UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

PEDRO HENRIQUE DE OLIVEIRA IGNÁCIO

SEMIGRUPOS NUMÉRICOS E O PROBLEMA DO TROCO DE FROBENIUS

FORTALEZA

2019

PEDRO HENRIQUE DE OLIVEIRA IGNÁCIO

SEMIGRUPOS NUMÉRICOS E O PROBLEMA DO TROCO DE FROBENIUS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática. Área de Concentração: Ensino de Matemática

Orientador: Prof. Dr. José Alberto Duarte Maia

FORTALEZA

2019

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

I27s Ignácio, Pedro Henrique de Oliveira.
Semigrupos numéricos e o problema do troco de Frobenius / Pedro Henrique de Oliveira Ignácio. – 2019.
58 f.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2019.
Orientação: Prof. Dr. José Alberto Duarte Maia.

1. Eliminação inteira. 2. Equações diofantinas. 3. Número de Frobenius. 4. Semigrupos. 5. Problema do Troco de Frobenius. I. Título.

CDD 510

PEDRO HENRIQUE DE OLIVEIRA IGNÁCIO

SEMIGRUPOS NUMÉRICOS E O PROBLEMA DO TROCO DE FROBENIUS

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática. Área de Concentração: Ensino de Matemática

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. José Alberto Duarte Maia (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Marcelo Ferreira de Melo
Universidade Federal do Ceará (UFC)

Prof. Dr. Joserlan Perote da Silva
Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)

Dedico este trabalho a Deus, o criador do Universo, à minha querida esposa Christianne e minhas amadas filhas, Ingrid e Letícia. Em memória de meu pai, João Ignácio. A minha mãe, Maria Lêda, e aos meus irmãos Francisco Jorge, Maria Conceição, Maria Elizabeth e João Inácio.

AGRADECIMENTOS

Aos aos meus professores do curso de mestrado PROFMAT por todo o conhecimento transmitido e a dedicação empenhada na missão de formar educadores competentes.

Especialmente ao Prof. Dr. José Alberto Duarte Maia, por seu incentivo e por sua confiança e sua orientação empregadas em minha dissertação de mestrado.

Ao meu amigo, Renato Marques de Oliveira, aluno de graduação no curso de Matemática Industrial, na Universidade Federal do Ceará, por fomentar os conhecimentos necessários da linguagem de marcação LaTeXe me auxiliar com a ferramenta.

Aos meus pais, por seus esforços para me formar com educação, valores e princípios que se estendem por toda a vida.

À minha esposa, por seu amor e seu suporte em todos os momentos. Às minhas filhas, por me apoiar e me instruir em meus projetos. Aos meus irmãos, por toda força e companheirismo.

Aos meus alunos, que são uma das minhas grandes motivações para a realização do curso, para que eu possa ser melhor por eles.

"A graça de Deus se manifestou para a salvação de todos os homens. Essa graça nos ensina a abandonar a impiedade e as paixões mundanas, para vivermos neste mundo com autodomínio, justiça e piedade."

(Tt. 2: 11-12)

RESUMO

O objetivo deste trabalho é apresentar o problema do Troco de Frobenius e os métodos utilizados para solucioná-lo, ilustrando a discussão com problemas encontrados no cotidiano. O problema do Troco de Frobenius consiste em encontrar uma cota mínima para uma sequência de números que podem ser formados através da combinação inteira de uma sequência inicial de números inteiros. Este problema é equivalente à encontrar a solução de uma equação diofantina, para o qual podemos aplicar o método da eliminação inteira, que é um procedimento similar à eliminação de Gauss, mas aplicado à sistemas lineares em $\mathbb{Z}$. Os conceitos e técnicas relacionados a esses problemas podem ser formalizados através de estruturas algébricas, em especial os semigrupos. A teoria dos semigrupos, quando conectada com o problema do Troco de Frobenius, fornece para este ferramentas simultaneamente formais e intuitivas para buscar soluções do mesmo.

Palavras-chave: Eliminação inteira. Equações diofantinas. Número de Frobenius. Semigrupos. Problema do Troco de Frobenius.

ABSTRACT

This thesis aims to present the Coin Problem and methods employed in the solution thereof, illustrating the discussion with everyday problems. The Coin Problem consists in finding a lower bound to the sequence of numbers that can be formed by an integer linear combination of a starting sequence of integers. This problem is equivalent to finding the solution of a diophantine equation, to which we can apply the method of integer elimination, which itself is an algorithm similar to Gaussian elimination, but is applied to linear systems in $\mathbb{Z}$. The concepts and techniques related to these problems can be formalized by algebraic structures, especially the semigroups. The theory of semigroups when connected to the Coin Problem provides the latter with simultaneously formal and intuitive tools for searching for its solutions.

Keywords: Diophantine equations. Coin Problem. Frobenius number. Integer elimination. Semigroups.

LISTA DE SÍMBOLOS

$\mathrm{Ap}(n, H)$	Conjunto de Apèry de H com relação à n.
f	Número de Frobenius.
g	Gênero do semigrupo.
L	Conjunto de lacunas do semigrupo.
l_g	Elemento máximo do conjunto de lacunas.
mdc	Máximo divisor comum.
mod	Operador módulo.
$\mathbb{N}$	Conjunto dos números naturais.
$\mathbb{R}$	Conjunto dos números reais.
$\mathbb{Z}$	Conjunto dos números inteiros.
$[a]_n$	Classe de congruência de a módulo n.
$\mid$	Operador “divide”.
$\setminus$	Operador complementar.
^{T}	Operador transposição da matriz.

SUMÁRIO

1 INTRODUÇÃO

O objetivo deste trabalho é apresentar o problema do Troco de Frobenius e os métodos utilizados para solucioná-lo, ilustrando a discussão com problemas encontrados no cotidiano. O problema do Troco de Frobenius consiste em encontrar uma cota mínima para uma sequência de números que podem ser formados através da combinação inteira (um tipo especial de combinação linear) de uma sequência inicial de números inteiros. Por exemplo, existe um valor mínimo para um saque no caixa eletrônico, a partir do qual quaisquer valores são possíveis de resgatar? A aplicação dos métodos que estudaremos é mais eficiente do que a estratégia de tentativa e erro comumente utilizada.

Ademais, este trabalho busca fomentar a possibilidade de uma melhor expressão matemática para enfrentar situações-problema que surgem no dia a dia com uma visão holística, permitindo o desenvolvimento de mais possibilidades e mais pontos de vista para os alunos quanto à aprendizagem matemática, estimulando suas habilidades cognitivas e o processo de ensino-aprendizagem.

Para isso, são apresentados enunciados, conceitos e definições de alguns resultados essenciais provenientes da Teoria dos Números, além das demonstrações de teoremas, axiomas e proposições acerca de Divisibilidade, Divisão Euclidiana, Máximo Divisor Comum, Algoritmo de Euclides e, finalmente, as Equações Diofantinas, estas últimas as quais vão embasar a resolução dos problemas por nós considerados. Estes conceitos citados de Teoria dos Números constituem o Capítulo 2.

Em seguida, no Capítulo 3 são abordados os Sistemas lineares nos inteiros e sua interpretação geométrica, operações elementares, definições e exemplos. Os Sistemas Lineares constituem um ramo da álgebra linear importante para a construção de algoritmos e modelos matemáticos. Uma introdução à teoria dos sistemas lineares foi colocada no Apêndice A. Para a resolução de sistemas de equações lineares abordamos o escalonamento matricial e é proposta a estratégia da Eliminação Inteira, uma pequena variante da Eliminação de Gauss para matrizes em $\mathbb{Z}^n$. Este método visualiza todas as soluções inteiras existentes num sistema linear.

A partir disso, temos os conceitos e o aprendizado necessários para as aplicações do Problema do Troco de Frobenius, assunto do Capítulo 4, onde expressamos a proposição da Boa Posição, teoremas do caso $n = 2$ (dois termos) e $n = 3$ (três termos), exercícios solucionados com os métodos anteriormente apresentados, proporcionando aplicações e facilitando o entendimento do assunto e, por fim, no capítulo 5, fazemos uma introdução à estruturas algébricas relacionadas

a Semigrupos Numéricos, que formalizam muitas das noções estudadas até essa altura do texto e fornecem intuições mais aguçadas para o assunto.

Conforme os Parâmetros Curriculares Nacionais (PCN), a resolução de problemas é o ponto de partida da atividade matemática, não constituindo uma mera reprodução de procedimentos e acúmulo de informações e ganhando significado. Dessa forma, torna-se importante e necessária a relação da aplicação das Equações Diofantinas como método para a resolução de problemas.

2 CONCEITOS DE TEORIA DOS NÚMEROS

2.1 Divisibilidade

A Teoria dos números trata de propriedades dos números naturais $1, 2, 3, 4, \ldots$, também chamados *inteiros positivos*. Juntando estes números com os inteiros negativos e o zero, formamos o conjunto dos inteiros ($\mathbb{Z}$). As propriedades desses números tem sido estudadas desde tempos remotos. Além de propriedades conhecidas, a teoria dos números contém vários problemas ainda não resolvidos. Entretanto, para ao menos expressarmos muitos desses problemas, já se faz necessária uma certa base teórica (NIVEN *et al.*, 1991).

Assim, iniciamos nosso estudo estabelecendo uma definição formal do conjunto dos números naturais ($\mathbb{N}$), através dos Axiomas de Peano, que historicamente ajudaram a sedimentar uma base para a teoria dos números. Em seguida, podemos extrair algumas propriedades dos inteiros. Transcrevemos a definição a seguir da referência (SHOKRANIAN, 2008).

Definição 2.1.1 (Axiomas de Peano)**.**

1. $\mathbb{N}$ contém o número 1.
2. Existe uma função $\delta : \mathbb{N} \longrightarrow \mathbb{N}$ chamada de **função sucessora** que associa a cada $n \in \mathbb{N}$ o seu sucessor $\delta(n)$. A função δ é injetora e para todo $n \in \mathbb{N}$ vale a desigualdade $\delta(n) \neq 1$.
3. Se um subconjunto Q de $\mathbb{N}$ tem as seguintes propriedades:
   a) $1 \in Q$;
   b) Se $n \in Q$ implica $\delta(n) \in Q$,

   então $Q = \mathbb{N}$.

O Axioma (3) é chamado **princípio da indução**.

Também vamos assumir no texto que se segue o princípio da boa ordenação, como enunciado em (APOSTOL, 2013), que pode ser derivado do princípio da indução (e vice-versa). Este princípio é importante para a demonstração de certas propriedades dos inteiros.

Teorema 2.1.1 (Princípio da Boa Ordenação)**.** Se Q é um conjunto não vazio de naturais, então Q possui um elemento mínimo.

Existem outras formulações que podem embasar a teoria dos números, como a Teoria Axiomática dos Conjuntos, onde se pode demonstrar os princípios admitidos aqui como axiomas.

Uma das propriedades dos inteiros mais importantes para o presente estudo é a divisibilidade. Definimos essa propriedade de acordo com (NIVEN *et al.*, 1991).

Definição 2.1.2. Um inteiro b é divisível por um inteiro a não-nulo se existir um inteiro x tal que $b = ax$, donde escrevemos $a|b$.

Desta forma, teremos a como um divisor ou fator de b ou, também, que b é múltiplo de a ou que b é divisível por a.

A partir da definição, podemos estabelecer as seguintes propriedades da divisibilidade.

Proposição 2.1.2. Sejam $a, b, c \in \mathbb{Z}$. Tem-se que

i. $1|a$, $a|a$ e $a|0$.

ii. Se $a|b$ e $b|c$, então $a|c$.

iii. Se $a|b$ e $b|a$, então $a = \pm b$.

iv. se $a|b$ e $a|c$, então $a|(bx + cy)$, para quaisquer $x, y \in \mathbb{Z}$.

Demonstração.

i. Isto decorre das igualdades $a = a \cdot 1$, $a = 1 \cdot a$, $0 = 0 \cdot a$.

ii. $a|b$ e $b|c$ implica que existem x e $y \in \mathbb{Z}$, tais que $b = x \cdot a$ e $c = y \cdot b$. Substituindo o valor de b da primeira equação na outra, obtemos $c = y \cdot b = y\dot{(}xa) = (yx) \cdot a$, o que nos mostra que $a|c$.

iii. Se $a|b$, temos que $b = aq_1$, com $q_1 \in \mathbb{Z}$, e se $b|a$, segue que $a = bq_2$ com $q_2 \in \mathbb{Z}$. Portanto, $a = a(q_1 q_2)$, daí $q_1 q_2 = 1$, o que implica $q_1|1$, ou seja, $q_1 = \pm 1$. Logo, $a = \pm b$.

iv. A última propriedade permite uma extensão óbvia à qualquer conjunto finito, assim:

$$a|b_1, a|b_2, \ldots, a|b_n \implies a|\sum_{j=1}^{n} b_j x_j \quad \forall x_j \in \mathbb{Z}.$$

□

2.2 Congruências

Definição 2.2.1. Sejam $a, b, n \in \mathbb{Z}$ com $n > 0$. Se $n|a - b$, então a é congruente a b módulo n, ou seja,

$$a \equiv b \pmod{n}.$$

A congruência é uma forma de equivalência entre dois números, dada a condição "módulo n" para algum n, isto é, n deve dividir a diferença entre os dois números.

Exemplo 1.

$$20 \equiv 6 \pmod 7$$

Definição 2.2.2. Sejam a e n inteiros com $n > 0$. A classe de congruência de a módulo n, denotada por $[a]_n$, é o conjunto de todos os inteiros congruentes a a módulo n, ou seja,

$$[a]_n = \{z \in \mathbb{Z} \mid a - z = kn, \text{ para algum } k \in \mathbb{Z}\}.$$

Exemplo 2.

$$\begin{aligned}[4]_5 &= \{4, 4 \pm 5, 4 \pm 10, 4 \pm 15, \dots\} \\ &= \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\}\end{aligned}$$

O conjunto das classes de congruência módulo n, $\{[i]_n\}_{i \in \{0,1,\dots,n-1\}}$, forma uma partição de $\mathbb{Z}$. Para ver isso, considere os lemas a seguir.

A partir da definição de classe de congruência obtemos o seguinte lema:

Lema 2.2.1. Sejam $a, n \in \mathbb{Z}$. Então $[a]_n = a + n\mathbb{Z}$.

Observe que se X é subconjunto de $\mathbb{Z}$, então $a + nX = \{a + nx \mid x \in X, \ \forall n \in \mathbb{Z}\}$.

Lema 2.2.2. Sejam $c, a, n \in \mathbb{Z}$. Se $c \in [a]_n$, então $[c]_n = [a]_n$.

