



**INSTITUTO FEDERAL DA PARAÍBA  
CAMPUS CAJAZEIRAS  
CURSO DE LICENCIATURA EM MATEMÁTICA**

**LARISSA SOARES DE SOUSA**

**APLICAÇÕES DO ALGORITMO DE EUCLIDES**

**CAJAZEIRAS**

**2022**

LARISSA SOARES DE SOUSA

APLICAÇÕES DO ALGORITMO DE EUCLIDES

Monografia apresentada junto ao **Curso de Licenciatura em Matemática** do **Instituto Federal da Paraíba**, como requisito à obtenção do título de **Licenciado em Matemática**.

**Orientador:**

Prof. Dr. Vinicius Martins Teodosio Rocha.

**Coorientadora:**

Profa. Ma. Kissia Carvalho.

Cajazeiras

2022

LARISSA SOARES DE SOUSA

## APLICAÇÕES DO ALGORITMO DE EUCLIDES

Monografia apresentada ao programa de **Curso de Licenciatura em Matemática** do **Instituto Federal da Paraíba**, como requisito à obtenção do título de **Licenciado em Matemática**.


Data de aprovação: 05/05/2022

Banca Examinadora:



---

**Prof. Dr. Vinicius Martins Teodosio Rocha**  
Instituto Federal da Paraíba - IFPB

Documento assinado digitalmente  
 KISSIA CARVALHO  
Data: 16/05/2022 11:56:29-0300  
Verifique em <https://verificador.iti.br>


---

**Profa. Ma. Kissia Carvalho**  
Instituto Federal da Paraíba - IFPB



---

**Prof. Me. José Doval Nunes Martins**  
Instituto Federal da Paraíba - IFPB

Documento assinado digitalmente  
 REGINALDO AMARAL CORDEIRO JUNIOR  
Data: 17/05/2022 18:05:35-0300  
Verifique em <https://verificador.iti.br>

---

**Prof. Me. Reginaldo Amaral Cordeiro Junior**  
Instituto Federal da Paraíba - IFPB

IFPB / Campus Cajazeiras  
Coordenação de Biblioteca  
Biblioteca Prof. Ribamar da Silva  
Catalogação na fonte: Suellen Conceição Ribeiro CRB-2218

S725a Sousa, Larissa Soares de

Aplicações do algoritmo de Euclides / Larissa Soares de Sousa. –  
Cajazeiras/PB: IFPB, 2022.

68f.:il.

Trabalho de Conclusão de Curso (Graduação em Matemática) - Instituto  
Federal de Educação, Ciência e Tecnologia da Paraíba-IFPB, Campus  
Cajazeiras. Cajazeiras, 2022.

Orientador(a): Prof. Dr. Vinicius Martins Teodosio Rocha; Coor.: Profa.  
Ma. Kissia Carvalho.

1. Matemática. 2. Algoritmo. 3. Euclides.

I. Sousa, Larissa Soares de. II. Título.

CDU: 51 S725a

*Dedico este trabalho a minha família, em especial minha mãe Lindalva Soares de Sousa, que sempre acreditou em mim e fez tudo o que podia para que eu realizasse os meus sonhos.*

## AGRADECIMENTOS

Agradeço a Deus, por toda força, sabedoria e saúde para enfrentar todos os obstáculos que surgiram durante toda minha trajetória na vida e no curso de Licenciatura em Matemática. Sem Ele eu nada seria.

Aos meus pais, Lindalva Soares de Sousa e Eduardo Soares de Sousa, por todo amor, incentivo e força durante toda minha vida, principalmente nesses últimos quatro anos. É por vocês que eu nunca desisto, mesmo com todas as dificuldades que surgem em minha vida.

Aos meus irmãos Willian Soares de Sousa, Kelma Kercia Soares de Sousa, Francisco Wlises Soares de Sousa, Luzia Soares de Sousa e Kaike Soares de Sousa, por todo apoio emocional quando eu mais precisei e por entenderem minha ausência em muitas reuniões de família enquanto eu estava estudando.

Aos meus sobrinhos Sávio, Dafne, Guilherme e Arthur por todos os momentos de alegria que vocês proporcionam em minha vida.

Ao meu companheiro Abner, por todo amor, incentivo e ajuda nos meus momentos mais difíceis.

A todos os meus colegas de curso, por terem feito desses quatro anos memórias que nunca irei esquecer. Guardarei vocês para sempre em meu coração.

Ao meu grande amigo José Jorge, colega de curso e irmão que a vida me deu, por ter enfrentado todos os momentos difíceis e felizes ao meu lado.

Aos meus orientadores Prof. Dr. Vinicius Martins Teodósio Rocha e Profa. Ma. Kissia Carvalho, por toda dedicação, paciência, conselhos e ideias durante a realização deste trabalho.

Aos membros da banca examinadora, Prof. Me. José Doval Nunes Martins e Prof. Me. Reginaldo Amaral Cordeiro Junior, pela disposição e pela contribuição com este trabalho.

À toda comunidade do IFPB, campus Cajazeiras, professores e demais funcionários, por toda contribuição em todos esses anos.

A todos que contribuíram, diretamente ou indiretamente, para que eu conseguisse chegar até aqui.

*“Não venci todas as vezes que lutei, mas perdi todas as vezes que deixei de lutar.”*

**Cecília Meireles**

## RESUMO

O Algoritmo de Euclides (AE), é um método de divisões sucessivas que permite encontrar o Máximo Divisor Comum (MDC) entre dois ou mais números inteiros. Embora o AE seja um procedimento simples e que é visto nas escolas de ensino básico, percebe-se que seu uso acaba ficando restrito muitas vezes à encontrar o MDC entre dois ou mais números inteiros, não sendo abordadas outras de suas possibilidades. Com isso, o presente trabalho tem a seguinte questão norteadora: Existem outras aplicações do AE para além do cálculo de MDC? Dito isto, o objetivo deste trabalho é compreender o desenvolvimento do AE e algumas de suas aplicações. Desse modo, para alcançar esse objetivo, recorreremos à uma pesquisa bibliográfica de abordagem qualitativa, caráter exploratório e de natureza básica, onde foi possível concluir que sim, há outras aplicações do AE fora o cálculo de MDC. Entre essas aplicações, abordamos no nosso trabalho como o AE pode auxiliar na busca de soluções de Equações Diofantinas Lineares. Uma outra aplicação que discutimos foi sobre sua contribuição para encontrar aproximações em frações contínuas para números racionais. Por fim, discutimos como o AE pode ser aplicado para escrever números primos da forma  $4k + 1$  como soma de quadrados perfeitos. Contudo, mesmo havendo outras aplicações do AE, concluímos que cumprimos com o objetivo geral deste trabalho, dado que conseguimos compreender o desenvolvimento do AE e de suas aplicações.

**Palavras-chave:** Algoritmo de Euclides; Aplicações; Matemática; Teoria dos números.



## ABSTRACT

The Euclidean Algorithm (EA) is a method for computing the greatest common divisor (GCD) of two integers by doing successive long divisions. Even though, the EA consists of a simple mechanism, often learned on high school, we notice that its use is regularly restricted to find the GCD between two or more integers, while its other possibilities are neglected. By these means, this work has the following leading question: Are there other applications for the EA beyond the GCD calculation? The goal of this text is to understand the development of the EA and some of its applications. In order to attain this objective, we overtook a bibliographical research, with a qualitative approach along which we concluded that there are other usages of the EA. Among these applications, we show how the EA can be used in the analysis of Linear Diophantine Equations. Another application found is its contribution to the construction of continued fractions for rational numbers. Finally, we discuss how the EA can be used to write primes of the form  $4k + 1$  as a sum of perfect squares. We thereby conclude that the goal was attained, since we managed to expose the EA and its applications.

**Keywords:** Euclidean Algorithm; Applications; Mathematics; Number Theory.

## LISTA DE FIGURAS

|  |    |
|--|----|
| Figura 1.1 – Euclides de Alexandria . . . . .  | 19 |
| Figura 1.2 – Fragmento de Elementos encontrado em <i>Oxyrhynque</i> , no Egito . . . . . | 20 |
| Figura 1.3 – Segmentos Iniciais . . . . .  | 33 |
| Figura 1.4 – Destacando o Segmento Menor . . . . .                                       | 33 |
| Figura 1.5 – Subtraindo $\overline{AB}$ de $\overline{CD}$ . . . . .                     | 33 |
| Figura 1.6 – Resultado de $\overline{AB} - \overline{ED}$ . . . . .                      | 34 |
| Figura 1.7 – Resultado de $\overline{FB} - \overline{ED}$ . . . . .                      | 34 |
| Figura 1.8 – Resultado de $\overline{ED} - \overline{GB}$ . . . . .                      | 34 |
| Figura 1.9 – Resultado de $\overline{GB} - \overline{HD}$ . . . . .                      | 34 |
| Figura 1.10–Retângulo de Dimensões $20 \times 12$ . . . . .                              | 35 |
| Figura 1.11–Preenchendo o Retângulo com um Quadrado de Lado Igual a 12 . . . . .         | 36 |
| Figura 1.12–Preenchendo o Retângulo com um Quadrado de Lado Igual a 8 . . . . .          | 36 |
| Figura 1.13–Preenchendo o Retângulo com dois Quadrados de Lados Iguais a 4 . . . . .     | 37 |
| Figura 1.14–Representação Geométrica do mdc entre 15 e 4 . . . . .                       | 38 |
| Figura 1.15–Representação geométrica do mdc entre 13 e 8 . . . . .                       | 40 |
| Figura 1.16–Representação geométrica do mdc entre 21 e 13 . . . . .                      | 41 |
| Figura 1.17–Representação geométrica do mdc entre 34 e 21 . . . . .                      | 42 |
| Figura 2.1 – Soluções inteiras e não negativas da equação $3x + 6y = 30$ . . . . .       | 50 |
| Figura 2.2 – Reta determinada pela equação $15x + 18y = 4$ . . . . .                     | 51 |

# SUMÁRIO

|   |           |
|---|-----------|
| INTRODUÇÃO . . . . .  | 16        |
| <b>1</b> <b>ALGORITMO DE EUCLIDES . . . . .</b>                     | <b>19</b> |
| 1.1 <b>Contexto Histórico . . . . .</b>                             | <b>19</b> |
| 1.2 <b>Conceitos Preliminares . . . . .</b>                         | <b>21</b> |
| 1.2.1    Divisibilidade em $\mathbb{Z}$ . . . . .                   | 21        |
| 1.2.2    O Algoritmo da Divisão . . . . .                           | 24        |
| 1.2.3    Máximo Divisor Comum . . . . .                             | 25        |
| 1.2.4    Decomposição em Fatores Primos . . . . .                   | 26        |
| 1.2.5    Congruência . . . . .                                      | 28        |
| 1.3 <b>O Algoritmo . . . . .</b>                                    | <b>29</b> |
| 1.4 <b>Interpretação Geométrica . . . . .</b>                       | <b>32</b> |
| 1.5 <b>Uma Comparação com a Fatoração . . . . .</b>                 | <b>42</b> |
| <b>2</b> <b>APLICAÇÕES . . . . .</b>                                | <b>45</b> |
| 2.1 <b>Equações Diofantinas Lineares . . . . .</b>                  | <b>45</b> |
| 2.2 <b>Frações Contínuas . . . . .</b>                              | <b>51</b> |
| 2.2.1    Uma Breve Contextualização . . . . .                       | 52        |
| 2.2.2    O AE aplicado à Frações Contínuas . . . . .                | 53        |
| 2.3 <b>Soluções da Equação <math>p = a^2 + b^2</math> . . . . .</b> | <b>65</b> |
| REFERÊNCIAS . . . . .   | 71        |

## INTRODUÇÃO

Euclides (325 a.C. - 265 a.C.) foi um matemático da cidade de Alexandria, no Egito, que muito contribuiu para diversas áreas da Matemática (CHAQUIAM, 2017). Sua obra mais famosa é “Elementos”, composto por 13 livros que discutem sobre Geometria Plana, Aritmética e Geometria Espacial. Precisamente nos livros VII-X são apresentadas proposições acerca de Teoria dos Números. No livro VII, especificamente, Euclides apresenta o que é conhecido hoje como Algoritmo de Euclides (AE), o método de divisões sucessivas que permite encontrar o Máximo Divisor Comum (mdc) entre dois ou mais números inteiros.

Embora o AE seja um procedimento simples e que é incorporado nas escolas de ensino básico, percebe-se que seu uso acaba ficando restrito muitas vezes à encontrar o mdc entre dois ou mais números inteiros, não sendo abordadas outras de suas possibilidades. Dessa forma, reconhecendo essa problemática, a motivação principal do presente trabalho veio da minha admiração pela disciplina de Teoria dos Números, onde me identifiquei principalmente com os assuntos que tangem à Divisibilidade. Aliado à isso, outro fator que me motivou foi ter conhecido uma aplicação do AE e ter percebido que haviam outras possibilidades além das que eu já conhecia, embora não fossem tão exploradas como o cálculo do mdc.

Nessa ótica, o presente trabalho pode servir de referência para professores da disciplina de Teoria dos Números que pretendem abordar outras aplicações do AE além do cálculo de mdc. Ademais, pode ser uma boa alternativa para alunos da referida disciplina que queiram estudar sobre aplicações do AE, já que o trabalho apresenta uma linguagem simples, direta e com bastante exemplos. Dessa forma, na tentativa de ampliar o reconhecimento do AE e de suas potencialidades, pretendemos fazer a seguinte investigação: **Existem outras aplicações do Algoritmo de Euclides para além do cálculo de mdc?**

Acreditamos que seja possível demonstrar e aplicar o AE de uma forma intuitiva, mostrando que esse resultado está presente em outros conteúdos matemáticos de forma natural. Dito isto, o objetivo deste trabalho é compreender o desenvolvimento do AE e algumas de suas aplicações. Para isso, pretendemos contextualizar historicamente o AE, uma vez que desejamos compreender o seu desenvolvimento desde seu surgimento. Além disso, planejamos também apresentar o AE de forma algébrica e geométrica, onde veremos diferentes perspectivas do algoritmo. E, por fim, apresentar aplicações do AE diferentes do cálculo de mdc.

Dessa forma, recorreremos a uma pesquisa de caráter qualitativa, e de natureza básica, pois busca o aprofundamento em um determinado conteúdo. Sendo assim, foi realizada uma pesquisa bibliográfica exploratória, bibliográfica porque a pesquisa foi desenvolvida com base em materiais que já existiam, e exploratória, pois buscava uma maior familiaridade com o problema (GIL, 2002). A coleta de dados foi realizada fazendo uso de livros e de base de dados como BDTD, Google Acadêmico, repositórios de universidades e anais de congressos para busca de artigos e demais trabalhos acadêmicos.

Em um primeiro momento foi realizada uma leitura da obra “Elementos”, com a finalidade de entender como o algoritmo foi descrito por Euclides em sua época. Posteriormente, iniciamos a busca por referências dos principais tópicos de divisibilidade, máximo divisor comum, fatoração e congruência aritmética, com o objetivo de introduzir os conhecimentos básicos e necessários para o trabalho. Em seguida, buscamos referências sobre aplicações do AE, no qual escolhemos as aplicações que mostraríamos em nosso trabalho. É válido ressaltar que optamos por omitir algumas das demonstrações para manter o trabalho conciso, focando apenas na parte algorítmica/prática das aplicações, mostrando como elas funcionam e como utilizam o AE. Além disso, usamos a plataforma *sagemath* para realizar cálculos que exigiam muito trabalho.

Em alguns pontos deste trabalho mencionamos a efetividade com a qual computadores conseguem resolver determinados problemas. A formalização de tal discussão é amparada pela Teoria da Complexidade Computacional, responsável por classificar problemas com base na sua dificuldade. Não é o nosso objetivo adentrar numa discussão sobre a Teoria da Complexidade Computacional, mas como citamos algumas vezes no decorrer deste trabalho sobre a efetividade computacional dos algoritmos, é necessário frisar que quando estamos falando sobre a dificuldade ou tempo que o computador leva para resolver algum problema, estamos falando dos recursos necessários para isso, podendo ser tempo, armazenamento, quantidade de comunicações, entre outros (WIKIPÉDIA, 2019).

Em nossas pesquisas, ficou evidente como a maioria das referências que discutiam sobre as aplicações do AE traziam uma linguagem mais técnica e que rapidamente iam para um nível mais abstrato de compreensão. Assim, esperamos que este trabalho possa contribuir para que professores, alunos da disciplina de Teoria dos Números e todos que se interessam pelo estudo do AE encontrem um material com uma linguagem mais simples acerca do AE e suas aplicações. Desejamos também que esse trabalho contribua para a desmistificação de que o AE serve apenas para o cálculo de mdc, ampliando os conhecimentos do leitor, principalmente daqueles que irão em algum momento ensinar sobre o AE.

Desse modo, iniciamos esse trabalho fazendo uma contextualização histórica da

vida de Euclides, da obra Elementos e do AE. Além disso, para que o leitor compreendesse o restante do trabalho, apresentamos uma revisão dos conteúdos de Teoria dos Números. Ademais, apresentamos o AE de forma algébrica e geométrica, além da sua comparação com o método de fatoração para cálculo do mdc entre números inteiros. Posteriormente, mostramos como o AE pode auxiliar na busca de soluções para Equações Diofantinas Lineares. Em seguida, discutimos como o AE pode ser aplicado à teoria de Frações Contínuas. Por fim, discutimos brevemente como o AE pode auxiliar para escrever primos da forma  $4k + 1$  como soma de quadrados perfeitos.

# 1 ALGORITMO DE EUCLIDES

Este Capítulo tem como finalidade, essencialmente, apresentar o Algoritmo de Euclides ao leitor. Sendo assim, serão abordados, inicialmente, aspectos históricos do Algoritmo de Euclides, seguido da apresentação de alguns conceitos preliminares que embasam o Capítulo 2 deste trabalho, servindo como revisão ou apresentação de tópicos de Teoria dos Números. Posteriormente, será mostrada a representação geométrica do Algoritmo de Euclides e, por fim, discutiremos brevemente sobre as diferenças entre o Algoritmo de Euclides e o método de fatoração para encontrar o máximo divisor comum entre dois números.

