Universidade Federal de Uberlândia
Instituto de Matemática e Estatística
Curso de Graduação em Matemática

SEMIGRUPOS NUMÉRICOS E EQUAÇÕES DIOFANTINAS: UMA RELAÇÃO ENTRE ELEMENTOS GERADOS E QUANTIDADE DE SOLUÇÕES

Rodrigo Carneiro

Uberlândia - MG
2025

Rodrigo Carneiro

SEMIGRUPOS NUMÉRICOS E EQUAÇÕES DIOFANTINAS: UMA RELAÇÃO ENTRE ELEMENTOS GERADOS E QUANTIDADE DE SOLUÇÕES

Monografia apresentada ao Curso de Graduação em Matemática da Universidade Federal de Uberlândia, como parte dos requisitos para a obtenção de título de **BACHARELADO EM MATEMÁTICA**.

Área de concentração: Matemática

Linha de pesquisa: Álgebra

Orientador(a): Victor Gonzalo Lopez Neumann

Uberlândia - MG
2025

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

C289 Carneiro, Rodrigo, 2000-
2025 Semigrupos Numéricos e Equações Diofantinas [recurso eletrônico] : Uma relação entre elementos gerados e quantidade de soluções / Rodrigo Carneiro. - 2025.

Orientador: Victor Gonzalo Lopez Neumann.
Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Uberlândia, Graduação em Matemática.
Modo de acesso: Internet.
Inclui bibliografia.

1. Matemática. I. Neumann, Victor Gonzalo Lopez,1974-, (Orient.). II. Universidade Federal de Uberlândia. Graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Instituto de Matemática e Estatística
Av. João Naves de Àvila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: +55 (34) 3239-4158/4156/4126 - www.ime.ufu.br - ime@ufu.br

ATA DE DEFESA - GRADUAÇÃO

Curso de Graduação em:	Bacharelado em Matemática				
Defesa de:	Trabalho de Conclusão de Curso 2 (FAMAT 31804)				
Data:	17/09/2025	Hora de início:	9:00	Hora de encerramento:	10:30
Matrícula do Discente:	11821MAT007				
Nome do Discente:	Rodrigo Carneiro				
Título do Trabalho:	Semigrupos Numéricos e Equações Diofantinas: Uma relação entre elementos gerados e quantidade de soluções				
A carga horária curricular foi cumprida integralmente?	(X) Sim ( ) Não				

Reuniu-se na sala 1F119, Campus Santa Mônica, da Universidade Federal de Uberlândia, a Banca Examinadora, designada pelo Colegiado do Curso de Graduação em Matemática, composta pelos docentes: Victor Gonzalo Lopez Neumann (IME-UFU), como orientador, Alonso Sepúlveda Castellanos (IME-UFU) e Guilherme Chaud Tizziotti (IME-UFU).

Iniciando os trabalhos, o presidente da mesa, Victor Gonzalo Lopez Neumann, apresentou a Comissão Examinadora e o candidato, agradeceu a presença do público, e concedeu ao discente a palavra, para a exposição do seu trabalho. A duração da apresentação do discente e o tempo de arguição e resposta foram conforme as normas do curso.

A seguir o senhor presidente concedeu a palavra, pela ordem sucessivamente, aos examinadores, que passaram a arguir o candidato. Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, avaliou a apresentação oral e o trabalho escrito e atribuiu o resultado final, considerando o candidato:

Aprovado com nota 90

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Victor Gonzalo Lopez Neumann**, **Professor(a) do Magistério Superior**, em 24/09/2025, às 07:57, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Alonso Sepulveda Castellanos**, **Professor(a) do Magistério Superior**, em 24/09/2025, às 09:20, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Guilherme Chaud Tizziotti**, **Professor(a) do Magistério Superior**, em 24/09/2025, às 09:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6659393** e o código CRC **DF99A6D6**.

Referência: Processo nº 23117.062364/2025-38 SEI nº 6659393

Agradecimentos

Primeiramente, agradeço aos meus pais por todo o carinho e apoio proporcionado. Aos meus amigos que fiz durante essa trajetória, agradeço pelo companheirismo. Aos professores que tive ao longo de todos os anos, desde o ensino fundamental até o presente momento, agradeço à disponibilidade, à paixão de transferir conhecimento, aos bons momentos em sala de aula e, também aos momentos não tão agradáveis que proporcionaram amadurecimento e que, posteriormente, se tonaram momentos de diversão quando relembrados. À banca examinadora, pela disponibilidade de revisar e avaliar a base de conhecimento desenvolvida durante esse tempo. Aos programas de auxílio estudantil que contribuíram para o desenvolvimento de pesquisas científicas. Ao meu amigo, professor e orientador, Prof. Dr. Victor Gonzalo Lopez Neumann, a quem devo todas as pesquisas desenvolvidas durante a graduação, bem como todo o apoio acadêmico, dedicação e confiança em meu potencial, mesmo nos momentos mais desafiadores. É graças às vivências e convivências que sou quem sou hoje, tanto no aspecto intelectual quanto no pessoal.

Resumo

Esse trabalho apresenta uma introdução à Teoria de Números a partir de Equações Diofantinas e, posteriormente, ao estudo de Semigrupos Numéricos associados à essas equações. Inicialmente, desenvolvemos resultados fundamentais sobre equações diofantinas e semigrupos numéricos, permitindo a caracterização de alguns Semigrupos Numéricos, em particular, com dimensão de imersão máxima, com a propriedade Arf, saturados e irredutíveis. Esses resultados podem ser importantes em uma tentativa futura de solucionar o problema de encontrar o número de Frobenius para semigrupos gerados por três elementos e, em especial, formalizar um princípio de contagem para a quantidade de soluções de equações com três variáveis. Ademais, será desenvolvido um resultado autoral que conta a quantidade de soluções de uma equação com duas variáveis, o qual será comparado com outros resultados já conhecidos e sugere-se sua extensão para três variáveis, otimizando algoritmos existentes em casos particulares.

Palavras-chave: Equações Diofantinas Lineares, Semigrupos Numéricos, Caracterização de Semigrupos, Número de Frobenius, Contagem de Soluções.

Abstract

This work presents an introduction to Number Theory from the perspective of Diophantine Equations and, subsequently, to the study of Numerical Semigroups associated with these equations. Initially, we develop fundamental results on Diophantine equations and numerical semigroups, allowing the characterization of some Numerical Semigroups, in particular, those with maximal embedding dimension, with the Arf property, saturated, and irreducible. These results may be relevant in a future attempt to solve the problem of finding the Frobenius number for semigroups generated by three elements and, in particular, to formalize a counting principle for the number of solutions of equations with three variables. Furthermore, an original result will be developed that counts the number of solutions of an equation with two variables, which will be compared with other known results, and its extension to three variables is suggested, optimizing existing algorithms in particular cases.

Keywords: Linear Diophantine Equations, Numerical Semigroups, Characterization of Semigroups, Frobenius Number, Counting Solutions.

Sumário

Introdução

Considere uma estrada que liga, exclusivamente, duas cidades A e B. Suponha, adicionalmente, que existem outras diversas estradas que ligam A e B a um determinado ponto da estrada que liga as duas. Independente da estrada escolhida, no fim, estaríamos na única estrada que liga ambas cidades e, se continuássemos a trajetória em sentido único, eventualmente chegaríamos na outra cidade. Se o objetivo é chegar na outra cidade, independente do tempo tomado, é possível tomar infinitos caminhos distintos. De forma análoga, na matemática definimos um objetivo e podemos adotar diferentes abordagens para atingi-lo. Ainda que o percurso varie, em extensão ou complexidade, se o caminho escolhido fizer parte das rotas possíveis, eventualmente ele conduzirá ao resultado pretendido.

Desde os primórdios, grandes questões têm instigado pesquisadores: compreender a natureza dos números, desenvolver métodos para resolver equações e estudar as propriedades das operações. Matemáticos como Diofanto de Alexandria buscaram sistematizar as soluções inteiras de equações, originando o que hoje conhecemos como Equações Diofantinas. Séculos mais tarde, problemas aparentemente simples, como determinar quais números podem ser obtidos por combinações de valores específicos, conduziram ao estudo dos conjuntos que atualmente chamamos de Semigrupos Numéricos.

Embora cada um desses temas tenha se desenvolvido de forma independente, ambos compartilham a essência de investigar quais números pertencem a conjuntos definidos por restrições algébricas. Mesmo que a equivalência entre ambos seja construída de forma natural, a partir do momento que restringimos ainda mais essas ideias, a construção, formalização, estudo e relação entre esses resultados se estreitam de forma rigorosa.

Neste trabalho, abordaremos a temática principal: a contagem da quantidade de soluções inteiras não negativas de equações diofantinas com três variáveis, utilizando conceitos de Teoria dos Números e de Semigrupos Numéricos. Para tanto, será necessário apresentar previamente os fundamentos e definições relacionados aos semigrupos, de modo a integrá-los adequadamente à análise das equações e possibilitar a aplicação de suas propriedades na resolução e caracterização das mesmas. Vale ressaltar que estabelecer um princípio de contagem de soluções não necessita do estudo de Semigrupos Numéricos. No entanto,

Semigrupos Numéricos podem ser uma ferramenta necessária para obter tal resultado sem utilizar os raciocínios que serão apresentados no último capítulo.

Motivação

Definição 0.0.1. *Chamamos de números naturais os números que pertencem ao conjunto* $\{1, 2, 3, \dots\}$.

Observação 0.0.2. *Denotemos por* $\mathbb{N}$ *o conjunto dos números inteiros positivos, também chamado de números naturais.*

Imagine que queremos contar a quantidade de soluções de uma equação da forma $ax + by = d$, em que $a, b, d \in \mathbb{N}$ e queremos soluções $x, y \in \mathbb{N}$. Existe uma série de estudos por trás dessas equações mas, em particular, vamos tomar como exemplo a seguinte equação:

$$3x + 5y = 60.$$

Pelas propriedades de divisibilidade, sabemos que para um número ser múltiplo de 5, precisamos que o número termine com 0 ou 5. Portanto, analisaremos os valores que y assume a partir da variação de x, ou seja, $5y = 60 - 3x$. Note que $y = 12$ e $x = 0$ é uma solução e, o próximo valor de x que faz com que $y \in \mathbb{N}$ será $x = 5$, ou melhor, $x = 5t$, $t \in \mathbb{N}$. Portanto, temos:

$$\begin{aligned} x = 0 &\quad \to y = 12, \\ x = 5 &\quad \to y = 9, \\ x = 10 &\quad \to y = 6, \\ x = 15 &\quad \to y = 3, \\ x = 20 &\quad \to y = 0. \end{aligned}$$

Em outras palavras, temos exatamente 5 soluções distintas para o problema analisado. Observe que a cada 15 unidades, temos uma solução. Então, podemos contar a quantidade de soluções dessa equação da seguinte forma, $3x + 5y = 60 - 15n$, em que n é o maior inteiro tal que $60 - 15n \geq 0$. Mas, dessa forma, $n = 4$ e temos 5 soluções, portanto, precisamos garantir que $3x + 5y = 0$ possui solução. Em caso positivo, a quantidade de soluções é $n + 1$, em caso negativo, n. De fato, se queremos contar $3x + 5y = 61$, teremos exatamente 4 soluções, já que $3x + 5y = 1$ não possui solução e cujas soluções seriam:

$$\begin{aligned} x = 2 &\quad \to y = 11, \\ x = 7 &\quad \to y = 8, \\ x = 12 &\quad \to y = 5, \\ x = 17 &\quad \to y = 2. \end{aligned}$$

Podemos, ainda, incrementar essa análise. Note que o número 15 não é aleatório. Quando percorremos 15 unidades, incrementamos 5 nos valores de x e reduzimos 3 nos valores de y e isso se dá ao fato de que 15 é mínimo múltiplo comum de 3 e 5 ou, simbolicamente, $\mathrm{mmc}(a, b) = 15$, assim, podemos analisar a quantidade de soluções de qualquer equação diofantina linear com soluções naturais. O que nos levou a

desenvolver o seguinte resultado.

Sejam a e b inteiros positivos e c um inteiro não negativo múltiplo do máximo divisor comum de a e b, simbolicamente, $\mathrm{mdc}(a, b) \mid c$. Seja n o maior inteiro não negativo tal que $c - n \cdot \mathrm{mmc}(a, b) \geq 0$. Então o número de soluções inteiras não negativas N da equação $ax + by = c$ será

$$N = \begin{cases} n + 1, & \text{se } ax + by = c - n \cdot \mathrm{mmc}(a, b) \text{ possui solução em inteiros não negativos;} \\ n, & \text{caso contrário.} \end{cases}$$

Agora, com uma fórmula fechada para encontrar a quantidade de soluções de uma equação diofantina com duas variáveis, podemos verificar, ou melhor, podemos tentar obter uma fórmula fechada para a quantidade de soluções para uma equação do tipo $ax + by + cz = d$.

CAPÍTULO 1

Noções Preliminares

Iniciaremos essa seção apresentando os resultados que nos levaram ao estudo dos Semigrupos Numéricos e seus conceitos iniciais. Passaremos pelo que chamamos de Equações Diofantinas e apresentaremos alguns resultados importantes de Teoria de Números.

1.1 Equações Diofantinas

Equações diofantinas são equações polinomias de duas ou mais variáveis para as quais procuram-se soluções inteiras ou racionais. Tal nome se dá em homenagem ao matemático Diofanto de Alexandria, que acredita-se ter sido o primeiro a estudar tais equações. Nos atentaremos a estudar, especificamente, as soluções, em inteiros não negativos, das equações da forma $ax + by = c$, em que a, b e c são números inteiros, as quais são chamadas de equações diofantinas lineares. Vamos nos restringir ao caso em que a, b e c são positivos.

Proposição 1.1.1. *Sejam a e b números naturais, então* $\mathrm{mdc}(a, b) \cdot \mathrm{mmc}(a, b) = ab$.

Demonstração. Sejam $d = \mathrm{mdc}(a, b)$, $a = a_1 d$ e $b = b_1 d$ em que $a_1, b_1 \in \mathbb{Z}$ e $\mathrm{mdc}(a_1, b_1) = 1$. Temos $\mathrm{mmc}(a, b) = ax$ para algum $x \in \mathbb{Z}$. Como $b \mid \mathrm{mmc}(a, b)$, então $b_1 d \mid a_1 dx \iff b_1 \mid a_1 x \iff b_1 \mid x$ já que a_1, b_1 são primos entre si. Por definição de mínimo múltiplo comum, x deve ser o menor número divisível por b_1, portanto, $x = b_1$. Daí, $\mathrm{mdc}(a, b) \cdot \mathrm{mmc}(a, b) = d \cdot ax = d \cdot ab_1 = a \cdot b_1 = ab$. ■

1.2 Soluções das equações diofantinas lineares

Lembremos que estamos interessados em soluções inteiras não negativas. A existência da solução de uma equação diofantina linear é uma consequência direta do próximo teorema.

