GIORDANNI ZOPPELLARO

UM ESTUDO SOBRE SEMIGRUPOS NUMÉRICOS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título de *Magister Scientiae*.

Orientadora: Danielle Franco Nicolau

FLORESTAL – MINAS GERAIS
2021

Ficha catalográfica elaborada pela Biblioteca da Universidade Federal de Viçosa - Campus Florestal

T
Z88e
2021

Zoppellaro, Giordanni, 1992-
Um estudo sobre semigrupos numéricos [recurso eletrônico] / Giordanni Zoppellaro. – Florestal, MG, 2021.
122 f.: il. (algumas color.).

Orientador: Danielle Franco Nicolau.
Dissertação (mestrado) - Universidade Federal de Viçosa.
Referências bibliográficas: f.121-122.

1. Matemática. 2. Teoria dos grupos. 3. Semigrupos. I. Universidade Federal de Viçosa. Instituto de Ciências Exatas e Tecnológicas. Mestrado Profissional em Matemática em Rede Nacional. II. Título.

512.2

Bibliotecário(a) responsável: Maria Aparecida Alves de Oliveira 1174

GIORDANNI ZOPPELLARO

UM ESTUDO SOBRE SEMIGRUPOS NUMÉRICOS

Dissertação apresentada à Universidade Federal de Viçosa, como parte das exigências do Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, para obter o título de *Magister Scientiae*.

APROVADA: 18 de junho de 2021.

Assentimento:

Giordanni Zoppellaro

Giordanni Zoppellaro
Autor

Danielle Franco Nicolau
Orientadora

Dedicatória

Dedico esta dissertação ao meu pai, Derly Zoppellaro, e a minha mãe, Rosilene Alves Vieira, que sempre me apoiaram em todos os momentos da minha vida e se dedicaram ao máximo para que eu pudesse realizar os meus sonhos.

Agradecimentos

Primeiramente, gostaria de agradecer a Deus, ao meu mentor e a espiritualidade amiga por me permitirem concluir mais esta etapa de vida. Em segundo lugar, gostaria de agradecer aos meus pais, Derly Zoppellaro e Rosilene Alves Vieira, por tudo que fizeram e fazem por mim. Sem o suporte de vocês eu jamais poderia ter chegado até aqui. Se eu pude ter o luxo de trabalhar menos para poder estudar mais, se eu sempre tive um teto para morar, roupa para vestir, comida para comer, se sempre encontrei na nossa casa um lar acolhedor e todo o apoio que precisei, foi porque vocês abriram mão dos próprios sonhos para que eu pudesse realizar os meus. A vocês o meu eterno obrigado. Amo muito vocês!

Aos meus familiares, agradeço todo o apoio e os momentos felizes que passamos juntos. Ao João, agradeço o companheirismo e suporte ao longo desta jornada. Aos meus amigos, agradeço a compreensão nos momentos de ausência por causa dos estudos e por estarem sempre disponíveis quando precisava relaxar e espairecer. À Marcela, agradeço por me ajudar a cuidar de mim durante todo esse período.

Gostaria de agradecer especialmente a minha orientadora, Danielle Franco Nicolau, por me apresentar e permitir estudar estas estruturas algébricas tão interessantes que são os semigrupos numéricos. Obrigado, Dani, por toda a paciência e ajuda durante a realização deste trabalho. Aos demais professores da UFV, agradeço por enriquecerem grandemente a minha formação como matemático e professor. Aos colegas de curso, agradeço os diversos momentos de estudo que passamos juntos. Agradeço também aos professores da UFMG, instituição onde me graduei, especializei e construí a base que precisava para que pudesse concluir o mestrado.

A todos que de alguma forma contribuíram para a realização deste sonho, o meu muito obrigado!

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

Resumo

ZOPPELLARO, Giordanni, M.Sc., Universidade Federal de Viçosa, junho de 2021. **Um Estudo Sobre Semigrupos Numéricos**. Orientadora: Danielle Franco Nicolau.

A proposta deste trabalho é apresentar semigrupos numéricos e alguns de seus invariantes e propriedades. Também iremos tratar sobre o conjunto Apéry, algumas cadeias de semigrupos, ideais e ideais biduais. Abordaremos as famílias de semigrupos simétricos, pseudossimétricos, quase simétricos, Arf e semigrupos modulares. Mostraremos uma relação entre semigrupos numéricos e as soluções naturais de uma equação diofantina linear e também a relação entre semigrupos modulares e as inequações diofantinas modulares. Apresentaremos um algoritmo para decidir se um semigrupo é modular ou não e estabeleceremos uma conexão entre semigrupos cujo módulo é mínimo com respeito ao seu peso e os chamados UESY-semigrupos. Por fim, propomos algumas atividades que podem ser utilizadas na Educação Básica.

Palavras-chave: Semigrupos numéricos. Semigrupos numéricos modulares. Semigrupos simétricos. Semigrupos pseudossimétricos. Semigrupos quase simétricos. Semigrupos Arf. UESY-semigrupos. Equação diofantina linear. Inequação diofantina modular.

Abstract

ZOPPELLARO, Giordanni, M.Sc., Universidade Federal de Viçosa, June, 2021. **A Study About Numerical Semigroups**. Adviser: Danielle Franco Nicolau.

The purpose of this paper is to present numerical semigroups and some of its invariants and properties. We also discuss about the Apéry set, some semigroup chains, ideals and bidual ideals. We bring some semigroup families, such as symmetric, pseudosymmetric, almost symmetric, Arf and modular semigroups. It is shown a relation between numeric semigroups and the natural solutions of a linear diophantine equation and also a relation between modular semigroups and modular diophantine inequalities. We present an algorithm to decide whether a numerical semigroup is a modular one and establish a connection between modular semigroups whose moduli are minimal with respect to their weights and UESY-semigroups. Finally, we propose some activities that can be used in secondary and high school.

Keywords: Numerical semigroups. Modular numerical semigroups. Symmetric semigroups. Pseudosymmetric semigroups. Almost symmetric semigroups. Arf semigroups. UESY-semigroups. Linear diophantine equation. Modular diophantine inequation.

Lista de Figuras

Sumário

1

Introdução

Nesta dissertação, estudaremos semigrupos numéricos e algumas de suas propriedades. Um semigrupo numérico é um subconjunto S dos naturais $\mathbb{N} = \{0,\ 1,\ 2,\ \ldots\}$ que é fechado para a soma, contém o zero e cujo complementar $\mathbb{N} \setminus S$ é finito. Também iremos apresentar uma relação entre semigrupos e equações diofantinas lineares e inequações diofantinas modulares.

Semigrupos numéricos são estudados desde o século XIX e possuem aplicações em Álgebra Comutativa, Geometria Algébrica, Matemática Discreta e Teoria de Códigos. Alguns problemas de enunciado simples recaem na utilização de semigrupos numéricos na sua resolução, como o caso das moedas de Fröbenius (veja, por exemplo, [2]): Suponha que em uma cidade existam apenas moedas de \$2 e de \$7. Qual a maior quantia que não pode ser paga utilizando apenas essas moedas sem que haja troco? Embora o contexto seja de fácil compreensão, tais problemas nem sempre apresentam soluções simples de serem encontradas.

Este trabalho foi dividido da seguinte maneira: O capítulo 2 apresenta alguns preliminares aritméticos sobre números inteiros, necessários para o desenvolvimento da teoria, tais como divisibilidade, algoritmo de Euclides, mmc e mdc. Também são apresentadas as equações diofantinas lineares.

No capítulo 3 introduzimos os semigrupos numéricos e definimos alguns de seus invariantes como multiplicidade, condutor, número de Fröbenius e gênero. É apresentado o conjunto Apéry, algumas cadeias de semigrupos, ideais canônicos e biduais. Definimos também semigrupos simétricos, pseudossimétricos, quase simétricos e Arf, e apresentamos algumas de suas propriedades.

O capítulo 4 trata de semigrupos modulares do tipo $S = (a,b)$ e sua relação com inequações diofantinas modulares. É apresentado um algoritmo que permite determinar quando um semigrupo numérico é modular ou não. Em seguida, abordamos semigrupos modulares cujo módulo é igual ao seu peso mais 2 e sua relação com os chamados UESY-semigrupos.

Finalmente, no capítulo 5 apresentamos algumas propostas de atividades que podem ser aplicadas na Educação Básica abordando semigrupos numéricos e equações diofantinas lineares com o uso do software GeoGebra.

2

Preliminares Aritméticos

O objetivo deste capítulo é introduzir alguns conceitos e propriedades básicas envolvendo os números inteiros e, ao final, apresentar as equações diofantinas lineares. As principais referências para este capítulo são [8], [9] e [12].

2.1 Conceitos iniciais sobre números inteiros

Vamos considerar em $\mathbb{Z}$ as seguintes relações: dados $a,\ b \in \mathbb{Z}$ dizemos que a é menor que b, e representamos $a < b$, se existe $r \in \mathbb{N} \setminus \{0\}$ tal que $a + r = b$. Diremos que a é menor ou igual a b se $a < b$ ou $a = b$, e escrevemos $a \leq b$.

A relação $\leq$ é uma relação de ordem em $\mathbb{Z}$, pois é reflexiva, antissimétrica e transitiva, como podemos verificar em [8]. Essa relação de ordem nos garante algumas propriedades interessantes dos inteiros que veremos logo a seguir.

Definição 2.1: Um subconjunto A de $\mathbb{Z}$ é dito **limitado inferiormente** se existir $c \in \mathbb{Z}$ tal que $c \leq x$, para todo $x \in A$. Tal elemento c é denominado **cota inferior** de A. Convencionalmente, consideramos o conjunto vazio, $\{\ \}$, limitado inferiormente, tendo qualquer número como sua cota inferior.

Exemplo 2.1.1: Considere os subconjuntos de $\mathbb{Z}$

$$A_1 = \{x \in \mathbb{Z} \mid x^2 - 4 \leq 0\},$$
$$A_2 = \{x \in \mathbb{Z} \mid x^2 - 4 > 0\}.$$

Note que os elementos de A_1 são os inteiros x tais que $-2 \leq x \leq 2$. Já A_2 é formado pelos inteiros x tais que $x < -2$ ou $x > 2$. Temos então A_1 limitado inferiormente com -2 como sua cota inferior. Já A_2 não é limitado inferiormente.

Definição 2.2: Seja A um subconjunto de $\mathbb{Z}$. Um elemento $a \in A$ é dito **menor elemento** de A se $a \leq x$, para todo $x \in A$.

Exemplo 2.1.2: No exemplo acima, -2 é o menor elemento de A_1.

Vamos considerar o seguinte axioma em $\mathbb{Z}$:

Axioma 2.3 (Princípio da Boa Ordenação): Seja A um subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente. Então A possui menor elemento.

Em particular, todo subconjunto não vazio de $\mathbb{N}$ possui menor elemento, uma vez que qualquer subconjunto de $\mathbb{N}$ é limitado inferiormente por 0.

A partir do axioma 2.3 provamos diversas propriedades de $\mathbb{Z}$.

Proposição 2.4: Não existe nenhum número inteiro c tal que $0 < c < 1$.

Demonstração. Suponha, por absurdo, que exista tal inteiro c. Desse modo, o conjunto $A = \{x \in \mathbb{Z} \mid 0 < x < 1\}$ é não vazio e limitado inferiormente. Pelo Princípio da Boa Ordenação, A possui um menor elemento a. Uma vez que $a \in A$, temos que $0 < a < 1$ e, multiplicando esta desigualdade por a, obtemos

$$0 < a^2 < a < 1,$$

o que mostra que $a^2 \in A$ e $a^2 < a$, contradizendo o fato de a ser menor elemento de A. Portanto, devemos ter $A = \emptyset$.

□

Corolário 2.5: Dado $n \in \mathbb{Z}$, não existe $m \in \mathbb{Z}$ tal que $n < m < n + 1$. Em outras palavras, o sucessor de n é $n + 1$.

Demonstração. Dado n inteiro, suponha que exista $m \in \mathbb{Z}$ tal que $n < m < n + 1$. Então temos que $0 < m - n < 1$, contradizendo a proposição 2.4.

□

Corolário 2.6 (Propriedade Arquimediana dos Inteiros): Sejam a e b inteiros, com b não nulo. Então existe n inteiro tal que $nb > a$.

Demonstração. Como b é não nulo, segue que $|b| \neq 0$ e, da proposição anterior, temos que $|b| \geq 1$. Desse modo,

$$(|a| + 1)|b| \geq |a| + 1 > |a| \geq a.$$

Se $b > 0$, então $|b| = b$, e o resultado segue tomando $n = |a| + 1$. Agora, se $b < 0$, então $|b| = -b$, e assim basta tomar $n = -(|a| + 1)$.

□

Embora a divisão de um número inteiro por outro nem sempre seja possível, podemos definir em $\mathbb{Z}$ a relação de divisibilidade, dizendo quando a divide b.

Definição 2.7: Dados dois números inteiros a e b, dizemos que a **divide** b, e escrevemos $a \mid b$, se existe $c \in \mathbb{Z}$ tal que $b = ca$. Nessas condições, também é possível dizer que a é **divisor ou fator** de b, que b é **múltiplo** de a, ou ainda que b é **divisível** por a. Caso a não seja divisor de b, escrevemos $a \nmid b$.

Exemplo 2.1.3: Note que $6 \mid 84$, pois $84 = 14.6$ e que $3 \nmid 28$, pois não existe inteiro c tal que $28 = 3c$.

A aritmética em $\mathbb{Z}$ é muito interessante. Podemos encontrar divisores comuns de dois inteiros, e o maior deles tem um papel fundamental na teoria dos números inteiros.

Definição 2.8: Dados dois números inteiros a e b, dizemos que $d \geq 0$ é o **máximo divisor comum**, ou simplesmente mdc, de a e b se:

(i) d é divisor comum de a e b, ou seja, $d \mid a$ e $d \mid b$;

(ii) se existe $c \in \mathbb{Z}$ tal que $c \mid a$ e $c \mid b$, então $c \mid d$.

Representamos o mdc de a e b por $mdc(a,b)$, ou simplesmente (a,b). Como $1 \mid a$ e $1 \mid b$, o mdc entre dois números inteiros a e b sempre existe. Se $(a,b) = 1$, dizemos que a e b são **primos entre si** ou **coprimos**.

Exemplo 2.1.4: Observando que $24 = 8.3$ e $40 = 8.5$, temos que $(24,40) = 8$. Por outro lado, como $6 = 2.3$ e $35 = 5.7$, temos que $(6,35) = 1$, e 6 e 35 são primos entre si.

Números inteiros podem ser separados em grupos, de acordo com seus divisores. Por exemplo, começando por 2, temos o grupo dos números inteiros que possuem 2 como divisor, ditos números pares. Caso contrário, são denominados números ímpares.

Possuem 2 como divisor: $S_2 = \{2,\ 4,\ 6,\ 8,\ 10,\ 12,\ 14,\ \ldots\}$.

A partir do 2, o próximo inteiro que não pertence a S_2 é o 3. Tomamos então S_3, o conjunto dos inteiros que possuem 3 como divisor:

$$S_3 = \{3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ \ldots\}.$$

Note que o próximo inteiro que não está em S_2 e S_3 é o 5. Analogamente, temos

$$S_5 = \{5,\ 10,\ 15,\ 20,\ 25,\ 30,\ 35\ \ldots\}.$$

Podemos continuar este processo definindo

$$S_n = \{\text{inteiros que possuem } n \text{ como divisor}\}$$

para n não pertencente a S_i, com $2 \leq i \leq n-1$. Observe que $i \in S_i$ para todo i e é o primeiro elemento de S_i (escrito do menor para maior). Assim, esse inteiro n é o primeiro elemento de subconjuntos de $\mathbb{Z}$ construídos como acima.

Esses inteiros são elementos notáveis, de grande importância, e recebem o nome de números primos. Um identificação dos números primos pode ser verificada na definição a seguir:

Definição 2.9: Um número inteiro maior que 1 é chamado de **número primo** se só admite 1 e ele próprio como divisores positivos. Um número maior que 1 que não é primo é dito **composto**. O número 1 não é considerado nem primo e nem composto.

Exemplo 2.1.5: Os números 2, 3, 5, 7, 11, 13, 17 e 19 são números primos, e 4, 6, 9 e 15 são compostos.

Proposição 2.10: Seja $n > 1$ um número inteiro. Então o menor divisor de n diferente de 1 é um número primo.

Demonstração. Se n é primo não há o que mostrar, pois seu único divisor diferente de 1 é o próprio n. Suponha então n composto e seja p o menor divisor de n diferente de 1. Então existe $c \in \mathbb{N}$, com $1 < c < n$, tal que $n = pc$. Suponha que p seja composto. Então existe $q \in \mathbb{N}$, com $1 < q < p$ tal que $p = kq$ para algum $k \in \mathbb{N}$. Desse modo, temos que $n = pc = kqc$, mostrando assim que q divide n, contrariando a minimalidade de p. Portanto, p deve ser primo.

□

Duas perguntas surgem naturalmente: quantos números primos existem? Como encontrá-los? A segunda é tema de pesquisa entre os matemáticos até os dias atuais, pois não há uma fórmula para números primos, o que dificulta encontrá-los. Felizmente, a primeira pergunta pode ser respondida através de um dos resultados mais clássicos da Matemática: o Teorema de Euclides.

Teorema 2.11 (Teorema de Euclides): Existem infinitos números primos.

Demonstração. Suponha que exista uma quantidade finita de números primos, denotados por

$$p_1,\ p_2, \ldots,\ p_k.$$

Considere o número natural

$$n = p_1 p_2 \ldots p_k + 1,$$

e seja p o menor fator primo de n. Como supomos a quantidade de primos finita, devemos ter $p = p_i$ para algum $i \in \{1,\ 2, \ldots,\ k\}$ e, desse modo, $p \mid p_1 p_2 \ldots p_k$. Mas então $p \mid 1$, o que é um absurdo. Portanto, a quantidade de primos é infinita.

□

Um dos destaques de $\mathbb{Z}$ é a Divisão de Euclidiana, propriedade não encontrada em qualquer conjunto.

Teorema 2.12 (Divisão Euclidiana): Dados dois números inteiros a e b, com $b \neq 0$, existem dois únicos números inteiros q e r, chamados respectivamente de quociente e resto, tais que

$$a = bq + r, \quad \text{com} \quad 0 \leq r < |b|.$$

Demonstração. Considere o conjunto

$$A = \{a - bq \mid q \in \mathbb{Z}\} \cap \mathbb{N}.$$

Existência: Pela Propriedade Arquimediana, corolário 2.6, existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, ou seja, $a - nb > 0$, mostrando que A é não vazio. Seja $r = a - bq$ o menor elemento de A (tal elemento existe pelo Princípio da Boa Ordenação). Naturalmente, $r \geq 0$, portanto falta mostrar que $r < |b|$. Suponha por absurdo que $r \geq |b|$. Então existe um inteiro não negativo s tal que $r = |b| + s$, ou seja, $s = r - |b|$, mostrando que $0 \leq s < r$, já que $|b| > 0$. Se $b > 0$, então $s = r - |b| = a - bq - b = a - b(q+1) \in A$, o que é um absurdo, pois r é o menor elemento de A. Analogamente, se $b < 0$, então $s = r - |b| = a - bq + b = a - b(q-1) \in A$, o que também é um absurdo, pois r é o menor elemento de A. Logo, devemos ter $r < |b|$.

Unicidade: Suponha que existam $q,\ q_1,\ r,\ r_1 \in \mathbb{Z}$, com $0 \leq r < |b|$ e $0 \leq r_1 < |b|$, tais que $bq + r = a = bq_1 + r_1$, ou seja, $b(q - q_1) = r_1 - r$. Desse modo, temos que

$$-|b| < -r \leq r_1 - r \leq r_1 < |b|,$$

ou seja, $|r_1 - r| < |b|$. Como $b(q - q_1) = r_1 - r$, segue que

$$|b||q - q_1| = |r_1 - r| < |b|,$$

o que só é possível se $|q - q_1| = 0$, ou seja, se $q = q_1$. Por fim, se $q = q_1$, então $r_1 - r = b(q - q_1) = 0$ e, portanto, $r_1 = r$.

□

Exemplo 2.1.6: O quociente e o resto da divisão de 47 por 3 são $q = 15$ e $r = 2$, pois $47 = 3.15 + 2$. O quociente e o resto da divisão de -7 por 2 são $q = -4$ e $r = 1$, já que $-7 = 2.(-4) + 1$.

Lema 2.13: Sejam $a, b \in \mathbb{Z}$.

(i) $a \mid b \iff (a,b) = |a|$;

(ii) Se $a \nmid b$, sejam $q,\ r \in \mathbb{Z}$ tais que $b = qa + r$, com $0 < r < a$. Então

$$(a,b) = (a,r) = (a,b - qa).$$

Demonstração. Para a parte (i), note que se $a \mid b$, então $|a|$ divide a e $|a|$ divide b. Agora, se c é um divisor comum de a e b, então c divide $|a|$, mostrando que $(a,b) = |a|$.

Reciprocamente, se $(a,b) = |a|$, então $|a|$ divide b e, portanto, $a \mid b$.

Para a parte (ii), considere $(a,r) = (a,b - qa) = d$. Como $d \mid a$ e $d \mid (b - qa)$, temos que d divide $b = b - qa + qa$. Logo, d é divisor comum de a e b. Seja agora $c \in \mathbb{Z}$ tal que $c \mid a$ e $c \mid b$. Mas então c divide $b - qa$ e, portanto, $c \mid d$, o que nos permite concluir que $(a,b) = d$.

□

Vamos enunciar agora um importante algoritmo que nos permite determinar o mdc de dois números inteiros:

Teorema 2.14 (Algoritmo de Euclides): Dados dois inteiros positivos a e b, aplicamos sucessivamente a divisão euclidiana para obter a seguinte sequência de igualdades

$$\begin{cases} a = bq_1 + r_1, & 0 \leq r_1 < b, \\ b = r_1q_2 + r_2, & 0 \leq r_2 < r_1, \\ r_1 = r_2q_3 + r_3, & 0 \leq r_3 < r_2, \\ \vdots & \\ r_{n-2} = r_{n-1}q_n + r_n, & 0 \leq r_n < r_{n-1}, \\ r_{n-1} = r_nq_{n+1}, & \end{cases} \tag{2.1}$$

até algum r_n dividir r_{n-1}. Assim, $(a,b) = r_n$, ou seja, o mdc de a e b é o último resto não nulo no processo de divisão acima.

Demonstração. Observe que o processo de divisão em (2.1) é finito, uma vez que cada número r_i da sequência de inteiros não negativos $r_1 > r_2 > \ldots > r_n$ pertence ao conjunto $\{r \in \mathbb{Z} \mid 0 \leq r < a\}$, que é limitado inferiormente e, pelo Princípio da Boa Ordenação, possui menor elemento r_n. Aplicando o lema 2.13 nas igualdades de (2.1), temos que

$$(a,b) = (a,r_1) = (r_1,r_2) = \ldots = (r_{n-1},r_n) = r_n.$$

□

Exemplo 2.1.7: Determinemos o mdc de 747 e 216 através do Algoritmo de Euclides:

$$\begin{aligned} 747 &= 3.216 + 99 \\ 216 &= 2.99 + 18 \\ 99 &= 5.18 + 9 \\ 18 &= 2.9 \end{aligned}$$

Como o último resto não nulo na sequência de divisões acima é 9, segue que $(747,216) = 9$.

Teorema 2.15 (Teorema de Bachet-Bézout): Sejam a e b inteiros não ambos nulos tais que $(a,b) = d$. Então existem números inteiros x e y tais que

$$ax + by = d.$$

Demonstração. Consideremos o conjunto $A(a,b) = \{ax + by \mid x,\ y \in \mathbb{Z}\}$, ou seja, o conjunto das combinações lineares inteiras de a e b. Note que S é não vazio, pois quando $x = y = 0$, temos que $0 \in S$. Seja $m = \min A(a,b) \cap \mathbb{N} \setminus \{0\}$, ou seja, $m = ax + by$ o menor inteiro positivo contido em $A(a,b)$ (tal número existe pelo Princípio da Boa Ordenação) e suponha que $m \nmid a$. Pela divisão euclidiana, existem inteiros q e r tais

que $a = qm + r$, com $0 < r < m$. Então

$$r = a - qm = a - q(ax + by) = a(1 - qx) + b(-qy),$$

mostrando que $r \in A(a,b)$, o que é um absurdo, pois m é o menor inteiro positivo em $A(a,b)$. Portanto, $m \mid a$ e, analogamente, $m \mid b$. Desse modo, $m \mid d = (a,b)$. Como $(a,b) = d$, existem $a_1,\ b_1 \in \mathbb{Z}$ tais que $a = da_1$ e $b = db_1$. Assim,

$$m = ax + by = da_1x + db_1y = d(a_1x + b_1y),$$

o que mostra que $d \mid m$ e, portanto, devemos ter $m = d$.

□

Observação 2.16: O Teorema de Bachet-Bézout nos permite concluir que o mdc de a e b é a menor combinação linear inteira positiva desses dois números, ou seja, $(a,b) = \min A(a,b)$.

Corolário 2.17: Dados $a,\ b \in \mathbb{Z}$ não ambos nulos e $n \in \mathbb{N}$, tem-se que

$$(na,nb) = n(a,b).$$

Demonstração. Note que

$$(na,nb) = \min A(na,nb) = n \min A(a,b) = n(a,b).$$

□

Corolário 2.18: Dados a e b inteiros não ambos nulos, tem-se que

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$$

Demonstração. Pelo corolário anterior, temos que

$$(a,b)\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = \left((a,b)\frac{a}{(a,b)}, (a,b)\frac{b}{(a,b)}\right) = (a,b),$$

provando o resultado.

□

Proposição 2.19: Dois números inteiros a e b são primos entre si se, e somente se, existem x e y inteiros tais que

$$ax + by = 1.$$

Demonstração. Suponha que a e b são primos entre si, ou seja, $(a,b) = 1$. O Teorema de Bachet-Bézout (2.15) nos garante que existem x e y inteiros tais que $ax + by = 1$.

Reciprocamente, suponha que existam inteiros x e y tais que $ax + by = 1$ e seja $d = (a,b)$. Temos que $d \mid ax + by$, ou seja, $d \mid 1$, o que só é possível se $d = 1$, mostrando assim que a e b são primos entre si.

□

Lema 2.20 (Lema de Gauss): Sejam a, b e c números inteiros. Se $a \mid bc$ e $(a,b) = 1$, então $a \mid c$.

Demonstração. Se $a \mid bc$, então existe $k \in \mathbb{Z}$ tal que $bc = ak$. Se $(a,b) = 1$, pela proposição 2.19 existem x e y inteiros tais que

$$1 = ax + by.$$

Multiplicando ambos os membros da igualdade por c, segue que

$$c = axc + byc.$$

Como $bc = ak$, temos que

$$c = axc + aky = a(xc + ky),$$

mostrando que $a \mid c$.

□

Poderíamos nos perguntar quando, em geral, sempre que $a \mid bc$, então $a \mid b$ ou $a \mid c$. A resposta é apresentada no lema abaixo:

Lema 2.21 (Lema de Euclides): Sejam $a,\ b$ e p números inteiros, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonstração. Suponha, sem perda de generalidade, que $p \mid ab$ mas $p \nmid a$. Portanto, $(p, a) = 1$ e, pelo lema 2.20 (Lema de Gauss), segue que $p \mid b$.

□

Corolário 2.22: Sejam $p,\ p_1, \ldots,\ p_n$ números primos. Se $p \mid p_1 \ldots\ p_n$, então $p = p_i$, para algum $i = 1, \ldots,\ n$.

Demonstração. Provaremos por indução sobre n, o número de fatores primos de $p_1 \ldots\ p_n$. Se $n = 1$, o resultado é trivial, pois se $p \mid p_i$, então $p = p_i$. Suponha o resultado válido para todo natural menor do que n. Sejam $p,\ p_1, \ldots,\ p_n$ números primos e suponha que $p \mid p_1 \ldots\ p_n$. Se $p = p_n$, não há o que provar. Se $p \neq p_n$, então $p \nmid p_n$ e, portanto, $p \mid p_1 \ldots\ p_{n-1}$. Pela hipótese de indução, segue que $p = p_i$, para algum $i = 1, \ldots,\ n-1$.

□

Definição 2.23: Dados dois números inteiros a e b, dizemos que $m \geq 0$ é o **mínimo múltiplo comum**, ou simplesmente mmc, de a e b se:

(i) m é um múltiplo comum de a e b, ou seja, $a \mid m$ e $b \mid m$;

(ii) se existe $c \in \mathbb{Z}$ tal que $a \mid c$ e $b \mid c$, então $m \mid c$.

Representamos o mmc de a e b por $mmc(a, b)$, ou simplesmente $[a, b]$.

Note que $[a, b] = 0$ se, e somente se, $a = 0$ ou $b = 0$. De fato, se $a = 0$ ou $b = 0$, então 0 é o único múltiplo comum de a e b, portanto $[a, b] = 0$. Reciprocamente, se $[a,b] = 0$, então $0 \mid ab$, logo $ab = 0$ e, portanto, $a = 0$ ou $b = 0$.

Se $a \mid m$ e $b \mid m$, naturalmente $(-a) \mid m$ e $(-b) \mid m$, e pode-se mostrar que

$$[-a,b] = [a, -b] = [-a, -b] = [a,b].$$

Exemplo 2.1.8: Listando os primeiros múltiplos de 6 e 10, podemos ver que [6,10] = 30:

Múltiplos de 6: $M(6) = \{0,\ 6,\ 12,\ 18,\ 24,\ 30,\ 36,\ 42,\ \ldots\}$.

Múltiplos de 10: $M(10) = \{0,\ 10,\ 20,\ 30,\ 40,\ 50,\ 60,\ 70,\ \ldots\}$.

A proposição abaixo nos dá uma relação interessante entre o mdc e o mmc de dois números inteiros:

Proposição 2.24: Dados dois números inteiros a e b, temos que

$$[a,b](a,b) = |ab|.$$

Demonstração. Se $a = 0$ ou $b = 0$, a igualdade é trivialmente satisfeita. Suponha, sem perda de generalidade, que a e b são naturais não nulos. Temos que

$$\frac{ab}{(a,b)} = a\frac{b}{(a,b)} = b\frac{a}{(a,b)}$$

é um múltiplo comum de a e b. Pela minimalidade de $[a,b]$, segue que

$$[a,b] \leq \frac{ab}{(a,b)} \implies [a,b](a,b) \leq ab \tag{2.2}$$

Pelo Algoritmo de Euclides, existem $q,\ r \in \mathbb{Z}$ tais que

$$ab = [a,b]q + r, \qquad 0 \leq r < [a,b].$$

Note que r deve ser múltiplo comum de a e b, uma vez que ab e $[a,b]$ também o são. Como $[a,b]$ é o menor múltiplo comum, devemos ter $r = 0$. Portanto, $[a,b] \mid ab$. O inteiro

$$\frac{ab}{[a,b]} = \frac{a}{[a,b]/b} = \frac{b}{[a,b]/a}$$

é um divisor comum de a e b. Como o mdc é o maior divisor comum, segue que

$$\frac{ab}{[a,b]} \leq (a,b) \implies ab \leq [a,b](a,b). \tag{2.3}$$

De (2.2) e (2.3), segue que

$$[a,b](a,b) = ab.$$

□

Corolário 2.25: Se a e b são números inteiros primos entre si, então

$$[a,b] = |ab|.$$

Demonstração. De fato, se a e b são números inteiros primos entre si, então $(a,b) = 1$, e a igualdade segue. □

Exemplo 2.1.9: Do exemplo 2.1.4, vimos que $(24,\ 40) = 8$ e $(6,\ 35) = 1$. Portanto,

$$[24,\ 40] = \frac{24.40}{8} = 120$$

e

$$[6,\ 35] = 6.35 = 210.$$

Encerramos esta seção com a demonstração de um resultado clássico e de extrema importância para a aritmética dos números inteiros:

Teorema 2.26 (Teorema Fundamental da Aritmética): Todo número natural n maior que 1 ou é primo ou se escreve de modo único, a menos da ordem dos fatores, como um produto de números primos.

Demonstração. (Existência): Se $n = 2$ não há o que provar, pois 2 é primo.

Suponhamos o resultado válido para todo natural menor do que n (hipótese de indução). Se n é primo, o resultado segue imediatamente. Se n é composto, existem $n_1,\ n_2 \in \mathbb{N}$ tais que

$$n = n_1 n_2, \quad \text{com } 1 < n_1 < n \quad \text{e} \quad 1 < n_2 < n.$$

Pela hipótese de indução, existem primos $p_1,\ p_2, \ldots,\ p_k$ e $q_1,\ q_2, \ldots,\ q_s$ tais que $n_1 = p_1 p_2 \ldots p_k$ e $n_2 = q_1 q_2 \ldots q_s$. Portanto, segue que

$$n = n_1 n_2 = p_1 p_2 \ldots p_k q_1 q_2 \ldots q_s.$$

(Unicidade): Se $n = 2$ não há o que provar, pois 2 é primo e admite fatoração trivial (e única).

Suponhamos o resultado válido para todo natural menor do que n (hipótese de indução). Suponha que existam primos $p_1,\ p_2, \ldots,\ p_k$ e $q_1,\ q_2, \ldots,\ q_s$ tais que

$$p_1 p_2 \ldots p_k = n = q_1 q_2 \ldots q_s.$$

Uma vez que $p_1 \mid q_1 q_2 \ldots q_s$, pelo corolário 2.22, segue que $p_1 = q_j$, para algum j. Reordenando, se necessário, os fatores $q_1 q_2 \ldots q_s$, podemos supor, sem perda de generalidade, que $p_1 = q_1$. Desse modo, segue que

$$p_2 \ldots p_k = q_2 \ldots q_s.$$

Como $p_2 \dots p_k = q_2 \dots q_s < n$, a hipótese de indução nos garante que $k = s$ e os p_i e q_j são iguais aos pares, mostrando assim que a fatoração é única.

□

2.2 Equações diofantinas lineares

Utilizando os conceitos e propriedades apresentados neste capítulo, vamos agora definir as equações diofantinas lineares.

Definição 2.27: Uma **equação diofantina linear** é toda equação do tipo

$$ax + by = c,$$

em que a, b e c são números inteiros.

Qualquer par de inteiros x_0 e y_0, tal que $ax_0 + by_0 = c$, é denominado solução inteira da equação diofantina.

Exemplo 2.2.1: Algumas soluções inteiras possíveis da equação diofantina linear $2x+3y = 12$ são:

$x_1 = 0$ e $y_1 = 4$, pois $2.0 + 3.4 = 12$;
$x_2 = 6$ e $y_2 = 0$, pois $2.6 + 3.0 = 12$;
$x_3 = 3$ e $y_3 = 2$, pois $2.3 + 3.2 = 12$;
$x_4 = -3$ e $y_4 = 6$, pois $2.(-3) + 3.6 = 12$;
$x_5 = 9$ e $y_5 = -2$, pois $2.9 + 3.(-2) = 12$.

Exemplo 2.2.2: Observe que a equação diofantina $6x+8y = 49$ não admite solução inteira, pois para quaisquer $x_0,\ y_0 \in \mathbb{Z}$ temos que $6x_0 + 8y_0$ é um número par e, portanto, não pode ser igual a 49.

Conforme vimos no exemplo acima, não podemos dizer que toda equação diofantina tem solução. Assim, uma pergunta se torna necessária: quando uma equação diofantina tem solução? A proposição abaixo nos dá a resposta.

Proposição 2.28: Sejam $a,\ b,\ c \in \mathbb{Z}$. A equação diofantina linear $ax + by = c$ admite soluções inteiras se, e somente se, $(a,b) \mid c$.

Demonstração. Seja $x_0,\ y_0$ uma solução inteira da equação $ax + by = c$ e considere $(a,b) = d$. Então existem $a_1,\ b_1 \in \mathbb{Z}$ tais que $a = da_1$ e $b = db_1$. Assim,

$$c = ax_0 + by_0 = da_1x_0 + db_1y_0 = d(a_1x_0 + b_1y_0),$$

mostrando que $d \mid c$.

Reciprocamente, se $d \mid c$, então existe q inteiro tal que $c = dq$. O Teorema de Bachet-Bézout (2.15) nos garante que existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = d$.

Multiplicando ambos os membros dessa igualdade por q, temos que

$$ax_0q + by_0q = dq = c,$$

mostrando que o par $x_1,\ y_1$, com $x_1 = x_0q$ e $y_1 = y_0q$, é solução da equação diofantina. □

Observação 2.29: A equação diofantina $ax + by = c$, com a e b não ambos nulos e $(a,b) \mid c$, é equivalente à equação

$$a_1x + b_1y = c_1,$$

em que

$$a_1 = \frac{a}{(a,b)}, \quad b_1 = \frac{b}{(a,b)} \quad \text{e } c_1 = \frac{c}{(a,b)}.$$

Pelo corolário 2.18, temos que $(a_1,b_1) = 1$ e, portanto, podemos analisar apenas equações do tipo

$$ax + by = c, \quad \text{com } (a,b) = 1,$$

que sempre têm soluções inteiras.

Vimos no exemplo 2.2.2 que a solução da equação diofantina não é única. Porém há uma relação entre as soluções.

Proposição 2.30: Suponha que a equação $ax + by = c$, com $a,\ b,\ c \in \mathbb{Z}$ e $(a,b) = 1$ admita a solução inteira $x_0,\ y_0$. Então as soluções inteiras $x,\ y$ desta equação são da forma

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

Demonstração. Seja $x_0,\ y_0$ uma solução inteira de $ax + by = c$. Então

$$ax_0 + by_0 = c = ax + by,$$

ou seja,

$$a(x - x_0) = b(y_0 - y). \tag{2.4}$$

Como $(a,b) = 1$, segue que $b \mid (x - x_0)$. Logo,

$$x - x_0 = tb, \quad t \in \mathbb{Z}. \tag{2.5}$$

Substituindo esta última expressão em (2.4), temos que

$$y_0 - y = ta.$$

Das duas últimas igualdades, concluímos que $x = x_0 + tb$ e $y = y_0 - ta$.

Por outro lado, note que se $x = x_0 + tb$ e $y = y_0 - ta$, com $t \in \mathbb{Z}$, então $x,\ y$ é solução da equação, pois

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + by_0 = c.$$

□

Exemplo 2.2.3: Vamos determinar todas as soluções inteiras da equação

$$12x + 33y = 27.$$

Note que a equação tem solução, pois (12,33) | 27. Dividindo ambos os membros da equação por 3 = (12,33), obtemos a equação equivalente

$$4x + 11y = 9.$$

Pelo Algoritmo de Euclides, temos que

$$\begin{aligned} 11 &= 2.4 + 3 \\ 4 &= 1.3 + 1. \end{aligned}$$

Utilizando a segunda igualdade, podemos reescrever a primeira como

$$11 = 4.2 + (4 - 1),$$

que é equivalente a

$$4.3 + 11.(-1) = 1.$$

Multiplicando esta última igualdade por 9, obtemos

$$4.27 + 11.(-9) = 9,$$

o que nos mostra que $x_0 = 27$ e $y_0 = -9$ é uma solução particular da equação e, consequentemente, as soluções inteiras são

$$x = 27 + 11t, \quad y = -9 - 4t, \quad \text{com } t \in \mathbb{Z}.$$

Vários problemas podem ser solucionados com o uso de uma equação diofantina linear. Considere a seguinte situação: o caixa de um estabelecimento só possui notas de 2 e 5 reais e precisa voltar R$27 de troco a um cliente. De quais maneiras ele pode dar o troco? Este exemplo simples nos mostra que, em alguns contextos, estamos interessados nas soluções naturais de equações diofantinas da forma $ax + by = c$, em que $a,\ b,\ c \in \mathbb{N}$ e $(a,b) = 1$. O estudo de semigrupos numéricos, objeto do próximo capítulo deste texto, irá nos ajudar nessa situação.

3

Semigrupos Numéricos

Neste capítulo estudaremos semigrupos numéricos, uma estrutura algébrica presente em diversas áreas da Matemática como Álgebra, Geometria Algébrica, Matemática Discreta e Teoria dos Números. Nosso objetivo é relacionar as soluções naturais de uma equação diofantina linear com semigrupos numéricos, bem como apresentar os semigrupos simétricos, pseudossimétricos, quase simétricos e Arf e algumas de suas propriedades. Os principais resultados deste capítulo podem ser encontrados em [1], [8], [10], [11] e [18].

3.1 Semigrupos numéricos: definição e exemplos

Para que possamos relacionar as soluções naturais de uma equação diofantina linear com semigrupos numéricos, vamos inicialmente definir o que é um semigrupo numérico e apresentar alguns de seus invariantes e propriedades básicas.

Definição 3.1: Um **semigrupo numérico** S é um subconjunto dos números naturais $\mathbb{N}$ que satisfaz as três condições abaixo:

1. $0 \in S$;
2. $x + y \in S$, para todos $x, y \in S$;
3. $\mathbb{N} \setminus S$ é finito.

Todo semigrupo numérico S pode ser representado pela notação

$$S = \{0,\ s_1,\ s_2,\ \ldots,\ s_n,\ \rightarrow\},$$

em que $s_i > s_j$ para todo $i > j$, e a seta significa que todos os elementos de $\mathbb{N}$ a partir de s_n pertencem a S.

Por simplicidade, nesta dissertação escreveremos apenas **semigrupo** para nos referirmos a um semigrupo numérico.

Exemplo 3.1.1: O conjunto $S = \{0,\ 3,\ 6,\ 7,\ 9,\ \rightarrow\}$ é um semigrupo. De fato, note que S é fechado para a adição, $0 \in S$ e $\mathbb{N} \setminus S = \{1, 2, 4, 5,\ 8\}$.

Definição 3.2: Dado um semigrupo $S = \{0,\ s_1,\ s_2,\ \ldots,\ s_n,\ \rightarrow\}$, definimos alguns conceitos importantes:

Multiplicidade: menor inteiro positivo pertencente a S, ou seja, o elemento s_1. Notação: $\mu(S)$, ou simplesmente μ.

Condutor: menor inteiro positivo pertencente a S a partir do qual todos os inteiros maiores pertencem ao semigrupo, ou seja, o elemento s_n. Notação: $\beta(S)$, ou simplesmente β.

Lacunas: as lacunas de um semigrupo S são os elementos do complementar $\mathbb{N} \setminus S$.

Número de Fröbenius: maior inteiro não pertencente ao semigrupo S, ou seja, a maior lacuna de S. Notação: $\gamma(S)$, ou simplesmente γ. Note que $\gamma = \beta - 1$.

Gênero: é o número de lacunas de S, ou seja, a cardinalidade do conjunto $\mathbb{N} \setminus S$. Notação: $g(S)$, ou simplesmente g.

Exemplo 3.1.2: $S = \{0,\ 3,\ 6,\ 9,\ \rightarrow\}$ é um semigrupo com multiplicidade $\mu = 3$, condutor $\beta = 9$ e número de Fröbenius $\gamma = 8$. O conjunto das lacunas de S é $\mathbb{N} \setminus S = \{1,\ 2,\ 4,\ 5,\ 7,\ 8\}$ e o seu gênero é $g = 6$.