## 1.1 CONTEXTO HISTÓRICO

Euclides de Alexandria foi um importante matemático grego que contribuiu para diversas áreas da Matemática, principalmente para a Geometria. Segundo (ROQUE, 2012) há poucas informações sobre a vida de Euclides, não é comprovado ao menos que ele nasceu em Alexandria, entretanto, (CHAQUIAM, 2017) afirma que há relatos que ele viveu entre 325 a.C. e 265 a.C.

**Figura 1.1 – Euclides de Alexandria**



**Fonte: Ebiografia, 2021**

Os Elementos, famoso documento escrito por Euclides por volta do ano 300 a.C., é composto por treze livros que apresentam resultados de Geometria Plana, Aritmética e Geometria Espacial, sendo dividido da seguinte forma:

- Geometria Plana: Livros I – VI;
- Aritmética: Livros VII – X;
- Geometria Espacial: Livros XI – XIII.

Apesar de ser uma obra que muito contribuiu com a Matemática, não há uma versão original do documento. Segundo Roque,

não temos registros da obra original, somente versões e traduções tardias. Um dos fragmentos mais antigos de uma dessas versões, encontrado entre diversos papiros gregos em *Oxyrhynque*<sup>1</sup>, cidade às margens do Nilo, data, provavelmente, dos anos 100 da Era Comum (ROQUE, 2012, p. 132).

**Figura 1.2 – Fragmento de Elementos encontrado em *Oxyrhynque*, no Egito**



Fonte: (ROQUE, 2012)

Embora Elementos tenha sido escrito por Euclides, é necessário frisar que muitos dos resultados matemáticos exibidos no livro já eram do conhecimento de outros estudiosos da época. De acordo com (WEIL, 1984, p. 4), “é geralmente aceito que muito, se não todo o conteúdo desses livros é de origem anterior, mas pouco pode ser dito sobre a história por trás deles”. Por não haver publicações anteriores que organizassem logicamente os resultados da forma que Euclides fez, os Elementos é considerado um dos livros mais reproduzidos e estudados na história ocidental, perdendo apenas para a Bíblia (BURTON, 2011). (SILVA, 2014, p. 16), afirma ainda que “a grande inovação feita por Euclides, nos Elementos, é a adoção do método axiomático-dedutivo, no qual, partindo de alguns conceitos primitivos, aceitos como triviais ou intuitivos, demonstram-se consequências chamadas de teoremas ou proposições”.

<sup>1</sup> No texto original de (ROQUE, 2012) a palavra *Oxyrhynque* não se encontra em itálico. Entretanto, por se tratar de uma palavra em outro idioma, preferimos escrever em itálico nesse trabalho.



Apesar de toda a obra apresentar importantes resultados para várias áreas da Matemática, neste trabalho daremos ênfase ao Livro VII, pois é o livro no qual Euclides apresenta o que é conhecido hoje como Algoritmo de Euclides (AE), o método de divisões sucessivas que permite encontrar o Máximo Divisor Comum (mdc) entre dois ou mais números inteiros. Apesar de existir evidências históricas de que o procedimento já existia antes de Euclides, há pelo menos um século, o algoritmo recebe o nome de “Algoritmo Euclidiano” (BURTON, 2011). Segundo (NASCIMENTO, 2013), o procedimento original foi descrito para números naturais ou comprimentos geométricos, só posteriormente que foi generalizado para outras classes numéricas. Ao ler Elementos, principalmente os Livros VII-IX, é perceptível esse tratamento que Euclides dava aos números. Segundo Baumgart:

O desenvolvimento da notação algébrica evoluiu ao longo de três estágios: o retórico (ou verbal), o sincopado (no qual eram usadas abreviações de palavras) e o simbólico. No último estágio a notação passou por várias modificações e mudanças, até tornar-se razoavelmente estável ao tempo de Isaac Newton (c. 1700) (BAUMGART, 1992, p. 3).

Dessa forma, com a leitura de Elementos é perceptível que a linguagem matemática utilizada por Euclides na época não é a mesma que utilizamos hoje. É até importante que a leitura seja feita de forma minuciosa, já que não estamos tão acostumados a representar números por meio de segmentos de reta. Além disso, as demonstrações eram exibidas de forma verbal, utilizando também, eventualmente, o auxílio de segmentos.

## 1.2 CONCEITOS PRELIMINARES

Antes de iniciarmos de fato a falar do Algoritmo de Euclides, é importante rever algumas definições e teoremas importantes que baseiam nosso objeto de estudo. Nessa perspectiva, esta Seção será destinada à revisão de alguns conceitos de Teoria dos Números. Dessa forma, acreditamos que a Seção será suficiente para o entendimento do trabalho, mesmo que o leitor não tenha conhecimento algum sobre Teoria dos Números. Os autores em que nos baseamos nesta Seção são (BEZERRA, 2018), (SANTOS, 1998), (OLIVEIRA, 2011) e (HEFEZ, 2014).

### 1.2.1 Divisibilidade em $\mathbb{Z}$

Falar de divisibilidade é imprescindível para entender o Algoritmo de Euclides, já que o algoritmo trabalha diretamente com divisões. Dessa forma, mesmo que seja algo simples e até mesmo elementar para alguns leitores, é importante que todos os tópicos abordados a seguir sejam lidos com atenção. Para os leitores que desejem se aprofundar um pouco mais no conteúdo de divisibilidade, sugerimos as leituras referenciadas no começo da Seção 1.2.

**Definição 1.2.1** Sejam  $a, b \in \mathbb{Z}$ ,  $b \neq 0$ . Dizemos que  $b$  divide  $a$  (denotamos por  $b \mid a$ ) se existir um  $c \in \mathbb{Z}$ , tal que

$$a = bc.$$

Se  $b \mid a$ , dizemos ainda que  $a$  é divisível por  $b$  ou que  $a$  é **múltiplo** de  $b$ . Podemos afirmar ainda que  $b$  é **divisor** de  $a$ . Caso contrário, se  $b$  não divide  $a$ , denotamos por  $b \nmid a$  e dizemos que  $a$  não é divisível por  $b$  ou que  $a$  não é múltiplo de  $b$ .

**Exemplo 1.2.1** Dados os números 4 e 36, sabemos que  $4 \mid 36$ , pois  $36 = 4 \cdot 9$  e  $9 \in \mathbb{Z}$ . Portanto, podemos afirmar que 36 é divisível por 4 ou que 36 é múltiplo de 4. Agora, dados os números 5 e 32, sabemos que  $5 \nmid 32$ , pois não existe um  $c \in \mathbb{Z}$ , tal que  $32 = 5 \cdot c$ . Assim, concluímos que 32 não é múltiplo de 5.

**Observação.** É importante não confundir as notações  $a \mid b$  e  $\frac{b}{a}$ . Na notação  $a \mid b$  estamos afirmando que  $a$  divide  $b$ , enquanto na notação  $\frac{b}{a}$  estamos apenas representando uma fração, que pode ter um resultado inteiro ou não. Embora sejam notações que expressam diferentes resultados, há uma relação entre elas, já que  $a \mid b$  se, e somente se o número racional representado por  $\frac{b}{a} \in \mathbb{Z}$ .

A Definição 1.2.1 dá origem a algumas proposições muito importantes para divisibilidade. Vejamos algumas a seguir.

**Proposição 1.2.1** Sejam  $a, b$  e  $c \in \mathbb{Z}$ , se  $a \mid b$  e  $b \mid c$ , então  $a \mid c$ .

*Demonstração.* Pela Definição 1.2.1, sabemos que  $b = d_1 a$  para algum  $d_1 \in \mathbb{Z}$ . Além disso,  $c = d_2 b$  para algum  $d_2 \in \mathbb{Z}$ . Substituindo o valor de  $b$  na última equação, temos

$$c = d_2(d_1 a) = (d_2 d_1) a = d_3 a$$

para  $d_3 \in \mathbb{Z}$ . Logo, concluímos que  $a \mid c$ . ■

**Proposição 1.2.2** Sejam  $a, b$  e  $c \in \mathbb{Z}$ , se  $a \mid b$  e  $a \mid c$ , então  $a \mid (bm + cn)$ , para quaisquer  $m$  e  $n \in \mathbb{Z}$ .

*Demonstração.* De forma análoga a demonstração da Proposição 1.2.1, sabemos que

$$b = d_1 a \tag{1}$$

para algum  $d_1 \in \mathbb{Z}$ , e

$$c = d_2 a \tag{2}$$

para algum  $d_2 \in \mathbb{Z}$ . Multiplicando 1 por um  $m$  qualquer, tal que  $m \in \mathbb{Z}$ , e 2 por um  $n$  qualquer, tal que  $n \in \mathbb{Z}$ , temos:

$$bm = (d_1m)a \quad (3)$$

e

$$cn = (d_2n)a \quad (4)$$

Somando 3 e 4, obtemos:

$$bm + cn = (d_1m)a + (d_2n)a = a(d_1m + d_2n).$$

Sabemos que  $d_1m + d_2n \in \mathbb{Z}$ . Portanto, concluímos que  $a \mid bm + cn$ . ■

**Exemplo 1.2.2** Como  $6 \mid 36$  e  $6 \mid 60$ , então  $6 \mid (36m + 60n)$ , para quaisquer  $m, n \in \mathbb{Z}$ . Se escolhermos, por exemplo,  $m = 124$  e  $n = 168$ , teremos  $6 \mid (36 \cdot 124 + 60 \cdot 168) = 14544$ . De fato,  $14544 = 6 \cdot 2424$ .

**Proposição 1.2.3** Dados  $a, b$  e  $c \in \mathbb{Z}$ , valem as seguintes propriedades:

1. Para todo  $a \in \mathbb{Z}/\{0\}$ ,  $a \mid a$ .
2. Se  $a \mid b$ , então  $ac \mid bc$ .
3. Se  $ab \mid ac$  e  $a \neq 0$ , então  $b \mid c$ .
4. Para todo  $a \in \mathbb{Z}$ ,  $1 \mid a$ .
5. Para todo  $a \in \mathbb{Z}/\{0\}$ ,  $a \mid 0$ .
6. Se  $a \mid b$  e  $b \neq 0$ , então  $|a| \leq |b|$ .
7. Se  $a \mid b$  e  $b \mid a$ , então  $|a| = |b|$ .
8. Se  $a \mid b$  e  $a \neq 0$ , então  $(b/a) \mid b$ .

*Demonstração.* Iremos demonstrar algumas das propriedades acima:

1. A demonstração é imediata, basta observar que  $a = 1 \cdot a$ .
2. Da definição, segue que se  $a \mid b$ , então  $b = ad$ , para algum  $d \in \mathbb{Z}$ . Logo, multiplicando ambos os membros por  $c$ , temos  $bc = adc = (ac)d$ . Portanto,  $ac \mid bc$ .
3. Já que  $ab \mid ac$ , então  $ac = (ab)d$ , para algum  $d \in \mathbb{Z}$ . Dividindo ambos os membros por  $a$ , ficamos com  $c = bd$ . Portanto, concluímos que  $b \mid c$ .
4. De fato, já que  $a = 1 \cdot a$ .

5. Basta observar que  $0 = a \cdot 0$ .
6. A demonstração pode ser encontrada em (OLIVEIRA, 2011).
7. A demonstração pode ser encontrada em (OLIVEIRA, 2011).
8. Se  $a \mid b$ , então existe um inteiro  $c$ , tal que  $b = ac$ . Dessa forma, dividindo ambos os membros por  $a$ , temos  $(b/a) = c$ . Logo,  $(b/a) \in \mathbb{Z}$ . Como  $b = (b/a)a$ , segue que  $(b/a) \mid b$ .

■

### 1.2.2 O Algoritmo da Divisão

Agora que já vimos as principais definições e propriedades de divisibilidade, já podemos começar a falar sobre o Algoritmo da Divisão. Definiremos, adiante, quociente e resto, termos bastante importantes para este trabalho.

**Teorema 1.2.1** Dados  $a$  e  $b \in \mathbb{Z}$ , com  $b > 0$ , existe um único par de inteiros  $q$  e  $r$  que satisfazem

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

*Demonstração.* Para a demonstração deste Teorema usaremos um resultado chamado Teorema de Eudoxius, encontrado na referência (SANTOS, 1998). Pelo Teorema de Eudoxius, como  $b > 0$ , existe um  $q$  satisfazendo

$$qb \leq a < (q+1)b.$$

Disso, decorre que  $0 \leq a - qb$  e  $a - qb < b$ . Logo, se definirmos  $r = a - qb$ , garantimos a existência de  $q$  e  $r$ . Para provar a unicidade, vamos supor que existam um outro par  $q_1$  e  $r_1$  que satisfaçam

$$a = q_1b + r_1, \text{ com } 0 \leq r_1 < b.$$

Com isso, temos  $(qb + r) - (q_1b + r_1) = 0 \Rightarrow b(q - q_1) = r_1 - r$ , o que implica que  $b \mid (r_1 - r)$ . Mas, como  $r_1 < b$  e  $r < b$ , temos  $|r_1 - r| < b$  e, portanto como  $b \mid (r_1 - r)$ , devemos ter  $r_1 - r = 0 \Rightarrow r_1 = r$ . Assim,  $q_1b = qb \Rightarrow q_1 = q$ , uma vez que  $b \neq 0$ . ■

**Observação.** Os números  $q$  e  $r$  são chamados respectivamente de **quociente** e **resto** da divisão de  $a$  por  $b$ , enquanto  $a$  é chamado de **dividendo** e  $b$  é denominado **divisor**.

**Exemplo 1.2.3** Dados os números 108 e 15, ao efetuarmos a divisão de 108 por 15, obtemos um quociente  $q = 7$  e um resto  $r = 3$ , já que  $108 = 7 \cdot 15 + 3$ .

**Exemplo 1.2.4** Já com os números  $-108$  e 15, teremos um quociente  $q = -8$  e  $r = 12$ , já que  $-108 = -8 \cdot 15 + 12$ .

**Observação.** Sejam  $a$  e  $b \in \mathbb{Z}$ , com  $a > 0$ . Seja  $r$  o resto da divisão de  $b$  por  $a$ , então

$$a \mid b \Leftrightarrow r = 0.$$

*Demonstração.* De fato, se  $a \mid b$ , então  $b = aq = aq + 0$ . Logo,  $r = 0$ . Analogamente, se  $r = 0$ , então  $b = aq$ . Portanto,  $a \mid b$ . ■

### 1.2.3 Máximo Divisor Comum

É impossível falar do Algoritmo de Euclides sem uma noção, ainda que básica, de Máximo Divisor Comum (mdc). De início, é importante lembrar que se  $a$  e  $b \in \mathbb{Z}$ , então  $b$  é divisor de  $a$  sempre que  $a$  for múltiplo de  $b$ . Em outras palavras, sempre que na divisão de  $a$  por  $b$  deixar um  $r = 0$ , então  $b$  é divisor de  $a$ .

**Definição 1.2.2** O conjunto de divisores de  $a \in \mathbb{Z}$  é dado por

$$D(a) = \{d \in \mathbb{Z}^+ \setminus \{0\}; d \mid a\}.$$

Vejam alguns exemplos:

1.  $D(10) = \{1, 2, 5, 10\}$ ;
2.  $D(12) = \{1, 2, 3, 4, 6, 12\}$ ;
3.  $D(19) = \{1, 19\}$ ;
4.  $D(20) = \{1, 2, 4, 5, 10, 20\}$ ;
5.  $D(0) = \mathbb{Z} \setminus \{0\}$  (Relembre a Propriedade 5 da Proposição 1.2.1).

Pelos exemplos acima, podemos notar que alguns números têm divisores em comum. Por exemplo, 1, 2 e 4 são divisores tanto de 12 como de 20. É importante destacar que, se  $a \neq 0$ , então  $D(a)$  é limitado, ou seja,  $a$  possui finitos divisores. Dessa forma, o conjunto  $D(a) \cap D(b)$  nunca será vazio, já que pelo menos um dos conjuntos de divisores é limitado. Além disso, a Propriedade 4 da Proposição 1.2.1 afirma que, para todo  $a \in \mathbb{Z}$ ,  $1 \mid a$ . Portanto,  $D(a) \cap D(b) \neq \{\}$ .

**Definição 1.2.3** Sejam  $a$  e  $b \in \mathbb{Z}$ ;  $a \neq 0$ . Definimos o máximo divisor comum de  $a$  e  $b$  como o maior elemento de  $D(a) \cap D(b)$  e denotamos por  $\text{mdc}(a, b)$ .

**Exemplo 1.2.5** Dados os números 10 e 15, listemos seus divisores:

$$D(10) = \{1, 2, 5, 10\};$$

$$D(15) = \{1, 3, 5, 15\}.$$

Como  $D(10) \cap D(15) = \{1, 5\}$ , concluimos que o maior divisor comum entre 10 e 15 é 5, e denotamos por  $\text{mdc}(10, 15) = 5$ .

**Exemplo 1.2.6** Já considerando os números 9 e 14, temos que  $\text{mdc}(9, 14) = 1$ , pois eles só possuem 1 como divisor comum.  $D(9) = \{1, 3, 9\}$ ,  $D(14) = \{1, 2, 7, 14\}$ .

**Observação.** Pela Propriedade 4 da Proposição 1.2.1, sabemos que, para todo  $a \in \mathbb{Z}$ ,  $1 \mid a$ . Dessa forma, quaisquer que sejam  $a$  e  $b \in \mathbb{Z}$ ,  $\text{mdc}(a, b) \geq 1$ .

**Definição 1.2.4** Seja  $n \in \mathbb{Z}$ , tal que  $n \geq 2$ . Dizemos que  $n$  é um número **primo** quando seus únicos divisores **positivos** são 1 e o próprio  $n$ . Caso contrário,  $n$  é chamado de número **composto**.

Quando o  $\text{mdc}(a, b) = 1$ , dizemos que  $a$  e  $b$  são **primos entre si**, ou ainda, **coprimos**.

