UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

JUSCIMAR DA SILVA ARAUJO

Soluções de Equações Diofantinas Lineares Padrões de Ordem Superior

Campinas

2020

Juscimar da Silva Araujo

Soluções de Equações Diofantinas Lineares Padrões de Ordem Superior

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática Aplicada e Computacional.

Orientador: Simão Nicolau Stelmastchuk

Este exemplar corresponde à versão final da Dissertação defendida pelo aluno Juscimar da Silva Araujo e orientada pelo Prof. Dr. Simão Nicolau Stelmastchuk.

Campinas

2020

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

Ar15s

Araujo, Juscimar da Silva, 1989-
Soluções de equações diofantinas lineares padrões de ordem superior / Juscimar da Silva Araujo. – Campinas, SP : [s.n.], 2020.

Orientador: Simão Nicolau Stelmastchuk.
Dissertação (mestrado profissional) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Teoria dos números. 2. Equações diofantinas. 3. Python (Linguagem de programação de computador). 4. Algoritmos. I. Stelmastchuk, Simão Nicolau, 1977-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Solutions of higher-order standard linear diophantine equations
Palavras-chave em inglês:
Number theory
Diophantine equations
Python (Computer program language)
Algorithms
Área de concentração: Matemática Aplicada e Computacional
Titulação: Mestre em Matemática Aplicada e Computacional
Banca examinadora:
Simão Nicolau Stelmastchuk [Orientador]
José Plínio de Oliveira Santos
Robson da Silva
Data de defesa: 02-10-2020
Programa de Pós-Graduação: Matemática Aplicada e Computacional

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0001-5328-0825
- Currículo Lattes do autor: http://lattes.cnpq.br/8297581117307997

Dissertação de Mestrado Profissional defendida em 02 de outubro de 2020 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SIMÃO NICOLAU STELMASTCHUK

Prof(a). Dr(a). JOSÉ PLÍNIO DE OLIVEIRA SANTOS

Prof(a). Dr(a). ROBSON DA SILVA

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Aos meus pais Luis e Daci e aos meus irmãos.

Agradecimentos

Ao longo dos anos de trabalho que resultaram nesta dissertação, pessoas e instituições me ajudaram, ensinando e apoiando. Agora que alcanço meus objetivos não poderia deixar de reconhecê-las.

Ao Naruto Uzumaki por ensinar-me que nunca devemos desistir.

Começo, como não poderia ser diferente, por agradecer a Deus que me acompanhou e me conduziu nesse processo, e que sempre me deu forças nas horas que fraquejei e nos momentos em que pensei em desistir. Aos meus pais, Luis e Daci e aos meus irmãos, por tudo que representam em minha vida.

Aos meus avós que, apesar de não estarem aqui do meu lado, tenho certeza que de algum lugar eles acompanham o desenvolvimento deste trabalho. Dedico este em memória a minha vovó Antônia Pereira, minha vovó Lindomar Araujo e meu vovô Raimundo Campelo, vovô Adão Araujo (ainda vivo) que, junto com meus pais, foram os grandes responsáveis por minha formação pessoal.

Ao professor que sempre será minha inspiração na Matemática; José Coelho (meu professor do ensino fundamental) e minha mãe-mentora científica professora Mara, que acolheu-me como filho científico desde o início da graduação e a quem devo muito. Serei eternamente grato!

Ao meu orientador e professor Simão Nicolau, pela orientação, paciência, amizade e confiança. Aos professores e servidores do IMECC-UNICAMP; em especial ao Prof. Cristiano Torezzan, sem vocês isso não seria possível.

Aos colegas de turma, principalmente aos amigos-irmãos Emerson Dutra, Adriano Monteiro e George Almeida. Com igual carinho ao Edu (Eduardo), Altenize, Eider, Paulo, Anderson, Carol, Cris (e aos seus chás) e ao Ricardo (Rick). Ao meu eterno "quarteto fantástico" da graduação: Laila, Janaina e Talita, que sempre incentivaram a continuação dos estudos.

Aos meus eternos mestres, os professores do Departamento de Matemática do CESBA-UEMA: Mara, Franzé, Nilson, Olívio e Sérgio.

Aos amigos que a vida deu-me: Renato Borseti, Filipe Igor, Gisele Bosso, Clovis Caface, Eduardo (Edu) Aragão, Mauro, Marco Antônio, Zilmar, Alba, Adriana, Hilza, Cintia, João (Capitão América) e Otávio, cada de vocês tem um lugar especial em minha história de vida.

"É preciso força pra sonhar e perceber que a estrada vai além do que se vê".
(Marcelo Camelo)

Resumo

Neste trabalho temos como objetivo o estudo das equações diofantinas lineares padrões. Em verdade, apresentamos um algoritmo modificado de Jacobi-Perron para construir soluções de uma equação diofantina padrão. O método em si é um algoritmo. Sendo assim, implementamos um código na linguagem de programação Phyton para gerar os vetores soluções padrões de uma equação diofantina linear padrão.

Palavras-chave: Teoria dos Números, Equações Diofantinas, Python.

Abstract

In this work we aim to study standard linear Diophantine equations. In In fact, we present a modified Jacobi-Perron algorithm to build solutions from one standard Diophantine equation. The method itself is an algorithm. Therefore, we implemented a code in the Phyton programming language to generate the standard solutions vectors of a standard linear Diophantine equation.

Keywords: Number Theory, Diophantine Equations, Python.

Lista de símbolos

N :	Conjunto dos números Naturais.
Z :	Conjunto dos números Inteiros.
Z^* :	Conjunto dos números Inteiros não-nulos.
Z_+ :	Conjunto dos números Inteiros positivos.
Z_- :	Conjunto dos números Inteiros negativos.
$\in$:	Pertence a.
$\mid$:	Divide.
:	Não divide.
; :	Tal que.
$\neq$:	Diferente de.
=:	Igual a.
$\lfloor x \rfloor$:	Maior inteiro menor ou igual a x.
$\forall$:	Para todo.

Lista de Códigos-fonte

Sumário

Introdução

A Teoria dos Números é um ramo da Matemática Pura. Dentre seus enfoques, destacamos o estudo dos números inteiros. Dentro dessa temática dos inteiros, temos estudos relacionados a soluções de equações com valores inteiros para suas incógnitas.

O problema de resolver equações diofantinas, que tem destaque especial e antigo na Teoria dos Números, vem sendo objeto de estudo de muitos pesquisadores ao longo dos anos. Assim, como exemplo, o problema de determinar em quais circunstâncias equações do tipo $c_1x_1 + c_2x_2 = c$ são ou não solúveis, já foi objeto de muitos trabalhos. Aqui nos propomos a apresentar equações diofantinas do tipo $c_1x_1 + c_2x_2 + \ldots + c_nx_n = 1$, para $n > 2$ e apresentamos formas de determinar sua solução, quando existe.

Nesta dissertação, apresentamos o estudo de um tipo especial de equação diofantina de ordem superior e um algoritmo que facilita a resolução desse tipo de equação e para isto, iniciaremos por uma revisão dos principais tópicos elementares da teoria dos números.

Este trabalho foi estruturado da seguinte maneira:

No Capítulo 1, são apresentados alguns conceitos históricos e definições elementares da teoria elementar dos números, como, divisibilidade em inteiros, máximo divisor comum, algoritmo da divisão de Euclides, alguns teoremas importantes (a exemplo do de Bézout) relativos ao estudo de equações diofantinas em duas variáveis.

No Capítulo 2, faremos uma abordagem das equações diofantinas lineares padrão, onde apresentamos condições que caracterizam essas equações e teoremas sobre soluções destas equações, bem como mostramos um algoritmo de Jacobi-Perron, como determinar um vetor solução e finalizamos o capítulo com alguns exemplos numéricos.

Por fim, no Capítulo 3, apresentamos aplicações numéricas das equações diofantinas lineares padrão, fazendo uso de um código desenvolvido em Python e disponível no apêndice desta dissertação.

No Apêndice apresentamos todos os códigos utilizados no decorrer do trabalho.

1 Equações Diofantinas

Este capítulo é voltado ao estabelecimento da história, das definições e propriedades elementares referentes à relação de divisibilidade no conjunto dos números inteiros, enfatizando o algoritmo da divisão de Euclides, a noção de máximo divisor comum e o estudo de um tipo especial de equação.

Do algoritmo da divisão de Euclides decorre a possibilidade de estudarmos um tipo especial de equação: as *Equações Diofantinas*, assim chamadas em homenagem a Diofanto de Alexandria que morreu por volta de 300 a.C.. Tais equações nada mais são do que equações com coeficientes e soluções inteiras apresentadas geralmente com mais de uma variável. Neste capítulo veremos algumas definições e resultados que nos permitirão entender melhor sobre essas importantes equações. Para um maior aprofundamento podem ser consultadas as referências (BOYER, C. B.,), (BURTON, D. M.,), (CAJORI, F.,), (EVES, H.,), (FONSECA, R. V. F.,), (HEFEZ, A., a), (HEFEZ, A., b), (LEVEQUE, W.J.,), (LOVÁSZ, L.; PELIKÁN, J; VESZTERGOMBI, K.,), (NETO, A. C. M., b), (NIVEN, I.; ZUCKERMAN, H.S.,), (SANTOS, J. P. O.,), (SOUZA, R. S.,).

1.1 Teoria dos Números

Segundo (LOVÁSZ, L.; PELIKÁN, J; VESZTERGOMBI, K.,), Teoria dos Números é um campo verdadeiramente venerável; suas raízes estão no início da matemática grega.

A História da Matemática nos diz que um dos importantes nomes da Teoria dos Números é Diofanto [1]; que tem o seu nome ligado à cidade que foi o maior centro de atividade matemática na Grécia Antiga, a cidade de Alexandria [2]. Pouco sabe-se acerca da sua vida, a incerteza impede-nos mesmo de fixar com segurança em que século viveu. A única prova positiva quanto à data de suas atividades é que o bispo de Laodiceia, que começou seu episcopado em 270, dedicou um livro sobre cálculo egípcio para seu amigo Diofanto. Têm sido sugeridas datas distanciadas de um século, antes ou depois do ano 250 d.C.. Pode-se pensar que com 2500 anos de pesquisa, saberíamos essencialmente tudo sobre o assunto.

Por uns versos encontrados no seu túmulo, escritos em forma de um enigmático problema, deduz-se que viveu 84 anos. No entanto, tal problema não deve ser tomado como o paradigma dos problemas sobre os quais se interessou Diofanto, pois, segundo

[1] Considerado o maior algebrista grego - "o pai da Álgebra".
[2] Importante e abundante cidade do Egito.

(BOYER, C. B.,), ele pouca atenção deu a equações do 1º grau. Alexandria foi sempre um centro muito cosmopolita e a Matemática que se originou nela não era toda do mesmo tipo; os resultados de Heron eram bem diferentes dos de Euclides ou dos de Apolônio ou dos de Arquimedes, e na obra de Diofanto há novamente uma quebra repentina da tradição clássica grega.

Sabe-se, através do Jornal de Matemática Elementar, que os gregos, na época clássica, dividiram a aritmética em dois ramos; a aritmética propriamente dita como "teoria dos números naturais", que frequentemente, tinha mais em comum com a filosofia platônica e pitagórica do que com o que habitualmente se considera como Matemática, e logística ou cálculo prático que estabelecia as regras práticas de cálculo que eram úteis à Astronomia, à Mecânica, etc.

A principal obra de Diofanto conhecida, e que ao que parece, só em parte chegou até nós, é a *Arithmetica* [3]. Segundo (DOMINGUES, H. H.,), apenas seis dos livros originais em grego e quatro em árabe sobreviveram, o número total treze não passa de uma suposição; algo apresentado ao longo da história. Era um tratado caracterizado por um alto grau de habilidade matemática e de engenho, pelo que pode ser comparado aos grandes clássicos da primeira idade Alexandrina, ou seja, da época de ouro da matemática grega; no entanto, quase nada têm em comum com esses ou, na verdade, com qualquer matemática grega tradicional. Representa essencialmente um novo ramo e usa um método diferente, daí a época em que possivelmente Diofanto viveu se chamar segunda idade Alexandrina, conhecida por sua vez como época de prata da matemática grega.

Diofanto, mais que um cultor da aritmética, e, sobretudo da geometria, como o foram os matemáticos gregos anteriores, deve ser considerado um precursor da Álgebra, e, em certo sentido, mais vinculado com a matemática dos povos orientais, que com a dos gregos. A sua "Aritmética" assemelha-se à álgebra babilônica em muitos aspectos, mas enquanto os matemáticos babilônicos se ocupavam principalmente com soluções aproximadas de equações determinadas e, sobretudo de equações indeterminadas do 2º e do 3º graus das formas canônicas, em notação atual, $Ax^2+Bx+C=y^2$ e $Ax^3+Bx^2+C=y^2$, ou conjuntos - sistemas - destas equações. É exatamente, por esta razão, em homenagem a Diofanto - que a esta "Análise indeterminada" chama-se "Análise Diofantina" ou "Análise Diofântica".

No desenvolvimento histórico da Álgebra considera-se, em geral, que podem ser reconhecidos três estágios, a saber: o primitivo ou retórico, em que tudo era completamente escrito em palavras, um intermédio ou sincopado, em que foram adaptadas algumas abreviaturas e convenções, e um final ou simbólico, em que são usados somente símbolos. A

[3] Descrita como o mais antigo tratado sobre Álgebra, onde encontrou-se o primeiro uso sistemático da notação matemática, embora os símbolos empregados fossem abreviações das palavras em vez de símbolos algébricos no sentido empregado nos dias atuais.

"Aritmética" de Diofanto deve ser colocada no segundo estágio; pois, nos seus seis livros há um uso sistemático de abreviaturas para potências de números e para relações e operações.

A Teoria dos Números é considerada um ramo da Matemática que dá concentração especial ao estudo dos Números Inteiros (Z). É de certo modo surpreendente que a Teoria dos Números seja atualmente uma das áreas de pesquisa mais efervescentes da Matemática, objeto de estudo de muitos pesquisadores e que, de forma intensa, continue a fascinar e desafiar as atuais gerações de matemáticos. São três os principais ramos em que se divide a Teoria dos Números: Teoria Elementar, Teoria Analítica e Teoria Algébrica. Neste capítulo vamos nos limitar à parte elementar, onde apresentaremos resultados básicos, através de definições, proposições, corolários, teoremas e exemplos; que serão necessários para definir um método que fornece o número total de soluções inteiras das Equações Diofantinas.

1.2 Alguns resultados elementares da Teoria dos Números

Os números têm uma importância fundamental na existência da Matemática; foram considerados durante milênios como entes intuitivos e algumas de suas propriedades, como por exemplo, a comutatividade e a associatividade da adição e da multiplicação eram consideradas inerentes à sua própria natureza, e assim, não necessitando de demonstração - seriam como axiomas matemáticos.

O vasto e grandioso avanço e desenvolvimento matemático a partir da criação do Cálculo Diferencial, no século XVII, trouxe aos matemáticos novos problemas que, para serem mais bem compreendidos, interpretados e solucionados, requeriam uma fundamentação mais rigorosa do conceito de número. Os números naturais ainda resistiram às investidas por algum tempo. Só no final do século XIX, quando os fundamentos de toda a Matemática foram questionados e intensamente repensados, é que a noção de número passou a ser baseada em conceitos da Teoria dos Conjuntos, considerados mais primitivos.

Os números inteiros foram gradualmente perdendo sua associação à superstição e ao misticismo, mas seu interesse para os matemáticos nunca diminuiu. Euclides, fez contribuições originais à Teoria dos Números, embora sua geometria fosse amplamente uma compilação de resultados anteriores. Diofanto de Alexandria, um dos primeiros algebristas, deixou sua marca na Teoria dos Números. Fermat [4] (1601-1665), um dos jurista de Toulouse e um dos maiores matemáticos de sua época, iniciou o trabalho moderno neste campo. Euler (1707-1783), o mais prolífero dos matemáticos, incluiu muito da Teoria dos Números em suas pesquisas. Outros nomes destacados na história da Matemática podem ser incluídos: Legendre, Dirichlet e Riemann.

[4] Pierre de Fermat foi um magistrado, entusiasta matemático e cientista. Por não ter formação em Matemática, é considerado Príncipe dos Amadores.

Já Gauss [5], (1777-1855), o maior matemático dos tempos modernos, dedicou-se a muitos ramos diferentes da Matemática; diz-se que ele expressou sua opinião sobre a Teoria dos Números na seguinte observação: "A Matemática é a rainha das ciências e a Teoria dos Números é a rainha da Matemática."

Um marco da construção dos números foi encerrado em 1888, com o trabalho de Dedekind [6]. A construção de Dedekind não teve muita amplitude na época por ser complexa; tornando-se mais popular com a axiomática que Giuseppe Peano deu no século XIX. Para os números inteiros daremos um tratamento axiomático, tendo como ponto de partida uma lista de propriedades básicas que os caracterizarão completamente, para delas deduzir as demais propriedades.

A noção básica de conjunto não é definida, isto é, é aceita intuitivamente e, por isso, chamada noção primitiva. Ela foi utilizada primeiramente por Georg Ferdinand Ludwig Philip Cantor, matemático nascido em São Petersburgo, na Rússia, em 3 de março de 1845, e falecido em Halle, Alemanha, em 6 de janeiro de 1918. Segundo ele, a noção de conjunto designa uma coleção de objetos bem definidos e discerníveis, chamados elementos do conjunto. Segundo Bertrand Russel, denomina-se número natural a "tudo que for definido por um conjunto e, por todos os conjuntos que lhe sejam equivalentes". A maioria das proposições na Teoria dos Números, da mesma forma que na Matemática como um todo, estão relacionadas não a um objeto isolado, mas a toda uma classe de objetos com alguma propriedade comum. Consideremos o conjunto dos naturais como sendo,

$$N = \{0, 1, 2, 3, 4, \ldots\}$$

isto é, o conjunto dos inteiros não negativos.

O conjunto (Z) dos números inteiros é munido de duas operações; uma adição ($+$) que tem como elemento neutro o número inteiro zero (0) e uma multiplicação ($\cdot$) que também tem seu elemento neutro, o número inteiro um (1). Consideremos o conjunto dos números inteiros como sendo,

$$Z = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}$$

ou seja, o conjunto formado pelos números naturais e os números inteiros negativos, e

$$Z^* = \{\pm 1, \pm 2, \pm 3, \pm 4, \ldots\}$$

que representa os números inteiros não nulos,

[5] Johann Carl Friedrich Gauss, considerado o Príncipe dos Matemáticos

[6] Dedekind publicou um trabalho onde, a partir de noções básicas da Teoria dos Conjuntos, é elaborado um modelo para os números naturais, definindo as operações de adição e multiplicação e demonstrando as suas propriedades básicas.

$$Z_+ = \{1, 2, 3, 4, \ldots\}$$

que representa os números inteiros positivos, e

$$Z_- = \{\ldots, -4, -3, -2, -1\}$$

que representa os números inteiros negativos. Sendo a e b dois números inteiros quaisquer, denotaremos por $a + b$ a soma de a e b e $a \cdot b$ (ou ab) o produto de a por b.

Vejamos algumas propriedades que assumiremos aqui como axiomas.

Dados $a, b, c, d \in Z$, segue:

1. A adição e a multiplicação são bem definidas:

$$a = c \text{ e } b = d \Rightarrow a + b = c + d \text{ e } a \cdot b = c \cdot d.$$

2. A adição e a multiplicação são comutativas:

$$a + b = b + a \text{ e } a \cdot b = b \cdot a.$$

3. A adição e a multiplicação são associativas:

$$(a + b) + c = a + (b + c) \text{ e } (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

4. A multiplicação é distributiva em relação à adição:

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

5. Tricotomia: Dados $a, b \in Z$, uma, e apenas uma, das seguintes possibilidades é verificada:

   i) $a = b$;

   ii) Existe $c \in Z^*, b = a + c$ (também equivale a dizer que $a < b$);

   iii) Existe $c \in Z^*, a = b + c$ (também equivale a dizer que $b < a$).

6. Lei da existência de Inversos Aditivos:

   Para todo inteiro a existe um inteiro x tal que $a + x = x + a = 0$. Nesse caso, denotamos x por $-a$ que pode ser chamado também de oposto ou simétrico de a. Sendo a e b dois inteiros, define-se $a - b = a + (-b)$.

7. Lei do Cancelamento da Multiplicação:

   Se a, b, $c \in Z$, com $c \neq 0$ e $a \cdot c = b \cdot c$ então $a = b$.

8. Lei do Cancelamento da Adição:

   Se $a, b, c \in Z$ e $a + c = b + c$ então $a = b$.

1.2.1 Divisibilidade em Z

Sabe-se que nem sempre é possível dividir de modo exato um elemento por outro, a noção de divisibilidade assume um papel importante.

O tema divisibilidade no conjunto dos inteiros é extremamente importante para a resolução de problemas em Teoria dos Números. Abaixo, definiremos uma relação binária no conjunto dos inteiros: a divisibilidade. Para um estudo mais aprofundado sobre o tema, ver (ALENCAR, F. E.,) e (MARTINEZ, F. et al,).

Dados $a, b, c \in Z$ e $b \neq 0$ dizemos que b divide a, ou que a é um múltiplo de b, ou ainda que b é um divisor de a se, existe $c \in Z$ tal que $a = b \cdot c$.

Destacamos quatro consequências imediatas dessa definição.

i) Para todo $a \in Z$, 1 divide a; já que $a = 1 \cdot a$.

ii) Para todo $a \in Z^*$, a divide a; já que $a = a \cdot 1$.

iii) Para todo $a \in Z^*$, a divide 0; já que $0 = a \cdot 0$.

iv) Para todo $a, c \in Z$, c divide a implica que $|c| \leqslant |a|$.