Exemplo 3.1.3: $S = \{0,\ 6,\ 7,\ 8,\ 11,\ \rightarrow\}$ é um semigrupo com multiplicidade $\mu = 6$, condutor $\beta = 11$ e número de Fröbenius $\gamma = 10$. O conjunto das lacunas de S é $\mathbb{N} \setminus S = \{1,\ 2,\ 3,\ 4,\ 5,\ 9,\ 10\}$ e o seu gênero é $g = 7$.

Para semigrupos com condutor muito alto, pode ser difícil determinar o valor do gênero. A proposição abaixo nos dá uma estimativa deste valor:

Proposição 3.3: Seja S um semigrupo com gênero g, número de Fröbenius γ e condutor β. Então

$$g \geq \frac{\gamma + 1}{2} = \frac{\beta}{2}.$$

Demonstração. Essa desigualdade decorre do fato de que se $s \in S$, então $\gamma - s \notin S$, pois caso contrário teríamos que $(\gamma - s) + s = \gamma \in S$, o que é um absurdo.

De fato, note que as lacunas de S pertencem ao conjunto $A = \{1,\ 2,\ \ldots,\ \gamma\}$. Além de γ, pelo menos um número de cada um dos $\left\lfloor \frac{\gamma}{2} \right\rfloor$ pares

$$(1, \gamma - 1),\ (2, \gamma - 2),\ \ldots,\ \left(\left\lfloor \frac{\gamma}{2} \right\rfloor, \left\lceil \frac{\gamma}{2} \right\rceil\right)$$

também é uma lacuna de S, em que $\left\lfloor \frac{\gamma}{2} \right\rfloor$ é o maior inteiro menor ou igual a $\frac{\gamma}{2}$. Portanto,

$$g \geq \left\lfloor \frac{\gamma}{2} \right\rfloor + 1 \geq \frac{\gamma + 1}{2} = \frac{\beta}{2}.$$

□

Note que o semigrupo do exemplo 3.1.2 é gerado por 3, 10 e 11, no sentido de que todo elemento de S é combinação linear de 3, 10 e 11. Um subconjunto $G \subseteq S$ com essa propriedade de gerar S é dito conjunto gerador de S. Se $G = \{x_1,\ x_2,\ \ldots,\ x_n\}$, com $x_i < x_j$ para todo $i < j$, utilizamos a notação $S = \langle x_1,\ x_2,\ \ldots,\ x_n\rangle$, e os elementos de G são geradores de S. Sendo G um conjunto finito, dizemos que S é finitamente gerado.

Exemplo 3.1.4: Voltemos ao exemplo 3.1.3, em que $S = \{0,\ 6,\ 7,\ 8,\ 11,\ \rightarrow\}$. Podemos observar que $S = \langle\ 6,\ 7,\ 8,\ 11\ \rangle$, ou seja, S é finitamente gerado.

Todo semigrupo possui um conjunto gerador? A resposta é sim, já que S é gerado por todos os seus elementos e, nesse caso, a quantidade de geradores é infinita. Surge então uma pergunta: é sempre possível encontrar um conjunto finito de geradores de S? A proposição abaixo responde esse questionamento:

Proposição 3.4: Todo semigrupo é finitamente gerado.

Demonstração. Temos que

$$S = \langle s_1,\ \ldots,\ s_n = \beta,\ \beta + 1,\ \ldots,\ \beta + s_1 - 1\rangle.$$

De fato, considere $G = \{s_1,\ \ldots,\ s_n = \beta,\ \beta + 1,\ \ldots,\ \beta + s_1 - 1\}$. Como $S = \{0,\ s_1,\ \ldots,\ s_n = \beta,\ \rightarrow\}$, segue que $G \subseteq S$. Observe também que

$$0,\ s_1, \ldots,\ s_n \in \langle s_1,\ \ldots,\ s_n = \beta,\ \beta + 1,\ \ldots,\ \beta + s_1 - 1\rangle.$$

Seja agora $x \in S$ tal que $x > s_n = \beta$. Pelo algoritmo de Euclides, existem $q,\ r \in \mathbb{N}$ tais que $x = q\beta + r$, com $q \geq 1$ e $0 \leq r < \beta$.

Se $r = 0$, temos $x = q\beta$. Logo, $x \in \langle s_1,\ \ldots,\ s_n = \beta,\ \beta + 1,\ \ldots,\ \beta + s_1 - 1\rangle$.

Se $0 < r < \beta$, novamente pelo algoritmo de Euclides obtemos $q_1,\ r_1 \in \mathbb{N}$ tais que $r = q_1 s_1 + r_1$, com $0 \leq r_1 < s_1$. Desse modo,

$$x = q\beta + r = q\beta + q_1 s_1 + r_1 = (q-1)\beta + q_1 s_1 + (\beta + r_1),$$

o que implica em $x \in \langle s_1,\ \ldots,\ s_n = \beta,\ \beta + 1,\ \ldots,\ \beta + s_1 - 1\rangle$, pois $(q-1) \in \mathbb{N}$ e $\beta,\ s_1,\ \beta + r_1 \in G$.

□

Exemplo 3.1.5: Seja $S = \{0,\ 8,\ 9,\ 10,\ 13,\ 14,\ 16,\ \rightarrow\}$. De acordo com a proposição 3.4, S é finitamente gerado e seu conjunto gerador é

$$G = \{8,\ 9,\ 10,\ 13,\ 14,\ 16,\ 17,\ 18,\ 19,\ 20,\ 21,\ 22,\ 23\}$$

O subconjunto $G = \{s_1,\ \ldots,\ s_n = \beta,\ \beta + 1,\ \ldots,\ \beta + s_1 - 1\}$ dado pela proposição 3.4 não é o menor conjunto gerador de S. Para determinar o conjunto minimal de geradores de S, basta retirar de G aqueles elementos que sejam soma de outros dois anteriores.

Exemplo 3.1.6: Considere novamente $S = \{0,\ 8,\ 9,\ 10,\ 13,\ 14,\ 16,\ \rightarrow\}$. Do exemplo

3.1.5, o conjunto

$$G = \{8,\ 9,\ 10,\ 13,\ 14,\ 16,\ 17,\ 18,\ 19,\ 20,\ 21,\ 22,\ 23\}$$

é gerador de S. Retirando de G os elementos que são combinações lineares de outros, obtemos o conjunto minimal de geradores de S, a saber:

$$G' = \{8,\ 9,\ 10,\ 13,\ 14\}.$$

Lema 3.5: Seja $S = \langle n_1,\ n_2,\ \ldots,\ n_k\rangle$. Se S é semigrupo numérico com conjunto minimal de geradores $\{n_1,\ n_2,\ \ldots,\ n_k\}$, então $mdc(n_1,\ n_2,\ \ldots,\ n_k) = 1$.

Demonstração. Suponha S semigrupo e considere $mdc(n_1,\ n_2,\ \ldots,\ n_k) = d$. Então sabemos que $d \mid n_i$ para todo $i \in \{1,\ 2,\ \ldots,\ k\}$, ou seja, para cada $1 \leq i \leq k$ existe $a_i \in \mathbb{N}$ tal que $n_i = da_i$.

Seja $s \in S$. Então existem $x_1, \ldots, x_k \in \mathbb{N}$ tais que $s = x_1n_1 + \ldots + x_kn_k$. Logo, segue que

$$s = x_1da_1 + \ldots + x_kda_k = d(x_1a_1 + \ldots + x_ka_k),$$

ou seja, $S \subseteq \langle d\rangle = \{md \mid m \in \mathbb{N}\}$. Desse modo, $\mathbb{N} \setminus \langle d\rangle \subseteq \mathbb{N} \setminus S$.

Suponha que $d \neq 1$. Temos então que

$$\{md + 1 \mid m \in \mathbb{N}\} \subseteq \mathbb{N} \setminus \langle d\rangle \subseteq \mathbb{N} \setminus S.$$

Isso implica que $\mathbb{N} \setminus \langle d\rangle$ não é finito, o que é um absurdo, pois como S é semigrupo, $\mathbb{N} \setminus S$ é finito. Portanto, devemos ter $d = 1$.

□

Proposição 3.6: O conjunto minimal de geradores de um semigrupo S é único.

Demonstração. Suponha, por absurdo, que existam $G_1 = \{n_1,\ n_2,\ \ldots,\ n_k\}$ e $G_2 = \{m_1,\ m_2,\ \ldots,\ m_l\}$ conjuntos minimais de geradores de S distintos e seja $x \in G_1 \setminus G_2$. Como $x \in G_1 \subseteq S$ e G_2 é conjunto gerador de S, então $x = \sum_{j=1}^{r} a_j m_{i_j}$, para alguns $m_{i_j} \in G_2$ e $a_j \in \mathbb{N} \setminus \{0\}$. Como cada $m_{i_j} \in G_2 \subseteq S$ e G_1 é conjunto gerador de S, então todo m_{i_j} pode ser escrito na forma $\sum_{p=1}^{s} b_{j_p} n_{i_p}$ para alguns $n_{i_p} \in G_1$ e $b_{j_p} \in \mathbb{N} \setminus \{0\}$. Portanto, $x = \sum_{j=1}^{r}\sum_{p=1}^{s} a_j b_{j_p} n_{i_p}$, o que é um absurdo, pois G_1 é conjunto gerador minimal e nenhum de seus elementos pode ser escrito como combinação linear de outros. Portanto, não existe tal $x \in G_1 \setminus G_2$, e então $G_1 \subseteq G_2$. De maneira análoga, podemos mostrar que $G_2 \subseteq G_1$, concluindo assim que devemos ter $G_1 = G_2$.

□

Convencionalmente, a notação $S = \langle n_1,\ \ldots,\ n_k\rangle$, com $n_i < n_j$ para todo $i < j$, indicará que $\{n_1,\ \ldots,\ n_k\}$ é o conjunto minimal de geradores de S. Cada elemento n_i é um gerador minimal de S.

3.2 Semigrupos numéricos e equações diofantinas lineares

Agora estamos prontos para relacionar as soluções naturais de uma equação diofantina linear com semigrupos numéricos. Considere uma equação diofantina da forma $ax + by = c$, em que $a,\ b,\ c \in \mathbb{N}$ e $(a,b) = 1$. Note que tal equação possui solução natural se, e somente se, $c \in S = \langle a,b\rangle = \{ax + by \mid x,\ y \in \mathbb{N}\}$. Nesta seção estudaremos essa solução, bem como o semigrupo $S = \langle a,b\rangle$.

Proposição 3.7: Sejam a e b números naturais com $(a,b) = 1$. Todo número inteiro c pode ser escrito de modo único na forma

$$c = ma + nb, \quad \text{com } 0 \leq m < b \ \text{ e } \ n \in \mathbb{Z}.$$

Demonstração. Existência: O Teorema de Bachet-Bézout (2.15) nos garante a existência de inteiros x e y tais que

$$ax + by = 1.$$

Multiplicando esta igualdade por c, obtemos

$$axc + byc = c.$$

Pela divisão euclidiana, existem q e m inteiros, com $0 \leq m < b$, tais que $xc = qb + m$. Substituindo esse valor de xc na igualdade acima, temos

$$c = axc + byc = aqb + am + byc = ma + (aq + yc)b = ma + nb,$$

com $0 \leq m < b$ e $n = aq + yc \in \mathbb{Z}$.

Unicidade: Suponha que existam $m,\ m_1,\ n,\ n_1 \in \mathbb{Z}$, com $0 \leq m < b$ e $0 \leq m_1 < b$, tais que $ma + nb = c = m_1a + n_1b$, ou seja, $a(m - m_1) = b(n_1 - n)$. Desse modo, temos que

$$-b < -m_1 \leq m - m_1 \leq m < b,$$

mostrando que $|m - m_1| < b$. Como $(a,b) = 1$ e $a(m - m_1) = b(n_1 - n)$, temos que $b \mid (m - m_1)$, o que só é possível se $|m - m_1| = 0$, ou seja, se $m = m_1$. Por fim, se $m = m_1$, então $(n_1 - n)b = a(m - m_1) = 0$ e, portanto, $n_1 = n$.

□

Proposição 3.8: Seja o semigrupo $S = \langle a,b\rangle$. Então $c \in S$ se, e somente se, existem $m,\ n \in \mathbb{N}$, com $m < b$, tais que $c = ma + nb$.

Demonstração. Naturalmente, se $c = ma + nb$, com $m,\ n \in \mathbb{N}$ e $m < b$, então $c \in S$. Reciprocamente, se $c \in S$, existem $x,\ y \in \mathbb{N}$ tais que $c = ax + by$. Pela divisão

euclidiana, existem inteiros q e m, com $0 \leq m < b$ tais que $x = qb + m$. Substituindo este valor de x na igualdade acima, temos que

$$c = ax + by = aqb + am + by = ma + (aq + y)b = ma + nb,$$

em que $0 \leq m < b$ e $n = aq + y \in \mathbb{N}$. Observe que a proposição 3.7 garante a unicidade de m e n.

□

As lacunas também nos fornecem informações sobre o semigrupo.

Corolário 3.9: Seja o semigrupo $S = \langle a, b \rangle$. Então o conjunto das lacunas de S é dado por

$$\mathbb{N} \setminus S = \{ma - nb \in \mathbb{N} \mid m,\ n \in \mathbb{N},\ \ m < b\}.$$

Demonstração. Seja c um número natural. Pela proposição 3.7, existem $m,\ n$ únicos, com $0 \leq m < b$ e $n \in \mathbb{Z}$, tais que $c = ma + nb$. Entretanto, pela proposição 3.8, $c \in S$ se, e somente se, $n \geq 0$. Portanto, se $n < 0$, podemos escrever $c = ma - nb$, considerando $n \in \mathbb{N} \setminus \{0\}$ e então $c \notin S$, ou seja, $c \in \mathbb{N} \setminus S$. Reciprocamente, se $c \in \mathbb{N} \setminus S$, novamente pelas proposições 3.7 e 3.8 segue que $c = ma - nb$, com $m,\ n \in \mathbb{N},\ \ m < b$.

□

Corolário 3.10: Seja o semigrupo $S = \langle a, b \rangle$. O número de Fröbenius γ de S é

$$\gamma = (b - 1)a - b.$$

Assim sendo, o condutor β de S é

$$\beta = (a - 1)(b - 1).$$

Demonstração. Pelo corolário 3.9, segue que a maior lacuna de S ocorre quando m é máximo e n é mínimo e não nulo, ou seja, quando $m = b - 1$ e $n = 1$. Portanto, segue que

$$\gamma = ma - nb = (b - 1)a - b.$$

Como $\beta = \gamma + 1$, segue que

$$\beta = \gamma + 1 = (b - 1)a - b + 1 = ab - a - b + 1 = (a - 1)(b - 1).$$

□

De que maneira semigrupos numéricos podem nos ajudar na solução de equações diofantinas? O teorema abaixo nos ajuda nesse questionamento.

Teorema 3.11: A equação diofantina $ax + by = c$, com $a,\ b,\ c \in \mathbb{N}$ e $(a,b) = 1$, tem solução em números naturais se, e somente se,

$$c \notin \mathbb{N} \setminus S = \{ma - nb \in \mathbb{N} \mid m,\ n \in \mathbb{N},\ \ m < b\},$$

em que $S = \langle a,b \rangle$, ou seja, se, e somente se, c não é lacuna de S.

Demonstração. Uma vez que a equação $ax + by = c$ admite solução se, e somente se, $c \in S$, o resultado segue diretamente do corolário 3.9.

□

Dada a equação $ax + by = c$, com $a,\ b,\ c \in \mathbb{N}$ e $(a,b) = 1$, com o algoritmo de Euclides e o teorema 3.11 podemos obter $m_1,\ n_1 \in \mathbb{N}$ tais que

$$1 = (a,b) = m_1 a - n_1 b.$$

Multiplicando esta igualdade por c, obtemos

$$c = m_1 ac - n_1 bc.$$

Pela divisão euclidiana, existem inteiros q e m, com $0 \leq m < b$, tais que $cm_1 = qb + m$. Substituindo este valor de cm_1 na igualdade acima, temos:

$$c = \begin{cases} ma + (qa - cn_1)b, & \text{se } qa \geq cn_1 \\ ma - (cn_1 - qa)b, & \text{se } cn_1 > qa \end{cases}$$

No primeiro caso, fazendo $n = qa - cn_1$, temos que $c \in S = \langle a,b \rangle$ e, portanto, a equação admite solução natural.

Já no segundo caso, fazendo $n = cn_1 - qa$, temos que $c \notin S = \langle a,b \rangle$, ou seja, $c \in \mathbb{N} \setminus S$ e, portanto, a equação não admite solução natural.

Definição 3.12: Dada a equação $ax + by = c$, com $a,\ b, c \in \mathbb{N}$ e $(a,b) = 1$, a única solução natural $m,\ n$ tal que $m < b$ é denominada **solução minimal**, no sentido de que se o par (x, y) é solução da equação, então $x \geq m$. Note que as proposições 3.7 e 3.8 garantem a unicidade da solução minimal.

Proposição 3.13: Suponha que a equação $ax + by = c$, com $a,\ b,\ c \in \mathbb{N}$ e $(a,b) = 1$, admita a solução minimal $x_0 = m$ e $y_0 = n$. Então as soluções naturais $x,\ y$ da equação são da forma

$$x = m + tb, \quad \text{e} \quad y = n - ta, \quad t \in \mathbb{N}, \quad n - ta \geq 0.$$

Demonstração. Seja $x,\ y$ uma solução natural de $ax + by = c$. Então

$$am + bn = c = ax + by,$$

ou seja,

$$a(x - m) = b(n - y). \tag{3.1}$$

Como $(a,b) = 1$, segue que $b \mid (x - m)$. Como $m,\ n$ é solução minimal, $x \geq m$. Portanto,

existe $t \in \mathbb{N}$ tal que

$$x - m = tb, \quad t \in \mathbb{N}. \tag{3.2}$$

Substituindo esta última expressão em (3.1), temos que

$$n - y = ta.$$

Das duas últimas igualdades, concluímos que $x = m + tb$ e $y = n - ta \geq 0$.

Por outro lado, note que se $x = m + tb$ e $y = n - ta$, com $t \in \mathbb{N}$ e $n - ta \geq 0$, então $x,\ y$ é solução da equação, pois

$$ax + by = a(m + tb) + b(n - ta) = am + bn = c.$$

□

Exemplo 3.2.1: Considere a equação

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

Note que para $c \geq 8$ esta equação possui solução natural. De fato, sendo $S = \langle 3, 5 \rangle$, o corolário 3.10 nos diz que

$$\beta(S) = (3 - 1)(5 - 1) = 2.4 = 8.$$

Aplicando o corolário 3.9, temos que

$$\mathbb{N} \setminus S = \{3m - 5n \in \mathbb{N} \mid m,\ n \in \mathbb{N},\ m < 5\}.$$

Para $m = 1$, temos que $3.1 - 5n \notin \mathbb{N}$.
Para $m = 2$, temos que $3.2 - 5n \in \mathbb{N}$ se $n = 1$. Logo, 1 é lacuna de S.
Para $m = 3$, temos que $3.3 - 5n \in \mathbb{N}$ se $n = 1$. Logo, 4 é lacuna de S.
Para $m = 4$, temos que $3.4 - 5n \in \mathbb{N}$ para $n = 1$ e $n = 2$. Logo, 7 e 2 são lacunas de S.
Desse modo, segue que a equação $3x + 5y = c$ admite solução natural se

$$c \notin \mathbb{N} \setminus S = \{1,\ 2,\ 4,\ 7\},$$

ou, equivalentemente, se

$$c \in S = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}.$$

Exemplo 3.2.2: Vamos determinar as soluções naturais de $3x + 5y = 74$. Pelo Algoritmo de Euclides, temos:

$$5 = 1.3 + 2,$$
$$3 = 1.2 + 1.$$

Logo,

$$1 = 3 - 2 = 3 - (5 - 3) = 2.3 - 5.$$

Multiplicando esta igualdade por 74, temos

$$\begin{aligned}
74 &= 74.2.3 - 74.3,\\
74 &= 148.3 - 74.5,\\
74 &= (3 + 5.29).3 - 74.5,\\
74 &= 3.3 + 87.5 - 74.5,\\
74 &= 3.3 + 13.5.
\end{aligned}$$

Segue que $m = 3$ e $n = 13$ é a solução minimal da equação. Portanto, as demais soluções naturais são

$$x = 3 + 5t, \quad y = 13 - 3t, \quad \text{com } t \in \mathbb{N}, \quad 13 - 3t \geq 0.$$

Temos então que $t = 0,\ 1,\ 2,\ 3,\ 4$, e as soluções naturais da equação são $x_0 = 3$ e $y_0 = 13$, $x_1 = 8$ e $y_1 = 10$, $x_2 = 13$ e $y_2 = 7$, $x_3 = 18$ e $y_3 = 4$ e $x_4 = 23$ e $y_4 = 1$.

Exemplo 3.2.3: Vamos retomar o exemplo apresentado no final do capítulo anterior: o caixa de um estabelecimento só possui notas de 2 e 5 reais e precisa voltar R$27 de troco a um cliente. De quais maneiras ele pode dar o troco?

Vamos determinar as soluções naturais de $2x + 5y = 27$. Pelo Algoritmo de Euclides, temos:

$$5 = 2.2 + 1, \quad \text{ou seja,} \quad 1 = 5 - 2.2.$$

Multiplicando esta igualdade por 27, temos

$$\begin{aligned}
27 &= 27.5 - 2.27.2,\\
27 &= 27.5 - 54.2,\\
27 &= (11.2 + 5).5 - 54.2,\\
27 &= 55.2 + 5.5 - 54.2,\\
27 &= 1.2 + 5.5.
\end{aligned}$$

Segue que $m = 1$ e $n = 5$ é a solução minimal da equação. Portanto, as demais soluções naturais são

$$x = 1 + 5t, \quad y = 5 - 2t, \quad \text{com } t \in \mathbb{N}, \quad 5 - 2t \geq 0.$$

Temos então que $t = 0,\ 1,\ 2$, e as soluções naturais da equação são $x_0 = 1$ e $y_0 = 5$, $x_1 = 6$ e $y_1 = 3$ e $x_2 = 11$ e $y_2 = 1$. Desse modo, o caixa poderia dar de troco uma nota de R$2 e cinco notas de R$5, seis notas de R$2 e três notas de R$5, ou ainda onze notas de R$2 e uma nota de R$5.

Em situações em que estamos trabalhando com números pequenos, como no exemplo acima, não é necessário resolver a equação diofantina utilizando as técnicas estudadas nesta seção: para este caso, bastava determinar quais valores de y, com $0 \leq y \leq 5$ tornam o número $27 - 5y$ par.

3.3 Ideais, cadeias de semigrupos e semigrupos Arf

Nesta seção, iremos apresentar mais propriedades sobre semigrupos numéricos, bem como definir algumas cadeias de semigrupos e introduzir um novo tipo de semigrupo: os semigrupos Arf. Para continuarmos a nossa caracterização, precisamos definir as operações abaixo entre subconjuntos de $\mathbb{Z}$, pois elas serão importantes para estabelecermos o conceito de ideal de um semigrupo numérico.

Definição 3.14: Sejam $E,\ F$ subconjuntos de $\mathbb{Z}$, $x \in \mathbb{Z}$ e $n \in \mathbb{N} \setminus \{0\}$. Definimos as seguintes operações:

(i) $E + F = \{a + b \mid a \in E,\ b \in F\}$;

(ii) $E + x = \{a + x \mid a \in E\}$;

(iii) $nE = E + E + \ldots + E,\ n$ vezes;

(iv) $E - F = \{a \in \mathbb{Z} \mid a + F \subseteq E\}$.

Observação 3.15: Dado um subconjunto E de $\mathbb{Z}$, usaremos a mesma notação utilizada para semigrupo, ou seja, se $E = \{-5,\ -2\} \cup \mathbb{N} \setminus \{1,\ 3,\ 6\}$, escreveremos

$$E = \{-5,\ -2,\ 0,\ 2,\ 4,\ 5,\ 7,\ \rightarrow\}.$$

Exemplo 3.3.1: Sejam

$$E = \{-6,\ -3,\ 0,\ 8,\ 17,\ 19,\ \rightarrow\} \text{ e}$$
$$F = \{-1,\ 0,\ 7,\ 10,\ 14,\ \rightarrow\}.$$

Temos:

$$\begin{aligned} E + F &= \{-7,\ -6,\ -4,\ -3,\ -1,\ 0,\ 1,\ 4,\ 7,\ \rightarrow\}, \\ E + 2 &= \{-4,\ -1,\ 2,\ 10,\ 19,\ 21,\ \rightarrow\}, \\ 2E = E + E &= \{-12,\ -9,\ -6,\ -3,\ 0,\ 2,\ 5,\ 8,\ 11,\ 13,\ \rightarrow\}, \\ E - F &= \{a \in \mathbb{Z} \mid a + F \subseteq E\} = \{20,\ \rightarrow\}. \end{aligned}$$

Definição 3.16: Um **ideal relativo** de um semigrupo S é um conjunto não vazio $E \subseteq \mathbb{Z}$ tal que:

(i) $S + E \subseteq E$;

(ii) $x + E \subseteq S$, para algum $x \in \mathbb{Z}$.

Caso $E \subseteq S$, E é dito apenas **ideal** de S.

Observação: Se E e F são ideais relativos de S tais que $F \subseteq E$, então $S - E \subseteq S - F$.

Definição 3.17: Seja S um semigrupo. O conjunto $M = \{s \in S \mid s > 0\}$ é um ideal de S, denominado **ideal maximal** de S. De fato, note que $S + M \subseteq M$, pois S é fechado para soma e $S = M \cup \{0\}$. O inteiro x da segunda condição de ideal relativo pode ser qualquer $s \in S$, inclusive o zero.

Exemplo 3.3.2: Seja $S = \langle 3,\ 5\rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$. Então os conjuntos

$$E = \{-3,\ 0,\ 2,\ 3,\ 5,\ \rightarrow\},$$

$$I = \{5,\ 6,\ 8,\ \rightarrow\},\ \text{e}$$

$$M = \{3,\ 5,\ 6,\ 8,\ \rightarrow\}$$

são, respectivamente, ideal relativo, ideal e ideal maximal de S.

Proposição 3.18: Seja $S = \{0,\ s_1,\ s_2,\ \ldots,\ s_n,\ \rightarrow\}$ um semigrupo numérico e M seu ideal maximal. Se $S \neq \mathbb{N}$, então:

(i) $S - M = M - M$;

(ii) $S - R = M - R$ para todo semigrupo $R \subseteq \mathbb{N}$ que contém S propriamente.

Demonstração. Para a parte (i), queremos mostrar que $S - M = M - M$, ou seja, $\{a \in \mathbb{Z} \mid a + M \subseteq S\} = \{a \in \mathbb{Z} \mid a + M \subseteq M\}$. Claramente, $M - M \subseteq S - M$, pois $M \subset S$. Vamos mostrar que $S - M \subseteq M - M$, e assim concluir a igualdade desejada.

Suponha que $S - M \nsubseteq M - M$. Então existe $x \in S - M$ tal que $x \notin M - M$. Assim, existe $s_i \in M$ tal que $x + s_i = 0$, pois $S \setminus M = \{0\}$, o que implica $x = -s_i$. Se $s_i \neq s_1$, tome $s_j < s_i$, $s_j \in M$. Então $x + s_j \in S$, o que é um absurdo, pois $x + s_j = -s_i + s_j < 0$ e $S \subset \mathbb{N}$. Logo, devemos ter $s_i = s_1$ e, assim, $x = -s_1$. Tome agora $s = \beta + s_1 - 1$ elemento de M. Então $x + s = -s_1 + \beta + s_1 - 1 = \beta - 1 = \gamma \in S$, o que é um absurdo. Portanto, tal elemento x não existe. Desse modo, $S - M \subseteq M - M$, e a igualdade é verdadeira.

Para a parte (ii), devemos mostrar que $S - R = M - R$, ou seja, $\{a \in \mathbb{Z} \mid a + R \subseteq S\} = \{a \in \mathbb{Z} \mid a + R \subseteq M\}$. Note que $M - R \subseteq S - R$, pois $M \subset S$. Mostraremos então que $S - R \subseteq M - M$, para assim concluir a igualdade desejada.

Suponha que $S - R \nsubseteq M - R$. Então existe $x \in S - R$ tal que $x \notin M - R$. Assim, existe $r_i \in R$ tal que $x + r_i = 0$, pois $S \setminus M = \{0\}$, o que implica $x = -r_i$. Se $r_i = s_k \in M$, por um argumento análogo ao apresentado no item anterior, concluímos que $S - R \subseteq M - R$. Agora, se $r_i \in R \setminus S$ (perceba que $R \setminus S \neq \emptyset$, pois R contém S propriamente), então $x + s_1 \in S$, o que é um absurdo, pois $x + s_1 = -r_i + s_1 < s_1$. Portanto, este elemento x não existe, e assim $S - R \subseteq M - M$.

□

Um dos motivos de se estudar ideais relativos é o auxilio que eles nos dão à procura do conjunto minimal de geradores de um semigrupo S. Para estabelecer essa relação, vamos definir a dimensão de mergulho de S.

Definição 3.19: Seja $S = \langle n_1,\ \ldots,\ n_k\rangle$, com $\{n_1,\ \ldots,\ n_k\}$ o conjunto minimal de geradores de S. O número k é denominado **dimensão de mergulho** de S, e é denotado por $e(S)$.

Exemplo 3.3.3: Dado o semigrupo $S = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$, temos que $S = \langle 3,\ 5\rangle$, e sua dimensão de mergulho é $e(S) = 2$.

Exemplo 3.3.4: Dado o semigrupo $S = \{0,\ 6,\ 7,\ 8,\ 11,\ \rightarrow\}$, temos que $S = \langle 6,\ 7,\ 8,\ 11\rangle$, e sua dimensão de mergulho é $e(S) = 4$.

Lema 3.20: Se E é um ideal relativo de um semigrupo S e M seu ideal maximal, então o conjunto minimal de geradores de E é $E \setminus (M + E)$.

Demonstração. Um elemento $x \in E$ não é gerador minimal de E se, e somente se, $x = y + s$, para algum $y \in E$ e $s \in S$, $s \neq 0$, o que significa que x não é elemento gerador de E se e somente se $x \in M + E$.

□

Corolário 3.21: Seja S um semigrupo. Então $e(S) = card(M \setminus 2M)$. Em particular, $G = M \setminus 2M$ é o conjunto minimal de geradores de S.

Demonstração. Basta considerar, no lema anterior, o caso particular em que $E = M$, e observar que o conjunto minimal de geradores de M é o mesmo de $S = M \cup \{0\}$.

□

Exemplo 3.3.5: Seja $S = \{0,\ 8,\ 10,\ 11,\ 13,\ 14,\ 16,\ \rightarrow\}$. De acordo com o corolário anterior, $e(S) = card(M \setminus 2M)$. De fato,

$$\begin{aligned} M &= \{8,\ 10,\ 11,\ 13,\ 14,\ 16,\ \rightarrow\},\\ 2M &= \{16,\ 18,\ \rightarrow\},\\ M \setminus 2M &= \{8,\ 10,\ 11,\ 13,\ 14,\ 17\}. \end{aligned}$$

Logo, $e(S) = 6$ e $S = \langle 8,\ 10,\ 11,\ 13,\ 14,\ 17\rangle$.

Vamos agora definir um conjunto muito interessante, dito Apéry:

Definição 3.22: Seja $a \in I$, I ideal do semigrupo S. O **conjunto Apéry** do elemento a é definido como o conjunto

$$Ap(I,a) = \{s \in I \mid s - a \notin I\} = I \setminus (a + I).$$

O conjunto Apéry será essencial para entendermos melhor os semigrupos numéricos.

Proposição 3.23: Seja $a \in I$, I ideal do semigrupo S. Para cada $i = 0,\ 1,\ \ldots,\ a-1$, seja $x_i = \min\{x \in I \mid x \equiv i \mod (a)\}$. Então $Ap(I,a) = \{x_0,\ x_1,\ \ldots,\ x_{a-1}\}$. Em particular, $card(Ap(I,a)) = a$.

Demonstração. Consideremos inicialmente x_i como definido na proposição. Então existe $k \in \mathbb{Z}$ tal que $x_i = ka + i$. Então $x_i - a = (k-1)a + i \notin I$, pois caso contrário $x_i - a$ iria contrariar a minimalidade de x_i. Logo, $x_i \in Ap(I,a)$.

Agora, dado $x \in Ap(I,a)$, temos que $x \equiv i \mod (a)$, para algum $i \in \{0,\ 1,\ \ldots,\ a-1\}$. Desse modo, $x \geq x_i$. Sejam $k_1,\ k_2 \in \mathbb{Z}$ tais que $x_i = k_1a + i$ e $x = k_2a + i$ e suponha $x > x_i$, ou seja, $k_2 > k_1$. Então $x - a = k_2a + i - a = (k_2 - (k_1+1))a + k_1a + i \in I$, pois $(k_2 - (k_1+1))a \in I$ (já que $k_2 - (k_1+1) \geq 0$) e $k_1a + i = x_i \in I$, o que é um absurdo, pois $x \in Ap(I,a)$. Logo, $x = x_i$ e, portanto, $Ap(I,a) = \{x_0,\ x_1,\ \ldots,\ x_{a-1}\}$.

□

Exemplo 3.3.6: Sejam $S = \langle 3,\ 5\rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$ e $I = \{5,\ 6,\ 8,\ \rightarrow\}$. Para cada $i = 0,\ 1,\ 2,\ 3,\ 4,\ 5$, seja $x_i = \min\{x \in I \mid x \equiv i \mod 6\}$. Da proposição 3.23 temos que:

$$Ap(I,6) = \{5,\ 6,\ 8,\ 9,\ 10,\ 13\},\ \text{e}\ card(Ap(I,6)) = 6.$$

Corolário 3.24: Seja S um semigrupo. Então $e(S) \leq \mu(S)$.

Demonstração. Basta observar que $\mu(S) + M \subseteq 2M$ (pois $\mu(S) \in M$). Logo

$$M \setminus 2M \subseteq M \setminus (\mu(S) + M) = Ap(M, \mu(S)),$$

o que implica $card(M \setminus 2M) \leq card(Ap(M,\mu(S)))$, ou seja, $e(S) \leq \mu(S)$.

□

Proposição 3.25: Seja S um semigrupo, M o seu ideal maximal e $m \in M$ tal que $Ap(M,m) = \{x_0,\ x_1,\ \ldots,\ x_{m-1}\}$, em que $x_i = \min\{x \in M \mid x \equiv i \mod (m)\}$ para cada $i = 0,\ 1,\ \ldots,\ m-1$. Então $S = \langle x_0,\ x_1,\ \ldots,\ x_{m-1}\rangle$.

Demonstração. Naturalmente, $\{x_0,\ x_1,\ \ldots,\ x_{m-1}\} \subseteq S$. Note que $x_0 = m$. Seja agora $s \in M$. Se $m \mid s$, então existe $a \in \mathbb{N}$ tal que $s = am = ax_0 + 0x_1 + \ldots + 0x_{m-1}$. Desse modo, $s \in \langle x_0,\ x_1,\ \ldots,\ x_{m-1}\rangle$. Agora, se $m \nmid s$, então existem $i \in \{1,\ 2,\ \ldots,\ m-1\}$ e $q \in \mathbb{N}$ tais que $s = qm + i$. Pela minimalidade de x_i, existe $k \in \mathbb{N}$ tal que $s = km + x_i \in \langle x_0,\ x_1,\ \ldots,\ x_{m-1}\rangle$, uma vez que km é múltiplo de x_0.

□

Exemplo 3.3.7: Sejam $S = \{0,\ 4,\ 5,\ 6,\ 8, \rightarrow\}$ e $M = \{4,\ 5,\ 6,\ 8, \rightarrow\}$ seu ideal maximal. Para cada $i = 0,\ 1,\ 2,\ 3$, seja $x_i = \min\{x \in I \mid x \equiv i \mod 4\}$. De acordo com a proposição 3.23, $Ap(M,4) = \{4,\ 5,\ 6,\ 11\}$. Note que $S = \langle 4,\ 5,\ 6,\ 11\rangle$, satisfazendo a proposição 3.25. Como $11 = 5 + 6$, temos que $\{4,\ 5,\ 6\}$ é o conjunto minimal de geradores de S. Desse modo, $e(S) = 3 \leq 4 = \mu(S)$, conforme o corolário 3.24.

Na teoria de semigrupos há o estudo de algumas sequências, e nessa seção iremos apresentar algumas delas. Para isso, iniciaremos com a definição abaixo:

Definição 3.26: O **tipo** de um semigrupo S é definido por

$$tipo(S) = card((S - M) \setminus S)$$

e, por simplicidade, podemos escrever $tipo(S) = t(S)$.

Para $S \neq \mathbb{N}$, definimos $T(S) = (S - M) \setminus S$, também representado simplesmente por T. Observe que $T \neq \emptyset$, pois $\gamma(S) \in T$. Um elemento de $T(S)$ é chamado de **pseudonúmero de Fröbenius** de S.

Exemplo 3.3.8: Seja $S = \langle 6,\ 7,\ 8,\ 10,\ 11\rangle = \{0,\ 6,\ 7,\ 8,\ 10,\ \rightarrow\}$. Temos:

$$\begin{aligned} M &= \{6,\ 7,\ 8,\ 10,\ \rightarrow\} \\ S - M &= \{0,\ 4,\ \rightarrow\} \\ T &= \{4,\ 5,\ 9\} \end{aligned}$$

Portanto, $t(S) = 3$.

Vamos agora definir algumas cadeias de semigrupos. Seja o semigrupo

$$S = \{0 = s_0,\ s_1,\ s_2,\ \ldots,\ s_n,\ \rightarrow\}.$$

Para cada $i \geq 0$, consideremos os conjuntos $S_i = \{s \in S \mid s \geq s_i\}$ e $S(i) = S - S_i$. Note que $S_1 = M$ e $S(i) = S - S_i$ é um ideal relativo. De fato, seja $x \in S + S(i)$. Então $x = s + a$, com $s \in S$ e $a \in S(i)$. Seja agora $s_j \in S_i$. Então $x + s_j = s + a + s_j \in S$, pois $a + s_j \in S$, já que $a \in S(i)$. Portanto, $x \in S(i)$, e assim $S + S(i) \subseteq S(i)$. Sendo β o condutor de S, $\beta + i$ é um inteiro tal que $(\beta + i) + S(i) \subseteq S$.

Para cada $0 \leq i \leq n$, note que $S(i) = S_i - S_i$ e $S(i)$ é um semigrupo: naturalmente, $S_i - S_i \subseteq S - S_i$. Seja agora $x \in S - S_i$. Então $x + S_i \subseteq S$. Suponha que $x < 0$. Então devemos ter $x \in \{-1, -2, \ldots, -s_i\}$, pois se $x < -s_i$, teríamos $x + s_i < 0 \in S$, o que é um absurdo. Note que $-x - 1 \geq 0$, então $(\beta - x - 1) \in S_i$, para todo $0 \leq i \leq n$. Mas então teríamos $x + \beta - x - 1 = \beta - 1 = \gamma \in S$, o que é um absurdo. Portanto, devemos ter $x \geq 0$. Desse modo, segue que $x + s_i \geq s_i$ para todo $s_i \in S_i$. Portanto, $x + S_i \subseteq S_i$, ou seja, $x \in S_i - S_i$, e temos então que $S - S_i \subseteq S_i - S_i$, concluindo assim que $S(i) = S_i - S_i$.

Para verificar que $S(i)$ é semigrupo, observe que $S(i) \subseteq \mathbb{N}$, pois acabamos de mostrar que se $x \in S(i)$, então $x \geq 0$. Naturalmente, $0 \in S(i)$. Sejam agora $x, y \in S(i)$. Então $x + S_i \subseteq S_i$ e $y + S_i \subseteq S_i$, logo $x + y + S_i \subseteq S_i$, mostrando que $x + y \in S(i)$. Por fim, se $w \in \mathbb{N} \setminus S(i)$, então $1 \leq w \leq \beta$, mostrando que $\mathbb{N} \setminus S(i)$ é finito.

É fácil ver que

$$\begin{aligned} S(0) &= S, \\ S(1) &= M - M, \\ S(n-1) &= \{0,\ s_n - s_{n-1},\ \rightarrow\}, \\ S(n) &= \mathbb{N}. \end{aligned}$$

Temos assim a cadeia de semigrupos

$$S = S(0) \subseteq S(1) = M - M \subseteq S(2) \subseteq \ldots \subseteq S(n) = \mathbb{N},$$

denominada $\mathbf{S}(\cdot)$.

Exemplo 3.3.9: Seja $S = \langle 3,\ 5\rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$. Temos:

$S_0 = S$	$S(0) = S$
$S_1 = \{3,\ 5,\ 6,\ 8,\ \rightarrow\} = M$	$S(1) = \{0,\ 3,\ 5,\ \rightarrow\} = M - M$
$S_2 = \{5,\ 6,\ 8,\ \rightarrow\}$	$S(2) = \{0,\ 3,\ \rightarrow\}$
$S_3 = \{6,\ 8,\ \rightarrow\}$	$S(3) = \{0,\ 2,\ \rightarrow\} = \{0,\ s_n - s_{n-1},\ \rightarrow\}$
$S_4 = \{8,\ \rightarrow\}$	$S(4) = \mathbb{N}$

E a cadeia $\mathbf{S}(\cdot)$ é

$$S = S(0) \subseteq S(1) \subseteq S(2) \subseteq S(3) \subseteq S(4) = \mathbb{N}.$$

Proposição 3.27: Seja $S = \{0 = s_0,\ s_1,\ \ldots,\ s_n,\ \rightarrow\}$, $S \neq \mathbb{N}$ e $i \in \{0,\ 1,\ \ldots,\ n\}$. Então $\gamma(S(i)) = \gamma(S) - s_i$.

Demonstração. Sejam $x \in \mathbb{Z}$ tal que $x > \gamma(S) - s_i$ e $s \in S_i$. Então $x + s > \gamma(S) + s - s_i \geq \gamma(S)$, o que mostra que $x + s \in S$, implicando que $x \in S - S_i = S(i)$. Observe que $\gamma(S) - s_i \notin S(i)$, pois caso contrário $\gamma(S)$ pertenceria a S, o que é um absurdo. Portanto, $\gamma(S(i)) = \gamma(S) - s_i$.

□

Definição 3.28: Para $1 \leq i \leq n$, denotamos $t_i(S) = card(S(i) \setminus S(i-1))$ e definimos a **sequência tipo** de S como $(t_1(S),\ t_2(S),\ \ldots,\ t_n(S))$. Note que o item (i) da proposição 3.18 garante que $t_1(S) = t(S) = tipo(S)$.