Teorema 1.2.1 (Bachet-Bézout)**.** *Sejam $a, b \in \mathbb{Z}^*$, então existem inteiros $x, y \in \mathbb{Z}$ tal que $ax + by = \mathrm{mdc}(a, b)$.*

Demonstração. Ver [3, Teorema 1.7]. ■

Corolário 1.2.2. *Sejam a,b e c inteiros. A equação $ax + by = c$ possui solução se, e somente se, $\mathrm{mdc}(a, b) \mid c$.*

Demonstração. Ver [2, Corolário 1.8]. ■

Teorema 1.2.3. *Considere uma equação diofantina $ax + by = c$, com $a \neq 0$, $b \neq 0$ e $\mathrm{mdc}(a, b) = 1$. Seja (x_0, y_0) uma solução particular da equação diofantina. Para todo inteiro t, o par*

$$(x, y) = (x_0 + bt, y_0 - at) \tag{1.1}$$

é solução da equação diofantina e toda solução pode ser escrita dessa forma.

Demonstração. Como (x_0, y_0) é uma solução particular da equação diofantina, então $ax_0 + by_0 = c$. Por outro lado, se (x, y) é uma solução de $ax + by = c$, então $ax + by = ax_0 + by_0$. Daí,

$$a(x - x_0) = b(y_0 - y). \tag{1.2}$$

Como $\mathrm{mdc}(a, b) = 1$, então $a \mid (y_0 - y)$, logo existe um inteiro t, tal que $at = y_0 - y$, o que implica $y = y_0 - at$. Substituindo $y_0 - y = at$ em (1.2), obtemos o resultado desejado

$$(x, y) = (x_0 + bt, y_0 - at).$$

■

Proposição 1.2.4. *Sejam a, b naturais e $\mathrm{mdc}(a, b) = 1$. Então não existem inteiros não negativos x e y tais que $ax + by = ab - a - b$.*

Demonstração. Note que

$$ab - a - b = a(-1) + b(a - 1).$$

Então $x = -1$ e $y = a - 1$ é uma solução de $ax + by = ab - a - b$. Pelo *Teorema* 1.2.3 podemos escrever as soluções da seguinte forma:

$$x = -1 + bt, \quad y = a - 1 - at, \quad \text{com } t \in \mathbb{Z}.$$

Para que $x > 0$, temos que escolher um valor de t positivo. Mas, se $t > 0$, temos que $1 - t \leq 0$ e então $y = a - 1 - at = a(1 - t) - 1 \leq -1$. Ou seja, tentar obter um valor de t para que x seja não negativo faz com que y seja negativo. Conclui-se que é impossível achar uma solução não negativa para $ax + by = ab - a - b$. ■

Proposição 1.2.5. *Assumindo $a > 1$ e $b > 1$ e $\mathrm{mdc}(a, b) = 1$. Se $n \geq ab - a - b + 1$, então existem inteiros x e y não negativos tais que $ax + by = n$.*

Demonstração. Pelo *Teorema* 1.2.1 existe um par de inteiros (x_0, y_0) tal que $ax_0 + by_0 = n$ e todas as soluções dessa equação diofantina se escrevem na forma

$$x = x_0 + bt, \quad y = y_0 - at, \quad \text{com } t \in \mathbb{Z}.$$

Pelo Algoritmo da Divisão Euclidiana, existem inteiros t_1 e y_1, tais que

$$y_0 = at_1 + y_1 \quad \text{e} \quad 0 \leq y_1 < a.$$

Como $y_1 = y_0 - at_1$ então, escolhendo $x_1 = x_0 + bt_1$, o par (x_1, y_1) é solução da equação $ax + by = n$. Suponha, por absurdo, que $x_1 \leq -1$. Nesse caso, como $a > 1$, $b > 1$ e $y_1 \leq a - 1$, temos

$$n = ax_1 + by_1 \leq a(-1) + b(a - 1) = ab - a - b.$$

Mas, por hipótese, $n \geq ab - a - b + 1$. Logo (x_1, y_1) é uma solução não negativa. ■

1.3 Número de soluções não negativas de uma equação diofantina linear

Dados inteiros não negativos a, b e c, é possível encontrar a quantidade de soluções inteiras não negativas da equação $ax + by = c$ fazendo uma simples análise da solução dada em (1.1). Em outras palavras, deve-se calcular o número de valores possíveis de $t \in \mathbb{Z}$ que satisfazem $x_0 + bt \geq 0$ e $y_0 - at \geq 0$. No entanto, é possível encontrar o número de soluções de forma mais simples e rápida.

Teorema 1.3.1. *Sejam a e b inteiros positivos e c um inteiro não negativo múltiplo de $\mathrm{mdc}(a, b)$. Considere n o maior inteiro não negativo tal que $c - n \cdot \mathrm{mmc}(a, b) \geq 0$. Então o número de soluções inteiras não negativas N da equação $ax + by = c$ será*

$$N = \begin{cases} n + 1, & \text{se } ax + by = c - n \cdot \mathrm{mmc}(a, b) \text{ possui solução em inteiros não negativos;} \\ n, & \text{caso contrário.} \end{cases}$$

Demonstração. Denotemos $d = \mathrm{mdc}(a, b)$ e $m = \mathrm{mmc}(a, b)$ e $ab = dm$ pela Proposição 1.1.1. Suponha, inicialmente, que $c < m$. Provemos que $ax + by = c$ possui no máximo uma solução em inteiros não

negativos. Seja (x_0, y_0) uma solução em inteiros não negativos. Observe que $x_0 \leq \frac{c}{a} < \frac{m}{a} = \frac{b}{d}$ e $y_0 \leq \frac{c}{b} < \frac{m}{b} = \frac{a}{d}$. Veja também que (x_0, y_0) é solução de $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$ e pelo Teorema 1.2.1 as soluções são da forma

$$(x, y) = (x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t), \quad \text{para } t \in \mathbb{Z}. \tag{1.3}$$

Se $t \geq 1$, então $y \leq y_0 - \frac{a}{d} < \frac{a}{d} - \frac{a}{d} < 0$ e se $t \leq -1$, então $x \leq x_0 - \frac{b}{d} < \frac{b}{d} - \frac{b}{d} = 0$. Isso prova que $ax + by = c$ possui no máximo uma solução em inteiros não negativos, nesse caso.

Se $c < m$ e $ax + by = c$ não possui soluções em inteiros não negativos, então $ax + by = c + m$ possui uma solução. De fato, essa equação é equivalente à equação $\frac{a}{d}x + \frac{b}{d}y = \frac{c+m}{d}$. Como $\text{mdc}(\frac{a}{d}, \frac{b}{d}) = 1$, pela Proposição 1.2.5, $\frac{a}{d}x + \frac{b}{d}y = \frac{c+m}{d}$ possui solução em inteiros não negativos, já que $\frac{c+m}{d} > \frac{m}{d} = \frac{ab}{d^2} > \frac{a}{d} \cdot \frac{b}{d} - \frac{a}{d} - \frac{b}{d}$. Suponha que $ax + by = c + m$ possui duas soluções. Essas soluções em inteiros não negativos seriam da forma (x_0, y_0), $(x_0 + \frac{b}{d}, y_0 - \frac{a}{d})$. Nesse caso o par $(x_0, y_0 - \frac{a}{d})$ seria solução de $ax + by = c$, o que contradiz a hipótese. Portanto $ax + by = c + m$ possui exatamente uma solução em inteiros não negativos.

Considere, agora, que $ax + by = c$ possui N soluções, sendo (x_0, y_0) a solução não negativa com o menor valor possível de x_0. Dessa forma, por (1.3), as soluções não negativas são da forma

$$(x_0, y_0), (x_0 + \frac{b}{d}, y_0 - \frac{a}{d}), \ldots, (x_0 + (N-1)\frac{b}{d}, y_0 - (N-1)\frac{a}{d}),$$

com $x_0 - \frac{b}{d} < 0$ e $y_0 - N\frac{a}{d} < 0$. Provemos que $ax + by = c + m$ tem uma solução a mais. As soluções em inteiros não negativos de $ax + by = c + m$ são

$$(x_0, y_0 + \frac{a}{d}), (x_0 + \frac{b}{d}, y_0), \ldots, (x_0 + N\frac{b}{d}, y_0 - (N-1)\frac{a}{d}).$$

Como $x_0 - \frac{b}{d} < 0$ e $y_0 - N\frac{a}{d} < 0$, essas são as únicas $N + 1$ soluções de $ax + by = c + m$.

As afirmações acima provam o resultado, já que se $ax + by = c - nm$ não possui soluções em inteiros não negativos, então $ax + by = c - nm + m$ possui uma solução, $ax + by = c - nm + 2m$ possui duas soluções e assim por diante, $ax + by = c$ possui n soluções. Agora, se $ax + by = c - nm$ possui uma solução, então $ax + by = c - nm + m$ possui duas soluções e assim por diante, $ax + by = c$ possui $n + 1$ soluções. ■

O problema de encontrar uma solução particular de uma equação diofantina se dá quando os valores de a e b são suficientemente grandes, criando diversos números que não podem ser escritos como a combinação linear de ambos. No entanto, com esse Teorema, conseguimos limitar a quantidade de soluções possíveis. Ademais, resolveremos uma equação muito mais simples que a inicial e, em muitos momentos, será possível verificar se há ou não solução de forma imediata. Note que apenas pelas suposições feitas na demonstração torna-se imediato que para alguns valores de c a equação possuirá a mesma quantidade de soluções e, com

isso, podemos agrupá-los por classes.

Exemplo 1.3.2. Qual a quantidade de soluções inteiras não negativas de $3x + 5y = 48$ e determine todos os valores de c para os quais a equação $3x + 5y = c$ possui exatamente 6 soluções inteiras não negativas.

Solução. Seguiremos os passos do Teorema para a resolução. Inicialmente procuramos o maior valor de n e resolver a equação a seguir:

$$3x + 5y = 48 - n \cdot \text{mmc}(3, 5) \quad | \quad 48 - n \cdot \text{mmc}(3, 5) \geq 0.$$

Daí, $n \leq 3$ e, portanto, a equação possui 3 ou 4 soluções. Precisamos verificar se $3x + 5y = 3$ possui solução inteira não negativa, o que, de forma imediata, possui. Logo, a equação $3x + 5y = 48$ possui exatamente 4 soluções inteiras não negativas. Pela Proposição 1.2.5, todo $c \geq 7 = 3 \cdot 5 - 3 - 5$ pode ser escrito como combinação linear de 3 e 5 e, como o número de soluções aumenta a cada intervalo de tamanho $\text{mmc}(3, 5)$ de valores possíveis de c, verificaremos para que valores de c entre 0 e 14 a equação possui ou não solução. Seja P o conjunto de valores de c para os quais a equação não possui solução. Temos

$$P = \{1, 2, 4, 7\}.$$

Assim, quando $c = p + 15 \cdot 6$, $p \in P$, teremos exatamente 6 soluções. Para os demais casos, quando $c = p_c + 15 \cdot 5$, $p_c \in P^c = \{0, 3, 5, 6, 8, 9, 10, 11, 12, 13, 14\}$. Logo, para $c = \{75, 78, 80, 81, 83, 84, 85, 86, 87, 88, 89, 91, 92, 94, 97\}$, a equação $3x + 5y = c$ terá 6 soluções inteiras não negativas. ■

A partir desse exemplo surgem os seguintes questionamentos: Esses resultados são mantidos para uma equação do tipo $ax + by + cz = d$? Se não são mantidos, é possível encontrar uma fórmula fechada para a quantidade de soluções? A quantidade de elementos nas classes será $\text{mmc}(a, b, c)$? Qual será o maior elementos que não pode ser escrito como combinação linear? A partir de agora, em busca de tais resultados, entraremos no vasto mundo dos Semigrupos Numéricos.

1.4 Semigrupos Numéricos

Os semigrupos numéricos possuem aplicações práticas em áreas como teoria da códigos, otimização e criptografia, oferecendo resultados significativos para modelar e resolver problemas envolvendo restrições lineares inteiras. Nos basearemos no livro [4] para todos os resultados sobre Semigrupos Numéricos.

Definição 1.4.1. *Um semigrupo é um par $(S, +)$, em que S é um conjunto não vazio e $+$ é uma operação binária sobre S que é associativa.*

Observação 1.4.2. *Todos os semigrupos considerados neste trabalho são comutativos ($a + b = b + a$ para todos $a, b \in S$). Por tal, evitaremos essa classificação e nos limitaremos, também, a escrever S, sem a operação binária.*

Definição 1.4.3. *Um subsemigrupo T de um semigrupo S é um subconjunto que é fechado sob a operação binária considerada em S.*

Definição 1.4.4. *Seja A um subsemigrupo, $a_1, \ldots, a_n \in A$. Dizemos que um subsemigrupo é gerado por $a_1, \ldots, a_n$ se para todo $x \in A$, x pode ser escrito como $a_1\lambda_1 + \cdots + a_n\lambda_n$, em que $\lambda_1, \ldots, \lambda_n \in \mathbb{N} \setminus \{0\}$.*

É claro que a interseção de subsemigrupos de um semigrupo S é novamente um subsemigrupo de S.

Definição 1.4.5. *Dado um subconjunto A não vazio de S, o menor subsemigrupo de S que contém A é a interseção de todos os subsemigrupos de S que contêm A. Denotamos esse semigrupo por $\langle A \rangle$, e o chamamos de subsemigrupo gerado por A.*

Definição 1.4.6. *Um semigrupo M é um monóide se possui um elemento neutro, ou seja, existe um elemento em M, denotado por 0, tal que $0 + a = a + 0 = a$ para todo $a \in M$.*

Definição 1.4.7. *Um subconjunto $N \subseteq M$ é um submonóide se for um subsemigrupo de M e contiver o elemento 0.*

Observação 1.4.8. *De maneira análoga aos semigrupos, a interseção de submonóides é também um submonóide.*

Definição 1.4.9. *Uma função $f : X \to Y$ entre dois semigrupos é um homomorfismo se $f(a + b) = f(a) + f(b)$ para todo $a, b \in X$. Se f for injetora, sobrejetora ou bijetora, dizemos que é um monomorfismo, epimorfismo ou isomorfismo, respectivamente. Essas definições se estendem para os monóides.*

O conjunto $\mathbb{N}$ com a operação de adição é um monóide. Estamos principalmente interessados nos submonóides de $\mathbb{N}$. Veremos a seguir que eles podem ser classificados, a menos de isomorfismo, por aqueles que possuem, ou não, complemento finito em $\mathbb{N}$.

