UNIVERSIDADE FEDERAL DE SERGIPE - UFS
CENTRO DE CIÊNCIAS EXATAS E TECNOLOGIA - CCET
DEPARTAMENTO DE MATEMÁTICA - DMA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

SISTEMAS DE EQUAÇÕES DIOFANTINAS LINEARES

JOSÉ ANTÔNIO DOS SANTOS NETO

SÃO CRISTÓVÃO-SE
2020

JOSÉ ANTÔNIO DOS SANTOS NETO

SISTEMAS DE EQUAÇÕES DIOFANTINAS LINEARES

Dissertação apresentada ao Corpo Docente do Programa de Mestrado Profissional em Matemática (PROFMAT) da Universidade Federal de Sergipe como requisito parcial para a obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. José Anderson Valença Cardoso

SÃO CRISTÓVÃO-SE
2020

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Santos Neto, José Antônio
S237s Sistemas de equações diofantinas lineares /
José Antônio dos Santos Neto; orientador José
Anderson Valença Cardoso – São Cristóvão, 2020.
86 f. : il.

Dissertação (Mestrado Profissional em Matemática) –
Universidade Federal de Sergipe, 2020.

1. Equações diofantinas. 2. Aritmética. 3. Matrizes.
4. Algorítmos. I. Cardoso, José Anderson Valença,
orient. II. Título.

CDU: 517.956

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Sistemas de Equações Diofantinas Lineares

por

José Antonio dos Santos Neto

Aprovada pela banca examinadora:

Prof. José Anderson Valença Cardoso - UFS
Orientador

Prof. Evilson da Silva Vieira - UFS
Primeiro Examinador

Prof. Diego Ferraz de Souza - UFRN
Segundo Examinador

São Cristóvão, 17 de Fevereiro de 2021

Dedico este trabalho ao professor Edson Ferreira de Souza, amigo e mentor, que com toda dedicação e amor à profissão, apresentou-me, do ponto de vista mais entusiástico possível, a Matemática.

Agradecimentos

Agradeço primeiramente a Deus, por ter me dado saúde, força, coragem e determinação para conquistar mais uma vitória.

A minha mãe, pelo amor, carinho, afeto e atenção sempre presentes na minha existência.

A minha amada Ry, pelo companheirismo e amor a mim dedicados.

Aos demais familiares, amigos de infância, do trabalho e da vida, que mesmo não estando sempre presentes, sei que estão torcendo por mim.

Aos professores do departamento de matemática da UFS: Prof. Dr. Almir, Prof. Dr. Naldisson, Prof. Dr. Alysson, Prof. Dr. Evilson, Prof. Dr. Fábio e, especialmente, ao meu orientador Prof. Dr. Anderson, por toda dedicação, ensinamento, paciência e compreensão durante esse árduo período. Muito obrigado a todos vocês.

Aos colegas do PROFMAT: Eduardo, Vinícius e Lucas, pela amizade, companheirismo, e troca de experiência em toda essa jornada.

Enfim, agradeço a todos que de uma forma ou de outra contribuíram para a realização deste sonho.

Resumo

O presente trabalho tem como principal objetivo discutir e propor um método para encontrar todas as soluções inteiras dos sistemas de equações lineares, possíveis e indeterminados, com coeficientes e termos independentes inteiros, nomeados aqui de sistemas de equações Diofantinas lineares. Para tanto, foi necessário um prévio estudo sobre divisibilidade, divisão euclidiana, máximo divisor comum, algoritmo de Euclides e equações Diofantinas, bem como, a generalização de alguns conceitos e resultados presentes nesses tópicos. Além disso, revisamos os conteúdos básicos de matrizes e determinantes, os quais são necessários em algumas demonstrações e para compreensão do algoritmo proposto para solucionar os citados sistemas.

Palavras Chaves: Aritmética dos Inteiros, Equações Diofantinas Generalizadas, Matrizes Unimodulares, Sistemas de Equações Diofantinas Lineares, Algoritmo de Euclides Estendido Generalizado.

Abstract

The present work has as main objective to discuss and propose a method to find all possible solutions of the systems of linear equations, possible and indeterminate, with integer independent terms and coefficients, named here as systems of linear Diophantine equations. For this, it was necessary a previous study on divisibility, Euclidean division, maximum common divisor, Euclid's algorithm and Diophantine equations, as well as the generalization of some concepts and results present in these topics. In addition, we review the basic contents of matrices and determinants, which are necessary in some demonstrations and to understand the proposed algorithm to solve these systems.

Keywords: Integer Arithmetic, Generalized Diophantine Equations, Unimodular Matrices, Linear Diophantine Equation Systems, Generalized Extended Euclidean Algorithm.

Sumário

Introdução

Na busca por um tema para o presente trabalho, uma das opções cogitadas inicialmente foi abordar os conceitos fundamentais da Álgebra Linear sobre uma estrutura algébrica diferente do corpo dos reais. Mais precisamente, sobre os inteiros módulo n. Contudo, se n for um número primo, ainda teremos um corpo, e sendo n não primo, teremos uma estrutura de anel. Diante disso, optamos por iniciar nossa abordagem sobre a ótica dos inteiros modulo 1, conjunto o qual somos habituados a manejar desde o ensino fundamental.

Sendo a Álgebra Linear um ramo da Matemática que surgiu do estudo detalhado dos sistemas de equações lineares, no contexto em questão, foi conveniente começar analisando alguns sistemas em $\mathbb{Z}$. Seguindo essa linha de raciocínio, aconteceu algo, que aposto que já aconteceu com muitas pessoas que estão a procura de respostas. Em meio a uma pesquisa, você não consegue resposta para uma pergunta aparentemente básica e interessante. A primeira tentativa de preencher a lacuna falha. Você olha nos seus livros, busca na internet, pergunta aos amigos. Todas as investidas iniciais foram em vão. Você inicia novamente as tentativas e encontrar respostas para milhares de perguntas, menos para a sua. Ao mesmo tempo, você não pode acreditar que sua pergunta possa ter sido esquecida por gerações de matemáticos. Pensa até ser obvia demais para mencioná-la. Os dias passam, a dúvida continua.

Então, um dia, de uma forma ou de outra, você encontrará a resposta. No caso em questão, foi em uma das reuniões com o orientador, que sugeriu alguns artigos para leitura, entre eles o [9], que foi capaz de nortear os questionamentos feitos até então. Nele, o autor se inspira em um método bastante conhecido, mas que na literatura nacional não encontramos nenhum registro com essa aplicação em particular. A pergunta em questão era a seguinte: em quais condições, um sistema de equações lineares, possível e indeterminado, com coeficientes e termos independentes em $\mathbb{Z}$, possui soluções inteiras? Naturalmente, desdobram-se outras perguntas: quando existentes, como encontrar ou expressar todas as soluções?

Ao pensar nesse tipo de sistema que acabamos de propor, facilmente o associamos ao contexto das equações Diofantinas, o que abre espaço pra mais alguns questionamentos semelhantes aos que fizemos no parágrafo anterior: em quais condições uma generalização

das equações Diofantinas, ou seja, uma equação linear do tipo

$$a_1x_1 + a_2x_2 + ... + a_nx_n = b_1,$$

com $a_1, a_2, ..., a_n, b_1 \in \mathbb{Z}$, possui soluções inteiras? Como encontrá-las? Basicamente, são as perguntas que fizemos até aqui que impulsionam este trabalho, o qual está organizado do seguinte modo:

No Capitulo 1 tratamos de alguns tópicos relativos à Aritmética, tais como: a divisibilidade, a divisão euclidiana, o máximo divisor comum e o importante algoritmo de Euclides, um os pontos chave do nosso estudo. Abordamos ainda a definição e os métodos de resolução das equações Diofantinas com duas variáveis, bem como a generalização dessas equações e a generalização do conceito de máximo divisor comum, juntamente com algumas de suas propriedades.

Já no Capitulo 2, revisamos os conceitos e propriedades das matrizes e seus determinantes, fundamentais na resolução de sistemas de equações lineares, o que, consequentemente, foi imprescindível diante do tema que abordamos. Além de fornecerem ferramentas essenciais na demostração de alguns resultados.

Por fim, no Capitulo 3, discutimos os conceitos de transformações unimodulares, forma inteira escalonada de matrizes em $M_{m\times n}(\mathbb{Z})$ e de matrizes unimodualares. Conceitos os quais foram necessários para formalizarmos o método da eliminação inteira, que juntamente com o teorema central deste trabalho, nos permitiu descrever um algoritmo capaz de solucionar os sistema caracterizados nesta introdução.

Capítulo 1

Aritmética dos números inteiros

> A Aritmética é a base de toda a Matemática, pura ou aplicada. É a mais útil das ciências e provavelmente não existe nenhum outro ramo do conhecimento humano tão espalhado entre as massas. (LORENSATTI, E. J. C., 2012 apud Dantzig, T., 1970, p. 44.)

A Aritmética, considerada parte essencial da Teoria dos Números, teve como principal ponto de partida a obra *Os Elementos de Euclides*, de Euclides (apox. 300 a.C.), chegando ao seu auge com os trabalhos de Pierre de Fermat (1601-1665) e Leonard Euller(1707-1783). Mais adiante, no século XIX, graças a obra de Carl Friedrich Gauss (1777-1855), a Aritmética se transformou na Teoria dos Números, desenvolvendo-se grandiosamente. Entre os quatros protagonistas citados acima, surgiram outros grandes matemáticos que registraram resultados significantes em suas obras. Para um maior aprofundamento sobre o estudo da Aritmética e seus personagens vide [5].

Este capítulo foi baseado nos textos [**?**, 10, 14, 8] e parte da familiaridade do leitor com o *conjunto dos números inteiros*

$$\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\},$$

munido com as o operações de adição $(a, b) \mapsto a + b$ e de multiplicação $(a, b) \mapsto a \cdot b$ (denotaremos $a \cdot b$ ou $a \times b$ ou simplesmente ab), suas propriedades e relações de ordem. Desse conjunto, vamos relembrar apenas uma propriedade, a qual discutiremos a seguir.

1.1 O princípio da Boa Ordenação

O conjunto dos números reais, assim como o dos racionais, possuem todas as propriedades relacionadas a adição e multiplicação que o conjunto dos inteiros dispõe, contudo, existe uma propriedade adicional que caracteriza o conjunto dos inteiros e consequentemente só ele possui, o chamado Princípio da Boa Ordenação. Antes de enunciá-lo, vejamos a seguinte definição:

Definição 1.1. *Dado um subconjunto $S \subset \mathbb{Z}$, diremos que ele é limitado inferiormente se existir $c \in \mathbb{Z}$ tal que $c \leqslant x$ para todo $x \in S$. Diremos que $a \in S$ é um menor elemento de S se $a \leqslant x$ para todo $x \in S$.*

Note que a unicidade do menor elemento é bem direta, pois se a e $a^{'}$ são menores elementos, temos que $a \leq a^{'}$ e $a^{'} \leq a$, o que implica que $a = a^{'}$.

Como exemplos para a definição podemos observar o $\mathbb{Z}$, que não inferiormente e consequentemente não possui menor elemento. Ao passo que, o conjunto dos números Naturais ($\mathbb{N}$), um importante subconjunto dos inteiros, é limitado inferiormente e tem o 1 como menor elemento. O $\mathbb{N}$ é também um bom exemplo para o princípio que enunciaremos a seguir.

Principio da Boa Ordenação (P.B.O.): Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.

Trazendo o conceito da última definição para os conjuntos dos Reais ($\mathbb{R}$) e dos racionais ($\mathbb{Q}$), o intervalo $(0, 1)$, por exemplo, é limitado inferiormente por zero, porém não possui um menor elemento, pois sempre irá existir novos números racionais ou reais cada vez que nos aproximamos de zero pela esquerda.

Veja a seguir um exemplo de uma propriedade de $\mathbb{Z}$ que segue como consequência direta do P.B.O.:

Proposição 1.2. *Não existe nenhum número inteiro n tal que $0 < n < 1$.*

Demonstração.

Suponha por absurdo que existe um n que não satisfaça o que foi proposto. Logo, o conjunto $S = \{x \in \mathbb{Z} \ ; \ 0 < x < 1\}$ é não vazio, limitado inferiormente e subconjunto de $\mathbb{Z}$. Sendo assim, pelo Princípio da Boa Ordenação, S possui um menor elemento a, com $0 < a < 1$. Multiplicando esta última desigualdade por a, o que não a altera, ja que a é positivo, obtemos $0 < a^2 < a < 1$, o que implica que $a \in S$ e $a^2 < a$, o que é uma contradição, pois a e menor elemento. Portanto, $S = \varnothing$.

■

Corolário 1.3. *(PROPRIEDADE ARQUIMEDIANA) Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $nb > a$.*

Demonstração.

Da Proposição 1.2 temos que $|b| \geq 1$, pois $|b| \neq 0$ e $b \in \mathbb{Z}$. Logo

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

Agora, basta tomar $n = |a| + 1$, quando $b > 0$ e $n = -(|a| + 1)$ quando $b < 0$ para provar o que foi proposto.

■

1.2 Divisibilidade

No conjunto dos inteiros, nem sempre é possível dividir um elemento por outro, mas utilizando a próxima propriedade sempre conseguimos expressar essa possibilidade.

Definição 1.4. *Dados dois números inteiros a e b, dizemos que a divide b, ou b é múltiplo de a, e denotamos por $a|b$, quando existir um inteiro c tal que*

$$b = ac.$$

Se a não divide b, escrevemos $a \nmid b$.

Observe que o símbolo " | " não remete a uma fração, que tem a barra inclinada ou vertical, e não representa nenhuma operação. Denota apenas a veracidade da existência de um c, tal que $b = ac$. Para negar essa sentença usa-se " $\nmid$ ", que significa que não existe um inteiro c tal que $b = ac$.

Exemplo 1.5. *Como consequência direta da definição podemos observar que:*
$0|0$ (*pois* $0 = 0 \cdot n$, $\forall n \in \mathbb{Z}$) , $2|6$ (*pois* $6 = 2 \cdot 3$) *e* $-3|6$ (*pois* $6 = (-3) \cdot (-2)$).
No entanto, $4 \nmid 6$ (*pois* $\nexists\ n \in \mathbb{Z}$ *tal que* $6 = 4 \cdot n$).

A partir da definição é possível estabelecer algumas propriedades da divisão.

Proposição 1.6. *Sejam a e b números inteiros. Tem-se que:*

(i) $1|a, a|a$ *e* $a|0$.

(ii) $a|b \ \ e \ \ a \neq 0 \ \Rightarrow \ |a| \leq |b|$.

(iii) $a|b \ \ e \ \ b|a \ \Rightarrow \ |a| = |b|$.

Demonstração.

(i): Decorre das igualdades $a = a \cdot 1$, $a = 1 \cdot a$ e $0 = 0 \cdot a$.

(ii): De fato, se $a|b$, existe $c \in \mathbb{Z}$ tal que $b = ca$. Tomando módulos, temos que $|b| = |c||a|$. Como $b \neq 0$, segue que $c \neq 0$, logo $1 \leq |c|$, consequentemente, $|a| \leq |a||c| = |b|$.

(iii): De (ii) temos que: se $a|b$, então $|a| \leq |b|$ e se $b|a$, então $|b| \leq |a|$, o que implica que $|a| = |b|$.

■

Os itens (i) e (ii) da Proposição 1.6 nos dizem que todo número inteiro a é divisível por ± 1 e por $\pm a$. Observe também que (i) inclui o caso $0|0$ e, portanto, 0 tem infinitos divisores.

Proposição 1.7. *Considere a, b e c números inteiros. Se $a|b$ e $b|c$, então $a|c$.*

Demonstração.

$a|b$ e $b|c$, implica que existem inteiros k_1 e k_2 tais que

$$b = k_1 a \quad e \quad c = k_2 b.$$

Substituindo o valor de b na equação $c = k_2 b$ obtemos

$$c = k_2 k_1 a,$$

o que nos mostra que $a|c$, pois $k_1 k_2$ é um valor inteiro.

■

Exemplo 1.8. *Como* $3|15$ *e* $15|75$*, então* $3|75$.

Proposição 1.9. *Sejam* a, b, c *e* $d \in \mathbb{Z}$*, se*

$$a|b \text{ e } c|d \implies ac|bd.$$

Demonstração.

Se $a|b$ e $c|d$, então $\exists k_1, k_2 \in \mathbb{Z}$ tais que, $b = ak_1$ e $d = k_2 c$. Com isso, $bd = (k_1 k_2)(ac)$, logo, $ac|bd$.

■

Proposição 1.10. *Se* a*,* b*,* $c \in \mathbb{Z}$ *são tais que* $a|b$ *e* $a|c$*, então para todo* $x, y \in \mathbb{Z}$

$$a|(xb + yc).$$

Demonstração.

$a|b$ e $a|c$, implica que existem inteiros k_1 e k_2 tais que $b = k_1 a$ e $c = k_2 a$. Portanto

$$xb + yc = x(k_1 a) + y(k_2 a) = (xk_1 + yk_2)a$$

o que implica que $a|(xb + yc)$.

■

A Proposição acima nos mostra que: um divisor comum de dois números quaisquer, também será divisor de qualquer combinação linear formada por esses dois números. Mais à frente iremos generalizar tal resultado.

1.3 Divisão Euclidiana

Quando $b \nmid a$, $a, b \in \mathbb{Z}$ e $b \neq 0$, é sempre possível expressar a, de forma única, em função de um múltiplo de b adicionado a um resto r, também inteiro. Euclides, em sua maior obra (*Os elementos de Euclides*), utilizou de forma recorrente com números naturais esse importante resultado, mas sem nunca enunciá-lo explicitamente ou demostrá-lo. Faremos isso agora.

Teorema 1.11. *Dados a e $b \in \mathbb{Z}$, com $b \neq 0$, existe um único par de inteiros q e r tais que*

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

Demonstração.
Existência: Seja S o conjunto de todos os inteiros não-negativos que são da forma $a - by$, com $y \in \mathbb{Z}$, isto é:

$$S = \{a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

A propriedade arquimediana nos diz que existe $n \in \mathbb{Z}$ tal que $n(-b) > -a$, logo $a - nb > 0$, o que mostra que S é não vazio.

Limitado inferiormente por 0 e não vazio, pelo Princípio da Boa ordenação, o citado conjunto possui um menor elemento r. Suponhamos então que $r = a - bq$. Sabendo que $r \geq 0$, vamos mostrar que $r < |b|$. Suponhamos agora por absurdo que $r \geq |b|$. Portanto, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Porém, isso contradiz o fato de r ser o menor elemento de S, pois

$$s = r - |b| = a - bq \mp b = a - b(q \pm 1) \in S.$$

Unicidade: Suponha que $a = bq + r = bq' + r'$, onde q, q', r, $r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$. Então, teremos:

$$bq + r = bq' + r' \quad \Rightarrow \quad r - r' = b(q' - q) \quad \Rightarrow \quad b|(r - r').$$

Por outro lado,

$$0 \leq r < |b| \quad \text{e} \quad -|b| < -r' \leq 0,$$

implicando que

$$-|b| < r - r' < |b|,$$

ou seja,

$$|r - r'| < |b|.$$

Assim, $b|(r - r')$ e $|r - r'| < |b|$, o que só é possível se $|r - r'| = 0$. Logo, $r = r'$ e consequentemente $q = q'$, já que $b \neq 0$.

■

Na representação do Teorema acima, os números p e q são chamados, respectivamente, de *quociente* e *resto* da divisão de a por b. Esse resto será zero, se somente se, b divide a.

Exemplo 1.12. *O quociente e o resto da divisão de* 31 *por* 7 *são respectivamente* $q = 4$ *e* $r = 3$. *Já na divisão de* -18 *por* 7 *são* $q = -2$ *e* $r = 4$.

1.4 O Máximo Divisor Comum

Os resultados e conceitos presentes nessa seção, com pequenas alterações, encontram-se no Livro VII dos *Elementos de Euclides*.

Definição 1.13. *Um número natural d é dito máximo divisor comum (mdc) de a e b quando satisfizer as seguintes condições :*

(i) d é um divisor comum de a e b;

(ii) Se $c|a$ e $c|b$, então $c|d$.

O mdc, quando existir, será único e denotado por

$$mdc(a, b).$$

Observe-se que: a condição (i) define os divisores comuns de a e b, enquanto a condição (ii), define o maior dentre todos os divisores comuns.

No Ensino Fundamental é usual definir o *mdc* de dois números inteiros como sendo o maior elemento do conjunto de todos os divisores comuns do números em questão. Vejamos o seguinte exemplo:

Exemplo 1.14. *Seja D_x o conjunto dos divisores de x que pertencem a $\mathbb{Z}$, temos*

$$D_6 = \{-6, -3, -2, -1, 1, 2, 3, 6\} \quad e \quad D_8 = \{-8, -4, -2, -1, 1, 2, 4, 8\},$$

de modo que

$$D_6 \cap D_8 = \{-1, -2, 1, 2\}.$$

Logo, o $mdc(6, 8) = 2$.

Da forma apresentada no exemplo acima, tal definição de *mdc* não garantiria automaticamente a validade da propriedade (ii) da definição **??**, o que não trás vantagem, pois é essa propriedade que possibilita a prova de importantes resultados subsequentes.

A partir da definição é imediato observar que, dados os inteiros a e b, temos que:

- $mdc(a, b) = mdc(b, a)$;
- $mdc(a, b) = mdc(|a|, |b|)$.

Além disso, temos:

- $mdc(a, 1) = 1$;
- se $a|b$, então o $mdc(a, b) = |a|$;

Em particular, convencionamos:

- $mdc(0,0) = 0$.

Note que nesse último caso o máximo divisor comum não é o maior dos divisores comuns: como $1|0, 2|0, 3|0, ...$ não há um maior divisor comum para 0 e 0; isso é apenas um ajuste adequado.