Demonstração. Temos que $c = a + nk$, para algum $k \in \mathbb{Z}$. Então $c + n\mathbb{Z} = (a + nk) + n\mathbb{Z}$. Daí

$$\begin{aligned}[c]_n &= (a + nk) + n\mathbb{Z} \\ &= (a + nk) + \{\dots, -n(k+2), -n(k+1), -nk, -n(k-1), -n(k-2), \dots\} \\ &= \{\dots, a + n(-2), a + n(-1), a + n(0), a + n(1), a + n(2), \dots\} \\ &= a + n\mathbb{Z} = [a]_n.\end{aligned}$$

□

Imediatamente deste segue o próximo lema:

Lema 2.2.3. Sejam $a, b, c, n \in \mathbb{Z}$. Se $c \in [a]_n$ e $c \in [b]_n$, então $[a]_n = [b]_n$.

Como $a = a + n0$, $a \in [a]_n$ e, portanto, cada $[a]_n$ é não-vazio e $\mathbb{Z} \subset \bigcup_{a\in\mathbb{Z}} [a]_n$. Assim, os conjuntos $[a]_n$ formam uma partição de $\mathbb{Z}$. Esta conclusão implica no seguinte lema:

Lema 2.2.4. Duas classes de congruência módulo n são ou disjuntas ou idênticas.

Corolário 2.2.1. Existem n classes de congruência módulo n distintas, $[0]_n, [1]_n, \ldots, [n-1]_n$.

Demonstração. Se tomarmos

$$0 \leq s < t < n,$$

então $t - s < n$, de modo que n não divide $t - s$ e, assim, t não é congruente a s módulo n. As classes de congruência $[0]_n, [1]_n, \ldots [n-1]_n$ são, assim, distintas, pois nenhum par dentre $0, 1, \ldots, n-1$ é congruente. Tomando $m \in \mathbb{Z}$ e expressando $m = nq + r$ com $0 \leq r < n$, podemos rearranjar de modo que $m - r = nq$, logo $m \equiv r \pmod{n}$. Qualquer inteiro m é congruente módulo n a algum $r \in \{0, 1, \ldots, n-1\}$. □

2.3 Divisão Euclidiana

Conforme estudado nos conceitos anteriores de divisibilidade, existem números naturais onde a relação $a|b$ é exata. Contudo, não é sempre possível encontrar tal exatidão ao dividir. No entanto, é sempre possível realizar a divisão de a por b, com resto, demostrada no teorema a seguir.

Teorema 2.3.1 (Divisão Euclidiana)**.** Sejam a e b dois números inteiros positivos, com $b \neq 0$, então existem dois únicos números inteiros q e r tais que

$$a = qb + r \quad \text{com} \quad 0 \leq r < b$$

Onde q é o quociente e r é o resto. Se $r = 0$, então $b|a$.

Demonstração.

Sejam a, b inteiros fixos com $b \neq 0$ (note que $b^2 \geq 1$). Considere o conjunto

$$S = \{a - bt \mid t \in \mathbb{Z}\} \cap \mathbb{N}.$$

Primeiramente, mostraremos que o conjunto S é não-vazio. Note que $S \neq \emptyset$, pois, tomando $t_0 = -b|a|$, segue que

$$a - bt_0 = a - b(-b|a|) = a + b^2|a| \geq a + |a| \geq 0,$$

ou seja, $a - bt_0 \in S$.

Como S é subconjunto de $\mathbb{N}$, pelo princípio da boa ordenação, sabemos que S contém um elemento mínimo. Vamos denotá-lo por r. Como $r \in S$, existe $q \in \mathbb{Z}$ tal que

$$r = a - bq$$

e $r \geq 0$. Para mostrar que $r < |b|$, basta tomarmos $t_1 = q + \frac{|b|}{b}$ e observarmos que

$$r_1 := a - bt_1 = a - b\left(q + \frac{|b|}{b}\right) = a - bq - |b| = r - |b| < r.$$

Assim, a minimalidade de r implica que $r_1 \notin S$. Isso garante que $r_1 < 0$. Ou seja, $r - |b| < 0 \implies r < |b|$.

Para estabelecer a unicidade, note que se $s, t \in \mathbb{Z}$ são tais que $a = bt + s$, com $0 \leq s < |b|$, então $s = a - bt \in S$. Daí,

$$\begin{aligned} s \geq r \implies |b| &> s - r \\ s - r &= |s - r| \\ &= |a - bt - (a - bq)| \\ &= |a - bt - a + bq| \\ &= |b(q - t)| \\ &= |b||q - t| \end{aligned}$$

Logo, $|b| > |b||q - t|$. Mas isto implica que

$$0 \leq |q - t| < 1 \implies |q - t| = 0 \implies q = t \implies r = s.$$

□

2.4 Máximo Divisor Comum

Um dos resultados essenciais da Teoria dos Números é o conceito de Máximo Divisor Comum (MDC). As definições a seguir podem ser encontradas em (HEFEZ, 2006), que aponta a origem delas no próprio Euclides com seu livro *elementos*, tal é a importância desses conceitos.

Sejam dados dois inteiros a e b, distintos ou não. Um número inteiro d será dito um divisor comum de a e b se $d|a$ e $d|b$. Diremos que um número inteiro $d \geq 0$ é um máximo divisor comum (MDC) de a e b, se tiver as seguintes propriedades:

i. d é um divisor comum de a e b, e

ii. d é divisível por todo divisor comum de a e b, ou seja, se c é um divisor comum de a e b, então $c|d$.

E denotaremos $d = \text{mdc}(a,b)$.

O Lema de Euclides é apresentado para provar a existência do máximo divisor comum entre dois números da seguinte forma:

Lema 2.4.1 (Lema de Euclides)**.** Sejam $a,b,n \in \mathbb{Z}$. Se existe $\text{mdc}(a,b-na)$, então, $\text{mdc}(a,b)$ existe e

$$\text{mdc}(a,b) = \text{mdc}(a,b-na).$$

Demonstração. Seja $d = \text{mdc}(a,b-na)$. Como $d|a$ e $d|\text{mdc}(a,b-na)$, segue que d divide $b = b-na+na$. Portanto, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Assim, c é um divisor comum de a e $b-na$ e, portanto, $c|d$. Logo, $d = \text{mdc}(a,b)$. □

O Lema de Euclides pode ser usado para se calcular o MDC, e é a ferramenta básica para o algoritmo de Euclides que em breve utilizaremos para calcular o MDC de qualquer par de números naturais.

Exemplo 3. Vamos determinar os valores de a e n para os quais $a+1$ divide $a^{2n}+1$.

Temos, inicialmente, que

$$a+1|a^{2n}+1 \Leftrightarrow \text{mdc}(a+1,a^{2n}+1) = a+1.$$

Note que, para todo $a,b,n \in \mathbb{N}$, com $a \geq b > 0$, $a+b$ divide $a^{2n}-b^{2n}$, fato que pode ser verificado pela aplicação de produtos notáveis. Utilizando isto, como $a^{2n}+1 = (a^{2n}-1)+2$, e $a+1|a^{2n}-1$, segue, pelo lema de Euclides, que

$$\text{mdc}(a+1,a^{2n}+1) = \text{mdc}(a+1,(a^{2n}-1)+2) = \text{mdc}(a+1,2).$$

Assim, $a+1|a^{2n}+1$, para algum $n \in \mathbb{N}$, se, e somente se, $a+1 = \text{mdc}(a+1,2)$, o que, por sua vez, somente ocorre se $a = 0$ ou $a = 1$.

Exemplo 4. Vamos determinar os valores de a e n para os quais $a+1|a^{2n+1}-1$.

Temos, inicialmente, que

$$\text{mdc}(a+1,a^{2n+1}-1) = \text{mdc}(a+1,a(a^{2n}-1)+a-1) = \text{mdc}(a+1,a-1).$$

Assim, $a+1|a^{2n+1}-1$, para algum $n \in \mathbb{N}$, se, e somente se,

$$a+1 = \text{mdc}(a+1, a^{2n+1}-1) = \text{mdc}(a+1, a-1),$$

o que ocorre somente se $a = 1$.

2.5 Algoritmo de Euclides

O algoritmo constitui a prova construtiva da existência do MDC dada por Euclides.

Teorema 2.5.1 (Algoritmo de Euclides)**.** Sejam a, b inteiros positivos, com $b \neq 0$. Podemos aplicar a Divisão Euclidiana sucessivamente:

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 \leq r_1 < b \\
b &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2 \\
r_2 &= r_3 q_4 + r_4, \quad 0 \leq r_4 < r_3 \\
&\vdots \\
r_{n-2} &= q_n r_{n-1} + r_n \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}$$

E o $\text{mdc}(a, b) = r_n$, o último resto não nulo.

Demonstração. Note que pela divisão Euclidiana esses restos vão ficando cada vez menores. Como todos esse restos são números naturais, temos uma sequência estritamente decrescente de números naturais $b > r_1 > r_2 > r_3 > \ldots$, que é necessariamente finita, devido ao princípio da Boa Ordenação. Pelo lema de Euclides, temos que $\text{mdc}(a, b) = \text{mdc}(b, a - bq_1)$, que podemos reescrever como $\text{mdc}(b, r_1)$. Outra vez pelo Lema de Euclides $\text{mdc}(b, r_1) = \text{mdc}(r_1, b - r_1 q_2)$ e assim sucessivamente, até $\text{mdc}(a, b) = \text{mdc}(b, r_1) = \text{mdc}(r_1, r_2) = \cdots = \text{mdc}(r_{n-1}, r_n) = \text{mdc}(r_n, 0) = r_n$. □

Apresentaremos uma representação prática do algoritmo a seguir.

Primeiramente, efetuamos a divisão $a = bq_1 + r_1$ e colocamos os números envolvidos no diagrama abaixo:

	q_1	
a	b	
r_1		

Em seguida, continuamos efetuando a divisão $b = r_1q_2 + r_2$ e novamente colocamos os números no diagrama

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Prosseguindo até o término, obteremos

	q_1	q_2	q_3	$\dots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\dots$	r_{n-2}	r_{n-1}	$r_n = \text{mdc}(a,b)$
r_1	r_2	r_3	r_4	$\dots$	r_n	0	

Vamos achar $\text{mdc}(a,b)$ para cada par de números naturais nos exemplos a seguir.

Exemplo 5. 3887 e 637

Seguindo o molde anterior, fazemos o diagrama do algoritmo de Euclides, e a resposta será o último resto encontrado.

	6	9	1	4	
3887	637	65	52	13	
65	52	13	0		

Temos, então, que $\text{mdc}(3887, 637) = 13$.

Exemplo 6. 542 e 234

	2	3	6	6	
542	234	74	12	2	
74	12	2	0		

Temos, então, que $\text{mdc}(542, 234) = 2$.

2.6 Equações diofantinas

Um problema recorrente na aritmética é a busca de soluções, nos inteiros, de equações do tipo

$$ax + by = c, \tag{2.1}$$

com $a, b, c \in \mathbb{Z}$. Esse tipo de equação é chamado *equação diofantina* (em homenagem ao matemático grego do séc. III Diofanto de Alexandria). Os termos a e b são chamados *coeficientes* e c é chamado *termo constante*. Estamos interessados, entre outras coisas, em mostrar que o MDC de dois números a e b pode ser calculado através da soma $ar + bs$ para certos inteiros r e s.

O teorema a seguir nos mune de uma ferramenta para achar uma solução para uma equação diofantina.

Teorema 2.6.1 (Bachet-Bezout)**.** Sejam $a, b \in \mathbb{Z}$. Se $d = \text{mdc}(a, b)$, então existem m e $n \in \mathbb{Z}$ tais que

$$d = am + bn$$

Demonstração. Tomemos o conjunto

$$S(a, b) = \{ax + by | x, y \in \mathbb{Z}\} \cap \mathbb{N}^*$$

das combinações lineares inteiras de a e b.

Seja $v = ax_0 + by_0$ o menor elemento positivo de $S(a, b) \neq \emptyset$. Observamos que v divide todos os elementos do conjunto. Dado um elemento qualquer

$$u = ax_1 + by_1 \in S(a, b)$$

Pela Divisão Euclidiana, temos que existem q e r tais que

$$u = vq + r, \text{ com } 0 \leq r < v$$

Com base nas hipóteses tomadas,

$$r = u - vq = ax_1 + by_1 - q(ax_0 + by_0) = a(x_1 - qx_0) + b(y_1 - qy_0) \in S(a, b)$$

Contudo, teríamos que $r < v$, o que contraria a minimalidade de v. Assim, $r = 0$ e $v|u$. Observe que $a, b \in S(a, b)$, daí $v|a$ e $v|b$, e pela definição, $v|\text{mdc}(a, b)$. Porém, $\text{mdc}(a, b)|a$ e $\text{mdc}(a, b)|b$, então $\text{mdc}(a, b)|(ax_0 + by_0)$ para quaisquer x_0, y_0, daí $\text{mdc}(a, b)|v$. Logo, $\text{mdc}(a, b) = v$. Ou seja,

$$d = ax_0 + by_0, \text{ com } x_0, y_0 \in \mathbb{Z}.$$

□

Vamos voltar para os exemplos da seção anterior, 5 e 6, e determinar números inteiros m e n tais que $\text{mdc}(a,b) = ma + nb$

Exemplo 7. 3887 e 637

Lembre que o $\text{mdc}(3887, 637) = 13$. Observe que o algoritmo de Euclides fornece-nos

$$3887 = 6 \cdot 637 + 65$$

$$637 = 9 \cdot 65 + 52$$

$$65 = 1 \cdot 52 + 13$$

Donde segue que

$$13 = 65 - 1 \cdot 52 = 65 - 1 \cdot (637 - 9 \cdot 65) = 10 \cdot 65 - 637$$

$$= 10 \cdot (3887 - 6 \cdot 637) - 637 = 10 \cdot 3887 - 61 \cdot 637$$

Temos, então, que $13 = 10 \cdot 3887 + (-61) \cdot 637$. Portanto, $m = 10$ e $n = -61$.

Exemplo 8. 542 e 234

Lembre que o $\text{mdc}(542, 234) = 2$. Observe que o algoritmo de Euclides fornece-nos

$$542 = 2 \cdot 234 + 74$$

$$234 = 3 \cdot 74 + 12$$

$$74 = 6 \cdot 12 + 2$$

Donde segue que

$$2 = 74 - 6 \cdot 12 = 74 - 6 \cdot (234 - 3 \cdot 74) = 19 \cdot 74 - 6 \cdot 234$$

$$= 19 \cdot (542 - 2 \cdot 234) - 6 \cdot 234 = 19 \cdot 542 - 44 \cdot 234$$

Temos, então, que $2 = 19 \cdot 542 + (-44) \cdot 234$. Portanto, $m = 19$ e $n = -44$.

Vamos oficializar a nossa notação para as soluções de equações diofantinas com a seguinte proposição.

Proposição 2.6.2. Sejam $a, b \in \mathbb{Z}$. A equação

$$ax + by = c$$

admite solução inteira se, e somente se, $\text{mdc}(a,b) | c$.