Definição 1.4.10. *Um submonóide de $\mathbb{N}$ com complemento finito em $\mathbb{N}$ é chamado semigrupo numérico.*

Lema 1.4.11. *Para $A \subseteq \mathbb{N}$ não vazio, $\langle A \rangle$, o submonóide de $\mathbb{N}$ gerado por A, é um semigrupo numérico se, e somente se, o máximo divisor comum dos elementos de A é igual a 1.*

Demonstração. Seja $d = \mathrm{mdc}(A)$. Claramente, se $s \in \langle A \rangle$, então $d \mid s$. Como $\langle A \rangle$ é um semigrupo numérico, o complemento $\mathbb{N} \setminus \langle A \rangle$ é finito, e então existe $x \in \mathbb{N}$ tal que $d \mid x$ e $d \mid x + 1$, o que implica que

$d = 1$. Para o recíproco, basta mostrar que $\mathbb{N} \setminus \langle A \rangle$ é finito. Como $\mathrm{mdc}(A) = 1$, existem inteiros $z_1, \ldots, z_n$ e $a_1, \ldots, a_n \in A$ tais que $z_1 a_1 + \cdots + z_n a_n = 1$. Reagrupando os termos negativos do outro lado da igualdade, podemos escrever:

$$z_{i_1} a_{i_1} + \cdots + z_{i_k} a_{i_k} = 1 - z_{j_1} a_{j_1} - \cdots - z_{j_\ell} a_{j_\ell}$$

Assim, existe $s \in \langle A \rangle$ tal que $s + 1 \in \langle A \rangle$. Acabamos de encontrar, portanto, dois números primos entre si que estão no conjunto. Logo, pela Proposição 1.2.5, todo $n > s(s-1) - (s-1) - s$ também estará em $\langle A \rangle$. ■

Em particular, se a e b são inteiros positivos tais que $\mathrm{mdc}(a, b) = 1$, então o conjunto

$$S = \{ax + by \mid x, y \in \mathbb{N}\}$$

é um semigrupo numérico.

Proposição 1.4.12. *Seja M um submonóide não trivial de $\mathbb{N}$. Então M é isomorfo a um semigrupo numérico.*

Demonstração. Seja $d = \mathrm{mdc}(M)$. Defina $S = \{m/d \mid m \in M\}$. Como M é um submonoide de $\mathbb{N}$, então o submonóide gerado por S é o próprio S. Logo, pelo Lema 1.4.11, S é um semigrupo numérico. A função $f : M \to S$, definida por $f(m) = m/d$, é um isomorfismo de monóides. ■

Definição 1.4.13. *Se S é um submonóide de $\mathbb{N}$, denotamos por S^* o conjunto $S \setminus \{0\}$. O conjunto soma $S^* + S^*$ é o conjunto de todas as somas $x + y$, com $x, y \in S^*$.*

Lema 1.4.14. *Seja S um submonóide de $\mathbb{N}$. Então $S^* \setminus (S^* + S^*)$ é um sistema de geradores de S. Além disso, todo sistema de geradores de S contém $S^* \setminus (S^* + S^*)$.*

Demonstração. Seja s um elemento de S^*. Se $s \notin S^* \setminus (S^* + S^*)$, então existem $x, y \in S^*$ tais que $s = x + y$. Repetimos esse procedimento para x e y e, pelo princípio de Boa Ordem, após um número finito de passos, encontramos $s_1, \ldots, s_n \in S^* \setminus (S^* + S^*)$ tais que $s = s_1 + \cdots + s_n$. Isso prova que $S^* \setminus (S^* + S^*)$ é um sistema de geradores de S.

Agora, seja A um sistema de geradores de S. Tome $x \in S^* \setminus (S^* + S^*)$. Existem $\lambda_1, \ldots, \lambda_n \in \mathbb{N}$ e $a_1, \ldots, a_n \in A$ tais que $x = \lambda_1 a_1 + \cdots + \lambda_n a_n$. Como $x \notin S^* + S^*$, então $x = a_i$ para algum $i \in \{1, \ldots, n\}$. ■

Definição 1.4.15. *Seja S um semigrupo numérico e seja n um de seus elementos não nulos. O conjunto de Apéry de n em S é*

$$\mathrm{Ap}(S, n) = \{s \in S \mid s - n \notin S\}.$$

Lema 1.4.16. *Seja S um semigrupo numérico e seja n um elemento não nulo de S. Então*

$$\mathrm{Ap}(S, n) = \{0 = w(0), w(1), \ldots, w(n-1)\},$$

em que $w(i)$ é o menor elemento de S congruente com i módulo n, para todo $i \in \{0, \ldots, n-1\}$.

Demonstração. Para todo $i \in \{0, \ldots, n-1\}$ tem-se que $w(i) \equiv w(i) - n \equiv i \pmod{n}$. Por definição $w(i) \in S$ e $w(i) - n \notin S$, logo $w(i) \in \mathrm{Ap}(S, n)$. Provemos agora que todo $w \in \mathrm{Ap}(S, n)$ é da forma $w(i)$ para algum $i \in \{0, \ldots, n-1\}$. Pelo Algoritmo da Divisão Euclidiana, existem inteiros q, i tais que $w = qn + i$ e $0 \leq i < n$. Pela definiçaõ do conjunto de Apéry, $w - n = (q-1)n + i \notin S$. Em outras palavras, $w \equiv i \pmod{n}$, $w \in S$ e $w - n \notin S$. Isso implica que $w = w(i)$. ■

Observação 1.4.17. *Vale ressaltar que, os possíveis restos módulo n são $0, \ldots, n-1$, logo, a cardinalidade de $\mathrm{Ap}(S, n)$ é exatamente n. Por sua vez, podemos provar que S é o submonóide gerado por $\mathrm{Ap}(S, n) \cup \{n\}$.*

Como $\mathrm{Ap}(S, n) \cup \{n\} \subseteq S$, então $\langle \mathrm{Ap}(S, n) \cup \{n\} \rangle \subseteq S$. Por outro lado, se $s \in S$, então existe $i \in \{0, \ldots, n-1\}$ tal que $s \equiv i \pmod{n}$. Como $w(i)$ é o menor elemento de S congruente com i módulo n, então existe $q \geq 0$ tal que $s = w(i) + qn$. Em outras palavras, $s \in \langle \mathrm{Ap}(S, n) \cup \{n\} \rangle$.

Definição 1.4.18. *Dizemos que um sistema de geradores A de um semigrupo numérico é um sistema mínimo de geradores se não existe $B \subsetneq A$ que gere o semigrupo.*

1.5 Multiplicidade e dimensão de imersão

Teorema 1.5.1. *Todo semigrupo numérico admite um único sistema mínimo de geradores, em particular, esse sistema é finito.*

Demonstração. O Lema 1.4.14 afirma que $S^* \setminus (S^* + S^*)$ é o sistema mínimo de geradores de S. Por outro lado, para qualquer $n \in S$, $S = \langle \mathrm{Ap}(S, n) \cup \{n\} \rangle$. Como $\mathrm{Ap}(S, n) \cup \{n\}$ é finito, então $S^* \setminus (S^* + S^*)$ é finito. ■

Definição 1.5.2. *Seja S um semigrupo numérico com sistema mínimo de geradores $\{n_1 < n_2 < \cdots < n_p\}$. O elemento n_1 é chamado de multiplicidade de S, denotado por $m(S)$ e a cardinalidade do sistema mínimo de geradores p, é chamada de dimensão de imersão de S e será denotada por $e(S)$.*

Proposição 1.5.3. *Seja S um semigrupo numérico. Então:*

1. $m(S) = \min(S \setminus \{0\})$,
2. $e(S) \leq m(S)$.

Demonstração. O primeiro item segue diretamente da definição. A segunda afirmação decorre do fato de que $\{m(S)\} \cup \mathrm{Ap}(S, m(S)) \setminus \{0\}$ é um sistema de geradores de S com cardinalidade $m(S)$. ■

1.6 Número de Frobenius e gênero

Ferdinand George Frobenius foi um matemático alemão que propôs uma fórmula para encontrar o maior número inteiro não negativo que não é representado por uma combinação linear com coeficientes inteiros positivos, cujo máximo divisor comum é 1. Além disso, ele também procurou determinar quantos inteiros positivos não possuem tal representação.

Definição 1.6.1. *Seja S um semigrupo numérico. O maior inteiro que não pertence a S é conhecido como o número de Frobenius de S, denotado por $F(S)$.*

Vimos na Proposição 1.2.4, para $S = \langle a, b\rangle$, com a, b primos entre si, temos $F(S) = ab - a - b$.

Definição 1.6.2. *Seja S um semigrupo numérico. Definiremos por $G(S)$ o conjunto de todos os elementos que não podem ser escritos como combinação linear dos geradores de S e $g(S)$ sua cardinalidade, conhecida como gênero de S.*

Exemplo 1.6.3. Para $S = \langle 3, 5\rangle$, temos $F(S) = 7$, $G(S) = \{1, 2, 4, 7\}$ e $g(S) = 4$.

Proposição 1.6.4. *Seja S um semigrupo numérico e n um de seus elementos não nulos. Então*

(a) $\mathrm{F}(S) = \max(\mathrm{Ap}(S, n)) - n$.

(b) $\mathrm{g}(S) = \frac{1}{n}\big(\sum_{w\in \mathrm{Ap}(S,n)} w\big) - \frac{n-1}{2}$.

Demonstração. Pela definição do conjunto de Apéry, $\max(\mathrm{Ap}(S, n)) - n \notin S$. Assim, o número de Frobenius é maior ou igual a $\max(\mathrm{Ap}(S, n)) - n$. Se $x > \max(\mathrm{Ap}(S, n)) - n$, então $x + n > \max(\mathrm{Ap}(S, n))$. Isso implica que $x + n \notin \mathrm{Ap}(S, n)$ e, portanto $x \in S$. Dessa forma, o número de Frobenius deve ser menor ou igual a $\max(\mathrm{Ap}(S, n)) - n$. Isso prova que $\mathrm{F}(S) = \max(\mathrm{Ap}(S, n)) - n$. Pelo Lema 1.4.16, $\mathrm{Ap}(S, n) = \{0 = w(0), w(1), \ldots, w(n-1)\}$ e por definição, para todo $i \in \{0, \ldots, n-1\}$, $w(i) \equiv i \pmod n$. Logo, existe um inteiro não negativo k_i tal que $w(i) = k_i n + i$. Assim,

$$\mathrm{Ap}(S, n) = \{0, w(1) = k_1 n + 1, w(2) = k_2 n + 2, \ldots, w(n-1) = k_{n-1} n + n - 1\}.$$

Um inteiro x congruente com $w(i)$ módulo n pertence a S se, e somente se, $w(i) \leq x$. Portanto, para todo $i \in \{1, \ldots, n-1\}$, existem k_i elementos, são eles

$$i, n + i, \ldots, (k_i - 1)n + i,$$

que não pertencem a S. Por outro lado, para $i = 0$, temos $kn \in S$ para todo inteiro $k \geq 0$, pois $n \in S$. Dessa forma

$$\mathrm{g}(S) = k_1 + \cdots + k_{n-1}$$

$$= \frac{1}{n}((k_1 n + 1) + \cdots + (k_{n-1} n + n - 1)) - \frac{n-1}{2}$$
$$= \frac{1}{n} \sum_{w \in \mathrm{Ap}(S,n)} w - \frac{n-1}{2}.$$

■

Proposição 1.6.5. *Sejam a, b inteiros positivos primos entre si, então*

$$g(\langle a, b\rangle) = \frac{ab - a - b + 1}{2}.$$

Demonstração. Seja $i \in \{0, \ldots, a-1\}$. Claramente $ib \in \langle a, b\rangle$. Provemos que $ib - a \notin \langle a, b\rangle$. Trivial se $ib - a < 0$. Suponha, então, $ib - a \geq 0$ e que $ib - a \in \langle a, b\rangle$. Dessa forma, existem inteiros não negativos x, y tais que $ib - a = ax + by$. Logo $0 < a(x+1) = (i-y)b$, isto é, $a \mid (i-y)b$. Como a e b são primos entre si, então $a \mid i - y$. Por outro lado, $(i-y)b > 0$, então existe um inteiro positivo k tal que $i - y = ka$. Mas isso implicaria que $i = ka + y \geq a$, contradição. Assim, pela Proposição 1.6.4,

$$\mathrm{g}\left(\langle a, b\rangle\right) = \frac{1}{a}\Big(\sum_{i=0}^{a-1} ib\Big) - \frac{a-1}{2} = \frac{(a-1)b}{2} - \frac{a-1}{2} = \frac{(a-1)(b-1)}{2}.$$

■

Observação 1.6.6. *Note que para todo $s \in S$, $F(S) - s \notin S$ pois $F(S) = F(S) - s + s$, caso contrário $F(S) \in S$ e fugiria da definição. Portanto, para todo $x \leq F(S)$, temos que dentre x e $F(S) - x$, um deles não está em S. Logo, $g(S) \geq \dfrac{F(S)+1}{2}$.*

Lema 1.6.7. *Seja S um semigrupo numérico gerado por $\{n_1, n_2, \ldots, n_p\}$. Considere $d = \mathrm{mdc}(n_1, \ldots, n_{p-1})$ e defina $T = \left\{\dfrac{n_1}{d}, \ldots, \dfrac{n_{p-1}}{d}, n_p\right\}$. Então*

$$\mathrm{Ap}(S, n_p) = d \cdot \mathrm{Ap}(T, n_p).$$

Demonstração. Se $w \in \mathrm{Ap}(S, n_p)$, então $w \in \langle n_1, \ldots, n_{p-1}\rangle$. Logo $w/d \in \{n_1/d, \ldots, n_{p-1}/d\} \subseteq T$. Se $w/d - n_p \in T$, então $w - dn_p \in S$, o que é impossível. Considere $w \in \mathrm{Ap}(T, n_p)$. Então $w \in \langle n_1/d, \ldots, n_{p-1}/d\rangle$, e portanto $dw \in \langle n_1, \ldots, n_{p-1}\rangle \subseteq S$. Se $dw - n_p \in S$, então $dw - n_p = \lambda_1 n_1 + \cdots + \lambda_{p-1} n_{p-1} + \lambda_p n_p$, com $\lambda_1, \ldots, \lambda_p \in \mathbb{N}$. Como S é um semigrupo numérico, temos $\mathrm{mdc}(n_1, \ldots, n_p) = 1$, o que implica que $\mathrm{mdc}(d, n_p) = 1$. Isso leva a $d \mid (\lambda_p + 1)$ já que $(\lambda_p + 1)n_p = dw - (\lambda_1 n_1 + \cdots + \lambda_{p-1} n_{p-1})$. Mas então $w = \dfrac{\lambda_1 n_1}{d} + \cdots + \dfrac{\lambda_{p-1} n_{p-1}}{d} + \dfrac{\lambda_p + 1}{d} np$, com $\dfrac{\lambda_p + 1}{d}$ inteiro positivo. Contradição, pois $w \in \mathrm{Ap}(T, n_p)$. ■

Proposição 1.6.8. *Sejam S um semigrupo numérico com sistema mínimo de geradores $\{n_1, n_2, \ldots, n_p\}$, $d = \mathrm{mdc}(n_1, \ldots, n_{p-1})$ e $T = \{n_1/d, \ldots, n_{p-1}/d, n_p\}$. Então:*

1. $F(S) = d \cdot F(T) + (d-1)n_p$;
2. $g(S) = d \cdot g(T) + \dfrac{(d-1)(n_p - 1)n_p}{2}$.