A partir da convenção citada acima e do fato de que 1 é divisor comum de todos os números em $\mathbb{Z}$, podemos concluir que o *mdc* de dois números inteiros sempre irá existir e será no mínimo 1, quando os número em questão não forem ambos nulos. Mais a frente veremos que quando o $mdc(a,b) = 1$ a relação entre a e b será nomeada de forma especifica em relação ao *mdc*.

O próximo resultado é de fundamental importância para estabelecer o Algoritmo de Euclides, e foi também utilizado por ele para provar a existência do máximo divisor comum de dois números inteiros não negativos.

Lema 1.15. *(LEMA DE EUCLIDES) Sejam $a, b, n \in \mathbb{Z}$. Se existe o $mdc(a, b - na)$, então, o $mdc(a,b)$ existe e*

$$mdc(a,b) = mdc(a, b - na).$$

Demonstração.

Seja $d = mdc(a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que da Proposição 1.10 que d divide$(b - na) + na = b$, ou seja, d é um divisor comum de a e b. Agora, tome um c qualquer que seja divisor comum de a e b. Logo, c é um divisor comum de a e $b - na$ (combinação linear de a e b), portanto, $c|d$. Isso prova que $d = mdc(a,b)$.

■

Apresentaremos a seguir a prova construtiva das existência do *mdc*. Conhecido como *Algoritmo de Euclides*, o método, segundo HEFEZ (2016, p.77), "é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoá-lo em mais de dois milênios."

Teorema 1.16. *(ALGORITMO DE EUCLIDES) Sejam $r_0 = a$ e $r_1 = b$ números inteiros não negativos com $b \neq 0$. Se a Divisão Euclidiana for aplicado sucessivamente para se obter*

$$r_i = q_{i+1} r_{i+1} + r_{i+2},$$

com $i = 0, 1, \ldots, n-1$, $r_{n+1} = 0$ e $r_n \neq 0$, então $mdc(a,b) = r_n$.

Demonstração.

Sem perda de generalidade, suponha que $a, b \in \mathbb{N}$ e $b \leq a$. Se $b = 1$, $b = a$ ou $b|a$, nada temos a fazer, pois já vimos que, nesses casos, $mdc(a,b) = b$. Suponhamos então que $1 < b < a$ e que $b \nmid a$. Logo, pela Divisão Euclidiana, temos que

$$a = bq_1 + r_1, \quad com\ 0 < r_1 < b.$$

Com isso, teremos duas possibilidades:
a) $r_1|b$. Em tal caso, $r_1 = mdc(b, r_1)$, e, pelo Lema 1.15, concluímos que

$$r_1 = mdc(b, r_1) = mdc(b, a - q_1 b) = mdc(b, a) = mdc(a, b),$$

finalizando o algoritmo.
b) $r_1 \nmid b$. Já nesse caso, podemos efetuar a divisão de b por r_1, obtendo

$$b = r_1 q_2 + r_2, \quad com\ 0 < r_2 < r_1.$$

Novamente, temos duas possibilidades:
a') $r_2|r_1$. Nesse caso, $r_2 = mdc(r_1, r_2)$, e novamente, pelo Lema 1.15, segue que

$$r_2 = mdc(r_1, r_2) = mdc(r_1, b - q_2 r_1) = mdc(r_1, b) = mdc(a - q_1 b, b) = mdc(a, b),$$

resultado suficiente para interromper o algoritmo.
b') $r_2 \nmid r_1$. Nesse caso, podemos efetuar a divisão de r_1 por r_2, obtendo

$$r_1 = r_2 q_3 + r_3, \quad com\ 0 < r_3 < r_2.$$

O processo segue até que pare, o que sempre ocorrerá, pois, caso contrário, teríamos uma sequência de números naturais $b > r_1 > r_2 > \ldots$ que não possui menor elemento, o que iria contrariar o Principio da Boa Ordenação. Logo, para algum n, temos que $r_n|r_{n-1}$, implicando, pelo Lema de Euclides, que $mdc(a, b) = r_n$.

■

Note que, a demonstração da existência do *mdc* é construtiva. Na prática, o algoritmo que costuma ser empregado para encontra-lo é conhecido como **processo das divisões sucessivas** ou **Algoritmo de Euclides** e comumente resumido em forma de diagrama, como o que mostraremos a seguir.

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

O diagrama se traduz na seguinte regra: para se "achar" o $mdc(a, b)$, dividi-se a por b e encontra-se o "primeiro" resto r_1. O "segundo" resto r_2 é obtido pela divisão de b por r_1. O terceiro resto r_3 é obtido pela divisão de r_1 por r_2, e assim sucessivamente até encontrar um resto nulo. O último resto não nulo é o máximo divisor comum procurado.

Exemplo 1.17. *Achemos o* $mdc(630, 22)$ *a partir do Algoritmo de Euclides.*

Solução: Construindo o diagrama descrito acima, temos que:

	28	1	1	1	3
630	22	14	8	6	2
14	8	6	$\boxed{2}$	0	

Logo, $mdc(630, 22) = 2$.

A partir do algoritmo acima é possível obter as seguintes relações:

$$\begin{aligned} 630 &= 22 \times 28 + 14 \\ 22 &= 14 \times 1 + 8 \\ 14 &= 8 \times 1 + 6 \\ 8 &= 6 \times 1 + \boxed{2} \\ 6 &= 2 \times 3 + 0, \end{aligned}$$

donde, segue-se que

$$\begin{aligned} 2 &= 8 - 6 \times 1 \\ &= 8 - (14 - 8 \times 1) \\ &= -14 + 8 \times 2 \\ &= -14 + 2(22 - 14 \times 1) \\ &= 2 \times 22 - 3 \times 14 \\ &= 2 \times 22 - 3 \times (630 - 28 \times 22) \\ &= 630(-3) + 22(86). \end{aligned} \tag{1.1}$$

Observe que, através do uso do Algoritmo de Euclides de trás para frente, foi possível escrever o $mdc(630, 22) = 2$ como múltiplo de 630 somando a um múltiplo de 22. Porém, a representação do inteiro 2 como combinação linear desses números não é única. Somando e subtraindo o produto 630×22 ao segundo membro de (1.1), por exemplo, obtemos que:

$$2 = 630(-3 + 22) + 22(86 - 630) = 630(19) + 22(-544),$$

que é uma outra representação do $mdc(630, 22)$ como combinação linear de 630 e 22.

Nas próximas seções e capítulos demostraremos que é sempre possível escrever o *mdc* de números inteiros como combinação desses mesmos inteiros, além de podermos encontrar todos os outros números que façam parte dessa combinação.

1.5 Propriedades do mdc

Para auxilar na demostração dos resultados iniciais desta seção, definimos o conjunto

$$I(a,b) = \{ax + by; x, y \in \mathbb{Z}\}.$$

Note que, sendo a e b, não simultaneamente nulos, conseguimos garantir que $I(a,b) \cap \mathbb{N} \neq \emptyset$. De fato, temos que $a^2 + b^2 = a \cdot a + b \cdot b \in I(a,b) \cap \mathbb{N}$.

Em seguida utilizaremos a notação

$$d\mathbb{Z} = \{ld \in \mathbb{Z}\}$$

para representar todos os múltiplos de d.

Teorema 1.18. *Sejam a e $b \in \mathbb{Z}$, ambos não nulos. Se $d = minI(a,b) \cap \mathbb{N}$, então*

(i) d é o mdc de a e b;

(ii) $I(a,b) = d\mathbb{Z}$.

Demonstração.

(i) Para provar este item, basta mostrar que d divide qualquer elemento de $I(a,b)$ e que qualquer divisor de a e b, divide d.

Seja $z \in I(a,b)$, suponha por absurdo que $d \nmid z$. Logo, pela divisão euclidiana,

$$z = dq + r, \quad \text{com } 0 < r < d. \tag{1.2}$$

Como $z = ma + nb$ e $d = xa + yb$, para alguns $x, y, n, m \in \mathbb{Z}$, segue de (1.2) que

$$r = (m - qx)a + (n - qy)b \in I(a,b) \cap \mathbb{N}$$

o que é um absurdo, já que $d = minI(a,b) \cap \mathbb{N}$ e $r < d$. Dessa forma, d divide qualquer elemento de $I(a,b)$, em particular, $a = 1 \cdot a + 0 \cdot b$ e $b = 0 \cdot a + 1 \cdot b$.

Suponha agora que c divida a e b. Logo, pela Proposição 1.10, c divide qualquer numero inteiro da forma $ma + nb$, ou seja, c divide qualquer elemento de $I(a,b)$, e, consequentemente $c|d$.

Assim, provamos que $d = mdc(a,b)$.

(ii) Na demostração do item anterior, concluímos que todo elemento de $I(a,b)$ é múltiplo de d, portando, $I(a,b) \subset d\mathbb{Z}$. Por outro lado, para todo elemento de $d\mathbb{Z}$, temos que

$$ld = l(xa + yb) = (lx)a + (ly)b \in I(a,b)$$

e, assim sendo, $d\mathbb{Z} \subset I(a,b)$. O que nos permite concluir que $d\mathbb{Z} = I(a,b)$.

■

O resultado do item (i) também pode ser enunciado da seguinte forma:

Teorema 1.19. *(Bachet-Bézout) Sejam a e b números inteiros. Existem $x, y \in \mathbb{Z}$ tais que*

$$mdc(a, b) = ax + by.$$

Os teoremas anteriores, ao contrário do Algoritmo de Euclides, não fornecem um meio prático para obter o *mdc* de dois números, nem os inteiros x e y, porém, nos garante que tanto o *mdc* quanto os inteiros x e y existem. Como consequência direta desses teoremas, temos como exemplo o seguintes corolários:

Corolário 1.20. *Quaisquer de sejam $a, b \in \mathbb{Z}$, ambos não nulos, e $s \in \mathbb{N}$, tem-se que*

$$mdc(sa, sb) = s \cdot mdc(a, b).$$

Demonstração.

Inicialmente, observe que

$$I(sa, sb) = sI(a, b) = \{sz; z \in I(a, b)\}.$$

Como $s \in \mathbb{N}$, segue que

$$min(sI(a, b) \cap \mathbb{N}) = s\ min(I(a, b) \cap \mathbb{N}).$$

Com isso, é possível concluir o que foi proposto.

■

Corolário 1.21. *Dados $a, b \in \mathbb{Z}$, ambos não nulos, onde $d = mdc(a, b)$, tem-se que*

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

Demonstração.

Pelo Corolário anterior, como $d \neq 0$, temos que

$$d \cdot mdc\left(\frac{a}{d}, \frac{b}{d}\right) = mdc\left(d\frac{a}{d}, d\frac{b}{d}\right) = mdc(a, b) = d.$$

Então

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

■

Quando o *mdc* de dois números inteiros for igual a 1, eles serão ditos primos entre si ou coprimos. Diante dessa definição, temos o seguinte resultado:

Proposição 1.22. *Dois números inteiros a e b são primos entre si se, somente se, existem números inteiros x e y tais que $am + bn = 1$.*

Demonstração.

Sendo a e b primos entre si, então o $mdc(a, b) = 1$, o que implica, a partir do Teorema 1.19, que existem inteiros m e n tais que $ma + nb = mdc(a, b) = 1$.

Por outro lado, suponha que existam inteiros m e n tais que $ma + nb = 1$. Se $d = mdc(a, b)$, temos, pela Proposição 1.10 que $d|(ma + nb)$, o q implica que $d|1$, ou seja, $d = 1$.

■

A relação entre as estruturas aditivas e multiplicativas dos número naturais, estabelecidas na Proposição anterior, permite-nos provar diversos resultados importante, a exemplo do teorema a seguir.

Teorema 1.23. *(LEMA DE GAUSS) Sejam $a, b, c \in \mathbb{Z}$. Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.*

Demonstração.

Se $a|bc$, então existe $f \in \mathbb{Z}$ tal que $bc = af$. Como por hipótese $mdc(a, b) = 1$, pelo Corolário 1.22, temos que existe $m, n \in \mathbb{Z}$, tais que

$$1 = ma + nb.$$

Multiplicando ambos os lados da igualdade por c, obtemos

$$c = mac + nbc.$$

Substituindo bc por af, concluímos que

$$c = mac + naf = a(mc + nf)$$

e, portanto, $a|c$.

■

1.6 Equações Diofantinas

As equações Diofantinas são chamadas assim em homenagem Diofanto de Alexandria (apox. 300 d.C.). Um matemático grego, que considerado por muitos estudiosos como o "pai da Álgebra", desempenhou, nessa área, um papel semelhante ao de Euclides na Geometria. Pouco se sabe da vida de Diofanto. Da suas poucas obras que resistiram ao tempo, a mais famosa é a *Arithmetica*. Composta de 13 livros e que, segundo [5],

é caracterizada por um alto grau de habilidade matemática e de engenho, além de ser inédita para a matemática grega tradicional já desenvolvida até aquela época.

Ainda sobre a maior obra de Diofanto, não se trata de uma exposição sistemática de proposições, comum aos trabalhos da época, mas sim, de uma coleção de problemas sob forma de exemplos numéricos específicos, que tratam principalmente da busca por uma solução inteira em equações indeterminadas com coeficientes também inteiros.

A modelagem de diversos problemas aritméticos recaem sobre as clássicas equações Diofantinas do tipo

$$aX + bY = c, \quad \text{com } a, b, c \in \mathbb{Z}.$$

No entanto, essas equações nem sempre possuem soluções em $\mathbb{Z}$. Veja, por exemplo, a equação

$$2X + 6Y = 7$$

não tem solução inteira, pois, $2X + 6Y = 2(X + 3Y)$ é sempre par. Portando, nunca será 7. Dessa forma, é natural perguntar-se: em qual condição tais equações possuem soluções? E, caso as tenha, como determiná-las?

As respostas para tais perguntas serão dadas nas duas proposições a seguir.

Proposição 1.24. *Sejam a, b e $c \in \mathbb{Z}$. A equação $aX + bY = c$ admite soluções inteiras se, e somente se, $mdc(a, b)|c$.*

Demonstração.

Do Teorema 1.18, segue que

$$I(a, b) = \{ma + nb;\ m, n \in \mathbb{Z}\} = mdc(a, b)\mathbb{Z}.$$

Diante disso, é natural perceber que a igualdade $aX + bY = c$ so é verdadeira se, somente se, $c \in I(a, b)$. Contudo, isso equivale a $c \in mdc(a, b)\mathbb{Z}$, que, por sua vez, é equivalente a $mdc(a, b)|c$.

■

Observe que, dada a equação $aX + bY = c$, onde a $\neq 0$ ou $b \neq 0$ e $mdc(a, b)|c$, é sempre possível obter uma equação equivalente

$$a_1X + b_1Y = c_1$$

onde,

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

Segue dessa observação e do Corolário 1.21 que o $mdc(a_1, b_1) = 1$ e, com isso, podemos nos restringir apenas as equações do tipo

$$aX + bY = c, \quad \text{com } mdc(a, b) = 1,$$

que sempre tem soluções e uma relação que expressa os coeficientes com os menores valores possíveis.

O próximo resultado nos mostrará como determinar as infinitas soluções em $\mathbb{Z}$ de uma equação Diofantina, como a exibida acima, a partir de uma solução particular qualquer x_0, y_0.

Proposição 1.25. *Seja x_0, y_0 uma solução particular da equação $aX + bY = c$, onde $mdc(a, b) = 1$. Então essa equação admite infinitas soluções e seu conjunto é dado por*

$$S = \{x_0 + tb, y_0 - ta;\ t \in \mathbb{Z}\}.$$

Demonstração.

Sendo x_0, y_0 soluções de $aX + bY = c$, temos que

$$ax_0 + by_0 = aX + bY = c.$$

Em seguida, agrupando e colando os teremos em evidência, obtemos

$$a(X - x_0) = b(y_o - Y). \tag{1.3}$$

Como o $mdc(a, b) = 1$, segue-se que $b|(X - x_0)$. Logo,

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

Substituindo $X - x_0$ por tb em (1.3), segue que

$$y_0 - Y = ta$$

o que fornece as soluções $X = x_0 + tb$ e $Y = y_0 - ta$.

Podemos também verificar na equação dada que a solução acima a satisfaz, pois

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

■

Juntamente com o resultado acima, o Algoritmo de Euclides nos fornece ferramentas suficientes para encontrar todas as soluções, quando existirem, de qualquer equação Diofantina com duas variáveis. Vejamos os exemplos a seguir.

Exemplo 1.26. *Determine a solução geral da equação diofantina* $12x + 27y = 33$.

Solução: Como $mdc(12; 27) = 3$ *e* $3|33$*, a equação dada tem solução. Sendo assim, dividindo ambos os membros por* 3*, podemos reescrevê-la da seguinte forma:*

$$4x + 9y = 11, \quad \textit{onde agora, } mdc(4, 9) = 1.$$

De imediato, é fácil ver que $x_0 = 5$ *e* $y_0 = 1$ *é uma solução particular da última equação. Portanto, pela Proposição 1.25, seu conjunto solução é dado por*

$$S = \{(5 - 9t; 1 - 4t); t \in \mathbb{Z}\}.$$

Exemplo 1.27. *Encontremos o conjunto solução da equação* $423x + 198y = 63$.

Solução: Primeiramente, vamos determinar o $mdc(423, 198)$ *utilizando o Algoritmo de Euclides.*

	2	7	3
423	198	27	9
27	$\boxed{9}$	0	

$$\begin{aligned} 423 &= 198(2) + 27 \\ 198 &= 27(7) + 9 \\ 27 &= 9(3) + 0 \end{aligned}$$

Logo, como $mdc(423, 198) = 9$ *e* $9|63$*, a equação Diofantina possui solução. Em seguida, reescrevendo o Algoritmo de Euclides de trás pra frente temos que*

$$9 = 198 - 27(7) = 198 - (423 - 198(2))7 = (-7)423 + (15)198.$$

Agora, multiplicamos ambos os lados por 7*, pois* $63 = 9 \cdot 7$*, segue que*

$$(-49)423 + (105)198 = 63.$$

Com isso, obtemos uma solução particular para equação inicial, porém, para chegarmos a solução geral, precisamos dividir a última relação por $mdc(423, 198)$*, obtendo assim a relação equivalente*

$$(-49)47 + (105)22 = 7.$$

Por fim, pela Proposição 1.25, temos que o conjunto solução da equação dada será

$$S = \{(-49 + 22t; 105 - 47t); t \in \mathbb{Z}\}.$$

1.7 A generalização do mdc

A definição de máximo divisor comum e suas propriedades, abordadas nas Seções 1.4 e 1.5, podem ser estendida de maneira natural para três ou mais números. Vejamos a seguir.

Definição 1.28. *Um número natural d é dito mdc dos inteiros $a_1, ..., a_n$, não todos nulos, quando satisfaz as seguintes condições:*

(i) d é um divisor comum de $a_1, ..., a_n$.

(ii) Se c é um divisor comum de $a_1, ..., a_n$, então $c|d$.

O mdc, quando existe, é único e será representado por

$$mdc(a_1, ..., a_n).$$

Para calcular o *mdc* de n números inteiros, podemos lançar mão da Proposição seguinte, que se resume em um método recursivo da aplicação do Algoritmo de Euclides para $n-1$ pares de inteiros.

Proposição 1.29. *Dados números inteiros $a_1, ..., a_n$, não todos nulos, o seu mdc existe e*

$$mdc(a_1, ..., a_n) = mdc(a_1, ..., a_{n-2}, mdc(a_{n-1}, a_n)) = mdc(mdc(a_1, ..., a_{n-1}), a_n).$$

Demonstração.

Usando indução sobre n (≥ 2), para $n = 2$ nada temos a provar. Suponha agora que o resultado vale para n.

Seja d o mdc de $a_1, \ldots, mdc(a_n, a_{n+1})$, temos por definição que $d|a_1, \ldots, d|a_{n-1}$ e $d|mdc(a_n, a_{n+1})$. Logo $d|a_1, \ldots, d|a_{n-1}, d|a_n$ e $d|a_{n+1}$. Considere agora c um divisor comum de $a_1, a_2, ..., a_{n-1}, a_n, a_{n+1}$. Logo, c é um divisor comum de $a_1, ..., a_{n-1}$ e $mdc(a_n, a_{n+1})$. Portando, $c|d$. Isso implica que $d = mdc(a_1, ..., a_n, a_{n+1})$.

A segunda parte da igualdade segue os mesmos passos da demostração acima.

■

Os inteiros $a_1, ..., a_n$ também serão ditos *primos entre si ou coprimos*, quando $mdc(a_1, ..., a_n) = 1$.

Exemplo 1.30. *Para calcular o $mdc(10, 18, 24)$ basta encontrar o $mdc(18, 24)$ e em seguida o $mdc(10, mdc(18, 24))$. Ou seja,*

$$mdc(10, 18, 24) = mdc(10, mdc(18, 24)) = mdc(10, 6) = 2$$

Na sequência, vamos ampliar o resultado da Proposição 1.10 para uma quantidade qualquer de números inteiros, o que nos ajudará na demostração dos teoremas e proposições que virão logo em seguida.

Proposição 1.31. *Se $a_1, ..., a_n \in \mathbb{Z}$ são tais que $b|a_i, i = 1, ...n$, então para todo $x_1, x_2, ..., x_n \in \mathbb{Z}$*

$$b|\sum_{i=1}^{n} a_i x_i.$$

Demonstração.

Se $b|a_i$, $i = 1, 2, ..., n$, então existem $q_1, q_2, ..., q_n \in \mathbb{Z}$ tais que $a_i = bq_i$. Sendo assim,

$$\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} bq_i x_i = b\sum_{i=1}^{n} q_i x_i$$

o que implica que $b|\sum_{i=1}^{n} a_i x_i$.

