UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
INSTITUTO DE GEOCIÊNCIAS E CIÊNCIAS EXATAS

Programa de Pós-Graduação em Matemática em Rede Nacional

Equações Diofantinas associadas a Funções Aritméticas

José Roberto Duarte

PROFMAT

Rio Claro
2020

Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Equações Diofantinas associadas a Funções Aritméticas

José Roberto Duarte

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de Rio Claro.

Orientador
Prof. Dr. Jamil Viana Pereira

Rio Claro
2020

D812e

Duarte, José Roberto
Equações Diofantinas associadas a Funções Aritméticas / José Roberto Duarte. -- Rio Claro, 2020
125 p. : il., tabs.

Dissertação (mestrado profissional) - Universidade Estadual Paulista (Unesp), Instituto de Geociências e Ciências Exatas, Rio Claro
Orientador: Jamil Viana Pereira

1. Equações Diofantinas. 2. Funções Aritméticas. 3. Fatorial. 4. Diophantus. 5. Algoritmo Euclidiano. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Geociências e Ciências Exatas, Rio Claro. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

TERMO DE APROVAÇÃO

José Roberto Duarte

Equações Diofantinas associadas a Funções Aritméticas

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Prof. Dr. Jamil Viana Pereira
Orientador

Prof. Dr. Tiago Picon
Departamento - USP - Ribeirão Preto

Profa. Dra. Marta Cilene Gadotti
Departamento - UNESP -Rio Claro

Rio Claro, 27 de outubro de 2020

À minha esposa Rosângela, a meus filhos Carolina e José Roberto e à minha sogra Lourdes, que muitas vezes se doaram e renunciaram aos seus sonhos, para que eu pudesse realizar os meus. Quero dizer que essa conquista não é só minha, mas nossa. Tudo que consegui só foi possível graças ao amor, apoio e dedicação que vocês sempre tiveram por mim. Sempre me ensinaram agir com respeito, simplicidade, dignidade, honestidade e amor ao próximo. E graças à união de todos, os obstáculos foram ultrapassados, vitórias foram conquistadas e alegrias divididas.
Agradeço pela paciência e compreensão com minha ausência durante essa longa jornada.
Muitíssimo obrigado.

Chega um momento em sua vida, que você sabe:
Quem é imprescindível para você,
quem nunca foi,
quem não é mais,
quem será sempre!
Charles Chaplin

Agradecimentos

A todos os meus professores de Mestrado da Universidade Paulista de São Paulo de Rio Claro - o Prof. Dr. Jamil Viana Pereira, a Profa. Dra. Marta Cilene Gadotti, a Profa. Dra. Renata Zotin Gomes de Oliveira, a Profa. Dra. Eliris Cristina Rizziolli, o Prof. Dr. Thiago de Melo e o Prof. Dr. Rawlilson de Oliveira Araujo que contribuíram para nossa formação acadêmica e como futuros professores.

Para o nosso orientador, Prof. Dr. Jamil Viana Pereira, pelo tempo que ele se dedicou ao aconselhamento, pelo tempo de sua família que ele sacrificou por nos ajudar a completar este trabalho. Por seu apoio e compreensão em todo momento e por causa do interesse que ele sempre mostrou.

À colega do PROFMAT Mariane Rodrigues Regonha pelo companheirismo e ajuda neste árduo caminho acadêmico onde compartilhou importantes conhecimentos acadêmicos estando sempre perto para ajudar quando necessário.

Um agradecimento especial a Profa. Leda Maria Zanetti Machado pela sua tão estimada ajuda, pelo carinho, dedicação e amizade.

Para todos eles, muito obrigado.

Se eu morrer antes de você, faça-me um favor:
Chore o quanto quiser, mas não brigue comigo.
Se não quiser chorar, não chore;
Se não conseguir chorar, não se preocupe;
Se tiver vontade de rir, ria;
Se alguns amigos contarem algum fato a meu respeito, ouça e acrescente sua versão;
Se me elogiarem demais, corrija o exagero.
Se me criticarem demais, defenda-me;
Se me quiserem fazer um santo, só porque morri, mostre que eu tinha um pouco de santo, mas estava longe de ser o santo que me pintam;
Se me quiserem fazer um demônio, mostre que eu talvez tivesse um pouco de demônio, mas que a vida inteira eu tentei ser bom e amigo...
E se tiver vontade de escrever alguma coisa sobre mim, diga apenas uma frase:
-"Foi meu amigo, acreditou em mim e sempre me quis por perto!"
Aí, então derrame uma lágrima.
Eu não estarei presente para enxugá-la, mas não faz mal.
Outros amigos farão isso no meu lugar.
Gostaria de dizer para você que viva como quem sabe que vai morrer um dia, e que morra como quem soube viver direito.
Amizade só faz sentido se traz o céu para mais perto da gente, e se inaugura aqui mesmo o seu começo.
Mas, se eu morrer antes de você, acho que não vou estranhar o céu.
"Ser seu amigo, já é um pedaço dele...?"
Chico Xavier

Resumo

Esta dissertação de mestrado trata do conceito de equações diofantinas, funções aritméticas e uma relação entre as equações diofantinas que se utilizam de funções Aritméticas.

A parte inicial é dedicada a um levantamento histórico percorrido pela Teoria dos Números desde a Antiguidade até a atualidade e uma abordagem sobre um proeminente matemático que viveu provavelmente no século III, em Alexandria, a quem agora chamamos de "Pai da Álgebra". Apenas algumas informações sobre sua vida sobreviveram, mas não podemos dizer com certeza se são verdadeiras, nem se sabe ao certo o nome exato deste matemático - existem várias mutações possíveis, nomeadamente: Diofanto, Diofante ou Diophantus. Para maior clareza, apresentaremos o nome deste matemático na forma de Diophantus.

Foi esse matemático que lidou, entre outras coisas, com equações indefinidas, que em sua homenagem são chamadas equações diofantinas. No entanto, o tópico da equação diofantina é relativamente extenso e normalmente aborda-se a teoria básica, como observamos após pesquisarmos no site do PROFMAT. Por isso, não nos ativemos a demonstrar os vários métodos de resolução e discutirmos sobre os mais variados tipos de equações diofantinas, uma vez que os mesmos já foram extenuadamente apresentados e discutidos. Portanto nesse trabalho, fizemos uma abordagem de certas equações diofantinas envolvendo fatoriais e algumas funções aritméticas bem conhecidas : ϕ a função totiente de Euler, σ a função soma dos divisores e τ a função número de divisores, bem como as mesmas se relacionam, além do exame e da análise de funções da forma $\frac{f(n!)}{m!} = a$, onde f é uma das funções aritméticas ϕ *ou* σ, e incorporando alguns problemas que fazem uso das funções aritméticas aqui estudadas.

O objetivo deste trabalho é criar um material que sirva de motivação para os leitores, para continuar a trabalhar no campo da pesquisa, e por conseguinte poder dar contribuições ao campo da Matemática. Que os professores possam usar este trabalho como um bom lembrete das equações diofantinas para sua preparação durante as aulas regulares e adicionais e que possa servir como um "trampolim"para o estudo de equações diofantinas mais complexas.

Palavras-chave: Equações Diofantinas, Funções Aritméticas, Fatorial, Diophantus, Algoritmo Euclidiano.

Abstract

This master's thesis deals with the concept of diophantine equations, arithmetic functions and relations between diophantine equations that use arithmetic functions.

The initial part is dedicated to a historical survey covered by Number Theory from ancient times to the present and an approach to a prominent mathematician who probably lived in the 3rd century, in Alexandria, whom we now call "Father of Algebra". Only a few pieces of information about his life survived but we cannot say for shure that they are true nor if he known by this exact name - there are several possible mutations for the name: Diophanto, Diophante or Diophantus. For clarity, we will present the name of this mathematician in the form of Diophantus.

It was this mathematician who dealt, among other things, with indefinite equations, which in his honor are called diophantine equations. However, the topic of the diophantine equation is relatively extensive and usually approaches basic theory, as we observed after researching the PROFMAT website. Therefore, let us not activate ourselves into demonstrating the various methods of resolution and discuss the most varied types of diophantine equations, since they have already been extensively presented and discussed. Thus, in this work, we have approached certain diophantine equations involving factorial and some well known arithmetic functions: ϕ Euler's totient function, σ the sum of divisors function and τ the number of divisors function, as well as they relate, besides the examination and analysis of functions of the form $\frac{f(n!)}{m!} = a$, where f is one of the arithmetic functions $\phi\, or$, σ, and incorporating some problems that make use of the arithmetic functions studied here.

The aim of this work is to create material that will motivate readers, to continue working in the field of research, and therefore be able to make contributions to the field of Mathematics. May teachers use this work as a good reminder of diophantine equations for their preparation during regular and additional classes and that it can serve as a "diving board" for the study of more complex diophantine equations.

Keywords: Diophantine Equations, Arithmetic Functions, Factorial, Diophantus, Euclidian Algorithim.

Lista de Figuras

Lista de Tabelas

Sumário

Introdução

A Matemática é possivelmente a língua natural do universo, segundo [32]. Desde o início de nossa existência como espécie, os números nos fascinaram profundamente. O estudo dos números naturais, a Teoria dos Números, é um dos mais antigos ramos da Matemática, no entanto, não é um assunto finalizado, pois, ainda existem muitos problemas não resolvidos.

A modelagem matemática de um problema real geralmente leva à resolução de uma "*equação*", um termo vago que pode abranger uma equação diferencial, algébrica, com derivadas parciais, transcendentais, entre outras, mas também diofantina cujas soluções fornecem a resposta para o problema.

A Teoria dos Números é, como o nome sugere, dedicada ao estudo dos números, primeiro e acima de tudo, dos números inteiros mas também a outros conjuntos de números discretos. Como os números geralmente são as primeiras entidades as quais os não matemáticos visualizam, quando pensam em matemática (ao contrário de objetos geométricos, funções etc.), talvez não seja surpreendente que essa área tenha atraído muita atenção em todos os tempos, pois os problemas clássicos costumam ser fáceis de formular exigindo conhecimento apenas de matemática básica e isso torna a área atraente. Infelizmente, muitas vezes apenas as formulações dos problemas são simples, as provas são muito longas, complicadas e técnicas e, com frequência, têm pouca semelhança com os questionamentos iniciais. Pode-se dizer que é fácil explicar o que é verdade, mas quase impossível explicar por que é verdade, como exemplo, temos um dos problemas mais famosos da Teoria dos Números e, talvez em toda a Matemática, o Último Teorema de Fermat.

Najera [32] afirma que a pureza da Teoria dos Números cativou os matemáticos geração após geração, cada um contribuindo para o ramo que Carl Gauss descreveu como a "*Rainha da Matemática*". Hoje, no entanto, um entendimento básico da Teoria dos Números é um precursor absolutamente crítico para a engenharia de software de ponta, especificamente software baseado em segurança. Ela está no centro da criptografia, a qual está experimentando um período fascinante de rápida evolução que vai do famoso algoritmo RSA ao mundo popular de blockchain.

O estudo de equações diofantinas, em homenagem a Diophantus, é um problema cuja origem se encontra na Antiguidade. Há mais de 2000 anos, os filósofos e matemáticos da época estavam muito interessados nestes tipos de problema, cuja beleza vem, em parte, do fato de que, mesmo que possam ser colocados de maneira simples, suas soluções são muitas vezes extremamente complexas.

Por que Equações Diofantinas?

Entre as razões mais importantes pelas quais escolhemos o tema sobre equações diofantinas como tema desta dissertação, enfatizamos:

- **Conteúdo Programático do Ensino Fundamental e Ensino Médio**

  Como currículo, as equações de Diophantus não estão explicitamente presentes nos currículos regulares de Matemática do ensino fundamental e ensino médio, contudo elas estão presentes no ensino e são usadas como um material adequado para a formação do conteúdo didático em todas as séries, porém em nenhum momento, se destacam e nem seu conceito é explicitado. Geralmente aparecem em tarefas e problemas resolvidos e, especialmente, em competições matemáticas de nível superior.

  A partir do quinto ano do ensino fundamental, elas estão presentes em vários quebra-cabeças matemáticos e problemas relacionados à divisibilidade de números, números primos, princípio de paridade, divisão de polinômios em fatores. Dentro do tópico de ensino do quinto ano, o seu estudo começa sem mencionar o próprio nome das equações diofantinas. No sexto ano, a realização do conteúdo do ensino no campo da divisibilidade e dos números primos também ocorre por meio das equações. No sétimo ano, elas estão presentes através do processamento de frações e números inteiros. No oitavo ano, o conteúdo é abordado através de problemas relacionados à classificação (uso do último dígito), na realização da desmontagem de polinômios (uso de produtos) e na realização de "*divisibilidade*". Pela primeira vez, as equações de Diofanthus são explicitamente mencionadas como um tópico de ensino do ensino adicional em programas de matemática do nono ano. Ele lida com equações diofantinas lineares, sistemas lineares mais simples e sua aplicação. Então as equações são resolvidas usando quocientes, somas, desigualdades, divisibilidade. As entidades organizadoras de olimpíadas de matemática colocam as equações diofantinas no currículo para a competição dos alunos do nono ano que já estão no nível estadual.

  Nos programas de aulas adicionais de Matemática para o ensino fundamental e ensino médio, especificamente para Olimpíadas Matemáticas, as equações diofantinas são apresentadas por meio de equações lineares mais complexas, porque se entende que o conhecimento elementar foi trazido aos alunos do ensino fundamental. A aplicação de transformações algébricas na resolução de equações diofantinas não lineares mais complexas, o conteúdo em equações diofantinas não lineares, equações diofantinas quadráticas não elementares, as equações que se reduzem a elas e equações diofantinas exponenciais além da equação de Pell são abordados.

- **Historicamente**

  A contribuição de Diophantus para a Matemática, especialmente na Aritmética, é extremamente significativa. Ele é chamado o "*Pai da Aritmética*", segundo [12], por isso acreditamos que mereça mais estudos e publicações e que os professores de Matemática devam aproximar as equações de Diophantus dos alunos.

  Na segunda metade do século XX, a análise de Diophantus tornou-se moderna devido à sua proximidade com a geometria algébrica. Surpreendentemente, praticamente nada foi escrito sobre Diophantus, cujo nome está ligado a uma análise de equações com indeterminações, sendo um dos cientistas mais interessantes da antiguidade. Segundo [12], até os historiadores da Matemática às vezes têm uma visão equivocada

de seu trabalho, ao afirmar que a maioria deles pensa que ele resolveu um problema específico, equivalente a uma equação indefinida, por alguns métodos específicos.

Mesmo a análise de problemas simples de Diophantus mostram que ele não apenas colocou o problema de encontrar soluções racionais em equações indefinidas, mas também deu alguns métodos gerais para obtê-las. Deve-se ter em mente que, na matemática antiga, os métodos gerais não eram apresentados em "forma pura", além de problemas gerais.

- **Relevância das Equações Diofantinas**

  As equações diofantinas são relevantes porque representam a síntese de quase tudo na Teoria dos Números (divisibilidade dos números, números primos, congruência, etc.), teoria das equações, polinômios, equações, lógica matemática, etc.

  O que é mais surpreendente na *"Arithmetica"* de Diophantus não é apenas que ele faça uso de uma linguagem completamente nova e sua ousada expansão do domínio dos números, mas também os problemas que ele acabou por colocar e resolver.

- **Metodologia**

  Muitos historiadores da ciência subestimaram o trabalho de Diophantus, pois pensavam que ele limitava seu trabalho a encontrar uma solução. Por exemplo. Henkel escreveu:

  > "... se 100 soluções diofantinas forem dominadas, o matemático moderno encontrará um problema na solução do 101º problema ..."

  Pode-se dizer que essa avaliação surgiu do fato de o livro de Henkel ter sido publicado antes do surgimento das anotações de Poincaré, que indicavam os problemas das equações de Diophantus.

  Como razão também importante temos ideia de organizar as mais importantes equações diofantinas em um só lugar e, com base no meu trabalho, ser capaz de dominar métodos para resolver equações diofantinas, desenvolver a capacidade de identificar, formular, analisar e resolver problemas que se reduzem às equações diofantinas.

  Uma equação algébrica ou sistema de equações algébricas com coeficientes reais cuja solução pertence a um conjunto de números inteiros (ou números racionais), ou a algum conjunto de seus subconjuntos, é chamada de equações diofantinas algébricas. A partir da própria definição da equação de Diophantus, pode-se concluir que os requisitos, através das tarefas, podem ser muito diferentes e diversos. As respostas às perguntas feitas são frequentemente muito difíceis, o que confere à teoria das equações diofantinas uma grande importância e a torna uma das áreas mais interessantes da Matemática Elementar. Esse fato requer o reconhecimento de um método apropriado para resolvê-lo. A sistematização estrita de métodos para resolver equações diofantinas certamente não seria completa, porque o procedimento geral pode ser definido apenas para algumas classes de equações.

Análise e Proposta

O Mestrado Profissional em Matemática em Rede Nacional - PROFMAT é um programa de Mestrado semipresencial na área de Matemática com oferta em nível superior

sendo coordenado pela Sociedade Brasileira de Matemática (SBM), com apoio do Instituto Nacional de Matemática Pura e Aplicada (IMPA). Visando atender prioritariamente os professores da Educação Básica da Rede Pública de Ensino e nesse sentido, os trabalhos de conclusão de curso devem abranger temas relativos ao currículo de Matemática da Educação Básica. Até a quarta semana de agosto de 2020 existiam 5.348 registros de dissertações no site do PROFMAT, publicadas desde o ano de 2013.

Ao fazermos uma pesquisa no site do PROFMAT para sabermos qual seria o enfoque dado sobre o tema que envolviam "equações diofantinas", veja [37] e a Tabela A.1 no anexo, constatamos a presença de 39 trabalhos distribuídos por 29 instituições de ensino espalhadas pelo país sobre o assunto, e após uma análise decidimos fazer um enfoque até então não dado as mesmas.

Nesta análise observamos que os trabalhos em quase sua totalidade acabam por apresentar algum tipo de relação com o contexto da Escola Básica. Em sua grande maioria as dissertações além de apresentar os conteúdos básicos referentes as equações diofantinas acabam por propor planos de aula, sequências didáticas, oficinas e atividades extraclasse, e, em alguns casos, inclusive apresentam aplicações e análise das mesmas ou bem como uma análise das consequências.

Em quase toda a sua totalidade a análise e do estudo das equações diofantinas lineares é o tema principal onde as equações lineares em duas variáveis são de alguma forma citada em todos os trabalhos, já analisando os trabalhos 1, 2, 8, 9, 10,17, 23, 29, 31, 34 e 37 presentes na Tabela A.1 encontramos as equações diofantinas em 3 variáveis, enquanto as equações lineares em n variáveis foram tema de 1, 2, 8, 9, 10, 11, 14, 23, 24, 29 e 34 na Tabela A.1.

Já as equações não-lineares na Tabela A.1 foram analisados por 1, 2, 9, 10, 14, 18, 19, 20, 22, 23, 24, 29, 34 e 37 onde a abordagem pelas ternas pitagóricas ou equações na forma $x^2 + y^2 = z^2$ e o estudo acerca de suas infinitas soluções foram abordados pelos trabalhos 1, 9, 10, 11, 14, 17, 18, 19, 20, 23, 29, 33 e 37 na Tabela A.1.

O estudo das equações diofantinas ajudou a desenvolver muitas ferramentas na moderna Teoria dos Números. Por exemplo, para a prova do Último Teorema de Fermat, muitas ferramentas de geometria algébrica, curvas elípticas, teoria dos números algébricos, etc, foram desenvolvidas. Os trabalhos 1, 12, 14, 17, 19 e 29 constantes da Tabela A.1 discorreram sobre este tema.

Entre os 23 problemas apresentados por Hilbert em 1900, o décimo problema dizia respeito às equações diofantinas, veja o trabalho 19 na Tabela A.1. Hilbert perguntou sobre a existência de um método universal para resolver todas as equações diofantinas. Aqui nós a reformulamos:

> "Dada uma equação diofantina com qualquer número de desconhecidos e com coeficientes numéricos racionais integrais: Para conceber um processo segundo o qual pode ser determinado por um número finito de operações se a equação é resolvível em inteiros".

Em 1970, Y. Matiyasevich [30] deu uma solução negativa para o décimo problema de Hilbert. Seu resultado é o seguinte.

> *Não há algoritmo que, para uma dada equação diofantina arbitrária, diga se a equação tem uma solução inteira ou não.*

Importante observarmos que para soluções racionais, o análogo do décimo problema de Hilbert ainda não foi resolvido. Ou seja, a questão de saber se existe um algoritmo

para decidir se uma equação diofantina tem uma solução racional ou não ainda está em aberto.

Uma vez que não há um método geral para resolver as equações diofantinas, algumas técnicas foram encontradas para resolver famílias particulares de equações diofantinas, como por exemplo o método de descida infinita de Fermat analisado na Tabela A.1 em 1, 12, 20, 23 e 24, ou a análise da equação de Pell $x^2 - Dy^2 = 1$, com $D > 0$ é um número natural e não um quadrado, em homenagem ao matemático John Pell, e cada uma dessas equações tem uma solução mereceram os trabalhos de 9, 14, 19, 20, 21 e 23 na Tabela A.1.

A nossa proposta caminha, então, como já mencionado, na direção de não nos atermos a esses assuntos já tão bem estudados e analisados pelos acadêmicos das mais diversas instituições e focarmos em uma análise de algumas funções aritméticas, função ϕ de Euler, a função σ e a função τ, bem como as mesmas se relacionam e trabalhar as equações diofantinas que envolvem essas funções aritméticas e assim analisarmos as funções da forma $\frac{f(n!)}{m!} = a$, analisadas por [27, 28], na qual f é uma das funções aritméticas ϕ a função totiente de Euler ou σ a função soma dos divisores além de incorporamos alguns problemas que fazem uso de funções aritméticas aqui estudadas.

Estrutura da Dissertação

As equações diofantinas são uma parte importante da Teoria dos Números a qual é um dos ramos mais antigos da matemática. A maioria dos grandes mestres das ciências matemáticas, em algum momento de suas carreiras, acabou por contribuir com a Teoria dos Números.

O tema das equações diofantinas é muito extenso e interessante, poucas pessoas percebem que os problemas que lidam com a vida cotidiana levam a equações diofantinas. Este trabalho lida, principalmente, com equações diofantinas de Brocard-Ramanujan e suas variações associando-as a funções aritméticas e fatoriais.

Na seção anterior elencamos o que nos levou à escolha das equações diofantinas, além de acabarmos por estabelecer uma breve relação entre os tópicos básicos de equações diofantinas e sua abordagem nos trabalhos de dissertação presentes no PROFMAT.

No Capítulo "Apresentação - Teoria dos Números" iniciamos elencando os principais conceitos e antecedentes históricos da Teoria dos Números até a atualidade. Em seguida, acabamos por situar Diophantus, com o seu pioneirismo, na utilização sistemática de abreviações para potências de números, para as relações e operações e as equações diofantinas dentro desse contexto.

Optamos por essa abordagem para oportunizar a professores, alunos do ensino fundamental e médio e demais interessados que entrem em contato com a evolução da Teoria dos Números no decorrer dos séculos, com Diophantus acerca de sua vida e obras de uma forma mais panorâmica, sendo um elo motivacional ao estudo das equações diofantinas.

O capítulo "Conceitos Básicos e Notações" tem como objetivo servir como referência ao apresentarmos algumas ferramentas que serão utilizadas ao longo de nossa dissertação, servindo assim como uma referência rápida ou uma atualização na Teoria dos Números. Além de fazermos uma breve introdução a equações diofantinas onde definimos as equações diofantinas lineares, demonstramos as principais propriedades que as envolvem e as aplicações que fazem uso de tais propriedades. Mostramos como encontrar a solução geral de uma equação diofantina linear.

A análise e estudo deste capítulo proporciona aos interessados uma grande ferramenta de auxílio na resolução dos mais diversos problemas, além de propiciar o desenvolvimento do raciocínio lógico, conciliando a interpretação dos problemas juntamente com as referidas resoluções e cálculos.

O estudo de funções é uma parte importante da matemática moderna. Existem funções peculiares a quase todos os ramos da matemática. Existem outras que, embora úteis em muitas áreas diferentes da matemática, têm sua origem em um ramo específico. Elas, geralmente, são identificadas de alguma forma com o ramo de sua origem.

As funções mais intimamente identificadas com a Teoria dos Números são geralmente chamadas de Funções Aritméticas. Elas são diferentes da maioria das funções encontradas na álgebra ou na análise, já que, geralmente, são definidas nos números inteiros ou em um subconjunto dos números inteiros. Às vezes, é feita uma extensão aos números reais e questões de comportamento analítico são estudadas. No entanto, elas geralmente são mais úteis no estudo de números naturais ou de números inteiros. No capítulo denominado Funções Aritméticas introduzimos algumas dessas funções, com suas respectivas propriedades e a inter-relação entre as funções σ, τ e ϕ abordadas nesse trabalho. Os fatoriais também são abordados apresentando-se sua definição e suas principais propriedades relacionado-os com as funções aritméticas.

Baseado no trabalho de Florian Luca [27, 28], o capítulo Equações Diofantinas associadas as funções aritméticas e fatoriais é parte central de nossa dissertação no qual estabelecemos uma relação entre esses três tópicos da Teoria dos Números e examinamos e classificamos as soluções para certas equações diofantinas envolvendo fatoriais e algumas funções aritméticas bem conhecidas. Analisamos as funções da forma $\dfrac{f(n!)}{m!} = a$, na qual f é uma das funções aritméticas ϕ a função totiente de Euler ou σ a função soma dos divisores. E finalizando o capítulo incorporamos alguns problemas que fazem uso de funções aritméticas por nós abordadas.

Na sociedade atual, a maioria dos estudantes ou adultos pensa que evitará usar operações numéricas mais complexas; muitos deles nunca ouviram falar de equações diofantinas e pensam que não precisam delas em suas vidas. Entretanto observamos que, em nosso dia a dia, deparamo-nos com equações diofantinas em muitos casos. No capítulo Transposição Didática, apresentamos algumas aplicações das equações diofantinas no cotidiano que podem ser resolvidas através da análise diofantina ou até mesmo através de estratégias de resolução como tentativa e erro, método pictórico e de conceitos da Teoria dos Números.

Esta dissertação é destinada não só a estudantes do ensino fundamental e médio, mas também a professores, universitários, participantes de competições matemáticas, bem como a qualquer interessado em matemática. No último capítulo, Considerações Finais, apresentamos nossas considerações finais e recomendações e esperamos que o contato com este trabalho permita a todos conjecturar, comparar e estabelecer estratégias mentais de forma criativa na resolução de situações-problema de outras áreas do conhecimento relacionando-as com as equações diofantinas.

1 Apresentação - Teoria dos Números

Teoria dos Números é um assunto vasto e desafiador; é tão antigo quanto a matemática e tão atual quanto as notícias de hoje. Seus problemas retêm seu fascínio por sua aparente mas, muitas vezes, enganosa simplicidade e uma beleza irresistível. Com uma história tão rica a Teoria dos Números certamente merece ser chamada, nas famosas palavras de Gauss, "*a Rainha da Matemática*".

O objetivo deste capítulo é mostrar como a Teoria dos Números evoluiu ao longo da história e quais tópicos foram de interesse até mesmo para os matemáticos da atualidade. Os primeiros matemáticos elaboraram muitos problemas, porém não tinham as ferramentas necessárias para solucioná-los. Com o desenvolvimento da Matemática ao longo dos anos, muitos resultados antigos foram comprovados.

A Teoria dos Números é o ramo da Matemática que lida com as propriedades dos inteiros, mais especificamente as propriedades dos inteiros positivos. Ao contrário da maioria dos outros campos da Matemática, ela remonta a mais de 4500 anos no passado. Apesar da idade, ainda existem algumas perguntas que não foram respondidas. Um grande número de princípios nesse campo foi descoberto por experimentos explícitos. Desde a Antiguidade Clássica e através do seu grande desenvolvimento de 1600 a 1800, a Teoria dos Números foi separada na maioria das vezes, de outros campos da Matemática. Os problemas da Teoria dos Números não são relevantes apenas para os matemáticos; atualmente, esses problemas são atraentes para muitos leigos e a Teoria dos Números é apontada como um campo da Matemática em que as sugestões e palpites de amadores apresentam muitos resultados valiosos. A maioria dos grandes pesquisadores de Ciências Matemáticas, em algum momento de suas carreiras, contribuiu para a Teoria dos Números.

A Teoria dos Números é um dos ramos mais antigos da Matemática Moderna, entretanto, ao longo dessa longa história, ela sempre foi considerada parte da Matemática Pura (teórica) e não se esperava que ela tivesse aplicações concretas. É uma disciplina com resultados demonstráveis e muitos de seus problemas podem ser declarados com facilidade, mas geralmente requerem métodos complexos de diferentes campos e áreas para serem estudados. Suas formulações modernas são de amplo alcance e têm laços estreitos com a Geometria Algébrica, Análise e Teoria de Grupos, juntamente com aspectos computacionais. Talvez, devido à natureza fundamental e profunda dos números inteiros, a Teoria dos Números desempenhe um papel especial em Matemática e suas aplicações.

1.1 Conceitos e Antecedentes Históricos da Teoria dos Números

A Teoria dos Números é, como o nome sugere, dedicada ao estudo dos números, primeiro e principalmente números inteiros mas também outros conjuntos discretos de números complexos. Como os números geralmente são a primeira entidade (em oposição aos objetos geométricos, funções, etc.) não é de surpreender que essa área tenha atraído mais atenção no campo dessa disciplina. Os problemas clássicos costumam ser fáceis de formular requerendo apenas algumas notações básicas e isso torna a área atraente. Infelizmente, muitas vezes são apenas as formulações dos problemas que são simples; as provas são muito longas, complicadas e técnicas e, frequentemente, têm pouca semelhança com as afirmações originais.

A primeira abordagem científica para o estudo de inteiros, ou seja, a verdadeira origem da Teoria dos Números segundo Burton [12] é atribuída aos gregos que estavam em dívida com os babilônios e antigos egípcios sobre um núcleo de informações das propriedades dos números naturais. Por volta de 600 a.C., Pitágoras e seus discípulos fizeram um estudo minucioso dos números naturais.

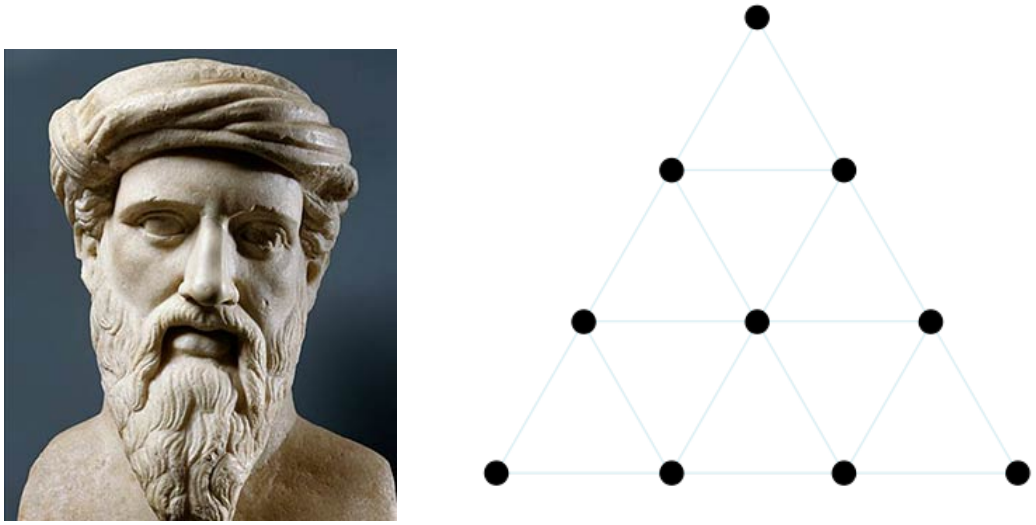
Sobre a vida de Pitágoras é quase impossível se afirmar algo com alguma certeza. De acordo com Aragão [4], com as melhores estimativas, ele nasceu entre 580 e 562 a.C. na ilha Aegeab de Samous, não muito longe de Mileto. Ele estudou no Egito e na Babilônia. Ele se estabeleceu em Cróton, um povoado grego próspero no sul da Itália, para onde fugiram muitos gregos antes da invasão persa. A Escola Pitagórica, segundo [12] não era apenas um local de estudo em Filosofia e Matemática, mas também uma comunidade que governava toda a vida de seus membros através de regras especiais. Sua escola estava concentrada em quatro matemáticas, ou assuntos de estudo: Arithmatica (Aritmética no sentido da Teoria dos Números não a arte de calcular), Harmonia (Música), Geometria (Geometria) e Astrologia(Astronomia).

De acordo com [12] Pitágoras dividiu seus alunos em dois grupos, a saber: os Probacionários (ou ouvintes) e os Pitagóricos. Os Pitagóricos formavam uma fraternidade muito unida, mantendo todos os bens do mundo em comum e limitada por um juramento de não revelar os segredos dos fundadores. Por tempo os Pitagóricos autocráticos conseguiram dominar o governo local em Cróton, todavia uma revolta popular em 501 a.C. levou ao assassinato de muitos de seus membros proeminentes e o próprio Pitágoras foi morto pouco depois.

Ainda em [12] encontramos que os Pitagóricos acreditavam que a chave para um esclarecimento acerca do universo estava em números e formas, sendo que seu pensamento era que "*Tudo é número*" (inteiro positivo). A doutrina pitagórica é uma estranha mistura de filosofia cósmica e misticismo numérico. Uma espécie de supernumerologia que atribuía um inteiro definido a todas as coisas materiais ou espirituais. A filosofia de Pitágoras é especial, visto que não atribui o papel a um problema, mas a números. Conhecimento de matemática e números é a chave para entender o mundo. Os números devem ser entendidos como matéria do mundo e como uma maneira de descrevê-lo. A matéria consiste basicamente em pontos, retas, planos e corpos geométricos que correspondem simbolicamente aos números $1, 2, 3$ *e* 4. A soma desses números - 10 (décadas), pelos pitagóricos, é um número perfeito (representado pela figura tetraktis) no qual o segredo do cosmos está oculto.

Segundo [12] uma ciência dos números divorciada da filosofia mística começou a se desenvolver inicialmente em Alexandria que permaneceu como centro cultural e comercial

Figura 1.1: Pitágoras e o Tetraktis -Década Pitagórica



Fonte: https://www.marcelouva.com.br/quem-foi-pitagoras-de-samos/ , https://pt.wikipedia.org/wiki/Tetraktys

do mundo helenístico por quase mil anos. Após a queda de Alexandria, a maioria dos estudiosos migrou para Constantinopla. De acordo com [12], durante os 800 anos seguintes, enquanto o aprendizado formal no Ocidente desaparecia, em Constantinopla se preservou o trabalho matemático das várias escolas gregas no Museu Alexandrino, um precursor da universidade moderna, reunindo na biblioteca mais de 700.000 volumes copiados à mão.

Em [12] de todos os nomes reconhecidos associados ao Museu, o de Euclides, organizador da Escola de Matemática, está em uma classe incomum. Embora, ao longo da história da humanidade, muitos estudiosos tenham dado seus postulados e várias teorias, é Euclides quem é chamado de "*Pai da Geometria*". Ele colecionou não apenas todas as suas reflexões e teorias, mas também as teorias de seus antecessores em sua obra *"Elements"* que saiu em mais de 1700 edições desde a primeira versão impressa em 1482 e, sem dúvida, fez de Euclides o principal matemático de todos os tempos. Além disso, não surpreende que sua obra seja considerada a obra mais traduzida, impressa e pesquisada da história da humanidade após a Bíblia. O nome de Euclides é frequentemente associado à geometria e é por isso que tendemos a esquecer que três dos livros VII, VIII e IX são dedicados à Teoria dos Números.