**Exemplo 1.2.7** Os números 2, 3, 5, 7, 11 e 13 são exemplos de números primos.

**Exemplo 1.2.8** Os números 18 e 25 são primos entre si, pois o  $\text{mdc}(18, 25) = 1$ .

Considerando o Teorema 1.2.1 e tudo que vimos nesta Subseção 1.2.3, podemos enunciar uma proposição fundamental para o AE.

**Proposição 1.2.4** Se  $a = bq + r$ , então  $\text{mdc}(a, b) = \text{mdc}(b, r)$ .

*Demonstração.* Como  $a = qb + r$ , decorre da Proposição 1.2.2 que todo divisor de  $b$  e de  $r$  também é divisor de  $a$ . Da mesma forma, como  $a = qb + r \Rightarrow r = a - qb$ , podemos concluir que todo divisor de  $a$  e  $b$  também é divisor de  $r$ . Portanto, o conjunto de divisores de  $a$  e  $b$  é igual ao conjunto de divisores de  $b$  e  $r$ , o que nos garante que  $\text{mdc}(a, b) = \text{mdc}(b, r)$ . ■

#### 1.2.4 Decomposição em Fatores Primos

Uma outra forma de encontrar o MDC entre dois números inteiros é pelo método de decomposição dos números em fatores primos. Na Seção 1.5 usaremos esse método

para fazer uma comparação com o Algoritmo de Euclides. Estaremos nesta Subseção nos baseando nas obras (SANTOS, 1998) e (HEFEZ, 2014).

**Teorema 1.2.2** (Teorema Fundamental da Aritmética) Todo número inteiro  $a > 1$  pode ser representado de maneira única (a menos de ordem) como um produto de fatores primos, tais que

$$a = p_1^{n_1} \cdots p_r^{n_r};$$

com números primos  $p_1 < \cdots < p_r$ ,  $n_1, \dots, n_r$  números naturais não nulos e  $r > 0$ .

A prova do Teorema 1.2.2 pode ser encontrada em (SANTOS, 1998). Com o Teorema 1.2.2, podemos escrever qualquer número inteiro maior do que 1 como produto de potências de primo.

**Exemplo 1.2.9** O número 504 pode ser escrito como  $2^3 \cdot 3^2 \cdot 7^1$ . Chamamos esse procedimento de Decomposição em Fatores Primos, ou simplesmente Fatoração. Para encontrar os fatores primos de 504 e suas respectivas potências, basta ir dividindo o número por números primos, até que se chegue à 1. Veja como isso acontece:

$$\begin{array}{r|l} 504 & 2 \\ 252 & 2 \\ 126 & 2 \\ 63 & 3 \\ 21 & 3 \\ 7 & 7 \\ 1 & \end{array}$$

Resumidamente, começamos dividindo 504 pelo menor número primo possível, que é o número 2. Caso 2 não dividisse 504, passaríamos para o próximo número primo e assim sucessivamente. No caso, como  $2 \mid 504$ , efetuamos a divisão e continuamos o procedimento, mas agora com o quociente da divisão de  $504/2$ . Como  $2 \mid 252$ , efetuamos novamente a divisão pelo número primo 2, encontrando o quociente 126. Da mesma forma,  $2 \mid 126$ , deixando quociente igual a 63. No entanto,  $2 \nmid 63$ . Com isso, passamos para o próximo número primo, que é 3. Como  $3 \mid 63$ , encontramos o quociente 21 deixado pela divisão e verificamos que  $3 \mid 21$ . Agora, como o quociente é 7 e  $3 \nmid 7$ , verificamos se  $5 \mid 7$ . Como  $5 \nmid 7$ , passamos para o próximo número primo. Como  $7 \mid 7$ , fizemos a divisão e encontramos o quociente igual a 1, não sendo possível fazer mais divisões. Com isso, concluímos que  $504 = 2^3 \cdot 3^2 \cdot 7^1$ .

Preferimos, neste exemplo, seguir uma ordem crescente dos números primos. No entanto, qualquer ordem vai resultar na mesma decomposição.

### 1.2.5 Congruência

No Capítulo 2 iremos usar um resultado importante de Congruência. Para isso, é necessário ver algumas definições importantes. Nesta Subseção, estaremos nos espelhando na obra (SANTOS, 1998).

**Definição 1.2.5** Seja  $m$  um número inteiro maior do que 1. Dizemos que dois números inteiros  $a$  e  $b$  são *congruentes módulo  $m$*  se  $m \mid (a - b)$ . Denotamos por

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

Quando  $a$  e  $b$  não são congruentes módulo  $m$ , escrevemos

$$a \not\equiv b \pmod{m}.$$

**Exemplo 1.2.10** Dados os números 33 e 18, podemos afirmar que

$$33 \equiv 18 \pmod{5},$$

já que  $5 \mid (33 - 18) = 15$ .

**Exemplo 1.2.11** Ao contrário do exemplo anterior, 33 e 18 não são congruentes módulo 2, isso porque  $2 \nmid (33 - 18) = 15$ . Neste caso, denotamos por

$$33 \not\equiv 18 \pmod{2}.$$

**Proposição 1.2.5** Se  $a$  e  $b$  são números inteiros, temos que  $a \equiv b \pmod{m}$  se, e somente se, existir um inteiro  $k$ , tal que

$$a = b + km.$$

*Demonstração.* Se  $a \equiv b \pmod{m}$ , então  $m \mid (a - b)$ . Logo, existe um inteiro  $k$ , tal que  $km = a - b$ , isto é,  $a = b + km$ . De forma análoga, se existe um inteiro  $k$  que satisfaça  $a = b + km$ , temos  $km = a - b \Rightarrow m \mid (a - b) \Rightarrow a \equiv b \pmod{m}$ . ■

**Exemplo 1.2.12** Como  $15 \equiv 8 \pmod{7}$ , então existe um inteiro  $k$  que satisfaz a equação  $15 = 8 + 7k$ . De fato, resolvendo a equação, temos

$$15 = 8 + 7k$$

$$15 - 8 = 7k$$

$$7 = 7k$$

$$k = 1$$



**Teorema 1.2.3** (Pequeno Teorema de Fermat) Seja  $p$  um número primo. Se  $p \nmid a$  então  $a^{p-1} \equiv 1 \pmod{p}$ .

Usaremos esse Teorema no Capítulo 2 deste trabalho. Caso o leitor queira ver a sua demonstração, pode consultar a referência (SANTOS, 1998).

### 1.3 O ALGORITMO

Como vimos anteriormente, nos exemplos 1.2.6 e 1.2.8, um método para encontrar o maior divisor entre dois ou mais números inteiros é listar todos os divisores dos números em questão e então destacar o maior entre os divisores comuns. Porém, quando esses números são muito grandes, esse método se torna exaustivo e demorado. Mencionaremos isso numa seção futura de forma mais clara. O Algoritmo de Euclides (AE), surge, então, como um procedimento mais simples e rápido para encontrar o mdc entre dois ou mais números inteiros. Estaremos tomando como base teórica nesta Seção as obras (EUCLIDES, 2009) e (SANTOS, 1998). Para entender como o AE funciona, vejamos as proposições I e II do Livro VII de Elementos:

Proposição I: *Sendo expostos dois números desiguais, e sendo sempre subtraído de novo o menor do maior, caso o que restou nunca meça exatamente o antes dele mesmo, até que reste uma unidade, os números do princípio serão primos entre si.*

Proposição II: *Sendo dados dois números não primos entre si, achar a maior medida comum deles.*

Podemos entender a Proposição I (P.I) dessa forma: Dados dois números diferentes, tal que um não seja múltiplo do outro. Esses dois números serão primos entre si, caso, subtraindo o menor do maior sucessivamente, se chegar no resto igual a 1. Essa é a descrição do AE dado por Euclides em Elementos para julgar se dois números são ou não primos entre si. Para entender como acontece na prática, vejamos alguns exemplos.

**Exemplo 1.3.1** Dado o par de números (10, 17), verifiquemos se os números são primos entre si, utilizando a P.I. Como  $17 > 10$ , temos

$$(10, 17) \Rightarrow (10, 17 - 10) = (10, 7).$$

De forma análoga, temos que  $10 > 7$ . Logo,

$$(10, 7) \Rightarrow (10 - 7, 7) = (3, 7).$$

Repetindo o mesmo procedimento até chegar em 0, temos:

$$(3, 7) \Rightarrow (3, 4) \Rightarrow (3, 1) \Rightarrow (2, 1) \Rightarrow (1, 1) \Rightarrow (1, 0).$$

Como chegamos no resto 1, concluímos que 10 e 17 são primos entre si. Note que subtraímos 10 de 17 apenas uma vez e tivemos um resto igual a 7. Não é difícil concluir que

$$17 = 1 \cdot 10 + 7.$$

Ficamos, então, com o par (10, 7). Em seguida, subtraímos por 7 apenas uma vez e tivemos um resto igual a 3. Portanto,

$$10 = 1 \cdot 7 + 3.$$

Agora com o par (3, 7), subtraímos por 3 duas vezes, chegando ao resto igual a 1. Então,

$$7 = 2 \cdot 3 + 1.$$

Novamente, agora com o par (3, 1), subtraímos por 1 três vezes e finalmente chegamos ao resto igual a 0. Logo,

$$3 = 3 \cdot 1 + 0.$$

Essa análise nos ajudará a entender melhor o funcionamento do AE futuramente.

**Exemplo 1.3.2** Dado o par de números (6, 28), verifiquemos se os números são primos entre si, utilizando a P.I. Seguindo a mesma lógica, temos

$$(6, 22) \Rightarrow (6, 16) \Rightarrow (6, 10) \Rightarrow (6, 4) \Rightarrow (2, 4) \Rightarrow (2, 2) \Rightarrow (2, 0).$$

Ao contrário do exemplo anterior, nesse caso não chegamos em um resto igual a 1. Portanto, 6 e 28 não são primos entre si, tendo, então, algum divisor em comum. Vendo por um outro lado, inicialmente subtraímos por 6 três vezes e chegamos a um resto 4. Assim,

$$22 = 3 \cdot 6 + 4.$$

Depois, subtraímos por 4 uma vez e tivemos um resto 2.

$$6 = 1 \cdot 4 + 2.$$

Continuando, subtraímos por 2 duas vezes e chegamos ao fim do procedimento.

$$4 = 2 \cdot 2 + 0.$$

Nesse exemplo já podemos falar sobre a Proposição II (P.II), já que os números não são coprimos. A P.II pede para encontrar a maior medida comum entre dois números que não são coprimos. Para isso, devemos observar o último par ordenado do processo. No caso desse exemplo, o último par foi (2, 0), indicando que o MDC entre 6 e 28 é 2.

**Observação.** De forma geral, sempre que chegamos ao par  $(1, 0)$ , os números iniciais são coprimos, já que o MDC entre eles é 1.

A descrição original do AE diz que devem ser feitas sucessivas subtrações entre o maior e menor número até que chegue no resto igual a 0. Uma forma equivalente e mais prática de realizar esse mesmo procedimento é fazer sucessivas divisões euclidianas do maior pelo menor número. Com isso, o número que era o maior passa a ser o primeiro resto da divisão e o número que era menor, passa a ser o maior número. Veremos isso de uma forma mais clara logo abaixo.

Partindo de uma visão algébrica, podemos entender como as proposições I e II determinam o AE da seguinte forma: Sejam  $a$  e  $b \in \mathbb{Z}$ ;  $a > b$  e  $a \neq 0$ , temos, utilizando sucessivas divisões:

$$\begin{aligned} a &= q_1 b + r_1 & 0 \leq r_1 < b; \\ b &= q_2 r_1 + r_2 & 0 \leq r_2 < r_1; \\ r_1 &= q_3 r_2 + r_3 & 0 \leq r_3 < r_2; \\ &\vdots & \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} & 0 \leq r_{n-1} < r_{n-2}; \\ r_{n-2} &= q_n r_{n-1} + r_n & 0 \leq r_n < r_{n-1}; \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Pela Proposição 1.2.4, temos que:

$$\text{mdc}(a, b) = \text{mdc}(b, r_1) = \text{mdc}(r_1, r_2) = \dots = \text{mdc}(r_n, 0) = r_n.$$

Portanto,  $\text{mdc}(a, b) = r_n$ .

**Exemplo 1.3.3** Para encontrar o  $\text{mdc}(2022, 108)$  utilizando o AE, devemos realizar sucessivas divisões até chegar no resto igual a 0. Começamos dividindo 2022 por 108 e vemos qual o resto dessa divisão. Em seguida, o divisor antigo (no caso 108) passa a ser dividendo e o resto antigo (no caso 78), passa a ser o novo divisor. Fazemos isso sucessivamente. Vejamos:

$$\begin{aligned} 2022 &= 18 \cdot 108 + 78 \\ 108 &= 1 \cdot 78 + 30 \\ 78 &= 2 \cdot 30 + 18 \\ 30 &= 1 \cdot 18 + 12 \\ 18 &= 1 \cdot 12 + 6 \\ 12 &= 2 \cdot 6 + 0. \end{aligned}$$

Logo,  $\text{mdc}(2022, 108) = \text{mdc}(108, 78) = \text{mdc}(78, 30) = \dots = \text{mdc}(6, 0) = 6$ .

## 1.4 INTERPRETAÇÃO GEOMÉTRICA

O tratamento geométrico do AE já era realizado por Euclides em Elementos, no qual ele considerava os números como medidas de segmentos de reta. Nas proposições acerca do AE e até mesmo em suas demonstrações, Euclides utilizava bastante essa linguagem geométrica. Não é o nosso objetivo aqui fazer uma tradução da linguagem usada por Euclides para a linguagem matemática atual, mas é interessante perceber o tratamento geométrico dado ao AE por Euclides, visto que é uma abordagem diferente da que trataremos aqui nesta Seção. Para isso, retomaremos a Proposição I do Livro VII de Elementos e sua respectiva demonstração. Estaremos nos baseando, nesta Seção, nas obras (EUCLIDES, 2009), (AZEVEDO, 2013) e (PACCI; RODRIGUES, 2013).

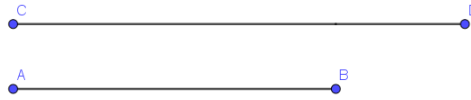
PI: “Sendo expostos dois números desiguais, e sendo sempre subtraído de novo o menor do maior, caso o que restou nunca meça exatamente o antes dele mesmo, até que reste uma unidade, os números do princípio serão primos entre si. ”

Demonstração dada por Euclides: “Pois, dos dois números (desiguais) AB, CD, sendo sempre subtraído de novo o menor do maior, o que restou jamais meça exatamente o antes dele mesmo, até que reste uma unidade; digo que os AB, CD são primos entre si, isto é, que uma unidade só mede os AB, CD. Pois, se os AB, CD não são primos entre si, algum número os medirá. Meça, e seja o E; e o CD medindo o BF, reste dele mesmo o menor FA, enquanto o AF, medindo o DG, reste dele mesmo o menor GC, e o GC, medindo o FH, reste a unidade HA. Como, de fato, o E mede o CD, e o CD mede o BF, portanto também o E mede o BF; e mede também o BA todo; portanto, medirá também o AF restante. E o AF mede o DG; portanto, o E também mede o DG; e também mede o DC todo; portanto, também medirá o CG restante. E o CG mede o FH; portanto, o E também mede o FH; e mede também o FA todo; portanto, medirá também a unidade AH restante, sendo um número; o que é impossível. Portanto, nenhum número medirá os números AB, CD; portanto, os AB, CD são primos entre si.”

A demonstração acima talvez cause um pouco de estranhamento durante a leitura devido à linguagem adotada por Euclides na época. Apesar disso, o que Euclides propõe nessas linhas é algo bastante simples de ser entendido. Mostraremos abaixo uma forma similar de fazer esse procedimento que Euclides descreveu. É importante ressaltar que não utilizaremos os mesmos nomes de segmentos da demonstração acima, já que o que iremos fazer não é a representação geométrica da demonstração. Apresentaremos uma outra perspectiva do tratamento geométrico que Euclides utilizava. Se dois segmentos de reta  $\overline{AB}$  e  $\overline{CD}$  têm comprimentos diferentes, então, subtraindo a medida do menor segmento do maior segmento, de forma sucessiva, caso reste apenas um segmento de reta de medida igual a uma unidade de segmento (denotaremos por 1 u.s), então os números que

representam os segmentos iniciais são primos entre si. De forma geométrica, isso acontece da seguinte maneira:

**Figura 1.3 – Segmentos Iniciais**



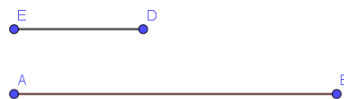
Fonte: Elaborado pelo Autor

**Figura 1.4 – Destacando o Segmento Menor**



Fonte: Elaborado pelo Autor

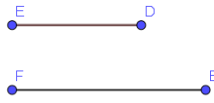
**Figura 1.5 – Subtraindo  $\overline{AB}$  de  $\overline{CD}$**



Fonte: Elaborado pelo Autor

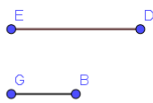
Esse mesmo procedimento deve ser repetido até que se reste apenas um segmento. Note que agora temos  $\overline{ED}$  sendo o menor segmento. No próximo passo, seu comprimento deve ser subtraído do segmento  $\overline{AB}$ . De forma resumida, esse passo a passo está ilustrado nas Figuras 1.6, 1.7, 1.8 e 1.9.