Da proposição 2.6.2 e do algoritmo de Euclides, aprendemos a encontrar pelo menos uma solução inteira para a equação $ax + by = c$. Agora, vamos determinar todas. Seguindo a exposição de (NIVEN *et al.*, 1991), se $a = b = c = 0$, então todo par (x, y) de inteiros é solução de 2.1, ou então, se $a = b = 0 \neq c$, não há solução. Suponha agora que pelo menos a ou b é não nulo e faça $d = \text{mdc}(a, b)$. Se d não divide c, então também não há solução. Por outro lado, pelo teorema 2.6.1, existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = d$, e portanto, se $d|c$, então o par $(cx_0/d, cy_0/d)$ é uma solução inteira da equação 2.1. Podemos encontrar x_0 e y_0 utilizando o algoritmo de Euclides, como feito anteriormente. Uma vez de posse de uma solução, digamos, $ax_1 + by_1 = c$, outras são encontradas ao tomarmos $x = x_1 + tb/d, y = y_1 - ta/d$. Aqui, t é um inteiro qualquer. Assim, 2.1 tem infinitas soluções inteiras caso possua uma. Agora mostramos que 2.1 não possui soluções além das que já encontramos. Para tanto, suponha que os pares $(x_1, y_1), (x, y)$ são soluções inteiras. Por subtração, temos que $a(x - x_1) + b(y - y_1) = 0$. Dividimos ambos os lados por d e obtemos

$$(a/d)(x - x_1) = (b/d)(y_1 - y).$$

Ou seja, a/d divide o produto $(b/d)(y_1 - y)$. Mas $\text{mdc}(a/d, b/d) = 1$, pelo que temos que $a/d|y_1 - y$. Isto é, $ta/d = y_1 - y$ para algum t. Substituindo na equação acima, encontramos $x - x_1 = tb/d$. Assim, demonstramos o seguinte teorema.

Teorema 2.6.3. Dada a equação $ax + by = c$ com $\text{mdc}(a, b)|c$ e (x_0, y_0) uma solução particular, então toda solução inteira é dada parametricamente por:

$$x = x_0 + \left(\frac{b}{d}\right)t$$
$$y = y_0 - \left(\frac{a}{d}\right)t$$

Pode ser bastante tedioso buscar uma parametrização para uma equação específica da forma 2.1 através da manipulação explícita de equações. Entretanto, no capítulo seguinte abordaremos alguns fundamentos de sistemas lineares e álgebra linear que nos permitirão construir um algoritmo muito prático para aplicar esses conceitos à solução de equações diofantinas e sistemas de equações lineares inteiras em geral.

3 SISTEMAS DE EQUAÇÕES LINEARES EM $\mathbb{Z}$

Nesta seção veremos um método prático para resolver equações diofantinas. O método adotado para resolver sistemas lineares nos reais é a eliminação Gaussiana: mostraremos aqui um método análogo, mas com as devidas restrições para permanecermos com nossas soluções nos inteiros. Chamaremos o método de eliminação inteira. O conteúdo deste capítulo é baseado fortemente em (GONDIM *et al.*, 2012).

No apêndice A foi explicado o método da eliminação Gaussiana, no qual fazemos os seguinte passos: associamos ao sistema sua forma matricial, definimos o que é uma matriz escalonada, definimos o que são operações elementares. Por fim mostramos um algoritmo de como colocar a matriz do sistema na forma escalonada por linhas. Mostramos também que é razoavelmente fácil obter esse novo sistema, que é equivalente ao primeiro, por substituição reversa.

3.1 A forma algorítmica

Fazendo uso da mesma metodologia, visto que a forma de associar a um sistema sua versão matricial é a mesma feita em $\mathbb{R}$, vamos definir o que é uma matriz estar na forma inteira escalonada por linhas. Suponha que $A_{m\times n}$ é uma matriz com todas as entradas em $\mathbb{Z}$.

Definição 3.1.1. Dizemos que $A_{m\times n}$ está na forma inteira escalonada por linhas se:

i. As linhas formadas só de zeros serão agrupadas nas linhas inferiores da matriz;
ii. O primeiro elemento não nulo de cada linha estará estritamente à direita do primeiro elemento não nulo da linha superior;

Este primeiro elemento não nulo de cada linha também será chamado de termo líder ou pivô, como no caso real, com a única diferença de que não exigiremos que este seja igual a 1. Poderá ser qualquer inteiro positivo. E esta será a única diferença entre uma matriz escalonada por linha e uma matriz nos inteiros escalonada por linha.

Diremos que uma operação numa dada matriz é unimodular se ela é da seguinte forma:

i. Trocamos duas linhas da matriz de posição;
ii. Multiplicamos uma linha por -1;
iii. Somamos duas linhas;

Se uma matriz está associada a uma operação unimodular, essa matriz será dita matriz unimodular.

Observe que o determinante de qualquer operação unimodular é ± 1, e que é possível trocar duas linhas de posição utilizando apenas as operações 2 e 3 repetidas vezes.

Proposição 3.1.1. É sempre possível através de operações unimodulares transformar a matriz

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{bmatrix} \quad \text{na matriz} \quad \begin{bmatrix} d \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

onde d é o $\text{mdc}(a_1, a_2, \ldots, a_n)$.

Demonstração. Seguimos o seguinte desenvolvimento:

i. Seja a_j o elemento de menor valor absoluto não nulo entre $a_1, a_2, \ldots, a_n$.

ii. Para cada $i \neq j$, aplique o algoritmo da divisão para obter $a_1 = k_i a_j + r_i$ com $0 \leq |r_i| < |a_j|$.

iii. Para cada $i \neq j$, faça k_i vezes a coluna j e subtraia da coluna i.

Observe que pelo algoritmo de Euclides $\text{mdc}(a_1, a_2) = \text{mdc}(a_1 - a_2 q_1, a_2) = \text{mdc}(r_1, a_2) = \text{mdc}(r_1, a_2 - r_1 q_2) = \text{mdc}(r_1, r_2) = \cdots = \text{mdc}(r_{n-1}, r_n) = \text{mdc}(r_n, 0) = r_n$. Então, o último resto não-nulo é $d = \text{mdc}(a, b)$. Definindo o

$$\text{mdc}(a_1, a_2, \ldots, a_{n-1}, a_n) = \text{mdc}(a_1, a_2, \ldots, a_{n-2}, \text{mdc}(r_n, 0)) = \text{mdc}(a_1, a_2, \ldots, a_{n-2}, r_n, 0).$$

Dessa forma escolha qualquer outro par e repita. No final só restará um único elemento não nulo, sendo este pelo Algoritmo de Euclides o MDC dos elementos n. Note que os passos acima são os mesmos do Algoritmo de Euclides, daí esse último elemento nulo também é MDC dos termos n, como queríamos demonstrar. □

Atenção ao fato de que em vez de manusear com a matriz associada ao sistema, faremos uso da matriz transposta. Isto se deve ao fato de termos construído toda a nossa teoria para matrizes escalonadas por linhas. Poderíamos ter desenvolvido toda a teoria para matrizes escalonadas por colunas, por ser bastante popular, mas preferimos manter a teoria para matrizes escalonadas por linhas.

Pelo processo de eliminação inteira, podemos colocar a matriz A^T na sua forma inteira escalonada por linhas, que denotaremos por S. Daí colocar A na sua forma escalonada é o mesmo que multiplicá-la pela esquerda por matrizes unimodulares. Denotaremos por U

a matriz dada pelo produto dessas matrizes. Logo, $U \cdot A^T = S \implies A \cdot U^T = S^T$ e denote $Z = (U^T)^{-1} \cdot \mathbf{X}$.

Perceba que $A \cdot \mathbf{x} = B \iff A(U^T)(U^T)^{-1}\mathbf{x} = B \iff S^T \cdot Z = B$. Atente-se que U é um produto de matrizes unimodulares, as quais tem determinantes iguais a ± 1. Portanto o determinante de U também será ± 1.

Afirmação 3.1.1. A matriz $(U^T)^{-1}$ tem todas as entradas inteiras.

Demonstração. Lembrando que a inversa de uma matriz quadrada qualquer M é dada por $M^{-1} = \frac{\text{adj}(M)}{\det(M)}$, na qual adj$(M)$ é a matriz adjunta de M.

Consequentemente, $(U^T)^{-1} = \frac{\text{adj}(U^T)}{\det(U^T)} = \pm\text{adj}(U^T)$.

A matriz adjunta tem como cada uma das suas entradas um subdeterminante. Determinantes são polinômios a coeficientes inteiros. Logo, se cada entrada da matriz é inteira, cada subdeterminante também será inteiro. Ou seja, adj(U^T) é uma matriz em que $u_{ij} \in \mathbb{Z}$. Isso implica que $(U)^{-1} = \pm\text{adj}(U^T)$ é um a matriz de entradas inteiras. □

Afirmação 3.1.2. O sistema $S^T \cdot Z = B$ tem soluções inteiras se, e somente se, $A \cdot \mathbf{x} = B$ tem soluções inteiras.

Demonstração. Z_0 é solução do sistema $S^T \cdot Z = B$ se, e somente se, $\mathbf{x_0} = U^T \cdot Z_0$. Daí, $x_{0j} = \sum u_{ij} z_{0i}$ e como a soma e o produto de números inteiros é ainda inteiro, e os u_{ij} são inteiros, Z_0 tem todas as entradas inteiras. □

Resumidamente poderíamos escrever o seguinte teorema:

Teorema 3.1.2. Para resolver o sistema $A \cdot \mathbf{x} = B$, usamos operações unimodulares em A para transformá-la em sua forma escalonada por linhas S^T. Assim $A \cdot \mathbf{x} = B$ tem solução em $\mathbb{Z}$, se, e somente se, $S^T \cdot Z = B$ tem solução em $\mathbb{Z}$. As soluções de $A \cdot \mathbf{x} = B$ são da forma $\mathbf{x} = U^T Z$.

Exemplo 9. Encontre todas as soluções inteiras da equação

$$3x + 2y = 17$$

utilizando o método da eliminação inteira.

$$\left[\begin{array}{c|cc} 3 & 1 & 0 \\ 2 & 0 & 1 \end{array}\right] \xrightarrow{L_1 \to L_1 - L_2} \left[\begin{array}{c|cc} 1 & 1 & -1 \\ 2 & 0 & 1 \end{array}\right] \xrightarrow{L_2 \to L_2 - 2L_1} \left[\begin{array}{c|cc} 1 & 1 & -1 \\ 0 & -2 & 3 \end{array}\right]$$

A equação $S^T \cdot Z = B$ é $\begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} 17 \end{bmatrix}$, ou seja, $z_1 = 17$ e z_2 pode ser qualquer valor inteiro, o qual denotaremos por $z_2 = t \in \mathbb{Z}$. Portanto, $Z_0 = \begin{bmatrix} 17 \\ t \end{bmatrix}$ e $x = U^t \cdot Z \Rightarrow \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & -2 \\ -1 & 3 \end{bmatrix} \cdot \begin{bmatrix} 17 \\ t \end{bmatrix} = \begin{bmatrix} 17-2t \\ -17+3t \end{bmatrix}$. Istoé, todas as soluções paramétricas são dadas por $\begin{cases} x &= 17-2t \\ y &= -17+3t \end{cases}$ com $t \in \mathbb{Z}$.

Exemplo 10. Encontre todas as soluções inteiras da equação

$$5x + 3y + 4z = 23$$

utilizando o método da eliminação inteira.

$$\left[\begin{array}{c|ccc} 5 & 1 & 0 & 0 \\ 3 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 \end{array}\right] \xrightarrow{L_1 \to L_1 - L_3} \left[\begin{array}{c|ccc} 1 & 1 & 0 & -1 \\ 3 & 0 & 1 & 0 \\ 4 & 0 & 0 & 1 \end{array}\right] \xrightarrow{L_2 \to L_2 - 3L_1}$$

$$\left[\begin{array}{c|ccc} 1 & 1 & 0 & -1 \\ 0 & -3 & 1 & 3 \\ 4 & 0 & 0 & 1 \end{array}\right] \xrightarrow{L_3 \to L_3 - 4L_1} \left[\begin{array}{c|ccc} 1 & 1 & 0 & -1 \\ 0 & -3 & 1 & 3 \\ 0 & -4 & 0 & 5 \end{array}\right]$$

A equação $S^T \cdot Z = B$ é $\begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = \begin{bmatrix} 23 \end{bmatrix}$, ou seja, $z_1 = 23$ e $z_2 = t \in \mathbb{Z}$ e $z_3 = s \in \mathbb{Z}$.

Portanto, $Z_0 = \begin{bmatrix} 23 \\ t \\ s \end{bmatrix}$ e $x = U^t \cdot Z \Rightarrow \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 & -3 & -4 \\ 0 & 1 & 0 \\ -1 & 3 & 5 \end{bmatrix} \cdot \begin{bmatrix} 23 \\ t \\ s \end{bmatrix} = \begin{bmatrix} 23-3t-4s \\ t \\ -23+3t+5s \end{bmatrix}$. Isto é, todas as soluções paramétricas são dadas por $\begin{cases} x &= 23-3t-4s \\ y &= t \\ z &= -23+3t+5s \end{cases}$ com $t, s \in \mathbb{Z}$.

Exemplo 11. Encontre todas as soluções inteiras do sistema

$$2x + y - z = 1$$

$$3x - y + z = 4$$

utilizando o método da eliminação inteira.

$$\left[\begin{array}{cc|ccc} 2 & 3 & 1 & 0 & 0 \\ 1 & -1 & 0 & 1 & 0 \\ -1 & 1 & 0 & 0 & 1 \end{array}\right] \xrightarrow[L_1 \to L_2]{L_2 \to L_1} \left[\begin{array}{cc|ccc} 1 & -1 & 0 & 1 & 0 \\ 2 & 3 & 1 & 0 & 0 \\ -1 & 1 & 0 & 0 & 1 \end{array}\right] \xrightarrow{L_2 \to L_2 - 2L_1}$$

$$\left[\begin{array}{cc|ccc} 1 & -1 & 0 & 1 & 0 \\ 0 & 5 & 1 & -2 & 0 \\ -1 & 1 & 0 & 0 & 1 \end{array}\right] \xrightarrow{L_3 \to L_3 + L_1} \left[\begin{array}{cc|ccc} 1 & -1 & 0 & 1 & 0 \\ 0 & 5 & 1 & -2 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{array}\right]$$

A equação $S^T \cdot Z = B$ é $\begin{bmatrix} 1 & 0 & 0 \\ -1 & 5 & 0 \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 4 \end{bmatrix}$, ou seja, $z_1 = 1$ e $-z - 1 + +5z_2 = 4 \Rightarrow z_2 = 1$ e z_3 pode ser qualquer valor inteiro, o qual denotaremos por $z_3 = t \in \mathbb{Z}$. Por conseguinte, $Z_0 = \begin{bmatrix} 1 \\ 1 \\ t \end{bmatrix}$ e $x = U^t \cdot Z \Rightarrow \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -2 & -1 \\ 0 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \\ t \end{bmatrix} = \begin{bmatrix} 1 \\ -1 + t \\ t \end{bmatrix}$. Isto é, todas as soluções paramétricas são dadas por $\begin{cases} x &= 1 \\ y &= -1 + t \quad \text{com } t \in \mathbb{Z}. \\ z &= t \end{cases}$

3.2 Interpretação geométrica

Um sistema de equações diofantinas lineares, assim como um sistema linear, possuindo k equações e n incógnitas pode ser representado matricialmente da seguinte forma:

$$A \cdot \mathbf{x} = B \tag{3.1}$$

Em que $A = (a_{ij})_{k \times n}$ é a matriz dos coeficientes das equações, $\mathbf{x} = (x_1, \ldots, x_n)^T$ é a matriz das incógnitas e $B = (b_1, \ldots, b_k)^T$ a matriz dos termos independentes.