Para [12] o que o mundo antigo sabia foi esquecido em grande parte durante o torpor intelectual da Idade das Trevas, e foi somente após o século XII que a Europa Ocidental voltou a ter consciência da Matemática. O renascimento da erudição clássica foi estimulado por traduções em latim do grego e, mais especialmente, do árabe. Infelizmente não foi encontrada nenhuma cópia do trabalho que data realmente do próprio tempo de Euclides, as edições modernas são descendentes de uma revisão preparada por Theon de Alexandria, um comentarista do século IV. De várias fontes, podemos aprender algo sobre Euclides como pessoa. Por exemplo, seu contemporâneo, o matemático Papus de Euclides, diz que ele era um homem virtuoso, humilde e quieto, ignorante da arrogância e do egoísmo. Ele era considerado um homem que vivia apenas para a ciência e persistia na visão de que o conhecimento era necessário apenas em benefício do próprio conhecimento,

Figura 1.2: Euclides - Pai da Geometria

Fonte : https://www.infoescola.com/biografias/euclides/

e não em benefício próprio.

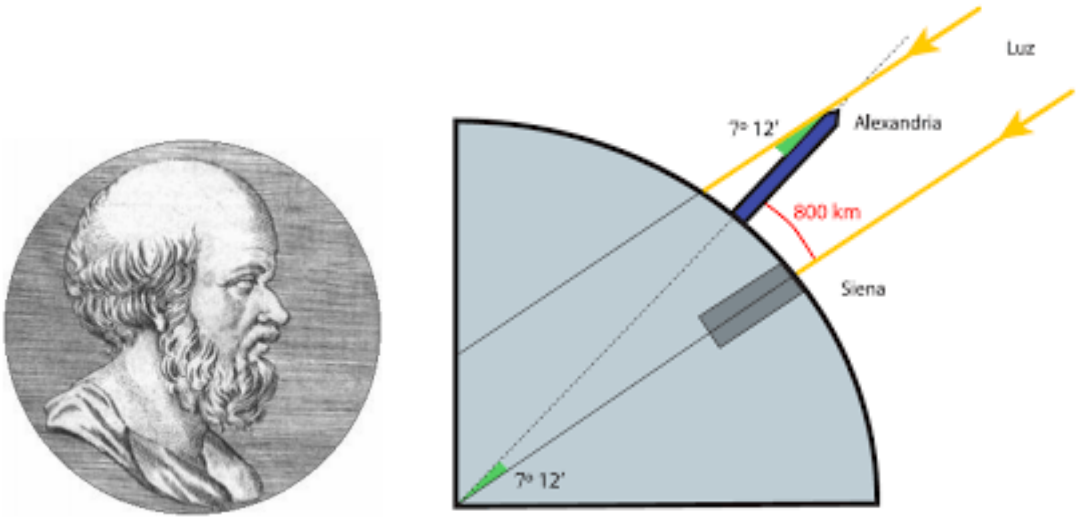
Outro matemático grego, segundo [12], cujo trabalho na Teoria dos Números permanece significativo, é Eratóstenes de Cirene(276-194 a.C.). Embora a posteridade se lembre dele principalmente como diretor da mundialmente famosa biblioteca em Alexandria, Eratóstenes era talentoso em todos os ramos da aprendizagem, sendo apelidado de "*Beta*" porque dizia-se que ele estaria pelo menos em segundo lugar em todos os campos. Talvez a façanha mais impressionante de Eratóstenes tenha sido ter calculado a medida exata da circunferência da Terra por uma simples aplicação da Geometria Euclidiana.

Para [9, 12] Eratóstenes é o primeiro a sistematizar a geografia, por isso não surpreende que hoje seja conhecido como o "*Pai da Geografia*". Ele projetou vários instrumentos astronômicos que são utilizados há séculos. Foi ele quem sugeriu que um dia bissexto fosse adicionado a cada quarto ano no calendário e tentou compilar uma cronologia precisa do mundo coletando datas de eventos científicos e políticos desde o cerco de Tróia. Eratóstenes determinou a inclinação da eclíptica, ou seja, a inclinação da Terra em direção ao círculo imaginário que o sol aparentemente está se movendo, medindo a inclinação da Terra com alta precisão. Eratóstenes, em seu trabalho *"Geografia"*, resumiu todos os seus métodos e os resultados de suas medições e cálculos, lançando as bases da orientação matemática em geografia. Infelizmente, nem a mencionada *"Geografia"* nem a obra *"Sobre a Medição da Terra"* são preservadas, entretanto aprendemos sobre elas com os escritos de filósofos posteriores, como Kleomed e Strabo. Ele também fez um mapa geográfico do mundo então conhecido. Além disso, ele esboçou, com muita precisão, a rota do Nilo para Cartum.

Eratóstenes era amigo de Aristóteles e, graças a essa correspondência, algumas das obras de Aristóteles foram preservadas.

[9, 12] afirmam que talvez o maior matemático da Idade Média tenha sido Leonardo Bigollo (Leonardo Pisano, Leonardo Pizanski, Leonardo de Pisa) nascido em Pisa, centro comercialmente importante localizado na Itália, viveu em meados dos séculos XII e XIII (1170-1240). Leonardo de Pisa é historicamente conhecido pelo apelido Fibonacci, um derivado de duas palavras fillius + bonnacci que, na mistura de latim e italiano, obtém o significado de "*filho do bem-intencionado*". Seu pai era um comerciante e grande parte de seus negócios era no norte da África, desta forma, Leonardo durante suas viagens com o

Figura 1.3: Eratóstenes e a Medição do Raio da Terra



Fonte : https://tecnoblog.net/meiobit/398976/professores-dia-21-de-marco-participem-do-experimento-eratostenes/, https://www.forcesystem.com.br/como-eratostenes-descobriu-que-a-terra-e-redonda-ha-2200-anos/

pai, teve a oportunidade de se encontrar com grandes matemáticos que estavam fora do chamado "*Círculo Oriental*" (Egito, Síria, Argélia, Grécia, etc.) descobrindo a magia dos algarismos arábicos e da matemática.

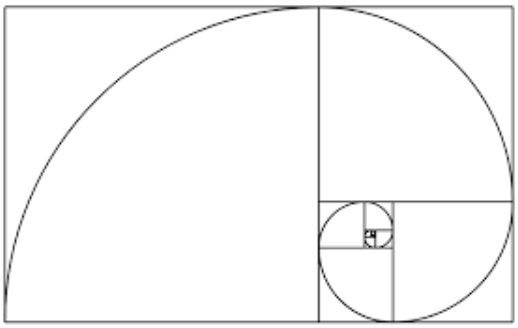
Mais tarde, Fibonacci retornou à Itália e, aos 32 anos, publicou a sua obra mais famosa intitulada *"Liber Abaci"* (1202) que se caracteriza como um tratado completo sobre os métodos e os problemas algébricos em que o uso dos numerais hindu-arábicos é fortemente recomendado em sua aplicação a uma ampla variedade de situações cotidianas durante o comércio.

Segundo [12] em seu capítulo inicial, o *"Liber Abaci"* traz a teoria de que a Aritmética e a Geometria são interligados e, por consequência, auxiliam-se mutuamente; porém, ao analisarmos a obra como um todo, Fibonacci discorre mais sobre números, descrevendo primeiro as nove cifras hindu-arábicas juntamente com o símbolo 0 (*zephiriunem* em árabe), explica métodos de cálculo com inteiros e frações, cálculo de raízes quadradas e cúbicas, resolução de equações lineares e quadráticas tanto pelo método da falsa posição como por processos algébricos. As raízes negativas e imaginárias não são admitidas, ademais, há uma farta coleção de problemas dentro os quais o que deu origem a famosa Sequência de Fibonacci - $S_n = (1, 1, 2, 3, 5, 8, 13, \dots)$:

> "Um homem coloca dois coelhos em um espaço cercado por uma parede por todos os lados. Quantos pares de coelhos podem ser produzidos a partir desse par em um ano se, em cada mês, cada par de coelhos novos trouxer ao mundo outro par, que se torna produtivo a partir do segundo mês?"([12])

Ainda segundo [12] em 1220 Fibonacci publicou *"Practica Geometriae"* uma coleção de material sobre Geometria e Trigonometria, num compilado de rigor euclidiano, com destaque à prova de que as medianas de um triângulo se dividem na razão 2 : 1 e um análogo tridimensional do Teorema de Pitágoras.

Figura 1.4: Leonardo de Pisa - Fibonacci e a Espiral de Fibonacci



Fonte : http://www.mat.uc.pt/ jaimecs/mce12/fibo.html

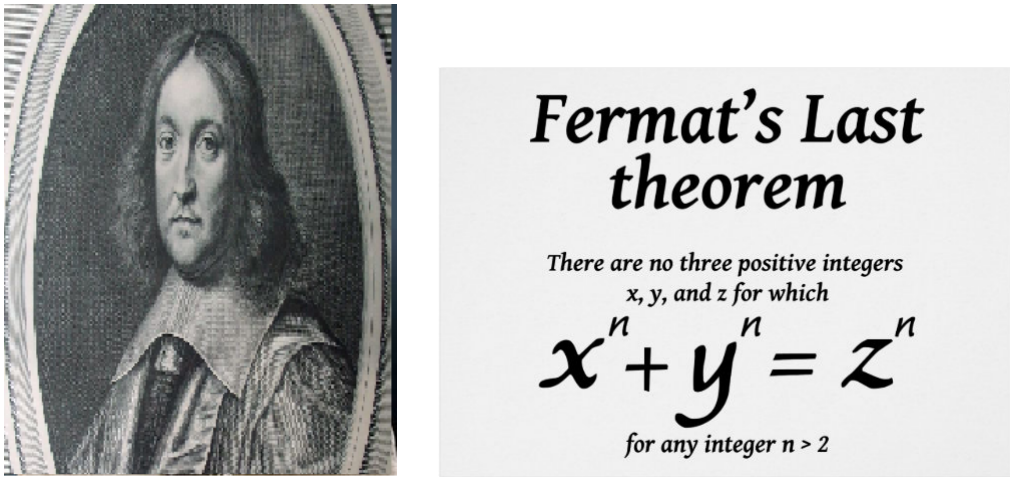
Em [9, 12] encontramos que as obras de Fibonacci aguçaram o interesse do imperador sacro-romano Frederico II e o convidou para participar de um torneio de matemática que promoveria em sua corte. Um dos problemas propostos era encontrar um número racional tal somando-se ou subtraindo-se 5 do quadrado do primeiro, o resultado seja o quadrado de um número racional. Tanto o problema quanto a sua solução se encontram descritos no *"Liber Quadratorum"*, um trabalho inteiramente dedicado a problemas diofantinos de segundo grau, como a obtenção da solução simultânea (racional) do par de equações $x^2 + 5 = y^2, x^2 - 5 = z^2$, sendo ainda digno de nota, a estimativa notavelmente exata da única raiz real da equação cúbica $x^3 + 2x^2 + 10x = 20$; seu valor, em notação decimal, de 1.3688081075..., está correto com nove casas decimais apresentado em seu tratado intitulado *"Flos"* (1225). Todos esses trabalhos acabaram por impulsionar Fibonacci no mundo da Matemática colocando-o numa posição de destaque entre os matemáticos mais importantes como Diophantus e Fermat.

É irônico que, apesar de suas muitas realizações, Fibonacci seja lembrado hoje, principalmente porque o teórico dos números do século XIX, Edouard Lucas atribuiu seu nome a uma sequência que aparece em um problema trivial no *"Liber Abaci"*.

Segundo [12] poucos períodos produziram tantos talentos para a Matemática como o século XVII, no qual surgiram tantos homens de notável capacidade quanto surgiram no milênio anterior. Apenas no Norte da Europa podemos destacar entre outros Desargues, Descartes, Pascal, Wallis, Bernoulli, Leibnitz e Newton. Outro estudioso brilhante, foi o funcionário público francês, Pierre de Fermat(1601-1665). Fermat, o *Príncipe dos Amadores*, foi o último grande matemático a usar o assunto como um subtópico do saber não científico. Tendo por profissão a advocacia e a magistratura ligada ao parlamento provincial em Toulouse, ele buscou refúgio da controvérsia na abstração da matemática. Fermat, evidentemente, não tinha nenhum treinamento particular em Matemática, sendo que ele não demonstrou nenhum interesse em seu estudo até os 30 anos. Para ele, era apenas um passatempo a ser cultivado no tempo livre, todavia nenhum praticante de seus dias

fez grandes descobertas ou contribuiu mais para o avanço da disciplina. Sendo um dos inventores da Geometria Analítica, ele estabeleceu as bases técnicas de cálculo diferencial e integral e com Pascal estabeleceu as diretrizes conceituais da teoria da probabilidade. O verdadeiro amor de Fermat pela matemática era, sem dúvida, a Teoria dos Números que ele resgatou do reino da superstição e do ocultismo, no qual há muito tempo estava aprisionada.

Figura 1.5: Pierre de Fermat e o seu último Teorema



Fonte: https://impa.br/wp-content/uploads/

Segundo [12] sua contribuição acabou por ofuscar os demais e podemos afirmar que o ressurgimento do interesse pelo lado abstrato da Teoria dos Números começou com Fermat que preferia o prazer que derivava da pesquisa matemática a qualquer reputação que isso pudesse lhe trazer. De fato, ele acabou por publicar,usando as iniciais M.P.E.A.S., apenas um manuscrito durante sua vida e, apenas cinco anos antes de sua morte. Como uma compensação parcial por seu desinteresse em publicação, Fermat manteve uma volumosa correspondência com matemáticos contemporâneos. Encontramos a maior parte de seu trabalho nas cartas para amigos com quem ele trocou problemas e a quem ele relatou seus sucessos. Eles fizeram o possível para divulgar o talento de Fermat, passando essas cartas de mão em mão ou fazendo cópias que foram despachadas pelo continente.

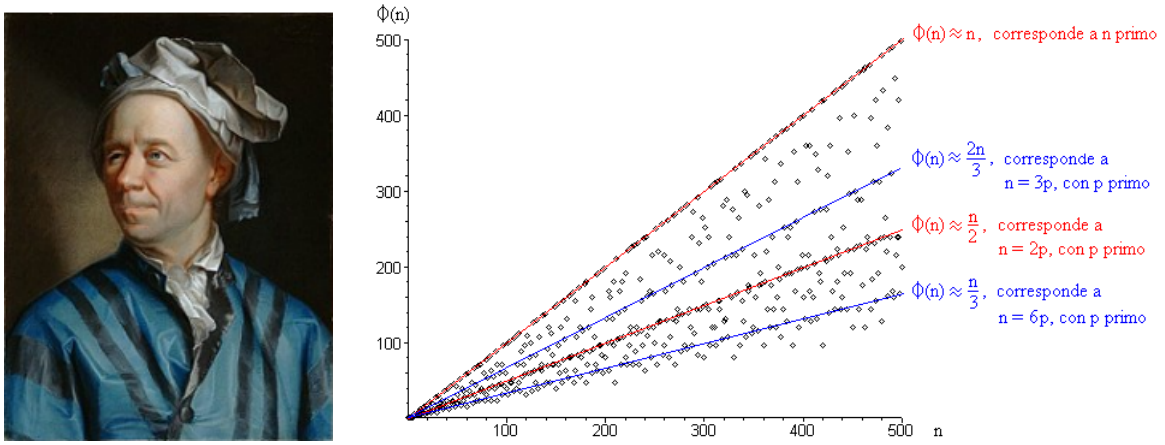
Ainda em [12] encontramos que as suas obrigações parlamentares exigiam cada vez mais de seu tempo e foi nas margens da cópia pessoal de Fermat da edição *"Bachet de Diophantus"* que ele mantinha muitos de seus famosos teoremas na Teoria dos Números. Após 5 anos de sua morte, esse material foi descoberto pelo seu filho Samuel que acabou por lançar uma nova edição da *Arithmetica* incorporando os celébres resultados obtidos por seu pai. Fermat tinha como hábito anotar alguns resultados, mas omitir todos os passos que levavam à conclusão, talvez pelo pouco espaço disponível. A posteridade, com certeza, desejou que as margens da *"Arithmetica"* fossem mais amplas ou que Fermat tivesse sido um pouco menos reservado quanto a seus métodos.

> A importância do trabalho de Fermat nem reside tanto em qualquer contribuição para a matemática de sua época, mas no impacto encorajador nas gerações posteriores de matemáticos acerca da Teoria dos Números.([12])

No final do século XVII e parte do início do século XVIII, o principal papel da Matemática foi assumido pelos seguidores de Newton e Leibniz que aplicaram suas ideias de cálculo para resolver vários problemas em física, astronomia e engenharia.

Burton em [12] afirma que transcorreu-se pelo menos um século até que um matemático de primeira linha, Leonhard Euler(1707-1783), compreendesse ou apreciasse o significado de sua obra. Muitos dos teoremas anunciados sem provas por Fermat cederam à sua habilidade e é provável que os argumentos utilizados por Euler não fossem substancialmente diferentes daqueles que Fermat disse possuir.

Figura 1.6: Leonhard Euler - Função Phi de Euler



Fonte: *https* : *//en.wikipedia.org/wiki/Leonhard*$_E$*uler*

Segundo [12] Euler pode ser considerado o matemático mais prolífico, visto que ele escreveu ou ditou mais de 700 livros e artigos em toda sua vida. Deixando tanto material não publicado que os mesmos continuaram a ser publicados pela Academia de São Petersburgo por aproximadamente 50 anos após a sua morte em 1783.

Ainda em [12] na Matemática Pura, Euler integrou o cálculo diferencial de Leibniz com o método de Newton em análise matemática. Ele refinou a noção de função, criou notações matemáticas e fundamentou a Teoria das Funções Especiais introduzindo as Funções Transcendentais Beta e Gamma. Euler foi pioneiro no campo da Topologia e e transformou a Teoria dos Números em uma ciência declarando a Teoria do Número Primo e a Reciprocidade Biquadrática. Na física, articulou a Dinâmica Newtoniana e introduziu os fundamentos da Mecânica Analítica, culminando na *"Teoria dos Movimentos dos Corpos Rígidos"*(1765). Euler faz seu trabalho público contrastar com o sigilo habitual no tempo de Fermat.

Em [9, 12] encontramos que Leonhard Paul Euler nasceu na Basileia, Suíça, sendo encaminhado por seu pai para a Universidade de Basileia visando aprofundamento em Teologia, no entanto a Geometria o cativou. Com a ajuda de Johann Bernoulli, Euler conseguiu o consentimento de seu pai para seguir os caminhos da Matemática, unindo-se em 1727 à Academia de Ciência de São Petersburgo, tornando-se professor de Física em 1730 e de Matemática em 1733. A reputação de Euler ganha notoriedade em 1736/37, após a publicação de alguns artigos e de seu livro intitulado *"Mechanica"*, que apresenta a Dinâmica Newtoniana em forma de Análise Matemática. Em 1745, Euler ingressa na Academia de Ciência de Berlim onde manteve sua cadeira por 25 anos. Durante esse período, tornou-se diretor de Seção Matemática e escreveu 200 artigos, 3 livros de

Análise Matemática e a popularização científica denominada *"Cartas"* para a princesa da Alemanha composta por 3 volumes que foram publicados entre 1768/1772.

Acabou retornando à Rússia em 1766 a convite de Catherine a Grande, no entanto devido a problemas oculares ficou praticamente cego, porém isso não o impediu de continuar suas pesquisas e fundamentar tratados em Ótica, Álgebra e Movimento Lunar.

Segundo [9, 12] Johann Bernoulli foi um matemático discípulo de Leibniz e juntamente com seu irmão Jacques Bernoulli introduziu em 1669 a palavra integral.

Figura 1.7: Johann Bernoulli

Fonte : https://alchetron.com/Johann-Bernoulli

Em 1671 iniciou os estudos na Teoria do Cálculo Diferencial e Integral , publicando um ano depois, dois livros sobre Cálculo. Para ganhar a vida, tornou-se professor particular de Guilherme François L'Hospital para o qual passava todas suas descobertas matemáticas, o que acabou culminando na publicação da Regra de L'Hospital; *"Análise dos Infinitamente Pequenos"* que focava na resolução de limites indeterminados. A publicação é categorizada como o primeiro livro de Cálculo Diferencial e Integral editado no mundo, sendo fundamental para a disseminação do Cálculo entre os estudiosos do século XVIII. Esse livro teve um sucesso tão grande que foi publicado durante dois séculos sendo que, no prefácio, L'Hospital agradece as contribuições de Bernoulli e Leibniz.

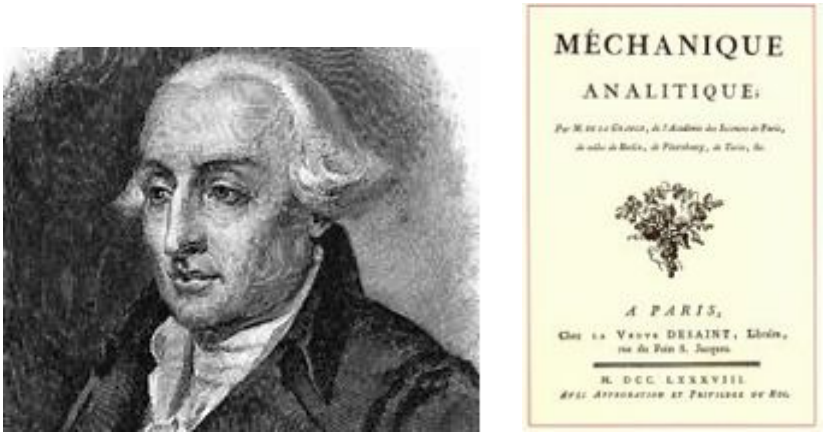
Ainda segundo [12], em 1675, inicia sua carreira de professor na Universidade de Groningen fundamentando os estudos que o levariam a desenvolver o Cálculo Variacional propondo, na *Revista Acta Eruditorium*, o problema do tempo mínimo de descida de um corpo sob a ação do campo gravitacional.

Em 1711, Bernoulli era amplamente conhecido por seus trabalhos dentro da matemática, física e engenharia, principalmente no que concerne a propriedade da catenária. Johann Bernoulli começa a apresentar uma séria paranoia em 1712 que o leva ao isola-

mento e a recusa de compartilhar seus conhecimentos e suas teorias. Após ficar isolado, seu quadro de saúde piora e acaba por falecer em 1748 aos 81 anos.

Na França, após a morte de Descartes, Pascal e Fermat segundo [12] nenhum matemático francês de estatura comparável apareceu por mais de um século. Na Inglaterra, a Matemática tinha nomes como Newton e depois Taylor, Sterling e Maclaurin, enquanto Leibniz aparecia na Alemanha. Bernoulli e Euler marcaram a atividade matemática na Suíça por seu trabalho. No final do século XVIII, Paris tornou-se novamente o centro dos estudos matemáticos devido ao glorioso trabalho de Lagrange, Laplace e Legendre.

Figura 1.8: Joseph Louis Lagrange e sua obra Mecanique Analityque



Fonte : https://www.thefamouspeople.com/profiles/joseph-louis-lagrange-446.php, https://archive.org/details/mcaniqueanalyt02lagr

Joseph-Louis Lagrange(1736-1813) era um matemático e astrônomo italiano de nascimento, alemão por adoção e francês por opção que viveu na Era do Iluminismo. Ele fez contribuições consideráveis nos campos da Análise Matemática e da Teoria dos Números. Segundo [12], Lagrange, quando entrou na universidade, tinha grande interesse em Física, porém ao ler um trecho dos méritos do cálculo newtoniano, ficou entusiasmado com a nova matemática que estava transformando a mecânica celeste. A Academia Francesa de Ciências logo se acostumou a incluir Lagrange em suas competições em seus prêmios bienais e, entre 1764-1788, ele ganhou cinco dos cobiçados prêmios por suas aplicações de matemática aos problemas da astronomia. Tornou-se professor de matemática na Escola de Artilharia de Turima aos 19 anos de idade e é conhecido por sua afirmação:

> "Se eu fosse rico, nunca faria matemática."

Leonhard Euler reconheceu seu talento e, frequentemente, revisou seus trabalhos. Grande parte da contribuição de Lagrange para a Teoria dos Números são as provas de teoremas já conhecidos.

Em [12], em 1766, quando Euler partiu de Berlim para São Petersburgo, Frederico providenciou que Lagrange preenchesse o posto vago acompanhando o seu convite com uma mensagem modesta que dizia:

> "É necessário que o maior geômetra da Europa viva perto do maior dos Reis."

Nos vinte anos seguintes, segundo [12], Lagrange atuou como diretor da Seção de Matemática da Academia de Berlim, produzindo trabalhos de alta distinção que acabaram por culminar em seu monumental tratado, o *"Mecanique Analytique"* (publicado em 1788 em quatro volumes).

Embora a pesquisa de Lagrange abrangesse um extraordinário espectro amplo, ele possuía, assim como Diophantus e Fermat, um talento especial para a Teoria dos Números .

O trabalho de Lagrange inclui a primeira prova do Teorema de Wilson que se n é primo, então $(n-1)! \equiv -1(mod\ n)$; a investigação das condições sob as quais ± 2 e ± 5 são resíduos quadráticos ou não resíduos de um primo ímpar (-1 e ± 3 foram discutidos por Euler); encontrando todas as soluções inteiras da equação $x^2 - ay^2 = 1$; e a solução de vários problemas colocados por Fermat no sentido de que certos primos podem ser representados de maneiras particulares (típico disso é o resultado que afirma que todo primo $p \equiv 3(mod\ 8)$ tem a forma $p = a^2 + 2b^2$). Além, é claro, a descoberta pela qual Lagrange adquiriu seu maior renome na Teoria dos Números, a prova de que todo número inteiro positivo pode ser expresso como a soma de quatro quadrados.

Em 1770, em *"Meditationes algebraicae"*, Edward Waring (1741-1793) afirmou que um de seus alunos, John Wilson, conjeturou que, se p é primo, ele divide $(p-1)! + 1$, mas a prova parecia difícil devido à falta de notação para expressar números primos.

Wilson parece ter advinhado isso com base em cálculos numéricos, segundo [12]. Nem ele nem Warring sabiam como provar, o que se pode atestar através de sua declaração de que:

> "Teoremas desse tipo serão muito difíceis de provar devido à ausência de uma notação para expressar números primos."

(Ao ler a passagem, Gauss pronunciou seu comentário revelador sobre "notações versus noções", segundo o qual em questões dessa natureza era a noção que realmente importava, não a notação). Apesar da previsão pessimista de Warring, Lagrange, logo depois, em 1771, deu uma prova do que na literatura é chamada de "Teorema de Wilson" e observou que o contrário também se mantém.

Ainda em [12], os estudos de Euler sobre resíduos quadráticos foram desenvolvidos pelo matemático francês Adrien Marie Legendre (1752-1833). As memórias de Legendre *"Recherches d'Analyse Indeterminee"* (1785) contêm uma descrição da Lei da Reciprocidade Quadrática e suas muitas aplicações, um esboço de uma teoria da representação de um número inteiro como a soma de três quadrados e a declaração de um famoso teorema:

> "Toda progressão aritmética $ax+b$, onde $mdc(a,b) = 1$, contém um número infinito de números primos."

Em [12], os tópicos abordados em *"Recherches"* foram desenvolvidos de maneira mais completa e sistemática em seu *"Essai sur la Theorie des Nombres"*, publicado em 1798. Isso representava o primeiro tratado "moderno" dedicado exclusivamente à Teoria dos Números, cujos precursores eram traduções ou comentários sobre Diophantus. O *"Essai sur la Theorie des Nombres"* de Legendre foi posteriormente expandido para sua *"Theorie des Nombres."*

Embora Legendre não tenha feito grandes inovações na Teoria dos Números, para [12] ele levantou questões frutíferas que forneceram objeto de investigação para os matemáticos do século XIX.

Figura 1.9: Adrien Marie Legendre

Fonte : https://www.thefamouspeople.com/profiles/adrien-marie-legendre-591.php

Ainda em [12] é extremamente importante que Carl Friedrich Gauss(1777-1855) tenha publicado "Disquisitiones Arithmeticae" em 1801 uma obra monumental, onde encontramos os fundamentos da Moderna Teoria dos Números. Nela, Gauss organizou e resumiu muitos trabalhos e, em seguida, adentrou com ousadia na fronteira da pesquisa. Ao observar que o problema de resolver números compostos em fatores primos era um dos mais importantes e úteis em aritmética, Gauss acabou por fornecer a primeira prova moderna do Teorema da Fatoração Única. Ele também deu a primeira prova da lei da Reciprocidade Quadrática, um resultado profundo da suposição anterior de Euler. Ele alegou que um teorema pertence àquele que faz a primeira demonstração rigorosa. O indignado Legendre foi levado a reclamar:

> "Esse excesso de insolência é inacreditável em um homem que tem mérito pessoal suficiente para não ter a necessidade de se apropriar das descobertas de outros."

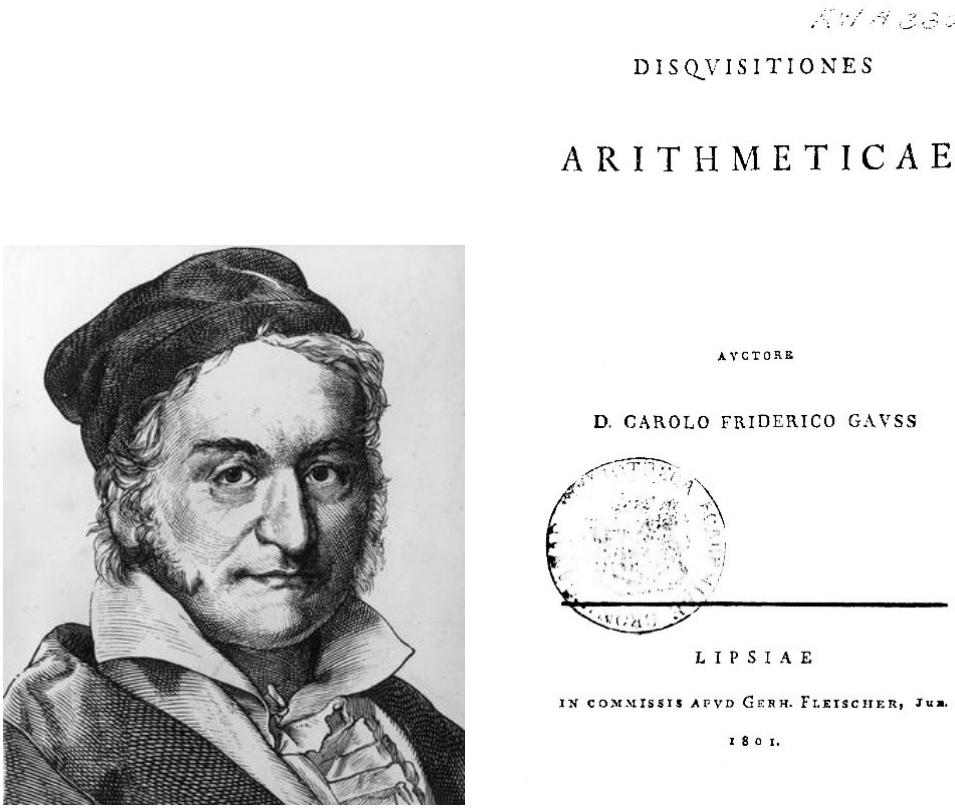
Toda discussão sobre prioridade entre os dois foi inútil, porque cada um se apegou à correção de sua posição, nenhum prestou atenção ao outro.

Para agilizar seu trabalho, de acordo com [12], Gauss introduziu a ideia de congruência entre os números, isto é, ele definiu a e b para ser congruente módulo m (escrito $a \equiv b \, mod \, m$) se m dividir igualmente a diferença $a - b$. Por exemplo, $39 \equiv 4 \, mod \, 7$. Essa inovação, quando combinada com resultados como o Pequeno Teorema de Fermat, tornou-se um elemento indispensável da Teoria dos Números.

Gauss publicou cinco demonstrações diferentes do que chamou de "*a joia da Aritmética Superior*", e outra foi encontrada em seus artigos. Gauss seguiu para uma sucessão de triunfos, cada nova descoberta segue os passos de um trabalho anterior. A tese de Doutorado de Gauss de 1799 forneceu uma prova rigorosa do Teorema Fundamental da Álgebra. O Teorema Fundamental da Álgebra sempre foi um dos favoritos de Gauss e ele deu ao todo quatro demonstrações distintas.

Inspirados por Gauss, segundo [12], outros matemáticos do século XIX aceitaram o desafio. Sophie Germain (1776-1831), declarou certa vez: nunca paro de pensar na Teoria dos Números e acabou por fazer importantes contribuições ao Último Teorema de

Figura 1.10: Carl Friedrich Gauss e Disquisitiones Arithmeticae


DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Jun.

1801.

Fonte : https://www.alamy.com/stock-photo-historical-drawing-19th-century-johann-carl-friedrich-gauss-1777-1855-47544759.html,
https : //pt.wikipedia.org/wiki/Disquisitiones_Arithmeticae

Fermat, e Adrien-Marie Legendre(1752-1833) e Peter Gustav Lejeune Dirichlet(1805-59) confirmaram o teorema para $n = 5$, ou seja, eles mostraram que a soma de quintas potências retorna um número na quinta potência. Em 1847, Ernst Kummer(1810-1893) deduziu ainda mais esse fato, provando que o Último Teorema de Fermat era verdadeiro para uma grande classe de expoentes; mas infelizmente, ele não pôde descartar a possibilidade de que isso fosse falso para uma grande classe de expoentes; portanto, o problema permanecia sem solução.

Em [12] encontramos que o mesmo Dirichlet, que supostamente mantinha uma cópia das *"Disquisitiones Arithmeticae"* de Gauss, acabou por contribuir de forma única ao provar que, se a e b não possuem fator comum, a progressão aritmética $a, a+b, a+2b, a+3b, \ldots$ deve conter infinitos primos. Entre outras coisas, isso acabou por estabelecer a existência de infinitos primos na forma $4k + 1$ e também na forma $4k - 1$. Mas o que tornou esse teorema tão excepcional foi a utilização de técnicas de cálculo para se estabelecer um resultado na Teoria dos Números, e essa surpreendente estratégia, embora engenhosa, acaba por marcar o início de um novo ramo a Teoria Analítica dos Números.

O Teorema dos Números Primos é possivelmente uma das maiores realizações do século XIX e sobre isso podemos discorrer um pouco mais. Primeiro, vamos usar $\pi(n)$ para especificar o número de primos menor ou igual a n. Portanto, $\pi(10) = 4$ porque $2, 3, 5$ *e* 7 são os quatro números primos que não excedem 10. Da mesma forma $\pi(25) = 9$ e $\pi(100) = 25$. Em seguida, considere a proporção de números menor ou igual n que

Figura 1.11: Peter Gustav Lejeune Dirichlet

Fonte:
http://mfht206.aries.dyu.edu.tw/history/19/19germanyface/Dirichlet/Dirichlet.html

são primos, isto é $\frac{\pi(n)}{n}$. Claramente $\frac{\pi(10)}{10} = 0,40$, significando que 40% dos números que não excedem 10 são primos. Outras proporções são mostradas na Tabela 1.1 que se encontra a seguir.

Tabela 1.1: Teorema dos Números Primos

n	$\pi(n)$	$\frac{\pi(n)}{n}$	$\frac{1}{\log n}$
10^2	25	0.2500	0.2172
10^4	1.229	0.1229	0.1086
10^6	78.498	0.785	0.0724
10^8	5.761.455	0.0570	0.0543
10^{10}	455.052.511	0.0455	0.0434
10^{12}	37.607.912.018	0.0377	0.0362
10^{14}	3.204.941.750.802	0.0320	0.0310

O padrão não é muito claro, mas o Teorema do Número Primo pode pelo menos aproximar-se de um padrão e portanto, fornecer uma regra para a distribuição de números primos entre os números inteiros. O Teorema diz que, para n grande, a proporção $\frac{\pi(n)}{n}$ é aproximadamente $\frac{1}{\log n}$, $\log n$ é o logaritmo natural de n. Esse vínculo entre números primos e logaritmos é extraordinário, segundo [12].