Figura 1.6 – Resultado de  $\overline{AB} - \overline{ED}$



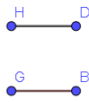
Fonte: Elaborado pelo Autor

Figura 1.7 – Resultado de  $\overline{FB} - \overline{ED}$



Fonte: Elaborado pelo Autor

Figura 1.8 – Resultado de  $\overline{ED} - \overline{GB}$



Fonte: Elaborado pelo Autor

Figura 1.9 – Resultado de  $\overline{GB} - \overline{HD}$



Fonte: Elaborado pelo Autor

Essa foi a interpretação geométrica do AE trazida por Euclides em Elementos. Se  $\overline{GB} = 1$  u.s, então os números de princípio são primos entre si, que no caso são os comprimentos de  $\overline{AB}$  e  $\overline{CD}$ . Essa mesma interpretação pode ser utilizada para encontrar o mdc entre quaisquer dois números naturais. Euclides denominava de encontrar a maior

medida em comum aos dois números. O procedimento é o mesmo, o que muda é apenas o comprimento do segmento de reta que restou: se for igual a 1 u.s, os números são primos entre si; se for alguma medida diferente de 1 u.s, então é a medida em comum aos dois números, que, em outras palavras, é o mdc entre os dois números.

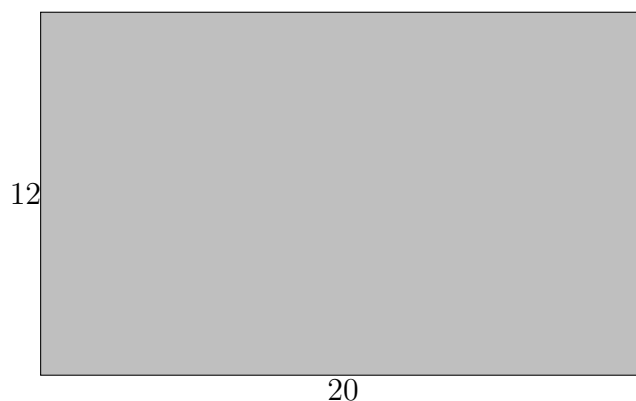
A interpretação geométrica do Algoritmo de Euclides é algo bastante interessante e que pouco é abordada em sala de aula. Desenvolver atividades que explorem o conhecimento geométrico junto ao AE podem, além de facilitar o entendimento do algoritmo por meio de uma nova abordagem, validar a idéia de que os conteúdos matemáticos não são isolados, mas sim interligados.

Partindo desse princípio e do conhecimento que temos do AE, a visualização geométrica do algoritmo consiste em construir um retângulo de dimensões iguais aos números que estão sendo trabalhados no AE (note que isso só faz sentido quando os números são naturais, já que na geometria euclidiana plana não existem medidas negativas). Feito isso, o próximo passo é preencher o interior do retângulo com os maiores quadrados possíveis. Com essa construção podemos enxergar as divisões euclidianas de uma outra forma, além de conseguir identificar o mdc entre os dois números em questão. Veremos isso de uma forma mais clara trabalhando com um exemplo numérico, mas de antemão podemos afirmar que **o mdc entre os dois números será igual a medida do lado do menor quadrado.**

**Exemplo 1.4.1** Utilizando o passo a passo descrito acima, podemos interpretar geometricamente o  $\text{mdc}(20, 12)$  da seguinte forma:

1. Inicialmente construímos um retângulo com as dimensões iguais aos números que queremos descobrir o mdc, no caso,  $20 \times 12$ .

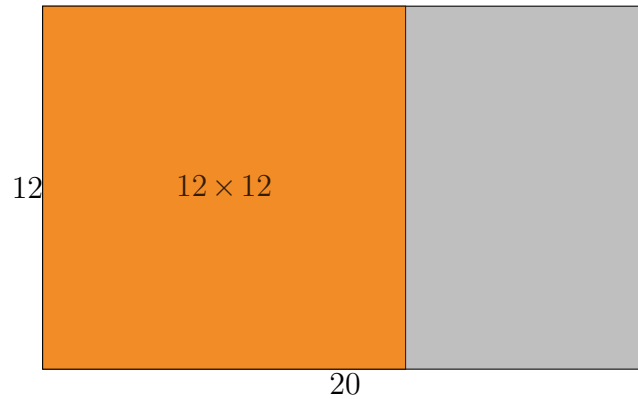
**Figura 1.10 – Retângulo de Dimensões  $20 \times 12$**



**Fonte: Elaborado pelo Autor**

2. Em seguida, iremos começar a preencher o interior do retângulo  $20 \times 12$  com os maiores quadrados possíveis. Note que o maior quadrado que cabe nesse retângulo é o quadrado de lado igual a 12, e só cabe um quadrado com essas dimensões.

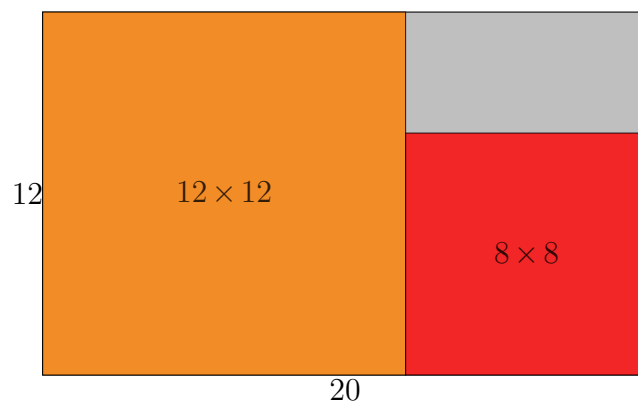
**Figura 1.11 – Preenchendo o Retângulo com um Quadrado de Lado Igual a 12**



**Fonte: Elaborado pelo Autor**

3. Agora, dado que dentro do retângulo  $20 \times 12$  existe um quadrado  $12 \times 12$ , sobra uma parte da figura. Essa parte que sobra é um retângulo de dimensões  $12 \times 8$ . Iremos fazer o mesmo procedimento, mas considerando agora o retângulo  $12 \times 8$ . Note que o maior quadrado que cabe dentro desse retângulo é o quadrado de lado igual a 8, e só cabe um quadrado com essas dimensões.

**Figura 1.12 – Preenchendo o Retângulo com um Quadrado de Lado Igual a 8**

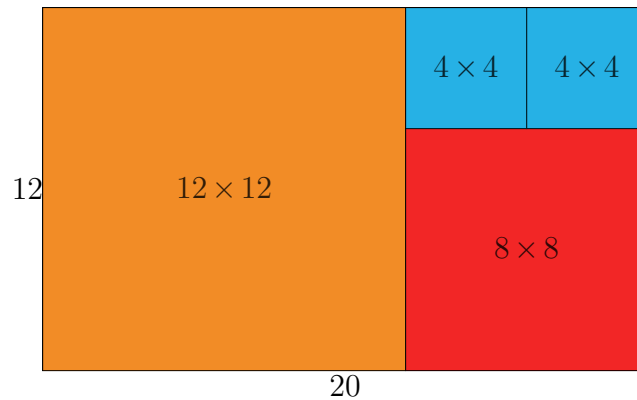


**Fonte: Elaborado pelo Autor**

4. Por fim, sobrou um retângulo com dimensões  $8 \times 4$ . O maior quadrado que cabe dentro retângulo tem lado igual a 4 e, nesse caso, cabem dois quadrados com essas dimensões, não sobrando nenhum espaço vazio na figura inicial.



**Figura 1.13 – Preenchendo o Retângulo com dois Quadrados de Lados Iguais a 4**



**Fonte: Elaborado pelo Autor**

Note que o menor quadrado no interior da figura tem lado igual a 4. Isso significa que o  $\text{mdc}(20, 12) = 4$ . De fato, se fizermos o AE, vamos chegar ao mesmo valor:

$$20 = 1 \cdot 12 + 8$$

$$12 = 1 \cdot 8 + 4$$

$$8 = 2 \cdot 4 + 0$$

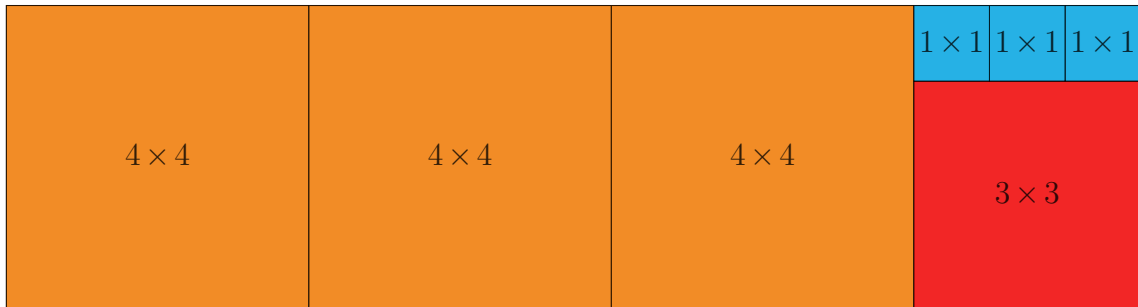
Isso implica que  $\text{mdc}(20, 12) = \text{mdc}(12, 8) = \text{mdc}(8, 4) = \text{mdc}(4, 0) = 4$ .

Perceba também que a Figura 1.13, de uma forma geométrica, mostrando as divisões euclidianas do AE feito com os números 20 e 12. Primeiramente, o retângulo inicial tem dimensões  $20 \times 12$ . Isso implica que no AE estarão sendo considerados os números 20 e 12 para o cálculo do mdc. Na Figura 1.11, vimos que coube apenas um quadrado de lado 12 e sobrou um espaço de dimensões  $12 \times 8$ . Se olharmos para o AE, a primeira linha está traduzindo numa linguagem algébrica essa informação:  $20 = 1 \cdot 12 + 8$ . Considerando agora que o próximo maior quadrado foi o de lado igual a 8, podemos observar na Figura 1.12 que só coube um e sobrou um espaço  $8 \times 4$ . Essa informação está traduzida algebricamente na segunda linha do AE:  $12 = 1 \cdot 8 + 4$ . E, por fim, sobrou um retângulo de dimensões  $8 \times 4$ , que foi preenchido com dois quadrados de lado igual a 4, preenchendo todo o retângulo original. Essa informação se encontra na última linha do AE:  $8 = 2 \cdot 4 + 0$ .

Quando os números que estão sendo trabalhados são primos entre si, sempre vai haver quadrados de lados iguais a 1 na representação geométrica do AE, independente de quantos quadrados sejam. Portanto, sempre que no retângulo aparecer pelo menos um quadrado  $1 \times 1$ , então os números em questão (que são as dimensões do maior retângulo) são primos entre si. Vejamos um exemplo:

**Exemplo 1.4.2** Vejamos geometricamente a representação do AE com os números 15 e 4.

**Figura 1.14 – Representação Geométrica do mdc entre 15 e 4**



**Fonte: Elaborado pelo Autor**

O maior quadrado que cabe no retângulo  $15 \times 4$  tem lado igual a 4. Perceba que cabem três quadrados com essas dimensões e sobra um retângulo  $4 \times 3$ . Da mesma forma, o maior quadrado que cabe no retângulo  $4 \times 3$  tem lado igual a 3, e só cabe um quadrado com essas dimensões. Por fim, sobra um retângulo de dimensões  $3 \times 1$ , onde cabem três quadrados de lado igual a 1. Como o menor quadrado tem lado igual a 1, concluímos que 15 e 4 são primos entre si, ou seja,  $\text{mdc}(15, 4) = 1$ . De fato, se usarmos o algoritmo, teremos:

$$15 = 3 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1$$

$$3 = 3 \cdot 1 + 0$$

onde  $\text{mdc}(15, 4) = \text{mdc}(4, 3) = \text{mdc}(3, 1) = \text{mdc}(1, 0) = 1$ .

De forma geral, sendo  $a$  e  $b \in \mathbb{Z}$ ;  $a > b$  e  $a \neq 0$ , tal que

$$\begin{aligned} a &= q_1 b + r_1 & 0 \leq r_1 < b; \\ b &= q_2 r_1 + r_2 & 0 \leq r_2 < r_1; \\ r_1 &= q_3 r_2 + r_3 & 0 \leq r_3 < r_2; \\ &\vdots & \\ r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} & 0 \leq r_{n-1} < r_{n-2}; \\ r_{n-2} &= q_n r_{n-1} + r_n & 0 \leq r_n < r_{n-1}; \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

teremos, inicialmente um retângulo de dimensões  $a \times b$ , no qual cabem  $q_1$  quadrados de lado  $b$ ,  $q_2$  quadrados de lado  $r_1$ ,  $q_3$  quadrados de lado  $r_2$ , ... ,  $q_{n+1}$  quadrados de lado  $r_n$ , sendo  $r_n$  o lado do menor quadrado e também o  $\text{mdc}(a, b)$ .

A interpretação geométrica do AE se torna ainda mais interessante quando trabalhamos com números de uma sequência por recorrência. Veremos a seguir um caso particular: Sequência de Fibonacci. De forma resumida, sequências recorrentes são sequências de números  $x_0, x_1, x_2, \dots, x_n, \dots$ , na qual cada termo depende do termo anterior (MOREIRA, 2013). A Sequência de Fibonacci é uma das mais famosas sequências recorrentes, sendo definida por  $x_0 = 0, x_1 = 1, x_{n+2} = x_{n+1} + x_n, \forall n \in \mathbb{N}$ . Alguns números da Sequência de Fibonacci são: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ... .

Uma das particularidades que tornam os números da Sequência de Fibonacci interessantes quando estamos trabalhando com o AE, é que, se pegarmos números consecutivos da sequência (sem contar com os dois primeiros que são 0 e 1), teremos  $q_1 = q_2 = q_3 = \dots = q_n = 1$  e  $q_{n+1} = 2$ . Ou seja, só cabe um quadrado para cada lado  $b, r_1, r_2, r_3, \dots, r_{n-1}$ , e cabem dois quadrados de lado  $r_n$ . Além disso, os números  $a, b, r_1, r_2, r_3, \dots, r_n$  são números da Sequência de Fibonacci, na qual  $r_n = 1$ . Com isso podemos concluir que, para qualquer par de números  $a$  e  $b$  consecutivos da Sequência de Fibonacci, excluindo-se os dois primeiros que são 0 e 1, o  $\text{mdc}(a, b) = 1$ , e sempre existirão dois quadrados de lado 1 na visualização geométrica (isso porque  $q_{n+1} = 2$  e  $r_n = 1$ ).

Com isso, geometricamente, para cada par de números consecutivos da Sequência de Fibonacci que pegarmos, se desenharmos em cada quadrado de sua representação geométrica  $\frac{1}{4}$  de círculo com raio igual ao lado do quadrado, estaremos formando o que chamamos de Espiral de Fibonacci (PACCI; RODRIGUES, 2013). Relembre a lei de formação da Sequência de Fibonacci:

$$x_{n+2} = x_{n+1} + x_n. \quad (5)$$

Podemos reescrever (5) como

$$x_{n+2} = 1 \cdot x_{n+1} + x_n. \quad (6)$$

Agora, sabemos que a divisão euclidiana de  $x_{n+2}$  por  $x_{n+1}$  é dada por:

$$x_{n+2} = q_1 \cdot x_{n+1} + r_1, \quad (7)$$

onde  $0 \leq r < x_{n+1}$ . Se compararmos (6) com (7), concluímos que  $q_1 = 1$  e  $r_1 = x_n$ . Agora, considerando o AE, a próxima divisão euclidiana acontece entre  $x_{n+1}$  e  $x_n$ . Sabemos da definição que

$$x_{n+1} = x_n + x_{n-1},$$

no qual podemos concluir novamente que  $q_2 = 1$  e  $r_2 = x_{n-1}$ . Isso é válido para todas as divisões euclidianas. Porém, perceba que todos os dividendos, divisores e restos são números da Sequência de Fibonacci em ordem decrescente. Isso implica que a última divisão euclidiana sempre será com o número 2 como número a ser dividido pelo seu antecessor da sequência, que é o número 1, obtendo resto igual a 0. Em outras palavras, a última divisão euclidiana sempre será  $2 = 2 \cdot 1 + 0$ , provando que na representação geométrica, sempre haverá dois quadrados de lados iguais a 1. Veremos alguns exemplos a seguir.