Demonstração. Os resultados são obtidos diretamente dos resultados da Proposição 1.6.4 e do Lema 1.6.7 ■

Finalizaremos essa seção com os *pseudo-números de Frobenius* ou números *pseudo-Frobenius* que, a grosso modo, são os números que quase pertenceriam a um semigrupo numérico. A partir daqui poderemos classificar semigrupos e caracterizá-los.

Definição 1.6.9. *Dizemos que um inteiro x é um pseudo-número de Frobenius se $x \notin S$ e $x + s \in S$ para todo $s \in S \setminus \{0\}$. Representaremos o conjunto desses números por $PF(S)$ e sua cardinalidade por $t(S)$, também conhecida por tipo de S.*

Definição 1.6.10. *Sobre o conjunto dos inteiros, definiremos a relação: $a \leq_S b$ se $b - a \in S$.*

Definição 1.6.11. *Dizemos que uma relação $\leq$ é uma relação de pré-ordem sobre um conjunto P se são satisfeitas as seguintes condições:*

- $\forall a \in P$, $a \leq a$ *(reflexiva);*
- $\forall a, b, c \in P$, *se* $a \leq b$ *e* $b \leq c$, *então* $a \leq c$ *(transitiva).*
  O conjunto $(P, \leq)$ é chamado de conjunto pré-ordenado. Se, além disso, valer:
- $\forall a, b, c \in P$, *se* $a \leq b$ *e* $b \leq a$, *então* $a = b$ *(antissimétrica).*
  Dizemos que $\leq$ é uma relação de ordem.

Além disso, o conjunto $(P, \leq)$ é chamado de conjunto ordenado ou parcialmente ordenado. Um conjunto $(P, \leq)$ é totalmente ordenado se para todo $a, b \in P$, $a \leq b$ ou $b \leq a$, em outras palavras, todos seus elementos são comparáveis.

Como S é um semigrupo numérico, a relação $\leq_S$ é reflexiva, transitiva e antissimétrica, ou seja, uma ordem parcial.

Definição 1.6.12. *Sejam $(P, \leq)$ um conjunto ordenado, $A \subseteq P$ não vazio e $m \in P$. Então*

- $\forall x \in A$, $m \leq x$, *dizemos que m é o elemento mínimo e o representaremos por* $\min A$.
- $\forall x \in A$, $x \leq m$, *dizemos que m é o elemento máximo e o representaremos por* $\max A$.
- *Se $m \in A$ e não existe $x \in A$ tal que $x \leq m$, dizemos que m é um elemento minimal de A, representaremos tais elementos por* $\mathrm{Minimals}_{\leq}$.
- *Se $m \in A$ e não existe $x \in A$ tal que $m \leq x$, dizemos que m é um elemento maximal de A, representaremos tais elementos por* $\mathrm{Maximals}_{\leq}$.

Proposição 1.6.13. *Seja S um semigrupo numérico, então:*

1. $PF(S) = \text{Maximals}_{\leq_S}(\mathbb{Z} \setminus S)$*;*

2. $x \in \mathbb{Z} \setminus S$ *se, e somente se, existe* $f \in PF(S)$ *tal que* $f - x \in S$*.*

Demonstração. 1. Seja $f \in PF(S)$. Suponha que existe $x \in \mathbb{Z} \setminus S$ tal que $f \leq_S x$. Então, $x - f \in S$. Por outro lado, por definição de $PF(S)$, se $x - f \neq 0$, então $f + (x - f) = x \in S$. Contradição, logo $x - f = 0$ e f é maximal em $(\mathbb{Z} \setminus S, \leq_S)$. Reciprocamente, se f é maximal em $(\mathbb{Z} \setminus S, \leq_S)$, então, para todo $s \in S$, em que $s \neq 0$, $f + s \notin \mathbb{Z} \setminus S$. Assim, $f \in PF(S)$.

2. Seja $x \in \mathbb{Z} \setminus S$. Considere o conjunto $A = \{s \mid x + s \notin S \text{ e } s \in S\}$. Visto que $0 \in A$, A é não vazio e, como S é semigrupo numérico, a partir de determinado momento toda soma $x + s \in S$, logo A é finito. Seja $r = \max(A)$, então $x + r \in PF(S)$ e $(x + r) - x = r \in S$. Reciprocamente, sejam $x \in \mathbb{N}$ e $f \in PF(S)$ tais que $x \leq_S f$. Se $x = f$, nada precisamos fazer. Suponha $x \neq f$. Se $x \in S$, então $(f - x) + x = f \in S$. Contradição, pois $f \in PF(S)$.

■

Proposição 1.6.14. *Seja* S *um semigrupo numérico e seja* n *um elemento não nulo de* S*. Então,*

$$PF(S) = \{w - n \mid w \in \textit{Maximals}_{\leq_S}(Ap(S, n))\}.$$

Demonstração. Seja $x \in PF(S)$. Então $x \notin S$ e $x + n \in S$, ou seja, $x + n \in Ap(S, n)$. Por outro lado, considere $w \in Ap(S, n)$ tal que $x + n \leq_S w$. Temos $w - (x + n) = w - x - n \in S$. Isso significa que $w - n = x + s$ para algum $s \in S$. Como $w - n \notin S$ e $x \in PF(S)$, então $s = 0$ e, portanto, $w = x + n$. Agora, tome $w \in \text{Maximals}_{\leq_S}(Ap(S, n))$, logo $w - n \notin S$. Se existir $s \in S \setminus \{0\}$ tal que $w - n + s \notin S$, então $w + s \in Ap(S, n)$. Contradição, já que w é maximal em $Ap(S, n)$ pela relação $\leq_S$. ■

Corolário 1.6.15. *Seja* S *um semigrupo numérico. Então:*

$$t(S) \leq m(S) - 1.$$

Demonstração. Seja $n_1 = m(S)$. Pela Proposição 1.6.14, $t(S)$ é igual ao número de elementos de $\text{Maximals}_{\leq_S}(Ap(S, n_1))$. Como $Ap(S, n_1)$ tem n_1 elementos e 0 não é maximal em $Ap(S, n_1)$, então $t(S) \leq m(S) - 1$. ■

Definição 1.6.16. *Seja* S *um semigrupo numérico. Denotaremos*

$$N(S) = \{s \in S \mid s < F(S)\}.$$

Sua cardinalidade é denotada por $n(S)$*.*

Com isso, se $N(S)$ e $F(S)$ são conhecidos, conseguimos reconstruir todo o conjunto S.

CAPÍTULO 2

Semigrupos Numéricos com Dimensão de Imersão Máxima

Como vimos anteriormente, a dimensão de imersão de um semigrupo numérico está limitada superiormente pela sua multiplicidade. Assim, dizemos que S possui *dimensão de imersão máxima* se $e(S) = m(S)$. Nesta seção, veremos que se S possui dimensão de imersão máxima, conseguimos expressar o número de Frobenius a partir de seus geradores, assim como no caso para dois geradores. Além disso, garantir essa propriedade permite uma caracterização mais refinada da estrutura interna de S, conectando a escolha de geradores à forma como elementos do semigrupo podem ser expressos como combinações lineares desses geradores.

Proposição 2.0.1. *Seja S um semigrupo numérico minimamente gerado por $\{n_1 < n_2 < \cdots < n_e\}$. Então S possui dimensão de imersão máxima se, e somente se,* $\mathrm{Ap}(S, n_1) = \{0, n_2, \ldots, n_e\}$.

Demonstração. Suponha que S possui dimensão de imersão máxima, isto é, $n_1 = e$. Já foi provado que

$$A = (\mathrm{Ap}(S, n_1) \setminus \{0\}) \cup \{n_1\}$$

é um conjunto gerador de S. Como $\{n_1, n_2, \ldots, n_e\} \subseteq A$ e A possui $n_1 = e$ elementos, então $\{n_1, n_2, \ldots, n_e\} = A$. Em outras palavras, $\mathrm{Ap}(S, n_1) = \{0, n_2, \ldots, n_e\}$.

Por outro lado, se $\mathrm{Ap}(S, n_1) = \{0, n_2, \ldots, n_e\}$, então $\mathrm{Ap}(S, n_1)$ possui $e = n_1$ elementos, ou seja S possui dimensão de imersão máxima . ■

Corolário 2.0.2. *Seja S um semigrupo numérico minimamente gerado por $\{n_1 < n_2 < \cdots < n_e\}$.*

1. *Se S possui dimensão de imersão máxima, então $F(S) = n_e - n_1$.*
2. *S possui dimensão de imersão máxima se, e somente se, $g(S) = \dfrac{1}{n_1}(n_2 + \cdots + n_e) - \dfrac{n_1 - 1}{2}$;*

3. S *possui dimensão de imersão máxima se, e somente se,* $t(S) = n_1 - 1$.

Demonstração. Consequência das Proposições 1.6.4, 1.6.14 e 2.0.1.

1. $\mathrm{F}(S) = \max(\mathrm{Ap}(S, n_1)) - n_1 = max\{0, n_2, \ldots, n_e\} - n_1 = n_e - n_1$.
2. $\mathrm{g}(S) = \frac{1}{n_1}\Big(\sum_{w \in \mathrm{Ap}(S,n_1)} w\Big) - \frac{n_1 - 1}{2} = \frac{1}{n_1}(0 + n_2 + \cdots + n_e) - \frac{n_1 - 1}{2}$.
3. Como $PF(S) = \{w - n \mid w \in \text{Maximals}_{\leq_S}(Ap(S, n_1))\}$ e $\text{Maximals}_{\leq_S}(Ap(S, n_1)) = \{n_2, \ldots, n_e\}$, então $t(S) = n_1 - 1$. A volta é imediata pelo Corolário 1.6.15.

■

Exemplo 2.0.3. O semigrupo numérico $S = \langle 4, 5, 11\rangle$ possui $F(S) = 11 - 4 = n_e - n_1$, mas não possui dimensão de imersão máxima.

Proposição 2.0.4. *Sejam* $n \in \mathbb{N} \setminus \{0\}$ *e* $C = \{w(0) = 0, w(1), \ldots, w(n-1)\} \subseteq \mathbb{N}$ *tais que* $w(i) \equiv i \pmod n$ *para todo* $i \in \{1, \ldots, n-1\}$. *Seja* S *o semigrupo numérico* $\langle\{n\} \cup C\rangle$. *As seguintes afirmações são equivalentes:*

1. $\mathrm{Ap}(S, n) = C$.

2. Para todos $i, j \in \{1, \ldots, n-1\}$, $w(i) + w(j) \geq w((i + j) \bmod n)$.

Demonstração. Note que $w(i) + w(j)$ e $w((i + j) \bmod n)$ são congruentes módulo n para todos i, j. Portanto, podemos reescrever a segunda afirmação da seguinte forma:

2.1 Para todos i, j, existe $t \in \mathbb{N}$ tal que $w(i) + w(j) = tn + w((i + j) \bmod n)$.

Se $\mathrm{Ap}(S, n) = C$, pelo Lema 1.6.7, $w(i) + w(j) = kn + c$ para algum $k \in \mathbb{N}$ e $c \in C$, com $w(i) + w(j) \equiv c \pmod n$, logo $c = w((i + j) \bmod n)$. Agora, suponha que a segunda condição seja satisfeita. Vamos mostrar que $\mathrm{Ap}(S, n) \subseteq C$. Se $s \in \mathrm{Ap}(S, n) \subseteq S$, então existem $c_1, \ldots, c_t \in C$ tais que $s = \sum_{i=1}^{t} c_i$. Aplicando 2.1 repetidamente, temos que $s \leq kn + c$ com $c \in C$ e $k \in \mathbb{N}$. Como $s \in \mathrm{Ap}(S, n)$, por definição, $k = 0$ e, consequentemente, $s = c \in C$. Como a cardinalidade de $\mathrm{Ap}(S, n) \subseteq C$ é n então $\mathrm{Ap}(S, n) = C$. ■

Com os resultados vistos, agora somos capazes de distinguir se um semigrupo numérico possui ou não dimensão de imersão máxima olhando diretamente para o conjunto de Apéry da multiplicidade de S. Antes de demonstrarmos resultados mais interessantes, estamos interessados em criar semigrupos numéricos com dimensão de imersão máxima a partir dos elementos de um semigrupo numérico arbitrário. Os seguintes corolários são consequências diretas das proposições desse capítulo.

Corolário 2.0.5. *Seja S um semigrupo numérico e $n \in S$. Então*

$$T = \langle n, w(1) + n, \ w(2) + n, \ \ldots, \ w(n-1) + n \rangle$$

é um semigrupo numérico de dimensão de imersão máxima, em que $n \in S$ e para todo $i \in \{1, \ldots, n-1\}$, $w(i)$ é o elemento de $\mathrm{Ap}(S, n)$ congruente com i módulo n. Além disso, $F(T) = F(S) + n$ e $m(T) = m(S) = n$.

