UNIVERSIDADE FEDERAL RURAL DO SEMIÁRIDO

PROREITORIA DE PESQUISA E PÓS-GRADUAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

ODAIR JOSÉ DE FREITAS

O MÉTODO DAS TERMINAÇÕES CARACTERÍSTICAS NA IDENTIFICAÇÃO DE NÚMEROS QUADRADOS PERFEITOS

MOSSORÓ-RN

2018

ODAIR JOSÉ DE FREITAS

O MÉTODO DAS TERMINAÇÕES CARACTERÍSTICAS NA IDENTIFICAÇÃO DE NÚMEROS QUADRADOS PERFEITOS

Dissertação apresentada à Universidade Federal Rural do Semiárido – UFERSA, campus Mossoró para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Walter Martins Rodrigues

MOSSORÓ-RN

2018

F862m Freitas, Odair José de.
O método das terminações características na identificação de números quadrados perfeitos / Odair José de Freitas. - 2018.
158 f. : il.

Orientador: Walter Martins Rodrigues.
Dissertação (Mestrado) - Universidade Federal Rural do Semi-árido, Programa de Pós-graduação em Matemática, 2018.

1. Números quadrados. 2. Método de identificação. 3. Congruência modular. 4. Equação Diofantina. 5. Terminação característica. I. Rodrigues, Walter Martins, orient. II. Título.

ODAIR JOSÉ DE FREITAS

O MÉTODO DAS TERMINAÇÕES CARACTERÍSTICAS NA IDENTIFICAÇÃO DE NÚMEROS QUADRADOS PERFEITOS

Dissertação apresentada a Universidade Federal Rural do Semiárido – UFERSA, Campus Mossoró para obtenção do título de Mestre em Matemática.

APROVADA EM: 08 / 06 / 2018

BANCA EXAMINADORA

Dr. WALTER MARTINS RODRIGUES - UFERSA

Presidente

Dr. ANTÔNIO GOMES NUNES - UFERSA

Membro interno

Dr. ANTÔNIO RONALDO GOMES GARCIA – UFERSA

Membro interno

MOSSORÓ/RN, 2018

Dedicatórias

Aos meus pais que não mediram esforços para que eu tivesse a melhor educação possível, dentro das suas humildes condições nos mais variados aspectos. Em especial, à minha mãe Maria de Fátima Freitas de Andrade que soube reconhecer a minha vocação para os estudos matemáticos, deixando claro que faria o que fosse necessário para que eu sempre frequentasse a escola. Em particular, ao meu pai, Niltaci Elias de Andrade que infelizmente não está mais entre a gente, porém, ficaria muito orgulhoso em saber que seu filho se tornou um homem de verdade e nunca o decepcionou, pelo contrário, absorveu praticamente todas as suas lições como a importância do trabalho honesto que fizeram de mim quem eu realmente sou.

Aos meus irmãos Onailson Elias de Freitas, Onailda Maria de Freitas e Uberlândia Maria de Freitas que sempre foram muito compreensivos comigo, apesar de existir certo distanciamento, mas esse foi o preço (alto) necessário para que eu pudesse conhecer a Matemática do modo como desejava e assim poder ajudá-los futuramente, dentro do possível. Infelizmente, não puderam se fazer presente em alguns dos momentos mais importantes da minha vida como na conclusão da minha graduação, porém, devo reconhecer que não foi culpa deles, na verdade, acabei optando pelo isolamento. Mas, gostaria que nesse momento, as coisas fossem diferentes.

A todos os meus alunos dos três níveis de ensino pela confiança de poder colaborar com a sua educação matemática de forma tão intensa. O meu trabalho como **professor particular** foi fundamental para tornar a minha base matemática extremamente sólida, permitindo mergulhar em projetos mais ousados, fazendo dessa jornada uma espécie de exceção, por isso mesmo, o meu orgulho pessoal por não temer o desconhecido que me desafia constantemente. Que Deus me conceda **saúde, paz e energia** para continuar com a minha missão, disseminar meu conhecimento matemático.

Agradecimentos

A Deus pela tua infinita misericórdia, sem a qual seríamos consumidos.

À minha família pelo apoio incondicional, sem o qual não teria conseguido.

À minha esposa e filhos pela paciência, compreensão e muito sacrifício.

Aos amigos pelas diversas palavras de apoio, sem as quais teria desistido.

À Universidade Federal Rural do Semiárido por essa incrível oportunidade.

Aos meus professores pelos ensinamentos que ficarão para sempre comigo.

Aos amigos do Mestrado por toda a paciência, gentileza e aprendizado.

Ao meu grande amigo **Sandro Moreti**, o primeiro a conhecer esse projeto.

Ao meu grande amigo **Joacir Pires** por todas as nossas belas conversas.

Ao meu grande amigo **Francisco Vidal** pelo seu exemplo de superação.

Ao meu professor da graduação, Doutor **João de Deus Lima dos santos.**

Ao meu professor Doutor **Walter Martins Rodrigues** pela sua competência.

Aos meus alunos de todos os níveis com os quais aprendi a arte de ensinar.

Resumo

O principal objetivo deste trabalho de pesquisa consiste na criação de uma nova ferramenta algébrica denominada de o Método das Terminações Características, capaz de auxiliar tanto na identificação de números quadrados perfeitos quanto no cálculo das aproximações de suas raízes quadradas, apesar dessa não ser a nossa maior prioridade, devido ao leque de métodos numéricos e eficientes na sua grande maioria, aos quais se pode recorrer. O trabalho partiu do estudo da sequência dos números quadrados**,** visando a sua devida caracterização, visto tratar-se de uma progressão aritmética de segunda ordem, incluindo a determinação da sua Densidade que concluiremos ser nula e indispensável para se justificar a criação do Método.

Tarefas que devem ser cumpridas, evitando-se a espinhosa busca pela sua decomposição em fatores primos, tendo-se em vista os inconvenientes computacionais diretamente associados como as divisões por números primos consecutivos. Há um aspecto fundamental para a compreensão do texto como um todo: O fato de haver uma grande preocupação em direcionar toda a análise para a dimensão discreta do problema, transportando as discussões mais relevantes para o conjunto dos inteiros positivos. Serão explorados ainda os principais métodos à nossa disposição, supostamente capazes de resolver ambos os problemas mencionados com a precisão que se desejar, dentro de condições específicas que em última análise comprometem a sua eficácia, a exemplo das Tentativas e Erros, apesar do seu inegável potencial pedagógico.

Palavras Chaves: Número Quadrado, Terminação Característica, Congruência Modular, Equação Diofantina, Fatoração Primária, Método de Identificação.

Abstract

The main objective of this research is the creation of a new algebraic tool called the Characteristic Terminations Method, capable of assisting both the identification of perfect square numbers and the calculation of the approximations of its square roots, although this is not our greatest priority, due to the range of numerical and efficient methods that can be used for the most part. The work started from the study of the sequence of the square numbers, aiming at its proper characterization, since it is a second order arithmetic progression, including the determination of its Density that we will conclude to be null and necessary to justify the creation of the Method.

Tasks that must be fulfilled, avoiding the thorny search for its decomposition into prime factors, taking into account the computational drawbacks directly associated as the divisions by consecutive prime numbers. There is a fundamental aspect to understanding the text as a whole: The fact that there is a great concern in directing the entire analysis to the discrete dimension of the problem, transporting the most relevant discussions to the set of positive integers. We will also explore the main methods at our disposal, supposedly capable of solving both mentioned problems with the desired precision, under specific conditions that ultimately compromise its effectiveness, for example the Tries and Errors, despite its undeniable potential pedagogical.

Key Words: Square Number, Characteristic Termination, Modular Congruence, Diophantine Equation, Primary Factor, Identification Method.

Lista de tabelas

Lista de Figuras

Lista de abreviaturas

MTC: Método das Terminações Características.

PTC: Presença de Terminação Característica.

TCI: Terminação Característica ímpar.

TCP: Terminação Característica Par.

PPA: Paridade da Parcela Adjacente.

ADP: Número Adjacente Par.

ADI: Número Adjacente Ímpar.

FAC: Forma Algébrica Compatível.

FAI: Forma Algébrica Incompatível.

EDF: Equação Diofantina Fundamental.

DRQ: Determinação da Raiz Quadrada.

TCE: Tabela das Classes de Equivalência.

TQP: Terminação da Quarta Parte.

DFP: Decomposição em Fatores Primos.

TFA: Teorema Fundamental da Aritmética.

SNQ: Sequência dos Números Quadrados.

NDE: Número Decimal Exato.

DPS: Dízima Periódica Simples.

DPC: Dízima Periódica Composta.

RCM: Relação de Congruência Modular.

ADE: Algoritmo da Divisão Euclidiana.

MDC: Máximo Divisor Comum.

MMC: Mínimo Múltiplo Comum.

Sumário

Capítulo I

Capítulo II

Capítulo III

Capítulo IV

Capítulo V

Capítulo VI

Capítulo VII

Capítulo VIII

Capítulo IX

Capítulo X

Introdução

A teoria dos números pode ser definida, em linhas gerais como a área da Matemática, cujo principal objetivo é descobrir e estabelecer as profundas relações que os números de diferentes tipos guardam entre si, especialmente os inteiros. O interesse pelos números e suas propriedades acompanham o desenvolvimento das mais diversas civilizações de que temos informações, desde os momentos iniciais de seus desenvolvimentos. Na obra “Os elementos de Euclides” já aparecem os conceitos de números pares, ímpares, assim como números primos e compostos.

Vários outros resultados importantes aparecem na obra mencionada acima como a demonstração da existência de uma **infinidade de números primos**, considerada uma das mais elegantes, dada a simplicidade dos seus argumentos, uma verdadeira obra de arte. O mesmo vale para os conceitos de MMC e MDC que permeiam toda a Teoria dos Números e atribui-se a ele o mérito pela fundação da **Escola de Alexandria**, sistematizando os conhecimentos esparsos que os gregos tinham da Matemática.

Embora os números naturais constituam, em certo sentido, o sistema mais elementar, é certo que o estudo de suas propriedades tem exercido grande fascínio na mente humana, desde as mais remotas épocas, desafiando inúmeras gerações de matemáticos e leigos, que apreciam seus enunciados simples e intrigantes. Podemos destacar quatro grandes áreas de pesquisa nesse campo: Teoria Elementar**,** Teoria Algébrica**,** Teoria Geométrica e Teoria Analítica dos Números**.**

Os gregos antigos foram os primeiros a discutir o conceito de número, e um paradigma importante na matemática grega – pelo menos desde os templos de Platão (429 – 348 A.C) até Diofanto (segunda metade do século III) – era o seguinte: O conceito de número era restrito aos inteiros positivos; ou seja, para os gregos, o conceito de número referia-se a magnitudes descontínuas, fato que teve importantes consequências na História da Matemática com destaque muito especial para a Crise dos Incomensuráveis que abalou a sociedade pitagórica.

O filósofo e matemático grego Pitágoras (570 – 500 A.C) fundou na atual Itália uma escola conhecida como a **Ordem Pitagórica** para transmitir suas ideias às classes mais privilegiadas que eram iniciados nos seus mais profundos segredos. Nessa escola também se podia aprender **Música, Política, Arte, Religião e Filosofia.** Com eles, surgiu a primeira divisão dos números em pares e ímpares, depois primos e compostos. Vale mencionar ainda que mesmo após a morte de Pitágoras, essa ordem cercada de misticismo, continuou ativa por mais de quatro séculos o que representa um fato surpreendente, devido às condições históricas extremamente desfavoráveis a sua manutenção.

A necessidade de contar objetos deu origem à ideia de número natural e de certa forma, todas as grandes civilizações que criaram algum tipo de linguagem escrita inventaram símbolos para os diferentes números e passaram a operar com eles, decorrido muito tempo para isso. Num primeiro estágio, não havia um conceito propriamente dito de número, de modo que para os povos antigos, número na sua língua era uma palavra como outra qualquer. Assim, utilizavam palavras diferentes para fazer referência a “três homens” ou “três pedras”.

Num estágio mais avançado, os números foram separados dos objetos e se tornaram entes abstratos o que representou um grande salto evolutivo, a partir deste momento, difícil de precisar com maior exatidão, começou a serem criados os chamados sistemas numéricos. Quando se tornou necessário efetuar contagens mais extensas, houve a necessidade de sistematizar tal processo, de modo que cada uma das grandes civilizações da antiguidade elaborou um **sistema de numeração**. De modo geral, isso foi feito dispondo as quantidades em grupos convenientes (agrupamento), sendo a ordem de grandeza destes grupos determinada exatamente por esse processo de correspondência fundamental.

Sobre o significado de número para o qual não temos uma definição precisa, visto que se trata de um conceito abstrato, valem mencionar as duas operações lógicas fundamentais que efetivamente colaboram para o seu pleno desenvolvimento: A Classificação e a Seriação. Na obra **Os fundamentos teóricos do pensamento humano (2.010)**, encontramos as seguintes definições para essas duas operações:

Classificação: Classificar é “juntar” por semelhança e “separar” por diferenças.
A pertinência e a inclusão são duas relações associadas à classificação (Pag.31).

Seriação: Seriar é ordenar diferenças, estabelecer relações entre elementos que diferem em certos aspectos (Pag. 33).

Isto consiste basicamente na escolha de um número n que admita um sentido representativo para a comunidade como base de tal sistema. No antigo Egito, vale destacar a predominância de dois sistemas numéricos, o de base 10 para auxiliar o processo de contagem e o de base 2, notadamente na multiplicação e adição. Na babilônia, desenvolveu-se o sistema de base 60 (sexagesimal) e o **Princípio da Escrita Posicional**. Aliás, este sistema muito utilizado, resistiu ao tempo, chegando até nós (mundo ocidental) na forma das unidades para medir tempo e ângulo. Na Grécia antiga, era usado um sistema de representação alfabética, na índia também se utilizava um sistema decimal bem desenvolvido.

Não podemos deixar de mencionar a importância histórica que **o cálculo de áreas**, ainda no Egito antigo, desempenhou no progresso da Matemática em geral, permitindo o surgimento gradual de conceitos fundamentais como o de número irracional. Vale mencionar ainda a figura dos **estiradores de cordas** que refaziam as medidas de terras todos os anos, devido às cheias do rio Nilo, movidos por questões administrativas relacionadas, dentre outras, à cobrança de impostos.

A imensa quantidade de objetos a serem contados, as atividades práticas e o espírito indagador do homem determinou a noção de conjunto numérico sem limites (infinito): Desse modo, o conjunto dos números naturais passou a ser considerado como não limitado superiormente, dando origem a discussões filosóficas que perduram até os dias atuais, desafiando a mente humana como nunca (Aritmética Transfinita). Para as medidas, o número racional se tornou uma necessidade que provocaria uma verdadeira revolução. O posterior desenvolvimento do conceito de número ocorreu principalmente devido às demandas intrínsecas à Matemática e vinculadas notadamente à resolução de equações algébricas.

Problema de Pesquisa

Como proceder para verificarmos, sem apelar para a sua fatoração primária, se um número inteiro positivo qualquer pertence à sequência dos quadrados perfeitos e ainda como calculamos a sua raiz quadrada na hipótese de uma resposta positiva?

Mesmo uma reflexão superficial sobre essa Relação de Pertinência revela a existência de um genuíno Problema Matemático**.** Isso nos coloca frente a frente com a operação de radiciação que desempenha o importante papel de inversa da potenciação e figura como uma das mais complexas da Álgebra em nível elementar.

Existe uma estratégia das mais rudimentares, utilizada numa abordagem inicial ao problema, conhecida como o **Método da Falsa Posição** ou Aproximações Sucessivas que não oferece sequer um ponto de partida, caracterizado pela realização de várias multiplicações com fatores iguais que devem cessar apenas na hipótese de atingirem o número fornecido ou obtermos o resultado procurado com a aproximação desejada (Critério de Parada). Aliás, seria mais eficiente se levasse em conta que um número quadrado e sua raiz têm a mesma paridade ($X^2 \pm X = 2M$).

Não podemos deixar de mencionar a clássica Relação de Ordem entre as Médias Aritmética, Geométrica e Harmônica como uma alternativa às aproximações sucessivas, devido à sua rápida Convergência, mas que não leva em conta um importante fato sobre a distribuição dos números quadrados**:** Eles constituem uma "minoria" entre os Naturais, pois apresentam uma Densidade nula**:** inf. {A(n) / n} = 0.

Agora, a ferramenta mais utilizada nesse contexto, reside na busca pela **Decomposição em Fatores Primos**, sendo esta a representação multiplicativa mais eficiente dos números Inteiros que é única pelo Teorema Fundamental da Aritmética. Ela pode ser obtida, dentre outras, através de múltiplas divisões por primos consecutivos, cuja quantidade é limitada pela raiz quadrada do número em questão.

Exigindo assim um Repertório de Primos que cresce muito rápido quando se mergulha nos Naturais, sendo este um dos seus maiores inconvenientes**.** Por isso, encontrar essa fatoração, também conhecida como forma padrão representa outro Problema ainda mais complicado dos dias atuais, notadamente na Ciência da Computação que ocupa um papel central na Moderna Teoria dos Números.

As dificuldades operacionais podem ser avaliadas pelo total de números primos que não superam o inteiro mais próximo, porém, não superior à raiz quadrada do número cuja decomposição deseja-se conhecer, já que nos indicará o número máximo de divisões, caso estejamos na presença de um primo. Ela mostra que temos um número quadrado se, e somente se, essa fatoração exibir somente expoentes pares.

De fato: $\boldsymbol{x = {p_1}^{q_1}.\ {p_2}^{q_2} \ldots\ {p_n}^{q_n} \iff x^2 = {p_1}^{2q_1}.{p_2}^{2q_2} \ldots, se\ x \in \mathbb{Z}.}$

Vale lembrar que os primos também formam uma sequência infinita crescente e apresentam apenas dois divisores positivos, mas sem uma fórmula simples para o seu termo geral. Sabemos que nenhuma Função Algébrica Racional (Boyer, 1996) é capaz de gerar exclusivamente números primos, cuja distribuição mostra-se extremamente complexa, figurando como um dos maiores desafios nesse contexto.

Assim, a possível presença de um primo que representa o pior dos cenários não deve causar impacto operacional relevante, capaz de comprometer o Método das Terminações Características**.** No que diz respeito ao cálculo de raízes quadradas, tomaremos como referência uma propriedade dos números Reais, segundo a qual podemos sempre obter aproximações racionais de números irracionais e vice-versa, sendo a mesma fundamental para a geração dessas aproximações, visto garantir a existência das mesmas, colocando-nos de encontro à operação de radiciação, que é das mais complexas entre as elementares notadamente na dimensão sua numérica.

Lembramos ainda que ela desempenhe o importante papel de operação inversa da Potenciação. O Método que procuramos desenvolver deve ser capaz de distinguir algebricamente quadrados de não quadrados, mostrando uma flexibilidade não encontrada em praticamente nenhuma das outras Rotinas que se prestam a essa finalidade; como se percebe no Algoritmo Chinês de Extração da Raiz Quadrada, todos os números Naturais recebem o mesmo tratamento, isso evidencia o que podemos chamar de Rigidez Metodológica que compromete a sua eficiência, pois também não leva em conta o fato de que os quadrados perfeitos são uma "minoria" entre os Naturais, exigindo assim uma espécie de tratamento diferenciado.

Objetivo Principal

Logo, o nosso principal objetivo e desafio consiste em estabelecermos condições mínimas que satisfeitas conjuntamente, viabilizem a construção de uma ferramenta eminentemente algébrica**,** designada de **O Método das Terminações Características** (MTC) com eficácia superior aos mencionados, capaz de resolver:

(1) Identificação de números quadrados perfeitos,
(2) Determinação de suas raízes quadradas.

Além de gerar aproximações decimais para estas com a precisão que desejarmos na hipótese de uma resposta negativa, apesar dessa não ser a nossa maior prioridade, haja vista as diversas ferramentas disponíveis que realizam essa tarefa de forma muito eficiente, conforme mostraremos. Tudo isso, a partir de um **repertório mínimo de quadrados**, formado pelos 10 primeiros termos, adotado para que a verificação da presença de um número quadrado seja efetivada no menor intervalo de tempo possível; conferindo agilidade, eficiência e permitindo a sua adoção nos níveis Fundamental, Médio e Superior de ensino da Matemática.

Referencial Teórico

Levando-se em conta que o Mestrado Profissional em Matemática (PROFMAT) que é coordenado pela Sociedade Brasileira de Matemática (SBM), apoiada pelo Instituto de Matemática Pura e Aplicada (IMPA) tem como um dos seus principais objetivos capacitar professores de matemática que atuam ou pretendem atuar nas escolas públicas da educação básica, achamos extremamente necessário escolher um autor cuja linha de pesquisa tenha como foco temas fundamentais para uma atuação mais efetiva por parte do professor de matemática na educação básica na sua dimensão pública com uma preocupação eminentemente mais pedagógica. Após algumas leituras, adotamos como referência a obra de **Nilson José Machado.**

Nada mais natural do que começar destacando um pouco da sua vida pessoal, formação e atuação profissional, incluindo uma inegável vocação como escritor, cuja qualidade do trabalho não costuma suscitar críticas negativas por parte do público para o qual a mesma está dirigida, noutras palavras, elas têm uma aceitação muito boa entre os educadores brasileiros. Nilson José Machado leciona, desde 1.972 na Universidade de São Paulo, inicialmente no Instituto de Matemática e Estatística, mas a partir de 1.984 muda para a Faculdade de Educação, atuando como livre docente e chefiando o Departamento de Metodologia do Ensino e Educação Comparada. Autor de diversas obras, entre elas: **Epistemologia e Didática** (São Paulo, Cortez, 1996) e **Cidadania para o Futuro** (São Paulo, Cortez, 1997).

Esse texto que tomamos como referência (Seis propostas para o novo milênio) foi publicado na Série **Educação Para Cidadania** do Instituto de Estudos Avançados da Universidade de São Paulo, em outubro de 1.998. Nessa obra, o autor procura abordar uma arquitetura de valores que na sua perspectiva são fundamentais para o sucesso de todo projeto educacional, enquanto política de estado, tudo isso, independente do país em questão. Vejamos quais são os tais princípios: **Cidadania, Profissionalismo, Tolerância, Integridade, Equilíbrio e Pessoalidade**.

De forma extremamente objetiva, ele traz uma discussão sobre cada um desses princípios, entretanto, achamos por bem escolher apenas o mais conveniente aqui, para que assim, possamos aprofundar um pouco a nossa discussão, não significando com isso, acreditar que os demais sejam menos importantes.

Porém, diferentemente de outras áreas da Matemática, acredita-se que para alcançar o sucesso na divulgação de conceitos e resultados especificamente da Teoria dos Números, devemos considerar elementos peculiares, dentre os quais, o **estímulo à curiosidade**, mediante um planejamento capaz de abordar os temas mais relevantes, despertando a atenção do leitor no sentido de que o mesmo deseje conhecer a essência da teoria dos números de uma forma cada vez mais intensa e constante, permitindo um futuro aprofundamento, mesmo sem o auxílio do professor.

Na mesma linha, temos a questão do **espírito investigativo**, fundamental para a construção da Matemática em termos eminentemente históricos. Para isso, deve-se deixar ao menos um questionamento em aberto, evitando a entrega de resultados por completo, passando assim a ideia de que o conhecimento matemático é algo pronto e acabado, quando na verdade, se constitui numa **construção histórica** das mais importantes para a nossa evolução em todos os aspectos. Isso fará com que o aluno incorra sempre em alguma pesquisa, abrindo caminho para que a aprendizagem seja significativa e de fato aconteça, um desafio para os professores.

Agora, o destaque especial vai para a **capacidade de resolver problemas** uma habilidade fundamental nas discussões relativas à educação matemática e que devem ser selecionados com o máximo de cautela: não podem ser muito simples, pois implicará na desistência por parte do aluno, mas também não devem ser muito complicados, ou seja, espera-se que o aluno seja capaz de superar tais problemas combinando seu conhecimento prévio com aqueles que ainda estão sendo adquiridos ou construídos, se assim preferir. Podemos tomar como belo exemplo os conceitos de número par e número ímpar, relativamente às duas operações básicas em cada um dos subconjuntos, devido ao elevado potencial pedagógico. Assim:

> "Deve existir a preocupação de fazer com que a aprendizagem seja vivenciada como uma experiência progressiva, interessante e formativa, apoiada na ação da descoberta, na reflexão e na comunicação". (**Dante**, 2.015. Pag. 333)

Isso porque somos instigados a utilizar a linguagem matemática diariamente, sem falar das diversas aplicações e situações que exigem a utilização deste conhecimento, respeitando obviamente o nível do contexto social em sua dimensão profissional onde as exigências são bem maiores, demandando formação específica como a participação em cursos oferecidos pelas mais diversas instituições espalhadas Brasil a fora, dentre as quais, vale ressaltar o SENAI como uma referência em termos de **educação profissional gratuita** e de qualidade, mesmo não sendo esta a nossa prioridade, dentro da discussão que estamos promovendo, mas convictos de que não haverá prejuízo significativo com relação aos comentários iniciais sobre os pilares que devem fundamentar todos os sistemas de educação.

De fato, diferentes profissionais utilizam diferentes conhecimentos da Matemática para o exercício das suas atividades, entretanto, durante o período escolar, sabemos que eles continuam sendo submetidos praticamente ao mesmo regime, Em outras palavras, não há muita preocupação com a possível identificação da sua **vocação profissional**. Imagina o estrago que isso provoca na maioria das pessoas, submetidas hoje em dia a uma quantidade cada vez maior de informação, sendo que a maioria delas será provavelmente descartada, dependendo da sua profissão.

> "Nos tempos atuais, nenhuma caracterização das Funções da Educação parece mais adequada do que a associação da mesma à formação do cidadão à construção da cidadania. Nos mais variados países e em diferentes contextos, Educação para a Cidadania tornou-se uma bandeira muito fácil de ser empunhado, um princípio, cuja legitimidade não parece inspirar qualquer dúvida. A não ser a que se refere ao próprio significado da expressão educar para a cidadania". (**Machado**, 1.998)

Segundo Machado, o conceito de cidadania ainda está relacionado com a aquisição de direitos, mas se refletirmos um pouco se chega à conclusão de que essa concepção não abarca todo o significado do termo. De fato, no passado, quando se tinham pouquíssimos direitos, éramos escravizados, torturados e humilhados pelas classes mais abastardas e impedidos de ter acesso ao conhecimento formal, acessível apenas aos detentores do poder econômico e aos membros da classe religiosa, ela seria mais pertinente, sem sombra de dúvidas. Mas, sabemos que nos dias atuais, o tecido social é completamente diferente nos mais variados aspectos. Mesmo em países onde os direitos humanos não costumam ser violados, vemos que a necessidade da formação do cidadão consciente felizmente permanece viva.

A capacidade de ter projetos pode ser identificada como a característica mais verdadeiramente humana. A inteligência humana consistiria, precisamente, nesta capacidade de antecipação, de invenção de metas, de criação de possibilidades. Naturalmente, não basta alimentar-se de projetos individuais: carecemos de projetos coletivos, que estimulem as ações individuais, articulando-as na construção do significado de algo maior. Tanto quanto da satisfação das necessidades básicas em sentido biológico ou econômico, necessitamos participar de projetos mais abrangentes, que transcendam nossos limites pessoais e impregnem nossas ações, nossos sonhos, de um futuro melhor, principalmente em termos de justiça social.

A referência direta feita pelo autor com respeito especificamente aos projetos individuais constitui um indício importante da preocupação em valorizar o ser humano, tomando-o como ponto de partida para as ações educativas, ao mesmo tempo em que se busca a valorização da **solidariedade,** da **tolerância**, elementos constituintes da noção de plena cidadania, evidenciando, portanto, um equilíbrio na dupla preocupação de formação pessoal e social. Insistimos em que nada parece mais característico da ideia de Cidadania do que a construção de instrumentos legítimos de articulação entre os projetos individuais e os coletivos.

Tal articulação possibilitará aos indivíduos, em suas ações ordinárias, em casa, no trabalho, ou onde quer que se encontrem a participação ativa no tecido social, assumindo responsabilidades relativamente aos interesses e ao destino de toda a coletividade. Neste sentido, **Educar para a Cidadania** significa prover os indivíduos de instrumentos para a plena realização desta participação motivada e competente, desta simbiose entre interesses pessoais e sociais, nesta disposição para sentir em si as dores do mundo.

O imperativo de conjuminar o **conhecimento dos direitos** com a **vontade de participação** encontra-se diretamente relacionado com a necessidade de ultrapassar o conforto de uma ética apenas da convicção, onde a coerência pessoal encontra-se garantida, mas não conduz a ações efetivas, aportando-se em uma ética da responsabilidade, onde crescemos com o aumento dos riscos e dos encargos assumidos em relação aos diversos contextos sociais.

Ainda nessa atmosfera de reflexão sobre a utilidade da Matemática e justificativas para a sua abordagem no sistema formal de ensino, discussão extremamente fértil, vale incluir um comentário do professor Elon Lages Lima, capaz de orientar os profissionais da educação em todos os níveis de ensino. Ela fornece indícios que nos permitem convencer sobre a presença da matemática no currículo escolar:

> "(...) embora a matemática possa ser cultivada, como um todo coerente, de elevado padrão intelectual, formado por conceitos e proposições de natureza abstrata, sua presença no currículo escolar não se deve apenas ao valor dos seus métodos para a formação mental dos jovens. A importância Social da Matemática provém de que ela fornece modelos para analisar situações da vida real. Assim, por exemplo, conjuntos são o modelo para disciplinar o raciocínio lógico, números naturais são o modelo para contagem e os números Reais são o modelo para a medida; (...)"
>
> .(A matemática do Ensino Médio, Volume 1, Pag. 29).

O texto será dividido em dez capítulos, cada qual abordando um subtema específico e necessário para uma compreensão global tanto do Problema de Pesquisa, quanto da sua respectiva solução. Assim, vejamos resumidamente do que tratará cada um dos capítulos, destacando apenas o essencial, uma tarefa imprescindível para a construção de um texto argumentativo capaz de conquistar a atenção do leitor.

Capítulo I

Aqui exploramos superficialmente a justaposição de dois números quadrados com a mesma quantidade de dígitos (ordem de grandeza) no caso particular de admitirem apenas dois algarismos. O objetivo consiste em verificarmos se tal processo é capaz de gerar números quadrados, exigindo a fixação de um repertório mínimo constituído pelos seus 10 primeiros membros. Como são 36 arranjos no total, vamos intencionalmente recorrer à calculadora, convictos de não haver quaisquer prejuízos em termos de aprendizagem. Na verdade, a sua utilização dever ser incentivada sempre que tal procedimento permitir a obtenção de resultados indispensáveis para a consolidação do método que tentamos desenvolver, gerando economia de tempo.

Após essa análise, concluiremos que somente um dos arranjos **(1.681)** integra os números quadrados, um resultado surpreendente, se levarmos em consideração que todos são de fácil identificação visual, permitindo assim a obtenção de um excelente subconjunto de inteiros que não integram os quadrados perfeitos. A extensão dessa análise pode ser posta em prática sem maiores dificuldades, mas não o faremos com o receio de tornar o texto mais denso do que o realmente necessário. Para o caso em que os números têm quatro dígitos, pode-se mostrar a existência de resultado semelhante, donde encontramos um único arranjo obtido através da justaposição (concatenação) que integra os quadrados: $24.019.801 = 4.901^{2.}$

Capítulo II

Buscamos conhecer com um pouco mais de profundidade a sequência dos números quadrados. Para isso, nada mais natural do que caracterizar a mesma, veremos tratar-se de uma progressão aritmética de segunda ordem. Em seguida, responderemos uma pergunta fundamental nesse contexto: Qual a probabilidade de que um número inteiro positivo escolhido aleatoriamente represente um quadrado perfeito. Com isso, colocamos em prática uma análise elementar sobre a distribuição dos quadrados, a exemplo do que acontece com os primos, sendo estes responsáveis pela geração de problemas muito difíceis na teoria dos números.

O sucesso dessa análise exige a utilização do conceito de operador diferença, associado ao estudo das recorrências lineares, através do qual definimos a ordem de uma progressão. Por fim, concluiremos que tal probabilidade é nula, outro resultado surpreendente, visto que não há um evento impossível associado à pergunta, contrariando o nosso senso comum. Antes, faremos um breve resumo histórico sobre o conceito de probabilidade moldado pelos matemáticos há mais de quatro séculos, mostrando um pouco de toda a complexidade que o circunda. Na verdade, veremos que a teoria matemática das probabilidades está intrinsicamente associada à teoria filosófica das contingências, justificando parte da complexidade.

Capítulo III

Para decidir se um inteiro positivo integra os números quadrados, podemos simplesmente calcular a sua raiz quadrada e observar se ela resulta inteira. Mas, sabemos que essa tarefa pode ser realizada de várias formas, de modo que se faz necessário explorar os principais métodos que permitem a extração de uma raiz quadrada que pode ser associada à posição de um dos seus termos na hipótese do mesmo representar um quadrado. Essa decisão nos coloca frente a frente ao conceito de número irracional, exigindo muita maturidade de ambas as partes (aluno e professor) na sua abordagem. Faremos também um resumo histórico tomando um texto do professor João Bosco Pitombeira de Carvalho como principal referência.