Exemplo 3.3.10: Seja $S = \langle 3,\ 11,\ 13\rangle = \{0,\ 3,\ 6,\ 9,\ 11,\ \rightarrow\}$. Temos:

$S_0 = S$	$S(0) = S$	
$S_1 = \{3,\ 6,\ 9,\ 11,\ \rightarrow\} = M$	$S(1) = \{0,\ 3,\ 6,\ 8,\ \rightarrow\} = M - M$	$t_1 = 2$
$S_2 = \{6,\ 9,\ 11,\ \rightarrow\}$	$S(2) = \{0,\ 3,\ 5,\ \rightarrow\}$	$t_2 = 2$
$S_3 = \{9,\ 11,\ \rightarrow\}$	$S(3) = \{0,\ 2,\ \rightarrow\} = \{0,\ s_n - s_{n-1},\ \rightarrow\}$	$t_3 = 2$
$S_4 = \{11,\ \rightarrow\}$	$S(4) = \mathbb{N}$	$t_4 = 1$

A sequência tipo de S é $(2,\ 2,\ 2,\ 1)$.
Observe também que $\gamma(S) = 10$, e a proposição 3.27 é satisfeita:

$$\gamma(S(0)) = \gamma(S) = 10 = 10 - 0 = \gamma(S) - s_0$$
$$\gamma(S(1)) = 7 = 10 - 3 = \gamma(S) - s_1$$
$$\gamma(S(2)) = 4 = 10 - 6 = \gamma(S) - s_2$$
$$\gamma(S(3)) = 1 = 10 - 9 = \gamma(S) - s_3$$
$$\gamma(S(4)) = \gamma(\mathbb{N}) = -1 = 10 - 11 = \gamma(S) - s_4$$

Uma outra cadeia de semigrupos é usada para definirmos o blowup de S. Antes de apresentá-la, porém, notemos que dado um semigrupo S, para cada ideal relativo E de S e para cada $n \in \mathbb{N}$, o conjunto $(nE - nE)$ é um semigrupo. De fato, seja $x \in (nE - nE)$ e suponha $x < 0$. Então $x + nE \subseteq nE$. Como $nE \subseteq \mathbb{Z}$, nE possui menor elemento z. Mas então $x + z < z \in nE$, o que é um absurdo. Portanto, devemos ter $x \geq 0$. Naturalmente,

$0 \in (nE - nE)$. Dados $a,\ b \in (nE - nE)$, então $a + b + nE \subseteq a + nE \subseteq nE$, onde a primeira inclusão vem do fato de que $b \in nE$, e a segunda de que $a \in nE$. Logo, $a + b \in (nE - nE)$. Por fim, como $(nE - nE) \subseteq \mathbb{N}$ e $S \subseteq (nE - nE)$, os possíveis elementos de $\mathbb{N} \setminus (nE - nE)$ são lacunas de S, mostrando assim que $\mathbb{N} \setminus (nE - nE)$ é finito.

Definição 3.29: Dado um semigrupo S, para cada ideal relativo E de S e para cada $n \in \mathbb{N}$, temos o semigrupo $(nE - nE)$. Sabendo que

$$S \subseteq (E - E) \subseteq (2E - 2E) \subseteq \ldots \subseteq (nE - nE) \subseteq \ldots \subseteq \mathbb{N},$$

podemos definir o semigrupo numérico $B_E S = \bigcup_{n \in \mathbb{N}} (nE - nE)$, denominado **Semigrupo Lipman de S com respeito a E**, ou **blowup de S com respeito a E**.

Exemplo 3.3.11: Seja $S = \langle 4,\ 7,\ 13 \rangle = \{0,\ 4,\ 7,\ 8,\ 11,\ \rightarrow\}$. Vamos calcular o blowup de S com respeito ao ideal relativo $E = \{0,\ 1,\ 4,\ 5,\ 7,\ 8,\ 9,\ 11,\ \rightarrow\}$. Temos:

$$\begin{aligned} E - E &= \{0,\ 4,\ 7,\ 8,\ 11,\ \rightarrow\} \\ 2E &= \{0,\ 1,\ 2,\ 4,\ \rightarrow\} \\ 2E - 2E &= \{0,\ 4,\ \rightarrow\} \\ 3E &= \mathbb{N} = 3E - 3E. \end{aligned}$$

Desse modo, $B_E S = \mathbb{N}$.

Proposição 3.30: Sejam S um semigrupo, I ideal próprio de S e i_1 o menor inteiro pertencente a I. Então existe $z \in \mathbb{N}$ tal que:

(i) $B_I S = zI - zI$;

(ii) $(z + 1)I = zI + i_1$.

Além disso, temos:

(iii) $I + B_I S = i_1 + B_I S$.

Demonstração. Para o item (i), do exposto acima temos que

$$S \subseteq (I - I) \subseteq (2I - 2I) \subseteq \ldots \subseteq (nI - nI) \subseteq \ldots \subseteq \mathbb{N}.$$

Os possíveis elementos de $(kI - kI) \setminus S$, com k inteiro positivo, são as lacunas de S. Como $\mathbb{N} \setminus S$ é finito, a cadeia ascendente $\{kI - kI \mid k \geq 1\}$ irá se estabilizar, ou seja, a partir de um $z \in \mathbb{N}$ temos que $zI - zI = (z + 1)I - (z + 1)I = \ldots$. Logo, existe $z \in \mathbb{N}$ tal que $B_I S = \bigcup_{n \in \mathbb{N}} (nI - nI) = zI - zI$.

Para o item (ii), mostraremos inicialmente que $(h + 1)I = hI + i_1$ para algum $h \geq 1$.

Para cada $j \geq 1$, considere o conjunto $B_j = \{a \in \mathbb{Z} \mid a \geq ji_1,\ a \notin jI\}$. Sabendo que jI é ideal de S, temos $jI + S \subseteq jI$, o que mostra que jI contém todos os inteiros a

partir de um certo ponto e, portanto, B_j é finito. Seja $b_j = card(B_j)$. Como o mapa

$$\begin{aligned} f_j : B_{j+1} &\longrightarrow B_j \\ a &\longmapsto a - i_1 \end{aligned}$$

é injetivo, temos $b_{j+1} \leq b_j$. I é ideal próprio de S, então $I + S \subseteq I$. Dado $a \in B_j$, $a \notin jI$ e, como $jI + S \subseteq jI$, existe $h \geq 1$ tal que $b_{h+1} = b_h$, pois $\mathbb{N} \setminus S$ é finito.

Suponha que exista $a \in (h+1)I \setminus (hI + i_1)$. Então $a \notin (hI + i_1)$, ou seja, $a - i_1 \notin hI$. Como $a \in (h+1)I$, $a \geq (h+1)i_1$, ou seja, $a - i_1 \geq hi_1$, mostrando que $a - i_1 \in B_h$. Pelo fato de f_h ser injetiva e $b_{h+1} = b_h$, segue que f_h é sobrejetiva, logo existe $a' \in B_{h+1}$ tal que $a - i_1 = f_h(a') = a' - i_1$, o que é um absurdo, pois teríamos $a = a' \notin (h+1)I$. Portanto, $(h+1)I \subseteq hI + i_1$ e, como a inclusão contrária é trivial, segue que $(h+1)I = hI + i_1$.

Seja agora $x = p - ki_1$, com $k \geq 1$ e $p \in kI$. Como $(h+1)I = hI + i_1$ para algum $h \geq 1$, segue por indução em k que $(h+k)I = hI + ki_1$. Temos que

$$x + (h+k)I = p - ki_1 + (h+k)I = p - ki_1 + hI + ki_1 = p + hI \subseteq kI + hI = (h+k)I,$$

mostrando que $p - ki_1 = x \in ((h+k)I - (h+k)I) \subseteq B_I S$. Como $B_I S = (zI - zI)$, segue que $\{p - ki_1 \mid k \geq 1,\ p \in kI\} \subseteq (zI - zI)$.

Tomando $k = 1$, temos:

$$I - i_1 \subseteq (zI - zI) \implies I - i_1 + zI \subseteq zI \implies (z+1)I - i_1 \subseteq zI \implies (z+1)I \subseteq zI + i_1.$$

A inclusão inversa é trivial, e assim $(z+1)I = zI + i_1$.

Para o item (iii), tomando novamente $k = 1$, temos $I - i_1 \subseteq (zI - zI)$, ou seja,

$$I - i_1 \subseteq B_I S \implies I \subseteq B_I S + i_1 \implies I + i_1 \subseteq B_I S + i_1$$

A inclusão inversa é trivial, e assim $I + B_I S = B_I S + i_1$.

□

Corolário 3.31: Sejam S, I e i_1 definidos como na proposição anterior. Então, para algum inteiro $z \geq 1$, são equivalentes:

(i) $I + (zI - zI) = i_1 + (zI - zI)$;

(ii) $card(zI \setminus (z+1)I) = i_1$;

(iii) $(z+1)I = zI + i_1$;

(iv) $B_I S = (zI - zI)$.

Demonstração. Para mostrar que (i) $\implies$ (iii), observe que, como $0 \in (zI - zI)$, então por (i) segue que $I \subseteq i_1 + (zI - zI)$. Desse modo, temos:

$$(z+1)I = zI + I \subseteq zI + i_1 + (zI - zI) = zI + i_1.$$

A outra inclusão é trivial, e assim $(z+1)I = zI + i_1$.

Para mostrar que (iii) $\implies$ (iv), observe que para cada $k \geq 1$ segue por indução em k que $(z+k)I = zI + ki_1$. Temos

$$(z+k)I - (z+k)I = (zI + ki_1) - (zI + ki_1) = (zI - zI).$$

Desse modo, a cadeia ascendente $\{kI - kI \mid k \geq 1\}$ estabiliza em $(zI - zI)$, mostrando que $B_I S = (zI - zI)$.

Para mostrar que (iv) $\implies$ (i), basta utilizar o item (iii) da proposição anterior, que nos diz que $I + B_I S = i_1 + B_I S$. Utilizando a hipótese de que $B_I S = (zI - zI)$, segue que $I + (zI - zI) = i_1 + (zI - zI)$.

Por fim, vamos mostrar que (ii) $\iff$ (iii). Sabemos que $zI + i_1 \subseteq (z+1)I \subseteq zI$. Para cada $j = 0,\ 1,\ \ldots,\ i_1 - 1$, seja $x_j = \min\{x \in zI \mid x \equiv j \mod (i_1)\}$. Então existe $k \geq 1$ tal que $x_j = ki_1 + j$. Então $x_j - i_1 = (k-1)i_1 + j \notin zI$, pois caso contrário $x_j - i_1$ iria contrariar a minimalidade de x_j. Portanto, $x_j \notin (zI + i_1)$, ou seja, $x_j \in zI \setminus (zI + i_1)$.

Agora, dado $x \in zI \setminus (zI + i_1)$, temos que $x \equiv j \mod (i_1)$, para algum $j \in \{0,\ 1,\ \ldots,\ i_1 - 1\}$. Desse modo, $x \geq x_j$. Sejam $k_1,\ k_2 \geq 1$ tais que $x_j = k_1 i_1 + j$ e $x = k_2 i_1 + j$ e suponha $x > x_j$, ou seja, $k_2 = k_1 + n$, $n \geq 1$. Então $x = k_2 i_1 + j = (k_1 + n)i_1 + j = k_1 i_1 + j + n i_1 = x_j + n i_1 \in zI + i_1$, o que é um absurdo, pois isso implica em $x \in (zI + i_1)$. Logo, $x = x_j$ e, portanto, $zI \setminus (zI + i_1) = \{x_0,\ x_1,\ \ldots,\ x_{i_1 - 1}\}$, ou seja, $card(zI \setminus (zI + i_1)) = i_1$. Recordando que $zI + i_1 \subseteq (z+1)I \subseteq zI$, segue que $card(zI \setminus (z+1)I) = i_1$ se, e somente se, $(z+1)I = zI + i_1$.

□

Exemplo 3.3.12: Seja $S = \langle 7,\ 8,\ 9,\ 11\rangle = \{0,\ 7,\ 8,\ 9,\ 11,\ 14,\ \rightarrow\}$. Vamos calcular o blowup de S com respeito ao ideal maximal M. Temos:

$$\begin{aligned} M &= \{7,\ 8,\ 9,\ 11,\ 14,\ \rightarrow\}, \\ M - M &= \{0,\ 7,\ \rightarrow\}, \\ 2M &= \{14,\ \rightarrow\}, \\ 2M - 2M &= \{0,\ 1,\ \rightarrow\} = \mathbb{N}, \\ 3M &= \{21,\ \rightarrow\} = 2M + 7. \end{aligned}$$

Desse modo, $B_M S = \mathbb{N}$, e o inteiro z do corolário anterior é 2.

Vamos definir mais duas importantes cadeias de semigrupos:

Definição 3.32: Consideremos as duas cadeias de semigrupos abaixo

$$S = B_0 \subseteq B(B_0) = B_1 \subseteq \ldots \subseteq B(B_h) = B_{h+1} \subseteq \ldots$$

e

$$S = Bl_0 \subseteq Bl(Bl_0) = Bl_1 \subseteq \ldots \subseteq Bl(Bl_h) = Bl_{h+1} \subseteq \ldots$$

definidas, respectivamente, por $\mathbf{B(S)}$ e $\mathbf{Bl(S)}$, em que $B(S) = S - M = M - M$ e $Bl(S) = B_M S = \bigcup_{n\in\mathbb{N}} \{nM - nM \mid n \geq 1\}$ é o **Blowup de S com respeito a M**, ou simplesmente o **Blowup de S**.

Exemplo 3.3.13: Seja $S = \langle 3, 5\rangle = \{0, 3, 5, 6, 8, \rightarrow\}$. Então:

$$B_0 = S,$$
$$M = \{3, 5, 6, 8, \rightarrow\},$$
$$B_1 = M - M = \{0, 3, 5, \rightarrow\}.$$

Considerando M_i o ideal maximal de B_i, segue que:

$$B_2 = B(B_1) = M_1 - M_1 = \{0, 2, \rightarrow\},$$
$$B_3 = B(B_2) = M_2 - M_2 = \mathbb{N}.$$

Assim, a cadeia $\mathbf{B(S)}$ é

$$S = B_0 \subseteq B_1 \subseteq B_2 \subseteq B_3 = \mathbb{N}.$$

Temos também que:

$$Bl_0 = S,$$
$$Bl_1 = Bl(Bl_0) = Bl(S) = B_M S :$$
$$2M = \{6, 8, \rightarrow\} \implies 2M - 2M = \{0, 2, \rightarrow\},$$
$$3M = \{9, 11, \rightarrow\} \implies 3M - 3M = \{0, 2, \rightarrow\},$$

mostrando que $Bl_1 = \{0, 2, \rightarrow\}$. Considerando M' o ideal maximal de Bl_1, temos:

$$Bl_2 = Bl(Bl_1) = B_{M'} Bl_1 :$$
$$M' = \{2, \rightarrow\} \implies M' - M' = \mathbb{N}.$$

Desse modo, a cadeia $\mathbf{Bl(S)}$ é

$$S = Bl_0 \subseteq Bl_1 \subseteq Bl_2 = \mathbb{N}.$$

Proposição 3.33: Sejam $S \neq \mathbb{N}$ um semigrupo, M seu ideal maximal e s_1 o menor elemento de S. As seguintes afirmações são equivalentes:

(i) $S(1) = S_1 - s_1$;

(ii) $e(S) = \mu(S)$;

(iii) $2M = M + s_1$;

(iv) $S(1) = Bl(S)$.

Demonstração. Basta utilizar o corolário 3.31 com $I = M$, $i_1 = s_1$ e $z = 1$, lembrando que $S_1 = M$ e $S(1) = S - M = M - M$.

De fato, para o item (i), do colorário 3.31 temos que $M + (M - M) = s_1 + (M - M)$, ou seja, $S_1 + S(1) = s_1 + S(1)$, o que implica em $S(1) = S_1 + S(1) - s_1$. Seja $x \in S(1) = S_1 + S(1) - s_1$. Então existem $s \in S_1$ e $a \in S(1)$ tais que $x = s + a - s_1$. Mas $s + a = r \in S_1$, logo $x = s + a - s_1 = r - s_1 \in S_1 - s_1$. Desse modo, $S_1 + S(1) - s_1 \subseteq S_1 - s_1$. A outra inclusão é trivial, portanto $S(1) = S_1 + S(1) - s_1 = S_1 - s_1$.

Aplicando os corolários 3.21 e 3.31 e recordando que $s_1 = \mu(S)$, obtemos o item (ii), pois

$$e(S) = card(2M \setminus M) = s_1 = \mu(S).$$

O item (iii) segue diretamente do corolário 3.31, lembrando que $I = M$ e $i_1 = s_1$.

Por fim, recordando que $B_M S = Bl(S)$ e aplicando o corolário 3.31, obtemos (iv):

$$Bl(S) = B_M S = M - M = S(1).$$

□

Observação 3.34: Seja $S = \{0 = s_0,\ s_1,\ \ldots,\ s_n,\ \rightarrow\}$ um semigrupo com condutor β e número de Fröbenius γ. Denotamos por $n(S)$, ou simplesmente n, o número de elementos de S menores que β.

Outra família, também muito importante na Teoria de Semigrupos, é a chamada família de semigrupos Arf.

Definição 3.35: Um semigrupo S é chamado de **Arf** se as cadeias $\mathbf{S}(\cdot)$ e $\mathbf{Bl}(\mathbf{S})$ coincidem, isto é, $Bl_i = S(i)$ para todo $i \in \mathbb{N}$.

Proposição 3.36: Seja S um semigrupo. As seguintes afirmações são equivalentes:

(i) As sequências $\mathbf{B}(\mathbf{S})$ e $\mathbf{Bl}(\mathbf{S})$ coincidem;

(ii) As sequências $\mathbf{S}(\cdot)$, $\mathbf{B}(\mathbf{S})$ e $\mathbf{Bl}(\mathbf{S})$ coincidem;

(iii) $e(S(i)) = \mu(S(i))$, para todo $0 \leq i \leq n(S)$;

(iv) $S(i) = S_i - s_i$, para todo $0 \leq i \leq n(S)$.

Demonstração. Sabendo, por definição, que $S(0) = S = B_0 = Bl_0$, $B_1 = B(B_0) = B(S) = S - M = M - M = S_1 - S_1 = S(1)$ e $Bl_1 = Bl(Bl_0) = Bl(S)$, a proposição 3.33 nos diz que:

$$B_1 = Bl_1 \Leftrightarrow S(1) = Bl(S) \Leftrightarrow e(Bl_0) = \mu(Bl_0) \Leftrightarrow S(1) = S_1 - s_1. \tag{3.3}$$

A equivalência acima é válida para todo semigrupo, e em particular vale para $N = S(i-1)$. Note que $N_1 = S_i - s_{i-1}$ possui $s_i - s_{i-1}$ como menor elemento e

$N(1) = N_1 - N_1 = (S_i - s_{i-1}) - (S_i - s_{i-1}) = S_i - S_i = S(i)$. Pela equivalência (3.3) aplicada ao semigrupo N, temos:

$$\begin{array}{c} B(S(i-1)) = Bl(S(i-1)) \\ \Updownarrow \\ S(i) = B(S(i-1)) = Bl(S(i-1)) \\ \Updownarrow \\ e(S(i-1)) = \mu(S(i-1)) \\ \Updownarrow \\ S(i) = S_i - s_i. \end{array} \tag{3.4}$$

Sabendo que $S(0) = S$ e $S(1) = M - M$, para $i = 1$ e $i = 2$, temos

$$\begin{array}{c} B(S) = Bl(S) \\ \Updownarrow \\ S(1) = B(S) = B_1 = Bl(S) = Bl_1 \\ \Updownarrow \\ e(S) = \mu(S) \\ \Updownarrow \\ S(1) = S_1 - s_1 \end{array} \quad \left| \quad \begin{array}{c} B(S(1)) = B_1 = Bl(S(1)) = Bl_2 \\ \Updownarrow \\ S(2) = B(S(1)) = B_2 = Bl(S(1)) = Bl_2 \\ \Updownarrow \\ e(S(1)) = \mu(S(1)) \\ \Updownarrow \\ S(2) = S_2 - s_2. \end{array} \right.$$

Observe agora que, considerando verdadeira cada afirmação da proposição 3.36, as equivalências são verificadas por indução em i, bastando analisar apenas (3.4).

□

Exemplo 3.3.14: Seja $S = \langle 3,\ 11,\ 13\rangle = \{0,\ 3,\ 6,\ 9,\ 11,\ \rightarrow\}$. Então:

$$\begin{array}{l|l|l} S_0 = S & S(0) = S & \\ S_1 = \{3,\ 6,\ 9,\ 11,\ \rightarrow\} = M & S(1) = \{0,\ 3,\ 6,\ 8,\ \rightarrow\} & t_1 = 2 \\ S_2 = \{6,\ 9,\ 11,\ \rightarrow\} & S(2) = \{0,\ 3,\ 5,\ \rightarrow\} & t_2 = 2 \\ S_3 = \{9,\ 11,\ \rightarrow\} & S(3) = \{0,\ 2,\ \rightarrow\} & t_3 = 2 \\ S_4 = \{11,\ \rightarrow\} & S(4) = \mathbb{N} & t_4 = 1 \end{array}$$

A sequência tipo de S é $(2,\ 2,\ 2,\ 1)$. Temos:

$$\begin{array}{r} M - M = \{0,\ 3,\ 6,\ 8,\ \rightarrow\} = S(1) = S_1 - 3, \\ 2M = \{6,\ 9,\ 12,\ 14,\ \rightarrow\} = M + 3, \\ 2M - 2M = \{0,\ 3,\ 6,\ 8,\ \rightarrow\} = M - M = S(1), \text{ logo } Bl_1 = Bl(S) = S(1), \\ e(S) = 3 = \mu(S). \end{array}$$

Note que as equivalências da proposição 3.33 são satisfeitas: a primeira linha se refere ao item (i), a segunda, ao item (iii), a terceira, ao item (iv) e a quarta linha se refere ao item (ii).

Considerando M_i o maximal de $S(i)$, temos:

$$M_1 - M_1 = \{0,\ 3,\ 5,\ \rightarrow\},\ 2M_1 = \{6,\ 9,\ 11,\ \rightarrow\} \text{ e}$$
$$2M_1 - 2M_1 = \{0,\ 3,\ 5,\ \rightarrow\}, \text{ logo } Bl_2 = S(2).$$
$$M_2 - M_2 = \{0,\ 2,\ \rightarrow\},\ 2M_2 = \{6,\ 8,\ \rightarrow\} \text{ e}$$
$$2M_2 - 2M_2 = \{0,\ 2,\ \rightarrow\}, \text{ logo } Bl_3 = S(3).$$
$$M_3 - M_3 = \mathbb{N}, \text{ logo } Bl_4 = S(4).$$

As sequências $\mathbf{S}(\cdot)$ e $\mathbf{Bl}(\mathbf{S})$ coincidem e, portanto, S é um semigrupo Arf.

Note que todas as equivalências da proposição 3.36 são satisfeitas: para o item (i), temos

$$B_1 = S - M = M - M = Bl_1,$$
$$B_2 = S(1) - M_1 = M_1 - M_1 = Bl_2,$$
$$B_3 = S(2) - M_2 = M_2 - M_2 = Bl_3,$$
$$B_4 = S(3) - M_3 = M_3 - M_3 = Bl_4,$$

e as sequências $\mathbf{B}(\mathbf{S})$ e $\mathbf{Bl}(\mathbf{S})$ coincidem. Como mostramos que S é Arf, concluímos que as cadeias $\mathbf{S}(\cdot)$, $\mathbf{B}(\mathbf{S})$ e $\mathbf{Bl}(\mathbf{S})$ coincidem, satisfazendo assim o item (ii).

Para o item (iii), temos que:

$$e(S) = 3 = \mu(S),$$
$$S(1) = \langle 3,\ 8,\ 10\rangle, \text{ logo } e(S(1)) = 3 = \mu(S(1)),$$
$$S(2) = \langle 3,\ 5,\ 7\rangle, \text{ logo } e(S(2)) = 3 = \mu(S(2)),$$
$$S(3) = \langle 2,\ 3\rangle, \text{ logo } e(S(3)) = 2 = \mu(S(3)).$$

Por fim, para o item (iv) segue que

$$S_1 = \{3,\ 6,\ 9,\ 11,\ \rightarrow\} \implies S(1) = S_1 - S_1 = \{0,\ 3,\ 6,\ 8,\ \rightarrow\} = S_1 - s_1,$$
$$S_2 = \{6,\ 9,\ 11,\ \rightarrow\} \implies S(2) = S_2 - S_2 = \{0,\ 3,\ 5,\ \rightarrow\} = S_2 - s_2,$$
$$S_3 = \{9,\ 11,\ \rightarrow\} \implies S(3) = S_3 - S_3 = \{0,\ 2,\ \rightarrow\} = S_3 - s_3,$$
$$S_4 = \{11,\ \rightarrow\} \implies S(4) = S_4 - S_4 = \mathbb{N} = S_4 - s_4.$$

Definição 3.37: Um semigrupo é chamado de **semigrupo com dimensão máxima de mergulho** quando $\mu(S) = e(S)$. Se $S = \langle n_1,\ \ldots,\ n_k\rangle$, então $k = s_1$.

Exemplo 3.3.15: Seja $S = \langle 3,\ 11,\ 13\rangle = \{0,\ 3,\ 6,\ 9,\ 11,\ \rightarrow\}$. Note que $e(S) = 3 = \mu(S)$, o que mostra que S é um semigrupo com dimensão máxima de mergulho. Conforme visto no exemplo anterior, S é também um semigrupo Arf.

Proposição 3.38: Todo semigrupo Arf é um semigrupo com dimensão máxima de mergulho.

Demonstração. Seja S um semigrupo Arf. Então as cadeias $\mathbf{S}(\cdot)$ e $\mathbf{Bl}(\mathbf{S})$ coincidem. Desse modo, o item (iv) da proposição 3.33 é satisfeito e, portanto, o item (ii) também,

mostrando que S é um semigrupo com dimensão máxima de mergulho.

□

Observação 3.39: A recíproca da proposição anterior é falsa, como ilustra o exemplo abaixo:

Exemplo 3.3.16: Considere o semigrupo

$$S = \langle 5,\ 14,\ 16,\ 17,\ 23\rangle = \{0,\ 5,\ 10,\ 14,\ 15,\ 16,\ 17,\ 19,\ \rightarrow\}.$$

Como $\mu(S) = 5 = e(S)$, vemos que S tem dimensão máxima de mergulho. Temos:

$S_0 = S$	$S(0) = S$
$S_1 = \{5,\ 10,\ 14,\ 15,\ 16,\ 17,\ 19,\ \rightarrow\}$	$S(1) = \{0,\ 5,\ 9,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\}$
$S_2 = \{10,\ 14,\ 15,\ 16,\ 17,\ 19,\ \rightarrow\}$	$S(2) = \{0,\ 5,\ 6,\ 7,\ 9,\ \rightarrow\}$
$S_3 = \{14,\ 15,\ 16,\ 17,\ 19,\ \rightarrow\}$	$S(3) = \{0,\ 5,\ \rightarrow\}$

Desse modo:

$$\begin{aligned} M - M &= \{0,\ 5,\ 9,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\} = S(1),\\ 2M &= \{10,\ 15,\ 19,\ 20,\ 21,\ 22,\ 24,\ \rightarrow\},\\ 2M - 2M &= \{0,\ 5,\ 9,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\} = M - M = S(1),\ \text{logo}\\ Bl_1 &= S(1). \end{aligned}$$

Considerando M_i o maximal de $S(i)$, temos:

$$\begin{aligned} &M_1 - M_1 = \{0,\ 5,\ 6,\ 7,\ 9,\ \rightarrow\},\ 2M_1 = \{10,\ 14,\ 15,\ 16,\ 17,\ 19,\ \rightarrow\} \text{ e}\\ &2M_1 - 2M_1 = \{0,\ 5,\ 6,\ 7,\ 9,\ \rightarrow\} = M_1 - M_1, \text{ logo } Bl_2 = S(2).\\ &M_2 - M_2 = \{0,\ 4,\ \rightarrow\},\ 2M_2 = \{10,\ \rightarrow\} \text{ e } 2M_2 - 2M_2 = \{0,\ 1,\ \rightarrow\} = \mathbb{N},\\ &\text{logo } Bl_3 = \mathbb{N} \neq S(3). \end{aligned}$$

Desse modo, as sequências $\mathbf{S}(\cdot)$ e $\mathbf{Bl}(\mathbf{S})$ não coincidem e, portanto, S não é um semigrupo Arf.

Definição 3.40: Um ideal relativo W é dito **canônico** se para qualquer ideal relativo E de S tivermos $W - (W - E) = E$.

Teorema 3.41: Seja S um semigrupo numérico com número de Fröbenius γ. Existe um ideal relativo K de S tal que, para quaisquer ideais relativos $F \subseteq E$, vale $card(E \setminus F) = card((K - F) \setminus (K - E))$.

Demonstração. Considere o conjunto

$$K = \{a \in \mathbb{Z} \mid \gamma - a \notin S\} = \{\gamma - a \mid a \notin S\}. \tag{3.5}$$

K é ideal relativo de S. De fato, seja $x \in S + K$, ou seja, $x = s + a$ com $s \in S$ e $a \in K$. Suponha que $x \notin K$. Então $\gamma - x = \gamma - s - a \in S$. Como $s \in S$, então

$\gamma - s - a + s = \gamma - a \in S$, o que é um absurdo, pois $a \in K$. Portanto, $x \in K$, o que mostra que $S + K \subseteq K$. O condutor $\beta = \gamma + 1$ de S é um inteiro tal que $\beta + K \subseteq S$, mostrando assim que K é ideal relativo de S.

Vamos mostrar agora que, para todo ideal relativo E de S, temos

$$K - E = \{\gamma - a \mid a \notin E\}.$$

Para isso, definimos os conjuntos

$$A = \{a \in \mathbb{Z} \mid a + E \subseteq K\} = K - E,$$
$$B = \{\gamma - b \mid b \notin E\}$$

e mostraremos que $A = B$.

Sejam $x \in E$ e $y = \gamma - b \in B$. Suponha que $b - x \in S$. Então $b \in x + S \subset E + S \subseteq E$, o que é um absurdo, pois como $y \in B$, então $b \notin E$. Desse modo, $b - x \notin S$. Com isso, temos que

$$b - x = \gamma - (\gamma - b) - x \notin S \implies \gamma - (y + x) \notin S \implies y + x \in K \implies y \in A,$$

mostrando que $B \subseteq A$.

Para mostrar a outra inclusão, tome $z \in A$ e escreva $z = \gamma - (\gamma - z)$. Suponha que $z \notin B$. Então $\gamma - z \in E$ e $z + (\gamma - z) = \gamma \in K$, o que é um absurdo, pois $0 \in S$. Desse modo, $z \in B$ e , portanto, $A \subseteq B$, o que nos permite concluir que $A = B$.

Por fim, temos então que

$$\begin{aligned} card((K - F) \setminus (K - E) &= card(\{\gamma - a \mid a \notin F\} \setminus \{\gamma - b \mid b \notin E\}) \\ &= card(\{\gamma - c \mid c \in E \setminus F\}) \\ &= card(E \setminus F) \end{aligned}$$

□

Teorema 3.42: Todo semigrupo S possui um ideal canônico.

Demonstração. Sejam $K = \{a \mid \gamma - a \notin S\}$ como definido em (3.5) e E um ideal relativo de S. Sabendo que $K - E = \{\gamma - a \mid a \notin E\}$, temos

$$\begin{aligned} K - (K - E) &= \{\gamma - b \mid b \notin (K - E)\} \\ &= \{\gamma - (\gamma - a) \mid a \in E\} \\ &= \{a \mid a \in E\} \\ &= E. \end{aligned}$$

Desse modo, K é ideal canônico de S.

□

Proposição 3.43: Seja K como definido em (3.5) ideal canônico do semigrupo S. Então $S \subset K$.

Demonstração. Observe inicialmente que $0 \in K$, pois $\gamma - 0 = \gamma \notin S$. Suponha que exista $s_i \in S$ tal que $s_i \notin K$. Então $\gamma - s_i \in S$, ou seja, existe $s_j \in S$ tal que $\gamma - s_i = s_j$. Mas isso implica em $\gamma = s_i + s_j \in S$, o que é um absurdo. Portanto, $S \subset K$.

□

Exemplo 3.3.17: Seja $S = \{0,\ 6,\ 7,\ 8,\ 11,\ \rightarrow\}$. Temos que $\gamma(S) = 10$. Então

$$K = \{a \in \mathbb{Z} \mid 10 - a \notin S\} = \{10 - a \mid a \notin S\} = \{0,\ 1,\ 5,\ 6,\ 7,\ 8,\ 9,\ 11,\ \rightarrow\}$$

é um ideal canônico de S. Observe que $S \subset K$.

Proposição 3.44: Seja E um ideal relativo de S tal que $S \subset E$. Então $E = E - S$.

Demonstração. Seja $e \in E$. Então $e + S \in E + S \subseteq E$, logo $e \in E - S$. Reciprocamente, considere $x \in E - S$. Então $x + S \subseteq E$ e, em particular, $x + 0 = x \in E$. Desse modo, $E = E - S$.

□

Corolário 3.45: Seja K um ideal canônico de S. Então $K - K = S$.

Demonstração. Basta considerar o caso particular em que $E = K$, e assim

$$K - K = K - (K - S) = S,$$

em que a última igualdade segue do fato de K ser ideal canônico.

□

Definição 3.46: Seja E um ideal relativo de um semigrupo S. Dizemos que $E^* = S - E$ é o **dual** de E.

Observação 3.47: Note que $E \subseteq E^{**} = S - (S - E)$. De fato, seja $a \in S - E$. Então $a + E \subseteq S$. Em particular, dado $e \in E$, temos que $e + a \in S$, mostrando que $e \in S - (S - E) = \{b \in \mathbb{Z} \mid b + (S - E) \subseteq S\}$.

Definição 3.48: Se $E = E^{**}$, dizemos que E é **ideal bidual** de S.

Exemplo 3.3.18: Sejam $S = \langle 3,\ 5\rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$, $E = \{-3,\ 0,\ 2,\ 3,\ 5,\ \rightarrow\}$ e $M = \{3,\ 5,\ 6,\ 8,\ \rightarrow\}$. O dual de E é

$$E^* = S - E = \{3,\ 6,\ 8,\ 11,\ \rightarrow\}.$$

Já o dual de M é

$$M^* = S - M = M - M = \{0,\ 3,\ 5,\ \rightarrow\}.$$

Note que M é ideal bidual, pois

$$M^{**} = S - (S - M) = \{3,\ 5,\ 6,\ 8,\ \rightarrow\} = M.$$

A proposição a seguir nos mostra que o semigrupo $S = \langle 3,\ 5\rangle$ não é o único que possui ideal maximal bidual.

Proposição 3.49: Seja $S \neq \mathbb{N}$ um semigrupo. Então seu ideal maximal M é bidual.

Demonstração. Sabendo que $M \subseteq M^{**} = S-(S-M)$, basta mostrar que $S-(S-M) \subseteq M$. Observe que $S \subsetneq S - M$, pois $\gamma \in (S - M)$, e assim temos que

$$S - (S - M) \subsetneq S - S = S.$$

Note que $0 \notin S - (S - M)$, pois caso contrário teríamos $(S - M) \subseteq S$, portanto

$$S - (S - M) \subseteq M,$$

e assim $M = S - (S - M) = M^{**}$, mostrando que M é bidual.

□

3.4 Semigrupos simétricos, pseudossimétricos e quase simétricos

Nesta seção, vamos definir três famílias importantes de semigrupos e algumas de suas propriedades: os semigrupos simétricos, pseudossimétricos e quase simétricos.

Definição 3.50: Um semigrupo S é chamado de **simétrico** se o seu condutor é igual ao dobro do seu gênero, ou seja, se $\beta = 2g$.

Exemplo 3.4.1: Seja $S = \langle 3,\ 5\rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$. S possui condutor $\beta = 8$ e gênero $g = 4$, pois o conjunto das lacunas de S é $\mathbb{N} \setminus S = \{1,\ 2,\ 4,\ 7\}$. Desse modo, S é um semigrupo simétrico.

Observação 3.51: Note que se S é simétrico, então $n(S) = \dfrac{\gamma + 1}{2} = \dfrac{\beta}{2}$, sendo $n(S)$ conforme definido na observação 3.34.

Proposição 3.52: Se S é um semigrupo simétrico com condutor β, então $i \in \mathbb{N}$ é uma lacuna de S se, e somente se, $\beta - 1 - i$ é um elemento de S.

Demonstração. Como S é simétrico, a quantidade de lacunas e de elementos entre 0 e $\beta - 1$ é a mesma. Seja então i uma lacuna de S e suponha que $\beta - 1 - i$ também o é. Desse modo, existe $k \in \mathbb{N}$ tal que k e $\beta - 1 - k$ são elementos de S. Temos então que

$$k + (\beta - 1 - k) = \beta - 1 = \gamma \in S,$$

o que é um absurdo. Portanto, $\beta - 1 - i \in S$.

Reciprocamente, seja $i \in \mathbb{N}$ tal que $\beta - 1 - i \in S$ e suponha que $i \in S$. Então

$$\beta - 1 - i + i = \beta - 1 = \gamma \in S,$$

o que é um absurdo. Logo, i é uma lacuna de S.

□

Podemos representar um semigrupo numérico através de um diagrama da seguinte maneira: o condutor é colocado na primeira coluna na linha inferior. Nas demais colunas, colocamos dois números inteiros cuja soma é o número de Fröbenius, listados em ordem crescente na linha superior e em ordem decrescente na linha inferior. Uma bolinha preta significa que o número correspondente pertence ao semigrupo. Já a bolinha com o interior branco indica que o número correspondente não pertence ao semigrupo. Observe abaixo o diagrama do semigrupo $S = \{0,\ 3,\ 6,\ 9,\ \rightarrow\}$:

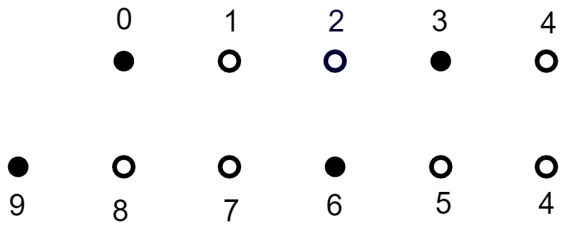

Figura 3.1: Diagrama do semigrupo $S = \langle 3,\ 10,\ 11\rangle$

Uma maneira de identificar um semigrupo simétrico através do seu diagrama é observar que, do teorema anterior, o diagrama possui uma bolinha preta em cada coluna. Naturalmente, essa bolinha preta deve ser única, pois a soma de dois elementos de uma mesma coluna é o número de Fröbenius do semigrupo.

Exemplo 3.4.2: Conforme vimos no exemplo 3.4.1, $S = \langle 3,\ 5\rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$ é um semigrupo simétrico. Este fato também pode ser verificado no seu diagrama abaixo:

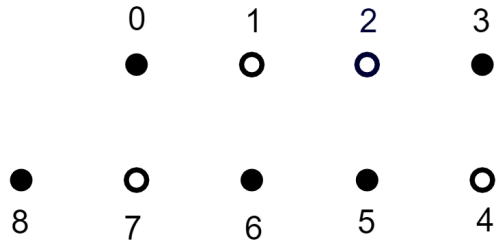

Figura 3.2: Diagrama do semigrupo $S = \langle 3,\ 5\rangle$

Exemplo 3.4.3: Seja $S' = \langle 4,\ 6,\ 11\rangle = \{0,\ 4,\ 6,\ 8,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\}$. S' possui condutor $\beta = 14$ e gênero $g = 7$, pois o conjunto das lacunas de S' é $\mathbb{N} \setminus S' = \{1,\ 2,\ 3,\ 5,\ 7,\ 9,\ 13\}$. Portanto, S' é um semigrupo simétrico, conforme ilustrado no diagrama abaixo:

Proposição 3.53: Sejam S um semigrupo e K o ideal canônico definido em (3.5). Então S é simétrico se, e somente se, $S = K$.

Demonstração. Suponha que S é simétrico. Da proposição 3.43, sabemos que $S \subset K$. Para mostrar que $K \subset S$, tome $a \in K$. Como $\gamma - a \notin S$, ou $\gamma - a$ é lacuna

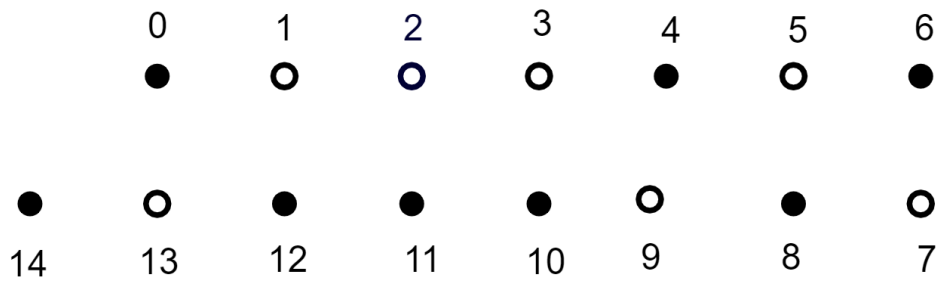

Figura 3.3: Diagrama do semigrupo $S' = \langle 4,\ 6,\ 11 \rangle$

de S, ou $\gamma - a < 0$. Se $\gamma - a$ é lacuna de S, pela proposição 3.52 temos que $\beta - 1 - (\gamma - a) = \gamma - (\gamma - a) = a \in S$. Se $\gamma - a < 0$, então $a > \gamma$, ou seja, $a \geq \beta$ e, portanto, $a \in S$. Assim, temos que $S = K$.

Reciprocamente, suponha que $S = K$ e seja $a < \beta$ um elemento de S. Desse modo, $a \in S = K$, e assim $\gamma - a \notin S$. Portanto, a quantidade de lacunas e de elementos de S entre 0 e $\beta - 1$ é a mesma e, pela observação 3.51, temos que

$$g(S) = \frac{n(S)}{2} = \frac{\beta}{2},$$

mostrando que S é simétrico.

□

Proposição 3.54: Um semigrupo S é simétrico se, e somente se, $tipo(S) = 1$.