Certamente, se $\mathbf{x_0}$ é uma solução particular do sistema, isto é, um vetor tal que $A \cdot \mathbf{x_0} = B$, podemos subtrair as equações e obter $A \cdot (\mathbf{x} - \mathbf{x_0}) = 0$, que, a menos de mudança de variáveis é um reticulado em $\mathbb{R}^n$. De fato, considere $\mathbf{y} = \mathbf{x} - \mathbf{x_0}$, o sistema $A\mathbf{y} = 0$ tem como solução um reticulado (de posto $r = \text{posto}(A) \leq k$) e portanto possui uma base $v_1, v_2, \ldots, v_{n-r}$. Logo, a solução geral de equações diofantinas é $\mathbf{x} = \mathbf{x_0} + a_1 v_1 + a_2 v_2 + \cdots + a_{n-r} v_{n-r}$.

Esta observação generaliza a ideia de que, numa reta, conhecido um ponto inteiro encontramos todos os outros usando um vetor diretor primitivo base do reticulado.

4 O PROBLEMA DO TROCO DE FROBENIUS

O enunciado a seguir é uma formulação clássica do problema que vamos discutir nesta seção. Imagine que você está visitando um restaurante McDonald's e pretende comprar algumas caixas de *chicken McNuggets* para a sua família. É importante que seja possível comprar um certo número de *McNuggets* de modo que não haja muita sobra, nem haja muita falta. Porém, o restaurante só vende em caixas de 4, 6 e 10. Se você combinar diferentes números dessas três caixas, haverá um certo número de *McNuggets* que você não poderá adquirir, mas que a partir do qual qualquer número maior poderá ser adquirido ao se combinar as três caixas em quantidades diferentes. Encontrar este número, esta "cota", é essencialmente no que consiste o problema do Troco de Frobenius. Curiosamente, a rede de *fast-food* chegou a lançar mais tamanhos de caixa para facilitar a compra. Podemos colocar o problema de forma abstrata perguntando qual é o maior natural que não pode ser representável como uma combinação inteira não-negativa de $a_1, \ldots, a_n$, onde estes últimos são inteiros não-negativos primos entre si. Este é o chamado problema do Troco de Frobenius, e o número a ser calculado é chamado "número de Frobenius", em homenagem à Ferdinand Georg Frobenius (1849-1917). Este problema pode parecer muito específico à princípio, porém é possível achar aplicações deste problema em muitas áreas, e vice-versa também: já foram empregados métodos de muitas áreas da matemática na tentativa de solucionar o problema do Troco de Frobenius (ALFONSIN, 2005).

4.1 Formulação geral

Definição 4.1.1. Dizemos que s é representável como uma combinação inteira não-negativa $a_1, \ldots, a_n$, com $a_i \geq 2$ e $\text{mdc}(a_1, \ldots, a_n) = 1$, caso existam inteiros $x_i \geq 0$ tais que

$$s = \sum_{i=1}^{n} x_i a_i. \tag{4.1}$$

O menor inteiro $\not{f}$ tal que qualquer $s > \not{f}$ seja representável como uma combinação inteira não-negativa de $a_1, \ldots, a_n$ é o número de Frobenius. Esse número é tradicionalmente denotado por $\not{f}(a_1, \ldots, a_n)$ (abreviado por $\not{f}$ neste texto quando conveniente).

Note que o Troco de Frobenius pode ser formulado da seguinte forma: determine o menor inteiro positivo $\not{f}$ tal que todo inteiro positivo $d > \not{f}$ pode ser escrito como combinação linear inteira de $a_1, a_2, \ldots, a_n$, coprimos, ou seja, a equação

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = d \tag{4.2}$$

possui solução não-negativa $x_i \geq 0$ para $i = 1, 2, \ldots, n$. Portanto, o problema pode ser representado por uma equação do tipo diofantina, e assim podemos dispor das ferramentas desenvolvidas nos capítulos anteriores para extrair resultados.

A seguir, demonstramos a existência de tal cota $f(a_1, \ldots, a_n)$ dadas as condições do problema.

Teorema 4.1.1. Se $\text{mdc}(a_1, \ldots, a_n) = 1$, então existe um inteiro N tal que todo inteiro $s \geq N$ pode ser escrito da forma $a_1x_1 + \cdots + a_nx_n$, com x_i não-negativo para todo $i = 1, \ldots, n$.

Demonstração. Podemos provar por indução em n (com ajuda do teorema 2.6.1) que se $\text{mdc}(a_1, a_2, \ldots, a_n) = 1$, então existem $m_1, \ldots, m_n$ tais que $m_1a_1 + \cdots + m_na_n = 1$. Sem perda de generalidade, podemos supor que os j primeiros inteiros m_i são não-negativos e os $n - j$ restantes são negativos. Considere $P := \sum_{i=1}^{j} m_ia_i$ e $Q := \sum_{i=j+1}^{n}(-m_i)a_i = P - 1$. Usando o algoritmo de Euclides da divisão, temos que todo $k \geq 0$ pode ser escrito na forma $ha_1 + h'$, com $0 \leq k' < a_1$. Portanto,

$$
\begin{aligned}
&(a_1 - 1)Q + k = (a_1 - 1)Q + ha_1 + k' = \\
&(a_1 - 1)Q + ha_1 + k'(P - Q) = (a_1 - 1)Q + ha_1 + k'P - k'Q = \\
&(a_1 - k' - 1)Q + ha_1 + k'P \quad \text{com} \quad a_1 - k' - 1 \geq 0;\ h \geq 0;\ k' \geq 0.
\end{aligned}
$$

Então P e Q pertencem ao conjunto

$$W := \{s \in \mathbb{N} \mid \exists r_1, \ldots, r_n \geq 0, \quad s = a_1r_1 + a_2r_2 + \cdots + a_nr_n\}.$$

Note que definimos W como sendo o conjunto de inteiros que podem ser escritos na forma que nos interessa.

Como a_1,P e Q pertencem a W, então, para quaisquer $c, d, e \geq 0$, temos que $ca_1 + dP + eQ \in W$. Logo provamos anteriormente que para todo $K \geq 0$ temos que $(a_1 - 1)Q_k \in W$, isto é, qualquer número maior ou igual a $(a_1 - 1)Q$ pode ser escrito na forma $a_1x_1 + a_2x_2 + \cdots + a_nx_n$, com x_i não-negativo para todo $i \in 1, \ldots, n$. □

Este resultado atesta que sempre existe uma cota a partir da qual qualquer s é representável como combinação inteira não-negativa de um conjunto de inteiros coprimos, e o processo de prova fornece um limite superior para esta cota, $f(a_1, \ldots, a_n) < (a_1 - 1)Q$. Porém, este limite superior pode ser bastante melhorado. A importância de se encontrar limites superiores para o

número de Frobenius de um determinado problema vem do fato de que é difícil encontrar soluções para n muito grande. O caso $n = 2$, como veremos, é fácil. Para o caso $n = 3$, porém, já não é possível expressar o número de Frobenius por fórmulas fechadas de um certo tipo. Apesar de existirem vários algoritmos de tempo polinomial para o cálculo de $f(a_1, a_2, a_3)$, não encontramos uma fórmula explícita para o mesmo. Por outro lado, podemos em muitos casos encontrar limites superiores para f que são satisfatórios. Por exemplo, dizemos que r é uma cota relativamente ótima para o problema de Frobenius $a_1x_1 + a_2x_2 + \cdots + a_nx_n = d$ se r é uma cota e existe uma classe de problemas sobre a qual r é ótima.

4.2 O caso n = 2

Teorema 4.2.1. Sejam p, q inteiros positivos coprimos. Então,

$$f(p, q) = pq - p - q \tag{4.3}$$

Demonstração. Como $\text{mdc}(p, q) = 1$, a proposição 2.6.2 garante que a equação diofantina $px + qy = c$ possui solução para todo $c \in \mathbb{Z}$. Por outro lado, se $(x_0, y_0) \in \mathbb{Z}^2$ é uma solução dessa equação, então, usando o algoritmo da divisão, podemos escrever $x_0 = qx_1 + x_0'$, com $0 \leq x_0' < q$. Daí, substituindo na equação, vemos que $p(qx_1 + x_0') + qy_0 = c$, donde $px_0' + q(px_1 + y_0) = c$. Portanto, o par (x_0', y_0'), com $y_0' = px_1 + y_0$ também é solução da equação.

Além disso, (x_0', y_0') é a única solução para a qual a primeira coordenada é não-negativa e menor que q.

De fato, como vimos no teorema 2.6.3, a solução geral é dada por

$$\begin{cases} x &= x_0' + qt \\ y &= y_0' - pt \end{cases}, \text{ com } t \in \mathbb{Z}.$$

Daí, se $0 \leq x < q$, segue que $0 \leq x_0' + qt < q$. Mas, como $x_0' \geq 0$, temos $qt - q < -x_0' \leq 0 \implies q(t-1) < 0 \implies t < 1 \implies t \leq 0$.

Porém, se ocorresse $t \leq -1$, seguiria que $x = x_0' + qt \leq x_0' - q < 0$. Desse modo, $t = 0$ e $(x, y) = (x_0', y_0')$. Diremos que a solução (x_0', y_0') é a solução fundamental de $px + qy = c$. Agora, note que a equação $px + qy = c$ possuirá solução em $\mathbb{N}^2$ se e somente se a solução fundamental estiver em $\mathbb{N}^2$, isto é, $y_0' \geq 0$. Com efeito, se $y_0' \in \mathbb{N}$, claramente $(x_0', y_0') \in \mathbb{N}^2$. Reciprocamente, partindo de $(x_0, y_0) \in \mathbb{N}^2$, teremos $y_0' = p\left\lfloor \frac{x_0}{q} \right\rfloor + y_0 \geq 0$.

Desse modo, para que $px+qy=c$ não possua solução em $\mathbb{N}^2$ é necessário e suficiente que $y_0' < 0$, ou seja, $y_0' \leq -1$. Nesse caso, como $c = px_0' + qy_0'$, segue que $c \leq p(q-1)+q(-1) = p(q-1)-q = pq-p-q$. Logo, $f(p,q) = pq-p-q$. □

4.3 O caso n = 3

Infelizmente, nesse caso não temos um número fechado como no caso $n=2$. Conseguimos apenas estimativas para o número de Frobenius.

Proposição 4.3.1. Se $d \geq c(\text{mdc}(a,b)-1)+\text{mmc}(a,b)-a-b+1$, então o problema do troco de Frobenius $ax+by+cz=d$; $x,y,z,a,b,c \in \mathbb{N}$; $a,b,c>0$; $\text{mdc}(a,b,c)=1$ tem solução.

Demonstração. Fixe $d \geq c(\text{mdc}(a,b)-1)+\text{mmc}(a,b)-a-b+1$.

Considere o problema em v e z a seguir: $\text{mdc}(a,b)v+cz = d' := d-\text{mmc}(a,b)+a+b-\text{mdc}(a,b)$.

Mas $d' = d-\text{mmc}(a,b)+a+b-\text{mdc}(a,b) \geq c\cdot\text{mdc}(a,b)-c-\text{mdc}(a,b)+1$.

Logo, existem v_0 e $z_0 \in \mathbb{N}$ tais que $a = m\cdot\text{mdc}(a,b)$ e $b = n\cdot\text{mdc}(a,b)$. Como o problema em x e y dado por $mx+ny = v_0+mn-m-n+1$ tem solução paara todo $v_0 \in \mathbb{N}$, tome $x_0, y_0 \in \mathbb{N}$ tais que $mx_0+ny_0 = v_0+mn-m-n+1$. Finalmente,

$$\begin{aligned} ax_0+by_0+cz_0 =& \text{mdc}(a,b)(mx_0+ny_0)+cz+0 \\ =& \text{mdc}(a,b)(v_0+mn-m-n+1)+cz_0 \\ =& \text{mdc}(a,b)v_0+cz_0+\text{mmc}(a,b)-a-b-\text{mdc}(a,b) \\ =& d-\text{mmc}(a,b)+a+b-\text{mdc}(a,b)+\text{mmc}(a,b)-a-b-\text{mdc}(a,b) \\ =& d \end{aligned}$$

Logo, (x_0,y_0,z_0) é uma solução. □

Como consequência do resultado anterior, podemos estimar o valor de $f(a_1,a_2,a_3) \leq \min\{a_k(\text{mdc}(a_i,a_j)-1)+\text{mmc}(a_i,a_j)-a_i-a_j+1\}$, com $i\neq j$, $i\neq k$; $j\neq k$.

4.4 Exercícios

Questão 1. Em um pátio do Detran, sabe-se que há 400 pneus retirados de carros e motos que foram apreendidos no mês de outubro. Quantos veículos de cada categoria foram apreendidos

sabendo que a diferença entre carros e motos é a menor possível?

Seja C o número de carros e M o número de motos presentes nesse pátio. Sabendo que cada carro possui quatro pneus e cada moto possui dois pneus, o problema pode ser representado pela equação

$$4C + 2M = 400$$

Observe que esta equação possui solução, pois $\text{mdc}(2,4)|400$. A mesma equação pode ser reescrita como

$$2C + M = 200.$$

Utilizando o método da eliminação inteira,

$$\left[\begin{array}{c|cc} 2 & 1 & 0 \\ 1 & 0 & 1 \end{array}\right] \xrightarrow[L_2 \to L_1]{L_1 \to L_2 - 2L_1} \left[\begin{array}{c|cc} 1 & 0 & 1 \\ 2 & 1 & 0 \end{array}\right] \xrightarrow{L_2 \to L_2 - 2L_1} \left[\begin{array}{c|cc} 1 & 0 & 1 \\ 0 & 1 & -2 \end{array}\right].$$

A equação $S^T \cdot Z = B$ é $[1 \quad 0] \cdot \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = [200]$, ou seja, $z_1 = 200$ e $z_2 = t \in \mathbb{Z}$. Portanto, $Z = \begin{bmatrix} 200 \\ t \end{bmatrix}$ e $X = U^t \cdot Z \implies \begin{bmatrix} C \\ M \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \cdot \begin{bmatrix} 200 \\ t \end{bmatrix} = \begin{bmatrix} t \\ 200 - 2t \end{bmatrix}$. Isto é, todas as soluções paramétricas são dadas por

$$\begin{cases} C = \quad t \\ M = \quad 200 - 2t \end{cases} \text{ com } \ t \in \mathbb{Z}.$$

Sabendo que $C > 0$ e $M > 0$, temos que $0 < t < 100$. A diferença entre o número de carros e o número de motos pode ser expressa por $C - M = t - 200 + 2t = 3t - 200$. Logo, devemos ter $t = 67$ para que a diferença $C - M$ seja a menor possível. Assim, o número de carros no pátio é 67 e o número de motos é 66.