Através da mesma, ficarão evidentes os principais desafios na consolidação desse conceito pelas mais importantes civilizações da antiguidade. Serão analisados ainda os inconvenientes computacionais dos principais métodos para a extração da raiz quadrada com destaque especial para o Método da Falsa Posição, via tentativas e erros pelo seu **elevado potencial pedagógico**. Incluímos aqui a Decomposição em Fatores Primos, já que a mesma tem presença garantida na imensa maioria dos livros didáticos que abordam o problema da raiz quadrada. Mas, devido a sua importância até mesmo prática, essa representação dos inteiros será abordada novamente no próximo capítulo, onde teremos condições de explorar com mais profundidade as diversas aplicações como o cálculo da quantidade de divisores.

A essa altura, somos capazes de convencer o leitor da necessidade de uma nova ferramenta no ataque ao nosso problema central, abrimos caminho assim para o Método das Terminações Características. Ficará evidente que nenhum dos métodos anteriores leva em conta o fato dos números quadrados constituírem uma minoria entre os números naturais (Densidade nula).

Capítulo IV

Sabe-se que se pode identificar um número quadrado perfeito, mediante a sua decomposição nos primos. Mas, o fato é que encontrar essa representação figura nos dias atuais como um dos maiores problemas de todos os tempos na teoria dos números. A procura por métodos determinísticos tem gerado uma explosão de pesquisa, devido à utilização dos números primos na **segurança da informação**, notadamente como suporte para as operações comerciais através da internet, uma tendência que cresce cada vez mais, exigindo atenção por parte do usuário e maiores investimentos das empresas responsáveis pela prestação de tais serviços.

A busca pela fatoração nos primos exige uma quantidade de operações aritméticas que cresce muito rápido, admitindo que tal busca seja feita mediante a divisão por primos consecutivos, limitada pela sua raiz quadrada. Os estudos mostram que para diminuir o tempo de busca, faz-se necessário utilizar conceitos cada vez mais refinados, difíceis de compreender para a maioria das pessoas. Noutras palavras, devemos construir teorias sofisticadas, colocando-nos frente a frente com uma verdadeira avalanche de problemas muito difíceis, mesmo para os especialistas.

Sem dúvidas, tal conhecimento (fatoração) permite responder praticamente qualquer pergunta a respeito de um inteiro, a exemplo da sua quantidade de divisores que será explorando de forma superficial, dada a inegável importância do tema cercado de grandes desafios. Um destes consiste na determinação do menor inteiro positivo que admite certa quantidade de divisores positivos fixada inicialmente. Ficará evidente a complexidade do problema citado, justificando a sua não aparição nos principais textos didáticos e mesmo artigos sobre a teoria elementar dos números.

Capítulo V

A construção do método das terminações características exigirá a utilização de vários resultados associados à teoria das congruências. O que será feito de forma objetiva, destacando os principais conceitos e propriedades dessa relação. Veremos os principais tipos de relações com destaque para as **reflexivas, simétricas e transitivas** que fazem da congruência uma genuína relação de equivalência**,** gerando partições imprescindíveis para o sucesso do método em questão.

A ideia de resíduo quadrático módulo um primo será fundamental para iniciarmos o ataque às equações de congruências quadráticas, assim como o conceito de números relativamente primos, primos entre si ou ainda co-primos. Felizmente, não será necessário nos aprofundar no estudo de tais equações, um fato que torna o método das terminações características acessível, permitindo que o mesmo seja amplamente divulgado em todos os níveis de ensino. Somente um dos diversos teoremas desse campo será adotado, de modo que ele permite entender o porquê da relação de congruência poder ser considerada uma espécie de igualdade.

Capítulo VI

Esse é o ponto onde o método das terminações características ficará determinado em todas as suas etapas. Para isso, tomaremos como ponto de partida o conjunto dos primeiros 25 números quadrados que forneceram pares de números inteiros fundamentais para a consolidação do referido método. Será utilizado o teorema fundamental da relação de equivalência e serão feitas diversas convenções com o objetivo de facilitar a exposição dos principais resultados, evitando repetições e procurando tornar o texto o mais fluente possível. Serão obtidas 22 classes de equivalências, mas concentraremos a nossa atenção numa dessas classes, visto estarmos diante de uma equivalência, de modo que os resultados mais significativos podem ser naturalmente estendidos às demais, facilitando a conclusão do trabalho.

Os principais resultados serão reunidos numa tabela especial que deverá ser consultada sempre que desejarmos aplicar o método. Serão estabelecidos ainda critérios capazes de verificar a eficiência de uma relação particular para a identificação de números quadrados, desde que não haja utilização de outras ferramentas algébricas. Isso ajudará a entender melhor o papel das congruências no contexto geral.

Serão resolvidos diversos problemas que servirão como referência para uma eficiente aplicação do método das terminações características com destaque especial para aquele no qual se procura escrever um inteiro em função do quadrado mais próximo, procedimento corriqueiro em todo o texto. Finalmente, será adotada **a técnica de completar quadrados** que permitirá a evolução do método em questão.

Capítulo VII

Seria muita ingenuidade de nossa parte, colocar todas as congruências num mesmo **patamar de eficiência**. Entretanto, para isso, será adotado um critério capaz de avaliar até que ponto a Relação em questão ajuda na identificação de números quadrados. De fato, veremos que a Relação citada será tanto mais eficiente quanto maior o número de classes residuais “eliminadas” quando a mesma deixa de operar entre os inteiros e passa a atuar exclusivamente entre os números quadrados.

Nesse sentido, será adotada a **porcentagem de classes residuais** incapazes de abrigar números quadrados como principal parâmetro na avaliação da eficiência numérica de uma congruência particular. Assim, concluiremos facilmente que a congruência módulo 100 admite uma eficiência de 78%. De fato, tomando apenas o parâmetro acima como referência, pode-se dizer que as relações do tipo 10^{2n} são as mais eficientes, até porque estamos adotando o sistema de numeração decimal.

Porém, há outro detalhe que precisa ser mencionado: ele diz respeito ao aumento absoluto da quantidade crescente de classes capazes de abrigar números quadrados, representando uma espécie de efeito colateral altamente indesejável. Além disso, são necessários exatos 250 quadrados consecutivos para determinar o conjunto dos arranjos dos três últimos dígitos dos quadrados perfeitos que devido às inevitáveis repetições geram 165 classes de números quadrados. Nesse sentido, se busca generalizar o **conceito de terminação característica** e justificarmos o porquê de adotarmos, dentre outras a relação de congruência módulo 100.

Capítulo VIII

Aplicações avançadas para o método das terminações características. Vale ressaltar que a maioria desses problemas é de minha autoria, sendo essa uma habilidade que vem sendo desenvolvida há bastante tempo, constituindo verdadeiros desafios, alguns dos quais exigindo uma boa dose de criatividade, além de todo o aparato colocado a disposição do leitor até o momento. Um destaque especial para a **concatenação de números quadrados**, dado que tal conceito não aparece nos principais livros didáticos. Além disso, tive o privilégio de abordar boa parte desses desafios em sala de aula, visto que atuo nas séries finais do ensino fundamental.

Capítulo IX

Abordaremos uma nova classe de equações algébricas associadas aos números inteiros que são soma de dois quadrados perfeitos com mesma ordem de grandeza. Mais que isso, esses inteiros coincidem com a concatenação das raízes quadradas. Ficará evidente a complexidade dessas equações que em última análise exigem a decomposição de inteiros da forma $\mathbf{10^{2n} + 1}$, além do teorema que fornece as condições segundo as quais se pode escrever um inteiro positivo como soma de dois quadrados perfeitos, além das diferentes formas de efetuarmos esta expansão.

Capítulo X

Conclusões.

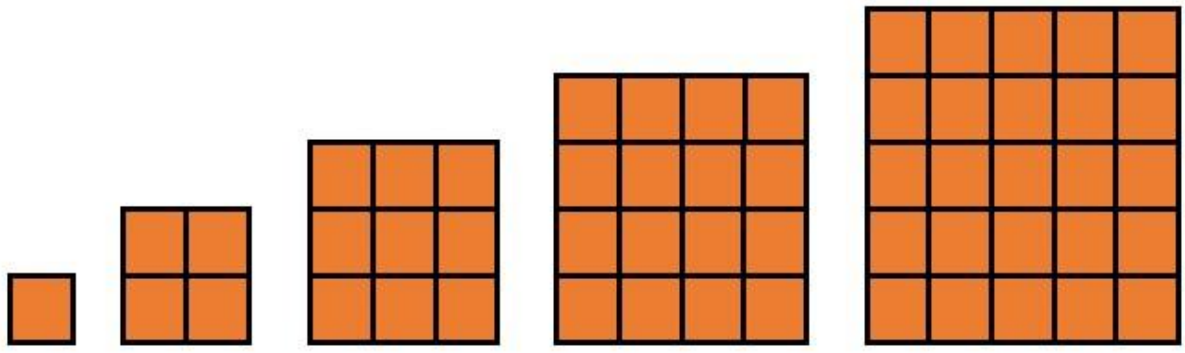
Capítulo I

Números quadrados perfeitos

Os números quadrados perfeitos são definidos como todos aqueles que resultam da multiplicação entre dois inteiros iguais. Eles formam uma sequência infinita crescente que há séculos desperta a atenção dos matemáticos. Um exemplo histórico desse fascínio são os Triplos Pitagóricos Primitivos como (8, 15, 17) cujos termos são primos entre si, admitindo máximo divisor comum igual a um e ainda verificam a relação $(8)^2 + (15)^2 = (17)^2$ associada ao famoso **Teorema de Pitágoras.**

Eles funcionam como uma espécie de Base para os demais, já que são capazes de gerar uma Infinidade Enumerável de outros triplos, através da multiplicação dos seus termos por uma constante não nula. Tudo isso implica na existência, entre os quadrados perfeitos, de infinitos membros que são soma de outros dois. Acrescentamos ainda que entre os cubos, quartas, quintas**,** etc. não existe elementos com essa notável propriedade**.** Veja que sem dúvidas, esse é um resultado fundamental sobre o qual tomamos conhecimento recentemente (1995), já que está diretamente ligado ao **Último Teorema de Fermat** (1.601 - 1.665) cuja verdadeira face mostrou com o tempo, um nível surpreendente de complexidade que desafiou várias gerações de grandes matemáticos incluindo a do próprio Euler.

Uma interpretação geométrica para os números quadrados perfeitos:



https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcStOarTGagqMWzwcREfA7dW1nyjtF-IN6JawoeSjGoQ12l5To2MAA

Euler sem dúvidas tem presença garantida entre os cinco maiores de todos os tempos, na eventual construção de uma lista dos dez que mais contribuíram com o desenvolvimento da Matemática em todos os tempos. Com isso, muitos matemáticos modernos começaram a duvidar se Fermat realmente conseguira, conforme escrevera: “Descobri uma demonstração demasiadamente maravilhosa, porém comprida demais para caber nessa margem” (**Singh**, 2.004).

1.1: Geração de Números Quadrados

Outra maneira curiosa à qual podemos recorrer para a geração de números quadrados perfeitos, consiste na soma de ímpares consecutivos a começar pela unidade, como vemos: 1 + 3 + 5 + 7 + 9 + 11 = 36. Destacamos que pelo menos a princípio, essa informação é útil e eficiente principalmente para o cálculo efetivo dessa soma pelo quadrado do número de parcelas (Raiz) que a constitui; de modo que o caminho inverso exige certamente um pouco mais de trabalho e criatividade.

Devido à existência de números que não se enquadram naquela definição, concluímos que a mesma decompõe (partição) os números naturais em dois importantes subconjuntos disjuntos designados como **quadrados e não quadrados.** Definimos a raiz quadrada de um termo qualquer daquela sequência como o único inteiro positivo que multiplicado por ele mesmo resulta no termo em questão. Esse conceito pode ser facilmente estendido para o Corpo dos Números Racionais. Mas, o grande questionamento que se deve fazer após esses comentários é o seguinte:

1.2: Concatenação de números quadrados

Para facilitar ainda mais a nossa difícil tarefa de identificar números quadrados perfeitos sem apelarmos para a sua Decomposição em Fatores Primos; vamos considerar um subconjunto particular de inteiros positivos formados pela “concatenação” de números quadrados com a mesma quantidade de dígitos. Partiremos da situação mais elementar possível que consiste precisamente na formação desses números, tomando os quadrados com apenas dois dígitos.

$$T = \{16, 25, 36, 49, 64, 81\}.$$

A nossa tarefa por enquanto é realmente muito simples e consiste de um exercício elementar sobre Análise Combinatória, mediante a utilização do **Princípio Fundamental da Contagem** também conhecido como Princípio Multiplicativo ou ainda a Regra do Produto**.** Vamos formar todos os 36 arranjos possíveis de dois membros desse conjunto, incluindo aqueles com repetição. Dessa forma, obtém-se:

Tabela 1

1.625	1.636	1.649	1.664	1.681	2.536	2.549	2.564	2.581
3.649	3.664	3.681	4.964	4.981	6.481	2.516	3.616	4.916
6.416	8.116	3.625	4.925	6.425	8.125	4.936	6.436	8.136
6.449	8.149	8.164	1.616	2.525	3.636	4.949	6.464	8.181

Agora, deve-se verificar mediante a utilização de calculadora, dado o excessivo número de candidatos, a existência de quadrados perfeitos na tabela que acabamos de construir. Feito isso, encontramos apenas uma resposta: $1.681 = 41^2$**.** Observe ainda que todos os seus membros são de fácil identificação visual, de modo que para esses inteiros, não existem maiores dificuldades na tomada de decisão sobre a quadratura dos mesmos. Esse resultado precisa ser levado em conta por parte de professores e alunos, devido à evidente simplicidade dos resultados associados.

Assim, para cada um dos 36 números inteiros listados, conclui-se imediatamente que os mesmos não são quadrados, sem a utilização de qualquer método como tentativas e erros, mas principalmente a Decomposição em Fatores Primos**.** Quer dizer, se um número é formado pela concatenação de dois quadrados perfeitos com apenas dois dígitos, então ele certamente não integra os quadrados perfeitos, salvo 1.681 que pode ser considerado uma verdadeira “celebridade” entre os demais.

O nosso objetivo é que ao nos depararmos com qualquer desses termos, sejamos capazes de decidir prontamente não tratar-se de um quadrado perfeito, devido à forma particular do mesmo. Isso exigirá um pequeno e compensador esforço de memória, já que evitará a utilização de todos os métodos de identificação até agora.

Logo, já podemos concluir, pelo menos nesse contexto que a concatenação de dois quadrados perfeitos com a mesma ordem de grandeza não forma quadrados; salvo uma única exceção (1.681). Fazendo com que o nosso repertório aumente ainda mais, passando a 36 termos para os quais não encontramos qualquer dificuldade na hora de decidirmos, mediante um critério simplesmente visual sobre a sua quadratura. Assim, de todos os arranjos possíveis, incluindo as repetições formadas por quadrados com dois algarismos, apenas um deles (1.681) integra o conjunto dos números quadrados. Mais uma vez, chamamos a atenção para a nossa estratégia de considerar os inteiros com apenas quatro algarismos como um excelente ponto de partida em termos eminentemente didáticos.

Nesse caso, vale ressaltar que não há necessidade de utilizarmos qualquer método de identificação como Tentativas e Erros ou decomposição em primos, sendo este o nosso principal objetivo, tendo-se em vista todas as dificuldades computacionais associadas. Na verdade, estamos considerando uma espécie de restrição aritmética que após esses comentários, mostrou-se muito forte, quer dizer, exigir que um número quadrado seja formado pela concatenação de dois quadrados com a mesma ordem de grandeza figura como uma restrição muito forte, haja vista apenas um dos arranjos (1.681), num conjunto com 36 verificar essa condição que sem dúvidas pode ser utilizada como estratégia didática no sentido de promover uma ampliação no repertório de números não pertencentes aos quadrados perfeitos.

1.3: Proposição O número 2.536 não representa um quadrado perfeito.

Demonstração. 2.536 = 2.500 + 36. Como $2.500 = 50^2$, então $2.536 = 50^2 + 36$. De fato, sabemos que $51^2 – 50^2 = 101 > 36$. Assim, vemos que o número em questão situa-se entre os quadrados consecutivos 2.500 e 2.601. Agora, deve-se chamar a atenção do leitor para o fato de que em geral, não é tarefa fácil, escrever um inteiro positivo em função do quadrado mais próximo, utilizando somente as operações de adição e subtração**.** Mediante procedimento semelhante, chega-se à mesma conclusão para os demais termos do conjunto que figura nessa discussão sobre a justaposição de números quadrados, permitindo um maior aprofundamento no tema.

É natural nos perguntarmos o que acontece no caso geral, quer dizer, será que a justaposição (concatenação) de dois quadrados com quatro dígitos, por exemplo, é capaz de formar quadrados? Não podemos incorrer no risco de continuar com essa análise, pois tal procedimento tornaria o texto demasiadamente extenso.

Porém, uma análise semelhante (mais simples) para os quadrados com quatro algarismos que não será posta em prática, revela a existência de resultados semelhantes, resumidos da seguinte forma: Dentre todos os arranjos possíveis formados pela “concatenação” de dois números quadrados com quatro dígitos, apenas um figura entre os quadrados (**$24.019.801 = 4.901^2$)** como acontece com o conjunto elencado, alimentando ainda mais esse padrão extremamente interessante.

Capítulo II

2.1 O Conceito de Raiz Quadrada

Aspectos Históricos

Será tomado como referência um excelente texto do professor João Bosco Pitombeira de Carvalho, titular do Instituto de Matemática da Universidade Federal do Rio de Janeiro, apresentado durante a V Bienal da **Sociedade Brasileira de Matemática**, realizada em outubro de 2.010. Com o título “A raiz quadrada ao longo dos séculos”, o autor aborda o problema do cálculo de uma raiz quadrada em praticamente todos os seus aspectos, notadamente Históricos. Por esse motivo, justifica-se a adoção do texto em questão que nos parece suficiente para os propósitos do nosso trabalho de pesquisa.

Entretanto, vale lembrar que estamos muito mais interessados na dimensão discreta do referido problema, assim, serão omitidas diversas passagens relacionadas à sua dimensão contínua. De acordo com autor: O cálculo da raiz quadrada sempre despertou o interesse de grandes civilizações ao longo da História como se o domínio dessa operação representasse uma espécie de supremacia em relação às demais nações, dando-lhes vantagens, dentre outras, no domínio das principais técnicas de engenharia.

> “Essa operação tem uma nítida importância geométrica, pois permite calcular efetivamente a medida do lado de um quadrado, cuja área é conhecida. Além disso, muitos dos problemas que formulados em nossa moderna linguagem algébrica, conduzem ao cálculo de raízes quadradas”. (**Carvalho**, 2010, pág. 1)

Destaca ainda que as primeiras civilizações encaravam o problema da raiz quadrada geometricamente, uma afirmação até certo ponto natural, levando-se em conta que o desenvolvimento de uma linguagem algébrica ocorreria vários séculos depois. Com isso, foi possível atacar o problema com um arsenal de técnicas muito superior.

Nesse sentido, o cálculo de uma raiz quadrada passa a figurar numa categoria particular de um problema mais geral, onde se busca os zeros de uma equação polinomial, dando origem a algoritmos extremamente poderosos, capazes de gerar excelentes aproximações decimais. A leitura do texto permite concluir ainda sobre a necessidade de o professor recorrer aos aspectos históricos atrelados ao conceito mencionado sempre que abordá-lo na sala de aula. Na verdade, essa é uma recomendação geral para todos os conceitos, Em outras palavras, abordar o surgimento e a sua evolução contribui de forma significativa para sua compreensão.

Entretanto, não podemos ficar presos ao contexto geométrico, pois, há diversos problemas para os quais o enfoque analítico se mostra extremamente presente. Mas, sem dúvidas, encarar a raiz quadrada como a medida do lado de um quadrado representa uma estratégia didática extremamente bem sucedida, tomando por base a nossa experiência como professores no contexto da educação básica. Naturalmente, mais cedo ou mais tarde, fica evidente a necessidade de “mergulhos” mais profundos, exigindo a utilização de outros métodos mais eficientes.

Por último, vale uma menção ao algoritmo chinês que segundo o autor, não tem mais espaço em sala de aula, supostamente pelos inconvenientes característicos da sua aplicação. Outro ponto a destacar, diz respeito ao cálculo da $\sqrt{2}$, devido a sua inegável importância histórica na compreensão dos números Reais. O texto deixa claro que esse é um resultado conhecido há bastante tempo, apesar de que uma análise mais rigorosa, extrapolando o conceito de irracionalidade, explorando o fato do mesmo representar um número algébrico, seria possível apenas no início do século XIX com o aprofundamento na compreensão dos números Reais, enquanto **corpo ordenado completo, determinado a menos de um isomorfismo**.

Um fato notável, diz respeito à presença de três demonstrações distintas para a irracionalidade da $\sqrt{2}$**.** Isso mostra a enorme importância desse resultado que historicamente está associado à Crise dos Incomensuráveis, um grande abalo para a Escola Pitagórica. É bem conhecida a maneira de demonstrar a irracionalidade de tal número Real, mediante a técnica de redução ao absurdo. Segundo Carvalho:

> "A demonstração clássica da irracionalidade da raiz quadrada de 2 pelos matemáticos gregos foi exaustivamente reconstruída com base numa observação de Aristóteles, de que com as propriedades do par e do ímpar, os pitagóricos tinham demonstrado a incomensurabilidade entre as medidas da diagonal e do lado de um mesmo quadrado." (**Carvalho**, 2.010, pág. 3).

Esse procedimento pode ser generalizado de modo a incluir todos os números não quadrados perfeitos. Assim, sabendo, por exemplo, que o número 19 não figura entre os quadrados perfeitos, não há maiores dificuldades em mostrar que sua raiz quadrada indica um número irracional. Além disso, algébrico também, dado que o mesmo pode desempenhar o papel de raiz numa equação algébrica de coeficientes são racionais. Na continuidade do texto, são expostas ainda diversas técnicas que surgiram em cada uma das grandes civilizações da antiguidade como Grécia, Egito, Índia, Mesopotâmia, China, etc.

Ressaltamos ainda os cuidados que devemos tomar na abordagem do conceito de raiz quadrada em sala de aula, devido às deficiências típicas dos alunos no nível da educação básica. Tomando um exemplo, nos expressaremos de forma mais objetiva: Convencer um aluno do ensino fundamental de que a raiz quadrada de 19 representa um número não é o que podemos chamar de uma tarefa fácil. Isso exige uma profunda exploração do conceito de número, abstrato na sua essência, muito difícil de ser posta em prática, entre outras, devido ao excesso de informações a que eles são submetidos diariamente, incluindo as péssimas condições estruturais das escolas públicas na sua grande maioria com professores sem estímulo algum.

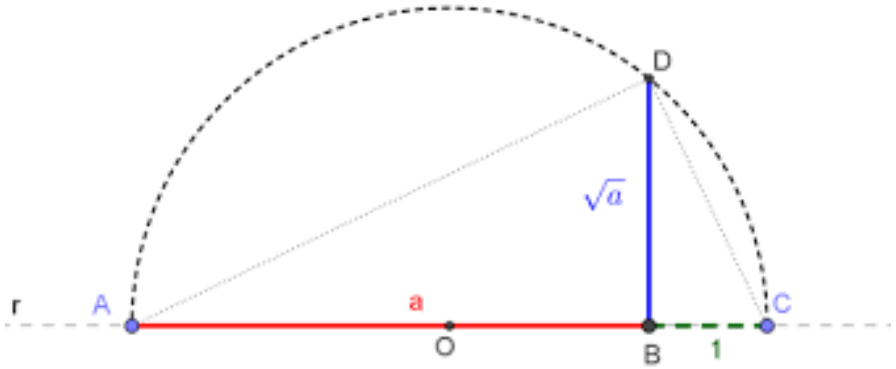
Para isso, o professor deve planejar uma atividade específica sobre o cálculo da raiz quadrada, a começar pela gênese geométrica, mediante a utilização de calculadoras como forma de permitir ao aluno um primeiro contato com os números, cuja representação decimal é infinita e não periódica (irracionais). Com isso, surgirá naturalmente a questão de como se calcular essas aproximações decimais sem a utilização daqueles recursos computacionais.

2.2 Definição. Definimos a Raiz Quadrada de um termo qualquer daquela sequência (números quadrados) como o único número inteiro positivo que quando multiplicado por ele mesmo, uma única vez resulta no termo em questão, indicando efetivamente a sua posição na sequência mencionada.

Não podemos deixar de mencionar a fantástica possibilidade de transportar de uma forma certamente mais sutil, em termos numéricos, a ideia de raiz quadrada para o **Corpo dos Números Racionais**. Vamos aproveitar a oportunidade e recordar nos próximos parágrafos o significado de Campo Numérico (Corpo) que é fundamental para o sucesso da nossa empreitada. Essa Transposição acarretará certamente algumas “complicações” que de certa forma já são esperadas, se considerarmos as enormes diferenças, notadamente conceituais assim como os aspectos mais particulares sobre as propriedades que de cada um daqueles conjuntos numéricos fundamentais.

Levando-se em conta a interpretação geométrica de um número quadrado como a medida da área de um quadrado, conforme visto no capítulo I, resulta que a raiz quadrada representa a medida do lado desse quadrado. Esses comentários reforçam a necessidade de um apelo geométrico para a abordagem eficiente de ambos os conceitos. Além disso, esse procedimento também fornece um significado para cada um dos conceitos mencionados. As relações métricas no triângulo retângulo, especialmente envolvendo a altura relativa à hipotenusa e as projeções dos catetos sob a hipotenusa permitem a seguinte construção auxiliar fundamental para o significado da raiz quadrada.

Figura 2: Uma interpretação geométrica para a raiz quadrada



https://encryptedtbn0.gstatic.com/images?q=tbn:ANd9GcS8SlZxw8q65vXq7Y4JmInVMtMEilIYdhVGgbEyt0RRuCg-aGm3

2.3 O Conceito de Corpo.

É útil considerar os números não mais como entes em si, isto é, individualmente, mas como elementos de um conjunto. Evidentemente, há uma infinidade de tais conjuntos, como por exemplo: O conjunto dos números inteiros, o conjunto dos números negativos, etc. Nem todos estes conjuntos oferecem o mesmo interesse, dependendo de certas propriedades que eles verifiquem ou não. Seja F um conjunto de números, tal que:

(1) F contém a Soma, Diferença, Produto e Quociente (exceto por zero) de dois quaisquer de seus números;
(2) Os números de F obedecem às leis de Comutatividade e Associatividade para a adição;
(3) Os números de F obedecem às leis da Comutatividade, Associatividade e Distributividade para a multiplicação.

Diz-se, neste caso que F constitui um Corpo. Os exemplos clássicos são os conjuntos dos números Reais e Racionais, referidos comumente como o “Corpo Real” e o “Corpo Racional”. Os números inteiros e positivos, por exemplo, não constituem um corpo, porquanto são “abertos” à subtração (que produz números negativos) e à divisão (que produz números quebrados). Todavia, um corpo constitui um conjunto extremamente amplo. É lícito indagar se esta mesma ideia, porém restrita a conjuntos de efetivos finitos, teria alguma significação. A resposta é afirmativa – desde que se associe a esses “pequenos” conjuntos a ideia de ordem ou sequência.

O cálculo de uma raiz quadrada com aproximação de pelo menos uma casa decimal, permite decidir prontamente se o número em questão representa de fato um quadrado perfeito. Quer dizer, podemos considerar o mesmo como uma Condição Suficiente, mas deve-se esclarecer que a mesma não é uma Condição Necessária. Assim, podemos tomar a decisão sobre a quadratura de um inteiro positivo, sem calcularmos a sua raiz quadrada o que é surpreendente para os nossos objetivos nesse importante projeto de pesquisa.

Isso porque aponta na direção de um ganho significativo em termos computacionais. Isso ocorre, por exemplo, quando o número mencionado não admite, dentre outras possibilidades, uma terminação característica de quadrado perfeito, cuja totalidade será determinada nos próximos capítulos, configurando um conjunto de 22 Classes de Equivalências. Quer dizer, nesse caso, podemos concluir automaticamente e sem a necessidade de efetuarmos cálculos complicados que o número em questão não representa um quadrado perfeito, já que essa é uma dentre as várias condições necessárias e diretamente associadas ao Método das Terminações Características para que um inteiro positivo figure como membro dos quadrados perfeitos.

Temos plena consciência de que essa tarefa pode ser desempenhada de forma muita satisfatória pela **Teoria das Frações Contínuas,** principalmente se atentarmos para as representações periódicas completamente conhecidas da comunidade matemática há bastante tempo. Na verdade, devemos ser mais justos nesse contexto: enquanto Linguagem Matemática Superior**,** ela resolve o último desses problemas da forma mais eficiente possível. Quer dizer, através daquela somos capazes de aproximar números irracionais mediante racionais, cujas aproximações não têm comparação com nenhuma teoria desenvolvida até o momento. Agora, precisamos deixar claro, a sutil diferença em termos de **Complexidade Computacional** que existe em linhas gerais entre identificar um número quadrado perfeito (mais difícil) e calcular sua raiz quadrada (mais fácil).

Não podemos negar que a matemática coloca à nossa disposição pelo menos uma dezena de Métodos**,** numéricos em sua maioria, através dos quais podemos calcular raízes quadradas de números reais positivos. Mas, o mesmo não se pode afirmar sobre a existência de estratégias eficientes para a identificação de números quadrados. Aqui, deve-se chamar a atenção para a dimensão discreta do problema de pesquisa. Nesse sentido, estamos interessados em trabalhar somente com os números inteiros pelos mais variados motivos, incluindo aqueles de natureza didática, já que levar o problema mesmo para o Corpo dos Números Racionais exige um esforço ainda maior dos professores no sentido de que o campo numérico mencionado tem propriedades de difícil abordagem.

Observa-se facilmente em nosso cotidiano da sala de aula que muitos alunos têm dificuldades em encontrar uma boa aproximação racional para o Problema da Raiz Quadrada**,** mesmo diante da exigência de determiná-la com apenas duas casas decimais sem a utilização de uma calculadora. Por isso, seria muito interessante se abordássemos nas escolas um método preferencialmente algébrico e mais prático em relação aos tradicionais.

De modo que nos permitisse resolvê-lo de maneira mais eficaz, através da aplicação de alguma fórmula que em linhas gerais nos deixa mais confortáveis. Utilizando um intervalo de tempo considerado razoável para a sua efetiva aplicação (Tempo Médio de Processamento)**.**

Para a extração de raízes quadradas não exatas, que sabemos representarem Números Irracionais; alunos e mesmo uma boa parte dos professores da educação básica não encontram a ajuda de que realmente precisam nos principais livros didáticos.

2.4: Método da Falsa Posição

Sem dúvidas, essa é a primeira ferramenta que os professores costumam abordar em sala de aula quando abordam a problemática da raiz quadrada, tanto nos inteiros quanto nos Racionais. São vários os motivos que os levam a tomar essa decisão, sendo sua simplicidade certamente a mais forte de todas. Ela consiste basicamente na realização de multiplicações com fatores iguais até que se consiga alcançar o número, cuja raiz quadrada se deseja encontrar.

De um modo geral, sabemos que ela é de fácil aplicação e não apresenta maiores dificuldades com relação a sua abordagem, mesmo no ensino fundamental onde os alunos costumam apresentar muitas dificuldades no que diz respeito às operações básicas, notadamente a divisão nas séries iniciais assim como potenciação e radiciação nas séries finais.

Mais do que isso, sabemos que no início das apresentações, o professor costuma tomar o cuidado de abordar o problema escolhendo apenas quadrados perfeitos, generalizando para os inteiros positivos e atingindo finalmente o Corpo dos Números Racionais. Esse é um procedimento recomendável a nosso ver, quer dizer, encarar os números quadrados nessa etapa inicial ajuda a entender o problema da raiz quadrada na sua totalidade.

Nesse caso, estamos adotando a estratégia de começar do particular para o geral, respeitadas as condições de ensino e o nível onde estamos imersos. Na verdade, a nossa experiência tem mostrado que na maioria das vezes, os alunos fornecem sinais de que esse é praticamente o único “método” que fica depois que os ensinamos a identificar números quadrados e calcular raízes.

Como existe uma preocupação muito forte com relação aos aspectos didáticos dessa pesquisa, noutras palavras, desejamos que os resultados sejam aplicáveis à educação básica, mesmo que isso não seja possível em sua totalidade; achamos conveniente escolher um exemplo de aplicação e mostrar como o mesmo seria resolvido, via “tentativas e erros” numa apresentação de rotina do professor de matemática, em nível fundamental de ensino e supostamente nos anos finais, já que essa é a minha realidade, consciente de que essa restrição não trará qualquer prejuízo para o desfecho da pesquisa.