Um dos primeiros a notar isso foi o jovem Gauss, segundo [12], cujo exame de tabelas e números primos sugeria isso à sua mente fértil. Após a exploração de Dirichlet das técnicas analíticas na Teoria dos Números, Bernhard Riemann(1826-1866) e Pafnuty Chebyshev(1821- 1894) fizeram progressos substanciais antes que o Teorema do Número

Primo fosse provado em 1896 por Jacques Hadamard(1865- 1963) e Charles Jean de la Vallée-Poussin (1866-1962). Isso levou o século XIX a um fim triunfante.

Para Burton [12], o século seguinte assistiu um crescimento explosivo na pesquisa da Teoria dos Números. Juntamente com a Teoria dos Números Clássica e Analítica, os estudiosos passaram a explorar subcampos especiais, como Teoria dos Números Algébricos, Teoria dos Números Geométricos e Teoria dos Números Combinatórios. Os conceitos se tornaram mais abstratos e as técnicas mais complexas. Inquestionavelmente, o assunto havia crescido além dos sonhos mais loucos de Fermat.

Para [12] o gênio incandescente Srinivasa Ramanujan(1887-1920) foi um dos grandes colaboradores no início do século XX. O treinamento formal de Ramanujan foi limitado por sua curta vida, e ele invadiu o campo da Matemática através de uma série de descobertas notáveis onde a Teoria dos Números Analíticos foi sua especialidade. Suas publicações traziam títulos como *"Números altamente compostos"* e *"Prova de que quase todos os números n são compostos por fatores primos* $\log(\log n)$*."*

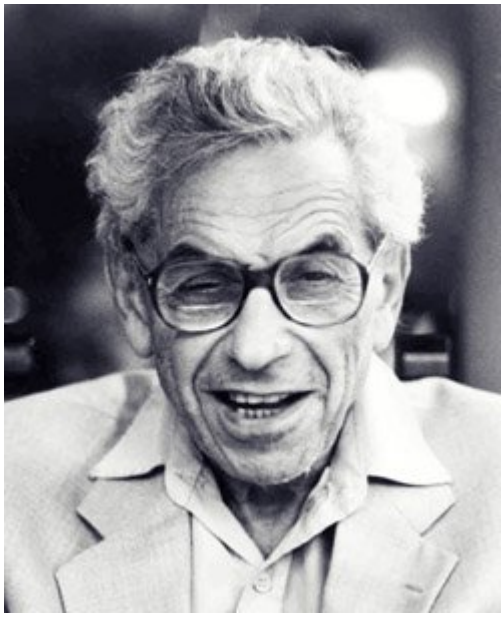
Figura 1.12: Srinivasa Ramanujan

Fonte : https://www.ndtv.com/education/national-mathematics-day-country-remembers-man-who-knew-infinity-srinivasa-ramanujan-2152613

Em [5, 23] encontramos que Paul Erdös (1913-1996) é uma figura lendária na Teoria dos Números do século XX. Foi um gênio húngaro conhecido por suas ideias profundas, seu amplo círculo de colaboradores e suas particularidades pessoais. Nascido em Budapeste, filho de pais professores de matemática do ensino médio acabou aprendendo matemática à distância. Com quatro anos de idade, ele estava familiarizado com números negativos e foi capaz de multiplicar números de quatro dígitos. Ele entreteve os amigos de sua mãe convertendo a idade deles em segundos. Ele disse a si mesmo que, quando criança, tinha um senso muito bom de números. Questionado sobre por que os números são bonitos, ele respondeu: É como perguntar por que a Nona Sinfonia de Beethoven é bonita. Se eles não são bonitos, nada é bonito. Aos 16 anos, seu pai lhe ensinou séries infinitas e a teoria dos conjuntos. Erdös, aos 18 anos, acabou por publicar uma prova bastante simplificada de um teorema de Chebyshev, afirmando que, se $n \geqslant 2$, então deveria existir um primo entre n e $2n$. Este é o primeiro de uma série de resultados teóricos numéricos que durariam a maior parte do século. Nesse processo, Erdös, que também se envolveu com combinatória,

teoria de grafos e teoria das dimensões, publicou mais de 1500 artigos com mais de 500 colaboradores de todo o mundo, tornando-se assim ao lado de Euler o matemático mais prolífico ao longo do tempo. Ele era um nômade, constantemente procurando novas matemáticas de uma universidade para outra, e obtendo resultados surpreendentes. Não era incomum ele chegar, sem aviso prévio, declarando que seu cérebro estava aberto e logo em seguida mergulhar entusiasticamente nos problemas mais recentes.

Figura 1.13: Paul Erdös



Fonte: https://numeroimaginario.wordpress.com/2016/09/20/paul-erdos-uma-vida-dedicada-a-matematica/

Cabe ressaltar que existem dois desenvolvimentos que merecem ser ressaltados. O primeiro foi a invenção do computador eletrônico, cuja velocidade foi vantajosamente aplicada a questões da Teoria dos Números. Por exemplo, Euler especulou que pelo menos quatro quarta potências devem ser somadas para que a soma seja uma quarta potência. Mas em 1988, usando uma combinação de discernimento matemático e o uso do computador, o americano Noam Elkies descobriu que $2.682.440^4 + 15.365.639^4 + 18.796.760^4 = 20.615.673^4$. Um contra-exemplo estupendo que destruiu a conjectura de Euler (O número à direita contém 30 dígitos, portanto, não é de admirar que Euler tivesse cometido um erro).

E o segundo é que a Teoria dos Números ganhou um estilo aplicado, pois desempenhou um papel instrumental no projeto de esquemas de criptografia amplamente utilizados no governo e nos negócios. Ele se baseia na decomposição de gigantescos números em números primos - uma fatoração que é conhecida pelos usuários do código, enquanto a possível quebra de código não. Essa aplicação contradiz a visão de longa data da Teoria dos Números, ou seja, a Teoria dos Números ser bonita, mas essencialmente inútil.

A Teoria dos Números do século XX atingiu um clímax em 1995, quando o inglês Andrew Wiles juntamente com seu colega britânico Richard Taylor acabam provando o Último Teorema de Fermat. Wiles teve sucesso onde muitos falharam com uma prova de 130 páginas de incrível complexidade, que certamente não caberia em nenhuma margem.

Alguns problemas ainda permanecem em aberto apesar do esforço de muitos. Provavelmente, assim como o Último Teorema de Fermat eles acabem por serem resolvidos, ou acabem permanecendo como desafios no futuro. Desta forma estes mistérios, que exigem esforços de pesquisa em uma ampla gama de disciplinas matemáticas acabem por justificar a caracterização da Teoria dos Números como o último grande continente incivilizado da matemática.

1.2 Revisão histórica de Diophantus e sua Arithmetica

Segundo Bashmakova [6] na segunda metade do século XX, a análise de Diophantus se tornou moda devido à sua proximidade com a geometria algébrica. Surpreendentemente, praticamente nada foi escrito sobre Diophantus, cujo nome está ligado à análise de indeterminados e é um dos estudiosos mais interessantes da Antiguidade. Até os historiadores da Matemática às vezes têm uma visão equivocada de seu trabalho. A maioria deles pensa que ele resolveu um problema específico equivalente a uma equação indefinida por alguns métodos específicos.

Até os simples problemas de Diophantus a partir da análise mostram que ele não apenas colocou o problema de encontrar soluções racionais em equações indeterminadas, mas também deu alguns métodos gerais para obtê-las. Deve-se lembrar que na matemática antiga, métodos gerais não eram apresentados em "forma pura", além de problemas gerais. Por exemplo, quando Archimedes calculou a área de uma elipse e o volume de uma esfera, ele usou o método de somas integrais e o caminho de limites sem fornecer, no entanto, uma descrição geral e abstrata dos métodos utilizados. Nos séculos XVII e XVIII, os cientistas tiveram que estudar cuidadosamente suas obras e interpretá-las para estudar o método geral. O mesmo vale para Diophantus. Seus métodos foram entendidos e transformados para a solução de novos problemas por Viete e Fermat no momento em que os trabalhos de Archimedes estavam sendo decifrados.

Em [6] embora a descoberta do cálculo diferencial e integral por Newton e Leibniz basicamente tenham encerrado o método de integração de Archimedes, a evolução dos métodos diofantianos foi estendida por vários séculos e entrelaçada com a teoria das funções algébricas e com a geometria algébrica. A evolução das ideias de Diophantus pode ser rastreada até o trabalho de Henri Poincaré e André Weil. Isso torna interessante a história da análise de Diophantus.

Muitos historiadores da ciência pensam que Diophantus se limitou a números racionais positivos e não tinha conhecimento de números negativos. Vamos tentar mostrar que esse não é o caso, que em sua *"Arithmetica"* ele estendeu o domínio ao campo dos números racionais. A visão que a maioria tem da matemática está baseada nos *"Elements"* de Euclides e nas obras de Archimedes e Apolônio, mas Diophantus acaba por nos proporcionar um mundo igualmente rico e bonito de aritmética e álgebra.

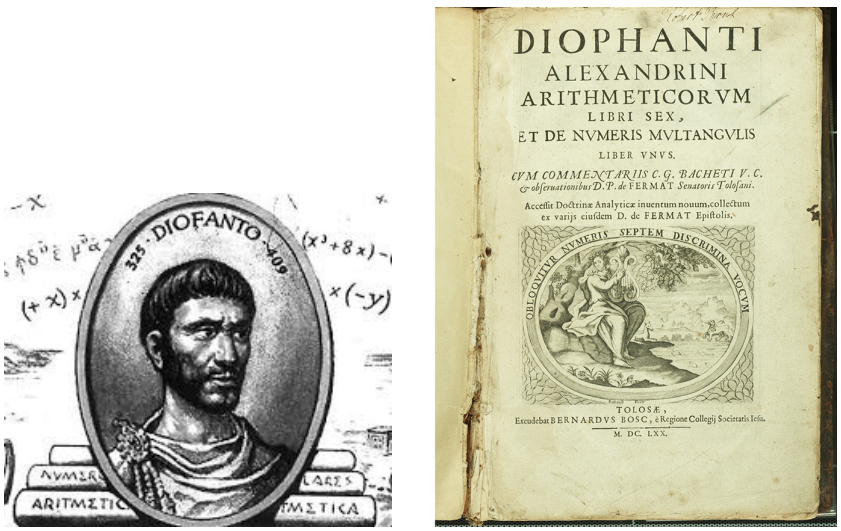
1.3 Diophantus

Bashmakova em [6] afirma que Diophantus representa um dos maiores quebra cabeças da história da Ciência. Não sabemos quando ele viveu e não conhecemos os seus predecessores que podem ter trabalhado na mesma área. Suas obras lembram um fogo piscando em uma escuridão impenetrável.

Ele pode ter vivido a qualquer momento durante um período de 500 anos. O limite inferior é facilmente determinado, porque em seu livro sobre Polígonos, Diophantus menciona com frequência, o matemático Hipsikles de Alexandria que viveu no século II a.C. Por outro lado, nos comentários de *"Almagest de Ptolomeu"*, Theon de Alexandria cita trechos do trabalho de Diophantus. Theon viveu em meados do século IV aC. Daí o período de 500 anos.

Em [6] o historiador francês de Matemática Paul Tannery, responsável pelos mais completos textos de Diophantus, tentou estreitar este intervalo de tempo. Na Biblioteca Escurial ele encontrou escritos do intelectual Michael Psellus, um estudioso bizantino do século XI, que foi usado para datar Diophantus com maior precisão. Nesse escrito, Psellus menciona o trabalho sobre Arithmetica (o *"Método Egípcio dos Números"*, como ele o chama) por um certo Anatolius que foi dedicado a Diophantus. Tannery identificou esse autor com o historicamente conhecido Anatolius de Alexandria, um filósofo que era o bispo de Laodicéia (uma cidade antiga na atual costa Síria) por volta de 270-280 d.C., e que de fato foi o autor de um tratado sobre Aritmética, dos quais temos fragmentos. Supondo que um tratado possa ser "*dedicado*" apenas a uma pessoa ainda viva, isso colocaria Diophantus no século III d.C.. Trechos deste trabalho *"Introdução a Aritmética"* são citados em obras preservadas de Iamblichus e Eusebius.

Figura 1.14: Diophantus



Fonte : https://br.pinterest.com/pin/793407659334320638/, https://www.maa.org/press/periodicals/convergence/mathematical-treasure-bachets-arithmetic-of-diophantus

Segundo [6] a *"Arithmetica"* de Diophantus é dedicada ao "reverendo Dionysus" que interessava-se pela Aritmética e seu estudo. Enquanto o nome Dionysus era relativamente comum na época, Tannery assumiu que o "reverendo Dionysus" tinha que ser procurado entre as pessoas conhecidas desse período que ocupavam posições proeminentes. Surpreendentemente, descobriu-se que um certo Dionysus, que de 231 em diante foi diretor da escola cristã de Alexandria, tornou-se bispo da cidade em 247. É por este motivo que Tannery identificou este Dionysus com o que Diophantus dedicou a sua obra, e assim chegou à conclusão que Diophantus viveu em meados do século III. Na ausência de uma cronologia melhor, temos a de Paul Tannery.

Todavia o lugar onde Diophantus viveu é bem conhecido. É a famosa Alexandria, centro do pensamento científico do mundo helênico.

Após o colapso do enorme império de Alexandre - o Grande,segundo [6], o Egito foi governado por Ptolomeu Lagus, um dos generais de Alexandre, que fez da nova cidade de Alexandria sua capital. Esse centro comercial multilíngue logo se tornou uma das mais belas cidades da antiguidade. Por muitos séculos, Alexandria foi o centro científico e cultural do mundo antigo, por causa da fundação do Museu por Ptolomeu, o templo das Musas, uma espécie de Academia de Ciências que atraiu importantes estudiosos que eram remunerados e seu dever era essencialmente meditar e envolver-se em discussões com seus alunos. Essa Academia de Ciências incluía uma esplêndida biblioteca que, em certa época, chegou a ter por volta de 700.000 manuscritos. Não é de admirar que os estudiosos e os jovens sedentos de conhecimento se dirigissem a Alexandria para ouvir filósofos ilustres, aprender Astronomia e Matemática e mergulhar no estudo de manuscritos únicos nas salas da biblioteca.

Segundo [6], na virada do século III para o século II a.C., o museu brilhou com os nomes de Euclides, Apollonius, Eratosthenes e Hippharcus. Nos primeiros séculos d.C. sofreu um declínio temporário, devido ao declínio da casa dos Ptolomeus e às conquistas romanas (Alexandria foi conquistado em 31 d.C.), mas nos primeiros séculos d.C. foi regenerada devido ao apoio dos imperadores romanos. Do Século I ao século III, estudiosos como Heron, Ptolomeu e Diophantus trabalharam ali. Alexandria continuou a ser o centro científico do mundo. A esse respeito, Roma nunca foi sua rival, pois, simplesmente não existia a ciência romana.

A fim de fazer uso de tudo o que se sabe sobre a pessoa de Diophantus, citamos o seguinte enigma:

> "Caminhante! Aqui estão sepultados os restos de Diofanthus. E os números podem mostrar (milagre!) quão longa foi a sua vida, cuja sexta parte foi a sua bela infância. Tinha decorrido mais uma duodécima parte de sua vida, quando seu rosto se cobriu de pêlos. E a sétima parte de sua existência decorreu com um casamento estéril. Passou mais um quinquênio e ficou feliz com o nascimento de seu querido primogênito, cuja bela existência durou apenas metade da de seu pai, que com muita pena de todos desceu à sepultura quatro anos depois do enterro de seu filho."

O texto traduzido para a língua da Álgebra teria o seguinte significado:

- O número correspondente ao seu tempo de vida - $\mathbf{x}$
- Um sexto de sua vida é constituído por uma infância maravilhosa - $\frac{x}{6}$
- Um dozeavos é sua juventude - $\frac{x}{12}$
- Diophantus passou um sétimo de sua vida casado sem filhos - $\frac{x}{7}$
- Mais cinco anos se passaram até Hímen lhe dar um filho - 5
- Destino quis que seu filho vivesse duas vezes menos que seu pai - $\frac{x}{2}$
- O velho viveu por mais quatro anos em profunda dor por seu filho perdido - 4

Para traduzir isso na equação algébrica:

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

A partir disso, é fácil concluir que Diophantus viveu 84 anos. Não é necessário conhecer a arte de Diophantus para dominar isso. Basta saber que você resolve uma equação de primeira ordem com uma variável desconhecida, algo que os escribas egípcios sabiam e fizeram já em 2000 a.C.

Mas para [6] o enigma mais mistificador é o trabalho de Diophantus. Apenas seis dos 13 livros que compõem a *"Arithmetica"* chegaram até nós. Seu estilo e conteúdo diferem radicalmente das obras antigas clássicas na Teoria dos Números e Álgebra cujos modelos sabemos dos *"Elements"* e *"Dados"* de Euclides e dos lemas de Archimedes e Apollonius. A *"Arithmetica"* é, sem dúvida, o resultado de numerosas investigações que são completamente desconhecidas para nós. Nós só podemos adivinhar as suas raízes e admirar a riqueza e beleza dos seus resultados.

Segundo [6], *"Arithmetica"* de Diophantus é uma coleção de problemas que vêm com uma ou mais soluções e as explicações necessárias. Daí a impressão inicial de que isso não é um trabalho teórico. Mas uma leitura minuciosa mostra que os problemas foram cuidadosamente escolhidos e servem para ilustrar métodos definidos e rigorosamente pensados. Seguindo a norma da antiguidade, os métodos não são declarados de forma geral, mas reaparecem nas soluções de problemas do mesmo tipo.

1.4 Números e Símbolos

Para Bashmakova [6] o primeiro livro de Diophantus é precedido por uma "*Introdução Geral*" onde começa com definições fundamentais e uma descrição literal dos símbolos que serão utilizados.

Na matemática clássica grega, em *"Elements"* de Euclides, os números ($\acute{\alpha}\rho\iota\vartheta\mu\acute{\sigma}\zeta$, a partir dessa palavra era chamada de "*Aritmética*" (a Ciência dos Números) significavam coleções de unidades, que eram números inteiros. Frações e irracionais não eram chamadas de números. Estritamente não há frações nos *"Elements"*, a "unidade" foi vista como indivisível, e em vez de frações de unidade, foi considerada como proporções de números inteiros. Quantidades irracionais assumiram a forma de proporções de segmentos incomensuráveis. Assim, para os gregos do período clássico o número que agora é denotado por $\sqrt{2}$ foi a relação entre a diagonal de um quadrado de lado um. Não houve números negativos e nem equivalentes de números negativos. No caso de Diophantus a imagem é radicalmente diferente.

Em [6] encontramos que Diophantus dá a definição tradicional de um número como uma coleção de unidades, mas quando se trata de seus problemas, ele procura racionalmente soluções positivas e chama cada uma delas de número "$\acute{\alpha}\rho\iota\vartheta\mu\acute{\sigma}\zeta$."

Mas isso não é tudo. Diophantus introduz números negativos: ele se refere a eles pelo termo especial "$\lambda\varepsilon\tau\psi\tilde{\imath}\zeta$", derivada da palavra "$\lambda\varepsilon\tilde{\imath}\pi\omega$" estar ausente, não basta - para que o próprio termo pudesse ser traduzido como "escassez". Diophantus chama um número positivo "$\upsilon\pi\alpha\rho\xi\iota\zeta$" de existência, ser. A forma plural dessa palavra denota propriedade. Assim, termos de Diophantus para os números assinalados são próximos aos utilizados durante a Idade Média no Oriente e na Europa. Muito provavelmente, esses termos eram simplesmente traduções do grego para o árabe, sânscrito e latim, e depois nas diferentes línguas europeias.

Muitos tradutores de Diophantus processam "$\lambda\varepsilon\tilde{\imath}\psi\iota\zeta$" como subtraendo. Isto está errado. De fato, para indicar a operação de subtração Diophantus usa os termos "$\acute{\alpha}\varphi\varepsilon\lambda\varepsilon\tilde{\imath}\nu$" ou "$\acute{\alpha}\varphi\alpha\tilde{\imath}\rho\varepsilon\iota\nu$" derivados da palavra "$\acute{\alpha}\varphi\alpha\tilde{\imath}\rho\varepsilon\omega$", para subtrair. Ao transformamos as equações diofantinas freqüentemente usamos a expressão padrão "vamos adicionar a ambos os lados $\lambda\varepsilon\tilde{\imath}\psi\iota\zeta$".

Ao entrarmos numa análise filológica detalhada do texto de Diophantus nos convencemos de que é correto traduzir os termos de Diophantus como "positivo" e "negativo".

Bashmakova afirma que Diophantus formula para números relativos a seguinte regra de sinais: "um negativo multiplicado por um negativo produz um positivo, enquanto um negativo por um positivo produz um negativo e o sinal distintivo, pois, o negativo é "$\pitchfork$", invertido e encurtado (letra) ψ."

Ele continua:

> "Agora que eu expliquei a você a multiplicação de potências e seus recíprocos, a divisão de tais expressões também se torna clara. Agora será uma boa coisa para o iniciante fazer exercícios envolvendo adição, subtração e multiplicação de expressões algébricas. Ele deve saber como adicionar expressões positivas e negativas com coeficientes diferentes para outras expressões, que podem ser positivos ou, igualmente, positivos e negativos, e subtrair de expressões que podem ser somas ou diferenças de outras grandezas. [6]"

Note que enquanto Diophantus está procurando apenas por soluções racionais positivas, ele prontamente usa números negativos em cálculos intermediários. Assim, é seguro dizer que Diophantus estendeu o domínio do número para o campo dos racionais, onde se pode facilmente realizar todos as operações aritméticas.

Segundo [6] em *"Arithmetica"* encontramos pela primeira vez o simbolismo literal. Diophantus introduziu as seguintes notações para as seis potências x, x^2, ..., x^6 da incógnita x:

- a primeira potência - ζ
- a segunda potência - Δ^{υ} de $\Delta\acute{\upsilon}\nu\alpha\mu\iota\zeta$, força, potência;
- a terceira potência - κ^{υ}, de $\kappa\acute{\upsilon}\beta\sigma\zeta$, cubo;
- a quarta potência - $\Delta^{\upsilon}\Delta$ de $\Delta\acute{\upsilon}\nu\alpha\mu\sigma\delta\acute{\upsilon}\nu\alpha\mu\iota\zeta$, quadrado quadrado;
- a quinta potência - $\Delta\kappa^{\upsilon}$ de $\Delta\acute{\upsilon}\nu\alpha\mu\sigma\chi\acute{\upsilon}\beta\sigma\iota$, cubo quadrado;
- a sexta potência - $\kappa^{\upsilon}\kappa$ $\kappa\acute{\upsilon}\beta\sigma\chi\acute{\upsilon}\beta\sigma\zeta$, cubo cubo.

Conforme [6], Diophantus denota o termo constante, isto é x^{σ}, pelo símbolo $M^{\mu\sigma}$, isto é, pelas primeiras duas letras em $\mu\sigma\nu\alpha\zeta$; ou unidade.

Ainda, segundo [6], ele introduziu um símbolo especial $^{\chi}$ para expoentes negativos. Nesse caminho ele poderia denotar os primeiros seis expoentes negativos da incógnita. Por exemplo, ele denotou x^{-2} e x^{-3} por $\Delta^{\upsilon\chi}$ e $\kappa^{\upsilon\chi}$ respectivamente.

Assim, para [6], Diophantus tinha um simbolismo para denotar potências positivas e negativas de uma única incógnita x até a sexta potência. Ele não conseguiu introduzir um símbolo para uma segunda incógnita o que acabou por complicar grandemente a solução de problemas. Às vezes, dentro de um único problema ζ denota mais de um número desconhecido(incógnita). Em adição a estes símbolos, Diophantus usou o símbolo $\square$ para

um quadrado indeterminado. Por exemplo, se, a condição do problema, é a soma dos produtos de dois números e um deles é para ser um quadrado, então o último é denotado por $\square$.

Então Diophantus dá as regras para a multiplicação de x^m por x^n para m e n positivos e negativos ($\mid m \mid \leqslant 6$, $\mid n \mid \leqslant 6$).

Para o sinal de igualdade Diophantus usou o símbolo $\iota\sigma$ - as duas primeiras letras da palavra $\iota\sigma\varrho\zeta$; que significa igual. Tudo isso permite que ele escreva equações na forma literal. Por exemplo, ele escreveu a equação :

$$202x^2 + 13 - 10x = 13$$

mais precisamente

$$x^2 202 + x^0 13 - x10 = x^0 13$$

como

$\Delta^{\upsilon}\overline{\sigma\beta}^{\circ}\overline{\iota\gamma}\ \pitchfork\ \varsigma\bar{\iota}\ \iota''\sigma\mathring{\mathrm{M}}\overline{\iota\gamma}.$

Os gregos usavam as letras do alfabeto com barras sobre elas para denotar números. As primeiras nove letras $\overline{\alpha}, \overline{\beta}, ...\overline{\upsilon}$ denotaram os números de 1 a 9. Os nove seguintes denotaram os múltiplos de 10 de 10 a 90. Os últimos nove (o alfabeto de 24 letras foi aumentado pela adição de três letras mais antigas) denotava as novecentas. Assim, por exemplo, $\overline{\sigma} = 200$, $\overline{\beta} = 2$, de modo que $\overline{\sigma\beta} = 202$. Similarmente, $\bar{\iota} = 10$, $\overline{\beta}3$, assim $\overline{\iota\beta} = 13$, segundo [6].

Na introdução, de acordo com [6], Diophantus formula regras de transformação de equações que envolviam a adição de termos iguais aos dois lados da equação e redução de termos semelhantes. Mais tarde, essas duas regras se tornaram bem conhecidas sob seus nomes arabizados de " *al-jabr*" e "*al-muqabala*".

Vemos que, de acordo com [6], quando se trata de nomear e denotar as potências de incógnitas conhecidas Diophantus prefere usar os termos geométricos "*quadrado*" e "*cubo*". Mas quando estabelece equações, ele adiciona um quadrado ou um cubo para um lado, ou seja, ele os trata não como imagens geométricas, mas como números. Além disso, ele acha possível introduzir "*quadrados quadrados*" e "*cubos quadrados*", e assim por diante, sem qualquer pensamento de amarrá-los a espaços tridimensionais. Em outras palavras, no uso da terminologia geométrica. Diophantus estava meramente seguindo uma tradição estabelecida.

Assim segundo [6], encontramos aqui uma construção completamente nova da álgebra, com base na aritmética e não, como no caso de Euclides, na geometria. Mas longe de ser um simples retorno à álgebra numérica dos babilônios, esse é o começo de uma construção da álgebra literal, que encontrou sua linguagem adequada nas obras de Diophantus.

Para Bashmakova em [6], ele foi o primeiro a empregar símbolos na álgebra grega, usando o símbolo (arithmos) para uma quantidade desconhecida, bem como símbolos para operações algébricas e para potências. *"Arithmetica"* também é significativo por seus resultados na Teoria dos Números, como o fato de que nenhum inteiro da forma $8n + 7$ pode ser escrito como a soma de três quadrados.

" Arithmetica" é uma coleção de problemas que dão informações sobre soluções aproximadas para equações até o grau três e que também contém equações que lidam com

equações indeterminadas. Acredita-se que a *"Arithmetica"* original tenha compreendido 13 livros, mas os manuscritos gregos sobreviventes contêm apenas seis. Os outros são considerados obras perdidas. É possível que esses livros foram perdidos em um incêndio que ocorreu pouco depois de Diophantus morrer.

Diophantus de Alexandria foi fundamental no desenvolvimento da Matemática simplesmente porque ele introduziu algumas abreviações e caracteres para simplificar a notação. Ele nos deixou muitas das tarefas que estabeleceu para si mesmo, ou que já são conhecidas pelos matemáticos que viveram antes dele. A maioria das atribuições de Diophantus interfere na Teoria dos Números e ele está sempre procurando soluções entre números naturais ou racionais. Geralmente, suas tarefas exigem encontrar alguns números que satisfaçam certas condições algébricas e acaba por escolher números constantes para que a tarefa seja solucionável e satisfeita com uma solução. Diophantus, além de considerar os resultados negativos e nulos sem sentido, introduziu a relação de igualdade de números e as regras de como lidar com eles, alguns têm Diophantus como "Pai da Álgebra".

2 Conceitos Básicos e Notações

O objetivo desse capítulo é servir como uma referência útil, por isso, apresentamos algumas ferramentas que serão utilizadas ao longo de nossa dissertação, servindo assim como uma referência rápida ou uma atualização na Teoria dos Números.

As presentes anotações são baseadas no texto de James K. Strayer [43], embora o material coberto seja bastante padrão e possa ser encontrado, com pequenas variações, na maioria dos textos de Teoria dos Números a nível de graduação.

2.1 Divisibilidade e Fatorização

A Teoria Elementar dos Números é o estudo das propriedades de divisibilidade dos inteiros. Na medida em que essas propriedades de divisibilidade formam a base para o estudo de tópicos mais avançados na Teoria dos Números, elas podem ser pensadas como a base para toda a área da Teoria dos Números.

Um conjunto de números está bem ordenado quando cada um de seus subconjuntos não vazios tem um elemento mínimo.

Teorema 2.1. *(Princípio da Boa Ordenação)- Existe um elemento mínimo em qualquer conjunto não vazio de inteiros positivos.*

Demonstração. Admitindo que $0 \notin A$, pois caso $0 \in A$ certamente seria 0 o menor elemento de A, assim $I_n \neq \emptyset$, já que $0 \notin A$, logo $0 \in I_n$. Temos que o menor elemento de A deve ser um número da forma $n+1$ para algum $n \in \mathbb{N}$, desta forma, $I_n \subset \mathbb{N} - A = \{x \in \mathbb{N},\ tal\ que, x \notin A\}$.

Consideremos o conjunto:

$$X = \{x \in \mathbb{N} \mid I_n \subset \mathbb{N} - A\}.$$

Podemos observar que $I_n = \{0, 1, \ldots, n\} \subset \mathbb{N} - A$ significa que nenhum elemento de I_n pertence a A. Consequentemente, todos os elementos de A são maiores que n. Como $A \neq \emptyset$, então $X \notin \mathbb{N}$, de modo que, não podemos aplicar o quarto axioma de Peano ao conjunto X, ou seja, existe algum $n \in X$ tal que $n+1 \notin X$. Assim todos os elementos de A são maiores que n, mas nem todos maiores que $n+1$. Daí $n+1$ é o menor elemento de A. □

Observação 2.2. (Quarto Axioma de Peano) - Seja X um conjunto de números naturais (isto é, $X \in \mathbb{N}$). Se $0 \in X$ e se além disso, o sucessor de todo elemento de X ainda pertencer a X, então temos que $X = \mathbb{N}$.

Este princípio pode ser tomado como um axioma sobre inteiros e será a chave para provar muitos teoremas. Como resultado, vemos que qualquer conjunto de inteiros positivos está bem ordenado, enquanto o conjunto de todos os inteiros não está bem ordenado.

Definição 2.3. (Divisibilidade) - Sejam a e b dois inteiros. Dizemos que a divide b (denotamos por $a \mid b$) se existe um inteiro k tal que $b = ka$. Se a não divide b, denotaremos $a \nmid b$.

Propriedade 2.4. (Propriedades de Divisibilidade) - Sejam a, b e c três inteiros. Então:

- (i) $a \mid a$,
- (ii) Se $a \mid b$ e $b \mid a$ então $\mid a \mid = \mid b \mid$,
- (iii) Se $a \mid b$ e $b \mid c$ então $a \mid c$,
- (iv) Se $a \mid b$ e $b \mid c$ então $a \mid bx + cy$, para todo $(x, y) \in \mathbb{Z}^2$,
- (v) Se $b \neq 0$ e $a \mid b$ então $\mid a \mid \leq \mid b \mid$.

Proposição 2.5. ***(Algoritmo Euclidiano)*** *- Sejam a e b dois inteiros tais que $b \neq 0$, então existe um número inteiro único q e um número inteiro único r tal que temos:*

$$a = qb + r, \ com \ 0 \leq r \leq \mid b \mid .$$

Demonstração. **(Existência)** Supomos que $b > 0$ (a mesma prova deve ser feita para $b < 0$). Seja q o maior inteiro tal que $qb \leq a$ então $q = \lfloor \frac{b}{a} \rfloor$ onde $\lfloor x \rfloor$ denota a parte inteira de x. Então temos

$$qb \leq a \leq (q+1)b. \tag{2.1}$$

Podemos colocar $r = a - qb$ e, portanto, a Equação(2.1) implica que $0 \leq r \leq b$. **(Unicidade)** - Assumimos que $a = qb + r = q'b + r'$. Então temos:

$$(qb + r) - (q'b + r') = 0 \Rightarrow qb - qb' + r - r' = 0 \Rightarrow (q - q')b = r' - r.$$

Podemos assumir que $r' \geq r$ então $r' - r \in \{0, \ldots, b-1\}$ e se $(q' - q)b = r' - r$, temos (uma vez que $(q - q')$ é um inteiro) que $b \mid r' - r$. Então,

$$r' - r = 0 \Rightarrow r' = r,$$

e, portanto, $(q - q')b = 0$ implica que $(q - q') = 0$. □

Nesta seção, definimos o máximo divisor comum (mdc) de dois inteiros e discutimos suas propriedades. Também provamos que o máximo divisor comum de dois inteiros é uma combinação linear desses inteiros. Dois inteiros a e b, não nulos, podem ter apenas finitos divisores e, portanto, podem ter apenas finitos divisores comuns. Estamos interessados no máximo divisor comum de a e b e notamos que os divisores de a e de $\mid a \mid$ são os mesmos.

Definição 2.6. (Máximo Divisor Comum) - Para um número inteiro positivo k denotamos por D_k o conjunto de todos os seus divisores positivos. É claro que D_k é um conjunto finito. Para inteiros positivos m, n o maior elemento no conjunto $D_m \cap D_n$ é chamado de máximo divisor comum de m e n e é denotado por $mdc(m, n)$ ou simplesmente (m, n), também definimos que $(0, 0) = 0$.

As seguintes propriedades podem ser derivadas diretamente da definição anterior.

Propriedade 2.7.

- Se $d = mdc(m,n), m = dm', n = dn'$, então $mdc(m',n') = 1$.
- Se $d = mdc(m,n), m = d'm'', n = d'n'', mdc(m'',n'') = 1$, então $d' = d$.
- Se d' é um divisor comum de m e n, então d' divide $mdc(m,n)$.
- Se $m = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ e $n = p_1^{\beta_1} \dots p_k^{\beta_k}, \alpha_i, \beta_i \geq 0, \alpha_i + \beta_i \geq 1, i = 1, \dots, k$, então

$$mdc(m,n) = p_1^{min(\alpha_1,\beta_1)} \dots p_k^{min(\alpha_k,\beta_k)}.$$

- Se $m = nq + r$ então $mdc(m,n) = mdc(n,r)$.

Lema 2.8. *Sejam a, b, q e r inteiros tais que $a = qb + r$ então $mdc(a,b) = mdc(b,r)$.*

Demonstração. Para isso, mostramos que $mdc(a,b) \leq mdc(b,r)$ e que $mdc(b,r) \leq mdc(a,b)$.

1. Estabelecemos $d = mdc(a,b)$ então $d \mid a$ e $d \mid b$. Assim, $d \mid a - qb$ o que implica que $d \mid r$ e como $d \mid r$, temos $d \leq mdc(b,r)$.
2. Estabelecemos $d' = mdc(b,r)$ então $d' \mid b$ e $d' \mid r$. Assim, $d' \mid bq + r$ e então $d \mid a$. Portanto, temos $d \mid a$ e $d \mid b$, portanto $d' \leq mdc(a,b)$.