Questão 2. Um parque de diversão cobra U$2,00 a entrada de crianças e U$5,00 a de adultos. Para que a arrecadação de um dia seja U$200,00, qual o maior número de pessoas, entre adultos e crianças, que poderiam frequentar o parque aquele dia? Quantas crianças e quantos adultos?

Consideremos c o número de crianças e a o de adultos. Como cada criança paga U$2,00 e cada adulto U$5,00 e o total faturado foi de U$200,00, a equação que modela o problema é

$$2c + 5a = 200.$$

Utilizando o método da eliminação inteira,

$$\left[\begin{array}{c|cc} 2 & 1 & 0 \\ 5 & 0 & 1 \end{array}\right] \xrightarrow{L_2 \to L_2 - 2L_1} \left[\begin{array}{c|cc} 2 & 1 & 0 \\ 1 & -2 & 1 \end{array}\right] \xrightarrow[L_1 \to L_2]{L_2 \to L_1} \left[\begin{array}{c|cc} 1 & -2 & 1 \\ 2 & 1 & 0 \end{array}\right] \xrightarrow{L_2 \to L_2 - 2L_1} \left[\begin{array}{c|cc} 1 & -2 & 1 \\ 0 & 5 & -2 \end{array}\right].$$

A equação $S^T \cdot Z = B$ é $[1 \quad 0] \cdot \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = [200]$, ou seja, $z_1 = 200$ e $z_2 = t \in \mathbb{Z}$. Portanto, $Z = \begin{bmatrix} 200 \\ t \end{bmatrix}$ e $X = U^t \cdot Z \implies \begin{bmatrix} c \\ a \end{bmatrix} = \begin{bmatrix} -2 & 5 \\ 1 & -2 \end{bmatrix} \cdot \begin{bmatrix} 200 \\ t \end{bmatrix} = \begin{bmatrix} -400 + 5t \\ 200 - 2t \end{bmatrix}$. Isto é, todas as soluções paramétricas são dadas por

$$\begin{cases} c &= -400 + 5t \\ a &= 200 - 2t \end{cases} \text{ com } t \in \mathbb{Z}.$$

Como $c = -400 + 5t > 0$ e $a = 200 - 2t > 0$, temos que $80 < t < 100$. Queremos o número máximo de pessoas, então o valor máximo para t é 99, e portanto o número de crianças presentes no parque é 95 e de adultos é 2.

Questão 3. (Problema do Século XVI) Um total de 41 pessoas entre homens, mulheres e crianças foram a um banquete e juntas gastaram 40 patacas. Cada homem pagou 4 patacas, cada mulher 3 patacas e cada criança um terço de pataca. Quantos homens, quantas mulheres e quantas crianças havia no banquete?

Consideremos as seguintes equações:

$$\begin{cases} H + M + C &= 41 \\ 4H + 3M + \frac{C}{3} &= 40 \end{cases}.$$

Multiplicando a segunda equação por 3, obtemos $12H + 9M + C = 120$. Porém, utilizando a primeira equação, obtemos uma equação diofantina de duas variáveis, como segue

$$11H + 8M + (H + M + C) = 120 \implies 11H + 8M = 79.$$

Utilizando o método da eliminação inteira,

$$\left[\begin{array}{c|cc} 11 & 1 & 0 \\ 8 & 0 & 1 \end{array}\right] \xrightarrow{L_1 \to L_1 - L_2} \left[\begin{array}{c|cc} 3 & 1 & -1 \\ 8 & 0 & 1 \end{array}\right] \xrightarrow{L_2 \to L_2 - 2L_1} \left[\begin{array}{c|cc} 3 & 1 & -1 \\ 2 & -2 & 3 \end{array}\right] \xrightarrow{L_1 \to L_1 - L_2}$$

$$\left[\begin{array}{c|cc} 1 & 3 & -4 \\ 2 & -2 & 3 \end{array}\right] \xrightarrow{L_2 \to L_2 - 2L_1} \left[\begin{array}{c|cc} 1 & 3 & -4 \\ 0 & -8 & 11 \end{array}\right].$$

A equação $S^T \cdot Z = B$ é $[1 \quad 0] \cdot \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = [79]$, ou seja, $z_1 = 79$ e $z_2 = t \in \mathbb{Z}$. Portanto, $Z = \begin{bmatrix} 79 \\ t \end{bmatrix}$ e $X = U^t \cdot Z \implies \begin{bmatrix} H \\ M \end{bmatrix} = \begin{bmatrix} 3 & -8 \\ -4 & 11 \end{bmatrix} \cdot \begin{bmatrix} 79 \\ t \end{bmatrix} = \begin{bmatrix} 237 - 8t \\ -316 + 11t \end{bmatrix}$. Isto é, todas as soluções paramétricas são dadas por

$$\begin{cases} H = 237 - 8t \\ M = -316 + 11t \end{cases} \text{ com } t \in \mathbb{Z}.$$

Como $H = 237 - 8t$ e $M = -316 + 11t$, então $\frac{316}{11} < t < \frac{237}{8}$. Logo, $t = 29$, daí $H = 5$, $M = 3$ e $C = 33$. Portanto, haviam 5 homens, 3 mulheres e 33 crianças no banquete.

5 SEMIGRUPOS NUMÉRICOS

No início do capítulo anterior (seção 4.1), colocamos o problema do Troco de Frobenius em termos de uma sequência de números que podem ser gerados através das combinações inteiras não-negativas de números pertencentes a uma sequência inicial finita. Além disso, relacionamos cada uma dessas combinações inteiras não-negativas a uma equação diofantina cujas soluções podem ser parametrizadas com auxílio do método da eliminação inteira. Essa parametrização é importante porque permite avaliar as soluções respeitando algumas restrições.

Ocorre que nós dispomos de estruturas algébricas que formalizam, entre outros conceitos, a noção de uma sequência gerada a partir de combinações inteiras de uma sequência inicial finita de inteiros positivos. Dessas estruturas, a mais importante para nós será o semigrupo, que além de conter uma sequência gerada a partir de combinações inteiras de uma sequência inicial, possui propriedades importantes como o conjunto de suas lacunas. O conjunto das lacunas de um semigrupo consiste num conjunto de todos os números em $\mathbb{N}$ que não podem ser gerados pela sequência inicial que gera o semigrupo. Se esse conjunto for finito, pela ordenação de $\mathbb{N}$ temos que ele conterá um elemento máximo. Esse elemento máximo é um Número de Frobenius, pois ele é o maior número que não pode ser expresso como combinação inteira de uma determinada sequência finita de inteiros positivos. Podemos estudar a cardinalidade do conjunto das lacunas do semigrupo e algumas outras propriedades do semigrupo para relacioná-las ao Número de Frobenius desse semigrupo, de modo que essa estrutura algébrica pode ser poderosa na nossa análise do problema do Troco de Frobenius. Ao final do capítulo, poderemos aplicar o método da eliminação inteira para determinar as propriedades de um semigrupo e assim dispormos de uma técnica formal para solucionar o problema do Troco de Frobenius.

As notações e demonstrações foram baseadas em (ROCHA, 2015).

5.1 Grupos, semigrupos e monoides

Introduziremos agora algumas estruturas algébricas que formalizam as noções do problema do Troco de Frobenius e ao mesmo tempo dão uma intuição matemática para o problema.

Definição 5.1.1. Dados os conjuntos X, Y e Z, é chamada de binária uma função f tal que

$$f : X \times Y \to Z,$$

onde $X \times Y$ denota o produto cartesiano de X e Y.

Definição 5.1.2. Um semigrupo é um conjunto munido de uma função binária associativa.

Exemplo 12. O conjunto $\mathbb{N}$ com adição.

Definição 5.1.3. Um grupo é um conjunto munido de uma função binária associativa, dotado de um elemento identidade (ou "neutro") e, para cada um de seus elementos, dotado de um elemento inverso.

Exemplo 13. O conjunto $\mathbb{Z}$ com adição.

Se descartarmos o requerimento de que um grupo seja dotado de elementos inversos, criamos uma espécie de estrutura intermediária entre grupos e semigrupos.

Definição 5.1.4. Um monoide é um semigrupo que contém o elemento identidade.

Exemplo 14. $H \subset \mathbb{N}$ fechado para adição com $0 \in H$.

No resto do texto, utilizaremos uma notação muito versátil para definir monoides que põe em evidência a sequência inicial que gera os seus elementos através de combinações inteiras. Uma tal sequência inicial finita nós chamaremos de conjunto de geradores, e fazendo todas as combinações inteiras positivas possíveis dos elementos do conjunto de geradores, nós geraremos um monoide específico para esses geradores. Os conjuntos de geradores encapsulam algumas das propriedades mais importantes dos monoides e semigrupos que geram, de modo que podemos fazer bom uso dessa notação em definições e provas.

Definição 5.1.5. Seja $H \subset \mathbb{N}$ um monoide. Seja $S \subset H$ tal que

$$\langle S \rangle := \{c_1 s_1 + c_2 s_2 \cdots + c_n s_n \mid c_1, c_2, \ldots, c_n, n \in \mathbb{N} \text{ e } s_1, s_2, \ldots, s_n \in S\}$$

e $H = \langle S \rangle$. Então S é dito um conjunto de geradores de H.

Se S é um conjunto de geradores de H, então todo elemento de H pode ser escrito como combinação linear com coeficientes em $\mathbb{N}$ de elementos de S.

Exemplo 15. $\langle 5, 8, 9 \rangle = \{0, 5, 8, 9, 10, 13, 14, 15, 16, 17, 18, 19, 20, \ldots\}$.

Definição 5.1.6. Um conjunto de geradores $S \subset H$ é dito minimal se nenhum de seus conjuntos próprios gerar H.

Não é difícil de ver que todo monoide possui conjunto minimal de geradores único e finito. A estrutura a seguir nos permite estabelecer que o conjunto minimal de geradores é finito.

5.2 Conjunto de Apèry

Definição 5.2.1. Se H é um monoide e $n \in H^*$, o conjunto $\mathrm{Ap}(n, H)$ tal que

$$\mathrm{Ap}(n, H) := \{h \in H \,|\, h - n \notin H\},$$

é o conjunto de Apèry de H com relação à n.

Exemplo 16. Considere $\mathrm{Ap}(5, \langle 5, 8, 9\rangle)$:

$$\langle 5,8,9\rangle = \{0, \cancel{5}, 8, 9, \cancel{10}, \cancel{13}, \cancel{14}, \cancel{15}, 16, 17, \cancel{18}, \cancel{19}, \cancel{20}, \dots\}$$

$$\mathrm{Ap}(5, \langle 5,8,9\rangle) = \{0, 8, 9, 16, 17\}$$

Agora, tomemos algum $m \in H$. Observe que se $m < n$, então $m \in \mathrm{Ap}(n, H)$, já que $m - n < 0$, logo $m - n \notin H$. Mas, se $m \geq n$, podemos expressar m como $m = nq + r$, $0 \leq r < n$. Daí, se $m \notin \mathrm{Ap}(n, H)$, então $(q-1)n + r \in H$. Isso indica que $m \in \mathrm{Ap}(n, H)$ se, e somente se, $q = \lfloor \frac{m}{n} \rfloor$ é o menor inteiro tal que $nq + r \in H$. Ou seja, o conjunto de Apèry tem no máximo um representante de cada classe de congruência $[0]_n, [1]_n, \dots, [n-1]_n$, de modo que

$$|\mathrm{Ap}(n, H)| \leq n. \tag{5.1}$$

A próxima proposição nos permite gerar um monoide a partir de um conjunto de Apèry. Inversamente, podemos usar o conjunto de Apèry para encontrar um conjunto de geradores de um monoide. Esse tipo de operação conecta com o processo de gerar uma sequência de combinações lineares inteiras relacionadas ao problema do Troco de Frobenius, e mais a seguir poderemos utilizar isto para encontrar um teto para cota $f(a, b)$.

Proposição 5.2.1. O conjunto $\{n\} \cup \mathrm{Ap}(n, H)^*$ é um conjunto de geradores para H.

Demonstração. Seja $m \in H$. Podemos escrever $m = nq + r$, com $0 \leq r < n$. Escolha w_r o menor elemento de H tal que $w_r \equiv r (\mathrm{mod}\ n)$. Assim, $w_r \in \mathrm{Ap}(n, H)$ e $w_r = tn + r$, com $t \leq q$. Portanto, $m = qn + r = (q-t)n + tn + r = (q-t)n + w_r \in \langle \{n\} \cup \mathrm{Ap}(n, H)^* \rangle$. □

Com isso, temos que todo monoide possui um conjunto de geradores finito, e assim o seu conjunto minimal também deve ser finito. Agora, vamos construir um conjunto de geradores minimal. Para tanto, façamos uso da seguinte definição para soma de conjuntos em $\mathbb{Z}$.

Definição 5.2.2. Se A e B são dois subconjuntos de $\mathbb{Z}$, definimos $A+B \equiv \{a+b \mid a \in A \text{ e } b \in B\}$.

Exemplo 17. Se $A = \{5,8,9,10\}$ e $H = \langle A \rangle$, então

$$H^* + H^* = \{10,13,14,15,16,17,18,19,20,\dots\}.$$

O conjunto $H^* + H^*$ é um tipo de conjunto de combinações de elementos de A. Calculando $H^* \setminus (H^* + H^*) = \{5,8,9\}$, obtemos um conjunto de geradores que já utilizamos no exemplo anterior, de modo que $H = \langle 5,8,9 \rangle$. Este tipo de construção motiva a proposição a seguir.

Proposição 5.2.2. Se $H \subset \mathbb{N}$ é um monoide, então $S = H^* \setminus (H^* + H^*)$ é um conjunto de geradores para H. Além disso, qualquer conjunto de geradores para H necessariamente contém S.

Demonstração. Vamos provar que S é um conjunto de geradores para H. Suponha que S não é um conjunto de geradores de H, ou seja, $H \setminus \langle S \rangle \neq \emptyset$. Seja $h \in H \setminus \langle S \rangle$ o elemento mínimo desse conjunto. Temos que $h \neq 0$, logo $h \in H^*$. Mas $h \notin S = H^* \setminus (H^* + H^*)$ implica em $h \in H^* + H^*$. Podemos expressar h como $h = h_1 + h_2$, com $h_1, h_2 \in H^*$. Além disso, a minimalidade de h implica que $h_1, h_2 \in \langle S \rangle$, um absurdo. Portanto, S é um conjunto de geradores de H.

Vamos provar agora que qualquer conjunto de geradores de H contém S. Seja A um conjunto de geradores de H. Se $s \in S$, então existem $a_1, \dots, a_m \in A$ tal que $s = d_1 a_1 + \cdots + d_m a_m$, onde $d_1, \dots, d_m \in \mathbb{N}$. Como $s \notin H^* + H^*$, então $s = a_i$ para algum $i \in \{1, \dots, m\}$ e portanto $s \in A$, de modo que $S \subset A$. □

5.3 Semigrupos numéricos

Definição 5.3.1. Seja H um monoide. O conjunto L tal que $L := \mathbb{N} \setminus H$ é chamado de conjunto de lacunas de H. Sua cardinalidade $|L|$ é chamada de gênero do semigrupo H, e é denotada por $g(H)$.