■

Anteriormente, vimos que é sempre possível escrever o *mdc* de dois inteiros como uma combinação linear dos números em questão (Proposição 1.19). O mesmo acontece para o *mdc* de n número inteiros, como mostraremos no próximo Teorema:

Teorema 1.32. *Sejam $a_1, a_2, ..., a_n \in \mathbb{Z}$, não todos nulos. Se $d = min\ I(a_1, a_2, ..., a_n) \cap \mathbb{N}$, então*

(i) d é o mdc de $a_1, ..., a_n$;

(ii) $I(a_1, ..., a_n) = d\mathbb{Z}$.

Demonstração.

(i) Para provar este item, basta mostrar que d divide qualquer elemento de $I(a_1, ..., a_n)$ e que qualquer divisor de $a_1, ..., a_n$, divide d. De início, considere o conjunto

$$I(a_1, ..., a_n) = \left\{ \sum_{i=1}^{n} a_i x_i; x_i \in \mathbb{Z} \right\}.$$

Observe que, sendo $a_1, ..., a_n$, não simultaneamente nulos, conseguimos garantir que $I(a_1, ..., a_n) \cap \mathbb{N} \neq \emptyset$. De fato, basta tomar $x_i = a_i$ para $i = 1, ..., n$, que concluiremos que

$$\sum_{i=1}^{n} a_i a_i = \sum_{i=1}^{n} a_i^2 \in I(a, b) \cap \mathbb{N}.$$

Seja $z \in I(a_1, ..., a_n)$, pela divisão euclidiana temos que

$$z = dq + r, \quad \text{com } 0 \leq r < d. \tag{1.4}$$

Como $z = \sum_{i=1}^{n} a_i y_i$ e $d = \sum_{i=1}^{n} a_i x_i$, para $y_1, ..., y_n, x_1, ..., x_n \in \mathbb{Z}$, segue de (1.4) que

$$r = \sum_{i=1}^{n} a_i y_i - q \sum_{i=1}^{n} a_i x_i$$
$$r = \sum_{i=1}^{n} a_i y_i - q \cdot a_i x_i$$
$$r = \sum_{i=1}^{n} a_i (y_i - q x_i) \in I(a_1, ..., a_n) \cap \mathbb{N}.$$

Contudo, $r < d$, onde d é o menor elemento de $I(a_1, ..., a_n) \cap \mathbb{N}$. Logo, pelo Princípio da Boa Ordenação, $r = 0$, o que implica que d divide qualquer elemento de $I(a_1, ..., a_n)$. Em particular, $d|a_i, \forall\ i = 1, ..., n$, pois sempre é possível escrever a_k, $1 \leq k \leq n$, como $\sum_{i=1}^{n} a_i x_i$. Basta tomar $x_i = 1$, para $i = k$ e $x_i = 0$ para $i \neq k$.

Suponha agora que c divida $a_1, ..., a_n$, logo, pela Proposição 1.7, c divide qualquer número inteiro da forma $z = \sum_{i=1}^{n} a_i x_i$, ou seja, c divide qualquer elemento de $I(a_1, ..., a_n)$, e, consequentemente $c|d$.

Assim, provamos que $d = mdc(a_1, ..., a_n)$.

(ii) Na demostração do item anterior, concluímos que todo elemento de $I(a_1, ..., a_n)$ é múltiplo de d, portando, $I(a_1, ..., a_n) \subset d\mathbb{Z}$, onde $d\mathbb{Z} = \{ld; l \in \mathbb{Z}\}$. Por outro lado, para todo elemento de $d\mathbb{Z}$, temos que

$$ld = l \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i (l x_i) \in I(a_1, ..., a_n)$$

e, portanto, $d\mathbb{Z} \subset I(a_1, ..., a_n)$. Em conclusão temos que $d\mathbb{Z} = I(a_1, ..., a_n)$.

■

O resultado do item (i) também pode ser enunciado da seguinte forma:

Teorema 1.33. *(Generalização de Bachet-Bézout) Sejam $a_1, a_2, ..., a_n$ números inteiros. Existem $x_1, x_2, ..., x_n \in \mathbb{Z}$ tais que*

$$mdc(a_1, a_2, ..., a_n) = a_1 x_1 + a_2 x_2 + ... + a_n x_n = \sum_{i=1}^{n} a_i x_i.$$

Para exemplificar o resultado acima, usaremos o mesmo mecanismo do exemplo 1.17, só que agora aplicando o Algoritmo de Euclides de forma recursiva em pares de inteiros até acharmos o *mdc*. Algo garantido pela Proposição 1.31.

Exemplo 1.34. *Para escrevermos o $mdc(6, 14, 21)$ como combinação linear dessas inteiros, procederemos do seguinte modo:*

Solução: Primeiramente, vamos encontrar o $mdc(14, 21)$ *a partir do algoritmo de Euclides.*

	1	2
21	14	7
$\boxed{7}$	0	

$$\begin{aligned} 21 &= 14(1) + 7 \\ 14 &= 7(2) + 0 \end{aligned}$$

Em seguida, calculamos o $mdc(6, 7)$

	1	
7	6	1
$\boxed{1}$	0	

$$\begin{aligned} 7 &= 6(1) + 1 \\ 6 &= 6(1) + 0 \end{aligned}$$

Logo, pela Proposição 1.31, temos que $mdc(6, 14, 21) = 1$*. E reescrevendo as relações do algoritmo de trás pra frente, obtemos que*

$$1 = 7 - 6(1) = 21 - 14(1) - 6(1) = 21(1) + 14(-1) + 6(-1)$$

$$1 = 21(1) + 14(-1) + 6(-1). \tag{1.5}$$

A técnica usada acima nos permite escrever o *mdc* de n números inteiros como combinação linear deles, contudo, como veremos mais a frente, essa representação não é única e este método não é o mais eficiente e elaborado que temos.

Para finalizar o capítulo, vejamos o seguinte resultado:

Proposição 1.35. *A equação diofantina linear generalizada* $a_1x_1 + a_2x_2 + ... + a_nx_n = c$*,* $a_i \in \mathbb{Z}$ *e* $a_i \neq 0$ *para* $\forall i = 1, ..., n$*, com* $c \in \mathbb{Z}$ *admite solução inteiras se, e somente se,* $mdc(a_1, a_2, ..., a_n)|c$*.*

Demonstração.

Pelo Teorema 1.28, temos que

$$I(a_1, a_2, ..., a_n) = \left\{ \sum_{k=1}^{n} a_i x_i;\ x_1 \in \mathbb{Z} \right\} = mdc(a_1, a_2, ..., a_n)\mathbb{Z}.$$

É fácil perceber que a equação $a_1x_1 + a_2x_2 + ... + a_nx_n = c$ possui solução se, somente se, $c \in I(a_1, a_2, ..., a_n)$, o que é equivalente a $c \in mdc(a_1, a_2, ..., a_n)\mathbb{Z}$, que, por sua vez, é equivalente a $mdc(a_1, a_2, ..., a_n)|c$.

■

A Proposição acima nos mostra como verificar se uma equação com n variáveis e coeficientes inteiros possui ou não solução em $\mathbb{Z}$. Por exemplo, a equação

$$6x_1 + 14x_2 + 21x_3 = 11$$

tem soluções inteiras, já que $1 = mdc(6, 14, 21)|11$. Sabendo disso, para encontrarmos uma dessas soluções, basta complementarmos a técnica usada no exemplo 1.34. Isto é, após escrevermos o $mdc(6, 14, 21)$ como combinação linear dos número em questão, basta multiplicarmos toda expressão por $11/mdc(6, 14, 21)$, ou seja, multiplicar 1.5 por 11 para obtermos a expressão

$$6(-11) + 14(-11) + 21(11) = 11$$

que nos entrega a solução $(-11, -11, 11)$.

Observe que, como temos mais variáveis que equações, a solução inteira acima possivelmente não será única. Sendo assim, como encontrar ou expressar todas as soluções? No último capítulo apresentaremos um algoritmo que nos dará ferramentas suficientes para realizar tal tarefa.

Capítulo 2

Matrizes e Determinantes

Neste capítulo, que teve como referência os textos [11, 4, 3, 12], abordaremos conceitos básicos sobre matrizes, que a depender do como modo como são apresentadas podem ser vistas apenas com finalidades organizacionais, porém, são importantes ferramentas na resolução de diversos tipos de problemas, como por exemplo, os sistemas lineares, além de serem base para a Álgebra Linear.

Abordaremos também a função determinante e suas propriedades, que nos serão úteis na demostração de alguns resultados.

2.1 Matrizes

Considere a seguinte notícia:

A produção de frutas cítricas em determinado pais acontece nas regiões A, B e C. No ano de 2019, a região A produziu 18 mil toneladas de acerola, 17 mil de caju e 14 mil de laranja. Enquanto isso, a cidade B, produziu 15 mil toneladas de acerola, 16 mil de caju e 10 mil de laranja, e por fim, a região C produziu 22 toneladas de acerola, 19 mil de caju e 20 mil de laranja. Já no ano de 2020, houve uma baixa significativa na produção de frutas cítricas de todo território, as regiões A, B e C produziram respectivamente 11, 9 e 15 mil toneladas de acerola, 12, 10 e 13 mil toneladas de caju e 8, 6 e 14 mil toneladas de laranja.

Os dados contidas na notícia acima, também poderem ser apresentados da seguinte forma:

Produção de frutas cítricas (em milhares de toneladas) durante 2019			
	Acerola	Caju	Laranja
Região A	18	17	14
Região B	15	16	10
Região C	22	19	20

Produção de frutas cítricas (em milhares de toneladas) durante 2020			
	Acerola	Caju	Laranja
Região A	11	12	8
Região B	9	10	6
Região C	15	13	14

Comparando as duas formas de apresentação fica evidente a vantagem de trabalhar com informações desse tipo de maneira tabular, sendo essa disposição ordenada dos dados em forma de matriz indispensável para problemas quem envolvem uma quantidade muito grande de variáveis. Não é por acaso que softwares voltados para esse tipo de trabalho possuem uma estrutura baseada nas matrizes, como por exemplo o Excel e o Calc.

Ao abstrairmos o significado das linhas e colunas das tabelas, temos as seguintes matrizes:

$$\begin{bmatrix} 18 & 17 & 14 \\ 15 & 16 & 10 \\ 22 & 19 & 20 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 12 & 12 & 8 \\ 10 & 10 & 6 \\ 15 & 13 & 14 \end{bmatrix}$$

que são definidas formalmente do seguinte modo:

Definição 2.1. *Dados m e n em $\mathbb{N}\backslash\{0\}$, definimos uma matriz m por n (escreve-se $m\times n$) como sendo toda tabela M formada por elementos distribuídos em m linhas e n colunas. E representaremos por:*

$$M_{m\times n} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} = [a_{ij}]_{m\times n}.$$

Cada elemento é indicado por a_{ij} e é chamado de *entrada da matriz M*. O índice i indica a linha e o índice j a coluna às quais o elemento pertence, sendo as linhas enumeradas de cima para baixo (de 1 até m) e as colunas da esquerda para a direita (de 1 até n). Usaremos sempre letras maiúsculas para denotar as matrizes, e quando for necessário especificar a ordem de uma matriz M (isto é , o número de linhas e colunas), escreveremos $M_{m\times n}$. Além de utilizarmos colchetes ou parenteses. Por exemplo:

$$A_{2\times 3} = \begin{pmatrix} -3 & 5 & -1 \\ 0 & 4 & 2 \end{pmatrix}.$$

Para localizar um elemento de uma matriz dizemos a linha e a coluna que ele está. Por exemplo, o elemento da segunda linha e terceira coluna da matriz A acima é o 2, ou seja, $a_{23} = 2$.

2.2 Matrizes especiais

Há matrizes que, por apresentarem uma utilidade maior na teoria, recebem nomes especiais. Considere uma matriz com m linhas e n colunas que denotaremos por $A_{m\times n}$:

2.2.1 Matriz linha

É uma matriz do tipo $1 \times n$, isto é, tem uma única linha.
Exemplos:

$$\begin{bmatrix} 0 & 9 & -1 & 7 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 0 & 9 \end{bmatrix}.$$

2.2.2 Matriz coluna

É uma matriz do tipo $m \times 1$, ou seja, tem uma única coluna.
Exemplos:

$$\begin{bmatrix} 5 \\ 1 \\ -3 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} a \\ b \end{bmatrix}.$$

2.2.3 Matriz nula

É aquela onde todas as entradas são nulas, isto é, $a_{ij} = 0$, para todo i e j.
Exemplo:

$$A_{2\times 3} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Podemos usar a notação $0_{m\times n}$ para representar a matriz nula quando houver possibilidade de confundirmos com o número zero.

2.2.4 Matriz quadrada de ordem n

É uma matriz cujo numero de linhas é igual ao número de colunas, isto é, $m = n$.
Exemplos:

$$\begin{bmatrix} 1 & 2 & 4 \\ 6 & 5 & 7 \\ -9 & 0 & 1 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 7 \end{bmatrix}.$$

Chama-se **diagonal principal** de uma matriz quadrada de ordem n, o conjunto das entradas em que i é igual j, ou seja:

$$\{a_{ij} | i = j\} = \{a_{11}, a_{22}, a_{33}, \ldots, a_{nn}\}.$$

Chama-se **diagonal secundária** de uma matriz quadrada de ordem n, o conjunto das entradas em que a soma de i e j seja igual a $n+1$, isto é:

$$\{a_{ij} | i + j = n + 1\} = \{a_{1n}, a_{2,n-1}, a_{3,n-2}, \ldots, a_{n1}\}.$$

Exemplo: A matriz

$$M = \begin{bmatrix} 8 & 9 & -7 \\ 6 & 4 & -5 \\ -1 & 2 & 3 \end{bmatrix}$$

é quadrada de ordem 3. Sua diagonal principal é $\{8, 4, 3\}$ e sua diagonal secundária é $\{-7, 4, -1\}$.

2.2.5 Matriz diagonal

É uma matriz quadrada ($m = n$), onde $a_{ij} = 0$, para todo $i \neq j$. Isto é, os elementos que não estão na diagonal principal são zero.

Exemplos::

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & -5 & 0 \\ 0 & 0 & 4 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 5 & 0 & 0 & 0 \\ 0 & 5 & 0 & 0 \\ 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 5 \end{bmatrix}.$$

2.2.6 Matriz identidade de ordem n (I_n)

É uma matriz diagonal onde

$$\begin{cases} 1, & \text{se} \quad i = j \\ 0, & \text{se} \quad i \neq j \end{cases}.$$

Exemplos:

$$I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad \text{e} \quad I_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

2.2.7 Matriz triangular superior

É uma matriz quadrada onde todos os elementos abaixo da diagonal principal são nulos, isto é, $m = n$ e $a_{ij} = 0$, para $i > j$.

Exemplos:

$$\begin{bmatrix} 2 & -1 & 0 \\ 0 & -1 & 4 \\ 0 & 0 & 3 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} x & z \\ 0 & y \end{bmatrix}.$$

2.2.8 Matriz triangular inferior

É uma matriz quadrada em que $m = n$ e $a_{ij} = 0$, para $i < j$.

Exemplo:

$$\begin{bmatrix} 2 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 1 & 2 & 2 & 0 \\ 1 & 0 & 5 & 4 \end{bmatrix}.$$

2.2.9 Matriz simétrica

É aquela onde $m = n$ e $a_{ij} = a_{ji},\ \forall\ i, j,\ 1 \leq i, j \leq n$.

Exemplo:

$$\begin{bmatrix} 4 & 3 & -1 \\ 3 & 2 & 0 \\ -1 & 0 & 5 \end{bmatrix}.$$

Observe que, no caso de uma matriz simétrica, a parte superior é uma "reflexão" da parte inferior, em relação à diagonal principal.

2.3 Operações com Matrizes

A necessidade de estabelecer relações e efetuar certas operações com as matrizes surge naturalmente ao utilizarmos tais estruturas numéricas. Abordaremos nesta seção as relações e operações básicas entre matrizes.

2.3.1 Igualdade de Matrizes

Definição 2.2. *Duas matrizes $A_{m\times n} = [a_{ij}]$ e $B_{r\times s} = [b_{ij}]$, são ditas iguais quando têm o mesmo número de linhas ($m = r$) e de colunas ($n = s$), e todos os seus elementos correspondentes são iguais ($a_{ij} = b_{ij}$).*

Exemplo:

$$\begin{bmatrix} 4! & \frac{4}{2} \\ 3^2 & \log\ 1 \\ 1 & \sqrt{16} \end{bmatrix} = \begin{bmatrix} 24 & 2 \\ 9 & 0 \\ 1 & 4 \end{bmatrix}.$$

2.3.2 Adição

Definição 2.3. *A soma de duas matrizes de mesma ordem, $A_{m\times n} = [a_{ij}]$ e $B_{m\times n} = [b_{ij}]$, denotada por $A+B$, consiste em uma matriz $m\times n$ cujas entradas são soma dos elementos correspondentes de A e B. Simbolicamente,*

$$A + B = [a_{ij} + b_{ij}]_{m\times n}.$$

Exemplo: Na situação problema que usamos no inicio da seção, caso queiramos saber a produção total de cada fruta em cada região, basta somar as matrizes extraídas das tabelas.

$$\begin{bmatrix} 18 & 17 & 14 \\ 15 & 16 & 10 \\ 22 & 19 & 20 \end{bmatrix} + \begin{bmatrix} 12 & 12 & 8 \\ 10 & 10 & 6 \\ 15 & 13 & 14 \end{bmatrix} = \begin{bmatrix} 30 & 29 & 22 \\ 25 & 26 & 16 \\ 37 & 32 & 34 \end{bmatrix}.$$

Note que, da forma que foi definida, a soma de matrizes tem as mesmas propriedades da adição de números reais.

Propriedades:

Dadas as matrizes A, B e C de mesma ordem $m \times n$, temos:

i) $A + B = B + A$ (comutatividade)

ii) $A + (B + C) = (A + B) + C$ (associatividade)

iii) $A + 0 = A$, onde 0 denota a matriz nula $m \times n$.

A verificação dessas propriedades é simples e podem ser encontradas em [4, 1].

2.3.3 Multiplicação por Escalar

Definição 2.4. *O produto de um número k por uma matriz $A = [a_{ij}]_{m\times n}$ é definido por*

$$kA = [ka_{ij}].$$

Cada elemento da matriz kA é igual ao produto da entrada correspondente de A, pelo número k.

Exemplo:

$$4\begin{bmatrix} 2 & -5 \\ 3 & 0 \\ 1 & 6 \end{bmatrix} = \begin{bmatrix} 8 & -20 \\ 12 & 0 \\ 4 & 24 \end{bmatrix}.$$

Propriedades:

Sendo A e B matrizes de mesma ordem e k_1 e k_2 números quaisquer, tem-se que:

i) $k_1(A + B) = k_1A + k_1B$;

ii) $k_1(k_2A) = k_2(k_1A) = (k_1k_2)A$;

iii) $(k_1 + k_2)A = k_1A + k_2A$;

iv) $1A = A$.

A verificação dessas propriedades é simples. O leitor pode encontrá-las em [4, 1].

2.3.4 Transposição

Definição 2.5. *Dada uma matriz $A = [a_{ij}]_{m\times n}$, podemos obter uma outra matriz $A^t = [b_{ij}]_{n\times m}$, cujas linhas são as colunas de A, ou seja, $b_{ij} = a_{ji}$. A^t é intitulada transposta de A.*

Exemplo 1*:*

$$A = \begin{bmatrix} 7 & 1 \\ 0 & 5 \\ -1 & 4 \end{bmatrix}_{3\times 2} \Rightarrow \quad A^t = \begin{bmatrix} 7 & 0 & -1 \\ 1 & 5 & 4 \end{bmatrix}_{2\times 3}.$$

Exemplo 2*:*

$$B = \begin{bmatrix} 2 & 7 \\ 7 & 1 \end{bmatrix}_{2\times 2} \quad \Rightarrow \quad B^t = \begin{bmatrix} 2 & 7 \\ 7 & 1 \end{bmatrix}_{2\times 2}.$$

Propriedades:

i) Uma matriz é simétrica se, e somente se, ela é igual à sua transposta, isto é, se, e somente se, $A = A^t$. (vide Exemplo 2 acima.)

ii) $(A^t)^t = A$. Isto é, a transposta da transposta de uma matriz é ela mesma.

iii) $(A + B)^t = A^t + B^t$. Em palavras, a transposta de uma soma é igual à soma das transpostas.

iv) $(kA)^t = kA^t$, onde k é qualquer escalar.

A verificação dessas propriedades é simples e podemos encontrá-las em [4, 1].

2.3.5 Multiplicação de Matrizes

A definição de produto de matrizes que veremos nesta seção é fundamental para a resolução de sistemas de equações lineares com o uso de matrizes. Mas antes, vejamos um exemplo que pode ocorrer na prática.

Para calcular a pontuação geral em um determinado concurso, o candidato deve multiplicar a nota obtida em cada matéria por seu respectivo peso e em seguida somar todos os valores encontrados. Escrevendo as notas em uma matriz linha e os pesos em uma matriz coluna, a operação que vai nos fornecer a nota geral é

$$\begin{bmatrix} 4 & 5 & 3 & 2 & 3 \end{bmatrix} . \begin{bmatrix} 4 \\ 5 \\ 2 \\ 1 \\ 3 \end{bmatrix} = 4.4 + 5.5 + 3.2 + 2.1 + 3.3 = [56].$$

O exemplo acima esboça a definição de multiplicação de matrizes A e B, quando A é uma matriz linha e B uma matriz coluna. De maneira formal fica da seguinte forma:

Definição 2.6. *Sejam $A = (a_{ij})_{m\times k}$ e $B = (b_{ij})_{k\times n}$ matrizes. Consideremos a linha i de A e a coluna j de B, isto é:*

$$\begin{bmatrix} a_{i1} & a_{i2} & a_{i3} & \cdots & a_{ik} \end{bmatrix} \quad e \quad \begin{bmatrix} b_{1j} \\ b_{2j} \\ b_{3j} \\ \vdots \\ b_{kj} \end{bmatrix}.$$

O produto da linha pela coluna é dado por:

$$a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \ldots + a_{ik}b_{1k},$$

ou seja, multiplicamos, ordenadamente, os elementos da linha i pelos elementos da coluna j e somamos os resultados obtidos.