Corolário 2.0.6. *Seja S um semigrupo numérico com dimensão de imersão máxima e multiplicidade m. Para todo $i \in \{1, \ldots, m-1\}$, considere $w(i)$ o único elemento de $\mathrm{Ap}(S, m)$ congruente com i módulo m. Tome $T = \langle m, w(1) - m, \ldots, w(m-1) - m \rangle$. Então T é um semigrupo numérico com $\mathrm{Ap}(T, m) = \{0, w(1) - m, \ldots, w(m-1) - m\}$.*

Proposição 2.0.7. *Seja S um semigrupo numérico. As seguintes condições são equivalentes:*

1. *S possui dimensão de imersão máxima;*
2. *Para todo $x, y \in S^*$, temos $x + y - m(S) \in S$;*
3. *$-m(S) + S^*$ é um semigrupo numérico.*

Demonstração. $(1 \Rightarrow 2)$: Se $x - m(S) \in S$ ou $y - m(S) \in S$, nada precisamos fazer. Suponha que $x, y \in \mathrm{Ap}(S, m(S))$. Basta aplicar o caso particular da Proposição 2.0.4, $i, j \in \{1, \ldots, n-1\}$, $w(i) + w(j) > w((i + j) \bmod n)$.

$(2 \Rightarrow 3)$: Trivial.

$(3 \Rightarrow 1)$: Seja $w(i)$ o único elemento de $\mathrm{Ap}(S, m(S))$ congruente com i módulo m, com $1 \leq i \leq m-1$. Usamos novamente o caso particular da Proposição 2.0.4. Se $w(i) + w(j) = w((i + j) \bmod m) + m(S)$ para algum $j \in \{1, \ldots, m(S) - 1\}$, então:

$$w(i) - m(S) + w(j) - m(S) = w((i + j) \bmod m(S)) - 2m(S) \notin \{x - m(S) \mid x \in S^*\},$$

contradizendo que esse conjunto é um semigrupo numérico. ■

Corolário 2.0.8. *Seja S um semigrupo numérico. Então S possui dimensão de imersão máxima se, e somente se, existe um semigrupo numérico T e $t \in T \setminus \{0\}$ tal que $S = (t + T) \cup \{0\}$.*

Demonstração. Da Proposição 2.0.7, tome $T = -m(S) + S^*$ e, pelo Corolário 2.0.5, obtemos o resultado desejado. ■

Lema 2.0.9. *Sejam S e T semigrupos numéricos. Para $s \in S^*$ e $t \in T^*$, então $(s + S) \cup \{0\} = (t + T) \cup \{0\}$ se, e somente se, $S = T$ e $s = t$.*

Demonstração. Suponha que $(s + S \cup \{0\}) = (t + T \cup \{0\})$. Note que $m((s + S) \cup \{0\}) = s$ e $m((t + T) \cup \{0\}) = t$, logo $s = t$. Além disso, $S = -s + (s + S) = -t + (t + T) = T$. A volta é imediata. ■

2.1 Semigrupos Numéricos Arf

De forma similar aos semigrupos com dimensão de imersão máxima, a propriedade Arf permitem gerar os elementos do semigrupo de maneira sistemática e bem definida. Essa regularidade estrutural torna possível analisar o comportamento dos elementos e a forma como combinações lineares se distribuem dentro do semigrupo. Além disso, quando essa propriedade é satisfeita, podemos construir outros conjuntos cujas características são preservadas em relação ao conjunto original, os chamados invariantes.

Definição 2.1.1. *Um semigrupo numérico S é Arf, ou possui a propriedade Arf, se para todos $x, y, z \in S$, em que $x \geq y \geq z$, tem-se que $x + y - z \in S$.*

Observação 2.1.2. *Dado um semigrupo numérico. Nos limitaremos a utilizar a notação "$\rightarrow$"para indicar que todos os elementos posteriores ao último elemento apresentado são elementos do semigrupo numérico. Por exemplo, $S = \langle 3, 5\rangle$, $S = \{3, 5, 6, 8, 9, 10, \dots\} = \{3, 5, 6, 8, \rightarrow\}$.*

Exemplo 2.1.3. $S = \{0, 3, 5, 6, \rightarrow\}$ é Arf. No entanto, $S_1 = \{0, 3, 4, 6, \rightarrow\}$ não possui a propriedade Arf pois $4 + 4 - 3 = 5$ e $5 \notin S_1$.

Proposição 2.1.4. *Sejam S um semigrupo numérico e $x \in S^*$. Então S é de Arf se, e somente se, $S' = (x + S) \cup \{0\}$ é Arf.*

Demonstração. Seja S um semigrupo numérico de Arf. Pela Proposição 2.0.7, S possui dimensão de imersão máxima. Logo existe um semigrupo numérico S' e $x \in S' \setminus \{0\}$ tal que $S = (x + S') \cup \{0\}$. Se $S \neq \mathbb{N}$, então $S \subsetneq S'$. Assim, como S é Arf, segue que S' também é Arf. Podemos repetir esse processo com S', e obter um semigrupo numérico de Arf S'' e $y \in S' \setminus \{0\}$ tal que $S' = (y + S'') \cup \{0\}$. Como $\mathbb{N} \setminus S$ possui uma quantidade finita de elementos, esse processo é finito, obtendo assim uma cadeia de semigrupos numéricos Arf da forma $S_0 \subsetneq S_1 \subsetneq \dots \subsetneq S_n = \mathbb{N}$ em que $S_i = (x_{i+1} + S_{i+1}) \cup \{0\}$, para algum $x_{i+1} \in S_{i+1} \setminus \{0\}$. ■

Proposição 2.1.5. *A interseção de uma quantidade finita de semigrupos numéricos de Arf é um semigrupo numérico de Arf.*

Demonstração. A interseção de finitos semigrupos numéricos Arf contém todos os elementos a partir do maior número de Frobenius. Como cada elemento de cada conjunto possui a propriedade Arf, então os elementos da interseção finita também a possuem. ■

Como o complementar de S em $\mathbb{N}$ é finito, o conjunto dos semigrupos numéricos de Arf que contém S também é finito. Assim, podemos definir o menor semigrupo numérico Arf que contém S.

Definição 2.1.6. *Seja S um semigrupo numérico. Como o complemento de S em $\mathbb{N}$ é finito, o conjunto dos semigrupos numéricos Arf que contêm S também é finito. A interseção desses semigrupos é novamente um semigrupo numérico Arf. Denotaremos essa interseção por $\mathrm{Arf}(S)$ e a chamaremos de fecho Arf de S.*

Lema 2.1.7. *Seja S um submonoide de $\mathbb{N}$. Então*

$$S' = \{x + y - z \mid x, y, z \in S,\ x \geq y \geq z\}$$

é um submonóide de $\mathbb{N}$ e $S \subseteq S'$.

Demonstração. Seja $x \in S$. Então $x + x - x = x \in S'$, logo $S \subseteq S'$ e, naturalmente, $S' \subseteq \mathbb{N}$. Seja $a, b \in S'$. Por definição, existem $x_1, x_2, y_1, y_2, z_1, z_2 \in S$ tal que $a = x_1 + y_1 - z_1$, $b = x_2 + y_2 - z_2$ em que $x_i \geq y_i \geq z_i$, $i \in \{1, 2\}$. Logo, $a + b = (x_1 + y_1 - z_1) + (x_2 + y_2 - z_2) = (x_1 + x_2) + (y_1 + y_2) - (z_1 + z_2)$. Como $x_1 + x_2, y_1 + y_2, z_1 + z_2 \in S$ e $x_1 + x_2 \geq y_1 + y_2 \geq z_1 + z_2$, então $a + b \in S'$. ■

Definição 2.1.8. *Para um dado submonóide S de $\mathbb{N}$, vimos que podemos construir uma cadeia finita estacionária de submonóides até obtermos $\mathrm{Arf}(S)$. Assim, definiremos*

$$S^0 = S, \quad S^{n+1} = (S^n)'.$$

Proposição 2.1.9. *Seja S um semigrupo numérico. Existe $k \in \mathbb{N}$ tal que $S^k = \mathrm{Arf}(S)$.*

Demonstração. Para $n = 0$, $S^0 = S \subseteq \mathrm{Arf}(S)$ por definição. Suponha $S^k \subseteq \mathrm{Arf}(S)$ para algum $k \in \mathbb{N}$. $S^{k+1} = (S^k)'$ são todos os elementos ordenados x, y, z em que $x + y - z \in S^{k+1}$. Assim, por hipótese de indução, $S^{k+1} \subseteq \mathrm{Arf}(S)$. Como S tem complemento finito em $\mathbb{N}$, o número de semigrupos numéricos que contêm S é finito, logo existe $k \in \mathbb{N}$ tal que $S^k = S^{k+1}$ para algum $k \in \mathbb{N}$. Portanto, S^k é um semigrupo numérico Arf que está contido em $\mathrm{Arf}(S)$ e conclui-se que $S^k = \mathrm{Arf}(S)$. ■

Lema 2.1.10. *Sejam $m, r_1, \ldots, r_p \in \mathbb{N}$ tal que $\mathrm{mdc}(m, r_1, \ldots, r_p) = 1$. Então:*

$$m + \langle m, r_1, \ldots, r_p \rangle^n \subseteq \mathrm{Arf}(m, m + r_1, \ldots, m + r_p).$$

Demonstração. Para $n = 0$, provaremos que $m + \langle m, r_1, \ldots, r_p \rangle \subseteq \mathrm{Arf}(m, m + r_1, \ldots, m + r_p)$. Sejam $i, j \in \{1, \ldots, p\}$ tais que $m, m + r_i, m + r_j \in \mathrm{Arf}(m, m + r_1, \ldots, m + r_p)$, já que $m + r_i + r_j = (m + r_i) + (m + r_j) - m \in \mathrm{Arf}(S)$. Para $k \in \{1, \ldots, p\}$, temos que $m + r_i + r_j + r_k = (m + r_j) + (m + r_k) - m \in \mathrm{Arf}(S)$. Então para todo $a_1, \ldots, a_p \in \mathbb{N}$, $(a + 1)m + a_1 r_1 + \cdots + a_p r_p \in \mathrm{Arf}(m, m + r_1, \ldots, m + r_p)$, logo

$$m + \langle m, r_1, \ldots, r_p \rangle \subseteq \mathrm{Arf}(m, m + r_1, \ldots, m + r_p).$$

Suponha que $m + \langle m, r_1, \ldots, r_p\rangle^n \subseteq \text{Arf}(m, m + r_1, \ldots, m + r_p)$. Considere, também, $a \in m + \langle m, r_1, \ldots, r_p\rangle^{n+1}$, então $a = m + b$, com $b \in \langle m, r_1, \ldots, r_p\rangle^{n+1}$, ou seja, existem $x, y, z \in \langle m, r_1, \ldots, r_p\rangle^n$ tal que $b = x + y - z$. Dessa forma, por hipótese de indução,$a = m + b = m + x + y - z = (m + x) + (m + y) - (m + z) \in \text{Arf}(m, m + r_1, \ldots, m + r_p)$. ■

Proposição 2.1.11. *Sejam* $m, r_1, \ldots, r_p$ *inteiros não negativos e* $\text{mdc}(m, r_1, \ldots, r_p) = 1$. *Então:*

$$\text{Arf}(m, m + r_1, \ldots, m + r_p) = (m + \text{Arf}(m, r_1, \ldots, r_p)) \cup \{0\}.$$

Demonstração. Pela Proposição 2.1.9 e pelo Lema 2.1.7, temos: $(m + \text{Arf}(m, m + r_1, \ldots, m + r_p)) \cup \{0\} \subseteq \text{Arf}(m, m + r_1, \ldots, m + r_p)$. Por outro lado, observamos que $m, m + r_1, \ldots, m + r_p \in (m + \text{Arf}(m, r_1, \ldots, r_p)) \cup \{0\}$ é um semigrupo numérico Arf pela Proposição 2.1.4. ■

Agora somos capazes de escrever um método recursivo de calcular os elementos que estão no fecho de Arf.

Proposição 2.1.12. *Dado* $X \subseteq \mathbb{N} \setminus \{0\}$ *tal que o máximo divisor comum de seus geradores seja* 1. *Seja* $A_1 = X$ *e* $A_{n+1} = (\{x - \text{min}A_n \mid x \in A_n\} \setminus \{0\}) \cup \{\text{min}A_n\}$. *Então*

$$\textit{Arf}(X) = \{0, \text{min}A_1, \text{min}A_1 + \text{min}A_2, \ldots, \sum_{i=1}^{q-1} \text{min}A_i, \rightarrow\}.$$

Demonstração. Pelo Algoritmo de Euclides para o máximo divisor comum, existe $q = \text{min}\{k \in \mathbb{N} \mid 1 \in A_k\}$. Como $1 \in A_k$ temos que $\text{Arf}(A_q) = \mathbb{N}$. Por outro lado, $\text{Arf}(A_{q-1}) = (\text{min}A_{q-1} + \mathbb{N}) \cup \{0\} = \{0, \text{min}A_{q-1}, \rightarrow\}$. Suponha que

$$\text{Arf}(A_{q-i}) = \{0, \text{min}A_{q-i}, \text{min}A_{q-i} + \text{min}A_{q-i+1}, \ldots, \sum_{m=0}^{q-1} \text{min}A_{q-i+m}, \rightarrow\}.$$

Vamos provar que

$$\text{Arf}(A_{q-i-1}) = \{0, \text{min}A_{q-i-1}, \text{min}A_{q-i-1} + \text{min}A_{q-i}, \ldots, \sum_{m=0}^{q-1} \text{min}A_{q-i+m}, \rightarrow\}.$$

Pela Proposição 2.1.11, sabemos que:

$$\text{Arf}(A_{q-i-1}) = (\text{min}A_{q-i-1} + \text{Arf}(A_{q-i})) \cup \{0\}.$$

Como consequência direta da Proposição 2.1.11,

$$\text{F}(\text{Arf}(m, m + r_1, \ldots, m + r_p)) = m + \text{F}(\text{Arf}(m, r_1, \ldots, r_p)).$$

Utilizando a hipótese de indução, $\text{Arf}(X) = \{0, \text{min}A_1, \text{min}A_1 + \text{min}A_2, \ldots, \sum_{i=1}^{q-1} \text{min}A_i, \rightarrow\}$. ■

Exemplo 2.1.13. Vamos calcular $\text{Arf}(\langle 9, 24, 35\rangle)$.

$$A_1 = \{9, 24, 35\}, \qquad \text{min}A_1 = 9,$$

$$A_2 = \{9, 15, 26\}, \qquad \min A_2 = 9,$$
$$A_3 = \{9, 6, 17\}, \qquad \min A_3 = 6,$$
$$A_4 = \{3, 6, 5\}, \qquad \min A_4 = 3,$$
$$A_5 = \{3, 3, 2\}, \qquad \min A_5 = 2,$$
$$A_5 = \{1, 1, 2\}.$$

Então $\mathrm{Arf}(\langle 9, 24, 35\rangle) = \{0, 9, 18, 24, 27, 29, \rightarrow\}$.