Como em 5.1, $|\mathrm{Ap}(n,H)| \leq n$. Ademais, para termos $|\mathrm{Ap}(n,H)| = n$, necessitamos que H contenha um representante de cada classe de congruência $[0]_n, [1]_n, \dots, [n-1]_n$. Agora, tomemos novamente w_r o menor elemento de H tal que $w_r = r \pmod n$, com $0 \leq r < n$. Fazendo $w_r = q_r n + r$, temos que $nq + r \in H \iff q \geq q_r$. Assim,

$$L \cap [r]_n = \{r, n+r, \dots, (q-1)n+r\}.$$

Portanto,

$$L := N \setminus H = \{t_1 n + 1 \mid 0 \leq t_1 < q_1\} \cup \cdots \cup \{t_{n-1} n + (n-1) \mid 0 \leq t_{n-1} < q_{n-1}\}.$$

Logo, o conjunto $\mathbb{N} \setminus H$ é finito.

Se supomos $\mathbb{N} \setminus H$ finito, podemos tomar $q \in \mathbb{N}$ suficientemente grande tal que $qn + r \in H$ para todo $r \in \{0, 1, 2, \ldots, n-1\}$, de modo que H contém representantes de todas as classes de congruência módulo n, logo $|\mathrm{Ap}(n, H)| = n$.

Definição 5.3.2. Se $H \subset \mathbb{N}$ é monoide e $L := \mathbb{N} - H$ é finito, dizemos que H é semigrupo numérico.

As lacunas são os elementos de $\mathbb{N}$ que não podem ser escritos como combinação linear natural de uma sequência finita $A \subset \mathbb{N}$, onde $\langle A \rangle = H$.

Note que, aplicando as notações já utilizadas,

$$g(H) = \sum_{i=1}^{n-1} q_i = \sum_{i=1}^{n-1} \frac{w_i - i}{n} = \frac{1}{n} \sum_{i=1}^{n-1} w_i - \frac{n-1}{2}$$

Costumamos escrever o conjunto L como $\{l_1, l_2, \ldots, l_g\}$ com $l_1 < l_2 < \ldots < l_g$ onde $g(H)$ ou simplesmente g é o gênero do semigrupo numérico H. Também escrevemos $H = \{0, n_1, n_2, \ldots\}$, com elementos em ordem crescente. Observe que n_1 é a multiplicidade de H. Claramente, $n_1 = 1$ implica $H = \mathbb{N}$ e, portanto, $L = \emptyset$. Por conta disso, iremos considerar apenas semigrupos numéricos de multiplicidade maior que 1.

Teorema 5.3.1. Seja $H = \langle A \rangle \subset \mathbb{N}$ um monoide gerado por um subconjunto $A \subset \mathbb{N}$. Então, H é um semigrupo numérico se, e somente se, $\mathrm{mdc}(A) = 1$.

Demonstração. Seja um semigrupo numérico $\langle A \rangle$ com $d = \mathrm{mdc}(A)$. Vamos provar primeiro o "se". Se $a \in \langle A \rangle$, então existem $a_1, \ldots, a_n \in A$ tal que $a = c_1 a_1 + c_2 a_2 \cdots + c_n a_n \mid c_1, c_2, \ldots, c_n \in \mathbb{N}$. Assim, $d \mid a_i$ para $i \in \{1, \ldots, n\}$ e portanto $d \mid a$. Por termos suposto $\langle A \rangle$ um semigrupo numérico, temos que $\mathbb{N} \setminus A$ é finito, e portanto existe $n \in \mathbb{N}$ tal que n e $n+1$ estão em $\langle A \rangle$. Logo, $d \mid n$ e $d \mid (n+1)$, o que implica que $d = 1$.

Vamos mostrar agora a outra direção. Nesse caso, só precisamos provar que $\mathbb{N} \setminus \langle A \rangle$ é finito. Já que $\mathrm{mdc}(A) = 1$, existem $c_1, \ldots, c_n \in \mathbb{Z}$ e $a_1, \cdots, a_n$ tais que $c_1 a_1 + \cdots + c_n a_n = 1$. Pondo os termos com os c_i negativos no segundo membro, existem $i_1, \ldots, i_k, j_1, \ldots, j_l \in \{1, \ldots, n\}$ tais que $c_{i_1} a_{i_1} + \cdots + c_{i_k} a_{i_k} = 1 - c_{j_1} a_{j_1} - \cdots - c_{j_l} a j_l$. Desse modo, pondo $s = -c_{j_1} a_{j_1} - \cdots - c_{j_l} a j_l$, temos $s, s+1 \in \langle A \rangle$.

Vamos mostrar que se $n \geq (s-1)s+(s-1)$, então $n \in \langle A \rangle$. Pelo algoritmo da divisão, existem inteiros q e r tais que $n = qs + r$ com $0 \leq r < s$. Como estamos supondo $n \geq (s-1)s+(s-1)$, temos que $q \geq s-1 \geq r$. Portanto, $n = (rs+r)+(q-r)s = r(s+1)+(q-r)s \in \langle A \rangle$. Daí segue que os elementos de $\mathbb{N} \setminus \langle A \rangle$ são estritamente menores que $(s-1)s+(s-1)$, logo $\mathbb{N} \setminus \langle A \rangle$ é finito. □

Observação: Se H é um semigrupo numérico, então l_g é o maior inteiro que não pertence à H. Se $H = \langle a_1, \ldots, a_n \rangle$, com $\text{mdc}(a_1, a_2, \ldots, a_n) = 1$, então l_g é o maior valor de b para o qual a equação diofantina

$$a_1x_1 + a_2x_2 + \cdots + a_lx_l = b,$$

com $x_i \in \mathbb{N}$ não possui solução.

5.4 Número de Frobenius e o gênero do semigrupo

Considere o semigrupo numérico H. Estamos interessados em determinar ou estimar l_g, o elemento máximo do conjunto de lacunas de H, que corresponde ao número de Frobenius da sequência dada por um conjunto de geradores para H. Podemos utilizar a fórmula para o gênero de H para deduzir uma cota inferior para l_g:

$$g = \frac{1}{n}\sum_{i=1}^{n-1} w_i - \frac{n-1}{2} \leq \frac{1}{n}(n-1)(l_g+n) - \frac{n-1}{2} \implies l_g \geq \frac{n}{n-1}g - \frac{n}{2} \tag{5.2}$$

Observando que $\frac{n}{n-1}g - \frac{n}{2}$ é decrescente como função de n, temos que seu valor máximo é obtido quando $n_1 = n = 2$ (já que nos semigrupos que estamos considerando, $n_1 > 1$). Esse valor máximo é, portanto, $2g-1$.

Note que se l é lacuna de H, então para todo $m \in H \cap [0,l]$ temos que $l-m$ é lacuna, visto que H é fechado para adição. Entretanto, se $m \in L \cap [0,l]$, não podemos dizer nada sobre $l-m$. Vamos estabelecer os casos em que podemos garantir $l-m \in H, \forall m \in L \cap [0,l]$.

Proposição 5.4.1. Para todo semigrupo numérico H temos que $l_j \leq 2j-1$, para todo $j = 1, \ldots, g$. Além disso, os seguintes fatos são equivalentes:

i. $l_j = 2j-1$

ii. $|H \cap [0,l_j]| = |L \cap [0,l_j]|$

iii. $m \in L \cap [0,l_j] \iff l_j - m \in H \cap [0,l_j]$

Demonstração. Para cada $j \in \{1,2,\ldots,g\}$, considere a função $\varphi_j : [0,l_j] \to [0,l_j]$ definida por $\varphi_j(m) = l_j - m$. Observe que φ_j é uma bijeção tal que $\varphi_j^{-1} = \varphi_j$. Além disso, como já observamos, se $m \in H$, então $l_j - m \in L$. Dessa forma, $\varphi_j(H \cap [0,l_j]) \subset L \cap [0,l_j]$. Portanto, segue que

$$l_j + 1 - j = |H \cap [0,l_j]| = |\varphi_j(H \cap [0,l_j])| \leq |L \cap [0,l_j]| = j.$$

Assim, temos $l_j \leq 2j-1$. Além disso, vale a igualdade se, e somente se, $\varphi_j(H \cap [0,l_j]) = L \cap [0,l_j]$, ou, equivalentemente, $|H \cap [0,l_j]| = |L \cap [0,l_j]|$. Por fim, como $\varphi_j^{-1} = \varphi_j$, a igualdade $\varphi_j(H \cap [0,l_j]) = L \cap [0,l_j]$ equivale a $\varphi_j(L \cap [0,l_j]) = H \cap [0,l_j]$. Essas igualdades garantem que $m \in L \cap [0,l_j] \iff l_j - m \in H$. Reciprocamente, a propriedade descrita no item (iii) garante que $\varphi_j(L \cap [0,l_j]) \subset H \cap [0,l_j]$, o que implica em $|L \cap [0,l_j]| = |H \cap [0,l_j]|$, pois φ_j é injetiva e já sabemos que $|H \cap [0,l_j]| \leq |L \cap [0,l_j]|$. □

Obtemos, portanto, que para todo semigrupo numérico $l_g \leq 2g-1$. O número de Frobenius l_g de um semigrupo de gênero g e elemento mínimo n satisfaz a seguinte condição:

$$\frac{n}{n-1}g - \frac{n}{2} \leq l_g \leq 2g-1$$

Para $n = 2$, a cota inferior coincide com a cota superior, o que suscita a seguinte definição.

Definição 5.4.1. Um semigrupo numérico é dito simétrico se l_g atinge a cota máxima, isto é, se $l_g = 2g-1$.

Exemplo 18. Considere $H = \langle 5,8 \rangle$, com conjunto de lacunas $L_{\langle 5,8 \rangle}$. Este caso com $n = 2$ termos é simples o suficiente para que possamos calcular muitos membros de H e de $L_{\langle 5,8 \rangle}$ manualmente. Além disso, podemos utilizar a fórmula para o problema do Troco de Frobenius para $n = 2$ para verificar a lacuna máxima l_g.

O número de Frobenius é $l_g = l_{14} = 8 \cdot 5 - 8 - 5 = 27$, e como $2g - 1 = 28 - 1 = 27$, temos que $\langle 5,8 \rangle$ é simétrico.

$$\langle 5,8 \rangle = \{0,5,8,10,13,15,16,18,20,21,23,24,25,26,28,29,\ldots\}$$
$$L_{\langle 5,8 \rangle} = \{1,2,3,4,6,7,9,11,12,14,17,19,22,27\}$$

O gênero do semigrupo $g = |L_{\langle 5,8 \rangle}| = 14$.

Os demais elementos de H podem ser obtidos por inspeção.

Exemplo 19. Vamos agora para um caso mais complexo, $H = \langle 5, 8, 9 \rangle$. Seja $n_1 = 5$. Para cada $r \in \{1, 2, 3, 4\}$ precisamos determinar o menor elemento $w_r \in H$ tal que $w_r \equiv r \pmod 5$. Isso equivale a resolver a equação diofantina

$$8x + 9y = 5w + r,$$

com w o menor possível, ou equivalentemente $-5w + 8x + 9y = r$. Vamos resolver usando o método da eliminação inteira.

$$\left[\begin{array}{c|ccc} -5 & 1 & 0 & 0 \\ 8 & 0 & 1 & 0 \\ 9 & 0 & 0 & 1 \end{array}\right] \xrightarrow[L_2 \to L_2 + L_1]{L_3 \to L_3 - L_1} \left[\begin{array}{c|ccc} -5 & 1 & 0 & 0 \\ 3 & 1 & 1 & 0 \\ 4 & 1 & 0 & 1 \end{array}\right] \xrightarrow{L_3 \to L_3 - L_2} \left[\begin{array}{c|ccc} -5 & 1 & 0 & 0 \\ 3 & 1 & 1 & 0 \\ 1 & 0 & -1 & 1 \end{array}\right] \xrightarrow[L_1 \to L_1 + 5L_3]{L_2 \to L_2 - 3L_3}$$

$$\left[\begin{array}{c|ccc} 0 & 1 & -5 & 5 \\ 0 & 1 & 4 & -3 \\ 1 & 0 & -1 & 1 \end{array}\right]$$

Portanto, as soluções são

$$\begin{cases} w &= t + s &\geq 0 \\ x &= -r - 5t + 4s &\geq 0 \\ y &= r + 5t - 3s &\geq 0 \end{cases}$$

Se ocorresse $t < 0$, como $r \leq 4$ teríamos $r + 5t < 0$, daí, como $y \geq 0$, seguiria que

$$3s \leq r + 5t < 0,$$

donde teríamos $s < 0$ e assim $w = t + s < 0$, o que não ocorre. Portanto, $t \geq 0$.

Desse modo, observando que $x \geq 0$, temos $4s \geq 5t + r \implies s \geq \frac{5}{4}t + \frac{r}{4}$, logo $s > t \geq 0$. Consequentemente, $w = s + t \geq 1$.

Agora note que se $r \in \{3, 4\}$ podemos tomar $t = 0$ e $s = 1$ de modo que w atinge seu menor valor $w = 1$ com $x = 4 - r \geq 0$ e $y = r - 3 \geq 0$.

Por outro lado, se $r \in \{1, 2\}$, então, para que $y \geq 0$ devemos ter $5t \geq 3s - r \geq 3 - r > 0$, logo $t > 0$. Portanto, $t \geq 1$ e, como $s > t$, segue que $s \geq 2$. Assim, nesse caso, $w \geq 3$. Então, tomando $t = 1$ e $s = 2$, temos que w atinge seu menor valor $w = 3$, e além disso $x = 3 - r \geq 0$ e $y = r - 1 \geq 0$.

Da análise anterior, segue que

$$\begin{aligned} w_1 &= 3\cdot 5+1 = 16 \\ w_2 &= 3\cdot 5+2 = 17 \\ w_3 &= 1\cdot 5+3 = 8 \\ w_4 &= 1\cdot 5+4 = 9 \end{aligned}$$

Usando o que foi visto, segue que o conjunto de lacunas do semigrupo $H = \langle 5,8,9\rangle$ é dado por

$$\begin{aligned} L &= \{1,6,11,2,7,12,3,4\} \\ &= \{1,2,3,4,6,7,11,12\}, \end{aligned}$$

onde seu gênero é $g = 8$ e sua maior lacuna é $l_g = 12$. Logo,

$$H = \{0,5,8,9,10,13,\rightarrow\},$$

onde a seta "$\rightarrow$" dentro da notação de conjuntos serve para indicar que a sequência se estende indefinidamente, com incrementos unitários.

Proposição 5.4.2. Todo semigrupo numérico gerado por dois elementos é simétrico.

Demonstração. Seja $H = \langle p,q\rangle$ com $\text{mdc}(p,q) = 1$. Já sabemos que $l_g = pq - p - q$. Falta calcularmos o gênero $g = |L|$.