Estendendo para um caso mais geral temos a seguinte conceito.

Definição 2.7. *Sejam $A = [a_{ij}]_{m\times k}$ e $B = [b_{ij}]_{n\times s}$ duas matrizes. O produto de A por B, denotado por AB ou $A \cdot B$, é definido como sendo a matriz $C = [c_{ij}]_{m\times s}$ tal que*

$$c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = a_{i1}b_{1j} + \ldots + a_{in}b_{nj}$$

para todo $1 \leq i \leq m$ e para todo $1 \leq j \leq s$.

Exemplo:

$$\begin{bmatrix} 2 & 5 \\ 1 & 0 \\ 8 & -3 \end{bmatrix} \begin{bmatrix} -1 & 1 \\ 2 & -1 \end{bmatrix} = \begin{bmatrix} 2(-1)+5(2) & 2(1)+5(-1) \\ 1(-1)+0(2) & 1(-1)+0(1) \\ 8(-1)+(-3)(2) & 8(1)+(-3)(-1) \end{bmatrix} = \begin{bmatrix} 8 & -3 \\ -1 & -1 \\ -14 & 11 \end{bmatrix}.$$

Observação 2.8. *Se A e B são matrizes, então:*

1. *o produto AB é definido apenas quando o número de colunas de $A_{m\times n}$ for igual ao número de linhas de $B_{r\times s}$, ou seja, $n = r$. Por exemplo, com as matrizes*

$$A_{2\times 2} = \begin{bmatrix} 1 & -1 \\ 0 & 4 \end{bmatrix} \quad e \quad B_{3\times 2} = \begin{bmatrix} 2 & 1 \\ 4 & 2 \\ 5 & 3 \end{bmatrix}$$

   não é possível efetuar o produto AB, pois o número de colunas da matriz A é diferente do número de linhas da matriz B. Já o produto BA é possível.

2. *a matriz C tal que $C = AB$ possui o mesmo número de linhas de A e o mesmo número de colunas de B, isto é:*

$$\underbrace{A_{m\times k}\underbrace{B_{k\times n}}} = \underbrace{C_{m\times n}}$$

3. *em geral $AB \neq BA$. Por exemplo, sejam*

$$A = \begin{bmatrix} 1 & -1 & 1 \\ -3 & 2 & -1 \\ -2 & 1 & 0 \end{bmatrix} \quad e \quad B = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 4 & 6 \\ 1 & 2 & 3 \end{bmatrix}.$$

   Então

$$AB = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \quad e \quad BA = \begin{bmatrix} -11 & 6 & -1 \\ -22 & 12 & -2 \\ -11 & 6 & -1 \end{bmatrix}.$$

   Note ainda que $AB = 0$, sem que $A = 0$ ou $B = 0$.

Propriedades:

Desde que as operações sejam possíveis, as seguintes afirmações são válidas:

i) $A(B + C) = AB + AC$ (distributividade à esquerda da multiplicação, em relação à soma);

ii) $(A+B)C = AC+BC$ (distributividade à direita da multiplicação, em relação à soma);

iii) $(AB)C = A(BC)$ (associatividade);

iv) $AI = IA = A$ (Isto justifica o nome da matriz identidade.);

v) $(AB)^t = B^t A^t$.

A verificação dessas propriedades é simples. O leitor pode encontrá-las em [4, 1], com exceção do item **(v)** que iremos demostrar a seguir.

Demonstração.

v) Considere as matrizes $A = [a_{ij}]_{n\times s}$ e $B = [b_{ij}]_{s\times m}$. Da definição de produto temos que

$$AB = C = [c_{ij}]_{n\times m} \quad \text{,onde} \quad c_{ij} = \sum_{k=1}^{m} a_{ik}b_{kj}.$$

Sendo assim,

$$(AB)^t = C^t = [c'_{ij}]_{m\times n} \quad \text{tal que} \quad c'_{ij} = c_{ji} = \sum_{k=1}^{n} a_{jk}b_{ki}.$$

Por outro lado, temos que

$$B^t = [b'_{ij}]_{m\times s} = [b_{ji}]_{m\times s} \quad \text{e} \quad A^t = [a'_{ij}]_{s\times n} = [a_{ji}]_{s\times n}$$

Dessa forma,

$$B^t A^t = D = [d_{ij}]_{m\times n} \quad \text{onde} \quad d_{ij} = \sum_{k=1}^{n} b'_{ik}a'_{kj} = \sum_{k=1}^{n} b_{ki}a_{jk} = \sum_{k=1}^{n} a_{jk}b_{ki}.$$

O que nos permite concluir que,

$$(AB)^t = B^t A^t.$$

■

Terminaremos está seção apresentando o conceito de matrizes em blocos.

Definição 2.9. *Uma matriz A composta por blocos consiste em uma matriz cujos elementos matriciais também são matrizes. Denominam-se blocos essas submatrizes.*

As subdivisões em blocos são geralmente apresentadas por linhas horizontais ou verticais. Por exemplo

$$\begin{bmatrix} 5 & 6 & 1 & 0 & 0 \\ 6 & 11 & 0 & 1 & 0 \\ 8 & 7 & 0 & 0 & 1 \end{bmatrix} = \left[\begin{array}{cc|ccc} 5 & 6 & 1 & 0 & 0 \\ 6 & 11 & 0 & 1 & 0 \\ 8 & 7 & 0 & 0 & 1 \end{array}\right]$$

e

$$\left[\begin{array}{ccccc} 1 & 4 & 1 & 0 & 0 \\ 6 & 3 & 0 & 1 & 7 \\ 8 & 7 & 5 & 2 & 1 \\ 4 & 3 & 0 & 1 & 2 \end{array}\right] = \left[\begin{array}{ccc|cc} 1 & 4 & 1 & 0 & 0 \\ 6 & 3 & 0 & 1 & 7 \\ \hline 8 & 7 & 5 & 2 & 1 \\ 4 & 3 & 0 & 1 & 2 \end{array}\right] = \left[\begin{array}{ccc|cc} 1 & 4 & 1 & 0 & 0 \\ 6 & 3 & 0 & 1 & 7 \\ 8 & 7 & 5 & 2 & 1 \\ \hline 4 & 3 & 0 & 1 & 2 \end{array}\right].$$

Note que podemos subdividir as matrizes de várias maneiras diferentes.

Uma característica interessante das matrizes em blocos é que, sendo possível e feita as devidas partições, ao realizarmos as mesmas operações, de adição ou multiplicação, separadamente nos blocos correspondentes de duas ou mais matrizes, ao juntarmos os blocos resultantes, a matriz obtida será igual a matriz resultante caso realizemos as operações sem subdividir as matrizes em blocos.

O conceito que acabamos de apresentar também é muito usado no cálculo do determinante, tema que abordaremos na próxima seção.

2.4 Determinante

Historicamente, segundo [16], os determinantes foram usados muito antes das matrizes, a princípio, somente como uma propriedade para verificar se um sistema de equações lineares possuía uma única solução (que ocorre precisamente se o determinante da matriz dos coeficientes for diferente de zero). Os indícios mais antigas desta utilização são as inscrições em tabletas babilônicas feitas de argila datadas de cerca de 300 a.C. e as representações dos coeficientes de sistemas lineares em barras de bambu, que constam no livro *Os nove capítulos da arte matemática*, publicado entre 200 a.C. e 100 a.C. na China.

Ainda, conforme [16], a ideia inicial de determinante, como polinômio que associa a um quadrado de números, surgiu em 1683, com o matemático japonês Seki Takakazu (1642-1708), que sistematizou o velho procedimento chinês somente para o caso de duas equações. Paralelamente no ocidente, o uso dos determinantes também se iniciou em 1683, através do matemático alemão Leibniz (1649-1716), que em uma correspondência para o matemático francês L'Hospital (1661-1704), usou combinações de coeficientes para resolver sistemas de equações lineares e encontrou uma maneira de indexar tais coeficientes com números.

De maneira resumida, o Determinante pode ser visto como uma função que associa a cada matriz quadrada um único elemento. Contudo, a definição formal envolve muitos símbolos e conceitos e não compensa ser abordada aqui, mas pode ser encontrada em [4].

A caracterização das funções determinantes por meio das propriedades, que pode ser encontrado em [11], também não se fazem necessária. Nosso objetivo é apresentar um conceito minimamente fundamentado, capaz de definir o determinante indutivamente através da ordem da matriz, dando origem a uma relação de recorrência que nos permita

calcular um determinante de qualquer ordem.

Quando nos referirmos ao determinante de uma matriz A, escreveremos:

$$\det(A) \quad \text{ou} \quad det[a_{ij}] \quad \text{ou} \quad |A| = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Determinante de uma matriz de 1ª ordem

Define-se o determinante de uma matriz $A = [a_{11}]$, de 1ª ordem, como o valor do seu único elemento a_{11}, ou seja:

$$\det(A) = |a_{11}| = a_{11}.$$

Exemplo: Se $M = (4)$, então $\det(M) = 4$.

Determinante de uma matriz de 2ª ordem

Para uma matriz quadrada $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, de 2ª ordem, o determinante de A é definido por

$$det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

Note que

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}\det[a_{22}] - a_{12}\det[a_{21}].$$

Exemplo: Para calcular o determinante da matriz $M = \begin{bmatrix} 2 & -3 \\ 1 & 5 \end{bmatrix}$ temos que:

$$\det(M) = \begin{vmatrix} 2 & -3 \\ 1 & 5 \end{vmatrix} = 2 \cdot 5 - (-3) \cdot 1 = 10 + 3 = 13.$$

Determinante de uma matriz de 3ª ordem

Com certa analogia ao caso anterior, dada uma matriz

$$A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix},$$

de 3ª ordem, definimos seu determinante da seguinte forma:

$$\det(A) = a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$

Exemplo: Dada a matriz $M = \begin{bmatrix} 1 & 3 & 4 \\ 5 & 2 & -3 \\ 1 & 4 & 2 \end{bmatrix}$, a partir da definição acima, obteremos que

$$\det(M) = 1\cdot2\cdot2+1\cdot(-3).3+4\cdot4\cdot5-1\cdot2\cdot4-2\cdot3\cdot5-1\cdot4\cdot(-3) = 4-9+80-8-30+12 = 49.$$

2.4.1 Desenvolvimento de Laplace

Acabamos de ver que

$$|A| = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

$$= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$

Contudo, podemos escrever esta soma como

$$= a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{12}(a_{21}a_{33} - a_{23}a_{31}) + a_{13}(a_{21}a_{32} - a_{22}a_{31}),$$

ou ainda:

$$|A| = a_{11}\det\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12}\det\begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13}\det\begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}.$$

Observe que o determinante de uma matriz de 3ª ordem, pode ser obtido a partir das submatrizes 2×2

$$A_{11} = \begin{bmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{bmatrix}, \quad A_{12} = \begin{bmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{bmatrix} \quad \text{e} \quad A_{13} = \begin{bmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{bmatrix}.$$

Isto é,

$$\det(A) = a_{11}|A_{11}| - a_{12}|A_{12}| + a_{13}|A_{13}|$$

onde A_{ij} é a submatriz obtida da matriz A quando se retira a i-ésima e linha e a j-ésima coluna. Se escrevermos

$$\Delta_{ij} = (-1)^{i+j}|A_{ij}|,$$

obtemos a expressão,

$$\det(A) = a_{11}\Delta_{11} + a_{12}\Delta_{11} + a_{13}\Delta_{11}.$$

Para uma matriz de ordem n, essa propriedade continua sendo válida. Por isso, podemos expressar:

$$\begin{aligned} det(A_{n\times n}) &= a_{i1}\Delta_{i1} + \cdots + a_{in}\Delta_{in}. \\ &= \sum_{k=1}^{n} a_{ij}(-1)^{i+j} det(A_{ij}) \\ &= \sum_{k=1}^{n} a_{ij}\Delta_{ij} \end{aligned} \tag{2.1}$$

O método que apresentamos aqui é chamado de Desenvolvimento de Laplace e nos permite calcular determinantes de matrizes com ordem n, para $n \geq 2$. O termo Δ_{ij} (que é afetado diretamente pelo sinal $(-1)^{i+j}$ da submatriz A_{ij}, obtida de A retirando-se a i-ésima linha e a j-ésima coluna) é chamado de *cofator do elemento* a_{ij} ou *complemento algébrico do elemento* a_{ij}. Observe que em (2.1) o determinante foi desenvolvido para a i-ésima linha. Uma forma análoga é válida para as colunas.

Exemplo 2.10. *Dada a matriz* $M = \begin{bmatrix} 1 & -2 & 3 \\ 2 & 1 & -1 \\ -2 & -1 & 2 \end{bmatrix}$, *o cálculo do determinante, a partir da segunda coluna, fica da seguinte forma*

$$|M| = \begin{vmatrix} 1 & -2 & 3 \\ 2 & 1 & -1 \\ -2 & -1 & 2 \end{vmatrix} = (-2)\Delta_{12} + 1\Delta_{22} + (-1)\Delta_{32},$$

onde

$$\begin{aligned} \Delta_{12} &= (-1)^{1+2}\begin{vmatrix} 2 & -1 \\ -2 & 2 \end{vmatrix} = -\begin{vmatrix} 2 & -1 \\ -2 & 2 \end{vmatrix} = -2 \\ \Delta_{12} &= (-1)^{1+2}\begin{vmatrix} 2 & -1 \\ -2 & 2 \end{vmatrix} = -\begin{vmatrix} 2 & -1 \\ -2 & 2 \end{vmatrix} = -2 \\ \Delta_{22} &= (-1)^{2+2}\begin{vmatrix} 1 & 3 \\ -2 & 2 \end{vmatrix} = 8 \\ \Delta_{32} &= (-1)^{3+2}\begin{vmatrix} 1 & 3 \\ 2 & -1 \end{vmatrix} = 7. \end{aligned}$$

Portanto

$$|M| = (-2)\cdot(-2) + 1\cdot 8 + (-1)\cdot 7 = 5.$$

O desenvolvimento de Laplace é uma fórmula de recorrência que permite calcular o determinante de uma matriz de ordem n, a partir dos determinantes das submatrizes quadradas de ordem $n-1$. Em grande parte dos casos ele simplifica muito o cálculo de determinantes, principalmente se for utilizado em conjunto com outras propriedades do determinante, as quais veremos a seguir.

2.4.2 Propriedades:

i) Se todos os elementos de uma linha (ou coluna) de uma matriz A são nulos, então $\det(A) = 0$;

ii) $\det(A) = \det(A^t)$;

iii) Se multiplicarmos uma linha (ou coluna) da matriz por uma constante, o determinante fica multiplicado por esta constante;

iv) Uma vez trocada a posição de duas linhas (ou colunas), o determinante troca de sinal;

v) O determinante de uma matriz que tem duas linhas (ou colunas) iguais é zero;

vi)
$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ b_{i1}+c_{i1} & \dots & b_{in}+c_{in} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ b_{i1} & \dots & b_{in} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ c_{i1} & \dots & c_{in} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix};$$

Cuidado! Observe que aqui temos a soma numa linha, e não uma soma de matrizes. De modo geral, o determinante de uma soma de duas matrizes não é igual à soma dos determinantes das matrizes. Ou seja, em geral pode acontecer de

$$\det(A+B) \neq \det(A) + \det(B).$$

vii) O determinante não se altera se somarmos a uma linha (ou coluna) outra linha (ou coluna) multiplicada por uma constante;

viii) $\det(AB) = \det(A)\det(B)$.

Mais detalhes sobre essas propriedades podem ser encontrados, por exemplo, em [4, 1].

Como precisaremos usar a generalização da última propriedade mais a frente, iremos demonstrá-la a seguir.

Proposição 2.11. *Sejam $A_1, A_2, \dots A_n$ matrizes quadradas de mesma ordem. Então*

$$\det(A_1 A_2 \cdots A_n) = \det(A_1) det(A_2), \cdots \det(A_n).$$

Demonstração.

Vamos provar isso por indução sobre n. Da propriedade **(viii)** dos determinantes segue que, para $n = 2$, $\det(A_1A_2) = \det(A_1)\det(A_2)$.

Suponha para $n = k$ que $\det(A_1A_2 \cdots A_k) = \det(A_1)det(A_2), \cdots \det(A_k)$.

Agora, para $n = k + 1$ temos que

$$\det(A_1A_2 \cdots A_kA_{k+1}) = \det(A_1A_2 \cdots A_k)\det(A_{k+1}) = \det(A_1)det(A_2) \cdots \det(A_k)\det(A_k).$$

Como queríamos demostrar.

■

2.5 Matriz Adjunta

Consideremos a seguinte matriz quadrada:

$$\left[\begin{array}{ccc|c|cc} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ a_{31} & a_{32} & \dots & a_{3j} & \dots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \hline a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \hline \vdots & \vdots & \dots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nj} & \dots & a_{nn} \end{array}\right].$$

Como vimos anteriormente, a partir de cada entrada a_{ij} podemos obter o "cofator do elemento a_{ij}", indicado por Δ_{ij} e definido por:

$$\Delta_{ij} = (-1)^{i+j}\det(A_{ij}),$$

onde A_{ij} é a matriz que se obtém eliminando a linha i e a coluna j da matriz A. Com esses cofatores podemos formar uma nova matriz $\overline{A}$, denominada matriz dos cofatores de A, ou seja,

$$\overline{A} = [\Delta_{ij}].$$

Exemplo 2.12. *Dada a matriz*

$$A = \begin{bmatrix} 2 & 1 & 0 \\ -3 & 1 & 4 \\ 1 & 6 & 5 \end{bmatrix},$$

determine a matriz dos cofatores de A.

Solução: Usando a definição e desenvolvendo os cálculos obtemos

$$\Delta_{11} = (-1)^{1+1} \begin{vmatrix} 1 & 4 \\ 6 & 5 \end{vmatrix} = -19;$$

$$\Delta_{12} = (-1)^{1+2} \begin{vmatrix} -3 & 4 \\ 1 & 5 \end{vmatrix} = 19;$$

e

$$\Delta_{13} = (-1)^{1+3} \begin{vmatrix} -3 & 1 \\ 1 & 6 \end{vmatrix} = -19.$$

Prosseguindo, obteremos a matriz

$$\overline{A} = \begin{bmatrix} -19 & 19 & -19 \\ -5 & 10 & -11 \\ 4 & -8 & 5 \end{bmatrix}.$$

Definição 2.13. *Dada uma matriz quadrada A, chamaremos de matriz adjunta de A à transposta da matriz dos cofatores de A. Representada simbolicamente por:*

$$adj(A) = \overline{A}^t.$$

Exemplo 2.14. *Usando a matriz dos cofatores de A do exemplo anterior, é imediato concluir que*

$$adj(A) = \overline{A}^t = \begin{bmatrix} -19 & -5 & 4 \\ 19 & 10 & -8 \\ -19 & -11 & 5 \end{bmatrix}.$$

Agora, a partir das matrizes A e $adj(A)$ dos dois exemplos anteriores, é possível observar que

$$A \cdot adj(A) = \begin{bmatrix} 2 & 1 & 0 \\ -3 & 1 & 4 \\ 1 & 6 & 5 \end{bmatrix} \begin{bmatrix} -19 & -5 & 4 \\ 19 & 10 & -8 \\ -19 & -11 & 5 \end{bmatrix} = \begin{bmatrix} -19 & 0 & 0 \\ 0 & -19 & 0 \\ 0 & 0 & -19 \end{bmatrix}$$

$$= -19 \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = -19I_3.$$ Esse caso particular não se trata de uma mera coincidência, pois na verdade temos em geral o seguinte teorema.

Teorema 2.15. *Seja A uma matriz quadrada de ordem n. Então*

$$A \cdot adj(A) = adj(A) \cdot A = \det(A) I_n.$$

Demonstração.

Para realizar a demostração de maneira mais didática, a faremos esquematicamente para uma matriz de ordem 3. A demostração é simular para matrizes de ordem n.