Demonstração. Suponha que S é simétrico, ou seja, $S = K$. Aplicaremos o teorema 3.41 com $F = S$ e $E = S - M$. Temos:

$$\begin{aligned} tipo(S) &= card((S - M) \setminus S) \\ &= card((K - S) \setminus (K - (S - M)) \\ &= card((S - S) \setminus (K - (K - M)) \\ &= card(S \setminus M) \\ &= 1. \end{aligned}$$

Reciprocamente, suponha que $tipo(S) = 1$ e que S não é simétrico, ou seja, $S \neq K$. Considere

$$b = max\{a \in (K \setminus S)\}.$$

Dado $s \in M$, temos que $s \neq \gamma - b$, pois caso contrário teríamos $\gamma - b \in S$, o que é um absurdo já que $b \in K$. Desse modo, se $s > \gamma - b$, então $b + s > \gamma$, e assim $(b + s) \in M$. Agora, se $s < \gamma - b$, temos $(b + s) \in M$ ou $(b + s) \notin M$. Suponha que $(b + s) \notin M$. Como $s < \gamma - b$, então $b + s < \gamma$, ou seja, $b + s = \gamma - a,\ a > 0$. Se $a = s_i \in M$, então $b + s = \gamma - s_i \implies \gamma = b + s + s_i = b + s_j,\ s_j \in M$, implicando que $\gamma - b = s_j \in M \subset S$, o que é um absurdo pois $b \in K$. Logo, $b + s = \gamma - a$, com $a \notin M$, e então $(b + s) \in K$,

contrariando a maximalidade de b. Portanto, devemos ter $(b+s) \in M$, o que implica em $b \in ((M-M) \setminus S) = ((S-M) \setminus S)$. Observe que $\gamma \in ((S-M) \setminus S)$ e $b \neq \gamma$, pois $b \in K$. Assim, segue que $tipo(S) \geq 2$, o que é um absurdo. Portanto, devemos ter $S = K$, o que mostra que S é simétrico.

□

Exemplo 3.4.4: Consideremos novamente o semigrupo

$$S = \langle 3,\ 5 \rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}.$$

Conforme vimos no exemplo 3.4.2, S é simétrico. De fato, observe que

$$K = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\} = S$$

e também que

$$\begin{aligned} M &= \{3,\ 5,\ 6,\ 8,\ \rightarrow\} \\ S - M &= \{0,\ 3,\ 5,\ \rightarrow\} \\ T &= (S-M) \setminus S = \{7\} \\ tipo(S) &= 1. \end{aligned}$$

Note que $n(S) = 4 = \dfrac{\beta}{2}$.

Definição 3.55: Seja S um semigrupo com condutor β e gênero g. S é chamado de **pseudossimétrico** se $\beta = 2g - 1$.

Exemplo 3.4.5: Seja $S = \langle 3,\ 5,\ 7 \rangle = \{0,\ 3,\ 5,\ \rightarrow\}$. O conjunto das lacunas de S é $\mathbb{N} \setminus S = \{1,\ 2,\ 4\}$. Observe que S possui gênero $g = 3$ e condutor $\beta = 5 = 2.3 - 1$. Desse modo, S é um semigrupo pseudossimétrico.

Proposição 3.56: Se S é um semigrupo pseudossimétrico com condutor β, então $i \in \mathbb{N} \setminus \left\{ \dfrac{\beta - 1}{2} \right\}$ é uma lacuna de S se, e somente se, $\beta - 1 - i$ é um elemento de S.

Demonstração. A demonstração é análoga a apresentada em 3.52, bastando observar que, como S é pseudossimétrico, entre 0 e $\beta - 1$ há uma lacuna a mais que elementos de S, uma vez que $\dfrac{\beta-1}{2} \notin S$. De fato, se $\dfrac{\beta-1}{2} \in S$, como S é fechado para a soma, teríamos que

$$\frac{\beta-1}{2} + \frac{\beta-1}{2} = \beta - 1 = \gamma \in S,$$

o que é um absurdo.

□

Uma maneira de identificar um semigrupo pseudossimétrico através do seu diagrama é observar que, do teorema anterior, o diagrama possui uma única bolinha preta em cada coluna, exceto na última.

Exemplo 3.4.6: Conforme vimos no exemplo 3.4.5, $S = \langle 3,\ 5,\ 7\rangle = \{0,\ 3,\ 5,\ \rightarrow\}$ é um semigrupo pseudossimétrico. Este fato também pode ser verificado no seu diagrama abaixo:

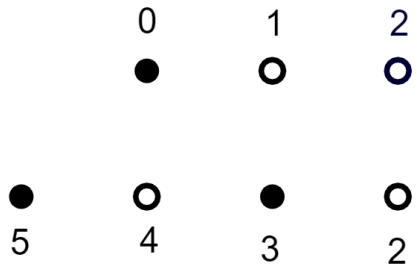

Figura 3.4: Diagrama do semigrupo $S = \langle 3,\ 5,\ 7\rangle$

Exemplo 3.4.7: Seja $S' = \langle 4,\ 7,\ 9\rangle = \{0,\ 4,\ 7,\ 8,\ 9,\ 11,\ \rightarrow\}$. O conjunto das lacunas de S' é $\mathbb{N} \setminus S' = \{1,\ 2,\ 3,\ 5,\ 6,\ 10\}$. Observe que S' possui gênero $g = 6$ e condutor $\beta = 11 = 2.6 - 1$. Desse modo, S' é um semigrupo pseudossimétrico, conforme ilustrado no diagrama abaixo:

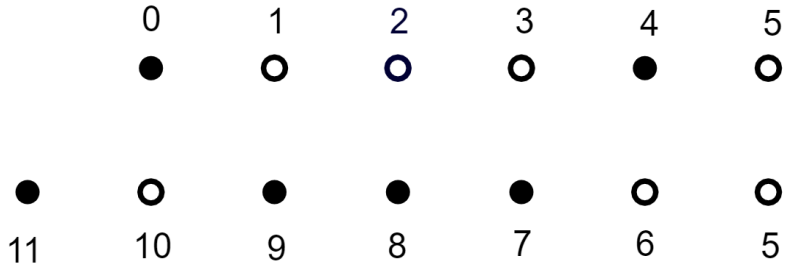

Figura 3.5: Diagrama do semigrupo $S' = \langle 4,\ 7,\ 9\rangle$

Definição 3.57: Seja S um semigrupo com número de Fröbenius γ. Definimos os seguintes conjuntos:

$$H(S) = \{a \in \mathbb{N} \mid \gamma - a \in S\}$$
$$L(S) = \{a \in \mathbb{N} \mid a \notin S,\ \gamma - a \notin S\}.$$

Os elementos de $H(S)$ são chamados de **furos positivos de primeiro tipo**, enquanto os elementos de $L(S)$ são denominados **furos positivos de segundo tipo**. Por simplicidade, podemos representar $L(S)$ apenas por L e $H(S)$ apenas por H.

Exemplo 3.4.8: Seja $S = \langle 4,\ 5\rangle = \{0,\ 4,\ 5,\ 8,\ 10,\ 12, \rightarrow\}$. Então

$$H(S) = \{1,\ 3,\ 6,\ 7,\ 11\}$$
$$L(S) = \{2,\ 9\}.$$

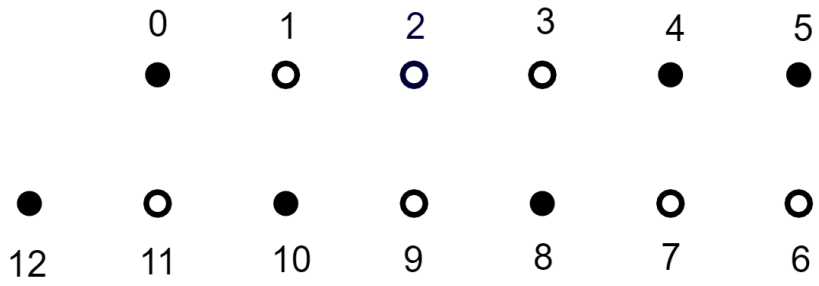

Figura 3.6: Diagrama do semigrupo $S = \langle 4,\ 5\rangle$

Observação 3.58: Os conjuntos H e L podem ser identificados no diagrama do semigrupo: os furos do primeiro tipo são aqueles números que acompanham uma bolinha branca em uma coluna em que a outra bolinha é preta. Já os furos do segundo tipo são aqueles números em que não há bolinha preta na coluna. Observe também que

$$K = S \cup L, \quad L = K \setminus S, \quad \mathbb{N} \setminus S = H \cup L, \quad \mathbb{N} = H \cup L \cup S.$$

De fato, seja $a \in S \cup L$. Se $a \in S$, de acordo com a proposição 3.43 temos que $a \in K$. Agora, se $a \in L$, então $\gamma - a \notin S$, mostrando que $a \in K$. Logo, $S \cup L \subseteq K$. Reciprocamente, dado $a \in K = \{a \in \mathbb{Z} \mid \gamma - a \notin S\}$, temos duas possibilidades: ou $a \in S$ ou $a \notin S$. No segundo caso, segue que $a \in L$, e assim $K \subseteq S \cup L$. Dessa forma, $K = S \cup L$ e, consequentemente, $L = K \setminus S$.

Seja agora $a \in H \cup L$. Se $a \in H$, então $\gamma - a \in S$ e, portanto, a é lacuna de S, pois caso contrário, pelo fato de S ser fechado para a soma, teríamos que $(\gamma - a) + a = \gamma \in S$, o que é um absurdo. Agora, se $a \in L$, pela definição 3.57 segue que $a \in \mathbb{N}$ e $a \notin S$. Logo, $H \cup L \subseteq \mathbb{N} \setminus S$. Reciprocamente, seja a uma lacuna de S. Então ou $\gamma - a \in S$, e assim $a \in H$, ou $\gamma - a \notin S$, e então $a \in L$. Desse modo, $\mathbb{N} \setminus S \subseteq H \cup L$. Portanto, $\mathbb{N} \setminus S = H \cup L$, o que nos permite concluir que $\mathbb{N} = H \cup L \cup S$.

Exemplo 3.4.9: Seja $S = \langle 5,\ 14,\ 16,\ 17,\ 23\rangle = \{0,\ 5,\ 10,\ 14,\ 15,\ 16,\ 17,\ 19,\ \rightarrow\}$. Temos:

$$K = \{0,\ 5,\ 6,\ 7,\ 9,\ 10,\ 11,\ 12,\ 14,\ 15,\ 16,\ 17,\ 19,\ \rightarrow\}$$
$$H = \{1,\ 2,\ 3,\ 4,\ 8,\ 13,\ 18\}$$
$$L = \{6,\ 7,\ 9,\ 11,\ 12\}$$

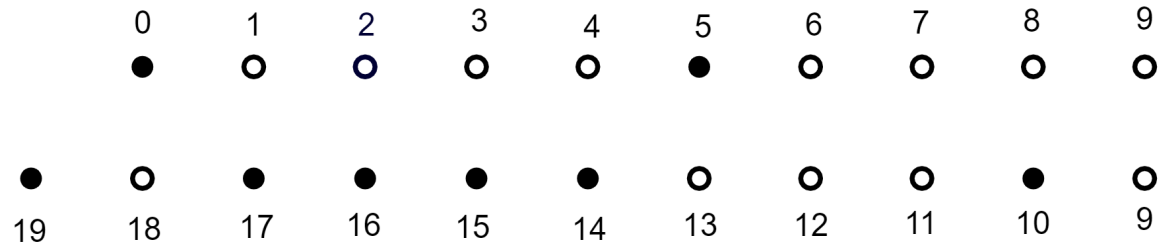

Figura 3.7: Diagrama do semigrupo $S = \langle 5,\ 14,\ 16,\ 17,\ 23\rangle$

Proposição 3.59: Sejam S um semigrupo com número de Fröbenius γ e $L(S)$ o conjunto dos furos de segundo tipo de S. Então:

(i) $L(S) = \emptyset$ se, e somente se, S é simétrico;

(ii) $L(S) = \left\{\frac{\gamma}{2}\right\}$ se, e somente se, S é pseudossimétrico.

Demonstração. Observe que $L(S) = K \setminus S$, em que $K = \{a \in \mathbb{Z} \mid \gamma - a \notin S\}$ é o ideal canônico de S.

Para (i), note que

$$L(S) = \emptyset \iff K = S \iff S \text{ é simétrico.}$$

Para (ii), suponha inicialmente que $L(S) = \left\{\frac{\gamma}{2}\right\}$. Seja $a \neq \frac{\gamma}{2}$ uma lacuna de S. Então $\gamma - a \in S$ pois, caso contrário, $a \in L(S)$. Desse modo, $a \in H$, mostrando assim que entre 0 e β existem $\frac{\beta+1}{2} - 1$ furos do primeiro tipo (pois $\frac{\gamma}{2}$ é furo de segundo tipo). Da observação 3.58, segue que $card(\mathbb{N} \setminus S) = card(H) + card(L)$, ou seja,

$$g = \frac{\beta+1}{2} - 1 + 1 \implies 2g - 1 = \beta,$$

mostrando assim que S é pseudossimétrico.

Reciprocamente, considere S pseudossimétrico e suponha que exista um natural a tal que $a \neq \frac{\gamma}{2}$ e $a \in L(S)$. Como $\gamma - a \notin S$, ou $\gamma - a$ é lacuna de S, ou $\gamma - a < 0$. Se $\gamma - a$ é lacuna de S, pela proposição 3.56 temos que $\beta - 1 - (\gamma - a) = \gamma - (\gamma - a) = a \in S$, o que é um absurdo. Se $\gamma - a < 0$, então $a > \gamma$ e, consequentemente, $a \in S$, tendo novamente um absurdo. Portanto, tal natural a não existe, e assim $L(S) = \left\{\frac{\gamma}{2}\right\}$. □

Exemplo 3.4.10: Consideremos novamente o semigrupo

$$S = \langle 3,\ 5\rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}.$$

Conforme vimos no exemplo 3.4.2, S é simétrico. Note também que

$$L(S) = \{a \in \mathbb{N} \mid a \notin S,\ 7 - a \notin S\} = \emptyset.$$

Exemplo 3.4.11: Consideremos novamente o semigrupo

$$S = \langle 3,\ 5,\ 7\rangle = \{0,\ 3,\ 5,\ \rightarrow\}.$$

Conforme vimos no exemplo 3.4.6, S é pseudossimétrico. Note que

$$L(S) = \{a \in \mathbb{N} \mid a \notin S,\ 4 - a \notin S\} = \{2\} = \left\{\frac{4}{2}\right\}.$$

Proposição 3.60: Sejam S um semigrupo com número de Fröbenius γ e K o ideal canônico definido em (3.5). Então S é pseudossimétrico se, e somente se,

$$K = S \cup \left\{\frac{\gamma}{2}\right\}.$$

Demonstração. Da observação 3.58, temos que $K = S \cup L$. Portanto,

$$K = S \cup \left\{\frac{\gamma}{2}\right\} \iff L = \left\{\frac{\gamma}{2}\right\} \iff S \text{ é pseudossimétrico,}$$

conforme a proposição 3.59.

□

Exemplo 3.4.12: Consideremos novamente o semigrupo

$$S = \langle 3,\ 5,\ 7\rangle = \{0,\ 3,\ 5,\ \rightarrow\}.$$

Conforme vimos nos exemplo 3.4.6 e 3.4.11, S é pseudossimétrico e $L(S) = \{2\}$. Note que

$$K = \{a \in \mathbb{Z} \mid 4 - a \notin S\} = \{0,\ 2,\ 3,\ 5,\ \rightarrow\} = S \cup \{2\}.$$

Proposição 3.61: Seja S um semigrupo, $L(S)$ o conjunto dos furos de segundo tipo de S e $T(S) = (S - M) \setminus S$, conforme definido em 3.26. Então $T(S) \subseteq L(S) \cup \{\gamma\}$.

Demonstração. Inicialmente, observe que $\gamma \in T(S)$, pois $\gamma + M \subseteq S$. Seja agora $x \in T(S)$ com $x \neq \gamma$. Suponha que $\gamma - x \in S$. Desse modo, $\gamma - x \in M$, implicando em $x + (\gamma - x) = \gamma \in S$, o que é um absurdo. Logo $\gamma - x \notin S$, ou seja, $x \in L(S)$, mostrando que $T(S) \subseteq L(S) \cup \{\gamma\}$.

□

Corolário 3.62: Seja S um semigrupo pseudossimétrico. Então $tipo(S) = 2$.

Demonstração. Seja S um semigrupo pseudossimétrico. Utilizando a proposição 3.61 e a parte (ii) de 3.59, temos que $T(S) \subseteq \left\{\frac{\gamma}{2}\right\} \cup \{\gamma\}$, ou seja,

$$tipo(S) = card(T(S)) \leq card\left(\left\{\frac{\gamma}{2}\right\} \cup \{\gamma\}\right) = 2.$$

Da proposição 3.54, não podemos ter $tipo(S) = 1$, portanto concluímos que $tipo(S) = 2$.

□

Exemplo 3.4.13: O semigrupo $S = \langle 3,\ 5,\ 7\rangle = \{0,\ 3,\ 5,\ \rightarrow\}$ é pseudossimétrico, como vimos no exemplo 3.4.6. Observe que

$$\begin{aligned} M &= \{3,\ 5,\ \rightarrow\} \\ S - M &= \{0,\ 2,\ \rightarrow\} \\ T &= \{2,\ 4\}, \end{aligned}$$

mostrando que $tipo(S) = 2$.

Semigrupos simétricos são todos os semigrupos de tipo 1 (conforme demonstrado em 3.54), enquanto semigrupos pseudossimétricos são casos particulares de semigrupos de tipo 2. Nem todo semigrupo de tipo 2 é pseudossimétrico, como ilustra o exemplo abaixo:

Exemplo 3.4.14: Seja $S = \langle 3,\ 11,\ 16\rangle = \{0,\ 3,\ 6,\ 9,\ 11,\ 12,\ 14,\ \rightarrow\}$. Então $\gamma(S) = 13$, e como

$$\mathbb{N} \setminus S = \{1,\ 2,\ 4,\ 5,\ 7,\ 8,\ 10,\ 13\},$$

$g(S) = 8$, mostrando que S não é pseudossimétrico, uma vez que $\beta = 14 \neq 15 = 2g - 1$ (tal fato também pode ser facilmente observado no diagrama abaixo). Entretanto,

$$\begin{aligned} M &= \{3,\ 6,\ 9,\ 11,\ 12,\ 14,\ \rightarrow\} \\ S - M &= \{0,\ 3,\ 6,\ 8,\ 9,\ 11,\ \rightarrow\} \\ T(S) &= \{8,\ 13\} \\ tipo(S) &= 2. \end{aligned}$$

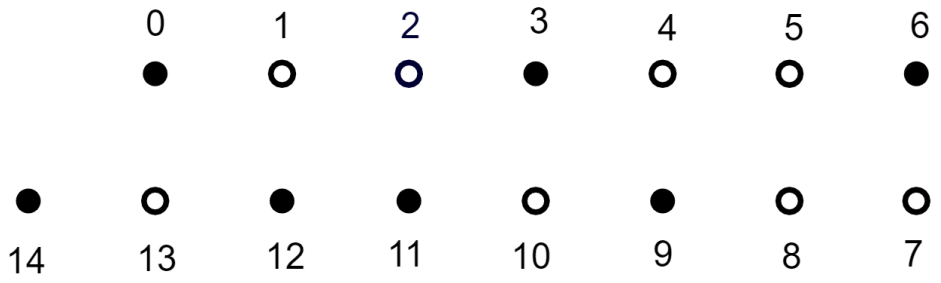

Figura 3.8: Diagrama do semigrupo $S = \langle 3,\ 11,\ 16\rangle$

Observação 3.63: O número de furos positivos de S, isto é, $card(H(S) \cup L(S))$ é dado por

$$card(H(S) \cup L(S)) = \gamma + 1 - n = \sum_{i=1}^{n} t_i(S),$$

e o número de furos de primeiro tipo é dado por

$$card(H(S)) = n = \frac{1}{2}\left(\gamma + 1 - card(L(S))\right).$$

De fato, se $a \in S(i) \setminus S(i-1)$, vamos mostrar que a é um furo de S. Inicialmente, note que $a \notin S$, pois $a \notin S(i-1)$. Logo, a é lacuna e, portanto, furo de S, pois se $\gamma - a \in S$, então $a \in H$, e a é furo de primeiro tipo de S. Se $\gamma - a \notin S$, então $a \in L$, e a é furo de segundo tipo de S.

Se observarmos a cadeia $S(\cdot)$, vemos que na inclusão de $S(i-1)$ em $S(i)$, estamos acrescentando lacunas (furos) de S. Por isso

$$card(H(S) \cup L(S)) = \sum_{i=1}^{n} t_i(S).$$

Note que $\gamma + 1$ é a quantidade de naturais entre 1 e $\gamma + 1 = \beta$. Sabemos que n é a quantidade de elementos de S menores que β. Portanto, $\gamma + 1 - n$ é a quantidade de lacunas (furos) de S, ou seja, $card(H(S) \cup L(S)) = \gamma + 1 - n$.

Como n é a quantidade de elementos de S menores que $\beta = \gamma + 1$, existem n elementos da forma $\gamma - a \in S$, com $a \in \mathbb{N}$, ou seja, existem n elementos em $H(S)$, ou seja, $card(H(S)) = n$.

Como $H(S) \cap L(S) = \emptyset$, temos que $card(H(S)) + card(L(S)) = card(H(S) \cup L(S))$, ou seja, $card(H(S)) + card(L(S)) = \gamma + 1 - n$. Então

$$n = card(H(S)) = \gamma + 1 - n - card(L(S)),$$

implicando em

$$card(H(S)) = n = \frac{1}{2}\left(\gamma + 1 - card(L(S))\right).$$

Proposição 3.64: Sejam S um semigrupo, E ideal relativo de S, e R um semigrupo tal que $S \subseteq R \subseteq \mathbb{N}$. Então:

(i) $card((K - E) \setminus S) = card(K \setminus E)$;

(ii) $card(R \setminus S) \leq card(S \setminus (S - R)) + card(K \setminus S)$, e a igualdade vale se, e somente se, $(K - (S - R)) = R$;

(iii) $card(\mathbb{N} \setminus S) = card(S \setminus (S - \mathbb{N})) + card(K \setminus S)$;

(iv) $tipo(S) = card(K \setminus (K + M))$;

(v) $card(\mathbb{N} \setminus S) \geq card(S \setminus (S - \mathbb{N})) + tipo(S) - 1$, e a igualdade vale se, e somente se, $K + M = M$;

(vi) $tipo(S) \leq card(K \setminus S) + 1$, e a igualdade vale se, e somente se, $K + M = M$.

Demonstração. Para o item (i), temos:

$$\begin{aligned} card((K-E)\setminus S) &= card((K-E)\setminus K) + card(K\setminus S) \\ &= card((K-K)\setminus (K-(K-E))) + card(K\setminus S) \\ &= card(S\setminus E) + card(K\setminus S) \\ &= card(K\setminus E), \end{aligned}$$

aplicando o teorema 3.41 com $E = K - E$ e $F = K$ na passagem da primeira igualdade para a segunda.

Para o item (ii), observe que $R \subseteq R^{**} = (S-(S-R)) \subseteq (K-(S-R))$, cuja última inclusão segue do fato de que $S \subseteq K$, e assim:

$$\begin{aligned} card(R\setminus S) &= card((K-(S-R))\setminus S) - card((K-(S-R))\setminus R) \\ &\leq card((K-(S-R))\setminus S) \\ &= card((K-(S-R)\setminus K) + card(K\setminus S) \\ &= card((K-K)\setminus K-(K-(S-R))) + card(K\setminus S) \\ &= card(S\setminus (S-R)) + card(K\setminus S), \end{aligned}$$

obtida com a aplicação do teorema 3.41 com $E = K-(S-R)$ e $F = K$ na passagem da segunda para a terceira igualdade.

Observe agora que, como $card(R\setminus S) \leq card((K-(S-R))\setminus S)$ e $R \subseteq (K-(S-R))$, a igualdade acontecerá se, e somente se, $R = (K-(S-R))$.

Para o item (iii), aplicaremos o teorema 3.41 com $E = \mathbb{N}$ e $F = K$, e assim:

$$\begin{aligned} card(\mathbb{N}\setminus S) &= card(\mathbb{N}\setminus K) + card(K\setminus S) \\ &= card((K-K)\setminus (K-\mathbb{N})) + card(K\setminus S) \\ &= card(S\setminus (K-\mathbb{N})) + card(K\setminus S) \\ &= card(S\setminus (K-(K+\mathbb{N}))) + card(K\setminus S) \\ &= card(S\setminus ((K-K)-\mathbb{N}))) + card(K\setminus S) \\ &= card(S\setminus (S-\mathbb{N})) + card(K\setminus S). \end{aligned}$$

Para o item (iv), novamente com o uso do teorema 3.41 com $E = K$ e $F = K + M$, temos:

$$\begin{aligned} card(K\setminus (K+M)) &= card((K-(K+M))\setminus (K-K)) \\ &= card((K-K)-M\setminus S) \\ &= card((S-M)\setminus S) \\ &= tipo(S). \end{aligned}$$

Para o item (v), basta observar que, como $M \subseteq K+M$, então $card(K\setminus M) \geq card(K\setminus (K+M))$. Note também que $S\setminus M = \{0\}$, então $card(K\setminus S) = card(K\setminus M)-1$.

Utilizando os itens (iii) e (iv), segue o resultado:

$$\begin{aligned} card(\mathbb{N} \setminus S) &= card(S \setminus (S - \mathbb{N})) + card(K \setminus S) \\ &= card(S \setminus (S - \mathbb{N})) + card(K \setminus M) - 1 \\ &\geq card(S \setminus (S - \mathbb{N})) + card(K \setminus (K + M)) - 1 \\ &= card(S \setminus (S - \mathbb{N})) + tipo(S) - 1. \end{aligned}$$

O item (vi) segue de (iv) e da observação feita em (v):

$$\begin{aligned} tipo(S) &= card(K \setminus (K + M)) \\ &\leq card(K \setminus M) \\ &= card(K \setminus S) + 1. \end{aligned}$$

□

Exemplo 3.4.15: Sejam $S = \langle 6,\ 7,\ 8,\ 11\rangle = \{0,\ 6,\ 7,\ 8,\ 11,\ \rightarrow\}$, $R = \langle 3,\ 5,\ 7\rangle = \{0,\ 3,\ 5,\ \rightarrow\}$, $K = \{0,\ 1,\ 5,\ 6,\ 7,\ 8,\ 9,\ 11\ \rightarrow\}$ e $E = \{-1,\ 5,\ 6,\ 7,\ 10\ \rightarrow\}$. Temos:

$$\begin{aligned} K - E &= \{1,\ 2,\ 6,\ 7,\ 8,\ 9,\ 10,\ 12,\ \rightarrow\}, \\ (K - E) \setminus S &= \{1,\ 2,\ 9,\ 10\}, \\ K \setminus E &= \{0,\ 1,\ 8,\ 9\}, \end{aligned}$$

e assim $card((K - E) \setminus S) = 4 = card(K \setminus E)$.

Observe também que

$$\begin{aligned} R \setminus S &= \{3,\ 5,\ 9,\ 10\}, \\ S - R &= \{\ 8,\ 11,\ \rightarrow\}, \\ S \setminus (S - R) &= \{0,\ 6,\ 7\}, \\ K \setminus S &= \{1,\ 5,\ 9\}. \end{aligned}$$

Desse modo, $card(R \setminus S) = 4 \leq 3 + 3 = card(S \setminus (S - R)) + card(K \setminus S)$.

Note ainda que

$$\begin{aligned} \mathbb{N} \setminus S &= \{1,\ 2,\ 3,\ 4,\ 5,\ 9,\ 10\}, \\ S - \mathbb{N} &= \{11,\ \rightarrow\}, \\ S \setminus (S - \mathbb{N}) &= \{0,\ 6,\ 7,\ 8\}, \end{aligned}$$

mostrando que $card(\mathbb{N} \setminus S) = 7 = 4 + 3 = card(S \setminus (S - \mathbb{N})) + card(K \setminus S)$.

Por fim,

$$\begin{aligned} M &= \{6,\ 7,\ 8,\ 11,\ \rightarrow\}, \\ S - M &= \{0,\ 5,\ \rightarrow\}, \\ (S - M) \setminus S &= \{5,\ 9,\ 10\}, \\ K + M &= \{6,\ 7,\ 8,\ 9,\ 11,\ \rightarrow\}, \\ K \setminus (K + M) &= \{0,\ 1,\ 5\}, \end{aligned}$$

e então

$$\begin{aligned} tipo(S) &= 3 = card(K \setminus (K + M)), \\ card(\mathbb{N} \setminus S) &= 7 \geq 4 + 3 - 1 = card(S \setminus (S - \mathbb{N})) + tipo(S) - 1, \\ tipo(S) &= 3 \leq 3 + 1 = card(K \setminus S) + 1. \end{aligned}$$

Definição 3.65: Sejam S um semigrupo, $L(S)$ o conjunto dos furos de segundo tipo de S e $T(S) = (S - M) \setminus S$. S é dito **quase simétrico** se $L(S) \subseteq T(S)$.

Exemplo 3.4.16: Seja $S = \langle 6,\ 7,\ 8,\ 10,\ 11\rangle = \{0,\ 6,\ 7,\ 8,\ 10,\ \rightarrow\}$. Temos

$$\begin{aligned} M &= \{6,\ 7,\ 8,\ 10,\ \rightarrow\} \\ S - M &= \{0,\ 4,\ \rightarrow\} \\ T(S) &= \{4,\ 5,\ 9\} \\ L(S) &= \{4,\ 5\}. \end{aligned}$$

Como $L(S) \subseteq T(S)$, então S é quase simétrico.

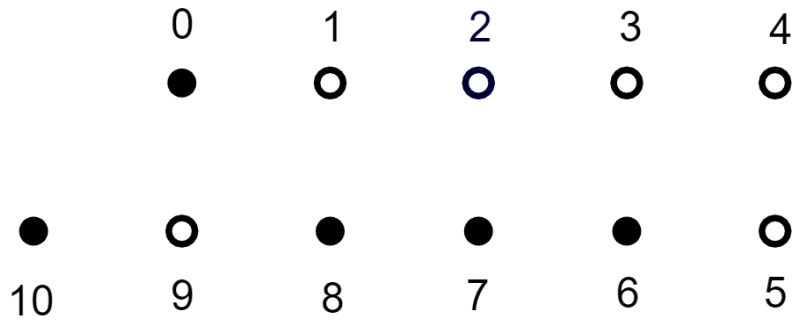

Figura 3.9: Diagrama do semigrupo $S = \langle 6,\ 7,\ 8,\ 10,\ 11\rangle$

Proposição 3.66: As seguintes proposições são equivalentes:

(i) S é quase simétrico;

(ii) $T(S) = L(S) \cup \{\gamma\}$;

(iii) $M = K + M$.

Demonstração. Suponha, inicialmente, S quase simétrico, ou seja, $L(S) \subseteq T(S)$. Como $\gamma \in T(S)$, então $L(S) \cup \{\gamma\} \subseteq T(S)$. Da proposição 3.61, concluímos que (i) $\implies$ (ii). A implicação (ii) $\implies$ (i) é trivial.

Agora, do fato de $M \subseteq K + M$, sabemos que $M = K + M \iff K + M \subseteq M$. Note que $K + M \subseteq M \iff K \subseteq S \cup T$.

De fato, suponha que $K + M \subseteq M$ e seja $a \in K$. Então $a \in S$ ou $a \notin S$. No segundo caso, temos que $a \in T = (S - M) \setminus S$, pois $a + M \subseteq M \subset S$. Portanto, $K \subseteq S \cup T$.

Reciprocamente, suponha que $K \subseteq S \cup T$ e tome $a \in K$. Se $a \in S$, então $a + M \subseteq S + M \subseteq M$. Se $a \in T$, então $a \notin S$ e $a \in S - M$, ou seja, $a + M \subseteq S$. Sabemos que a é natural, portanto $a + M \subseteq M$, e assim $K + M \subseteq M$.

Como $K = S \cup L$, temos $M = K + M \iff S \cup L \subseteq S \cup T \iff L \subseteq T \iff S$ é quase simétrico, mostrando que (iii) $\iff$ (i). □

Corolário 3.67: Pela proposição 3.66, um semigrupo S é quase simétrico se, e somente se, $M = K + M$ e, de acordo com a proposição 3.64 itens (v) e (vi), temos as seguintes equivalências:

(i) S é quase simétrico;

(ii) $card(\mathbb{N} \setminus S) = card(S \setminus (S - \mathbb{N})) + tipo(S) - 1$;

(iii) $tipo(S) = card(K \setminus S) + 1$.

Novamente pela proposição 3.66 temos que S é quase simétrico se, e somente se, $T(S) = L(S) \cup \{\gamma\}$, ou seja, $(S - M) \setminus S = (K \setminus S) \cup \{\gamma\}$.

Exemplo 3.4.17: Seja $S = \langle 6,\ 7,\ 8,\ 10,\ 11\rangle = \{0,\ 6,\ 7,\ 8,\ 10,\ \rightarrow\}$. Do exemplo 3.4.16, sabemos que S é quase simétrico e que $T(S) = L(S) \cup \{\gamma\}$. Note ainda que $tipo(S) = 3 = card(K \setminus S) + 1$, uma vez que $K \setminus S = L(S)$. Também temos que

$$\begin{aligned} K &= \{0,\ 4,\ 5,\ 6,\ 7,\ 8,\ 10,\ \rightarrow\},\\ K + M &= \{\ 6,\ 7,\ 8,\ 10,\ \rightarrow\} = M,\\ \mathbb{N} \setminus S &= \{1,\ 2,\ 3,\ 4,\ 5,\ 9\},\\ S - \mathbb{N} &= \{10,\ \rightarrow\},\\ S \setminus (S - \mathbb{N}) &= \{0,\ 6,\ 7,\ 8\}, \end{aligned}$$

mostrando que $card(\mathbb{N} \setminus S) = 6 = 4 + 3 - 1 = card(S \setminus (S - \mathbb{N})) + tipo(S) - 1$.

Proposição 3.68: Seja S um semigrupo.

(i) Se S é simétrico, então S também é quase simétrico;

(ii) Se S é pseudossimétrico, então S também é quase simétrico.

Demonstração. Se S é simétrico, então $L(S) = \emptyset$. Logo, $L(S) \subseteq T(S)$ e, portanto, S é quase simétrico.

Agora, se S é pseudossimétrico, pela proposição 3.59 e pelo corolário 3.62, $K \setminus S = L(S) = \left\{\frac{\gamma}{2}\right\}$ e $tipo(S) = 2$. Desse modo, $tipo(S) = 2 = card(K \setminus S) + 1$, satisfazendo o item (iii) do corolário 3.67, o que nos permite concluir que S é quase simétrico.

□

Proposição 3.69: Seja S um semigrupo quase simétrico e R um semigrupo que contenha S propriamente. São equivalentes:

(i) R é ideal bidual;

(ii) $L(S) \subseteq R$;

(iii) $card(R \setminus S) = card(S \setminus (S - R)) + card(L(S))$.

Demonstração. Considere R bidual. Como $S - R \subseteq M$ e S é quase simétrico, então

$$L(S) \subseteq T(S) \subseteq S - M \subseteq S - (S - R) = R^{**} = R,$$

mostrando que (i) $\implies$ (ii).

A implicação (ii) $\implies$ (iii) é verdadeira mesmo sem a hipótese de que S é quase simétrico: basta lembrar que $L(S) = K \setminus S$ e aplicar o teorema 3.41 com $E = R$ e $F = K$ na passagem da primeira igualdade para a segunda. Temos então:

$$\begin{aligned} card(R \setminus S) &= card(R \setminus K) + card(K \setminus S) \\ &= card((K - K) \setminus (K - R)) + card(K \setminus S) \\ &= card(S \setminus (K - (K + R))) + card(K \setminus S) \\ &= card((S \setminus ((K - K) - R))) + card(K \setminus S) \\ &= card(S \setminus (S - R)) + card(L(S)). \end{aligned}$$

Para mostrar que (iii) $\implies$ (i), suponha que R não seja bidual. Então $R^{**} = S - (S - R)$ contém R estritamente. Como $S - R = S - R^{**}$, aplicando o item (ii) da proposição 3.64, temos

$$\begin{aligned} card(R \setminus S) &< card(R^{**} \setminus S) \\ &\leq card(S \setminus (S - R)) + card(L(S)), \end{aligned}$$

o que é um absurdo. Portanto, R deve ser bidual.

□

Exemplo 3.4.18: Sejam o semigrupo $S = \langle 6,\ 7,\ 8,\ 10,\ 11\rangle = \{0,\ 6,\ 7,\ 8,\ 10,\ \rightarrow\}$ e o ideal $R = \{0,\ 4,\ \rightarrow\}$. Do exemplo 3.4.16, sabemos que S é quase simétrico e que $L(S) = \{4,\ 5\}$. Note que $L(S) \subseteq R$. R é ideal bidual, pois

$$\begin{aligned} R^* &= S - R = \{6,\ 7,\ 8,\ 10,\ \rightarrow\}, \\ R^{**} &= S - (S - R) = \{0,\ 4,\ \rightarrow\} = R. \end{aligned}$$

Por fim, temos

$$R \setminus S = \{4,\ 5,\ 9\},$$
$$S \setminus (S - R) = \{0\},$$

mostrando que $card(R \setminus S) = 3 = 1 + 2 = card(S \setminus (S - R)) + card(L(S))$.

Proposição 3.70: Seja S um semigrupo com número de Fröbenius γ e R um semigrupo que contenha S propriamente. Então:

(i) Se todo $a \in R \setminus S$ é um furo de primeiro tipo de S, ou seja, se $R \setminus S \subseteq H(S)$, então $a \in R \setminus S$ se, e somente se, $\gamma - a \in S \setminus (S - R)$. Portanto, $card(R \setminus S) = card(S \setminus (S - R))$.

(ii) Se todo furo de segundo tipo de S pertence a R, ou seja, se $L(S) \subseteq R$, então $a \in R \setminus S$ se, e somente se, $\gamma - a \in S \setminus (S - R)$ ou $a \in L(S)$. Portanto, $card(R \setminus S) = card(S \setminus (S - R)) + card(L(S))$.

Demonstração. Para a parte (i), suponha que $a \in R \setminus S \subseteq H(S)$. Então $\gamma - a \in S$, pois a é furo de primeiro tipo de S. Como $a \in R$ e $(\gamma - a) + a = \gamma \notin S$, então $\gamma - a \notin (S - R)$. Logo, se $a \in R \setminus S$, temos $\gamma - a \in S \setminus (S - R)$.

Reciprocamente, seja $a \in S \setminus (S - R)$. Vamos mostrar que $\gamma - a \in R \setminus S$. Como $a \in S$, então $\gamma - a \notin S$, pois caso contrário teríamos $a + \gamma - a = \gamma \in S$. Como $a \notin S - R$, existe $r \in R$ tal que $a + r \notin S$. Como $a \in S \subset R$, então $a + r \in R \setminus S \subseteq H(S)$, ou seja $a + r$ é furo de primeiro tipo. Logo, $\gamma - (a + r) \in S$, e então $\gamma - a = (\gamma - a - r) + r \in R \setminus S$.

Para a parte (ii), suponha que $a \in R \setminus S$. Se $a \in H(S)$, então $\gamma - a \in S \setminus (S - R)$, conforme mostrado acima. Caso contrário, $a \in L(S)$.

Reciprocamente, seja $a \in S \setminus (S - R)$. Vamos mostrar que $\gamma - a \in R \setminus S$. Como $\gamma - a \notin S$ e $a \notin S - R$, existe $r \in R$ tal que $a + r \notin S$. Se $a + r \in H(S)$, então $\gamma - (a + r) \in S$, e assim $\gamma - a = (\gamma - a - r) + r \in R \setminus S$. Se $a + r \in L(S)$, então $\gamma - (a + r) \notin S$, e assim $\gamma - (a + r) \in L(S) \subseteq R$. Portanto, $\gamma - a = (\gamma - a - r) + r \in R \setminus S$. □

Corolário 3.71: Seja S um semigrupo com número de Fröbenius γ e R um semigrupo que contenha S propriamente. Então:

(i) Se S é simétrico, então $a \in R \setminus S$ se, e somente se, $\gamma - a \in S \setminus (S - R)$. Portanto, $card(R \setminus S) = card(S \setminus (S - R))$.

(ii) Se S é pseudossimétrico, então $a \in R \setminus S$ se, e somente se, $\gamma - a \in S \setminus (S - R)$ ou $a = \frac{\gamma}{2}$. Portanto, $card(R \setminus S) = card(S \setminus (S - R))$, se $\frac{\gamma}{2} \notin R$, e $card(R \setminus S) = card(S \setminus (S - R)) + 1$, se $\frac{\gamma}{2} \in R$.

Demonstração. Para (i), se S é simétrico, a proposição 3.59 nos garante que $L(S) = \emptyset$. Portanto, $R \setminus S \subseteq H(S)$, e o resultado segue aplicando o item (i) da proposição 3.70.

Para (ii), se S é pseudossimétrico, a proposição 3.59 nos garante que $L(S) = \left\{\frac{\gamma}{2}\right\}$. Se $\frac{\gamma}{2} \in R$, o resultado segue aplicando o item (ii) da proposição 3.70. Agora, se $\frac{\gamma}{2} \notin R$, o resultado segue aplicando o item (i).

□

Exemplo 3.4.19: Sejam $S = \langle 4,\ 6,\ 11\rangle = \{0,\ 4,\ 6,\ 8,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\}$ e $R = \{0,\ 4,\ \rightarrow\}$. Sabemos do exemplo 3.4.3 que S é simétrico. Temos:

$$\begin{aligned} R \setminus S &= \{5,\ 7,\ 9,\ 13\}, \\ S - R &= \{10,\ 11,\ 12,\ 14,\ \rightarrow\}, \\ S \setminus (S - R) &= \{0,\ 4,\ 6,\ 8\}. \end{aligned}$$

Observe que $a \in R \setminus S$ se, e somente se, $13 - a \in S \setminus (S - R)$. De fato, $card(R \setminus S) = card(S \setminus (S - R))$.

Exemplo 3.4.20: Sejam $S = \langle 4,\ 7,\ 9\rangle = \{0,\ 4,\ 7,\ 8,\ 9,\ 11,\ \rightarrow\}$ e $R = \{0,\ 4,\ \rightarrow\}$. Sabemos do exemplo 3.4.7 que S é pseudossimétrico, Temos:

$$\begin{aligned} R \setminus S &= \{5,\ 6,\ 10\}, \\ S - R &= \{7,\ 8,\ 9,\ 11,\ \rightarrow\}, \\ S \setminus (S - R) &= \{0,\ 4\}. \end{aligned}$$

Observe que $a \in R \setminus S$, com $a \neq 5$, se, e somente se, $10 - a \in S \setminus (S - R)$, ou então se $a = 5$. Como $5 \in R$, segue que $card(R \setminus S) = 3 = card(S \setminus (S - R)) + 1$.

Teorema 3.72: Um semigrupo S é quase simétrico se, e somente se, sua sequência tipo é $(t,\ 1,\ 1, \ldots,\ 1)$, para algum $t > 0$.

Demonstração. Seja S um semigrupo quase simétrico. Então $L \subseteq T = (S - M) \setminus S$. Como $S - M = M - M$, segue que $L \subseteq (M - M) \setminus S$. Visto que

$$S = S(0) \subseteq S(1) = M - M \subseteq S(2) \subseteq \ldots \subseteq S(n) = \mathbb{N},$$

concluímos que $L \subseteq S(i) = S_i - S_i$, para todo $1 \leq i \leq n$.