□

Teorema 2.9. ***(Algoritmo de Euclides)*** *- Sejam a e b dois inteiros. Temos então cinco casos:*

1. *Se $a = 0$, então $mdc(a,b) =\mid b \mid$.*
2. *Se $b = 0$, então $mdc(a,b) =\mid a \mid$.*
3. *Se $a \mid b$ então $mdc(a,b) =\mid a \mid$.*
4. *Se $b \mid a$ então $mdc(a,b) =\mid b \mid$.*
5. *Se não temos esses quatro casos, devemos realizar sucessivas divisões euclidianas para obter uma série de equações:*

$$a = q_1 b + r_1, \; com \; 0 < r_1 <\mid b \mid,$$

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

$$r_1 = q_3 r_2 b + r_3, \; com \; 0 < r_3 < r_2,$$

$$\dots$$

$$r_{n-2} = q_n r_{n-1} + r_{n-2}, \; com \; 0 < r_n < r_{n-1},$$

$$r_{n-1} = q_{n+1} r_n, \; com \; r_n = 0,$$

então $mdc(a,b) = r_n$ (este é o último resto diferente de zero).

Demonstração. O Teorema 2.9 é justificado pelo Lema 2.8. Temos que:

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = \dots = mdc(r_n, r_{n+1} = r_n,$$

porque $r_{n+1} = 0$. □

Definição 2.10. (Mínimo Múltiplo Comum) - Para um número inteiro positivo k denotamos por M_k o conjunto de todos os múltiplos de k. Oposto ao conjunto D_k definido anteriormente nesta seção, M_k é um conjunto infinito. Para inteiros positivos s e t o elemento mínimo do conjunto $M_s \cap M_t$ é chamado de mínimo múltiplo comum de s e t e é denotado por $mmc(s,t)$ ou simplesmente $[s,t]$.

As seguintes propriedades podem ser derivadas diretamente da definição anterior.

Propriedade 2.11.

- Se $m = mmc(s,t), m = ss' = tt'$, então $mdc(s',t') = 1$.
- Se m' é um múltiplo comum de s e t e $m' = ss' = tt', mdc(s',t') = 1$, então $m' = m$.
- Se m' é um múltiplo comum de s e t, então $m \mid m'$.
- Se $s = p_1^{\alpha_1} \dots . p_k^{\alpha_k}$ e $t = p_1^{\beta_1} \dots p_k^{\beta_k}, \alpha_i, \beta_i \geq 0, \alpha_i + \beta_i \geq 1, i = 1, \dots, k$, então

$$mmc(s,t) = p_1^{max(\alpha_1,\beta_1)} \dots p_k^{max(\alpha_k,\beta_k)}.$$

Proposição 2.12. ***(Relação entre mdc e mmc)*** - *Para quaisquer m, n inteiros vale a seguinte relação:*

$$m.n = mdc(m,n).mmc(m,n).$$

Demonstração. $m = p_1^{\alpha_1} \dots . p_k^{\alpha_k}$ e $n = p_1^{\beta_1} \dots p_k^{\beta_k}, \alpha_i, \beta_i \geq 0, \alpha_i + \beta_i \geq 1, i = 1, \dots, k$, então:

$$mdc(m,n).mmc(m,n) = p_1^{min(\alpha_1,\beta_1)} \dots p_k^{min(\alpha_k,\beta_k)}.p_1^{max(\alpha_1,\beta_1)} \dots p_k^{max(\alpha_k,\beta_k)}.$$

$$= p_1^{min(\alpha_1,\beta_1)+max(\alpha_1,\beta_1)} \dots p_k^{min(\alpha_k,\beta_k)+max(\alpha_k,\beta_k)}.$$

$$= p_1^{\alpha_1+\beta_1} \dots p_k^{\alpha_k+\beta_k} = m.n.$$

□

Lema 2.13. *Sejam a, b inteiros positivos e $t \in \mathbb{Z}$, então $mdc(a,b) = mdc(a, b+at)$ e $mdc(a,b) = mdc(a+bt, b)$.*

Demonstração. Seja $d = mdc(a,b)$ *e* $d' = mdc(a, b+at)$, então:

$$d \mid a \text{ e } d \mid b \Rightarrow d \mid a, d \mid at \text{ e } d \mid b \Rightarrow d \mid a \text{ e } d \mid b + at.$$

Assim d é um divisor comum de a e $b + at$ e como d' é o maior divisor comum temos que $d' \geq d$.

Temos que

$$d' \mid a \text{ e } d' \mid a = bt \Rightarrow d' \mid a, d' \mid at \text{ e } d \mid b + at$$

$$\Rightarrow d' \mid a \text{ e } d' \mid b + at - at \Rightarrow d' \mid a \text{ e } d' \mid b.$$

Assim d' é um divisor comum de a *e* b, e como d é o maior divisor comum, temos que $d \geq d'$. De modo que obtemos $d = d'$, como queríamos.

A outra identidade se demonstra de forma análoga. □

Teorema 2.14. ***(Algoritmo da Divisão de Euclides)*** *- Dados dois inteiros a e b, considere as divisões sucessivas, onde as letras q são quociente e as letras r são restos:*

$$a = q_0 b + r_0$$

$$b = q_1 r_0 + r_1$$

$$r_0 = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\vdots$$

$$r_k = q_{k+1} r_{k+1} + r_{k+2}$$

$$r_{k+1} = q_{k+2} r_{k+2}.$$

Observe que essas divisões sucessivas em algum momento vão acabar, pois pelo algoritmo da divisão temos que $b > r_0 > r_1 > r_2 > \ldots$, e se a sequencia de restos não acabasse, em algum momento teríamos um resto negativo o que é um absurdo. Então $mdc(a, b) = r_{k+2}$ é o último resto não nulo das divisões sucessivas.

Teorema 2.15. ***(Teorema de Bezout)*** *- Dados a e b inteiros positivos, existem inteiros x, y tais que:*

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

Demonstração. Analisando novamente as divisões sucessivas, temos que:

$$r_{k+2} = -q_{k+1} r_{k+1} + r_k.$$

Agora, $r_{k+1} = -q_k r_k + r_{k-1}$, de modo que ao substituirmos r_{k+1} na equação acima:

$$r_{k+2} = -q_{k+1}(-q_k r_k + r_{k-1}) + r_k = (q_{k+1} q_k + 1) r_k - q_{k+1} r_{k-1}.$$

Chamando $x_k = k + 1 q_k + 1$ e $y_k = -q_{k+1}$, temos x_k, y_k inteiros e:

$$r_{k+2} = x_k r_k + y_k r_{k-1}.$$

Agora, $r_k = -q_{k-1} r_{k-1} + r_{k-2}$, de modo que, ao substituirmos r_k na equação acima:

$$r_{k+2} = x_k(-q_{k-1} r_{k-1} + r_k - 2) + y_k r_{k-1} = (-q_{k-1} x_k + y_k) r_{k-1} + x_k r_{k-2}.$$

Chamando $x_{k-1} = -q_{k-1} x_k + y_k$ e $y_{k-1} = x_k$, temos x_{k-1}, y_{k-1} inteiros e:

$$r_{k+2} = x_{k-1} r_{k-1} + y_{k-1} r_{k-2}.$$

Tomando esse processo sucessivamente, obtemos que existem inteiros x_1, y_1, tais que:

$$r_{k+2} = x_1 r_1 + y_1 r_0.$$

Agora sendo $r_1 = b - q_1 r_0$ e $r_0 = a - q_0 b$, temos que ao substituirmos r_1 e em seguida r_0:

$$r_{k+2} = x_1(b - q_1 r_0) + y_1 r_0 = (y_1 - x_1 q_1) r_0 + x_1 b$$

$$= (y_1 - x_1 q_1)(a - q_0 b) + x_1 b$$

$$= a(y_1 - x_1 q_1) + b(-q_0 y1 + x_1 q_0 q_1 + x_1).$$

Chamando $x = y_1 - x_1 q_1$ e $y = -q_0 y_1 + x_1 q_0 q_1 + x_1$, temos que x, y são inteiros e como $r_{k+2} = mdc(a, b)$, segue que $mdc(a, b) = ax + by$, mostrando assim a existência de x, y inteiros. □

Observação 2.16. Observe que com os artifícios dessa demonstração é possível encontrar x, y bastando para isso encontrar x_k, y_k, depois x_{k-1}, y_{k-1} e assim por diante.

Observação 2.17. Observe que todo múltiplo de $mdc(a, b)$ pode ser escrito na forma $ax + by$. Com efeito se $M = kmdc(a, b)$ é um múltiplo, então $M = k(ax + by) = a(kx) + b(ky)$. Além disso todos os números da forma $ax + by$, com $x, y \in \mathbb{Z}$ são múltiplos de $mdc(a, b)$, pois a e b são múltiplos também.

Definição 2.18. (Algoritmo Estendido de Euclides) - Já sabemos como podemos encontrar o mdc de dois números pelo Algoritmo de Euclides. Suponha que $r_n = (a, b), a > b\, e$:

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r_1 = q_3 r_2 + r_3$$
$$r_2 = q_4 r_3 + r_4$$
$$\vdots$$
$$r_{i-1} = q_{i+1} r_i + r_{i+1}$$
$$\vdots$$
$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}$$
$$r_{n-2} = q_n r_{n-1} + r_n$$
$$r_{n-1} = q_{n+1} r_n + 0.$$

Quando queremos escrever mdc de dois inteiros como uma combinação linear desses inteiros, usamos o processo da seguinte maneira. A equação $(a, b) = r_n = r_{n-2} - r_{n-1} q_n$ expressa (a, b) como uma combinação linear de r_{n-2} e r_{n-1}. Se passarmos para a penúltima equação, podemos escrever;

$$r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}.$$

Então, temos :

$$\begin{aligned} r_n &= r_{n-2} - (r_{n-3} - r_{n-2} q - n - 1).q_n \\ &= r_{n-2}(1 + q_{n-1} q_n) - q_n.r_{n-3}. \end{aligned}$$

A última expressão nos mostra que é uma combinação linear de r_{n-2} e r_{n-3}. Continuamos a processar (expressar (a, b) como uma combinação linear de cada par de restos) até encontrar (a, b) como uma combinação linear de a e b. Se escrevermos uma linha particular,

$$(a, b) = k.r_i + m.r_{i-1}.$$

Desde que

$$r_i = r_{i-2} - r_{i-1}.q_{i-1}.$$

Então, temos

$$\begin{aligned} (a, b) &= k(r_{i-2} - r_{i-1}.q_{i-1}) + m.r_{i-1} \\ &= k r_{i-2} + (m - k q_{i-1}).r_{i-1}. \end{aligned}$$

Se continuarmos até a linha superior, podemos encontrar (a, b) como uma combinação linear de a e b. O teorema a seguir fornece o método de indução para encontrar (a, b) como uma combinação linear de a e b.

Teorema 2.19. *Sejam a e b inteiros positivos. Então $(a,b) = k_n.a + m_n.b$ onde k_n e m_n os enésimos termos das sequências definidas recursivamente por*

$$k_0 = 1, m_0 = 0$$

$$k_1 = 0, m_1 = 1.$$

e

$$k_i = k_{i-2} - q_{i-1}.k_{i-1}, m_i = m_{i-2} - q_{i-1}.m_{i-1},$$

para $i = 1, 2, \ldots, n$ onde q_i são os quocientes nas divisões do Algoritmo Euclidiano quando usado para encontrar (a,b).

Demonstração. Vamos demonstrar que

$$r_i = k_i.a + m_i.b \tag{2.2}$$

para $i = 1, 2 \ldots, n$ uma vez que $(a,b) = r_n$, mencionamos a Equação(2.2), sabemos que

$$(a,b) = r_n = k_n.a + m_n.b.$$

Se usarmos a indução matemática na Equação(2.2) Para $i = 0$

$$r_0 = k_0.a + m_0.b$$

$$= 1.a + 0$$

$$= a.$$

Para $i = 1$

$$r_1 = k_1.a + m_1.b$$

$$= 0.a + 1.b$$

$$= b.$$

Podemos ver que a Equação(2.2) é válida para $j = 0, 1$. Agora, assumimos que

$$r_i = k_i.a + m_i.b,$$

para $i = 1, 2, \ldots, p-1$. Então, da p-ésima etapa do algoritmo euclidiano, sabemos que

$$r_p = r_{p-2} - r_{p-1}.q_{p-1}.$$

Se usarmos o método de indução, obtemos

$$r_p = (k_{p-2}.a + m_{p-2}.b) - (k_{p-1}.a + m_{p-1}.b).q_{p-1}$$

$$= (k_{p-2} - k_{p-1}.q_{p-1}).a + (m_{p-2} - m_{p-1}.q_{p-1}).b$$

$$= k_p.a + m_p.b.$$

E, como resultado, podemos escrever o (a,b) como uma combinação linear de a e b. A prova termina. □

Definição 2.20. (Função Parte Inteira) - A função $\lfloor x \rfloor$ representa o maior inteiro não excedendo x. Em outras palavras, para x real, $\lfloor x \rfloor$ é o inteiro único tal que

$$x - 1 < \lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

Agora listamos algumas propriedades de $\lfloor x \rfloor$ que serão usadas posteriormente ao longo dessa dissertação.

1. $\lfloor x + n \rfloor = \lfloor x \rfloor + n$, se n é um inteiro.
2. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$.
3. $\lfloor x \rfloor + \lfloor -x \rfloor$ é 0 se x é um inteiro e -1 caso contrário.
4. O número de inteiros m para os quais $x < m \leq y$ é $\lfloor y \rfloor - \lfloor x \rfloor$.
5. O número de múltiplos de m os quais não excedem x é dado por $\lfloor \frac{x}{m} \rfloor$.

Usando a definição de $\lfloor x \rfloor$, será fácil ver que as propriedades acima são consequências diretas da definição.

Definição 2.21. (Classes de Equivalência) - Fixe $m > 0$. A classe de resíduo de um módulo m (ou classe de congruência, ou classe de equivalência de um módulo m) é $[a] = \{x \mid x \equiv a (mod\ m)\}$, o conjunto de todos os inteiros congruentes a um módulo m.

Note que $[a]$ é um conjunto.

$$[a] = \{mq + a \mid q \in \mathbb{Z}\} = \{\ldots, -2m + a, -m + a, a, m + a, 2m + a, \ldots\}.$$

Teorema 2.22. *Se $m > 0$ então $[a] = [b] \Leftrightarrow a \equiv b (mod\ m)$.*

Demonstração. Primeiro, suponha que $[a] = [b]$. Observe que $a \in [a]$ porque $a \equiv a (mod\ m)$. E, porque $[a] = [b]$, temos $a \in [b]$. Por definição de $[b]$, então $a \equiv b (mod\ m)$.

Para a implicação da outra forma, assuma que $a \equiv b (mod\ m)$, visando provar que os conjuntos $[a]$ e $[b]$ são iguais. Para provar que os conjuntos são iguais, provaremos que cada elemento do primeiro é membro do segundo e vice-versa.

Suponha que $x \in [a]$, de modo que $x \equiv a\,(mod\ m)$. Já que $a \equiv b\,(mod\ m)$, por transitividade de equivalência, $x \equiv b\,(mod\ m)$, e assim $x \in [b]$. O argumento para mostrar que se $x \in [b]$ então $x \in [a]$ é semelhante. □

Teorema 2.23. *Seja $m > 0$. Para todo a existe um único $r \in [0 \ldots m)$ tal que $[a] = [r]$.*

Demonstração. Seja $r \equiv\ a\,(mod\ m)$ so that $0 \leq r < m$, e $a \equiv r\ (mod\ m)$, e pelo Teorema 2.22 , $[a] = [r]$. Para provar a unicidade de r, suponha que $[a] = [r_0]$, onde $0 \leq r_0 < m$. Pelo Teorema 2.22, que implica que $a \equiv r_0\ (mod\ m)$. Isso, juntamente com a restrição $0 \leq r_0 < m$, implica que $r_0\ = a\ mod\ m = r$. □

Teorema 2.24. *Seja $m > 0$, existem exatamente m distintas classes de resíduos módulo m, nomeadamente, $[0], [1], \ldots,$ e $[m - 1]$.*

Demonstração. Pelo Teorema 2.23 nós sabemos que classe de resíduo $[a]$ é igual a uma das distintas classes: $[0]$, *ou* $[1], \ldots,$ *ou* $[m - 1]$. Portanto, todas as classes de resíduos estão nesta lista. Essas classes de resíduos são distintas: se $0 \leq r_1 < m$ e $0 \leq r_2 < m$ e $[r_1] = [r_2]$ então pela parte da unicidade do Teorema 2.23, devemos ter $r_1 = r_2$. □

Definição 2.25. Qualquer elemento $x \in [a]$ é um representante de classe. O elemento de $[a]$ que está em $[0 \ldots m]$ é o principal representante da classe ou resíduo principal.

Definição 2.26. O conjunto $\{[a] \mid a \in \mathbb{Z}\}$ de todas as m classes residuais do módulo m é denotado por $\mathbb{Z}_{>}$.

Definição 2.27. (Sistema Completo de Resíduos) - Um conjunto de m inteiros $\{a_0, a_1, \ldots, a_{m-1}\}$ é um módulo de sistema de resíduos completo m (ou um conjunto completo de representantes para Z_m) se o conjunto Z_m for igual ao conjunto $\{[a_0], [a_1], \ldots, [a_{m-1}]\}$.

Teorema 2.28. *Fixe $m > 0$. Se $m = 2k$ então $\{0, 1, 2, \ldots, k-1, k, -(k-1), \ldots, -2, -1\}$ é um sistema de resíduos completo módulo m. Se $m = 2k + 1$, então*

$$\{0, 1, 2, \ldots, k, -k, \ldots, -2, -1\},$$

é um sistema de resíduos completo módulo m.

Demonstração. Se $m = 2k$, então, como

$$Z_m = \{[0], [1], \ldots, [k], [k+1], \ldots, [k+i], [k+k-1]\},$$

é suficiente notar que

$$[k+i] = [k+i-2k] = [-k+i] = [-(k-i)],$$

no qual

$$[k+1] = [-(k-1)], [k=2] = [-(k-2)], \ldots, [k+k-1] = [-1],$$

conforme desejado.

No caso de $n = 2k + 1$, temos

$$[k+i] = [-(2k+1) + k + i] = [-k+i+1] = [-(k-i+1)],$$

então

$$[k+1] = [-k], [k+2] = [-(k-1)], \ldots, [2k] = [-1],$$

conforme desejado. □

2.2 Relativamente primos entre si - Conceitos e propriedades

Definição 2.29. (Número Primo) - Um inteiro primo é um inteiro $p > 1$ tal que os únicos divisores de p são $-1, -p, 1$ e p.

Observação 2.30. Seja n um inteiro e p um número primo. Se $p \nmid n$, então $mdc(p, n) = 1$.

Proposição 2.31. *Seja n um inteiro tal que $n > 1$ então existe um número primo p tal que $p \mid n$.*

Demonstração. Suponha que haja um inteiro $n > 1$ tal que nenhum número primo p divida n. Colocamos o conjunto:

$$\mathbb{E} = \{a \in \mathbb{Z}, a > 1 \text{ e nenhum número primo divide } a, \}$$

então $n \in \mathbb{E}$, e $\mathbb{E} \neq \varnothing$. Seja $m \in \mathbb{E}$ o menor elemento de $\mathbb{E}$, então $m > 1$e m não é um número primo. Portanto, existe $d \in \mathbb{Z}$ tal que $d \mid n$ e $1 < d < m$. Mas $d < m$ implica que $d \notin \mathbb{E}$, portanto, existe um número primo p tal que $p \mid d$. Agora $p \mid d$ e $d \mid m$, portanto $p \mid m$, o que nos leva a uma contradição. □

Teorema 2.32. ***(Teorema Fundamental da Aritmética)*** *- Qualquer número inteiro $n > 1$ pode ser escrito como um produto de números primos, ou seja, n é escrito:*

$$n = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

com $p_1, p_2, \dots, p_k$ números primos, α_k inteiros maiores que 1 e $k \geq 1$. Esta decomposição é única, exceto pela ordem dos fatores.

Demonstração. Provamos o teorema pelo absurdo. Suponha que exista um inteiro $n > 1$ que não é o produto de números primos. Então

$$\mathbb{E} = \{a \in \mathbb{Z}, a > 1\, e\ a \text{ não é um número primo.}\}$$

$\mathbb{E}$não é um conjunto vazio porque $n \in \mathbb{E}$, então $\mathbb{E}$ tem um elemento menor m. Portanto, há um número primo tal que $p \mid n$ e, portanto, m pode ser escrito $m = pm'$ com $1 < m' < n$. Agora $m' < m$, onde $m' \in \mathbb{E}$ e m' é um produto de números primos, o qual escrevemos:

$$m' = p_1^{\beta_1}.p_2^{\beta_2} \dots p_r^{\beta_r}.$$

Como

$$m = pm' = p.p_1^{\beta_1}.p.p_2^{\beta_2} \dots p.p_r^{\beta_r},$$

é, portanto, um produto de números primos. Agora mostramos a singularidade da decomposição. Suponha que :

$$n = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k} = q_1^{\beta_1}.q_2^{\beta_2} \dots q_r^{\beta_r},$$

com números primos p_i, q_j. Então temos

$$p_i^{\alpha_i} \mid n \Rightarrow p_i^{\alpha_i} \mid q_1^{\beta_1}.q_2^{\beta_2} \dots q_r^{\beta_r},$$

daí a existência de um índice $1 \leq i \leq j$ tal que $p_i = q_j$ e $\beta_j \geq \alpha_i$. Da mesma forma:

$$q_r^{\beta_r} \mid n \Rightarrow q_r^{\beta_r} \mid p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k},$$

portanto, existe um índice $1 \leq i \leq j$ tal que $p_i = q_j$ e $a_i \geq b_j$. A conclusão de tudo isso é que $k = r, \{p_1, \dots, p_k\} = \{q_1, \dots, q_r\}$ e para todo i existe j tal que $a_i = b_j$ demonstra a unicidade na ordem dos fatores. □

Definição 2.33. (Relativamente primos entre si) - Os inteiros a e b são relativamente primos se o $mdc(a, b) = 1$. Para os inteiros $a_1, a_2, \dots, a_n$, dizemos que eles são relativamente primos se $mdc(a_1, a_2, \dots, a_n) = 1$, e que eles são relativamente primos entre si se $mdc(a_i, a_j) = 1$ para todos os $1 \leqslant i, j \leqslant n$ e $i \neq j$.

Teorema 2.34. *(**Algoritmo da Divisão de Euclides**)- Para um número natural arbitrário a e um número inteiro b, existem números inteiros únicos q e r tais que $b = qa + r, 0 \leqslant r < a$.*

Demonstração. Definimos o conjunto $S = \{b - am \geqslant 0 : m \in \mathbb{Z}\}$. Então S é não vazio e limitado inferiormente. Pelo Princípio de Boa Ordenação, S tem o número inteiro mínimo único r. Então, há um único inteiro q tal que $b - qa = r$. Portanto, temos que:

$$b = qa + r.$$

Claramente, $r \geq 0$ e afirmamos que $r < a$. Suponha que $r \geq a$. Então, temos que:

$$b - (q + 1)a = (b - qa) - a = r - a \geq 0.$$

Isso significa que $r - a$ é um elemento de S, mas menor que r. Isto é uma contradição, pois, r é o elemento mínimo em S. □

Teorema 2.35. $mdc(b, c) = min(\{bx + cy, : x, y \in \mathbb{Z}\} \cap \mathbb{N})$.

Demonstração. Considere o conjunto $S = \{ax + by > 0 \mid a, b \in \mathbb{Z}\}$. Seja $d = min\{S\}$. Agora mostramos o seguinte:

- d é um divisor comum de a e b.
- qualquer divisor comum de a e b deve dividir d.

Para mostrar que d divide a e b, suponha por contradição que d não divide a. Então, $a = qd + r$, onde $q \geq 0$ e $0 < r < d$. Dado que:

$$a = qd + r \Rightarrow qd = a - r,$$

e como

$$d = ax + by \Rightarrow q(ax + by) = a - r,$$

então, $r = a(1 - qx) - bqy$. Portanto, r é uma combinação linear de a e b e, como $r > 0$, significa que $r \in S$. Visto que $r < d$ e supondo que $d = min\{S\}$, temos uma contradição. Portanto, d deve dividir a. De modo análogo provamos que d deve dividir b.

Agora devemos mostrar que qualquer divisor comum de a e b deve dividir d. Tomando $a = uc$ e $b = vc$, então $d = ax + by = c(ux + vy)$, então c divide d. Assim, d é o maior divisor comum de a e b, e tem a forma $ax + by$. □

Corolário 2.36. *Se a e b são relativamente primos, podemos encontrar inteiros m e n tais que $ma + nb = 1$.*

Proposição 2.37. *Se $(a, m) = (b, m) = 1$, então $(ab, m) = 1$.*

Demonstração. Pelo Teorema 2.35, existem $x_0, y_0, x_1, y_1 \in \mathbb{Z}$ de modo que $1 = ax_0 + my_0 = bx_1 + my_1$. A partir de que $ax_0bx_1 = (1 - my_0)(1 - my_1) = 1 - my_2$, no qual $y_2 = y_0 + y1 - my_0y_1$. Agora, de $abx_0x_1 + my_2 = 1$, concluímos que $(ab, m) = 1$. □

Proposição 2.38. $(a, b) = (a, b + ax)$.

Demonstração. Suponha que $(a, b) = c$. Então c certamente divide $b + ax$, visto que c divide a e b. Então $(a, b + ax) \geq (a, b)$. Agora suponha que $(a, b + ax) = d$. Então d divide a, o que significa que divide ax, portanto, como deve dividir $b + ax$, também deve dividir b. Assim, como d divide a e b e além disso, $(a, b) \geq (a, b + ax)$ segue que $(a, b) = (a, b + ax)$. □

Dois inteiros são relativamente primos ou coprimos se o seu maior divisor comum for 1. Também podemos dizer que m é primo de n se eles são relativamente primos entre si. Por exemplo 24 e 35 são relativamente primos entre si.

Teorema 2.39. *Dividindo-se cada um dos dois inteiros a e b relativamente primos entre si pelo $mdc(a,b)$ obtemos números relativamente primos.*

Demonstração. Sejam a e b dois inteiros, $d = mdc(a,b)$ e $a_1 = a \mid d$, $b_1 = b \mid d$. Se os inteiros a_1 e b_1 não são relativamente primos, seu mdc d_1 poderia ser maior que 1, e então nós poderíamos obter $a_2 = a_1 \mid d_1$ e $b_2 = b_1 \mid d_1$, com a_2 e b_2 sendo inteiros. Mas, então obtemos as igualdades $a = dd_1a_2$ e $b = dd_1b_2$, implicando que o inteiro dd_1, é o divisor comum dos inteiros a e b, com $dd_1 \leqslant d$, o que é impossível, pois, $d_1 > 1$. Isto mostra que os inteiros a_1 e b_1 precisam ser relativamente primos , o que completa a demonstração do Teorema 2.39. □

Lema 2.40. *Se a é relativamente primo com b e $a \mid bc$ então $a \mid c$.*

Demonstração. Desde que a e b sejam relativamente primos então pelo Corolário 2.36, encontramos inteiros m e n tais que $ma + nb = 1$. Assim temos que $mac + nbc = c$. Agora $a \mid mac$ e $a \mid nbc$. Consequentemente $a \mid (mac + nbc)$ desde que $mac + nbc = c$ e concluímos que $a \mid c$.

Portanto, se a é relativamente primo com b, mas $a \mid bc$ então $a \mid c$. □

2.3 Equações Diofantinas - uma perspectiva

Embora os números tenham fascinado o homem por milênios, os gregos antigos são considerados os pioneiros nos cálculos numéricos tradicionais, apesar de sua abordagem do problema fosse por meio da geometria, eles continuaram se interessando por problemas relacionados a números. Os Pitagóricos estudaram muitas propriedades dos números naturais e o famoso Teorema de Pitágoras, embora o conteúdo geométrico tivesse todo esse apelo teórico de número.

De fato, os babilônios haviam anotado muito antes as tríades pitagóricas $(3,4,5)$; $(5,12,13)$; esses são exemplos de números naturais a,b,c de modo que $a^2 + b^2 = c^2$. Um tablete de argila de cerca de 1500 a.C. inclui a tripla $(4961, 6480, 8161)$, demonstrando que as técnicas sofisticadas e a arte de tais cálculos eram dominados pelos babilônios.

Encontrar soluções de equações no conjunto dos números inteiros é um dos problemas matemáticos mais antigos. Já no início do segundo milênio antes de Cristo os antigos babilônios conseguiram resolver sistemas de equações com duas incógnitas. Este ramo da Matemática floresceu em grande medida na Grécia Antiga. A principal fonte é a *"Arithmetica"* de Diophantus, que contém diferentes tipos de equações e sistemas e onde Diophantus antecipou uma série de métodos para o estudo de equações do segundo e terceiro grau que só foram totalmente desenvolvidas no século XIX [44].

As equações diofantinas foram nomeadas em homenagem ao matemático Diophantus, que estudou várias equações com duas ou mais incógnitas cujas soluções pertencem a um conjunto de números racionais ou inteiros.

Definição 2.41. Seja $n \in \mathbb{N}_{\nvdash}, a_0, a_1; \ldots, a_n \in \mathbb{Z}$ tal que $a_n \neq 0$ e x é variável. A expressão $p(x) = \sum_{i=0}^{n} a_i x^i$ é um polinômio da variável x, grau n com coeficientes inteiros. O conjunto de polinômios com coeficientes inteiros da variável x é denotado por $\mathbb{Z}[x]$.

Definição 2.42. (Equações Diofantinas) - Por equação diofantina de n incógnitas, queremos dizer uma equação polinomial indefinida na forma

$$f(x_1, x_2, x_3, \ldots, x_n) = 0,$$

na qual as variáveis $x_1, x_2, \ldots, x_n$ assumem apenas valores do campo de inteiros. Ao resolver esta equação, chamaremos cada n-upla $[a_1, a_2, \ldots, a_n]$, para a qual $f(a_1, a_2, \ldots, a_n) = 0$.

Definição 2.43. Uma equação polinomial da forma

$$f(x_1, x_2, x_3, \ldots, x_n) = 0,$$

com $n \geq 2$, na qual f é um dado polinômio com coeficientes inteiros nas variáveis $x_1, x_2, \ldots, x_n$ é chamada de equação diofantina.

A criação da Teoria dos Números racionais pelos cientistas da Grécia Antiga levou ao estudo de soluções racionais de equações indefinidas. Este ponto de vista é seguido sistematicamente por Diophantus, embora seu trabalho contenha apenas soluções de equações diofantinas específicas, há razões para acreditar que ele também estava familiarizado com alguns métodos gerais.

2.3.1 Equações Diofantinas Lineares

Definição 2.44. (Equações Diofantinas Lineares)- Equações lineares diofantinas de n incógnitas são equações algébricas na forma:

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

na qual os coeficientes $a_1, a_2, \ldots, a_n \in \mathbb{Z}, b \in \mathbb{Z}$.

As equações diofantinas mais simples são as lineares e possuem a forma:

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{2.3}$$

$a_1, a_2, \ldots, a_n, b$ são números inteiros. Isto significa escrevermos b como sendo uma combinação linear inteira de todos os $a_k (1 \leq k \leq n)$. Assim, encontrar uma solução para a Equação(2.3) significa encontrar um conjunto de valores inteiros $\alpha_1, \alpha_2, \ldots, \alpha_n$ de tal forma que ao substituirmos na respectiva posição da n-upla $(x_1, x_2, \ldots, x_n)$ a Equação (2.3) se torna verdadeira.

Equações lineares diofantinas também são encontradas por pessoas que nunca ouviram o termo. Inconscientemente, eles são resolvidos na vida cotidiana, em jardins de infância ou mesmo na escola primária - são situações de vida comuns transcritas apenas na linguagem da matemática. Normalmente, as pessoas resolvem equações diofantinas lineares por experimentação ou " *tentativa e erro*", veja o Exemplo 5.1.

Para essas equações, temos uma teoria completa, que descreve quando equações dessa natureza têm soluções, bem como métodos para encontrar todas as soluções.

Os teoremas e corolários que se seguem, bem como suas demonstrações podem ser encontrados em [1, 3, 12, 20, 31].

Definição 2.45. Sejam a, b e c três números inteiros. A equação $ax + by = c$ é uma equação diofantina se as soluções procuradas x e y são números inteiros.

Teorema 2.46. ***Resultado da existência de uma solução***
Seja a, b e c inteiros. Temos que a equivalência:

$$ax + by = c$$

admite (pelo menos) uma solução inteira se, e somente se, $mdc(a, b)$ divide c.

Demonstração. É óbvio que $mdc(a, b)$ divide ax e by, então $mdc(a, b)$ divide sua soma que vale c (porque x e y são soluções inteiras da equação $ax + by = c$).

Por outro lado, pelo Teorema de Bezout, existem dois inteiros m e n tais que:

$$am + bn = mdc(a, b).$$

Esses dois números inteiros m e n são encontrados graças ao algoritmo euclidiano estendido.

Por hipótese, existe $k \in \mathbb{Z}$ que:

$$mdc(a, b)k = c \Leftrightarrow k = \frac{c}{mdc(a, b)},$$

então, multiplicando-se a equação acima por k, obtemos:

$$a(mk) + b(nk) = mdc(a, b) = c.$$

Por esse motivo, o par $(x; y) = (mk; nk)$ é uma solução de $ax + by = c$. □

Observação 2.47. Antes de resolver uma equação diofantina, sempre verificamos se ela admite solução usando este resultado da existência. De fato, se a equação não admitir uma solução, então o problema está resolvido. Encontrada uma solução é possível mostrar que ela não é única, utilizando-a para deduzir todas as outras, conforme veremos a seguir.

2.3.2 Procurar uma solução específica para equação diofantina

No caso em que a existência de uma solução é verificada, pode-se começar a procurar as soluções da equação diofantina.

O método de encontrar uma solução específica é encontrado na prova construtiva do resultado da existência de uma solução para a equação diofantina.

1. Graças ao algoritmo euclidiano estendido, encontramos uma solução particular $(m; n)$ para a equação $ax + by = mdc(a, b)$.

2. Para encontrar uma solução específica (x_0, y_0) da equação $ax+by = c$, multiplicamos x e y por $\frac{c}{mdc(a, b)}$. Assim, temos que :

$$(x_0, y_0) = \left(x.\frac{c}{mdc(a, b)}; y.\frac{c}{mdc(a, b)} \right).$$

Teorema 2.48. *(**Teorema para resolver uma equação diofantina**) - Seja a equação diofantina (ED): $ax+by = c$ e $(x_0; y_0)$ uma solução específica. Seja também a equação homogênea associada (EH): $ax + by = 0$. Temos que :*

- *Se $(x_h; y_h)$ é uma solução de(EH), então $(x_h + x_0; y_h + y_0)$ é uma solução de (ED).*

- *Se $(x; y)$ é uma solução de (ED), então $(x - x_0; y - y_0)$ é uma solução de (EH).*

Em outras palavras, através da solução específica $(x_0; y_0)$, para cada solução de (ED) corresponde uma única solução de (EH) e vice-versa.

Demonstração. Supomos que conhecemos uma solução específica (x_0, y_0) da equação (ED). Devemos mostrar:

- Se $(x_h; y_h)$ é uma solução de (EH), então $(x; y) = (x_h + x_0; y_h + y_0)$ é uma solução de (ED). Basta verificar (ED) para $(x; y)$.

$$ax + by = a.(x_h + x_0) + b.(y_h + y_0) = ax_h + by_h + ax_0 + by_0 = c.$$

  Assim, (x, y) é de fato uma solução da equação diofantina (ED).

- Se $(x; y)$ é uma solução de (ED), então $(x_h; y_h) = (x - x_0; y - y_0)$ é uma solução de (EH).