**Exemplo 1.4.3** Dados os números 13 e 8 da Sequência de Fibonacci, usando o AE, temos:

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

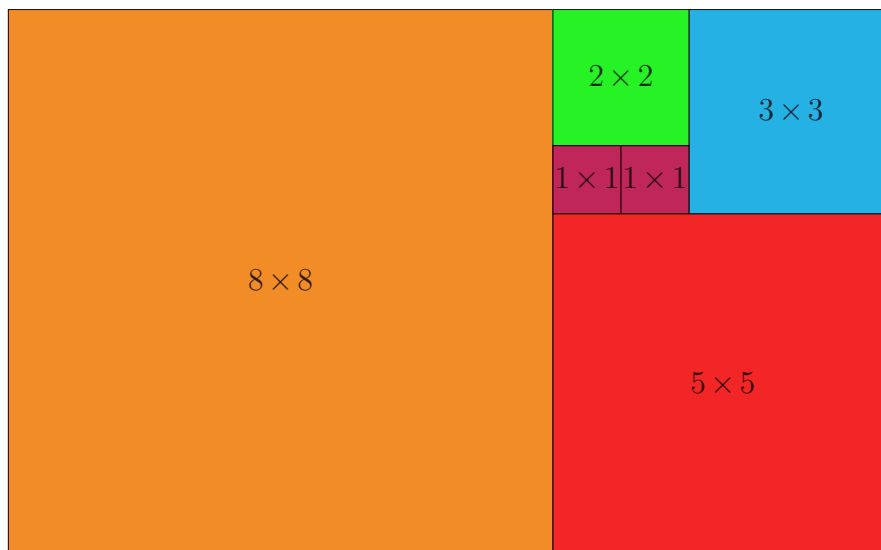
$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

De forma geométrica, teremos:

**Figura 1.15 – Representação geométrica do mdc entre 13 e 8**



**Fonte: Elaborado pelo Autor**

**Exemplo 1.4.4** Agora com os números 21 e 13 da Sequência de Fibonacci, usando o AE, temos:

$$21 = 1 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

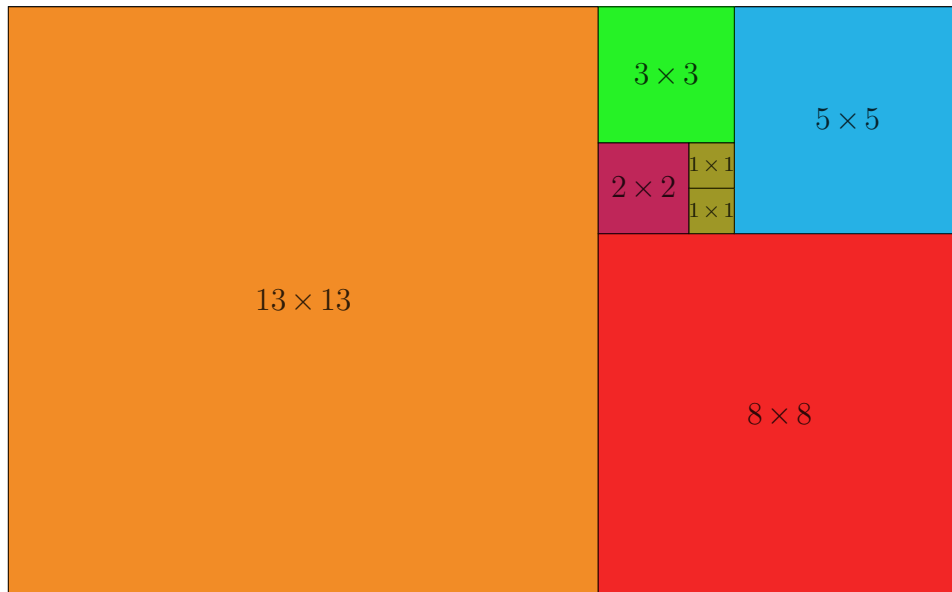
$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

De forma geométrica, teremos:

**Figura 1.16 – Representação geométrica do mdc entre 21 e 13**



Fonte: Elaborado pelo Autor

**Exemplo 1.4.5** Já com os números 34 e 21, temos:

$$34 = 1 \cdot 21 + 13$$

$$21 = 1 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

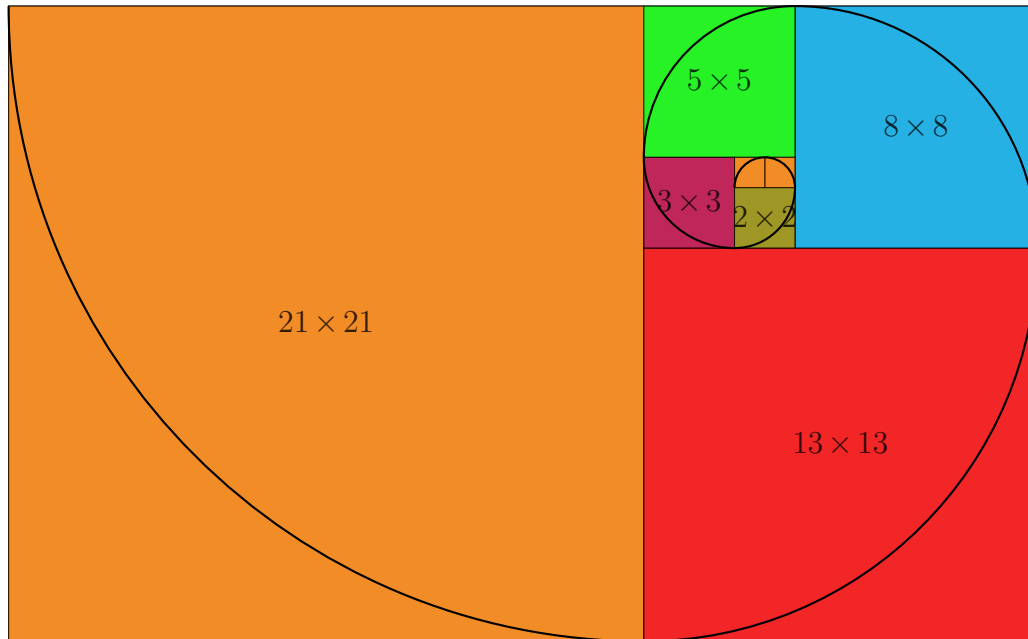
$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

(8)

De forma geométrica, teremos:

Figura 1.17 – Representação geométrica do mdc entre 34 e 21



Fonte: Elaborado pelo Autor

Os Exemplos 1.4.3, 1.4.4 e 1.4.5 mostram como vai sendo formado o Retângulo de Fibonacci<sup>1</sup>. Caso o autor se interesse em estudar mais sobre a Sequência de Fibonacci, é válida a leitura da obra (AZEVEDO, 2013).

## 1.5 UMA COMPARAÇÃO COM A FATORAÇÃO

Vimos no Capítulo 1 que fatorar um número consiste em decompô-lo em fatores primos. Quando estamos em busca do mdc entre dois números naturais, muitas vezes a fatoração pode ser um caminho rápido para chegar ao resultado. Por exemplo, para calcular  $\text{mdc}(8, 28)$ , poderíamos fatorar os dois números. Sabemos que  $8 = 2^3$ , e  $28 = 2^2 \cdot 7$ , com isso, concluímos que a maior potência de primos em comum aos dois números é  $2^2 = 4$ . Portanto,  $\text{mdc}(8, 28) = 4$ . Uma outra forma de encontrar o  $\text{mdc}(8, 28)$  seria listar os divisores de cada um e encontrar o maior. Na verdade, esse procedimento se resume ao mesmo da fatoração, já que seriam feitas todas as possíveis combinações com as potências dos números primos da fatoração. No caso de  $8 = 2^3$ , seus divisores são  $2^0 = 1$ ,  $2^1 = 2$ ,  $2^2 = 4$  e  $2^3 = 8$ . Já com  $28 = 2^2 \cdot 7$ , seus divisores são  $2^0 \cdot 7^0 = 1$ ,  $2^1 \cdot 7^0 = 2$ ,  $2^2 \cdot 7^0 = 4$ ,  $2^0 \cdot 7^1 = 7$ ,  $2^1 \cdot 7^1 = 14$  e  $2^2 \cdot 7^1 = 28$ . Diante disso, listamos todos os divisores de 8 e 28, que são, respectivamente,  $D(8) = \{1, 2, 4, 8\}$ ;  $D(28) = \{1, 2, 4, 7, 14, 28\}$ . Portanto, facilmente concluímos que  $\text{mdc}(8, 28) = 4$ . No entanto, esse procedimento se torna muito demorado quando estamos trabalhando com números grandes. Por exemplo, usando fatoração, quanto tempo você demoraria para calcular  $\text{mdc}(20222021, 20212022)$ ? Teríamos que encontrar a

<sup>1</sup> Retângulo de Fibonacci é um retângulo que tem dimensões iguais a números da Sequência de Fibonacci.

decomposição desses dois números em fatores primos. Não é algo difícil de se fazer, mas é muito demorado. Já usando o AE, podemos calcular esse resultado de uma forma mais rápida:

$$20222021 = 1 \cdot 20212022 + 9999$$

$$20212022 = 2021 \cdot 9999 + 4043$$

$$9999 = 2 \cdot 4043 + 1913$$

$$4043 = 2 \cdot 1913 + 217$$

$$1913 = 8 \cdot 217 + 177$$

$$217 = 1 \cdot 177 + 40$$

$$177 = 4 \cdot 40 + 17$$

$$40 = 2 \cdot 17 + 6$$

$$17 = 2 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + 1$$

$$5 = 5 \cdot 1 + 0.$$

Logo, concluímos que  $\text{mdc}(20222021, 20212022) = 1$ . De forma computacional, acaba se tornando mais ágil também calcular o mdc entre dois ou mais números inteiros através do AE, isso porque o que está por trás do algoritmo são apenas divisões euclidianas, e isso o computador consegue calcular rapidamente. Para exemplificar isto, vamos considerar o *software sagemath*, que é um *software* para a manipulação de objetos matemáticos. O *sagemath* consegue rapidamente encontrar o mdc entre dois números e ainda, dependendo do código utilizado, pode mostrar a fatoração de cada um desses números e todas as divisões euclidianas para o cálculo do mdc. Porém, com números extremamente grandes, alguns desses códigos demoram mais para mostrar o resultado. Por exemplo, existem números extremamente grandes usados em sistemas de criptografia, tais que a fatoração em números primos de cada um desses números é da forma  $p \cdot q$ , ou seja, eles possuem exatamente dois fatores primos. Esses números são chamados de Números RSA (*Rivest-Shamir-Adleman*) (CAMPOS, 2020). Alguns desses números não tiveram sua fatoração encontrada até hoje, como é o caso dos números *RSA – 260* e *RSA – 270*.

$$p = \text{RSA} - 270 = 233\ 108\ 530\ 344\ 407\ 544\ 527\ 637\ 656\ 910\ 680\ 524\ 145\ 619\ 812\ 480\ 305\ 449\ 042\ 948\ 611\ 968\ 495\ 918\ 245\ 135\ 782\ 867\ 888\ 369\ 318\ 577\ 116\ 418\ 213\ 919\ 268\ 572\ 658\ 314\ 913\ 060\ 672\ 626\ 911\ 354\ 027\ 609\ 793\ 166\ 341\ 626\ 693\ 946\ 596\ 196\ 427\ 744\ 273\ 886\ 601\ 876\ 896\ 313\ 468\ 704\ 059\ 066\ 746\ 903\ 123\ 910\ 748\ 277\ 606\ 548\ 649\ 151\ 920\ 812\ 699\ 309\ 766\ 587\ 514\ 735\ 456\ 594\ 993\ 207$$

$$q = \text{RSA} - 260 = 22\ 112\ 825\ 529\ 529\ 666\ 435\ 281\ 085\ 255\ 026\ 230\ 927\ 612\ 089\ 502\ 470\ 015\ 394\ 413\ 748\ 319\ 128\ 822\ 941\ 402\ 001\ 986\ 512\ 729\ 726\ 569\ 746\ 599\ 085\ 900$$

330 031 400 051 170 742 204 560 859 276 357 953 757 185 954 298 838 958 709 229 238  
 491 006 703 034 124 620 545 784 566 413 664 540 684 214 361 293 017 694 020 846 391  
 065 875 914 794 251 435 144 458 199

O  $RSA - 260$  possui 260 dígitos, enquanto o  $RSA - 270$  possui 270. Apesar de serem números enormes, com um simples código no *sagemath* é possível encontrar o mdc entre eles. O *sagemath* devolve esse resultado em menos de 1 segundo. O código utilizado é  $gcd(a, b)$ , substituindo os valores de  $a$  e  $b$  pelos números  $RSA - 260$  e  $RSA - 270$ . Mostraremos aqui as primeiras e últimas divisões no AE com esses dois números (são necessárias ao todo 547 divisões.)

$$\begin{aligned}
 p &= 10541779476 \cdot q + 2084287 \cdots 6869483 \\
 &\vdots \\
 1201 &= 5 \cdot 237 + 16 \\
 237 &= 14 \cdot 16 + 13 \\
 16 &= 1 \cdot 13 + 3 \\
 13 &= 4 \cdot 3 + 1
 \end{aligned}
 \tag{9}$$

A rapidez com que o *sagemath* mostra que o mdc entre esses dois números é 1 torna-se ainda mais interessante pelo fato desses dois números ainda não terem sido fatorados até hoje. Se usarmos o código que exhibe a fatoração de um número com o  $RSA - 260$  ou  $RSA - 270$ , o software não vai conseguir exibir o resultado. Dessa forma, não é possível encontrar o mdc entre esses dois números pelo método de fatoração. Diante desse exemplo, fica evidente como o AE é um método eficiente e rápido, mesmo para números enormes, em comparação com o método de fatoração. É óbvio que no caso de números muito grandes, que é exatamente o caso dos números  $RSA$ , o AE pode ter muitas divisões euclidianas, mas o computador consegue fazer essas divisões rapidamente, chegando ao resultado final.



## 2 APLICAÇÕES

Diante de tudo que foi visto no primeiro capítulo, finalmente podemos conhecer algumas das aplicações do AE. Apesar de haverem outras, veremos neste trabalho três aplicações: Como o AE pode auxiliar na busca de soluções de equações diofantinas lineares, sua utilização na representação de números racionais em forma de fração contínua e, por fim, como se dá sua contribuição para encontrar soluções de equações da forma  $p = a^2 + b^2$ .

### 2.1 EQUAÇÕES DIOFANTINAS LINEARES

Antes de falarmos precisamente das Equações Diofantinas Lineares, precisamos entender um pouco da história por trás do matemático Diofanto. Estaremos usando como referência, nesta Seção, as obras (EVES, 2011), (HEFEZ, 2014), (SOUZA, 2017) e (BEZERRA, 2018). As **Equações Diofantinas Lineares** recebem esse nome em referência ao matemático Diofanto de Alexandria, considerado como “pai da álgebra”. Esse título não foi por acaso, já que seus estudos foram muito importantes para o desenvolvimento da Álgebra, que posteriormente, contribuíram também para o desenvolvimento da Teoria dos Números (EVES, 2011). Pouco se sabe sobre sua vida, mas a maioria dos historiadores afirmam que seu trabalho se desenvolveu na cidade de Alexandria, no Egito, durante o século III. Apesar dessas poucas informações, há um epigrama<sup>1</sup> na obra *Antologia Grega* que dá alguns detalhes de sua vida: “Diofanto passou 1/6 de sua vida como criança, 1/12 como adolescente e mais 1/7 na condição de solteiro. Cinco anos depois de se casar nasceu-lhe um filho que morreu 4 anos antes de seu pai, com metade da idade (final) de seu pai”.

Sendo  $x$  a idade em que Diofanto morreu, sabemos que

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + 4 + \frac{x}{2} \Rightarrow x = 84.$$

Diante disso, concluímos que Diofanto se casou com 33 anos, teve um filho aos 38 anos (que morreu com 42 anos de idade, quando Diofanto tinha 80 anos) e morreu com cerca de 84 anos. Diofanto escreveu três grandes obras, *Aritmética*, *Sobre números poligonais* e *Porismas*. *Aritmética* foi considerada a obra mais importante e é nela que Diofanto apresenta seus estudos de teoria algébrica dos números e equações de primeiro e segundo grau.

Apesar de existirem muitos resultados interessantes nas obras de Diofanto, nesse trabalho nos preocuparemos com as **Equações Diofantinas Lineares**. Vejamos a seguinte

<sup>1</sup> Composição poética, breve e satírica, que expressa, de forma incisiva, um pensamento ou um conceito malicioso; sátira. Definição encontrada em Oxford Languages.

situação: João vai sacar R\$180,00 em um caixa eletrônico no centro de sua cidade. Ao chegar no caixa, observou que haviam disponíveis apenas notas de R\$10,00 e R\$20,00. De quantas formas o caixa eletrônico pode liberar esse saque?

Considerando  $x$  o número de notas de R\$10,00 e  $y$  o número de notas de R\$20,00, podemos compreender esse problema por meio da equação

$$10x + 20y = 180.$$

Note que, para esse exemplo, só faz sentido obter soluções inteiras não negativas. Mas, como saber se essa equação tem solução? E se tiver, como obter soluções inteiras não negativas? Uma solução possível é  $x = 10$  e  $y = 4$ , mas essa seria a única? Esse tipo de equação é justamente o que estudaremos nesta Seção, as Equações Diofantinas Lineares.

**Definição 2.1.1** Sejam  $a, b$  e  $c \in \mathbb{Z}$  fixos e ambos não nulos. Todas as equações da forma

$$ax + by = c$$

com  $x$  e  $y \in \mathbb{Z}$ , são chamadas de **Equações Diofantinas Lineares**.

Agora que já definimos as equações diofantinas lineares, podemos enunciar o Teorema de Bézout-Bachet, que afirma que o  $\text{mdc}(a, b)$  pode ser escrito como uma combinação linear de  $a$  e  $b$ .

**Teorema 2.1.1** (Bézout-Bachet) Sejam  $a, b \in \mathbb{Z}$ , tal que  $a, b \neq 0$ , existem  $x, y \in \mathbb{Z}$  satisfazendo

$$ax + by = \text{mdc}(a, b).$$

Observe que o Teorema de Bézout é um caso particular das equações diofantinas lineares, quando  $c = \text{mdc}(a, b)$ . A demonstração desse Teorema não é construtiva, mas iremos mostrar como o AE garante a existência de uma solução. Vejamos, com alguns exemplos abaixo, como o AE e o Teorema de Bézout auxiliam na busca de soluções para equações diofantinas lineares.

**Exemplo 2.1.1** Utilizando o AE e o Teorema de Bézout, encontraremos as soluções da equação  $21x + 13y = 1$ . Uma vez que  $1 = \text{mdc}(21, 13)$ , o Teorema 2.1.1 garante a existência de uma solução. O primeiro passo é desenvolver o AE:

$$21 = 1 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0.$$

Pelo AE, temos que  $\text{mdc}(21, 13) = \text{mdc}(13, 8) = \dots = \text{mdc}(3, 2) = \text{mdc}(2, 1) = \text{mdc}(1, 0) = 1$ . O segundo passo é isolar todos os restos não nulos e ir substituindo na expressão, iniciando do último resto não nulo, que é 1. Faremos isso de trás para frente com todos os restos. Vejamos na prática como esse procedimento acontece:

$$1 = 3 - (1 \cdot 2). \quad (10)$$

O resto anterior à 1 é 2, isolaremos ele e substituiremos na Equação (10).

$$1 = 3 - (1 \cdot (5 - (1 \cdot 3))) = (-1) \cdot 5 + 2 \cdot 3.$$

Repetindo o processo com os outros restos, temos:

$$\begin{aligned} 1 &= (-1) \cdot 5 + 2 \cdot (8 - (1 \cdot 5)) \\ &= 2 \cdot 8 + (-3) \cdot 5 \\ &= 2 \cdot 8 + (-3) \cdot (13 - (1 \cdot 8)) \\ &= (-3) \cdot 13 + 5 \cdot 8 \\ &= (-3) \cdot 13 + 5 \cdot (21 - (1 \cdot 13)) \\ &= 5 \cdot 21 + (-8) \cdot 13. \end{aligned}$$

Logo,  $x = 5$  e  $y = -8$ . De fato,  $21 \cdot 5 + 13 \cdot (-8) = 105 - 104 = 1 = \text{mdc}(21, 13)$ .