A partir de agora usaremos a notação $b|a$ para indicar que b divide a. Note que $b|a \Leftrightarrow a = b \cdot c$, para algum $c \in Z$. Se $b \neq 0$, o inteiro c nas condições da definição é único; pois se existisse outro $c' \in Z$ tal que $a = b \cdot c'$, teríamos $b \cdot c' = b \cdot c$, daí obtemos que $c = c'$, pela lei do cancelamento multiplicativo. Esse c assim definido é chamado de quociente de a por b.

Por outro lado, veja que $0|a$ se, e somente se, $a = 0$. Neste caso o quociente não é único, pois $0 \cdot c = 0$, para todo $c \in Z$. Por isso excluímos o caso em que o divisor é nulo.

De acordo com a definição de divisibilidade, apresentamos as seguintes proposições:

Dados a, b, c, x e y números inteiros; segue que:

1. Se $a|1$ então $a| \pm 1$.
2. Se a, b, c e d são inteiros com $a, b \neq 0$, tais que $a|b$ e $c|d$ então $ac|bd$.
3. Se a, b, c são inteiros com $a \neq 0$ e $b \neq 0$, tais que $a|b$ e $b|c$ então $a|c$.
4. Sejam a e b inteiros e diferentes de zero, se $a|b$ e $b|a$ então $a = \pm b$.
5. Sejam a e b inteiros e diferentes de zero, se $a|b$ então $|a| \leqslant |b|$.
6. Se a, b, c, x, y são inteiros com $a \neq 0$, tais que se $a|b$ e se $a|c$ então $a|(b \cdot x + c \cdot y)$.

(1) Suponhamos que a divide 1, então existe $q \in Z$ tal que $1 = q \cdot a$. Isto implica que $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$, concluímos assim que $a = \pm 1$.
(2) Suponhamos que $a|b$ e $c|d$, então existam $u, v \in Z$ tais que $b = a \cdot u$ e $d = v \cdot c$. Multiplicando-se as equações membro a membro temos que $b \cdot d = (u \cdot v) \cdot ac$ daí $ac|bd$.
(3) Suponhamos que $a|b$ e $b|c$, então existam $u, v \in Z$ tais que $b = a \cdot u$ e $c = b \cdot v$. Logo, $c = a \cdot (u \cdot v)$ e, assim, $a|c$.
(4) Suponhamos que $a|b$ e $b|a$, então existam $u, v \in Z$ tais que $b = a \cdot u$ e $a = b \cdot v$. Logo $a = a \cdot (u \cdot v)$ que implica $u \cdot v = 1$. Assim $u|1$ e daí temos que $u = \pm 1$. Disso, $a = \pm b$.
(5) Suponhamos que $a|b$. Logo existe $u \in Z$ com $u \neq 0$ tal que $b = a \cdot u$. Disso, $|b| = |a| \cdot |u|$. Como $u \neq 0$ temos que $|u| \geqslant 1$. Desse modo segue que $|b| \geqslant |a|$.
(6) Assumamos que $a|b$ e $a|c$. Assim, existem $u, v \in Z$ tais que $b = a \cdot u$ e $c = a \cdot v$. Logo, para quaisquer que sejam os inteiros x e y temos que

$$b \cdot x + c \cdot y = (a \cdot u)x + (a \cdot v)y = a \cdot (u \cdot x) + a \cdot (v \cdot y) = a \cdot (u \cdot x + v \cdot y).$$

Isto implica que $a|(bx+cy)$.

1.2.2 Máximo Divisor Comum

A definição de máximo divisor comum é muito usada em inúmeras áreas da Ciência. Desde analisar ou inferir em relação ao ciclo de vida de alguns seres vivos, prever alinhamentos de corpos celestes, até avaliar e interpretar o desperdício em construções civis. As noções fundamentais de *máximo divisor comum* são de grande e relevante importância na fundamentação deste e do próximo capítulo, pois compõem uma parcela significativa da Teoria Elementar dos Números; com isso pretendemos mostrar esta relevância através da seguinte abordagem teórico-científica. Para mais detalhes, ver (FIORELLI, J. O.,).

Dados dois números inteiros a e b, com $a \neq 0$ ou $b \neq 0$, dizemos que um inteiro d é um divisor comum de a e b quando $d|a$ e $d|b$. Disto, segue a definição dada por (MARTINEZ, F. et al,).

Dados dois números inteiros a e b com $a \neq 0$ ou $b \neq 0$, a cada um deles pode-se associar seu conjunto de divisores positivos, D_a e D_b respectivamente, e a intersecção de tais conjuntos $D_a \cap D_b$ é finita e não vazia (visto que 1 pertence à intersecção). Por ser finito, $D_a \cap D_b$ possui elemento máximo, que é chamado de *máximo divisor comum* dos números a e b. Denotaremos este número por (a, b). Para $a = b = 0$ convencionamos $(0, 0) = 0$. Quando $(a, b) = 1$ dizemos que a e b são primos entre si.

A seguir mostraremos um teorema muito importante para a Teoria Elementar dos Números, bastante utilizado na resolução de problemas envolvendo inteiros; objeto desse trabalho. Trata-se de uma famosa identidade cujo nome é creditado ao matemático

francês Étienne Bézout (1730 - 1783). Tal identidade relaciona números a e b com seu máximo divisor comum.

(**Teorema de Bézout**) Dados inteiros a e b, quaisquer, se $d = (a, b)$, então existem inteiros n e m tais que $d = an + bm$. Consideremos o conjunto $W = \{ax + by;\ x, y \in Z \text{ e } ax + by > 0\}$. Notemos que W não é vazio. De fato, para $x = y = 1$, $a \cdot 1 + b \cdot 1 = a + b > 0 \Rightarrow a + b \in W$. Assim, pelo Princípio da Boa Ordem, W possui menor elemento, digamos $\lambda = min\ W$. Vamos mostrar que $\lambda = (a, b)$. Como $\lambda \in W$, existem $n, m \in Z$ tais que

$$\lambda = an + bm \tag{1.1}$$

Usando o algoritmo da divisão com os elementos a e λ, temos

$$a = \lambda q + r, \text{com } 0 \leqslant r < \lambda. \tag{1.2}$$

Substituindo o valor de λ em (1.1) na igualdade de (1.2), segue que $r = a - \lambda q = a - (an + bm)q = a - aqn - bqm$. Daí, $r = a(1 - qn) + b(-qm)$. Logo, temos que $r = au + bv$ com $u = 1 - qn$ e $v = -qm$. Consequentemente, $r = 0$, caso contrário, $r > 0$ e, assim, $r \in W$, o que contraria o fato de λ ser o menor elemento de W, visto que $r < \lambda$. Portanto, $a = \lambda q$, ou seja, $\lambda |\ a$. Analogamente, prova-se que $\lambda | b$. Sendo $d = (a, b)$, existem λ_1 e λ_2 tais que $a = d\lambda_1$ e $b = d\lambda_2$. Logo, por (1.1), $\lambda = (d\lambda_1)n + (d\lambda_2)m = d(\lambda_1 n + \lambda_2 m)$, ou seja, $d | \lambda$, e como $\lambda | d$, pois $d = (a, b)$, segue que $d = \lambda$. Portanto, $d = an + bm$.

□

Mostraremos a seguir uma outra caracterização de máximo divisor comum, a qual é usada correntemente nos cursos da Educação Básica.

Sejam a e b inteiros não simultaneamente nulos. Um inteiro positivo d é máximo divisor comum de a e b se, e somente se, satisfaz as seguintes condições:

i) $d | a$ e $d | b$;

ii) se $c | a$ e se $c | b$ então $c | d$.

($\Rightarrow$) Seja $d = (a, b)$. Então, obviamente, d satisfaz a condição (i). Além disso, existem inteiros x e y tais que $d = ax + by$. Se $c | a$ e $c | b$ então $c | ax + by$ e, portanto, $c | d$, isto é, a condição (ii) também é satisfeita.
($\Leftarrow$) Seja d um inteiro positivo satisfazendo i) e ii). Da condição i) vemos que d pertence ao conjunto D_a dos divisores de a e ao conjunto D_b dos divisores de b. Agora a hipótese da proposição ii) nos diz que dado um c pertence a $D_a \cap D_b$ então ele divide d. Pelo ítem 5. da Proposição 1.2.1, $|c| < d$. Isto nos diz que d é o máximo dos divisores de a e de b, e a prova segue.

□

Vejamos que, da condição *(i)*, d é um divisor comum de a e b, e pela condição *(ii)*, d é o maior dentre todos os divisores comuns de a e b. O conceito de máximo divisor comum mostrado acima, estende-se de maneira natural a mais de dois inteiros. A definição de máximo divisor comum para inteiros a e b, também é válida para uma quantidade finita de inteiros $a_1, a_2, ..., a_n$, como exemplo, o (a_1, a_2, a_3).

Sejam a, b, c inteiros não todos nulos, o máximo divisor comum desses inteiros, denotado por (a, b, c), é o inteiro positivo d que satisfaz as seguintes condições:

1. $d|a,\ d|b$ e $d|c$;
2. Se k é um inteiro tal que $k|a,\ k|b$ e $k|c$, então $k \leqslant d$.

Segue um resultado importante, referente ao cálculo de (a, b, c).

Sejam a, b, c inteiros, com $a \neq 0$. Então o $(a, b, c) = ((a, b), c)$. Sejam $d = (a, b, c)$ e $k = (a, b)$. Desejamos mostrar que $d = (k, c)$. Por definição, temos que $d|a$, $d|b$ e $d|c$. Então, pelo Teorema 1.2.2, $d|k$. Logo $d|k$ e $d|c$. Se $f \in Z$ é tal que $f|k$ e $f|c$, então $f|a$ e $f|b$ e, consequentemente, $f|a$, $f|b$ e $f|c$. Concluímos, pela definição de máximo divisor comum, que , $f|d$. Portanto, $d = (k, c)$.

$$(8, 16, 24) = (((8, 16), 24)) = (8, 24) = 8.$$

1.2.3 Algoritmo da Divisão Euclidiana

Na Matemática contemporânea, a divisão é definida como uma aplicação da multiplicação. Essa era uma situação de debate no contexto da filosofia grega, pois para alguns filósofos, em geral, a fração e divisão não foram consideradas na forma que vemos hoje em dia.

Nesta seção apresentaremos o *Algoritmo* [7] *de Euclides* que permite calcular efetivamente o máximo divisor comum de dois inteiros. Este método encontra-se nos *Elementos de Euclides* (BICUDO, I.,) e nos permitirá também calcular o máximo divisor comum de mais de dois números inteiros; que é ferramenta importante na resolução de equações diofantinas com três ou mais variáveis.

Os Elementos estão divididos em treze livros ou capítulos, dos quais os seis primeiros são sobre geometria plana elementar, os três seguintes sobre Teoria dos Números, o Livro X sobre incomensuráveis e os três últimos versam principalmente sobre geometria no espaço. Não há introdução ou preâmbulo, e o primeiro livro começa abruptamente com uma lista de vinte e três definições. A deficiência, aqui é que algumas definições não são

[7] Um algoritmo é um método sistemático de cálculo.

precisas, pois não há um conjunto prévio de elementos não definidos em termos dos quais os outros sejam conhecidos. Assim, dizer como Euclides, que "um ponto é o que não tem parte", ou que "uma reta é o comprimento sem largura", ou que "uma superfície é o que tem apenas comprimento e largura" não é definir esses entes, pois uma definição deve ser expressa em termos de coisas precedentes que são melhor conhecidas que as coisas definidas.

Em relação a Euclides, sabe-se pouco sobre sua vida; obras clássicas como (BOYER, C. B.,), (CAJORI, F.,) e (EVES, H.,) apresentam registros referentes a este importante nome na Teoria dos Números. Conhecido como Euclides [8] de Alexandria; mestre, escritor de origem provavelmente grega; é até hoje, na História da Matemática, considerado como um dos mais significativos estudiosos deste campo na antiga Grécia. Uma das obras mais importantes do mundo ocidental o tratado matemático de Euclides no sétimo livro, trata de um processo algébrico para achar o máximo divisor comum de dois ou mais números inteiros e ainda usa para verificar se dois inteiros são primos entre si, conhecido como Algoritmo Euclidiano.

Os livros VII, VIII e IX, que no total têm cento e duas proposições, tratam da Teoria Elementar dos Números. O livro VII começa por uma lista de vinte e duas definições distinguindo vários tipos de números - ímpares e pares, primos e compostos, planos e sólidos (isto é, os que são produtos de dois ou três inteiros) e finalmente definindo número perfeito como "aquele que é igual às suas partes". Em seguida versa sobre o processo, hoje conhecido como Algoritmo Euclidiano, para achar o máximo divisor comum de dois ou mais números inteiros e o usa para verificar se dois inteiros são primos entre si.

O resultado abaixo é conhecido como o algoritmo da divisão para números inteiros e é um dos pilares da teoria básica de divisibilidade.

(Algoritmo da Divisão de Euclides) Para quaisquer $a, b \in Z$, com $b > 0$, existe um único par de inteiros q e r, de modo que $a = b \cdot q + r$, onde $0 \leqslant r < b$. Primeira parte (prova da existência): Seja b um número inteiro positivo não nulo. Se $a \in Z$, então a é múltiplo de b ou está compreendido entre dois múltiplos consecutivos de b, isto é, $b \cdot q \leqslant a < b \cdot (q + 1)$. Se $b \cdot q \leqslant a$, então $a = b \cdot q + r$, onde $r \in Z$ e $r \geqslant 0$. Se $a < b \cdot (q + 1)$, temos que $b \cdot q + r < b \cdot q + b$ e daí $r < b$. Logo, podemos afirmar que $a = b \cdot q + r$, com $0 \leqslant r < b$.

Segunda parte(prova da unicidade): Suponhamos que existam inteiros q_1, q_2, r_1, r_2 onde $q_1 \neq q_2$ e $r_1 \neq r_2$, com $r_1 > r_2$ e que satisfaçam às igualdades: $a = b \cdot q_1 + r_1$, com $0 \leqslant r_1 < b$ e $a = b \cdot q_2 + r_2$, com $0 \leqslant r_2 < b$. Se $b > r_1$ e $b > r_2$, então $b > (r_1 - r_2)$ e temos que $a = b \cdot q_1 + r_1 = b \cdot q_2 + r_2$ o que implica que $b \cdot (q_2 - q_1) = r_1 - r_2$. Fazendo $k = (q_2 - q_1)$, temos que $r_1 - r_2 = b \cdot k$, com $k \in Z$, mostrando que $b|(r_1 - r_2)$.

[8] Matemático da escola platônica, e conhecido como o "pai da Geometria", nasceu na Síria aproximadamente em 330 a.C. e realizou seus estudos em Atenas.

Portanto $b \leqslant (r_1 - r_2)$ é absurdo, pois contradiz a hipótese. Logo, $r_1 = r_2$ e concluímos também que $b \cdot (q_2 - q_1) = 0$. Se $b \neq 0$, temos $(q_2 - q_1) = 0$, mostrando que $q_2 = q_1$. □

Segue um exemplo da aplicação do algoritmo.

Determinar $d = (2040, 496)$.

Resolução: Pelo Algoritmo de Euclides, com $a = 2040$ e $b = 496$, temos,

$$\begin{aligned} &2040 = 496 \cdot 4 + 56 \Rightarrow (2040, 496) = (496, 56), \\ &496 = 56 \cdot 8 + 48 \Rightarrow (496, 56) = (56, 48), \\ &56 = 48 \cdot 1 + 8 \Rightarrow (56, 48) = (48, 8), \\ &48 = 8 \cdot 6 + 0 \Rightarrow (8, 0) = 8. \end{aligned} \tag{1.3}$$

Portanto, $d = (2040, 496) = 8$.

Segue uma proposição bastante útil no estudo do máximo divisor comum de dois números inteiros.

Quaisquer que sejam $a, b \in Z$, existe $d \in Z$ que é o máximo divisor comum de a e b. O caso que $a > 0$ e $b > 0$. Seja $K = \{ax + by > 0;\ x, y \in Z\}$. Tomando os elementos estritamente positivos de K. Seja d o menor desses elementos. Vamos mostrar que d é o máximo divisor comum entre a e b.

i) como $d \in K$ então $d \geqslant 0$.

ii) como $d \in K$ então existem x_0 e y_0 tais que;

$$d = ax_0 + by_0. \tag{1.4}$$

Aplicando o algoritmo da divisão aos elementos a e d segue que

$$a = dq + r, \text{com } 0 \leqslant r < d. \tag{1.5}$$

Das duas igualdades temos:

$$\begin{aligned} a &= (ax_0 + by_0)q + r, \\ a &= ax_0q + by_0 + r, \\ r &= a(1 - x_0q) + b(-y_0q). \end{aligned}$$

Dessa forma $r \in K, r \geqslant 0$. Como $r < d$ e d é o menor elemento de K, temos, $r = 0$. De onde tiramos que $a = dq$, o que significa que $d|a$. Aplicando o algoritmo da divisão aos

elementos b e d temos $b = dq^{'} + r^{'}$, com $0 \leqslant r^{'} < d$. Agora, substituindo (1.4) em (1.5), temos que, $b = (ax_0 + by_0) \cdot q^{'} + r^{'}$, o que mostra que,

$$\begin{aligned} r^{'} &= b - by_0q^{'} - ax_0q^{'} \\ r^{'} &= b(1 - q^{'}y_0) + a(-x_0)q^{'}. \end{aligned}$$

Logo $r^{'} = 0$. Concluímos assim que $b = dq^{'}$ e, consequentemente. que $d|b$.

iii) Se $d^{'}|a$ e $d^{'}|b$, existem números k e q tais que $a = d^{'}k$, e $b = d^{'}q$. Multiplicando por x_0 e y_0, respectivamente, as igualdades anteriores vemos que $ax_0 = d^{'}kx_0$ e $by_0 = d^{'}qy_0$. Logo,

$$\begin{aligned} ax_0 + by_0 &= d^{'}(kx_0 + qy_0), \\ d &= d^{'}(kx_0 + qy_0). \end{aligned}$$

Concluímos assim que $d^{'}|d$, o que implica $d = (a, b)$.

1.3 Equações Diofantinas

Alguns resultados aqui expostos podem ser encontrados em (CAMPOS, G. D. M.,). Segundo (FONSECA, R. V. F.,), a teoria das Equações Diofantinas é o ramo da Teoria dos Números que investiga as soluções inteiras de equações polinomiais, como por exemplo:

A equação $x^2 + y^2 = z^2$ possui infinitas soluções representadas pelas ternas ordenadas (x, y, z) conhecidas como ternos pitagóricos.

A equação $x^n + y^n = z^n$ não possui soluções não nulas para para $n > 2$, e é conhecida como o Último Teorema de Fermat [9].

A equação $y^2 = x^3 + 17$ é válida, por exemplo, para os seguintes valores positivos: $(2, 5), (4, 9), (43, 282), (52, 375), \ldots$

A *Equação de Pell* é dada por $x^2 - ny^2 = 1$, em que n é um inteiro positivo que não seja um quadrado.

A equação $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$ é conhecida como a Conjectura de Erdos-Straus, que indaga se para todo $n > 1$, com $n \in N$, existe uma solução inteira positiva (x, y, z).

[9] Essa afirmação foi provada por *Andrew Wiles,* matemático britânico; professor da Universidade de Princeton, com a colaboração de *Richard Lawrence Taylor,* em 1994.

A equação $2^n - 7 = x^2$ é a equação de Ramanujan-Nagell.

As equações de *Fermat, Pell, Erdos-Straus e Ramanujan-Nagell* são classificadas como equações diofantinas não lineares [10].

Uma equação diofantina linear com duas incógnitas x_1 e x_2 é dada por $c_1x_1 + c_2x_2 = c$, em que c_1, c_2 e c são inteiros dados, sendo $c_1, c_2 \neq 0$. Todo par de inteiros (x_n, y_n) tais que a $c_1x_n + c_2y_n = c$ diz-se uma solução inteira ou apenas uma solução da equação $c_1x_1 + c_2x_2 = c$.

Consideremos, por exemplo, a equação diofantina linear com duas incógnitas, definida por $3x_1 + 6x_2 = 18$. Temos:

$$\begin{aligned} &3 \cdot 4 + 6 \cdot 1 = 18 \\ &3 \cdot (-6) + 6 \cdot 6 = 18 \\ &3 \cdot 10 + 6 \cdot (-2) = 18. \end{aligned} \tag{1.6}$$

Logo, os pares de inteiros $(4; 1)$, $(-6; 6)$, $(10; -2)$ são soluções da equação $3x_1 + 6x_2 = 18$.

Existem equações diofantinas lineares com duas incógnitas que não têm solução. Assim, por exemplo, a equação diofantina linear $2x_1 + 4x_2 = 13$, não tem solução, porque $2x_1 + 4x_2$ é um inteiro par para quaisquer que sejam os valores inteiros de x_1 e x_2, enquanto que 13 é um inteiro ímpar (observe-se que $2 = (2, 4)$ não divide 13). A partir de agora, vamos estudar as equações diofantinas lineares. Veremos alguns exemplos desse tipo especial de equação, para mais detalhes, ver (FONSECA, R. V. F.,). Serão chamadas equações diofantinas todas as equações polinomiais (não importando o número de incógnitas) com coeficientes inteiros, sempre que for tomado como conjunto solução das variáveis da equação o conjunto dos números inteiros. Visto a importância, existência de métodos de resolução e quantidade de problemas que se enquadram neste formato, tomaremos como foco do nosso estudo a compreensão e resolução das equações diofantinas lineares com duas, três ou n variáveis.