  Basta verificar (EH) para $(x_h; y_h)$.

$$ax_h + by_h = a(x - x_0) + b.(y - y_0) = ax + by - (ax_0 + by_0) = 0.$$

  Assim, $(x_h; y_h)$ é uma solução da equação homogênea (EH).

□

Teorema 2.49. *(**Solução geral da equação diofantina**) - Quando o $mdc(a, b)$ divide c e se exite uma solução particular (x_0, y_0) existem infinitas soluções, todas tendo a forma:*

$$\begin{cases} x = x_0 - \dfrac{b}{mdc(a,b)}.k \\ y = y_0 + \dfrac{a}{mdc(a,b)}.k \quad , k \in \mathbb{Z} \end{cases},$$

na qual cada solução possui um k único (o mesmo para as duas equações) e para cada número inteiro k temos uma solução única, cuja unicidade depende de (x_0, y_0).

Demonstração. Seja $d = mdc(a, b)$. Por hipótese d divide c, então o Teorema 2.48 garante a existência de uma solução particular $x = x_0$ *e* $y = y_0$ para o sistema. Assim,

$$ax_0 + by_0 = c.$$

Agora, dividindo ambos os lados desta equação pelo maior divisor comum de a e b, teremos,

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d}.$$

Sendo $\dfrac{c}{d}$ um número inteiro e $\dfrac{a}{d}, \dfrac{b}{d}$ números inteiros primos entre si, logo o maior divisor comum entre eles é igual a 1 e como 1 divide a $\dfrac{c}{d}$, o Teorema 2.48 garante a existência de uma solução particular x_1, y_1 para esta equação, então temos que :

$$\frac{a}{d}x_1 + \frac{b}{d}y_1 = \frac{c}{d}.$$

Assim temos que :

$$\left.\begin{array}{l} \frac{a}{d}x_1 + \frac{b}{d}y_1 = \frac{c}{d} \\ \frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d} \end{array}\right\} \Rightarrow \frac{a}{d}(x_1 - x_0) + \frac{b}{d}(y_1 - y_0) = 0,$$

portanto

$$\frac{a}{d}(x_1 - x_0) = \frac{b}{d}(y_0 - y_1),$$

se, e somente se, $\frac{b}{d} \mid \frac{a}{d}(x_1 - x_0)$.

E sendo $\frac{b}{d}$ primo com $\frac{a}{d}$, dividirá a $(x_1 - x_0)$, logo temos que

$$\frac{b}{d} \Leftrightarrow \exists k \in \mathbb{Z} : x_1 - x_0 = k\frac{b}{d} \Rightarrow x_1 = x_0 + k\frac{b}{d}.$$

Substituindo-se o valor de $x_1 - x_0$ em $\frac{a}{d}(x_1 - x_0) + \frac{b}{d}(y_1 - y_0) = 0$ temos que

$$\frac{a}{d}k\frac{b}{d} + \frac{b}{d}(y_1 - y_0) = 0 \Rightarrow \frac{a}{d}k + (y_1 - y_0) = 0 \Rightarrow y_1 = y_0 - k\frac{a}{d}.$$

Vamos ver, finalmente, que x_1 *e* y_1 é uma solução da equação $ax + by = c$, pois, temos que:

$$\begin{aligned} ax_1 + by_1 &= a\left(x_0 + k\frac{b}{d}\right) + b\left(y_0 - k\frac{a}{d}\right) \\ &= ax_0 + ak\frac{b}{d} + by_0 - bk\frac{a}{d} \\ &= ax_0 + by_0 = c. \end{aligned}$$

Logo, temos que :

$$\left\{\begin{array}{l} x = x_0 - \dfrac{b}{mdc(a,b)}.k \\ y = y_0 + \dfrac{a}{mdc(a,b)}.k \end{array}\right. , k \in \mathbb{Z}$$

é a solução da equação $ax + by = c$ qualquer que seja $k \in \mathbb{Z}$. Vamos chamá-la de Solução Geral desta equação.

Para identificarmos que não existe outra forma suponha agora que (x, y) seja uma solução da equação. A subtração das relações $ax + by = c$ e $ax_0 + by_0 = c$ produz $a(x - x_0) = b(y_0 - y)$. Escrevendo $a = du$ e $b = dv$, onde $d = mdc(a, b)$ e $mdc(u, v) = 1$, obtemos $u(x - x_0) = v(y_0 - y)$. Uma vez que $u \mid v(y_0 - y)$ e $mdc(u, v) = 1$, pelo Lema de Gauss, podemos encontrar um número inteiro t tal que $y_0 - y = ut$. Então $x - x_0 = vt$, portanto, $a = x_0 + vt$ e $y = y_0 - ut$. A prova está, portanto, terminada. □

Observação 2.50.

- Desde que $mdc\left(\frac{a}{mdc(a,b)}; \frac{b}{mdc(a,b)}\right) = 1$, o máximo divisor comum das soluções da equação homogênea é o valor absoluto de k. Portanto, se tivermos soluções cujo mdc é igual a 1, essas soluções serão:

$$x = -\frac{b}{mdc(a,b)} \text{ e } y = \frac{a}{mdc(a,b)}, \text{ ou } x = \frac{b}{mdc(a,b)} \text{ e } y = -\frac{a}{mdc(a,b)}.$$

Tabela 2.1: Algoritmo Euclidiano Estendido

	a	b	
a	1	0	quociente
b	0	1	q_1
...	...	...	...
($\star$) mdc(a,b)	m	n	q_n
($\star\star$) 0	$\pm\frac{b}{mdc(a,b)}$	$\pm\frac{b}{mdc(a,b)}$	

- As duas últimas linhas do Algoritmo Euclidiano Estendido são muito importantes:
  Na linha ($\star$), encontramos uma solução $(m; n)$ da equação $ax + by = mdc(a, b)$.
  Assim $(x_0; y_0) = \left(m.\frac{c}{mdc(a,b)}; n.\frac{c}{mdc(a,b)}\right)$ é uma solução particular da equação diofantina $ax + by = c$.
  Na linha ($\star\star$), encontramos os coeficientes de k da solução geral da equação homogênea $ax + by = 0$. Para demonstrar que esse é o caso, basta combinar a observação anterior com a consequência de que a e b são primos entre si.

Corolário 2.51. *Sejam a, b, c, inteiros e $d = (a, b)$. Se $d \nmid c$, então equação*

$$ax + by = c \tag{2.4}$$

não tem solução inteira. Se $d \mid c$, então (2.4) tem infinitas soluções inteiras. Se (x_1, y_1) é uma solução, então todas as soluções são dadas com :

$$x = x_1 + \frac{b}{d}.k, y = y_1 - \frac{a}{d}.k,$$

no qual $k \in \mathbb{Z}$.

Teorema 2.52. *Sejam $a_1, a_2, \ldots, a_n$ os números inteiros não nulos. Em seguida equação diofântica linear*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \tag{2.5}$$

existem soluções se, e somente se, $(a_1, a_2, ..., a_n) \mid c$. Além disso, se (2.5) tem pelo menos uma solução, então há um número infinito de soluções.

Demonstração. A existência de uma solução de (2.5) obviamente retrata que $(a_1, a_2, ..., a_n) \mid c$. Vamos provar por indução matemática que se $(a_1, a_2, ..., a_n) \mid c$, então (2.5) possui infinitas soluções.

Para $n = 2$ é válido pelo Teorema 2.51, então suponha que seja válido para equações com $n - 1$ variáveis. Tomemos $d = (a_{n-1}, a_n)$.

Por hipótese de indução, a equação $a_1x_1 + \cdots + a_{n-2}x_{n-2} + dy = c$ apresenta infinitas soluções $(x_1, ..., x_{n-2}, y)$. Para cada solução dessa equação, vamos ver a equação

$$a_{n-1}x_{n-1} + a_nx_n = dy.$$

Pelo fato de que $(a_{n-1}, a_n) \mid dy$ segue que esta equação tem infinitas alternativas (x_{n-1}, x_n). Desta forma, obtemos infinitas soluções $(x_1, \ldots, x_n)$ para (2.5). □

3 Funções Aritméticas

O conceito de função é um dos mais difundidos em toda a matemática. Portanto, não é surpreendente que as funções desempenhem um papel fundamental na Teoria dos Números. A teoria analítica dos números é um dos ramos da Teoria dos Números que envolve o estudo de funções aritméticas, suas propriedades e as inter-relações existentes entre essas funções. Neste capítulo consideramos algumas funções aritméticas como a soma e o número de divisores de um número inteiro positivo e a função totiente de Euler. Abordamos suas propriedades básicas, e explicamos como calcular seu valor para qualquer número inteiro positivo, ilustrando com exemplos adequados. Além disso, declaramos e provamos o teorema de Euler, que é parte constituinte da função de Euler, tendo inúmeras aplicações em diversas áreas da Teoria dos Números e criptografia.

Uma propriedade chamada multiplicatividade nos permitirá obter fórmulas compactas para a avaliação das algumas das funções mais importantes da teoria dos números. Além disso, a consideração de uma determinada função resultará em uma classe de números conhecida como números perfeitos que fundamentalmente geram vários dos problemas não resolvidos mais intrigantes da Teoria dos Números hoje.

3.1 Função Aritmética - Conceito

As definições dessas funções aritméticas e alguns lemas que refletem suas propriedades foram utilizadas nessa dissertação a fim de se provar algumas proposições aqui abordadas.

Definição 3.1. Chama-se **função aritmética** toda função f definida no conjunto $\mathbb{Z}_+$ dos inteiros positivos e com valores no conjunto $\mathbb{C}$ dos números complexos , isto é, $f : Z_+ \to C$.

Antes de abordarmos algumas funções aritméticas propriamente ditas necessitamos retomar conceitos e propriedades de números que sejam relativamente primos entre si, baseado nas anotações de [3, 22, 31, 40].

3.2 Funções Multiplicativas

Existem diferentes tipos de funções associadas à Teoria dos Números. Uma maneira usual de classificá-las parece ser chamá-las de "multiplicativas", "aditivas" dentre outras. A classe de funções multiplicativas é bem definida por uma propriedade matemática precisa.

Definição 3.2. A função aritmética f é multiplicativa se for diferente da função nula e se for para todos os pares de números relativamente primos m e n vale a propriedade:

$$f(mn) = f(m)f(n). \tag{3.1}$$

Uma função f não nula, é completamente multiplicativa se a propriedade (3.1) puder ser estendida para qualquer dois números inteiros positivos m e n.

Observação 3.3. Se f é multiplicativa ou completamente multiplicativa vale que $f(1) = 1$.

Seja $m \in \mathbb{N}$ tal que $f(m) \neq 0$. Então, como o $mdc(m, n) = 1$ temos que:

$$f(m) = f(m.1) = f(m).f(1).$$

Assim, $f(m)\,[1 - f(1)] = 0$ e como $f(m) \neq 0$ temos que $f(1) = 1$.

De acordo com o Teorema Fundamental da Aritmética, qualquer número natural pode ser escrito na forma:

$$n = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

no qual $p_1, p_2, \dots, p_r$ são diferentes números primos e α expoentes de números naturais. Os números $p_i^{\alpha_i}$ e $p_j^{\alpha_j}$ são relativamente primos para $i \neq j$. Portanto, o valor da função multiplicativa no número n pode ser escrito na forma:

$$f(n) = f(p_1^{\alpha_1})f(p_2^{\alpha_2}) \dots f(p_r^{\alpha_r}).$$

Teorema 3.4. ***(Caracterização da Função Multiplicativa)*** *A função aritmética f é multiplicativa se, e somente se, $f(1) = 1$ e para $n \geqslant 2$. temos que :*

$$f(n) = \prod_{p^m | n} f(p^m). \tag{3.2}$$

Observação 3.5. O resultado mostra que uma função multiplicativa é determinada exclusivamente por seus valores em potências primas,

Demonstração. Suponha primeiro que f satisfaça $f(1) = 1$ e (3.2) para $n \geqslant 2$. Sejam n_1 e n_2 números relativamente primos $n_1, n_2 \geqslant 2$. Então, nenhum fator primo de n_1 é um fator primo de n_2 e vice-versa. Assim, temos que:

$$n_1 = p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_r^{\alpha_r} \text{ e } n_2 = q_1^{\beta_1}.q_2^{\beta_2} \dots q_s^{\beta_s}$$

onde $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ são diferentes números primos, $\alpha_1, \alpha_2, \dots, \alpha_r, \beta_1, \beta_2, \dots, \beta_s$ são números naturais. Então, de acordo com (3.2),se mantém que :

$$f(n_1) = f(p_1^{\alpha_1})f(p_2^{\alpha_2}) \dots f(p_r^{\alpha_r}).$$

$$f(n_2) = f(q_1^{\beta_1})f(q_2^{\beta_2}) \dots f(q_s^{\beta_s}).$$

$$f(n_1 n_2) = f(p_1^{\alpha_1})f(p_2^{\alpha_2}) \dots f(p_r^{\alpha_r}).f(q_1^{\beta_1})f(q_2^{\beta_2}) \dots f(q_s^{\beta_s}).$$

Obviamente, $f(n_1 n_2) = f(n_1).f(n_2)$. Se, sem perda da generalidade,$n_2 = 1$ e $n_1 \geqslant 2$, então para um par de números relativamente primos n_1, n_2, temos que:

$$f(n_1.n_2) = f(n_1.1) = f(n_1) = f(n_1).1 = f(n_1).f(n_2).$$

Assim, em qualquer caso, obtemos que a propriedade definidora da função multiplicativa é válida, ou seja, temos que f é multiplicativa. Assumindo que f é multiplicativa, então f é não nula, portanto, existe $n \in \mathbb{N}$ tal que $f(n) \neq 0$. Aplicando-se (3.1), o par $(n_1, n_2) = (n, 1)$, obtemos $f(n) = f(1.n) = f(1)f(n)$, daí dividindo por $f(n)$ segue-se que $f(1) = 1$.

Além disso, para $n \geqslant 2$, temos $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Os números $p_1^{\alpha_1}, \ldots, p_{k-1}^{\alpha_{k-1}}$ e $p_k^{\alpha_k}$ são relativamente primos, portanto, usando a propriedade de (3.1), temos que :

$$f(n) = f(p_1^{\alpha_1} \ldots p_{k-1}^{\alpha_{k-1}} p_k^{\alpha_k}) = f(p_1^{\alpha_1} \ldots p_{k-1}^{\alpha_{k-1}}) f(p_k^{\alpha_k}).$$

Os números $p_1^{\alpha_1} \ldots p_{k-2}^{\alpha_{k-2}}$ e $p_{k-1}^{\alpha_{k-1}}$ são relativamente primos, portanto a expressão acima é igual a:

$$f(n) = f(p_1^{\alpha_1} \ldots p_{k-2}^{\alpha_{k-2}}) f(p_{k-1}^{\alpha_{k-1}}) f(p_k^{\alpha_k}).$$

Continuando, temos que:

$$f(n) = f(p_1^{\alpha_1}) \ldots f(p_k^{\alpha_k})$$

que é exatamente a propriedade de (3.2). □

Corolário 3.6. *A função é completamente multiplicativa se, e somente se, as condições do Teorema 3.4 se aplicarem e se $f(p^m) = f(p)^m$ para todos os números primos p e m naturais.*

Demonstração. Se f é completamente multiplicativa, então, para qualquer número primo p temos o seguinte:

$$f(p^m) = f(p^{m-1}.p) = f(p^{m-1}).f(p) = \cdots = f(p)^m.$$

Por outro lado, se f é multiplicativa e satisfaz $f(p^m) = f(p)^m$ para todos os números primos da forma p^m, então (3.1) pode ser escrita como $f(n) = \prod_{i=1}^{r} f(p_i)$, na qual $n = \prod_{i=1}^{r} p_i$ é uma fatoração de n em fatores primos (não necessariamente distintos). Sejam n_1 e n_2 números naturais cujas fatorações para fatores primos são as seguintes:

$$n_1 = p_1 p_2 \ldots p_r,$$

$$n_2 = q_1 q_2 \ldots q_s,$$

então $f(n_1 n_2) = f(p_1) f(p_2) \ldots f(p_r) f(q_1) f(q_2) \ldots f(q_s) = f(n_1) f(n_2)$. Portanto, f é completamente multiplicativa. □

Teorema 3.7. - *(**Produtos e Quocientes de Funções Multiplicativas**) - Suponha que f e g sejam funções multiplicativas. Segue que:*

- *o produto fg é multiplicativo;*
- *se g não for nula, o quociente de $\dfrac{f}{g}$ é multiplicativo.*

Demonstração. O resultado segue diretamente da definição de multiplicidade. O produto fg de duas funções aritméticas f e g é definido como $(fg)(n) = f(n)g(n)$. Vamos provar a primeira afirmação. Seja m e n números relativamente primos. Da multiplicidade das funções f e g segue que:

$$f(mn) = f(m)f(n),$$
$$g(mn) = g(m)g(n),$$

então temos que

$$(fg)(mn) = f(mn)g(mn) = f(m)f(n)g(m)g(n) = (fg)(m).(fg)(n),$$

isto é, fg é uma função multiplicativa. De forma análoga se demonstra a segunda afirmação. □

Teorema 3.8. *Sejam f uma função multiplicativa e*

$$F(n) = \sum_{d|n} f(d).$$

Então F é multiplicativa.

Demonstração. Suponha que $m = m_1 m_2$ e $(m_1, m_2) = 1$. Se $d \mid m$, tomando $d_1 = (d, m_1)$ e $d_2 = (d, m_2)$ temos que $d = d_1 d_2, d_1 \mid m_1$ e $d_2 \mid m_2$. Por outro lado, se d_1, d_2 são divisores de m_1 e m_2, então $d = d_1 d_2$ é um divisor de m e $d_1 = (d, m_1), d_2 = (d, m_2)$. Então fizemos a conexão entre o divisor d de m e d_1, d_2 como divisor de m_1 e m_2. Então vale que:

$$F(m) = \sum_{d|m} f(d) = \sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1 d_2).$$

Além disso, o fato de que (m_1, m_2) implica em $(d_1, d_2) = 1$, logo, partindo da suposição de que f é multiplicativa temos que:

$$\sum_{d_1|m_1} \sum_{d_2|m_2} f(d_1 d_2) = \left(\sum_{d_1|m_1} f(d_1) \right) \left(\sum_{d_2|m_2} f(d_2) \right) = F(m_1) F(m_2).$$

□

3.3 Função Totiente de Euler - ϕ

Leonhard Euler (1707-1783) trabalhou em muitos campos de matemática pura e aplicada, tais como a Álgebra, Cálculo das Diferenças Finitas, Cálculo Diferencial e Integral, Cálculo das Variações, Astronomia, Mecânica Analítica, além da Teoria dos Números. No último campo ele descobriu a lei de Reciprocidade Quadrática, forneceu a prova e a generalização do Teorema de Fermat, mostrando que todo primo da forma $4n+1$ pode ser expresso como uma soma de dois quadrados em exatamente de modo único, como também fez muitas descobertas, uma das quais é a função ϕ e suas propriedades, investigada por Euler por volta de 1760. A notação $\phi(n)$, no entanto, é devida a Gauss (foi introduzida por ele em 1801) - esta é a razão pela qual alguns autores a chamam de função de Gauss $\phi(n)$.

Definição 3.9. A função ϕ de Euler é uma função aritmética que associa a cada número natural n o número de inteiros não negativos menores que n que são relativamente primos com n.

Exemplo 3.10. Vamos calcular $\phi(n)$ para $n = 12$ e $n = 11$.

Solução: números menores que 12 que são relativamente primos com 12 são $1, 5, 7\, e\, 11$, então $\phi(12) = 4$.

O número 11 é um número primo e todos os números menores que ele são relativamente primos. Assim, $\phi(11) = 10$. Esta conclusão para $n = 11$ pode ser generalizada para qualquer número primo.

Se n é um número primo, então $\phi(n) = n - 1$. Vemos imediatamente que o inverso também é válido, ou seja, se $\phi(n) = n - 1$, então o número n deve ser primo.

Lema 3.11. *Se $ax \equiv ay \pmod{n}$ e $(a, n) = 1$, então $x \equiv y \pmod{n}$.*

Demonstração. $ax \equiv ay \ (mod\, n)$ desde que que n divide $ax - ay$. Como a e n são relativamente primos, n deve dividir $x - y$ e, portanto, a afirmação é provada. □

Lema 3.12. *Se A é um sistema completo de resíduos módulo n, e m e c são inteiros tais que $(m, n) = 1$, então o conjunto $Am + c = \{am + c : a \in A\}$ é um sistema completo de resíduos.*

Demonstração. Seja $am + c \equiv a'm + c \ (mod\, n)$, na qual $a, a' \in A$. Subtraindo o número c e dividindo por m de acordo com o Lema 3.11, segue que $a \equiv a' \ (mod\, n)$ então $a = a'$. Portanto, todos os n elementos $am + c$ estão em classes de equivalência diferentes e juntos formam um sistema completo de resíduos do módulo n. □

Teorema 3.13. *A função ϕ de Euler é multiplicativa.*

Demonstração. Sejam m e n relativamente primos. Sejam m, n números naturais tais que $(m, n) = 1$. Para $m = n = 1$ temos $\phi(1) = 1$. Se $m = 1\, e\, n > 1$, a afirmação é válida porque $\phi(1.m) = \phi(m) = 1.\phi(m) = \phi(1).\phi(m)$. Da mesma forma, verifique se temos $n = 1$, portanto, resta verificar o caso $m, n > 1$. Podemos classificar todos os números que não excedam mn na tabela retangular com m linhas e n colunas, como segue:

Tabela 3.1: Função de Euler

1	m+1	2m+1	...	(n-1)m+1
2	m+2	2m +2	...	(n-1)m+2
3	m+3	2m +3	...	(n-1)m+3
⋮	⋮	⋮	⋮	⋮
r	m+r	2m +r	...	(n-1)m+r
⋮	⋮	⋮	⋮	⋮
m	2m	3m	...	nm

Os i números da tabela formam um sistema completo de remanescentes módulo mn, então há $\phi(mn)$ números que são relativamente primos com mn, respectivamente $(i, m) = (i, n) = 1$. Todos os números em uma determinada coluna são mutuamente congruentes módulo m, ou seja, na mesma coluna temos números que, quando divididos por m, retornam o mesmo resto, e todas as m colunas correspondem a m classes de equivalência módulo m. Assim, os números na mesma coluna são todos relativamente primos com m ou nenhum é relativamente primo com m. Portanto, exatamente $\phi(m)$ colunas consistem em m números relativamente primos, enquanto as outras colunas contêm i números tais que $(i, m) > 1$. Tomemos agora uma dessas colunas $\phi(m)$. Que seja a r-ésima coluna. Esta coluna é composta pelos números $k, m + r, 2m + r, \ldots, (n - 1)m + r$. De acordo com o Lema 3.12, os números desta coluna formam o sistema completo de resíduos módulo n, uma vez que cada um desses números dá um resto diferente ao dividir n e $(m, n) = 1$. Ou seja, se dois números $mx_1 + r, mx_2 + r, x_1, x_2 \in \{0, 1, \ldots, n - 1\}, (x_1 \neq x_2)$ deu o mesmo resto quando dividido por n, teríamos que:

$$mx_1 + r \equiv mx_2 + r \ (mod\, n),$$

isto é, $mx_1 \equiv mx_2 \ (mod\, n)$. Uma vez que $(m, n) = 1$, seguir-se-ia que

$$x_1 \equiv x_2 \ (mod\, n),$$

o que é impossível, pois, a diferença de dois números diferentes do conjunto $\{0, 1, \ldots, n-1\}$ não pode ser divisível por n. Portanto, cada uma das colunas na tabela contém $\phi(n)$ números relativamente primos a n, de modo que essas $\phi(m)$ colunas fornecem $\phi(m)\phi(n)$ números e relativamente primos a m e a n. Portanto, $\phi(mn) = \phi(m)\phi(n)$ e a afirmação está provada.

Os números na r-ésima linha desta tabela são da forma $km + r$, pois k vai de 0 a $m-1$. Tomando $d = (r, m)$. Se $d > 1$, então nenhum número na r-ésima linha da tabela é relativamente primo a mn, uma vez que $d \mid (km+r)$ para todo k. Portanto, para contar os resíduos relativamente primos com mn, precisamos apenas olhar para as linhas indexadas por valores de r tais que $(r, m) = 1$, e existem $\phi(m)$ tais linhas. Se $(r, m) = 1$, então cada entrada na r-ésima linha é relativamente primo com m, já que $(km + r; m) = 1$ pelo algoritmo euclidiano. Segue que as entradas em tal linha formam um sistema de resíduos completo módulo n. Assim, exatamente $\phi(n)$ deles será relativamente primo com n e, portanto, relativamente primo com mn.

Mostramos que há $\phi(m)$ linhas na tabela que contêm números relativamente primos a mn, e cada uma delas contém exatamente $\phi(n)$ tais números. Portanto, há, no total, $m.n$ números na tabela que são relativamente primos a mn. Assim, temos que $\phi(mn) = \phi(m)\phi(n)$ e isso prova o teorema. □

Teorema 3.14. *Se p é um número primo e k é natural, então temos que :*

$$\phi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right).$$

Demonstração. Se um número menor que p^k não for relativamente primo com p^k, será um múltiplo de p porque é o único fator primo do número p^k. Todos esses múltiplos têm a forma mp, com $1 \leqslant m \leqslant p^{k-1}$ e tendo exatamente p^{k-1} múltiplos. Isso significa que números menores que p^k que são relativamente primos com p^k retorna

$$\phi(n) = p^k - p^{k-1}$$

e, portanto, o teorema está demonstrado. □

Teorema 3.15. *Para qualquer número natural n é verdadeiro*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_s}\right) = n.\prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right),$$

na qual $p_1, p_2, \ldots, p_s$ são todos os seus vários fatores primos.

Demonstração. Se n é o número natural da forma $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, então temos que:

$$\begin{aligned}
\phi(n) &= \phi\left(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}\right) \\
&= \phi(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \ldots f(p_s^{\alpha_s}) \\
&= \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}\right)\ldots\left(p_s^{\alpha_s} - p_s^{\alpha_s - 1}\right) \\
&= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\ldots p_s^{\alpha_s}\left(1 - \frac{1}{p_s}\right) \\
&= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_s}\right)
\end{aligned}$$

$$= n.\prod_{i=1}^{s}\left(1-\frac{1}{p_i}\right).$$

□

Teorema 3.16. *A função Totiente de Euler ϕ satisfaz:*

$$\sum_{d|n}\phi(d) = n, \forall n \in \mathbb{N}$$

Demonstração. Seja $n = p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_k^{\alpha_k}$. Devido a multiplicidade da função ϕ temos que:

$$\sum_{d|n}\phi(d) = \prod_{i=1}^{k}(1+\phi(p_i)+\phi(p_i^2)+\cdots+\phi(p_i^{\alpha_i})). \tag{3.3}$$

Multiplicando-se os fatores à direita de (3.3) obtemos a soma dos fatores na forma

$$\phi(p_1^{\beta_1}).\phi(p_2^{\beta_2})\dots\phi(p_k^{\beta_k}) = \phi(p_1^{\beta_1}.p_2^{\beta_2}\dots p_k^{\beta_k}),$$

na qual $0 \leq \beta_i \leq \alpha_i, i = 1, 2, \dots, k$, e este é exatamente o lado esquerdo de (3.3). Agora temos que:

$$\sum_{d|n}\phi(d) = \prod_{i=1}^{k}(1+(p_i-1)+(p_i^2-p_i)+\cdots+(p_i^{\alpha_i}-p_i^{\alpha_i-1})) = \prod_{i=1}^{k}p_i^{\alpha_i} = n,$$

e assim obtemos o desejado. □

Teorema 3.17. ***(Teorema de Euler)*** *- Quando temos $(a, n) = 1$ então*

$$a^{\phi(n)} \equiv 1 \ (mod\ n).$$

Demonstração. Seja $r = \phi(n)$. Denotando por $k_1, \dots, k_r$ números menores que n e relativamente primos com n. Como a e n são relativamente primos, os números $ak_1, ..., ak_r$ são relativamente primos com n. Ao mesmo tempo, seus resíduos ao dividir por n são diferentes um do outro. Especificamente, supondo que ak_i e ak_j para $k_i \neq k_j$ forneçam o mesmo resto ao dividir por n, seguiria que $a(k_i - k_j)$ é divisível por n, o que não é possível, pois a é relativamente primo enquanto $k_i - k_j$ é menor que n. É por isso que temos que :

$$ak_i \equiv a_i \ (mod\ n)$$

para cada $i = 1, \dots, r$, onde $a_1, a_2, \dots, a_r$ são os mesmos números que $k_1, k_2, \dots, k_r$, mas não necessariamente na mesma ordem. Ao multiplicarmos essas congruências, obtemos que $a^r \equiv 1 \ (mod\ n)$. □

Corolário 3.18. ***(Pequeno Teorema de Fermat)*** *- Seja p um número primo e a um natural. Se p não dividir a, então $a^{p-1} \equiv 1 \ (mod\ p)$.*

Demonstração. Se p não divide a, então $(a, p) = 1$ e $a^{\phi(p)} \equiv 1 \ (mod \ p)$. Pois, ao listarmos os primeiros $p-1$ múltiplos positivos de a temos que

$$a, 2a, 3a, ...(p-1)a.$$

Supondo que $ra \equiv sa \, (mod \, p)$, então temos $r \equiv s(mod \, p)$, então os $p-1$ múltiplos de a são distintos e diferentes de zero; ou seja, eles devem ser congruentes a $1, 2, 3, \ldots, p-1$ em alguma ordem. Multiplicando-se todas essas congruências, encontramos que

$$a(2a)(3a)\ldots((p-1)a) \equiv 1.2.3\ldots(p-1)(mod \, p),$$

onde

$$a(p-1)(p-1)! \equiv (p-1)!(mod \, p).$$

Dividindo-se os dois lado por $(p-1)!$ (isso é possível porque, uma vez que $p \nmid (p-l)!$), nossa linha de raciocínio culmina na afirmação de que $a^{p-l} \equiv 1(mod \, p)$, que é o Teorema de Fermat. Ao calcularmos $\phi(p)$, temos que todos os números $1, 2, \ldots, p-1, p$, exceto p, são relativamente primos com p. Assim, temos $\phi(p) = p-1$, o que prova o Pequeno Teorema de Fermat. □

Teorema 3.19. *Para $n > 2$, $\phi(n)$ é um número inteiro par.*

Demonstração. Considere dois casos em que n é uma potência de 2 e quando n não é uma potência de 2.

1. Tomando n como uma potência de 2,ou seja, $n = 2^k, k \geqslant 2$.

   Consequentemente, temos que:

   $$\phi(n) = \phi(2^k) = 2^k\left(1 - \frac{1}{2}\right) = 2^{k-1},$$

   portanto $\phi(n)$ é par.

2. Quando n não é uma potência de 2. Então é divisível por um número primo ímpar p, então $n = p^k.m$ onde $k \geqslant 1$ e $mdc(p^k, m) = 1$.

   Pela natureza multiplicativa da função ϕ, temos que:

   $$\phi(n) = \phi(p^k m) = \phi(p^k)\phi(m) = p^{k-1}(p-1)\phi(m).$$

   Consequentemente $\phi(n)$ é par, porque $(p-1)$ é divisível por 2.

□

3.4 Função Soma dos Divisores σ

Definição 3.20. A soma dos divisores é uma função aritmética σ que está associada à soma de todos os divisores do número n. Em outras palavras temos que :

$$\sigma(n) = \sum_{d|n} d.$$

Exemplo 3.21. Vamos calcular $\sigma(n)$ para $n = 12$ e $n = 11$.

Solução: Números menores que 12 que são divisores de 12 são $1, 2, 3, 4, 6, 12$, então $\sigma(12) = 1+2+3+4+6+12 = 28$. Números menores que 11 que são divisores de 11 são $1, 11$, então $\sigma(11) = 1 + 11 = 12$.

Teorema 3.22. *A função $\sigma(n)$ é multiplicativa.*

Demonstração. Se n tiver uma representação::

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_r^{\alpha_r},$$

$$1 \leqslant \alpha_1,$$

na qual $p_1, \dots, p_r$ são números primos, $\alpha_1, \dots, \alpha_r$ são naturais, então todos os divisores desse número são:

$$p_1^{\beta_1}.p_2^{\beta_2}\dots p_r^{\beta_r}, 0 \leqslant \beta_i \leqslant \alpha_i.$$

Portanto, temos que :

$$\sigma(n) = \sum_{i=1}^{r} p_1^{\beta_1}.p_2^{\beta_2}\dots p_r^{\beta_r}, 0 \leqslant \beta_i \leqslant \alpha_i,$$

na qual é somado por todos os valores dos expoentes β_i. Essa soma é facilmente calculada porque é um termo geral no desenvolvimento do termo

$$\sigma(n) = (1 + p_1 + \dots + p_1^{\alpha_1})\dots(1 + p_r + \dots + p_r^{\alpha_r})$$

$$= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \dots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1},$$

a partir daqui segue que se $(x, y) = 1$, então $\sigma(xy) = \sigma(x)\sigma(y)$. Em outras palavras, σ é uma função multiplicativa. □

Observação 3.23. Se d é um divisor de n, então $\dfrac{n}{d}$ é um divisor de n. Dessa forma temos que:

$$\sigma(n) = n\left(\frac{1}{d_1} + \dots + \frac{1}{d_k}\right),$$

na qual $d_1, \dots, d_k$ são todos os divisores de n.

Teorema 3.24. *Se $n = p_1^{\beta_1}.p_2^{\beta_2}.\dots.p_s^{\beta_s}$, então $\sigma(n) = \prod_{i=1}^{s}\left(\dfrac{p_i^{\beta_i+1} - 1}{p_i - 1}\right)$.*

Demonstração. Note que os divisores de $p_1^{\beta_1}$ são $1, p_1^2, p_1^3, \dots, p_1^{\beta_1}$. Assim, temos que

$$\sigma(p_1^{\beta_1}) = 1 + p_1^2 + p_1^3 + \dots + p_1^{\beta} = \left(\frac{p_i^{\beta_i+1} - 1}{p_i - 1}\right).$$

Uma prova de que σ é uma função multiplicativa pode ser encontrada no Teorema 3.22 e em Andrews [3]. □

3.5 Função Soma Total dos Divisores - σ_α

Definição 3.25. Para um número real ou complexo α e para qualquer número natural n, definimos que:

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha.$$

A função σ_α é chamada Soma Total dos Divisores de n.

Quando $\alpha = 0$, $\sigma_0(n)$ é o número dos divisores do número n, que denotamos em seguida neste texto por $\tau(n)$. Quando $\alpha = 1$, $\sigma_1(n)$ é a soma dos divisores do número n, que denotamos na seção anterior por $\sigma(n)$.

Para calcular $\sigma_\alpha(p^a)$, observamos que os divisores do número primo p^a são:

$$1, p, p^2, \ldots, p^a$$

portanto, temos que :

$$\sigma_\alpha(p^a) = 1^\alpha + p^\alpha + p^{2\alpha} + \cdots + p^{a\alpha} = \begin{cases} \dfrac{p^{\alpha(a+1)} - 1}{p^\alpha - 1}; \alpha \neq 0 \\ a + 1; \alpha = 0 \end{cases}$$

Do mesmo modo, prova-se que para $\alpha \neq 0$, temos que :

$$\sigma_\alpha(n) = \frac{p_1^{\alpha(a_1+1)} - 1}{p_1^\alpha - 1} \ldots \frac{p_r^{\alpha(a_r+1)} - 1}{p_r^\alpha - 1},$$

na qual $n = p_1^{a_1}.p_2^{a_2} \ldots p_r^{a_r}$. Dessa forma concluímos que σ_α é uma função multiplicativa.

3.6 Função Número de Divisores τ

Definição 3.26. O número de divisores é uma função aritmética τ que está associada ao número inteiro n, a quantidade de divisores de n.