Usando o Teorema de Bézout podemos afirmar ainda quando uma equação diofantina linear tem ou não solução. Vejamos o seguinte Teorema:

**Teorema 2.1.2** A equação diofantina  $ax + by = c$  admite solução se, e somente se,  $\text{mdc}(a, b)$  divide  $c$ .

*Demonstração.* Considere  $x_0$  e  $y_0$  soluções da equação. Com isso, vale a igualdade

$$ax_0 + by_0 = c.$$

Sabemos que  $\text{mdc}(a, b) \mid a$  e  $\text{mdc}(a, b) \mid b$ , assim, podemos concluir que

$$\text{mdc}(a, b) \mid ax_0 + by_0$$

e, portanto,

$$\text{mdc}(a, b) \mid c.$$

Reciprocamente, suponha que  $\text{mdc}(a, b) \mid c$ . Com isso, podemos concluir que

$$c = \text{mdc}(a, b) \cdot d, \quad (11)$$

para algum inteiro  $d$ . Por outro lado, pelo Teorema 2.1.1, sabemos que existem  $n$  e  $m$  inteiros, tais que

$$\text{mdc}(a, b) = a \cdot n + b \cdot m. \quad (12)$$

Multiplicando ambos os lados da Equação (12) por  $d$ , temos

$$\text{mdc}(a, b) \cdot d = a \cdot (n \cdot d) + b \cdot (m \cdot d). \quad (13)$$

Agora, substituindo (11) em (13), temos

$$c = a \cdot (n \cdot d) + b \cdot (m \cdot d).$$

Logo, a equação diofantina  $ax + by = c$  admite pelo menos a solução  $x = n \cdot d$  e  $y = m \cdot d$ . ■

Com o Teorema 2.1.2, podemos afirmar facilmente se uma equação diofantina linear possui ou não pelo menos uma solução. Vejamos os exemplos abaixo.

**Exemplo 2.1.2** Considerando a equação diofantina  $23x + 150y = 12354$ , podemos afirmar que ela possui ao menos uma solução. Para chegar nesta conclusão, é necessário encontrar o  $\text{mdc}(23, 150)$ , e em seguida, usar o Teorema 2.1.2. Primeiramente, sabemos que

$$150 = 6 \cdot 23 + 12$$

$$23 = 1 \cdot 12 + 11$$

$$12 = 1 \cdot 11 + 1$$

$$11 = 11 \cdot 1 + 0.$$

Logo,  $\text{mdc}(150, 23) = 1$  e  $1 \mid 12354$ , portanto, pelo Teorema 2.1.2, concluímos que a equação possui pelo menos uma solução.

**Exemplo 2.1.3** Considerando agora a equação  $5x + 20y = 33$ , sabemos que

$$20 = 1 \cdot 15 + 5$$

$$15 = 3 \cdot 5 + 0$$

Logo,  $\text{mdc}(5, 20) = 5$ , e sabemos que  $5 \nmid 33$ . Portanto, a equação não possui soluções inteiras.

Enunciaremos agora um resultado que nos dá uma fórmula para encontrar soluções para a equação diofantina linear  $ax + by = c$  sempre que  $\text{mdc}(a, b) = 1$ .

**Teorema 2.1.3** Dados  $x_0$  e  $y_0$  uma solução particular da equação  $ax + by = c$ , onde  $\text{mdc}(a, b) = 1$ . Então as soluções da equação são da forma  $x = x_0 + tb$  e  $y = y_0 - ta$ , para  $t$  variando em  $\mathbb{Z}$ .

*Demonstração.* Considerando  $x$  e  $y$  uma solução qualquer da equação, temos que

$$ax + by = ax_0 + by_0 = c, \quad (14)$$

onde

$$a(x - x_0) = b(y - y_0). \quad (15)$$

De (15), segue que  $a \mid b(y - y_0)$  e  $b \mid a(x - x_0)$ . Como  $\text{mdc}(a, b) = 1$ , segue  $a \mid (y - y_0)$  e  $b \mid (x - x_0)$ . Logo,

$$y - y_0 = ta; x - x_0 = sb, \quad (16)$$

para alguns inteiros  $t$  e  $s$ . Substituindo (16) em (15), temos

$$asb = bta \Rightarrow s = t.$$

Logo, substituindo  $s = t$  em (16), temos que a solução é dada por  $x = x_0 + bt$  e  $y = y_0 - at$ . Substituindo  $x = x_0 + bt$  e  $y = y_0 - at$  na equação  $ax + by = c$ , temos

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + abt + by_0 - abt = ax_0 + by_0 = c.$$

■

Com o Teorema 2.1.3 podemos retomar ao Exemplo 2.1.2 e encontrar suas soluções inteiras.

**Exemplo 2.1.4** Dada a equação  $23x + 150y = 12354$ , sabemos que

$$150 = 6 \cdot 23 + 12$$

$$23 = 1 \cdot 12 + 11$$

$$12 = 1 \cdot 11 + 1$$

$$11 = 11 \cdot 1 + 0,$$

e que  $\text{mdc}(150, 23) = 1$ . Logo, fazendo o procedimento apresentado no Exemplo 2.1.1, temos

$$\begin{aligned} 1 &= 12 - 1 \cdot 11 \\ &= 12 - 1 \cdot (23 - 1 \cdot 12) \\ &= -23 + 2 \cdot 12 \\ &= -23 + 2 \cdot (150 - 6 \cdot 23) \\ &= 23 \cdot (-13) + 150 \cdot (2) \end{aligned}$$

Com isso, concluímos que  $x = -13$  e  $y = 2$  é uma solução para a equação  $23x + 150y = 1$ . Mas, como  $c = 12354 = \text{mdc}(a, b) \cdot 12354$ , temos  $x_0 = (-13) \cdot 12354 = -160602$  e  $y_0 =$

$2 \cdot 12354 = 24708$  sendo uma solução para  $23x + 150y = 12354$ . Portanto, pelo Teorema 2.1.3, concluímos que as soluções da equação são dadas por  $x = -160602 + t \cdot 150$  e  $y = 24708 - t \cdot 23$ . Se quisermos ainda encontrar as soluções não negativas, basta apenas resolver o sistema

$$\begin{cases} -160602 + t \cdot 150 \geq 0 \\ 24708 - t \cdot 23 \geq 0 \end{cases}.$$

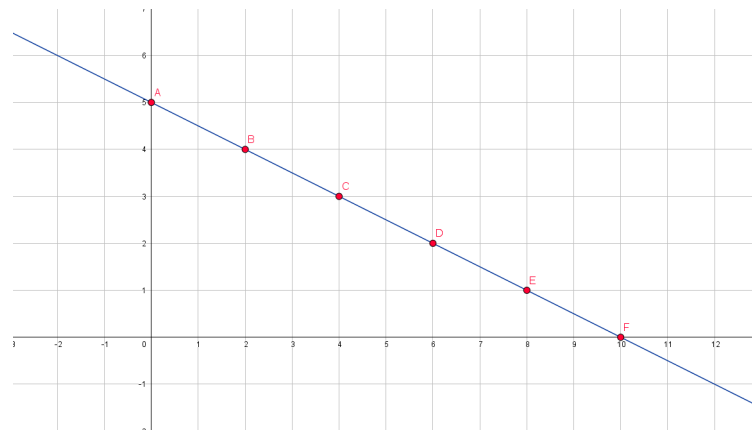
Resolvendo esse sistema, concluímos que  $t \in \left[ \frac{26767}{25}, \frac{24708}{23} \right]$ . Como queremos  $t \in \mathbb{Z}$ , temos que  $t = 1071$  ou  $t = 1072$  ou  $t = 1073$  ou  $t = 1074$  para soluções não negativas.

Note ainda que, por se tratar de uma equação linear nas variáveis  $x$  e  $y$ , encontrar soluções inteiras pode ser interpretado como encontrar pares ordenados de números inteiros na reta determinada pela equação  $ax + by = c$ . Vejamos um exemplo:

**Exemplo 2.1.5** O professor João pretende separar a turma de Teoria dos Números em grupos de 3 e 6 alunos para que eles possam fazer mini-projetos usando o *software sagemath*. Sabendo que a turma é composta de 30 alunos, quantos grupos de 3 e 6 pessoas será possível montar de modo que nenhum aluno fique sem equipe?

Interpretando esse problema em forma de uma equação, sendo  $x$  o número de grupos de 3 pessoas e  $y$  o número de grupos de 6 pessoas, teremos  $3x + 6y = 30$ . Assim, como estamos falando de quantidades de grupos de alunos, só faz sentido encontrar soluções inteiras e não negativas. Note que encontrar essas soluções é equivalente a encontrar pares ordenados inteiros e não negativos da reta determinada pela equação  $3x + 6y = 30$  (ou ainda,  $x + 2y = 10$ ). Vejamos essa reta no plano cartesiano:

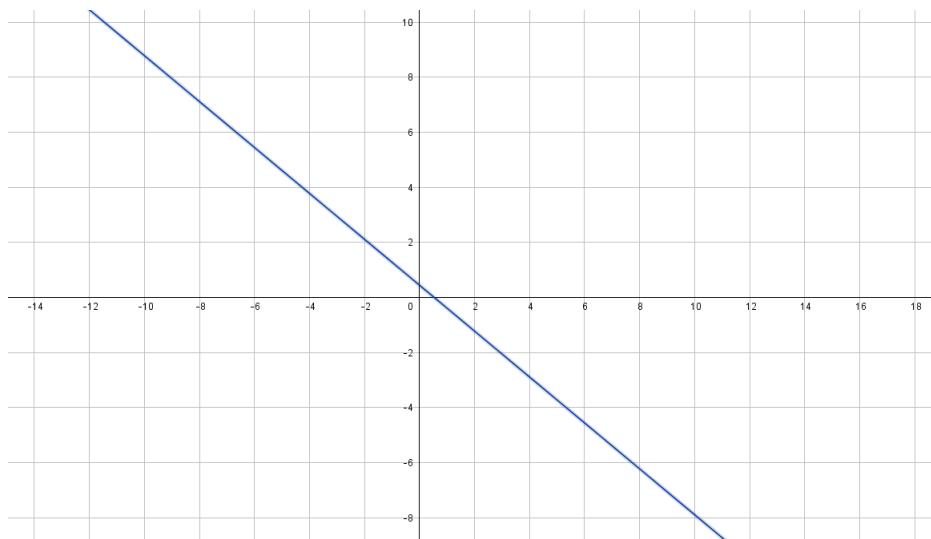
**Figura 2.1 – Soluções inteiras e não negativas da equação  $3x + 6y = 30$**



Fonte: Elaborada pelo Autor

Perceba que os pares ordenados formados por números inteiros e não negativos são  $(0, 5), (2, 4), (4, 3), (6, 2), (8, 1)$  e  $(10, 0)$ . Logo, o professor João pode montar grupos de 3 e 6 pessoas de seis formas distintas. Observe na Figura 2.1 que também existem pares ordenados com números inteiros, mas com pelo menos uma coordenada negativa, são os pontos  $(-2, 6)$  e  $(12, -1)$ . Esses pares também são soluções inteiras da equação  $3x + 6y = 30$ , mas não condizem com as soluções que procuramos para o nosso exemplo. Agora, se tivermos, por exemplo, a equação  $15x + 18y = 4$ , a priori não conseguimos encontrar nenhum par ordenado de números inteiros na reta determinada pela equação.

**Figura 2.2 – Reta determinada pela equação  $15x + 18y = 4$**



**Fonte: Elaborada pelo Autor**

Apesar da Figura 2.2 não exibir todos os pontos da reta, podemos verificar se realmente não há nenhuma solução inteira através do Teorema 2.1.2. Portanto, esse método de visualizar pares ordenados de números inteiros em retas não é suficiente em alguns casos. Porém, vimos nesta Seção que para verificar se uma equação diofantina linear tem soluções, encontrar soluções (caso existam) ou ainda encontrar possíveis soluções não negativas, exige basicamente conhecimento do AE.

## 2.2 FRAÇÕES CONTÍNUAS

Nesta Seção iremos falar de uma outra aplicação importante do AE, as Frações Contínuas. As Frações Contínuas apresentam algumas aplicações importantes para a Matemática, além da Física e Química. Algumas dessas aplicações se tratam de encontrar aproximações em forma de frações contínuas para números e expressões irracionais, cálculo de logaritmos e soluções de equações. Nesta Seção, entretanto, veremos uma pequena parte desse objeto de estudo. Focaremos no que tange ao AE, sendo, portanto, as representações

em frações contínuas de frações ordinárias com números racionais. Estaremos nos fundamentando nesta Seção nas obras (NASCIMENTO, 2013), (DUTRA, 2019), (OLIVEIRA, 2014), (PACCI; RODRIGUES, 2013), (COUTO, 2017), (TUYL, 1996) e (SANTOS, 1998). Caso o leitor queira ver mais aplicações das Frações Contínuas, as obras acima oferecem uma excelente abordagem sobre o assunto.

### 2.2.1 Uma Breve Contextualização

As informações citadas aqui foram retiradas das referências citadas no início da Seção 2.2. O ano exato e o estudioso que teria dado início aos estudos acerca de Frações Contínuas é algo que não se pode afirmar, já que há evidências da presença das Frações Contínuas em diferentes épocas e civilizações, mas, tradicionalmente, atribuem seu início ao momento em que houve a formulação do Algoritmo de Euclides, pois o algoritmo teria contribuído significativamente para seu estudo. Aryabhata (476 - 550), matemático indiano, utilizou as frações contínuas, mas de forma limitada, apenas para resolver alguns problemas de equações diofantinas. No século XVI, surge novamente estudiosos das Frações Contínuas, um deles foi Rafael Bombelli (1526 - 1572) que encontrou uma aproximação em forma de fração contínua para o número irracional  $\sqrt{13}$ .

Um outro cientista da mesma época, chamado Pietro Antonio Cataldi (1548 - 1626), encontrou uma aproximação para  $\sqrt{18}$ . O matemático inglês John Wallis (1616 - 1703), por sua vez, apresenta em seu livro "*Opera Mathematica*", fundamentos básicos de frações contínuas, discutindo também como calcular o n-ésimo convergente. A primeira aplicação prática de frações contínuas foi realizada pelo matemático e astrônomo Christian Huygens (1629 - 1695), que utilizou frações contínuas para encontrar relações de transmissão entre engrenagens para construir um modelo reduzido do sistema solar com uma escala adequada. Tratando-se da teoria moderna de frações contínuas, seus principais contribuidores foram Leonhard Euler (1707 - 1783), Johan Heinrich Lambert (1728 - 1777) e Joseph Louis Lagrange (1736 - 1813).

Euler encontrou aproximações para os números  $e$  e  $e^2$ , provando sua irracionalidade. Além disso, Euler também mostrou que todo número racional pode ser representado por uma fração contínua finita, assim como todo número irracional pode ser expresso como uma fração contínua infinita. Outro resultado que Euler mostrou, foi que toda fração contínua periódica é raiz de uma equação de segundo grau. Lambert, por sua vez, encontrou aproximações para  $\frac{e^x-1}{e^x+1}$ ,  $\log(1+x)$ ,  $\arctan(x)$  e  $\tan(x)$ , provando que  $e^x$  e  $\tan x$  são irracionais se  $x$  for racional. Lagrange utilizou as frações contínuas para encontrar aproximações para raízes irracionais. A teoria de Frações Contínuas continua se desenvolvendo até hoje, contribuindo com pesquisas de diversas áreas, como química, física, computação e teoria dos números. Essa pequena contextualização histórica é importante



para que o leitor conheça os pesquisadores que contribuíram com essa teoria, além de entender como se deu a construção desse objeto de estudo.