Tudo isso, levando-se em conta também que por diversas vezes, tive oportunidade de abordar o tema exatamente nesse contexto, permitindo que essa análise seja feita de forma mais eficiente, dado que falamos do cotidiano. Se bem que não haveria qualquer desconforto, caso tomasse a decisão de enveredar nessa discussão pela matemática superior, mas isso representaria um desvio dos objetivos traçados inicialmente que precisam ser respeitados, do contrário, seria altamente provável que a pesquisa perdesse sua razão de ser, pois na pior das hipóteses, faltaria um mínimo de coerência da nossa parte.

Exemplo. Verificar se o número 5.284 representa um quadrado perfeito.

Adotaremos como hipótese inicial que ele está entre os quadrados perfeitos. Assim, deve-se escolher um inteiro positivo e multiplicá-lo por ele mesmo, até chegarmos o mais próximo de 5.284. A princípio, procede-se dessa maneira sem estabelecer critérios mais específicos, quanto a isso, não deve haver maiores preocupações o que importa é a plena consciência do que se está fazendo em termos matemáticos.

Admita que escolhermos 43, então multiplicando por ele mesmo, obtemos $1.849 < 5.284$. A primeira tentativa mostra que o valor escolhido esta “distante” do fornecido. Assim, para continuar, escolhemos um número maior, digamos 63. Multiplicando por ele mesmo, obtém-se $3.969 > 5284$. Mesmo menor, ele está mais próximo, isso significa que avançamos em nossa busca. Agora, tomando 75, encontramos $5.625 > 5.284$. Fica evidente que ultrapassamos o 5.284, exigindo a escolha de outro valor, digamos 72, donde obtemos $5.184 < 5.284$.

Temos somente mais um caso a considerar, dada a proximidade do último resultado: 73 x 73 = 5.329 > 5.284. Finalmente, estamos em condições de concluir por todas as multiplicações realizadas até o momento, que o número dado inicialmente não figura entre os quadrados perfeitos. Existe ainda uma forma de tornar essa busca um pouco mais eficiente: Basta levarmos em conta que um número quadrado e sua raiz quadrada têm a mesma paridade, conforme comentado na introdução. Assim, de posse dessa informação, deve-se atentar para os aspectos de Paridade antes das referidas multiplicações.

Para o problema que acabamos de resolver, podemos encarar essa informação como um Refinamento das Tentativas e Erros, permitindo que o número de operações seja drasticamente reduzido o que é surpreendente e importante para tornar o processo um pouco mais eficiente. Assim, levando-se em conta que 5.284 é número par, deve-se escolher apenas números pares como candidatos a raiz daquele (vale ressaltar que outras congruências também podem ser adotadas).

Essa questão precisa ser trabalhada com prioridade, pois diminuir as operações representa um dos principais objetivos em praticamente todas as Rotinas do Cálculo Numérico, mesmo numa dimensão elementar como é o caso da nossa. Resumindo, concluímos que os números escolhidos devem ter a mesma paridade do número fornecido, se o interesse é verificar a quadratura ou calcular suas raízes quadradas.

Aliás, essa conclusão pode ser estendida para as demais potências. Faremos uma última colocação numa tentativa de aumentar ainda mais a eficiência do Método da Falsa posição: Ela diz respeito à relação entre as quantidades de dígitos envolvidos nos quadrados e suas respectivas raízes. Se um número quadrado tem uma quantidade par de dígitos, então a sua raiz quadrada tem exatamente metade dessa quantidade. Voltando ao número 5.284, temos que são quatro os seus dígitos, então a sua raiz tem dois dígitos.

A essa altura, deve-se combinar as duas informações, fazendo com que a nossa busca chegue ao final de forma mais rápida. Logo, para o número em questão e de posse dessa informação, escolhemos somente números pares com dois dígitos. Vale ressaltar que ambas as informações são de fácil entendimento e devem ser abordadas, visando um incrível **ganho computacional,** pois vivemos cercados de complexidade que não permite desperdiçar esse recurso tão precioso que é o tempo sobre o qual sempre nos surpreendendo e somos desafiados a usá-lo da forma mais racional possível.

Por último, achamos por bem ressaltar que o Método da Falsa Posição tem uma característica que a torna ainda mais importante no ensino da matemática: Ela é altamente intuitiva, quer dizer, caso não seja fornecida uma alternativa ou ferramenta ao aluno para que o mesmo resolva o problema da raiz quadrada na sua dimensão discreta, ele certamente concluirá (depois de uma reflexão) que deve escolher um número inteiro e multiplica-lo por ele mesmo, até encontrar um resultado o mais próximo possível do número em questão.

Naturalmente, desde que lhe seja dado tempo para a devida reflexão sobre o problema, permitindo a superação do mesmo. Conclusões semelhantes podem ser obtidas quando se discute o cálculo da raiz quadrada com aproximação decimal, desde que seja estabelecido um critério de parada fundamental nas mais diversas rotinas do cálculo numérico. A forma mais elementar nesse caso, diz respeito à especificação do número de casas decimais que podem ser consideradas corretas pelo agente responsável.

Essa conclusão aparece de forma completamente espontânea em nossa prática diária como professores de matemática em nível fundamental de ensino. O mesmo não podemos dizer sobre os dois refinamentos que contribuem para o amadurecimento do método. Nesse caso, eles precisam de uma intervenção por parte do professor, aliás, essa é uma de suas principais funções: Orientar o processo de ensino aprendizagem e avaliação matemática, mesmo não sendo uma tarefa das mais fáceis, na verdade, um grande desafio.

2.5: Raiz Quadrada Via Fatoração Primária

Nesse caso, temos pouquíssimas opções, dentre as quais destacamos a espinhosa busca pela Decomposição em Fatores Primos (forma padrão) como a mais adotada entre os números inteiros. Existem tabelas disponíveis em livros revistas, periódicos, etc., nas quais encontramos excelentes, porém desanimadoras estimativas sobre o Tempo Médio de Processamento como um dos principais parâmetros para a obtenção da fatoração primária pelo método das tentativas e erros, mediante divisões sucessivas por primos consecutivos numa máquina de Turing.

Não temos o menor receio de exagerar ao afirmar que a busca por métodos capazes de fornecer essa representação em tempo polinomial figura como um dos maiores desafios computacionais da atualidade. Para isso, é fundamental abordar ambos os conceitos de números primos e números compostos**,** destacando os resultados mais notáveis a respeito desses notáveis conjuntos.

O aluno deve experimentar as dificuldades de se obter a fatoração completa de inteiros nos Primos. Depois, coloca-se uma tabela de primos consecutivos à disposição, permitindo explorar os conceitos mencionados com mais ênfase. Destacamos o fato de haver uma infinidade enumerável tanto de primos quanto de compostos. Finalmente, abordamos o Teorema Fundamental da Aritmética.

Apenas como exemplo, vamos tomar o número 105 e escrever o mesmo como um produto de primos, admitindo que o mesmo figure entre os compostos. Para isso, verificamos se o mesmo é divisível por três, dado que estamos diante de um ímpar, donde a resposta é positiva. Assim, já temos uma nova representação para 105: 3 x 35. Repetimos o procedimento para o 35, cuja resposta agora é negativa. Aliás, nesse caso em particular, tem-se um critério de divisibilidade extremamente eficiente à disposição, cuja resposta depende apenas do último dígito, conforme sabemos.

Mas, esse mesmo número é divisível por cinco: 35 = 5 x 7, de onde resulta uma nova e definitiva maneira de escrevê-lo como um produto de primos, extremamente especial na Aritmética: $105 = 3\,x\,5\,x\,7$. Veja que nossa empreitada chegou ao final, já que o último dos quocientes é ele próprio um primo. Naturalmente, devemos consultar, na maioria das vezes, uma tabela de primos consecutivos por questão de praticidade.

Tudo bem que nesse caso foram necessárias apenas três divisões. Entretanto, não se engane com as aparências, principalmente quando se tratar dos primos assim como da busca pela sua fatoração completa de inteiros. Para que o número em questão seja quadrado perfeito, a condição necessária e suficiente é a de que todos os expoentes da sua fatoração (forma padrão) sejam pares.

Mesmo após vários ataques realizados por centenas de matemáticos profissionais ao redor do planeta com impacto direto na recém-criada criptografia RSA que vem sendo encarada por várias nações como um **Assunto de Segurança Nacional**. Acreditamos que esses detalhes passam despercebidos pela maioria dos professores que lidam diariamente com a matemática na sala de aula, principalmente para a extração de raízes quadradas não exatas, que sabemos representarem Números Irracionais**.**

Uma dificuldade que os alunos dos níveis fundamental e médio de ensino encontram é saber trabalhar com números irracionais. Quando extraímos uma raiz quadrada usando um processo iterativo, algoritmo ou mesmo uma calculadora surge com muita frequência a seguinte pergunta: Mas qual é o verdadeiro valor dessa raiz quadrada? Isso mostra claramente uma falta de compreensão sobre o importante conceito de Número Irracional e a falta de conhecimento de que um número Real é racional se, e somente se, sua representação decimal é infinita periódica ou tem uma quantidade finita de dígitos não nulos.

Todos esses comentários deixam clara a importância de um planejamento o mais detalhado possível para a abordagem dos números irracionais amparado, sem sombra de dúvidas no conceito de raiz quadrada. Vale lembrar ainda que o professor deve possibilitar aos alunos o contato com outros números irracionais igualmente importantes como aquele que historicamente representa o quociente do comprimento de uma circunferência pelo seu diâmetro. Em outras palavras, o famoso número $\prod \cong 3,14159265$.

2.6: O Método de Newton

Faremos apenas uma pequena referência ao clássico Método de Newton (tangentes) como sendo um dos mais eficientes entre os algoritmos Numéricos, mas que dificilmente encontraria espaço nas salas de aula, principalmente do ensino fundamental, haja vista utilizar conceitos matemáticos extremamente refinados para esse nível como **Limites, Derivadas, Convergência,** etc. Sem falar que ele também confere o mesmo tratamento a todos os inteiros positivos.

Quer dizer, não leva em conta o importante fato de fácil demonstração, segundo o qual os números quadrados representam uma “minoria” entre os Naturais, conforme veremos através do cálculo de sua Densidade que sabemos ser nula, estando à mesma diretamente associada à Probabilidade de que um inteiro positivo escolhido aleatoriamente seja um quadrado perfeito.

Esse tema merece alguns novos comentários com um pouco mais de profundidade dada a sua enorme importância no universo da **Análise Numérica** assim como a sua inegável eficiência que ficará evidente após algumas simulações nas quais a nossa atenção focar-se-á nas sucessivas aproximações decimais de um número irracional quadrático**,** geradas através da sua efetiva aplicação. Podemos tomar a quantidade de algarismos corretos em cada iteração como um excelente parâmetro inicial para avaliarmos a eficiência numérica do método em questão.

De um modo geral, dizemos que o Método de Newton converge quadraticamente dentro das condições impostas por um Teorema específico que envolve a função de iteração correspondente**:** $F(X) = X^2 - A$, uma desigualdade na qual comparecem ainda suas derivadas de primeira e segunda ordem ambas comparadas à unidade.

Quando afirmamos que um método converge de forma quadrática, significa que o número de algarismos significativos (corretos) dobra em média a cada nova iteração. O leitor deve concordar que esse é um resultado fantástico relacionado obviamente ao fato da função de iteração ser do tipo polinomial e apresentar-se de uma forma "comportada" tomando como principal referência tanto os aspectos de crescimento quanto aqueles relacionados com a Continuidade.

Falando especificamente sobre o cálculo de raízes quadradas de inteiros positivos, verificamos facilmente que o Método de Newton converge de forma muito eficiente, conforme veremos mediante exemplo um escolhido de modo criterioso para evitar a obtenção de resultados particulares que possam de alguma forma, comprometer a Análise Numérica na qual estamos imersos. Vale lembrar que os métodos iterativos exigem apenas uma boa aproximação inicial que pode e deve ser combinada com a experiência por parte do analista. Vejamos a fórmula iterativa "condensada" para o cálculo da raiz quadrada de um inteiro positivo A, segundo o Método de Newton:

$$X_{n+1} = \left({X_n}^2 + A\right)/2X_n$$

No caso em questão, admitiremos que o nosso objetivo seja calcular a $\sqrt{29}$ até a terceira casa decimal. A nossa aproximação inicial corresponde a raiz do quadrado perfeito mais próximo do radicando. Sendo assim, tomar-se-á como ponto de partida $\boldsymbol{X_0 = 5.}$ Em seguida, substituímos esse valor na função iterativa, obtendo aproximações cada vez melhores no sentido de que seus quadrados estarão ainda mais próximos do número, cuja raiz quadrada busca-se determinar. De fato, após a primeira substituição, obtemos $\boldsymbol{X_1 = 5,4}$ cujo quadrado difere de 29 por apenas 0,16.

Podemos continuar com a aplicação do método gerando novas aproximações até atingirmos a estimativa previamente determinada que nesse caso, corresponde à terceira casa decimal. Assim, com mais uma iteração, obtemos $\boldsymbol{X_2 = 5,3851851}$ ..., Ainda não podemos encerrar o problema, pois não sabermos quando vale a terceira casa, noutras palavras, há dúvidas nesse sentido até pela falta de parâmetros que viabilizem a referida comparação. $\boldsymbol{X_3 = 5,38516480}$ ...

Veja que esse resultado coincide com o anterior até a quarta casa, de modo que atingimos a precisão almejada com pouquíssimas iterações, fazendo desta uma das soluções mais bem sucedidas entre as principais ferramentas. Logo, concluímos finalmente que $\sqrt{29} \cong 5{,}3851$, isso até a quarta casa decimal, superando na verdade o nosso objetivo inicial centrado na terceira.

Mediante o exemplo citado, percebemos que de um modo geral, as sucessivas substituições geram uma sequência de números reais positivos, cujos quadrados estão cada vez mais próximos de 29. Como esse número não é um quadrado perfeito**,** sabemos que a sua raiz quadrada é um número irracional, cuja expansão decimal é infinita e aperiódica**.** Na verdade, tanto a aproximação inicial quanto os resultados obtidos com a substituição, costumam ser expressos inicialmente na forma de fração e somente depois buscamos a sua representação decimal para efeitos de comparação em relação aos resultados anteriores.

O leitor mais atento perceberá a possibilidade de nos depararmos com dízimas periódicas, cujo período pode ser longo, sendo de difícil determinação; configurando um ponto negativo do Método das Tangentes, já que o ideal seria visualizar o período em questão por completo, configurando outra habilidade. Sendo assim, pelo menos teoricamente, o Método pode ser aplicado quantas vezes forem necessárias, dependendo dos objetivos específicos e desconsiderando as restrições computacionais. Por último, o Teorema mencionado no início dos comentários garante a Convergência da sequência correspondente, sendo possível estimar o número de iterações necessárias para atingir uma determinada precisão numérica.

Noutras palavras, quantas vezes o Método de Newton precisa ser aplicado para atender as restrições numéricas impostas (Critério de Parada) como a de que, por exemplo, o erro cometido seja inferior a um milésimo. Na verdade, há várias formas de se interpretar o conceito de erro, por isso, ele precisa ser destacado, antes de começar a aplicação do método em questão. Ele pode ser avaliado pela diferença entre duas aproximações consecutivas.

Queremos com isso dizer que a diferença entre o número 29 e o quadrado da sua raiz numa determinada etapa do processo mostra-se inferior a um milésimo, esse é o entendimento básico que alunos e professores precisam levar em conta quando da abordagem de problemas nos quais se busca aproximações decimais de números irracionais quadráticos mediante iterações numéricas; independentemente do método escolhido para atacar o problema.

Por tudo o que já foi exposto e levando-se em conta as diversas leituras feitas durante a realização dessa pesquisa, fica evidente que o Método de Newton mostra-se muito eficiente quando aplicado no cálculo de raízes sejam elas quadradas, cúbicas, quartas, etc. Mas, principalmente na dimensão contínua do problema relacionado ao cálculo das raízes enésimas de um modo geral.

Entretanto, como professores, devemos atentar para a necessidade de realizarmos diversas adaptações ao método em questão, caso se decida adotá-lo em sala de aula. São vários os motivos, dentre eles, destacamos o alto nível de maturidade por parte do aluno para uma efetiva compreensão dessa ferramenta numérica, cujo potencial é simplesmente indiscutível.

Acreditamos que o melhor ponto de partida para isso, consiste no aprofundamento do conceito de número quadrado perfeito juntamente com a Partição que o conceito em questão determina no conjunto dos números naturais que a essa altura, esta devidamente caracterizada, sem falar que o mesmo costuma ser abordado nas primeiras séries do ensino fundamental, conforme sabemos pela nossa própria experiência educacional.

Deve ficar claro por todo o exposto que o método de Newton resolve o problema da raiz quadrada quando considerado na sua dimensão contínua, mas o nosso objetivo nesta etapa dos trabalhos consiste em atacar o problema em questão na sua **dimensão eminentemente discreta**.

Noutras palavras, estamos interessados em descobrir se um determinado inteiro positivo figura entre os quadrados, sem apelar para a sua Decomposição em Fatores Primos. Nesse sentido, fica evidente que o Método de Newton perde muito da sua força, enquanto ferramenta numérica, se bem que esse fato não diminui de forma alguma a importância do mesmo no âmbito geral do Cálculo Numérico.

A justificativa para isso é muito simples: O método aqui explorado confere o mesmo tratamento algébrico a todos os números reais positivos, quer dizer, a priori, ele não tem condições de fazer qualquer distinção entre quadrados e não quadrados. Aliás, essa é uma característica comum a diversos métodos utilizados no cálculo de raízes quadradas como já constatamos e reiteramos com a menção ao algoritmo chinês que não aparece mais nos livros didáticos.

Capítulo III

3.1: A Decomposição em Fatores Primos

O conhecimento da Fatoração Primária de um número inteiro permite resolver os mais diversos problemas da teoria dos números. Dentre eles, podemos citar como os mais relevantes para um contato inicial com aquela disciplina: a determinação do máximo divisor comum, do mínimo múltiplo comum, da quantidade de divisores, da soma dos divisores positivos, etc. Mas, há outro problema que ocupa um papel central na teoria dos números, ele diz respeito à classificação dos números inteiros em primos e compostos, constituindo uma partição fundamental no aprofundamento das investigações nesse profícuo campo de pesquisa.

Essa é uma tarefa difícil de realizar, mesmo quando apoiados em recursos computacionais, devido ao elevado número de operações envolvidas no processo, especialmente as divisões, cuja quantidade cresce muito rapidamente, podendo ser modelada, em linhas gerais pela função exponencial. De acordo com o **teorema fundamental da aritmética**, todo inteiro composto se escreve de modo único como um produto de primos, a menos da ordem dos sinais dos fatores correspondentes.

Esse é um resultado dos mais importantes e sem dúvida, conhecido há bastante tempo pela comunidade matemática. Tendo-se em vista que o mesmo já foi explorado no capítulo referente às principais estratégias que permitem o cálculo da raiz quadrada, tomar-se-á a liberdade de não entrar em maiores detalhes quanto aos aspectos que já foram discutidos previamente, mesmo que de uma forma superficial.

Noutras palavras, desejamos convencê-lo sobre a importância dessa representação multiplicativa na qual são utilizados especificamente os infinitos números primos de forma muito eficiente, conforme sabemos inclusive da nossa própria experiência como educadores matemáticos, independente do nível de ensino no qual atuamos.

Dada a enorme importância de tais ideias, acredita-se que seja necessário buscar referências mais sólidas, visando facilitar o contato inicial com os chamados **Campos Conceituais Multiplicativos**, tema que se explorado de modo conveniente pode facilitar bastante todo o processo de ensino-aprendizagem-avaliação matemática, notadamente quando se decidi explorar as operações de multiplicação e divisão, que são inversas uma da outra. O primeiro detalhe que chama atenção diz respeito à interpretação da multiplicação como uma adição com as parcelas iguais.

Numa análise geral, não se pode dizer que a mesma esteja equivocada, mas, é preciso enxergar a operação de multiplicação numa dimensão mais ampla, não necessariamente atrelada à adição mencionada. Aliás, uma frase que se costuma ouvir com muita frequência nas salas de aula, é a seguinte: Para dividir, o aluno tem que de fato saber multiplicar, incluindo o domínio dos algoritmos correspondentes.

Naturalmente, ela faz uma referência direta às multiplicações e divisões comuns, ou seja, definidas no conjunto dos inteiros. Aliás, a possibilidade de transportá-la para os números racionais é evidente, mas não precisa ser considerada no momento, tendo-se em vista que a relação custo-benefício na compreensão das estruturas multiplicativas, não se mostra interessante.

Um primeiro aspecto que precisa ser mencionado, diz respeito à ideia de base necessária para se representar tanto os números inteiros quanto os demais Reais. Assim, por exemplo, o **Sistema de Numeração Decimal** figura como um dos temas mais importantes da Matemática nas séries iniciais do ensino fundamental.

Do seu estudo, sabemos que com apenas 10 símbolos e algumas regras simples, podemos representar todos os números Reais. Apesar da sua ampla divulgação, não se pode afirmar que se trata da única base capaz de realizar essa sublime tarefa, através da qual, conseguimos abordar diversos conceitos do universo matemático em todos os níveis de ensino.

De fato, há uma vasta literatura sobre o assunto e uma das lições que aprendemos ao consultá-la, diz respeito à relação que o numero 10 guarda com a quantidade de dedos que temos, tanto nas mãos, quanto nos pés, tenho o homem utilizado seu próprio corpo como ferramenta para auxiliar o processo de contagem, seja para controle do seu rebanho, das mercadorias, das suas vestes, etc. Posteriormente, o homem continuou utilizando partes do seu corpo para auxiliar a realização de medições, como o palmo, a polegada, etc.

Nesse sentido, quando comparamos a ideia de **base nas estruturas multiplicativas**, surge uma diferença fundamental, através da qual, conseguimos entender um pouco da sua complexidade, enquanto conceito fundamental da Matemática: A base necessária para obter aquela representação é infinita, quer dizer, constituída por todos os números primos. Noutras palavras, temos cada vez mais dificuldades de encontrar uma representação multiplicativa quando os números envolvidos crescem mesmo tomando como parâmetro inicial apenas a ordem de grandeza de tais números.

> "Dentre os vários conceitos a serem construídos na escola estão aqueles que envolvem as operações de multiplicação e divisão. Estas operações são essenciais para a compreensão de outros conceitos do universo matemático. A Teoria dos Campos Conceituais das estruturas multiplicativas é um conjunto de problemas e situações cujo tratamento requer **conceitos, procedimentos e representações** de diferentes tipos, mas intimamente relacionadas" (**VERGANUD**, 2009).

O conceito matemático é definido como sendo um conjunto de três subconjuntos: (S) conjunto das situações que dão sentido ao conceito; (I) invariantes, os quais são responsáveis pela operacionalidade dos conceitos e por último: (R) representações simbólicas são as formas de linguagem utilizadas para representar os invariantes e as situações, bem como os procedimentos para lidar com elas. Quando trabalhamos com um campo conceitual, é importante apresentar as situações problema em diferentes quadros, por exemplo, **o aritmético, o algébrico e o geométrico** nos quais os conceitos, os procedimentos e as representações se concretizam.

A Teoria dos Campos Conceituais fornece aos professores da educação básica, especialmente dos anos finais, diversos elementos fundamentais para analisar as dificuldades de aprendizagem dos seus alunos. Isso constitui uma possibilidade de organizar a didática referente ao que se ensina nos conteúdos, mas também se mostra ferramenta útil para a **construção de situações-problemas** que desafiem os alunos, colocando-os em constante processo de aprendizagem cooperativa.

Buscando fundamentar essas afirmações, adotaremos um texto do VIII encontro nacional de educação matemática, uma publicação da **Sociedade Brasileira de Educação Matemática (SBEM)**, ocorrido de 16 a 18 de julho, 2.004 na cidade do Recife. A autora do minicurso Mônica Bertoni dos Santos, professora titular da Pontifícia Universidade Católica do Rio Grande do Sul à época, aborda a questão de forma muito coerente e concisa, conforme uma das suas declarações. Com isso, tem-se a oportunidade de conhecer melhor as enormes contribuições que a SBEM traz para a educação matemática, desde a sua criação. Nesse sentido:

> "A teoria dos campos conceituais precisa constantemente ser explorada por pesquisadores e por professores na qualidade de cientistas e pesquisadores, dada a sua complexidade e a sua relevância como suporte para as aprendizagens científicas. Trata da conceptualização do real e presta-se para diferentes áreas do conhecimento tendo sido elaborada para explicar estruturas matemáticas de base como a aditiva e a multiplicativa". (SANTOS, Mônica Bertoni, Anais do VIII ENEM-minicurso, GT-2).

Outro ponto que precisa ser mencionado no momento, diz respeito ao significado preciso do termo fatoração. Rigorosamente falando, fatorar um número inteiro composto significa escrever o mesmo como um produto de dois ou mais inteiros. Nesse sentido, um mesmo número pode admitir várias fatorações. De fato, veja o caso do número 60 que admite: $2x30, 3x20, 4x15, 5x12, 6x10, 2x3x10, 3x4x5, 6x2x5$. Assim, a explicação para a existência de tantas representações multiplicativas, está relacionada à presença de números compostos em cada uma dessas fatorações.

Logo, visando uniformizar essa representação, surge a condição clássica de utilizar somente os fatores primos na construção desse produto. Feito isso, o número em questão admitirá uma, e somente uma representação, conhecida como a sua fatoração primária, forma padrão ou ainda forma canônica, dada à enorme importância que os números primos têm na história da Matemática. Dessa forma, concluímos que a única maneira de escrever aquele número, mediante um produto de primos, sem levar em conta a ordem: $60 = (2)^2 \, x \, (3) \, x \, (5)$.

Aproveitaremos a oportunidade para recordar como proceder para determinar a quantidade de divisores do número 60, tomando como referência a sua fatoração primária. O procedimento é muito simples, exigindo apenas a utilização do **Princípio Fundamental da Contagem**, já que todo divisor de 60 é da forma $2^m \, x \, 3^n \, x \, 5^p$, onde $m \in \{0,1,2\}, n \in \{0,1\} \, e \, p \in \{0,1\}$. De acordo com o princípio mencionado, o total de divisores de 60 é $3 \, x \, 2 \, x \, 2 = 12$.

Como o número em questão é pequeno, podemos ainda listar esses divisores, de fato: $D(60) = \{1,2,3,4,5,6,10,12,15,20,30,60\}$. Entretanto, não se pode esquecer que todas essas informações, dependem essencialmente do conhecimento da decomposição nos primos, porém, já comentamos que a busca por esse produto exige em geral muito tempo de processamento, dado o elevado número de divisões associadas, admitindo a não utilização de ferramentas mais avançadas, ou seja, métodos distintos dos apresentados aqui ou amplamente divulgados nos textos introdutórios sobre a teoria dos números.

Da mesma forma, também podemos determinar a soma dos divisores positivos**,** a partir daquela fatoração. Entretanto, dada a importância e profundidade do tema, decidimos concluir a exposição, tomando o número 60, tendo-se em vista que os seus divisores já foram determinados. Dessa forma, a soma em questão vale 168. Mas, deve-se ressaltar que esse mesmo resultado pode ser obtido, sem o conhecimento explícito de cada um dos divisores. De fato, levando-se em conta mais uma vez que $60 = (2)^2 x \, (3) \, x \, (5)$ pode-se provar que a soma dos divisores é:

$$S(60) = (2^2 + 2^1 + 2^0).(3^1 + 3^0).(5^1 + 5^0) = 168.$$

O leitor mais atento perceberá que cada um dos fatores de S(60) corresponde à soma dos termos de uma progressão geométrica, cujos expoentes são consecutivos e decrescentes a começar pelo expoente que figura na fatoração do número. Apesar de não desejarmos aprofundar tais discussões, vale mencionar a presença nesse texto de duas das mais importantes funções da teoria elementar dos números: **Número de divisores D(n) e Soma dos divisores S(n)**. Infelizmente, não podemos enquadrá-las entre as funções "bem comportadas", incluindo aspectos de sobrejetividade e Injetividade, já que ambas estão ausentes, por exemplo, na última.

Nesse sentido, pode-se afirmar, por exemplo, que existem infinitos inteiros que admitem 12 divisores positivos, da mesma forma, ao menos dois inteiros, cuja soma dos divisores vale 168. Todas essas informações nos dão as primeiras pistas para a compreensão da enorme importância que a fatoração primária tem na teoria dos números, inclusive na sua dimensão mais avançada, distante de vários estudantes que não podem ou talvez não precisem de um contato mais intenso com problemas muito difíceis em sua maioria, dentre os quais, podemos certamente citar a famosa e desafiadora **Conjectura de Goldbach.**

Para encerrar as discussões, resolvemos citar um interessante problema que surgiu durante as leituras dos textos tomados como referência na construção da dissertação. Ainda com relação à função que associa a cada inteiro positivo, seu total de divisores positivos: Já sabemos que essa função não deve ser considerada "bem comportada" no aspecto geral, conforme afirmação anterior.

Assim, qual o menor inteiro positivo que admite exatamente 64 divisores positivos?

Infelizmente, esse enunciado simples nos proporciona uma excelente oportunidade de aprofundar todas as discussões elencadas. Apresentaremos a solução do problema acima, mas sem entrar em maiores detalhes, pelo menos por enquanto. Sem dúvidas, temos aqui um excelente enunciado, cujas possibilidades de exploração em sala de aula são inúmeras. Contudo, deve-se ressaltar que a abordagem do mesmo mostrar-se-á mais produtiva quando incorporada a um projeto antecedido por uma ampla introdução aos conceitos fundamentais de múltiplo e divisor de um inteiro, incluindo a discussão sobre ambos os conjuntos associados.

Porém, segundo nossas leituras, não costuma ser abordado tanto na educação básica quanto na graduação. Como suspeitava, depois de uma boa reflexão, conclui-se que este é um problema muito interessante e diferente dos demais neste contexto em vários aspectos. A superação do mesmo exige a utilização de vários resultados importante com destaque para a decomposição nos primos que é única.

Os 64 divisores de 7.560: {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 18, 20, 21, 24, 27, 28, 30, 35, 36, 40, 42, 45, 54, 56, 60, 63, 70, 72, 84, 90, 105, 108, 120, 126, 135, 140, 168, 180, 189, 210, 216, 252, 270, 280, 315, 360, 378, 420, 504, 540, 630, 756, 840, 945, 1.080, 1.260, 1.512, 1.890, 2.520, 3.780, 7.560}.

Uma curiosidade interessante nesse caso é constatar a existência de outro número inteiro com esse mesmo total de divisores e ordem de grandeza.

Os 64 divisores de 9.240: {1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 15, 20, 21, 22, 24, 28, 30, 33, 35, 40, 42, 44, 55, 56, 60, 66, 70, 77, 84, 88, 105, 110, 120, 132, 140, 154, 165, 168, 210, 220, 231, 264, 280, 308, 330, 385, 420, 440, 462, 616, 660, 770, 840, 924, 1.155, 1.320, 1.540, 1.848, 2.310, 3.080, 4.620, 9.240}.

3.2: Distribuição dos Números Primos.

A Distribuição dos Primos é bastante irregular, sendo possível provar que existem saltos arbitrariamente grandes (Deserto) entre primos consecutivos. Apesar da evidente irregularidade na Distribuição estudada há vários séculos, a densidade média da sequência correspondente pode ser considerada “suficientemente regular” a ponto de merecer a atenção de vários Matemáticos.

De fato, admita que desejemos encontrar uma lista de números compostos e consecutivos com cinco elementos. Para isso, procedemos da seguinte forma: Tomamos como ponto de partida o fatorial de 5 + 1 = 6, ou seja, 6! = 720, conforme a definição de fatorial. Agora, construímos uma sequência com cinco termos adicionando respectivamente 2, 3, 4, 5 e 6 ao fatorial em questão.

$$\{6! + 2, 6! + 3, 6! + 4, 6! + 5, 6! + 6\} = \{722, 723, 724, 725, 726\}.$$

Observe que cada um dos termos tem como divisores respectivamente por 2, 3, 4, 5 e 6. Assim, fica evidente que são todos números compostos, mesmo admitindo a existência de outros divisores, não importa. O fato é que o conjunto acima atende as condições impostas. Mas vale ressaltar que existem outros conjuntos com essa característica, porém formados por números menores.

De fato, o exemplo de solução mais eficiente para o problema é {24, 25, 26, 27, 28}. O processo pode ser generalizado para uma quantidade arbitrária de números inteiros compostos e consecutivos. Sem dúvidas, permitindo concluir sobre a existência de uma solução, mas não pela sua unicidade. Assim, de modo geral, temos que a sequência abaixo admite n inteiros compostos e consecutivos.

$$(n+1)!+2, (n+1)!+3, (n+1)!+4, \ldots (n+1)!+n+1.$$

Mais precisamente, vemos na vasta Literatura sobre o assunto que em 1752, **Goldbach** demonstrara que nenhum polinômio em X com coeficientes inteiros, admite essa propriedade (geração dos números primos), mesmo para X suficientemente grande. Posteriormente, **Legendre** demonstra que nenhuma **Função Algébrica Racional** é capaz de gerar exclusivamente primos, cuja distribuição tem se mostrado há muito tempo, extremamente complexa, figurando certamente como um dos maiores desafios nesse contexto histórico.