Para cada $r \in \{1,2,\ldots,p-1\}$, denotando por $w_r \in H$ o menor elemento que deixa resto r na divisão por p e escrevendo $w_r = pq_r + r$ (note que $q_r = \left\lfloor \frac{w_r}{p} \right\rfloor$), segue que $L = \{1+pt_1 \mid 0 \le t_1 < q_1\} \cup \{2+pt_2 \mid 0 \le t_2 < q_2\} \cup \cdots \cup \{p-1+pt_{p-1} \mid 0 \le t_{p-1} < q_{p-1}\}$, logo $|L| = q_1 + q_2 + \cdots + q_{p-1}$.

Por outro lado, considerando a sequência $q, 2q, 3q, \ldots, (p-1)q$, temos que os termos são incongruentes módulo p dois a dois, pois $\text{mdc}(p,q) = 1$. Assim, $\{w_1, w_2, \ldots, w_{p-1}\} = \{q, 2q, \ldots, (p-1)q\}$. Logo,

$$\begin{aligned} |L| &= \left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{2q}{p} \right\rfloor + \left\lfloor \frac{3q}{p} \right\rfloor + \ldots \left\lfloor \frac{(p-1)q}{p} \right\rfloor \implies \\ 2|L| &= \left(\left\lfloor \frac{q}{p} \right\rfloor + \left\lfloor \frac{(p-1)q}{p} \right\rfloor \right) + \left(\left\lfloor \frac{2q}{p} \right\rfloor + \left\lfloor \frac{(p-2)q}{p} \right\rfloor \right) + \cdots + \left(\left\lfloor \frac{(p-1)q}{p} \right\rfloor + \left\lfloor \frac{q}{p} \right\rfloor \right) \\ &= \sum_{j=1}^{p-1} \left(\left\lfloor \frac{jq}{p} \right\rfloor + \left\lfloor \frac{(p-j)q}{p} \right\rfloor \right). \end{aligned} \tag{5.3}$$

Agora, observe que $\left\lfloor \frac{jq}{p} \right\rfloor \le \frac{jq}{p} < \left\lfloor \frac{jq}{p} \right\rfloor + 1$ implica que $-\left\lfloor \frac{jq}{p} \right\rfloor - 1 < -\frac{jq}{p} \le -\left\lfloor \frac{jq}{p} \right\rfloor$. Além disso, como $1 \le j < p$ e p não divide q, temos que $-\frac{jq}{p} \in \mathbb{Z}$. Daí, $\left\lfloor -\frac{jq}{p} \right\rfloor = -\left\lfloor \frac{jq}{p} \right\rfloor - 1$, donde

$\left\lfloor \frac{-jq}{p} \right\rfloor + \left\lfloor \frac{jq}{p} \right\rfloor = -1$. Com isso, temos $\left\lfloor \frac{jq}{p} \right\rfloor + \left\lfloor \frac{(p-j)q}{p} \right\rfloor = \left\lfloor \frac{jq}{p} \right\rfloor + \left\lfloor q + \frac{(p-j)q}{p} \right\rfloor = q + \left(\left\lfloor \frac{jq}{p} \right\rfloor + \left\lfloor \frac{-jq}{p} \right\rfloor \right) = q - 1$.

Substituindo em 5.3:

$$2g = 2|L| = \sum_{j=1}^{p-1}(q-1) = (q-1)(p-1) = pq - p - q + 1 = l_g + 1.$$

Portanto, $l_g = 2g - 1$. □

Exemplo 20. Considere $H = \langle 3,7 \rangle$, com conjunto de lacunas $L_{\langle 3,7 \rangle}$. Como $n = 2$, encontraremos manualmente os termos de H, L e, consequentemente, a lacuna máxima l_g.

De fato, $l_g = 3 \cdot 7 - 3 - 7 = 21 - 10 = 11$, $L = \{1,2,4,5,8,11\}$ e $H = \{0,3,6,7,9,10,12,\rightarrow\}$.

Daí, $g = |L_{\langle 3,7 \rangle}| = 6$ e $l_g = 11$. Assim, $l_g = 2g - 1$, ou seja, $H = \langle 3,7 \rangle$ é simétrico.

6 CONCLUSÕES

A teoria dos semigrupos numéricos encapsula muitos aspectos do problema do Troco de Frobenius, e os conceitos e teoremas associados com semigrupos podem ser de extrema utilidade para a solução do mesmo. Semigrupos são estruturas algébricas que podem ser definidas construtivamente de maneira análoga ao modo como construímos sequências quando trabalhamos com o Troco de Frobenius, ou seja, através da combinação inteira de uma sequência inicial finita de inteiros positivos. O modo de construção desses semigrupos nos permitiu analisar propriedades muito úteis, em especial o conjunto de lacunas do semigrupo. Esse conjunto de lacunas é identificado com o conjunto de números que não podem ser expressos como uma combinação de números iniciais como enunciado no problema do Troco de Frobenius. Assim, lançando mão de resultados da teoria de semigrupos, pudemos determinar quando o conjunto de lacunas de um problema pertinente é finito. Por exemplo, a definição 5.3.2 atrela a definição de semigrupo à finitude do conjunto de lacunas, e o teorema 5.3.1 fornece uma condição necessária e suficiente para que o conjunto de lacunas seja finito.

O fato de estarmos lidando com conjuntos ordenados, como estabelecido no início do capítulo 2, nos fornece que um conjunto de lacunas finito possui um elemento máximo l_g, que consiste no Número de Frobenius de um determinado problema correspondente. A equação 5.2, quando aplicada no contexto da proposição 5.4.1, nos fornece um algoritmo para calcular l_g. O algoritmo foi demonstrado no exemplo 19. Esse algoritmo utiliza o método da eliminação inteira, que foi estabelecido no contexto de solucionar equações diofantinas, utilizando as bases teóricas da divisibilidade. Esse algoritmo, portanto, conecta todos os conceitos explorados no trabalho para fornecer um procedimento relativamente simples (em termos de etapas de execução) para a busca do Número de Frobenius de sequências com mais de dois termos (mas não muito mais do que dois termos). Como vimos no final da seção 4.1, não é possível encontrar fórmulas fechadas para esses casos, portanto algoritmos como esse podem ser bastante úteis, especialmente se forem claros e intuitivos.

Vimos também ao final da seção 4.1 e na seção 4.2 que o caso $n = 2$ é simples o suficiente para fornecer uma solução analítica. Através da teoria de semigrupos, particularmente a definição 5.4.1 (de semigrupos simétricos), demonstramos que semigrupos com conjuntos minimais de dois elementos são simétricos, e aplicamos esse resultado a sequências geradas nos problemas de Troco de Frobenius com dois valores iniciais, e assim demonstramos que esses problemas sempre geram semigrupos simétricos.

REFERÊNCIAS

ALFONSIN, J. **The Diophantine Frobenius Problem**. Oxford: Oxford University Press, 2005. (Oxford lecture series in mathematics and its applications). ISBN 9780191718229.

ANTON, H.; RORRES, C. **Elementary Linear Algebra: Applications Version**. Hoboken: John Wiley & Sons, 2010. ISBN 9780470432051.

APOSTOL, T. **Introduction to Analytic Number Theory**. Nova Iorque: Springer New York, 2013. (Undergraduate Texts in Mathematics). ISBN 9781475755794.

GONDIM, R.; GUEDES, G.; NAZIAZENO, E.; MOURÃO, B. **Notas do minicurso Aritmética Linear**. Recife: VI Bienal da SBM, 2012.

HEFEZ, A. **Elementos de aritmética**. [S.l.]: SBM, 2006. (Textos Universitários). ISBN 9788585818258.

LEON, S. **Linear Algebra with Applications**. Upper Saddle River: Pearson/Prentice Hall, 2010. (Featured Titles for Linear Algebra (Introductory) Series). ISBN 9780136009290.

NIVEN, I.; ZUCKERMAN, H.; MONTGOMERY, H. **An Introduction to the Theory of Numbers**. Hoboken: Wiley, 1991. ISBN 9780471625469.

ROCHA, R. Mestrado em Matemática, **Semigrupos de Weierstrass e o ideal canônico de curvas não-trigonais.** Fortaleza: [s.n.], 2015.

SHOKRANIAN, S. **Uma Introdução à teoria dos números**. Rio de Janeiro: Ciencia Moderna, 2008. ISBN 9788573937534.

APÊNDICE A – SISTEMAS DE EQUAÇÕES LINEARES

A.1 Introdução

Em diversos contextos matemáticos, a informação costuma ser organizada em arranjos retangulares de linhas e colunas, que acabam constituindo as matrizes (ANTON; RORRES, 2010). Um tipo notório de informação a ser arranjado na forma de matriz é um sistema de equações lineares, por exemplo

$$\begin{aligned} 2x+7y &= 5 \\ -5x+3y &= 4 \end{aligned} \quad \Longrightarrow \quad \begin{bmatrix} 2 & 7 & 5 \\ -5 & 3 & 4 \end{bmatrix}.$$

Assim, sistemas de equações lineares, como as que consideramos no capítulo anterior, podem ser arranjados de forma prática e compacta. Além disso, podemos executar determinadas operações nessas matrizes para obter soluções desses sistemas de forma bastante prática. Vistas como objetos matemáticos por si mesmas, as matrizes ainda fornecem ferramentas para facilitar a manipulação dessas operações na forma de matrizes elementares no caso geral, e matrizes unimodulares no caso de soluções inteiras.

A.2 Sistemas de equações lineares

Uma *equação linear em n incógnitas* é uma equação da forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \tag{A.1}$$

De modo que $x_1, x_2, \ldots, x_n$ são variáveis, $a_1, a_2, \ldots, a_n$ são números reais, denominados *coeficientes* e b um número real, denominado *termo independente*.

Um *sistema linear* de m equações em n incógnitas é um sistema da seguinte forma(LEON, 2010)

$$\begin{aligned} a_{11}x_1 + \quad & a_{12}x_2 + \quad \cdots + \quad a_{1n}x_n = \quad b_1 \\ a_{21}x_1 + \quad & a_{22}x_2 + \quad \cdots + \quad a_{2n}x_n = \quad b_2 \\ \vdots \quad & \quad \vdots \quad \quad \ddots \quad \quad \vdots \\ a_{m1}x_1 + \quad & a_{m2}x_2 + \quad \cdots + \quad a_{mn}x_n = \quad b_m \end{aligned} \tag{A.2}$$

Uma *solução* de um sistema $m \times n$ é uma ênupla de números $(x_1, x_2, \ldots, x_n)$ que satisfazem todas as equações do sistema.

Exemplo 21. O par de equações

$$\begin{aligned} x_1 - x_2 + x_3 &= 2 \\ 2x_1 + x_2 - x_3 &= 4 \end{aligned} \tag{A.3}$$

é um sistema 2×3. Qualquer tripla da forma $(2, \alpha, \alpha)$, com $\alpha \in \mathbb{R}$ é uma solução desse sistema. Assim, este sistema possui infinitas soluções.

O conjunto de todas as soluções de um sistema linear é chamado *conjunto solução* do sistema. Determinar os conjuntos soluções de sistemas lineares significa "resolver" estes sistemas, e para tanto, contamos com diversos algoritmos que são ensinados em diferentes níveis acadêmicos. Comum a todos os estudos de resolução de sistemas lineares é a noção de sistemas equivalentes.

Definição A.2.1. Dois sistemas de equações envolvendo as mesmas variáveis são denominados **equivalentes** caso possuam o mesmo conjunto solução.

Podemos fazer algumas operações num sistema de modo a transformá-lo enquanto preservamos seu conjunto solução. Por exemplo, podemos adicionar um múltiplo de uma equação à outra equação, e o novo sistema será equivalente ao original. Podemos ver isso do seguinte modo. Se tomarmos duas equações desse sistema,

$$\begin{aligned} a_{i1}x_1 + \dots a_{in}x_n &= b_i, \\ a_{j1}x_1 + \dots a_{jn}x_n &= b_j, \end{aligned}$$

a tupla $(x_1, x_2, \dots, x_n)$ satisfaz essas equações se e somente se ela também satisfaz as equações

$$\begin{aligned} a_{i1}x_1 + \cdots + a_{in}x_n &= b_i \\ (a_{j1} + \alpha a_{i1})x_1 + \cdots + (a_{jn} + \alpha a_{in})x_n &= b_j + \alpha b_i. \end{aligned}$$

Na verdade, existem três operações que podemos realizar num sistema para obter um sistema equivalente:

i. A ordem de quaisquer duas equações pode ser trocada.
ii. Os dois lados de uma equação podem ser multiplicados por um número real não-nulo.
iii. Um múltiplo de uma equação pode ser adicionado à outra.

No método da substituição, utilizamos dessas operações elementares para obter um sistema equivalente que tenha uma forma "triangular", ou seja, um sistema em que para a k-ésima

equação $a_{k1}, a_{k2}, \ldots, a_{k(k-1)} = 0$ e $a_k \neq 0$, sendo $k = 1, \ldots n$. Podemos reescrever o sistema A.3 na forma triangular como abaixo,

$$\begin{aligned} x_1 - x_2 + x_3 &= 2 \\ x_2 - x_3 &= 0 \end{aligned}$$

de tal modo que fica claro que obtemos uma solução quando fazemos $x_1 = 2$ e $x_2 = x_3 = \alpha$, para qualquer $\alpha \in \mathbb{R}$.

A.3 Interpretação geométrica

Sabemos da geometria analítica que uma equação $r_1 : \ ax + by + c = 0$ representa uma reta no plano cartesiano. Daí, estudar a solução de um sistema de duas variáveis se torna análogo a estudar as possíveis interseções de duas retas no plano. Sendo o sistema

$$S_1 \begin{cases} r_1 : \ a_1 x + b_1 y = c_1 \\ r_2 : \ a_2 x + b_2 y = c_2 \end{cases} \tag{A.4}$$

Temos duas retas no plano cartesiano. De posse delas, podemos fazer um estudo qualitativo das soluções desse sistema. Pela intuição geométrica, o par ordenado (x, y) só pode ser solução do sistema S_1 caso o ponto (x, y) pertença às duas retas r_1 e r_2. Só existem três configurações que essas retas podem assumir relativamente, e elas vão determinar a natureza do conjunto solução do sistema S_1.

i. Se as retas r_1 e r_2 são paralelas, não há pontos (x, y) que pertençam à ambas. Logo, o sistema S_1 é impossível.

ii. Se as retas r_1 e r_2 se encontram num único ponto, isto é, as retas são transversais e existe um único ponto (x, y) que pertence a ambas. Logo, o sistema S_1 é possível e determinado, possuindo solução única.

iii. Se r_1 e r_2 possuem mais de um ponto em comum, então elas são coincidentes. Assim, existem infinitos pontos (x, y) que pertencem às ambas. Logo, S_1 é possível e diz-se indeterminado. Um sistema indeterminado possui infinitas soluções.