Para $n = 3$

$$A \cdot adj(A) = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \cdot \begin{bmatrix} \Delta_{11} & \Delta_{21} & \Delta_{31} \\ \Delta_{12} & \Delta_{22} & \Delta_{32} \\ \Delta_{13} & \Delta_{23} & \Delta_{33} \end{bmatrix} = [c_{ij}]$$

Calculando as entradas c_{ij}, encontramos que

$$c_{11} = a_{11}\Delta_{11} + a_{12}\Delta_{21} + a_{13}\Delta_{13} = det(A),$$

pela expressão (2.1), e

$$c_{12} = a_{11}\Delta_{21} + a_{12}\Delta_{22} + a_{13}\Delta_{32} = 0$$

pois,

$$\begin{aligned} c_{12} &= a_{11}\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{12}\begin{vmatrix} a_{11} & a_{13} \\ a_{31} & a_{33} \end{vmatrix} + a_{13}\begin{vmatrix} a_{11} & a_{12} \\ a_{31} & a_{32} \end{vmatrix}. \\ &= a_{11}(a_{12}a_{33} - a_{13}a_{32}) - a_{12}(a_{11}a_{33} - a_{13}a_{31}) + a_{13}(a_{11}a_{32} - a_{12}a_{31}) \\ &= a_{11}a_{12}a_{33} - a_{11}a_{13}a_{32} - a_{12}a_{11}a_{33} + a_{12}a_{13}a_{31} + a_{13}a_{11}a_{32} - a_{13}a_{12}a_{31} \\ &= \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{11} & a_{12} & a_{13} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}, \end{aligned}$$

que tem duas linhas iguais (propriedade **v)** de determinantes). Analogamente, teremos que

$$\begin{cases} det(A), & \text{se } i = j, \\ 0, & \text{se } i \neq j, \end{cases}$$

ou seja,

$$A \cdot adj(A) = \begin{bmatrix} det(A) & 0 & 0 \\ 0 & det(A) & 0 \\ 0 & 0 & det(A) \end{bmatrix} = det(A)I_3.$$

■

2.6 Matriz Inversa

Definição 2.16. *Dada uma matriz quadrada A de ordem n, diz-se que A é inversível quando existe uma matriz B de ordem n tal que $AB = BA = I_n$, onde I_n é a matriz identidade de ordem n. Denotamos B por A^{-1} e a chamamos de inversa de A.*

Exemplo 2.17. *Seja*

$$A = \begin{bmatrix} 8 & 3 \\ 11 & 4 \end{bmatrix}.$$

Assumindo a princípio a existência da inversa, podemos procurar

$$B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

tal que $AB = I_2$ e $BA = I_2$. Impondo a primeira condição, temos que

$$\begin{bmatrix} 8 & 3 \\ 11 & 4 \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

ou seja,

$$\begin{bmatrix} 8a+3c & 8b+3d \\ 11a+4c & 11b+4d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Portanto,

$$\begin{cases} 8a + 3c = 1 \\ 11a + 4c = 0 \end{cases} \quad e \quad \begin{cases} 8b + 3d = 0 \\ 11b + 4d = 1 \end{cases}.$$

Resolvendo os sistemas, encontramos $a = -4, b = 3, c = 11$ e $d = -8$. Então

$$A^{-1} = B = \begin{bmatrix} -4 & 3 \\ 11 & -8 \end{bmatrix}$$

é a inversa da matriz A. Comprovamos facilmente fazendo

$$AB = \begin{bmatrix} 8 & 3 \\ 11 & 4 \end{bmatrix} \begin{bmatrix} -4 & 3 \\ 11 & -8 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

e

$$BA = \begin{bmatrix} -4 & 3 \\ 11 & -8 \end{bmatrix} . \begin{bmatrix} 8 & 3 \\ 11 & 4 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Como consequência da definição, podemos demostrar as seguinte proposição:

Proposição 2.18. *Dadas A e B matrizes quadradas de ordem n.*

i) *Se A e B são inversíveis, então AB é inversível e $(AB)^{-1} = B^{-1}A^{-1}$.*

ii) *Se A é inversível, então A^{-1} também é inversível e $(A^{-1})^{-1} = A$.*

Demonstração.

i) Como A e B são inversíveis temos que

$$(AB)(B^{-1}A^{-1}) = A(BB^{-1})A^{-1} = AIA^{-1} = AA^{-1} = I.$$

Analogamente,

$$(B^{-1}A^{-1})(AB) = I.$$

Assim, AB é inversível e $(AB)^{-1} = B^{-1}A^{-1}$.

ii) Se A é invertível então $AA^{-1} = A^{-1}A = I$, o que implica também que A é a inversa de A^{-1}, ou seja, $(A^{-1})^{-1} = A$.

■

Para finalizar esta seção, veremos uma importante relação entre matrizes inversas, determinantes e matriz adjunta.

Teorema 2.19. *Uma matriz quadrada A de ordem n é inversível se, e somente se,* $\det(A) \neq 0$. *Neste caso,*

$$A^{-1} = \frac{1}{\det(A)} adj(A).$$

Demonstração. ($\Rightarrow$) Se A é inversível, então existe matriz quadrada A^{-1} tal que $AA^{-1} = A^{-1}A = I_n$. Logo, temos

$$\det(AA^{-1}) = \det(A^{-1}A) = \det(I_n).$$

Pela Propriedade viii) de determinante, juntamente com o fato que $\det(I_n) = 1$, temos que

$$\det(A)\det(A^{-1}) = \det(A^{-1})\det(A) = 1.$$

Concluímos então que $\det(A) \neq 0$ (pois caso contrário, isto é, se $\det(A) = 0$, teríamos $\det(A)\det(A^{-1}) = 0$).

($\Leftarrow$) Suponha agora que $\det(A) \neq 0$. Sendo A uma matriz quadrada de ordem n, pelo Teorema 2.15, temos que $A \cdot adj(A) = adj(A) \cdot A = \det(A)I_n$. Assim, sendo $\det(A) \neq 0$, podemos concluir que

$$A\left(\frac{1}{\det(A)} adj(A)\right) = \left(\frac{1}{\det(A)} adj(A)\right) A = I_n.$$

Logo, A é invertível e sua inversa é

$$A^{-1} = \frac{1}{\det(A)} adj(A). \tag{2.2}$$

■

Exemplo 2.20. *Considere a matriz*

$$A = \begin{bmatrix} 6 & 2 \\ 11 & 4 \end{bmatrix}.$$

Temos que $\det(A) = 24 - 22 = 2 \neq 0$ *, portanto, existe a inversa de* A*. Calculemos a inversa pela fórmula* (2.2)*. Desenvolvendo os cálculos, obtemos*

$$\overline{A} = \begin{bmatrix} 4 & -11 \\ -2 & 6 \end{bmatrix} \quad e \quad adj(A) = \begin{bmatrix} 4 & -2 \\ -11 & 6 \end{bmatrix}.$$

Então,

$$A^{-1} = \frac{1}{\det(A)} \cdot adj(A) = \frac{1}{2} \begin{bmatrix} 4 & -2 \\ -11 & 6 \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -\frac{11}{2} & 3 \end{bmatrix}.$$

A partir do teorema anterior também é possível dar exemplos de matrizes quadradas que não são inversíveis. Como é o caso da matriz

$$A = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$$

que não é inversível, pois $\det(A) = 0$.

Capítulo 3

Transformações elementares unimodualres e resolução de sistemas Diofantinos

Segundo [11], desde a antiguidade, em diversas áreas de conhecimento, muitos problemas são modelados matematicamente por sistemas de equações lineares.

No modelo de ensino atual, o estudo dos sistemas, inicia-se no Ensino Fundamental, onde, didaticamente, são abordados de forma simples, com apenas duas equações e duas incógnitas, tendo a adição, a comparação e a substituição como técnicas para solucioná-los. Damos a seguir um exemplo desses sistemas:

$$\begin{cases} x + y = 24 \\ x - y = 2, \end{cases}$$

onde subentendesse que estamos buscando dois números reais que somados valem 24 e cuja diferença vale 2. Por um dos métodos concluímos facilmente que $x = 13$ e $y = 11$ é uma solução, pois obtemos as igualdades:

$$\begin{cases} 13 + 11 = 24 \\ 13 - 11 = 2. \end{cases}$$

Já no Ensino Médio, os sistemas de equações lineares começam a ser vistos de formas mais generalizada, com m equações e n incógnitas do tipo

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases}$$

onde os a_{ij}'s e os b_i's, para $1 \leq i \leq m$ e $1 \leq i \leq n$ são números reais dados e a n-upla de

números $(x_1, x_2, ..., x_n) \in \mathbb{R}$ será solução do sistema quando satisfizer simultaneamente as m equações.

Conforme [17], entre os métodos diretos para resolução de sistemas, o que possui o menor custo computacional é a *eliminação Gaussiana*[1] (ou método de escalonamento) e, consequentemente, a *eliminação de Gauss-Jordam*, ambos devido a Gauss, onde o segundo foi aperfeiçoado por Camille Jordan (França, 1838-1922). Tais métodos consistem basicamente em associar os sistemas as suas formas matriciais e realizar operações elementares nas linhas das matrizes que preservam as igualdades das equações, de modo a obter uma matriz mais simples na forma escalonada (ou escada), que pode ser associada a um novo sistema equivalente ao original. A diferença básica entre eles é que um é uma complementação do outro. Enquanto o método de Gauss exige apenas que a matriz dos coeficientes fique na forma triangular, o método de Gauss-Jordam exige que tal matriz fique na forma identidade (forma escalonada reduzida).

Para relembrar o método da *eliminação Gaussiana*, vejamos o seguinte exemplo: (Para efeito de visualização, colocaremos o sistema e a matriz associada a ele lado a lado.)

$$(I)\begin{cases} x_1 + 4x_2 + 3x_3 = 1 & (1) \\ 2x_1 + 5x_2 + 4x_3 = 4 & (2) \\ x_1 - 3x_2 - 2x_3 = 5 & (3) \end{cases} \qquad \left[\begin{array}{ccc|c} 1 & 4 & 3 & 1 \\ 2 & 5 & 4 & 4 \\ 1 & -3 & -2 & 5 \end{array}\right].$$

1º passo: Eliminamos x_1 das equações (2) e (3). Para isto, multiplicamos a equação (1) por -2 e somamos com a equação (2) e multiplicamos a equação (1) por -1 e somamos com a equação (3), obtendo, respectivamente, as equações $(2')$ e $(3')$. Isto resulta no seguinte sistema:

$$(II)\begin{cases} x_1 + 4x_2 + 3x_3 = 1 & (1') \\ 0x_1 - 3x_2 - 2x_3 = 2 & (2') \\ 0x_1 - 7x_2 - 5x_3 = 4 & (3') \end{cases} \qquad \left[\begin{array}{ccc|c} 1 & 4 & 3 & 1 \\ 0 & -3 & -2 & 2 \\ 0 & -7 & -5 & 4 \end{array}\right].$$

2º passo: Tornamos o coeficiente de x_2, da equação $(2')$ igual a 1. Para isto, multiplicamos a equação $(2')$ por $-1/3$. Resultando em:

$$(III)\begin{cases} x_1 + 4x_2 + 3x_3 = 1 & (1'') \\ 0x_1 + x_2 + \frac{2}{3}x_3 = -\frac{2}{3} & (2'') \\ 0x_1 - 7x_2 - 5x_3 = 4 & (3'') \end{cases} \qquad \left[\begin{array}{ccc|c} 1 & 4 & 3 & 1 \\ 0 & 1 & \frac{2}{3} & -\frac{2}{3} \\ 0 & -7 & -5 & 4 \end{array}\right].$$

3º passo: Eliminamos x_2 da equação $(3'')$. Para isto, multiplicamos a equação $(2'')$ por 7 e somamos com a equação $(3'')$. O sistema resultante é:

[1] Em homenagem a Carl Friedrich Gauss (Alemanha, 1777-1855), que segundo [5], é considerado um dos maiores matemáticos de todos os tempos.

$$(IV)\begin{cases} x_1+4x_2+3x_3 &= 1 \quad (1''') \\ 0x_1+x_2+\frac{2}{3}x_3 &= -\frac{2}{3} \quad (2''') \\ 0x_1+0x_2-\frac{1}{3}x_3 &= -\frac{2}{3} \quad (3''') \end{cases} \qquad \left[\begin{array}{ccc|c} 1 & 4 & 3 & 1 \\ 0 & 1 & \frac{2}{3} & -\frac{2}{3} \\ 0 & 0 & -\frac{1}{3} & -\frac{2}{3} \end{array}\right].$$

Da equação $(3''')$ do último sistema concluímos que $x_3 = 2$, onde substituindo em $(2''')$ obtemos que $x_2 = -2$ e por fim, substituindo o valor de x_3 e x_2 em $(1''')$ obtemos que $x_1 = 3$. Dessa forma, o sistema pode ser escrito da seguinte maneira:

$$\begin{cases} x_1 = & 3 \\ x_2 = & -2 \\ x_3 = & 2. \end{cases}$$

Observe que cada sistema foi obtido a partir do sistema anterior através das seguintes operações conhecidas como transformações elementares:

(i) Multiplicar uma equação por um número real diferente de zero.

(ii) Adicionar a equação a outra.

Existe ainda outra operação que as vezes precisamos realizar nesse procedimento.

(iii) Permutar duas equações.

Desse modo, por serem operações reversíveis e que preservam as igualdades, podemos garantir que a solução encontrada é também solução de todas os sistemas anteriores, incluindo o (I). No Teorema 3.16 veremos uma demostração formal deste fato.

É notório que, em sistemas que apresentam mais de uma solução é necessário ter-se uma forma clara de expressar todas elas. No próximo exemplo, veremos um sistema com essas carateristas. Na resolução, usaremos somente as matrizes associadas aos sistemas e uma simbologia de fácil compreensão, que definiremos mais adiante. Considere o seguinte sistema:

$$\begin{cases} 5x+6y+8z = & 1 \\ 6x-11y+7z = & 9. \end{cases}$$

Usando o método de Gauss-Jordan para colocá-lo na forma escolada reduzida, temos que

$$\left[\begin{array}{ccc|c} 5 & 6 & 8 & 1 \\ 6 & -11 & 7 & 9 \end{array}\right] \xrightarrow{L_1 \leftarrow \frac{1}{5}L_1} \left[\begin{array}{ccc|c} 1 & \frac{6}{5} & \frac{8}{5} & \frac{1}{5} \\ 1 & -17 & -1 & 8 \end{array}\right] \xrightarrow{L_2 \leftarrow L_2 - 6L_1}$$

$$\left[\begin{array}{ccc|c} 1 & \frac{6}{5} & \frac{8}{5} & \frac{1}{5} \\ 0 & \frac{-91}{5} & \frac{-13}{5} & \frac{39}{5} \end{array}\right] \xrightarrow{L_2 \leftarrow \frac{5}{-91}L_2} \left[\begin{array}{ccc|c} 1 & \frac{6}{5} & \frac{8}{5} & \frac{1}{5} \\ 0 & 1 & \frac{1}{7} & \frac{-3}{7} \end{array}\right] \xrightarrow{L_1 \leftarrow L_1 - \frac{6}{5}L_2}$$

$$\left[\begin{array}{ccc|c} 1 & 0 & \frac{10}{7} & \frac{5}{7} \\ 0 & 1 & \frac{1}{7} & \frac{-3}{7} \end{array}\right] \longrightarrow \begin{cases} 1x+\frac{10}{7}z = & \frac{5}{7} \\ -1y+\frac{1}{7}z = & -\frac{3}{7} \end{cases}$$

Reinterpretando o sistema, vemos que z é uma variável livre, ou seja, tomando $z = t$ obtemos a representação de todas as soluções do sistema.

$$\begin{cases} x = & \frac{5}{7} - \frac{10}{7}t \\ y = & -\frac{3}{7} + \frac{1}{7}t \\ z = & t \end{cases} , t \in \mathbb{R}.$$

Em sistemas como do exemplo acima é comum definir a quantidade de variáveis livres como sendo o grau de liberdade da solução. Sendo assim, no último exemplo temos uma solução com grau de liberdade 1.

Para sistemas lineares em geral, particularmente os com grande número de incógnitas, a *eliminação Gauss-Jordam* é a técnica de resolução mais atual e efetiva que dispomos, visto que pode ser quase sempre aplicada e facilmente mecanizada. Por outro lado, para modelar vários problemas aplicados necessitamos do uso de sistemas onde os coeficientes, bem como as soluções procuradas, são números inteiros. Caso tais sistemas tenham mais de uma solução, o método, que relembramos aqui, não é suficiente, pois não garante que as soluções encontradas estejam em função de números inteiros (veja no exemplo anterior) ou que a partir delas consigamos encontrar todas as soluções inteiras.

Um bom modelo para os sistemas que acabamos de descrever surge na tentativa de balancear as equações químicas, que são representações gráficas das reações químicas que ocorrem entre os diversos elementos presentes na tabela periódica. Em toda combustão, por exemplo, teremos sempre um combustível e um comburente resultando em gás carbônico e água. No caso da combustão completa do benzeno, a equação química que a representa é dada da seguinte forma

$$xC_6H_6 + yO_2 \rightarrow zCO_2 + wH_2O$$

onde precisamos ajustar os coeficientes estequiométricos (x, y, z, w) de modo que o número de moléculas de cada elemento na equação química seja conservado. Isto é, o número de moléculas de um determinado elemento é o mesmo no reagente (lado esquerdo da equação) e no produto (lado direito da equação). Podemos interpretar o balanceamento da equação química acima a partir do seguinte sistema:

$$\begin{cases} 6x = & z \\ 6x = & 2w \\ 2y = & 2z + w. \end{cases}$$

Considerando que os coeficientes estequiométricos estão representando moléculas, a solução para o sistema, que implica em uma forma de balancear a equação química, precisa ser formada por números inteiros, sendo eles os menores possíveis.

Reescrevendo o sistema de maneira mais organizada, temos

$$\begin{cases} 6x + 0y - z + 0w &= 0 \\ 6x + 0y + 0z - 2w &= 0 \\ 0x + 2y - 2z - w &= 0 \end{cases} \qquad \left[\begin{array}{cccc|c} 6 & 0 & -1 & 0 & 0 \\ 6 & 0 & 0 & -2 & 0 \\ 0 & +2 & -2 & -1 & 0 \end{array}\right]$$

ou seja, o número de equações é menor que o número de incógnitas, dessa forma, caso o sistema seja possível, ele terá infinitas soluções, das quais queremos apenas a menor entre as soluções que pertencem a $\mathbb{N}$.

Diante de tudo que foi colocado, é natural perguntar se existe algum método prático para encontrar tais soluções inteiras? Veremos mais adiante que sim.

3.1 Sistemas Diofantinos e matrizes

Um sistema linear de equação Diofantina com m equações e n incógnitas é um conjunto de equações do tipo

$$(*) \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases}$$

onde os a_{ij}'s e os b_i's, para $1 \leq i \leq m$ e $1 \leq i \leq n$ $(m < n)$ são números inteiros conhecidos e a n-upla $(x_1, x_2, \ldots, x_n)$ solução do sistema apenas quando pertencer a $\mathbb{Z}^n$.

Tratando individualmente as equações, a definição que acabamos de enunciar caracteriza uma generalização das equações Diofantinas lineares, o que nos leva a nomear tais sistemas com o título deste trabalho.

Uma característica essencial dos problemas Diofantinos é possuir a quantidade de equações menor que a quantidade de variáveis desconhecidas, ou seja, $m < n$. Se estes sistema fossem possíveis e determinados eles teriam uma única solução, contudo, mesmo tendo todos os coeficientes inteiros, é fácil intuir que as chances dessa única solução também ser inteira é muito pequena, pois estamos fazendo uma restrição muito forte. Por esse motivo, daremos ênfase aos sistemas possíveis e indeterminados, pois esses, possuem infinitas soluções reais das quais queremos determinar apenas as soluções inteiras. Note que, uma única equação com duas ou mais variáveis pode ser interpretada como um sistema.

Observe também que, apesar de estarmos restringindo os coeficientes ao conjunto dos inteiros, qualquer equação com coeficientes racionais tem sempre uma equação equivalente com coeficientes inteiros, basta multiplicar toda equação pelo mínimo múltiplo comum dos denominadores dos coeficientes racionais. Sendo assim, feitos os devidos ajustes, o que

iremos apresentar neste capítulo pode ser estendido para uma classe maior de sistemas.

Formalizando o que já havíamos discutido na seção anterior, segue a seguinte definição:

Definição 3.1. *Dois sistemas de equações lineares são equivalentes quando toda solução de qualquer um do ssistemas também é solução do outro.*

Os sistemas e as matrizes estão totalmente interligados, basta perceber que, a partir da Definição 2.7, podemos escrever $(*)$ da seguinte forma matricial:

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

ou $A \cdot X = B$, onde

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

é a matriz dos coeficientes,

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

a matriz das incógnitas e

$$B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

a matriz dos coeficiente e dos termos independentes, respectivamente.

Uma outra matriz que podemos associar ao sistema é

$$\left[\begin{array}{cccc|c} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_n \end{array}\right]$$

chamada de *matriz ampliada do sistema*, onde cada linha desta matriz é uma representação abreviada dos coeficiente e termos independentes das equações do sistema.

A seguir, juntaremos diversos resultados vistos até aqui para consolidar um algorítimo para solucionar os sistemas lineares de equações Diofantinas. Parte do algoritmo é inspirado no método da *eliminação Gaussiana*, porém, com as devidas restrições para permanecermos com os coeficientes e termos independentes nos inteiros. Nomearemos essa parte de método da eliminação inteira e no mais, seguiremos os seguintes passos: associar o sistema a sua forma matricial, definir o que são operações elementares unimodulares, definir o que é uma matriz na forma inteira escalonada por linhas, e por fim, mostrar um algoritmo de como colocar uma matriz proveniente do sistema inicial na forma escalonada por linhas. A matriz resultante desse escalonamento nos fornecerá um novo sistema, equivalente ao primeiro, porém, razoavelmente mais fácil, que tendo soluções inteiras, também nos dará, na forma paramétrica, soluções inteiras para o sistema inicial.

Denotaremos por "$M_{m\times n}(\mathbb{Z})$" o conjunto das matrizes $m \times n$ com entradas inteiras.

3.2 Transformação de matrizes em $M_{m\times n}(\mathbb{Z})$

As transformações unimodulares que veremos a seguir, nada mais são que transformações elementares que envolvem apenas números inteiros.

3.2.1 Transformações elementares unimodulares em uma matriz

Definição 3.2. *Uma transformação elementar unimodular em uma matriz $m \times n$, com entradas em $\mathbb{Z}$, consiste em uma das três operações a seguir:*

(i) permutar duas linhas ($L_i \leftrightarrow L_j$);

(ii) multiplicar uma linha por -1 ($L_i \to -L_i$);

(iii) adicionar um múltiplo inteiro de uma linha a outra ($L_i \to L_i + kL_j$).

Exemplo 3.3.

$$\begin{bmatrix} 3 & 2 \\ -5 & 4 \end{bmatrix} \to \begin{bmatrix} -5 & 4 \\ 3 & 2 \end{bmatrix} \to \begin{bmatrix} 5 & -4 \\ 3 & 2 \end{bmatrix} \to \begin{bmatrix} -1 & -8 \\ 3 & 2 \end{bmatrix}$$

No exemplo acima, aplicamos em sequência, as três operações elementares descritas na definição. Permutamos a linha 1 com a linha 2, multiplicamos a linha 1 por -1 e por fim, adicionamos a linha 2 multiplicada por -2, a linha 1. Observe que as matrizes transformadas permanecem com suas entradas em $\mathbb{Z}$, algo esperado, já que as operações unimodulares utilizam apenas combinações lineares envolvendo números inteiros.