Observe que S_i é bidual. De fato, suponha que exista $x \in S_i^{**} \setminus S_i$. Dado $s \in S_i$, se $x - s \in S$, então $x - s + s = x \in S_i$, o que é uma contradição. Logo, $x - s \notin S$. Agora, se $x - s \in L \subseteq S(i) = S_i - S_i$, novamente teríamos $x - s + s = x \in S_i$. Portanto $x - s \in H$ e, desse modo, $\gamma - (x - s) = \gamma - x + s \in S$ para todo $s \in S_i$, o que implica em $\gamma - x \in S - S_i$. Como $\gamma - (\gamma - x) = x \in S_i^{**} = S - (S - S_i)$, temos que $x + \gamma - x = \gamma \in S$, o que é um absurdo. Logo, não pode existir tal $x \in S_i^{**} \setminus S$, mostrando que S_i é bidual. Portanto, $S_i = S - (S - S_i)$, ou seja, $S - S(i) = S_i$.

Sabendo que $card(S \setminus S_i) = i$, e utilizando a proposição 3.69 ora com $R = S(i)$, ora

com $R = S(i-1)$, temos

$$\begin{aligned} t_i(S) &= card(S(i) \setminus S(i-1)) \\ &= card(S(i) \setminus S) - card(S(i-1) \setminus S) \\ &= card(S \setminus (S - S(i))) + card(L) - (card(S \setminus (S - S(i-1)) + card(L))) \\ &= i + card(L) - (i - 1 + card(L)) \\ &= 1, \end{aligned}$$

para todo $2 \leq i \leq n$. Portanto, a sequência tipo de S é $(t,\ 1,\ 1, \ldots,\ 1)$, para algum $t > 0$.

Reciprocamente, se $(t,\ 1,\ 1, \ldots,\ 1)$ é a sequência tipo de S, então a quantidade de furos positivos de S, conforme a observação 3.63, é dada por

$$\gamma + 1 - n = \sum_{i=1}^{n} t_i = t + (n-1),$$

e assim temos que

$$n = \frac{1}{2}(\gamma - t + 2).$$

Utilizando esta última igualdade e novamente a observação 3.63, segue que

$$\frac{1}{2}(\gamma - t + 2) = n = card(H(S)) = \frac{1}{2}(\gamma + 1 - card(L(S)),$$

o que implica em $t = card(L(S))+1$. Como $t = card(T)$ e sempre temos que $T \subseteq L \cup \{\gamma\}$, concluímos que $T = L \cup \{\gamma\}$, mostrando que S é quase simétrico.

□

Exemplo 3.4.21: Seja $S = \langle 4,\ 10,\ 11,\ 17\rangle = \{0,\ 4,\ 8,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\}$. Observe que $\gamma(S) = 13$. Temos:

$$\begin{aligned} M &= \{4,\ 8,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\}, \\ S - M &= \{0,\ 4,\ 6,\ 7,\ 8,\ 10,\ \rightarrow\}, \\ T &= \{6,\ 7,\ 13\}, \text{ e assim } tipo(S) = 3, \\ H &= \{1,\ 2,\ 3,\ 5,\ 9,\ 13\}, \\ L &= \{6,\ 7\}, \\ K &= \{0,\ 4,\ 6,\ 7,\ 8,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\}. \end{aligned}$$

Como $L(S) \subseteq T(S)$, então S é quase simétrico.

Note que a proposição 3.66 também é satisfeita, pois $T = L \cup \{\gamma\}$ e $M = K + M$.

Temos ainda que:

$$\begin{aligned} \mathbb{N} \setminus S &= \{1,\ 2,\ 3,\ 5,\ 6,\ 7,\ 9,\ 13\}, \\ card(\mathbb{N} \setminus S) &= 8, \\ S - \mathbb{N} &= \{14,\ \rightarrow\}, \\ card(S \setminus (S - \mathbb{N})) &= 6, \\ tipo(S) &= card(T) = 3, \\ card(K \setminus S) &= card(L) = 2, \end{aligned}$$

satisfazendo as equivalências da observação 3.67.

Por fim, observe também que

$S_0 = S$	$S(0) = S$	
$S_1 = M$	$S(1) = \{0,\ 4,\ 6,\ 7,\ 8,\ 10,\ \rightarrow\}$	$t_1 = 3$
$S_2 = \{8,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\}$	$S(2) = \{0,\ 4,\ 6,\ \rightarrow\}$	$t_2 = 1$
$S_3 = \{10,\ 11,\ 12,\ 14,\ \rightarrow\}$	$S(3) = \{0,\ 4,\ \rightarrow\}$	$t_3 = 1$
$S_4 = \{11,\ 12,\ 14,\ \rightarrow\}$	$S(4) = \{0,\ 3,\ \rightarrow\}$	$t_4 = 1$
$S_5 = \{12,\ 14,\ \rightarrow\}$	$S(5) = \{0,\ 2,\ \rightarrow\}$	$t_5 = 1$
$S_6 = \{14,\ \rightarrow\}$	$S(6) = \mathbb{N}$	$t_6 = 1$

e a sequência tipo de S é $(3,\ 1,\ 1,\ 1,\ 1,\ 1)$, satisfazendo o teorema 3.72.

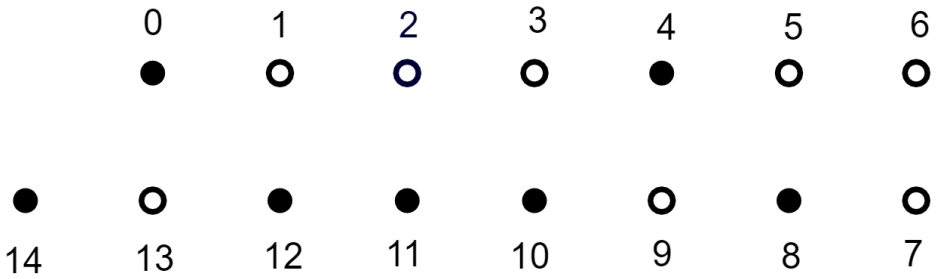

Figura 3.10: Diagrama do semigrupo $S = \langle 4,\ 10,\ 11,\ 17 \rangle$

Corolário 3.73: Seja S um semigrupo.

(i) S é simétrico se, e somente se, sua sequência tipo é $(1,\ 1, \ldots,\ 1)$;

(ii) Se S é pseudossimétrico, então sua sequência tipo é $(2,\ 1,\ 1, \ldots,\ 1)$.

Demonstração. Para (i), se S é simétrico, da proposição 3.68 sabemos que S é quase simétrico. Logo, de acordo com o teorema 3.72, a sequência tipo de S é $(t,\ 1,\ 1,\ \ldots,\ 1)$, com $t = t_1 = tipo(S)$. A proposição 3.54 nos diz que $tipo(S) = 1$, e assim segue o resultado.

Reciprocamente, se a sequência tipo de S é $(1,\ 1, \ldots,\ 1)$, do teorema 3.72 temos que S é quase simétrico. Como $tipo(S) = t_1 = 1$, concluímos que S é simétrico.

Para a parte (ii), se S é pseudossimétrico, o corolário 3.62 e a proposição 3.68 nos garantem que $tipo(S) = 2$ e que S é quase simétrico. Do teorema 3.72, temos que

a sequência tipo de S é $(t,\ 1,\ 1,\ \ldots,\ 1)$, com $t = t_1 = tipo(S) = 2$, donde segue o resultado.

□

Exemplo 3.4.22: Seja $S = \langle 3,\ 5\rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$. Sabemos do exemplo 3.4.1 que S é simétrico. Temos:

$S_0 = S$	$S(0) = S$	
$S_1 = \{3,\ 5,\ 6,\ 8,\ \rightarrow\} = M$	$S(1) = \{0,\ 3,\ 5,\ \rightarrow\}$	$t_1 = 1$
$S_2 = \{5,\ 6,\ 8,\ \rightarrow\}$	$S(2) = \{0,\ 3,\ \rightarrow\}$	$t_2 = 1$
$S_3 = \{6,\ 8,\ \rightarrow\}$	$S(3) = \{0,\ 2,\ \rightarrow\}$	$t_3 = 1$
$S_4 = \{8,\ \rightarrow\}$	$S(4) = \mathbb{N}$	$t_4 = 1$

A sequência tipo de S é $(1,\ 1,\ 1,\ 1)$.

Exemplo 3.4.23: Seja $S = \langle 4,\ 7,\ 9\rangle = \{0,\ 4,\ 7,\ 8,\ 9,\ 11,\ \rightarrow\}$. Sabemos do exemplo 3.4.7 que S é pseudossimétrico. Temos:

$S_0 = S$	$S(0) = S$	
$S_1 = \{4,\ 7,\ 8,\ 9,\ 11,\ \rightarrow\} = M$	$S(1) = \{0,\ 4,\ 5,\ 7,\ \rightarrow\}$	$t_1 = 2$
$S_2 = \{7,\ 8,\ 9,\ 11,\ \rightarrow\}$	$S(2) = \{0,\ 4,\ \rightarrow\}$	$t_2 = 1$
$S_3 = \{8,\ 9,\ 11,\ \rightarrow\}$	$S(3) = \{0,\ 3,\ \rightarrow\}$	$t_3 = 1$
$S_4 = \{9,\ 11,\ \rightarrow\}$	$S(4) = \{0,\ 2,\ \rightarrow\}$	$t_4 = 1$
$S_5 = \{11,\ \rightarrow\}$	$S(5) = \mathbb{N}$	$t_5 = 1$

A sequência tipo de S é $(2,\ 1,\ 1,\ 1)$.

4

Semigrupos Numéricos Modulares

Neste capítulo iremos abordar uma outra família de semigrupos numéricos: os semigrupos numéricos modulares. Vamos definir mais um invariante, o peso de um semigrupo, e analisaremos aqueles semigrupos modulares cujo módulo é mínimo com respeito ao seu peso. Apresentaremos também um algoritmo que permite determinar se um semigrupo S é modular ou não e definiremos os chamados UESY-semigrupos. Os semigrupos numéricos modulares estão associados às inequações diofantinas modulares, que serão definidas neste capítulo. Os principais resultados aqui apresentados podem ser encontrados em [3], [15] e [16].

4.1 Semigrupos numéricos e inequações diofantinas modulares

Definição 4.1: Uma **inequação diofantina modular** é uma expressão na forma

$$ax \mod b \leq x,$$

com a e b inteiros não negativos e $b \neq 0$.

Recordemos que, dados a e b inteiros não negativos, com b diferente de zero, $a \mod b$ denota o resto da divisão euclidiana de a por b. Ao resolvermos uma inequação diofantina modular, estamos buscando aqueles inteiros x que, quando multiplicados por a, deixam resto menor ou igual a x na divisão por b. Como os possíveis restos dessa divisão são $0,\ 1, \ldots,\ b-1$, as soluções de uma inequação diofantina modular $ax \mod b \leq x$ são números inteiros não negativos.

Exemplo 4.1.1: Considere a inequação diofantina modular $2x \mod 4 \leq x$. Note que 2 é uma solução desta inequação, pois $4 \mod 4 \leq 2$. É fácil perceber que qualquer inteiro maior ou igual a 2 será também solução. Desse modo, a solução da inequação é o semigrupo $S = \{0,\ 2,\ \rightarrow\}$.

Exemplo 4.1.2: Considere a inequação diofantina modular $3x \mod 5 \leq x$. Note que 2 é solução, pois $6 \mod 5 \leq 2$, mas 3 não o é, pois $9 \mod 5 \leq 3$ é falso. Temos $3.4 \mod 5 = 2 \leq 4$ e 4 é solução de $3x \mod 5 \leq x$.

Os possíveis valores de um inteiro módulo 5 são 0, 1, 2, 3 e 4. Assim, todo inteiro maior que 4 é solução de $3x \mod 5 \leq x$. Portanto, o conjunto solução dessa inequação diofantina modular é o semigrupo $S = \{0,\ 2,\ 4,\ \rightarrow\}$.

Proposição 4.2: O conjunto das soluções inteiras de uma inequação diofantina modular é um semigrupo numérico.

Demonstração. Sejam a e b inteiros não negativos, com b diferente de zero, e $S = \{x \in \mathbb{N} \mid ax \mod b \leq x\}$ o conjunto das soluções inteiras da inequação diofantina modular $ax \mod b \leq x$. Naturalmente, $0 \in S$. Sejam $x,\ y \in S$. Então

$$a(x+y) \mod b = (ax+ay) \mod b \leq (ax \mod b) + (ay \mod b) \leq x+y,$$

mostrando que $x+y \in S$ e, portanto, S é fechado para soma. Por fim, note que se $x \geq b$, então $x \in S$, logo $\mathbb{N} \setminus S$ é finito.

□

Definição 4.3: Dados a e b inteiros com $b \neq 0$, denotamos o semigrupo solução da inequação diofantina modular $ax \mod b \leq x$, $S = \{x \in \mathbb{N} \mid ax \mod b \leq x\}$, por $S(a,b)$, em que a e b são denominados, respectivamente, **fator** e **módulo** do semigrupo.

Exemplo 4.1.3: Na inequação $3x \mod 5 \leq x$ do exemplo 4.1.2, 3 é o fator e 5 é o módulo do semigrupo $S = \langle 2,\ 5\rangle$, que também pode ser denotado por $S(3,5)$.

Definição 4.4: Um **semigrupo numérico modular**, ou simplesmente, semigrupo modular, é um semigrupo S para o qual existem a e b inteiros, com $b \neq 0$, tais que $S = S(a,b)$. Neste caso, dizemos que $S(a,b)$ é uma **representação modular** para S.

A inequação $ax \mod b \leq x$ tem as mesmas soluções que $(a \mod b)x \mod b \leq x$. De fato, suponha que $a \mod b = r$. Então existe $q \in \mathbb{Z}$ tal que $a = bq + r$. Logo, $ax \mod b = (bq+r)x \mod b = (bqx \mod b) + (rx \mod b) = 0 + rx \mod b = (a \mod b)x \mod b$. Pela unicidade do quociente e do resto na divisão euclidiana, temos também que $ax \mod b = ax \mod (-b)$ e, se $a \in \{0,\ 1\}$, então $S(a,b) = \mathbb{N}$ para qualquer módulo $b \neq 0$. Desse modo, podemos supor $2 \leq a < b$. O exemplo abaixo mostra que a representação modular de um semigrupo modular não é necessariamente única.

Exemplo 4.1.4: $S = \{0,\ 2,\ \rightarrow\} = S(2,3) = S(2,4)$. Note que este semigrupo é solução da inequação $2x \mod 4 \leq x$, apresentada no exemplo 4.1.1.

Os resultados seguintes nos ajudarão a encontrar a solução de uma inequação diofantina modular.

Lema 4.5: Sejam a e b inteiros tais que $0 \leq a < b$. Então $ax \mod b \leq x$ se, e somente se, $(b+1-a)x \mod b \leq x$, ou seja, $S(a,b) = S(b-a+1,b)$.

Demonstração. Se $ax \mod b \leq x$, então existem $q,\ r \in \mathbb{N}$ tais que $ax = qb + r$, com $0 \leq r \leq x$. Temos

$$(b+1-a)x = bx + x - ax = bx + x - qb - r = (x-q)b + x - r,$$

e assim $(b+1-a)x \mod b \leq x-r \leq x$.

Reciprocamente, se $(b+1-a)x \mod b \leq x$, considere $a' = b+1-a$. Então $a'x \mod b \leq x$ e, pelo que acabamos de mostrar acima, segue que $(b+1-a')x \mod b \leq x$, donde segue o resultado, pois $b+1-a' = b+1-(b+1-a) = a$.

□

Exemplo 4.1.5: Note que as inequações $7x \mod 8 \leq x$ e $2x \mod 8 \leq x$ admitem o semigrupo $S = \{0,\ 4,\ \rightarrow\}$ como solução. Desse modo, $S(7,8) = S(2,8)$.

Lema 4.6: Seja S um semigrupo modular com módulo $b \geq 2$. Então existe um inteiro positivo a tal que

$$a \leq \frac{b+1}{2} \quad \text{e} \quad S = S(a,b).$$

Demonstração. Por hipótese, existem a e b inteiros com $0 \leq a < b$ tais que $S = S(a,b)$. Do lema 4.5, temos também que $S = (b+1-a,b)$. Suponha que ambos a e $b+1-a$ sejam maiores que $\frac{b+1}{2}$. Mas então

$$a > \frac{b+1}{2} \implies 2a > b+1,$$

e

$$b+1-a > \frac{b+1}{2} \implies 2b+2-2a > b+1 \implies b+1 > 2a,$$

o que é um absurdo. Portanto, devemos ter a ou $b+1-a$ menor ou igual a $\frac{b+1}{2}$, e o resultado segue.

□

Lema 4.7: Sejam a e b inteiros tais que $0 \leq a < b$ e seja $x \in \mathbb{N}$. Então

$$a(b-x) \mod b = \begin{cases} 0, & \text{se } ax \mod b = 0 \\ b - (ax \mod b), & \text{se } ax \mod b \neq 0, \end{cases}$$

e se $ax \mod b > x$, então $a(b-x) \mod b < b-x$.

Demonstração. Se $ax \mod b = 0$, então existe $q \in \mathbb{Z}$ tal que $ax = qb$. Desse modo,

$$a(b-x) \mod b = ab - ax \mod b = ab - qb \mod b = 0.$$

Se $ax \mod b = r$, com $0 < r < b$, então $b \mid ax - r$. Portanto,

$$b \mid (ab - b - (ax - r)) \text{ e } ab - b - (ax - r) = ab - ax - b + r = a(b-x) - (b-r),$$

mostrando que $a(b-x) \mod b = b - (ax \mod b)$.

Por fim, se $ax \mod b > x$, então

$$a(b-x) \mod b = b - (ax \mod b) < b - x.$$

□

Como consequência do lema acima, temos o seguinte corolário:

Corolário 4.8: Seja o semigrupo $S = S(a,b)$. Se $x \in \mathbb{N} \setminus S$, então $b - x \in S$.

Demonstração. Se $x \in \mathbb{N} \setminus S$, então $ax \mod b > x$. Aplicando o lema anterior, segue que $a(b-x) \mod b < b - x$ e, portanto, $b - x \in S$.

□

Para encontrarmos o semigrupo S solução da inequação $ax \mod b \leq x$, conhecer $\gamma(S)$ é essencial. A proposição abaixo nos dá uma pista do seu valor:

Proposição 4.9: Suponha que $S = S(a,b)$ para a e b inteiros positivos. Se $S \neq \mathbb{N}$, então $\gamma(S) \leq b - 2$.

Demonstração. Inicialmente, note que se $x \geq b$, então $x \in S$, pois $ax \mod b < x$. Suponha que $b - 1 \in \mathbb{N} \setminus S$. Pelo corolário 4.8 temos que $b - (b-1) = 1 \in S$, o que é um absurdo, uma vez que $S \neq \mathbb{N}$. Desse modo, $b - 1 \in S$ e, portanto, $\gamma(s) \leq b - 2$.

□

Exemplo 4.1.6: Considere a inequação modular $7x \mod 8 \leq x$. Pela proposição 4.9, $S(7,8)$ tem número de Fröbenius $\gamma(S) \leq 6$.

Note que se $x \geq 8$, $x \in S = S(7,8)$. Agora, por uma simples conferência, temos que $4,\ 5,\ 6,\ 7 \in S$, e assim $S = \langle 4,\ 5,\ 6,\ 7\rangle = \{0,\ 4,\ \rightarrow\}$ e $\gamma(S) = 3$.

Exemplo 4.1.7: Dado $S = S(4,7)$, vamos encontrar $\gamma(S)$.

Temos que $x \in S$ se, e somente se, $4x \mod 7 \leq x$. Pela proposição 4.9, $\gamma(S) \leq 5$. Neste exemplo, é fácil ver que $S = \{0,\ 2,\ 4,\ 6,\ \rightarrow\}$ e $\gamma(S) = 5$.

Vamos estudar o caso em que $\gamma(S) = b - 2$, no qual $S = S(a,b)$.

Lema 4.10: Dados a e b inteiros com $2 \leq a < b$, seja $S = S(a,b) \neq \mathbb{N}$. Então $\gamma(S) = b - 2$ se, e somente se, $S = \left(\frac{b+1}{2}, b\right)$, com b ímpar. Além disto, $S = \langle 2,\ b\rangle$.

Demonstração. Se $\gamma(S) = b - 2$, então pelo corolário 4.8 temos que $b - (b-2) = 2 \in S$. Se b fosse par, então $\gamma(S) = b - 2$ também o seria, pertencendo assim a S, o que é um absurdo. Portanto, b é ímpar e $S = \langle 2,\ b\rangle$. Como $2 \in S$, temos que $2a \mod b \leq 2$. Note que $2a \neq b$, pois b é ímpar e, se tivéssemos $2a < b$, então $2a \mod b = 2a \leq 2$, ou seja, $a \leq 1$, o que é um absurdo, pois $a \geq 2$ já que $S \neq \mathbb{N}$. Assim sendo, temos que $2a > b$, ou ainda, $a > \frac{b}{2}$. O lema 4.6 nos garante que podemos tomar $a \leq \frac{b+1}{2}$. Essas duas desigualdades implicam que $a = \frac{b+1}{2}$ e, portanto, $S = S\left(\frac{b+1}{2}, b\right)$.

Reciprocamente, seja $S = S\left(\frac{b+1}{2}, b\right)$, com b ímpar. Observe que $2 \in S$, pois $b+1 \mod b \leq 2$. Logo, $S = \langle 2, b\rangle$. Note que se $x \geq b$, então $x \in S$. Como $b-1$ é par, então também pertence a S. Entretanto, $b-2$ não pertence a S, pois é ímpar e não pode ser gerado como combinação linear (com coeficientes inteiros não negativos) de 2 e b. Assim, temos que $\gamma(S) = b-2$.

□

Exemplo 4.1.8: Sejam b um inteiro positivo tal que $b \geq 2$ e $S = S(2,b)$. Então $S = \left\{0,\ \left\lfloor \frac{b+1}{2} \right\rfloor,\ \rightarrow\right\}$.

Observe que se $x \geq b$, então $x \in \left\{0,\ \left\lfloor \frac{b+1}{2} \right\rfloor,\ \rightarrow\right\}$. Seja agora $0 < x < b$. Então $x \in S(2,b)$ se, e somente se, $2x \mod b \leq x$. Temos que $2x \mod b = 2x$ se, e somente se $2x < b$, e neste caso $x \notin \left\{0,\ \left\lfloor \frac{b+1}{2} \right\rfloor,\ \rightarrow\right\}$, pois temos $x < \frac{b}{2}$. Se $2x \geq b$, então $2x \mod b = b - 2x \leq x$, e assim $x \in S(2,b)$.

Vimos no corolário 4.8 que se $x \notin S$, então $b - x \in S$. Mas o que ocorre se $x \in S$?

Lema 4.11: Sejam a e b inteiros tais que $0 \leq a < b$, $S = S(a,b)$ e x um inteiro tal que $0 \leq x \leq b$. Então $x \in S$ e $b - x \in S$ se, e somente se, $ax \mod b \in \{0,x\}$.

Demonstração. Suponha que $ax \mod b \notin \{0,x\}$. Então o lema 4.7 nos garante que $a(b-x) \mod b = b - (ax \mod b)$. Se $x \in S$, então $ax \mod b < x$, e assim

$$a(b-x) \mod b = b - (ax \mod b) > b - x,$$

logo $b - x \notin S$.

Reciprocamente, se $ax \mod b = 0$, segue que $x \in S$. O lema 4.7 nos diz que $a(b-x) \mod b = 0$, mostrando que $b - x \in S$. Por fim, se $ax \mod b = x \neq 0$, então $x \in S$ e, novamente pelo lema 4.7, temos que

$$a(b-x) \mod b = b - (ax \mod b) = b - x,$$

mostrando que $b - x \in S$.

□

Exemplo 4.1.9: Seja $S = S(7,8)$. Do exemplo 4.1.6, sabemos que $S = \langle 4,\ 5,\ 6,\ 7\rangle = \{0,\ 4,\ \rightarrow\}$. Para $0 \leq x \leq 8$, temos que $x \in S$ e $8 - x \in S$ se $x \in \{0,\ 4,\ 8\}$. Note que

$$7.0 \mod 8 = 0,$$
$$4.7 \mod 8 = 4,$$
$$7.8 \mod 8 = 0.$$

Lema 4.12: Sejam a e b inteiros positivos e seja x um inteiro tal que $0 \leq x < b$. Então

(i) $ax \mod b = 0$ se, e somente se, x é um múltiplo de $\frac{b}{(a,b)}$;

(ii) $ax \mod b = x$ se, e somente se, x é um múltiplo de $\dfrac{b}{(b,a-1)}$.

Demonstração. Para (i), se $ax \mod b = 0$, então existe um inteiro q tal que $ax = qb$. Logo, $\dfrac{ax}{(a,b)} = \dfrac{qb}{(a,b)}$. Como $\left(\dfrac{a}{(a,b)}, \dfrac{b}{(a,b)}\right) = 1$, o lema 2.20 (Lema de Gauss) nos garante que $\dfrac{b}{(a,b)} \mid x$, mostrando que x é um múltiplo de $\dfrac{b}{(a,b)}$.

Reciprocamente, se x é um múltiplo de $\dfrac{b}{(a,b)}$, então existe q inteiro tal que $x = q\dfrac{b}{(a,b)}$. Portanto,

$$ax \mod b = aq\frac{b}{(a,b)} \mod b = q\frac{a}{(a,b)}b \mod b = 0.$$

Para (ii), basta repetir o raciocínio do item (i) considerando $a-1$ no lugar de a.

□

Exemplo 4.1.10: Tome $a = 3$ e $b = 6$. Então $(a,b) = (3,6) = 3$ e $(a-1,b) = (2,6) = 2$. Note que $3.2 \mod 6 = 0$ e $3.3 \mod 6 = 3$.

Lema 4.13: Seja $S = S(a,b)$ com a e b inteiros positivos tais que $0 < a < b$. Sejam $(a,b) = d_1$, $(a-1,b) = d_2$ e x um inteiro tal que $0 \leq x \leq b$. Então $x \in S$ e $b - x \in S$ se, e somente se,

$$x \in X = \left\{0, \frac{b}{d_2},\ 2\frac{b}{d_2}, \ldots,\ (d_2-1)\frac{b}{d_2},\ \frac{b}{d_1},\ 2\frac{b}{d_1}, \ldots,\ (d_1-1)\frac{b}{d_1},\ b\right\}.$$

Ademais, $card(X) = d_1 + d_2$.

Demonstração. O lema 4.11 nos garante que $x \in S$ e $b - x \in S$ se, e somente se, $ax \mod b \in \{0,x\}$. O lema 4.12 nos permite concluir que $x \in X$.

Vamos mostrar que não há duplicação nos elementos de X: suponha que $k_1\dfrac{b}{d_1} = k_2\dfrac{b}{d_2}$ para alguns $k_1,\ k_2 \in \mathbb{N}$. Então $k_1d_2 = k_2d_1$. Como $(a-1,a) = 1$, então $(d_1,d_2) = 1$ e, consequentemente, existe $k \in \mathbb{N}$ tal que $k_1d_2 = k_2d_1 = kd_1d_2$. Portanto, $k_1 = kd_1$ e $k_2 = kd_2$. Desse modo, seque que a cardinalidade de X é, de fato, $d_1 + d_2$.

□

Teorema 4.14: Seja $S = S(a,b)$ com a e b inteiros tais que $0 \leq a < b$. Então

$$g(S) = card(\mathbb{N} \setminus S) = \frac{b + 1 - (a,b) - (a-1,b)}{2}.$$

Demonstração. Sejam d_1, d_2 e X como no lema 4.13. Para $0 \leq x \leq b$, o corolário 4.8 e o lema 4.13 nos garantem que ou $x \in S$ ou $b - x \in S$ (e exatamente um deles), a não ser que $x \in X$. Portanto,

$$g(S) = card(\mathbb{N} \setminus S) = \frac{b + 1 - card(X)}{2} = \frac{b + 1 - d_1 - d_2}{2},$$

e segue o resultado.

□

Exemplo 4.1.11: Seja $S = S(a,p)$, com a inteiro e p um primo ímpar. Para todo $0 < a < p$, temos que

$$g(S) = \frac{p+1-1-1}{2} = \frac{p-1}{2}.$$

O que podemos dizer de duas inequações modulares que possuem a mesma solução? O corolário abaixo nos dá uma relação interessante.

Corolário 4.15: Suponha que $S(a_1,b_1) = S(a_2,b_2)$, para $a_1,\ a_2,\ b_1$ e b_2 inteiros positivos. Então

$$b_1 - (a_1,b_1) - (a_1 - 1,b_1) = b_2 - (a_2,b_2) - (a_2 - 1,b_2).$$

Demonstração. Como $S(a_1,b_1) = S(a_2,b_2)$, então $\mathbb{N} \setminus S(a_1,b_1) = \mathbb{N} \setminus S(a_2,b_2)$. Portanto, o teorema 4.14 nos garante que

$$\frac{b_1 + 1 - (a_1,b_1) - (a_1 - 1,b_1)}{2} = \frac{b_2 + 1 - (a_2,b_2) - (a_2 - 1,b_2)}{2},$$

e o resultado segue.

□

Exemplo 4.1.12: A recíproca do corolário 4.15 é falsa: Observe que

$$12 - (3,12) - (2,12) = 7 = 10 - (2,10) - (1,10).$$

Entretanto,

$$\langle 4,\ 5,\ 6\rangle = S(3,12) \neq \langle 5,\ 6,\ 7,\ 8,\ 9\rangle = S(2,10).$$

Definição 4.16: Seja $S = S(a,b)$ para a e b inteiros tais que $0 \leq a < b$. Definimos o **peso** de S como

$$w(S) = b - (a,b) - (a - 1,b).$$

Note que $w(\mathbb{N}) = -1$, pois $\mathbb{N} = S(0,1)$.

Observação 4.17: O teorema 4.14 e o corolário 4.15 nos garantem que

$$w(S) = 2card(\mathbb{N} \setminus S) - 1 = 2g(S) - 1$$

e, portanto, $w(S)$ é um invariante de S, ou seja, independe de a e b.

Exemplo 4.1.13: Seja $S = S(7,8)$. Então o peso de S é

$$w(S) = 8 - (7,8) - (6,8) = 8 - 1 - 2 = 5.$$

Do exemplo 4.1.6, sabemos que $S = \langle 4,\ 5,\ 6,\ 7\rangle = \{0,\ 4,\ \rightarrow\}$. Portanto,

$$\mathbb{N} \setminus S = \{1,\ 2,\ 3\},$$
$$g(S) = 3.$$

Note que $w(S) = 5 = 2g(S) - 1$.

Proposição 4.18: Seja $S = S(a,b) \neq \mathbb{N}$. Então, $w(S) \geq 1$.

Demonstração. Inicialmente, vamos mostrar que

$$(a,b) + (a-1,b) \leq \frac{b}{2} + \frac{b}{3} = \frac{5b}{6} : \tag{4.1}$$

Como $S(a,b) \neq \mathbb{N}$, podemos tomar a e b tais que $2 \leq a < b$. Seja $(a,b) = d_1$. Existem q_1 e k_1 inteiros positivos tais que $a = q_1 d_1$ e $b = k_1 d_1$. Suponha que $d_1 > \frac{b}{2}$. Então

$$a = q_1 d_1 > q_1 \frac{b}{2} \text{ e, portanto, } 2a > q_1 b.$$

Como $2a < 2b$, devemos ter $q_1 = 1$ e, consequentemente, $a = d_1$. Desse modo,

$$2a > q_1 b = b = k_1 d_1 = k_1 a, \text{ ou seja, } 2 > k_1,$$

mostrando que $k_1 = 1$ e $b = d_1 = a$, o que é um absurdo. Portanto, devemos ter $(a,b) = d_1 \leq \frac{b}{2}$.

Seja agora $(a-1,b) = d_2$. Existem q_2 e k_2 inteiros positivos tais que $a - 1 = q_2 d_2$ e $b = k_2 d_2$. Se $d_2 \leq \frac{b}{3}$, a desigualdade (4.1) é satisfeita. Suponha então que $d_2 > \frac{b}{3}$. Desse modo,

$$a - 1 = q_2 d_2 > q_2 \frac{b}{3} \implies 3(a-1) > q_2 b.$$

Como $3(a-1) < 3a < 3b$, devemos ter $q_2 = 1$ ou $q_2 = 2$.

Se $q_2 = 1$, então $a - 1 = d_2$, e assim

$$3(a-1) > q_2 b = b = k_2 d_2 = k_2(a-1) \implies 3 > k_2,$$

o que implica em $k_2 = 2$, já que $k_2 > 1$ pois $a < b$. Desse modo, $b = 2d_2 = 2(a-1)$, ou seja, $d_2 = \frac{b}{2}$.

Uma vez que $(a-1,a) = 1$, devemos ter $(a,b) = (a, 2(a-1)) = d_1 < \frac{b}{2}$. Sabemos que existem q e k inteiros tais que $a = q d_1$ e $b = 2(a-1) = k d_1$. Suponha que

$d_1 > \dfrac{b}{3} = \dfrac{2(a-1)}{3}$. Então

$$2(a-1) = kd_1 > k\frac{2(a-1)}{3} \implies 6(a-1) > k2(a-1) \implies 3 > k,$$

o que implica em $k = 1$ ou $k = 2$.

Se $k = 1$, segue que $2(a-1) = d_1$, o que é um absurdo pois $2(a-1) = b > a$. Se $k = 2$, temos que $a - 1 = d_1$, mas isso também é um absurdo, pois então teríamos que $a - 1 \mid a$, com $a > 2$. Portanto, devemos ter $(a,b) = d_1 \leq \dfrac{b}{3}$, mostrando que a desigualdade (4.1) é satisfeita.

Agora, se $q_2 = 2$, então $a - 1 = 2d_2$. Logo,

$$3(a-1) > q_2 b = 2b \implies 3.2d_2 > 2k_2 d_2 \implies 3 > k_2.$$

Se $k_2 = 1$, temos que $b = d_2 < 2d_2 = a - 1$, o que é um absurdo. Se $k_2 = 2$, então $b = 2d_2 = a - 1$, o que também é um absurdo.

Portanto, a desigualdade (4.1) é sempre satisfeita.

Como $(a,b) + (a-1,b) \leq \dfrac{b}{2} + \dfrac{b}{3} < b$, segue que

$$w(S) = b - (a,b) - (a-1,b) \geq 1.$$

□

O peso é um importante invariante de um semigrupo, e saber calculá-lo é necessário. A proposição abaixo nos ajuda nesse processo.

Proposição 4.19: Seja $S = S(a,b)$ um semigrupo modular. Então $w(S)$ é ímpar e $w(S) \geq \gamma(S)$.

Demonstração. Da observação 4.17, temos que $w(S) = 2g(S) - 1$, que é um número ímpar. Recordando que $card(\mathbb{N} \setminus S) = g(S)$, a proposição 3.3 nos garante que

$$w(S) = 2g(S) - 1 \geq 2\left(\frac{\gamma(S)+1}{2}\right) - 1 = \gamma(S) + 1 - 1 = \gamma(S).$$

□

Exemplo 4.1.14: Tomando $S = S(7,8)$, do exemplo 4.1.13 temos que

$$w(S) = 5 \geq 3 = \gamma(S).$$

A proposição abaixo nos dá uma dimensão da importância do peso de um semigrupo modular:

Proposição 4.20: Seja S um semigrupo modular. Então

(i) S é simétrico se, e somente se, $w(S) = \gamma(S)$;

(ii) S é pseudossimétrico se, e somente se, $w(S) = \gamma(S) + 1$.

Demonstração. Para (i), note que se S é simétrico, de acordo com a definição 3.50 temos que $\beta(S) = 2g(S)$, ou seja,

$$\gamma(S) + 1 = 2g(S) \implies g(S) = \frac{\gamma(S) + 1}{2}.$$

O teorema 4.14 nos diz que

$$g(S) = \frac{w(S) + 1}{2}.$$

Das duas igualdades segue que $w(S) = \gamma(S)$.

Agora, se $w(S) = \gamma(S)$, o teorema 4.14 nos diz que

$$g(S) = \frac{w(S) + 1}{2} = \frac{\gamma(S) + 1}{2} \implies \gamma(S) + 1 = 2g(S) \implies \beta = 2g,$$

mostrando que S é simétrico.

Para a parte (ii), o argumento é análogo, considerando que um semigrupo S é pseudossimétrico se $\beta(S) = 2g - 1$.

□

Exemplo 4.1.15: Se b é um inteiro ímpar, então sempre existe um semigrupo modular S com $w(S) = b$. De fato, basta tomar $S = S(2,b+2)$, pois

$$w(S(2,b+2)) = b + 2 - (2,b+2) - (1,b+2) = b + 2 - 1 - 1 = b.$$

4.2 Um algoritmo para determinar se um semigrupo numérico é modular

Nesta seção, iremos apresentar um algoritmo que permite concluir se um semigrupo S é modular ou não e, em caso afirmativo, obter uma representação modular para S. Iniciaremos com um lema que limita o valor do módulo de um semigrupo modular.

Lema 4.21: Seja $S = S(a,b) \neq \mathbb{N}$, com $2 \leq a < b$. Então

$$b \leq 12g(S) - 6.$$

Observe que este lema nos diz que o número de representações modulares para um semigrupo modular é finito.

Demonstração. O teorema 4.14 nos garante que

$$b = 2g(S) + (a,b) + (a-1,b) - 1.$$

Aplicando a desigualdade 4.1, demonstrada na proposição 4.18, temos que

$$b \leq 2g(S) + \frac{b}{2} + \frac{b}{3} - 1 = 2g(S) + \frac{5b}{6} - 1 \implies b \leq 12g(S) - 6.$$

□

Lema 4.22: Seja $S = S(a,b)$ com multiplicidade $\mu(S)$. Então

$$b - \mu(S) \in S \quad \text{se, e somente se,} \quad \mu(S) = min\left\{\frac{b}{(a,b)}, \frac{b}{(a-1,b)}\right\}.$$

Demonstração. O resultado segue imediatamente do lema 4.13: sejam $(a,b) = d_1$, $(a-1,b) = d_2$. Então $\mu(S) \in S$ (o que é sempre verdade) e $b - \mu(S) \in S$ se, e somente se,

$$\mu(S) \in X = \left\{0, \frac{b}{d_2},\ 2\frac{b}{d_2}, \ldots,\ (d_2-1)\frac{b}{d_2},\ \frac{b}{d_1},\ 2\frac{b}{d_1}, \ldots,\ (d_1-1)\frac{b}{d_1},\ b\right\}.$$

Uma vez que $\mu(S)$ é o menor inteiro positivo pertencente a S, devemos ter $\mu(S) = min\left\{\frac{b}{d_1}, \frac{b}{d_2}\right\}$.

□

Exemplo 4.2.1: Seja $S = S(7,8)$. Do exemplo 4.1.6, sabemos que $S = \langle 4,\ 5,\ 6,\ 7\rangle = \{0,\ 4,\ \rightarrow\}$ e $g(S) = 3$. Note que $8 \leq 12.3 - 6$, $\mu(S) = 4$ e $8 - 4 = 4 \in S$, visto que $4 = \min\{4,\ 8\}$.

Os próximos lemas no dão uma cota inferior para o módulo de um semigrupo e quando ele atinge o seu valor mínimo.

Lema 4.23: Seja $S = S(a,b)$ com multiplicidade $\mu(S)$ e número de Fröbenius $\gamma(S)$. Então

$$b \geq \mu(S) + \gamma(S).$$

Demonstração. Como $1,\ 2, \ldots,\ \mu(S)-1$ não pertencem a S, o corolário 4.8 nos garante que $b - \mu(S) - 1, \ldots,\ b - 1$ são todos elementos de S. Sabemos que tanto b quanto $\mu(S)$ pertencem a S, portanto $\{b - \mu(S) + 1,\ \rightarrow\} \subseteq S$. Desse modo, podemos concluir que $\gamma(S) \leq b - \mu(S)$, ou seja, $b \geq \mu(S) + \gamma(S)$.

□

Lema 4.24: Seja $S = S(a,b)$ com multiplicidade $\mu(S)$ e número de Fröbenius $\gamma(S)$. Então

$$b = \mu(S) + \gamma(S) \quad \text{se, e somente se,} \quad \mu(S) \neq \min\left\{\frac{b}{(a,b)}, \frac{b}{(a-1,b)}\right\}.$$

Demonstração. Se $b = \mu(S) + \gamma(S)$, então $b - \mu(S) = \gamma(S) \notin S$, e o lema 4.22 nos permite concluir que $\mu(S) \neq \min\left\{\frac{b}{(a,b)}, \frac{b}{(a-1,b)}\right\}$.

Reciprocamente, suponha que $\mu(S) \neq \min\left\{\frac{b}{(a,b)}, \frac{b}{(a-1,b)}\right\}$. Do lema 4.22, segue que $b-\mu(S) \notin S$. O lema 4.23 nos diz que $b \geq \mu(S)+\gamma(S)$. Se $b > \mu(S)+\gamma(S)$, temos que $b-\mu(S) > \gamma(S)$, o que é um absurdo, pois implica em $b-\mu(S) \in S$. Portanto, devemos ter $b = \mu(S)+\gamma(S)$.

□

Vamos agora enunciar o algoritmo que permite verificar se um semigrupo numérico é modular e, em caso afirmativo, escrevê-lo na forma $S = S(a,b)$.

Algoritmo 4.25: Seja $S = \langle n_1,\ n_2, \ldots,\ n_k\rangle \neq \mathbb{N}$ um semigrupo numérico:

(1) Calcule $\mu(S)$, $\gamma(S)$ e $g(S) = card(\mathbb{N} \setminus S)$.

(2) Seja $b = \mu(S)+\gamma(S)$.

(3) Para cada $a \in A = \left\{ a \in \mathbb{N} \;\middle|\; \begin{array}{c} 2 \leq a < \frac{b+1}{2}, \\ b = 2g(S)+(a,b)+(a-1,b)-1, \\ \mu(S) < \min\left\{\frac{b}{(a,b)}, \frac{b}{(a-1,b)}\right\} \end{array} \right\}$, calcule $S(a,b)$. Se $S = S(a,b)$ então S é modular com módulo b e fator a, e o algoritmo termina nesta etapa.

(4) Determine $B = \{b \in C \mid 2g(S)+1 \leq b \leq 12g(S)-6\}$, em que $C = \{k\mu(S) \mid k \in \mathbb{N}\}$.

(5) Para cada $b \in B$, determine o conjunto

$$A_b = \left\{ a \in \mathbb{N} \;\middle|\; \begin{array}{c} 2 \leq a < \frac{b+1}{2}, \\ b = 2g(S)+(a,b)+(a-1,b)-1, \\ \mu(S) = \min\left\{\frac{b}{(a,b)}, \frac{b}{(a-1,b)}\right\} \end{array} \right\},$$

(6) Para cada $b \in B$ e cada $a \in A_b$, calcule $S(a,b)$. Se $S = S(a,b)$ então S é modular com módulo b e fator a, e o algoritmo termina nesta etapa.

(7) S não é um semigrupo modular.