Podemos generalizar a associação entre retas em $\mathbb{R}^2$ e equações em duas variáveis, de modo a associarmos hiperplanos em $\mathbb{R}^n$ à equações em n variáveis. Esta intuição nos leva a enxergar o estudo de um sistema linear do tipo A.2 de forma análoga ao estudo das interseções entre hiperplanos no espaço $\mathbb{R}^n$.

A.4 Resolvendo sistemas lineares

A.4.1 Representação matricial

Quando aprendemos a resolver sistemas no colegial, nos são ensinados dois métodos: eliminação e substituição. Esses são, na verdade, duas faces do mesmo. Assim, no método da eliminação, tentamos fazer uma série de operações de tal forma a "nos livrarmos" de um certo número de variáveis, chegando assim num sistema novo, de maneira tal que seja fácil encontrar as soluções do novo sistema.

Essas operações utilizadas para chegar ao novo sistema são as três descritas anteriormente, e portanto esse novo sistema é equivalente ao primeiro. Tanto a eliminação como a substituição se valem de que é conveniente converter uma das equações do sistema em uma equação envolvendo apenas uma das variáveis. Podemos determinar o valor dessa variável e através de substituições determinar o valor das outras variáveis em outras equações uma a uma, de maneira similar.

Para formalizar esses métodos, vamos reescrever os sistemas lineares na forma de matrizes. Considerando o sistema linear A.2, podemos representar seus coeficientes numa matriz A e os termos independentes num vetor $\mathbf{b}$ da seguinte forma

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}, \quad \mathbf{b} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}.$$

Podemos juntar uma matriz B $m \times p$ ao final de uma matriz A $m \times n$ para obtermos uma *matriz aumentada* $(A|B)$. Se utilizarmos as matrizes referentes ao sistema A e $\mathbf{b}$, podemos escrever a matriz aumentada do sistema linear, $(A|\mathbf{b})$

$$\left[\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ \vdots & \ddots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} & b_m \end{array}\right]. \tag{A.5}$$

Assim, o sistema pode ser resolvido através de operações nas linhas da matriz aumentada. Essas operações correspondem às três operações mencionadas anteriormente.

Operações elementares de linha

i. Trocar duas linhas.
ii. Multiplicar uma linha por um número real não-nulo.
iii. Trocar uma linha pela sua soma com um múltiplo de outra linha.

Para completar a representação do sistema linear na forma matricial, precisamos definir operações que transformem uma equação matricial de volta na forma de sistema linear. Definamos primeiro as operações para o caso mais simples. Um *vetor* é uma matriz que possui apenas uma coluna. A *transposta* de um vetor $\mathbf{v}$ é uma representação do vetor na forma de uma linha, denotado por $\mathbf{v}^T$. Por sua vez, a *transposta* de uma matriz A, denotada por A^T, é a matriz cujas linhas correspondem às colunas da matriz original. Assim, podemos representar a matriz A por $[\mathbf{a_1}\ \mathbf{a_2}\ \mathbf{a_3} \dots\ \mathbf{a_n}]$, ou por $(\mathbf{a_1}, \mathbf{a_2}, \mathbf{a_3} \dots \mathbf{a_n})$, onde o vetor $\mathbf{a_k}$, $k = 1, 2, ..., n$ é a k-ésima coluna de A. O produto de uma matriz A por um número c, é a matriz cA cujas entradas são ca_{ij}.

Definição A.4.1. A soma de duas matrizes A e B de mesma dimensão $m \times n$ é a matriz C cuja entrada $c_{ij} = a_{ij} + b_{ij}$, para $i = 1, 2, \dots, m$, $j = 1, 2, \dots, n$.

Definição A.4.2. Se $\mathbf{a_1}, \mathbf{a_2}, \dots \mathbf{a_n}$ são vetores em $\mathbb{R}^n$ e $c_1, c_2, \dots, c_n$ são números reais (chamados *escalares*), então a soma da forma

$$c_1\mathbf{a_1} + c_2\mathbf{a_2} \dots c_n\mathbf{a_n}$$

é dita *combinação linear* dos vetores $\mathbf{a_1}, \mathbf{a_2}, \dots \mathbf{a_n}$.

Definição A.4.3. Se A é uma matriz $m \times n$ e $\mathbf{x}$ é um vetor em $\mathbb{R}^n$, então

$$A\mathbf{x} = x_1\mathbf{a_1} + x_2\mathbf{a_2} + \cdots + x_n\mathbf{a_n}.$$

Da definição acima, fica evidente que o produto de uma matriz por um vetor resulta em um novo vetor. O produto de duas matrizes fica definido do seguinte modo:

Definição A.4.4. Se A é uma matriz $m \times n$ e B é uma matriz $n \times r$, então

$$AB = (A\mathbf{b_1}, A\mathbf{b_2}, \dots, A\mathbf{b_n}).$$

Observe que a matriz AB definida acima possui dimensões $m \times r$.

Consideremos agora um sistema indeterminado em n variáveis, e imaginemos geometricamente (em $\mathbb{R}^n$). Utilizando a notação matricial que desenvolvemos acima, escrevemos o

nosso sistema na forma

$$A\mathbf{x} = \mathbf{b}.$$

Esta notação pode ser "desempacotada" através da multiplicação de matrizes, de modo a recuperarmos a notação original do nosso sistema de equações lineares.

Um sistema $A\mathbf{x} = \mathbf{b}$ é representado por uma infinidade de pontos na interseção de um conjunto de hiperplanos. Digamos que é conhecido um ponto da interseção, o vetor $\mathbf{x_0}$. Logo,

$$A(\mathbf{x} - \mathbf{x_0}) = 0$$

representa um subespaço vetorial, de modo que todos os vetores que satisfazem esta equação podem ser representados como uma combinação linear de um certo número de vetores $\mathbf{v_1}, \mathbf{v_2}, ..., \mathbf{v_k}$ e, portanto, a solução geral do sistema é da forma

$$\mathbf{x} = \mathbf{x_0} + a_1\mathbf{v_1} + a_2\mathbf{v_2} + \cdots + a_k\mathbf{v_k}. \tag{A.6}$$

A.4.2 Matrizes escalonadas por linhas

Até agora fizemos um estudo qualitativo dos sistemas lineares quanto às suas soluções. Porém não aprendemos ainda a resolver de fato um sistema. Antes disso, poderíamos nos perguntar analiticamente se ao menos é exequível resolver o sistema. Para isso, precisamos transferir o método de substituição para a notação matricial. De posse da matriz aumentada de um sistema linear, o primeiro passo envolve construir uma matriz *escalonada por linhas*, conforme definido abaixo, através de operações elementares de linha.

Definição A.4.5. Dizemos que uma matriz está na forma **escalonada por linhas** se:

i. O primeiro elemento não-nulo de uma linha não-nula qualquer é igual à 1 (este elemento é chamado de líder ou **pivô**).
ii. O pivô de uma linha inferior fica estritamente a direita do pivô da linha superior.
iii. As linhas nulas, se houverem, são agrupadas abaixo das linhas não-nulas da matriz.

O processo de construção de uma matriz escalonada por linhas a partir da matriz aumentada de um sistema é análogo ao processo de produção de um sistema "triangular" através de operações elementares nas equações desse sistema. A partir da matriz escalonada, facilmente obtemos o conjunto solução do sistema linear correspondente pelo método da substituição/eliminação. Além disso, é costume continuar o processo de eliminação até que as entradas da matriz acima de cada pivô tenham sido eliminadas. Isto leva à próxima definição:

Definição A.4.6. Uma matriz é dita da forma **escalonada reduzida** se

i. A matriz está na forma escalonada.

ii. A primeira entrada não-nula em cada linha é a única entrada não-nula em sua coluna.

A.4.3 Eliminação de Gauss

O algoritmo que consiste em colocar a matriz aumentada de um sistema linear em sua forma escalonada de modo a resolver esse sistema é chamado **Eliminação de Gauss.** O processo de se utilizar operações elementares de linha para se transformar uma matriz na sua forma escalonada reduzida é chamado *algoritmo de redução de Gauss-Jordan*.

Podemos resumir o algoritmo da eliminação de Gauss da seguinte maneira:

i. Se todas as entradas da 1ª coluna são nulas, passe para a próxima coluna que possui pelo menos uma entrada não-nula. Considere essa a primeira coluna;

ii. Se $a_{11} = 0$, troque a primeira linha com alguma linha cuja primeira entrada é não-nula;

iii. Se $a_{11} \neq 0$, multiplique toda a linha por $\frac{1}{a_{11}}$ para obter um pivô (ou *termo líder*);

iv. Elimine todos as outras entradas não nulas da 1ª coluna utilizando de operações elementares de linha;

v. Ignore a primeira linha e a primeira coluna e repita o processo para a submatriz obtida.

Exemplo 22. Vamos utilizar o algoritmo de redução de Gauss-Jordan para resolver o sistema abaixo:

$$\begin{aligned} 3x_1 \quad +4x_2 \quad\quad\quad\quad &= 2 \\ -x_2 \quad +x_3 \quad\quad &= 4 \\ -x_3 \quad -3x_4 \quad &= 3 \\ x_1 \quad +x_2 \quad +x_3 \quad +x_4 \quad &= 0 \end{aligned} \tag{A.7}$$

Após colocar o sistema na forma de equação matricial $A\mathbf{x} = \mathbf{b}$, onde $\mathbf{x} = (x_1, x_2, x_3, x_4)^T$, extraímos a matriz aumentada. Em seguida, aplicamos o algoritmo de Gauss-Jordan para obter a matriz reduzida, donde a solução do sistema fica evidente.

$$\left[\begin{array}{cccc|c} 3 & 4 & 0 & 0 & 2 \\ 0 & -1 & 1 & 0 & 4 \\ 0 & 0 & -1 & -3 & 3 \\ 1 & 1 & 1 & 1 & 0 \end{array}\right] \xrightarrow{L_1 \to L_1 - 2L_4} \left[\begin{array}{cccc|c} 1 & 2 & -2 & -2 & 2 \\ 0 & -1 & 1 & 0 & 4 \\ 0 & 0 & -1 & -3 & 3 \\ 1 & 1 & 1 & 1 & 0 \end{array}\right] \xrightarrow{L_1 \to L_1 + 2L_2}$$

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & -2 & 10 \\ 0 & -1 & 1 & 0 & 4 \\ 0 & 0 & -1 & -3 & 3 \\ 1 & 1 & 1 & 1 & 0 \end{array}\right] \xrightarrow{L_4 \to L_4 - L_1} \left[\begin{array}{cccc|c} 1 & 0 & 0 & -2 & 10 \\ 0 & -1 & 1 & 0 & 4 \\ 0 & 0 & -1 & -3 & 3 \\ 0 & 1 & 1 & 3 & -10 \end{array}\right] \xrightarrow[L_3 \to -L_3]{L_2 \to -L_2}$$

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & -2 & 10 \\ 0 & 1 & -1 & 0 & -4 \\ 0 & 0 & 1 & 3 & -3 \\ 0 & 1 & 1 & 3 & -10 \end{array}\right] \xrightarrow{L_2 \to L_2 + L_3} \left[\begin{array}{cccc|c} 1 & 0 & 0 & -2 & 10 \\ 0 & 1 & 0 & 3 & -7 \\ 0 & 0 & 1 & 3 & -3 \\ 0 & 1 & 1 & 3 & -10 \end{array}\right] \xrightarrow{L_4 \to L_4 - L_2}$$

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & -2 & 10 \\ 0 & 1 & 0 & 3 & -7 \\ 0 & 0 & 1 & 3 & -3 \\ 0 & 0 & 1 & 0 & -3 \end{array}\right] \xrightarrow{L_4 \to L_4 - L_3} \left[\begin{array}{cccc|c} 1 & 0 & 0 & -2 & 10 \\ 0 & 1 & 0 & 3 & -7 \\ 0 & 0 & 1 & 3 & -3 \\ 0 & 0 & 0 & -3 & 0 \end{array}\right] \xrightarrow{L_4 \to -\frac{1}{3} L_4}$$

$$\left[\begin{array}{cccc|c} 1 & 0 & 0 & -2 & 10 \\ 0 & 1 & 0 & 3 & -7 \\ 0 & 0 & 1 & 3 & -3 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right] \xrightarrow[L_3 \to L_3 - 3L_4]{\substack{L_1 \to L_1 + 2L_4 \\ L_2 \to L_2 - 3L_4}} \left[\begin{array}{cccc|c} 1 & 0 & 0 & 0 & -3 \\ 0 & 1 & 0 & 0 & 10 \\ 0 & 0 & 1 & 0 & -7 \\ 0 & 0 & 0 & 1 & 0 \end{array}\right]$$

Temos então que a nova equação matricial equivalente ao sistema A.7 é $I\mathbf{x} = (-3, 10, -7, 0)^T$, de modo que a solução para o sistema é $x_1 = -3$, $x_2 = 10$, $x_3 = -7$, $x_4 = 0$.

Obs.:

Por I se entende a matriz quadrada onde as únicas entradas diferentes de zero se encontram na diagonal principal e são iguais a 1. Quando a ordem da matriz não estiver clara pelo contexto, costuma-se indicar uma matriz identidade de ordem n por I_n.

A.4.4 Matrizes elementares

Definição A.4.7. Uma matriz A $n \times n$ é dita *não singular* ou *invertível* caso exista uma matriz B tal que $AB = BA = I$. A matriz B é chamada de *inverso multiplicativo* de A, e é normalmente

escrita como A^{-1}. Caso a matriz A não possua inverso multiplicativo, ela e chamada *singular*.

Caso B e C sejam ambas inversos multiplicativos de A, então

$$B = BI = B(AC) = (BA)C = IC = C$$

Assim, uma matriz invertível possui um inverso multiplicativo único. A matriz A^{-1} é mais normalmente chamada de *inversa* de A.

Retomando o conceito de sistemas equivalentes, podemos facilmente obter um sistema equivalente à $A\mathbf{x} = B$ se multiplicarmos ambos os lados por uma matriz invertível M:

$$A\mathbf{x} = b$$

$$MA\mathbf{x} = Mb$$

É evidente que uma solução da primeira equação também será solução da segunda. Se multiplicarmos os dois lados da segunda equação por M^{-1}, obtemos que os dois sistemas são equivalentes.

Esta noção é extremamente útil para representarmos operações elementares de linha. Através da definição a seguir, somos capazes de representar uma operação elementar de linha na matriz A através da multiplicação de A por uma matriz E_1.

Definição A.4.8. A matriz E resultante da aplicação de exatamente uma operação elementar de linha na matriz identidade I é chamada *matriz elementar*.

Assim, se escolhermos E_1 como sendo a matriz resultante de se executar uma troca de linhas na matriz I, a matriz E_1A será a matriz resultante de se executar esta mesma operação na matriz A. Se escolhermos diversas matrizes $E_1, E_2, \ldots, E_k$ correspondendo a diferentes operações elementares de linha cada uma, a matriz $E_k \ldots E_2E_1A$, representando a matriz A transformada por cada operação elementar em ordem, pode ser abreviada, através da multiplicação de matrizes, por E^*A, onde $E^* = E_k \ldots E_2E_1$. Esta é uma notação bastante conveniente por ser tão compacta.