Diante do conceito acima, é possível definir a seguinte relação de equivalência:

Definição 3.4. *Sejam A e B matrizes de ordem $m \times n$. A matriz A é dita ser unimodularmente equivalente por linhas à matriz B se B pode ser obtida de A pela aplicação sucessiva de um número finito de transformações elementares unimodulares sobre linhas.*

Exemplo 3.5. $A = \begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix}$ *é unimodularmente equivalente a* $B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, *pois*

$$\begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix} \xrightarrow{L_2 \leftarrow L_2 - 2L_1} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \xrightarrow{L_1 \leftarrow L_1 - L_2} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Como havíamos comentado no início da seção, as operações elementares, que contém as operações unimodulares, são sempre reversíveis, como veremos na Proposição a seguir. Tal resultado nos ajuda a garantir que sistemas associados a matrizes equivalentes também são equivalente.

Proposição 3.6. *Toda transformação elementar unimodular u nas linhas de matrizes em $M_{m\times n}(\mathbb{Z})$ é reversível, no sentido de que existe uma transformação elementar unimodular u' tal que $u'(u(A)) = A$ e $u(u'(A)) = A$, para todo $A \in M_{m\times n}(\mathbb{Z})$.*

Demonstração.

Se u uma transformação elementar unimodular do tipo $L_i \leftrightarrow L_j$ ou $L_i \to -L_i$, tome $u' = u$. Se for do tipo $L_i \to L_i + kL_j.$, tome u' como a transformação $L_i \to L_i - kL_j$.

■

Observe que, facilmente nos convencemos que em cada caso da demostração anterior, u' é a única transformação unimodular em que $A \in M_{m\times n}(\mathbb{Z})$.

Exemplo 3.7.

$$\begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix} \xrightarrow{u=L_2 \leftarrow L_2 - 2L_1} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \xrightarrow{u'=L_2 \leftarrow L_2 + 2L_1} \begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix} \xrightarrow{u=L_2 \leftarrow -L_2} \begin{bmatrix} 1 & 1 \\ -3 & -2 \end{bmatrix} \xrightarrow{u'=L_2 \leftarrow -L_2} \begin{bmatrix} 1 & 1 \\ 3 & 2 \end{bmatrix}$$

3.2.2 Forma inteira escalonada de uma matriz

Definição 3.8. *Uma matriz $m\times n$, com entradas em $\mathbb{Z}$, estará na forma inteira escalonada por linhas se:*

(i) *toda linha nula ocorre abaixo de todas as linhas não nulas;*

(ii) *o primeiro elemento não nulo de cada linha estiver estritamente à direita do primeiro elemento não nulo da linha superior.*

Por exemplo, a matriz

$$\begin{bmatrix} 6 & 7 & 1 & 0 & 4 \\ 0 & 3 & 4 & 2 & 3 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

esta na forma inteira escalonada, pois todas as condições da definição anterior estão sendo atendidas, mas as matrizes

$$\begin{bmatrix} 2 & 3 & 1 & 0 \\ 0 & 0 & 4 & 2 \\ 0 & 7 & 0 & 1 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 4 & 3 & 1 & 5 \\ 0 & 0 & 0 & 0 \\ 0 & 7 & 3 & 1 \end{bmatrix}$$

não estão na forma inteira escalonada, pois a primeira não satisfaz a condição (i), enquanto a segunda não atende a condição (ii).

Assim como nas definições de escalonamento por linhas para matrizes com entradas reais, o primeiro elemento não nulo de cada coluna também será chamado de termo líder ou pivô.

Caso, além das exigências da Definição 3.8, sejam atendias as exigências:

(iii) o primeiro elemento não nulo de cada linha não nula é 1;

(iv) cada coluna que contém o primeiro elemento não nulo de alguma linha tem todos os seus outros elementos iguais a zero.

Diremos que a matriz está na forma **inteira escalonada reduzida**. Por exemplo, as matrizes

$$\begin{bmatrix} 1 & 0 & 0 & 3 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \end{bmatrix} \quad \text{e} \quad \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

estão na forma que acabamos de definir.

3.2.3 Matrizes unimodulares e aplicações

Analogamente ao que acontece com as transformações unimodulares, o conjunto das matrizes unimodulares é um subconjunto do conjunto das matrizes elementares, cujos elementos podem ser definidos formalmente da seguinte maneira:

Definição 3.9. *Uma matriz unimodular de ordem n é uma matriz quadrada obtida a partir da identidade, através da aplicação de uma única operação unimodular.*

Por exemplo, a matriz identidade é uma matiz unimodular, assim como

$$u(I_3) = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \text{, onde } u : L_1 \leftrightarrow L_2.$$

Teorema 3.10. *Seja u uma transformação elementar unimodular sobre matrizes de $M_{m\times n}(\mathbb{Z})$. Considere a matriz unimodular $U = u(I_m)$. Então*

$$u(A) = UA, \text{ para todo } A \in M_{m\times n}(\mathbb{Z}).$$

A demostração desse teorema é um tanto simples, porém extensa. Consiste em aplicar a mesma transformação unimodular u em uma matriz $A \in M_{m\times n}(\mathbb{Z})$ e na matriz identidade I_m. Em seguida verificar que a matriz $u(A)$ será igual a matriz $u(I_m)A$. Fazendo isso com as três operações da Definição 3.2, o Teorema estará provado.

Como consequência do Teorema acima temos os seguintes resultados:

Corolário 3.11. *Sejam A e B em $M_{m\times n}(\mathbb{Z})$. Então A é unimodularmente equivalente a B se, somente se, existem matrizes unimodulares $U_1, \ldots, U_s$ de ordem n tais que*

$$U_s \cdots U_2 U_1 A = B.$$

Demonstração.

Por definição, A é unimodularmente equivalente a B quando existem transformações elementares unimodulares $u_1, \ldots, u_s$ tais que

$$u_s(\ldots(u_2(u_1(A)))\ldots) = B.$$

Mas, pelo teorema anterior, a igualdade acima equivale a

$$U_s \cdots U_2 U_1 A = B$$

onde $U_i = u_i(I_m)$, para cada $1 \leq i \leq s$.

■

Corolário 3.12. *Toda matriz unimodular é invertível e sua inversa também é uma matriz unimodular.*

Demonstração.

Seja U uma matriz unimodular e u uma transformação elementar unimodular tal que $U = u(I)$. Se u' é a transformação unimodualar inversa de u e se $U' = u'(I)$, pelo Teorema 3.10 segue que

$$I = u'(u(I)) = u'(U) = u'(I)U = U'U$$

e

$$I = u(u'(I)) = u(U') = u(I)U' = UU'.$$

Logo U é invertível e $U^{-1} = U'$.

■

Antes de apresentarmos os próximos resultados, vejamos a seguinte definição:

Definição 3.13. *Diremos que uma matriz A é* ***invertível em $M_{n\times n}(\mathbb{Z})$*** *ou* ***unimodularmente invertível****, quando A for invertível e A^{-1} também pertencer a $M_{n\times n}(\mathbb{Z})$.*

O Teorema a seguir caracteriza as matrizes que acabamos de definir.

Teorema 3.14. *Para uma matriz quadrada A em $M_{n\times n}(\mathbb{Z})$, são equivalentes:*

(i) A é invertível em $M_{n\times n}(\mathbb{Z})$;

(ii) Se B é uma matriz na forma inteira escalonada reduzida equivalente a A, então $B = I_n$;

(iii) A é uma matriz unimodular ou um produto de matrizes unimodualres.

Demonstração.

Vamos começar provando que $(i) \Rightarrow (ii)$. De inicio, como B é unimodularmente equivalente a A, temos pelo Corolário 3.11 que existem matrizes unimodualres $U_1, U_2, \ldots, U_s$ tais que

$$U_s \cdots U_2 U_1 A = B.$$

Como, pelo Corolário 3.12, cada U_i é invertível e por hipótese A é invertível, temos pelo item (ii) da Proposição 2.18 que B é invertível, o que implica que $\det(B) \neq 0$. Sendo assim, B é uma matriz quadrada que não tem nenhuma linha ou coluna nula e, por hipótese, está na forma inteira escalona reduzida, o que nos permite concluir que $B = I_n$

A implicação $(ii) \Rightarrow (iii)$ é evidente, ja que $A = U_1^{-1}U_2^{-1}\cdots U_s^{-1}B$, onde $B = I_n$ e cada U_i^{-1}, pelo Corolário 3.12, é uma matriz unimodular.

Por fim, para prova que $(iii) \Rightarrow (i)$, temos por hipótese que existe matrizes unimodulares $U_1^{-1}, ..., U_s^{-1}$ tais que

$$A = U_1^{-1} \cdots U_s^{-1}.$$

Como, pela Corolário 3.12, toda matriz unimodular é invertível, iniciaremos multiplicando ambos os lados da igualdade acima por U_s (inversa de U_s^{-1}), ou seja,

$$AU_s = U_1^{-1} \cdots U_s^{-1}U_s \Rightarrow AU_s = U_1^{-1} \cdots U_{s-1}^{-1}I.$$

Se continuarmos esse processo de U_{s-1}^{-1} até U_1^{-1} segue que

$$AU_s = U_1^{-1} \cdots U_{s-1}^{-1}$$

$$\vdots$$

$$AU_s \cdots U_1 = I.$$

Portanto, podemos concluir que A é invertível e

$$A^{-1} = U_s \cdots U_1.$$

■

Como podemos ver, toda matriz invertível em $M_{n\times n}(\mathbb{Z})$ pode ser escrita como um produto de matrizes elementares unimodulares e vice-versa. Sendo assim, dentro do conjunto das matrizes invertíveis, existem aquelas formadas apenas por uma ou um produto de matrizes elementares unimodulares.

A demostração do Teorema acima também nos permite concluir que U é unimodularmente equivalente a I, pois existe uma sequência de matrizes unimodulares, ou ainda, de transformações unimodulares, que transforma U em I. A recíproca dessa conclusão também é verdadeira e nos rende uma boa aplicação para as matrizes unimodulares.

Proposição 3.15. *Seja A uma matriz invertível em $M_{(n\times n)}(\mathbb{Z})$ e $u_1, ..., u_s$ uma sequencia de transformações unimodulares tais que $u_s(...(u_2(u_1(A)))...) = I$. Então essa mesma sequência de transformações elementares aplicada a I produz A^{-1}; isto é,*

$$u_s(...(u_2(u_1(I)))...) = A^{-1}.$$

Demonstração.

Para cada $1 \leq i \leq s$, seja U_i a matriz unimodular correspondente a transformação unimodular u_i. Então, pelo Teorema 3.10, temos que

$$U_s \cdots U_2 U_1 A = I.$$

Assim,

$$(U_s \cdots U_2 U_1 I)AA^{-1} = IA^{-1},$$

donde

$$U_s \cdots U_2 U_1 I = A^{-1}$$

■

Na prática, uma forma de utilizar o resultado anterior, é operarmos simultaneamente com as matrizes A e I, através de operações unimodulares, até chegarmos à matriz I na posição correspondente à matriz A. Assim, a matriz obtida no lugar correspondente à matriz I será a inversa de A:

$$[A|I] \longrightarrow [I|A^{-1}].$$

Exemplo 3.16. *Considere*

$$A = \begin{bmatrix} 1 & 2 & 7 \\ 0 & 3 & 1 \\ 0 & 5 & 2 \end{bmatrix}$$

e verifique se tal matriz possui inversa em $M_{n\times n}(\mathbb{Z})$. Em caso positivo, escreva A^{-1}.

Solução: coloquemos a matriz junto com a matriz identidade e apliquemos as operações unimodulares sobre linhas, para reduzir a parte esquerda (que corresponde a A) à forma da identidade. Cada operação deve ser efetuada simultaneamente na parte direita da matriz:

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 7 & 1 & 0 & 0 \\ 0 & 3 & 1 & 0 & 1 & 0 \\ 0 & 5 & 2 & 0 & 0 & 1 \end{array}\right] \xrightarrow{L_2 \leftrightarrow L_3} \left[\begin{array}{ccc|ccc} 1 & 2 & 7 & 1 & 0 & 0 \\ 0 & 5 & 2 & 0 & 0 & 1 \\ 0 & 3 & 1 & 0 & 1 & 0 \end{array}\right] \xrightarrow{L_2 \leftarrow L_2 - 2L_3}$$

$$\left[\begin{array}{ccc|ccc} 1 & 2 & 7 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 & -2 & 1 \\ 0 & 3 & 1 & 0 & 1 & 0 \end{array}\right] \xrightarrow{L_2 \leftarrow -L_2} \left[\begin{array}{ccc|ccc} 1 & 2 & 7 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & -1 \\ 0 & 3 & 1 & 0 & 1 & 0 \end{array}\right] \xrightarrow{L_1 \leftarrow L_1 - 2L_2}$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 7 & 1 & -4 & 2 \\ 0 & 1 & 0 & 0 & 2 & -1 \\ 0 & 3 & 1 & 0 & 1 & 0 \end{array}\right] \xrightarrow{L_3 \leftarrow L_3 - 3L_2} \left[\begin{array}{ccc|ccc} 1 & 0 & 7 & 1 & -4 & 2 \\ 0 & 1 & 0 & 0 & 2 & -1 \\ 0 & 0 & 1 & 0 & -5 & 3 \end{array}\right] \xrightarrow{L_1 \leftarrow L_1 - 7L_3}$$

$$\left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 31 & -19 \\ 0 & 1 & 0 & 0 & 2 & -1 \\ 0 & 0 & 1 & 0 & -5 & 3 \end{array}\right].$$

Finalmente, obtemos a identidade à esquerda e a inversa de A à direita. Portanto,

$$A^{-1} = \begin{bmatrix} 1 & 31 & -19 \\ 0 & 2 & -1 \\ 0 & -5 & 3 \end{bmatrix}.$$

Ainda sobre as matrizes unimodularmente invertíveis, temos o seguinte resultado:

Proposição 3.17. *Seja A uma matriz inversível em $M_{n\times n}(\mathbb{Z})$, então $det(A) = \pm 1$.*

Demonstração.

Por hipótese, temos que A é invertível, o que implica que $det(A) \neq 0$ e que existe $A^{-1} \in M_{(n\times n)}(\mathbb{Z})$ tal que $AA^{-1} = I$. Logo, pela Propriedade *viii*) dos determinantes

$$det(AA^{-1}) = det(I) = det(A)det(A^{-1}) = 1.$$

Como A e A^{-1} são matrizes com entradas inteiras, $det(A)$ e $det(A^{-1})$, por serem combinações lineares dessas entradas, resultam sempre em números também inteiros. Sendo assim, $det(A)det(A^{-1}) = 1$ só é possível se $det(A) = det(A^{-1}) = \pm 1$.

■

Para finalizar esta seção, veremos uma proposição que nos ajudará na demostração do Teorema 3.22.

Proposição 3.18. *Seja U um produto de matrizes unimodulares, então (U^t) é inversível e $(U^t)^{-1} \in M_{n\times n}(\mathbb{Z})$.*

Demonstração.

As matrizes unimodulares, por serem provenientes da matriz identidade e das transformações unimodulares, sempre são quadradas e com entradas inteiras. Portanto, a matriz resultante do produto entre elas também é quadrada e com entradas em $\mathbb{Z}$, visto que o produto de matrizes em $M_{n\times n}(\mathbb{Z})$, permanece nesse conjunto. Dessa forma, a partir da Proposição anterior e da Propriedade *ii*) dos determinantes concluímos que

$$det(U^t) = det(U) = \pm 1$$

e que, a partir da Equação 2.2, a inversa de U^t é dada por

$$(U^t)^{-1} = \frac{adj(U^t)}{det(U^t)} = \pm adj(U^t).$$

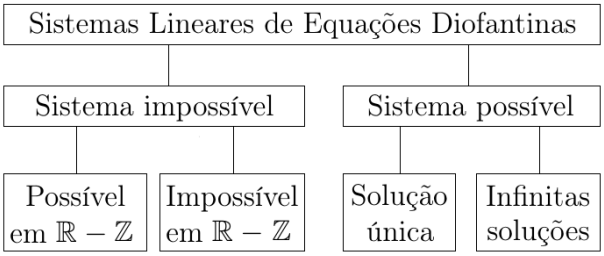
Como as entradas de uma matriz adjunta são formadas por subdeterminantes, concluímos que $adj(U^t)$ é uma matriz em que $u_{ij} \in \mathbb{Z}$, pois as entradas de U^t são inteiras. Isso implica que $(U^t)^{-1} = adj(U^t)$ também é uma matriz com entradas em $\mathbb{Z}$, como queríamos demostrar.

A existência de $(U^t)^{-1}$ esta vinculada ao fato do $det(U^t) \neq 0$, o que, como vimos mais acima, sempre acontece.

■

3.3 Resolução de sistemas lineares Diofantinos

Quanto as suas soluções, um sistema Diofantino se classifica da seguinte forma:



ou seja, um sistema Diofantino pode ser impossível em $\mathbb{Z}$, mas possível $\mathbb{R} - \mathbb{Z}$, ou, impossível também em $\mathbb{R}$. Quando possível em $\mathbb{Z}$, pode ter uma única ou infinitas soluções.

A próxima proposição é baseada no Algoritmo de Euclides e praticamente descreve o algoritmo do método da eliminação inteira, além de ser fundamental para a demostração do principal Teorema deste capítulo.

Proposição 3.19. *É sempre possível, através das operações unimodulares, transformar*

$$a\ matriz \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} \quad na\ matriz \begin{bmatrix} d \\ 0 \\ \vdots \\ 0 \end{bmatrix},$$

onde d é o $mdc(a_1, a_2, \ldots, a_n)$ e $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$.

Demonstração.

Façamos o seguinte processo, que envolve apenas operações unimodulares, até que haja apenas uma entrada diferente de zero:

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

(ii) Para cada $i \neq j$, aplique o algoritmo da divisão para obter

$$a_i = k_i a_j + r_i \qquad \text{com} \qquad 0 \leq |r_i| < |a_j|.$$

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

$$\begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_j \\ \vdots \\ a_n \end{bmatrix} \longrightarrow \begin{bmatrix} a_1 - k_1 a_j \\ a_2 - k_2 a_j \\ \vdots \\ a_j \\ \vdots \\ a_n - k_n a_j \end{bmatrix} \longrightarrow \begin{bmatrix} r_1 \\ r_2 \\ \vdots \\ a_j \\ \vdots \\ r_n \end{bmatrix} \cdots \begin{bmatrix} 0 \\ 0 \\ \vdots \\ d \\ \vdots \\ 0 \end{bmatrix} \longrightarrow \begin{bmatrix} d \\ 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Cada vez que esse processo é aplicado, o valor absoluto de cada entrada se reduz estritamente ao resto da divisão por a_j. Perceba que os passos descritos acima, nada mais são do que a aplicação simultânea do Algoritmo de Euclides, o qual nos garante que em determinado ciclo, o resto da divisão de a_j por a_i será zero, para todo $i \neq j$. Nesse caso excepcional, todas as entradas, exceto uma, torna-se diferente de zero. Na sequência, trocando as linhas e, possivelmente, multiplicando por -1, podemos mover a entrada diferente de zero para o topo e torná-la positiva.

Usando o Lema de Euclides juntamente com a Proposição 1.29 é fácil ver que

$$mdc(a_1, a_2, \ldots, a_n) = mdc(a_1 - k_1 a_j, a_2, \ldots, a_n),$$

o que pode ser estendido para todos os elementos diferentes de a_j, ou seja,

$$\begin{aligned} mdc(a_1, a_2, \ldots, a_n) &= mdc(a_1 - k_1 a_j, a_2 - k_2 a_j, \ldots, a_j, \ldots, a_n - k_n a_j) \\ &= mdc(r_1, r_2, \ldots, a_j, \ldots, r_n) \\ &\vdots \\ &= mdc(0, 0, \ldots, \pm d, \ldots, 0) \\ &= d. \end{aligned}$$

■

Aplicando o algoritmo da proposição acima em todas as colunas de uma matriz com entradas inteiras, podemos obter o seguinte resultado:

Teorema 3.20. *Toda Matriz em $M_{m\times n}(\mathbb{Z})$ é equivalente a uma matriz na forma inteira escalonada.*

Demonstração.

Usando o processo descrito na proposição anterior, que envolve sucessivas transformações unimodulares (método da eliminação inteira), é sempre possível reduzir uma matriz em $M_{m\times n}(\mathbb{Z})$ a sua forma inteira escalonada. Basta aplicar o processo até que todas as entradas da primeira coluna sejam zero, com exceção da primeira, que será o *mdc* das entradas dessa coluna. Em seguida, ignoramos a primeira linha e repetimos o processo com as linhas restantes até que os elementos da segunda coluna zerem, exceto o

primeiro, que não estamos manipulando, e o segundo. O processo segue até que a matriz inicial esteja reduzida a forma

$$\begin{bmatrix} d_1 & * & \dots & * \\ 0 & d_2 & \dots & * \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_m \end{bmatrix}.$$

■

O próximo Teorema fecha uma sequência de resultados que nos permite concluir que: ao manipular uma matriz associada a um sistema linear através das transformações unimodulares para obter uma nova matriz escalonada, o sistema associado a essa nova matriz é equivalente ao sistema inicial.

Teorema 3.21. *Dois sistemas lineares Diofantinos que possuem matrizes ampliadas equivalentes são equivalentes.*

Demonstração.

Sejam A e A' matrizes unimodularmente equivalentes por linhas. Segue do Corolário 3.11 que $A' = MA$, onde M é um produto de matrizes elementares unimodulares, e do Teorema 3.14 que M é invertível. Os sistemas (I) e (II) que tem A e A' como matrizes ampliadas podem ser escritos respectivamente da seguinte forma:

$$NX = B \quad \text{e} \quad N'X = B'$$

onde N é a matriz dos coeficientes e B a matriz dos termos independentes de (I) (Idem para N' e B' no sistema (II)). Além disso, é fácil verificar que

$$N' = MN \quad \text{e} \quad B' = MB.$$

Portanto,

$$NX = B \Leftrightarrow MNX = MB \Leftrightarrow N'X = B'.$$

Isto significa que os sistemas (I) e (II) são equivalentes, pois toda matriz

$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

que é solução de (I) será solução de (II) e virse-versa.