Exemplo 3.27. Vamos calcular $\tau(n)$ para $n = 12$ e $n = 11$.

Solução: Os números que são divisores de 12 são $1, 2, 3, 4, 6, 12$, então $\tau(12) = 6$. Os números menores ou iguais a 11 que são divisores de 11 são $1, 11$, então $\tau(11) = 2$.

Teorema 3.28. *A função $\tau(n)$ é multiplicativa.*

Demonstração. Seja $t = m.n$, com m e n números naturais relativamente primos, ou seja, $(m, n) = 1$. Aplicando-se o Teorema Fundamental da Aritmética, podemos dividir em fatores primos da seguinte forma:

$$m = p_1^{\alpha_1}.p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

$$n = q_1^{\beta_1}.q_2^{\beta_2} \ldots q_s^{\beta_s},$$

na qual cada p_j e q_i são primos. Além disso, como m e n são relativamente primos, concluímos que :

$$t = p_1^{\alpha_1}.p_2^{\alpha_2}\dots p_r^{\alpha_r}.q_1^{\beta_1}.q_2^{\beta_2}\dots q_s^{\beta_s}.$$

Agora cada divisor de t é da forma:

$$t = p_1^{k_1}.p_2^{k_2}\dots p_r^{k_r}.q_1^{\gamma_1}.q_2^{\gamma_2}\dots q_s^{\gamma_s},$$

com $0 \leq k_j \leq \alpha_j$ e $0 \leq \gamma_i \leq \beta_i$, e para cada divisor obtemos um divisor de m e outro divisor de n, dados respectivamente por:

$$u = p_1^{k_1}.p_2^{k_2}\dots p_r^{k_r}, v = q_1^{\gamma_1}.q_2^{\gamma_2}\dots q_s^{\gamma_s}.$$

Sendo assim, cada respectivo divisor de m e n tem a forma acima, e para cada par o seu produto também é um divisor de t. Portanto, obtemos uma bijeção entre o conjunto dos divisores positivos de t e o conjunto de pares de divisores de m e n, respectivamente. Tal bijeção implica que as cardinalidades de ambos os conjuntos é a mesma e, portanto, temos que :

$$\tau(m.n) = \tau(m).\tau(n).$$

□

Teorema 3.29. *Sejam p um primo e $n = p_1^{a_1}p_2^{a_2}...p_t^{a_t}$ um inteiro positivo. Então temos que*

$$\tau(p^a) = a + 1,$$

e como resultado

$$\tau(n) = \prod_{j=1}^{t}(a_j + 1).$$

Demonstração. Os divisores de p^a como mencionado anteriormente são $1, p, p^2, ..., p^a$. então

$$\tau(p^a) = a + 1.$$

Agora, como $\tau(n)$ é multiplicativa, nós temos que

$$\begin{aligned}\tau(n) &= \tau(p^{a_1})\tau(p^{a_2})...\tau(p^{a_t}) \\ &= (a_1+1)(a_2+1)...(a_t+1) \\ &= \prod_{j=1}^{t}(a_j+1).\end{aligned}$$

□

Exemplo 3.30. Como $12 = 2^2.3$ obtemos $\tau(12) = (2+1)(1+1) = 6$. Esse mesmo resultado foi obtido no exemplo anterior quando calculamos $\tau(12)$ por definição.

Aqui apresentamos algumas consequências:

Corolário 3.31. *$\tau(n) = 2$ se, e somente se, n for primo.*

Demonstração. Se n é um número primo, então é divisível pelo número 1 e por si próprio, então $\tau(n) = 2$. Por outro lado, se $\tau(n) = 2$ e uma vez que apenas 1 e n estão incluídos nos divisores, então n é primo. □

Corolário 3.32. *$\tau(n) = 3$ se, e somente se, n tiver a forma $n = p^2$, p é primo.*

Demonstração. Se n é da forma $n = p^2$ na qual p é um número primo, então o número p^2 é divisível pelos números $1, p$ e p^2 e, portanto, temos que $\tau(n) = 3$. Por outro lado, se $\tau(n) = 3$, sabemos que n tem três divisores. Os números 1 e n estão incluídos nos divisores e, daí segue que, o número n é $n = p^2$ e é um número primo.

Todo $\tau(n)$ ímpar implica que n é um quadrado perfeito, pois, supondo que $n = p_1^{k_1} \dots p_i^{k_i}$ temos que $\tau(n) = (k_1 + 1) \dots (k_i + 1)$. Para que seja ímpar, precisamos de todo o $k_j + 1$ seja ímpar, o que significa que todo o k_i é par. Assim, $k_i = 2j_i$ para todo i e então $n = p_1^{j_1} \dots p_i^{j_i}$. □

Exemplo 3.33. Determinar o menor inteiro positivo que possui 21 divisores positivos.

Solução: Como $21 = 3.7$, o número procurado tem a forma p^2q^6 com p e q sendo primos distintos ou a forma p^{20} com p primo. Os menores números sob esta forma são :

$$2^2.3^6 = 2.916$$

$$3^2.2^6 = 576$$

$$2^{20} = 1.048.576$$

Portanto, 576 é o número procurado.

3.7 Relações entre as Funções Aritméticas ϕ, σ e τ

Nesta parte vamos investigar algumas relações entre a função totiente de Euler ϕ, função τ e a função σ usando os conhecimentos da Teoria dos Números para estabelecer estas referidas relações e suas respectivas provas conforme pode ser observado em [3], [22] e [35].

Teorema 3.34. *Temos que $\phi(1) = \sigma(1) = \tau(1) = 1$.*

Demonstração. Inicialmente podemos citar que pelas próprias definições das funções aritméticas $\phi(m)$, $\sigma(m)$ e $\tau(m)$, ou seja, que:

$$\phi(m) = \#\{i : 1 \leqslant i \leqslant m, mdc(i, m) = 1\}, e$$

$$\sigma(m) = \sum_{\substack{d|m, \\ 1 \leqslant d \leqslant m}} d,$$

$$\tau(m) = \sum_{d|m} 1.$$

Temos que $\phi(1) = 1$, pois para $m = 1$, o único número inteiro no intervalo de 1 a m é o próprio 1 e $mdc(1, 1) = 1$, a função $\sigma(m)$ é definida em m como sendo a soma de todos os divisores inteiros positivos de m, portanto 1, e a função número de divisores $\tau(m)$ retorna o número de divisores de m, no caso 1. Assim sendo temos que $\phi(1) = \sigma(1) = \tau(1) = 1$. □

Lema 3.35. *Sejam a um número inteiro não negativo e p um número primo positivo. Se $n = p^a$, então:*

$$\sum_{\substack{1 \leqslant k \leqslant n \\ (k,n)=1}} k = \frac{n.\phi(n)}{2}.$$

Demonstração. Tomando A como a soma dos inteiros positivos menores ou iguais a p^a temos que :

$$A = 1 + 2 + 3 + 4 + \cdots + p^a$$
$$A = \frac{p^a(p^a+1)}{2}.$$

Tomando B como a soma dos inteiros positivos r menores ou iguais a p^a e $(r, p^a) \neq 1$, temos que :

$$B = p + p^2 + p^3 + \cdots + p^a$$
$$B = p\left(1 + p + p^2 + \cdots + p^{a-1}\right)$$
$$B = \frac{p\left(p^{a-1}\right)\left(p^{a-1}+1\right)}{2}.$$

Então, temos que

$$\sum_{\substack{1\leqslant k\leqslant n,\\(k,n)=1}} k = A - B = \frac{p^a\left(p^a+1\right)}{2} - \frac{p\left(p^{a-1}\right)\left(p^{a-1}+1\right)}{2}$$

$$= \frac{p^a}{2}\left(p^a + 1 - p^{a-1} - 1\right)$$
$$= \frac{p^a}{2}\left(p^a - p^{a-1}\right)$$
$$= \frac{n.\phi(n)}{2}.$$

□

Corolário 3.36. *Se k e n são inteiros positivos, então temos que:*

$$\sum_{\substack{1\leqslant k\leqslant n,\\(k,n)=1}} k = \frac{n.\phi(n)}{2}.$$

Demonstração.

1. Caso I - Se n é primo, então :

$$\sum_{\substack{1\leqslant k\leqslant n,\\(k,n)=1}} k = 1 + 2 + \cdots + (n-1) = \frac{n(n-1)}{2} = \frac{n.\phi(n)}{2}.$$

2. Caso II - Se n não é primo e $n = p_1^{\alpha_1}.p_2^{\alpha_2}\ldots p_m^{\alpha_m}$, na qual $p_1, p_2, \ldots, p_m$ são primos distintos e $\alpha_1, \alpha_2, \ldots, \alpha_m$ são inteiros positivos, então:

$$\sum_{\substack{1\leqslant k\leqslant n,\\(k,n)=1}} k = 2^{m-1}\left(\sum_{\substack{1\leqslant k_1\leqslant p_1^{\alpha_1},\\(k_1,p_1^{\alpha_1})=1}} k_1\right)\left(\sum_{\substack{1\leqslant k_2\leqslant p_2^{\alpha_1},\\(k_2,p_2^{\alpha_2})=1}} k_2\right)\ldots\left(\sum_{\substack{1\leqslant k_m\leqslant p_m^{\alpha_m},\\(k_m,p_m^{\alpha_m})=1}} k_m\right)$$

$$= 2^{m-1}\left(\frac{p_1^{\alpha_1}}{2}(p_1^{\alpha_1} - p_1^{\alpha_1-1})\right)\left(\frac{p_2^{\alpha_2}}{2}(p_2^{\alpha_2} - p_1^{\alpha_2-1})\right)\ldots\left(\frac{p_m^{\alpha_m}}{2}(p_m^{\alpha_m} - p_m^{\alpha_m-1})\right)$$

$$= \frac{2^{m-1}}{2^m}\left(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_m^{\alpha_m}\right)\left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right)\left(p_2^{\alpha_2} - p_2^{\alpha_2-1}\right)\ldots\left(p_m^{\alpha_m} - p_m^{\alpha_m-1}\right)$$

$$= \frac{n\phi(n)}{2}.$$

□

Teorema 3.37. *Sejam α e n números inteiros positivos. Se $n = 2^\alpha$ e $2^{\alpha+1} - 1$ é um número primo, então:*

$$\phi(\phi(n)) = 2n = 2^{\tau(n)}.$$

Demonstração. Tomando α, n inteiros positivos se $n = 2^\alpha$ temos que $2^{\alpha-1} - 1$ é primo. Desde que

$$\phi(n) = \phi(2^\alpha) = 2^{\alpha+1} - 1,$$

então

$$\phi(\phi(n)) = \phi(2^{\alpha+1} - 1) = 2^{\alpha+1} = 2n$$

e

$$\tau(n) = \tau(2^\alpha) = \alpha + 1.$$

Portanto,

$$\phi(\phi(n)) = 2n = 2.2^\alpha = 2^{\alpha+1} = 2^{\tau(n)}.$$

□

Teorema 3.38. *Se p é um número primo, então*

$$\sigma(p) = \phi(p) + \tau(p).$$

Demonstração. Seja p um número primo. Então

$$\sigma(p) = p + 1,\ \phi(p) = p - 1 \ e\ \tau(p) = 2.$$

Logo, temos que

$$\phi(p) + \tau(p) = p - 1 + 2 = p + 1 = \sigma(p).$$

Portanto

$$\sigma(p) = \phi(p) + \tau(p),\ \text{na qual p é um número primo.}$$

□

Tabela 3.2: Alguns valores p para $\sigma(p) = \phi(p) + \tau(p)$

p	$\phi(p)$	$\tau(p)$	$\sigma(p)$	$\phi(p) + \tau(p)$
2	1	2	3	3
3	2	2	4	4
5	4	2	6	6
7	6	2	8	8
11	10	2	12	12

Teorema 3.39. *Se $n = 2p$ e p é um número primo ímpar, então*

$$\sigma(n) = n + \phi(n) + \tau(n).$$

Demonstração. Seja $n = 2p$ e p um número primo ímpar. Então:

$$\sigma(n) = \sigma(2p) = \sigma(2)\sigma(p) = 3(p+1) = 3p+3,$$

$$\phi(n) = \phi(2p) = \phi(2)\phi(p) = p-1,$$

e

$$\tau(n) = \tau(2p) = \tau(2)\tau(p) = 2(2) = 4,$$

então

$$n + \phi(n) + \tau(n) = 2p + p - 1 + 4 = 3p + 3.$$

Portanto

$$\sigma(n) = n + \phi(n) + \tau(n), \text{ na qual n = 2p e p é um número primo ímpar.}$$

□

Tabela 3.3: Alguns valores p para $\sigma(p) = n + \phi(p) + \tau(p)$

p	$n = 2p$	$\phi(p)$	$\tau(p)$	$\sigma(p)$	$n + \phi(p) + \tau(p)$
3	6	2	4	12	12
5	10	4	4	18	18
7	14	6	4	24	24
11	22	10	4	36	36
13	26	12	4	42	42

Teorema 3.40. *Se $n = 3p$ e p é um número primo diferente de* 3*, então*

$$\sigma(n) = 2(\phi(n) + \tau(n)).$$

Demonstração. Seja $n = 3p$ e p um número primo não igual a 3. Então:

$$\sigma(n) + \sigma(3p) = \sigma(3)\sigma(p) = 4(p+1) = 4p+4,$$

$$\phi(n) = \phi(3p) = \phi(3)\phi(p) = 2p-2$$

e

$$\tau(n) = \tau(3p) = \tau(3)\tau(p) = 2(2) = 4,$$

logo, temos que

$$2(\phi(n) + \tau(n)) = 2(2p - 2 + 4) = 4p + 4.$$

Portanto,

$$\sigma(n) = 2(\phi(n) + \tau(n)), \text{ na qual n= 3p e p é um número primo diferente de 3.}$$

□

Tabela 3.4: Alguns valores p para $\sigma(n) = 2(\phi(n) + \tau(n))$.

p	$n = 3p$	$\phi(p)$	$\tau(p)$	$\sigma(p)$	$n + \phi(p) + \tau(p)$
2	6	2	4	12	12
5	15	8	4	24	24
7	21	12	4	32	32
11	33	20	4	48	48
13	39	24	4	56	56

Teorema 3.41. *Se $n = 2^k$ e k é um inteiro não negativo, então*

$$\sigma(n) = 2n - 1.$$

Demonstração. Tomando $n = 2^k$ e k um inteiro não negativo, então:

$$\sigma(n) = \sigma(2^k) = \frac{2^{k+1} - 1}{2 - 1} = 2n - 1.$$

Portanto,

$$\sigma(n) = 2n - 1.$$

Tabela 3.5: Alguns valores n para $\sigma(n) = 2n - 1$.

k	$n = 2^k$	$\sigma(n)$	$2n - 1$
0	1	1	1
1	2	3	3
2	4	7	7
3	8	15	15
4	16	31	31

□

Teorema 3.42. *Se $n = 1$ ou $n = p$ é um número primo, então*

$$\sigma(n) + \phi(n) = 2n.$$

Demonstração. Quando $n = 1$ é óbvio. Se $n = p$ é um número primo, então

$$\sigma(n) = \sigma(p) = p + 1$$

e

$$\phi(n) = \phi(p) = p - 1.$$

Portanto,

$$\sigma(n) + \phi(n) = 2p = 2n\text{na qual n = 1 ou n = p é um número primo.}$$

Tabela 3.6: Alguns valores n para $\sigma(n) + \phi(n) = 2n$.

n	$2n$	$\sigma(n)$	$\phi(n)$	$\sigma(n) + \phi(n)$
1	2	1	1	2
2	4	1	3	4
3	6	2	4	6
5	10	4	6	10
7	14	6	8	14

□

Teorema 3.43. *Se p é um número primo, então*

$$\phi(p) = p - (\tau(p))^2 + 3.$$

Demonstração. Tomando p um número primo. Então

$$\phi(p) = p - 1$$

e

$$\tau(p) = 2,$$

então temos que

$$p - (\tau(p))^2 + 3 = p - 2^2 + 3 = p - 1.$$

Portanto,

$$\phi(p) = p - (\tau(p))^2 + 3, \text{quando p é um número primo.}$$

□

Tabela 3.7: Alguns valores p para $\phi(p) = p - (\tau(p))^2 + 3$.

p	$\tau(p)$	$(\tau(p))^2$	$\phi(p)$	$p - (\tau(p))^2 + 3$
2	2	4	1	1
3	2	4	2	2
5	2	4	4	4
7	2	4	6	6
11	2	4	10	10

Teorema 3.44. *Se $n = 2p$ e p é um número primo ímpar, então*

$$\sigma(n) = \frac{n}{2} - 1.$$

Demonstração. Seja $n = 2p$ e p é um número primo ímpar, então

$$\sigma(n) = \sigma(2p) = \sigma(2)\sigma(p) = p - 1 = \frac{2p}{p} - 1 = \frac{n}{2} - 1.$$

Portanto,

$$\sigma(n) = \frac{n}{2} - 1, \text{quando n= 2p e p é um número primo ímpar.}$$

□

Tabela 3.8: Alguns valores n para $\phi(n) = \frac{n}{2} - 1$.

p	$n = 2p$	$(\sigma(n)$	$\left(\frac{n}{2} - 1\right)$
3	6	2	2
5	10	4	4
7	14	6	6
11	22	10	10
13	26	12	12

Teorema 3.45. *Se $n = 4p$ e p é um número primo ímpar, então :*

$$\phi(n) = \frac{n}{2} - 2.$$

Demonstração. Seja $n = 4p$ e p é um número primo ímpar, então :

$$\phi(n) = \phi(4p) = \phi(4)\phi(p) = 2(p-1) = 2p - 2 = \frac{4p}{2} - 2 = \frac{n}{2} - 2.$$

Portanto,

$$\phi(n) = \frac{n}{2} - 2, \text{quando n = 4p e p é um número primo ímpar.}$$

□

Tabela 3.9: Alguns valores n para $\phi(n) = \frac{n}{2} - 2$.

p	$n = 4p$	$(\sigma(n)$	$\left(\frac{n}{2} - 1\right)$
3	12	4	4
5	20	8	8
7	28	12	12
11	44	20	20
13	52	24	24

3.7.1 Números Perfeitos

Existem infinitos números n para os quais $\sigma(n) < 2n$. Por exemplo, para um primo p, $\sigma(p) = 1 + p < 2p$. Como existem infinitos números primos, segue-se que existem uma infinidade de números para os quais $\sigma(n) < 2n$.

Existem infinitos números n para os quais $\sigma(n) > 2n$. Por exemplo:

$$\sigma(2^k.3) = \sigma(2^k).\sigma(3) = \frac{2^{k+1}-1}{2-1}.\frac{3^2-1}{3-1}$$

$$= (2^{k+1}-1).4 > 2^{k+1}.3 = 2n.$$

No entanto, não sabemos se existem infinitos números para os quais $\sigma(n) = 2n$.

Definição 3.46. Um número é perfeito quando a soma de seus divisores (exceto o próprio número) é igual ao número fornecido, ou ainda se $\sigma(n) = 2n$.

O algoritmo para encontrar números perfeitos foi dado por Euclides. Calculamos somas parciais da ordem $1+2+4+8+\ldots$ e se a soma for um número primo, multiplique pelo último número somado e obtenha o número perfeito. Então, por exemplo, temos:

$$1 + 2 = 3 \Rightarrow 3.2 = 6.$$

$$1 + 2 + 4 = 7 \Rightarrow 7.4 = 28.$$

$$1 + 2 + 4 + 8 + 16 = 31 \Rightarrow 31.16 = 496.$$

$$1 + 2 + 4 + 8 + 16 + 32 + 64 = 127 \Rightarrow 127.64 = 8128.$$

Esses números eram conhecidos pelos antigos gregos, e até o momento 48 números perfeitos são conhecidos.

Tabela 3.10: Números Perfeitos

p	$2^p - 1$	$n = 2^{p-1}(2^p - 1)$
2	3	6
3	7	28
5	31	496
7	127	8.128
13	8.191	335.500.336
17	131.071	8.589.869.056

Teorema 3.47. *Um número par n é perfeito se, e somente se, pode ser representado na forma*

$$n = 2^{p-1}(2^p - 1)$$

na qual o número $2^p - 1$ é primo.

Demonstração. Primeiramente vamos mostrar que se $n = 2^{p-1}(2^p - 1)$, na qual $2^p - 1$ primo, então n é perfeito. Perceba que desde que $2^p - 1$ é ímpar, temos que $(2^{p-1}, 2^p - 1) = 1$. Pelo fato de 2^{p-1} e $2^p - 1$ serem relativamente primos entre si e a função σ ser multiplicativa, segue que

$$\sigma(n) = \sigma(2^{p-1}).\sigma(2^p - 1).$$

Como $\sigma(2^{p-1}) = (2^p - 1)$ e $\sigma(2^p - 1) = 2^p$, e uma vez que assumimos que $2^p - 1$ é primo , então :

$$\sigma(n) = (2^p - 1).2^p = 2n,$$

demonstrando que o número n é perfeito.

Por outro lado, como n é perfeito, escrevendo-o na forma $n = 2^s.t$, onde s, t são inteiros positivos e t é ímpar. Uma vez que $(2^s, t) = 1$, então temos que:

$$\sigma(n) = \sigma(2^s.t) = \sigma(2^s).\sigma(t) = (2^{s+1} - 1).\sigma(t). \tag{3.4}$$

Se n é perfeito temos que :

$$\sigma(n) = 2n = (2^{s+1})t. \tag{3.5}$$

Combinando-se (3.4) e (3.5) temos que :

$$(2^{s+1}-1)\sigma(t) = (2^{s+1})t. \tag{3.6}$$

Uma vez que $(2^{s+1}, 2^{s+1}-1) = 1$, segue que $2^{s+1} \mid \sigma(t)$. Portanto, existe um número inteiro k tal que $\sigma(t) = (2^{s+1})k$. Inserindo-se essa expressão em (3.6) temos que $(2^{s+1}-1).2^{s+1}k = 2^{s+1}t$, e portanto:

$$(2^{s+1}-1)k = 1. \tag{3.7}$$

Logo, temos que $k \mid t$ e $k \neq t$.

Substituindo t pela expressão do lado esquerdo de (3.7), encontramos que

$$t + k = (2^{s+1}-1)k + k = 2^{s+1}k = \sigma(t). \tag{3.8}$$

Agora vamos mostrar que $k = 1$. Note que se $k \neq 1$, então há pelo menos três divisores positivos distintos de t, a saber: $1, k$ *e* t. Isso implica que $\sigma(t) \geq t+k+1$, o que contradiz (3.8.)

Desde que $k = 1$ e a partir de (3.7) concluímos que $t = 2^{s+1}-1$. Também a partir de (3.8.), vimos que $\sigma(t) = t+1$, portanto t dever ser primo, pois, seus únicos divisores são 1 *e* t. Assim

$$n = 2^s(2^{s+1}-1),$$

onde $2^{s+1}-1$ é primo. □

3.8 Fatoriais

A função fatorial $n!$ é geralmente definida como o número de permutações de n objetos distintos (ou equivalentemente o produto $n.(n-1)\ldots.1$) na qual n é um número natural, surgindo em muitas fórmulas combinatórias diferentes e em teoremas da Teoria dos Números.

Definição 3.48. Para um número natural $n \in \mathbb{N}$, definimos um número natural "n fatorial" com a notação $n!$ como sendo:

$$n! = 1.2.3.\ldots.n = \prod_{i=0}^{n-1}(n-i),$$

com $0! = 1$.

Lema 3.49. *Se $n \geqslant 3$ e $p_1, \ldots, p_s$ são os números primos ímpares menores ou iguais a n, então existem números inteiros $\alpha \in \mathbb{N}$ $\alpha_1, \ldots, \alpha_s \in \mathbb{N}^*$ tal que:*

$$n! = 2^{\alpha}.p_1^{\alpha_1}.(p_1-1).\ldots.p_s^{\alpha_s}.(p_s-1).$$

Demonstração. Podemos escrever que:

$$n! = \prod_{i=1}^{s}(p_i-1)p_i m_i$$

na qual m_i são inteiros positivos e podem ser escritos na forma :

$$m_i = 2^{\beta}p_1^{\beta_1}\ldots p_s^{\beta_s},$$

na qual $\beta, \beta_1, \ldots, \beta_s \in \mathbb{N}$ e $p_i - 1 \nmid m_i$.. □

Teorema 3.50. *Para todos os $n \in \mathbb{N}$, $n!$ está na imagem da função ϕ Totiente de Euler.*

Demonstração. Como $0! = 1! = 1$ e $2! = 2$ o resultado é verdadeiro para $n = 0, 1, 2$. Do Lema 3.49, para $n \geqslant 2$ temos que :

$$n! = 2^{\alpha}.p_1^{\alpha_1}.(p_1 - 1).\ldots.p_s^{\alpha_s}.(p_s - 1).$$

Mas se n é um inteiro positivo com fatoração em primos dada por $p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_s^{\alpha_s}$ temos que :

$$\phi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_1} - p_2^{\alpha_1 - 1})\ldots(p_s^{\alpha_s} - p_1^{\alpha_s - 1}),$$

portanto,

$$n! = \phi(2^{\alpha+1}.p_1^{\alpha_1+1}.\ldots.p_s^{\alpha_n+1}).$$

Isso termina a prova. □

Definição 3.51. A maior potência de um número primo que é fator de $n!$ é dado por: Seja a um inteiro positivo, então $\lfloor\frac{n}{a}\rfloor$ é o maior inteiro tal que $\alpha a \leqslant n$. Esta definição equivale a dizer que $\lfloor\frac{n}{a}\rfloor = \alpha$ onde $n = \alpha a + r$ com $0 \leqslant r < a$.

Teorema 3.52. *Sejam $n, a, b > 0$ e tomando-se $\alpha = \lfloor\frac{n}{a}\rfloor$ e $\beta = \lfloor\frac{n}{b}\rfloor$, temos que:*

$$\lfloor\frac{\alpha}{b}\rfloor = \lfloor\frac{n}{ab}\rfloor$$

Demonstração. Tomemos $\lfloor\frac{n}{a}\rfloor = \alpha$ e $\lfloor\frac{\alpha}{b}\rfloor = \beta$ de modo que:

$$n = \alpha a + r_1, 0 \leqslant r_1 < a$$

$$\alpha = \beta b + r_2, 0 \leqslant r_2 < b,$$

portanto

$$n = \beta ab + ar_2 + r_1$$

e

$$\lfloor\frac{n}{ab}\rfloor = \beta + \lfloor\frac{ar_2 + r_1}{ab}\rfloor.$$

No entanto, r_2 é no máximo $b - 1$, e r_1 é no máximo $a-1$ e, portanto, $ar_2 + r_1$ é no máximo $a(b-1) + a - 1 = ab - 1$. Logo $\lfloor ar_2 + \frac{r_1}{ab}\rfloor$, segue que:

$$\lfloor\frac{n}{ab}\rfloor = \beta = \lfloor\frac{\alpha}{b}\rfloor.$$

□

Corolário 3.53. *Como sugerido no Teorema 3.52, tomando $\beta = \frac{p^s}{p^t}$ e p é número primo positivo temos que*

$$\lfloor\frac{n}{\beta}\rfloor = \lfloor\frac{n}{p^{s+t}}\rfloor.$$

Corolário 3.54. *Se $n \geqslant a > 0$ e $b > 1$ então*

$$\lfloor\frac{n}{a}\rfloor > \lfloor\frac{n}{ab}\rfloor.$$

Corolário 3.55. *Se a, m e n são positivos então*

$$\lfloor \frac{mn}{a} \rfloor \geqslant m \lfloor \frac{n}{a} \rfloor.$$

Corolário 3.56. *Se $n = n_1 + n_2 + n_3 + \cdots + n_t$, na qual n_i, $i = 1, 2, \ldots, t$ são positivos então*

$$\lfloor \frac{n}{a} \rfloor \geqslant \lfloor \frac{n_1}{a} \rfloor + \lfloor \frac{n_2}{a} \rfloor + \cdots + \lfloor \frac{n_t}{a} \rfloor.$$

Se p é um primo positivo, então defina $\alpha_p(m)$ o expoente da maior potência do primo p que é um divisor de m. Usando este símbolo, provaremos o Teorema 3.57 devido a Legendre (1752-1833). Isso nos ajudará a avaliar como $\alpha_p(n!)$ aumenta à medida que n aumenta.

Teorema 3.57. ***(Teorema de Legendre)*** *- Se n e o primo p forem positivos, o expoente da maior potência de p que divide $n!$ é*

$$\alpha_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots + \lfloor \frac{n}{p^s} \rfloor,$$

sendo s o menor expoente, tal que $\lfloor \frac{n}{p^{s+1}} \rfloor = 0$.

Demonstração. Considere o conjunto dos inteiros

$$1, 2, 3, \ldots, p, \ldots, 2p, \ldots, p^k, \ldots, n. \tag{3.9}$$

O último inteiro do conjunto que é divisível por p é $\lfloor \frac{n}{p} \rfloor p$, e o coeficiente de p mostra que existem $\lfloor \frac{n}{p} \rfloor$ múltiplos de p neste conjunto. Todos os demais inteiros do conjunto são primos de p. Portanto,

$$\alpha_p(n!) = \alpha_p \left(p.2p \ldots p^k. \ldots \lfloor \frac{n}{p} \rfloor p \right)$$

Ao retirarmos um fator p de cada um desses múltiplos de p que estão no conjunto dado por (3.9), obtendo assim o fator $p^{\lfloor \frac{n}{p} \rfloor}$.

Assim sendo,

$$\alpha_p(n!) = \lfloor \frac{n}{p} \rfloor + \alpha_p \left(1.2. \ldots \lfloor \frac{n}{p} \rfloor \right)$$

Mas o último inteiro do novo conjunto

$$1, 2, \ldots, \lfloor \frac{n}{p} \rfloor,$$

que é múltiplo de p é dado por

$$\lfloor \frac{\lfloor \frac{n}{p} \rfloor}{p} \rfloor p = \lfloor \frac{n}{p^2} \rfloor p.$$

Nós podemos, como anteriormente, remover o fator $p^{\lfloor \frac{n}{p^2} \rfloor}$, e a partir do produto de inteiros do novo conjunto mostrar que:

$$\alpha_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots + \alpha_p \left(1.2 \ldots \lfloor \frac{n}{p^2} \rfloor \right).$$

Da mesma forma nós removemos os fatores $p^{\lfloor \frac{n}{p^3} \rfloor}$, $p^{\lfloor \frac{n}{p^4} \rfloor}$, ... até que nós encontremos $p^s \leqslant n < p^{s+1}$ de modo que $\lfloor \frac{n}{p^s} \rfloor \neq 0$, enquanto $\lfloor \frac{n}{p^{s+1}} \rfloor = 0$. Assim sendo temos que :

$$\alpha_p(n!) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \cdots + \lfloor \frac{n}{p^s} \rfloor.$$

□

Lema 3.58. *Sejam $a_1, \ldots, a_m, b \in \mathbb{N}$, sendo $b \neq 0$. Temos então que*

$$\lfloor \frac{a_1, \ldots, a_m}{b} \rfloor \geq \lfloor \frac{a_1}{b} \rfloor + \cdots + \lfloor \frac{a_m}{b} \rfloor.$$

Demonstração. Sejam a_i o quociente e q_i o resto da divisão de a_i por b. Somando todos os a_i temos que:

$$a_1, \ldots, a_m = (q_1 + \cdots + q_m)\, b + r_1 + \cdots + r_m.$$

Dividindo $a_1, \ldots, a_m$ por b, o quociente é maior que ou igual a $(q_1 + \cdots + q_m)$, pois $r_1, \ldots, r_m \geq 0$ e poderia aparecer mais fatores de b na soma. □

Corolário 3.59. *Sejam $a_1, \ldots, a_m$ então*

$$\frac{(a_1 + \cdots + a_m)!}{(a_1)! \ldots (a_m)!} \in \mathbb{N}.$$

Demonstração. Sabemos pelo Lema 3.58 que, $\forall p$ primo e $i \in \mathbb{N}$:

$$\lfloor \frac{a_1 + \cdots + a_m}{p^i} \rfloor \geq \lfloor \frac{a_1}{p^i} \rfloor + \cdots + \lfloor \frac{a_n}{p^i} \rfloor.$$

Ou seja, temos que $\alpha_p((a_1 + \cdots + a_m)!) \geq \alpha_p(a_1)! + \cdots + \alpha_p(a_m)!$. Isso nos diz que $(a_1 + \cdots + a_m)!$ possui mais fatores de cada primo que $a_1! \ldots a_m!$.Daí segue o resultado. □

Teorema 3.60. *Seja p um primo e seja $n = a_0 p^s + \cdots + a_s$ a expansão de base p de n, então temos que*

$$\alpha_p(n!) = \frac{n - \sum_{i=0}^{s} a_i}{p - 1}.$$

Demonstração. Como temos que $n = a_0 p^s + a_1 p^{s-1} + \cdots + a_s$ com $a < a_0 < p$ e $0 \leqslant a_i < p$ para $i = 1, 2, \ldots, s$, assim :

$$\lfloor \frac{n}{p} \rfloor = a_0 p^{s-1} + a_1 p^{s-2} + \cdots + a_{s-2} p + a_{s-1}$$

$$\lfloor \frac{n}{p^2} \rfloor = a_0 p^{s-2} + a_1 p^{s-3} + \cdots + a_{s-2}$$

$$\cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots$$

$$\lfloor \frac{n}{p^s} \rfloor = a_0.$$

Logo,

$$\lfloor \frac{n}{p} \rfloor + \cdots + \lfloor \frac{n}{p^s} \rfloor = a_0 \frac{p^s - 1}{p - 1} + a_1 \frac{p^{s-1} - 1}{p - 1} + \cdots + a_{s-1}$$

ou

$$\alpha_p(n!) = \frac{a_0 p^s + a_1 p^{s-1} + \cdots + a_{s-1} p - a_0 - a_1 - \cdots - a_{s-1}}{p - 1}$$

$$\alpha_p(n!) = \frac{a_0 p^s + \cdots + a_{s-1}p + a_s - a_0 - a_1 - \cdots - a_{s-1} - a_s}{p-1}$$

$$\alpha_p(n!) = \frac{n - (a_0 + a_1 + \cdots + a_s)}{p-1}$$

$$\alpha_p(n!) = \frac{n - \sum_{i=0}^{s} a_i}{p-1}.$$

□

Observação 3.61. Se $n \in \mathbb{N}$, então para $n!$ as funções ϕ e σ podem ser calculadas da seguinte forma:

$$\phi(n!) = \prod_{p \leq n} p^{\alpha_p - 1}.(p-1) \text{ e } \sigma(n!) = \prod_{p \leq n} \frac{p^{\alpha_p + 1} - 1}{(p-1)},$$

onde os produtos são considerados todos os primos menores ou iguais a n.

Exemplo 3.62. Encontre o expoente de maior potência de 5 em 138!.

Solução:

$$138 = 27.5 + 3; \lfloor \frac{138}{5} \rfloor = 27$$

$$27 = 5.5 + 2; \lfloor \frac{138}{5^2} \rfloor = 5$$

$$5 = 1.5 + 0; \lfloor \frac{138}{5^3} \rfloor = 1$$

Consequentemente $\alpha_5(138!) = 27 + 5 + 1 = 33$.

Nós podemos utilizar o resultado do Teorema 3.60 para $\alpha_p(n!)$. Escrevendo-se 138 na base 5, nós temos que

$$5^3 + 0.5^2 + 2.5^1 + 3.$$

Assim sendo temos que:

$$\alpha_5(138!) = \frac{(138 - 6)}{4} = 33.$$

4 Equações diofantinas associadas as funções aritméticas e fatoriais

Neste capítulo, examinaremos e classificaremos soluções para algumas das equações diofantinas que envolvem funções aritméticas e fatoriais famosas. Florian Luca [27] mostrou que existe um número finito de soluções para a equação:

$$f(n!) = a.m!,$$

na qual f é uma das funções aritméticas $\phi,\ ou\ \sigma$ e a é um número racional.