Apesar de verificarmos que em linhas gerais, a sua Densidade diminui à medida que se avança para inteiros sempre maiores. Na verdade, existe uma fórmula capaz de gerar todos os números primos e descoberta a pouquíssimo tempo. Entretanto, a mesma não é o que podemos chamar de prática, de modo que em linhas gerais, não vislumbramos aplicações mais fortes no seu manejo. Agora, o simples fato de a mesma ser capaz de gerar todos os primos, inclusive na exata ordem em que eles aparecem naturalmente, representa um resultado extremamente surpreendente, pois não havia muita crença na sua existência.

Vale ressaltar que esses comentários têm como objetivo principal mostrar alguns fatos sobre a magia envolvida nos mais variados aspectos na complexa Distribuição dos Números Primos de fácil percepção, bastando que o leitor admita o conhecimento de um primo qualquer e procure descobrir onde aparecerá o próximo termo desta sequência. Paralelamente a isso, chamamos a atenção para as enormes dificuldades que circundam a Decomposição em Fatores Primos. Novamente, gostaríamos de esclarecer a diferença entre:

(1) Decidir se um inteiro positivo qualquer figura entre os primos,
(2) Descobrir a fatoração completa de um inteiro entre os primos.

São dois problemas completamente distintos, apesar de que resolvendo o segundo, automaticamente resolve-se o primeiro. Agora, a recíproca não é verdadeira. Assim, para decidir se um inteiro positivo é primo, precisa-se descobrir se ele possui ao menos um divisor diferente dele mesmo e da unidade. Agora, fatorar o número completamente nos inteiros, significa escrevê-lo como um produto de primos, configurando essa uma tarefa pelo menos teoricamente sempre possível, segundo o Teorema Fundamental da Aritmética.

Conforme se percebe de modo superficial através dos seus primeiros termos que serão exibidos numa quantidade suficiente para identificarmos qualquer número primo com até seis algarismos em Sistema Decimal. Uma simples consulta a Lista de Primos Consecutivos permite verificarmos que para esse subconjunto, nosso repertório deve contar com **165 divisores**, configurando certamente um resultado muito expressivo para abordarmos numa sala de aula. Chegamos a essa conclusão tomando o maior primo de seis dígitos disponível em tabelas amplamente divulgadas na internet e (contando) os termos que não superam a raiz quadrada desse primo.

2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97 101 103 107 109 113 127 131 137 139 149 151 157 163 167 173 179 181 191 193 197 199 211 223 227 229 233 239 241 251 257 263 269 271 277 281 283 293 307 311 313 317 331 337 347 349 353 359 367 373 379 383 389 397 401 409 419 421 431 433 439 443 449 457 461 463 467 479 487 491 499 503 509 521 523 541 547 557 563 569 571 577 587 593 599 601 607 613 617 619 631 641 643 647 653 659 661 673 677 683 691 701 709 719 727 733 739 743 751 757 761 769 773 787 797 809 811 821 823 827 829 839 853 857 859 863 877 881 883 887 907 911 919 929 937 941 947 953 967 971 977 983 991 997...

Como um II exemplo, vamos determinar a fatoração completa de 165 nos primos. Noutras palavras, escrever o mesmo como um produto de primos na hipótese dele figurar entre os compostos. Para isso, verificamos se o mesmo é divisível por três, donde vemos que a resposta é positiva. Assim, resulta: $165 = 3\,x\,55$. Repetimos o procedimento para o 55 cuja resposta é negativa. Aliás, nesse caso em particular, temos um critério de divisibilidade extremamente eficiente à nossa disposição, amplamente divulgado nos principais textos sobre a teoria elementar dos números.

Mas, esse mesmo número é divisível por cinco: $\mathbf{55 = 5\,x\,11,}$ donde resulta uma nova e definitiva maneira de escrevê-lo como um produto de primos: $\mathbf{165 = 3\,x\,5\,x\,11}$. Veja que nossa empreitada chegou ao final, já que o último quociente é ele próprio um primo. Tudo bem que nesse caso particular, foram necessárias apenas três divisões. Entretanto, não se engane com as aparências principalmente quando se trata dos primos assim como da fatoração completa de inteiros “maiores”.

O momento é ideal para recordarmos de que forma a DFP pode ajudar na identificação de números quadrados. Para isso, nada mais recomendável do que escolher um número quadrado e evidenciar a sua fatoração primária. Assim, considerando que $\mathbf{1.764 = 42^2 = (2)^2 x\,(3)^2\,x\,(7)^2}$ chamamos a atenção especificamente com relação à **Paridade dos expoentes** que integram a fatoração.

Na verdade, esse é o principal resultado que nos interessa quando da identificação de um quadrado perfeito. Assim, procedendo de forma semelhante com os demais quadrados, chegaremos à mesma conclusão:

3.3: Proposição. Um inteiro positivo será número quadrado perfeito se, e somente se, forem pares todos os expoentes integrantes da fatoração primária.

$$x = p_1^{q_1}.p_2^{q_2}.\ldots.p_n^{q_n} \iff x^2 = p_1^{2q_1}.p_2^{2q_2}.\ldots.p_n^{2q_n}$$

Agora, vale recordar que em último caso, decidir se um número inteiro é quadrado fica nesse contexto, reduzido a buscar sua decomposição em primos. Mas, já sabemos que esse configura outro problema ainda mais complexo em termos numéricos e computacionais da mais elevada importância na Teoria dos Números.

Sem mais delongas, percebemos facilmente que incorrer na busca pela fatoração nos primos para decidir se um inteiro positivo figura entre os quadrados perfeitos, definitivamente não é uma boa ideia, principalmente quando o número em questão não tem uma forma especial ou simplesmente representa um primo. A justificativa é muito simples: nessas condições, será exigido o máximo de recurso computacional para o sucesso da empreitada.

Agora, se o leitor decidir enveredar por esse caminho, pode acelerar o processo, dividindo o número em questão sempre por quadrados consecutivos, mas com a mesma paridade. De fato: admita que realizamos uma divisão por três que resultou exata. Em seguida, continuamos com o mesmo divisor de modo que a mesma agora resultou negativa.

Então, já estamos em condições de concluir que o número mencionado não é quadrado, pois isso exigiria que o três figurasse com expoente par. Mas, o expoente em questão vale um. De forma resumida, recomendamos a todos que sejam feitas divisões por quadrados consecutivos até que ao menos uma delas resulte exata.

Há mais um ponto que precisa ser esclarecido nesse momento: não estamos afirmando que todos os primos com seis dígitos exigem o mesmo número de divisões para a sua efetiva identificação, mediante a estratégia amplamente conhecida nos mais diversos textos como tentativas e erros**.** Ela consiste basicamente na divisão do número, cuja fatoração, queremos conhecer pelos primos consecutivos não superiores a raiz quadrada do número em questão.

3.4 Aplicações da Decomposição Primária

O conhecimento da Decomposição em Fatores Primos de um inteiro nos permite responder de uma forma praticamente imediata qualquer pergunta a seu respeito. Assim, somos capazes de determinar apenas como exemplo seu total de divisores positivos (Princípio Fundamental da Contagem) incluindo a listagem dos mesmos, caso isso seja realmente necessário. Outra aplicação que merece evidência consiste na classificação da Representação Decimal de um número Racional, donde sabemos que existem três casos para a expansão:

- ✓ Número Decimal Exato,
- ✓ Dízima Periódica Simples,
- ✓ Dízima Periódica Composta.

Não há dificuldades nesse contexto, pois tudo depende de dois fatores que assumem um papel muito especial na resolução desse Problema que pode ser considerado elementar, desde que não haja necessidade de buscar a sua Fatoração Primária pelos vários motivos já expostos nessa pesquisa de uma maneira muito objetiva. De modo que a essa altura, o leitor certamente já deve estar convencido das principais dificuldades que cercam essa busca com um destaque especial para o Tempo Médio de Processamento das divisões sucessivas via tentativas e erros.

Tudo isso, mediante as divisões sucessivas por primos consecutivos, cuja eficiência e praticidade são facilmente questionáveis por qualquer pessoa com um mínimo de conhecimento sobre a **Ciência da Computação**. Para uma ideia mais precisa, basta mencionar-se que inteiros positivos com apenas oito dígitos sem forma especial, podem exigir na pior das hipóteses (Primo) aproximadamente 1.200 divisões como acontece com todos os primos entre $9.967^2 = 99.341.089$ e $9.973^2 = 99.460.729$.

Esses dados revelam uma das maiores contradições durante a realização dessa investigação: O método mais utilizado em sala de aula para identificar os números quadrados perfeitos e calcular as suas raízes quadradas reside na busca pela sua decomposição nos primos ou forma canônica que figura entre as mais “inconvenientes” do ponto de vista especificamente computacional.

Estamos diante de uma verdadeira contradição didática, levando-se em conta a difícil tarefa de justificar esse procedimento em termos metodológicos que está enraizado de um modo geral na Educação Brasileira; para isso, basta consultar qualquer livro didático sobre o assunto que logo aparece a recomendação para tentarmos descobrir imediatamente a fatoração completa do número em questão que geralmente tem poucos dígitos, um fato que reforça essa importante tese.

Pelo menos os autores têm consciência desse fato quando escolhe números pequenos para a construção dos exercícios. Assim, temos a nítida impressão de que os professores, mergulhados sem sombra de dúvidas na sua zona de conforto, continuam insistindo nessa estratégia porque não têm Ciência de que há outras ferramentas disponíveis e capazes de dispensar a fatoração primária, mas que infelizmente não costumam ser abordadas durante a graduação.

Os gregos dentre os quais **Euclides**, já tinham uma ideia muito precisa a esse respeito, de modo que mesmo conscientes de que poderiam utilizar a fatoração para a determinação, por exemplo, do Máximo Divisor Comum (dentre outros), desenvolveram um algoritmo extremamente eficiente para essa finalidade que, aliás, não sofreu praticamente nenhuma alteração, mesmo após vários séculos da sua descoberta e publicação (Algoritmo Euclidiano Estendido).

Uma análise elementar permite concluir estarmos perante um Moderno Problema Computacional**,** cujos inconvenientes tanto numéricos quanto algébricos podem ser medidos superficialmente pelo número de divisões por primos consecutivos que crescem de forma certamente exponencial, evidenciando traços da sua complexidade.

Exigindo por tudo isso, a larga utilização de recursos “caros” como Tempo e memória**,** assim como profissionais cada vez mais qualificados, donde sabemos que os mesmos são indispensáveis para que o algoritmo suporte da solução computacional seja utilizado com toda a sua capacidade de processamento.

Veja que mesmo nos dias atuais, uma tarefa como fatorar completamente um número inteiro com apenas 180 dígitos decimais sem forma especial (escolhido de maneira aleatória) representa um grande desafio até mesmo para um supercomputador que em geral precisa de um intervalo de tempo absurdo da ordem de centenas ou até milhares de anos, dependendo principalmente da quantidade de dígitos (ordem de grandeza) que pode ser considerado um excelente parâmetro indicativo do custo computacional para obter a fatoração.

Não temos a menor pretensão de exagerar ao mencionarmos esses dados numéricos que aparecem amplamente divulgados em livros, revistas, periódicos, etc. já vimos que os especialistas em **Ciência da Computação** costumam escolher mediante a poderosa ferramenta da recém-descoberta Criptografia RSA (1.977) um par de números primos e multiplicá-los para a construção de uma Chave de Codificação Pública.

A justificativa é muito simples, se levarmos em conta principalmente que não ainda não temos métodos eficientes para fatorarmos “números grandes”, digamos com algumas dezenas de dígitos. Assim, tomando dois primos com 100 dígitos e multiplicando-os, obtemos um inteiro com 200 dígitos que também será extremamente difícil de fatorar, ficando atrás somente dos primos.

Essa informação parece contraditória se levarmos em conta que nos dias atuais, o maior **Primo de Merssene** conhecido mediante uma incrível utilização da nossa capacidade de computação no seu limite, tem quase $13.000.000$ de dígitos. Isso não quer dizer que sejamos capazes de fatorar completamente números com Ordem de Grandeza. Na verdade, estamos muito longe disso, os estudos mostram que em linhas gerais é muito mais "fácil" identificar primos grandes com uma forma especial do que fatorar números "grandes".

Esse parece configurar um verdadeiro dilema que levará muito tempo para avançarmos em direção à construção de **Métodos determinísticos** ou Testes de Primalidade com tempo de resposta polinomial e eficiente, se bem que qualquer avanço significativo pode ser facilmente superado pelos respectivos agentes de segurança, mediante a utilização de primos cada vez maiores e como há uma verdadeira infinidade deles ficam evidentes as maiores dificuldades do problema.

Acredito que a essa altura, fica claro o que de fato estou tentando dizer quando se afirma que o problema da busca pela fatoração completa de inteiros pode desfiar a humanidade por vários séculos ou quem sabe até vários milênios. O segredo está na base utilizada para representar os números, cuja expansão se pretende classificar, tomando como hipótese que a fração esteja na forma irredutível.

Em outras palavras, que tenhamos numerador e denominador primos entre si. Admitindo a utilização da Base Decimal, sabemos que $10 = 2\,x\,5$ de modo que ter-se-á uma representação decimal exata se, e somente se, esses forem os únicos fatores primos do denominador. Utilizaremos a sigla NDE para menção a esse caso.

Por outro lado, teremos uma Dízima Periódica Simples se, e somente se, nenhum daqueles fatores integra o denominador do racional em questão. Da mesma forma, adotar-se-á para este caso a sigla DPS. Assim, não restará dúvida sobre a natureza das representações que não ficam determinadas pelas suas expansões. Observe que quando escrevemos $X = 3,666\ldots$, não temos como garantir tratar-se de uma dízima periódica simples, pois as reticências indicam apenas uma expansão infinita.

Observe que esse caso é fácil de ser percebido, já que exige apenas a constatação de que o número presente no denominador não é divisível por 2 nem por 5 e sabemos da existência de **Critérios de Divisibilidade** bem práticos e eficientes associados a esses importantes fatores primos. Observe ainda que toda a nossa atenção está voltada para o denominador de modo que você deve está se perguntando qual o papel do numerador nesse contexto. A resposta é simples, se admitirmos mais uma vez que o racional em questão está na forma irredutível. Ele pode ser substituído pela unidade sem prejuízo para a classificação da representação decimal posta em discussão.

Como último caso a ser considerado, um número racional admitirá uma representação da forma **Dízima Periódica Composta** se, e somente se, verificarmos que o denominador é divisível por dois ou por cinco e pelo menos por outro fator primo diferente destes. Há dois outros vocábulos que surgem nessa pesquisa: **Dividendo e Divisor** que devem ser utilizados somente quando se busca a representação decimal de um número racional.

Nesse caso, tudo se passe como se os termos **antecedente e consequente** ganhassem novo significado. De uma forma mais precisa, temos que mediante a simplificação elencada, o antecedente assume o papel de numerador que por sua vez adquire o status de dividendo. Da mesma forma, o consequente atua como denominador, transformando-se posteriormente em divisor.

Já para o Consequente, temos que o mesmo assume o papel de denominador e posteriormente adquire o status de divisor. Observe que todos os termos mencionados estão envolvidos nesse contexto de uma forma muito particular, cuja distinção exige muita atenção da nossa parte quando levamos em conta a importante Questão da Linguagem Matemática sobre a qual acabamos de fazer uma espécie de mergulho, ampliando o nosso repertório de conceitos matemáticos e permitindo que a utilizemos de uma maneira mais eficiente.

Acredito que os comentários ficarão muito mais claros se tomarmos ao menos um exemplo numérico apelando novamente para os aspectos didáticos indispensáveis ao sucesso do nosso projeto de pesquisa, até porque, queremos que o Método das Terminações Características de Números Quadrados Perfeitos seja eficiente e razoável para uma abordagem na sala de aula principalmente no nível da educação básica, cujas carências são mais evidentes em relação ao nível superior de ensino.

3.5: Aplicação elementar: Representação Decimal de Racionais

Determine a natureza da representação decimal de cada uma das frações abaixo. A seguir, determine o período correspondente admitindo o mesmo diferente de zero.
$(a)\ 1/50$. Para isso, basta fatorarmos o denominador, donde obtemos 50 = 2^2 x 5. Pelo exposto, concluímos que se trata de um NDE: $1/50 = 0{,}02$. Além do mais, pode-se provar o número de casas decimais que fica determinado pelo maior dos expoentes que figuram naquela fatoração.

$(b)\ 1/21$. Procedendo da mesma forma com o denominador: 21 = 3 x 7. Ainda pelo exposto, fica evidente que se trata de uma dízima periódica simples (DPS). Procedendo com a respectiva divisão, resulta a seguinte expansão decimal 0, 047619047619..., ou seja, com período 047619.

$(c)\ 1/14$. Não há dificuldades com a fatoração do denominador. De fato, temos que 14 = 2 x 7. Novamente pelo exposto, fica evidente que se trata de uma dízima periódica composta (DPC), cuja expansão decimal corresponde a 0,0714285714285... , sendo o período 714285.

Um comentário adicional precisa ser feito para uma distinção mais completa dos três casos considerados: As dízimas periódicas compostas admitem um período que não aparece imediatamente após a vírgula, diferentemente das simples. Além do mais, o período de uma dízima também pode ser indicado, mediante um tracinho acima do(s) dígito(s) que se repetem indefinidamente. Aliás, essa é uma notação muito mais eficiente do que aquela normalmente encontrada na maioria dos livros.

3.6: Sobre a Partição Racional x Irracional

O fato é que em linhas gerais, não se pode classificar um número Real em racional ou irracional mediante apenas a sua representação decimal, salvo para o caso em que a mesma é finita ou infinita previsível como vemos em $\mathbf{7,12112111211112111112}\ldots$ (irracional), admitindo que o evidente padrão que não indica periodicidade (fundamental para a classificação em questão) seja mantido em toda a sua extensão decimal.

Caso isso seja possível, deve-se indagar sobre a efetiva quantidade de dígitos necessários para a realização dessa tarefa. Assim, mediante uma análise mais rigorosa sobre a representação decimal dos números reais, não faz muito sentido problemas como aqueles nos quais se exibe uma representação decimal (para a qual sempre existe um único real associado) e solicita-se que o leitor decida se o número em questão é um número racional.

Estamos perante um problema clássico de aritmética que exige um pouco mais de maturidade dos professores quando da sua abordagem em sala de aula. Imagine que seja fornecida a seguinte expansão de um número Real: $\mathbf{7,122122122122122122}\ldots$ (racional ou irracional?). O leitor deve levar em conta a partição oriunda dos números reais com relação à possibilidade do mesmo ser racional ou irracional. Aliás, seria muito interessante uma notação especial para nos certificar da manutenção do padrão nas expansões decimais de tais números.

Agora, experimente descobrir mediante qualquer estratégia o que acontece na continuidade dessa representação. Na verdade, não temos a menor ideia do que vem a seguir como se pudéssemos utilizar um termo oriundo da Estatística e dizer que essa “amostra” em questão não é “significativa” a ponto de se descobrir como se comporta o restante da dízima. Talvez você deva está se perguntando como isso é possível se estamos diante de uma dízima periódica simples? Observe que se conhece apenas 18 dígitos da sua representação infinita e através dos mesmos não temos a menor ideia de como determinar os demais.

Somente o contexto aliado à notação decimal pode nos dá condições suficientes para afirmar tratar-se de uma Dízima Periódica Simples, Composta ou mesmo um número Irracional. De fato, considere a possibilidade de que a continuidade daquela representação esteja associada um número irracional, bastando para isso que a notação decimal em questão seja aperiódica. Afinal de contas, essa possibilidade é perfeitamente viável de modo que a essa altura, o leitor já deva está convencido a respeito da impossibilidade de se classificar um número real em racional ou irracional tomando como parâmetro apenas a sua notação decimal.

Não entraremos em mais detalhes pelo simples fato de que o nosso verdadeiro objetivo, consiste em mostrar ao leitor que existe uma teoria matemática madura e capaz de auxiliar o trabalho de um matemático, sempre que ele precisar obter excelentes (na verdade, as melhores) aproximações decimais de números irracionais quadráticos. Assim, não seria prudente, deixar o leitor alheio a esses comentários como se quiséssemos passar a falsa impressão de que essa nova ferramenta chamada Método das Terminações Características não tem concorrentes a sua altura quando se trata de aproximar irracionais.

Capítulo IV

A Distribuição dos Números Quadrados

Um Pouco de História

O primeiro trabalho realizado contendo expectativas e previsões quanto aos resultados sobre jogos de azar é encontrado no **Livro dos Jogos de Azar,** do matemático italiano Gerolamo Cardano, publicado no ano de 1560. Coube, porém a **Blaise Pascal** (1.623–1.662) e **Pierre de Fermat** (1.601–1.665) o desenvolvimento da Teoria das Probabilidades. O interesse de Pascal e Fermat para com os problemas relativos às probabilidades se deve aos pedidos dos nobres, jogadores profissionais, em especial de seu amigo Chevalier Méré.

Pascal escreveu a Fermat sobre esses tipos de problemas e questões a eles relacionadas. A correspondência entre eles passou a ser considerado o ponto de partida para o estabelecimento da **Teoria Matemática das Probabilidades.** Embora nem Pascal nem Fermat tivessem publicado seus resultados, o holandês **Cristhian Huygens** (1.629 – 1.695) ao visitar Paris, ouvindo falar dessa correspondência, interessou-se por ela. Ele próprio procurou respostas àqueles problemas e o resultado foi o livro **O Raciocínio nos Jogos de Dados***,* (1.657), o primeiro tratado sobre possibilidades baseado no conceito de Esperança Matemática.

> Daí em diante, a teoria das probabilidades deixou de se preocupar tão somente com os jogos de azar e direcionou-se para outras áreas. Contribuíram para isso o suíço Jacques Bernoulli (1.654–1.705), Abraham De Moivre (1.667–1.751) e Pierre Simon Laplace (1.749–1.827). Atualmente, ela representa um poderoso instrumento para as mais diversas áreas do conhecimento, como Economia, Administração, Biologia, em especial no ramo da Genética, com grande aplicação na Agricultura e criação de animais. (Bianchini, 1.995).

4.1: Definição de probabilidade a priori

Considere o experimento aleatório, de fácil reprodução que consiste no lançamento de um dado comum e não viciado, cujas faces foram numeradas como 1, 2, 3, 4, 5 e 6. Um dos conceitos mais importantes nesse contexto, diz respeito ao **Espaço Amostral** que consiste no conjunto de todos os resultados possíveis de um experimento que apresente alguma Regularidade Estatística**.** Admita ainda que esta haja interesse em determinar as possibilidades da face voltada para cima ser número par. Acredita-se que é natural postular, de inicio, que todas as faces têm a mesma "possibilidade" de assumir a posição superior. Então, há um evento (subconjunto do espaço amostral) associado no qual se tem interesse: E = {2, 4, 6}.

Mas, a palavra possibilidade já equivale de certa forma, à palavra probabilidade, precisamente o conceito que tentamos definir. Temos aqui um exemplo clássico de circularidade, impossível de se contornar completamente: A definição da coisa pela coisa. Nesse sentido, dizemos que o experimento em questão tem um **Espaço Amostral Equiprovável**. Tem-se aqui um modelo para o estudo das probabilidades que é simplesmente fundamental, pelo menos numa primeira abordagem à teoria em questão. Assim, de acordo com a Definição de Laplace (1.814), temos:

"A probabilidade é o quociente do número de casos favoráveis pelo número de casos possíveis". (**Maciel**, Vozes; 1974).

Assim, como são seis os casos possíveis e levando-se em conta que todos têm a mesma chance de assumir a posição superior, pode-se dizer que cada um dos membros no espaço amostral constitui um Evento Elementar com uma Probabilidade de $1/6$. Mas, o evento no qual estamos interessados é formado por três elementos (composto), sendo assim, conclui-se ainda pela definição clássica que a sua probabilidade é igual a $3/6 = 1/2$. Costuma-se expressar os resultados através das porcentagens, portanto o evento em questão tem Probabilidade de 50%.

4.2: Definição de Probabilidade a Posteriori

Percebe-se que a definição de Laplace não é capaz de abarcar todos os problemas relativos à probabilidade. Noutras palavras, com o passar do tempo, os matemáticos depararam-se com problemas impossíveis de superar, mediante a definição clássica, quer dizer, ela certamente não tem um **caráter universal**. A dificuldade formal mais séria da definição a priori de probabilidade é a que surge quando o número de casos possíveis é infinito**.** Aliás, exatamente o que acontecerá quando se iniciar a análise da sequência dos números quadrados em termos distributivos. Agora, tem-se um experimento que pode ser considerado mais "Complexo" com relação ao primeiro:

Escolhido um número inteiro positivo, qual a probabilidade de que o mesmo represente um quadrado perfeito? Há princípio, não tem como realizar essa divisão.

Nesse caso, fica evidente que não se pode recorrer à definição clássica, assim ela tem que ser ampliada ou substituída por outra capaz de responder a perguntas como essa formulada acima. Do contrário, isso exigiria a divisão de duas quantidades infinitas: Os números quadrados pelos números inteiros, mas como fazer isso no contexto da definição de Laplace? Está-se aqui diante de uma tarefa impossível, mostrando-nos as limitações conceituais advindas da sua adoção, mesmo assim, não se pode desprezar a sua importância histórica, notadamente na da educação básica, onde ela se faz presente quase que com certa exclusividade.

Assim como na graduação onde a mesma tem papel relevante no estudo da Teoria das Probabilidades, sem falar que não existe uma definição universal, tudo depende do contexto onde se está inserido. Os problemas mais fortes exigem uma definição axiomática, tendo-se em vista o sucesso dessa abordagem no contexto da Geometria Euclidiana que permaneceu inalterada por quase dois mil anos, mostrando o caminho que outras teorias deveriam seguir para resistir principalmente aos ataques eminentemente Filosóficos.

Quer dizer, no contexto da educação básica não há um contato mesmo que superficial com outra definição de Probabilidade, salvo algumas menções pontuais que exigem um esforço muito maior dos estudantes, ao que parece, não sendo fixado pela sua grande maioria, dadas as dificuldades inerentes à mesma e diretamente relacionados com a Lei dos Grandes Números.

A compreensão exige que se faça uma menção a esta lei assim como a ideia de regularidade estatística, sem a qual, não temos condições de utilizar as ferramentas da Teoria Matemática das Probabilidades, constituindo Um modelo matemático para descrição e interpretação dos fenômenos que mostram uma regularidade estatística.

Insiste-se que a busca por uma definição universal de probabilidade tem desafiado a comunidade matemática há pelo menos quatro séculos. A justificativa para tal dificuldade pode ser compreendida levando-se em conta que ela representa, de certa forma a resposta da Matemática para uma antiga questão Filosófica conhecida como a **Teoria da Contingência**. Ainda de acordo com Maciel, temos:

“Numa palavra, define-se a contingência como a possibilidade de que “algo” seja (ou aconteça) e a possibilidade de que “algo” não seja (ou não aconteça)”.

Em termos filosóficos, somos conduzidos a duas possíveis linhas de análises para uma Contingência, conforme esse algo seja uma Proposição, resultando o **Sentido Lógico**, por outro lado, quando esse algo for outro objeto qualquer, temos o **Sentido Ontológico**. Logo, pode-se concluir que à Teoria Matemática das Probabilidades corresponde a Teoria Filosófica das Contingências. Um detalhe que precisa ser mencionado diz respeito à importância dessas duas teorias:

> “Ora, o lugar dessas duas teorias acha-se implicitamente assegurado em função do fato de que o conhecimento que o homem tem das coisas é sempre incompleto. Quer dizer, na medida em que ele ignora fatalmente e em certa medida as condições dentro das quais este ou aquele fenômeno se realizará, terá de lidar com processos, cujos resultados finais são essencialmente aleatórios, ou seja, sujeitos ao acaso.” (Maciel**,** Pag. 334 – 335).

Numa tentativa de contornar essas dificuldades, ou seja, buscar uma ampliação dessa ideia matemática fundamental nasce a Definição de Probabilidade a posteriori, isto é, uma definição baseada na observação e na indução. Para isso, deve-se entender uma Probabilidade como uma medida da frequência com que determinado evento acontece quando se repete um experimento aleatório o maior número de vezes possível. Na verdade, quanto mais repetirmos o experimento, nas mesmas condições, mais confiáveis serão as nossas conclusões subsequentes.

É fato comprovado que a repetição de um experimento aleatório como o lançamento de um dado ou uma moeda, repetidas vezes apresenta certa regularidade de caráter nitidamente estatístico. Assim, admitindo-se que o experimento seja repetido n vezes e que o evento de interesse tenha ocorrido com uma frequência absoluta F_a. Definimos a frequência relativa do evento como $Fr = Fa / n.$ A experiência mostra que para n “muito grande”, o quociente acima tende a se estabilizar e assumir um valor constante, desde que a análise esteja apoiada na Lei dos Grandes Números.

Chamamos de Probabilidade a Posteriori, precisamente o limite desse quociente quando o número de experimentos tende ao infinito. Percebe-se assim que o conceito de Probabilidade como frequência relativa é mais abrangente e eficiente do que a definição a priori. No entanto, uma análise mais apurada que não será posta em prática, mostra que ela não está completamente isenta de dificuldades lógicas. Veja que ela depende da experiência, exigindo a repetição do experimento um grande número de vezes o que nem sempre é possível ou desejável pelos mais variados motivos.

4.3: Definição de Probabilidade Axiomática

Numa tentativa mais recente de ampliar o alcance daquele conceito e superar as dificuldades notadamente lógicas, a teoria das probabilidades passou a ser fundamentada de modo axiomático, muito provavelmente devido ao sucesso da Axiomatização no universo da Geometria Euclidiana.

Define-se assim, o conceito matemático de probabilidade através dos três axiomas a seguir: Considere uma função definida no conjunto de todos os resultados possíveis de um experimento aleatório, ou seja, espaço amostral probabilístico que associa um número real a cada um dos eventos elementares do espaço em questão. A função mencionada deve satisfazer os seguintes axiomas:

(I) Para todo acontecimento A, $0 \leq P(A) \leq 1$,

(II) Ao espaço amostral corresponde à probabilidade máxima, $P(S) = 1$;

(III) Se A e B são mutuamente exclusivos, $P(A \cup B) = P(A) + P(B)$.

Já vimos que a disposição dos números quadrados constitui uma sequência estritamente crescente de inteiros positivos com $a_1 = 1$. Agora, veja que a mesma disposição para os cubos perfeitos, também gera uma sequência com todas aquelas características. Assim, deve-se buscar destacar mais informações sobre a sequência daqueles números, de modo que eles sejam devidamente caracterizados.

Tudo isso porque um dos nossos principais objetivos consiste no aprofundamento das suas propriedades, mediante análise da sua disposição clássica, amplamente divulgada nos textos tradicionais sobre a teoria elementar dos números. Para isso, far-se-á uso do chamado Operador Diferença de fundamental importância para o estudo das sequências de números Reais, especialmente quando estes são inteiros.

4.4 Definição de Progressão Aritmética

Define-se uma progressão aritmética (P. A) como toda sequência de números Reais na qual a diferença entre termos consecutivos resulta sempre numa constante. Devido a sua importância, essa constante será chamada de razão da progressão. Apenas como exemplo tome os ímpares positivos de termo geral $\boldsymbol{A(n) = 2n - 1}$ para verificar que a mesma se encaixa perfeitamente na definição acima. Quer dizer, termos consecutivos daquela sempre diferem por 2. De fato, basta verificar-se que:

$$\mathbf{A}\,(\boldsymbol{n}) = \boldsymbol{2n - 1} \implies \boldsymbol{A}\,(\boldsymbol{n+1}) - \boldsymbol{A}\,(\boldsymbol{n}) = \boldsymbol{2}, \forall \boldsymbol{n}.$$

Na verdade, os termos de uma progressão aritmética não precisam ser necessariamente números inteiros. Mas, essa restrição é fundamental para uma abordagem eficiente das suas propriedades, se levarmos em conta que as principais discussões desse projeto de pesquisa têm como foco o Conjunto dos Inteiros Positivos, dada a nossa disposição para encontrarmos um método eficiente com vistas à identificação de números quadrados perfeitos e cálculo de suas raízes.

Evitando sempre a busca pela sua Decomposição em Fatores Primos pelos vários expostos relacionados às enormes dificuldades de se obter essa representação. Há um detalhe que não se pode deixar passar em branco: Consideramos apenas os n primeiros termos de uma sequência infinita de Reais, não há como saber, rigorosamente falando e de acordo com a definição acima, se a mesma representa de fato uma progressão aritmética.