### 2.2.2 O AE aplicado à Frações Contínuas

Durante todo esse trabalho citamos alguns conjuntos numéricos, como os  $\mathbb{N}$  (naturais),  $\mathbb{Z}$  (inteiros) e  $\mathbb{R}$  (reais). Não nos aprofundamos em nenhum, mas o que o leitor precisa saber é que  $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ . Dessa forma, sendo  $\mathbb{Q}$  o conjunto dos números racionais, sabemos que todos os seus elementos são também elementos do conjunto  $\mathbb{R}$ . Mas a recíproca nem sempre é válida, visto que existem números reais que não são racionais. Em suma, um número real é considerado também um número racional, quando ele pode ser representado por uma razão entre dois números inteiros, com o denominador um número diferente de 0:

$$\mathbb{Q} = \left\{ \frac{a}{b}; a, b \in \mathbb{Z}; b \neq 0 \right\},$$

no qual  $a$  recebe o nome de **numerador** e  $b$  recebe o nome de **denominador**. Quando um número não é racional, dizemos que ele é irracional (pertence ao conjunto  $\mathbb{I}$ ). É válido mencionar também que  $\mathbb{Q} \cup \mathbb{I} = \mathbb{R}$ . Apesar de não podermos representar números irracionais como razão entre dois números inteiros, com denominador não nulo, podemos encontrar aproximações por meio de **Frações Contínuas** utilizando o AE. Esse procedimento também vale para encontrar outras representações fracionárias para números racionais, mas primeiro iremos definir o que é uma Fração Contínua e de que forma o AE pode ser aplicado nessa teoria. Para introduzirmos o conteúdo de frações contínuas, vejamos primeiro o AE, por exemplo, com os números 43 e 30:

$$43 = 1 \cdot 30 + 13$$

$$30 = 2 \cdot 13 + 4$$

$$13 = 3 \cdot 4 + 1$$

$$4 = 4 \cdot 1 + 0.$$

Assim, podemos representar  $\frac{43}{30}$  da forma

$$\begin{aligned} \frac{43}{30} &= \frac{1 \cdot 30 + 13}{30} \\ &= 1 + \frac{13}{30} \\ &= 1 + \frac{1}{\frac{30}{13}} \end{aligned}$$

$$\begin{aligned}
&= 1 + \frac{1}{\frac{2 \cdot 13 + 4}{13}} \\
&= 1 + \frac{1}{2 + \frac{4}{13}} \\
&= 1 + \frac{1}{2 + \frac{\frac{1}{13}}{\frac{4}{13}}} \\
&= 1 + \frac{1}{2 + \frac{1}{\frac{3 \cdot 4 + 1}{4}}} \\
&= 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4}}}.
\end{aligned}$$

Essa representação recebe o nome de Fração Contínua e é dela que falaremos nesta Seção. Para iniciarmos essa discussão, voltaremos a descrição do AE. Relembre que, dados  $a$  e  $b \in \mathbb{Z}$ ;  $a > b$  e  $a, b \neq 0$ , utilizando sucessivas divisões, podemos desenvolver o AE da seguinte forma:

$$\begin{aligned}
a &= q_1 b + r_1, & 0 \leq r_1 < b; \\
b &= q_2 r_1 + r_2, & 0 \leq r_2 < r_1; \\
r_1 &= q_3 r_2 + r_3, & 0 \leq r_3 < r_2; \\
&\vdots \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, & 0 \leq r_{n-1} < r_{n-2}; \\
r_{n-2} &= q_n r_{n-1} + r_n, & 0 \leq r_n < r_{n-1}; \\
r_{n-1} &= q_{n+1} r_n + 0,
\end{aligned}$$

com  $r_n = \text{mdc}(a, b)$ . Interpretando essas mesmas divisões de uma outra forma, veja que

$$\frac{a}{b} = q_1 + \frac{r_1}{b} \tag{17}$$

$$\frac{b}{r_1} = q_2 + \frac{r_2}{r_1} \tag{18}$$

$$\frac{r_1}{r_2} = q_3 + \frac{r_3}{r_2}. \quad (19)$$

Fazendo isso com todas as equações, chegamos na última com o seguinte resultado:

$$\frac{r_{n-1}}{r_n} = q_{n+1}. \quad (20)$$

Substituindo (18) em (17), temos

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}}. \quad (21)$$

Da mesma forma, substituindo (19) em (21), temos

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{r_3}{r_2}}}. \quad (22)$$

Fazendo isso com todas as equações, chegamos em

$$\frac{a}{b} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{1}{q_4 + \dots \frac{1}{q_{n+1}}}}}$$

Essa representação de  $\frac{a}{b}$  nós chamamos de **Fração Contínua**, com  $q_2, q_3, q_4, \dots$  números inteiros e  $q_1$  é um número inteiro positivo. É natural também considerar casos em que as divisões sucessivas acontecem indefinidamente, iremos considerar tais exemplos mais adiante. Um exemplo de fração contínua é

$$3 + \frac{1}{3 + \frac{1}{3 + \frac{1}{3 + \dots}}}$$

Para facilitar a notação de frações contínuas, iremos representá-las como  $[q_1; q_2, q_3, q_4, \dots, q_{n+1}]$ . O termo  $q_1$  é a parte inteira da fração contínua, sendo separado dos outros números por ponto e vírgula, justamente para ser evidenciado como parte inteira. A parte inteira recebe o nome de **primeiro quociente incompleto**. Já os outros números  $q_2, q_3, q_4, \dots, q_n$  são os demais **quocientes incompletos**. Vejamos alguns exemplos de como encontrar a fração contínua de um número racional usando o AE.

**Exemplo 2.2.1** No Capítulo 1, vimos o desenvolvimento do AE para encontrar o  $\text{mdc}(2022, 108)$ . O primeiro passo para encontrar a representação de  $\text{mdc}(2022, 108)$  em frações contínuas é justamente desenvolver o algoritmo com os dois números. Como 2022 é o numerador, ele será o número que vai ser dividido primeiro. Como 108 é o denominador, ele vai ser o primeiro divisor no AE.

$$2022 = 18 \cdot 108 + 78$$

$$108 = 1 \cdot 78 + 30$$

$$78 = 2 \cdot 30 + 18$$

$$30 = 1 \cdot 18 + 12$$

$$18 = 1 \cdot 12 + 6$$

$$12 = 2 \cdot 6 + 0.$$

Utilizando agora a definição de frações contínuas, destacaremos todos os quocientes do algoritmo, seguindo a mesma ordem das divisões. Portanto,  $q_1 = 18, q_2 = 1, q_3 = 2, q_4 = 1, q_5 = 1, q_6 = 2$ . Substituindo os quocientes na forma geral das frações contínuas, temos

$$\frac{2022}{108} = 18 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}}}}}$$

Representando da outra forma,  $\frac{a}{b} = [18; 1, 2, 1, 1, 2]$ . Veja que, como  $\frac{2022}{108} \in \mathbb{Q}$ , o número de termos da fração contínua foi finito.

**Observação.** Nos casos em que o numerador é menor que o denominador, o procedimento é o mesmo. O numerador é o primeiro número a ser dividido e o denominador é o primeiro divisor.

Com esse exemplo, podemos nos questionar se há outra fração contínua finita que represente  $\frac{2022}{108}$  e se qualquer número racional tem representação em forma de fração contínua. A resposta para essas perguntas pode ser dada pelos seguintes Teoremas:

**Teorema 2.2.1** Qualquer número racional pode ser representado por uma fração contínua simples finita. Reciprocamente, qualquer fração contínua simples finita representa um número racional. Além disso, há duas possibilidades de representação por uma fração contínua: uma com um número par de termos, e a outra, com um número ímpar. Uma com o último termo igual a 1, e a outra, com esse termo maior de que 1.

A demonstração do Teorema 2.2.1 pode ser encontrada em (SANTOS, 1998). De acordo com os Teorema 2.2.1, podemos concluir que  $\frac{2022}{108}$ , por ser um número racional, tem representação em forma de uma fração contínua finita (como vimos no Exemplo 2.2.1). Além disso, há duas representações possíveis: uma já vimos no Exemplo 2.2.1 e a outra pode ser obtida com uma pequena mudança no último quociente incompleto. Se usarmos  $2 = 1 + \frac{1}{1}$ , chegaremos à outra fração contínua simples:

$$\frac{2022}{108} = 18 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}}}}$$

Agora, tendo em mente esses dois teoremas, veremos mais alguns exemplos.

**Exemplo 2.2.2** Se quisermos saber a representação em fração contínua de  $\frac{3082}{225}$ , primeiro utilizaremos o AE:

$$\begin{aligned} 3082 &= 13 \cdot 225 + 157 \\ 225 &= 1 \cdot 157 + 68 \\ 157 &= 2 \cdot 68 + 21 \\ 68 &= 3 \cdot 21 + 5 \\ 21 &= 4 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0. \end{aligned}$$

Com o conhecimento que já temos de fração contínua, podemos afirmar que:  $\frac{3082}{225} = [13; 1, 2, 3, 4, 5]$ . Há ainda a outra possibilidade de representação, mas não é necessário encontrar.

**Exemplo 2.2.3** Da mesma forma que o exemplo anterior, iremos encontrar a fração contínua de  $\frac{6164}{450}$ .

$$\begin{aligned} 6164 &= 13 \cdot 450 + 314 \\ 450 &= 1 \cdot 314 + 136 \\ 314 &= 2 \cdot 136 + 42 \\ 136 &= 3 \cdot 42 + 10 \\ 42 &= 4 \cdot 10 + 2 \\ 10 &= 5 \cdot 2 + 0. \end{aligned}$$

Dessa forma, concluímos que  $\frac{6164}{450} = [13; 1, 2, 3, 4, 5]$ .

A escolha desses dois últimos exemplos não foi aleatória. Note que ambas frações possuem a mesma fração contínua. Perceba também que  $\frac{2}{2} \cdot \frac{3082}{225} = \frac{6164}{450}$ . Isso acontece porque frações equivalentes possuem a mesma representação em frações contínuas. Veja só, considerando  $\frac{a}{b}$ , o desenvolvimento do AE é dado por:

$$\begin{aligned} a &= q_1b + r_1, & 0 \leq r_1 < b; \\ b &= q_2r_1 + r_2, & 0 \leq r_2 < r_1; \\ r_1 &= q_3r_2 + r_3, & 0 \leq r_3 < r_2; \\ &\vdots \\ r_{n-1} &= q_{n+1}r_n + 0. \end{aligned}$$

Logo,  $\frac{a}{b} = [q_1; q_2, q_3, \dots, q_{n+1}]$ . Agora, considerando uma fração equivalente  $\frac{ac}{bc}$ , tal que  $c \in \mathbb{Z}$  podemos entender a construção do AE da seguinte forma: Sendo  $a = q_1b + r_1$ , temos que

$$ac = (q_1b + r_1)c = q_1(bc) + r_1c.$$

Agora, para a próxima linha do AE, temos

$$bc = (q_2r_1 + r_2)c = q_2(r_1c) + r_2c.$$

Fazendo sucessivamente até o fim do AE, chegamos em

$$\begin{aligned} ac &= q_1(bc) + r_1c \\ bc &= q_2(r_1c) + r_2c \\ r_1c &= q_3(r_2c) + r_3c \\ &\vdots \\ r_{n-1}c &= q_{n+1}(r_nc) + 0. \end{aligned}$$

Portanto,  $\frac{ac}{bc} = \frac{a}{b} = [q_1; q_2, q_3, \dots, q_{n+1}]$ .

Vimos no primeiro Capítulo, na Seção de Interpretação Geométrica do AE, como números consecutivos da Sequência de Fibonacci apresentam um comportamento curioso quanto ao AE. Isso se dá pelo fato de todos os quocientes das divisões sucessivas (exceto o último) serem iguais a 1. Da mesma forma, é muito interessante observar como se dão as representações em forma de frações contínuas simples com números dessa sequência, já que as frações contínuas simples estão estritamente ligadas aos quocientes do algoritmo. Veremos alguns exemplos e por fim, analisaremos a relação das frações contínuas com números da sequência com a fração contínua do número de ouro.

**Exemplo 2.2.4** Considerando os números 13 e 8, vamos encontrar a fração contínua que representa  $\frac{13}{8}$ . Utilizando o AE, temos

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0.$$

Logo,  $\frac{13}{8} = [1; 1, 1, 1, 2]$ . Mas, como  $2 = 1 + \frac{1}{1}$ , podemos dizer que  $\frac{13}{8} = [1; 1, 1, 1, 1, 1]$ .

**Exemplo 2.2.5** Agora, trabalharemos com  $\frac{21}{13}$ :

$$21 = 1 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0.$$

Portanto, concluímos que  $\frac{21}{13} = [1; 1, 1, 1, 1, 2] = [1; 1, 1, 1, 1, 1, 1]$ .

**Exemplo 2.2.6** Encontrando a fração contínua simples de  $\frac{34}{21}$ , temos

$$34 = 1 \cdot 21 + 13$$

$$21 = 1 \cdot 13 + 8$$

$$13 = 1 \cdot 8 + 5$$

$$8 = 1 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0.$$

Logo,  $\frac{34}{21} = [1; 1, 1, 1, 1, 1, 2] = [1; 1, 1, 1, 1, 1, 1, 1]$ .

De forma geral, esses exemplos mostram como as frações contínuas de números consecutivos da Sequência de Fibonacci possuem todos os quocientes incompletos iguais a

1. Essa semelhança com as frações contínuas simples dos Exemplos 2.2.4, 2.2.5 e 2.2.6 não é por acaso. Isso acontece porque o número de ouro pode ser obtido por meio da divisão entre o  $n$ -ésimo e o termo anterior, de tal forma que, quanto maior for o  $n$ -ésimo termo, mais aproximado será do valor real do número de ouro. O procedimento para encontrar a fração contínua de  $\phi$  (número de ouro) é bastante simples. Para isso, usando o fato de que  $\phi$  é raiz do polinômio  $x^2 - x - 1$ , temos:

$$\begin{aligned}\phi^2 - \phi - 1 &= 0 \\ \frac{\phi^2}{\phi} - \frac{\phi}{\phi} - \frac{1}{\phi} &= \frac{0}{\phi} \\ \phi - 1 - \frac{1}{\phi} &= 0 \\ \phi &= 1 + \frac{1}{\phi}.\end{aligned}$$

Como sabemos que  $\phi = 1 + \frac{1}{\phi}$ , podemos fazer essa substituição e continuar a fração contínua. Dessa forma, temos

$$\begin{aligned}\phi &= 1 + \frac{1}{1 + \frac{1}{\phi}} \\ &= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\phi}}} \\ &= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\phi}}}}\end{aligned}$$



$$= 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\phi}}}}}$$

Esse procedimento continua infinitamente, isso porque  $\phi$  é um número irracional. Há um teorema que afirma que a fração contínua de um número irracional tem infinitos termos. Enunciaremos esse teorema logo abaixo, mas quanto à fração contínua de  $\phi$ , ela vai ficar com essa cara:

$$\phi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\dots}}}}}}$$

Assim, semelhante aos Exemplos 2.2.4, 2.2.5 e 2.2.6, a fração contínua de  $\phi$  é dada por  $[1; 1, 1, 1, 1, 1, 1, 1, 1, 1, 1, \dots]$ .

**Teorema 2.2.2** Qualquer fração contínua simples infinita representa um número irracional. Reciprocamente, qualquer número irracional  $x$  pode ser representado de forma única essencialmente única por uma fração contínua simples infinita  $[q_1; q_2, q_3, q_4, \dots]$ .

Dados os Teoremas 2.2.1 e 2.2.2, podemos enunciar um outro teorema:

**Teorema 2.2.3** Se um número  $a \in \mathbb{R}$ , então ele possui representação em frações contínuas e ela é essencialmente única.

Com o Teorema 2.2.3, sabemos que qualquer número real pode ser escrito como fração contínua, a diferença é o procedimento usado para chegar nessa representação. Usamos o AE quando estamos trabalhando com números racionais. Já para números irracionais, o procedimento é similar ao que usamos para encontrar a fração contínua de  $\phi$  (que é um número irracional). Apesar de estarmos focando apenas no uso do AE neste trabalho, ou seja, frações contínuas de números racionais, encontraremos a fração contínua de  $\pi$  para ilustrarmos o método para números irracionais. Para isso, tome  $\pi = 3,141592\dots$ . Assim, temos

$$\begin{aligned}
\pi &= 3,141592\dots \\
&= 3 + 0,141592\dots \\
&= 3 + \frac{1}{7,06251\dots} \\
&= 3 + \frac{1}{7 + 0,06251\dots} \\
&= 3 + \frac{1}{7 + \frac{1}{\frac{1}{0,06251\dots}}} \\
&= 3 + \frac{1}{7 + \frac{1}{15,99744\dots}} \\
&= 3 + \frac{1}{7 + \frac{1}{15 + 0,99744\dots}} \\
&= 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{0,99744\dots}}} \\
&= 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1,00257\dots}}} \\
&= 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \dots}}}
\end{aligned}$$

Como  $\pi$  é um número irracional, sua fração contínua tem infinitos termos. Apesar disso, vimos como as frações contínuas fornecem aproximações em racionais para números irracionais. Quanto mais termos encontrarmos, mais aproximado será do valor de  $\pi$ . A fração contínua de  $\pi$  é dada por

$$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, \dots].$$

Se considerarmos apenas  $\pi = [3; 7, 15]$ , teríamos a fração contínua

$$3 + \frac{1}{7 + \frac{1}{15}} = \frac{333}{106} \approx 3,14150943.$$

As aproximações por frações contínuas são as melhores para se obter aproximações para números irracionais. Por exemplo, conseguimos uma boa aproximação para  $\pi$  usando apenas a fração contínua  $[3; 7, 15] = \frac{333}{106}$ . Se fossemos usar expansão decimal, teríamos a fração  $\frac{314151}{100000}$ , com números bem maiores que 333 e 106.

Dentro desse universo de frações contínuas de números irracionais, há um resultado bastante interessante sobre números irracionais que são raízes de um polinômio de segundo grau. Segundo (SANTOS, 1998), Lagrange mostrou em 1770 que a fração contínua infinita que representa um número irracional é periódica, se e somente se, esse irracional for raiz do polinômio  $ax^2 + bx + c = 0$ , com  $a, b$  e  $c \in \mathbb{Z}$ . Fração Contínua Periódica é aquela que tem uma sequência de números se repetindo periodicamente. Como vimos anteriormente, a fração contínua de  $\phi$  é periódica, dado que  $\phi = [1; 1, 1, 1, 1, 1, \dots]$ , com o período 1 (sequência de número que se repete) da fração contínua. Com isso, podemos afirmar que  $\phi$  é raiz de um polinômio de segundo grau.

**Exemplo 2.2.7** Para encontrar o polinômio que  $\phi$  é raiz, considere sua fração contínua

$$\phi = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$$

recuperar esse polinômio, podemos fazer o procedimento a seguir, considerando  $x = \phi$ :

$$x = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$$

$$x - 1 = \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \dots}}}$$

(23)

$$x - 1 = \frac{1}{1 + \left( \frac{1}{1 + \frac{1}{1 + \dots}} \right)}$$

$$x - 1 = \frac{1}{1 + (x - 1)}$$

$$x - 1 = \frac{1}{x}$$

$$x^2 - x = 1$$

$$x^2 - x - 1 = 0.$$

Portanto  $\phi \approx \frac{1+\sqrt{5}}{2}$  é raiz da equação de segundo grau  $x^2 - x - 1 = 0$ .