Considere a equação diofantina: $c_1x_1 + \ldots + c_nx_n = c$, com $c_1, \ldots, c_n, c$ inteiros. Uma solução desta equação é uma k-upla de inteiros $k_1, \ldots, k_n$ tal que $c_1k_1 + \ldots + c_nk_n = c$. Se uma equação diofantina tem solução, ela é dita solúvel.

Um importante resultado na resolução de equações diofantinas de duas variáveis, é o teorema abaixo:

A equação diofantina linear $c_1x_1 + c_2x_2 = c$ tem solução se, e somente se, d divide c, sendo $d = (c_1, c_2)$. Suponhamos que a equação $c_1x_1 + c_2x_2 = c$ tem uma solução, isto é, que existe um par de inteiros (x_n, y_n) tais que $c_1x_n + c_2y_n = c$. Por ser o $(c_1, c_2) = d$, existem inteiros r e s tais que $c_1 = dr$ e $c_2 = ds$, e temos $c = c_1x_0 + c_2y_0 =$

[10] São equações diofantinas não lineares todas as equações que possuem ao menos um termo com grau superior a 1.

$drx_0 + dsy_0 = d(rx_0 + sy_0)$, e como $rx_0 + sy_0$ é um inteiro, segue-se que d divide c. Reciprocamente, suponhamos que d divide c, isto é, que $c = dt$, em que t é um número inteiro. Por ser o $(c_1, c_2) = d$, existem inteiros x_0 e y_0 tais que $d = c_1x_0 + c_2y_0$. Isto implica que $c = dt = (c_1x_0 + c_2y_0)t = c_1(tx_0) + c_2(ty_0)$. Assim sendo, o par de inteiros, $x = tx_0 = \left(\frac{c}{d}\right) x_0$, e $y = ty_0 = \left(\frac{c}{d}\right) y_0$ é uma solução da equação $c_1x_1 + c_2x_2 = c$.

□

Apresentamos agora um teorema importante para resolução de equações da forma $c_1x_1 + c_2x_2 = c$.

Se d divide c, sendo $d = (c_1, c_2)$, e se o par de inteiros (x_0, y_0) é um solução particular da equação diofantina linear $c_1x_1 + c_2x_2 = c$, então todas as outras soluções desta equação são dadas pelas fórmulas:

$$x = x_0 + \left(\frac{c_2}{d}\right) t \text{ e } y = y_0 - \left(\frac{c_1}{d}\right) t, \text{ onde } t \text{ é um inteiro arbitrário.}$$

Suponhamos que o par de inteiros (x_0, y_0) é uma solução particular da equação $c_1x_1 + c_2x_2 = c$, e seja (x_1, y_1) uma outra solução qualquer desta equação. Então, temos que $c_1x_0 + c_2y_0 = c = c_1x_1 + c_2y_1$ e, portanto $c_1(x_1 - x_0) = c_2(y_1 - y_0)$. Por ser $(c_1, c_2) = d$, existem inteiros r e s tais que $c_1 = dr$ e $c_2 = ds$, com r e s primos entre si. Substituindo estes valores de c_1 e c_2 na igualdade anterior e cancelando o fator com d, obtemos: $r(x_1 - x_0) = s(y_0 - y_1)$. Assim sendo, $r|s(y_0 - y_1)$, e como o $(r, s) = 1$, segue-se que $r|\ y_0 - y_1$, isto é, $y_0 - y_1 = rt$ e $x_1 - x_0 = st$, em que t é um inteiro. Portanto, temos as fórmulas:

$$x_1 = x_0 + st = x_0 + \left(\frac{c_2}{d}\right) t \text{ e } y_1 = y_0 - rt = y_0 - \left(\frac{c_1}{d}\right) t.$$

Assim os valores de x_1 e y_1 satisfazem a equação $c_1x_1 + c_2x_2 = c$, qualquer que seja o inteiro t, pois temos:

$$c_1x_1+c_2y_1 = c_1\left[x_0 + \left(\frac{c_2}{d}\right) t\right]+c_2\left[y_0 - \left(\frac{c_1}{d}\right) t\right] = c_1x_0+c_2y_0+\left(\frac{c_1c_2}{d} - \frac{c_1c_2}{d}\right) t = c+0.t = c.$$

□

Como vemos, se $d = (c_1, c_2)$ divide c, então a equação diofantina linear $c_1x_1 + c_2x_2 = c$ admite um número infinito de soluções, uma para cada valor do inteiro arbitrário t.

Se o $(c_1, c_2) = 1$ e se (x_0, y_0) é uma solução particular da equação diofantina linear $c_1x_1 + c_2x_2 = c$, então todas as outras soluções são dadas pelas fórmulas $x = x_0 + c_2t$ e $y = y_0 - c_1t$, em que t é um inteiro arbitrário. Consideremos agora a equação da forma $c_1x_1 + c_2x_2 + c_3x_3 = c$, em que os c_i, para $i = 1, 2, 3$, são inteiros não nulos simultaneamente. De forma análoga ao que foi apresentado acima, sabemos que essa

equação admite soluções se, $d = (c_1, c_2, c_3)$ divide c. Usaremos este fato para construir uma solução particular para equação diofantina anterior.

Vimos, anteriormente, como calcular o máximo divisor comum de uma quantidade finita de números. Usaremos isto agora. Iniciamos por analisar $(c_1, c_2) = d_1$ e a partir deste, o $(d_1, c_3) = d$. Se $d_1 = (c_1, c_2)$, então existem $k_1, k_2 \in Z$ para os quais $c_1k_1 + c_2k_2 = d_1$. E como $d = (d_1, c_3)$, então existem $k, z_0 \in Z$ de maneira que $d = d_1k + c_3z_0$. Logo $d = (c_1k_1 + c_2k_2)k + c_3z_0 = c_1(k_1k) + c_2(k_2k) + c_3z_0$. Escrevendo $k_1k = x_0$ e $k_2k = y_0$ segue que $c_1x_0 + c_2y_0 + c_3z_0 = d$. Assim, se $c_1x + c_2y + c_3z = c$ admite uma solução e se $c = dq$, para algum $q \in Z$, então, $c_1(x_0q) + c_2(y_0q) + c_3(z_0q) = dq = c$, o que mostra que (x_0q, y_0q, z_0q) é uma solução particular para a equação diofantina linear $c_1x_1 + c_2x_2 + c_3x_3 = c$.

1.3.1 Equação Diofantina Linear com n Variáveis

Apresentamos nessa seção, um método que nos permitirá encontrar uma solução particular de uma equação diofantina com n variáveis, bem como todas as suas soluções.

De (NETO, A. C. M., a), temos que se $c_1, c_2, \ldots, c_n$ são inteiros não nulos, dizemos que um inteiro d é um divisor comum de $c_1, c_2, \ldots, c_n$ quando $d|c_1, d|c_2, \ldots, d|c_n$. Note que $c_1, c_2, \ldots, c_n$ sempre têm divisores comuns: 1, por exemplo. Ademais, como qualquer inteiro não nulo tem apenas um número finito de divisores, $c_1, c_2, \ldots, c_n$ têm apenas um número finito de divisores comuns. Assim, a definição a seguir tem sentido.

O máximo divisor comum dos inteiros não nulos $c_1, c_2, \ldots, c_n$, denotado por $(c_1, c_2, \ldots, c_n)$, é o maior dentre os divisores comuns de $c_1, c_2, \ldots, c_n$. Os inteiros $c_1, c_2, \ldots, c_n$ são primos entre si, ou relativamente primos, se $(c_1, c_2, \ldots, c_n) = 1$.

Para o teorema a seguir, que é uma generaliação do Teorema 1.2.2 creditado ao matemático francês Étienne Bézout, dado $n \in Z$, denote por $n \cdot Z$ o conjunto dos múltiplos inteiros de n, isto é,

$$n \cdot Z = \{n \cdot x;\ x \in Z\} = \{0,\ \pm n,\ \pm 2n,\ \pm 3n,\ \ldots\}.$$

(Bézout) Sejam $c_1, c_2, \ldots, c_n$ inteiros não nulos dados. Se

$$S = \left\{ \sum_{i=1}^{n} c_i x_i;\ x_i \in Z,\ \forall\ 1 \leqslant i \leqslant n \right\},$$

então $S = d \cdot Z$, onde $d = (c_1, c_2, \ldots, c_n)$. Em particular, existem números inteiros $u_1, u_2, \ldots, u_n$ tais que $(c_1, c_2, \ldots, c_n) = c_1u_1 + c_2u_2 + \ldots + c_nu_n$. É imediato que todo múltiplo de um elemento de S pertence a S. Por outro lado, como d divide $c_1x_1 + c_2x_2 + \ldots + c_nx_n$ para todos os $x_1, x_2, \ldots, x_n \in Z$, temos que $S \subset d \cdot Z$. Para estabelecer a inclusão contrária, note primeiro que S contém inteiros positivos. De fato, escolhendo $x_1 =$

$c_1,$ e $x_2 = \ldots = x_n = 0$, por exemplo, concluímos que $(c^2)_1 = c_1x_1 + c_2x_2 + \ldots + c_nx_n \in S$. Como S contém inteiros positivos, existe um menor inteiro positivo $d^{'}$ em S. Se mostrarmos que $d^{'} = d$, seguirá que $d \in S$ e nossa observação inicial garantirá que $d \cdot Z \subset S$. Afirmamos, inicialmente, que $d^{'}|c_1, c_2, \ldots, c_n$. De fato, como $d^{'} \in S$, existem $u_1, u_2, \ldots, u_n \in Z$ tais que $d^{'} = c_1u_1 + c_2u_2 + \ldots + c_nu_n$. Agora, seja $c_1 = d^{'}q + r$, com $q, r \in Z$ e $0 \leqslant r < d^{'}$. Então

$$\begin{aligned} r &= c_1 - d^{'}q \\ &= c_1 - (c_1u_1 + c_2u_2 + \ldots + c_nu_n)q \\ &= c_1(1 - u_1q) + c_2(-u_2q) + \ldots + c_n(-u_nq), \end{aligned} \tag{1.7}$$

de sorte que $r \in S$. Se $0 < r < d^{'}$, teríamos uma contradição ao fato de ser $d^{'}$ o menor inteiro positivo pertencente a S. Logo, $r = 0$ e $d^{'}|c_1$. Analogamente, $d^{'}|c_2, \ldots, c_n$.

Para terminar, como $d^{'}$ é um divisor comum de $c_1, c_2, \ldots, c_n$, para mostrarmos que $d^{'} = d$ basta que $d^{'} \geqslant d$. Mas, se $c_1 = dq_1, c_2 = dq_2, \ldots, c_n = dq_n$, com $q_1, q_2, \ldots, q_n \in Z$, então

$$\begin{aligned} d^{'} &= c_1u_1 + c_2u_2 + \ldots + c_nu_n \\ &= dq_1u_1 + dq_2u_2 + \ldots + dq_nu_n \\ &= d\left(q_1u_1 + q_2u_2 + \ldots + q_nu_n\right), \end{aligned} \tag{1.8}$$

ou seja, $0 < d|d^{'}$. Logo, $d \leqslant d^{'}$.

□

Para tal, consideremos agora a equação $c_1x_1 + c_2x_2 + c_3x_3 + \ldots + c_{n-1}x_{n-1} + c_nx_n = c$, onde cada c_i, com $i = 1, 2, 3, \ldots, n$, sejam inteiros não nulos simultaneamente. Sabemos que essa equação admite soluções se, $d = (c_1, c_2, c_3, \ldots, c_n)$ divide c. Se $d_1 = (c_1, c_2)$, então existem k_1 e $k_2 \in Z$ para os quais $c_1k_1 + c_2k_2 = d_1$. E como $d_2 = (d_1, c_3)$, então existem $k_3, k_4 \in Z$ de maneira que $d_2 = d_1k_3 + c_3k_4$. Procedendo de forma análoga $n - 1$ vezes, chegaremos em $d = (d_{(n-1)}, c_n)$, então, $c_1(x_{(1)_0}q) + c_2(x_{(2)_0}q) + c_3(x_{(3)_0}q) + \ldots + c_{n-1}(x_{(n-1)_0}q) + c_n(x_{(n)_0}q) = dq = c$ para algum $q \in Z$, o que mostra que $\left(x_{(1)_0}q, x_{(2)_0}q, x_{(3)_0}q, \ldots, x_{(n-1)_0}q, x_{(n)_0}q\right)$ é uma de suas soluções particulares. No próximo capítulo, investigaremos como podemos encontrar soluções de tipos especiais de equações diofantinas com n variáveis.

2 Um método para resolver Equações Diofantinas Lineares de n variáveis

Neste capítulo, apresentaremos um método para resolver um tipo especial de equação diofantina linear com n variáveis. Segundo (BREZINSKI, C.,), o século XIX foi marcado por contribuições valiosas no estudo, por exemplo, de frações contínuas como ferramenta de resolução de problemas na área de Teoria dos Números. Neste século deram valiosas contribuições matemáticos como Jacobi, Perron, Hermite, Gauss, Cauchy e Stieljes.

Dentre esses, tomaremos por referência estudos de dois matemáticos alemães, Oskar Perron e Carl Gustav Jakob Jacobi. Mais detalhes sobre o tema podem ser vistos com mais detalhes em (BERNSTEIN, L.,), (BERNSTEIN, l.,) e (OSKAR, P.,).

2.1 Alguns aspectos inicias quanto a equação

No capítulo anterior mostramos métodos para resolver equações com duas variáveis, agora mostraremos como resolver um tipo particular de equação diofantina. A solução da Equação Diofantina Linear com n variáveis da forma

$$c_1x_1 + c_2x_2 + \ldots + c_nx_n = c,$$

com $n \geqslant 2; c_1, c_2, \ldots, c_n, c$ inteiros, é um problema que pode ser avaliado sob várias abordagens; isso depende das características dos coeficientes da equação, por exemplo. Uma bordagem voltada para soluções computacionais será objeto do próximo capítulo. Para $n = 2$, ou seja, para uma equação com duas variáveis, vimos que é possível obter soluções pelo Teorema 1.3. A questão de nosso estudo é como encontrar a solução para equações diofantinas lineares com mais de duas variáveis. Ao longo do capítulo, formalizaremos um método para buscar soluções para uma equação diofantina linear nos caso em que $n > 2$ com a condição $x_i \neq 0$ com $i = 1, \ldots, n$ com base em uma modificação do algoritmo de Jacobi-Perron, que será mostrado ao longo do texto; onde veremos que, se uma equação for consistente, ou seja, se tiver solução, esse método nos levará à uma solução. Com alguns exemplos numéricos, apresentaremos a teoria em torno do problema.

2.2 Uma equação diofantina linear padrão

Dada uma equação diofantina linear de n variáveis da forma

$$c_1x_1 + c_2x_2 + \ldots + c_nx_n = 1, \text{ com } n > 2 \tag{2.1}$$

chamaremos de *equação diofantina linear padrão de grau n* ou apenas *equação padrão de grau n*, se verificadas as seguintes condições em relação aos seus coeficientes:

a. c_i é um número natural para $i = 1, \ldots, n$;
b. $1 < c_1 < c_2 < \ldots < c_n$;
c. $(c_1, c_2, \ldots, c_n) = 1$, ou seja, c_i são primos entre si,
d. $c_i c_{i+j};\ i, j \geqslant 1,\ i + j \leqslant n$;
e. $\left(c_{k_1}, c_{k_2}, \ldots, c_{k_{n-1}}\right) = d > 1; k_i, k_j = 1, \ldots, n; k_i \neq k_j;$ com $i, j = 1, \ldots, n-1.$

(2.2)

Uma equação diofantina linear com n variáveis e coeficientes inteiros

$$a_1 y_1 + a_2 y_2 + \ldots + a_m y_m = A,\ m > 1;\ a_i \neq 0;\ i = 1, \ldots, m \tag{2.3}$$

será dita *trivial* se

$$a_i = 1 \text{ para pelo menos um } i;$$

caso contrário será chamada *não trivial*. Isso faz-se necessário, pois desse modo teremos a garantia de que a_i divide todos os termos, visto que, em valor absoluto, temos $|a_i| = 1$. Logo, as soluções serão dadas por

$$y_1, y_2, \ldots, y_{i-1}, y_{i+1}, \ldots, y_m \text{ quaisquer inteiros, } 1 < i < m;$$

$$y_i = a_i \left(A - a_1 y_1 - a_2 y_2 - \ldots - a_{i-1} y_{i-1} - a_{i+1} y_{i+1} - \ldots - a_m y_m\right);$$

e semelhante para $i = 1$ ou $i = m$. Suponha que a equação (2.3) seja não trivial; então será dita *reduzida*, se

$$(a_1, a_2, \ldots, a_m, A) = 1$$

e *não reduzida*, se

$$(a_1, a_2, \ldots, a_m, A) = d > 1.$$

Caso a equação seja não reduzida, podemos reduzir os coeficientes $a_1, \cdots, a_m, A$ na equação (2.3) dividindo por d. E observada a condição $a_i \neq 0$, por um resultado análogo ao Teorema 1.3 temos que

$$(a_1, a_2, \ldots, a_m) \,|A, \tag{2.4}$$

caso contrário, não possui solução.

Enunciamos agora um importante resultado que garante a transformação de equações não triviais e solúveis em uma equação padrão, objeto de estudo desse capítulo.

Se uma equação diofantina linear da forma (2.3) é solúvel, reduzida e não trivial, então ela pode ser tranformada em uma equação padrão. Suponhamos que uma

equação diofantina linear da forma (2.3) seja solúvel, reduzida e não trivial. Então é claro que

$$(a_1, a_2, \ldots, a_m, A) = 1;\ |a_i| > 1,\ i = 1, \ldots, m. \tag{2.5}$$

Substituindo em (2.3) a seguinte mudança de coordenadas

$$y_i = Az_i,\ i = 1, \ldots, m$$

obtemos a seguinte equação

$$a_1z_1 + a_2z_2 + \ldots + a_mz_m = 1. \tag{2.6}$$

Sendo (2.3) solucionável, segue que $(a_1, a_2, \ldots, a_m)\,|A$. Além disso, $(a_1, a_2, \ldots, a_m)$ é um divisor dele mesmo. Assim, por (2.5) concluímos que

$$(a_1, a_2, \ldots, a_m) = 1.$$

Vamos denotar

$$\begin{aligned} z_{k_i} &= u_{k_i},\ \text{se}\, b_{k_i} = a_{k_i} > 0, \\ z_{k_i} &= -u_{k_i},\ \text{se}\, b_{k_i} = -a_{k_i} > 0,\ \text{com},\ k_i = 1, \ldots, m. \end{aligned}$$

Pela mudança de coordenadas acima, a equação (2.6) assume a forma

$$b_1u_1 + b_2u_2 + \ldots + b_mu_m = 1\ \text{com}\ (b_1, b_2, \ldots, b_m) = 1. \tag{2.7}$$

Assumamos, sem perda de generalidade, que

$$1 < b_1 \leqslant b_2 \leqslant b_3 \leqslant \ldots \leqslant b_m.$$

Seja b_i o primeiro coeficiente na sequência acima tal que

$$b_i | b_{k_s},\ k_s > i,\ s = 1, \ldots, m-n;\ m-n < m-i;\ i+1 \leqslant k_s \leqslant m. \tag{2.8}$$

Isto significa que b_i é o primeiro termo a dividir algum coeficiente maior que ele. Observe que isto não implica que ele divide todos os termos maiores do que ele. Fazendo,

$$b_{k_s} = t_sb_i,\ s = 1, \ldots, m-n,$$

vemos que

$$u_i + t_1u_{k_1} + t_2u_{k_2} + \ldots + t_{m-n}u_{k_{m-n}} = v_i. \tag{2.9}$$

Substituindo os u_i acima na equação (2.7) e fazendo as manipulações adequadas obtemos a equação

$$b_1u_1 + b_2u_2 + \ldots + b_{i-1}u_{i-1} + b_iv_i + b_{r_1}u_{r_1} + \ldots + b_{r_{n-i}}u_{r_{n-i}} = 1,$$

em que os coeficientes, b_i satisfazem

$$b_i b_{r_1}, b_{r_2}, \ldots, b_{r_{n-i}}; i+1 \leqslant r_q \leqslant m,\ q = 1, \ldots, n-i.$$

Afirmamos que

$$(b_1, b_2, \ldots, b_{i-1}, b_i, b_{r_1}, b_{r_2}, \ldots, b_{r_{n-i}}) = 1.$$

De fato, suponhamos que

$$(b_1, b_2, \ldots, b_{i-1}, b_i, b_{r_1}, b_{r_2}, \ldots, b_{r_{n-i}}) = d > 1.$$

Pelas condições assumidas em (2.8), segue que

$$(b_1, b_2, \ldots, b_i, b_{i+1}, \ldots, b_m) =$$

$$(b_1, b_2, \ldots, b_{i-1}, b_i, b_{k_1}, \ldots, b_{k_{m-n}}, b_{r_1}, \ldots, b_{r_{n-i}}) \geqslant$$

$$(b_1, b_2, \ldots, b_{i-1}, b_i, b_{r_1}, b_{r_2}, \ldots b_{r_{n-i}}) = d > 1,$$

o qual contradiz a condição em (2.7). Se existir b_{r_q} tal que $b_{r_q} | b_{r_p}$, com $p > q$ esse processo é repetido como antes. Caso contrário, usando a notação

$$\begin{aligned} &b_j = h_j,\ j = 1, \ldots, i; \\ &u_j = v_j,\ j = 1, \ldots, i-1; \\ &b_{r_j} = h_{i+j}; \\ &u_{r_j} = v_{i+j},\ j = 1, \ldots, n-i, \end{aligned}$$

obtemos a seguinte equação,

$$h_1 v_1 + h_2 v_2 + \ldots + h_n v_n = 1, \tag{2.10}$$

a qual satisfaz as condições

$$1 < h_1 < h_2 < \ldots < h_n;\ \text{com}\,(h_1, \ldots, h_n) = 1,\ h_i h_j;\ j > i.$$