Pelos nossos estudos de matemática elementar, sabe-se que uma disposição de números inteiros define uma P.A se, e somente se, o termo geral da mesma é um polinômio do 1º grau numa variável. No caso de uma sequência finita, deve-se calcular todos os pares de diferenças entre termos consecutivos para concluirmos, na hipótese de resultados iguais, tratar-se de uma progressão aritmética.

Quer dizer, a operação em questão deve ser realizada, enquanto se verificar resultados iguais para a mesma. Não custa recordar uma importante classificação das progressões aritméticas de números Reais em relação especificamente ao seu crescimento, de acordo com a sua razão. São três os casos que se deve considerar:

(1) a progressão será crescente se a razão for positiva,
(2) a progressão será decrescente se a razão for negativa,
(3) a progressão será constante se a razão for zero.

Esse fato ocorrerá sempre, pois estamos no universo das **sequências monótonas,** todas aquelas cujo comportamento em termos de crescimento não pode sofrer qualquer tipo de variação que possa ser considerada “abrupta”.

Noutras palavras, será impossível para uma P.A crescer numa dada região e decrescer ou permanecer constante noutra região e vice-versa, fazendo da mesma uma sequência “bem comportada”, pelo menos nesse sentido. Entretanto, não se deve subestimá-las, pois dependendo da perspectiva sob qual ela é observada, é possível se deparar com dificuldades teóricas praticamente intransponíveis, pelo menos à primeira vista.

Não podemos negar que aquela característica representa um facilitador para os nossos estudos. Assim, concluímos que o **Comportamento Global** em termos de crescimento das progressões aritméticas de números reais, fica completamente determinado pelo seu **Comportamento Local.** Infelizmente, essa conclusão não pode ser generalizada, pois sabemos que não é possível definir qualquer Relação de Ordem no Campo dos Números Complexos.

4.5: Soma dos Primeiros Termos

Quando se aborda as progressões aritméticas principalmente no ensino médio, sabe-se que há um resultado dos mais importantes que precisa ser explorado nesse contexto. Ele diz respeito à soma dos seus n primeiros termos. Felizmente, trata-se de um problema simples e certamente compreensível para a maioria dos alunos da Educação Básica. A questão fica mais clara quando se leva em conta que a soma de dois termos equidistantes dos extremos é igual à soma dos extremos.

Essa constante facilita bastante a descoberta de tal fórmula, pois permite que seus termos sejam reduzidos pela metade. Naturalmente, considerando somente as progressões finitas, caso contrário, não faria sentido buscar a soma dos elementos. Assim, basta agrupar os seus temos aos pares de acordo com a propriedade para concluirmos que a soma em questão vale:

$$S(n) = (a_1 + a_n)\ n/2.$$

Observe que ela representa uma função quadrática, fato que fica mais claro quando se leva em conta que $\mathrm{A}(n) = a_1 + (n-1)R$**.** Procedendo com as devidas substituições, conclui-se que $S(n) = [Rn^2 + (2a_1 - R)n]\,1/2$**.** Uma análise mais apurada mostra que a mesma indica uma função desprovida de termo independente.

Será visto nas próximas linhas que o grau deste polinômio exige que de certa forma seja atribuída uma espécie de ordem às progressões aritméticas, não que as mesmas coincidam, entretanto, guardam uma relação simples e que nos permite superar diversos problemas.

Mais precisamente, vale ressaltar que se o termo geral de uma P. A é polinômio de grau n, então a soma dos seus n primeiros termos é um polinômio de grau n + 1, desprovido de termo independente. Nesse sentido, voltando nossa atenção para a sequência dos números quadrados, é fato que sendo a mesma uma P.A, cujo termo geral vale $\boldsymbol{A(n) = n^2}$**,** então à soma dos n primeiros termos, associa-se um polinômio de grau três com termo independente nulo. Dos nossos estudos de álgebra, sabemos que tais polinômios ficam determinados por apenas três pontos.

$$S(n) = an^3 + bn^2 + cn^1$$

Dessa forma, não há maiores dificuldades para se encontrar o mesmo. De fato, sendo $S(1) = 1$, $S(2) = 5$ e $S(3) = 14$, resulta um sistema de equações lineares, cuja solução é $S(n) = (2n^3 + 3n^2 + n)\,1/6$. Mais apropriadamente:

$$S(n) = [n\,(n+1)(2n+1)]\,1/6.$$

Finalmente, justifica-se esse procedimento, tendo-se em vista que os mesmos permitem conhecer a sequência dos números quadrados com maior profundidade. Assim, a essa altura, já reunimos diversas informações que fazem da mesma um objeto fascinante, sem dúvidas, porém menos misterioso.

O momento é ideal para se definir a ordem de uma progressão aritmética. Sabe-se que nessas sequências, a diferença entre termos consecutivos resulta numa constante (R) utilizada para a sua caracterização, ao lado termo inicial (a_1). Agora, tem-se conhecimento de outras sequências nas quais essa constante aparece, logo após a tomada dessa diferença por duas ou mais vezes. Isso ocorre com os quadrados: **(1, 4, 9, 16, 25, 36,...**). De fato, realizando essa operação duas vezes, resultam respectivamente as sequências (**3, 5, 7, 9, 11, 13,...) e (2, 2, 2, 2, 2, 2,...)**.

4.6: Operador Diferença

Seja A o conjunto de todas as sequências de números Reais. Define-se o operador diferença e o indicaremos por Δ como sendo a função Real com domínio no conjunto A e que associa a cada par de termos consecutivos de $\boldsymbol{A(n)}$**,** sua diferença. Em outras palavras: Δ: A → $\mathbb{R}$ / $\Delta\, \boldsymbol{A(n) = A(n+1) - A(n)}$.

Infelizmente, esse é um daqueles importantes conceitos que de forma quase inexplicável não costuma ser abordado na Educação Básica, pelo menos não de uma forma explícita. Na verdade, mesmo nos cursos de graduação, praticamente não se encontra referências a esse conceito, principalmente nos currículos de Matemática que representa o nosso maior interesse.

Logo, define-se a ordem de uma progressão aritmética como o número de vezes que o operador diferença deve atuar até obtermos uma sequência constante não nula, desconsiderando aquelas com termos iguais, dada a sua enorme simplicidade. Assim, não há maiores dificuldades em verificar serem necessárias exatamente duas atuações do Operador em questão para obtermos uma sequência constante.

De fato: A$(n) = n^2 \Longrightarrow A(n+1) = (n+1)^2$, de modo que $\Delta A(n) = (n+1)^2 - (n^2)$, donde se obtém: $\Delta A(n) = 2n + 1$. Veja que não indica uma sequência constate.

Agora, observe o que acontece após uma nova atuação do operador no resultado da primeira. Seja $\mathrm{B}(n) = 2n + 1 \Longrightarrow \mathrm{B}(n + 1) = 2n + 3.$ Assim, concluímos que $\Delta B(n) = 2$. Nesse sentido, se diz que a sequência dos números quadrados perfeitos constitui uma progressão aritmética infinita crescente de inteiros positivos, determinada pela fórmula geral $\mathrm{A}(n) = n^2$. Além disso, pelo exposto a mesma é de segunda ordem.

Quando não mencionarmos a ordem de uma progressão aritmética, deve ficar subtendido tratar-se duma sequência de primeira ordem. Veja que nesse momento, não existe mais a possibilidade de confundirmos aquela com a sequencia dos cubos perfeitos, conforme os comentários iniciais. Isso quer dizer que apesar das características em comum (infinitas, crescentes, inteiros), basta considerarmos a atuação do operador diferença para uma verdadeira caracterização de ambas.

Assim, conclui-se que a disposição dos cubos perfeitos representa, na verdade uma progressão aritmética infinita crescente de inteiros positivos, mas de terceira ordem. O leitor já deve ter percebido que se o termo geral de uma sequência é um polinômio de grau n, então a mesma indica uma progressão aritmética de ordem n.

Estabelecemos uma relação entre a ordem e o grau do polinômio que determina o termo geral de uma progressão aritmética. Tenho a obrigação de chamar a atenção do leitor principalmente para alguns aspectos relativos tanto à identificação quanto a distribuição dos números quadrados entre os naturais, procurando responder fundamentalmente à seguinte pergunta:

Qual a probabilidade no sentido axiomático do termo de que um número inteiro positivo que seja escolhido aleatoriamente represente um quadrado perfeito?

A busca dessa resposta permite um conhecimento mais profundo sobre a sequência dos números quadrados, de fato concluiremos que a Probabilidade é zero**.** Esse é um resultado chocante para muitas pessoas que ainda presas ao conceito clássico de probabilidade (Laplaciana) responderiam imediatamente: como pode ser isso, eu sei que existem quadrados perfeitos?

Mas, numa análise mais apurada, sabemos da existência de eventos com probabilidade nula, mas que simplesmente não são impossíveis, sendo isso muito comum nos casos em que o Espaço Amostral associado ao evento em questão é infinito, seja ele Enumerável ou não. Agora, não podemos deixar de mencionar a veracidade da sua recíproca, ou seja, se um dado evento de um espaço amostral é impossível, então não há dúvidas de que a sua probabilidade de fato é nula.

Quando se afirma que os números quadrados são uma “minoria” entre os naturais, não existe a menor pretensão de alimentar a ideia (certamente equivocada) de que existem menos números quadrados do que não quadrados. Na verdade, mesmo numa abordagem elementar através da **Aritmética Transfinita**, sabe-se da possibilidade de se estabelecer uma Correspondência Biunívoca entre cada um desses subconjuntos e os Naturais. Numa linguagem mais moderna, se diz ainda que ambos os conjuntos mencionados nesse parágrafo têm a mesma Cardinalidade.

Na ponta desses comentários, somos capazes de tirar outras conclusões bem interessantes como a probabilidade de que um número natural (sem forma especial) escolhido aleatoriamente não figure entre os quadrados perfeitos. Por mais incrível que pareça, levando-se em conta principalmente que esses números são muito mais frequentes do que os quadrados, não encontraríamos maiores dificuldades para o cálculo da referida Probabilidade. De fato, basta recorrermos ao Conceito de Eventos Complementares, cuja soma das probabilidades resulta sempre na unidade e que continua válido mesmo quando os conjuntos são infinitos como ocorre aqui.

Assim, chega-se à conclusão de que a probabilidade em questão vale 100%. Agora, há pelo menos um ponto que precisa ser esclarecido nesse momento: O fato é que no sentido moderno do conceito fundamental de probabilidade não podemos concluir tratar-se de evento certo, quer dizer, apenas a proposição recíproca é verdadeira, ou seja, se um evento é certo então a sua probabilidade é 100%. Acredito que a essa altura das discussões, o leitor já deve ter percebido as peculiaridades que circundam o conceito de probabilidade que atualmente ocupa papel central na Estatística.

As várias leituras necessárias ao desfecho dessa pesquisa mostram-nos que o mesmo vem sendo moldado pelos matemáticos, tanto profissionais quanto amadores (Fermat) há mais ou menos quatro séculos. Ainda assim, ainda não existe um consenso sobre o mesmo em contextos mais gerais, tudo isso principalmente por causa dos aspectos relacionados à Questão da Continuidade que nasce na Filosofia e deságua na Matemática. Aliás, como também ocorre com a ideia de infinito, já que hoje sabemos ser possível contar os elementos de conjuntos desse tipo, mediante o artifício da Correspondência Biunívoca, tomando os Naturais como referência.

Faremos agora uma análise elementar sobre a Distribuição dos números quadrados perfeitos entre os inteiros positivos que certamente permitirá um maior aprofundamento no conhecimento daquela que direta ou indiretamente, figura como uma das mais importantes sequências matemáticas, pelo menos depois dos números primos. Essa notoriedade fica evidente principalmente quando voltamos nossa atenção, dentre outros para o clássico Problema da representação de inteiros positivos como uma soma de quadrados, remetendo-nos ao **Teorema de Lagrange**:

“Todo número natural pode ser obtido, mediante uma soma de no máximo quatro quadrados”. Nesse sentido, vale mencionar um texto do professor **Paulo Ribenboin,** publicado na Revista Matemática Universitária (edição 20, 1.996) no qual se analisa a chamada **Conjectura de Catalan** que assim como outras afirmações clássicas, tem um enunciado muito simples, mas que desafia toda a comunidade matemática. Considere a sequência dos inteiros positivos que são cubos ou quadrados perfeitos:

1, 4, 8, 9, 16, 25, 27, 36, 49, 64,...

Um fato chama a nossa atenção imediatamente quando a observamos com um pouco mais de cuidado: observe que os termos 8 e 9 são inteiros consecutivos. A primeira questão que pode ser levantada, diz respeito à existência de outros pares, cujos termos são consecutivos.

Da mesma forma, devemos indagar quantos são os pares com essa propriedade? Finitos? Infinitos? Na verdade, estes enunciados pertencem a uma classe mais ampla de problemas que continuam em aberto. Estão relacionadas às sequências das potências de primos consecutivos. Em 1.899, Catalan conjecturou que 8 e 9 são os únicos inteiros consecutivos de potências perfeitas em relação a primos.

Questionamentos semelhantes podem ser feitos, dentre os quais, destacamos o problema da existência de três inteiros consecutivos que são potências perfeitas, ainda em aberto. Além disso, o texto menciona um terceiro problema de mesma natureza, mas com a diferença de que os primos não são necessariamente consecutivos, mas a sequência é finita. Ainda assim, fica evidente a manutenção da Complexidade, visto que ainda não se conhece uma solução para tais problemas.

Seja E um conjunto não vazio e finito de primos e E^X o conjunto de todos os números naturais, cujos fatores primos pertencem a E. Quantos são os pares de inteiros consecutivos que figuram em E^X?

Ainda de acordo com Ribenboin, todos os problemas que acabamos de enunciar podem ser expressos na Linguagem das Equações Diofantinas**.** Assim, o primeiro deles equivale a descobrir raízes para qualquer uma das equações abaixo nos números naturais. Uma tarefa que a princípio parece simples, mas tem se mostrado muito difícil, exigindo esforços descomunais.

$$x^2 - y^3 = 1, x^3 - y^2 = 1.$$

Já o último dos problemas pode ser descrito pela simples equação $\boldsymbol{X - Y = 1}$. Todas essas dificuldades estão de alguma forma, relacionadas com a restrição que fazemos no conjunto verdade (solução). Quer dizer, impor a condição de que as raízes sejam inteiros positivos torna diversos problemas bem mais complicados do que quando considerados, por exemplo, no Corpo dos Reais. Sem dúvidas, o fato das sequências de potências crescerem rapidamente torna difícil a sua abordagem.

Na continuidade do texto, o autor aborda os principais avanços obtidos no ataque à primeira das conjecturas mencionadas. Esses avanços datam de aproximadamente 1.320 e são devidos a **Levi Bem Gerson**, famoso astrônomo da época. Ele demonstrou que, de fato, 8 e 9 são as únicas potências de 2 e 3 expressas por dois números consecutivos. Nas palavras do autor, a prova hoje é considerada um exercício trivial de congruências, apesar disso, a mesma será omitida.

Voltando a questão da representação de números naturais como soma de quadrados, deve-se tomar muito cuidado para evitar conclusões precipitadas, enquanto analisamos a frequência relativa dos números quadrados. De fato:

> "Note, por exemplo, que 10% dos naturais até 100 são quadrados, 1% são quadrados até 10.000, até 1.000.000, apenas 1 em cada 1.000 são quadrados, e assim por diante. Apesar dessa rarefação de quadrados, Lagrange provou que todo número natural pode ser escrito como uma soma de no máximo quatro quadrados. É Como se quadrados estivessem ocupando posições estratégicas" (**Ribenboin**, RMU – 45).

São abordados ainda os métodos algébricos e analíticos que se mostraram bem sucedidos diante dos problemas de Catalan. A conjectura dos primos gêmeos também foi mencionada como não poderia deixar de ser, dada a sua importância histórica, assim como o fato da mesma continuar nos desafiando. Por último, são analisados diversos problemas que guardam semelhança, onde os mesmos foram divididos nas seguintes categorias especiais: Problemas de Adição, Problemas de subtração, Números Primos.

Essa análise permitirá verificar-se definitivamente a necessidade de da construção de um novo Método de cunho algébrico que seja capaz principalmente de identificar números quadrados, evitando a todo custo a "espinhosa" busca pela sua DFP pelos vários motivos já expostos com destaque especial para aquilo que podemos chamar de "inconvenientes computacionais" como o Tempo Médio de Processamento para as divisões sucessivas por primos consecutivos e recursos de memória associados.

Tudo isso, admitindo-se a não utilização de métodos de identificação mais eficientes, haja vista estarmos concentrados no nível da educação básica. Esse problema figura certamente como um dos mais explorados na modernidade que coloca à nossa disposição uma tecnologia verdadeiramente surpreendente, mesmo para aquelas pessoas que admitem uma formação mais sólida na Matemática Aplicada.

Sabemos que uma das primeiras providências consiste em descobrirmos como se comportam dois termos consecutivos quaisquer da referida sequência. Quer dizer, dado um número quadrado qualquer, sabemos onde surgirá o próximo quadrado? Veremos, a seguir que a resposta para essa questão é positiva.

Antes, vale destacar um resultado que apesar de elementar e facilmente comprovável, desempenhará um papel crucial nesse contexto: A diferença entre quadrados consecutivos vale 2n + 1**.** Dizemos que dois quadrados perfeitos são consecutivos quando as suas raízes quadradas são números inteiros consecutivos.

Esse resultado é importante porque abre caminho para que possamos realmente avançar em nossa análise distributiva. Na verdade, também podemos interpretar o resultado acima de outra forma: Todo número ímpar pode ser escrito como uma diferença de quadrados que na “pior das hipóteses” (Primo) são consecutivos e ainda de fácil determinação.

A essa altura, fica clara a existência de sequências arbitrariamente longas formada por inteiros positivos e consecutivos que não figuram entre os números quadrados. Elas são realmente de fácil obtenção, conforme teremos oportunidade de verificar na relação de desafios colocada à disposição do leitor no final do material de pesquisa.

Apenas dois casos precisam ser considerados durante a resolução desse subproblema, conforme os aspectos de paridade. O passo seguinte exige que procuremos a resposta para uma pergunta, cuja importância é simplesmente fundamental para o desfecho dessa análise essencialmente distributiva sobre a sequência dos quadrados perfeitos:

4.7: Contando Números Quadrados

Aspectos Históricos

A continuidade dessa análise exige a adoção de novas definições e teoremas que a rigor só podem ser encontradas em obras mais específicas e modernas da teoria avançada dos números, visto que os textos tradicionais não fornecem instrumentos suficientes para uma resposta satisfatória àquela pergunta. Assim, adotaremos o texto da III Bienal da Sociedade Brasileira de Matemática: Densidade de Shnirel' Man, Teorema de Mann e a Conjectura de Goldbach. O ponto de partida do texto diz respeito ao enunciado dessa Conjectura:

Todo número inteiro $n > 5$ pode ser obtido mediante a soma de 3 Primos.

No entanto, ainda segundo o texto: O Matemático suíço Euler logo percebeu que essa conjectura poderia ser reescrita de uma forma muito mais eficiente:

Todo número par $2n \geq 4$ pode ser obtido através da soma de dois primos.

A seguir, são apresentados casos particulares que nos permitem constatar a validade da Conjectura. Tudo isso fornece os primeiros indícios e facilita o contato inicial com esse problema, cuja importância para a história da matemática é inquestionável. Tem-se aqui um problema com enunciado simples, mas de solução extremamente difícil, haja vista desafiar a comunidade matemática há quase três séculos. O momento é oportuno para evidenciar o papel da computação frente à conjectura de Goldbach, pois a mesma permite a verificação de sua validade para um número muito maior de inteiros positivos, permitindo a continuidade da pesquisa.

4 = 2 + 2, 6 = 3 + 3, 8 = 3 + 5, 10 = 5 + 5, 12 = 7 + 5, 14 = 11 + 3 = 7 + 7, 16 = 11 + 5, 18 = 11 + 7, 20 = 17 + 3, 22 = 19 + 3 = 17 + 5.

Um fato que chama a atenção inicialmente é a existência de números pares que admitem mais de uma representação como uma soma de dois primos.

Mas, essas verificações tornam-se cada vez mais difíceis, à medida que n aumenta, com isso, pode-se perceber um pouco das enormes dificuldades enfrentadas pelos matemáticos ao tentar demonstrá-la. Sem falar da existência de inteiros que admitem duas ou mais representações desse tipo, evidenciando uma importante perda de Unicidade em comparação com a representação multiplicativa clássica que também utiliza os números primos, donde sabemos que ela é única, a menos da ordem e sinais dos fatores utilizados. Além disso:

> "Apesar da simplicidade do seu enunciado, progressos significativos na resolução do problema de Goldbach só vieram a ocorrer na primeira metade do século XX. Aproximadamente 200 anos após a carta recebida por Euler, em 1930, o matemático bielo-russo Lev G Shnirel'man deu aquele que é considerado o primeiro grande passo no sentido de responder afirmativamente a Conjectura de Goldbach, propondo e demonstrando o seguinte teorema" (Eduardo Leandro & Gabriel Guedes, III Bienal da SBM, 2.006).

Existe uma constante S_0 tal que todo número inteiro maior do que 1 é a soma de no máximo S_0 números primos. Ele encontrou $S_0 = 300.000$ como valor inicial para essa constante. Desde então, vários matemáticos mergulharam numa tentativa (bem sucedida) de reduzir essa constante. O texto destaca ainda que o menor valor obtido até hoje corresponde a $S_0 = 6$ o que representa uma excelente estimativa, visto que a demonstração da Conjectura de Goldbach corresponde, de fato, a $S_0 = 3$.

Outras sequências também são abordadas no texto como aquela na qual todos os seus termos são livres de números quadrados, donde se conclui que a mesma tem Densidade maior do que $1/2$. Da mesma forma, as progressões geométricas que nos são mais familiares, sendo possível demonstrar que todas têm Densidade de Shnirel'man nula. Vale destacar ainda o seguinte resultado:

> "Um lugar especial no estudo da densidade de sequências de naturais é ocupado pelo Teorema de Mann, segundo o qual a densidade da soma de duas sequências é maior ou igual que a soma das densidades das sequências somadas - em termos mais técnicos, diz-se que a densidade de Shnirel'man é superaditiva". (Eduardo Leandro & Gabriel Guedes, III Bienal da SBM, 2.006).

Naturalmente, não abordaremos os pormenores do Teorema de Mann, incluindo a sua demonstração, visto que implicaria desvio dos nossos objetivos. Veremos apenas como ele definiu o conceito de densidade de uma sequência estritamente crescente de inteiros positivos com primeiro o termo unitário. Destacamos, por último, o maior objetivo do texto que nos serve de referência, consistindo precisamente na busca por métodos elementares da Teoria Aditiva dos Números.

Um destaque especial para aqueles que permitem saber quando uma determinada classe de números naturais (pares, ímpares, primos, compostos, etc.) pode ser completamente descrita através da soma dos elementos de uma sequência em particular. Nesse sentido, podemos fazer uma "releitura" da conjectura de Goldbach, afirmando que três cópias dos números primos são suficientes para a obtenção de qualquer número Natural.

Para que o leitor tenha uma ideia mais precisa sobre a importância deste Teorema, basta acrescentar que podemos situar nesse contexto a famosa Conjectura de Goldbach, segundo a qual todo número par maior do que dois pode ser escrito como soma de dois primos, figurando como um dos mais fantásticos problemas da Matemática em aberto. Se bem que há uma evidente perda de Unicidade nesse domínio com relação especificamente ao Teorema Fundamental da Aritmética.

Esse é um resultado que certamente pertence à Teoria Aditiva dos Números na qual não se pretende entrar diretamente, devido a sua enorme complexidade sem falar que esta é uma área de pesquisa muito recente (com menos de um século) de modo que mesmo aqueles resultados eventualmente considerados mais elementares ainda não se fazem presentes de um modo geral nos cursos de graduação em Matemática, assim como na pós-graduação. Serão tomados números quadrados como ponto de partida e procurar-se-á responder à pergunta crucial aos objetivos relacionada com a frequência dos números quadrados em intervalos de amplitudes cada vez maiores, descobrindo o que acontece com o limite do quociente no infinito. Para isso, será confeccionada uma tabela através da qual se pode concluir que o total de números quadrados que existem até um dado n corresponde ao $[\sqrt{n}]$.

Logo, considerando toda essa discussão, fica evidente que a resposta corresponde àquele inteiro mais próximo, porém, não superior à raiz quadrada do número em questão. Na verdade, somos conduzidos à Função Máximo Inteiro (função escada). Estamos diante de um contexto no qual o conceito de raiz quadrada adquire uma espécie de novo significado: Indica a quantidade de quadrados perfeitos que não superam um determinado número natural. A ideia de comparar esses pares de resultados associados, através de uma razão surge de uma forma espontânea e remete-nos ao moderno conceito de Densidade das sequências constituídas por inteiros positivos, a começar pela unidade, donde exigimos ainda que a mesma seja estritamente crescente.

Ressalte-se também que a possibilidade já explorada de representar qualquer inteiro ímpar como uma diferença de quadrados pode ser utilizada como uma ferramenta ainda em estudo para uma Tomada de Decisão sobre a classificação dos naturais em Primos ou Compostos (Método da Fatoração de Fermat). Agora, um mesmo ímpar pode admitir várias expansões desse tipo, mas essa conclusão não vale para os Primos. Sabe-se que para estes, essa eficiente representação é única, fazendo desta uma das mais fortes distinções com relação aos números ímpares compostos.

4.8: Definição da densidade de uma sequência

Seja A uma sequência estritamente crescente de inteiros positivos a começar pela unidade. Vamos denotar por A (n) a quantidade de termos da mesma que não superam o inteiro n. Segue daí que a razão $A(n)/n \in [0,1]$. Denotaremos por D(A) a Densidade de A, definida por D(A) = inf. $\{A(n)/n\}$, onde "**inf.**" significa o maior dos números Reais que não excedem cada um dos termos.

Em linhas gerais, dois fatos são fundamentais no estudo das Distribuições:
(1) Uma sequência de números naturais possui Densidade máxima, D(A) = 1 se, e somente se, ela coincide com o conjunto N dos números Naturais.
(2) Toda sequência com Densidade positiva pode desempenhar papel de Base.

Procedendo dessa forma, concluímos facilmente que a Densidade dos ímpares é $1/2$. De fato, a sua fórmula do termo geral é $I(n) = 2n - 1$. Agora, devemos responder a seguinte pergunta: Quantos são os números ímpares que não superam $I(n)$. Uma inspeção elementar permite concluir sobre a existência de n + 1 termos com essa propriedade.

Assim, de acordo com a definição, temos que $A(n) = n + 1,$ de modo que a Densidade corresponde ao Inf. $\{(n+1)/(2n-1)\}$. Observe que todos os termos desta sequência são números positivos, de modo que seu ínfimo certamente coincide com o limite.

Assim, concluímos que esse limite vale $1/2$. Observe ainda que o limite que acabamos de calcular corresponde exatamente ao inverso da sua razão. Veremos daqui a pouco que isso não é aquilo que eventualmente podemos chamar de uma coincidência Matemática. Tomamos a sequência dos ímpares positivos como referência simplesmente pelo fato da mesma representar uma das mais elementares progressões aritméticas de primeira ordem nos inteiros.

O momento é oportuno para interpretarmos o resultado em termos Probabilísticos: Temos assim que a probabilidade de um inteiro positivo, escolhido aleatoriamente ser ímpar vale 50%. Infelizmente, não temos como abordar esse resultado na educação básica, devido tanto ao conceito de infinito como de limite, sem falar da necessidade de recorrermos a Teoria Axiomática das Probabilidades que convenhamos não é uma tarefa elementar.

Agora, o leitor não pode esquecer em momento algum que estamos adotando o conceito de Probabilidade no sentido axiomático do termo, ou seja, como o limite da frequência relativa quando o número de experimentos tende ao infinito. Uma interpretação mais forte desse resultado, associado à densidade dos ímpares positivos pode ser vislumbrada, admitindo a possibilidade de representar qualquer natural mediante uma soma de ímpares.

Nesse sentido, basta descobrir quantos ímpares são necessários, no mínimo para efetuarmos tal representação que é aditiva e pouco abordada. Tomemos como exemplo 24 = 13 + 11. Observe que o número escolhido é par o que é muito razoável, já que o ponto de partida são os ímpares de modo que não faz sentido uma interrogação semelhante para os mesmos.

Assim, conclui-se que com no máximo dois ímpares, somos capazes de representar qualquer número par. Em linhas mais gerais, resulta que mediante a utilização de apenas duas cópias dos ímpares, pode-se representar através duma soma, qualquer número natural. Esse é o verdadeiro significado da densidade de uma sequência de inteiros positivos a começar pela unidade. Ela nos diz quantas cópias da mesma são necessárias, no mínimo para escrever qualquer número natural mediante uma soma, cujas parcelas devem figurar entre os termos da referida sequência.

Aliás, esse é o grande questionamento implícito na famosa Conjectura de Goldbach**,** segundo a qual (supostamente) somos capazes de representar todos os naturais mediante uma soma de no máximo três primos.

Enquanto não conseguimos demonstrar (ou refutar) uma afirmação desse nível; utilizamos toda a nossa capacidade de processamento para continuar alimentando-a. Isso é muito importante, pois permite obtermos cada vez mais indícios e continuar com as investigações nesse campo de pesquisa extremamente promissor com impacto relevante nas mais diversas áreas de estudo.

Toda essa análise permitirá concluir que a Densidade de uma progressão aritmética de primeira ordem formada por inteiros positivos a começar pela unidade, corresponde ao inverso da sua razão. Apenas como curiosidade, uma investigação semelhante para as Progressões Geométricas de inteiros positivos indica que elas também têm uma Densidade nula, equiparando-se, pelo menos nesse sentido à sequência dos primos, cuja incrível Distribuição, mostra-se evidentemente mais Complexa e fundamental para a solução de diversos problemas, ainda em aberto.

Mencionamos as progressões geométricas pelo fato de sabermos que elas têm muitas aplicações (finanças) e uma constituição relativamente simples, sem falar que também costumam ser abordadas na segunda série do ensino médio, imediatamente após o estudo das progressões aritméticas. Mas, infelizmente, podemos destacar uma distinção muito forte com relação ao aspecto de crescimento em comparação com as aritméticas: quando a razão da P.G é negativa, verificamos que os sinais alternam-se indefinidamente.

4.9 Proposição. A Densidade de uma progressão aritmética I (n) de primeira ordem, formada por inteiros positivos (a_1 = 1) é igual ao inverso da sua razão.

Demonstração. De fato, seja $I(n) = a_1 + (n-1)R$. Devemos responder quantos são os termos da mesma que não superam o número $I(n)$. Mediante uma análise elementar, concluímos que $A(n) = n$. Assim, de acordo com a definição de Densidade explorada, concluímos que ela é igual ao Inf. $\{n/I(n)\}$.

Nesse momento, utilizaremos os conhecimentos de Cálculo Diferencial e Integral com destaque para os Limites no Infinito, envolvendo uma razão entre funções Polinomiais com domínio Real. Na oportunidade, aprendemos que o limite em questão fica determinado pela razão dos termos de maior grau.

$$\lim_{n \to \infty} [n/I(n)]$$

A justificativa para tal procedimento é simples: como todos os termos da sequência em questão são inteiros positivos, então seu ínfimo coincide com o limite em questão. Logo, dividindo todos os termos por n, obtemos uma nova função: $F'(n) = 1/[a_1/n + (n-1)/nR]$, cujo limite deve ser calculado em duas etapas. Veja que a primeira parcela constante no denominador tende a zero, já a segunda tende a um. Assim, concluímos que o limite em questão vale $1/R$**.**

Vislumbramos agora a possibilidade de calcularmos a Densidade dos números quadrados perfeitos, levando-se em conta principalmente que a mesma representa uma progressão aritmética de segunda ordem de inteiros positivos. Na verdade, ao que parece, podemos estabelecer uma regra geral para o cálculo da Densidade de uma progressão aritmética com essas características em função da sua ordem.

Os primeiros indícios mostram que todas aquelas com ordem superior a 1 têm Densidade nula, noutras palavras, cubos, quartas, quintas potências, etc. Sem dúvidas, trata-se de um resultado evidente até certo ponto, levando-se em conta que as frequências dessas potências diminuem à medida que se avança nos naturais.

Na hipótese de se confirmar a veracidade dessa informação, podemos tirar algumas conclusões interessantes, dentre às quais: a Probabilidade nula de que um natural escolhido aleatoriamente represente um cubo perfeito. Enunciaremos nas próximas linhas o principal resultado deste capítulo que está diretamente associado à Probabilidade no sentido axiomático de que um inteiro positivo, escolhido aleatoriamente, represente um número quadrado perfeito.

4.9.1 Teorema

A sequência dos números quadrados perfeitos tem densidade igual a zero.

Demonstração. $Q(n) = n^2 \rightarrow A(n) = [\sqrt{n}]$. Assim, D(A) = $Inf.\left(\left[\sqrt{n}\right]/n\right)$.