2.2 Semigrupos Numéricos Saturados

Definição 2.2.1. *Dizemos que um semigrupo numérico é saturado se para todos $s, s_1, \ldots, s_r \in S$ e $z_1, z_2, \ldots, z_s \in \mathbb{Z}$ se cumpre a seguinte condição: se $s \geq s_i$, para todo $i \in \{1, \ldots, r\}$, e $z_1 s_1 + \cdots + z_r s_r \geq 0$, então $s + z_1 s_1 + \cdots + z_r\, s_r \ \in \ S$.*

Exemplo 2.2.2. O semigrupo numérico $S = \{0, 5, 7, 9, 10, \rightarrow\}$ é de Arf mas não é saturado. Note que $5, 7 \in S$ e $8 = 3 \cdot 5 - 1 \cdot 7 \notin S$.

Lema 2.2.3. *Todo semigrupo numérico saturado possui a propriedade de Arf.*

Demonstração. Sejam S um semigrupo numérico saturado em que $x, y, z \in S$, $x \geq y \geq z$. Então $x + y - z \geq 0$ e, como S é saturado, $x + y - z \in S$. Portanto, S é Arf e, consequentemente, possui dimensão de imersão máxima. ■

A partir de agora estamos interessados em caraterizar os semigrupos numéricos saturados.

Definição 2.2.4. *Para $A \subseteq \mathbb{N}$ e $a \in A \setminus \{0\}$, definimos*

$$d_A(a) = \mathrm{mdc}\{x \in A \mid x \leq a\}.$$

Exemplo 2.2.5. Seja $A = \{3, 5, 9, 11, 13\}$. Então $d_A(9) = \mathrm{mdc}(3, 5, 9) = 1$.

Lema 2.2.6. *Sejam S um semigrupo numérico saturado e $s \in S$. Então $s + d_S(s) \in S$.*

Demonstração. Seja $\{s_1, \ldots, s_r\} = \{x \in S \mid x \leq s\}$. Pelo Teorema 1.2.1, existem inteiros $z_1, \ldots, z_r$ tais que $z_1 s_1 + \cdots + z_r s_r = d_S(s)$. Como S é saturado, $s + d_S(s) \in S$. ■

Lema 2.2.7. *Seja A um subconjunto não vazio de inteiros positivos tal que $mdc(A) = 1$ e $a + d_A(a) \in A$ para todo $a \in A$. Então $a + k d_A(a) \in A$ para todo $k \in \mathbb{N}$ e $A \cup \{0\}$ é um semigrupo numérico.*

Demonstração. Usaremos indução em $d_A(a)$. Note que $d_A(a) > 0$. Vamos mostrar que se $d_A(a) = 1$, então $a + k \in A$ para todo $k \in \mathbb{N}$. Para $k = 0$ é imediato. Suponha que $a + k \in A$. Como $d_A(a + k) \leq d_A(a) = 1$, então $d_A(a + k) = 1$. Logo, $a + k + 1 = a + k + d_A(a + k) \in A$. Agora, assuma que se $a' \in A$ com $d_A(a') < d_A(a)$, então $a' + kd_A(a') \in A$ para todo $k \in \mathbb{N}$. Suponha $d_A(a) \geq 2$ e provemos que $a + kd_A(a) \in A$ para todo $k \in \mathbb{N}$. Como $\mathrm{mdc}(A) = 1$, existe $b \in A$ tal que $d_A(b) = 1$. Se $d_A(a + kd_A(a)) = d_A(a)$ e $a + kd_A(a) \in A$, então $a + (k + 1)d_A(a) = a + kd_A(a) + d_A(a + kd_A(a)) \in A$. Assim, existe um menor inteiro positivo t tal que $a + td_A(a) \in A$ e $d_A(a + td_A(a)) < d_A(a)$. Daí, pela hipótese de indução, $(a + td_A(a)) + kd_A(a + td_A(a)) \in A$ para todo $k \in \mathbb{N}$. Como $d_A(a + td_A(a))$ divide $d_A(a)$, logo $d_A(a) = ld_A(a + td_A(a))$ para algum inteiro positivo l. Portanto, $a + td_A(a) + \frac{k}{l}d_A(a) \in A$ para todo $k \in \mathbb{N}$ e, consequentemente, $a + (t + n)d_A(a) \in A$ para todo natural n. Segue, pela definição de t, $a + kd_A(a) \in S$ para todo $k \in \{1, \ldots, t\}$ e, por tal, $a + kd_A(a) \in S$ para todo $k \in \mathbb{N}$. Por fim, provemos que $A \cup \{0\}$ é um semigrupo numérico. Como $\mathrm{mdc}(A) = 1$, basta provar que para quaisquer $a, b \in A$, $a + b \in A$. Suponha que $a \leq b$, então $d_A(b)$ divide $d_A(a)$, ou seja, existe $\lambda \in \mathbb{N}$ tal que $d_A(a) = \lambda d_A(b)$. Por outro lado, por definição, $d_A(a)$ divide a, então existe $\mu \in \mathbb{N}$ tal que $a = \mu d_A(a)$. Finalmente, $a + b = \mu d_A(a) + b = \mu\lambda d_A(b) + b$ que, como provado anteriormente, pertence a S. ■

Proposição 2.2.8. *Seja A um subconjunto não vazio de $\mathbb{N}$ tal que $0 \in A$ e $\mathrm{mdc}(A) = 1$. As seguintes condições são equivalentes:*

1. *A é um semigrupo numérico saturado.*
2. *$a + d_A(a) \in A$ para todo $a \in A \setminus \{0\}$.*
3. *$a + kd_A(a) \in A$ para todo $a \in A \setminus \{0\}$ e $k \in \mathbb{N}$.*

Demonstração. $(1 \Rightarrow 2)$: Lema 2.2.6.

$(2 \Rightarrow 3)$: Lema 2.2.7.

$(3 \Rightarrow 1)$: Pelo Lema 2.2.7, sabemos que A é um semigrupo numérico. Sejam $a, a_1, \ldots, a_r \in A$, $a_i \leq a$ para todo $i \in \{1, \ldots, r\}$ e $z_1, \ldots, z_r \in \mathbb{Z}$ tais que $z_1a_1 + \ldots + z_ra_r \geq 0$. Como $a_i \leq a$, então $d_A(a)$ divide a_i para todo $i \in \{1, \ldots, r\}$. Assim, existe $k \in \mathbb{N}$ tal que $z_1a_1 + \ldots + z_ra_r = kd_A(a)$ e, portanto, $a + z_1a_1 + \ldots + z_ra_r = a + kd_A(a) \in A$. Logo, A é saturado. ■

Agora tentaremos obter uma caracterização, assim como nos semigrupos numéricos Arf, para os semigrupos numéricos saturados.

Proposição 2.2.9. *Seja S um semigrupo numérico. As seguintes condições são equivalentes:*

1. *S é saturado.*

2. Existe $x \in S^*$ tal que $(x + S) \cup \{0\}$ é um semigrupo numérico saturado.

Demonstração. $(1 \Rightarrow 2)$: Suponha que $S = \{0 < s_1 < s_2 < \ldots < s_n < \ldots\}$. Provemos que $(s_1 + S) \cup \{0\} = \{0 < s_1 < s_1 + s_1 < s_1 + s_2 < \ldots < s_1 + s_n < \ldots\}$ é saturado. Pela Proposição 2.2.8, basta mostrar que para todo $n \in \mathbb{N}$, $s_1 + s_n + \mathrm{mdc}(0, s_1, s_1 + s_1, \ldots, s_1 + s_n) \in (s_1 + S) \cup \{0\}$. Como S é saturado, $s_n + \mathrm{mdc}(0, s_1, \ldots, s_n) \in S$. Além disso, $\mathrm{mdc}(0, s_1, s_1 + s_1, \ldots, s_1 + s_n) = \mathrm{mdc}(0, s_1, \ldots, s_n)$, portanto, $s_1 + s_n + \mathrm{mdc}(0, s_1, s_1 + s_1, \ldots, s_1 + s_n) \in (s_1 + S) \cup \{0\}$.

$(2 \Rightarrow 1)$: Se $S = \{0 < s_1 < \ldots < s_n < \ldots\}$, então $(x + S) \cup \{0\} = \{0 < x < s_1 + x < \ldots < s_n + x < \ldots\}$. Seja $a = \mathrm{mdc}(0, x, x + s_1, \ldots, x + s_n)$ e $b = \mathrm{mdc}(0, x, s_1, \ldots, s_n)$. Como $a = b$ então a divide $\mathrm{mdc}(0, s_1, \ldots, s_n)$, logo existe $k \in \mathbb{N}$ tal que $ka = \mathrm{mdc}(0, s_1, \ldots, s_n)$. Como $(x + S) \cup \{0\}$ é um semigrupo numérico saturado, pela Proposição 2.2.8, $x + s_n + ka \in (x + S) \cup \{0\}$ e, consequentemente, $s_n + 0, \mathrm{s}_1, \ldots, \mathrm{s}_\mathrm{n} \in S$, logo S é saturado. ■

Corolário 2.2.10. *Seja S um semigrupo numérico. Então S é saturado se, e somente se, $(m(S) + S) \cup \{0\}$ é saturado.*

Demonstração. Segue diretamente do segundo item da proposição anterior. ■

De forma análoga à feita em semigrupos numéricos, a interseção finita de semigrupos numéricos saturados é também um semigrupo numérico saturado e também é possível calculá-lo.

Definição 2.2.11. *Dado um semigrupo numérico S, denotaremos por $\mathrm{Sat}(S)$ a interseção de todos os semigrupos numéricos saturados que contém S. Nomearemos esse semigrupo como o fecho saturado de S.*

Proposição 2.2.12. *Sejam $n_1 < n_2 < \ldots < n_e$ inteiros positivos tais que $\mathrm{mdc}(n_1, \ldots, n_e) = 1$. Para cada $i \in \{1, \ldots, e\}$, defina $d_i = \mathrm{mdc}(n_1, \ldots, n_i)$ e para todo $j \in \{1, \ldots, e-1\}$, defina $k_j = \max\{k \in \mathbb{N} \mid n_j + kd_j < n_{j+1}\}$. Então*

$$\mathrm{Sat}(n_1, \ldots, n_e) = \{0, n_1, n_1 + d_1, \ldots, n_1 + k_1 d_1, n_2, n_2 + d_2, \ldots, n_2 + k_2 d_2, \ldots, n_{e-1}, n_{e-1} + d_{e-1}, \ldots, n_{e-1} + k_{e-1} d_{e-1}, n_e, n_e + 1, \to\}.$$

Demonstração. Seja

$$A = \{0, n_1, n_1 + d_1, \ldots, n_1 + k_1 d_1, n_2, n_2 + d_2, \ldots, n_2 + k_2 d_2, \ldots, n_{e-1}, n_{e-1} + d_{e-1}, \ldots, n_{e-1} + k_{e-1} d_{e-1}, n_e, n_e + 1, \to\}.$$

Note que A não é vazio, $0 \in A$, $\mathrm{mdc}(A) = 1$ e $a + d_A(a) \in A$ para todo $a \in A$. Pela Proposição 2.2.8, A é um semigrupo numérico saturado e, como $\{n_1, \ldots, n_e\} \subseteq A$, $\mathrm{Sat}(n_1, \ldots, n_e) \subseteq A$. Agora, seja $a \in A$, então existe $i \in \{1, \ldots, e\}$ e $k \in \mathbb{N}$ tal que $a = n_i + kd_i$, nesse caso, $d_e = 1$. Como $\{n_1, \ldots, n_e\} \subseteq$

$\mathrm{Sat}(n_1, \ldots, n_e)$, temos que $d_{\mathrm{Sat}(n_1,\ldots,n_e)}(n_i)$ divide d_i. Logo, existe $l \in \mathbb{N}$ tal que $d_i = l d_{\mathrm{Sat}(n_1,\ldots,n_e)}(n_i)$. Pela Proposição 1.6.4, $n_i + t d_{\mathrm{Sat}(n_1,\ldots,n_e)}(n_i) \in \mathrm{Sat}(n_1, \ldots, n_e)$ para todo $t \in \mathbb{N}$ e, portanto, $a = n_i + kd_i = n_i + kl d_{\mathrm{Sat}(n_1,\ldots,n_e)(n_i)} \in \mathrm{Sat}(n_1, \ldots, n_e)$. ■

Exemplo 2.2.13.

$$\mathrm{Sat}(\{4, 10, 23\}) = \{0, 4, 8, 10, 12, 14, 16, 18, 20, 22, 23, \rightarrow\}.$$

CAPÍTULO 3

Semigrupos Numéricos Irredutíveis

Definição 3.0.1. *Um semigrupo numérico é dito irredutível se não puder ser expresso como uma interseção de dois semigrupos numéricos que o contém.*

Vamos mostrar que semigrupos numéricos irredutíveis são maximais no conjunto dos semigrupos numéricos com numérico de Frobenius fixo. Primeiramente vamos provar que adicionando o número de Frobenius a um semigrupo numérico obtemos também um semigrupo numérico.

Lema 3.0.2. *Seja S um semigrupo numérico diferente de $\mathbb{N}$. Então, $S \cup F(S)$ é, novamente, um semigrupo numérico.*

Demonstração. Note que o complemento de $S \cup \{F(S)\}$ em $\mathbb{N}$ é finito pois $\mathbb{N} \setminus S$ é finito. Sejam $a, b \in S \cup \{F(S)\}$. Se $a = F(S)$ ou $b = F(S)$, então que $a + b \geq F(S)$, portanto, $a + b \in S \cup \{F(S)\}$. Se $a, b \in S$, então $a + b \in S \subseteq S \cup \{F(S)\}$. Por fim, como $0 \in S \cup \{F(S)\}$, então $S \cup \{F(S)\}$ é um semigrupo numérico. ■

Teorema 3.0.3. *Seja S um semigrupo numérico. Então as seguintes condições são equivalentes.*

1. *S é irredutível.*
2. *S é maximal no conjunto de todos os semigrupos numéricos com o número de Frobenius $F(S)$.*
3. *S é maximal no conjunto de todos os semigrupos numéricos que não contém $F(S)$.*

Demonstração. $(1 \Rightarrow 2)$: Seja T um semigrupo numérico tal que $S \subseteq T$ e $F(T) = F(S)$. Então $S = (S \cup \{F(S)\}) \cap T)$. Como S é irredutível, segue que $S = T$.