■

No restante do capítulo, ao invés de manejar as matrizes associadas aos sistemas, teremos que manejar a matriz transposta. Isto se deve ao fato de termos construído todo nossa teoria para matrizes escalonadas por linha.

Adiante, será enunciado, provado e exemplificado o resultado central desse trabalho: o **Algoritmo de Euclides Estendido Generalizado**, ferramenta suficiente para resolver qualquer sistema linear Diofantino ou equação Diofantina, independente do número de variáveis. Tal resultado está presente nos textos [9, 13] e foi um dos pontos chave da pesquisa.

Teorema 3.22. *Para resolver um sistema linear de equações Diofantinas $AX = B$, usamos operações unimodulares para transformar $[A^t|I]$ em $[R|T]$, onde R está na forma inteira escalonada por linhas. Assim, $AX = B$ tem solução em $\mathbb{Z}$ se, e somente se, $R^tK = B$ tem soluções inteiras para K, e todas as soluções para $AX = B$ são da forma $X = T^tK$.*

Demonstração.

A partir da forma matricial $AX = B$ do sistema Diofantino dado, compomos a matriz em blocos $[A^t|I]$, que pertence a $M_{m\times n}(\mathbb{Z})$ e consequentemente, pela demostração do teorema anterior, é sempre possível reduzir a sua forma inteira escalonada $[R|T]$. Colocar $[A^t|I]$ na forma escalonada é o mesmo que multiplica-lá a esquerda por matrizes unimodulares, como vimos no Corolário 3.11. Denotaremos por U o produto dessas matrizes unimodulares. Isto é,

$$U[A^t|I] = [R|T] \Leftrightarrow [UA^t|U] = [R|T].$$

Portanto,

$$U = T \text{ e } UA^t = R \Rightarrow TA^t = R. \tag{3.1}$$

Na sequência, usando as propriedades da transposição de matrizes e multiplicando (à direita) ambos os lados da igualdade por $(T^t)^{-1}$, obtemos

$$TA^t = R \Leftrightarrow AT^t = R^t \Leftrightarrow A = R^t(T^t)^{-1}.$$

Dessa forma, denotando $(T^t)^{-1}X$ por K concluímos que

$$AX = B \Leftrightarrow R^t(T^t)^{-1}X = B \Leftrightarrow R^tK = B$$

e

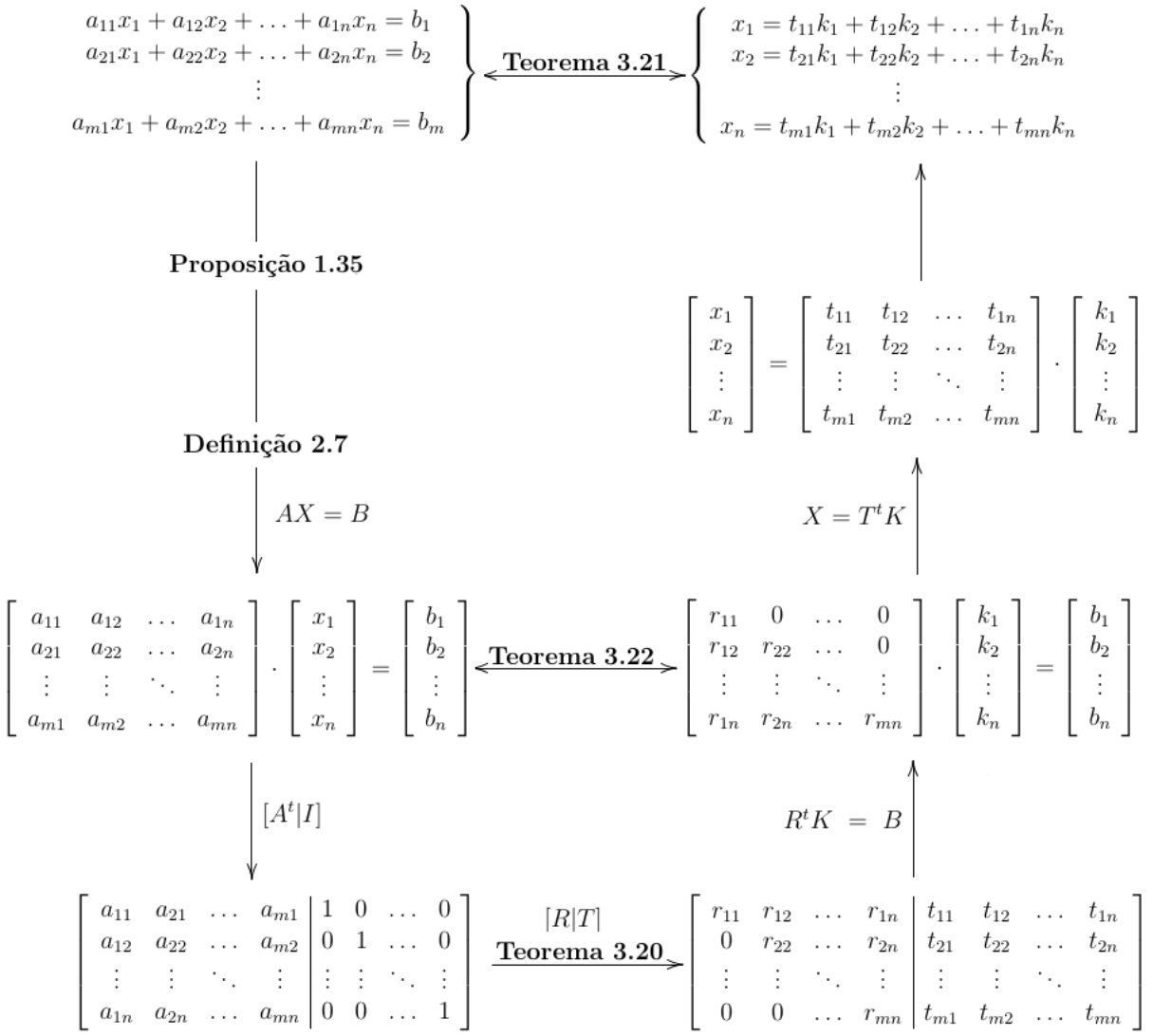
$$K = (T^t)^{-1}X \Leftrightarrow X = T^tK. \tag{3.2}$$

Por fim, na Proposição 3.18 vimos que a matriz $(T^t)^{-1}$ sempre existirá e todas as suas entradas, bem como em T^t, estarão sempre em $\mathbb{Z}$. Sendo assim, de (3.2), podemos inferir

que K terá entradas inteiras se, somente se, X também tiver, pois, a soma e o produto de números inteiros sempre resulta em números também inteiros .

■

Podemos representar o algorítimo para resolução das equações Diofantinas no seguinte diagrama:



Juntamente com o método da eliminação inteira, o Teorema 3.22 fornece um algoritmo interessante para solucionar os sistemas estudados neste capítulo. Porém, antes de iniciar a aplicação do algoritmo, o resultado da Proposição 1.35 pode ser usado como um teste de grande valia, evitando trabalhos desnecessários. Caso ele falhe em uma das equações, o sistema fica condenado a não ter soluções inteiras. Mas caso não falhe em nenhuma, é necessário prosseguir com o uso do algoritmo, pois possuir individualmente soluções inteiras não garante o mesmo para o sistema. Obviamente, quando temos apenas uma equação, o teste é totalmente efetivo. Para melhor entendimento, resolveremos alguns exemplos.

Na resolução das questões, seguiremos o seguinte roteiro: verificaremos, conforme o resultado da Proposição 1.35, se as equações do sistema possuem soluções inteiras. Sendo favorável o resultado, a partir da forma matricial do sistema, vamos escrever a matriz $[A^t|I]$ e, através do método da eliminação inteira, transforma-la na forma inteira escalonada $[R|T]$. Em seguida, a partir dessa ultima matriz, obteremos o sistema $R^tK = B$, que também estará na forma inteira escalonada, proporcionando uma resolução rápida e fácil. Por fim, se o sistema $R^tK = B$ possuí soluções inteiras, significa que o sistema inicial também possui e tais soluções serão dadas pela relação $X = T^tK$.

Exemplo 3.23. *Encontre todas as soluções inteiras do sistema linear*

$$\begin{cases} 5x + 6y + 8z = 1 \\ 6x - 11y + 7z = 9. \end{cases}$$

Solução: a parir do resultado da Proposição 1.35 é fácil verificar que individualmente, as equações possuem soluções inteiras. Sendo assim, colocando o sistema na forma matricial $AX = B$, obtemos

$$\begin{bmatrix} 5 & 6 & 8 \\ 6 & -11 & 7 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 9 \end{bmatrix}.$$

Agora, vamos compor a matriz $[A^t|I]$, e utilizando o método da eliminação inteira, transformá-la na sua forma inteira escalonada $[R|T]$.

$$\left[\begin{array}{cc|ccc} 5 & 6 & 1 & 0 & 0 \\ 6 & 11 & 0 & 1 & 0 \\ 8 & 7 & 0 & 0 & 1 \end{array}\right] \xrightarrow[L_3 \leftarrow L_3 - L_1]{L_2 \leftarrow L_2 - L_1} \left[\begin{array}{cc|ccc} 5 & 5 & 1 & 0 & 0 \\ 1 & -17 & -1 & 1 & 0 \\ 3 & 1 & -1 & 0 & 1 \end{array}\right] \xrightarrow[L_3 \leftarrow L_3 - 3L_2]{L_1 \leftarrow L_1 - 5L_2}$$

$$\left[\begin{array}{cc|ccc} 0 & 91 & 6 & -5 & 0 \\ 1 & -17 & -1 & 1 & 0 \\ 0 & 52 & 2 & 3 & 1 \end{array}\right] \xrightarrow[L_2 \leftarrow -L_2 + 2L_3]{L_1 \leftrightarrow L_2} \left[\begin{array}{cc|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & 13 & 2 & 1 & -2 \\ 0 & 52 & 2 & -3 & 1 \end{array}\right] \xrightarrow{L_3 \leftarrow L_3 - 4L_2}$$

$$\left[\begin{array}{cc|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & 13 & -2 & -1 & 2 \\ 0 & 0 & 10 & 1 & -7 \end{array}\right].$$

Dessa forma, obtemos a matriz $[R|T]$, donde segue que o sistema $R^tK = B$ é dado por

$$\begin{bmatrix} 1 & 0 & 0 \\ -17 & 13 & 0 \end{bmatrix} \cdot \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 9 \end{bmatrix},$$

ou seja, $k_1 = 1$ *e* $-17k_1 + 13k_2 = 9 \to k_2 = 2$*, onde* k_3 *pode ser qualquer valor inteiro, o qual denotaremos por* t*. Por conseguinte,*

$$K = \begin{bmatrix} 1 \\ 2 \\ t \end{bmatrix} \; e \; \begin{bmatrix} x \\ y \\ z \end{bmatrix} = T^t K = \begin{bmatrix} -1 & -2 & 10 \\ 1 & -1 & 1 \\ 0 & 2 & -7 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 2 \\ t \end{bmatrix} = \begin{bmatrix} -5 + 10t \\ -1 + t \\ 4 - 7t \end{bmatrix},$$

isto é, todas as soluções paramétricas são dadas por

$$\begin{cases} x = & -5 + 10t; \\ y = & -1 + t; \qquad para \quad t \in \mathbb{Z}; \\ z = & 4 - 7t. \end{cases}$$

ou ainda, $(x, y, z) = (-5, -1, 4) + (10, -1, -7)t$*.*

Em geral, saber se sistema tem soluções inteiras depende da relação entre os pivôs de R e as entradas de B. Em todas as transformações, o *mdc* dos elementos das linhas de R^t precisa dividir o elemento correspondente da linhas de B. Caso essa relação não exista, possivelmente não precisemos mais concluir o escalonamento. Tal observação também é amparada pela Proposição 1.35.

Exemplo 3.24. *Determine, caso existam, todas as soluções inteiras do sistema linear*

$$\begin{cases} 6x + 14y + 20z = & 11 \\ 14x - 11y + 7z = & 15 \end{cases}$$

Solução: pela Proposição 1.35, temos que o $mdc(6, 14, 20) = 2 \nmid 11$*, ou seja, a primeira equação não possui solução inteira, o que implica que o sistema também não possui.*

Exemplo 3.25. *Resolva o seguinte sistema linear*

$$\begin{cases} x + y - 2z + 3w = & 4 \\ 2x + 3y + 3z - w = & 3 \\ 5x - 7y + 4z + w = & 5. \end{cases}$$

Solução: seguindo o script, a partir da forma matricial $A \cdot X = B$*, vamos montar a matriz* $[A^t|I]$ *e colocá-la na forma inteira escalonada.*

$$\left[\begin{array}{ccc|cccc} 1 & 2 & 5 & 1 & 0 & 0 & 0 \\ 1 & 3 & -7 & 0 & 1 & 0 & 0 \\ -2 & 3 & 4 & 0 & 0 & 1 & 0 \\ 3 & -1 & 1 & 0 & 0 & 0 & 1 \end{array}\right] \xrightarrow[L_4 \leftarrow L_4 + L_3]{L_2 \leftarrow L_2 - L_1} \left[\begin{array}{ccc|cccc} 1 & 2 & 5 & 1 & 0 & 0 & 0 \\ 0 & 1 & -12 & -1 & 1 & 0 & 0 \\ -2 & 3 & 4 & 0 & 0 & 1 & 0 \\ 1 & 2 & 5 & 0 & 0 & 1 & 1 \end{array}\right] \xrightarrow[L_4 \leftarrow L_4 - L_1]{L_3 \leftarrow L_3 + 2L_1}$$

$$\left[\begin{array}{ccc|cccc} 1 & 2 & 5 & 1 & 0 & 0 & 0 \\ 0 & 1 & -12 & -1 & 1 & 0 & 0 \\ 0 & 7 & 14 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 1 \end{array}\right] \xrightarrow{L_3 \leftarrow L_3 - 7L_2} \left[\begin{array}{ccc|cccc} 1 & 2 & 5 & 1 & 0 & 0 & 0 \\ 0 & 1 & -12 & -1 & 1 & 0 & 0 \\ 0 & 0 & 98 & 9 & -7 & 1 & 0 \\ 0 & 0 & 0 & -1 & 0 & 1 & 1 \end{array}\right].$$

Com a matriz na forma $[R|T]$ concluímos que a equação $R^t \cdot K = B$ ficará da seguinte forma

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 0 \\ 5 & -12 & 98 & 0 \end{bmatrix} \cdot \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{bmatrix} = \begin{bmatrix} 4 \\ 3 \\ 5 \end{bmatrix},$$

ou seja, $k_1 = 4$, $2k_1 + k_2 = 3 \to k_2 = -5$ e $5k_1 - 2k_2 + 98k_3 = 5 \to k_3 = -75/98$. Dessa forma, pelo Teorema 3.22, concluímos que o sistema dado não possui soluções em $\mathbb{Z}$, já que o sistema $R^tK = B$ não possui soluções inteiras para K.

Observe ainda que podemos concluir que o sistema proposto tem soluções fora do conjuntos inteiros, pois o sistema $R^tK = B$ possui soluções em $\mathbb{R} - \mathbb{Z}$.

Exemplo 3.26. *Na equação $6x_1 + 14x_2 + 21x_3 = 11$, encontre todas as soluções em $\mathbb{Z}$, caso existam.*

Solução: Como $mdc(6, 14, 21) = 1$ divide 11, segue da Proposição 1.35 que a equação dada tem soluções em $\mathbb{Z}$. Assim, a partir da forma matricial $AX = B$ construímos a matriz $[A^t|I]$ e procedemos com seu escalonamento usando o método da eliminação inteira. Ou seja,

$$\left[\begin{array}{c|ccc} 6 & 1 & 0 & 0 \\ 14 & 0 & 1 & 0 \\ 21 & 0 & 0 & 1 \end{array}\right] \xrightarrow[L_3 \leftarrow L_3 - 3L_1]{L_2 \leftarrow L_2 - 2L_2} \left[\begin{array}{c|ccc} 6 & 1 & 0 & 0 \\ 2 & -2 & 1 & 0 \\ 3 & -3 & 0 & 1 \end{array}\right] \xrightarrow[L_3 \leftarrow L_3 - L_2]{L_1 \leftarrow L_1 - 2L_3} \left[\begin{array}{c|ccc} 0 & 7 & -3 & 0 \\ 2 & -2 & 1 & 0 \\ 1 & -1 & -1 & 1 \end{array}\right]$$

$$\xrightarrow{L_2 \leftarrow L_2 - 2L_3} \left[\begin{array}{c|ccc} 0 & 7 & -3 & 0 \\ 0 & 0 & 3 & -2 \\ 1 & -1 & -1 & 1 \end{array}\right] \xrightarrow[L_2 \leftrightarrow L_3]{L_1 \leftrightarrow L_2} \left[\begin{array}{c|ccc} 1 & -1 & -1 & 1 \\ 0 & 7 & -3 & 0 \\ 0 & 0 & 3 & -2 \end{array}\right].$$

Assim, obtemos a matriz $[R|T]$ *e pelo Teorema 3.22, a equação* $R^tK = B$ *é*

$$\begin{bmatrix} 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} = \begin{bmatrix} 11 \end{bmatrix},$$

ou seja, $k_1 = 11$*, ao passo que* k_2 *e* k_3 *podem assumir qualquer valor inteiro, os quais denotaremos por* t_2 *e* t_3*, respectivamente. Com isso,*

$$K = \begin{bmatrix} 11 \\ t_2 \\ t_3 \end{bmatrix} \; e \; \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = T^t \cdot K = \begin{bmatrix} -1 & 7 & 0 \\ -1 & -3 & 3 \\ 1 & 0 & -2 \end{bmatrix} \cdot \begin{bmatrix} 11 \\ t_2 \\ t_3 \end{bmatrix} = \begin{bmatrix} -11 + 7t_2 \\ -11 - 3t_2 + 3t_3 \\ 11 - 2t_3 \end{bmatrix}$$

isto é, todas as soluções paramétricas são dadas por

$$\begin{cases} x_1 = & -11 + 7t_2; \\ x_2 = & -11 - 3t_2 + 3t_3; \qquad para \quad t_2, t_3 \in \mathbb{Z}; \\ x_3 = & 11 - 2t_3. \end{cases}$$

ou ainda, $(x_1, x_2, x_3) = (-11, -11, 11) + (7, -3, 0)t_2 + (0, 3, -2)t_3$*.*

Observe que, em sistemas com apenas uma equação, o algoritmo utilizado acima pode ser visto como uma forma de passar uma equação da forma algébrica para a forma paramétrica.

Exemplo 3.27. *No inicio do capítulo vimos que para balancear a equação química*

$$xC_6H_6 + yO_2 \to zCO_2 + wH_2O$$

que representa a combustão completa do benzeno, precisamos encontrar a menor solução inteira para o sistema

$$\begin{cases} 6x + 0y - z + 0w & = 0 \\ 6x + 0y + 0z - 2w & = 0 \\ 0x + 2y - 2z - w & = 0. \end{cases}$$

Sendo assim, vamos escrever o sistema acima na forma matricial $A \cdot X = B$

$$\begin{bmatrix} 6 & 0 & -1 & 0 \\ 6 & 0 & 0 & -2 \\ 0 & 2 & -2 & -1 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

Agora, utilizando o método da eliminação inteira para transformar a matriz $[A^t|I]$ na sua forma escalonada inteira $[R|T]$, temos que:

$$\left[\begin{array}{cccc|cccc} 6 & 6 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 \\ -1 & 0 & -2 & 0 & 0 & 1 & 0 \\ 0 & -2 & -1 & 0 & 0 & 0 & 1 \end{array}\right] \xrightarrow[L_2 \leftrightarrow L_4]{L_1 \leftarrow L_1+6L_3} \left[\begin{array}{cccc|cccc} 0 & 6 & -12 & 1 & 0 & 6 & 0 \\ 0 & -2 & -1 & 0 & 0 & 0 & 1 \\ -1 & 0 & -2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 \end{array}\right] \xrightarrow{L_1 \leftarrow L_1+3L_2}$$

$$\left[\begin{array}{cccc|cccc} 0 & 0 & -15 & 1 & 0 & 6 & 3 \\ 0 & -2 & -1 & 0 & 0 & 0 & 1 \\ -1 & 0 & -2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 \end{array}\right] \xrightarrow{L_1 \leftrightarrow L_3} \left[\begin{array}{cccc|cccc} -1 & 0 & -2 & 0 & 0 & 1 & 0 \\ 0 & -2 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & -15 & 1 & 0 & 6 & 3 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 \end{array}\right] \xrightarrow[L_1 \leftarrow -L_1]{L_3 \leftarrow L_3+3L_4}$$

$$\left[\begin{array}{cccc|cccc} 1 & 0 & 2 & 0 & 0 & -1 & 0 \\ 0 & -2 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 1 & 7 & 6 & 3 \\ 0 & 0 & 2 & 0 & 1 & 0 & 0 \end{array}\right] \xrightarrow{L_4 \leftarrow L_4+2L_3} \left[\begin{array}{cccc|cccc} 1 & 0 & 2 & 0 & 0 & -1 & 0 \\ 0 & -2 & -1 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 1 & 7 & 6 & 3 \\ 0 & 0 & 0 & 2 & 15 & 12 & 6 \end{array}\right].$$

Com isso, segue que o sistema $R^t \cdot K = B$ é dado por

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 \\ 2 & -1 & -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix},$$

o que implica que $k_1 = 0$, $k_2 = 0$, $k_3 = 0$, onde k_4 pode ser qualquer valor inteiro, o qual denotaremos por t. Por conseguinte,

$$K = \begin{bmatrix} 0 \\ 0 \\ 0 \\ t \end{bmatrix} \; e \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} = T^t \cdot K = \begin{bmatrix} 0 & 0 & 1 & 2 \\ -1 & 0 & 7 & 15 \\ -1 & 0 & 6 & 12 \\ 0 & 1 & 3 & 6 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 0 \\ 0 \\ t \end{bmatrix} = \begin{bmatrix} 2t \\ 15t \\ 12t \\ 6t \end{bmatrix}$$

Isto é, todas as soluções paramétricas são dadas por

$$\begin{cases} x = & 2t; \\ y = & 15t; \\ z = & 12t; \\ w = & 6t; \end{cases} \qquad \text{para } t \in \mathbb{Z};$$

ou ainda, $(x, y, z) = (2, 15, 12, 6)t$.