Uma análise sobre esse quociente revela que seu limite no infinito é zero. Como a função em questão é estritamente decrescente e positiva, temos que D (A) = 0.

Tabela 2: A Distribuição dos Números Quadrados

n	$[\sqrt{n}]$	$[\sqrt{n}]/n$
9	3	0,33333333333
54	7	0,12962962962
324	18	0,05555555555
1.944	44	0,02263374485
11.664	108	0,00925925925
69.984	264	0,00377229080
419.904	648	0,00154320987
2.519.424	1.587	0,00062990588
15.116.544	3.888	0,00025720164
90.699.264	9.523	0,00010499533
544.195.584	23.328	0,00004286694
3.265.173.504	57.141	0,00001750014
19.591.041.024	139.968	0,00000714449
117.546.246.144	342.850	0,00000291672
705.277.476.864	839.808	0,00000119074

Capítulo V

Introdução à Aritmética Modular

Visando facilitar a compreensão dos principais resultados que serão apresentados nos próximos capítulos, algumas noções são fundamentais de serem exploradas, dentre elas, destaca-se a Relação de Divisibilidade e suas propriedades mais relevantes, o algoritmo de Euclides assim como o Mínimo Múltiplo Comum e o Máximo Divisor Comum entre dois ou mais números inteiros. Apresentaremos ainda o Teorema Fundamental da Aritmética, tendo-se em vista a sua inegável importância para demonstração dos resultados mais notáveis da teoria dos números, tanto em nível elementar quanto avançado.

Antes, porém, será feito um breve comentário sobre a definição geral de relação, cuja justificativa pode ser dada levando-se em conta os vários tipos de relações que surgirão no decorrer do texto, algumas mais simples, outras nem tanto. Assim, nada mais natural do que começar essa apresentação, buscando-se a definição de relação mais apropriada para o contexto. Falamos dessa forma, porque há toda uma problemática de **natureza filosófica** envolvida nessa discussão. Mesmo assim, algumas restrições precisam ser consideradas, sem as quais será impossível avançar na compreensão dos conceitos necessários para se desenvolver o MTC.

Levando-se em conta o fato de que em sua maioria, tais conceitos e propriedades têm ampla divulgação e são conhecidos do público em geral, constituídos por professores ou mesmo alunos da graduação, serão omitidas algumas demonstrações, mas que podem ser encontradas na bibliografia correspondente. Dessa forma, permitir-se-á a construção de um texto objetivo, leve, enxuto, coerente e de fácil entendimento, sendo a situação ideal. Além disso, serão abordadas as relações de equivalência, haja vista existir sempre uma partição associada.

O nosso principal exemplo de Relação de Equivalência será a Congruência Modular que sem a menor sombra de dúvidas, revolucionou o estudo da Aritmética, permitindo tratar de uma forma muito mais eficiente e elegante os principais resultados sobre Divisibilidade, possibilitando a obtenção de muitos outros segundo verificar-se-á no decorrer da exposição. Foi o grande matemático alemão Carl Friedrich Gauss (1.777–1.855) quem introduziu este conceito (1.801) no seu livro Disquisitiones Aritmeticae (Investigações Aritméticas) quando tinha apenas 24 anos.

Quando Gauss começou a trabalhar na sua obra, a Teoria dos Números era meramente uma amálgama de resultados isolados. Em Disquisitiones, ele introduziu a noção de congruência e, ao fazê-lo, simplesmente unificou a Teoria dos Números. Várias das ideias utilizadas atualmente nesse campo foram introduzidas no seu trabalho, uma Obra Prima da Matemática.

Até mesmo o símbolo de Congruência (≡) com o qual se trabalha hoje em dia, já era utilizado por Gauss naquela época. Trazendo simplicidade e elegância para a álgebra, o trabalho de Gauss é a prova de que uma boa notação é a principal engrenagem para uma Teoria bem sucedida.

De um ponto de vista estritamente lógico, uma Relação é, em geral, um conjunto de pares ordenados; mais precisamente, uma Relação é uma Classe de pares (x, y) para os quais certa Função Proposicional F(x, y) é verdadeira. Quer dizer, pode-se substituir toda uma gama de valores em lugar de x, de modo que a função se transforma numa proposição propriamente dita. Matematicamente, entretanto, o conceito de Relação assume um sentido mais específico. Isso significa que, por trás de toda Relação haverá sempre um produto cartesiano de dois ou mais conjuntos.

Suponha que se tem em S uma Relação de Equivalência. Seja dado ainda um elemento qualquer x de S; considerando C_X o conjunto de todos os elementos de S equivalentes a x, então, todos os elementos de C_X são equivalentes entre si; como consequência imediata das propriedades de Simetria, Reflexividade e Transitividade características de uma Relação de Equivalência, como consequência da Definição.

Além disso, pode-se mostrar facilmente que se x e y são elementos quaisquer de S, então ou $C_x = C_y \, ou \, C_x e \, C_y$ não têm elementos em comum, noutras palavras, são disjuntas**.** Diz-se ainda que cada C_X indica uma Classe de Equivalência. Assim, claramente vê-se que Relação de Equivalência determina uma Decomposição de S.

5.1: Tipos Especiais de Relação

Relação Inversa.

Se R é uma relação de A e B, chama-se relação inversa de R, e se nota R^{-1}, a Relação cujos pares ordenados quando invertidos a sua ordem transformam-se exatamente nos pares de R. Assim, podemos escrever que (a, b) $\in R^{-1}$ se, e somente se, (b, a) $\in$ R.

Relação Reflexiva.

Uma relação R definida em um conjunto A, diz-se Reflexiva se, para todos os a em A, tivermos que (a, a) pertence a R. Em outras palavras, a Relação de Reflexividade consiste em que um ente qualquer tem consigo mesmo a própria Relação. A Relação de Identidade é o exemplo clássico de Relação Reflexiva.

Relação Simétrica.

Uma Relação R definida em um conjunto A é Simétrica se para todos a, b em A tivermos: Se a ~ b então b ~ a. Podemos escrever também se (a, b) pertence a R então (b, a) pertence a R, um exemplo de Relação Simétrica é a Diversidade.

Relação Antissimétrica.

Uma relação R definida em um conjunto A é antissimétrica se para todos a, b em A tivermos a ~ b e b ~ a então a = b. quer dizer, a existência de um par afasta a possibilidade do par simétrico. A Relação de Inclusão é antissimétrica.

Relação Transitiva.

Uma relação R diz-se transitiva quando para todos a, b e c tivermos se a ~ b e b ~ c então a ~ c. Que se interpreta da seguinte forma: a relação de a para b e de b para c implica na relação de a para c. A relação, por assim dizer, transita de a para c. através do termo médio.

Relação de Ordem.

Uma relação R definida em um conjunto A, é uma relação de ordem se é simultaneamente reflexiva, antissimétrica e transitiva. Esta Relação é também importantíssima seu estudo, entretanto, por conduzir aos chamados Reticulados, não poderá ser feito aqui. As Relações Unívocas são particularmente importantes para a Matemática, que as estuda quase que com exclusividade. São elas também de fundamental importância para a **Teoria Geral dos Sistemas** embora, para esta, sejam igualmente importantes e necessárias as Relações Multívocas.

5.2 A Relação de Divisibilidade

Definição: Relação de Divisibilidade. Dados dois números inteiros a e b com $b > 0$, diremos que a divide b, se e somente se, existirem únicos inteiros q e r, tais que verifiquem a seguinte relação $a = bq + r$, sendo $0 \leq r < b$.

Notação: $\boldsymbol{a \mid b \Leftrightarrow \exists\, q\, e\, r\ /\ a = bq + r}$.

Por outro lado, diremos que a não divide b, se, e somente se, não existirem inteiros q e r tais que $a = bq + r, com\ 0 \leq r < b$.

Notação: a $\boldsymbol{\nmid b \Leftrightarrow \nexists\, q\, e\, r / a = bq + r}$.

Exemplo. Nesse sentido, dizemos que $7 \mid 14$, pois $\exists\, 2 \in \mathbb{N}/14 = 2x7$. Por outro lado, temos que $11 \nmid 24, pois \nexists\, q \in \mathbb{Z}/11xq = 24$.

Definição 5.3: Algoritmo de Euclides. Dados dois números a e b com b > 0, temos que existem únicos q e r com 0 ≤ r < q que satisfazem $a = bq + r$.

O algoritmo de Euclides representa um processo com presença garantida nos mais variados problemas da teoria dos números, justificando a sua importância. Um excelente exemplo consiste na determinação do **Máximo Divisor Comum** de dois ou mais inteiros que permite, dentre outras, resolver equações de congruências, equações Diofantinas, etc. Ele aparece ainda na teoria das frações contínuas, onde se atribui uma única representação para cada número Real, dotada de propriedades que fazem da mesma uma linguagem superior.

Agora, um dos resultados mais fantásticos obtido por Euclides no campo da Aritmética está diretamente relacionado à questão da Sequência dos Primos, mais especificamente no que diz respeito à quantidade de primos. Euclides demonstrou que existem infinitos números primos. Noutras palavras, dado um primo qualquer, existe sempre outro primo maior do que ele.

Esse é um resultado fantástico para aquela época, levando-se em conta todas as condições políticas, econômicas, sociais, culturais, etc., características da antiguidade e que não contribuíam em geral com o desenvolvimento da Matemática. A demonstração em questão é considerada por vários escritores da Teoria dos Números uma das mais belas, notadamente pela simplicidade dos seus argumentos que podem ser compreendidos com muita facilidade, inclusive por amadores.

Ela contém um resultado profundo da Aritmética cuja demonstração é de fácil compreensão mesmo para um iniciante. Posteriormente, outros matemáticos como **Goldbach** encontraram novas demonstrações para a infinidade (Enumerável) dos primos levando em conta a existência de sequências infinitas nas quais dois termos quaisquer da mesma são primos entre si de modo que cada um dos seus membros apresenta ao menos um primo que não aparece nos demais termos da sequência.

Para isso, esse brilhante matemático tomou como referência os “Primos de Fermat”, apesar de se saber hoje, graças principalmente a Euler que tais números não são todos primos de modo que ficamos mais inclinados numa direção contrária à proposta incialmente por Fermat, donde se passa a acreditar que não há outros primos desse tipo, diferente dos conhecidos na atualidade de acordo com todos os indícios colocados à nossa disposição com o advento da Ciência da Computação.

Aliás, esse é um fato que particularmente nos chama a atenção há muito tempo. Em geral, os matemáticos precisam de muitos indícios para começar a acreditar na existência de uma regularidade ou padrão numérico, geométrico, algébrico etc. até mesmo nossos professores costumam destacar como alerta que o fato de uma propriedade ser verdadeira para centenas, milhares ou milhões de números não significa necessariamente que ela seja verdade para os demais números inteiros.

Essa ideia figura como uma lição básica sobre o ensino da Matemática mesmo em nível elementar. Sendo assim, cabe perguntar como um Matemático do porte de Fermat, mesmo não sendo profissional correu esse tremendo risco ao fazer uma afirmação dessa magnitude sobre os inteiros daquela forma? Imagine como a história seria diferente se ele tivesse resistido.

Quer dizer, ele conhecia apenas quatro números primos daquela forma. Essa é uma quantidade insignificante para acreditar-se na existência de alguma propriedade ou regularidade matemática. Ao refletir sobre essa intrigante questão, sobram pouquíssimas alternativas capazes de sustentar a crença desse genial matemático.

Ainda nesse sentido, mesmo não possuindo formação acadêmica e dedicando-se à matemática apenas nas suas horas de lazer; projetou seu nome entre os maiores matemáticos de todos os tempos com destaque para o campo da Aritmética, sendo ele considerado o fundador da Moderna Teoria dos Números, haja vista toda a estagnação matemática constatada até a época do seu nascimento.

Naquela época mais remota dos pitagóricos assim como a de Euclides, essas ideias envolvendo números primos e números compostos já estavam bem maduras segundo a literatura sobre o assunto principalmente com relação à obra de Euclides de Alexandria (os Elementos). Dentre elas, pode-se destacar mais uma partição associada aos números naturais: Um número natural qualquer será primo ou composto, porém, nunca as duas coisas**.** O conceito de paridade pode ser utilizado com sucesso numa primeira abordagem ao problema da identificação de números quadrados perfeitos, aliado ao Método da falsa posição, mediante tentativas e erros.

O leitor deve concordar que esse é um daqueles feitos que merece uma atenção especial da nossa parte enquanto educadores no sentido de procurar, sempre que possível, divulgar um pouco da vida e obra desse verdadeiro gigante da Matemática. Vale lembrar que ele também trouxe contribuições para outras áreas da Matemática como na Geometria Analítica ao lado do Francês Rene Descartes (1596 - 1650).

Se bem que em geral costuma-se por uma questão talvez de tradição escolar, atribuir praticamente todos os créditos pela criação da Geometria Analítica a Descartes mediante outra obra prima da Ciência: **O Discurso do Método.** Mas, de forma surpreendente, sabe-se que os números de Fermat são dois a dois primos entre si. Com relação aos números compostos, conclui-se facilmente que também são infinitos assim como se verifica para os primos. Nesse sentido, é possível sim estabelecer uma bijeção entre o conjunto dos primos e o conjunto dos compostos.

Aliás, encontra-se nesse contexto envolvendo Euclides, Grécia antiga e números primos o primeiro registro histórico da utilização de uma poderosa técnica para as demonstrações: **Redução ao Absurdo**. Ela consiste basicamente em adotar uma ou mais hipóteses contrárias à que se quer demonstrar e mediante manipulações algébricas, aritméticas ou geométricas mostrar que as mesmas nos levam a uma contradição. Dessa forma, sendo constatada a contradição, não existe alternativa senão rejeitar as hipóteses tomadas inicialmente como Verdadeiras, isso equivale a demonstrar aquela hipótese contrária (Lógica Binária) na qual estamos interessados.

Assim, em linhas gerais, para demonstrar que existem infinitos primos, admite-se como hipótese que os primos são finitos e mediante uma manipulação apropriada e adoção de alguma propriedade característica dos primos, somos levados a uma contradição. Claro que o leitor que deve recordar nesse momento os três Postulados da Lógica Clássica, com destaque especial para o Princípio do Terceiro Excluído, através dos quais foram obtidos resultados fantásticos da Matemática. Verifica-se de forma imediata que a Relação de Congruência acima definida é de Equivalência no sentido de que goza das seguintes propriedades:

Proposição 5.4 Princípio da Boa ordenação. Seja $X \subset \mathbb{N}$. Se X $\neq \emptyset$, então X possui um elemento mínimo.

Proposição 5.5 (Princípio da indução finita – primeira forma) Seja P(n) uma propriedade associada a cada $n \in \mathbb{N}$. Se P é válida para p = 1 e vale para n = k + 1 sempre que vale para n = k, então P é válida para todo $n \epsilon \mathbb{N}$.

Proposição 5.6 (princípio da indução finita – segunda forma) Seja P(n) uma proposição associada a cada $n \in \mathbb{N}$. Se P é válida para n = 1 e vale para n = k + 1 sempre que vale para todo n = i ($i \epsilon I_n$), então P é válida para todo $n \epsilon \mathbb{N}$.

Definição 5.7: Máximo divisor comum: Sejam a e b inteiros com $a \neq o\, e\, b \neq 0$. O máximo divisor comum (MDC) de a e b, denotado por m.d.c. (a, b), é um inteiro positivo que satisfaz as condições:

(i) $d \mid a\, e\, d \mid b$

(ii) $Se\ \exists\ c \in \mathbb{Z}\ tal\ que\ c \mid a\, e\, c \mid b, então\ c \mid d$

O item (i) nos diz que m.d.c. (a, b) é um divisor comum de a e b. Já o item (ii) diz que d é o maior divisor comum de a e b.

Exemplos:

Como podemos verificar $mdc\,(15{,}36) = 5, mdc\,(-6,-18) = 6, mdc(17,29) = 1$. Neste caso, dizemos que os números são primos entre si.

Calcular o MDC de tais números não é uma tarefa difícil, pois são relativamente pequenos, em outras palavras, formados por poucos dígitos. Quer dizer, não há maiores dificuldades na determinação dos conjuntos de seus divisores para em seguida, operarmos com a interseção de ambos os conjuntos citados. Entretanto, essa mesma tarefa pode se tornar um verdadeiro desafio, se os números são mais extensos ou aparecem em maior quantidade.

Na verdade, os livros didáticos em geral recomendam considera a fatoração primária de cada um dos inteiros. De fato, sendo conhecida essa fatoração, podemos determinar facilmente o MDC dos números em questão. Para isso, basta tomar os fatores comuns em ambos com os menores expoentes. Felizmente, podemos recorrer ao algoritmo de Euclides estendido que dispensa a fatoração primária, uma vantagem operacional que nunca foi superada, mesmo depois de tantos séculos.

Proposição 5.8: Da definição de MDC dada resultam as propriedades abaixo:

(i) $mdc\ (a,b)\ =\ mdc\ (b,a)$
(ii) se a é não nulo, então $m.d.c.(a,0)\ =\ |a|$
(iii) se $a|b$, então $mdc(a,b)$ = $|a|$.

As demonstrações são decorrentes diretamente da definição, por isso, as deixaremos a cargo do leitor. O momento é oportuno para uma indagação: Será que sempre existe o MDC de dois inteiros dados? Na hipótese de uma resposta positiva, será que O MDC é único? Felizmente, há um teorema que garante tanto a existência quanto a unicidade do Máximo Divisor Comum.

Naturalmente, essa é uma questão bastante antiga, cuja demonstração é conhecida também há muito tempo. Assim, ela pode ser encontrada em praticamente qualquer livro sobre a teoria elementar dos números. Um corolário importante diz respeito à possibilidade de representar o MDC de a e b, mediante uma combinação linear. Assim, existem únicos m e n tais que $d\ =\ am\ +\ bn,$ onde d é o MDC de a e b.

Há vários outros teoremas relacionados ao conceito de máximo divisor comum, entretanto, eles não são necessários para a compreensão geral do método das terminações características. Assim, a nossa decisão de abordar esse conceito superficialmente, está relacionada à sua inegável importância no contexto geral da teoria dos números. Ao lado do mínimo múltiplo comum, formam duas poderosas e indispensáveis ferramentas que permitem avançar cada vez mais nesse universo.

Definição 5.9: Dados os inteiros a e b, definimos seu Mínimo Múltiplo Comum, m.m.c. (a, b) como o menor inteiro positivo múltiplo de ambos os números.

Exemplo. Sejam a = 15 e b = 12, temos então que conforme a definição acima:
$M(15) = \{(15, 30, 45, 60, 75, 90, \dots)\ e\ M(12) = \{(12, 24, 36, 48, 60, 72, 84, \dots)$.

Assim, concluímos facilmente que MMC (15, 12) = {60}. Logo, a consequência imediata da definição acima é: $M(15) \cap M(12) = M(60)$. Aqui, utilizamos a notação M(a) para indicar o conjunto de todos os múltiplos do número inteiro a.

Da mesma forma que fizemos com o MDC, podemos calcular o MMC de dois números atentando para a sua decomposição nos primos. Para isso, basta calcular o produto dos fatores comuns e não comuns de a e b com os maiores expoentes. Mas, aqui também, chamamos a atenção para as dificuldades de obtenção dessa fatoração. Assim, o momento é dos mais oportunos para mencionar a relação:

$$mdc\ (a, b) x\ mmc\ (a, b) = a.b$$

Devido a mesma, temos que a forma mais eficiente de determinar seus respectivos valores consiste na determinação inicial do MDC para em seguida:

$$mmc\ (a, b) = ab/mdc(a, b).$$

Temos aqui outro conceito fundamental na teoria dos números, mas que será pouquíssimo utilizado. Por isso, a sua apresentação de forma tão superficial.

Definição 5.9.1: Relação de Congruência Modular.
Seja n um inteiro positivo e x, y inteiros quaisquer. Diz-se que x é congruente a y Módulo n se, e somente se existe um número inteiro m tal que $x - y = mn$.

Notação: $\boldsymbol{X \equiv Y\ Mod\ n \iff \exists M \in \mathbb{Z} / X - Y = Mn}$.

Como por hipótese n ≠ 0, haja vista desempenhar o papel de divisor, concluímos que x – y é um inteiro divisível por n ou ainda um de seus múltiplos.

Baseando-se em Divisibilidade, o conceito de congruência modular decorre da, bem como acarreta a multiplicidade de um número em relação à diferença de outros dois. Ou melhor, analisar se há congruência entre dois números é o mesmo que analisar se n é múltiplo da diferença desses números. Será visto a seguir que várias propriedades decorrem diretamente da congruência de dois números e problemas que antes eram difíceis de solucionar, foram resolvidos de forma rápida e elegante.

Escrevemos a Relação de Congruência: $X \equiv Y\ Mod\ n$ Se, porém, n não é um múltiplo de x - y, então, dizemos que X não é congruente a Y módulo N.

Notação: $x \not\equiv y\ Mod\ n \iff \nexists\ m \in \mathbb{Z} / x - y = mn$.

Exemplos: $12 \equiv 2\ (mod. 5), pois\ 12 - 2 = 10\ e\ 5|10$. Também podemos afirmar que $13 \equiv -2\ (mod. 5), pois\ 13 - (-2) = 15\ e\ 5|15$.
Porém, veja que $42 \not\equiv 13\ (mod\ 2), pois\ 42 - 13 = 29\ e\ o\ 2\ não\ divide\ o\ 29$.

Uma das principais propriedades da Congruência, a dela ser uma Relação de Equivalência, será estabelecida pela próxima proposição. Com ela, se ganha a liberdade de realizar manipulações de modo a obter ainda mais propriedades que serão de grande utilidade. Além de ser uma Relação de Equivalência, a Congruência Modular tem propriedades interessantes. O próximo Teorema justifica a afirmação de que a mesma pode ser considerada uma “igualdade” na maioria dos casos.

Reflexiva. $X \equiv X\ (Mod\ n)$, $\forall X$.
Como $n \mid 0$, segue-se que $n \mid (x - x)$, logo $x \equiv x\ (mod\ n)$.

Simétrica. Se $X \equiv Y\ (Mod\ n)$, então $Y \equiv X\ (Mod\ n)$.
$X \equiv Y(Mod\ n) \rightarrow n \mid (X - Y)$. Logo, $n \mid (Y - X) \rightarrow Y \equiv X\ (mod\ n)$.

Transitiva. Se $X \equiv Y\ (Mod\ n)\ e\ Y \equiv Z\ (Mod\ n)$, então $X \equiv Z\ (Mod\ n)$.
Se $X \equiv Y\ e\ Y \equiv Z$, então $n \mid (X - Y)\ e\ n \mid (Y - Z)$. Logo, $n \mid [(X - Y) + (y - Z)]$, isto é, $n \mid (X - Z)$, donde concluímos que $X \equiv Z$.

5.9.2 Teorema

Se a, b, c, d e n são inteiros, tais que $a \equiv b\ (mod.n)\ e\ c \equiv d\ (mod.n)$, então:
(I) $a + c \equiv b + d\ (mod.n)$, em particular $a + k \equiv b + k\ (mod.n)$.
(II) $ac \equiv bd\ (mod.n)$, em particular, $ak \equiv bk\ (mod.n)$.

Demonstração. (I) Como, por hipótese, $a \equiv b\ (mod.n)\ e\ c \equiv d\ (mod.n)$, segue que existem k_1, k_2 inteiros tais que $a - b = nk1\ e\ c - d = nk2$. Somando estas igualdades membro a membro, agrupando e colocando n em evidência, ficamos com $a + c - (b + d) = (k1 + k2)n$, ou seja, $a + c \equiv b + d\ (mod.n)$.

(II) como $a \equiv b\ (mod.n)\ e\ c \equiv d\ (mod.n)$, ou melhor, $n \mid (a - b)\ e\ n \mid (c - d)$, temos que $n \mid (ac - bc)\ e\ n \mid (bc - bd)$, donde resulta que $n \mid [(ac - bc) + (bc - bd)]$, isto é, implica ainda que $n \mid (ac - bd)$, o que equivale a $ac \equiv bc\ (mod.n)$.

Definição 5.9.3 Um número natural a é um resíduo quadrático módulo P (primo) quando a equação $x^2 \equiv \boldsymbol{a}\ (\boldsymbol{ModP})$ tem solução em $\{\mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots, \boldsymbol{P} - \mathbf{1}\}$.

Decorre imediatamente da definição acima que se a é um Resíduo Quadrático Módulo P, então a e x são primos entre si ou relativamente primos. Noutras palavras, o Máximo Divisor Comum deles corresponde sempre à unidade.

De fato, caso os números admitissem algum divisor comum diferente da unidade, teríamos como implicação, segundo a equação $\boldsymbol{x^2 \equiv a\ (ModP)}$ que P seria divisor de X, já que por hipótese, esse primo divide a diferença e um dos termos da Diferença. Entretanto, isso é impossível, pois X integra: $\{\mathbf{1, 2, 3}, \ldots, \boldsymbol{P - 1}\}$**.** De acordo com a hipótese da definição. Logo, X não pode dividir P.

Vale ressaltar que esse é um dos conceitos mais importantes dentre os que efetivamente permitem avançar no estudo da Teoria Elementar dos Números, mais precisamente das Equações Modulares quadráticas que já foram abordadas de forma superficial, dada as enormes dificuldades de cunho algébrico, associadas ao tema e que somente agora achamos conveniente abordar com mais profundidade.

Serão considerados vários exemplos como estratégia que visa facilitar o entendimento por parte do leitor, destacadamente aos que porventura não tenham uma base matemática mais sólida. Para isso, recomenda-se a fixação de um primo escolhido arbitrariamente, desde que o seu módulo permita a realização das operações com destaque para as substituições inevitáveis nesse contexto particular.

Assim, tomando P = 7, podem-se tirar algumas conclusões interessantes de fácil verificação. A primeira delas consiste numa proposição afirmativa: "O número dois é um resíduo quadrático módulo sete".

De fato, para a devida comprovação, basta encontrar um elemento do conjunto $\{\mathbf{1, 2, 3, 4, 5, 6}\}$ capaz de verificar $x^2 \equiv \mathbf{2}\ \boldsymbol{Mod}\ \mathbf{7}$. Fazendo isso, constata-se facilmente que apenas o três figura como uma raiz da equação mencionada. Faremos todas as substituições, já que o conjunto em questão tem um efetivo pequeno, permitindo-nos uma excelente experiência Didática. Procedendo dessa forma, chega-se às seguintes conclusões:

$$\mathbf{12} \equiv \mathbf{2}\ (\boldsymbol{Mod.}\mathbf{7}), \mathbf{22} \equiv \mathbf{2}\ (\boldsymbol{Mod.}\mathbf{7}), \mathbf{32} \equiv \mathbf{2}\ (\boldsymbol{Mod.}\mathbf{7}), \mathbf{42} \equiv \mathbf{2}\ (\boldsymbol{Mod.}\mathbf{7}), \mathbf{52} \equiv \mathbf{2}\ (\boldsymbol{Mod.}\mathbf{7}) \boldsymbol{e}\ \mathbf{62} \equiv \mathbf{2}\ (\boldsymbol{Mod.}\mathbf{7}).$$

Agora, há um ponto que precisa ser esclarecido com relação ao conceito de resíduo quadrático: a exigência de que um inteiro positivo seja primo com P deve ser entendida precisamente como uma Condição necessária, mas não suficiente.

Não precisa ser gênio para perceber que o problema associado à verificação quanto ao número ser ou não ser um resíduo quadrático módulo um primo, figura como um daqueles verdadeiramente complicados para os primos grandes. Tudo isso, devido à necessidade de pelo menos no primeiro momento, fazer a verificação de todos os elementos presentes no conjunto dos inteiros positivos começando pela unidade e terminando com o antecessor do primo em questão. Assim, para decidir se o número 19 é um Resíduo Quadrático Módulo 57, teríamos muito trabalho certamente devido às várias substituições necessárias em linhas gerais para essa Tomada de Decisão.

Imagine todas as dificuldades numéricas correspondentes aos primos maiores digamos com algumas dezenas de dígitos, cuja presença é certa nos mais variados problemas computacionais com destaque para a Criptografia RSA. Logo, os Matemáticos resolveram buscar critérios mais eficientes, mediante os quais seja possível tomar a decisão de forma a realizar o menor número possível de operações. Noutras palavras, com o mínimo de substituições e máximo de eficiência. O primeiro a encontrar um critério capaz de verificar essas condições foi o notável matemático suíço Euler. O teste de Euler definido a seguir, apresenta uma condição necessária e suficiente para que um inteiro positivo seja um resíduo quadrático.

5.9.4 Teste de Euler

Seja P um primo ímpar e a um inteiro positivo não divisível por P. Então a será um resíduo quadrático módulo P se, e somente se, tivermos $\mathbf{a^{(p-1)/2} \equiv 1\ Mod\ p}$.

Infelizmente pode-se verificar facilmente que este não é o que podemos chamar de critério eficiente sob o ponto de vista computacional. De fato, para decidir se 17 é um resíduo quadrático módulo 1.987, implica verificar se $13^{998} \equiv 1\ Mod 1987$. O leitor há de concordar que essa é uma tarefa delicada, onde a mesma justifica a falta de razoabilidade do Critério de Euler**,** principalmente para os primos “muito grandes”.

Isso porque são exatamente esses os que definitivamente exigem a criação de critérios mais eficientes para essa Tomada de Decisão. Agora, não podemos negar que historicamente representou um grande avanço rumo à demonstração do Conjunto das Leis de Reciprocidade Quadrática de Gauss que aparece como um dos resultados mais fortes na Moderna Teoria dos Números, chamando nossa atenção inclusive pela grande quantidade de demonstrações.

Para encerramos essas discussões sobre Aritmética Modular, apresentaremos um resultado particular sobre as equações de congruências quadráticas que permitirá uma continuidade no estudo das mesmas, caso haja interesse por parte do leitor.

Na verdade, houve um esforço contínuo no sentido de tornar o texto cada vez mais enxuto para evitar que o mesmo se torne cansativo. Para isso, gostaríamos de apresentar um lema fundamental também para um aprofundamento sobre o **Teorema de Wilson**, sendo o principal resultado no tratamento de equações de congruência envolvendo o conceito de fatorial.

5.9.5 Lema: Se P é um primo ímpar, então o inteiro positivo a coincide com o seu inverso módulo P, se, e somente se $\boldsymbol{a \equiv 1\ (mod P)\ ou\ a \equiv -1 (mod P)}$.

Demonstração. Se a coincide com o seu inverso, então $a^2 \equiv 1$ (mod. P) que por sua vez, implica $\boldsymbol{p \mid (a^2 - 1)}$. Mas, sendo isto verdade, então há somente duas possibilidades a se considerar, devido à fatoração da expressão do lado direito: $\boldsymbol{P \mid (a - 1)\ ou\ P \mid (a + 1)}$, donde concluirmos que $\boldsymbol{a \equiv 1 ou\ a \equiv -1 (mod\ P)}$.

Por último, gostaríamos de esclarecer que não está entre os nossos objetivos abordar de forma pormenorizada as propriedades mais fortes da Relação de Congruência. Assim, para que o leitor tenha um entendimento por completo das principais discussões colocadas neste projeto, se faz necessário que ele possua uma base a mais sólida possível com relação ao assunto em questão.

Agora, isso não quer dizer que o mesmo precisa ser um especialista no assunto. De forma alguma, até por que mesmo nos casos em que as discussões parecem exigir a utilização de resultados mais profundos dessa parte da teoria dos números, ficará claro que felizmente, isso não é necessário.

Veja o caso das equações de congruências quadráticas cuja abordagem pode ser considerada delicada pelo fato de a mesma ter sido resolvida há pouco mais de dois séculos, mediante a obra do alemão Gauss (Teorema da Reciprocidade Quadrática). Elas são complicadas, mas para sorte nossa não deve haver preocupação nesse sentido, dado todo o cuidado com esses aspectos na hora de criarmos o MTC, através do qual é possível identificar números quadrados e calcular as suas raízes.

Além do mais, apelar para sua fatoração primária, conhecida também forma padrão ou canônica. Em momento algum, o leitor precisará resolver equações desse tipo, assim também ocorre com as Equações Diofantinas Lineares**,** às quais já fizemos os devidos comentários e através deles o leitor certamente deve ter compreendido que não precisará resolver tais equações, se bem que elas não oferecem maiores dificuldades, haja vista exigirem a utilização de apenas dois Teoremas.

Na verdade, garantimos que no máximo, como uma espécie de rotina associada ao MTC de números quadrados, deverá verificar se um determinado par de inteiros positivos satisfaz uma Equação Diofantina Linear em particular, obtida mediante consulta à Tabela 3 das Classes de Equivalência (TCE) na qual estão reunidas as principais conclusões oriundas desse trabalho. Dentre elas, a fórmula através da qual calculamos a raiz quadrada de qualquer um dos membros das Classes de Equivalências. Vale lembrar ainda que o método em questão é o único que coloca à nossa disposição uma fórmula binomial simples para o cálculo da raiz quadrada.