Vamos brevemente discutir a justificativa do algoritmo 4.25. Nos passos (2) e (3) estamos verificando se S é ou não um semigrupo modular com módulo $\mu(S)+\gamma(S)$, de acordo com os lemas 4.6 e 4.24 e o teorema 4.14. Se S não é um semigrupo modular com módulo $\mu(S)+\gamma(S)$, então o lema 4.24 nos diz que $\mu(S) = \min\left\{\frac{b}{(a,b)}, \frac{b}{(a-1,b)}\right\}$, o que nos permite concluir que $\mu(S)$ divide b, ou seja, b é múltiplo de $\mu(S)$. O teorema 4.14 nos garante que $b = 2g(S)+(a,b)+(a-1,b)-1$, e assim $b \geq 2g(S)+1$. Por fim, o lema 4.21 assegura que $b \leq 12g(S)-6$, e assim os passos (4), (5), (6) e (7) cobrem o caso $b \neq \mu(S)+\gamma(S)$. Podemos verificar se $S = S(a,b)$ nos passos (3) e (6) observando se os sistemas minimais de geradores de cada semigrupo coincidem, ou ainda comprovando se $S \subseteq S(a,b)$ e $g(S) = g(S(a,b))$.

Exemplo 4.2.2: Seja $S = \langle 3,\ 5\rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$. Então $\mathbb{N} \setminus S = \{1,\ 2,\ 4,\ 7\}$, $g(S) = 4$, $\mu(S) = 3$ e $\gamma(S) = 7$. Dos passos (2) e (3), tomamos $b = 3 + 7 = 10$ e obtemos $A = \{2,\ 3,\ 4\}$. Assim,

$$S(2,10) = \langle 5,\ 6,\ 7,\ 8,\ 9\rangle, \quad S(3,10) = \langle 4,\ 5,\ 6\rangle, \quad S(4,10) = \langle 3,\ 5\rangle = S.$$

Portanto, o algoritmo 4.25 nos diz que S é modular com módulo 10 e fator 4.

Do exemplo 3.4.1, sabemos que S é simétrico. Note que a proposição 4.20 é de fato satisfeita:

$$w(S) = b - (a,b) - (a-1,b) = 10 - 2 - 1 = 7 = \mu(S).$$

De maneira geral, se já soubermos que o semigrupo em questão é simétrico, a proposição 4.20 nos garante que $b = \gamma(S) + (a,b) + (a-1,b)$, e podemos usar este valor de b no algoritmo 4.25.

Exemplo 4.2.3: Seja $S = \langle 3,\ 5,\ 7\rangle = \{0,\ 3,\ 5,\ \rightarrow\}$. Então $\mathbb{N} \setminus S = \{1,\ 2,\ 4\}$, $g(S) = 3$, $\mu(S) = 3$ e $\gamma(S) = 4$. Dos passos (2) e (3), tomamos $b = 3+4 = 7$ e obtemos $A = \{2,\ 3,\ 4\}$. Assim,

$$S(2,7) = \langle 4,\ 5,\ 6,\ 7\rangle, \quad S(3,7) = \langle 3,\ 5,\ 7\rangle = S, \quad S(4,7) = \langle 2,\ 7\rangle.$$

Portanto, o algoritmo 4.25 nos diz que S é modular com módulo 7 e fator 3.

Do exemplo 3.4.5, sabemos que S é pseudossimétrico. Note que a proposição 4.20 é de fato satisfeita:

$$w(S) = b - (a,b) - (a-1,b) = 7 - 1 - 1 = 5 = \mu(S) + 1.$$

Analogamente ao caso em que S é simétrico, se já soubermos que o semigrupo em questão é pseudossimétrico, a proposição 4.20 nos garante que $b = \gamma(S)+(a,b)+(a-1,b)+1$, e podemos usar este valor de b no algoritmo 4.25.

Exemplo 4.2.4: Seja $S = \langle 3,\ 8,\ 10\rangle = \{0,\ 3,\ 6,\ 8,\ \rightarrow\}$. Então $\mathbb{N} \setminus S = \{1,\ 2,\ 4,\ 5,\ 7\}$, $g(S) = 5$, $\mu(S) = 3$ e $\gamma(S) = 7$. Dos passos (2) e (3), tomamos $b = 3 + 7 = 10$ e obtemos $A = \emptyset$. Do passo (4) obtemos

$$B = \{12,\ 15,\ 18,\ 21,\ 24,\ 27,\ 30,\ 33,\ 36,\ 39, 42,\ 45,\ 48,\ 51,\ 54\}.$$

O único conjunto A_b não vazio, com $b \in B$, é $A_{15} = \{5\}$. Entretanto,

$$S(5,15) = \langle 3,\ 7,\ 11\rangle \neq S,$$

e o algoritmo nos informa que S não é um semigrupo numérico modular.

4.3 Semigrupos modulares cujo módulo é igual ao seu peso mais dois

Vamos estudar semigrupos modulares $S = (a,b)$ cujo módulo é igual a $w(S) + 2$. Sabemos que $b = w(S) + (a,b) + (a-1,b) \geq w(S) + 2$. Portanto, $b = w(S) + 2$ se, e somente se, $(a,b) = (a-1,b) = 1$, o que implica em b ímpar. A condição $b = w(S) + 2$ caracteriza semigrupos modulares cujo módulo é mínimo com respeito ao seu peso.

Proposição 4.26: Seja $S = S(a,b)$ com $2 \leq a < b$ e $(a,b) = (a-1,b) = 1$. Então

(i) $b = \gamma(S) + \mu(S)$;

(ii) $g(S) = \dfrac{\gamma(S) + \mu(S) - 1}{2}$;

(iii) b é o maior gerador minimal de S.

Demonstração. Para a parte (i), note que como $2 \leq a < b$, então $1 \notin S$. Do corolário 4.8 temos que $b - 1 \in S$ e, portanto, $\mu(S) \neq b$. Desse modo, o lema 4.24 nos garante que $b = \mu(S) + \gamma(S)$.

A parte (ii) é uma consequência imediata do teorema 4.14.

Para a parte (iii), suponha que b não seja um gerador minimal de S, ou seja, suponha que existam $x,\ y \in S \setminus \{0\}$ tais que $b = x + y$. Então $ax \mod b \leq x$ e $ay \mod b \leq y$, e assim $(ax \mod b \leq x) + (ay \mod b \leq y) \leq x + y = b$. Temos também que

$$(ax \mod b) + (ay \mod b) = a(x+y) \mod b = ab \mod b = 0,$$

e assim $(ax \mod b) + (ay \mod b) \in \{0,\ b\}$. Temos duas possibilidades:

1. $ax \mod b = 0$ e $ay \mod b = 0$, ou
2. $ax \mod b = x$ e $ay \mod b = y$.

Entretanto, os dois casos contradizem o lema 4.12, uma vez que $(a,b) = (a-1,b) = 1$. Portanto, b é gerador minimal de S.

Seja $x \in S$, com $x > b$. Do item (i), segue que $x > \mu(S) + \gamma(S)$, ou seja, $x - \mu(S) > \gamma(S)$, o que implica em $x - \mu(S) \in S$. Desse modo, $x = \mu(S) + (x - \mu(S))$ não pode ser um gerador minimal de S. Portanto, b é o maior gerador minimal de S. □

A proposição 4.26 nos permite relacionar os semigrupos modulares desta seção com os chamados semigrupos numéricos UESY. Abaixo, vamos definir tais semigrupos e apresentar algumas de suas propriedades. A sigla UESY vem do inglês "*unitary extension of a symmetric numerical semigroup*".

Definição 4.27: Um semigrupo numérico S é um **UESY-semigrupo**, ou **semigrupo UESY**, se existe um semigrupo simétrico S' tal que $S' \subseteq S$ e $card(S \setminus S') = 1$.

Exemplo 4.3.1: $S = \langle 3,\ 5,\ 7\rangle = \{0,\ 3,\ 5,\ \rightarrow\}$ é um semigrupo UESY. De fato, $S' = \langle 3,\ 5\rangle = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$ é simétrico, com $S' \subseteq S$ e $card(S \setminus S') = 1$, pois $S \setminus S' = \{7\}$.

Naturalmente, se $S \neq \mathbb{N}$ é um semigrupo, então $R = S \cup \{\gamma(S)\}$ também o é. De fato, note que $0 \in S \subset R$ e $\mathbb{N} \setminus R$ é finito, pois $\mathbb{N} \setminus R \subset \mathbb{N} \setminus S$. Uma vez que S é fechado para a soma, R também será. Como $\gamma(S) = \beta(S) - 1 \in R$, então $\beta(R) < \beta(S)$. Logo, para qualquer $s \in S$, $s + \gamma(S) > \beta(R)$ e, portanto, pertence a R.

Proposição 4.28: Um semigrupo S é um UESY-semigrupo se, e somente se, existe um semigrupo simétrico S' tal que $S = S' \cup \{\gamma(S')\}$.

Demonstração. Se S é um UESY-semigrupo, então existe um semigrupo simétrico S' e um inteiro positivo $h \in S \setminus S'$ tal que $S = S' \cup \{h\}$. Como $h \notin S'$ e S' é simétrico, a proposição 3.52 nos garante que $\gamma(S') - h \in S'$. Desse modo, $\{h,\ \gamma(S') - h\} \subseteq S$ e, portanto, $h + (\gamma(S') - h) = \gamma(S') \in S$. Como $\gamma(S') \notin S'$, segue que $\gamma(S') \in \{h\}$, ou seja, $\gamma(S') = h$.

Reciprocamente, se existe um semigrupo simétrico S' tal que $S = S' \cup \{\gamma(S')\}$, então $S' \subseteq S$ e $card(S \setminus S') = 1$ e, portanto, S é um UESY-semigrupo.

□

A proposição 4.28 nos diz que UESY-semigrupos são semigrupos da forma $S \cup \{\gamma(S)\}$, sendo S um semigrupo simétrico. Os próximos dois lemas determinam a multiplicidade e o número de Fröbenius de $S \cup \{\gamma(S)\}$.

Lema 4.29: Seja $S \neq \mathbb{N}$ um semigrupo simétrico. Então

$$\gamma(S \cup \{\gamma(S)\}) = \gamma(S) - \mu(S).$$

Demonstração. Uma vez que $\mu(S) \in S$ e $\gamma(S) \notin S$, segue que $\gamma(S) - \mu(S) \notin S$ e, portanto, $\gamma(S) - \mu(S) \notin S \cup \{\gamma(S)\}$. Sabemos que $\mu(S)$ é o menor inteiro positivo pertencente a S, logo $\{1,\ 2, \ldots,\ \mu(S) - 1\} \subseteq \mathbb{N} \setminus S$ e, sendo S simétrico, a proposição 3.52 garante que $\{\gamma(S) - 1,\ \gamma(S) - 2, \ldots,\ \gamma(S) - (\mu(S) - 1)\} \subseteq S$. Portanto, $\{\gamma(S) - \mu(S) + 1,\ \gamma(S) - \mu(S) + 2, \ldots,\ \gamma(S) - 1,\ \gamma(S)\} \subseteq S \cup \{\gamma(S)\}$. Utilizando o fato de que $\mu(S) \in S \cup \{\gamma(S)\}$, e como todo inteiro $x > \gamma(S) - \mu(S)$ pode ser escrito como $(\gamma(S) - \mu(S) + i) + k\mu(S)$ para algum k inteiro e $i \in \{1, \ldots,\ \mu(S)\}$, temos que $\{x \in \mathbb{N} \mid x > \gamma(S) - \mu(S)\} \subseteq S \cup \{\gamma(S)\}$. Portanto, concluímos que $\gamma(S \cup \{\gamma(S)\}) = \gamma(S) - \mu(S)$.

□

Lema 4.30: Seja S um semigrupo tal que $S \neq \mathbb{N}$ e $S \neq \mathbb{N} \setminus \{1\}$. Então

$$\mu(S \cup \{\gamma(S)\}) = \mu(S).$$

Demonstração. Naturalmente, $\mu(S \cup \{\gamma(S)\}) \leq \mu(S)$. Se $\mu(S \cup \{\gamma(S)\}) < \mu(S)$, então $\gamma(S) = \mu(S) - 1$ pois, caso contrário, o condutor $\beta(S) = \gamma(S) + 1$ seria menor que a multiplicidade $\mu(S)$. Então S é da forma $\{0,\ \mu(S) = \beta(S),\ \rightarrow\}$. Como $S \neq \mathbb{N} \setminus \{1\}$,

$\mu(S) > 2$, logo $\mu(S) - 2 \notin S$ e, como S é simétrico, temos que

$$\gamma(S) - (\mu(S) - 2) = (\mu(S) - 1) - (\mu(S) - 2) = 1 \in S,$$

implicando em $S = \mathbb{N}$, o que é um absurdo. Portanto, devemos ter $\mu(S \cup \{\gamma(S)\}) = \mu(S)$.

□

Exemplo 4.3.2: Sejam $S = \{0,\ 3,\ 5,\ 6,\ 8,\ \rightarrow\}$ e $S \cup \{7\} = \{0,\ 3,\ 5,\ \rightarrow\}$. Temos $\gamma(S) = 7$ e $\mu(S) = 3$. Note que $\gamma(S \cup \{7\}) = 4 = \gamma(S) - \mu(S)$ e $\mu(S \cup \{7\}) = 3 = \mu(S)$.

Proposição 4.31: Seja $S \neq \mathbb{N}$ um UESY-semigrupo. Então

$$g(S) = \frac{\gamma(S) + \mu(S) - 1}{2}.$$

Demonstração. Seja S um UESY-semigrupo. Pela proposição 4.28, existe um semigrupo simétrico S' tal que $S = S' \cup \{\gamma(S')\}$. Como $S \neq \mathbb{N}$, temos que $S' \neq \mathbb{N}$ e $S' \neq \mathbb{N} \setminus \{1\}$. Dos lemas 4.29 e 4.30, obtemos $\gamma(S) = \gamma(S') - \mu(S')$ e $\mu(S) = \mu(S')$. Do fato de S' ser simétrico, temos $\beta(S') = \gamma(S') + 1 = 2g(S')$. Ademais, $g(S) = g(S') - 1$, portanto

$$g(S) = \frac{\gamma(S') + 1}{2} - 1 = \frac{\gamma(S) + \mu(S) - 1}{2}.$$

□

Exemplo 4.3.3: Seja $S = \langle 3,\ 5,\ 7\rangle = \{0,\ 3,\ 5,\ \rightarrow\}$. Temos:

$$\begin{aligned} \mu(S) &= 3, \\ \gamma(S) &= 4, \\ \mathbb{N} \setminus S &= \{1,\ 2,\ 4\}, \\ g(S) = 3 &= \frac{4 + 3 - 1}{2}. \end{aligned}$$

Podemos encontrar um gerador minimal de um UESY-semigrupo apenas somando sua multiplicidade e seu número de Fröbenius.

Proposição 4.32: Seja $S \neq \mathbb{N}$ um UESY-semigrupo. Então $\gamma(S) + \mu(S)$ é um gerador minimal de S.

Demonstração. Seja S um UESY-semigrupo. Pela proposição 4.28, existe um semigrupo simétrico S' tal que $S = S' \cup \{\gamma(S')\}$. Naturalmente, $\gamma(S')$ é um gerador minimal de S (pois pertence a S e não pode ser escrito como combinação linear de elementos de S'). Dos lemas 4.29 e 4.30, concluímos que $\gamma(S') = \gamma(S) + \mu(S)$.

□

Exemplo 4.3.4: Considere, novamente, $S = \langle 3,\ 5,\ 7\rangle = \{0,\ 3,\ 5,\ \rightarrow\}$. Note que $\gamma(S) + \mu(S) = 4 + 3 = 7$ é gerador minimal de S.

Ainda sobre o gerador minimal, podemos afirmar que um elemento s de S é gerador minimal se, e somente se, $S \setminus \{s\}$ é semigrupo.

Lema 4.33: Sejam S um semigrupo e $s \in S$. Então $S \setminus \{s\}$ é um semigrupo se, e somente se, s é um gerador minimal de S.

Demonstração. Sejam S um semigrupo, $s \in S$ e suponha que $S \setminus \{s\}$ é um semigrupo. Se s não fosse gerador minimal de S, então existiriam $x,\ y \in S$ tais que $s = x + y$. Mas então $s = x + y \notin S \setminus \{s\}$, contradizendo o fato de $S \setminus \{s\}$ ser semigrupo.

Reciprocamente, se s é gerador minimal de S, então $S \setminus \{s\}$ é semigrupo: $0 \in S \setminus \{s\}$, $\mathbb{N} \setminus (S \setminus \{s\}) = (\mathbb{N} \setminus S) \cup \{s\}$ é finito e, dados $x,\ y \in S \setminus \{s\}$, temos que $x + y \in S \setminus \{s\}$, pois $x + y \in S$ e $x + y \neq s$.

□

Exemplo 4.3.5: Seja $S = \langle 4,\ 6,\ 11\rangle = \{0,\ 4,\ 6,\ 8,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\}$.

Note que $S \setminus \{6\} = \{0,\ 4,\ 8,\ 10,\ 11,\ 12,\ 14,\ \rightarrow\}$ é semigrupo, mas $S \setminus \{10\} = \{0,\ 4,\ 6,\ 8,\ 11,\ 12,\ 14,\ \rightarrow\}$ não o é, pois $4 + 6 = 10 \notin S \setminus \{10\}$.

As proposições 4.31 e 4.32 trazem condições necessárias para S ser um UESY-semigrupo. O teorema a seguir nos diz que essas condições são também suficientes.

Teorema 4.34: Seja o semigrupo $S \neq \mathbb{N}$. Então as seguintes afirmações são equivalentes:

(i) S é um UESY-semigrupo;

(ii) $g(S) = \dfrac{\gamma(S) + \mu(S) - 1}{2}$ e $\gamma(S) + \mu(S)$ é um gerador minimal de S.

Demonstração. Note que a implicação (i) $\Longrightarrow$ (ii) é uma consequência direta das proposições 4.31 e 4.32.

Para mostrar que (ii) $\Longrightarrow$ (i), note que sendo $\gamma(S) + \mu(S)$ um gerador minimal de S, o lema 4.33 nos garante que $S' = S \setminus \{\gamma(S) + \mu(S)\}$ é um semigrupo numérico, e naturalmente $\gamma(S') = \gamma(S) + \mu(S)$. Ademais, temos que

$$g(S') = g(S) + 1 = \frac{\gamma(S) + \mu(S) - 1}{2} + 1 = \frac{\gamma(S') + 1}{2} \implies \beta(S') = 2g(S'),$$

o que mostra que S' é simétrico. Como $S = S' \cup \{\gamma(S')\}$, a proposição 4.28 nos garante que S é um UESY-semigrupo.

□

Dado um semigrupo $S \neq \mathbb{N}$, recordemos que $e(S)$ é a dimensão de mergulho de S, $T(S) = (S - M) \setminus S$, e $tipo(S) = t(S) = card(T(S))$. Em [15] se prova que se $S \neq \mathbb{N}$ é um UESY-semigrupo, então $t(S) = e(S) - 1$. Utilizando este fato, a proposição 4.26 e o teorema 4.34, obtemos o seguinte resultado:

Corolário 4.35: Seja $S = S(a,b)$ com $2 \leq a < b$ e $(a,b) = (a - 1,b) = 1$. Então $t(S) = e(S) - 1$ e existe um semigrupo simétrico S' tal que $S = S' \cup \{\gamma(S')\}$.

Exemplo 4.3.6: Seja $S = S(4,7)$. Do exemplo 4.1.7, sabemos que $S = \langle 2,\ 7\rangle = \{0,\ 2,\ 4,\ 6,\ \rightarrow\}$. S é um UESY-semigrupo, pois $S = S' \cup \{7\}$, com $S' = \{0,\ 2,\ 4,\ 6,\ 8,\ \rightarrow\}$. De fato,

$$\begin{aligned} \mathbb{N} \setminus S' &= \{1,\ 3,\ 5,\ 7\}, \\ g(S') &= 4, \end{aligned}$$

e assim $\beta(S') = 8 = 2g(S')$, mostrando que S' é simétrico. Note também que

$$\begin{aligned} \mu(S) &= 2,\ \gamma(S) = 5,\ e(S) = 2, \\ \gamma(S) + \mu(S) &= 7 \text{ é gerador minimal de } S, \\ M &= \{2,\ 4,\ 6,\ \rightarrow\}, \\ S - M &= \{0,\ 2,\ 4,\ \rightarrow\}, \\ T(S) &= \{5\}, \\ tipo(S) &= t(S) = 1 = e(S) - 1, \\ \mathbb{N} \setminus S &= \{1,\ 3,\ 5\}, \\ g(S) &= 3 = \frac{5+2-1}{2} = \frac{\gamma(S) + \mu(S) - 1}{2}. \end{aligned}$$

Vamos agora caracterizar os semigrupos modulares cujo módulo é mínimo com respeito ao seu peso:

Teorema 4.36: Seja $S = S(a,b)$. Então $b = w(S) + 2$ se, e somente se, S é um UESY-semigrupo e b é um gerador minimal de S.

Demonstração. Se $b = w(S) + 2$, conforme discutido no início da seção temos que $(a,b) = (a-1,b) = 1$. Pelo corolário 4.35 e pela proposição 4.28, concluímos que S é um UESY-semigrupo, e pela proposição 4.26, segue que b é gerador minimal de S.

Reciprocamente, sendo b um gerador minimal de S, na demonstração da proposição 4.26 vimos que se $x > \gamma(S) + \mu(S)$, então x não é gerador minimal de S. Do lema 4.23, segue que $b = \gamma(S) + \mu(S)$. Do teorema 4.34, temos que $g(S) = \dfrac{\gamma(S) + \mu(S) - 1}{2}$, e do teorema 4.14 segue que $g(S) = \dfrac{w(S) + 1}{2}$, donde podemos concluir que $b = w(S) + 2$. □

Exemplo 4.3.7: Consideremos, novamente, $S = S(4,7)$. Do exemplo 4.3.6, sabemos que S é UESY-semigrupo e $b = 7$ é gerador minimal de S. Note que

$$w(S) = 7 - (4,7) - (3,7) = 5,$$

mostrando que $b = w(S) + 2$.

Os próximos dois corolários ilustram a importância dos semigrupos modulares:

Corolário 4.37: Seja $S = S(a,b)$ um semigrupo modular. Então $b = w(S) + 2$ se, e somente se, $S \setminus \{b\}$ é um semigrupo simétrico. Ademais, se b é primo, então $S \setminus \{b\}$ é um semigrupo

simétrico.

Demonstração. Suponha que $b = w(S)+2$. Do teorema 4.36, temos que b é um gerador minimal de S, e o lema 4.33 garante que $S' = S \setminus \{b\}$ é semigrupo numérico. Note que $\gamma(S') = b$. Como $S = S' \cup \{\gamma(S')\}$ é UESY-semigrupo, temos que S' é simétrico.

Reciprocamente, se $S' = S \setminus \{b\}$ é simétrico, então $S = S' \cup \{b\}$ é UESY-semigrupo, e b é gerador minimal de S. Do teorema 4.36, segue que $b = w(S) + 2$.

Por fim, se b é primo, então $(a,b) = (a-1,b) = 1$, e assim $w(S) = b-(a,b)-(a-1,b) = b - 2$, o que implica, conforme demonstrado acima, que $S \setminus \{b\}$ é simétrico.

□

Exemplo 4.3.8: Dado $S = S(4,7)$, dos exemplos 4.3.6 e 4.3.7 vimos que $b = w(S) + 2$ e $S \setminus \{7\} = \{0,\ 2,\ 4,\ 6,\ 8,\ \rightarrow\}$ é simétrico.

Corolário 4.38: Seja b um número inteiro maior ou igual que 3. Então b é primo se, e somente se, b é o maior gerador minimal de $S(a,b)$ para todo $2 \leq a \leq \sqrt{b}$.

Demonstração. Seja $b \geq 3$ primo. Então as condições da proposição 4.26 são satisfeitas, mostrando que b é gerador minimal de $S(a.b)$.

Reciprocamente, se b não é primo, então existe $c \in \mathbb{N} \setminus \{0,\ 1\}$ tal que $b = ac$. Suponha, sem perda de generalidade, que $a \leq \sqrt{b}$. Então, se $S = S(a,b)$, temos que $ac \mod b = b \mod b = 0 \leq c$, e assim $c \in S$. Como $b = ac$, segue que b não pode ser um gerador minimal de S.

□

Exemplo 4.3.9: Seja $S = S(4,11)$. Então $w(S) = 11-(4,11)-(3,11) = 9$, ou seja, o módulo de S é igual ao seu peso mais dois. Analisando a inequação modular $4x \mod 11 \leq x$, temos que $S = \langle 3,\ 7,\ 11\rangle = \{0,\ 3,\ 6,\ 7,\ 9, \rightarrow\}$, e $b = 11$ é o maior gerador minimal de S.

O semigrupo $S' = \{0,\ 3,\ 6,\ 7,\ 9,\ 10,\ 12, \rightarrow\}$ é simétrico, pois $\mathbb{N} \setminus S' = \{1,\ 2,\ 4,\ 5,\ 8,\ 11\}$ e $\beta(S') = 12 = 2.6 = 2g(S')$. Como $S = S' \cup \{\gamma(S')\}$, sendo $\gamma(S') = 11$, segue que S é um UESY-semigrupo, satisfazendo assim o teorema 4.36. Note que $S' = S \setminus \{11\}$, satisfazendo o corolário 4.37.

Analisando as inequações modulares $2x \mod 11 \leq x$ e $3x \mod 11 \leq x$, constatamos que $S(2,11) = \langle 6,\ 7,\ 8,\ 9,\ 11\rangle = \{0,\ 6,\ \rightarrow\}$ e $S(3,11) = \langle 4,\ 5,\ 11\rangle = \{0,\ 4,\ 5,\ 8,\ \rightarrow\}$, mostrando que 11 é o maior gerador minimal de $S(2,11)$ e $S(3,11)$, e o corolário 4.38 é verificado.

O corolário 4.38 nos mostra que o estudo de semigrupos modulares possui importantes aplicações na Matemática, como na determinação de números primos.

5

Aplicações na Educação Básica

Segundo a BNCC [4], a Matemática deve desenvolver "competências e habilidades de raciocinar, representar, comunicar e argumentar matematicamente, de modo a favorecer o estabelecimento de conjecturas, a formulação e a resolução de problemas em uma variedade de contextos, utilizando conceitos, procedimentos, fatos e ferramentas matemáticas". Neste aspecto, trazer para a sala de aula novos problemas em que os alunos podem trabalhar individualmente ou em grupo, buscando resolvê-los através de tópicos já vistos previamente, permite que os estudantes construam o seu próprio conhecimento, participando ativamente como protagonistas de seus processos de aprendizagem.

Na educação básica os alunos se deparam com as equações do primeiro grau para modelar diversas situações. No oitavo ano, aprendem a resolver sistemas de duas equações com duas incógnitas. Um questionamento natural é: e se tivéssemos apenas uma equação com duas incógnitas? Nosso objetivo é apresentar situações envolvendo equações diofantinas e trabalhar nas suas possibilidades de solução e sua relação com semigrupos numéricos. Para isso, seguem algumas atividades que podem ser aplicadas no final do ensino fundamental e no ensino médio. As principais referências para este capítulo são [13], [14], [19] e [20].

5.1 Atividades propostas

5.1.1 Atividade 1

- **Título:** Revisão de múltiplos e divisores.
- **Objetivo:** Revisar conceitos e propriedades importantes dos números inteiros.
- **Duração:** Sugerimos de duas a três aulas de 50 minutos cada.
- **Metodologia:** Exposição e explicação do conteúdo, execução e correção de exercícios. Os alunos podem trabalhar individualmente, em duplas ou em grupos.
- **Comentários:** Inicialmente, recomendamos que o professor relembre alguns conceitos e propriedades importantes dos números inteiros: múltiplos e divisores, divisibilidade, algoritmo de Euclides, mínimo múltiplo comum (mmc) e máximo divisor comum (mdc). Deixamos como referências as definições 2.7, 2.8, 2.23 e 2.9, bem como os teoremas 2.12 e 2.14. Em seguida, os alunos trabalham individualmente ou em

duplas/grupos para a resolução dos exercícios propostos abaixo. Ao final desta atividade, espera-se que os alunos sejam capazes de identificar quais ferramentas matemáticas dos números inteiros eles podem utilizar na resolução de problemas. Comentários e objetivos específicos de cada exercício podem ser encontrados na seção 5.2.

Exercício 5.1.1: Determine os dez primeiros múltiplos de 3, 8 e 12.

Exercício 5.1.2: Determine os divisores de 16, 24 e 84.

Exercício 5.1.3: Determine a decomposição em fatores primos do número 1260.

Exercício 5.1.4: Calcule o mmc de 18 e 42.

Exercício 5.1.5: Calcule o mdc de 320 e 480.

Exercício 5.1.6: Os Jogos Olímpicos, realizados a cada quatro anos, são um dos maiores eventos esportivos do mundo. Em 2016, a 31^a edição desta competição aconteceu no Brasil, na cidade do Rio de Janeiro. Com base nessas informações, determine se haverá Jogos Olímpicos em cada um dos anos abaixo:

a) 2132

b) 3754

c) 2982

d) 4576

Exercício 5.1.7: Uma escola irá realizar um campeonato esportivo com 96 alunos. Serão formados times de vôlei com 6 atletas cada, times de futsal com 7 atletas cada, e times de handebol com 8 atletas cada.

a) Em qual(is) modalidade(s) haverá sobra de alunos na formação dos times?

b) Qual a quantidade mínima de alunos que deveriam participar deste campeonato para que fosse possível montar os times sem que houvesse sobra de atletas em nenhuma modalidade?

Exercício 5.1.8: As turmas do ensino médio de uma escola serão dividas em equipes para participarem de uma gincana escolar. Cada equipe deve conter a mesma quantidade de alunos, de modo que todos os alunos sejam da mesma turma, e que não sobre nenhum aluno sem equipe. Sabendo que foram inscritos, respectivamente, 72, 48 e 54 alunos das turmas de 1^a, 2^a e 3^a séries, e que será formada a menor quantidade possível de grupos, responda:

a) Quantos alunos haverá em cada equipe?

b) Quantas equipes ao todo irão participar da gincana?

5.1.2 Atividade 2

- **Título:** Equações diofantinas: introdução.
- **Objetivo:** Introduzir equações diofantinas através de exercícios simples e situações problema.
- **Duração:** Sugerimos de duas a três aulas de 50 minutos cada.
- **Metodologia:** Apresentação de uma situação problema que esteja relacionada com equação do primeiro grau com duas incógnitas que necessite de soluções inteiras. Definição de equação diofantina linear. Execução e correção de exercícios. Os alunos podem trabalhar individualmente, em duplas ou em grupos.
- **Comentários:** O objetivo desta atividade é mostrar como as equacões diofantinas lineares surgem naturalmente até mesmo em problemas de contexto simples. O professor deverá apresentar uma situação problema que esteja relacionada com uma equação diofantina linear para que os alunos busquem os seus próprios métodos de resolução (em geral, por inspeção dos possíveis resultados pelo método da tentativa e erro). O exemplo 3.2.3 pode ser um bom motivador para o estudo deste tipo de equação. Em seguida, o professor pode brevemente definir o que são equações diofantinas lineares (deixamos como sugestão a definição 3.2.3 e os exemplos subsequentes). É importante o professor salientar que buscamos soluções inteiras para essas equações e, em alguns casos, tais soluções inteiras não podem ser negativas (por isso a abordagem inicial através de uma situação problema é interessante). Por exemplo, se estiver trabalhando com o exercício 3.2.3, apesar de os pares $\left(2, \frac{23}{5}\right)$ e $(16, -1)$ serem soluções solução da equação de primeiro grau $2x + 5y = 27$, eles não satisfazem as condições do exercício, pois não é possível o caixa dar de troco uma quantidade não inteira ou negativa de notas de cinco reais. Por fim, os alunos trabalham individualmente ou em duplas/grupos para a resolução dos exercícios propostos abaixo. Caso alguns alunos tenham dificuldade em determinar todas as soluções naturais possíveis, durante a correção o professor deverá incentivá-los a encontrar mais soluções antes da apresentação de todas. Ao final da correção das atividades, é interessante conversar com os alunos sobre a eficácia e eficiência do método de resolução de equações diofantinas por tentativa e erro, e informar que na próxima aula irão estudar outra técnica de resolução. Ao final desta atividade, espera-se que os alunos sejam capazes de utilizar equações diofantinas para modelar algumas situações problemas, bem como buscar soluções inteiras (ou apenas naturais) para elas. Comentários e objetivos específicos de cada exercício podem ser encontrados na seção 5.2.

Exercício 5.1.9: Determine algumas soluções inteiras para as equações diofantinas abaixo:

a) $4x + 6y = 78$

b) $5x + 9y = 93$

c) $6x + 9y = 96$

d) $6x + 8y = 82$

Exercício 5.1.10: A equação $8x + 12y = 95$ admite souções inteiras? Justifique sua resposta.

Exercício 5.1.11: Uma sorveteria vende picolés de sabores simples por R$2,00 e picolés de sabores especiais por R$3,00. Sabendo que Laura foi a esta sorveteria com R$15,00 e pretende gastar todo esse dinheiro, responda:

a) Quais são as possibilidades de compras que Laura pode fazer?

b) Represente esta situação através de uma equação.

Exercício 5.1.12: Pedro possui passarinhos e cachorros como animais de estimação. Se o número total de patas desses animais é 14, responda:

a) Quais são as possibilidades para a quantidade de passarinhos e cachorros que Pedro pode ter?

b) Represente esta situação através de uma equação.

Exercício 5.1.13: Em uma lanchonete são vendidas fatias de tortas salgadas no valor de R$6,00 e fatias de tortas doces por R$8,00. Sabendo que Marcela foi a esta lanchonete com R$60,00 e pretende gastar todo esse dinheiro, responda:

a) Quais são as possibilidades de compras que Marcela pode fazer?

b) Represente esta situação através de uma equação.

Exercício 5.1.14: Em uma praça, crianças brincam com skates e bicicletas. Sabendo que cada criança brinca com apenas um desses brinquedos, responda:

a) Se há ao todo 18 rodas, quais são as possibilidades de quantidade de skates e bicicletas?

b) Represente a situação do item a) através de uma equação.

c) É possível haver, ao todo, 15 rodas? Justifique sua resposta.

d) Represente a situação do item c) através de uma equação.

5.1.3 Atividade 3

- **Título:** Equações diofantinas: desenvolvimento.
- **Objetivo:** Apresentar o método de resolução de equações diofantinas através do algoritmo de Euclides. Definir e relacionar semigrupos numéricos com soluções naturais de equações diofantinas lineares. Identificar soluções inteiras e naturais de equações diofantinas no software GeoGebra, bem como determinar alguns elementos dos semigrupos associados.
- **Duração:** Sugerimos de três a cinco aulas de 50 minutos cada.
- **Metodologia:** Exposição e explicação do conteúdo, execução e correção de exercícios. Os alunos podem trabalhar individualmente, em duplas ou em grupos.
- **Comentários:** Neste momento, o professor deverá trabalhar a resolução de equações diofantinas utilizando o algoritmo de Euclides, bem como esclarecer como verificar se uma equação possui solução ou não, além de definir e relacionar semigrupos numéricos com as soluções naturais de equações diofantinas. Deixamos como sugestão de referências as proposições 2.28, 2.30, 3.8 e 3.13, bem como os corolários 3.9 e 3.10, e o teorema 3.11. Em seguida, os alunos trabalham individualmente ou em duplas/grupos para a resolução dos exercícios propostos abaixo. Ao final desta atividade, espera-se que os alunos sejam capazes de utilizar o algoritmo de Euclides para encontrar as soluções gerais de uma equação diofantina linear, bem como possam utilizar semigrupos numéricos e suas propriedades na determinação de soluções naturais destas equações e saibam como identificá-las em sua representação geométrica no software GeoGebra. Comentários e objetivos específicos de cada exercício podem ser encontrados na seção 5.2.

Observação 5.1: Ensinaremos aqui como representar equações diofantinas lineares no GeoGebra. O software é gratuito e pode ser baixado no site https://www.geogebra.org/ ou acessado online em https://www.geogebra.org/classic?lang=pt_BR. Abaixo, podemos visualizar a imagem do ambiente do GeoGebra. Caso os eixos coordenados e a malha não estejam aparecendo, basta clicar com o botão direito do mouse e selecionar as opções "Exibir eixos" e "Exibir malha". Eles facilitarão na busca e identificação de soluções inteiras das equações.

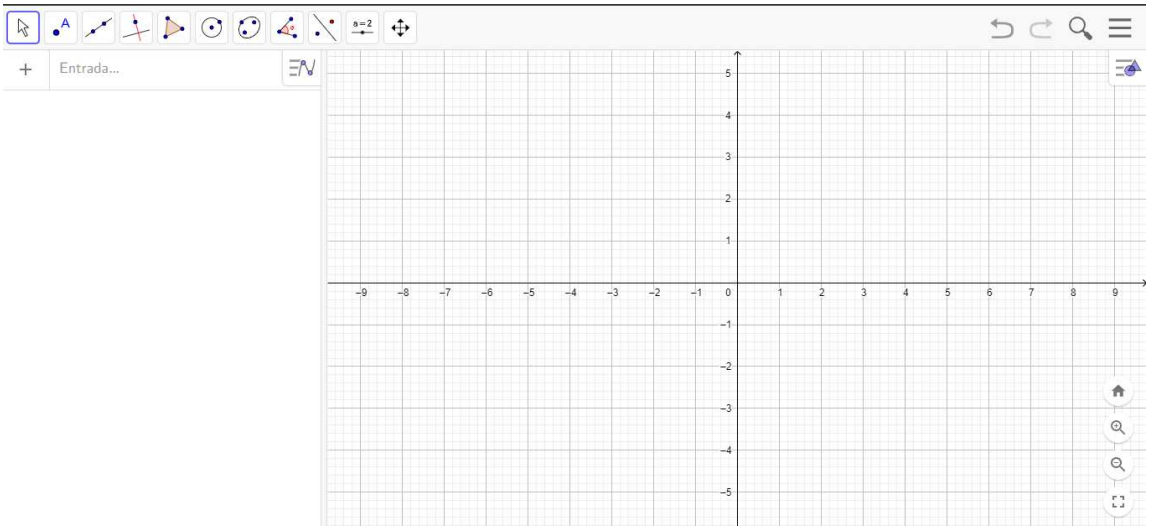

Figura 5.1: Ambiente do GeoGebra.

Na região onde está escrito "Entrada...", digitamos a equação que desejamos representar. Abaixo, ilustramos a equação $3x + 5y = 16$. Note que a malha facilita na identificação da solução inteira $x = 2$ e $y = 2$ (recomendamos marcar este ponto no gráfico usando a ferramenta "Ponto" no segundo ícone no canto superior esquerdo). Para melhorar a visualização da reta, é possível clicar no último ícone no canto superior esquerdo e selecionar "Mover Janela de Visualização", e também "Ampliar" e "Reduzir" o zoom.

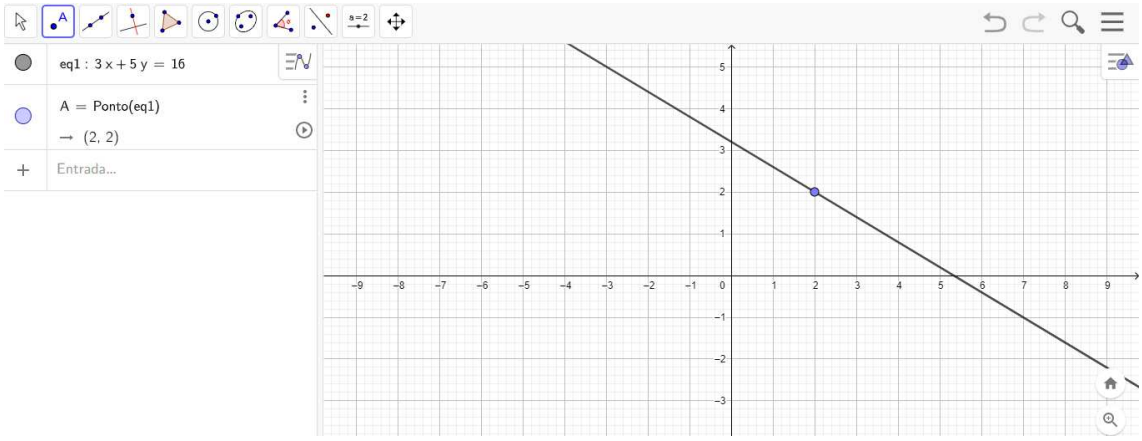

Figura 5.2: Representação da equação $3x + 5y = 16$. O ponto destaca a solução natural $x = 2$ e $y = 2$.

Vamos agora construir uma equação diofantina linear utilizando a ferramenta "Controle Deslizante", disponível no penúltimo ícone do canto superior esquerdo. Primeirante, selecionamos a opção "Controle Deslizante" e clicamos em um ponto qualquer da Janela de Visualização, e então abrirá uma janela de opções (conforme ilustrado na figura abaixo). Colocamos um nome (sugerimos a letra c, que já aparece nos exercícios), marcamos a opção "Inteiro" e definimos um valor mínimo (sugerimos o 1), um valor máximo (dependerá de acordo com o exercício), o incremento (deverá ser 1) e clicamos em OK.

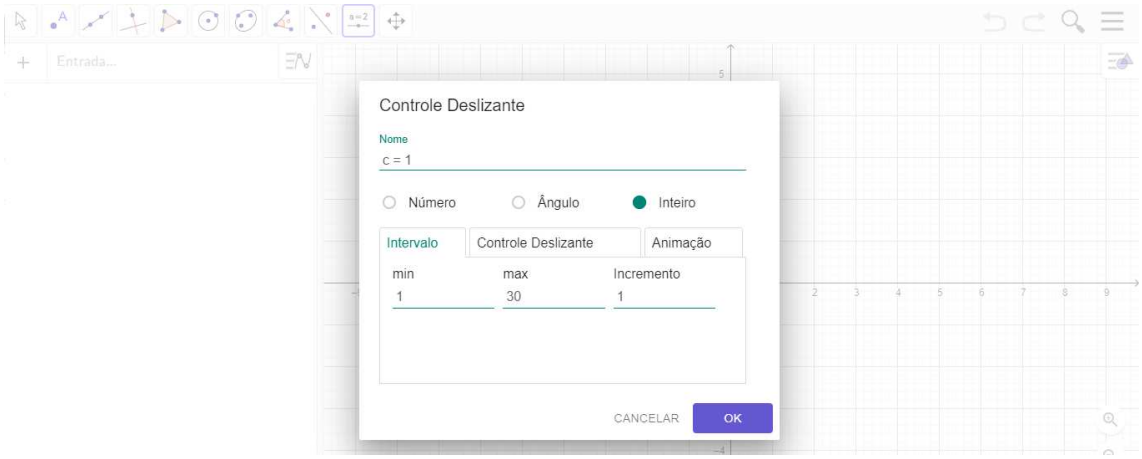

Figura 5.3: Janela de opções do Controle Deslizante.