Por (2.9), notamos que os valores de $u_i, u_{k_1}, u_{k_2}, \ldots, u_{k_{m-n}}$ na equação acima são obtidos dos de v_i em (2.10) da seguinte maneira

$$u_{k_1}, \ldots, u_{k_{m-n}} \text{ quaisquer números inteiros};\ u_i = v_i - t_1 u_{k_1} - \ldots - t_{m-n} u_{k_{m-n}}.$$

Se algum h_i com $i = 1, \ldots, n$ em (2.10) não satisfaz a condição (e) de (2.2), vamos escolher n números primos diferentes p_i tais que

$$p_i h_1 h_2 \ldots h_n,\ i = 1, \ldots, n;\ p_1 > p_2 > \ldots > p_n. \tag{2.11}$$

Usemos as seguintes notações,

$$p_1 p_2 \ldots p_n = P;\ v_i = (p_i)^{-1} P x_i;\ c_i = (p_i)^{-1} P h_i,\ i = 1, \ldots, n.$$

Pelas notações acima a equação (2.10) se transforma numa equação (2.1):

$$c_1x_1 + c_2x_2 + \ldots + c_nx_n = 1,$$

Vamos agora verificar que a equação acima satisfaz as condições (2.2). De

$$c_1 = h_1(p_i)^{-1}P = h_1p_2p_3\ldots p_m > h_1,$$

obtemos,

$$c_1 > 1.$$

Além disso, pela condição em (2.11), para $i \geqslant 1$, obtemos que

$$c_i = h_i(p_i)^{-1}P < h_{i+1}(p_i)^{-1}P < h_{i+1}(p_{i+1})^{-1}P = c_{i+1},\ c_i < c_{i+1}\ i = 1, 2, \ldots, n-1.$$

Mas,

$$\left((p_1)^{-1}P, (p_2)^{-1}P,\ \ldots, (p_n)^{-1}P\right) = 1,\ \text{e}\ (h_1, h_2, \ldots, h_n) = 1,$$

e como $p_ih_1h_2\ldots h_n$, obtemos, que

$$\left(h_1(p_1)^{-1}P, h_2(p_2)^{-1}P, \ldots,\ h_n(p_n)^{-1}P\right) = 1$$

de modo que,

$$(c_1, c_2, \ldots, c_n) = 1. \tag{2.12}$$

Por fim, afirmamos que os números c_i com $i = 1, \ldots, n$ satisfazem a condição (e) em (2.2). Com efeito, provaremos para uma $(n-1) - upla$ de c_i em particular, pois o caso geral para qualquer $(n-1) - upla$, se prova de maneira análoga. Do exposto acima,

$$(c_1, c_2, \ldots, c_{n-1}) = \left(h_1(p_1)^{-1}P, h_2(p_2)^{-1}P, \ldots, h_{n-1}(p_{n-1})^{-1}P\right) =$$

$$(h_1p_2p_3\ldots p_n, h_2p_1p_3\ldots p_n, \ldots, h_{n-1}p_1\ldots p_{n-2}p_n) \geqslant p_n > 1.$$

Usamos na primeira igualdade que

$$\begin{aligned}
c_1 &= (p_1)^{-1}Ph_1 = (p_1)^{-1}(p_1p_2\ldots p_n)h_1 = h_1p_2\ldots p_n,\\
c_2 &= (p_2)^{-1}Ph_2 = (p_2)^{-1}(p_1p_2\ldots p_n)h_2 = h_2p_1\ldots p_n,\\
&\vdots\\
c_n &= (p_n)^{-1}Ph_n = (p_n)^{-1}(p_1p_2\ldots p_n)h_n = h_np_1p_2\ldots p_{n-1}.
\end{aligned}$$

Dos itens *c.* e *d.* de (2.2) e do desenvolvimento acima, fazendo as devidas substituições temos que,

$$\left(c_{k_1}, c_{k_2}, \ldots, c_{k_{n-1}}\right) = p_{k_n} > 1,\ k_i \neq k_j \text{ para } i \neq j.$$

□

As equações diofantinas lineares com n incógnitas que satisfazem as condições *a.*, *b.*, *c.* e *d.* de (2.2) serão chamadas de *equação padrão suprimida de grau n.*

Seja $h_1v_1 + h_2v_2 + \ldots + h_nv_n = 1$ uma equação padrão suprimida de grau n. Vimos que todas as equações diofantinas reduzidas e não triviais podem ser transformadas em equação padrão suprimida, sendo $n > 2$.

Uma $n - upla$ de números inteiros $(x_1, x_2, \ldots, x_n)$ que satisfaz uma equação padrão suprimida

$$h_1x_1 + h_2x_2 + \ldots + h_nx_n = 1; \tag{2.13}$$

é dita *vetor solução padrão*, se verificarmos que $x_i \neq 0$ para todo $i = 1, \ldots, n$. O objetivo aqui é encontrar uma solução para uma equação padrão suprimida. Observado que a equação padrão suprimida não cumpre a condição (e) de (2.2), ou seja, os coeficientes da equação não são primos entre si, deve-se buscar uma $(n-1) - upla$ de números entre os $h_1, \ldots, h_n$ que sejam relativamente primos. Assumamos então que

$$(h_1, h_2, \ldots, h_{n-1}) = 1, \tag{2.14}$$

e que $(x_1, x_2, \ldots, x_{n-1})$ é um vetor solução de

$$h_1v_1 + h_2v_2 + \ldots + h_{n-1}v_{n-1} = 1.$$

Isso implica que $(x_1, x_2, \ldots, x_{n-1}, 0)$ é um vetor solução de (2.13), mas não é um vetor solução padrão. Um vetor solução padrão seria dada por

$$(x_1, x_2, \ldots, x_{n-1} - th_n, th_{n-1}), \ t \in Z, \ x_{n-1} \neq th_n.$$

De fato, substituindo o vetor acima em (2.13) vemos que

$$h_1x_1 + h_2x_2 + \ldots + h_{n-1}x_{n-1} - h_{n-1}th_n + h_n(th_{n-1}) = h_1x_1 + h_2x_2 + \ldots + h_{n-1}x_{n-1} = 1$$

Deste modo, o problema de uma equação padrão suprimida de grau n, a qual não é uma equação padrão de grau n, é reduzido ao caso de encontrarmos um vetor solução padrão de uma equação padrão suprimida de grau $n-1$.

Uma equação padrão de grau n possui apenas vetores de solução padrão.

Consideremos um vetor solução $(x_1, x_2, \ldots, x_k, 0, 0, \ldots, 0)$ de uma equação padrão de grau n tais que $x_i \neq 0, \ i = 1, \ldots, k$. De fato, suponhamos que $k = 1$. Então trabalhamos com a solução $(x_1, 0, \ldots, 0)$. Substituindo isso na equação (2.13) obtemos $h_1x_1 = 1$. Isso implica que $h_1 = 1$ ou $h_1 = -1$. Em ambos os casos h_i contradiz com o item $b)$ de (2.2). Assumamos que $k \leqslant n-1$. A disposição dos componentes do vetor solução pode ser assumida sem perda de generalidade. Então

$$c_1x_1 + c_2x_2 + \ldots + c_kx_k = 1. \tag{2.15}$$

Sendo

$$(c_1, c_2, \ldots, c_k, c_{k+1}, \ldots, c_{n-1}) = p_n,$$

segue que,

$$(c_1, c_2, \ldots, c_k) \geqslant p_n > 1,$$

o qual contradiz (2.15), pois os seus coeficientes devem satisfazer a condição (c) de (2.2), o que não acontece. Aí está a contradição.

Novamente, seja

$$h_1v_1 + h_2v_2 + \ldots + h_nv_n = 1$$

uma equação padrão suprimida de grau n e

$$h_1v_1 + h_2v_2 + \ldots + h_nv_n = 0 \tag{2.16}$$

sua parte homogênea. No que segue, usaremos a seguinte notação,

$$D(h_1, \ldots, h_n) = \begin{vmatrix} th_1 & v_{1,1} & v_{1,2} & \ldots & v_{1,n-2} & h_1 \\ th_2 & v_{2,1} & v_{2,2} & \ldots & v_{2,n-2} & h_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ th_n & v_{n,1} & v_{n,2} & \ldots & v_{n,n-2} & h_n \end{vmatrix}, \quad \begin{array}{l} t, v_{i,j} \text{ algum inteiro,} \\ i = 1, \ldots, n;\ j = 1, \ldots, n-2. \end{array}$$

Também denotamos por $H_{k,n}$ o cofator algébrico do elemento $a_{k,n}$. Observemos que para qualquer $t, v_{i,j}$ inteiros com $i = 1, \ldots, n$ e $j = 1, \ldots, n-2$, tem-se

$$\begin{vmatrix} th_1 & v_{1,1} & v_{1,2} & \ldots & v_{1,n-2} & h_1 \\ th_2 & v_{2,1} & v_{2,2} & \ldots & v_{2,n-2} & h_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ th_n & v_{n,1} & v_{n,2} & \ldots & v_{n,n-2} & h_n \end{vmatrix} = t \cdot \begin{vmatrix} h_1 & v_{1,1} & v_{1,2} & \ldots & v_{1,n-2} & h_1 \\ h_2 & v_{2,1} & v_{2,2} & \ldots & v_{2,n-2} & h_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ h_n & v_{n,1} & v_{n,2} & \ldots & v_{n,n-2} & h_n \end{vmatrix} = t \cdot 0.$$

Portanto, uma simples conta mostra que

$$D(h_1, \ldots, h_n) = h_1H_{1,n} + h_2H_{2,n} + \ldots + h_nH_{n,n} = 0. \tag{2.17}$$

Terminamos esta seção com a demonstração da solução geral de uma equação padrão suprimida. Seja $(x_1, x_2, \ldots, x_n)$ um vetor solução de uma equação padrão suprimida de grau n e seja $(H_{1,n}, H_{2,n}, \ldots, H_{n,n})$ um vetor solução de sua parte homogênea. Então um vetor $(x_1 + H_{1,n}, x_2 + H_{n,2}, \ldots, x_n + H_{n,n})$ é solução da equação padrão suprimida dada. Inicialmente notemos de (2.13) que o vetor $(x_1, x_2, \ldots, x_n)$ é solução da equação $h_1x_1 + h_2x_2 + \ldots + h_nx_n = 1$. Observemos ainda que de (2.17) temos que o vetor $(H_{1,n}, H_{2,n}, \ldots, H_{n,n})$ é solução da equação $h_1H_{1,n} + h_2H_{2,n} + \ldots + h_nH_{n,n} = 0$. Adicionando as equações em (2.13) e (2.17), segue que

$$h_1x_1 + h_1H_{1,n} + h_2x_2 + h_2H_{2,n} + \ldots + h_nx_nh_nH_{n,n} = 1$$

$$h_1\left(x_1 + H_{1,n}\right) + h_2\left(x_2 + H_{2,n}\right) + \ldots + h_n\left(x_n + H_{n,n}\right) = 1$$

Concluímos assim que o vetor $(x_1 + H_{1,n}, x_2 + H_{n,2}, \ldots, x_n + H_{n,n})$ é solução da equação padrão suprimida.

2.3 Um algoritmo modificado de Jacobi-Perron

Tomando como referência estudos de Jacobi e Perron, modificaremos um algoritmo que leva o nome dos dois matemáticos. Com o intuito de encontrarmos um vetor solução padrão de uma equação padrão suprimida de grau n, apresentaremos uma modificação do algoritmo de Jacobi-Perron, conforme descreveremos a seguir.

Denotaremos por V_{n-1} o espaço vetorial das $(n-1) - uplas$ dos números reais ordenados $(a_1, a_2, \ldots, a_{n-1})$, com $n = 2, 3, \ldots$.

Seja,

$$a^{(0)} = \left(a_1{}^{(0)}, a_2{}^{(0)}, \ldots, a_{n-1}{}^{(0)}\right)$$

um vetor em V_{n-1}. Tomamos também

$$b^{(v)} = \left(b_1{}^{(v)}, b_2{}^{(v)}, \ldots, b_{n-1}{}^{(v)}\right)$$

uma sequência de vetores em V_{n-1}, que são dados arbitrariamente ou derivados de $a^{(0)}$ por uma certa transformação de V_{n-1}. Introduziremos agora a seguinte transformação,

$$Ta^{(v)} = a^{(v+1)} = \frac{1}{a_1{}^{(v)} - b_1{}^{(v)}} \left(a_2{}^{(v)} - b_2{}^{(v)}, \ldots, a_{n-1}{}^{(v)} - b_{n-1}{}^{(v)}, 1\right), \tag{2.18}$$

em que $a_1{}^{(v)} \neq b_1{}^{(v)}$, com $v = 0, 1, \ldots$.

Definiremos os números reais $A_i{}^{(v)}$ pelas fórmulas de recursão abaixo,

$$\begin{aligned} &A_i{}^{(i)} = 1;\ A_i{}^{(v)} = 0;\ i, v = 0, 1, \ldots, n-1;\ i \neq v, \\ &A_i{}^{(v+n)} = A_i{}^{(v)} + \sum_{j=1}^{n-1} b_j{}^{(v)} A_i{}^{(v+j)},\ i = 0, 1, \ldots, n-1;\ v = 0, 1, \ldots \end{aligned} \tag{2.19}$$

então, como foi enunciado por Perron, temos a seguinte fórmula:,

$$D_v = \begin{vmatrix} A_0{}^{(v)} & A_0{}^{(v+1)} & \ldots & A_0{}^{(v+n-1)} \\ A_1{}^{(v)} & A_1{}^{(v+1)} & \ldots & A_1{}^{(v+n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n-1}{}^{(v)} & A_{n-1}{}^{(v+1)} & \ldots & A_{n-1}{}^{(v+n-1)} \end{vmatrix} = (-1)^{v(n-1)} \ ;\ \text{com } v = 0, 1, \ldots. \tag{2.20}$$

Provaremos por indução em v que $D_v = (-1)^{v(n-1)}$, com $v = 0, 1, \ldots$. De (2.19), e fazendo $v = 0$, temos que,

$$D_0 = \begin{vmatrix} {A_0}^{(0)} & {A_0}^{(1)} & \ldots & {A_0}^{(n-1)} \\ {A_1}^{(0)} & {A_1}^{(1)} & \ldots & {A_1}^{(n-1)} \\ \ldots & \ldots & \ldots & \ldots \\ {A_{n-1}}^{(0)} & {A_{n-1}}^{(1)} & \ldots & {A_{n-1}}^{(n-1)} \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \end{vmatrix} = 1 = (-1)^{0(n-1)}.$$

Suponhamos que $D_v = (-1)^{v(n-1)}$. De (2.20) temos para $v+1$ que

$$D_{v+1} = \begin{vmatrix} {A_0}^{(v+1)} & {A_0}^{(v+2)} & \ldots & {A_0}^{(v+n)} \\ {A_1}^{(v+1)} & {A_1}^{(v+2)} & \ldots & {A_1}^{(v+n)} \\ \ldots & \ldots & \ldots & \ldots \\ {A_{n-1}}^{(v+1)} & {A_{n-1}}^{(v+2)} & \ldots & {A_{n-1}}^{(v+n)} \end{vmatrix}$$

$$= \begin{vmatrix} {A_0}^{(v+1)} & {A_0}^{(v+2)} & \ldots & {A_0}^{(v)} + \sum_{j=1}^{n-1} b_j{}^{(v)} {A_0}^{(v+j)} \\ {A_1}^{(v+1)} & {A_1}^{(v+2)} & \ldots & {A_1}^{(v)} + \sum_{j=1}^{n-1} b_j{}^{(v)} {A_1}^{(v+j)} \\ \ldots & \ldots & \ldots & \ldots \\ {A_{n-1}}^{(v+1)} & {A_{n-1}}^{(v+2)} & \ldots & {A_{n-1}}^{(v)} + \sum_{j=1}^{n-1} b_j{}^{(v)} {A_{n-1}}^{(v+j)} \end{vmatrix}$$

$$= \begin{vmatrix} {A_0}^{(v+1)} & {A_0}^{(v+2)} & \ldots & {A_0}^{(v)} \\ {A_1}^{(v+1)} & {A_1}^{(v+2)} & \ldots & {A_1}^{(v)} \\ \ldots & \ldots & \ldots & \ldots \\ {A_{n-1}}^{(v+1)} & {A_{n-1}}^{(v+2)} & \ldots & {A_{n-1}}^{(v)} \end{vmatrix} + \sum_{j=1}^{n-1} \begin{vmatrix} {A_0}^{(v+1)} & \ldots & {A_0}^{(v)} + b_j{}^{(v)} {A_0}^{(v+j)} \\ \ldots & \ldots & \ldots \\ {A_{n-1}}^{(v+1)} & \ldots & {A_{n-1}}^{(v)} + b_j{}^{(v)} {A_{n-1}}^{(v+j)} \end{vmatrix}$$

$$= \begin{vmatrix} {A_0}^{(v+1)} & {A_0}^{(v+2)} & \ldots & {A_0}^{(v)} \\ {A_1}^{(v+1)} & {A_1}^{(v+2)} & \ldots & {A_1}^{(v)} \\ \ldots & \ldots & \ldots & \ldots \\ {A_{n-1}}^{(v+1)} & {A_{n-1}}^{(v+2)} & \ldots & {A_{n-1}}^{(v)} \end{vmatrix} + \sum_{j=1}^{n-1} b_j{}^{(v)} \begin{vmatrix} {A_0}^{(v+1)} & \ldots & {A_0}^{(v+j)} \\ \ldots & \ldots & \ldots \\ {A_{n-1}}^{(v+1)} & \ldots & {A_{n-1}}^{(v+j)} \end{vmatrix}$$

$$= (-1)^{(n-1)} \begin{vmatrix} {A_0}^{(v)} & {A_0}^{(v+1)} & \ldots & {A_0}^{(v+n-1)} \\ \ldots & \ldots & \ldots & \ldots \\ {A_{n-1}}^{(v)} & {A_{n-1}}^{(v+1)} & \ldots & {A_{n-1}}^{(v+n-1)} \end{vmatrix}$$

$$= (-1)^{(n-1)} \cdot D_v = (-1)^{(n-1)} \cdot (-1)^{v(n-1)} = (-1)^{(v+1)(n-1)},$$

onde usamos na quinta igualdade o fato dos determinantes terem duas colunas iguais.