$(2 \Rightarrow 3)$: Seja T um semigrupo numérico tal que $S \subseteq T$ e $F(S) \notin T$. Então, $T \cup \{F(S) + 1, F(S) +$

$2, \rightarrow\}$ é um semigrupo numérico que contém S com número de frobenius $F(S)$. Como S é maximal, segue que $S = T \cup \{F(S)+1, F(S)+2, \rightarrow\}$ e, consequentemente, $S = T$.

$(3 \Rightarrow 1)$: Sejam S_1, S_2 dois semigrupos numéricos que contém S. Por hipótese, temos que $F(S) \in S_1$ e $F(S) \in S_2$. Logo, $S \neq S_1 \cap S_2$. ■

Um semigrupo numérico é dito simétrico se é irredutível e $F(S)$ é ímpar e pseudo-simétrico se $F(S)$ for par.

Dado um semigrupo numérico S, se S não é irredutível, então pelo Teorema 2, temos que existe um semigrupo numérico irredutível T contendo S com $F(S) = F(T)$. O resultado abaixo pode ser visto como um procedimento para construir um semigrupo numérico irredutível.

Lema 3.0.4. *Seja S um semigrupo numérico e suponha que existe*

$$h = \max\{x \in \mathbb{Z} \setminus S \mid F(S) - x \notin S \text{ e } x \neq \frac{F(S)}{2}\}. \tag{3.1}$$

Então, $S \cup \{h\}$ é um semigrupo numérico com número de Frobenius $F(S)$.

Demonstração. Note que $S \cup \{h\}$ tem complemento finito em $\mathbb{N}$ e $0 \in S \cup \{h\}$. Tome $H = \{x \in \mathbb{Z} \setminus S \mid F(S) - x \notin S \text{ e } x \neq \frac{F(S)}{2}\}$. Se $x \in H$, então $F(S) - x \notin S$, logo $F(S) - x \in \mathbb{Z} \setminus S$. Daí, $F(S) - (F(S) - x) = x \notin S$ e, portanto, $F(S) - x \in H$. Como x ou $F(S) - x$ são maiores que $\frac{F(S)}{2}$, segue que $h > \frac{F(S)}{2}$. Seja $s \in S \setminus \{0\}$, se $h + s \notin S$, por h ser máximo, temos que $F(S) - (h + s) = t \in S$. Assim, $F(S) - h = t + s \in S$ que, por construção, não pode ocorrer. De modo análogo, se $2h \notin S$, então $F(S) - 2h = t \in S$. No entanto, $h + t = F(S) - h$ não pode pertencer a S. ■

3.1 Semigrupos Numéricos Simétricos e Pseudossimétricos

Definição 3.1.1. *Seja S um semigrupo numérico. Dizemos que S é simétrico se S é irredutível e $F(S)$ é ímpar. Por outro lado, se $F(S)$ é par, dizemos que S é pseudossimétrico. Por questão de simplificação, nos limitaremos a escrever S simétrico ou pseudossimétrico.*

Proposição 3.1.2. *Sejam S um semigrupo numérico e $x \in \mathbb{Z} \setminus S$, então:*

1. *S é simétrico se, e somente se, $F(S) - x \in S$.*
2. *S é pseudossimétrico se, e somente se, $F(S) - x \in S$ ou $x = \frac{F(S)}{2}$.*

Demonstração. Demonstraremos o primeiro item, o segundo é demonstrado de forma análoga. Suponha que existe $x \in \mathbb{Z} \setminus S$ tal que $F(S) - x \notin S$, então existe h máximo, conforme definido em (3.1). Logo,

$S \cup \{h\}$ é um semigrupo numérico cujo número de Frobenius é $F(S)$. Contradição, pelo Teorema 3.0.3, S é maximal. Para a recíproca, basta provar que S é maximal no conjunto de todos semigrupos numéricos que não contém $F(S)$. Sejam T um semigrupo numérico tal que $S \subsetneq T$ e $x \in T \setminus S \subseteq \mathbb{Z} \setminus S$. Então, por hipótese, $F(S) - x \in S$ e, portanto, $F(S) - x \in T$, o que implica que $F(S) = x + (F(S) - x) \in T$. ■

Pela proposição supracitada, somos capazes de caracterizar semigrupos simétrico e pseudossimétricos da seguinte forma.

Corolário 3.1.3. *1. S é simétrico se, e somente se, $g(S) = \dfrac{F(S)+1}{2}$.*

2. S é pseudo-simétrico se, e somente se, $g(S) = \dfrac{F(S)+2}{2}$.

Observação 3.1.4. *Pela Observação 1.6.6 e pelo corolário acima, concluímos que semigrupos numéricos irredutíveis são os que possuem o menor gênero possível em comparação a $F(S)$.*

Observação 3.1.5. *Pela Proposição 1.6.5, todo semigrupo numérico gerado por dois elementos é simétrico.*

A partir de agora estaremos interessados em caracterizar semigrupos numéricos irredutíveis em função do seu conjunto de Apéry,

Lema 3.1.6. *Seja S um semigrupo numérico e $n \in S \setminus \{0\}$. Se $x, y \in S$ são tais que $x + y \in \mathrm{Ap}(S, n)$, então $\{x, y\} \subseteq \mathrm{Ap}(S, n)$.*

Demonstração. De fato, se $x + y \in \mathrm{Ap}(S, n)$, por definição, $x + y - n \notin S$. Suponha, por absurdo, $x \notin \mathrm{Ap}(S, n)$, então $x - n \in S$. Como $y \in S$, então $(x - n) + y \in S$, o que é uma contradição. A demonstração para y é análoga, logo, $\{x, y\} \subseteq \mathrm{Ap}(S, n)$. ■

Proposição 3.1.7. *Sejam S um semigrupo numérico e n um inteiro positivo de S. Seja $\mathrm{Ap}(S, n) = \{a_0 < a_1 < \ldots < a_{n-1}\}$ o conjunto Apéry de n em S. Então, S é simétrico se, e somente se, $a_i + a_{n-1-i} = a_{n-1}$ para todo $i \in \{0, \ldots, n-1\}$.*

Demonstração. Pela Proposição 1.6.4, temos que $F(S) = a_{n-1} - n$. Como $a_i - n \notin S$ e S é simétrico, $F(S) - (a_i - n) = a_{n-1} - a_i \in S$. Pelo Lema 3.1.6, existe $j \in \{0, \ldots, n-1\}$ tal que $a_{n-1} = a_i + a_j \in S$. Assim, por hipótese, $j = n - 1 - i$. Por outro lado, por hipótese temos que $\{a_{n-1}\} = \mathrm{Maximals}_{\leq_S}\mathrm{Ap}(S, n)$. Pela Proposição 1.6.14, $PF(S) = \{F(S)\}$, logo $\{F(S)\} = \mathrm{Maximals}_{\leq_S}(\mathbb{Z} \setminus S)$. Em outras palavras, se $x \in \mathbb{Z} \setminus S$ então $F(S) - x \in S$, ou seja, se $\dfrac{F(S)}{2}$ é um inteiro então $\dfrac{F(S)}{2} \in \mathbb{Z} \setminus S$. Daí, $F(S) - \dfrac{F(S)}{2} = \dfrac{F(S)}{2} \in S$, contradição. Portanto $F(S)$ é ímpar e, consequentemente, S é simétrico. ■

A partir dessa proposição, podemos concluir o seguinte resultado.

Corolário 3.1.8. *Seja S um semigrupo numérico. São equivalentes:*

1. *S é simétrico.*
2. $PF(S) = \{F(S)\}$.
3. $t(S) = 1$.

Demonstração. Observe que $F(S)$ sempre pertence a $PF(S)$. Portanto o segundo e terceiro itens são equivalentes. Já a equivalência entre o primeiro e segundo itens segue diretamente pela demonstração da proposição acima. ■

Podemos obter uma caracterização similar para semigrupos numéricos pseudossimétricos.

Lema 3.1.9. *Sejam S um semigrupo numérico pseudossimétrico e n um inteiro positivo. Então,* $\dfrac{F(S)}{2} + n \in \mathrm{Ap}(S, n)$.

Demonstração. Desde que $\dfrac{F(S)}{2} \notin S$, basta mostrar que $\dfrac{F(S)}{2} + n \in S$. Se isso não ocorrer, pela Proposição 3.1.2, $F(S) - (F(S)/2 + n) = F(S)/2 - n \in S$. O que implica que $F(S)/2 = F(S)/2 - n + n \in S$, que é impossível. ■

Proposição 3.1.10. *Seja S um semigrupo numérico cujo número de Frobenius é par e $n \in S \setminus \{0\}$. Então S é pseudossimétrico se, e somente se,*

$$\mathrm{Ap}(S, n) = \{a_0 < a_1 < \ldots < a_{n-2} = F(S) + n\} \cup \left\{\frac{F(S)}{2} + n\right\},$$

em que $a_i + a_{n-2-i} = a_{n-2}$ para todo $i \in \{0, \ldots, n-2\}$.

Demonstração. Pelo Lema 3.1.9, temos que $(F(S)/2) + n \in \mathrm{Ap}(S, n)$. Note que $(F(S)/2) + n < \mathrm{maxAp}(S, n) = (F(S) + n$. Se $w \in \mathrm{Ap}(S, n) \setminus \{(F(S)/2) + n\}$, então $w - n \notin S$ e $w - n \neq F(S)/2$. Pela Proposição 3.1.2, $F(S) - (w - n) \in S$ e, consequentemente, $\mathrm{maxAp}(S, n) - w = F(S) + n - w \in S$. Pelo Lema 3.1.6, $\mathrm{maxAp}(S, n) - w \in \mathrm{Ap}(S, n)$. Além disso, $\mathrm{maxAp}(S, n) - w \notin (F(S)/2) + n$ já que, caso contrário, $w = F(S)/2$. O restante da demonstração segue de forma análoga à feita em 3.1.7. Por outro lado, seja x um inteiro tal que $x \neq F(S)/2$ e $x \notin S$. Provaremos que $F(S) - x \in S$. Seja $w \in \mathrm{Ap}(S, n)$ tal que $w \equiv x \pmod{n}$, então $x = w - kn$ para algum $k \in \mathbb{N} \setminus \{0\}$. Separaremos em dois casos:

1. Se $w = (F(S)/2) + n$ então, $F(S) - x = F(S) - ((F(S)/2) + n - kn) = (F(S)/2) + (k-1)n$. Por outro lado, se $x \notin F(S)/2$, então $k \neq 1$ e, portanto, $k \geq 2$. Assim, $F(S) - x \in S$.

2. Se $w \neq (F(S)/2) + n$, $F(S) - x = F(S) - (w - kn) = F(S) + n - w + (k-1)n = a_{n-2} - w + (k-1)n \in S$, já que, por hipótese, $a_{n-2} - w \in S$.

■

Agora, já somos capazes de caracterizar os pseudossimétricos da seguinte forma.

Corolário 3.1.11. *4.16 Seja S um semigrupo numérico. São equivalentes:*

1. *S é pseudossimétrico.*
2. $PF(S) = \{F(S), \frac{F(S)}{2}\}$.

CAPÍTULO 4

Contagem de Soluções de Equações Diofantinas Lineares

Nos capítulos anteriores relacionamentos equações diofantinas lineares com semigrupos numéricos, apresentamos elementos que todo semigrupo numérico possui e uma forma fechada para encontrar e/ou contar esses elementos em dimensão dois, apresentamos, também, caracterizações e algoritmos para definir semigrupos numéricos saturados, com a propriedade Arf e caracterizamos semigrupos simétricos e pseudos-simétricos. O nosso intuito a partir de agora é apresentar uma ideia inicial de contagem de soluções de uma equação diofantina linear com três variáveis a partir da forma apresentada nesse trabalho, mesmo sabendo que já existem fórmulas fechadas para tal.

Relembremos a fórmula de contagem apresentada.

4.1 Equação diofantina linear com duas variáveis

Sejam a e b inteiros positivos e c um inteiro não negativo múltiplo de $\mathrm{mdc}(a, b)$. Considere n o maior inteiro não negativo tal que $c - n \cdot \mathrm{mmc}(a, b) \geq 0$. Então o número de soluções inteiras não negativas N da equação $ax + by = c$ será

$$N = \begin{cases} n+1, & \text{se } ax + by = c - n \cdot \mathrm{mmc}(a, b) \text{ possui solução em inteiros não negativos;} \\ n, & \text{caso contrário.} \end{cases}$$

Vale ressaltar que esse é um resultado autoral que, de certa forma, otimiza o processo de contagem de soluções que já existia. Deixaremos aqui os algoritmos já existentes de contagem. Os próximos teoremas estão demonstrados em [6] e [1], respectivamente.

Teorema 4.1.1. *Seja $N(a, b; n)$ a quantidade de soluções da equação diofantina linear $ax + by = n$, em que a, b, n são inteiros não negativos, (x, y) as soluções não negativas da equação e $\mathrm{mdc}(a, b) = 1$.*

$$N(a, b; n) = \frac{n + aa'(n) + bb'(b)}{ab} - 1,$$

em que $a'(n) \equiv -na^{-1} \pmod{b}$, $1 \leq a'(n) \leq b$, $b'(n) \equiv -nb^{-1} \pmod{a}$, $1 \leq b'(n) \leq a$.

4.2 Equações diofantinas lineares com três variáveis

Dados inteiros positivos a, b, c, denotamos por:

- b'_1 é o inteiro que satisfaz $b'_1 \equiv -nb^{-1} \pmod{a}$, $1 \leq b'_1 \leq a$. Além disso, c'_1 é o inteiro que satisfaz $c'_1 \equiv bc^{-1} \pmod{a}$, $1 \leq c'_1 \leq a$.
- c'_2 é o inteiro que satisfaz $c'_2 \equiv -nc^{-1} \pmod{b}$, $1 \leq c'_2 \leq b$. Além disso, a'_2 é o inteiro que satisfaz $a'_2 \equiv ca^{-1} \pmod{b}$, $1 \leq a'_2 \leq b$.
- a'_3 é o inteiro que satisfaz $a'_3 \equiv -na^{-1} \pmod{c}$, $1 \leq a'_3 \leq c$. Além disso, b'_3 é o inteiro que satisfaz $b'_3 \equiv ab^{-1} \pmod{c}$, $1 \leq b'_3 \leq c$.
- $N_1 = n(n + a + b + c) + cbb'_1(a + 1 - c'_1(b'_1 - 1)) + acc'_2(b + 1 - a'_2(c'_2 - 1)) + baa'_3(c + 1 - b'_3(a'_3 - 1))$.