Capítulo VI

O Método das Terminações Características

Neste capítulo, iniciaremos o estudo de uma fascinante busca por um novo método, a partir da estrutura posicional dos números, para identificar um padrão dos números inteiros que são quadrados perfeitos com base nos dois últimos dígitos da representação destes na base dez. Pela importância que desempenham nessa pesquisa, passaremos a chamá-los de Terminações Características que naturalmente podem ser pares (TCP) ou ímpares (TCI).

Em outras palavras, se um inteiro X é representado por $X_nX_{n-1}\dots X_2X_1$ na base 10, ou seja, X_1 é o algarismo das unidades, X_2 o algarismo das dezenas e assim por diante, então, o número X_2X_1 receberá o nome de terminação característica, podendo ser par ou ímpar, conforme a paridade de X_1. A seguir, mostraremos que um estudo destas terminações fornece uma condição necessária, mas não suficiente para garantir que um dado inteiro positivo seja de fato um número quadrado perfeito.

6.1 Definição. A terminação característica de um número inteiro representado na base 10 por $X_nX_{n-1}\dots X_2X_1$, é dada pelo resto da sua divisão por 100, diremos que esse número tem terminação característica par (respectivamente ímpar), se X_1 é um número par (respectivamente ímpar) e a indicaremos por TC(X).

Em particular, a terminação característica de um número quadrado perfeito indica o resto da sua divisão por 100. Assim, temos que TC (x^2) = x^2 Mod.100. Exemplo 1. TC (43^2) = 43^2 Mod.100 = 1.849 Mod.100 = 49.

Neste trabalho, estamos considerando sempre a utilização exclusiva do Sistema de Representação Decimal, assim como 100 é múltiplo de 10, conclui-se que cada uma das terminações característica (que também são números) fica determinada pela “exclusão” dos seus primeiros n – 2 dígitos.

Será demonstrado através da Relação de Congruência Mod.100 que o Conjunto desses arranjos fica completamente determinado pelos seus 25 primeiros termos, donde resultarão 22 Classes de equivalência que serão devidamente caracterizadas.

6.2 Teorema. O conjunto de todas as terminações características que pode assumir um número inteiro positivo quadrado perfeito fica completamente determinado pelos 25 primeiros números quadrados: $X^2 \equiv (50 - X)^2 Mod\ 100$.

Hipótese: $X \equiv YModM \Leftrightarrow \exists M > 0 / M \mid (X - Y)$.
Tese: $X^2 \equiv (50 - X)^2 Mod 100, \forall\ X\ inteiro$.

De fato, $X^2 \equiv X^2\ Mod\ 100 \Longrightarrow X^2 \equiv (X^2 - 100X + 2.500) = (50 - X)^2$. ■

6.3 Etapa I. A Determinação do Conjunto das Terminações Características.

De acordo com o teorema que acabamos de demonstrar, fazemos $x^2\ Mod 100$. Assim, qualquer que seja $x^2\ Mod 100 \in A$, onde o conjunto:

$$A = \{01, 04, 09, 16, 25, 36, 49, 64, 81, 00, 21, 44, 69, 96, 56, 89, 24, 61, 41, 84, 29, 76\}.$$

Neste estudo, também descobrimos uma possibilidade fantástica de agruparmos essas terminações características em Classes de Equivalência**.** Este conceito é altamente significativo para a **Teoria dos Conjuntos** de modo geral e permite um estudo bem generalizado da Teoria das Relações entre Conjuntos.

A reunião dessas classes de equivalência compõe todo o conjunto, mediante partições, ou seja, essas 22 classes divide o conjunto dos quadrados perfeitos da forma mais eficiente, dado que a Congruência (mod100) é uma relação de equivalência sob os inteiros. Portanto, satisfaz as condições Reflexividade, Simetria e Transitividade**.** Isso caracteriza uma Relação de Equivalência e determina uma partição no conjunto onde a definimos, conforme o teorema da Lógica de Classes.

De acordo com o exposto, deve-se associar uma Classe de Equivalência a cada uma das terminações características que integram o referido conjunto A. Para isso, tomar-se-á o menor dos elementos em cada classe citada, visando a sua representação. Procedendo dessa forma, obtemos o seguinte conjunto de conjuntos:

$$\{\mathrm{R}(01), \mathrm{R}(04), \mathrm{R}(09), \mathrm{R}(16), \mathrm{R}(25), \mathrm{R}(36), \mathrm{R}(49), \mathrm{R}(64), \mathrm{R}(81), \mathrm{R}(00),$$
$$\mathrm{R}(121), \mathrm{R}(144), \mathrm{R}(169), \mathrm{R}(196), \mathrm{R}(256), \mathrm{R}(289), \mathrm{R}(324), \mathrm{R}(361),$$
$$\mathrm{R}(441), \mathrm{R}(484), \mathrm{R}(529), \mathrm{R}(576)\}.$$

6.3.1 Teorema Fundamental.

O Conjunto das Classes de Equivalência constitui uma Partição do conjunto em que se define uma Relação de Equivalência. (**MACIEL**, Jarbas 1.974, Pág.78)

Para justificar os principais resultados, assim como as expressões algébricas que permitirão a construção do Método das Terminações Características**,** definiremos a parcela adjacente (AD) de um quadrado perfeito como aquela imediatamente a esquerda da sua terminação característica podendo ser par (ADP) ou ímpar (ADI).

Notação. Dado um número inteiro positivo $X = X_n X_{n-1} \ldots X_2 X_1$, vamos representá-lo por AX_2X_1, sendo A = $X_n X_{n-1}$ ... X_3. Com estas notações, o número A será chamado de a parcela adjacente da terminação característica X_2X_1, como já definida anteriormente. Em outras palavras, a concatenação de A com X_2X_1 coincide exatamente com a representação de X na base dez.

6.4 Proposição. $AD\ (X^2) = (X^2 - X^2 Mod 100)/100,\ \nexists X^2$.

Demonstração. Como por hipótese $X^2 = 100A + X_2X_1$ e $X_2X_1 = X^2\ Mod 100$, então $X^2 = 100A + X^2\ Mod 100 \rightarrow A = (X^2 - X^2 Mod 100)/100$.

Exemplo. Considerando X^2 = 1.849, temos que X^2 = 18x100 + 49. Portanto, AD (X^2) = 18 e TC (X^2) = 49. Dessa forma, a concatenação $AD(X^2)TC(X^2)$ coincide com a representação em sistema decimal de X^2, conforme já constatado.

6.5 Etapa II. A Paridade das Parcelas Adjacentes (PPA).

De acordo com o Teorema 1 e levando-se em conta a posição de cada uma das terminações características de quadrados na exata ordem em que aparecem, somos capazes de descobrir os próximos termos de cada classe. Fica evidente que reaparecerão sempre que aumentarmos a sua raiz de 50. Tomando como base o fato de que $7^2 \equiv 43^2 \equiv 49$, concluímos naturalmente que os seus próximos dois termos são $(7 + 50)^2$ e $(43 + 50)^2$, ou seja, $(57)^2$ e $(93)^2$.

Observação: Perceba que na classe R(49) quando denotado cada elemento como a concatenação da parcela adjacente com a terminação característica, $AD(x)TC(x)$, então a parcela adjacente é sempre par, ou seja, $AD(x) = 2m$, enquanto que na classe R(324), não se verifica mais a ocorrência de tal fato, conforme ficará claro, mediante a observação dos quatro primeiros termos.

Veremos através de exemplos que todas as classes constituídas por quadrado ímpares admitem parcelas adjacentes com uma paridade fixa, enquanto todas as demais classes apresentam parcelas adjacentes com uma paridade variável. De fato, tomando os quatro primeiros termos da Classe R(49), temos:

$\{(7)^2, (43)^2, (57)^2, (93)^2\} = \{\mathbf{0}49, \mathbf{18}49, \mathbf{32}49 \; e \; \mathbf{86}49\}$. (57 – 7 = 93 – 43 = 50)

Não podemos simplesmente estender essa conclusão para os demais termos, mas demonstraremos que se trata sim de um resultado geral para essa Classe.

Procedendo de modo semelhante com a classe R(324), fica até mais evidente tudo o que se acabou de afirmar acima, exigindo a adoção de uma nova estratégia.

$\{(18)^2, (32)^2, (68)^2, (82)^2\} = \{\mathbf{3}24, \mathbf{10}24, \mathbf{46}24 \; e \; \mathbf{67}24\}$: 68 – 18 = 82 – 32 = 50

Agora vemos que os números adjacentes de cada um dos quadrados acima têm de fato paridade variável. O método que buscamos desenvolver não pode ficar indiferente a essa questão. Assim, para que haja um mínimo de simetria no algoritmo, buscaremos uma propriedade, mesmo de natureza acessória, associada apenas aos quadrados pares e que contribua com sua identificação.

6.6 Etapa III. A terminação da quarta parte dos quadrados pares (TQP).

Para compensar esse fato relativo aos quadrados pares, onde verificamos que as parcelas adjacentes não têm paridade fixa, a exemplo do que acontece com os quadrados ímpares, mudaremos o foco da análise em questão para a quarta parte do número, tomando como referência metodológica a seguinte afirmação:

6.6.1 Proposição: Um número inteiro positivo múltiplo de quatro será quadrado perfeito se, e somente se, o mesmo for verdadeiro para a sua quarta parte.

Demonstração. Como um número quadrado e sua raiz têm a mesma paridade:

A condição é necessária: $X = (2m)^2 = 4m^2 \implies X/4 = m^2$

A condição é suficiente: $X/4 = m^2 \implies X = 4m^2 = (2m)^2$

Exigiremos apenas que a mesma admita uma das Terminações Características já determinadas para evitarmos qualquer traço de Circularidade na execução do método em questão que está prestes a se tornar uma realidade, mais do que isso, uma nova e eficiente ferramenta algébrica para identificação de números quadrados, sem apelo a sua fatoração primária. Esta representa mais uma **Condição Necessária**, porém **não Suficiente** para que um inteiro positivo e múltiplo de quatro seja quadrado. A importância dessa etapa fica bem evidente na manipulação de números com representação decimal mais extensa.

Quer dizer, trata-se um cuidado que visa à não realização de cálculos desnecessários durante a aplicação do método das terminações características. Estamos nos referindo principalmente à quinta etapa que representa a mais exigente de todas. Assim, atentar para a quarta parte do número, antes da aplicação das etapas posteriores permitirá obter indícios capazes de justificar a continuidade do algoritmo, tornando-o mais eficiente.

Existe uma regra geral no Domínio dos Quadrados Perfeitos que permite associarmos uma única Terminação Característica a cada parcela adjacente, desde que verificada a condição AD (X^2) > 16. Noutras palavras, o simples conhecimento da parcela adjacente determina a sua terminação característica.

6.7 Proposição. Se a parcela adjacente de um número quadrado é maior do que 16, então a sua terminação característica fica completamente determinada:

$$Se\ X^2 = AD(X^2)TC(X^2)\ e\ Y^2 = AD(X^2)TC(Y^2), então\ TC(X^2) = TC(Y^2).$$

Demonstração. Vamos verificar a validade da proposição para os seguintes números quadrados consecutivos: (Veja que as suas raízes são consecutivas).

42^2 = 1.764, 43^2 = 1.849, 44^2 = 1.936, 45^2 = 2.025, 46^2 = 2.116, 47^2 = 2.209, 48^2 = 2.304, 49^2 = 2.401, 50^2 = 2.500

De fato, as parcelas adjacentes dos elementos que compõe o conjunto acima são distintas. Para demonstrar a manutenção do padrão, basta provar que a partir desse ponto $(n > 50)$, a diferença entre quadrados consecutivos será maior do que 100.

Assim, a parcela adjacente será necessariamente modificada, já que todas as terminações características têm apenas dois dígitos. Para isso, vale lembrar que $(n+1)^2 - (n)^2 = 2n + 1$. Como $n > 50$, resulta então $2\,n + 1 > 100$.

Explorando a Relação de Congruência Módulo 9

6.8: Etapa IV. Formas algébricas compatíveis com números quadrados (FAC).

Aprendemos a fazer uma exploração da congruência módulo 9 no estudo dos quadrados perfeitos. Segundo a aritmética, sabe-se que pelo Algoritmo da Divisão Euclidiana, qualquer número quadrado perfeito, quando dividido por nove, deixa restos 0, 1, 4 e 7. Dessa forma, o estudo de apenas quatro categorias é suficiente para a descrição dos quadrados perfeitos, usando a relação $Mod(9)$. Para comprovar tal resultado, basta calcular os resíduos dos quatro primeiros quadrados.

$$x^2 \equiv (m-x)^2\ Modm, já\ que\ (m-x^{\,2}) - x^2 = m(a-2m).$$

$$1^2 \equiv 1\ \mathrm{Mod}9, \qquad 2^2 \equiv 4\ \mathrm{Mod}9, \qquad 3^2 \equiv 0\ \mathrm{Mod}9 \text{ e } 4^2 \equiv 7\ \mathrm{Mod}9.$$

Dessa forma, conclui-se que nesse contexto, as únicas Formas Algébricas Compatíveis com os números quadrados, associadas à divisão por nove são:

$$\mathrm{FAC}: \{9m, 9m+1, 9m+4, 9m+7\}.$$

São Formas Algébricas Incompatíveis com os números quadrados perfeitos:

$$\mathrm{FAI}: \{9m+2, 9m+3, 9m+5, 9m+6, 9m+8\}.$$

Essa informação pode ser utilizada como uma espécie de filtro ou critério de eliminação, caracterizando mais uma condição necessária**,** porém não suficiente para decidirmos se o número fornecido é um quadrado. A escolha dessas formas está relacionada à simplicidade da verificação que pode ser feita pela soma dos valores absolutos dos algarismos que formam o número dado. Isso nos remete aos Critérios de Divisibilidade que são abordados em todos os níveis de ensino, porém com muito mais ênfase na educação superior. A adoção dessas formas também determina uma partição nos quadrados perfeitos, já que implica na utilização de uma congruência nodular, indicando sempre uma genuína relação de equivalência.

6.9: Etapa V. Equações Diofantinas Fundamentais das parcelas adjacentes.

O procedimento fundamental consiste em reescrevermos a parcela adjacente em função do quadrado mais próximo, utilizando somente as operações de adição e subtração, conforme a relação de ordem presente. Geramos assim, um par de números inteiros que passaremos a chamar respectivamente de Base(B) e Resto(R).

Obtém-se também um sinal que deve ser preservado e mostrará sua utilidade durante consulta que faremos rotineiramente à Tabela das Classes de Equivalência (TCE) que representa uma espécie de síntese dos principais resultados obtidos com esse projeto como, por exemplo, os pares de Equações Diofantinas Fundamentais (EDF) associadas a cada uma das classes em questão. Os números 2,6 e 12 são as únicas exceções a essa etapa. Portanto, devem ser escritos em função dos seus quadrados perfeitos imediatamente superiores: $2 = 2^2 - 2, 6 = 3^2 - 3, 12 = 4^2 - 4$.

6.9.1 Principais Resultados

Continuaremos tomando a classe R(49) como principal referência, sendo seu termo geral dado conforme abaixo, segundo a tabela 2 constante no apêndice.

$$\boldsymbol{a_m = \begin{cases} (25m - 18)^2 & , \ se \ m = 2t - 1. \\ (25m - 7)^2 & , \ se \ m = 2t. \end{cases}}$$

Depois escolhemos dois termos consecutivos na mesma, visando facilitar a obtenção dos principais resultados que culminarão com um teorema fundamental desta classe para então seguirmos as recomendações mencionadas: destacar a paridade da parcela adjacente e escrever a mesma em função do quadrado mais próximo, mediante uma adição ou subtração. Já que consideradas em conjunto, elas mostram a existência de padrões algébricos fundamentais para os nossos objetivos.

Naturalmente, procuramos relações algébricas simples, envolvendo as operações mais elementares possíveis que possam contribuir com o desenvolvimento do MTC. Três expressões algébricas mostraram uma forte conexão com a classe acima citada: **3B**, **5R** e **10B**, onde esta representa a aproximação mais grosseira para a raiz quadrada do inteiro em questão. Os termos gerais das demais classes foram omitidos temporariamente, mas serão apresentadas na parte destinada aos anexos.

De acordo com a fórmula do termo geral, temos que o segundo e o terceiro membros da classe R(49) são obtidos fazendo m = 2 e m = 3, donde resultam:

$$\boldsymbol{a_2 = 43^2 = 1.849}$$

Veja que a sua parcela adjacente corresponde a 18. Assim, escrevendo esta parcela em função do seu quadrado mais próximo, conforme procedimento fundamental desta etapa: $18 = 16 + 2\, ou\, 42 + 2 \rightarrow B = 4\, e\, R = 2$.

Assim, tomando como referência os resultados de experiências semelhantes realizadas com diversos outros termos desta mesma classe, concluímos que vale destacar as seguintes: $3B = 12, 5R = 20\, e\, 10B = 60$. Logo, as relações algébricas mais elementares entre estas são: $3B = 5R + 2\, e\, 10B + 3 = 43$.

$$\boldsymbol{a_3 = 57^2 = 3.249}$$

Veja que a sua parcela adjacente corresponde a 32. Assim, escrevendo esta parcela em função do seu quadrado mais próximo, conforme o procedimento fundamental:

$$32 = 36 - 4\, ou\, 62 - 4 \rightarrow B = 6\, e\, R = 5.$$

Assim, tomando como referência os resultados de experiências semelhantes realizadas com diversos outros termos desta classe, conclui-se que vale destacar as seguintes relações: $3B = 18, 5R = 20\, e\, 10B = 60$. Logo, as relações algébricas mais elementares entre estas são respectivamente: $3B = 5R - 2\, e\, 10B - 3 = 57$.

Os últimos resultados em cada um dos exemplos são suficientes para justificar a validade geral de ambos. Nesse sentido, não há necessidade de continuar operando semelhantemente com outros termos da classe R(49). A justificativa está relacionada ao fato de que com esse procedimento, haveria excesso de informações que poderiam comprometer a visão geral das relações algébricas entre os monômios.

Naturalmente, quanto mais experimentos, mais fortes ficam os indícios algébricos. Acrescente-se ainda que se esse procedimento foi repetido exaustivamente, fato que deixou cada vez mais evidente um padrão relativamente simples do qual resultou o teorema abaixo, cujo papel é fundamental na compreensão do método.

6.9.2 Teorema Fundamental

Uma condição necessária e suficiente para que o inteiro $X \equiv 49\, Mod 100$ seja número quadrado perfeito é apresentar uma parcela adjacente que escrita em função do quadrado mais próximo, satisfaça uma das equações $3B = 5R \pm 2$.

A condição é necessária:

Se $X^2 \equiv 49 Mod\ 100$, então $X = 50m \pm 7$ e $AD(X^2) = (X^2 - 49)\ /100$.

Se $X = 50m \pm 7$, então $X^2 = 2.500m^2 \pm 700m + 49$ e $AD(X)^2$ = 25m^2 ± 7m = $(5m)^2 \pm 7m$. Assim, facilitamos a identificação dos quadrados mais próximos das parcelas adjacentes de X^2 que valem respectivamente ·.

Escrevendo A em Função destes: $A_1 = 25m^2 + 7 = (5m + 1)^2 - (3m + 1)$. $se\ B_1 = 5m + 1\ e\ R_1 = 3m + 1\ então\ 3B_1 = 5R_1 - 2\ e\ 50m + 7 = 10B_1 - 3$.

Além disso, temos também que $A_2 = 25m^2 - 7 = (5m - 1)^2 + (3m - 1)$.
Se $B_2 = 5m - 1\ e\ R_2 = 3m - 1, então\ 3B_2 = 5R_2 + 2\ e\ 50m - 7 = 10B_2 + 3$.

A condição é suficiente:

Se $3B = 5R \pm 2 \rightarrow (3B)^2 = (5R \pm 2)^2 \rightarrow 9B^2 = 25R^2 \pm 20R + 4$.

Se $9B^2 = 25R^2 \pm 20R + 4 \rightarrow 900B^2 = 2.500R^2 \pm 2.000R + 400$.

$Se\ A = B^2 \pm R \rightarrow 900A = 900B^2 \pm 900R \rightarrow 900A = 2500R^2 \pm 2900R + 400$.

$Se\ X = 100A + 49 \rightarrow 9X = 900A + 441 \rightarrow 9X = 2500R^2 \pm 2900R + 841$.

$Se\ 2500R^2 \pm 2900R + 841 = (50R \pm 29)^2, então\ 9x = (50R \pm 29)^2$

Por hipótese, $Se\ 5R \pm 2 = 3B \rightarrow 50R \pm 20 = 30B \rightarrow 50R \pm 29 = 30B \pm 9$.

Logo, $Se\ 9X = (30B \pm 9)^2 \rightarrow 9X = 9(10B \pm 3)^2 \rightarrow X = (10B \pm 3)^2$ ■

6.9.3 Corolário

Todos os membros da Classe R(49) apresentam uma parcela adjacente par.

De fato, segundo o Teorema I, todas as parcelas adjacentes dos membros de R(49) verificam uma das equações $3B = 5R \pm 2$. Em qualquer dos casos, temos que $3B - 5R = 2\ ou\ 5R - 3B = 2$, implicando $par(3B) = par(5R)$. Além disso, como todos os coeficientes desta são ímpares: $Par(B) = Par(R)$. Assim, sendo $A = B^2 \pm R$, temos que A é par, pois Par(B^2) = par(B) = par(R).

(*) Quando se multiplica um número inteiro por outro ímpar, não alteramos a sua **Paridade**. Utilizamos a notação Par (X) como indicação da paridade do inteiro X. Procedendo analogamente com as demais classes, são obtidos resultados semelhantes que evidenciam a existência de uma incrível simetria algébrica com destaque especial para o monômio (5R), associado a todas as Classes que mostrará uma importância fundamental na determinação das etapas do Método em questão.

6.10: Etapa VI A Determinação da Raiz Quadrada (DRQ)

Chegamos ao ápice do método das terminações características. A essa altura, o inteiro positivo com o qual estamos operando, passou por todas as cinco etapas determinadas anteriormente, não havendo dúvidas que se trata realmente de um quadrado perfeito. Conforme dito no início da apresentação, o método em questão dever responder a duas perguntas fundamentais: (1) Se o número X é um quadrado perfeito e (2) Quanto vale a raiz quadrada de X na hipótese de resposta positiva.

Assim, o foco agora consiste na determinação da raiz quadrada para a qual não há maiores dificuldades, de acordo com o teorema 1, levando-se em conta os diversos traços de simetria presentes no texto como um todo, justificada principalmente pela relação de congruência modular, simétrica por natureza em consequência da sua definição. Observe que a demonstração do teorema em questão acaba fornecendo a raiz quadrada de todos os membros da referida classe, fato que se mantém presente quando consideramos os teoremas análogos para as demais classes de quadrados.

Tabela 3: Classes de quadrados e suas equações Diofantinas

Múltiplo Base	5R	5R±1	5R±2	5R±3	5R±4	Raiz Quadrada
0	R(100)					10B
1B	R(01)	R(121)	R(441)	R(961)	R(81)	10B±1
2B	R(04)	R(324)	R(144)	R(64)	R(484)	10B±2
3B	R(09)	R(529)	R(49)	R(169)	R(289)	10B±3
4B	R(16)	R(36)	R(256)	R(576)	R(196)	10B±4
5B	R(25)					10B±5

6.10.1 Orientações gerais para consulta à tabela das equações Diofantinas.

Sabemos que há sempre um par de equações Diofantinas lineares associadas a cada uma das classes de equivalência de números quadrados com exceção de R(100), visto que nesse caso, devemos voltar nossa atenção para a parcela adjacente do número em questão, levando-nos sempre para outra classe. Aliás, segundo essa informação, não haveria prejuízo significativo caso optássemos pela exclusão da referida classe na confecção dessa tabela.

O fato é que aquele par de equações fica determinado pela interseção da classe fornecida com a primeira linha e a primeira coluna da tabela em questão. Assim, tomando a classe R(324) como referência e seguindo a orientação concluímos que suas interseções fornecem o seguinte par $\boldsymbol{2B = 5R \pm 1}$. Quanto à localização da tabela, ela pode ser encontrada no apêndice.

Quanto ao binômio que permite calcular a raiz quadrada, ele fica determinado pela interseção da classe supostamente conhecida com a última coluna da tabela em questão. Logo, ainda com relação à R(324), temos que as raízes quadradas de qualquer um de seus membros devem ser calculadas pelos binômios $\boldsymbol{10B \pm 2}$. Vale ressaltar que apesar de haver dois binômios, somente um será efetivamente utilizado em cada problema sobre números quadrados.

Tomando mais um exemplo, vejamos o caso da classe R(289) para a qual encontramos as seguintes equações Diofantinas $3B = 5R \pm 4$ sendo que somente uma deve ser satisfeita pela parcela adjacente quando escrita em função do seu quadrado mais próximo e o par de binômios $10B \pm 3$ para o cálculo da respectiva raiz quadrada. Assim como em diversos outros contextos, acreditamos que tais consultas serão feitas de forma cada vez mais rápida quando adquirirmos alguma prática, de modo a ficar praticamente instantânea.

6.11 Aplicações do Método das Terminações Características

(1) Modelo de Aplicação Elementar.

Verifique se o número 3.136 é quadrado perfeito e calcule sua raiz quadrada.

Sol. Destacamos a presença de uma TCP (36) e um ADI (31), cuja soma dos dígitos exibe uma FAC $(9M + 4)$ com os números quadrados. Escrevendo a parcela adjacente em função do seu quadrado mais próximo, temos 31= 36 - 5 ou 6^2 - 5 → B = 6 e R = 5. Uma simples consulta à Tabela das Classes de Equivalência (TCE) resulta $4B = 5R - 1(24)$. Assim, temos um número quadrado, pois os valores numéricos destes monômios são iguais, além disso, sua raiz quadrada vale $10B - 4$ = 56. Outra forma seria admitir como hipótese que 3.156 é quadrado, então a sua raiz será $10B - 4 = 56$. De fato, 56^2 = 3.136.

(2) Modelo de Aplicação Elementar

Calcule através do Princípio Fundamental da Contagem o total das permutações simples dos dígitos 1, 2, 3, 4, 5 e 6. A seguir, demonstre via congruências que nenhuma delas representa um número quadrado perfeito.

Sol: Pelo princípio em questão, sabemos que o total das permutações de n elementos distintos é dado $P_n = n!$ Dessa forma, temos que $P_6 = 6! = 720$. Vamos tomar uma dessas permutações, por exemplo, 432.516 e observar a soma dos seus dígitos que corresponde a $21 = 9m + 3$.

Assim, fica evidente que a permutação em questão admite uma forma algébrica incompatível com os números quadrados perfeitos. Porém, o mesmo ocorrerá com todas as outras permutações, pois, elas diferem apenas pela ordem de seus elementos.

6.11 A Evolução do Método das Terminações Características

Sem dúvidas, a essa altura da pesquisa, o método em questão está completamente determinado pelas suas seis etapas, existindo inclusive uma tabela que deve ser consultada sempre que necessário para uma efetiva tomada de decisão sobre a presença de número quadrado sem apelarmos para a busca da sua fatoração primária; sendo essa a maior vantagem computacional do Método das Terminações Características (MTC) de números quadrados. Entretanto, temos preocupação com a sua abrangência, noutras palavras, se considerarmos inteiros com até quatro dígitos, não encontraremos maiores dificuldades para sua aplicação.

Mas, uma das etapas suscita preocupação particular: Como aplicamos o método se a parcela adjacente apresentar cinco ou mais dígitos? Para que o leitor compreenda melhor essa preocupação, vale recordar que verificada a presença de uma terminação característica (condição necessária), o passo seguinte na aplicação do MTC consiste em escrevermos a parcela adjacente em função do seu quadrado mais próximo. Mas, como faremos isso, se para todos os efeitos, nosso repertório conta com apenas 10 número quadrados?

Mesmo o leitor argumentando que tal repertório pode ser ampliado de várias formas como o acréscimo de um par de zeros, não desejamos que essa seja uma constante preocupação na aplicação do método. Em outras palavras, ampliar o repertório sempre que nos depararmos com números mais extensos seria altamente comprometedor para o sucesso do método que apesar de determinado, precisa evoluir de modo a manter sua eficiência mesmo na hipótese da presença de números com representação decimal mais extensa.

Naturalmente, como em qualquer outro contexto, números mais extensos costumam exigir sempre um pouco mais de trabalho, independente da natureza da operação em questão. Aliás, basta ver uma simples multiplicação via algoritmo tradicional: O número de operações aumenta com a extensão dos fatores, essa é uma conclusão de fácil verificação, sem dúvidas.

Mas, Voltando à questão, precisamos de uma ferramenta capaz de tornar o método das terminações características um pouco mais eficiente e abrangente. Nesse sentido, deseja-se escrever a parcela adjacente em função do quadrado mais próximo sem ampliar o nosso repertório de quadrados, cuja extensão mínima deve ser mantida, aliás, essa foi uma das promessas no início dos trabalhos.

6.12: O Método de Completar Quadrados

Todo matemático que se prese, seja profissional ou amador, já recorreu ao método de completar quadrados em algum momento dos seus estudos. De modo geral, ele surge na geometria e séculos depois vem sendo utilizado tanto na álgebra quantos em vários outros campos de pesquisa da matemática. Felizmente, não há limites para sua aplicação, ou seja, sempre que nos depararmos com números quadrados, funções quadráticas, formas quadráticas, etc.

Podemos recorrer ao método citado que tem um papel fundamental na surpreendente evolução da matemática. No contexto da Teoria dos Números, temos como razoável admitir que todo inteiro positivo pode ser escrito em função do seu quadrado mais próximo, além disso, essa representação é única, já que quadrados consecutivos têm paridades distintas.

Um exemplo tornará os comentários acima mais evidentes: Suponha que desejamos escrever 245 em função do seu quadrado mais próximo, no caso, desejamos mostrar que há somente uma representação nesse caso. Para isso, precisamos descobrir os dois quadrados consecutivos mais próximos do número dado. Por enquanto, faremos isso por tentativas e erros, respeitando o nosso tímido, mas importante repertório de números quadrados.

Feito isso, concluímos que $15^2 = 225 < 245 < 256 = 16^2$. Observe os desvios em relação aos quadrados: são 20 e 11 que têm paridades distintas. Esse é um resultado geral, quer dizer, não existe a possibilidade de tais desvios resultarem iguais. Assim, haverá sempre um menor, donde concluímos que existe, de fato, um quadrado o mais próximo possível do número fornecido.

Por tudo isso, escrevemos: 245 = 16^2 – 11 que fornecem a base e o resto necessários ao MTC. Não havendo dúvidas sobre a unicidade dessa representação, passaremos a detalhar como devemos proceder para a sua respectiva obtenção.

Como a nossa preocupação diz respeito aos números com pelo menos cinco dígitos, quer dizer, quando tais números assumem o papel de adjacente em relação a uma determinada terminação característica, tomemos um modelo de problema nas proximidades desse contexto.

Escreva o número 7.536 como uma função do seu quadrado mais próximo.

Para isso, divide-se o número em pares de dígitos a começar pela sua direita. Feito isso, resolvemos o problema para o primeiro $\mathbf{75 = 81 - 6 \rightarrow 75 = 92 - 6}$ **(I).** Veja que fizemos isso através de uma consulta ao nosso repertório de número quadrados que continua intacto, principalmente na sua extensão onde está a nossa verdadeira preocupação.

Agora, devemos avançar para a próxima Ordem de Grandeza, ou seja, 10^4. Depois de refletir um pouco sobre a questão, é fácil concluir que basta multiplicar ambos os membros de (I) por 10^2, resultando uma nova, mas não definitiva representação: 7.500 = 90^2 – 600.

Tomando por base a identidade $\boldsymbol{(a+b)^2 = a^2 + 2ab + b^2}$, amplamente conhecida do público em geral, concentramos nossa atenção no termo misto (2ab). Quer dizer, dobramos a base $(2\,x\,90 = 180)$ e buscamos o seu múltiplo mais próximo de 600 que vale $540 = 180\,x\,3$.

Assim, obtém-se $7.500 = 90^2 - 540 - 60 \Longrightarrow 7.536 = 90^2 - 540 - 24 \Longrightarrow 7.536 = 90^2 - 540 + 9 - 33 = 90^2 - 2\,x\,90\,x\,3 + 3^2 - 33 = (90-3)^2 - 33 = 87^2 - 33.$
De onde se conclui que o quadrado mais próximo de 7.536 é $87^2 = 7.569$

Figura 3: O Método de Completar Quadrados.

https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSj8i90J-msvv2X3Pq3fcwiyQbd6uJYcrWJQ-uHn5KmfSuFt9gpyQ

Naturalmente, por se tratar da primeira vez em que expomos o problema aqui, ele pode passar a impressão de ser extenso, mas um paralelo como outros algoritmos mais simples permite afirmar que basta um pouco de prática para que o mesmo se torne automático como ocorre, por exemplo, quando realizamos uma simples multiplicação de inteiros. Vale ressaltar ainda que não houve qualquer necessidade de ampliação do repertório fundamental de números quadrados que representa aqui a maior das nossas preocupações.