Outra fórmula enunciada por Perron foi

$$a_i{}^{(0)} = \frac{A_i{}^{(v)} + \sum_{j=1}^{n-1} a_j{}^{(v)} A_i{}^{(v+j)}}{A_0{}^{(v)} + \sum_{j=1}^{n-1} a_j{}^{(v)} A_0{}^{(v+j)}};\ \text{com } i = 1, \ldots, n-1;\ v = 0, 1, \ldots. \tag{2.21}$$

Ainda por indução provaremos (2.21). Pela segunda condição em (2.19), segue que

$$\frac{A_i{}^{(0)} + \sum_{j=1}^{i-1} a_j{}^{(v)} A_i{}^{(j)} + a_i{}^{(0)} A_i{}^{(i)} + \sum_{j=i+1}^{n-1} a_j{}^{(v)} A_i{}^{(j)}}{A_0{}^{(0)} + \sum_{j=1}^{n-1} a_j{}^{(v)} A_0{}^{(j)}} = \frac{0 + 0 + a_i{}^{(0)} + 0}{1 + 0} = \frac{a_i{}^{(0)}}{1} = a_i{}^{(0)}.$$

O que mostra que (2.21) é verdadeira para $v = t$. Vamos mostrar que a fórmula é válida para $v = t + 1$. De fato,

$$\frac{a_{n-1}{}^{(t+1)} \left(A_i{}^{(t)} + \sum_{j=1}^{n-1} b_j{}^{(t)} A_i{}^{(t+j)} \right) + \left(A_i{}^{(t+1)} + \sum_{j=1}^{n-2} a_j{}^{(t+1)} A_i{}^{(t+1+j)} \right)}{a_{n-1}{}^{(t+1)} \left(A_0{}^{(t)} + \sum_{j=1}^{n-1} b_j{}^{(t)} A_0{}^{(t+j)} \right) + \left(A_0{}^{(t+1)} + \sum_{j=1}^{n-2} a_j{}^{(t+1)} A_0{}^{(t+1+j)} \right)}$$

$$= \frac{a_{n-1}{}^{(t+1)} A_i{}^{(t+n)} + \left(A_i{}^{(t+1)} + \sum_{j=1}^{n-2} a_j{}^{(t+1)} A_i{}^{(t+1+j)} \right)}{a_{n-1}{}^{(t+1)} A_0{}^{(t+n)} + \left(A_0{}^{(t+1)} + \sum_{j=1}^{n-2} a_j{}^{(t+1)} A_0{}^{(t+1+j)} \right)}$$

$$\frac{A_i{}^{(t+1)} + \sum_{i=1}^{n-1} A_i{}^{(t+1+j)}}{A_0{}^{(t+1)} + \sum_{i=1}^{n-1} A_0{}^{(t+1+j)}} = a_i{}^{(0)}.$$

Temos que, D_v é o determinante da matriz de transformação de $Ta^{(v)}$. Podemos reescrever essa fórmula da seguinte maneira,

$$\begin{vmatrix} 1 & A_0{}^{(v+1)} & \ldots & A_0{}^{(v+n-1)} \\ a_1{}^{(0)} & A_1{}^{(v+1)} & \ldots & A_1{}^{(v+n-1)} \\ a_2{}^{(0)} & A_2{}^{(v+1)} & \ldots & A_2{}^{(v+n-1)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n-1}{}^{(0)} & A_{n-1}{}^{(v+1)} & \ldots & A_{n-1}{}^{(v+n-1)} \end{vmatrix} = \frac{(-1)^{v(n-1)}}{A_0{}^{(v)} + \sum_{j=1}^{n-1} a_j{}^{(v)} A_0{}^{(v+j)}}\ ;\ v = 0, \ldots. \tag{2.22}$$

Vamos provar que a equação (2.22) é verdadeira.Por (2.20), segue que

$$\frac{(-1)^{v(n-1)}}{A_0{}^{(v)} + \sum_{j=1}^{n-1} a_j{}^{(v)} A_0{}^{(v+j)}} = \frac{D_v}{A_0{}^{(v)} + \sum_{j=1}^{n-1} a_j{}^{(0)} A_0{}^{(v+j)}}$$

$$= \frac{1}{A_0{}^{(v)} + \sum_{j=1}^{n-1} a_j{}^{(v)} A_0{}^{(v+j)}} \begin{vmatrix} A_0{}^{(v)} + \sum_{j=1}^{n-1} a_j{}^{(v)} A_0{}^{(v+j)} & A_0{}^{(v+1)} & \ldots & A_0{}^{(v+n-1)} \\ \ldots & \ldots & \ldots & \ldots \\ A_{n-1}{}^{(v)} + \sum_{j=1}^{n-1} a_j{}^{(v)} A_{n-1}{}^{(v+j)} & A_{n-1}{}^{(v+1)} & \ldots & A_{n-1}{}^{(v+n-1)} \end{vmatrix}.$$

Note que, ao multiplicarmos cada elemento da primeira coluna desse determinante pela fração antes deste, obtemos como primeira coluna os elementos,

$$\begin{matrix} 1 \\ {a_1}^{(0)} \\ \vdots \\ {a_{n-1}}^{(0)} \end{matrix}, \tag{2.23}$$

o que prova a veracidade da igualdade. Segundo (OSKAR, P.,), as equações (2.20), (2.21) e (2.22) aqui demonstradas foram apresentadas, há época, sem demontração. Sabe-se também que os vetores $b^{(v)}$ não foram arbitrariamente escolhidos, e sim oriundos dos vetores $a^{(v)}$ por uma lei de formação especial. A construção dessa lei de formação exerce um papel importante na teoria dos algoritmos de Jacobi-Perron. Jacobi e Perron usavam somente a lei de formação:

$${b_i}^{(v)} = \lfloor {a_i}^{(v)} \rfloor, \text{ com } i = 1, \ldots, n-1;\ v = 0, 1, \ldots$$

em que $\lfloor x \rfloor$ denota o maior número inteiro que não excede x. Berstein em (BERNSTEIN, l.,) sugere a seguinte modificação do algoritmo de Jacobi-Perron para ${b_i}^{(v)}$,

$$\begin{array}{lcllcl} {b_1}^{(v)} & = & {a_1}^{(v)} & \text{se} & {a_1}^{(v)} & \neq & \lfloor {a_1}^{(v)} \rfloor; \\ {b_1}^{(v)} & = & {a_1}^{(v)} - 1; & \text{se} & {a_1}^{(v)} & = & \lfloor {a_1}^{(v)} \rfloor; \\ {b_k}^{(v)} & = & \lfloor {a_k}^{(v)} \rfloor; & & & & \end{array} \tag{2.24}$$

com $k = 2, \ldots, n-1$ e $v = 0, 1, \ldots$.

É possível acontecer que, para algum v, ${a_i}^{(v)} = \lfloor {a_i}^{(v)} \rfloor$ para todo i. Nesse caso, o algoritmo segundo a lei (2.24) é considerado concluído, e adotamos ${b_i}^{(v)} = {a_i}^{(v)}$, com $i = 1, \ldots, n-1$.

O algoritmo dos vetores $(a^{(v)})$ dado por (2.1) será dito periódico se existirem dois números inteiros p, q $(p \geqslant 0,\ q \geqslant 1)$ tal que a transformação T produz

$$T^{V+q} = T^V, \text{ com } v = p, p+1, \ldots. \tag{2.25}$$

Em caso de periodicidade, os vetores $a^{(v)}$ com $v = 0, p, \ldots, p-1$ dizemos que formam o pré-período e os vetores $a^{(v)}$ com $v = p, p+1, \ldots, p+q-1$ formam o período do algoritmo; $min\ (p) = s$ e $min\ (q) = t$ são chamados, respectivamente, os comprimentos do pré-período e período; $s + t$ é chamado o comprimento do algoritmo, o qual será puramente periódico se $s = 0$.

2.4 Um vetor solução da equação padrão de grau n

Consideremos a equação padrão de grau n

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n = 1. \tag{2.26}$$

Seja $a^{(0)}$ um vetor de V_{n-1} dado por

$$a^{(0)} = \left({a_1}^{(0)}, \ldots, {a_{n-1}}^{(0)}\right);\ {a_i}^{(0)} = \frac{c_{i+1}}{c_1},\ \text{com } i = 1, \ldots, n-1. \tag{2.27}$$

No que segue enunciamos o principal resultado dessa seção:

Seja $a^{(0)}$ um vetor dado por (2.27). Se um vetor $a^{(v)}$ é transformado de $a^{(0)}$ segundo a lei de formação (2.24), então existe um número natural t tal que as componentes do vetor $a^{(t)}$ são inteiros, isto é,

$$a^{(t)} = \left({a_1}^{(t)}, \cdots, {a_{n-1}}^{(t)}\right);\ \text{com } {a_i}^{(t)} \text{ um inteiro, para } i = 1, \ldots, n-1. \tag{2.28}$$

Iniciamos por observar que $c_1 c_2$. Logo, $\lfloor {a_1}^{(0)} \rfloor \neq {a_1}^{(0)}$. Assim obtemos de (2.24),

$${b_i}^{(0)} = \left\lfloor \frac{c_{i+1}}{c_1} \right\rfloor,\ \text{com } i = 1, \ldots, n-1. \tag{2.29}$$

De (2.29), obtemos,

$$c_{i+1} = {b_i}^{(0)} c_1 + {c_i}^{(1)},\ \text{com } {c_1}^{(1)} \text{ um inteiro.} \tag{2.30}$$

Além disso observamos a seguinte desigualdade, obtida do algoritmo da divisão $0 < {c_i}^{(1)} < {c_n}^{(1)};\ {c_n}^{(1)} = c_1$; com $i = 1, \ldots, n-1$. De (2.27) e (2.30), obtemos

$${a_i}^{(0)} - {b_i}^{(0)} = \frac{c_{i+1}}{c_1} - \frac{c_{i+1} - {c_i}^{(1)}}{c_1} = \frac{{c_i}^{(1)}}{c_1}.$$

Considerando as transformações dadas em (2.18), vemos que as igualdades acima nos dão

$${a_i}^{(1)} = \frac{{c_{i+1}}^{(1)}}{{c_1}^{(1)}},\ \text{com } i = 1, \ldots, n-1. \tag{2.31}$$

Em consequência,

$${b_i}^{(1)} = \left\lfloor \frac{c_{i+1}^{(1)}}{{c_1}^{(1)}} \right\rfloor,\ \text{com } i = 2, \ldots, n-1$$

$${b_1}^{(1)} = \left\lfloor \frac{c_2^{(1)}}{{c_1}^{(1)}} \right\rfloor,\ \text{se } {c_1}^{(1)} {c_2}^{(1)}, \tag{2.32}$$

$${b_1}^{(1)} = \left(\frac{{c_2}^{(1)}}{{c_1}^{(1)}} - 1 \right),\ \text{se } {c_1}^{(1)} | {c_2}^{(1)}.$$

Se ${c_1}^{(1)} = 1$, o Teorema é verdadeiro com $t = 1$. Suponhamos, portanto, que ${c_1}^{(1)} > 1$. Dois casos possíveis: *i)* ${c_1}^{(1)} | {c_2}^{(1)}$ e *(ii)* ${c_1}^{(1)} {c_2}^{(1)}$. Primeiro investigaremos o caso *ii)*. Aqui obtemos,

$${c_{i+1}}^{(1)} = {b_i}^{(1)} {c_1}^{(1)} + {c_i}^{(2)},\ {c_i}^{(2)} \text{ um inteiro.}$$

Sendo ${c_i}^{(2)}$ o resto de uma divisão euclidiana, segue que

$$0 < {c_i}^{(2)} < {c_n}^{(2)};\ {c_n}^{(2)} = {c_1}^{(1)};\ \text{com } i = 2, \ldots, n-1. \tag{2.33}$$

Observemos que pela definição de ${b_1}^{(1)}$ também obtemos

$$0 < {c_1}^{(2)} < {c_n}^{(2)}.$$

Comparando a desigualdade acima com (2.30) é possível concluir que

$$0 < {c_1}^{(2)} < {c_1}^{(1)} < c_1.$$

Antes de investigar o caso i), provaremos o seguinte: Suponhamos que o vetor $a^{(v)}$ no algoritmo modificado de Jacobi-Perron construído segundo a lei de formação (2.27), tenha a forma

$$a^{(v)} = \left(\frac{{c_2}^{(v)}}{{c_1}^{(v)}}, \frac{{c_3}^{(v)}}{{c_1}^{(v)}}, \ldots, \frac{{c_n}^{(v)}}{{c_1}^{(v)}} \right),\ \text{com } v = 0, 1, \ldots, \tag{2.34}$$

então,

$$\left({c_1}^{(v)}, {c_2}^{(v)}, \ldots, {c_n}^{(v)} \right) = 1. \tag{2.35}$$

Iniciamos por observar que o Lema 2.4 é verdadeiro para $v = 0$. Basta observar que para $a^{(0)}$ as componentes são dadas pelos quocientes $\frac{c_i}{c_1}$. E sendo (2.26) uma equação padrão o resultado segue. Suponhamos que o Lema é verdadeiro para $v = k$, ou seja,

$$a^{(k)} = \frac{1}{{c_1}^{(k)}} \left({c_2}^{(k)}, {c_3}^{(k)}, \ldots, {c_n}^{(k)} \right) \text{ e } \left({c_1}^{(k)}, {c_2}^{(k)}, {c_3}^{(k)}, \ldots, {c_n}^{(k)} \right) = 1. \tag{2.36}$$

De (2.36) existem inteiros ${b_i}^{(k)}$ tais que,

$${c_{i+1}}^{(k)} = {b_i}^{(k)} {c_1}^{(k)} + {c_i}^{(k+1)};\ \text{com } {c_i}^{(k+1)} \text{ inteiro, para } i = 1, \ldots, n-1.$$

$$0 < {c_i}^{(k+1)} < {c_1}^{(k)}.$$

Denotaremos

$${c_1}^{(k)} = {c_n}^{(k+1)}, \tag{2.37}$$

$$\left({c_1}^{(k+1)}, {c_2}^{(k+1)}, \ldots, {c_n}^{(k+1)} \right) = d. \tag{2.38}$$

Se $d = 1$, o lema é verdadeiro. Assumamos que

$$d > 1.$$

Por (2.38) vemos que $d | {c_n}^{(k+1)}$. Já que ${c_1}^{(k)} = {c_n}^{(k+1)}$, segue que $d | {c_1}^{(k)}$. Dado que $d | {c_i}^{(k+1)}$ para qualquer $i = 1, \ldots, n-1$, por (2.37) conluímos que $d | {c_{i+1}}^{(k)}$. E isto nos leva a

$$\left({c_1}^{(k)}, {c_2}^{(k)}, \ldots, {c_n}^{(k)} \right) \geqslant d > 1.$$

mas isto contradiz (2.36). Portanto a suposição de que $d > 1$ é falsa, o que prova o Lema.

Retomamos ao caso (i) da demonstração do teorema e assumamos que

$$ {c_1}^{(1)} | {c_{i+1}}^{(1)}, \text{ para } i = 1, 2, \ldots, m. \tag{2.39} $$

Em vista do Lema 2.4 a seguinte restrição é válida,

$$ m \leqslant n - 2, $$

pois caso $m = n - 1$, obteríamos

$$ \left({c_1}^{(1)}, \ldots, {c_n}^{(1)} \right) = {c_1}^{(1)} > 1, $$

o qual contraria o Lema 2.4. Segue-se de (2.39) tendo em vista (2.24),

$$ \begin{aligned} &{c_2}^{(1)} = \left({b_1}^{(1)} + 1 \right) {c_1}^{(1)}, \text{ pois } {c_1}^{(1)} | {c_2}^{(1)}; \\ &{c_{i+1}}^{(1)} = {b_i}^{(1)} {c_1}^{(1)}, \text{ pois } {c_1}^{(1)} | {c_{i+1}}^{(1)} \text{ com } i = 0, \ldots, m; \\ &{c_{m+2}}^{(1)} = {b_{m+1}}^{(1)} {c_1}^{(1)} + {c_{m+1}}^{(2)}; \text{ com } 1 \leqslant {c_{m+1}}^{(2)} \leqslant {c_1}^{(1)}; \\ &{c_{m+2+j}}^{(1)} = {b_{m+1+j}}^{(1)} {c_1}^{(1)} + {c_{m+1+j}}^{(2)}; \\ &\text{com } \ 0 \leqslant {c_{m+1+j}}^{(2)} < {c_1}^{(1)}, \text{ para } j = 1, \ldots, n - m - 2. \end{aligned} \tag{2.40} $$

Denotemos

$$ {c_1}^{(1)} = {c_n}^{(2)} $$

De (2.24) vemos que ${b_1}^{(1)} = {a_1}^{(1)} - 1$. Isto implica que ${a_1}^{(1)} - {b_1}^{(1)} = 1$. De (2.31) sabemos que ${a_i}^{(1)} = \dfrac{{c_{i+1}}^{(1)}}{{c_1}^{(1)}}$. Já por (2.32) vemos que ${b_i}^{(1)} = \dfrac{{c_{i+1}}^{(1)}}{{c_1}^{(1)}}$ para $i = 2, \ldots, m$. Logo ${a_i}^{(1)} - {b_i}^{(1)} = 0$, para $i = 2, \ldots, m$. De formar análoga, temos que

$$ {a_{m+1}}^{(1)} - {b_{m+1}}^{(1)} = \frac{{c_{m+2}}^{(1)}}{{c_n}^{(2)}} - \frac{{c_{m+2}}^{(1)} - {c_{m+1}}^{(2)}}{{c_n}^{(2)}} = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}}. $$

Do mesmo modo, segue que

$$ \begin{aligned} {a_{m+1+j}}^{(1)} - {b_{m+1+j}}^{(1)} &= \frac{{c_{m+2+j}}^{(1)}}{{c_n}^{(2)}} - \frac{{c_{m+2+j}}^{(1)} - {c_{m+1+j}}^{(2)}}{{c_n}^{(2)}} \\ &= \frac{{c_{m+1+j}}^{(1)}}{{c_n}^{(2)}}, \text{ para } j = 1, \ldots, n - m - 2. \end{aligned} $$

Das igualdades acima e da transformação em (2.18), com $v = 1$ e observada a restrição $m \neq n-2$,

$$\begin{aligned}
{a_i}^{(2)} &= \frac{1}{{a_1}^{(1)} - {b_1}^{(1)}}\left({a_{i+1}}^{(1)} - {b_{i+1}}^{(1)}\right) = \frac{1}{1}(0) = 0, \text{ para } i = 1, \ldots, m-1;\\
{a_m}^{(2)} &= \frac{1}{{a_1}^{(1)} - {b_1}^{(1)}}\left({a_{m+1}}^{(1)} - {b_{m+1}}^{(1)}\right) = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}};\\
{a_{m+j}}^{(2)} &= \frac{1}{{a_1}^{(1)} - {b_1}^{(1)}}\left({a_{m+j+1}}^{(1)} - {b_{m+j+1}}^{(1)}\right) = \frac{{c_{m+1+j}}^{(2)}}{{c_n}^{(2)}}, \text{ com } j = 1, \ldots, n-m-2;\\
{a_{n-1}}^{(2)} &= \frac{1}{{a_1}^{(1)} - {b_1}^{(1)}} = 1.
\end{aligned} \tag{2.41}$$

Deve-se observar que todos os ${a_i}^{(2)}$ com $i = 1, \ldots, n-1$ têm o mesmo denominador ${c_n}^{(2)}$, pois se ${a_i}^{(2)} = 0$ colocamos ${a_i}^{(2)} = \dfrac{0}{{c_n}^{(2)}}$; se ${a_{n-1}}^{(2)} = 1$ colocamos,

$${a_{n-1}}^{(2)} = \frac{{c_n}^{(2)}}{{c_n}^{(2)}}.$$

Combinando (2.30) e (2.40) vemos que

$$1 < {c_{m+1}}^{(2)} < {c_1}^{(1)} < c_1.$$

Em virtude de (2.32) obtemos

$${c_{m+i+j}}^{(2)} < {c_1}^{(1)} = {c_n}^{(2)}, \text{ com } j = 1, \ldots, n-m-2.$$

Agora, considerando (2.24) deduzimos que

$$b_1^{(2)} = a_1^{(2)} - 1 = 0 - 1 = -1,$$

pois $a_1^{(2)} = 0 = \lfloor a_1^{(2)} \rfloor$; também, vemos para $i = 1, \ldots, n-3$ que

$${b_{i+1}}^{(2)} = \lfloor {a_{i+1}}^{(2)} \rfloor = 0$$

De forma análoga é possível mostrar que ${b_{n-1}}^{(2)} = 1$. Destas últimas equações é possível ver que ${b_1}^{(2)} = {a_1}^{(2)} - 1$. Isso implica que ${a_1}^{(2)} - {b_1}^{(2)} = 1$. Como foi mostrado para $i = 1, \ldots, m-2$ que ${a_{i+1}}^{(2)} = 0$ e ${b_{i+1}}^{(2)} = 0$ temos

$$a_{i+1}^{(2)} - b_{i+1}^{(2)} = 0, \text{ para } i = 1, \ldots, m-2.$$

Sabe-se que ${a_m}^{(2)} = \dfrac{{c_{m+1}}^{(2)}}{{c_1}^{(1)}}$, e disso segue

$${a_m}^{(2)} - {b_m}^{(2)} = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}}.$$

Agora para $j = 1, \ldots, n-m-2$ temos

$$a_{m+j}^{(2)} - b_{m+j}^{(2)} = \frac{{c_{m+1+j}}^{(2)}}{{c_n}^{(2)}}$$

Ainda vemos que

$${a_{n-1}}^{(2)} - {b_{n-1}}^{(2)} = 1 - 1 = 0,$$

Dos resultados acima, tendo em vista (2.18), obtemos

$${a_i}^{(3)} = \frac{1}{{a_1}^{(2)} - {b_1}^{(2)}} \left({a_{i+1}}^{(2)} - {b_{i+1}}^{(2)} \right)$$

Disso, segue facilmente que

$${a_i}^{(3)} = 0, \quad \text{para } i = 1, \ldots, m-2.$$

Também vemos que

$${a_{m-1}}^{(3)} = \frac{1}{{a_1}^{(2)} - {b_1}^{(2)}} \left({a_m}^{(2)} - {b_m}^{(2)} \right) = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}}$$

Agora para $j = 1, \ldots, n-m-2$ deduzimos que

$${a_{m-1+j}}^{(3)} = \frac{1}{{a_1}^{(2)} - {b_1}^{(2)}} \left({a_{m+j}}^{(2)} - {b_{m+j}}^{(2)} \right) = \frac{{c_{m+1+j}}^{(2)}}{{c_n}^{(2)}}.$$

Ainda para $v = 3$ cosneguimos calcular

$$\begin{aligned} {a_{n-2}}^{(3)} &= \frac{1}{{a_1}^{(2)} - {b_1}^{(2)}} \left({a_{n-1}}^{(2)} - {b_{n-1}}^{(2)} \right) = 0 \\ {a_{n-1}}^{(3)} &= \frac{1}{{a_1}^{(2)} - {b_1}^{(2)}} \left({a_n}^{(2)} - {b_n}^{(2)} \right) = 1. \end{aligned}$$

Mostraremos de forma indutiva que

$$\begin{aligned} &{a_i}^{(k+1)} = 0, \quad i = 1, \ldots, m-k \\ &{a_{m-k+1}}^{(k+1)} = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}} \\ &{a_{m-k+1+j}}^{(k+1)} = \frac{c_{m+1+j}^{(2)}}{c_n^{(2)}}; \quad \text{para} \quad j = 1, \ldots, n-m-2; \\ &{a_{n-k-1+s}}^{(k+1)} = 0; \quad \text{com} \quad s = 1, \ldots, k-1; \\ &{a_{n-1}}^{(k+1)} = 1, \end{aligned} \tag{2.42}$$

em que $k = 2, \ldots, m-1$. Pelo o que já foi demonstrado já sabemos que as igualdades acima valem para $k = 2$. Suponhamos que elas valem para $k = v$, isto é,

$$\begin{aligned} &{a_i}^{(v+1)} = 0, \quad i = 1, \ldots, m-v \\ &{a_{m-v+1}}^{(v+1)} = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}} \\ &{a_{m-v+1+j}}^{(v+1)} = \frac{c_{m+1+j}^{(2)}}{c_n^{(2)}}; \quad \text{para} \quad j = 1, \ldots, n-m-2; \\ &{a_{n-v-1+s}}^{(v+1)} = 0; \quad \text{com} \quad s = 1, \ldots, v-1; \\ &{a_{n-1}}^{(v+1)} = 1. \end{aligned}$$

