. J. Math. 58 (2007), 159–186.

[17] Y. Edel, *Sequences in abelian groups G of odd order without zero-sum subsequences of length exp(G)*, Des. Codes Cryptogr. **47** (2008), 125–134.

[18] P. Erdös, A. Ginzburg and A. Ziv, *Theorem in Additive Number Theory,* Bull. Res. Council Israel **10F** (1961), 41–43.

[19] B. Fine and G. Rosenberger, *The Fundamental Theorem of Algebra,* 1st ed., Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1997.

[20] W. D. Gao, *On zero-sum subsequences of restricted size. II*, Discrete Math. **271** (1-3) (2003), 51–59.

[21] W. D. Gao, A. Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math. **24** (2006), 337–369.

[22] W. D. Gao, A. Geroldinger, W. A. Schmid, *Inverse zero-sum problems*, Acta Arith. **128** (2007), 245–279.

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

[24] W. D. Gao, R. Thangadurai, *A variant of Kemnitz conjecture*, J. Combin. Theory Ser. A **107** (2004), 69–86.

[25] A. Geroldinger, F. Halter-Koch, *Non-Unique Factorizations: Algebraic, Combinatorial and Analytic Theory,* volume 278 of Pure and Applied Mathematics. Chapman & Hall/CRC; 2006.

[26] H. Godinho, A. Lemos, D. Marques, *Weighted zero-sum problems over* C_r^3, Algebra Discrete Math. **15** (2013), 201–212.

[27] S. Griffiths, *The Erdös-Ginzberg-Ziv theorem with units,* Discrete Math. **308** (23) (2008), 5473–5484.

[28] D. J. Grynkiewicz, *A weighted Erdös-Ginzburg-Ziv Theorem*, Combinatorica **26** (4) (2006), 445–453.

[29] D. J. Grynkiewicz, L. E. Marchan and O. Ordaz, *A Weighted Generalization of Two Theorems of Gao*, Ramanujan J. **28** (2012), 323–340.

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

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

[32] A. Lemos, *Problemas de Soma Zero com Peso sobre Grupos Abelianos Finitos*, Tese de Doutorado, UnB, 2010.

[33] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press (Cambridge, 1997), xiv+755 pp.

[34] F. Luca, *A generalization of a classical zero-sum problem*, Discrete Math. **307** (13) (2007), 1672-1678.

[35] L.E. Marchan, O. Ordaz, I. Santos, W. A. Schmid, *Multi-wise and constrained fully weighted Davenport constants and interactions with coding theory*, J. Comb. Theory Ser. A **135** (2015), 237–267.

[36] L. E. Marchan, O. Ordaz, D. Ramos, and W. Schmid, *Inverse results for weighted Harborth constants*, Int. J. Number Theory **12** (2016), no. 7, 1845–1861.

[37] B. K. Moriya, *On weighted zero sum subsequences of short length*, Integers **14** (2014), A21, 1–8.

[38] J. E. Olson, *A combinatorial problem on finite abelian groups I*, Jornal of Number Theory **1** (1969), 8–10.

[39] J. E. Olson, *A combinatorial problem on finite abelian groups II*, Jornal of Number Theory **1** (1969), 195–199.

[40] A. Potechin, *Maximal caps in* AG$(6, 3)$, Des. Codes Cryptogr. **46** (2008), 243–259.

[41] C. Reiher, *On Kemnitz' conjecture concerning lattice points in the plane*, Ramanujan J. **13** (2007), 333–337.

[42] S. Savchev, F. Chen, *Long Zero-Free Sequences in Finite Cyclic Groups*, Discrete Math. **307** (2007), 2671-2679.

[43] R. Thangadurai, *A variant of Davenport's constant*, Proc. Indian Acad. Sci. (Math. Sci.) **117** (2007), 147–158.

[44] P. Yuan, X. Zeng. *Davenport constant with weights*, European J. Combin. **31** (2010), 677–680.

[45] T. Yuster, B. Peterson, *A generalization of an addition theorem for solvable groups*, Canad. J. Math. **36** (1984), no. 3, 529–536.

[46] X. Xia. *Two generalized constants related to zero-sum problems for two special sets*, Integers Electron Comb. Number Theory **7** (2007), A52.

[47] X. Xia, Z. Li. *Some Davenport constants with weights and Adhikari and Rath's conjecture*, Ars. Combin. **88** (2008), 83–95.