Existem inúmeros fatos peculiares e fascinantes sobre fatoriais e funções Aritméticas e neste capítulo iremos investigar algumas de suas descobertas.

4.1 A Equação Diofantina de Brocard- Ramanujan

A Teoria dos Números apresenta numerosas questões que inicialmente parecem abertas, mas que com certeza acabam sendo impenetráveis. Para termos uma ideia de tais problemas vamos analisar a seguinte conjectura estudada independentemente por Brocard [10, 11] e Ramanujan [38, 39] da seguinte equação diofantina:

$$n! + 1 = y^2. \tag{4.1}$$

A equação (4.1) é chamada equação diofantina de Brocard-Ramanujan e encontrar soluções para esta equação equivale ao problema de encontrar valores inteiros para os quais o número $n! + 1$ é um quadrado perfeito. De fato, Ramanujan [38, 39] declarou o problema da seguinte maneira: "o número $n!+1$ é um quadrado para $n = 4, 5, 7$, encontre outros valores".

Usando-se o caso de fatoração de diferença entre dois quadrados a partir das soluções já conhecidas obtemos que:

$$4! + 1 = 5^2 \Rightarrow 4! = 5^2 - 1 = (5 + 1)(5 - 1) = 6.4 = 24.$$

$$5! + 1 = 11^2 \Rightarrow 5! = 11^2 - 1 = (11 + 1)(11 - 1) = 12.10 = 120.$$

$$7! + 1 = 71^2 \Rightarrow 7! = 71^2 - 1 = (71 + 1)(71 - 1) = 72.70 = 5040.$$

A análise da decomposição anterior nos conduz a soluções que possuem uma diferença de 2 unidades entre as soluções, ou seja, são dois números pares consecutivos, portanto, caso se encontre(m) outra(s) solução(ões) necessariamente ela(s) precisa(m) obedecer a relação estabelecida.

Salvador Cerdá em [14] mostra que através de seu método obtemos as mesmas soluções já conhecidas para $n < 8$ e que para $n \geq 8$ seremos conduzidos a encontrar dois números consecutivos cujo produto seja $\frac{n!}{4}$ verificando que não se encontra soluções diferentes para $n \leq 2000$.

Até o momento, pouco se sabe sobre (4.1) e o problema de encontrar todas as soluções inteiras ainda está em aberto: cálculos até $n = 63$ não deram outras soluções segundo Hansraj Gupta [19]. Recentemente, Berndt e Galway [8] fizeram alguns cálculos até $n = 10^9$ e mostraram que (4.1), exceto pelas soluções conhecidas não possui outras soluções. Overholt, em [34], implementou que a forma fraca da conjectura de Szpiro implica que (4.1) tem apenas un número finito de soluções. A forma fraca da conjectura de Szpiro é um caso especial de conjectura abc e afirma que existe uma constante tal que, se $a, b\, e\, c$ são inteiros positivos que satisfazem $a + b = c$ com $mcd(a, b) = 1$, então temos que :

$$\mid abc \mid \leqslant rad(abc)^s,$$

onde $rad(N)$ é o produto de todos os primos que dividem N obtidos sem repetição. Na mesma direção, Dufour e Kihel [16] implementaram recentemente que a forma fraca da conjectura de Hall (um caso especial de conjectura abc) implica que (4.1) tem apenas un número finito de soluções. A forma fraca da conjectura de Hall afirma que, para cada $\xi > 0$, existe uma constante C_ξ dependendo de $\xi > 0$ apenas de modo que se $x, y\, e\, k$ são números inteiros que satisfazem $y^2 = x^3 + k$, então temos que :

$$max(\mid x^3 \mid, \mid y^2 \mid) \leqslant C_\xi \mid k \mid^{6+\xi} .$$

Denotando A como um número inteiro fixo. Dabrowski [15] estudou a equação diofantina da forma

$$n! + A = y^2, \tag{4.2}$$

onde n e y são inteiros. O principal resultado em [15] é que, se A não é um quadrado, (4.2) tem um número finito de soluções. Este resultado foi estendido recentemente por Dufour e Kihel[16], onde eles conduzem se o número inteiro A não for a q-ésima potência de um número inteiro, com n e y números inteiros, então a equação

$$n! + A = y^q, \tag{4.3}$$

tem um número finito de soluções. Luca [28] constatou através da conjectura abc que, para qualquer $P \in \mathbb{Z}[X]$, a equação diofantina $P(x) = n!$ apresenta um número finito de soluções.

O maior número de resultados do problema de Brocard-Ramanujan e suas variações foi obtido a partir da utilização da conjectura abc ou de suas variantes. Surge naturalmente uma pergunta de como os resultados podem ser provados sem a ajuda dessa suposição? Somos tentados a acreditar na afirmação mais forte de que o problema de Brocard-Ramanujan não tem outras soluções, exceto $(m, n) = (5, 4), (11, 5), (71, 7)$; no entanto, não conseguimos estabelecer isso. A prova da existência de uma nova solução de (4.1) parece tão distante quanto o estabelecimento da inexistência de números perfeitos ímpares e os dois problemas, embora não equivalentes, não são diferentes.

4.2 Equações Diofantinas, Funções Aritméticas e Fatoriais

Nesta seção, mostraremos alguns trabalhos relacionados a equações diofantinas envolvendo funções aritméticas de fatoriais reproduzindo de forma mais detalhada o que foi desenvolvido por Luca em [27] de forma sucinta, além de acrescentarmos alguns problemas envolvendo as funções aritméticas aqui estudadas, com suas respectivas soluções.

Para qualquer número inteiro positivo k, vamos denotar $\phi(k)$, $\sigma(k)$ e $\tau(k)$ como sendo a função totiente de Euler, a soma do divisor e o número de divisores de k, respectivamente. Além disso p indica um número primo e para um número inteiro positivo n.

Em Rosser e Schoenfeld [41] encontramos o seguinte lema com sua devida demostração.

Lema 4.1. *Para $n \geq 2$ temos que*

$$1 + \frac{1}{(n-1)} \leqslant \frac{n}{\phi(n)};$$

também para $n \geqslant 3$,

$$\frac{n}{\phi(n)} < e^c \log\log(n) + \frac{2.50637}{\log\log(n)},$$

onde c representa a constante de Euler-Mascheroni ($c \approx 0.5772$).

Lema 4.2. *Para $n \geqslant e^{e^c}$, $\phi(n) > \dfrac{n}{2\log\log(n+1)}$.*

Demonstração. Baseados no Lema 4.1 , logo quando $n \geq e^{e^c}$, temos $n \geq 3$, então:

$$\phi(n) > \frac{n}{e^c \log\log(n) + \dfrac{2.50637}{\log\log(n)}}$$

$$> \frac{n}{2\log\log(n) + 1}$$

para $n \geqslant e^{e^c}$.

Perceba que $e^c < 2$. Também, note que $\log\log n > 2.50637$ se $n > e^{e^c}$. Então, para $n > e^{e^c}$ temos que a fração $\dfrac{2.50637}{\log\log(n)} < 1$. Conjuntamente isso nos retorna a desigualdade desejada. □

Em Carella [13] encontramos o lema abaixo com sua demonstração.

Lema 4.3.

$$\frac{n}{2\log(\log(n))} < \frac{n}{\phi(n)} < \frac{\sigma(n)}{n}, \text{ para } n > 2.10^9. \tag{4.4}$$

Teorema 4.4. *Seja a qualquer número racional e seja f uma das funções aritméticas ϕ, σ. Então, a equação*

$$\frac{f(n!)}{m!} = a, \tag{4.5}$$

possui um número finito de soluções (m, n).

Demonstração. Para conveniência do leitor reproduziremos aqui a prova encontrada em Luca [27].

Tomamos $f \in \{\phi, \sigma\}$ e fazemos uso do Lema 4.3 .

Assumindo $f = \phi$ vamos considerar os três casos $n < m$, $n > m$, e $n = m$.

1. Se $n < m$, então $n \leqslant m - 1$, obtemos que:

$$am! = \phi(n!) < n! \leqslant (m-1)!,$$

assim temos que

$$am! \leq (m-1)!$$

logo temos que $m \leqslant \dfrac{1}{a}$. Portanto, existe um número finito de valores para m e, consequentemente para n.

2. Se $n > m$.

Tomando $n > max(m, e^{e^c})$, usando os Lemas 4.2 e 4.3, o fato de que a função $\dfrac{x}{2\log(\log(x))}$ é uma função crescente em x, que a função $\dfrac{1}{\log(\log(x))}$ é decrescente, que $n \geqslant m+1$ e uma vez que $(m+1)! < (m+1)^{m+1}$, temos as seguintes implicações:

$$am! = \phi(n!) > \frac{n!}{2\log(\log(n!))} \geqslant \frac{(m+1!)}{2\log(\log(m+1)!)} > \frac{(m+1)!}{2\log(\log(m+1)^{m+1})}.$$

Segue que

$$m + 1 < 2a\log((m+1)\log(m+1)),$$

logo, temos que:

$$\frac{m+1}{\log((m+1)\log(m+1))} < 2a.$$

Assim, como $\lim_{m\to\infty} \dfrac{m+1}{\log((m+1)\log(m+1))} = \infty$, a última desigualdade diz que m é limitado por uma constante. Logo, (4.5) tem um número finito de soluções (m, n) com $m \neq n$.

3. Considerando finalmente que $m = n$ e usando o Teorema 3.15, obtemos que:

$$\frac{1}{a} = \frac{n!}{\phi(n!)} = \prod_{p \leqslant n} \left(1 + \frac{1}{p-1}\right). \tag{4.6}$$

O Terceiro Teorema de Mertens diz que :

$$lim_{n\longrightarrow\infty} \frac{1}{\log n} \prod_{p \leq n} \frac{p}{p-1} = e^c.$$

Um corolário trivial é que o produtório do lado direito da igualdade (4.6) tende ao infinito quando n tende ao infinito e consequentemente a equação tem apenas um número finito de soluções para $n = m$.

Portanto, (4.5) tem um número finito de soluções (m, n).

A prova para $f = \sigma$ é completamente análoga. □

Corolário 4.5. *As únicas soluções para a equação*

$$\phi(n!) = m! \tag{4.7}$$

são obtidas para $n = 0, 1, 2, 3$.

Demonstração. Novamente o Corolário 4.5 e sua demonstração podem ser obtidos em Luca [27].

Notamos que a afirmação é verdadeira para $n \leqslant 4$. Agora, suponha que $n \geqslant 5$ e que $ord_2(n!) = s$ onde $s > 0$.

Escrevendo $n! = 2^s t$ onde t é ímpar. Então $\phi(n!) = 2^{s-1}\phi(t)$ onde $\phi(t)$ é divisível por $\prod_{p \leqslant n}(p-1)$. Em particular, $\phi(t)$ é divisível por $(3-1)(5-1) = 8$. Agora segue que o expoente de 2 na decomposição do fator primo de $\phi(n!)$, ou seja, $ord_2(n!) \geq s-1+3 > s$.

Por outro lado, uma vez que $m! = \phi(n!) < n!$, segue que $m < n$. Assim, o expoente de 2 na decomposição do fator primo de $m!$ não pode exceder s, ou seja $ord_2(m!) \leq ord_2(n!) = s$ e isso retorna a contradição desejada. □

Tabela 4.1: Soluções para $\phi(n!) = m!$

n	m
0	1
1	1
2	1
3	2

Corolário 4.6. *As únicas soluções para a equação*

$$\sigma(n!) = m! \tag{4.8}$$

são obtidas para $n = 0, 1$.

Demonstração. Pode-se verificar que as soluções afirmadas para o Corolário 4.6 são de fato as únicas soluções para $n \leq 8$. Supondo que $n \geqslant 9$ obtemos a partir do Teorema 3.15, do Teorema 3.24 e do fato de que $n! = \prod_{p \leq n} p^{\alpha_p}$, onde $\alpha_p = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \cdots + \lfloor \frac{n}{p^n} \rfloor$ que:

$$\phi(n!) = n! \prod_{p \leqslant n} \left(1 - \frac{1}{p}\right) = n! \prod_{p \leqslant n} \left(\frac{p-1}{p}\right),$$

e que

$$\sigma(n!) = \prod_{p \leqslant n} \frac{p^{\alpha_p + 1} - 1}{p - 1}.$$

Então, temos que:

$$\sigma(n!).\phi(n!) = n! \prod_{p \leqslant n} \frac{p^{\alpha_{p+1}} - 1}{p} < n! \prod_{p \leqslant n} p^{\alpha_p} = n!.n!.$$

Segue que:

$$\frac{\sigma(n!)}{n!} < \frac{n!}{\phi(n!)} = \prod_{p \leqslant n} \frac{p}{p-1}.$$

Assim obtemos que:

$$\frac{\sigma(n!)}{n!} < \frac{n!}{\phi(n!)} = \prod_{p \leqslant n} \frac{p}{p-1} \leqslant \prod_{\substack{2 \leqslant k \leqslant n, \\ k \neq 4,6,8,9}} \frac{k}{k-1} = n.\frac{3}{4}.\frac{5}{6}.\frac{7}{8}.\frac{8}{9} < \frac{n}{2}.$$

Portanto, $n! < m! = \sigma(n!) \leqslant \frac{n}{2}.n! < (n+1)!$, o que é uma contradição, pois nenhum fatorial pode estar estritamente entre $n!$ e $(n+1)!$. □

Tabela 4.2: Soluções para $\sigma(n!) = m!$

n	m
0	1
1	1

Corolário 4.7. *As únicas soluções para a equação*

$$2\sigma(n!) = m! \tag{4.9}$$

são obtidas para $n = 2, 3, 4, 5$.

Demonstração. A demonstração é análoga ao do Corolário 4.6. Portanto, temos que $n! < m! \leqslant 2\sigma(n!) < 2.\left(\frac{n}{2}\right).n! < (n+1)!$, que é uma contradição. □

4.3 Alguns problemas envolvendo Funções Aritméticas

Exemplo 4.8. Mostre que se m e n são inteiros positivos e $(m; n) = p$; onde p é primo, então

$$\phi(m, n) = \frac{p\,\phi(m)\,\phi(n)}{p-1}.$$

Solução:

Uma vez que $(m; n) = p$; então $p \mid m$ e p |n; e p divide um dos dois inteiros m e n exatamente uma vez, caso contrário $(m; n) \geq p^2$; o que é uma contradição.

Suponha que $p \mid n$ mas $p^2 \nmid n$; então existe um inteiro k tal que $n = kp$ e $(k; p) = 1$; e uma vez que $p = (m; n)$; então $(m; k) = 1$ também, e portanto

$$\phi(n) = \phi(kp) = \phi(k)\phi(p) = \phi(k)(p-1).$$

Se $m = p^{\alpha}p_1^{\alpha_1} \dots p_r^{\alpha_r}$ é a decomposição da potência primária de m; então

$$\phi(mp) = p^{\alpha}(p-1)p^{\alpha_1-1}(p_1-1)\dots p_r^{\alpha_r-1}(p_r-1)$$

$$= p.p^{\alpha-1}(p-1)p^{\alpha_1-1}(p_1-1)\dots p_r^{\alpha_r-1}(p_r-1)$$

$$= p\phi(m),$$

de modo que

$$\phi(mn) = p\phi(m)$$

e

$$\phi(mn) = \phi(mkp) = \phi(mp)\phi(k) = \frac{p\,\phi(m)\,\phi(n)}{p-1}.$$

Exemplo 4.9. Mostre que se m e k são inteiros positivos, então

$$\phi(m^k) = m^{k-1}\phi(m).$$

Solução:
Seja $m = p^{\alpha}p_1^{\alpha_1}\dots p_r^{\alpha_r}$ a decomposição de potência primária de m; então

$$\phi(m) = p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\dots p_r^{\alpha_r-1}(p_r-1)$$

Desde que $m^k = p_1^{k\alpha_1}p_2^{k\alpha_2}\dots p_r^{k\alpha_r}$, então:

$$\phi(m^k) = p_1^{k\alpha_1-1}(p_1-1)p_2^{k\alpha_2-1}(p_2-1)\dots p_r^{k\alpha_r-1}(p_r-1)$$

$$\phi(m^k) = p_1^{(k-1)\alpha_1+\alpha_1-1}(p_1-1)p_2^{(k-1)\alpha_2+\alpha_2-1}(p_2-1)\dots p_r^{(k-1)\alpha_r+\alpha_r-1}(p_r-1)$$

$$\phi(m^k) = p_1^{(k-1)\alpha_1}p_1^{\alpha_1-1}(p_1-1)p_2^{(k-1)\alpha_2}p_2^{\alpha_2-1}(p_2-1)\dots p_r^{(k-1)\alpha_r}p_r^{\alpha_r-1}(p_r-1)$$

$$\phi(m^k) = m^{k-1}p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)p_r^{\alpha_r-1}(p_r-1)$$

$$\phi(m^k) = m^{k-1}\phi(m).$$

Exemplo 4.10. Mostre que se a e b são inteiros positivos e $d = (a;b)$; então

$$\phi(ab) = \frac{d\phi(a)\phi(b)}{\phi(d)}.$$

Conclua que se $d > 1$; então $\phi(ab) > \phi(a)\phi(b)$

Solução:
Sejam $p_1, p_2, \dots, p_r$ sejam aqueles primos dividindo a mas não b ,$q_1, q_2, \dots, q_s$ sejam aqueles primos dividindo b mas não a e $r_1, r_2, \dots, r_t$ sejam primos dividindo ambos a e b.
Definimos que :

$$P = \prod_{k=1}^{r}\left(1-\frac{1}{p_k}\right),\ Q = \prod_{k=1}^{s}\left(1-\frac{1}{q_k}\right)\ e\ R = \prod_{k=1}^{t}\left(1-\frac{1}{r_k}\right),$$

então temos que:

$$\phi(ab) = abPQR = \frac{aPRbQR}{R} = \frac{\phi(a)\phi(b)}{R}.$$

Contudo, temos que

$$\phi((a,b)) = (a,b)R$$

de modo que

$$R = \frac{\phi(d)}{d}$$

e uma vez que $d = (a; b)$, portanto temos que

$$\phi(ab) = \frac{d\phi(a)\phi(b)}{\phi(d)}.$$

Observe que se $d > 1$; então $\phi(d) \leq d - 1 < d$; de modo que

$$\frac{d}{\phi(d)} > 1$$

e

$$\phi(ab) = \frac{d\phi(a)\phi(b)}{\phi(d)} > \phi(a)\phi(b).$$

Exemplo 4.11. Para quais n inteiros positivos $\phi(n) \mid n$?

Solução:
Suponha que n seja um número inteiro positivo e tomemos :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}.$$

como sendo a decomposição de potência primas de n; então temos que :

$$\phi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \dots p_k^{\alpha_k - 1}(p_1 - 1)(p_2 - 1) \dots (p_k - 1)$$

Se $\phi(n) \mid n$ então

$$\frac{p_1}{p_1 - 1}.\frac{p_2}{p_2 - 1} \dots \frac{p_k}{p_k - 1}.$$

é um número inteiro positivo e, como o numerador pode ter no máximo um fator de 2; isso implica que o denominador pode conter no máximo um fator $(p_i - 1)$ onde p_i é um primo ímpar.

Portanto, na decomposição da potência primária de n; ou $n = 1$; $n = 2^\alpha$; *ou* $n = 2^\alpha p^\beta$; onde p é um primo ímpar e $\alpha \geq 1$ e $\beta \geq 1$:

1. Se $n = 2^\alpha$ onde $\alpha \geq 0$, então para $\alpha = 0$, nós temos $n = 1$ e $\phi(n) = 1$, enquanto que para $\alpha \geq 1$ temos que $n = 2^\alpha$ e $\phi(n) = 2^{\alpha-1}(2 - 1) = 2^{\alpha-1} = \frac{n}{2}$.

2. Se $n = 2^\alpha p^\beta$, onde p é um primo ímpar, $\alpha \geq 1$ e $\beta \geq 1$, então:

   $$\phi(n) = n.\frac{2 - 1}{1}\frac{p - 1}{p}.$$

   e desde que $\phi(n) \mid n$, então:

   $$k = \frac{n}{\phi(n)} = \frac{2p}{p - 1},$$

   é um número inteiro, de modo que $p - 1 = 2$; ou seja, $p = 3$; e$n = 2^\alpha p^\beta$ onde $\alpha \geq 1$ e $\beta \geq 1$.

Portanto, os únicos inteiros positivos n para os quais $\phi(n) \mid n$ são dados por:

$$n = 1, 2^\alpha \ e \ 2^\alpha 3^\beta,$$

onde $\alpha, \beta \geq 1$

Exemplo 4.12. Mostre que o número de pares ordenados de inteiros positivos com o mínimo múltiplo comum igual ao inteiro positivo n é $\tau(n^2)$.

Solução:

Vamos denotar o mínimo múltiplo comum entre os inteiros a e b como $[a, b]$.

Claramente, o resultado é verdadeiro se $n = 1$; desde então $\tau(n) = 1$; e o único par ordenado de inteiros positivos com menor múltiplo comum 1 é $(1; 1)$. Seja n um inteiro positivo com $n > 1$; e suponha que a decomposição em potências de primos de n seja dada por:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

onde $p_1 < p_2 < \cdots < p_r$ são primos distintos e $\alpha_k \geq 1$ e $1 \leq k \leq r$.

Agora suponha que b e c sejam inteiros positivos tais que $[b; c] = n$; então $b \mid n$ e $c \mid n$; de modo que suas decomposições em potência de primos são dadas por

$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r} \ \ e \ \ c = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r},$$

onde $0 \leq \beta_k \leq \alpha_k$ e $0 \leq \gamma_k \leq \alpha_k$ para $1 \leq k \leq r$.

Desde que $[b; c] = n$; então devemos ter o $max\{\beta_k; \gamma_k\}$ para $1 \leq k \leq r$ de modo que para cada um desses k; um deles β_k ou γ_k deve ser igual a α_k; enquanto o outro pode ser qualquer um dos inteiros $0 \leq l \leq \alpha_k$.

Portanto, para cada k com $1 \leq k \leq r$; o número de maneiras de escolher o par ordenado $(\beta_k; \gamma_k)$ de modo que exatamente um ou ambos de β_k e γ_k igual a α_k é igual a

$$\alpha_k + \alpha_k + 1 = 2\alpha_k + 1,$$

e o número de maneiras de escolher os expoentes

$$\beta_1, \beta_2 \dots, \beta_r, \gamma_1, \gamma_2, \dots, \gamma_r.$$

é igual a

$$(2\alpha_1 + 1)(2\alpha_2 + 1) \dots (2\alpha_r + 1) = \tau(n^2).$$

Assim, o número de pares ordenados de inteiros positivos $(b; c)$ tais que $[b; c] = n$ é igual a $\tau(n^2)$.

Exemplo 4.13. Mostre que se n é um número inteiro positivo, então

$$\left(\sum_{d|n} d \right)^2 = \sum_{d|n} \tau(d)^3$$

Solução:

Tomemos $F(n) = \left(\sum_{d|n} d \right)^2$ e $G(n) = \sum_{d|n} \tau(d)^3$ para $n \geq 1$; então F e G são multiplicativas visto que τ é multiplicativa, e para mostrar que a igualdade $F(n) = G(n)$ vale para todo $n \geq 1$; precisamos apenas mostrar que é verdade para $n = p^\alpha$, onde p é primo e $\alpha \geq 1$.

Os divisores de p^α são $1, p, p^2, \dots, p^\alpha$ e

$$\tau(1) = 1, \tau(p) = 2, \tau(p^2) = 3, \dots, \tau(p^\alpha) = \alpha + 1,$$

de modo que

$$F(p^\alpha) = \left(\sum_{k=1}^{\alpha+1} k \right)^2 = \sum_{k=1}^{\alpha+1} k^3 = G(p^\alpha).$$

5 Transposição Didática

A resolução de equações é um assunto que é apresentado no nível de ensino fundamental II já em seus anos iniciais sendo que ao mesmo tempo são estudados os diferentes conjuntos numéricos. Além disso, conceitos elementares da Teoria dos Números são revisados, tais como: máximo divisor comum, mínimo múltiplo comum, números primos, etc.

Neste capítulo apresentamos as equações diofantinas e suas aplicações no mundo real, além de resolvermos algumas funções aritméticas.

O estudo das equações diofantinas nos permite reforçar os conhecimentos adquiridos nos cursos anteriores e também fornece ao professor ideias para motivar o aluno no estudo de resolução de equações e, mais genericamente, aumentar o seu interesse no estudo da matemática.

Para introduzirmos o referido assunto podemos fazê-lo através de uma motivação histórica. Para tanto recomendamos a utilização dos capítulos iniciais desta dissertação que abordam toda a parte histórica da Teoria dos Números e também situa Diophantus e seu importante papel dentro do estudo sistemático de vários problemas da Teoria dos Números, abordando problemas que envolviam equações que apresentavam soluções racionais ou inteiras.

5.1 Aplicações de Equações Diofantinas

A Teoria dos Números teve pouca aplicação prática, por muitos anos, segundo alguns estudiosos. É sabido que o Godfrey Harold Hardy (1877-1947), grande teórico inglês que atuou na área dos números, acreditava que a Teoria dos Números não tinha aplicações práticas (veja o seu ensaio *"The Mathematician's Apology"*, [20]). No decorrer dos séculos XX e XXI essa situação mudou significativamente e contrariando a opinião de Hardy muitas aplicações práticas e interessantes da Teoria dos Números foram descobertas.

A maioria dos estudantes ou adultos na sociedade atual acredita que evitará usar as operações numéricas mais complicadas de suas vidas, e apenas as operações numéricas mais básicas podem ser usadas para o resto da vida. Muitos deles nunca ouviram falar do tipo de equações, como as diofantinas, e acreditam que não precisam delas em suas vidas.

Note, no entanto, que encontramos equações diofantinas em muitas ocasiões cotidianas. Mesmo as crianças da escola primária reconhecem exemplos simples que levam a equações diofantinas. Além disso, os alunos do segundo nível do ensino fundamental se familiarizam com vários exemplos de equações diofantinas no curso de equações lineares, apesar do nome equações diofantinas não ser explicitamente usado.

Estimar a solução de uma solução linear de equação diofantina através da experimentação, não pode ser considerado um método regular, mas este método é frequentemente

usado. O método consiste em substituir inteiros arbitrários na equação e determinar se eles são a solução. No entanto, na maioria dos casos, só obtemos algumas soluções.

Exemplo 5.1. Quantas maneiras podemos distribuir água de um barril de 29 litros em barris de dois e três litros?

Solução: Se resolvermos essa tarefa através da experimentação, primeiro pensaremos se é possível distribuir tudo em barris de 2 (dois) litros ou apenas de 3 (três) litros. No entanto, há um problema aqui, porque o número 29 não é divisível nem pelo número 2 nem pelo número 3. Então vamos tentar pensar em uma combinação de tambores de 2 e 3 litros para ajustar o número requerido de litros. Para algumas das nossas experiências, consulte a Tabela 5.1 para maior clareza:

Tabela 5.1: Algumas soluções experimentais para a tarefa

2 Litros	10	8.5	7	4	11.5	...
3 Litros	3	4	5	7	2	...
Resultado	Sol. Int	Não tem Sol. Int	Sol. Int	Sol. Int	Não tem Sol. Int	...

A Tabela 5.1 lista as diferentes soluções experimentais, mas apenas algumas delas são inteiras, como podemos observar na Tabela 5.2

Tabela 5.2: Algumas soluções inteiras para a tarefa

2 Litros	10	7	4	...
3 Litros	3	5	7	...

Como podemos perceber encontramos algumas soluções possíveis para o nosso problema.

5.2 O uso de Matrizes para a Resolução de Sistema de Equações Diofantinas

A equação diofantina não trivial mais simples é aquela com duas variáveis da forma $ax + by = c$, e geralmente é resolvida através do Algoritmo Euclidiano. Ao escrever-se o Algoritmo Euclidiano em termos de redução de linha de tal forma que o método seja generalizado para resolver qualquer sistema linear em qualquer número de variáveis, segundo [36], temos a exigência de soluções inteiras que implica que as reduções de linha devem envolver apenas inteiros; este tipo de operação de linha é denominado unimodular. Uma operação de linha unimodular elementar em uma matriz consiste em um dos três tipos de operações a seguir.

(i) Adicionar um múltiplo inteiro de uma linha da matriz a outra linha.

(ii) Trocar duas linhas da matriz de posição.

(iii) Multiplicar uma linha da matriz por -1.

Proposição 5.2. *É sempre possível uma linha reduzir a matriz coluna*

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \\ \vdots \\ a_n \end{bmatrix} \; para \; \begin{bmatrix} d \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

na qual $d = mdc(a_1, a_2, a_3, \ldots, a_n)$.

Demonstração. Repita o seguinte processo até que haja apenas uma entrada diferente de zero.

(i) Seja a_j um elemento de $a_1, a_2, \ldots, a_n$ que tem o menor valor absoluto diferente de zero.

(ii) Para cada $i \neq j$ aplique o Algoritmo da Divisão para obter

$$a_1 = k_i a_j r + r_i, \;\; onde \; 0 \leq \mid r_i \mid < \mid a_j \mid .$$

(iii) Para cada $i \neq j$, subtrair k; vezes a linha j da linha i.

Notamos que o maior valor absoluto de todas as entradas diminui estritamente, a menos que todas as entradas diferentes de zero tenham o mesmo valor absoluto cada vez que esse processo é aplicado. Nesse caso excepcional, todas as entradas, exceto uma, tornam-se diferentes de zero. Portanto, o algoritmo termina e, trocando as linhas e possivelmente multiplicando uma linha por -1, podemos mover a entrada diferente de zero para o topo e torná-la positiva. Usando qualquer uma das definições usuais do máximo divisor comum, é fácil mostrar que

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

Então

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

□

O sistema de equações diofantinas lineares pode ser expresso na forma matricial $AX = B$. Mostrar como determinar se o sistema possui uma solução inteira e, em caso afirmativo, como encontrar todas as suas soluções fazendo uso de uma definição mais fraca da forma de escalonamento de linha, em que a entrada inicial (pivô) pode ser qualquer número inteiro e não necessariamente igual a 1 foi discutido por A. Pathria e W. J. Gilbert em [36]. Ele afirma que uma matriz está escalonada se:

(i) todas as linhas zero estão na parte inferior da matriz;

(ii) a entrada principal em cada linha diferente de zero está à direita de todas as entradas principais nas linhas acima dela.

Teorema 5.3. *Para resolver o sistema de equações diofantinas lineares $AX = B$, a linha unimodular reduz $[A^t \mid I]$ para $[r \mid T]$, onde R está na forma de linha escalonada. Então o sistema $AX = B$ possui soluções inteiras se, e somente se, o sistema $R^tK = B$ possui soluções inteiras para K, e todas as soluções de $AX = B$ têm a forma $X = T^tK$.*

A equação matricial $R^tK = B$ pode ser facilmente resolvida para K por substituição. Uma equação típica apresenta a forma:

$$\begin{bmatrix} d_1 & & & \\ * & d_2 & & \\ * & * & d_3 & \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \\ \vdots \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ \vdots \end{bmatrix}$$

Exemplo 5.4. Encontre todas as soluções inteiras para o sistema de equações abaixo:

$$\begin{cases} 5x_1 + 6x_2 + 8x_3 = 1 \\ 6x_1 - 11x_2 + 7x_3 = 9 \end{cases}$$

Usando a redução de linha temos :

$$\left[\begin{array}{cc|ccc} 5 & 6 & 1 & 0 & 0 \\ 6 & -11 & 0 & 1 & 0 \\ 8 & 7 & 0 & 0 & 1 \end{array}\right] \rightarrow \left[\begin{array}{cc|ccc} 5 & 6 & 1 & 0 & 0 \\ 1 & -17 & -1 & 1 & 0 \\ 3 & 1 & -1 & 0 & 1 \end{array}\right] \left[\begin{array}{cc|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & 91 & 6 & -5 & 0 \\ 0 & 52 & 2 & -3 & 1 \end{array}\right]$$

$$\rightarrow \left[\begin{array}{cc|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & -13 & 2 & 1 & -2 \\ 0 & 52 & 2 & -3 & 1 \end{array}\right] \rightarrow \left[\begin{array}{cc|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & 13 & -2 & -1 & 2 \\ 0 & 0 & 10 & 1 & -7 \end{array}\right]$$

A equação $R^tK = B$ é dada por:

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

Consequentemente, temos que $k_1 = 1$ e $-17k_1 + 13k_2 = 9$. Portanto, $13k_2 = 26$ e, como o lado direito é divisível por 13, a equação tem uma solução inteira, ou seja, $k_2 = 2$. A variável k_3 pode ser qualquer valor inteiro, digamos $k_3 = k \in \mathbb{Z}$. Portanto,

$$K = \begin{bmatrix} 1 \\ 2 \\ k \end{bmatrix} e \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = T^tK = \begin{bmatrix} -1 & -2 & 10 \\ 1 & -1 & 1 \\ 0 & -2 & -7 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ k \end{bmatrix} = \begin{bmatrix} -5 + 10k \\ -1 + k \\ 4 - 7k \end{bmatrix}$$

A completa solução de inteiros para o sistema é dada por :

$$\begin{cases} x_1 = -5 + 10k \\ x_2 = -1 + k, para\ k \in \mathbb{Z} \\ x_3 = 4 - 7k \end{cases}$$

Em geral, a questão de saber se o sistema tem alguma solução inteira depende se certas combinações do lado direito são 0 (zero) ou são divisíveis pelos pivôs de R. No exemplo acima, os pivôs (entradas principais) são 1 e 13. Se as entradas no lado direito fossem b_1 e b_2, o sistema teria uma solução se, e somente se, a equação $k_1 = b_1$ e $-17k_1 + 13k_2 = b_2$ teriam soluções inteiras. Isso aconteceria se, e somente se, $17b_1 + b_2$ fossem divisíveis por 13.

Na solução de um sistema grande, você pode verificar cada linha do sistema $R^tK = B$ à medida que avança para determinar se o sistema ainda possui uma solução. Se não houver solução, talvez você não precise concluir a redução de linha.

5.3 Balanceamento de uma Equação Química

Outro exemplo de uma aplicação de equação diofantina na vida real é sua aplicação na química, mais diretamente na sua utilização no balanceamento de equações químicas.

No balanceamento de equações químicas, a abordagem diofantina, além de seu interesse intrínseco, tem as vantagens da aplicação mecânica e de ilustrar a variedade de métodos possíveis.

Considere uma equação química escrita na forma :

$$x_1A_{a_1}B_{b_1}C_{c_1}\ldots + x_2A_{a_2}B_{b_2}C_{c_2}\ldots + \ldots \rightarrow x_1'A_{a_1'}B_{b_1'}C_{c_1'}\ldots + x_2'A_{a_2'}B_{b_2'}C_{c_2'}\ldots + \ldots$$

na qual $A, B, C, \ldots$ são os elementos presentes na reação química, $a_1, b_1, c_1, \ldots, a_1', b_1', c_1', \ldots$ são inteiros positivos ou 0, e $x_1, x_2, \ldots, x_1', x_2', \ldots$ são os coeficientes desconhecidos dos reagentes e dos produtos. Então, temos que:

$$\begin{aligned} x_1a_1 + x_2a_2 + \cdots &= x_1'a_1' + x_2'a_2' + \ldots \\ x_1b_1 + x_2b_2 + \cdots &= x_1'b_1' + x_2'b_2' + \ldots \\ x_1c_1 + x_2c_2 + \cdots &= x_1'c_1' + x_2'c_2' + \ldots \\ &\ldots \end{aligned} \tag{5.1}$$

Percebe-se que para cada elemento particular $A, B, C, \ldots$, (5.1) tem uma equação que expressa a lei de conservação do número de átomos e um desconhecido para cada termo $x_1A_{a_1}B_{b_1}C_{c_1}\ldots$ - produto reagente - na reação. Encontrar-se todas as soluções inteiras $\{x_1, x_2, \ldots, x_1', x_2', \ldots\}$ de (5.1) é encontrarmos soluções para as equações diofantinas.