Lembramos por (2.40) que para $j = 1, \ldots, n-m-2$ é valido que ${c_{m+1+j}}^{(2)} < {c_n}^{(2)}$. Logo das igualdades acima e de (2.24) obtemos

$$\begin{aligned}
&{b_1}^{(v+1)} = a_1^{(v+1)} - 1 = -1;\\
&{b_{1+i}}^{(v+1)} = \lfloor a_{i+1}^{(v+1)} \rfloor = \left\lfloor \frac{c_{m+1+j}^{(2)}}{c_n^{(2)}} \right\rfloor = 0, \quad \text{para } i = 1, \ldots, n-3;\\
&{b_{n-1}}^{(v+1)} = a_{n-1}^{(v+1)} = 1.
\end{aligned}$$

Do que foi provado acima, deduzimos que

$$ {a_i}^{(v+1)} - {b_i}^{(v+1)} = 1 $$

Observando que $m - v - 1 \leqslant n - 2 - v - 1 = n - 3 - v$ temos

$$ {a_{1+i}}^{(v+1)} - {b_{1+i}}^{(v+1)} = 0, \text{ com } i = 1, \ldots, m-v-1. $$

Considerando que $v \geqslant 2$ conseguimos de maneira análoga acima que

$$ {a_{m-v+1}}^{(v+1)} - {b_{m-v+1}}^{(v+1)} = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}}, $$

É fato que $m - v - 1 + j \leqslant (n-3) - v$ para $j = 1, \ldots, n-m-2$. Então

$$ {a_{m-v-1+j}}^{(v+1)} - {b_{m-v-1+j}}^{(v+1)} = \frac{{c_{m+1+j}}^{(2)}}{{c_n}^{(2)}}, \text{ com } j = 1, \ldots, n-m-2; $$

Agora um simples cálculo mostra que $m - v + 1 + s \leqslant n - 2$ para $s = 1, \ldots, v-1$. Logo,

$$ {a_{m-v+1+s}}^{(v+1)} - {b_{m-v+1+s}}^{(v+1)} = 0, \text{ com } s = 1, \ldots, v-1. $$

Por fim, é visto de forma direta que

$$ {a_{n-1}}^{(v+1)} - {b_{n-1}}^{(v+1)} = 0. $$

Do que foi provado acima, em virtude de (2.18),

$$\begin{aligned}
&{a_i}^{(v+2)} = \frac{1}{{a_1}^{(v+1)} - {b_1}^{(v+1)}} \left({a_{i+1}}^{(v+1)} - {b_{i+1}}^{(v+1)} \right) = 0; \text{ com } i = 1, \ldots, m-v-1;\\
&{a_{m-v}}^{(v+2)} = \frac{1}{{a_1}^{(v+1)} - {b_1}^{(v+1)}} \left({a_{m-v+1}}^{(v+1)} - {b_{m-v+1}}^{(v+1)} \right) = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}};\\
&{a_{m-v+j}}^{(v+2)} = \frac{1}{{a_1}^{(v+1)} - {b_1}^{(v+1)}} \left({a_{m-v+j+1}}^{(v+1)} - {b_{m-v+j+1}}^{(v+1)} \right) = \frac{{c_{m+1+j}}^{(2)}}{{c_n}^{(2)}},\\
&\text{com } j = 1, \ldots, n-m-2;\\
&{a_{n-v-2+s}}^{(v+2)} = \frac{1}{{a_1}^{(v+1)} - {b_1}^{(v+1)}} \left({a_{n-v-1+s}}^{(v+1)} - {b_{n-v-1+s}}^{(v+1)} \right) = 0, \text{ com } s = 1, \ldots, v;\\
&{a_{n-1}}^{(v+2)} = 1.
\end{aligned}$$

Mas as igualdades acima são as fórmulas (2.42) para $k = v + 1$; assim, as fórmulas (2.42) são completamente comprovadas. Agora obtemos de (2.42), para $k = m - 1$,

$$\begin{aligned}
&{a_1}^{(m)} = 0;\\
&{a_2}^{(m)} = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}};\\
&{a_{2+j}}^{(m)} = \frac{{c_{m+1+j}}^{(2)}}{{c_n}^{(2)}}, \text{ com } j = 1, \ldots, n-m-2;\\
&{a_{n-m+s}}^{(m)} = 0, \text{ para } s = 1, \ldots, m-2;\\
&{a_{n-1}}^{(m)} = 1,
\end{aligned} \tag{2.43}$$

e de (2.43), em virtude de (2.24)

$$\begin{aligned}
&{b_1}^{(m)} = a_1^{(m)} - 1 = -1;\\
&{b_{1+i}}^{(m)} = \lfloor a_{i+1}^{(m)} \rfloor = \left\lfloor \frac{{c_{m+1+j}}^{(2)}}{{c_n}^{(2)}} \right\rfloor = 0, \quad \text{para } i = 1, \ldots, n-3; \ ,\\
&{b_{n-1}}^{(m)} = a_{n-1}^{(m)} = 1.
\end{aligned}$$

onde na segunda igualdade usamos que ${c_{m+1+j}}^{(2)} < {c_n}^{(2)}$ para $j = 1, \ldots, n-m-2$, isto devido a (2.40). Das igualdades acima e de (2.43), obtemos

$$\begin{aligned}
&{a_1}^{(m)} - {b_1}^{(m)} = 0;\\
&{a_2}^{(m)} - {b_2}^{(m)} = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}};\\
&{a_{2+j}}^{(m)} - {b_{2+j}}^{(m)} = \frac{{c_{m+1+j}}^{(2)}}{{c_n}^{(2)}}, \text{ para } j = 1, \ldots, n-m-2;
\end{aligned}$$

$${a_{n-m+s}}^{(m)} - {b_{n-m+s}}^{(m)} = 0, \text{ com } s = 1, \ldots, m-1,$$

e dessas igualdades, tendo em vista (2.18), deduzimos que

$$\begin{aligned}
&{a_1}^{(m+1)} = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}};\\
&{a_{1+j}}^{(m+1)} = \frac{{c_{m+1+j}}^{(2)}}{{c_n}^{(2)}}; \text{ com } j = 1, \ldots, n-m-2;\\
&{a_{n-m-1+s}}^{(m+1)} = 0, \text{ com } s = 1, \ldots, m-1,\\
&{a_{n-1}}^{(m+1)} = 1.
\end{aligned} \tag{2.44}$$

Novamente lembramos que ${c_{m+1}}^{(2)} < {c_n}^{(2)}$ por (2.40). Logo das igualdades acima e de (2.24) calculamos

$$\begin{aligned}
&{b_i}^{(m+1)} = \lfloor a_1^{(m+1)} \rfloor = \left\lfloor \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}} \right\rfloor = 0, \text{ com } i = 1, \ldots, n-2;\\
&{b_{n-1}}^{(m+1)} = 1,
\end{aligned}$$

e de (2.44) e dos valores acima segue que

$$\begin{aligned} &{a_1}^{(m+1)} - {b_1}^{(m+1)} = \frac{{c_{m+1}}^{(2)}}{{c_n}^{(2)}}; \\ &{a_{1+j}}^{(m+1)} - {b_{1+j}}^{(m+1)} = \frac{{c_{m+1+j}}^{(2)}}{{c_n}^{(2)}};\ \text{com } j = 1, \ldots, n-m-2; \\ &{a_{n-m-1+s}}^{(m+1)} - {b_{n-m-1+s}}^{(m+1)} = 0,\ \text{com } s = 1, \ldots, m. \end{aligned} \tag{2.45}$$

De (2.45), em virtude de (2.18), obtemos que

$$\begin{aligned} &{a_j}^{(m+2)} = \frac{{c_{m+1+j}}^{(2)}}{c_{m+1}^{(2)}};\ \text{com } j = 1, \ldots, n-m-2; \\ &{a_{n-m-2+s}}^{(m+1)} = 0,\ \text{com } s = 1, \ldots, m; \\ &{a_{n-1}}^{m+2} = \frac{{c_n}^{(2)}}{{c_{m+1}}^{(2)}}, \end{aligned} \tag{2.46}$$

ou de outra forma

$$\begin{aligned} &{a_j}^{(m+2)} = \frac{{c_{j+1}}^{(m+2)}}{{c_1}^{(m+2)}};\ \text{com } j = 1, \ldots, n-m-2; \\ &{a_{n-m-2+s}}^{(m+2)} = 0,\ \text{com } s = 1, \ldots, m; \\ &{a_{n-1}}^{m+2} = \frac{{c_n}^{(m+2)}}{{c_{m+1}}^{(m+2)}}; \end{aligned} \tag{2.47}$$

Afirmamos que

$$\begin{aligned} &{c_{m+i}}^{(2)} = {c_i}^{(m+2)},\ \text{com } i = 1, \ldots, n-m-1; \\ &{c_n}^{(2)} = {c_n}^{(m+2)}. \end{aligned}$$

De fato, lebramos que

$$c_{i+1}^{(m+1)} = b_i^{(m+1)} c_1^{(m+1)} + c_i^{(m+2)},\ \text{para } i = 1, \ldots, n-1.$$

Mas sabemos que $b_i^{(m+1)} = 0$ para $i = 1, \ldots, n-2$, então

$$c_{i+1}^{(m+1)} = c_i^{(m+2)},\ \text{para } i = 1, \ldots, n-2.$$

De forma análoga, temos que

$$c_{i+2}^{(m)} = b_{i+1}^{(m)} c_1^{(m)} + c_{i+1}^{(m+2)},\quad \text{para } i = 1, \ldots, n-1.$$

Também, sabemos que $b_{i+1}^{(m)} = 0$ para $i = 1, \ldots, n-3$. Logo

$$c_{i+2}^{(m)} = c_{i+1}^{(m+2)},\ \text{para } i = 1, \ldots, n-3.$$

Prosseguindo como este argumento, conseguiremos mostrar que

$$c_{m+i}^{(2)} = c_i^{(m+2)},\ \text{para } i = 1, \ldots, n-m-2.$$

O caso de $i = 1$ é consequência de (2.46) e (2.47). Isto também se aplica para mostrar que

$$c_n{}^{(2)} = c_n{}^{(m+2)}.$$

De (2.31) e (2.33), obtemos

$$a_1{}^{(1)} - b_1{}^{(1)} = \frac{c_1{}^{(2)}}{c_1{}^{(1)}};\ a_{1+j}{}^{(1)} - b_{1+j}{}^{(1)} = \frac{c_{1+j}{}^{(2)}}{c_1{}^{(1)}},\ \text{com } j = 1, \ldots, n-2, \tag{2.48}$$

e de (2.48), tendo em vista (2.18).

$$a_j{}^{(2)} = \frac{c_{1+j}{}^{(2)}}{c_1{}^{(2)}},\ \text{com } j = 1, \ldots, n-1;\ c_1{}^{(1)} = c_n{}^{(2)}. \tag{2.49}$$

Obtemos assim duas cadeias de desigualdades,

$$0 < c_1{}^{(2)} < c_1{}^{(1)} < c_1;\ 0 < c_1{}^{(m+2)} < c_1{}^{(1)} < c_1.$$

E se $c_1{}^{(2)}$ ou $c_1{}^{(m+2)} = 1$, o Teorema 2.4 está provado. Caso contrário, deduzimos de (2.47) ou (2.49), que mostra que os vetores $a^{(2)}$ e $a^{(m+2)}$ têm a mesma estrutura de seus componentes, como o algoritmo deve continuar. De qualquer forma, obtemos uma cadeia de desigualdades,

$$\begin{gathered} 0 < c_1{}^{(m_k)} < c_1{}^{(m_{k-1})} < \ldots < c_1{}^{(m_2)} < c_1{}^{(1)} < c_1, \\ m_2 = 2 \text{ se } c_1{}^{(1)} c_2{}^{(1)};\ m_2 = m+2 \text{ se } c_1{}^{(1)} | c_2{}^{(1)}, \ldots \end{gathered} \tag{2.50}$$

e como $c_i{}^{(m_i)}$ são números naturais, devemos necessariamente chegar a

$$c_1{}^{(t)} = 1,\ t = m_k \geqslant 1. \tag{2.51}$$

Isso prova o Teorema 2.4.

Agora estamos prontos para mostrar o vetor solução da equação padrão de grau n (2.26.)

Um vetor solução da equação padrão de grau n (2.26) é dado pela fórmula,

$$x = (x_1, x_2, \ldots, x_n);\ \ \text{com} \ \ x_i = (-1)^{(t+1)(n-1)} \cdot B_{i,n},\ \text{com } i = 1, \ldots, n \tag{2.52}$$

em que $B_{i,n}$ são cofatores dos elementos da n-ésima coluna no determinante

$$D_{t+1} = \begin{vmatrix} A_0{}^{(t+1)} & A_0{}^{(t+2)} & \cdots & A_0{}^{(t+n)} \\ A_1{}^{(t+1)} & A_1{}^{(t+2)} & \cdots & A_1{}^{(t+n)} \\ \vdots & \vdots & \ddots & \vdots \\ A_{n-1}{}^{(t+1)} & A_{n-1}{}^{(t+2)} & \cdots & A_{n-1}{}^{(t+n)} \end{vmatrix} \tag{2.53}$$

Em $D_{t+1},\ t$ tem o significado de (2.51) e para $v = t+1, t+2, \ldots, t+n$ temos que

$$A_i{}^{(t+n)} = A_i{}^{(t)} + \sum_{j=1}^{n-1} b_j{}^{(t)} A_i{}^{(t+j)},$$

como em (2.19) e pode ser obtido a partir do algoritmo Jacobi-Perron modificado do vetor $a^{(0)}$ fornecido a partir de (2.27) por meio da lei de formação (2.32). Iniciamos por lembrar que, segundo (2.32), todos os números $b_i{}^{(v)}$ são inteiros. Logo, pela definição em (2.19) vemos que

$$A_i{}^{(v)},\ \text{com } i = 0, 1, \ldots, n-1 \text{ e } v = 0, 1, \ldots$$

também são inteiros. Para $c_1{}^{(t)} = 1$ obtemos

$$a^{(t)} = (c_2{}^{(t)}, c_3{}^{(t)}, \ldots, c_n{}^{(t)}) = (a_1{}^{(t)}, \ldots, a_{n-1}{}^{(t)}),$$

$$b_i{}^{(t)} = a_i{}^{(t)} = c_{i+1}{}^{(t)},\ \text{com } i = 1, \ldots, n-1.$$

Usando as fórmulas (2.19), (2.21) e (2.27), obtemos,

$$a_i{}^{(0)} = \frac{A_i{}^{(t)} + \sum_{j=1}^{n-1} a_j{}^{(t)} A_i{}^{(t+j)}}{A_0{}^{(t)} + \sum_{j=1}^{n-1} a_j{}^{(t)} A_0{}^{(t+j)}} = \frac{A_i{}^{(t)} + \sum_{j=1}^{n-1} b_j{}^{(t)} A_i{}^{(t+j)}}{A_0{}^{(t)} + \sum_{j=1}^{n-1} b_j{}^{(t)} A_0{}^{(t+j)}} = \frac{A_i{}^{(t+n)}}{A_0{}^{(t+n)}}.$$

Agora segue que

$$\frac{c_{i+1}}{c_1} = \frac{A_i{}^{(t+n)}}{A_0{}^{(t+n)}},\ \text{com } i = 1, \ldots, n-1.$$

Disso

$$c_{i+1} = \frac{c_1 A_i{}^{(t+n)}}{A_0{}^{(t+n)}}.$$

Como $(c_1, c_2, \ldots, c_n) = 1,$ temos

$$\left(c_1, \frac{c_1 A_1{}^{(t+n)}}{A_0{}^{(t+n)}}, \frac{c_1 A_2{}^{(t+n)}}{A_0{}^{(t+n)}}, \ldots, \frac{c_1 A_{n-1}{}^{(t+n)}}{A_0{}^{(t+n)}}\right) = 1.$$

Em virtude de um Teorema conhecido,

$$\begin{gathered}\left(c_1 A_0{}^{(t+n)}, c_1 A_1{}^{(t+n)}, c_1 A_2{}^{(t+n)}, \ldots, c_1 A_{n-1}{}^{(t+n)}\right) = A_0{}^{(t+n)}, \\ c_1 \left(A_0{}^{(t+n)}, A_1{}^{(t+n)}, A_2{}^{(t+n)}, \ldots, A_{n-1}{}^{(t+n)}\right) = A_0{}^{(t+n)}.\end{gathered} \tag{2.54}$$

De (2.20), sabemos que

$$D_{t+1} = \begin{vmatrix} A_0{}^{(t+1)} & \ldots & A_0{}^{(t+n-1)} & A_0{}^{(t+n)} \\ \ldots & \ldots & \ldots & \ldots \\ A_{n-1}{}^{(t+1)} & \ldots & A_{n-1}{}^{(t+n-1)} & A_{n-1}{}^{(t+n)} \end{vmatrix} = (-1)^{(t+1)(n+1)}$$

Afirmamos que

$$\left(A_0{}^{(t+n)}, A_1{}^{(t+n)}, A_2{}^{(t+n)}, \ldots, A_{n-1}{}^{(t+n)}\right) = 1.$$

De fato, se $\left({A_0}^{(t+n)}, {A_1}^{(t+n)}, {A_2}^{(t+n)}, \ldots, {A_{n-1}}^{(t+n)}\right) = d > 1$, então a última coluna do determinante acima seria um múltiplo de d. Logo, concluíriamos que $D_{t+1} = d * z \neq (-1)^{(t+1)(n+1)}$, em que z é o valor do determinante depois da operação acima. Isto é uma contradição. Assim, do fato acima e de (2.54), vemos que

$$c_1 = {A_0}^{(t+n)}.$$

Disso segue que

$$c_{i+1} = {A_i}^{(t+n)}, \text{ com } i = 0, 1, \ldots, n-1,$$

Em virtude disso, obtemos

$$D_{t+1} = \begin{vmatrix} {A_0}^{(t+1)} & {A_0}^{(t+2)} & \cdots & {A_0}^{(t+n-1)} & c_1 \\ {A_1}^{(t+1)} & {A_1}^{(t+2)} & \cdots & {A_1}^{(t+n-1)} & c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ {A_{n-1}}^{(t+1)} & {A_{n-1}}^{(t+2)} & \cdots & {A_{n-1}}^{(t+n-1)} & c_n \end{vmatrix} = (-1)^{(t+1)(n-1)}.$$

Logo, denotando os cofatores do c_i em D_{t+1} por $B_{i,n}$, com $i = 1, \ldots, n$ deduzimos que

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

ou, multiplicando ambos os lados desta equação por $(-1)^{(t+1)(n-1)}$,

$$\sum_{i=1}^{n} \left((-1)^{(t+1)(n-1)} B_{i,n}\right) c_1 = 1,$$

o que prova o Teorema 2.4.

Na próximo capítulo mostraremos como constuir soluções de equações diofantinas padrões a partir dos Teoremas 2.4 e 2.4.

3 Aplicações numéricas das Equações Diofantinas padrões com n variáveis

Um problema ao estudar e resolver numericamente as equações diofantinas de ordem n é que demandam muitos cálculos manuais. Faremos uso do software Python, que é uma linguagem de programação de alto nível, para realizar os cálculos das soluções das equações diofantinas de grau n em nosso trabalho.

A opção pelo software Python justifica-se, principalmente, pela aproximação da escrita matemática com outras linguagens geralmente utilizada em Matemática Aplicada, também, por disponibilizar comandos simples que atendem aquilo que necessitamos nessa dissertação. O Python possui tipagem dinâmica e uma de suas principais características é permitir a fácil leitura do código e exigir poucas linhas de código se comparado com outros programa em outras linguagens. Como pré-requisito pedimos conhecimentos básicos sobre programação.

Nesse capítulo, iremos resolver equações diofantinas cujas teorias foram desenvolvidas no Capítulo 2.

3.1 Alguns exemplos numéricos para solução de uma equação padrão de grau n

Nesta seção, ilustraremos nossa teoria com exemplos numéricos. Para encontrar o vetor solução de uma equação diofantina padrão de n variáveis, utilizaremos o seguinte algoritmo:

1. Escolher uma equação;
2. Verificar se os coeficientes satisfazem as condições dadas em (2.2);
3. Obter os vetores $b^{(v)}$ segundo o Teorema 2.4;
4. Obtidos os vetores $b^{(v)}$ até t encontrado no Teorema 2.4, construir a matriz D_{t+1} dada (2.20);
5. Encontrar as soluções pelo Teorema 2.4;
6. Verificar que as soluções satisfazem a equação diofantina.

No que segue calcularemos passo a passo a solução do primeiro exemplo da seção 4 do artigo (BERNSTEIN, l.,).

Dada equação padrão de grau 4 abaixo, obter uma solução.

$$53x_1 + 117x_2 + 209x_3 + 300x_4 = 1.$$

Resolução: Iniciamos por observar que

$$c_1 = 53,\ c_2 = 117,\ c_3 = 209 \,\text{e}\, c_4 = 300.$$

De (2.2), verificamos que,

a. $53, 117, 209, 300 \in N$.
b. $1 < 53 < 117 < 209 < 300$.
c. $(53, 117, 209, 300) = 1$ ou seja, são primos entre si.
d. $c_1 c_{1+j};\ j = 1, 2, 3.$
   $c_2 c_{2+j};\ j = 1, 2.$
   $c_3 c_{2+j};\ j = 1.$
e. É uma equação padrão.