Teorema 4.2.1. *Dados inteiros positivos a, b, c e n tais que $\mathrm{mdc}(a, b) = \mathrm{mdc}(a, c) = \mathrm{mdc}(b, c) = 1$. Pela notação acima, a quantidade de soluções não negativas da equação $ax + by + cz = n$ é dada por:*

$$N(a, b, c; n) = \frac{N_1}{2abc} + \sum_{i=1}^{b'_1-1} \left\lfloor \frac{ic'_1}{a} \right\rfloor + \sum_{i=1}^{c'_2-1} \left\lfloor \frac{ia'_2}{b} \right\rfloor + \sum_{i=1}^{a'_3-1} \left\lfloor \frac{ib'_3}{c} \right\rfloor - 2.$$

Demonstração. Ver [1, Theorem 5]. ■

Sabemos que determinar o número de Frobenius para semigrupos numéricos com dimensão superior a dois ainda é um problema em aberto. Em [5], sob certas restrições impostas a um semigrupo numérico S, é possível encontrar o número de Frobenius para dimensão três. Determinar não apenas o número de Frobenius, mas também todos os elementos do gênero de S, aqueles que não podem ser escritos como combinação linear dos geradores do semigrupo, se tornarão importantes para a proposta de contagem que será apresentada. Como vimos no Capítulo 1, podemos associar as equações diofantinas com semigrupos numéricos.

4.2.1 Princípio de Contagem

Seja $ax + by + cz = d$ uma equação diofantina linear a coeficientes naturais, cujas soluções são ternas de números naturais. Suponha $\text{mdc}(a, b) = 1$. Analisaremos a seguinte equação:

$$ax + by = d - cz.$$

Comecemos pelos casos mais simples, tome $c = \text{mmc}(a, b)$. Assim, aplicando o princípio de contagem do Teorema 1.3.1, a quantidade de soluções será a soma de todas as soluções N em cada caso de $z \in \{0, \ldots, m\}$, em que m é o maior valor possível tal que $d - cz \geq 0$.

Exemplo 4.2.2. Calcular a quantidade de soluções de $3x + 5y + 15z = 93$.

Solução. Seja N_z a quantidade de soluções de $3x + 5y = 93 - 15z$, $z \in \{0, \ldots, 6\}$.

$$\begin{aligned}
&z = 0, && 3x + 5y = 93, && N_0 = 7.\\
&z = 1, && 3x + 5y = 78, && N_1 = 6.\\
&z = 2, && 3x + 5y = 63, && N_2 = 5.\\
&z = 3, && 3x + 5y = 48, && N_3 = 4.\\
&z = 4, && 3x + 5y = 33, && N_4 = 3.\\
&z = 5, && 3x + 5y = 18, && N_5 = 2.\\
&z = 6, && 3x + 5y = 3, && N_6 = 1.
\end{aligned}$$

A quantidade de soluções é $\sum_{z=0}^{m} N_z = \sum_{z=0}^{6} N_z = \sum_{z=0}^{6} N_6 + z = \sum_{z=0}^{6} 1 + z = \sum_{z=1}^{7} z = 28$. Note que, caso N_6 tivesse 0 soluções, isso é, $3x + 5y = 3$ não tivesse solução, então, pelo Teorema 1.3.1, em cada N_z, $z \in \{1, \ldots, 6\}$ teríamos uma solução a menos. ■

Corolário 4.2.3. *Sejam $ax + by + cz = d$ a coeficientes inteiros não negativos, $\text{mdc}(a, b) = 1$ e $c = \text{mmc}(a, b)$. Considere m o maior inteiro não negativo tal que $d - m \cdot c \geq 0$. Então a quantidade de soluções N será:*

$$N = \begin{cases} \displaystyle\sum_{z=1}^{m+1} z, & \text{se } ax + by = d - m \cdot c \text{ possui solução em inteiros não negativos;} \\ \displaystyle\sum_{z=0}^{m} z, & \text{caso contrário.} \end{cases}$$

Demonstração. Seja $e = d - m \cdot c$. Se $ax + by = e$ possui uma ou nenhuma solução, então pelo Teorema 1.3.1, $ax + by = e + c$ possui duas ou uma solução, respectivamente. Assim,

$$ax + by = e + m \cdot \text{mmc}(a, b) = e + m \cdot c = d$$

terá $m + 1$ ou m soluções, respectivamente. Mas, para cada soma de $\mathrm{mmc}(a, b)$ temos um valor distinto em z que, consequentemente, gera uma solução distinta para $ax + by + cz = d$. Portanto, basta somar a quantidade de soluções em cada etapa. ■

A contagem que estamos usando começa a ficar mais complexa a partir do momento em que c é um valor qualquer, já que precisamos começar a analisar os restos de cada subtração de c e verificar se cada resto está no conjunto $G(S)$ ou não. Lembremos que $G(S)$ são os elementos que não podem ser escritos como combinação linear dos geradores a, b, c. Vamos mostrar dois exemplos, separadamente, em que $c \equiv \pm 1$ módulo $\mathrm{mmc}(a, b)$.

Exemplo 4.2.4. Calcular a quantidade de soluções de $3x + 5y + 16z = 93$.

Solução. Seja N_z a quantidade de soluções de $3x + 5y = 93 - 16z$, $z \in \{0, \ldots, 5\}$.

$$
\begin{array}{lll}
z = 0, & 3x + 5y = 93, & N_0 = 7. \\
z = 1, & 3x + 5y = 77, & N_1 = 5. \\
z = 2, & 3x + 5y = 61, & N_2 = 4. \\
z = 3, & 3x + 5y = 45, & N_3 = 4. \\
z = 4, & 3x + 5y = 29, & N_4 = 2. \\
z = 5, & 3x + 5y = 13, & N_5 = 1.
\end{array}
$$

Então a quantidade de soluções é $\displaystyle\sum_{z=0}^{5} N_z = 23$. ■

Note que, a partir de agora, não conseguimos uma fórmula fechada imediata para a contagem de soluções. Mas, se verificarmos os restos em cada passo, talvez seja possível. Seja r_m o resto de $d - z \cdot c$ módulo $\mathrm{mmc}(a, b)$ em cada passo.

$$
\begin{array}{llll}
z = 0, & 3x + 5y = 93, & N_0 = 7, & r_0 = 3. \\
z = 1, & 3x + 5y = 77, & N_1 = 5, & r_1 = 2. \\
z = 2, & 3x + 5y = 61, & N_2 = 4, & r_2 = 1. \\
z = 3, & 3x + 5y = 45, & N_3 = 4, & r_3 = 0. \\
z = 4, & 3x + 5y = 29, & N_4 = 2, & r_4 = 14. \\
z = 5, & 3x + 5y = 13, & N_5 = 1, & r_5 = 13.
\end{array}
$$

A cada passo m, os restos diminuem exatamente 1 unidade em comparação com o passo anterior. Assim, se tivermos todos os elementos de $G(S)$, em que S é o semigrupo numérico relacionado à equação, conseguimos contar a quantidade de soluções. Em outras palavras, como $c = \mathrm{mmc}(a, b) + 1$, devemos verificar se $r_z - 1$ está em $G(S)$ ou não. Caso esteja, em cada passo, a quantidade de soluções aumenta/diminui

linearmente e, caso contrário, haverá saltos de 2 unidades. No caso em que $r_n \notin G(S)$ e $r_{n-1} \in G(S)$ para $n \in \{1, \ldots, m\}$, a quantidade de soluções no passo n e $n-1$ será igual.

Exemplo 4.2.5. Calcular a quantidade de soluções de $3x + 5y + 14z = 93$.

Solução. Seja N_z a quantidade de soluções de $3x + 5y = 93 - 14z$, $z \in \{0, \ldots, 6\}$.

$$\begin{array}{llll} z = 0, & 3x + 5y = 93, & N_0 = 7, & r_0 = 3. \\ z = 1, & 3x + 5y = 79, & N_1 = 5, & r_1 = 4. \\ z = 2, & 3x + 5y = 65, & N_2 = 5, & r_2 = 5. \\ z = 3, & 3x + 5y = 51, & N_3 = 4, & r_3 = 6. \\ z = 4, & 3x + 5y = 37, & N_4 = 2, & r_4 = 7. \\ z = 5, & 3x + 5y = 23, & N_5 = 2, & r_5 = 8. \\ z = 6, & 3x + 5y = 9, & N_6 = 1, & r_6 = 9. \end{array}$$

Então a quantidade de soluções é $\sum_{z=0}^{6} N_z = 26$. ■

Note que, em comparação com o exemplo passado, que estávamos reduzindo em uma unidade o resto anterior, nesse caso, estamos aumentando e o processo de cálculo se dá de forma análoga. Para o caso geral, se torna ainda mais complexo. Suponha que tenhamos $c \equiv i \pmod{\text{mmc}(a, b)}$ em que $i \neq \pm 1$. Nesse caso, seria necessário encontrar um valor k tal que $kc \equiv \pm 1 \pmod{\text{mmc}(a, b)}$ e, dessa forma, contar a quantidade de soluções em cada etapa de forma similar às anteriores. Perceba que, seria necessário traçarmos também a sequência de restos de $c, 2c, \ldots, kc$, o que, também, não é imediato.

Exemplo 4.2.6. Calcule a quantidade de soluções de $3x + 5y + 7z = 93$.

Solução. Seja N_z a quantidade de soluções de $3x + 5y = 93 - 7z$, $z \in \{0, \ldots, 13\}$.

$$
\begin{array}{llll}
z = 0, & 3x + 5y = 93, & N_0 = 7, & r_0 = 3. \\
z = 1, & 3x + 5y = 86, & N_1 = 6, & r_1 = 11. \\
z = 2, & 3x + 5y = 79, & N_2 = 5, & r_2 = 4. \\
z = 3, & 3x + 5y = 72, & N_3 = 5, & r_3 = 12. \\
z = 4, & 3x + 5y = 65, & N_4 = 5, & r_4 = 5. \\
z = 5, & 3x + 5y = 58, & N_5 = 4, & r_5 = 13. \\
z = 6, & 3x + 5y = 51, & N_6 = 4, & r_6 = 6. \\
z = 7, & 3x + 5y = 44, & N_7 = 3, & r_7 = 14. \\
z = 8, & 3x + 5y = 37, & N_8 = 2, & r_8 = 7. \\
z = 9, & 3x + 5y = 30, & N_9 = 3, & r_9 = 0. \\
z = 10, & 3x + 5y = 23, & N_{10} = 2, & r_{10} = 8. \\
z = 11, & 3x + 5y = 16, & N_{11} = 1, & r_{11} = 1. \\
z = 12, & 3x + 5y = 9, & N_{12} = 1, & r_{12} = 9. \\
z = 13, & 3x + 5y = 2, & N_{13} = 0, & r_{13} = 2.
\end{array}
$$

Então a quantidade de soluções é $\displaystyle\sum_{z=0}^{13} N_z = 48$. ■

Vale ressaltar que, neste exemplo, os coeficientes formam um semigrupo numérico com dimensão de imersão máxima. É notável a diferença na quantidade de soluções quando comparamos um semigrupo com dimensão de imersão máxima e outro que não apresenta essa propriedade. Observa-se que, à medida que reduzimos a distância entre os geradores, a quantidade de soluções tende a crescer de forma intensa e desordenada, ao menos nessa primeira abordagem. No exemplo supracitado, note que $2 \cdot 7 = 14 \equiv -1 \pmod{15}$. Perceba que os restos estão em ordem crescente/decrescente a cada duas unidades. Assim, podemos separar a quantidade de soluções em dois somatórios, sendo eles,

$$N = \sum_{z=0}^{\lfloor \frac{m}{2} \rfloor} N_{2z} + \sum_{z=1}^{\lfloor \frac{m}{2} \rfloor + 1} N_{2z-1}.$$

Com uma fórmula fechada para a variação de restos, poderíamos calcular separadamente cada um dos somatórios. Mas, afinal, se $kc \equiv \pm 1 \pmod{\operatorname{mmc}(a, b)}$ e conhecido um princípio de contagem para quantidade de soluções com variação de uma unidade nos restos, então poderíamos separar a quantidade de soluções em k somatórios conhecidos? A cada k passos, os restos r_i, r_{i+k}, r_{i+2k}, $\ldots$ estariam em ordem linear? Se k é ímpar, então o semigrupo associado aos geradores dos coeficientes dessa equação será pseudossimétrico? Semigrupos numéricos irredutíveis geram, a cada passo, uma quantidade linear

de soluções de sua equação associada? Dado um semigrupo, como gerar seu conjunto $G(S)$? Será que a existência de uma fórmula fechada para o cálculo do Frobenius de um semigrupo, implica que também existe uma fórmula fechada para a contagem de soluções? Deixamos esses questionamentos como a motivação para o próximo estudo sobre semigrupos numéricos e a quantidade de soluções de equações diofantinas lineares.

Referências Bibliográficas

[1] BINNER, D. S. "**The number of solutions to $ax + by + cz = n$ and its relation to quadratic residues**". Em: ***Journal of Integer Sequences*** 23.6 (2020), Article 20.6.5 (citado nas páginas 40, 41).

[2] KRAFT, J. S.; WASHINGTON, L. C. ***An introduction to number theory with cryptography***. Boca Raton: Chapman e Hall/CRC, 2018 (citado na página 14).

[3] MARTINEZ, F. B. et al. ***Teoria dos números: um passeio com primos e outros números***. Rio de Janeiro: IMPA, 2018 (citado na página 14).

[4] ROSALES, J. C.; GARCÍA-SÁNCHEZ, P. A. ***Numerical Semigroups***. Vol. 20. Developments in Mathematics. New York: Springer, 2009 (citado na página 17).

[5] TRIPATHI, A. "**Formulae for the Frobenius number in three variables**". Em: ***Journal of Number Theory*** 170 (2017), pp. 368–389 (citado na página 41).

[6] TRIPATHI, A. "**The number of solutions to $ax + by = n$**". Em: ***The Fibonacci Quarterly*** 38.4 (2000), pp. 290–294 (citado na página 40).