Em seguida, no local onde está escrito "Entrada...", digitamos a equação que desejamos representar. Abaixo, ilustramos a equação $3x + 5y = c$. Note que ao movermos o Controle Deslizante, a equação varia, e podemos identificar aquelas que possuem soluções inteiras ou não.

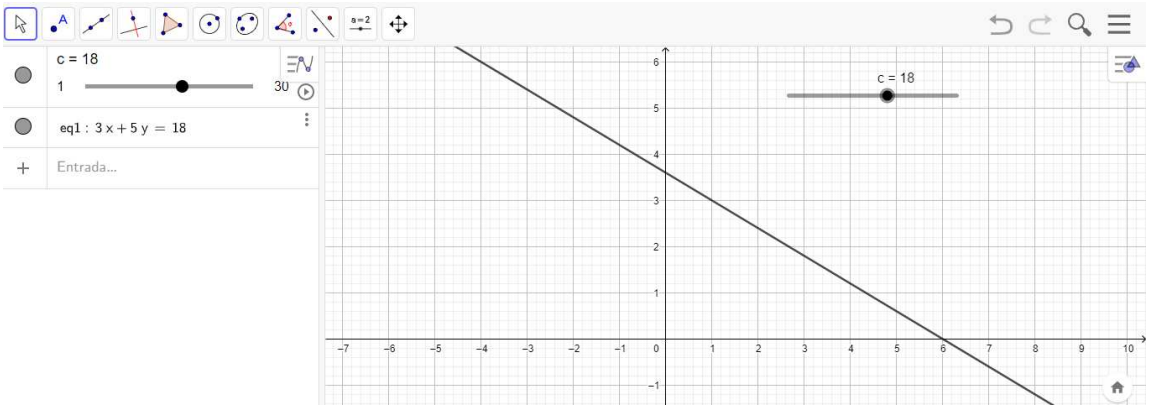

Figura 5.4: Reta da equação $3x + 5y = c$, com Controle Deslizante $c = 18$.

Exercício 5.1.15: Verifique se as equações diofantinas abaixo possuem soluções inteiras. Em caso afirmativo, determine-as e localize pelo menos uma delas no GeoGebra:

a) $45x + 14y = 11$

b) $3x + 6y = 22$

c) $24x - 39y = 75$

d) $30x + 58y = 108$

e) $104x + 56y = 234$

Exercício 5.1.16: Qual o menor valor inteiro de c a partir do qual a equação diofantina $5x + 9y = c$ sempre admite soluções naturais? Represente esta equação no GeoGebra e verifique sua resposta. Para isso, crie a equação $5x + 9y = c$, sendo c um controle deslizante

inteiro com valor mínimo 1, máximo 40 e incremento 1. Mova o controle deslizante e analise a reta formada pela equação e sua interseção com os eixos Ox, Oy e a malha do GeoGebra.

Exercício 5.1.17: Utilizando o GeoGebra, determine valores inteiros positivos de c para os quais a equação $8x+5y=c$ admita soluções naturais. Para isso, crie a equação $8x+5y=c$, sendo c um controle deslizante inteiro com valor mínimo 1, máximo 35 e incremento 1. Mova o controle deslizante e analise a reta formada pela equação e sua interseção com os eixos Ox, Oy e a malha do GeoGebra.

Exercício 5.1.18: Utilizando o GeoGebra, resolva cada item abaixo:

a) Aplicando o método de tentativa e erro, verifique se a equação $7x+13y=32$ admite solução natural. Em seguida, represente essa equação no GeoGebra e confirme sua resposta.

b) Determine valores naturais de c para os quais a equação $7x+13y=c$ admita soluções naturais. Para isso, crie a equação $7x+13y=c$, sendo c um controle deslizante inteiro com valor mínimo 1, máximo 75 e incremento 1. Mova o controle deslizante e analise a reta formada pela equação e sua interseção com os eixos Ox, Oy e a malha do GeoGebra.

c) Determine as soluções naturais da equação $7x+13y=300$. Em seguida, localize-as no GeoGebra.

Exercício 5.1.19: Suponha que em uma determinada cidade, as cédulas sejam apenas de \$7 e \$10. A partir de qual valor é sempre possível pagar, sem troco, qualquer quantia inteira? Utilizando o controle deslizante, escreva no GeoGebra uma equação diofantina linear que represente esta situação e verifique sua resposta.

Exercício 5.1.20: Em um caixa eletrônico há apenas cédulas de R\$20 e de R\$50, e uma uma pessoa deseja fazer um saque de 430 reais. Escreva e resolva uma equação diofantina que represente esta situação, determinando quais são as maneiras possíveis de o caixa eletrônico liberar o dinheiro. Em seguida, represente esta equação no GeoGebra e identifique as soluções que encontrou.

Exercício 5.1.21: Uma rede de fast food vende empanados de frango em embalagens com 5 e 12 unidades. Responda os itens abaixo e represente cada situação no GeoGebra através de uma equação diofantina linear. Utilize o controle deslizante quando necessário e verifique todas as suas respostas:

a) A partir de qual quantidade será sempre possível comprar uma quantia inteira desses empanados?

b) É possível comprar exatamente 38 empanados?

c) Determine outras quantidades de empanados que não é possível comprar nesta rede de fast food.

d) De quais maneiras uma pessoa poderá comprar 162 empanados?

5.2 Comentários e soluções dos exercícios propostos

5.2.1 Resolução da Atividade 1

Solução: Exercício 5.1.1:

O objetivo deste exercício é revisar múltiplos de um inteiro. Uma maneira simples de resolvê-lo é multiplicando o inteiro em questão por 0, 1, 2, 3, ..., 9.

Os dez primeiros múltiplos de 3 são:
M(3) = {0, 3, 6, 9, 12, 15, 18, 21, 24, 27}.
Os dez primeiros múltiplos de 8 são:
M(8) = {0, 8, 16, 24, 32, 40, 48, 56, 64, 72}.
Os dez primeiros múltiplos de 12 são:
M(12) = {0, 12, 24, 36, 48, 60, 72, 84, 96, 108}.

Solução: Exercício 5.1.2:

O objetivo deste exercício é revisar divisores de um inteiro. O professor pode aproveitar este momento para relembrar alguns critérios de divisibilidade.

Os divisores de 16 são:
D(16) = {1, 2, 4, 8, 16}.
Os divisores de 24 são:
D(24) = {1, 2, 3, 4, 6, 8, 12, 24}.
Os divisores de 42 são:
D(42) = {1, 2, 3, 6, 7, 14, 21, 42}.

Solução: Exercício 5.1.3:

O objetivo deste exercício é revisar a decomposição de um número em fatores primos. Para tanto, o aluno pode efetuar o processo de fatoração usual. O professor pode relembrar aos alunos que a ordem dos fatores na fatoração não altera o número em questão devido a unicidade da decomposição em fatores primos.

1260	2
630	2
315	3
105	3
35	5
7	7
1	

Portanto, a decomposição em fatores primos de 1260 é

$$1260 = 2^2.3^2.5.7.$$

Solução: Exercício 5.1.4:

O objetivo deste exercício é revisar o cálculo do mmc entre dois números. Uma maneira simples de resolvê-lo é através da fatoração simultânea:

18, 42	2
9, 21	3
3, 7	3
1, 7	7
1, 1	

Portanto, o mmc de 18 e 42 é $2.3^2.7 = 126$.

Solução: Exercício 5.1.5:

O objetivo deste exercício é revisar o cálculo do mdc entre dois números. Uma maneira simples de resolvê-lo é através da fatoração simultânea:

320, 480	2	divisor comum
160, 240	2	divisor comum
80, 120	2	divisor comum
40, 60	2	divisor comum
20, 30	2	divisor comum
10, 15	2	
5, 15	3	
5, 5	5	divisor comum
1, 1		

Portanto, o mdc de 320 e 480 é $2^5.5 = 160$.

Solução: Exercício 5.1.6:

O objetivo deste exercício é trabalhar a ideia de múltiplo de um inteiro em um problema contextualizado. Usando a informação de que os Jogos Olímpicos acontecem a cada quatro anos e sendo 2016 um múltiplo de 4, os alunos devem concluir que os anos em que acontecerão os Jogos Olímpicos serão aqueles que são múltiplos de 4. Para este exercício, apenas os anos 2132 e 4576 são múltiplos de 4 e, portanto, serão anos de Jogos Olímpicos:

$$2132 = 533.4$$
$$3754 = 938.4 + 2$$
$$2982 = 745.4 + 2$$
$$4576 = 1144.4$$

Os alunos podem verificar tal fato utilizando a divisão euclidiana, e o professor também pode aproveitar o exercício para relembrar o critério de divisibilidade por 4, estudado no sexto ano.

Solução: Exercício 5.1.7:

O objetivo do item a) é trabalhar a ideia de divisor de um inteiro. O aluno deve concluir que só haverá sobras na formação dos times para as modalidades em que a quantidade de

atletas por time não for um divisor de 96. Como $96 = 16.6$, $96 = 13.7 + 5$ e $96 = 12.8$, segue que haverá sobra de atletas apenas nos times com 7 pessoas, ou seja, nos times de futsal.

Já o item b) explora a ideia de mmc: para que não haja sobra de atletas na formação dos times, a quantidade total de participantes no campeonato deve ser um múltiplo comum de 6, 7 e 8. Como o enunciado pergunta a quantidade mínima de alunos, buscamos o mmc desses três números:

6, 7, 8	2
3, 7, 4	2
3, 7, 2	2
3, 7, 1	3
1, 7, 1	7
1, 1, 1	

Desse modo, o mmc de 6, 7 e 8 é $2^3.3.7 = 168$. Portanto, 168 é a menor quantidade de alunos que deveriam participar deste campeonato para que não houvesse sobra de atletas na formação dos times. É importante salientar com os alunos que isto não significa que qualquer quantidade maior que 168 irá garantir que não haja sobra de atletas.

Solução: Exercício 5.1.8:

O objetivo deste exercício é trabalhar a ideia de mdc em um problema contextualizado. Para que cada equipe tenha a mesma quantidade de alunos de uma mesma turma sem que haja sobras, é necessário que a quantidade de alunos por equipe seja um divisor comum de 48, 54 e 72. Para que a quantidade de equipes seja a menor possível, esse divisor deve ser o maior possível, ou seja, o mdc dos três números:

48, 54, 72	2	divisor comum
24, 27, 36	2	
12, 27, 18	2	
6, 27, 9	2	
3, 27, 9	3	divisor comum
1, 9, 3	3	
1, 3, 1	3	
1, 1, 1		

Portanto, o mdc de 48, 54 e 72 é $2.3 = 6$. Desse modo, cada equipe deve ter 6 alunos.
Para o item b), basta calcular a quantidade de equipes de cada série e depois somá-las:
Para as turmas da 1^a série, serão formadas

$72 : 6 = 12$ equipes.

Para as turmas da 2^a série, serão formadas

$48 : 6 = 8$ equipes.

Para as turmas da 3^a série, serão formadas

$$54 : 6 = 9 \text{ equipes.}$$

Portanto, participarão da gincana

$$12 + 8 + 9 = 29 \text{ equipes.}$$

5.2.2 Resolução da Atividade 2

Solução: Exercício 5.1.9:

O objetivo deste exercício é que os alunos busquem soluções inteiras para as equações diofantinas pelo método de tentativa e erro. É interessante o professor pedir aos alunos que comentem quais foram os caminhos que utilizaram para chegar nas soluções que encontraram.

Para o item a), algumas possíveis soluções são $x_1 = 18$ e $y_1 = 1$, $x_2 = 0$ e $y_2 = 13$, $x_3 = 3$ e $y_3 = 11$, $x_4 = -3$ e $y_4 = 15$ e $x_5 = 21$ e $y_5 = -1$.

Para o item b), algumas possíveis soluções são $x_1 = 6$ e $y_1 = 7$, $x_2 = 15$ e $y_2 = 2$, $x_3 = 24$ e $y_3 = -3$ e $x_4 = -3$ e $y_4 = 12$.

Para o item c), algumas possíveis soluções são $x_1 = 16$ e $y_1 = 0$, $x_2 = 1$ e $y_2 = 10$, $x_3 = -2$ e $y_3 = 12$ e $x_4 = 19$ e $y_4 = -2$.

Para o item d), algumas possíveis soluções são $x_1 = 3$ e $y_1 = 8$, $x_2 = 11$ e $y_2 = 2$, $x_3 = -1$ e $y_3 = 11$ e $x_4 = 15$ e $y_4 = -1$.

Solução: Exercício 5.1.10:

O objetivo deste exercício é que os alunos busquem, inicialmente, uma solução por tentativa e erro. Após notarem que não encontraram tal solução, deverão chegar à conclusão de que ela não é possível, pois a soma de dois números pares resulta em um número par. Caso os alunos não cheguem a essa conclusão sozinhos, o professor poderá guiá-los analisando a paridade de alguns resultados particulares dos produtos $8x$ e $12y$, bem como de sua soma.

Solução: Exercício 5.1.11:

Laura pode comprar cinco picolés de sabor especial, ou três picolés de sabor simples e três de sabor especial, ou ainda seis picolés de sabor simples e apenas um de sabor especial. Uma possível equação que representa esta situação é

$$2x + 3y = 15,$$

em que x representa a quantidade de picolés de sabor simples e y representa a quantidade de picolés de sabor especial.

Solução: Exercício 5.1.12:

Pedro pode ter um pássaro e três cachorros, ou três pássaros e dois cachorros, ou ainda cinco pássaros e apenas um cachorro. Para este exercício é interessante comentar que a solução "Pedro possui sete pássaros e nenhum cachorro" não satisfaz o enunciado que

afirma que Pedro possui pasarinhos e cachorros. Uma possível equação que representa esta situação é

$$2x + 4y = 14,$$

em que x representa a quantidade de passarinhos e y representa a quantidade de cachorros.

Solução: Exercício 5.1.13:

Marcela pode comprar dez fatias de torta salgada, ou duas fatias de torta salgada e seis de torta doce, ou ainda seis fatias de torta salgada e três de torta doce. Uma possível equação que representa esta situação é

$$6x + 8y = 60,$$

em que x representa a quantidade de fatias de torta salgada e y representa a quantidade de fatias de torta doce.

Solução: Exercício 5.1.14:

Para os itens a) e b) é possível que haja uma bicicleta e quatro skates, três bicicletas e três skates, cinco bicicletas e dois skates, ou ainda sete bicicletas e um skate. Uma possível equação que representa essa situação é

$$2x + 4y = 18,$$

em que x é a quantidade de bicicletas e y é a quantidade de skates.

Para os itens c) e d), é provável que alguns alunos tenham chegado à conclusão de que não é possível haver 15 rodas testando as possíveis quantidades de bicicletas e skates. É importante o professor comentar que não é necessário utilizar o método de tentativa e erro neste exercício, pois o número total de rodas deve ser um número par, já que a quantidade de rodas do skate e da bicicleta são números pares, e a soma de números pares resulta em um número par. O professor também deve mencionar que na aula seguinte estudarão uma outra maneira de verificar se uma equação diofantina possui ou não solução. Uma possível equação que representa esta situação é

$$2x + 4y = 15.$$

em que x é a quantidade de bicicletas e y é a quantidade de skates.

5.2.3 Resolução da Atividade 3

Solução: Exercício 5.1.15:

O objetivo deste exercício é verificar a existência de soluções inteiras de uma equação diofantina linear, bem como determiná-las utilizando o algoritmo de Euclides e localizar algumas delas no GeoGebra.

Item a): Como $(45,\ 14) = 1$, a equação admite soluções inteiras. Pelo algoritmo de

Euclides, temos:

$$45 = 3.14 + 3,$$
$$14 = 4.3 + 2,$$
$$3 = 1.2 + 1.$$

Substituindo as equações acima umas nas outras, obtemos

$$1 = 45.5 + 14.(-16).$$

Multiplicando esta última igualdade por 11, segue que

$$11 = 45.55 + 14.(-176),$$

mostrando que $x_0 = 55$ e $y_0 = -176$ é solução particular da equação diofantina e, portanto, as soluções inteiras são

$$x = 55 + 14t, \quad y = -176 - 45t, \quad \text{com } t \in \mathbb{Z}.$$

Ilustramos abaixo a solução $x = -1$ e $y = 4$ (quando $t = -4$):

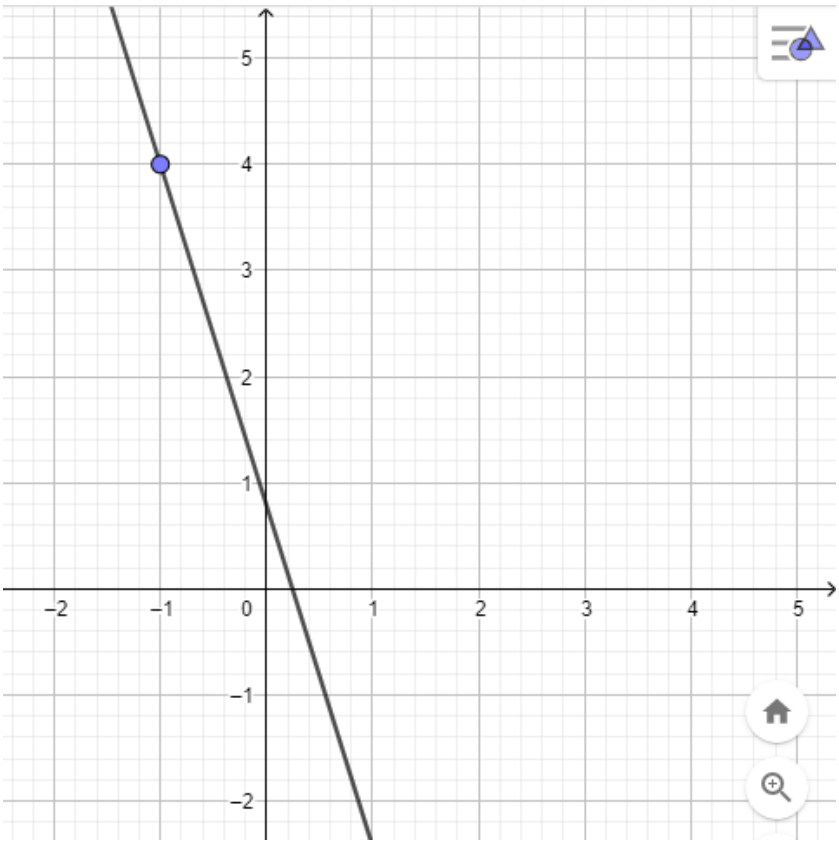

Figura 5.5: Reta da equação $45x + 14y = 11$. Note que $x = -1$ e $y = 4$ é solução inteira da equação.

Item b): Como $(3,\ 6) = 3$ e $3 \nmid 22$, a equação diofantina não admite soluções inteiras.

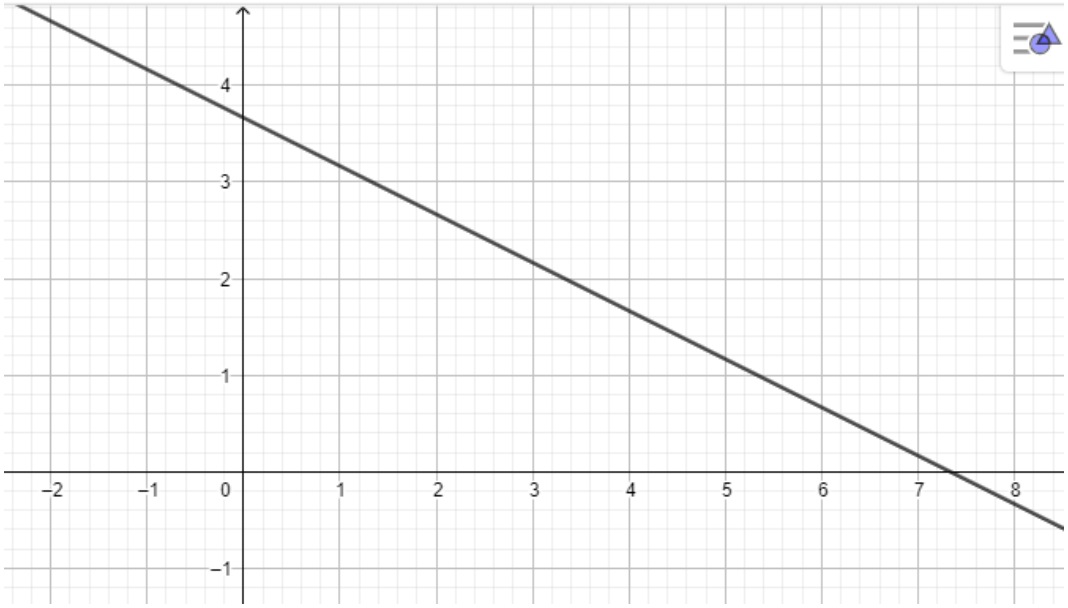

Figura 5.6: Reta da equação $3x + 6y = 22$. A equação não possui soluções inteiras. Apenas parte da representação é mostrada na imagem.

Item c): Como $(24,\ 39) = 3$ e $3 \mid 75$, a equação admite soluções inteiras. Dividindo ambos os membros da equação por 3, obtemos a equação equivalente

$$8x - 13y = 25.$$

Pelo algoritmo de Euclides, temos:

$$\begin{aligned} 13 &= 1.8 + 5, \\ 8 &= 1.5 + 3, \\ 5 &= 1.3 + 2, \\ 3 &= 1.2 + 1. \end{aligned}$$

Substituindo as equações acima umas nas outras, obtemos

$$1 = 8.5 - 13.3.$$

Multiplicando esta última igualdade por 25, segue que

$$25 = 8.125 - 13.175,$$

mostrando que $x_0 = 125$ e $y_0 = 75$ é solução particular da equação diofantina e, portanto, as soluções inteiras são

$$x = 125 - 13t, \quad y = 75 - 8t, \quad \text{com } t \in \mathbb{Z}.$$

Ilustramos abaixo a solução $x = 8$ e $y = 3$ (quando $t = 9$):

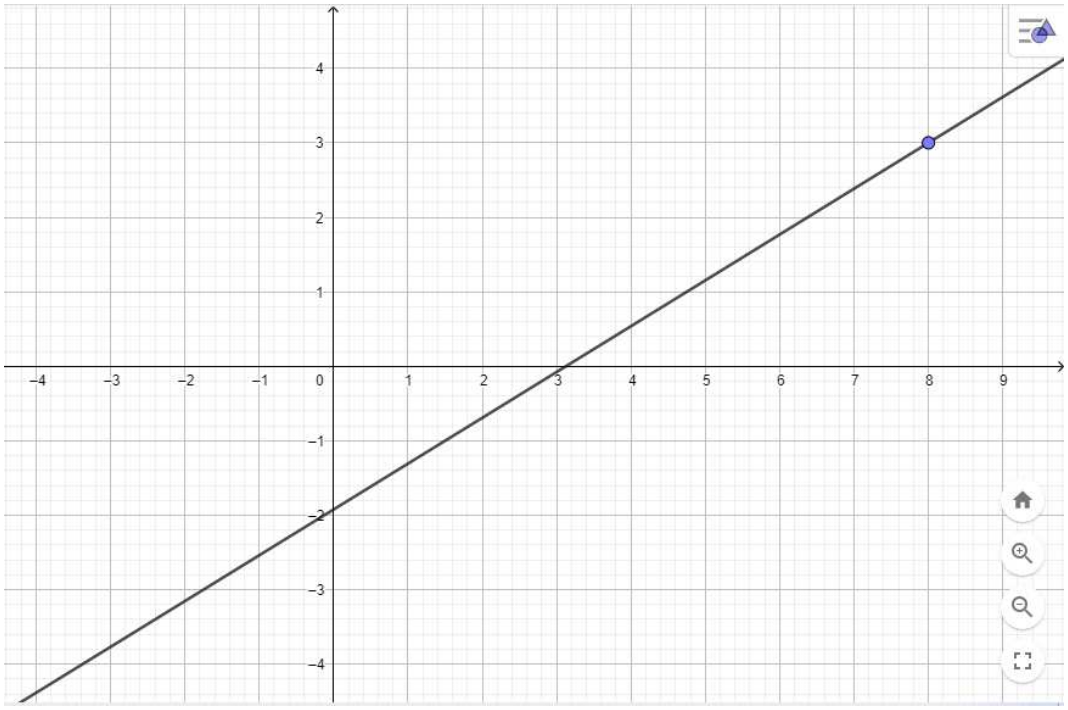

Figura 5.7: Reta da equação $24x - 39y = 75$. Note que $x = 8$ e $y = 3$ é solução inteira da equação.

Item d): Como $(30,\ 58) = 2$ e $2 \mid 108$, a equação admite soluções inteiras. Dividindo ambos os membros da equação por 2, obtemos a equação equivalente $15x + 29y = 54$. Pelo algoritmo de Euclides, temos:

$$29 = 1.15 + 14,$$
$$15 = 1.14 + 1.$$

Substituindo a primera equação acima na segunda, obtemos

$$1 = 15.2 + 29.(-1).$$

Multiplicando esta última igualdade por 54, segue que

$$54 = 15.108 + 29.(-54),$$

mostrando que $x_0 = 108$ e $y_0 = -54$ é solução particular da equação diofantina e, portanto, as soluções inteiras são

$$x = 108 + 29t, \quad y = -54 - 15t, \quad \text{com } t \in \mathbb{Z}.$$

Ilustramos abaixo a solução $x = -8$ e $y = 6$ (quando $t = -4$):

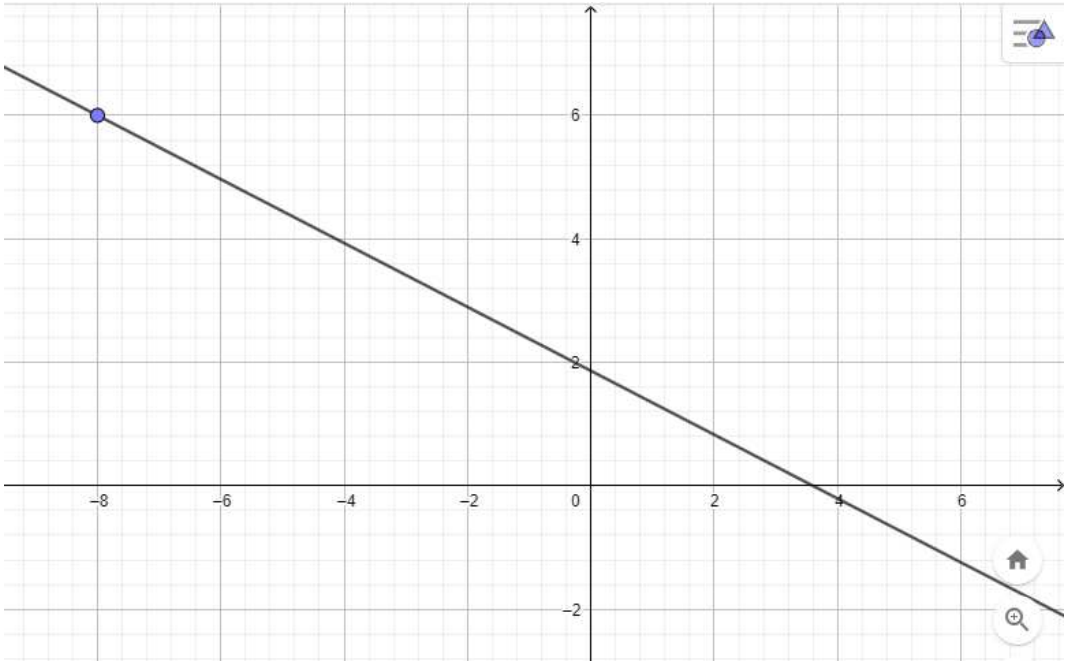

Figura 5.8: Reta da equação $30x + 58y = 108$. Note que $x = -8$ e $y = 6$ é solução inteira da equação.

Item e): Como $(104,\ 56) = 8$ e $8 \nmid 234$, a equação diofantina não admite soluções inteiras.

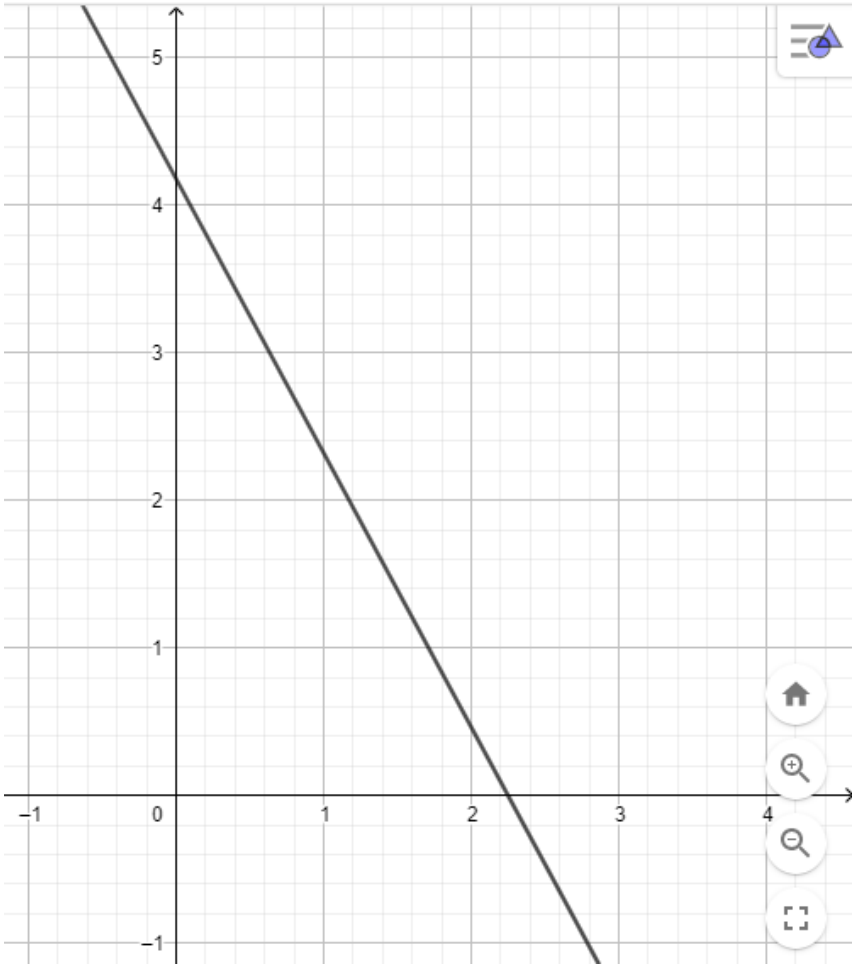

Figura 5.9: Reta da equação $104x + 56y = 234$. A equação não possui soluções inteiras. Apenas parte da representação é mostrada na imagem.

Solução: Exercício 5.1.16:

O objetivo deste exercício é verificar a compreensão do conceito e do cálculo do condutor de um semigrupo. O semigrupo S associado à equação $5x + 9y = c$ é $S = \langle 5,\ 9\rangle$. O corolário 3.10 nos diz que o condutor β é dado por

$$\beta = (5-1).(9-1) = 4.8 = 32.$$

Portanto, para qualquer inteiro $c \geq 32$, a equação $5x + 9y = c$ admite soluções naturais.

É importante comentar com os alunos que existem alguns inteiros $c < 32$ tais que a equação $5x + 9y = c$ também admite soluções naturais; 32 é número a partir do qual a equação sempre terá soluções. Estimule os estudantes a encontrar, utilizando o GeoGebra, outros valores de c (menores do que 32) para os quais a equação admita solução natural. Abaixo, ilustramos uma situação como esta e outra em que a equação não admite solução inteira positiva:

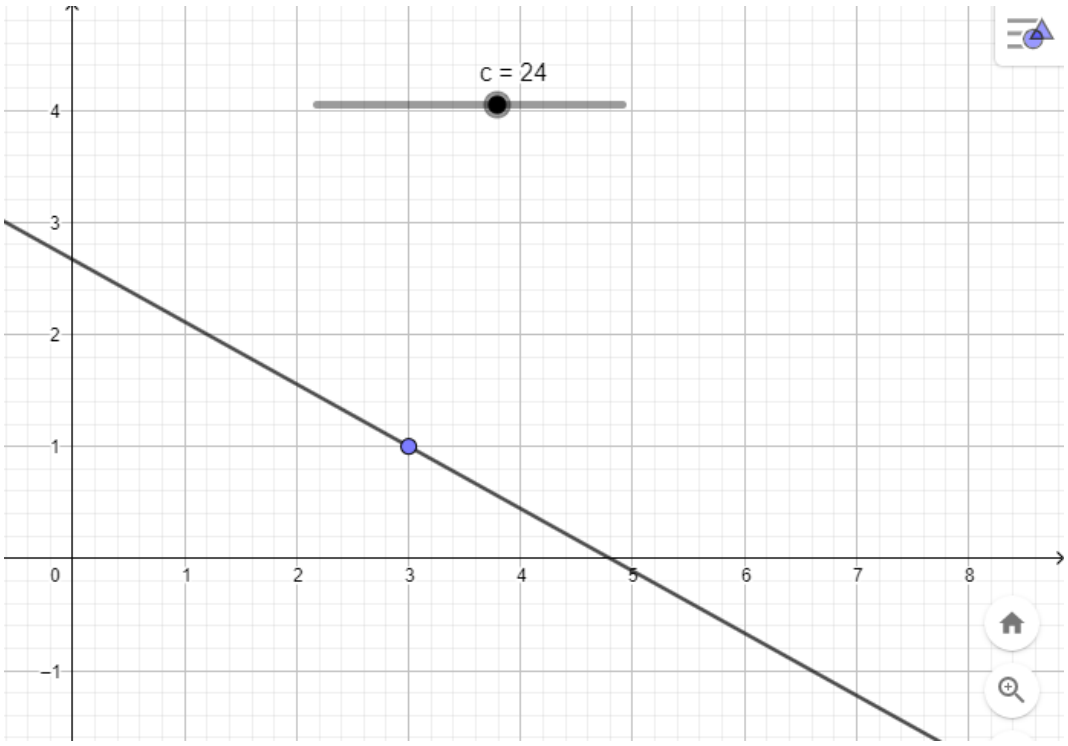

Figura 5.10: Reta da equação $5x + 9y = c$ para $c = 24$. Note que $x = 3$ e $y = 1$ é solução natural da equação.

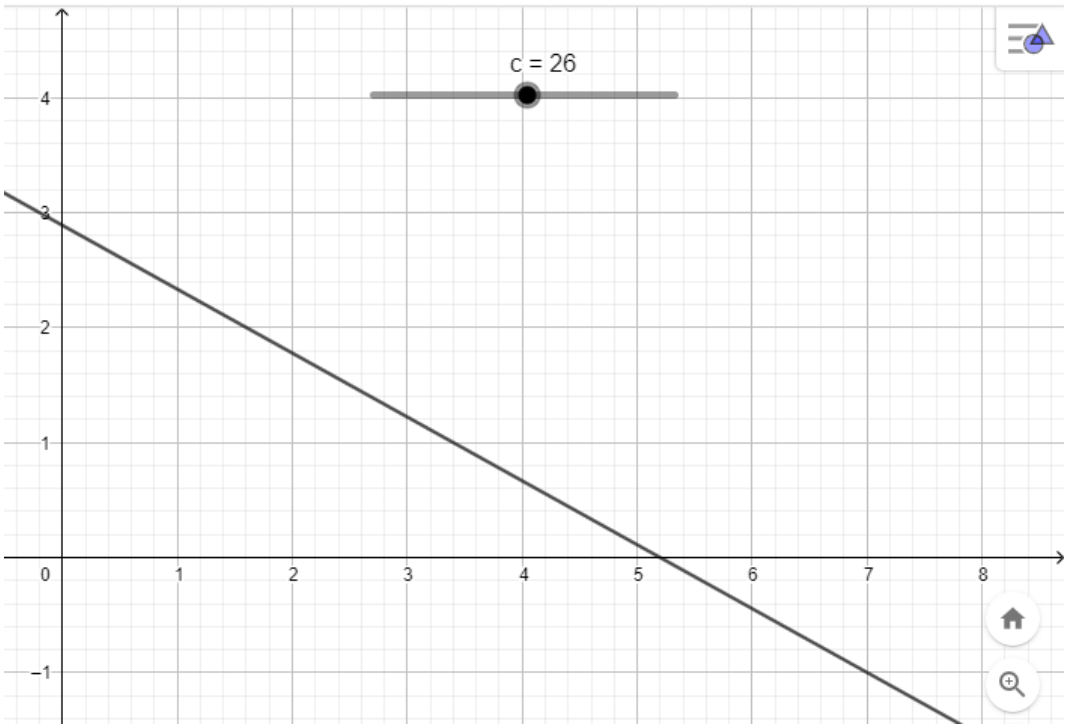

Figura 5.11: Reta da equação $5x + 9y = c$ para $c = 26$. Note que esta equação não possui solução natural.

Solução: Exercício 5.1.17: O objetivo deste exercício é identificar no GeoGebra soluções naturais de uma equação diofantina linear movendo o controle deslizante e analisando a

interseção da reta que representa a equação com os eixos coordenados e com a malha do GeoGebra. Recordamos que uma equação $ax + by = c$ só admitirá soluções naturais se c não for lacuna do semigrupo associado. Na figura abaixo representamos uma equação que possui solução inteira positiva:

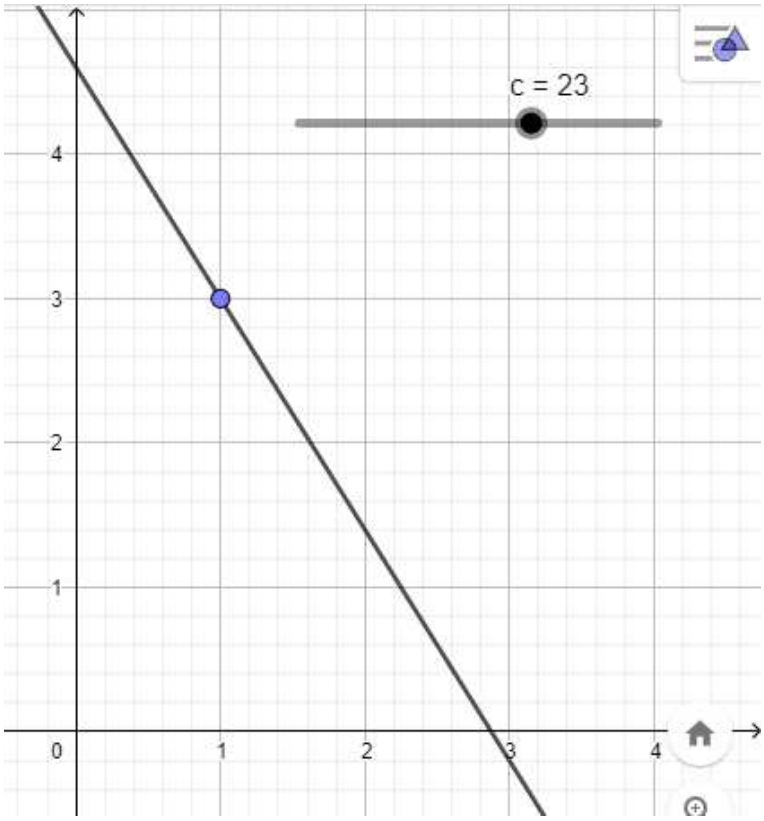

Figura 5.12: Reta da equação $8x + 5y = c$ para $c = 23$. Note $x = 1$ e $y = 3$ é solução natural da equação.

Abaixo ilustramos a situação em que foi determinada a lacuna 17 e, portanto, a equação não admite solução natural:

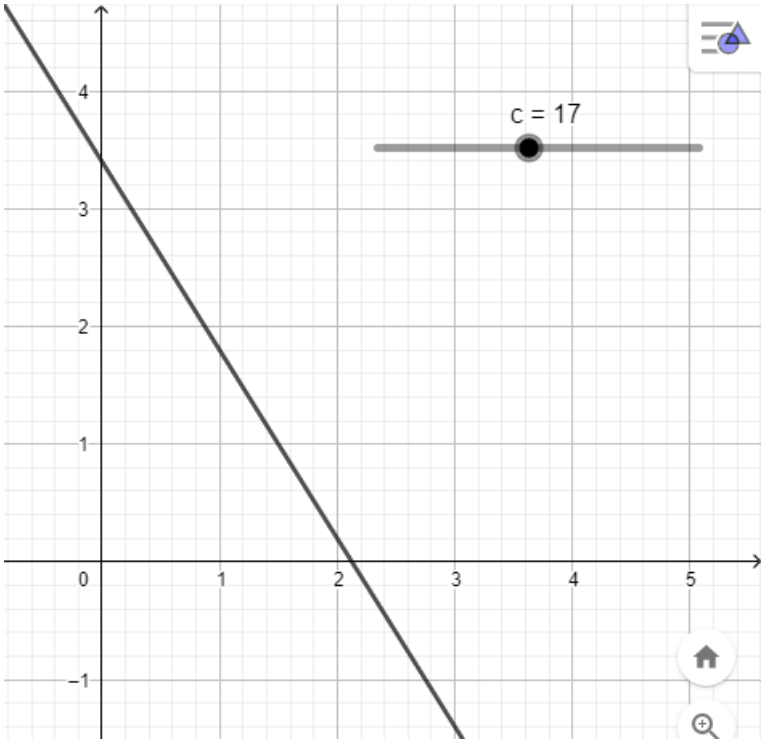

Figura 5.13: Reta da equação $8x + 5y = c$ para $c = 17$. Note que esta equação não possui solução natural.

O semigrupo associado à equação $8x+5y = c$ é $S = \langle 8,\ 5\rangle$ e, de acordo com o corolário 3.9, o conjunto das lacunas de S é

$$\mathbb{N} \setminus S = \{8m - 5n \in \mathbb{N} \mid m,\ n \in \mathbb{N},\ m < 5\}.$$

Para $m = 1$, temos que $8.1 - 5n \in \mathbb{N}$ se $n = 1$. Logo, 3 é lacuna de S.

Para $m = 2$, temos que $8.2 - 5n \in \mathbb{N}$ para $n = 1$, $n = 2$ e $n = 3$. Logo, 11, 6 e 1 são lacunas de S.

Para $m = 3$, temos que $8.3 - 5n \in \mathbb{N}$ para $n = 1$, $n = 2$, $n = 3$ e $n = 4$. Logo, 19, 14, 9 e 4 são lacunas de S.

Para $m = 4$, temos que $8.4 - 5n \in \mathbb{N}$ para $n = 1$, $n = 2$, $n = 3$, $n = 4$, $n = 5$ e $n = 6$. Logo, 27, 22, 17, 12, 7 e 2 são lacunas de S.