Com isso, garantimos que a equação é padrão.

Seja o vetor $a^{(0)} = \left({a_1}^{(0)}, {a_2}^{(0)}, {a_3}^{(0)}\right)$, obtemos suas componentes fazendo,

$${a_1}^{(0)} = \frac{117}{53}, {a_2}^{(0)} = \frac{209}{53}, {a_3}^{(0)} = \frac{300}{53}. \tag{3.1}$$

Agora vamos trabalhar para encontrar o vetor $b^{(0)} = \left({b_1}^{(0)}, {b_2}^{(0)}, {b_3}^{(0)}\right)$. Para isto, usaremos o seguinte fato

$$c_{i+1} = b_i^{(0)} c_1 + c_i^{(1)}, \quad \text{para, } i = 1, 2, 3.$$

e denotamos $c_4^{(1)} = c_1 = 53$. Contas diretas nos mostram que

$$\begin{aligned} 117 &= 2 \cdot 53 + 11 \\ 209 &= 3 \cdot 53 + 50 \\ 300 &= 5 \cdot 53 + 35 \end{aligned}$$

Logo, temos que,

$$b^{(0)} = (2, 3, 5) \text{ e } \ c_1 = (11, 50, 35, 53).$$

Agora usaremos o seguinte algoritmo

$$c_{i+1}^{(1)} = b_i^{(1)} c_1^{(1)} + c_i^{(2)}, \quad \text{para, } i = 1, 2, 3.$$

e denotamos $c_4^{(2)} = c_1^{(1)} = 11$. Calculemos

$$\begin{aligned} 50 &= 4 \cdot 11 + 6 \\ 35 &= 2 \cdot 11 + 2 \\ 53 &= 2 \cdot 11 + 9, \end{aligned}$$

Disso, vemos que

$$b^{(1)} = (4, 3, 4) \text{ e } \ c_2 = (6, 2, 9, 11).$$

Para calcular $b^{(1)}$ usaremos o algoritmo,

$$c_{i+1}^{(2)} = b_i^{(2)} c_1^{(2)} + c_i^{(3)}, \ \text{ para, } i = 1, 2, 3.$$

e $c_4^{(3)} = c_1^{(2)} = 6$. Efetuemos o algoritmo

$$\begin{aligned} 2 &= 0 \cdot 6 + 2 \\ 9 &= 1 \cdot 6 + 3 \\ 11 &= 1 \cdot 6 + 5, \end{aligned}$$

Logo,

$$b^{(2)} = (0, 1, 1) \ \text{ e } \ c_3 = (2, 3, 5, 6).$$

Novamente usamos o algoritmo

$$c_{i+1}^{(3)} = b_i^{(3)} c_1^{(3)} + c_i^{(4)}, \ \text{ para, } i = 1, 2, 3.$$

e $c_4^{(4)} = c_1^{(3)} = 6$ para estabelecer o vetor $b^{(3)}$. De fato,

$$\begin{aligned} 3 &= 1 \cdot 2 + 1 \\ 5 &= 2 \cdot 2 + 1 \\ 6 &= 3 \cdot 2 + 0, \end{aligned}$$

Assim obtemos que

$$b^{(3)} = (1, 2, 3) \ \text{ e } \ c_4 = (1, 1, 0, 6).$$

Como $c_4^{(1)} = 1$, pelo Teorema 2.4 o nosso algoritmo deve parar e $t = 4$. Façamos a conta para mostrar que isto acontece. De fato, usaremos o algoritmo

$$c_{i+1}^{(4)} = b_i^{(4)} c_1^{(4)} + c_i^{(5)}, \ \text{ para, } i = 1, 2, 3.$$

e $c_4^{(5)} = c_1^{(4)} = 1$. Calculemos

$$\begin{aligned} 1 &= 1 \cdot 1 + 0 \\ 0 &= 0 \cdot 1 + 0 \\ 2 &= 2 \cdot 1 + 0, \end{aligned}$$

Concluímos assim que

$$b^{(4)} = (1, 0, 2) \ \text{ e } \ c_5 = (0, 0, 0, 1).$$

Isto mostra como no Teorema 2.4 que o processo será estável, ou seja, sempre vamos conseguir os mesmos valores daqui para frente. Pelo algoritmo acima, obtemos a sequência de vetores,

$$b^{(0)} = (2, 3, 5)\,,\ b^{(1)} = (4, 3, 4)\,,\ b^{(2)} = (0, 1, 1)\,,\ b^{(3)} = (1, 2, 3)\,,\ b^{(4)} = (1, 0, 2)\,. \tag{3.2}$$

Além disso, vemos que pelo algoritmo temos

$$t = 4, \quad t + 1 = 5.$$

O nosso próximo passo é construir o determinante D_{t+1}. Para isso lembramos a definição dos $A_i^{(v+t)}$ segundo (2.20),

$$A_i{}^{(v+t)} = A_i{}^{(v)} + \sum_{j=1}^{n-1} \left(b_j{}^{(v)} A_i{}^{(v+j)} \right); \text{ com } i = 0, \ldots, n-1; v = 0, 1, \ldots$$

De (3.2) e n entre 0 e 4 calcularemos os valores $A_0{}^{(n+4)}$

$$A_0{}^{(4)} = A_0{}^{(0)} + b_1{}^{(0)} A_0{}^{(1)} + b_2{}^{(0)} A_0{}^{(2)} + b_3{}^{(0)} A_0{}^{(3)},$$

$$A_0{}^{(4)} = 1 + 2 \cdot 0 + 3 \cdot 0 + 5 \cdot 0 = 1.$$

$$A_0{}^{(1+4)} = A_0{}^{(1)} + \sum_{j=1}^{3} \left(b_j{}^{(1)} A_0{}^{(1+j)} \right),$$

$$A_0{}^{(5)} = A_0{}^{(1)} + b_1{}^{(1)} A_0{}^{(2)} + b_2{}^{(1)} A_0{}^{(3)} + b_3{}^{(1)} A_0{}^{(4)},$$

$$A_0{}^{(5)} = 0 + 4 \cdot 0 + 3 \cdot 0 + 4 \cdot 1 = 4.$$

$$A_0{}^{(2+4)} = A_0{}^{(2)} + \sum_{j=1}^{3} \left(b_j{}^{(2)} A_0{}^{(2+j)} \right),$$

$$A_0{}^{(6)} = A_0{}^{(2)} + b_1{}^{(2)} A_0{}^{(3)} + b_2{}^{(2)} A_0{}^{(4)} + b_3{}^{(2)} A_0{}^{(5)},$$

$$A_0{}^{(6)} = 0 + 0 \cdot 0 + 1 \cdot 1 + 1 \cdot 4 = 5.$$

$$A_0{}^{(3+4)} = A_0{}^{(3)} + \sum_{j=1}^{3} \left(b_j{}^{(3)} A_0{}^{(3+j)} \right),$$

$$A_0{}^{(7)} = A_0{}^{(3)} + b_1{}^{(3)} A_0{}^{(4)} + b_2{}^{(3)} A_0{}^{(5)} + b_3{}^{(3)} A_0{}^{(6)},$$

$$A_0{}^{(7)} = 0 + 1 \cdot 1 + 2 \cdot 4 + 3 \cdot 5 = 24.$$

$$A_0{}^{(4+4)} = A_0{}^{(4)} + \sum_{j=1}^{3} \left(b_j{}^{(4)} A_0{}^{(4+j)} \right),$$

$$A_0{}^{(8)} = A_0{}^{(4)} + b_1{}^{(5)} A_0{}^{(5)} + b_2{}^{(4)} A_0{}^{65)} + b_3{}^{(4)} A_0{}^{(7)},$$

$$A_0{}^{(8)} = 1 + 1 \cdot 4 + 0 \cdot 5 + 2 \cdot 24 = 53.$$

De (3.2) e n entre 0 e 4 calcularemos os valores ${A_1}^{(n+4)}$.

$$ {A_1}^{(0+4)} = {A_1}^{(0)} + \sum_{j=1}^{3} \left({b_j}^{(0)} {A_1}^{(0+j)} \right), $$

$$ {A_1}^{(4)} = {A_1}^{(0)} + {b_1}^{(0)} {A_1}^{(1)} + {b_2}^{(0)} {A_2}^{(2)} + {b_3}^{(0)} {A_1}^{(3)}, $$

$$ {A_1}^{(4)} = 0 + 2 \cdot 1 + 3 \cdot 0 + 5 \cdot 0 = 2. $$

$$ {A_1}^{(1+4)} = {A_1}^{(1)} + \sum_{j=1}^{3} \left({b_j}^{(1)} {A_1}^{(1+j)} \right), $$

$$ {A_1}^{(5)} = {A_1}^{(1)} + {b_1}^{(1)} {A_1}^{(2)} + {b_2}^{(1)} {A_1}^{(3)} + {b_3}^{(1)} {A_1}^{(4)}, $$

$$ {A_1}^{(5)} = 1 + 4 \cdot 0 + 3 \cdot 0 + 4 \cdot 2 = 9. $$

$$ {A_1}^{(2+4)} = {A_1}^{(2)} + \sum_{j=1}^{3} \left({b_j}^{(2)} {A_1}^{(2+j)} \right), $$

$$ {A_1}^{(6)} = {A_1}^{(2)} + {b_1}^{(2)} {A_1}^{(3)} + {b_2}^{(2)} {A_1}^{(4)} + {b_3}^{(2)} {A_1}^{(5)}, $$

$$ {A_1}^{(6)} = 0 + 0 \cdot 0 + 1 \cdot 2 + 1 \cdot 9 = 11. $$

$$ {A_1}^{(3+4)} = {A_1}^{(3)} + \sum_{j=1}^{3} \left({b_j}^{(3)} {A_1}^{(3+j)} \right), $$

$$ {A_1}^{(7)} = {A_1}^{(3)} + {b_1}^{(3)} {A_1}^{(4)} + {b_2}^{(3)} {A_1}^{(5)} + {b_3}^{(3)} {A_1}^{(6)}, $$

$$ {A_1}^{(7)} = 0 + 1 \cdot 2 + 2 \cdot 9 + 3 \cdot 11 = 53. $$

$$ {A_1}^{(4+4)} = {A_1}^{(4)} + \sum_{j=1}^{3} \left({b_j}^{(4)} {A_1}^{(4+j)} \right), $$

$$ {A_1}^{(8)} = {A_1}^{(4)} + {b_1}^{(4)} {A_1}^{(5)} + {b_2}^{(4)} {A_1}^{6)} + {b_3}^{(4)} {A_1}^{(7)}, $$

$$ {A_1}^{(8)} = 2 + 1 \cdot 9 + 0 \cdot 11 + 2 \cdot 53 = 117. $$

De (3.2) e n entre 0 e 4 calcularemos os valores ${A_2}^{(n+4)}$.

$$ {A_2}^{(0+4)} = {A_2}^{(0)} + \sum_{j=1}^{3} \left({b_j}^{(0)} {A_2}^{(0+j)} \right), $$

$$ {A_2}^{(4)} = {A_2}^{(0)} + {b_1}^{(0)} {A_2}^{(1)} + {b_2}^{(0)} {A_2}^{(2)} + {b_3}^{(0)} {A_2}^{(3)}, $$

$$ {A_2}^{(4)} = 0 + 2 \cdot 0 + 3 \cdot 1 + 5 \cdot 0 = 3. $$

$$ {A_2}^{(1+4)} = {A_2}^{(1)} + \sum_{j=1}^{3} \left({b_j}^{(1)} {A_2}^{(1+j)} \right), $$

$$ {A_2}^{(5)} = {A_2}^{(1)} + {b_1}^{(1)} {A_2}^{(2)} + {b_2}^{(1)} {A_2}^{(3)} + {b_3}^{(1)} {A_2}^{(4)}, $$

$$ {A_2}^{(5)} = 0 + 4 \cdot 1 + 3 \cdot 0 + 4 \cdot 3 = 16. $$

$$ {A_2}^{(2+4)} = {A_2}^{(2)} + \sum_{j=1}^{3} \left({b_j}^{(2)} {A_2}^{(2+j)} \right), $$

$$ {A_2}^{(6)} = {A_2}^{(2)} + {b_1}^{(2)} {A_2}^{(3)} + {b_2}^{(2)} {A_2}^{(4)} + {b_3}^{(2)} {A_2}^{(5)}, $$

$$ {A_2}^{(6)} = 1 + 0 \cdot 0 + 1 \cdot 3 + 1 \cdot 16 = 20. $$

$$ {A_2}^{(3+4)} = {A_2}^{(3)} + \sum_{j=1}^{3} \left({b_j}^{(3)} {A_2}^{(3+j)} \right), $$

$$ {A_2}^{(7)} = {A_2}^{(3)} + {b_1}^{(3)} {A_2}^{(4)} + {b_2}^{(3)} {A_2}^{(5)} + {b_3}^{(3)} {A_2}^{(6)}, $$

$$ {A_2}^{(7)} = 0 + 1 \cdot 3 + 2 \cdot 16 + 3 \cdot 20 = 95. $$

$$ {A_2}^{(4+4)} = {A_2}^{(4)} + \sum_{j=1}^{3} \left({b_j}^{(4)} {A_2}^{(4+j)} \right), $$

$$ {A_2}^{(8)} = {A_2}^{(4)} + {b_1}^{(4)} {A_2}^{(5)} + {b_2}^{(4)} {A_2}^{6)} + {b_3}^{(4)} {A_2}^{(7)}, $$

$$ {A_2}^{(8)} = 3 + 1 \cdot 16 + 0 \cdot 20 + 2 \cdot 95 = 209. $$

De (3.2) e n entre 0 e 4 calcularemos os valores ${A_3}^{(n+4)}$.

$$
\begin{aligned}
{A_3}^{(0+4)} &= {A_3}^{(0)} + \sum_{j=1}^{3} \left({b_j}^{(0)} {A_3}^{(0+j)} \right), \\
{A_3}^{(4)} &= {A_3}^{(0)} + {b_1}^{(0)} {A_3}^{(1)} + {b_2}^{(0)} {A_3}^{(2)} + {b_3}^{(0)} {A_3}^{(3)}, \\
{A_3}^{(4)} &= 0 + 2 \cdot 0 + 3 \cdot 0 + 5 \cdot 1 = 5.
\end{aligned}
$$

$$
\begin{aligned}
{A_3}^{(1+4)} &= {A_3}^{(1)} + \sum_{j=1}^{3} \left({b_j}^{(1)} {A_3}^{(1+j)} \right), \\
{A_3}^{(5)} &= {A_3}^{(1)} + {b_1}^{(1)} {A_3}^{(2)} + {b_2}^{(1)} {A_3}^{(3)} + {b_3}^{(1)} {A_3}^{(4)}, \\
{A_3}^{(5)} &= 0 + 4 \cdot 0 + 3 \cdot 1 + 4 \cdot 5 = 23.
\end{aligned}
$$

$$
\begin{aligned}
{A_3}^{(2+4)} &= {A_3}^{(2)} + \sum_{j=1}^{3} \left({b_j}^{(2)} {A_3}^{(2+j)} \right), \\
{A_3}^{(6)} &= {A_3}^{(2)} + {b_1}^{(2)} {A_3}^{(3)} + {b_2}^{(2)} {A_3}^{(4)} + {b_3}^{(2)} {A_3}^{(5)}, \\
{A_3}^{(6)} &= 0 + 0 \cdot 1 + 1 \cdot 5 + 1 \cdot 23 = 28.
\end{aligned}
$$

$$
\begin{aligned}
{A_3}^{(3+4)} &= {A_3}^{(3)} + \sum_{j=1}^{3} \left({b_j}^{(3)} {A_3}^{(3+j)} \right), \\
{A_3}^{(7)} &= {A_3}^{(3)} + {b_1}^{(3)} {A_3}^{(4)} + {b_2}^{(3)} {A_3}^{(5)} + {b_3}^{(3)} {A_3}^{(6)}, \\
{A_3}^{(7)} &= 1 + 1 \cdot 5 + 2 \cdot 23 + 3 \cdot 28 = 136.
\end{aligned}
$$

$$
\begin{aligned}
{A_3}^{(4+4)} &= {A_3}^{(4)} + \sum_{j=1}^{3} \left({b_j}^{(4)} {A_3}^{(4+j)} \right), \\
{A_3}^{(8)} &= {A_3}^{(4)} + {b_1}^{(4)} {A_3}^{(5)} + {b_2}^{(4)} {A_3}^{6)} + {b_3}^{(4)} {A_3}^{(7)}, \\
{A_3}^{(8)} &= 5 + 1 \cdot 23 + 0 \cdot 28 + 2 \cdot 136 = 300.
\end{aligned}
$$

Pelo cálculos acima, temos:

$$A_0{}^{(5)} = 4;\ A_0{}^{(6)} = 5;\ A_0{}^{(7)} = 24;\ A_0{}^{(8)} = 53.$$

$$A_1{}^{(5)} = 9;\ A_1{}^{(6)} = 11;\ A_1{}^{(7)} = 53;\ A_1{}^{(8)} = 117.$$

$$A_2{}^{(5)} = 16;\ A_2{}^{(6)} = 20;\ A_2{}^{(7)} = 95;\ A_2{}^{(8)} = 209.$$

$$A_3{}^{(5)} = 23;\ A_3{}^{(6)} = 28;\ A_3{}^{(7)} = 136;\ A_3{}^{(8)} = 300.$$

Portanto o determinante determinante D_{4+1} é disposto da seguinte forma,

$$\begin{vmatrix} 4 & 5 & 24 & 53 \\ 9 & 11 & 53 & 117 \\ 16 & 20 & 95 & 209 \\ 23 & 28 & 136 & 300 \end{vmatrix} = -1.$$

Pelo Teorema 2.4 o vetor solução $x = (x_1, x_2, x_3, x_4)$, é obtido por $x_i = (-1)^{(4+1)(4-1)} \cdot B_{i,4}$, com $i = 1, \ldots, n$, em que em que $B_{i,4}$ são cofatores dos elementos da coluna 4 no determinante acima. Calculemos

$$x_1 = (-1)^{15} \cdot B_{1,4} = (-1) \cdot \begin{vmatrix} 9 & 11 & 53 \\ 16 & 20 & 95 \\ 23 & 28 & 136 \end{vmatrix} = 3.$$

$$x_2 = (-1)^{15} \cdot B_{2,4} = (-1) \cdot \begin{vmatrix} 4 & 5 & 24 \\ 16 & 20 & 95 \\ 23 & 28 & 136 \end{vmatrix} = 3.$$

$$x_3 = (-1)^{15} \cdot B_{3,4} = (-1) \cdot \begin{vmatrix} 4 & 5 & 24 \\ 16 & 20 & 95 \\ 23 & 28 & 136 \end{vmatrix} = -1.$$

$$x_4 = (-1)^{15} \cdot B_{4,4} = (-1) \cdot \begin{vmatrix} 4 & 5 & 24 \\ 9 & 11 & 53 \\ 16 & 20 & 95 \end{vmatrix} = -1.$$

Assim pelo Teorema 2.4 o vetor solução da equação diofantina padrão

$$53x_1 + 117x_2 + 209x_3 + 300x_4 = 1.$$

é dado por

$$x = (3, 3, -1, -1).$$

Assim, como último passo vemos que

$$53 \cdot 3 + 117 \cdot 3 + 209 \cdot (-1) + 300 \cdot (-1) = 1,$$

e portanto a resolução está feita.

3.2 Alguns exemplos usando o algoritmo

No estudo que nos levou a encontrar as soluções das equações diofantinas padrão vemos a construção de um algoritmo. Na seção anterior, mostramos o passo a passo deste algoritmo para encontrar a solução do exemplo proposto. Observamos que o algortimo construído foi proposto no fim da década de 60, onde os computadores estavam ainda no seu berço. Já na atualidade, onde os computadores já evoluíram em muito, não faz sentido fazer cálculos algoritmos de maneira manual. Assim sendo, como último esforço deste trabalho propomos a escrita desse algoritmo na linguagem de programa Phyton. O código está descrito no apêndice A. A escolha dessa linguagem se dá por ser um software livre e ter um grande uso no mundo atual. É claro que outra linguagem de programação poderia desempenhar o mesmo papel. No que segue, usaremos o algoritmo para calcular algumas soluções de equações diofantinas. Para acessar o código e resolver as equações sugerimos acessar o endereço eletrônico:
<https://github.com/JuscimarAraujo/diofantinas>.

Usando o Código 4 do apêndice A, obteremos o vetor solução da equação diofantina $53x_1 + 117x_2 + 209x_3 + 300x_4 = 1$, como segue.
Equação:

$$53x_1 + 117x_2 + 209x_3 + 300x_4 = 1$$

Quantidade de passos $n = 4$.
Matriz b do algoritmo:

$$b = \begin{bmatrix} 2 & 3 & 5 \\ 4 & 3 & 4 \\ 0 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 0 & 2 \end{bmatrix}$$

Matriz A do algoritmo:

$$A = \begin{bmatrix} 4 & 5 & 24 & 53 \\ 9 & 11 & 53 & 117 \\ 16 & 20 & 95 & 209 \\ 23 & 28 & 136 & 300 \end{bmatrix}$$

Solução encontrada:

$$[3, 3, -1, -1]$$

Verificação da solução:

$$53 * 3 + 117 * 3 + 209 * (-1) + 300 * (-1) = 159 + 351 - 209 - 300 = 1$$

Veja que a matriz b é formada pelos vetores obtidos em (3.2).