Como queremos a menor solução inteira, basta tomar $t = 1$. *Desse modo, a equação balanceada fica da seguinte forma:*

$$2C_6H_6 + 15O_2 \rightarrow 12CO_2 + 6H_2O.$$

Conforme comentamos no inicio da Seção 3.1, todo sistema de equações com coeficiente racionais é equivalente a um sistema com coeficientes inteiros. Neste caso, se as soluções procuradas também forem números inteiros, recairemos em um sistema Diofantino, cuja solução pode ser encontrada a partir da técnica apresentada até aqui. Vejamos o exemplo a seguir:

Exemplo 3.28. *Sabe-se que uma jaca custa* $R\$10,00$, *uma maça* $R\$0,50$ *e um limão* $R\$0,10$. *Quantas jacas, maças e limões teremos que comprar para termos 100 frutas, gastando exatamente* $R\$100,00$ *?*

Solução: Seja j *a quantidade de jacas ,* m *a quantidade de maças e* l *quantidade de limões, escrevendo o sistema e fazendo ajustes necessários temos que*

$$\begin{cases} 10j + 0,5m + 0,1l = 100 \\ j + m + l = 100 \end{cases} \xrightarrow{x10} \begin{cases} 100j + 5m + 1l = 1000 \\ j + m + l = 100. \end{cases}$$

Continuando, vamos escrever o sistema da esquerda na forma matricial $A \cdot X = B$, *ou seja*

$$\begin{bmatrix} 100 & 5 & 1 \\ 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} j \\ m \\ l \end{bmatrix} = \begin{bmatrix} 1000 \\ 100 \end{bmatrix}.$$

Agora, utilizando o método da eliminação inteira, vamos compor a matriz $[A^t|I]$ *e transformá-la na sua forma inteira escalonada* $[R|T]$.

$$\left[\begin{array}{cc|ccc} 10 & 1 & 1 & 0 & 0 \\ 5 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right] \xrightarrow[L_2 \leftrightarrow L_4]{L_1 \leftarrow L_1 + 6L_3} \left[\begin{array}{cc|ccc} 0 & -19 & 1 & -20 & 0 \\ 0 & -4 & 0 & 1 & -5 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right] \xrightarrow{L_1 \leftarrow L_1 + 3L_2}$$

$$\left[\begin{array}{cc|ccc} 1 & 1 & 0 & 0 & 0 \\ 0 & -4 & 0 & 1 & -5 \\ 0 & -3 & 1 & -24 & 20 \end{array}\right] \xrightarrow{L_1 \leftrightarrow L_3} \left[\begin{array}{cc|ccc} 1 & 1 & 0 & 0 & 1 \\ 0 & -1 & -1 & 25 & -25 \\ 0 & -3 & 1 & -24 & 20 \end{array}\right] \xrightarrow[L_1 \leftarrow -L_1]{L_3 \leftarrow L_3 + 3L_4}$$

$$\left[\begin{array}{cc|ccc} 1 & 1 & 0 & 0 & 1 \\ 0 & -1 & -1 & 25 & -25 \\ 0 & 0 & 4 & -99 & 95 \end{array}\right] \xrightarrow{L_4 \leftarrow L_4 + 2L_3} \left[\begin{array}{cc|ccc} 10 & 1 & 1 & 0 & 0 \\ 5 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{array}\right].$$

Dessa forma, concluímos que o sistema $R^t \cdot K = B$ *fica da seguinte forma*

$$\left[\begin{array}{ccc} 1 & 0 & 0 \\ 1 & -1 & 0 \end{array}\right] \cdot \left[\begin{array}{c} k_1 \\ k_2 \\ k_3 \end{array}\right] = \left[\begin{array}{c} 1000 \\ 100 \end{array}\right],$$

o que implica que $k_1 = 1000$ *e* $k_2 = 900$*, onde* k_3 *pode ser qualquer valor inteiro, o qual denotaremos por* t*. Na sequência, obtemos que*

$$K = \left[\begin{array}{c} 1000 \\ 100 \\ t \end{array}\right] \; e \; \left[\begin{array}{c} j \\ m \\ l \end{array}\right] = \left[\begin{array}{ccc} 0 & -1 & 4 \\ 0 & 25 & -99 \\ 1 & -25 & 95 \end{array}\right] \cdot \left[\begin{array}{c} 1000 \\ 900 \\ t \end{array}\right] = \left[\begin{array}{c} -900 + 4t \\ 22500 - 99t \\ -21500 + 95t \end{array}\right].$$

Ou seja, todas as soluções paramétricas são dadas por

$$\begin{cases} j = & -900 + 4t; \\ m = & 22500 - 99t; \\ l = & -21500 + 95t; \end{cases} \qquad \text{para } t \in \mathbb{Z};$$

ou ainda, $(j, m, l) = (-900, 22500, -21500) + (4, -99, 95)t$*.*

Como queremos a menor solução inteira positiva, temos apenas uma opção, quando $t = 227$*. Desse modo, a solução procurada é*

$$\begin{cases} j = & 8 \\ m = & 27 \\ l = & 65. \end{cases}$$

Exemplo 3.29. *Resolva a equação Diofantina* $18X + 12Y = 6$*.*

Solução: sendo o mdc(18,12)=6, divisor do termo independente 6, a Proposição 1.24 nos garante que a equação dada tem solução nos inteiros. Sendo assim, usando o método da eliminação inteira, obtemos:

$$\left[\begin{array}{c|cc} 18 & 1 & 0 \\ 12 & 0 & 1 \end{array}\right] \xrightarrow{L_1 \leftarrow L_1 - L_2} \left[\begin{array}{c|cc} 6 & 1 & -1 \\ 12 & 0 & 1 \end{array}\right] \xrightarrow{L_2 \leftarrow L_2 - 2L_1} \left[\begin{array}{c|cc} 6 & 1 & -1 \\ 0 & -2 & 3 \end{array}\right]$$

e a partir da equação (3.1) *do Teorema 3.22 (*$TA^t = R$*), concluímos que*

$$\begin{bmatrix} 1 & -1 \\ -2 & 3 \end{bmatrix} \cdot \begin{bmatrix} 18 \\ 12 \end{bmatrix} = \begin{bmatrix} 6 \\ 0 \end{bmatrix},$$

ou seja,

$$\begin{cases} 18(1) + 12(-1) = 6 \\ 18(-2) + 12(3) = 0 \end{cases} \rightarrow \begin{cases} 18(1) + 12(-1) = 6 \\ 18(-2t) + 12(3t) = 0 \end{cases}, t \in \mathbb{Z}.$$

Agora, somando as equações, obtemos que $X = 1 - 2t$ *e* $Y = -1 + 3t$*, para* $t \in \mathbb{Z}$*.*

Aplicado em uma equação Diofantina com apenas duas variáveis, o algoritmo que generalizamos neste capítulo é apresentado nos livros de Aritmética como o Algoritmo de Euclides Estendido, onde, com estas condições, ao mesmo tempo que calcula o *mdc* de dois inteiro a e b, determina os inteiros s e t tais que $mdc(a, b) = sa + tb$. Neste trabalho, apresentaremos essa particularidade como um Corolário do Teorema 3.22.

Corolário 3.30. *(ALGORITMO DE EUCLIDES ESTENDIDO) Dados quaisquer inteiros* a *e* b*, é sempre possível por meio das operações unimodualares transformar*

$$\left[\begin{array}{c|cc} a & 1 & 0 \\ b & 0 & 1 \end{array}\right] \quad em \quad \left[\begin{array}{c|cc} d & s & t \\ 0 & s_1 & t_1 \end{array}\right].$$

Então, $d = mdc(a, b)$ *e a solução geral da equação* $ax + by = d$ *é*

$$\begin{array}{rl} x = & s + ks_1 \\ y = & t + kt_1 \end{array} \quad para\ k \in \mathbb{Z}.$$

Demonstração.

No Teorema 3.22 vimos que, através do método da eliminação inteira, é sempre possível reduzir

$$\left[\begin{array}{c|cc} a & 1 & 0 \\ b & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{c|cc} d & s & t \\ 0 & s_1 & t_1 \end{array}\right]$$

de tal forma que $d = mdc(a, b)$. Vimos também, na equação (3.1) da demostração do teorema, que é possível estabelecer a seguinte relação

$$\begin{bmatrix} s & t \\ s_1 & t_1 \end{bmatrix} \cdot \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} d \\ 0 \end{bmatrix}.$$

Sendo assim, basta retomar o sistema, multiplicar a segunda equação por um k inteiro e somar as equações, para obtermos

$$(s + ks_1)a + (t + kt_1)b = d$$

onde é fácil ver que $x = s + ks_1$ e $y = t + kt_1$ satisfaz a equação $ax + by = d$.

■

3.3.1 Interpretação geométrica

Do ponto de vista geométrico, a resolução de sistemas pode ser interpretado como a interseção entre hiperplanos de um espaço vetorial. Entre dois planos no caso do $\mathbb{R}^3$ ou entre duas retas no caso do $\mathbb{R}^2$. Nos sistemas lineares diofantinos as soluções estão sempre sobre esses hiperplanos, porém são apenas pontos de coordenadas inteiras, que formam os chamados reticulados. Nesse caso também é possível propor soluções sem necessariamente termos um sistema, basta apenas um elemento geométrico (retas ou planos), entre outros hiperplanos que representam situações aplicadas que não possuem representação geométrica. Na programação linear, tais soluções são chamadas de ideais. A seguir, vamos analisar geometricamente as soluções dos últimos exemplos da seção anterior.

(a) No Exemplo 3.23, o sistema representa dois planos cuja interseção da origem a uma reta, a qual queremos apenas os pontos com entradas em $\mathbb{Z}$ (...,A,B,C,D,E,...). Abaixo segue um gráfico que ilustra o que acabamos de descrever.

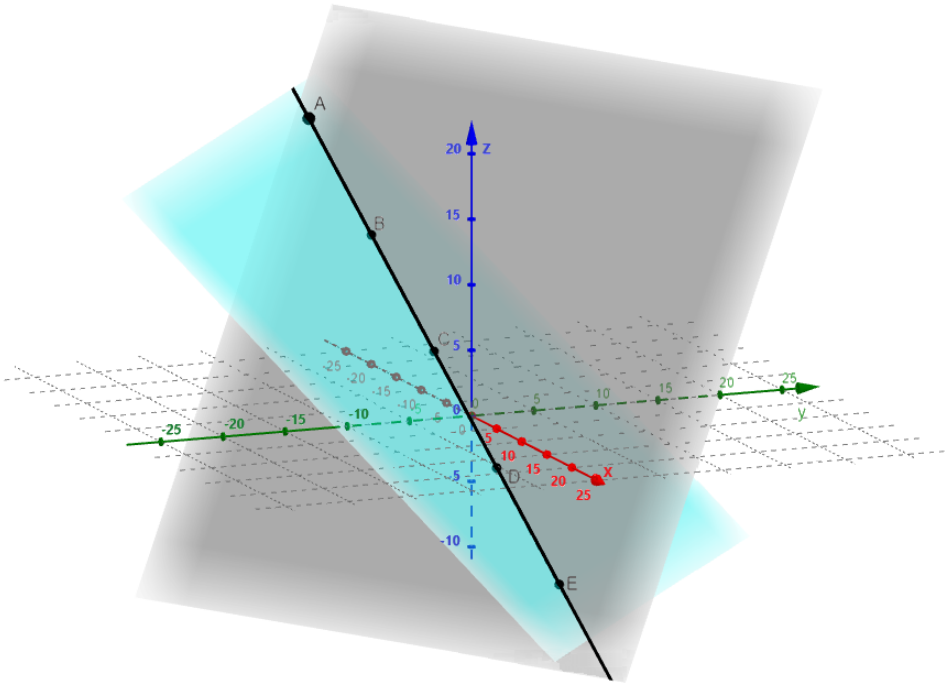


Figura 3.1: Interpretação geométrica do exemplo 3.23

(b) No Exemplo 3.26 temos apenas um plano, no qual as soluções são os pontos de coordenadas inteiras sobre ele. Observe que, visualmente, o reticulado gerado pela solução segue um padrão de formação.

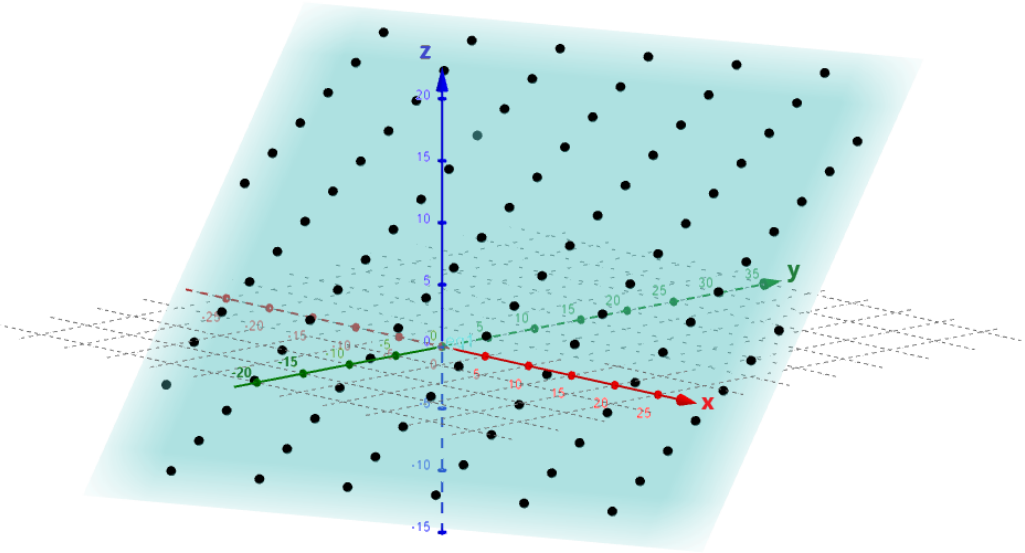


Figura 3.2: reticulado do exemplo 3.26

(*c*) Por fim, no Exemplo 3.29, o pontilhado sobre a reta dada representa a solução da equação Diofantina. Perceba que, dado o vetor diretor $(-2, 3)$ e o ponto $(-1, 1)$ de coordenadas inteiras pertencentes a reta, a partir da combinação linear desses dois elementos é possível obter as demais soluções. Como fica explicito na imagem abaixo.

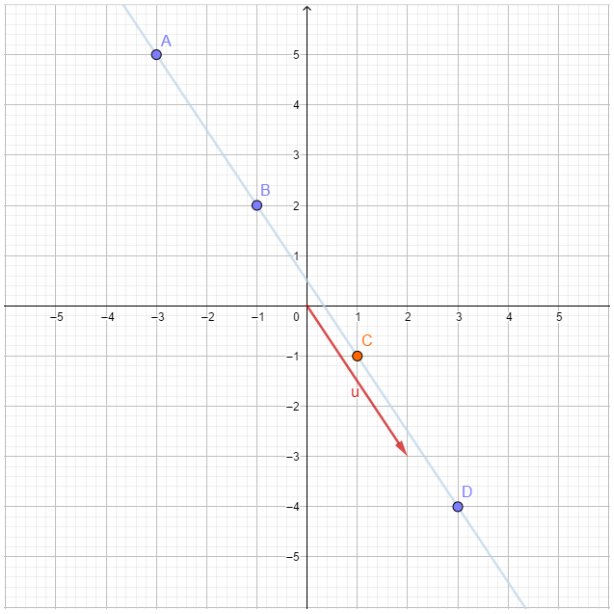


Figura 3.3: gráfico do exemplo 3.29

Vimos que em um sistema de equações lineares Diofantinas com m equações e n incógnitas pode ser representado matricialmente da seguinte forma:

$$AX = B,$$

em que $A = [a_{ij}]_{m\times n}$ é a matriz dos coeficientes das equações, $X = (x_1, \cdots, x_n)^t$ é a matriz das incógnitas e $B = (b_1, \cdots, b_m)^t$ a matriz dos termos independentes.

Claramente, se X_0 é uma solução particular do sistema, isto é, um vetor tal que $AX_0 = B$, podemos subtrair as equações e obter:

$$A(X - X_0) = 0$$

que, a menos de mudança de variáveis é um reticulado de $\mathbb{R}^n$. De fato, considere $Y = X - X_0$, o sistema $AY = 0$ tem como solução um reticulado ($de \quad posto = posto(A) \leq m$) e portanto possui uma base $v_1, v_2, \cdots, v_{n-m}$. Assim, a solução geral dos sistema de equações diofantinas é

$$X = X_0 + a_1v_1 + a_2v_2 + \ldots + a_{n-m}v_{n-m}.$$

Esta observação generaliza a ideia de que em um hiperplano, conhecido um ponto de coordenadas inteiras, encontramos todos os outros usando vetores diretores primitivos de entradas inteiras (base do reticulado).

Referências Bibliográficas

[1] ANTON, H.; RORRES, C. **Álgebra Linear com aplicações**. 8. ed. Porto Alegre: Editora Bookman, 2001.

[2] ATKINS, P. W.; JONES, L. **Princípios de química**: questionando a vida moderna e o meio ambiente. 3. ed. Porto Alegre: Editora Bookman, 2006.

[3] BARRETO, R. C. P. P. **Aritmética modular, códigos elementares e criptografia**. 2014. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal de Sergipe, São Cristóvão, 2014. Disponível em: `https://ri.ufs.br/bitstream/riufs/6508/1/REGENE_CHAVES_PIMENTEL_P_BARRETO.pdf`. Acessado em: 10 fev. 2019.

[4] BOLDRINI, J. L. **Álgebra Linear**. 3. ed. São Paulo: Editora Harbra, 1980.

[5] BOYER, C. B. **História da Matemática**; tradução Elza F. Gomide. 2. ed. São Paulo: Editora Edgard Blucher, 1996.

[6] EUCLIDES. **Os elementos**. Tradução e introdução de Irineu Bicudo. São Paulo: Editora UNESP, 2009.

[7] EVES, H. **Introdução à História da Matemática**. Tradução Hygino H. Domingues. Campinas: Editora da UNICAMP, 2004.

[8] FONSECA, R. V. **Teoria dos números**, Belém: EDUEPA, 2011. Disponível em: `https://ccse.uepa.br/downloads/material_2010/LIVRO_TN.pdf`. Acessado em: Acessado em: 11 fev. 2019.

[9] GILBERT, W. J.; PATHRIA, A. **Linear Diophantine Equations**. [Canadá: *s.n.*], 1990. Disponível em: `https://www.math.uwaterloo.ca/~wgilbert/Research/GilbertPathria.pdf`. Acessado em: 2 fev. 2019.

[10] HEFEZ, A. **Aritmética**. 2. ed. Rio de Janeiro: SBM, 2016. (Coleção PROFMAT).

[11] HEFEZ, A.; FERNANDEZ, C.S. **Introdução à álgebra linear**. 2. ed. Rio de Janeiro: SBM, 2016. (Coleção PROFMAT).

[12] IEZZI, G.; HAZZAN, S. **Sequências, matrizes, determinantes e sistemas**. 6. Ed., São Paulo: Editora Atual, 2001. (Coleção Fundamentos da Matemática Elementar, 4).

[13] LAZEBNIK, F. On system of linear diophantine equations. **Mathematcs Magazine**, [Washington], v. 69, n. 4, p. 261-266, 1996. Disponível em: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.94.6106&rep=rep1&type=pdf. Acessado em: 2 fev. 2019.

[14] LIMA, R. V. **Equações Diofantina**s. TCC (Graduação em Matemática licenciatura) - Universidade Federal de São João del-Rei, São João del-Rei, 2017. Disponível em: https://www.ufsj.edu.br/portal2-repositorio/File/comat/tcc_Ricardo.pdf. Acessado em: 18 maio 2019.

[15] LORENSATTI, E. J. C. Aritmetica: um pouco de história. In: Seminário de Pesquisa em Educação da Região Sul, 9., 2012, Caxias do Sul. **Anais...**. Caxias do Sul, 2012, p. 1-15. Disponível em: http://www.ucs.br/etc/conferencias/index.php/anpedsul/9anpedsul/paper/viewFile/1786/265. Acessado em: 19 maio 2019.

[16] SOUSA, F. B.; SABINO, Elizabeth R.; SABINO, Elizete R. Abordagem histórica e conceitual sobre os sistemas de equações lineares e sua relação com matrizes e determinantes. In: Jornada de estudos em Matemática, 3., 2017, Marabá. **Anais...**, Marabá, 2017, p. 1-15. Disponível em: https://jem.unifesspa.edu.br/images/3JEM/ABORDAGEM-HISTRICA-E-CONCEITUAL-SOBRE-OS-SISTEMAS-DE-EQUAES-LINEARES-.E-SUA-RELAO-COM-MATRIZES-E-DETERMINANTES.pdf Acessado em: 20 maio 2019.

[17] VITAL, F. T. **Métodos de resolução de sistemas e custo computacional**. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade de Brasília, Brasília, 2014. Disponível em: https://repositorio.unb.br/bitstream/10482/17197/1/2014_FelipeTorresVital.pdf. Acessado em: 20 jun. 2019.