Desse modo, segue que

$$\mathbb{N} \setminus S = \{1,\ 2,\ 3,\ 4,\ 6,\ 7,\ 9,\ 11,\ 12,\ 14,\ 17,\ 19,\ 22,\ 27\}.$$

Portanto, a equação $8x + 5y = c$ admite soluções naturais para todo c natural tal que

$$c \notin \{1,\ 2,\ 3,\ 4,\ 6,\ 7,\ 9,\ 11,\ 12,\ 14,\ 17,\ 19,\ 22,\ 27\}.$$

Solução: Exercício 5.1.18:

O objetivo do item a) é que o aluno busque alguma solução pelo método de tentativa e erro e chegue a hipótese de que tal solução não existe. Em seguida, deverá utilizar o GeoGebra para comprovar sua hipótese. Abaixo ilustramos a representação da equação

$7x + 13y = 32$. É importante que o professor diga aos alunos para observar a reta em todo o primeiro quadrante (região onde estarão as soluções naturais, caso existam).

Figura 5.14: Reta da equação $7x + 13y = 32$. Note que esta equação não possui solução natural.

O objetivo do item b) é que o aluno saiba identificar no GeoGebra soluções naturais de uma equação diofantina linear movendo o controle deslizante e analisando a interseção da reta que representa a equação com os eixos coordenados e com a malha do GeoGebra. Abaixo ilustramos uma equação que possui solução inteira positiva:

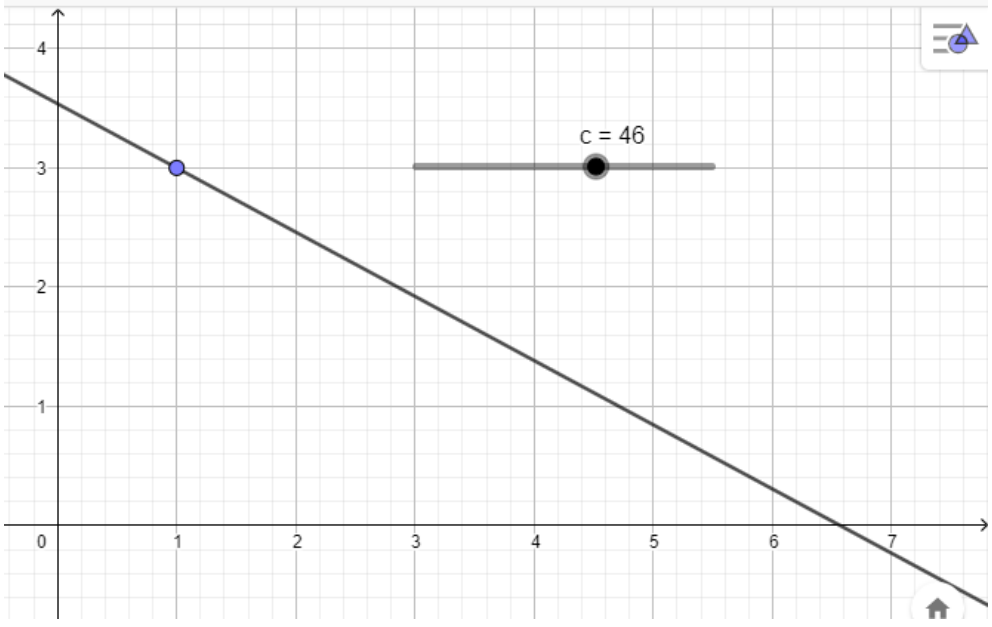

Figura 5.15: Reta da equação $7x + 13y = c$ com $c = 46$. Note que $x = 1$ e $y = 3$ é solução natural desta equação.

Na imagem abaixo, está representada uma equação que não possui solução natural, uma vez que c assumiu o valor de uma lacuna do semigrupo associado:

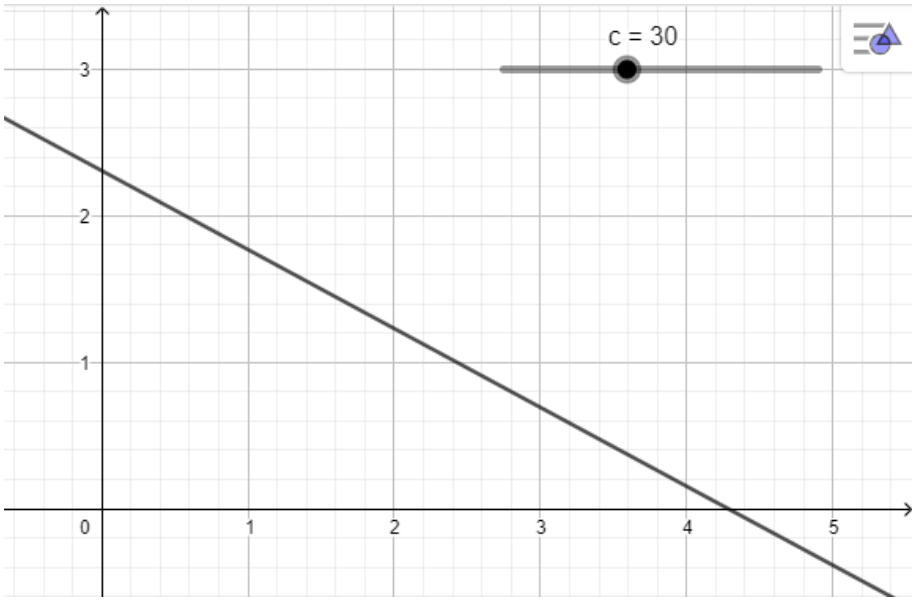

Figura 5.16: Reta da equação $7x + 13y = c$ com $c = 30$. Note que esta equação não possui solução natural.

O semigrupo associado à equação $7x + 13y = c$ é $S = \langle 7,\ 13 \rangle$. Aplicando o corolário 3.9, o conjunto das lacunas de S é

$$\mathbb{N} \setminus S = \{7m - 13n \in \mathbb{N} \mid m,\ n \in \mathbb{N},\ m < 13\}.$$

Para $m = 1$, temos que $7.1 - 13n \notin \mathbb{N}$.

Para $m = 2$, temos que $7.2 - 13n \in \mathbb{N}$ se $n = 1$. Logo, 1 é lacuna de S.

Para $m = 3$, temos que $7.3 - 13n \in \mathbb{N}$ se $n = 1$. Logo, 8 é lacuna de S.

Para $m = 4$, temos que $7.4 - 13n \in \mathbb{N}$ para $n = 1$ e $n = 2$. Logo, 15 e 2 são lacunas de S.

Para $m = 5$, temos que $7.5 - 13n \in \mathbb{N}$ para $n = 1$ e $n = 2$. Logo, 22 e 9 são lacunas de S.

Para $m = 6$, temos que $7.6 - 13n \in \mathbb{N}$ para $n = 1$, $n = 2$ e $n = 3$. Logo, 29, 16 e 3 são lacunas de S.

Para $m = 7$, temos que $7.7 - 13n \in \mathbb{N}$ para $n = 1$, $n = 2$ e $n = 3$. Logo, 36, 23 e 10 são lacunas de S.

Para $m = 8$, temos que $7.8 - 13n \in \mathbb{N}$ para $n = 1$, $n = 2$, $n = 3$ e $n = 4$. Logo, 43, 30, 17 e 4 são lacunas de S.

Para $m = 9$, temos que $7.9 - 13n \in \mathbb{N}$ para $n = 1$, $n = 2$, $n = 3$ e $n = 4$. Logo, 50, 37, 24 e 11 são lacunas de S.

Para $m = 10$, temos que $7.10 - 13n \in \mathbb{N}$ para $n = 1$, $n = 2$, $n = 3$, $n = 4$ e $n = 5$. Logo, 57, 44, 31, 18 e 5 são lacunas de S.

Para $m = 11$, temos que $7.11 - 13n \in \mathbb{N}$ para $n = 1$, $n = 2$, $n = 3$, $n = 4$ e $n = 5$. Logo, 64, 51, 38, 25 e 12 são lacunas de S.

Para $m = 12$, temos que $7.12 - 13n \in \mathbb{N}$ para $n = 1$, $n = 2$, $n = 3$, $n = 4$, $n = 5$ e $n = 6$. Logo, 71, 58, 45, 32, 19 e 6 são lacunas de S.

Desse modo, segue que o conjunto das lacunas de $S = \langle 7,\ 13\rangle$ é

$$\mathbb{N} \setminus S = \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 8,\ 9,\ 10,\ 11,\ 12,\ 15,\ 16,\ 17,\ 18,\ 19,\ 22,\ 23,\ 24,\ 25,\ 29,\ 30,\ 31,\ 32,\ 36,\ 37,\ 38,\ 43,\ 44,\ 45,\ 50,\ 51,\ 57,\ 58,\ 64,\ 71\}.$$

Portanto, a equação $7x + 13y = c$ admite soluções naturais para todo c natural tal que $c \notin \mathbb{N} \setminus S$. Em particular, como 32 é lacuna de S, a equação do item a) não possui solução natural.

O objetivo do item c) é que o aluno determine as soluções naturais $7x + 13y = 300$ pelo Algoritmo de Euclides e, em seguida, identifique-as no GeoGebra. Temos:

$$\begin{aligned} 13 &= 1.7 + 6, \\ 7 &= 1.6 + 1. \end{aligned}$$

Substituindo a primeira equação acima na segunda, obtemos

$$1 = 7 - 13 + 7 = 7.2 + 13.(-1).$$

Multiplicando esta última igualdade por 300, segue que

$$300 = 7.600 + 13.(-300) = 7.(46.13 + 2) + 13.(-300) = 7.2 + 13.22,$$

mostrando que $x_0 = 2$ e $y_0 = 22$ é a solução minimal da equação diofantina e, portanto, as soluções naturais são

$$x = 2 + 13t, \quad y = 22 - 7t, \quad \text{com } t \in \mathbb{N},$$

que só têm sentido para $t = 0$, $t = 1$, $t = 2$ e $t = 3$.

Para $t = 0$, temos a solução minimal $x_0 = 2$ e $y_0 = 22$.

Para $t = 1$, temos a solução $x_1 = 15$ e $y_1 = 15$.

Para $t = 2$, temos a solução $x_2 = 28$ e $y_2 = 8$.

Por fim, para $t = 3$, temos a solução $x_3 = 41$ e $y_3 = 1$.

O professor deverá pedir aos alunos que movimentem a tela do GeoGebra e apliquem o zoom quando necessário para que possam localizar as soluções naturais encontradas. Abaixo, ilustramos a solução $x_1 = 15$ e $y_1 = 15$:

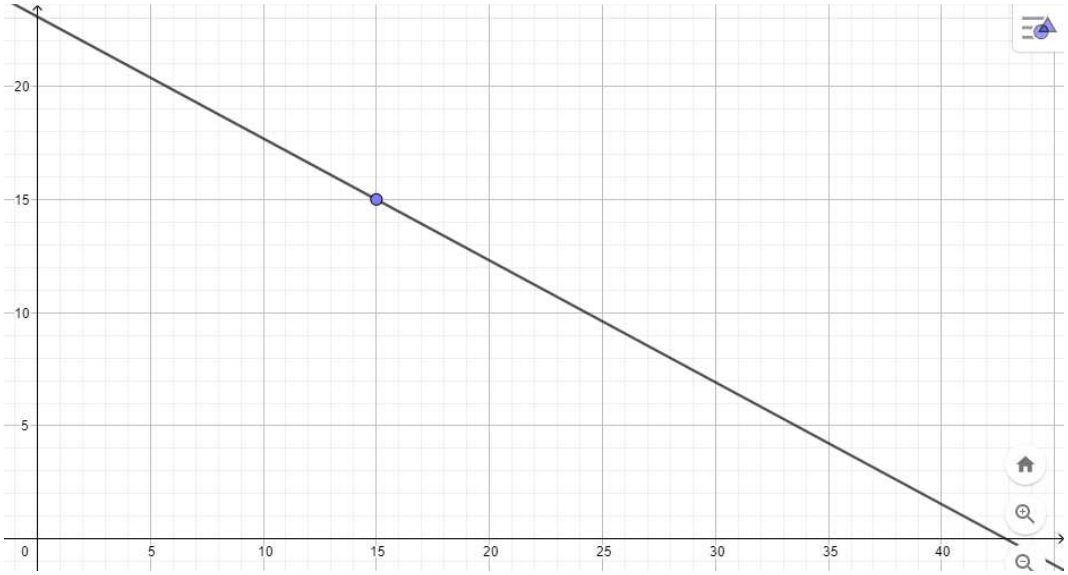

Figura 5.17: Reta da equação $7x + 13y = 300$. Note que $x = 15$ e $y = 15$ é solução natural desta equação.

Solução: Exercício 5.1.19:

O objetivo deste exercício é que o aluno possa representar uma situação problema através de uma equação diofantina linear e constatar que, para solucionar o exercício, não é necessário resolver a equação, mas apenas determinar o condutor do semigrupo associado a ela. Considerando x a quantidade de cédulas de \$7 e y a quantidade de cédulas de \$10, a equação que representa essa situação é

$$7x + 10y = c,$$

em que c é o valor que desejamos pagar. Para que qualquer pagamento seja sem troco, é necessário que c seja maior ou igual ao condutor do semigrupo $S = \langle 7,\ 10\rangle$, associado a essa equação. O corolário 3.10 nos diz que o condutor β é dado por

$$\beta = (7 - 1).(10 - 1) = 6.9 = 54.$$

Portanto, é possível pagar, sem troco, qualquer valor inteiro c maior ou igual a \$54. O professor deve comentar com os alunos que existem quantias inteiras menores que \$54 que também podem ser pagas sem troco. Uma maneira de eles verificarem esse fato é observando a representação desta situação no GeoGebra através da equação $7x + 10y = c$, em que c é um controle deslizante inteiro com valor mínimo 1, máximo 70 e incremento 1. Abaixo ilustramos essa situação:

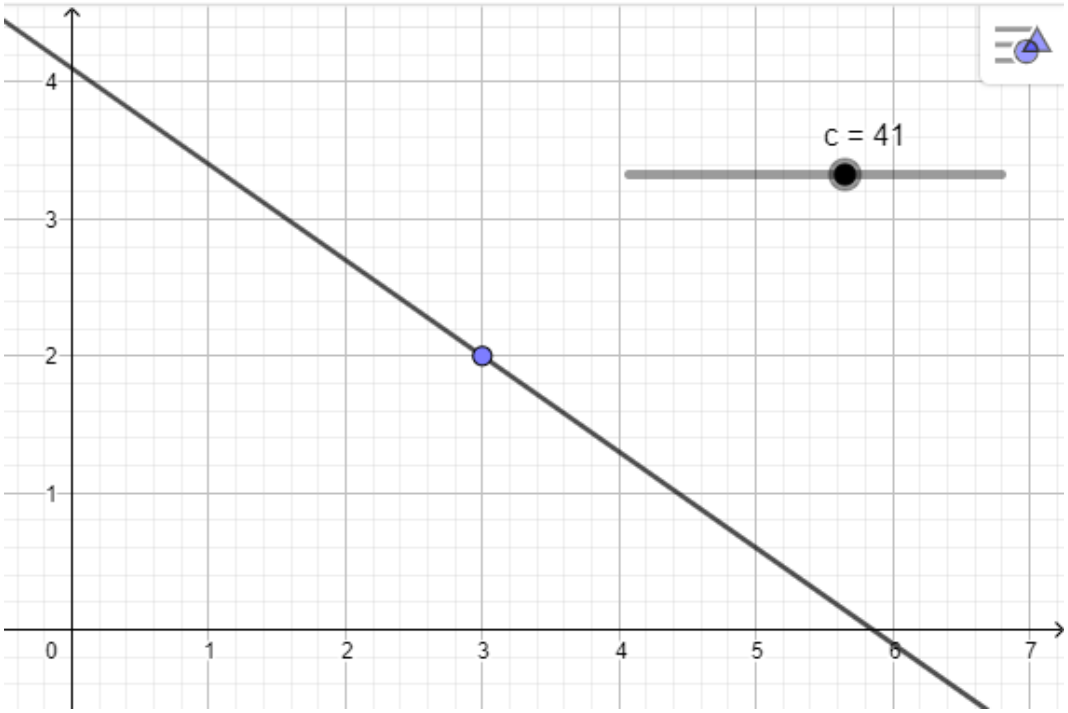

Figura 5.18: Reta da equação $7x + 10y = c$ com $c = 41$. Note que $x = 3$ e $y = 2$ é solução natural desta equação.

Solução: Exercício 5.1.20:

O objetivo deste exercício é que o aluno possa representar uma situação problema através de uma equação diofantina e resolvê-la. Considerando x a quantidade de cédulas de \$20 e y a quantidade de cédulas de \$50, a equação que representa essa situação é

$$20x + 50y = 430.$$

Como $(20,\ 50) = 10$ e $10 \mid 430$, essa equação possui solução. Dividindo ambos os membros da equação por 10, obtemos a equação equivalente

$$2x + 5y = 43$$

Pelo algoritmo de Euclides, temos:

$$5 = 2.2 + 1,$$

ou seja,

$$1 = 5.1 + 2.(-2).$$

Multiplicando esta última igualdade por 43, segue que

$$43 = 5.43 + 2.(-86) = 5.(2.21 + 1) + 2.(-86) = 2.19 + 5.1,$$

mostrando que $x_0 = 19$ e $y_0 = 1$ é a solução minimal da equação diofantina e, portanto, as

soluções naturais são

$$x = 19 + 5t, \quad y = 1 - 2t, \quad \text{com } t \in \mathbb{N},$$

que só têm sentido para $t = 0$. Desse modo, a equação só possui a solução minimal $x_0 = 19$ e $y_0 = 1$. Isso significa que o caixa eletrônico irá fornecer dezenove notas de R$20 e uma nota de R$50.

Abaixo, ilustramos essa solução no GeoGebra. O professor deverá instruir os alunos a movimentarem a tela e utilizarem o zoom para que possam visualizar toda a parte da reta situada no primeiro quadrante:

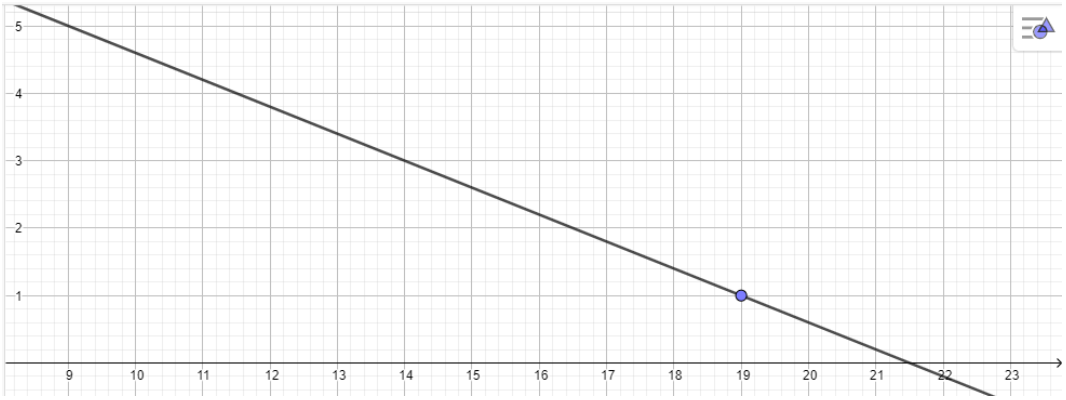

Figura 5.19: Reta da equação $20x + 50y = 430$. Note que $x = 1$ e $y = 19$ é a solução natural desta equação.

Solução: Exercício 5.1.21:

O objetivo deste exercício é que o aluno possa representar uma situação problema através de uma equação diofantina linear e resolvê-la.

Para o item a), basta que o aluno calcule o condutor do semigrupo associado a equação. Considerando x a quantidade de embalagens com 5 unidades de empanados e y a quantidade de embalagens com 12 unidades, a equação que representa essa situação é

$$5x + 12y = c,$$

em que c é a quantidade total de empanados que desejamos comprar. O semigrupo associado a essa equação é $S = \langle 5,\ 12 \rangle$, e o seu condutor é o número a partir do qual a equação sempre tem solução natural. O corolário 3.10 nos diz que o condutor β de S é dado por

$$\beta = (5 - 1).(12 - 1) = 4.11 = 44.$$

Portanto, é possível comprar qualquer quantidade inteira de empanados maior ou igual a 44. É importante mencionar aos alunos que também é possível comprar algumas quantidades inteiras menores que 44, e eles podem verificar tal fato representando a equação $5x + 12y = c$ no GeoGegebra, sendo c um controle deslizante inteiro com valor mínimo 1, máximo 50 e incremento 1. Abaixo ilustramos uma dessas situações:

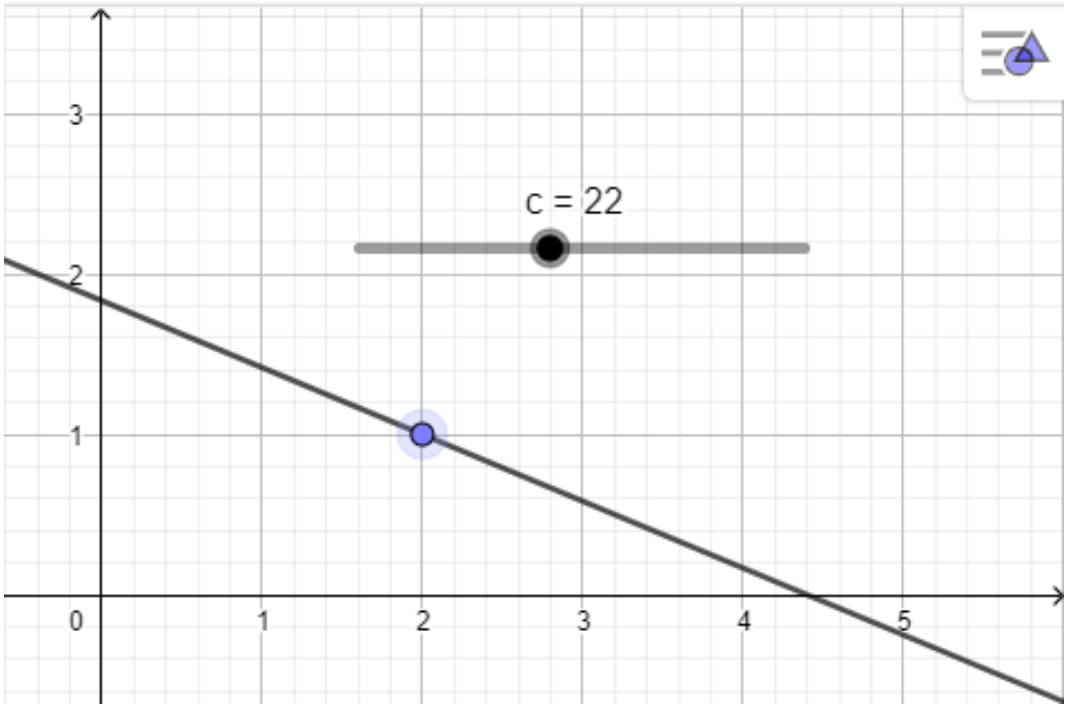

Figura 5.20: Reta da equação $5x + 12y = c$ com $c = 22$. Note que $x = 2$ e $y = 1$ é a solução natural desta equação.

O objetivo do item b) é que o aluno busque alguma solução pelo método de tentativa e erro e chegue a hipótese de que não existe tal solução. Em seguida, represente a equação $5x + 12y = 38$ no GeoGebra e confirme sua hipótese. Abaixo ilustramos essa representação:

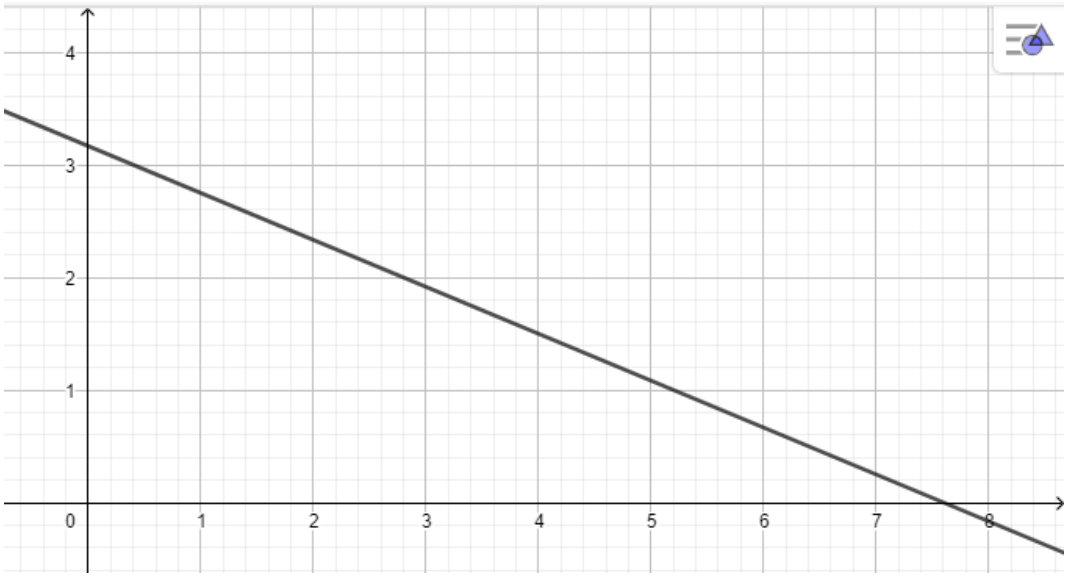

Figura 5.21: Reta da equação $5x + 12y = c$ com $c = 38$. Note que esta equação não possui solução natural.

O objetivo do item c) é determinar lacunas do semigrupo associado a equação $5x + 12y = c$. Para isso, os alunos irão variar o valor do controle deslizante c e verificar se a equação admite solução natural ou não. Abaixo, ilustramos duas situações em que foram determinadas as lacunas 18 e 31:

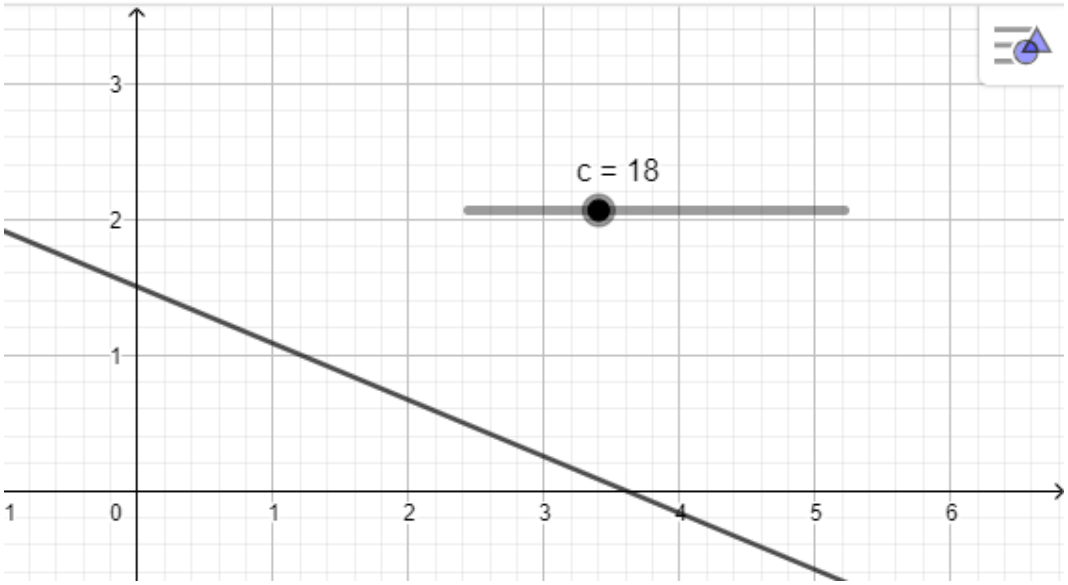

Figura 5.22: Reta da equação $5x + 12y = c$ para $c = 18$. Note que esta equação não possui solução natural.

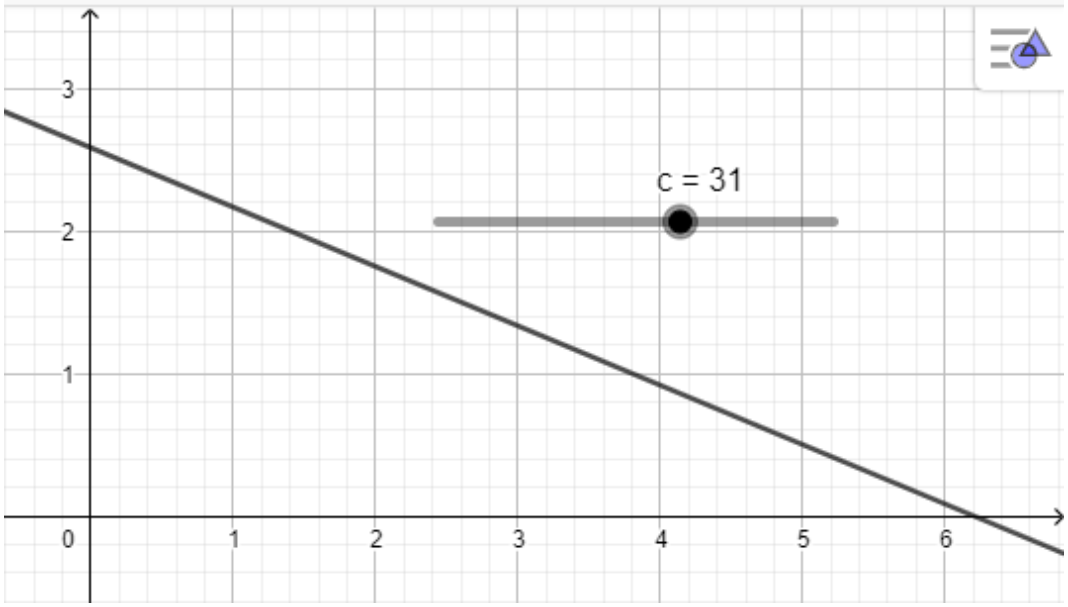

Figura 5.23: Reta da equação $5x + 12y = c$ para $c = 31$. Note que esta equação não possui solução natural.

Caso a turma não consiga encontrar todas as lacunas do semigrupo, o professor poderá apresentar aquelas que faltaram e pedir para que verifiquem a equação no GeoGebra. Conforme mencionado no item a), o semigrupo associado à equação $5x + 12y = c$ é $S = \langle 5,\ 12 \rangle$. Aplicando o corolário 3.9, o conjunto das lacunas de S é

$$\mathbb{N} \setminus S = \{5m - 12n \in \mathbb{N} \mid m,\ n \in \mathbb{N},\ m < 12\}.$$

Para $m = 1$, temos que $5.1 - 12n \notin \mathbb{N}$.
Para $m = 2$, temos que $5.2 - 12n \notin \mathbb{N}$.

Para $m = 3$, temos que $5.3 - 12n \in \mathbb{N}$ se $n = 1$. Logo, 3 é lacuna de S.

Para $m = 4$, temos que $5.4 - 12n \in \mathbb{N}$ se $n = 1$. Logo, 8 é lacuna de S.

Para $m = 5$, temos que $5.5 - 12n \in \mathbb{N}$ para $n = 1$ e $n = 2$. Logo, 13 e 1 são lacunas de S.

Para $m = 6$, temos que $5.6 - 12n \in \mathbb{N}$ para $n = 1$ e $n = 2$. Logo, 18 e 6 são lacunas de S.

Para $m = 7$, temos que $5.7 - 12n \in \mathbb{N}$ para $n = 1$ e $n = 2$. Logo, 23 e 11 são lacunas de S.

Para $m = 8$, temos que $5.8 - 12n \in \mathbb{N}$ para $n = 1$, $n = 2$ e $n = 3$. Logo, 28, 16 e 4 são lacunas de S.

Para $m = 9$, temos que $5.9 - 12n \in \mathbb{N}$ para $n = 1$, $n = 2$ e $n = 3$. Logo, 33, 21 e 9 são lacunas de S.

Para $m = 10$, temos que $5.10 - 12n \in \mathbb{N}$ para $n = 1$, $n = 2$, $n = 3$ e $n = 4$. Logo, 38, 26, 14 e 2 são lacunas de S.

Para $m = 11$, temos que $5.11 - 12n \in \mathbb{N}$ para $n = 1$, $n = 2$, $n = 3$ e $n = 4$. Logo, 43, 31, 19 e 7 são lacunas de S.

Desse modo, segue que o conjunto das lacunas de $S = \langle 5,\ 12\rangle$ é :

$$\begin{aligned}\mathbb{N} \setminus S = \{&1,\ 2,\ 3,\ 4,\ 6,\ 7,\ 8,\ 9,\ 11,\ 13,\ 14,\ 16,\ 18,\ 19,\ 21,\ 23,\ 26,\\ &28,\ 31,\ 33,\ 38,\ 43\}.\end{aligned}$$

Portanto, não é possível comprar uma quantidade c de empanados tal que $c \in \mathbb{N} \setminus S$.

O objetivo do item d) é que o aluno determine as soluções naturais da equação $5x + 12y = 162$ pelo algoritmo de Euclides e, em seguida, identifique-as no GeoGebra. Temos:

$$\begin{aligned}12 &= 2.5 + 2,\\ 5 &= 2.2 + 1.\end{aligned}$$

Substituindo a primera equação acima na segunda, obtemos

$$1 = 5 - 2.(12 - 5.2) = 5.5 + 12.(-2).$$

Multiplicando esta última igualdade por 162, segue que

$$162 = 5.810 + 12.(-324) = 5.(67.12 + 6) + 12.(-324) = 5.6 + 12.11,$$

mostrando que $x_0 = 6$ e $y_0 = 11$ é a solução minimal da equação diofantina e, portanto, as soluções naturais são

$$x = 6 + 12t, \quad y = 11 - 5t, \quad \text{com } t \in \mathbb{N},$$

que só têm sentido para $t = 0$, $t = 1$ e $t = 2$.

Para $t = 0$, temos a solução minimal $x_0 = 6$ e $y_0 = 11$, que representa que o cliente comprará seis caixas com cinco unidades de empanados e onze caixas com doze unidades.

Para $t = 1$, temos a solução $x_1 = 18$ e $y_1 = 6$, que representa que o cliente comprará dezoito caixas com cinco unidades de empanados e seis caixas com doze unidades.

Por fim, para $t = 2$, temos a solução $x_2 = 30$ e $y_2 = 1$, que representa que o cliente comprará trinta caixas com cinco unidades de empanados e uma caixa com doze unidades.

O professor deverá pedir aos alunos que movimentem a tela do GeoGebra e apliquem o zoom quando necessário para que possam localizar as soluções naturais encontradas. Abaixo, ilustramos a solução $x_1 = 18$ e $y_1 = 6$:

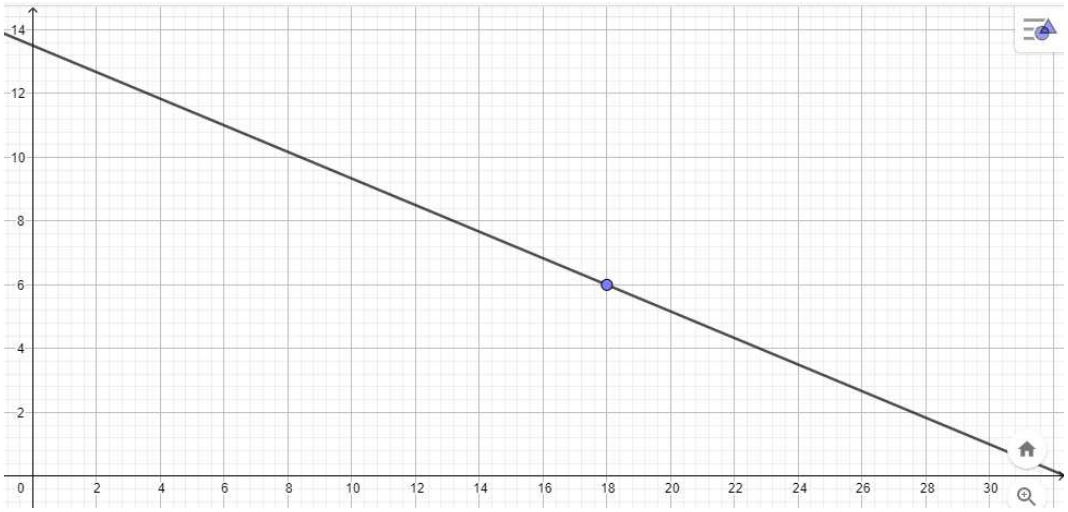

Figura 5.24: Reta da equação $5x + 12y = 162$. Note que $x = 18$ e $y = 6$ é solução natural desta equação.

6

Considerações Finais

Neste trabalho, apresentamos os semigrupos numéricos e algumas de suas propriedades. Introduzimos semigrupos numéricos simétricos, pseudossimétricos, quase-simétricos e Arf. Relacionamos semigrupos modulares com inequações diofantinas modulares e apresentamos um algoritmo que permite determinar se um semigrupo numérico é modular ou não. Introduzimos os chamados UESY-semigrupos e os relacionamos com semigrupos modulares cujo módulo possui valor mínimo em relação ao seu peso. Também foram apresentados resultados aritméticos sobre os números inteiros, bem como a relação entre equações diofantinas lineares e semigrupos. Por fim, trouxemos uma proposta de atividades para a Educação Básica abrangendo estes dois últimos tópicos.

Esperamos que este trabalho seja útil para professores e licenciandos em Matemática. Para aqueles que gostariam de aprofundar o estudo de semigrupos, em [10] é feita uma relação entre o estudo de anéis locais e semigrupos numéricos. Classificar um anel local não é simples, mas pode se tornar menos complexo a partir da análise de seu semigrupo correspondente. No capítulo 4 estudamos semigrupos modulares. Dados dois inteiros a e b positivos com $a < b$, encontrar uma fórmula em termos de a e b para o número de Fröbenius e para a multiplicidade de $S(a,b)$ ainda é um problema em aberto na Matemática. Em [3] é possível encontrar alguns resultados parciais para casos específicos. O estudo de semigrupos modulares pode ser generalizado, conforme em [3]: dados três números inteiros positivos a, b e c, uma inequação diofantina proporcionalmente modular é uma expressão da forma $ax \mod b \leq cx$ em que x é uma variável em $\mathbb{Z}$. O conjunto de soluções inteiras desta inequação, denotado por $S(a,b,c) = \{x \in \mathbb{N} \mid ax \mod b \leq cx\}$, é um semigrupo numérico chamado de semigrupo numérico proporcionalmente modular. Um semigrupo numérico S é chamado de PEPSY-semigrupo se existe um semigrupo pseudossimétrico S' tal que $S = S' \cup \left\{\gamma(S'), \frac{\gamma(S')}{2}\right\}$. De maneira parecida como fizemos no capítulo 4, os PEPSY-semigrupos estão relacionados com semigrupos modulares cujo módulo é igual ao seu peso mais três. Tal relação pode ser verificada também em [3].

Esta pesquisa me permitiu enriquecer e aprofundar conhecimentos matemáticos sobre estruturas que até então desconhecia. Foi interessante constatar como alguns tópicos aqui apresentados são objetos de pesquisa para problemas em aberto até os dias atuais. Por fim, destaco que este trabalho também contribuiu para me mostrar que mesmo que alguns

conteúdos sejam voltados para a ensino superior, eles também podem ser introduzidos na Educação Básica, oportunizando assim ao aluno do ciclo básico o contato com outras estruturas e conceitos importantes da Matemática.

Bibliografia

[1] Barucci, V. e Fröberg, R. "One-Dimensional Almost Gorenstein Rings". *Journal of Algebra* (1997).

[2] Bernardini, M. "Semigrupos Numéricos". *I Semat UNB* (2018).

[3] Blanco, J. M. U. "Semigrupos Numéricos Proporcionalmente Modulares". (Em espanhol.) Tese de dout. Universidad de Granada, Granada, Espanha, mar. de 2005.

[4] Brasil. "Base Nacional Comum Curricular - BNCC". *MEC* (2020). URL: http://basenacionalcomum.mec.gov.br (acesso em 6 de nov. de 2020).

[5] Fröberg, R., Gottlieb, C. e Häggkvist, R. "On Numerical Semigroups". *Semigroup Forum* (1987).

[6] Guedes, C. L. D. e, Pinto, J. L. M. e Silva Bruno, S. da. *SOMOS Sistemas de Ensino: ensino fundamental 2: matemática 1, 8º ano*. 1ª Ed. SOMOS Sistemas de Ensino, 2017.

[7] Guedes, C. L. D. e, Reis, B. F. dos e Devillart, J. C. R. *SOMOS Sistemas de Ensino: ensino fundamental 2: matemática, 6º ano*. 1ª Ed. SOMOS Sistemas de Ensino, 2017.

[8] Hefez, A. *Aritmética*. 2ª Ed. Coleção Profmat. SBM, 2016, p. 330.

[9] Hefez, A. *Exercícios Resolvidos de Aritmética*. 1ª Ed. Coleção Profmat. SBM, 2016, p. 204.

[10] Lara, D. F. N. "Semigrupos de Anéis Quase Gorenstein, Arf e Kunz". Diss. de mestr. Universidade Federal de Minas Gerais, fev. de 2010.

[11] Mota, S. D. "Semigrupos de Valores de Anéis Gorenstein, Kunz e Arf e a Árvore de Semigrupos Numéricos". Diss. de mestr. Universidade Federal de Viçosa, mai. de 2015.

[12] Oliveira, K. I. M. e Fernández, A. J. C. *Iniciação à Matemática: um curso com problemas e soluções*. 1ª Ed. Coleção Olimpíadas de Matemática. SBM, 2010, p. 283.

[13] Pommer, W. M. "Equações Diofantinas Lineares: Um Desafio Motivador para Alunos do Ensino Médio". Diss. de mestr. Pontifícia Universidade Católica de São Paulo, 2008.

[14] Rodrigues, A. L. F. "Semigrupos Numéricos com Multiplicidade Fixada e Proposta de Atividade para o Enino Médio com Utilização do GeoGebra". Diss. de mestr. Universidade de Brasília, set. de 2020.

[15] Rosales, J. C. "Numerical Semigroups that Differ from a Symmetric Numerical Semigroup in One Element". *Algebra Colloquium* (2008).

[16] Rosales, J. C., García-Sanchez, P. A. e Urbano-Blanco, J. M. "Modular Diophantine Inequalities and Numerical Semigroups". *Pacific Journal of Mathematics* (fev. de 2005).

[17] Silva, R. R. M. "Sobre Semigrupos Numéricos". Diss. de mestr. Universidade Estadual de Campinas, 2006.

[18] Silva Neris, N. G. da. "Estudo Local de Curvas Singulares via Valorizações e Semigrupos". Diss. de mestr. Universidade Federal de Juiz de Fora, 2017.

[19] Stanford Math Tournament, C. da. *Power Round Solutions*. 2013. URL: https://sumo.stanford.edu/old/smt/2013/test-files/power-solutions.pdf (acesso em 21 de set. de 2019).

[20] Vansan, A. H. “Equações Diofantinas: Um projeto para Sala de Aula e o uso do GeoGebra”. Diss. de mestr. Universidade Estadual de Maringá, fev. de 2014.