Usando o Código 4 do apêndice A, obteremos o vetor solução da equação diofantina $37x_1 + 89x_2 + 131x_3 + 401x_4 = 1$, como segue.
Equação:

$$37x_1 + 89x_2 + 131x_3 + 401x_4 = 1$$

Quantidade de passos n = 4
Matriz b do algoritmo:

$$b = \begin{bmatrix} 2 & 3 & 10 \\ 1 & 2 & 2 \\ 0 & 1 & 3 \\ 2 & 0 & 5 \end{bmatrix}$$

Matriz A do algoritmo:

$$A = \begin{bmatrix} 1 & 2 & 7 & 37 \\ 2 & 5 & 17 & 89 \\ 3 & 7 & 25 & 131 \\ 10 & 22 & 76 & 401 \end{bmatrix}$$

Solução encontrada:

$$[-6, -2, 0, 1]$$

Verificação da solução:

$$37 * (-6) + 89 * (-2) + 131 * 0 + 401 * 1 = -222 - 178 + 0 + 401 = 1$$

Do Teorema 2.2 e de (2.13) temos que a solução não é padrão, visto que uma das componentes do vetor solução é nula. Tomemos $p_1 = 2, p_2 = 3, p_3 = 5$ e $p_4 = 7$. Disso escrevemos $P = 2 \cdot 3 \cdot 5 \cdot 7$. Agora de (2.11) fazemos as seguintes mudanças de coordenadas

$$\begin{aligned} x_1^{'} &= 2 \cdot 3 \cdot 5 \cdot x_1 = 30 \cdot x_1 \\ x_2^{'} &= 2 \cdot 3 \cdot 7 \cdot x_2 = 42 \cdot x_2 \\ x_3^{'} &= 2 \cdot 5 \cdot 7 \cdot x_3 = 70 \cdot x_3 \\ x_4^{'} &= 3 \cdot 5 \cdot 7 \cdot x_4 = 105 \cdot x_4. \end{aligned}$$

Logo,

$$\begin{aligned} c_1 &= 2 \cdot 5 \cdot 7 \cdot 401 = 42105 \\ c_2 &= 2 \cdot 5 \cdot 7 \cdot 131 = 9170 \\ c_3 &= 2 \cdot 3 \cdot 7 \cdot 89 = 3738 \\ c_4 &= 2 \cdot 3 \cdot 5 \cdot 37 = 1110. \end{aligned}$$

Com isso obtemos a equação $1110x_1^{'} + 3738x_2^{'} + 9170x_3^{'} + 42105x_4^{'} = 1$, e, aplicando o algoritmo segue que

Equação:

$$1110x_1 + 3738x_2 + 9170x_3 + 42105x_4 = 1$$

Quantidade de passos $n = 7$
Matriz b do algoritmo:

$$b = \begin{bmatrix} 3 & 8 & 37 \\ 0 & 2 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \\ 29 & 17 & 54 \\ 1 & 1 & 2 \\ 1 & 0 & 2 \end{bmatrix}$$

Matriz A do algoritmo:

$$A = \begin{bmatrix} 3 & 272 & 552 & 1110 \\ 10 & 916 & 1859 & 3738 \\ 25 & 2247 & 4560 & 9170 \\ 114 & 10318 & 20939 & 42105 \end{bmatrix}$$

Solução encontrada:

$$[198, -23, -10, -1]$$

Verificação da solução:

$$1110*198+3738*(-23)+9170*(-10)+42105*(-1) = 219780-85974-91700-42105 = 1$$

Para obtermos a solução padrão da equação $73x_1 + 89x_2 + 131x_3 + 401x_4 = 1$, basta fazer

$$\begin{aligned} x_1 &= 30 \cdot 198 = 5940 \\ x_2 &= 42(-23) = -966 \\ x_3 &= 70 \cdot (-10) = -700 \\ x_4 &= 105 \cdot (-1) == -105. \end{aligned}$$

Solução encontrada:

$$[5940, -966, -700, -105]$$

Verificação da solução:

$$37*5940+98*(-966)+131*(-700)+401*(-105) = 219780-85974-91700-42105 = 1$$

Usando o Código 4 do apêndice A, obteremos o vetor solução da equação diofantina $41x_1 + 139x_2 + 543x_3 + 806x_4 = 1$, como segue.
Equação:

$$41x_1 + 139x_2 + 543x_3 + 806x_4 = 1$$

Quantidade de passos $n = 4$

Matriz b do algoritmo:

$$b = \begin{bmatrix} 3 & 13 & 19 \\ 0 & 1 & 2 \\ 1 & 0 & 1 \\ 9 & 6 & 10 \end{bmatrix}$$

Matriz A do algoritmo:

$$A = \begin{bmatrix} 1 & 2 & 2 & 41 \\ 3 & 7 & 7 & 139 \\ 13 & 26 & 27 & 543 \\ 19 & 39 & 40 & 806 \end{bmatrix}$$

Solução encontrada:

$$[-3, -1, -1, 1]$$

Verificação da solução:

$$41 * (-3) + 139 * (-1) + 543 * (-1) + 806 * 1 = -123 + (-139) + (-543) + 806 = 1$$

4 Considerações Finais

Nesse trabalho apresentamos alguns fatos históricos da Teoria dos Números e um estudo das equações diofantinas lineares padrões. Apresentamos ainda a construção de um código baseado no algoritmo modificado de Jacobi-Perron, que permite obtermos o vetor solução desse tipo especial de equação.

Aliando os conceitos e a teoria até então disponível e usando o programa Python versão 3.7, pudemos obter um código que simplica a solução das equações diofantinas de ordem superior, caso $n = 4$.

Com este trabalho buscamos apresentar uma abordagem computacional para as equações diofantinas lineares padrões, sem nenhuma pretenção em exaurir o tema abordado, deixando como motivação a ideia em desenvolver códigos que abordem outras ordens de tais equações.

Referências

ALENCAR, F. E. ***Teoria Elementar dos Números***. [S.l.: s.n.]. Citado na página 19.

BERNSTEIN, l. ***History of Continued Fractions and Pade Approximants***. [S.l.: s.n.]. Citado 3 vezes nas páginas 30, 40 e 52.

BERNSTEIN, L. ***The Modified Algorithm of Jacobi-Perron***. [S.l.: s.n.]. Citado na página 30.

BICUDO, I. ***Os elementos***. [S.l.: s.n.]. Único. Citado na página 22.

BOYER, C. B. ***História da matemática***. [S.l.: s.n.]. Citado 3 vezes nas páginas 14, 15 e 23.

BREZINSKI, C. ***The Jacobi-Perron Algorithm, Its Theory and Aplication***. [S.l.: s.n.]. Citado na página 30.

BURTON, D. M. ***Elementary Number Theory***. [S.l.: s.n.]. Citado na página 14.

CAJORI, F. ***Uma História da Matemática***. [S.l.: s.n.]. Citado 2 vezes nas páginas 14 e 23.

CAMPOS, G. D. M. ***Equações Diofantinas Lineares***. Dissertação(Mestrado Profissional em Matemática). Citado na página 25.

DOMINGUES, H. H. ***Álgebra moderna***. [S.l.: s.n.]. Único. Citado na página 15.

EVES, H. ***Introdução à história da matemática***. [S.l.: s.n.]. Citado 2 vezes nas páginas 14 e 23.

FIORELLI, J. O. ***Máximo divisor comum e mínimo múltiplo comum generalizados aplicados no ensino básico***. Dissertação(Mestrado Profissional em Matemática). Citado na página 20.

FONSECA, R. V. F. ***Teoria dos Números***. [S.l.: s.n.]. Citado 3 vezes nas páginas 14, 25 e 26.

HEFEZ, A. *Curso de Álgebra*. [S.l.: s.n.]. Citado na página 14.

_____. ***Elementos de Aritmética***. [S.l.: s.n.]. Citado na página 14.

LEVEQUE, W.J. ***Topics in Number Theory***. [S.l.: s.n.]. v. 1. Citado na página 14.

LOVÁSZ, L.; PELIKÁN, J; VESZTERGOMBI, K. ***Matemática Discreta***. [S.l.: s.n.]. Citado na página 14.

MARTINEZ, F. et al. ***Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro***. [S.l.: s.n.]. Citado 2 vezes nas páginas 19 e 20.

NETO, A. C. M. ***Teoria dos Números***. [S.l.: s.n.]. Citado na página 28.

_____. ***Tópicos de Matemática Elementar: Teoria dos Números***. [S.l.: s.n.]. Citado na página 14.

NIVEN, I.; ZUCKERMAN, H.S. ***An Introducion to the Theory of Numbers***. [S.l.: s.n.]. Citado na página 14.

OSKAR, P. ***Grundlagen fuer eine Theorie des Jacobischen Kettenbruchalgorithmus, 64***. [S.l.: s.n.]. Citado 2 vezes nas páginas 30 e 40.

SANTOS, J. P. O. ***Introdução à Teoria dos Números***. [S.l.: s.n.]. Citado na página 14.

SOUZA, R. S. ***Equações Diofantinas Lineares, Quadráticas e Aplicações***. type. Citado na página 14.

APÊNDICE A - Projeto Computacional

Com os resultados descritos nos Capítulos 1 e 2, foram feitos através de um programa computacional chamado Python, um código para obter soluções numéricas de algumas equações diofantinas.

Os códigos foram testados em ambientes com sistemas operacionais Windows10 e Linux Ubuntu 16.04 LTS e podem ser copiados da versão digital em PDF deste documento e podem ser inseridos no programa Python.

Os códigos também estão publicados na Internet pela ferramenta GitHub, podendo serem copiados ou mesmo feito o download, permitindo assim visualizar os arquivos criados com o Python, inclusive sendo possível fazer colaboração e/ou editá-los.

Para acessar o código, consultar <https://github.com/JuscimarAraujo/diofantinas>.

Seção A.1

Código-fonte 1 – Código Restrições

```
import prime
import sys

initial_numbers=[0, 37, 89, 131, 401]

class Restricted:

    """
        Verifica as restricoes.
    """

    def __init__(self, argv):
        if len(argv) == 1:
            argv = initial_numbers

        self.args = argv[1:] # valores recebidos tipo string

    def change_int_numbers(self):
        """
```

```
            Modifica os valores recebidos.
        """
        try:
            lst = []
            for num in self.args:
                _num = int(num)
                if _num > 0:
                    lst.append(_num) # lista de numeros
                       inteiros

        except BaseException as error:
            raise(error)

        return lst

    def ordered(self):
        """
            Retora a lista de numeros em ordem crescente.
        """
        return sorted(self.change_int_numbers())


    def max_number(self):
        """
            Retorna o maior valor inserido na lista de
               numeros.
        """
        return max(self.change_int_numbers())

    def take_numbers(self):
        """
            Retorna os numeros inseridos e verificados
            nas condicoes.
        """
        if self.is_prime():
            return self.ordered()

        return []
```

```
    def is_prime(self):
        """
            Retorna verdadeiro se sao numeros primos
            ou primos entre si
        """

        resp = True
        for i in range(len(self.ordered())):
            for j in self.ordered()[i+1:]:
                if not prime.verify_prime_between_numbers(
                self.ordered()[i],j):
                    resp = False

        if not resp:
            return False

        return True

if __name__ == "__main__":
    arg = Restricted(sys.argv)
    print(arg.take_numbers())
```

Código-fonte 2 – Código Coeficientes.

```
importar  numpy  como  np

"""
    Cria lista de numeros primos e verifica se um numero e
       primo.
"""
def verify_prime_between_numbers(a, b):

    try:
        _a = int(a)
        _b = int(b)

    except:
        raise BaseException

    if _a > _b:
```

```
        resp = _a % _b

    elif _a < _b:
        resp = _b % _a

    else:
        return False

    if resp == 0:
        return False

    return True

def verify_prime(num):
    """
        Verifica se o numero recebido em numero e primo.
    """

    if num > 2:
        for count in range(2,num):
            if num % count == 0:
                return False

    return True

def create_prime_number_list(num):
    """
        Retorna a lista de numeros primos
        menores que o numero recebido em num
    """

    _lst_prime = [] # lista de primos
    n = 2
    _num = num

    try:
        if isinstance(num, list):
            _num = max(num)
        elif isinstance(num, int) or isinstance(num, float):
```

```
            _num = int(num)
        elif isinstance(num, dict):
            _num = int(max(num.values()))
    except BaseException as error:
        raise(error)

    while n < _num+1:
        if verify_prime(n):
            _lst_prime.append(n)

        n = n + 1

    return _lst_prime

if __name__ == "__main__":
    n = []
    i = 1
    resp = input("Verificar se dois numeros sao primos entre
       si? ")
    if resp == "sim" or resp == "s" or resp == "yes" or resp
       == "y":
        a = input("Primeiro Numero: ")
        b = input("Segundo Numero: ")

        if verify_prime_between_numbers(a,b):
            print("{} e {} s o primos entre si".format(a,b))
        else:
            print("{} e {} n o s o primos entre si".format(
               a,b))
    else:
        print(
        "Criar uma lista de numeros para saber se sao primos"
           )
        while True:
            try:
                tmp = int(input("insira o {}   numero ".
                   format(i)))
            except:
                break
```

```
            n.append(tmp)
            i = i+1

        print('{} sao os numeros inseridos'.format(n))
        for i in n:
            print(
            "{}    numero primo? {}".format(i, verify_prime(i
               )))

        print(
        "tabela primos menores que {}: {}".format(
        max(n), create_prime_number_list(max(n))))
```

Código-fonte 3 – Código Matriz

```
"""
    Funcoes auxiliares para o calculo das equacoes
       diofantinas
"""
import numpy as np

def vec(numbers): # vetor formado por numeros tipo int

    vec = [] # vetor b
    vec_a = [] # vetor a

    tmp = [] # entradas para o vetor vec
    tmp_a = [] # entradas para o vetor vec_a

    for i in numbers[1:]:
        num = divmod(i,numbers[0])
        tmp.append(num[0])
        tmp_a.append(num[1])

    vec.append(tmp)
    vec_a.append(tmp_a)

    i=0
    while vec_a[i][0] != 0:
```

```
        tmp = [] # entradas para o vetor vec
        tmp_a = [] # entradas para o vetor vec_a
        for j in range(1,len(numbers)-1):
            calc = divmod(vec_a[i][j],vec_a[i][0])
            tmp.append(calc[0])
            tmp_a.append(calc[1])

        if i == 0:
            calc = divmod(numbers[0],vec_a[i][0])
        else:
            calc = divmod(vec_a[i-1][0],vec_a[i][0])

        tmp.append(calc[0])
        tmp_a.append(calc[1])
        vec.append(tmp)
        vec_a.append(tmp_a)
        i=i+1

    return np.array(vec)

def matrix(b, n=4):
    """
        Retorna o calculo da matriz A
        A_i^(v+n) = A_i^(v) + Sum_(j=1)^(n-1) [b_j^(v)*A_i^(v
           +j)]
        order = n
        valores de entrada:
        b = matriz b de valores
        n = ordem
    """
    lin_b = b.shape[0] # obtendo a quantidade de linhas da
       matriz b

    # Contruindo a matrix A[order, order + lin_b]
    m = np.eye(n, dtype=int) # bloco de matriz identidade
    de ordem B[order, order]
    m = np.c_[m, np.zeros((n, lin_b), dtype=int)]
    #um segundo bloco de matriz nula de ordem B[order, lin_b]
```

```
    for i in range(n): # linhas
        for v in range(lin_b): # colunas
            calc = m[i][v]
            for j in range(n-1): # j do trabalho
                calc = calc + b[v][j] * m[i][v+j+1]

            m[i][v+n] = calc

    m = np.delete(m, np.s_[0:-n], axis=1)
    # retirando as primeiras colunas, mantendo as n ultimas

    return m

def cofactor(A, lc =(0,0)):

    newMatrix = np.delete(A, lc[0], axis=0)
    newMatrix = np.delete(newMatrix, lc[1], axis=1)

    return newMatrix


if __name__ == "__main__":
    # initial_numbers=[37, 89, 131, 401] # para teste da
       funcao vec

    # para teste da funcao matrix
    # initial_numbers = np.array(
    #[[2,3,5],[4,3,4],[0,1,1],[1,2,3],[1,0,2]])
    #initial_numbers = np.array(
    #[[2, 3, 10], [1, 2, 2], [0, 1, 3], [2, 0, 5]])
    print(matrix(initial_numbers, 4))
```

Código-fonte 4 – Código Solução

```
import sys
import math
import time
import numpy as np
import auxiliar as aux
```

```
import pylatex

from restricted import Restricted

initial_first_numbers = [0, 37, 89, 131, 401]
initial_second_numbers = [0, 53, 117, 209, 300]

"""
    sequencia para os novos calculos
    aux = lista.pop(0) -> exclui o primeiro elemento
    lista.append(aux) -> inserir o elemento
"""


class Diofante:

    def __init__(self, argv):
        """
            Inicializacao:
            argv = numeros a serem trabalhados
            como parametro recebe uma
            quantidade de numeros inteiros, gerando
            uma lista a ser trabalhada, e caso nao
            receba nenhuma sequencia de numeros interios, a
            inicializacao da classe sera feita
            automaticamente com a sequencia de numeros
            0, 37, 89, 131, 401
            comandos anexados:
            -s = utiliza automaticamente a
            sequencia de numeros
            0, 53, 117, 209, 300
            -l = apresenta os dados finais
            em um arquivo .tex
            pdf = cria o arquivo .pdf gerado
            pelo arquivo .tex
        """

        self.in_latex = False
        if "-l" in argv:
```

```
            self.in_latex = True
            argv.remove('-l')
            self.create_pdf = False
            if "pdf" in argv:
                self.create_pdf = True
                argv.remove('pdf')

        initial_numbers = initial_first_numbers
        if '-s' in argv:
            initial_numbers = initial_second_numbers
            argv.remove('-s')

        self.with_time = False
        if '-t' in argv:
            self.initial_time = time.time()
            self.with_time = True
            argv.remove("-t")

        if len(argv) == 1:
            argv = initial_numbers

        args = Restricted(argv)
        self.numbers = args.take_numbers()
        self.order = len(self.numbers)

    def take_vec(self):
        """
            Cria e retorna a matriz b de valores inteiros
        """
        vec = aux.vec(self.numbers)

        return vec

    def take_matrix(self):
        """
            Cria e retorna a matriz A de valores
        """
        matrix = aux.matrix(self.take_vec(), self.order)
```

```
        return matrix

    def det_matrix(self):
        """
            Retorna o determinante da matriz self.take_matrix
               ()
        """
        return np.linalg.det(self.take_matrix())

    def cofactor_matrix(self):
        """
            Retorna a matriz cofatora
        """
        resp = []
        len_b = len(self.take_vec())
        for i in range(self.order):
            _matrix = aux.cofactor(self.take_matrix(),
                    (i, self.order-1)
                )
            _resp = math.pow(-1, len_b-1)
            _resp = _resp * np.linalg.det(_matrix)
            _resp = _resp * math.pow(-1, i * (self.order-1))
            resp.append(int(round(_resp)))

        return resp

    def print_latex(self):
        """
            Gerador de arquivos .tex e .pdf
        """

        pdf = pylatex.Document(
            "default"
        )

        with pdf.create(pylatex.Section(
                "Equa  es Diofantinas"
        )) as section:
```

```
            section.append("Equa   o:")
            ultimo = self.numbers[-1]
            eq = []
            cont = 1
            for i in self.numbers:
                simbolo = "+"
                if i == ultimo:
                    simbolo = "= 1"
                eq.append(
                    pylatex.NoEscape(
                        " {}x_{} {}".format(i, cont, simbolo)
                    )
                )
                cont = cont + 1

            section.append(pylatex.Math(data=eq))

            text = "n = {}".format(self.order)
            section.append(text)

            m = pylatex.Matrix(self.take_vec(), mtype='b')
            matrix = pylatex.Math(data=['b = ', m])
            section.append(matrix)

            m = pylatex.Matrix(self.take_matrix(), mtype='b')
            matrix = pylatex.Math(data=['A = ', m])
            section.append(matrix)

            section.append(
            "Resposta = {}".format(self.cofactor_matrix()))

            section.append(pylatex.LineBreak())
            section.append("Confirmando:")
            section.append(pylatex.LineBreak())
            s = 0
            for i in range(len(self.numbers)):
                r = self.numbers[i] * self.cofactor_matrix()[
                   i]
                s = s + r
```

```
                resp =
                "\t {}\t{} \t* \t{} \t= \t{} \t({})\n".format
                   (
                    i,
                    self.numbers[i],
                    self.cofactor_matrix()[i],
                    r,
                    s
                )
                section.append(resp)

        if self.create_pdf:
            pdf.generate_pdf()

        pdf.generate_tex()

    def show(self):
        '''
            Apresenta os resultados, exibindo-os na tela ou
            em arquivo .tex
        '''

        if self.in_latex:
            self.print_latex()

        else:
            resp = "numeros = {}\n".format(self.numbers)
            resp = resp + "n = {}\n".format(self.order)

            resp = resp + "\nb =\n{}\n\nA =\n{}\n".format(
                self.take_vec(),
                self.take_matrix(),
            )
            resp = resp + "Resposta =\n{} \n".format(
            self.cofactor_matrix())
            resp = resp + "Confirmando: \n"
            s = 0
            for i in range(len(self.numbers)):
                r = self.numbers[i] * self.cofactor_matrix()[
```

```
                    i]
                s = s + r
                resp = resp + "{} * {} = {} ({})\n".format(
                    self.numbers[i],
                    self.cofactor_matrix()[i],
                    r,
                    s
                )

            print(resp)

        if self.with_time:
            print("Tempo de execucao: {}".format(
            time.time() - self.initial_time))

if __name__ == '__main__':
    t = Diofante(sys.argv)
    t.show()
```