Exemplo 5.5. Consideremos a seguinte equação química:

$$x_1KMnO_4 + x_2H_2SO_4 + x_3H_2O_2 \rightarrow x_1'K_2SO_4 + x_2'MnSO_4 + x_3'H_2O_2 + x_4'O_2 \tag{5.2}$$

Solução:

Partindo-se da equação química (5.2) nós obtemos o seguinte sistema de equações:

$$\begin{aligned} 4x_1 + 4x_2 + 2x_3 &= 4x_1' + 4x_2' + x_3' + 2x_4' \text{ para } O \\ x_1 &= x_2' \text{ para } Mn \\ x_1 &= 2x_1' \text{ para } K \\ x_2 &= x_1' + x_2' \text{ para } S \\ 2x_2 + 2x_3 &= 2x_3' \text{ para } H \end{aligned} \tag{5.3}$$

Assim sendo, o sistema (5.3) pode ser facilmente reduzido para a equação diofantina

$$5x_1 + 2x_3 - 4x_4' = 0 \tag{5.4}$$

ou em um equivalentemente a uma equação diofantina linear em três variáveis.

Assim, temos que (5.4) apresenta como solução $\{x_1, x_3, x_4'\} = \{2, 1, 3\}$ e, portanto, temos que $\{x_1, x_2, x_3, x_1', x_2', x_3', x_4'\} = \{2, 3, 1, 1, 2, 4, 3\}$. Consequentemente temos que:

$$2KMnO_4 + 3H_2SO_4 + 1H_2O_2 \rightarrow 1K_2SO_4 + 2MnSO_4 + 4H_2O_2 + 3O_2 \tag{5.5}$$

É evidente que (5.5) não é a única solução do nosso problema de balanceamento. Uma outra solução para a nossa equação seria dada por

$$\{x_1, x_2, x_3, x_1', x_2', x_3', x_4'\} = \{2, 3, 3, 1, 2, 6, 4\}$$

ou ainda

$$\{x_1, x_2, x_3, x_1', x_2', x_3', x_4'\} = \{2, 3, 5, 1, 2, 8, 5\}.$$

De fato, após um breve cálculo, vemos que o conjunto S de todas as soluções inteiras positivas do Sistema (5.3) é infinito e pode ser escrito na forma

$$\mathrm{S} = \left\{ [2u, 3u, v, u, 2u, 3u + v, \frac{(5u + v)}{2}] : v, \frac{(5u + v)}{2} \in N \right\} \tag{5.6}$$

Observe agora que a solução de (5.5) pode ser obtida em (5.6) colocando $u = v = 1$. Assim, (5.5) é a menor solução possível do problema de balanceamento de (5.2). Finalmente, vemos que $\frac{(5u + v)}{2} \in \mathbb{N}$ se, e somente se $u \equiv v \ (mod\ 2)$. Por isso, prontamente segue-se que S pode ser escrito na forma $S = S_1 \cup S_2$ onde

$$S_1 = \{[4r - 2, 6r - 3, 2s - 1, 2r - 1, 4r - 2, 6r + 2s - 4, 5r + s - 3] : r, s \in \mathbb{N}\} \text{ e}$$

$$S_2 = \{[4r, 6r, 2s, 2r, 4r, 6r + 2s, 5r + 2] : r, s \in \mathbb{N}\}.$$

5.4 Determinação da Fórmula Molecular

Suponha que uma substância com um peso molecular m contém os elementos $A, B, C, \ldots$ com pesos atômicos $a, b, c, \ldots$ e que $x, y, z, \ldots$ representam os números de átomos de $A, B, C, \ldots$ em uma molécula. Então nós temos

$$ax + by + cz + \cdots = m. \tag{5.7}$$

Tomando $\alpha, \beta, \gamma, \ldots$ para denotar os inteiros mais próximos dos valores $a, b, c, \ldots$ e μ denotando o inteiro mais próximo m . Então, temos que (5.7) pode ser substituída pela equação diofantina linear :

$$\alpha x + \beta y + \gamma z + \cdots = \mu. \tag{5.8}$$

Segundo [25] devemos exigir que os valores $x, y, z, \ldots$ em 5.8 sejam razoavelmente pequenos, para a sua resolução, oiu seja, sob a condição

$$\frac{-1}{2} < (a - \alpha)x + (b - \beta)y + (c - \gamma)z + \cdots < \frac{1}{2} \tag{5.9}$$

Se vários conjuntos de valores (positivos) para x e y satisfazem (5.8), um conjunto pode ser substituído em (5.7) e encontrar um que satisfará (5.7), pelo menos com erro mínimo (derivação de m). Este conjunto será o conjunto correto de valores para x e y; isto é, a solução para (5.7). (Também um conjunto de valores satisfatórios de (5.9) pode conter um x ou y razoavelmente muito grande para o tamanho da molécula e, portanto, pode ser eliminado por causa disso.)

Exemplo 5.6. O peso molecular de uma substância contendo apenas H (hidrogênio) e S (enxofre) é 66.15. Determine a fórmula molecular deste composto.

Solução: Tomemos $x =$ número de átomos de Hidrogênio e $y =$ número de átomos de Enxofre. Usando a tabela periódica de elementos, descobrimos que $a = 1.008$ para o peso atômico do Hidrogênio e $b = 32.065$ para o peso atômico do enxofre. Assim temos que :

$$1.008x + 32.065y = 66.146 \tag{5.10}$$

Em seguida, vemos que $\alpha = 1, \beta = 32, \mu = 66$ e que $x \leqslant 34, y \leqslant 2$. Uma vez que $1.008 - 1 = 0.008$ e $32.065 - 32 = 0.065$ são diferenças muito pequenas, a molécula teria que conter muitos átomos (mais de 25 de enxofre, ou mais de 62 de hidrogênio, e, portanto, mais de 25 átomos em qualquer caso), de modo que $-\frac{1}{2} < (1.008-1)x+(32.065-32)y < \frac{1}{2}$ não seria satisfeito. Isso é virtualmente impossível para uma molécula desse tamanho; daí sujeito as essas condições, é fácil obter que a equação diofantina $x + 32y = 66$ tenha apenas duas soluções de inteiros positivos $[x, y] = [34, 1] e [x, y] = [2, 2]$.

Estes são os únicos conjuntos de valores positivos que satisfazem esta equação. Como é improvável que uma molécula deste tamanho contenha 34 átomos de hidrogênio (especialmente contendo apenas 1 átomo de enxofre), esse conjunto pode ser eliminado. Portanto,temos $[x, y] = [2, 2]$ e a fórmula molecular é H_2S_2. Embora se possa substituir esses conjuntos de valores na equação $1,008x + 31,98y = 66,15$ para descobrir qual satisfaz mais de perto essa equação, o método de eliminação acima funciona melhor quando pode ser aplicado. No entanto, na resolução deste problema, podemos proceder de uma forma mais eficiente. A equação $1.008x + 32.065y = 66.146$ pode ser convertida para a equação diofantina $1008x + 32065y = 66146$, que tem infinitas soluções inteiras $[x, y] = [2 + 32065.k, 2 - 1008.k], k \in \mathbb{Z}$. Como $x, y \in \mathbb{N}$ e $x \leqslant 34, y \leqslant 2$, a solução $[x, y] = [2, 2]$ segue imediatamente.

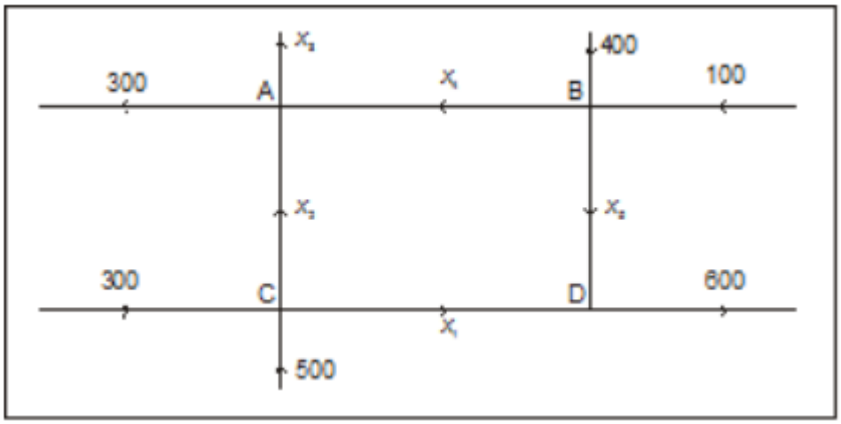
A ideia básica dessas aplicações é que o número de átomos (de um elemento) e o número de moléculas (de uma substância) deve ser um inteiro positivo, e assim ocorre um problema diofantino (que é um problema que leva a uma equação diofantina). Em geral, para ter qualquer tipo de problema diofantino, as incógnitas no problema devem ser inteiras.

Como pudemos observar, no balanceamento de equações químicas, todas as quantidades envolvidas são inteiras, todos os termos são inteiros e, portanto, obtém-se diretamente uma equação diofantina. Já na segunda aplicação, os pesos atômicos e moleculares não são exatamente inteiros, de modo que no início não se obtém realmente uma equação diofantina (já que os coeficientes das variáveis e do termo constante não são inteiros). No entanto, se a condição de (5.9) for satisfeita, pelo menos em um bom grau de probabilidade, a equação obtida primeiro pode ser substituída por uma equação diofantina.

5.5 Fluxo de Tráfego

Exemplo 5.7. O fluxo de Tráfego, em veículos por hora, em várias ruas de sentido único em uma cidade durante um típico começo de tarde é dado pelo diagrama a seguir. Determine os padrões gerais de fluxo de tráfego.

Figura 5.1: Fluxo de Tráfego.



Solução: O sistema gerado pela condição acima é dado por :

Interseção	Fluxo de Chegada	Fluxo de Saída
A	$x_2 + x_4$	$300 + x_3$
B	$400 + 100$	$x_4 + x_5$
C	$300 + 500$	$x_1 + x_2$
D	$x_1 + x_5$	600

como o fluxo total de chegada = fluxo total de saída temos que :

$$x_2 + x_4 + 400 + 100 + 300 + 500 + x_1 + x_5 = 300 + x_3 + x_4 + x_5 + x_1 + x_2 + 600$$

$$1300 = x_3 + 900$$

$$x_3 = 400$$

para uma solução simultânea, expressamos as condições acima

$$\begin{aligned} x_2 - x_3 + x_4 &= 300 \\ x_4 + x_5 &= 500 \\ x_1 + x_2 &= 800 \\ x_1 + x_5 &= 600 \\ x_3 &= 400 \end{aligned}$$

Como x_1, x_2, x_3, x_4, x_5 representa a quantidade de veículos, temos que x_1, x_2, x_3, x_4, x_5 devem ser números inteiros. Isto nos leva a que o sistema gerado acima é um sistema de

equações lineares diofantinas em 5 variáveis. Uma solução de simplificação é obtida da seguinte forma:

$$\begin{aligned} x_1 &= 600 - x_5 \\ x_2 &= 200 + x_5 \\ x_3 &= 400 \\ x_4 &= 500 - x_5 \\ x_5 &= variavel\ livre. \end{aligned}$$

Um fluxo negativo na ramificação de rede corresponde ao fluxo na direção oposta ao modelo mostrado acima, uma vez que as ruas no problema são unidirecionais, portanto nenhuma das variáveis pode ser negativa. Este fato leva a certas limitações para os possíveis valores das variáveis. Por instância $x_5 < 500$ (como x_4 não pode ser negativo), as soluções dependem da escolha de x_5 de 0 a 500 (números inteiros).

5.6 Exercícios com Fatoriais

Nesta seção fazemos a apresentação de alguns problemas que envolvem os conceitos explanados anteriormente nessa dissertação.

Exemplo 5.8. Seja p um primo e n um inteiro positivo. Mostre que o maior expoente $\alpha(n)$ tal que $p^{\alpha(n)}$é $\mid n!$ é dado pela fórmula de Polignac:

$$\alpha(n) = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \dots.$$

Solução: Para $k \geq 1$, os inteiros na sequência $1, 2, 3, \dots, n$ que são divisíveis por p^k são

$$p^k, 2.p^k, 3.p^k, \dots, q.p^k$$

no qual $q = \mid \frac{n}{p^k} \mid$. Portanto, o número de inteiros na sequência $1, 2, 3, \dots, n$ que são divisíveis por p^k é $\mid \frac{n}{p^k} \mid$. Por outro lado, o expoente $\alpha(n)$ da maior potência de p na fatoração em fatores primos de $n!$ é dado por

$$\lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p^2} \rfloor + \lfloor \frac{n}{p^3} \rfloor + \dots + \lfloor \frac{n}{p^r} \rfloor,$$

no qual r é determinado por n a partir de $p^r \leq n \leq p^{r+1}$(por exemplo, o número divisível por p^2 deve ser contado duas vezes, uma em $\lfloor \frac{n}{p} \rfloor$ e uma em $\lfloor \frac{n}{p^2} \rfloor$.

Exemplo 5.9. Mostre que para cada número inteiro positivo n,

$$n! = \prod_{i=1}^{n} mdc\left(1, 2, \dots, \lfloor \frac{n}{i} \rfloor\right).$$

Solução: Se tivermos $\alpha_p(a) = \alpha_p(b)$ para todos os primos p, então, em conclusão, teríamos $a = b$, uma vez que as fatorações de primos seriam as mesmas. Suponha que para este caso $p \leq n$ porque caso contrário, é claro que

$$\alpha_p(n!) = \alpha_p\left(\prod_{i=1}^{n} mdc\left(1, 2, \dots, \lfloor \frac{n}{i} \rfloor\right)\right) = 0.$$

Temos que $\alpha_p(n!) = \sum_{i=1}^{\infty} \left(\lfloor \frac{n}{i} \rfloor \right)$ .E podemos afirmar que é o mesmo que

$$\alpha_p \left(\prod_{i=1}^{n} mdc \left(1, 2, \ldots, \lfloor \frac{n}{i} \rfloor \right) \right).$$

(i) Quando $i \in \{1, 2, \ldots, \lfloor \frac{n}{p} \rfloor\}$ temos pelo menos uma potência de p no $mdc \left(1, 2, \ldots, \lfloor \frac{n}{i} \rfloor \right)$.
Portanto, adicionamos $\lfloor \frac{n}{p} \rfloor$.

(ii) Quando $i \in \{1, 2, \ldots, \lfloor \frac{n}{p^2} \rfloor\}$ temos pelo menos duas potências de p no $mdc \left(1, 2, \ldots, \lfloor \frac{n}{i} \rfloor \right)$.
No entanto, uma vez que precisamos contar a potência de p^2 um total de duas vezes e já foi contado uma vez, basta adicioná-lo uma vez.

Repetindo esse processo, chegamos a

$$\alpha_p \left(\prod_{i=1}^{n} mdc \left(1, 2, \ldots, \lfloor \frac{n}{i} \rfloor \right) \right) = \sum_{i=1}^{\infty} \left(\lfloor \frac{n}{i} \rfloor \right),$$

como desejado.

Exemplo 5.10. Dada a equação $(n-1)! + 1 = n^m$ mostre que se $1 \leqslant n \leqslant 5$, então $(n, m) = (2, 1), (3, 1), (5, 2)$.

Solução:

Tomemos $n \geqslant 6$.

$$(n-1)! + 1 = n^m$$
$$\Leftrightarrow (n-2)! = \frac{n^m - 1}{n-1}$$
$$1 + n + n^2 + \cdots + n^{m-2} + n^{m-1}$$
$$\Leftrightarrow (n-2)! - m =$$
$$(1-1)(n-1)(n^2-1) + \cdots + (n^{m-1} - 1)$$

Como $\frac{n-1}{2}$ são diferentes e para $\leqslant n-2$ então temos que :

$$\frac{n-1}{2} = n \mid (n-2)!$$

Para todo $a, b \in \mathbb{R}, k \geqslant 2, k \in \mathbb{Z}$, temos que:

$$a^k - b^k = (a-b)(a^{k-1}b^0 + a^{k-2}b^1 + \cdots + a^0 b^{k-1})$$

Se k é ímpar, $c = -b$, então:

$$a^k + c^k = (a+c)(a^{k-1}c^0 - a^{k-2}c^1 + \cdots + a^0 c^{k-1})$$

Tomando $a = n$, $b = 1$. Então, $n - 1 \mid n^{k-1}$ para todo $k \geqslant 0, k \in \mathbb{Z}$ porque $n - 1 \mid n^0 - 1 = 1 - 1 = 0$ e $n - 1 \mid n^1 - 1 = n - 1$.

$$n - 1 \mid m, \text{ então } \quad m \geqslant n - 1 \text{ (porque } m > 0) \; e$$

$n^m = (n-1)! + 1 = 1.2 \ldots (n-1) + 1 < (n-1).(n-1) \ldots (n-1) = (n-1)^{n-1} < n^{n-1}$, o que é uma contradição. Portanto temos como solução os pares $(2, 1), (3, 1), (5, 2)$.

Exemplo 5.11. Encontrar todos os pares de inteiros (x, y) que satisfaçam a equação

$$x^2 - y! = 2001.$$

Solução:

Analisando com módulo 7. Quando $y \geq 7; y \equiv 0\,(mod\,7)$ então temos $x^2 \equiv 2001 \equiv -1\ (mod\ 7)$. Portanto, se um x deve satisfazer esta equação, $x^2 \equiv 6\ (mod\ 7)$. Mas, ao analisar a Tabela 5.3 podemos ver que não há soluções para essa equação.

Tabela 5.3: $x^2(mod\ 7)$

x	$x^2\ (mod\ 7)$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Portanto, $y < 7$.

Agora observe que o menor quadrado perfeito maior que 2001 é $2025 = 45^2$, e isso (surpreendentemente) retorna duas soluções válidas: $(x, y) = (45, 4)$ *e* $(x, y) = (-45, 4)$. Isso cobre todos os casos com $y \leq 4$. Se $y = 5$, então $x^2 2 = 2001 + 5! = 2121$, mas esta equação não tem soluções inteiras, pois 2121 é divisível por 3, mas não por 9. Se $y = 6$, então $x^2 = 2001 + 6! = 2721$, que mais uma vez não tem soluções pelos mesmos motivos acima. Portanto, nossas únicas soluções são $(x, y) = (45, 4), (-45, 4)$.

6 Considerações Finais

Esta dissertação não é voltada apenas para alunos do ensino fundamental e médio, mas também para professores, estudantes universitários, participantes de olimpíadas e concursos de matemática e qualquer pessoa que se interesse por essa área de conhecimento e tem como intenção demonstrar a importância e o desenvolvimento da interpretação algébrica das equações diofantinas além de permitir comparar e estabelecer estratégias de pensamento de forma criativa para resolver problemas em outras áreas de conhecimento.

Sentimos a necessidade de ter um material que concentrasse em um mesmo local uma abordagem histórica da evolução da Teoria dos Números desde a antiguidade até a atualidade, por isso, da preocupação com o capítulo "Apresentação - Teoria dos Números".

É surpreendente que Diophantus, que viveu por volta do século III, tenha lidado com a maneira de resolver equações que têm soluções inteiras, sem o conhecimento matemático que temos hoje. Por exemplo, Diophantuss não fazia ideia da existência do número zero ou de números negativos. No entanto, mesmo sem esse conhecimento, ele estabeleceu as bases para as equações diofânticas, que foram abordadas por grandes matemáticos, e também tentamos penetrar na essência desta questão.

Em 1970, o matemático russo Yuri Vladimirovich Matiyasevich [30] provou que não havia uma maneira universal de resolver as equações diofantinas.

Com base neste trabalho, seguindo a orientação das teses já publicadas no PROFMAT, conforme análise feita no Capítulo "Motivação e Perspectiva" devemos aprender o método de resolver equações diofantinas e encontrar todas as soluções de equações diofantinas, não dependendo de um método inapropriado de tentativa e erro que controlamos sem um conhecimento matemático mais profundo. Fica clara a existência de inúmeras maneiras de atingir nosso objetivo, por isso depende da maneira como pensamos e do conhecimento que adquirimos e de como alcançar de maneira mais eficaz.

O tema das equações diofantinas é muito interessante e extenso, por isso, espero que ao propor este tópico em minha dissertação, onde lido com equações diofantinas associadas a funções aritméticas associadas a fatoriais deixar claro que este trabalho não é um conjunto de receitas de ensino prontas, mas contém muitas tarefas e métodos elaborados, convenientes para aplicação direta ou analógica, a partir de questões que raramente estão presentes em nossa literatura.

Eu não me deparei ao trabalhar com fontes literárias que lidam com equações diofantinas que envolvem funções aritméticas uma literatura abrangente sobre o assunto na língua portuguesa. Por isso, tentei processar as informações obtidas e torná-las em um texto coerente para que se torne de fácil leitura o quanto possível.

No capítulo "Funções Aritméticas" nos familiarizamos com algumas das funções aritméticas multiplicativas, apresentamos as suas várias propriedades, que se originaram principalmente do Teorema Básico da Aritmética, além de estabelecermos algumas relações

entre as mesmas. Além disso, acabamos por apresentar no final do capítulo uma série de problemas que envolvem funções Aritméticas.

Baseado no trabalho de Florian Luca [27, 28] no capítulo "Equações diofantinas associadas as funções aritméticas e fatoriais" adentramos o mundo das equações diofantinas que envolviam funções aritméticas de fatoriais examinando e classificando as soluções de certas equações diofantinas envolvendo fatoriais e algumas funções aritméticas bem conhecidas ϕ, a função totiente de Euler, σ a função soma dos divisores e τ. Florian Luca mostra que existe um número finito de soluções para a equação $\dfrac{f(n!)}{m!} = a$, na qual f é uma dessas funções aritméticas e a é um número racional.

Esperamos que os professores possam usar este trabalho como um bom lembrete das equações diofantinas para sua preparação durante as aulas regulares e adicionais principalmente com contextualização histórica sobre a Teoria dos Números. Além disso, os professores podem escolher entre uma grande quantidade de tarefas e exemplos disponibilizadas no capítulo "Transposição Didática" para os alunos, especialmente aqueles bem dotados para a Matemática abrindo assim inúmeras possibilidades para sua aplicação. Obviamente, para um aluno e professor talentosos pode ser uma recomendação e um incentivo para soluções metódicas originais, experimentação adicional e encontrar abordagens metódicas ainda mais eficientes e de qualidade.

Dentre as principais recomendações que podemos referendar com este trabalho podemos destacar :

1. Este trabalho de pesquisa é realizado para servir de motivação para os leitores, para continuar a trabalhar no campo da pesquisa, e por conseguinte poder dar contribuições no campo da Matemática.

2. As equações diofantinas são tão importantes que desde situações mais simples até mesmo as mais complexas do nosso dia a dia podem ser vistas como uma equação diofantina. Então encorajo o leitor a continuar pesquisando mais sobre essas equações diofantinas.

3. Para os estudantes de Matemática, deve ser de muita importância, o estudo de assuntos relacionados com a Teoria Elementar dos Números.

4. À nossa frente ainda está uma grande incógnita na forma de equações diofantinas quadráticas e do último Teorema de Fermat. Este trabalho pode, portanto, servir como um "trampolim"para o estudo de equações diofantinas mais complexas.

5. Novas aplicações atraentes da Teoria dos Números incluem criptografia, teoria de codificação e geração de números aleatórios, as quais fazem uso de equações diofantinas e com a evolução da capacidade de processamento dos computadores, esses campos se desenvolvem muito rapidamente, com sua importância aumentando continuamente.

Para concluir nosso trabalho, deixamos alguns questionamentos interessantes, como:

1. Dada a equação $\dfrac{f(n!)}{m!} = a$ na qual $a \in \mathbb{Q}$ quais outras funções aritméticas f de um fatorial poderá apresentar um conjunto de soluções?

2. Equações diofantinas desse modelo estudado podem auxiliar a elaborar provas ou demonstrações para problemas ainda não resolvidos na Teoria dos Números?

3. Como até o momento o maior número de resultados do problema de Brocard-Ramanujan $n! + 1 = m^2$ e suas variações foi obtido a partir da utilização da conjectura abc ou de suas variantes qual outras formas de se provar os resultados sem a ajuda dessa suposição?

Referências

[1] Andreescu,T. Andrica,D. Cucurezeanu, I.: An Introduction to Diophantine Equations. A Problem-Based Approach. Birkhäuser, Basel, 2010.

[2] Andrews,G.E.: The Theory of Partitions, Cambridge University Press (1998)

[3] Andrews, G. E.: Number Theory (1st Dover edition)- W. B. Saunders Company, Philadelphia, 1971.

[4] Aragão, M. J.: História da Matemática, Rio de Janeiro, Interciência, 2009.

[5] Babai, L.,Spencer Joel, U. P. : Notices of the AMS 45(1998).

[6] Bashmakova, I.G.: Diophantus and Diophantine Equations . The Dolciani Mathematical Expositions 20. The Mathematical Association of America, Washington, 1997.

[7] Bennett, M. A. et al.: Explicit bounds for primes in arithmetic progressions, 2018.

[8] Berndt, B.C. Galway, W.F.: The BrocardRamanujan diophantine equation $n! + 1 = m^2$, The Ramanujan Journal, 2000, 4.

[9] Boyer, C. B. : História da Matemática Tradução: Elza F. Gomide. São Paulo Editora Edgard Blücher, 1974.

[10] Brocard,H. : Question 166, Nouv. Corresp. Math. 2 (1876).

[11] Brocard,H. : Question 1532, Nouv. Ann. Math. 4 (1885)

[12] Burton, D. M.: Elementary Number Theory. Fifth edition. The McGraw-Hill Companies, Inc., 2002.

[13] Carella, N. A. : Sum Of Divisors Function Inequality disponível em https://arxiv.org/pdf/0912.1866.pdf -último acesso em 20/08/2020

[14] Cerdá, S. : The Brocard - Ramanjujam's Diophantine Equation $n! + 1 = m^2$ disponível https://arxiv.org/abs/1504.06694 - útimo acesso em 20/08/2020

[15] Dabrowski ,A. : On the Diophantine equation $x! + A = y^2$. Nieuw Arch. Wisk. (4) 14,No. 3 (1996), s. 321-324

[16] Dufour, B. and O. Kihel, O. : "The Brocard-Ramanujan Diophantine equation", Int. Math. J., 5,6, pp. 577-580, 2004

[17] Erdõs,P. ,Graham,S. W , A. Ivíc, A. and C. Pomerance,C.: On the number of divisors of n!, Chapter in Analytic Number Theory, Springer, 1996, 337-355.

[18] Gérardin A : Contribution a l'etude de l'a equation $1.2.3.4\ldots z+1=y^2$, Nouv. Ann. Math, 1906, 4-6

[19] Gupta,H. : On a Brocard Ramanujan problem, Math. Student 3 (1935)

[20] Hardy,G. H.: A Mathematician's Apology, Cambridge University Press , 1940.

[21] Heath, S. T. L. : Diophantus of Alexandria: A Study in the History of Greek Algebra. New York: Dover Publications, Inc., 1964.

[22] Hildebrand,A. J. : Introduction to Analytic Number Theory, Department of Mathematics,University od Illionis, 2013.

[23] Hoffman,P.: The man who only loved numbers: the story of Paul Erdös and the search for mathematical truth, [sn], 1998.

[24] Jakimczuk,R. : Logarithm of the exponents in the prime factorization of the factorial, International Mathematical Forum, 12 (2017), no. 13, 643-649.

[25] Klaska,J. : Partitions, compositions and divisibility, Ann. Univ. Mariae Curie - Sklodovska,Sect. A 49 (1995), 117-125.

[26] Klein, J. : Greek Mathematical Thought and the Origin of Algebra. Trans. Eva Brann. Cambridge, Massachusetts: The M.I.T. Press, 1968.

[27] Luca,F. : Equations involving arithmetic functions of factorials, Divulg. Mat. 8 (2000), 15-23.

[28] Luca,F. : The diophantine equation P(x) = n! and a result of M. Overholt, Glas. Mat. Ser. III 37(57)(2002), 269-273.

[29] Masser, D. W.: Open problems, in Chen, W. W. L., Proceedings of the Symposium on Analytic Number Theory (1985), London: Imperial College.

[30] Matiyasevich,Y. V. : Hilbert's 10th Problem, Cambridge, MIT Press (1993)

[31] Niven,I. Zuckerman,H. S. Montgomery,H. L. : An Introduction to the Theory of Number, 5th edition,Wiley 1991.

[32] Najera, J.: Number Theory — History and Overview, disponível em *https* : *//towardsdatascience.com/number − theory − history − overview* − 8*cd*0*c*40*d*0*f*01, último acesso 20 de agosto de 2020.

[33] Oesterlé, J.: Nouvelles approches du théoréme de Fermat, Astérisque, Séminaire Bourbaki, (1988) 694(161): 165-186.

[34] Overholt,M. : The Diophantine Equation $n!+1=m^2$, Bulletin London Math. Soc., 25 (1993), pp. 104-113

[35] Pakapongpun,A.: The Relation among Euler's Phi Function, Tau Function and sigma Function, International Journal of Pure and Applied Mathematics Volume 118 No. 3

[36] Pathria,A. and Gilbert, W.J. : Linear Diophantine Equations, disponível em http://www.math.uwaterloo.ca/ wgilbert/Research/GilbertPathria.pdf último acesso 20 de agosto de 2020.

[37] PROFMAT. Dissertações do PROFMAT. disponível em $https : //www.profmat - sbm.org.br/dissertacoes/?polo = \&titulo = diofantina\&aluno =$- último Acesso em 15 de agosto de 2020.

[38] Ramanujan,S. : Collected Papers, Chelsea, New York, 1962,4

[39] Ramanujan, S. : Question 469. J. Indian Math. Soc. 5 (1913), 59.

[40] Rosen,K. H.: Elementary Number Theory and its Applications, 5th edition, Pearson/Addison-Wesley, 0-321-23707-2

[41] Rosser,B. : Aproximate formulas for some functions of prime numbers, Illinois J. of Math. 6 (1962), 64-94.

[42] Rosser,B. :The n-th prime is greater than n log n, Proc. Lond. Math. Soc. (2) 45 (1939), 21-44.

[43] Strayer, J. K. : Elementary Number Theory, Waveland Press, Inc., Illinois (2002)

[44] Vinogradov,I. M. : Fundamentals of number theory, Nauka, Moscow (1972)

A Dissertações PROFMAT- Equações Diofantinas

Tabela A.1: Dissertações - Equações Diofantinas

Num.	**Defesa**	**Autor**	**Título**	**Instituição**
1	14/02/20	GONÇALVES, E. B.	Um breve estudo sobre equações diofantinas	UFTM
2	13/11/19	SILVA, A. L. A. D	Equações Diofantinas Lineares com n variáveis e aplicação em sala de aula utilizando o Geogebra	UEFS
3	22/10/19	PERRI, P.V. S.	Equações Diofantinas Lineares no Ensino Médio por meio de Trajetórias Hipotéticas de Aprendizagem	IFSP
4	26/09/19	SOUSA, E.M.R	Equações Diofantinas Lineares :uma abordagem para o Ensino Médio utilizando Jogo Matemático	UFERSA
5	30/08/19	SILVA, D. A.	Equações Diofantinas Lineares :um estudo com alunos da 1ª Série do Ensino Médio	UESPI
6	31/07/19	KIECKHOEFEL, D. E. N.	Equações diofantinas Lineares:entre o Formalismo do Ensino Superior e a Sala de Aula da Escola Básica	UDESC
7	26/04/19	SILVA, A. C.	As Equações Diofantinas Lineares no currículo da Educação Básica	UEPG
8	26/04/19	FERREIRA, A .A.L.	Equações Diofantinas Lineares	UECE
9	22/04/19	MATOS, F. A.	Uma abordagem para a difusão das Equações Diofantinas Lineares e Quadráticas	UFAM
10	16/04/19	SILVA, Y. F.	Equações Diofantinas	USP
11	28/12/18	SILVA. R. G.	Congruências e Equações Diofantinas: Algumas Aplicações	UEPB

12	31/08/18	VOELZ. M. E.	Utilização dos Métodos de Vieta Jumping e Descida Infinita na solução de Equações Diofantinas e Problemas envolvendo Divisibilidade	UTFPR
13	07/05/18	VIEIRA. B. M.	Equações Diofantinas: Uma proposta didática para o 9º ano do Ensino Fundamental	UFT
14	26/04/18	MAIA, L. F.	Equações Diofantinas	UFPA
15	25/04/18	OLIVEIRA, A.F.F.P.	Equações Diofantinas Lineares : uma proposta para as séries finais do Ensino Fundamental	UFRRJ
16	21/02/18	SOUZA, L.B.	Aproximações Diofantinas e a Teoria das Frações Contínuas	IMPA
17	20/12/17	ALVES, L. F.	Aplicações de Equações Diofantinas e um passeio pelo Último Teorema de Fermat	UFG
18	04/05/17	BARROS. E. F.	Equações Diofantinas Não Lineares:uma proposta didática para resolução de problemas	UFAL
19	15/02/17	DEUS, N. S. P.	Equações Diofantinas Lineares e o GPS:nova conexão curricular	UFBA
20	24/08/16	SILVA NETO, A.	Convite às Equações Diofantinas: uma abordagem para Educação Básica	UFRR
21	15/04/16	MARQUES, B. A.	Equações Diofantinas Lineares e Equação de Pell: uma abordagem via Frações Contínuas	UFSJ
22	27/10/15	PEREIRA JÚNIOR, J.	Frações Contínuas e Equações Diofantinas Lineares e Não-Lineares	UFMT
23	26/08/15	ANJOS, A. A.	Equações Diofantinas: Sequência Didática e o Método da Descida Infinita de Fermat	UECE
24	30/03/15	FREITAS, C. W. A.	Equações Diofantinas	UFC
25	13/03/15	CAMPOS, A.	Equações Diofantinas Lineares: possibilidades didáticas usando a Resolução de Problemas	UFSM
26	12/11/14	PAULA, J. C. C.	Tópicos de Aritmética: Equações Diofantinas	UFPR
27	05/06/14	RIBEIRO, R.	Equações Diofantinas :Uma abordagem para o Ensino Médio	UNB

28	29/04/14	LUZ, F. P.	O uso de Equações Diofantinas Lineares na Resolução de Problemas de Preparação Olímpica	UFPI
29	26/04/14	NASCIMENTO, N. M.	Equações Diofantinas e o Método das Secantes e Tangentes de Fermat	UFC
30	12/04/14	SAVÓIS, J. N.	Método para resolver Equações Diofantinas com coeficientes no conjunto dos Números Racionais	FURG
31	09/04/14	LEITE, K. G.	Equação Diofantina Linear : aplicações no Ensino Médio	UNIFAP
32	13/03/14	SALES, M. M.	Resolução de Problemas de Equações Diofantinas	UECE
33	24/02/14	VANSAN, A. H.	Equações Diofantinas: Um Projeto para a Sala de Aula e o uso do Geogebra	UEM
34	15/04/13	CAMPOS, G. E. M.	Equações Diofantinas Lineares	UFMT
35	15/04/13	MELO, F. D.	Uso das Matrizes na Parametrização das soluções de Euqações Diofantinas Lineares	UFERSA
36	12/04/13	SANTOS, P. S. A.	Congruência e Equações Diofantinas: uma proposta para o Ensino Básico	UFAL
37	12/04/13	DA SILVA, A. V.	Uso das Equações Diofantinas no Ensino Fundamental	UFAL
38	01/03/13	BORGES, F. V. A.	Equações Diofantinas Lineares em duas incógnitas e suas aplicações	UFG
39	01/03/13	RIOS, D. G.	Equações Diofantinas Lineares na Educação Básica	UFSJ

Fonte: Adaptado pelo Autor do site do PROFMAT(2020).