**Exemplo 2.2.8** Vejamos a expansão de  $\sqrt{2}$ . Sabemos que  $1 < \sqrt{2} < 2$ , já que  $\sqrt{1} = 1$  e  $\sqrt{4} = 2$ . Logo, podemos deduzir que

$$\sqrt{2} = 1 + \frac{1}{x},$$

com  $x > 1$ . Dessa forma, é equivalente afirmar que

$$\sqrt{2} = \frac{x+1}{x}$$

$$\sqrt{2} \cdot x = x + 1$$

$$\sqrt{2} \cdot x - x = 1$$

$$(\sqrt{2} - 1) \cdot x = 1$$

$$x = \frac{1}{\sqrt{2} - 1}$$

$$x = \sqrt{2} + 1.$$

Substituindo o valor de  $x$  na primeira equação, temos:

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2} + 1}.$$

Note que no último denominador aparece novamente  $\sqrt{2}$ . Iremos agora fazer o mesmo procedimento anterior.

$$\sqrt{2} = 1 + \frac{1}{1 + \frac{1}{x} + 1}$$

$$\begin{aligned}
&= 1 + \frac{1}{2 + \frac{1}{x}} \\
&= 1 + \frac{1}{2 + \frac{1}{\sqrt{2} + 1}}.
\end{aligned}$$

Repetindo o mesmo processo diversas vezes, chegaremos em

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \dots}}}}.$$

Assim,  $\sqrt{2} = [1; 2, 2, 2, 2, \dots]$ , que é uma fração contínua periódica. Dessa forma,  $\sqrt{2}$  é raiz de um polinômio de segundo grau. Fazendo o mesmo procedimento do Exemplo 2.2.7, encontramos que o polinômio é  $x^2 - 2 = 0$ .

Há outros números irracionais que têm fração contínua periódica com períodos maiores, por exemplo  $\sqrt{11} = [3; 3, 6, 3, 6, \dots]$ . No entanto, não nos aprofundaremos nessa parte de frações contínuas. Caso o leitor se interesse, pode consultar a referência (COUTO, 2017).

### 2.3 SOLUÇÕES DA EQUAÇÃO $p = a^2 + b^2$

Vimos na Seção 2.1 como o AE pode auxiliar na busca de soluções para equações diofantinas lineares. Acontece que o AE pode ser usado para encontrar soluções de outros tipos de equações. Veremos nesta Seção como escrever um número primo (veremos que não é qualquer primo) como soma de quadrados perfeitos, em outras palavras, como o AE pode nos auxiliar a encontrar soluções para a equação  $p = a^2 + b^2$ . Estaremos nos espelhando nesta Seção nas obras (SANTOS, 1998) e (WAGON, 1990).

**Teorema 2.3.1** Um primo  $p$  pode ser escrito de forma única como soma de quadrados perfeitos se, e somente se  $p \equiv 1 \pmod{4}$ , isto é,  $p = 4k + 1$  para algum  $k$  inteiro positivo.

A demonstração pode ser encontrada na referência (Plínio).

Sendo  $p = 13$ , sabemos que  $13 = 4 \cdot 3 + 1$ . Assim, 13 pode ser escrito como soma de dois quadrados perfeitos. Neste caso,  $13 = 3^2 + 2^2$ . Da mesma forma,  $17 = 4 \cdot 4 + 1$  e

pode ser escrito como  $17 = 4^2 + 1^2$ . No entanto, apenas primos da forma  $4k + 1$  podem ter essa representação. No caso de  $p = 7$ , sabemos que  $7 \neq 4k + 1$  para qualquer  $k$  inteiro, com isso, concluímos que 7 não pode ser escrito como soma de dois quadrados perfeitos. No entanto, como encontrar os valores de  $a$  e  $b$  para qualquer número primo da forma  $4k + 1$ ?

Vimos que com primos pequenos, como 13 e 17, conseguimos encontrar sem muita dificuldade testando alguns valores para  $a$  e  $b$ , mas quando estamos trabalhando com números primos grandes, esse método pode se tornar muito demorado. Para isso, podemos usar um algoritmo que utiliza resultados elementares e o AE. A demonstração de que o algoritmo realmente funciona é longa e por isso iremos omitir, mas o leitor pode acessá-la na referência (WAGON, 1990). Dado um número primo  $p$  da forma  $4k + 1$ , para encontrar  $a$  e  $b$ , seguiremos os dois passos a seguir:

Passo 1. Encontre  $x$ , tal que  $x^2 \equiv -1 \pmod{p}$ ;

Passo 2. Aplique o algoritmo de Euclides a  $p$  e  $x$ ;

Passo 3. Encontre os primeiros dois restos do AE menores que  $\sqrt{p}$ . Os dois primeiros restos imediatamente menores que  $\sqrt{p}$  serão  $a$  e  $b$ .

O passo 1 pode dar um pouco mais de trabalho dependendo do valor do número primo. Apesar disso, há uma forma mais simples de encontrar o valor de  $x$ . Para isso, relembre que na Seção (preliminares), vimos que, dados  $x$  e  $p$  coprimos,

$$x^{p-1} \equiv 1 \pmod{p}.$$

A formalização rigorosa para a discussão seguinte precisa de conceitos de Álgebra Abstrata, mas o argumento funciona intuitivamente. Dizer que  $x^{p-1} \equiv 1 \pmod{p}$  equivale a dizer que o polinômio  $f(x) = x^{p-1} - 1$  se anula módulo  $p$  em todo elemento não nulo módulo  $p$ . Mas podemos fatorar  $f(x)$  da seguinte forma

$$f(x) = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1) = (x^{2k} - 1)(x^{2k} + 1).$$

De forma algébrica, como todo elemento não nulo módulo  $p$  é uma raiz de  $f(x)$  e  $f(x)$  se fatora em dois polinômios de mesmo grau, então metade dos números módulo  $p$  anulam  $(x^{2k} - 1)$  e a outra metade anula  $(x^{2k} + 1)$ . Considerando o segundo caso e tomando  $x'$  um número que anula  $(x^{2k} + 1)$ , temos

$$((x')^{2k} + 1) \equiv 0 \pmod{p} \Rightarrow (x')^{2k} \equiv -1 \pmod{p}.$$

Note que  $x^{2k} = (x^k)^2$ . Assim, como  $((x')^{2k} + 1) \equiv 0 \pmod{p}$ , temos que

$$(x')^{2k} \equiv ((x')^k)^2 \equiv -1 \pmod{p}.$$

Portanto, se pegarmos  $x = (x')^k$ , temos

$$x^2 = ((x')^k)^2 \equiv -1 \pmod{p}.$$

Assim, o problema se resume a encontrar  $(x')^k$  tal que  $((x')^k)^2 \equiv -1 \pmod{p}$ .

**Exemplo 2.3.1** Tomando  $p = 29 = 4 \cdot 7 + 1$ , faremos o passo a passo descrito:

Passo 1. Precisamos encontrar  $x$ , tal que  $x^2 \equiv -1 \pmod{29}$ . Como  $p = 29 = 4 \cdot 7 + 1$ , concluímos que  $k = 7$ . Estamos então procurando um  $x'$  tal que  $((x')^7)^2 \equiv -1 \pmod{29}$ . Podemos ir substituindo o valor de  $x'$  por 2, 3, ..., até encontrar uma solução. Para  $x' = 2$ , temos

$$(2^7)^2 = 16384 \equiv -1 \pmod{29},$$

já que  $16384 = 565 \cdot 29 + (-1)$ . Portanto, como  $x' = 2$  e  $k = 7$ , chegamos a  $x = 2^7 = 128 = 4 \cdot 29 + 12 \equiv 12 \pmod{29}$ .

Passo 2. Faremos agora o AE com os números 29 e 12.

$$29 = 2 \cdot 12 + 5$$

$$12 = 2 \cdot 5 + 2$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Passo 3. Como  $\sqrt{29} \approx 5,38$ , os dois menores restos imediatamente menores que  $\sqrt{29}$  e, portanto, valores de  $a$  e  $b$ , são 5 e 2. Logo, podemos escrever 29 como  $29 = 5^2 + 2^2$ .

**Exemplo 2.3.2** Encontraremos agora  $a$  e  $b$ , tais que  $9973 = a^2 + b^2$ .

Passo 1. Precisamos encontrar  $x$ , tal que

$$x^2 \equiv -1 \pmod{9973}$$

Como  $9973 = 4 \cdot 2493 + 1$ , temos  $k = 2493$ . Estamos procurando então, um  $x'$  tal que

$$((x')^{2493})^2 = (x')^{4986} \equiv -1 \pmod{9973}.$$

Para isso, tomando  $x' = 2$ , temos

$$2^{4986} \equiv -1 \pmod{9973}.$$

Como  $2^{4986}$  é um número gigantesco, preferimos fazer esse cálculo módulo 9973 usando a plataforma *sagemath*. No entanto, esse cálculo pode ser feito de forma manual, usando exponenciação módulo 9973. Basta observar que

$$2^{4986} = 2^{3584} \cdot 2^{896} \cdot 2^{448} \cdot 2^{56} \cdot 2^2.$$

Para calcular cada uma dessas potências, podemos começar calculando

$$2^{14} = 16384 = 1 \cdot 9973 + 6411 \equiv 6411 \pmod{9973}.$$

Depois,

$$(2^{14})^2 = 2^{28} = 6411^2 \pmod{9973} = 41100921 = 4121 \cdot 9973 + 2188 \equiv 2188 \pmod{9973}.$$

Fazemos isso até chegar em  $2^{3584}$ , posteriormente substituímos os valores das potências em  $2^{4986} = 2^{3584} \cdot 2^{896} \cdot 2^{448} \cdot 2^{56} \cdot 2^2$  e chegamos em  $2^{4986} = 9972 \pmod{9973} \equiv -1 \pmod{9973}$ .

Logo, como  $x' = 2$  e  $k = 2493$ , temos  $x = (x')^k = 2^{2493} = 7175 \pmod{9973}$ . Neste exemplo, encontramos  $x' = 2$ , mas pode ocorrer casos em que  $x' = 2$  não seja uma solução, sendo necessário verificar outros números. Apesar disso, o procedimento é o mesmo.

Passo 2. Agora, sabendo que  $x = 7175$  e  $p = 9973$ , desenvolveremos o AE.

$$9973 = 1 \cdot 7175 + 2798$$

$$7175 = 2 \cdot 2798 + 1579$$

$$2798 = 1 \cdot 1579 + 1219$$

$$1579 = 1 \cdot 1219 + 360$$

$$1219 = 3 \cdot 360 + 139$$

$$360 = 2 \cdot 139 + 82$$

$$139 = 1 \cdot 82 + 57$$

Como  $\sqrt{9973} \approx 99,86$ , não é necessário terminar o desenvolvimento do AE, já que queremos apenas os dois primeiros restos imediatamente menores que 99,86.

Passo 3. Como  $\sqrt{9973} \approx 99,86$ , os restos que buscamos, e portanto valores de  $a$  e  $b$ , são  $a = 82$  e  $b = 57$ . De fato,  $9973 = 6724 + 3249 = 82^2 + 57^2$ .



## CONSIDERAÇÕES FINAIS

Começamos este trabalho com o seguinte questionamento: Existem outras aplicações do Algoritmo de Euclides para além do cálculo de MDC? Agora com o trabalho finalizado podemos afirmar que respondemos nossa questão norteadora e sim, existem outras aplicações do AE a não ser o cálculo de MDC. Porém, é importante destacar que neste trabalho mostramos apenas três dessas aplicações, embora existam outras. Com isso, concluímos que cumprimos com o objetivo geral deste trabalho, dado que conseguimos compreender o desenvolvimento do AE e suas aplicações. Apresentamos o contexto histórico do AE, vimos como o algoritmo se desenvolve de forma algébrica e geométrica, e também vimos como o AE pode ser aplicado em três outros tópicos matemáticos. Apesar disso, antes de iniciarmos o trabalho, pensamos em trabalhar a aplicação do AE nas Equações Diofantinas Lineares também de forma matricial, mas vimos que ficaria algo muito extenso e que não era necessário dado o objetivo deste trabalho.

Apesar da metodologia usada ter sido adequada, senti dificuldades na leitura de algumas referências, no qual a linguagem matemática utilizada nas definições, teoremas e demonstrações me fizeram buscar por materiais que tivessem uma linguagem mais simples. Apesar disso, essas dificuldades foram superadas nas reuniões com os orientadores. Em síntese, acreditamos que nossa hipótese foi satisfeita, visto que consideramos que este trabalho pode servir de referência para professores, alunos da disciplina de Teoria dos Números e todos que pretendem abordar/estudar outras aplicações do AE além do cálculo de MDC, já que o trabalho possui uma linguagem matemática mais simples e com muitos exemplos. Além disso, consideramos que conseguimos mostrar como é possível aplicar o AE de uma forma intuitiva, mostrando que esse resultado está presente em outros conteúdos matemáticos de forma natural.

Essa experiência contribuiu de diversas formas para o meu crescimento pessoal e para minha formação profissional. Consegui aprender mais acerca do LaTeX, algo que eu já vinha treinando há algum tempo, mas com a escrita deste trabalho vi um progresso maior. Também ampliei minha visão quanto à Teoria dos Números, principalmente quanto às aplicações do AE, pois antes deste trabalho eu só conhecia AE aplicado ao cálculo de MDC e às Equações Diofantinas Lineares. Também pude notar como nas disciplinas usuais não há uma preocupação com a efetividade computacional de algoritmos, já que não há uma discussão sobre o que dá pra fazer de forma manual, numa calculadora ou até o que é na prática impossível mesmo para um computador. Dessa forma, o trabalho é uma boa alternativa para aqueles que estão à procura de uma referência que fale acerca do AE e de suas aplicações de uma forma inicial.

Com isso, acreditamos que, para o ensino, este trabalho possa ser usado para professores que queiram trabalhar com as possibilidades do AE não só no ensino superior, mas também no ensino fundamental e médio, visto que, por exemplo, a representação geométrica do AE e sua contribuição para as Frações Contínuas são tópicos que podem ser abordados nestas séries. Além disso, para pesquisas futuras deixamos a sugestão de trabalhar a aplicação do AE nas Equações Diofantinas Lineares também de forma matricial.

## REFERÊNCIAS

- AZEVEDO, N. d. C. d. O número de ouro e construções geométricas. Universidade Federal de Goiás, 2013.
- BAUMGART, J. K. **Tópicos de História da Matemática para Uso em Sala de Aula**. [S.l.]: Editora Atual, 1992.
- BEZERRA, M. N. C. **Teoria dos Números**: Um curso introdutório. [S.l.]: Editora Universitária da Assessoria de Educação a Distância-EditAedi, 2018.
- BURTON, D. M. **A História da Matemática**: Uma introdução. 7. ed. [S.l.]: McGraw-Hill Science/Engineering/Math, 2011.
- CAMPOS, V. F. Criptografia rsa: Uma proposta de interdisciplinaridade. IFPB, 2020.
- CHAQUIAM, M. Ensaio temáticos: História e matemática em sala de aula. SBEM-PA, 2017.
- COUTO, A. G. Frações contínuas e números reais. Universidade Federal da Grande Dourados, 2017.
- DUTRA, A. Z. Frações contínuas: Uma leitura atualizada. Universidade Federal do Paraná, 2019.
- EUCLIDES. **Os Elementos**: Tradução e introdução de irineu bicudo. [S.l.]: Unesp, 2009.
- EVES, H. **Introdução à História da Matemática**. 5. ed. [S.l.]: Editada da UNICAMP, 2011.
- GIL, A. C. **Como Elaborar Projetos de Pesquisa**. [S.l.]: Atlas, 2002.
- HEFEZ, A. **Iniciação à aritmética**. [S.l.: s.n.], 2014.
- MOREIRA, C. G. Sequência recorrentes. Revista de Olimpíada, IME, Universidade Federal de Goiás, n. 8, p. 25–46, 2013. Disponível em: <[https://files.cercomp.ufg.br/weby/up/1170/o/3ro8\\_artigo1.pdf](https://files.cercomp.ufg.br/weby/up/1170/o/3ro8_artigo1.pdf)>.
- NASCIMENTO, A. M. d. Frações contínuas e aplicações no ensino médio. Universidade Federal de Goiás, 2013.
- OLIVEIRA, E. R. d. O uso de frações contínuas e do paradoxo de galileu: aplicações na resolução de problemas físicos na educação básica. Universidade Federal de Alagoas, 2014.
- OLIVEIRA, F. **Introdução à Teoria dos Números**. [S.l.]: Universidade Nova de Lisboa, 2011.
- PACCI, D. C.; RODRIGUES, C. T. V. Sequência de fibonacci. UNICAMP, 2013.
- ROQUE, T. **História da Matemática**: Uma visão crítica, desfazendo mitos e lendas. [S.l.]: Zahar, 2012.

SANTOS, J. P. de O. **Introdução à Teoria dos Números**. [S.l.]: Instituto de Matemática Pura e Aplicada, 1998.

SILVA, A. S. Um estudo sobre aplicação do algoritmo de euclides. Universidade Federal de Campina Grande, 2014.

SOUZA, R. S. Equações diofantinas lineares, quadráticas e aplicações. UNESP, 2017.

TUYL, A. L. V. An introduction to the theory and applications of continued fractions. 1996.

WAGON, S. **Editor's Corner**: The euclidean algorithm strikes again. [S.l.]: American Mathematical Monthly, 1990.

WEIL, A. Number theory: An approach through history from hammurapi to legendre. Springer Science & Business Media, 1984.

WIKIPÉDIA. **Complexidade computacional - Wikipédia, a enciclopédia livre**. 2019. [Online; accessed 8-abril-2019]. Disponível em: <[https://pt.wikipedia.org/w/index.php?title=Complexidade\\_computacional&oldid=54749052](https://pt.wikipedia.org/w/index.php?title=Complexidade_computacional&oldid=54749052)>.

## Documento Digitalizado Restrito

### Entrega do Trabalho de Conclusão de Curso

**Assunto:** Entrega do Trabalho de Conclusão de Curso  
**Assinado por:** Larissa Soares  
**Tipo do Documento:** Relatório  
**Situação:** Finalizado  
**Nível de Acesso:** Restrito  
**Hipótese Legal:** Informação Pessoal (Art. 31 da Lei no 12.527/2011)  
**Tipo do Conferência:** Cópia Simples

Documento assinado eletronicamente por:

- Larissa Soares de Sousa, ALUNO (201812020028) DE LICENCIATURA EM MATEMÁTICA - CAJAZEIRAS, em 23/05/2022 09:42:23.

Este documento foi armazenado no SUAP em 23/05/2022. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifpb.edu.br/verificar-documento-externo/> e forneça os dados abaixo:

Código Verificador: 524094  
Código de Autenticação: 14b44e82ac