Dada a importância Histórica do método de completar quadrados, achamos por bem acrescentar algumas observações a respeito da sua aplicabilidade, caso o leitor fique com a impressão de que tal método pode, em alguma medida, resolver o problema central desse projeto de pesquisa: Identificar números quadrados perfeitos sem apelarmos para a sua decomposição nos primos também conhecida como forma padrão, sem dúvidas, a mais eficiente de todas as representações multiplicação, também a mais difícil de ser obtida, por isso, a decisão de contorna-la, até porque já mostramos toda a sua complexidade.

Nesse sentido, o método de completar quadrados, pelo menos teoricamente pode ser utilizado na identificação de números quadrados, sem dúvidas. A resposta será positiva se, e somente se, tivermos resíduo nulo após sua aplicação. Entretanto, não faz qualquer distinção a princípio entre os números naturais, quer dizer, dispensa o mesmo tratamento a todos, configurando uma verdadeira deficiência frente ao MTC.

Assim, isolados, tanto o MTC quanto o método de completar quadrados têm suas limitações, mas unidos, eles são como a régua e o compasso na Geometria Euclidiana (capazes de construções maravilhosas). Esse paralelo nos parece apropriado e mostra que a inclusão do mesmo na construção do MTC representa uma evolução computacional. Quer dizer, de um lado, a dificuldade do MTC em escrever um inteiro como função do seu quadrado mais próximo, do outro, a incapacidade do MCQ em distinguir, a priori, números quadrados de não quadrados.

Caso ainda haja dúvidas sobre essa impossibilidade, acompanhe a simulação. Decida se o número 873.459 representa um quadrado perfeito, através do método de completar quadrados. Enquanto começarmos a resolver o problema com a realização de todos aqueles cálculos inevitáveis, conforme o exemplo veja o que diz o MTC: Esse número de fato não representa um quadrado perfeito, visto não apresenta sequer uma das terminações características dos quadrados perfeitos.

(3) Modelo de aplicação elementar

Escreva o número 3.265 como uma função do seu quadrado mais próximo.

Dividindo o número em pares de dígitos a começar pela direita e escrevendo o último par em função do seu quadrado mais próximo, concluímos que $32 = 36 - 4 \rightarrow 6^2 - 4$. Multiplicando ambos os membros desta por 100, resulta: $3.200 = 60^2 - 400$ que também pode ser reescrita como $3.265 = 60^2 - 335$. Aplicando o método de completar quadrados: $3.265 = 60^2 - 360 + 25 = 60^2 - 360 + 9 + 16 = 57^2 + 16$. Logo, não estamos perante um quadrado perfeito, devido à presença de um resíduo (16).

(4) Modelo de aplicação Elementar

Calcule a raiz de 50XY, sabendo que o mesmo representa um quadrado perfeito.
Sol. Devemos escrever a parcela adjacente em função do quadrado mais próximo. Assim, temos que 50 = 49 + 1 = 7^2 + 1 (x 100) → 5.000 = 70^2 + 100. Pela técnica de completar quadrados, temos que 2 x 70 = 140.

Assim, temos 5.000 = 70^2 + 140 – 40. → 5.000 = 70^2 + 2 x 70 x 1 + 1 – 41 = 71^2 - 41. Pelo exposto, deve-se somar 41 ambos os membros. Logo, essa é a terminação característica, quer dizer, XY = 41. Vale lembrar que a terminação em questão fica sempre determinada, desde que sua parcela adjacente seja superior a 16.

(5) Modelo de aplicação Elementar

Calcule a raiz quadrada de 19 com aproximação de duas casas decimais.
Sol: Escrevendo o número dado em função do seu quadrado mais próximo, temos que $19 = 16 + 3\, ou\, 19 = 4^2 + 3$ (I). Agora, multiplicamos ambos os membros de (I) por $100 = 10^2$, resultando $1.900 = 40^2 + 300\ (2\ x\ 40 = 80)$.

Pela técnica de completar quadrados, pode-se reescrever esta da seguinte forma: $1.900 = 40^2 + 320 - 20 = 40^2 + 2\ x\ 40\ x\ 4 + 16 - 36 = 44^2 - 36$, assim, ficamos com 1.900 = 44^2–36. Multiplicando novamente por 100=10^2, resulta finalmente que $190.000 = 440^2 - 3.600\ (2\ x\ 440 = 880)$. Recorrendo mais uma vez àquela técnica: $190.000 = 440^2 - 3.520 - 80$, onde esta ainda pode ser escrita como $190.000 = 440^2 - 2\ x\ 440\ x\ 4 + 16 - 96 = (440 - 4)^2 - 96 = 436^2 - 96$.

Finalmente, adotamos a seguinte aproximação: $190.000 \cong 436^2$, donde concluímos que $\sqrt{19} \cong 4{,}36$. Com a prática, somos capazes de realizar os cálculos de forma cada vez mais eficiente, assim como acontece com as operações básicas, a exemplo das multiplicações e divisões. Este problema em particular mostra a força da técnica de completar quadrados quando utilizada de forma apropriada.

(6) Modelo de aplicação Elementar

Verifique se a equação $X^2 = 170.569$ admite solução nos números inteiros positivos. Sol: Isso equivale a verificar se o número em questão é um quadrado perfeito. Observe que o mesmo apresenta uma terminação característica e parcela adjacente ímpar, cuja paridade é coerente com a classe R(169). Além disso, admite forma algébrica compatível (9m + 1). Desse modo, resta-nos escrever sua parcela adjacente em função do seu quadrado mais próximo, conforme visto anteriormente.

Procedendo dessa forma: $17 = 16 + 1 \rightarrow 17 = 4^2 + 1$. (I) Multiplicando ambos os membros por $100 = 10^2$: $1.700 = 40^2 + 100 \rightarrow 1.705 = 40^2 + 105$ $(2x40 = 80)$. Reescrevendo esta $1.705 = 40^2 + 80 + 1 + 24 = 41^2 + 24$. Este procedimento gera um par de inteiros designados de Base (B) e Resto (R) que valem B = 41 e R = 24.

Consultando a tabela das classes de equivalência, deve-se verificar se o par acima satisfaz a equação Diofantina fundamental $3B = 5R + 3$. De fato, resultam dois valores iguais. Dessa forma, se pode garantir que o número dado é quadrado perfeito e sua raiz quadrada vale $10B + 3 = 413$. Vale ressaltar que detalhamos o processo por se tratar do primeiro exemplo com um número com mais de 5 dígitos.

6.10: Um Modelo de aplicação avançada

Sobre a existência de triplos pitagóricos contendo ambos os números 33 e 56.

Os triplos pitagóricos são sequências de três números inteiros positivos (a, b, c) que verificam o Teorema de Pitágoras $a^2 = b^2 + c^2$. Exemplo $(3, 4, 5)$. De fato, temos que $3^2 + 4^2 = 5^2$. Uma consequência imediata da definição acima é a de que se multiplicarmos todos os termos de um triplo por um mesmo inteiro diferente de zero, obteremos outro triplo pitagórico. Nesse sentido, dizemos que um triplo é primitivo quando seus membros são primos entre si. Um primeiro detalhe que chama a atenção nesse contexto, diz respeito ao fato de que todos eles são da forma $\boldsymbol{(m^2 - n^2, 2mn, m^2 + n^2)}$ para algum par de inteiros positivos $\boldsymbol{m}$ **e** $\boldsymbol{n}$.

Uma análise elementar sobre a distribuição dos triplos no plano sugere uma forte simetria, indicando à primeira vista que todo inteiro maior do que dois parece fazer parte de algum triplo. Para reforçar essa ideia, nada mais natural do que buscar gráficos capazes de auxiliar a análise em questão que permite um maior aprofundamento no conhecimento desse fascinante objeto matemático atrelado, dentre outras à estrutura aditiva dos números quadrados. Nesse momento, achamos oportuno adotar a relação de congruência módulo quatro no sentido de obtermos uma partição entre os números primos que serão da forma $\boldsymbol{4m + 1\ ou\ 4m + 3}$.

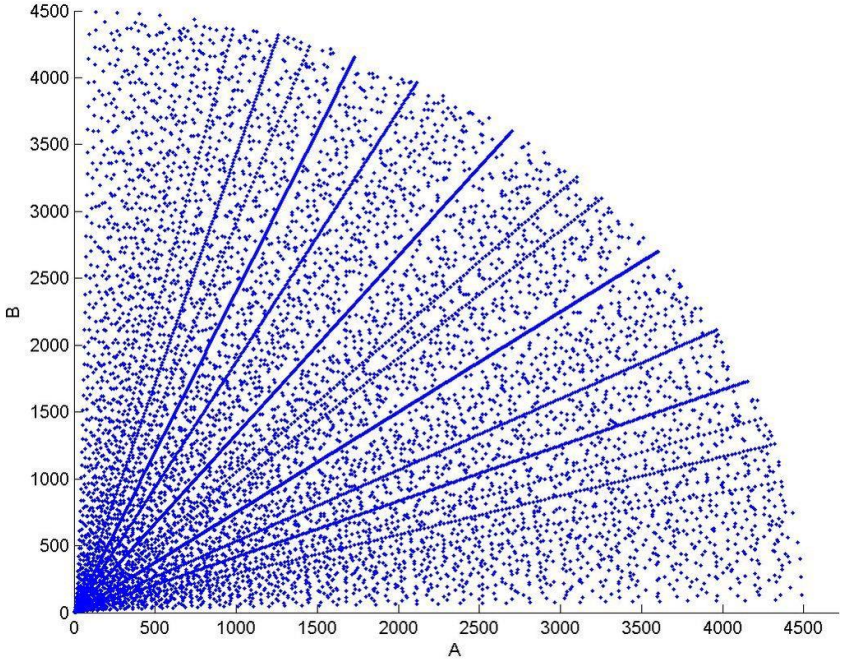
A justificativa está no fato de que todos os primos da primeira classe figuram exatamente em dois triplos. Já para os membros da última, pode-se demonstrar que todos figuram em somente um. Uma primeira justificativa pode ser dada pelo fato demonstrado, há séculos que todos os primos da primeira classe podem ser escritos de única forma como soma de dois números quadrados, possibilidade esta que pode ser estendida, mediante a **Identidade de Fibonacci** para o seu quadrado.

Diferentemente dos termos que integram a segunda classe para os quais não podemos associar uma representação desse tipo. Noutras palavras, nenhum primo da forma $\boldsymbol{4m + 3}$ pode ser escrito como uma soma de dois quadrados. De fato, sabemos que todo quadrado perfeito admite somente uma das formas algébricas $\boldsymbol{4m\ ou\ 4m + 1}$. Sendo assim, se as combinarmos duas a duas, obtemos três formas: $\boldsymbol{4m, 4m + 1\ e\ 4m + 2}$. Logo, para que um inteiro positivo seja uma soma de dois quadrados, deve apresentar pelo menos uma dessas formas algébricas.

Aliás, sabe-se que todo número ímpar pode ser escrito como uma diferença de quadrados. Assim, o mesmo vale para o quadrado desse número que ainda será ímpar. Quanto aos números pares, podemos operar uma análise semelhante e concluir que também para estes, há sempre um triplo do qual eles fazem parte.

Não temos o objetivo de aprofundar essa discussão, mas fornecer os principais conceitos e resultados que permitam o contato inicial com o tema. Adiante-se que tais objetos não devem ser subestimados em hipótese alguma, isso porque a literatura mostra uma grande variedade de problemas extremamente muito difíceis.

Refletindo sobre todas essas questões, encontramos um eficiente gráfico de dispersão que será fundamental para uma compreensão mais abrangente a respeito dos triplos, notadamente no aspecto distributivo. No eixo horizontal, marcamos o primeiro termo, no eixo vertical, o segundo. Como cada par ordenado determina um retângulo, então a sua diagonal indica o terceiro termo. Além disso, a sua leitura é simples, cada triplo será indicado por um ponto em azul. Observe que as regiões próximas da origem têm uma grande densidade de pontos, enquanto as mais distantes exibem menor densidade. Essa constatação é natural, se levarmos em conta a distribuição dos números quadrados, haja vista que a sua densidade é nula.



https://upload.wikimedia.org/wikipedia/commons/thumb/9/96/Pythagorean_triple_scatterplot.jpg/1200px-Pythagorean_triple_scatterplot.jpg

Porém, sabemos que analisar a distribuição dos triplos apoiados apenas no gráfico acima não permite demonstrar a tese mencionada, apesar da sua inegável simetria. Serão tomadas como base as duas proposições abaixo de demonstração elementar.

$$\boldsymbol{p = 2t + 1 \implies [(p^2 + 1)/2]^2 = [(p^2 - 1)/2]^2 + [p]^2}$$

$$\boldsymbol{p = 2t \implies [(p^2 + 4)/4]^2 = [(p^2 - 4)/4]^2 + [p]^2}$$

A combinação dessas duas identidades permite a obtenção de outros resultados fantásticos associados ao conceito de número quadrado. Como exemplo, ressaltamos que existem somas arbitrariamente longas de números quadrados que sempre resultam em números também quadrados.

Esse não é um resultado diretamente abordado na educação básica, devido a sua complexidade. Pode-se dizer que o teorema de Pitágoras seria a versão mais fraca dessa proposição sem esquecer a sua inegável importância histórica, notadamente na geometria para o qual existem mais de 400 demonstrações.

Voltando ao problema formulado inicialmente, veremos que há necessidade de elaborarmos uma estratégia mais específica para a superação do mesmo, visto que a definição de triplo menciona três números e não dois como é o caso desse problema.

Agora, temos uma considerável dificuldade em resolvermos o mesmo de forma que a solução não pode ser vislumbrada tão rapidamente quando atentando para a respectiva definição. Observe que a maior dificuldade é que mesmo sob a hipótese de uma resposta positiva que ainda não temos como faremos para determinar as posições ocupadas por ambos os termos? Portanto, temos três casos:

- ✓ (i) Os números fornecidos ocupam as duas primeiras posições de modo que a adição dos seus quadrados deve resultar em novo quadrado.

- ✓ (ii) Os números fornecidos ocupam as duas últimas posições de modo que a diferença entre seus quadrados deve resultar em novo quadrado.

- ✓ (iii) Os números fornecidos ocupam as posições extremas de modo que a diferença entre os seus quadrados deve resultar em novo quadrado.

Logo, o problema deve ser resolvido mediante a consideração tanto da soma quando da diferença dos quadrados dos números. Quer dizer, a resposta será positiva se pelo menos uma dessas operações resultar em número quadrado.

SOLUÇÃO. Veja que os seus quadrados valem $33^2 = 1.089\, e\, 56^2 = 3.136$. Agora, veja que a soma dos mesmos resulta em número quadrado, de fato $4.225 = 65^2$. Já para a sua diferença 2.047, vê-se que não figurando entre os quadrados, até porque não admite sequer uma terminação característica, apesar de possuir forma algébrica compatível ($\boldsymbol{9m + 4}$). Logo, o único triplo que contém ambos os números é $(33, 56, 65)$. Apesar do resultado, vale ressaltar a existência de inteiros que aparecem em dois ou mais triplos, para isso, basta observar os ímpares que podem ser escritos como diferença de quadrados de várias maneiras, dessa forma o mesmo vale para seu quadrado.

Capítulo VII

Análise de Rendimento Computacional

Há uma necessidade imediata de estabelecermos uma espécie de paralelo entre as diversas Relações de Congruência Modulares adotadas nesse projeto de pesquisa. Seria muita ingenuidade de nossa parte, colocar todas as Congruências num mesmo **patamar de eficiência**. Entretanto, para isso, deve-se adotar um critério capaz de avaliar até que ponto a relação em questão ajuda na identificação de números quadrados perfeitos. De fato, a relação será tanto mais eficiente quanto maior o número de classes residuais “eliminadas” quando a mesma deixa de operar entre os inteiros e passa a atuar entre os quadrados perfeitos. Esse é um tema da mais alta importância, haja vista a sua capacidade de justificar a adoção dessas congruências.

Talvez seja interessante construir uma tabela na qual conste a eficiência de uma relação de congruência principalmente aquelas expressas por uma potência de dez, já que as mesmas guardam uma relação direta com a base do Sistema de Numeração**.** Aliás, a classificação de um número quadrado não depende da Base em que o mesmo está representado. Assim, a escolha costuma ser feita apenas por uma questão de conveniência. A única vantagem que em linhas gerais uma **Mudança de Base** apresenta reside no fato de a mesma permitir uma diminuição na quantidade de algarismos tomando uma base maior que aquela na qual o número aparece representado inicialmente, mas isso exige uma análise muito mais apurada, pelo fato de que ainda não temos como avaliar a relação custo/benefício implícita**.**

Temos ainda condições de determinar com muita precisão a quantidade de quadrados perfeitos consecutivos necessários para determinarmos o conjunto dos n últimos dígitos como já fizemos para n = 2. Quer dizer, caso estejamos interessados, por exemplo, em conhecer o conjunto formado pelos arranjos dos três últimos dígitos, deve-se considerar a lista constituída pelos primeiros 250 quadrados.

7.1: Proposição O conjunto dos arranjos constituídos pelos três últimos dígitos dos números quadrados perfeitos fica determinado pelos 250 primeiros termos.

A ideia consiste em provarmos que os quadrados dos termos equidistantes dos extremos no conjunto {1, 2, 3,..., 497, 498, 499} são congruentes módulo1000.
De fato, $x^2 \equiv x^2 - 1.000x + 250.000 = (500 - x)^2 \implies x^2 \equiv (500 - x)^2$.

Se quisermos ser um pouco mais ousados, veremos de modo semelhante que o conjunto formado pelos arranjos dos quatro últimos dígitos fica determinado pelos primeiros 2.500 números quadrados. Todos esses resultados são de fácil demonstração de acordo com a Aritmética Modular e suas fantásticas propriedades, de onde ainda podemos estabelecer uma fórmula geral, através da qual fica evidente a alta eficiência das relações associadas às potências de dez que sem dúvidas, se justifica pela adoção do Sistema de Numeração Decimal atrelado ao revolucionário **Princípio da Escrita Posicional**.

Agora, fica claro também que existe um custo implícito em cada uma das Relações mencionadas que consiste precisamente no repertório mínimo de Classes de Equivalências necessárias à adoção da relação e dispostas evidentemente numa tabela conforme veremos. Assim, já vimos que a relação Módulo 100 com uma eficiência de 78% exige um repertório com apenas 22 Classes, já para Módulo 1.000**,** cuja eficiência é de aproximadamente incríveis 84% exigiria um repertório com 165 Classes**,** tornando a mesma pelo menos sob esse aspecto completamente indesejável. Veja o caso da Relação Módulo 10 com uma eficiência de apenas 40% que exige um repertório com 6 Classes.

7.2: Parâmetro de rendimento computacional para as congruências

Sem dúvidas, seria muita ingenuidade colocar todas as congruências modulares no mesmo patamar de eficiência**,** admitindo-se que a mesma pode ser avaliada de forma satisfatória tomando como principal parâmetro a porcentagem de classes residuais nas quais não encontramos números quadrados perfeitos.

Aliás, já nos referimos às mesmas como formas algébricas incompatíveis que sempre existirão seja qual for a Relação de Congruência escolhida com exceção daquela que indica paridade **(**mod2**)** à qual podemos associar eficiência nula.
Considerando que existem setenta e oito classes residuais associadas à Relação (mod100) e incapazes de abrigar números quadrados, dizemos que a mesma admite uma eficiência de 78%.

Sabe-se também que existem cinco classes residuais associadas à relação (mod9) nas quais não se encontra quadrados perfeitos, conclui-se que a mesma admite uma eficiência de aproximadamente 56%. Entretanto, vale destacar que a relação (mod9) apresenta a vantagem operacional de levar em conta todos os dígitos, diferentemente daquela (mod100) determinada pelos dois últimos algarismos. Ressalte-se ainda que a alta eficiência da relação (mod100) aliada a sua praticidade pode ser considerada a verdadeira mola propulsora no desenvolvimento do MTC.

Outra possível explicação para esse baixo rendimento Numérico é que a Tomada de Decisão sobre qual das formas algébricas com relação especificamente à divisibilidade por nove (partição) está presente, não leva em conta a ordem dos algarismos decimais. Assim, podemos ter milhares de números que se formados pelos mesmos algarismos, integrantes do **Conjunto das Permutações**, admitirão a mesma forma algébrica, conforme verificamos durante a análise elementar sobre a distribuição dos quadrados perfeitos.

Logo, quando considerada isoladamente, essa etapa que verifica a presença de formas algébricas compatíveis não tem muita força no sentido numérico, desempenhando, portanto, um papel de coadjuvante no processo de construção do Método das Terminações Características para uma eficiente identificação de quadrados perfeitos, sem apelarmos para a sua decomposição em fatores primos. Haja vista as enormes dificuldades tanto algébricas quanto numéricas que em linhas gerais sempre estão associadas a sua obtenção e configura há bastante tempo um problema extremamente complexo principalmente em termos computacionais com grande impacto na ciência da computação em especial no ramo **criptografia RSA.**

Há outra característica algébrica diretamente associada à Relação Módulo 100 sobre a qual não podemos deixar de fazer alguns comentários. O nosso objetivo nesse momento consiste em justificar de forma mais detalhada, a adoção da relação elencada, mesmo já tendo sido explorada sob o aspecto de eficiência com destaque para a **Porcentagem de Classes Residuais** incapazes de abrigar números quadrados. Em outras palavras, há ciência de que a relação módulo 100 admite uma eficiência de 78%. Isso quer dizer que das 100 classes residuais associadas à mesma, 78 delas são incapazes de abrigar números quadrados perfeitos.

Noutras palavras, não existe possibilidade de se encontrar números quadrados em qualquer uma dessas classes. Não se pode negar que mesmo isoladamente, esse é um resultado surpreendente para os nossos objetivos que visa à descoberta de um novo método predominantemente algébrico capaz de identificar quadrados perfeitos sem a necessidade de buscarmos a sua Decomposição em Fatores Primos. Apesar do inconveniente de levar em conta ou ficar determinada apenas pelos dois últimos dígitos constantes na sua representação em sistema de representação decimal.

Como se não bastasse essa alta eficiência numérica, vale mencionar outra consequência advinda da sua adoção: refiro-me ao fato de que todas as classes de equivalências associadas à relação supracitada são completamente Livres de Soma, com exceção de R(100). Em outras palavras, o número resultante da soma de dois termos em qualquer uma das classes mencionadas não integra a referida classe.

Isso reforça ainda mais a alta eficiência da partição associada à relação em questão, pois indica que ao se considerar a mesma com vistas à identificação de quadrados perfeitos, obtém-se uma partição na qual todas as classes são livres de soma. Observe que esse fato não ocorre para qualquer congruência. Veja o caso da congruência módulo três para a qual existem duas classes associadas nas quais se encontram quadrados: $3m\ e\ 3m\ +\ 1$ de modo que apenas esta é livre de somas.

7.3: Proposição A classe de números quadrados $Q_{100}(49)$ é livre de soma.

$x, y\ \in\ Q_{100}(49)\ \Longrightarrow x\ \equiv y\ \equiv 49\, mod\ 100\ \Longrightarrow x + y\ \equiv 98\, mod 100\ \notin\ Q_{100}(49)$

Na verdade, para qualquer congruência, sempre haverá ao menos uma classe associada que não será livre de somas. Tomemos como exemplo a relação Módulo 17 sobre a qual não sabemos de antemão quanto vale a sua eficiência, apesar da mesma ser de fácil determinação, exigindo a consideração dos restos dos oito primeiros quadrados perfeitos. Independente disso, sabe-se pela nossa experiência que há uma classe de números quadrados indicada por $Q_{17}(0)$**,** de modo que a mesma inclui todos os quadrados da forma $289t^2$. Logo, fica evidente que não é livre de soma, visto existirem ao menos dois termos, cuja soma ainda pertence à Classe.

Podemos traçar uma espécie de paralelo com a questão da eficiência numérica sobre a qual já comentamos o fato de que apenas a Congruência Módulo 2 admite uma eficiência nula (única exceção). Noutras palavras, escolhido um inteiro positivo, existe ao menos uma classe de equivalência associada ao mesmo incapaz de abrigar quadrados perfeitos o que é fantástico para os nossos objetivos, do contrário, não faria sentido falar em eficiência para uma relação de congruência.

7.4: Congruência Módulo 1.000: Uma relação mais eficiente?

Uma possibilidade interessante consiste na escolha de uma Relação de Congruência com alta porcentagem associada à eliminação de Classes Residuais nas quais não haja possibilidade de encontrar quadrado perfeito, conforme mostrado noutra seção da nossa pesquisa. Veja o caso da Relação Módulo 1.000**,** para a qual associamos apenas 165 classes residuais, capazes de abrigar números quadrados. Já comentamos que por tudo isso, a mesma admite uma eficiência de 83,5%.

Na verdade, há outro aspecto que torna a Relação (Mod.1000)**,** extremamente eficiente nesse contexto: Numericamente, ela fica perfeitamente determinada pelos três últimos dígitos do número em questão. Naturalmente, toda essa facilidade está associada ao fato do número 1.000 representar uma potência da base na qual o número está escrito, donde se sabe que a mesma é decimal. Assim, de modo geral, conclui-se que sob esses aspectos, as relações desse tipo são as mais eficientes, conforme se verifica com a ampliação da discussão elencada. Como os exemplos sempre costumam ajudar, tomaremos as seguintes classes residuais:

$$\{R(129), R(329), R(529), R(729), R(929)\}$$

De modo que apresentar ao menos uma das 165 terminações características passa a ser uma condição necessária, mas não suficiente para que um inteiro positivo figure entre os quadrados perfeitos. Escolhemos as mesmas pelo fato de admitirem os dois últimos dígitos em comum, facilitando nossos comentários. Imagine agora que escolhemos de forma aleatória o número 456.229 e precisamos decidir se ele integra os quadrados perfeitos. Nesse caso, não haveria a menor dificuldade, já que dentre as 165 classes elencadas, não existe R(229) o que de fato está relacionado à paridade (ímpar) das parcelas adjacentes dos seus termos. Logo, podemos concluir sem margem de erro que o número em questão não é quadrado perfeito, segundo a Congruência Módulo 1.000, adotada nesse caso como o único parâmetro decisório.

Na tentativa de tornar os comentários ainda mais claros, tomaremos novamente a classe R(49) como uma referência didática, de modo que seja mantida uma linha coerente em termos de metodologia cujo fundamento pode ser justificado pelo fato já mencionado de que estamos considerando uma relação simétrica, reflexiva e transitiva indicando por tudo isso, uma Relação de Equivalência, donde sabemos que a bem da verdade, qualquer uma das suas classes pode ser utilizada nas demonstrações sem prejuízo. Assim, todas essas conclusões podem ser naturalmente estendidas a qualquer uma das classes associadas à Congruência Módulo 100**,** admitindo-se que a mesma opere exclusivamente entre os quadrados.

Esperamos que haja um entendimento por completo dos comentários que acabamos de citar, principalmente pelo fato evidente de que não faria muito sentido exibir uma demonstração para cada uma das 22 Classes constantes neste artigo. Acredita-se que o leitor deve ser poupado de todo esse trabalho mais uma vez por uma questão principalmente de didática e pelo fato das relações envolvidas, serem simétricas fazendo da mesma uma tarefa certamente mais confortável. Assim, faremos uma pequena modificação na representação das classes em questão como uma forma de facilitar a comunicação com o leitor de modo que se possa identificar automaticamente o divisor implícito na representação de cada uma das classes.

Desse modo, passamos a escrever $\boldsymbol{Q_{100}}\ (\mathbf{49})$ para designar a classe dos números quadrados perfeitos que deixam resto 49, quando divididos por 100.

Essa pequena alteração fará uma enorme diferença principalmente quando houver necessidade de comparar duas ou mais congruências principalmente em termos de eficiência numérica. Aliás, vejamos mais uma vez o caso da divisibilidade por três. Já sabemos que nesse contexto, temos apenas duas classes de equivalências que agora podem ser representadas da seguinte forma: $\boldsymbol{Q_3}\ (\mathbf{0})$ **e** $\boldsymbol{Q_3}\ (\mathbf{1})$.

Sendo que a primeira indica os quadrados perfeitos que deixam resto zero quando divididos por três, já a segunda os quadrados que deixam resto um quando divididos por três. Observe que a primeira classe citada representa os quadrados múltiplos de três. Logo, adotada essa convenção, temos que o índice utilizado representa o resto e o número entre parênteses indica o divisor da divisão correspondente.

Não custa nada acrescentarmos que apesar de haver apenas duas classes associadas à divisibilidade por três, isso não quer dizer necessariamente que ela seja eficiente. Isso se justifica pelo fato de que estamos interessados mesmo é na porcentagem de classes residuais que são “aniquiladas” quando a relação deixa de operar entre os inteiros positivos e passa a atuar especificamente entre os quadrados perfeitos.

Sendo assim, das três classes conectadas à congruência módulo três, somente uma desaparece nessas condições. Em outras palavras, apenas uma delas é incapaz de abrigar quadrados: aquela formada pelos inteiros positivos da forma $3m + 2$. Logo, dizemos que a Congruência Módulo 3 admite uma eficiência de aproximadamente 33, 33%, já que apenas uma daquelas três classes não abriga números quadrados.

Agora o leitor certamente passa a entender a não utilização dessa relação na construção do Método das Terminações Características simplesmente pelo fato da mesma apresentar baixa eficiência em comparação com as demais, apesar da existência de um Critério de Divisibilidade de fácil aplicação em linhas gerais de análise. De fato, Um inteiro escrito em sistema decimal será divisível por três se, e somente se, a soma dos valores absolutos dos seus dígitos resulta divisível por três.

De fato, é muito frequente a sua utilização em vários problemas da Teoria dos Números tanto em caráter elementar como avançado. Esses comentários ficam bem mais evidentes quando atentamos para o problema da representação de inteiros positivos como uma soma de quadrados na qual se utiliza a mesma quase que com exclusividade.

Isso tudo vale principalmente para o caso particular que envolve a soma de dois quadrados, conforme comentamos em outras partes do texto numa referência ao Clássico Teorema de Lagrange que resolve o problema de forma definitiva ao afirmar que qualquer inteiro positivo pode ser representado mediante uma soma que utiliza no máximo quatro quadrados.

Aliás, esse pode ser considerado o marco inicial da Teoria Aditiva dos Números sobre a qual já fizemos alguns comentários e através deles, deixamos muito claro que não havia intenção da nossa parte em aprofundar as discussões pertinentes a essa Teoria principalmente pelo fato da mesma certamente fugir ao nível do nosso trabalho de pesquisa.

Sem falar ainda que não vislumbramos contribuições da mesma relativamente ao **Método das Terminações Características** de números quadrados, de modo que a sua abordagem evidentemente realizada de uma forma superficial figura em linhas gerais apenas como uma genuína curiosidade matemática ou talvez até como uma espécie de aprofundamento conceitual associado ao estudo em questão.

Capítulo VIII

Modelos de Aplicações Avançadas

(1) Fernando gosta muito de estudar Matemática. Numa determinada aula, ele precisou calcular o valor de uma potência como parte da tarefa escolar. Assim que terminou os cálculos, tratou de mostrá-lo ao professor que imediatamente estranhou a resposta fornecida pelo aluno $(678.543)^2 = 486.603.672.982.849$.

(2) Aplique o MTC para decidir se os números seguintes são quadrados perfeitos e calcule as suas raízes na hipótese de uma resposta positiva.

(a) 1.369 (b) 3.969 (c) 5.329 (d) 1.321.

(3) Demonstre que o número 1.089 representa quadrado perfeito, mesmo quando reescrito da direita para a esquerda e calcule ambas as raízes.

(4) Determine a soma de todos os números quadrados perfeitos com exatamente quatro algarismos quando representados em sistema de decimal.

(5) Classifique os números abaixo em Racionais (R) ou Irracionais (I) levando-se em conta a bipartição dos naturais pela definição de números quadrados.

(a) $\sqrt{247}$ (I) (b) $\sqrt{729}$ (R) (c) $\sqrt{1029}$ (I) (d) $\sqrt{4936}$ (I).

(6) Decida através do MTC de Números Quadrados sobre a existência de algum Polígono Convexo e Simples com um total de 1.235 Diagonais.

(7) Aplique o MTC para calcular tanto as terminações características quanto as raízes dos números abaixo, sabendo que os mesmos são quadrados perfeitos.

(a) 29XY (b) 31XY (c) 50XY (d) 37XY.

(8) Aplique o MTC para decidir se os números seguintes são quadrados perfeitos e calcule as suas raízes na hipótese de uma resposta positiva.

(a) 727.609 (b) 419.904 (c) 536.889 (d) 142.641

(9) Aplique o MTC para calcular tanto as terminações características quanto as raízes dos números abaixo, sabendo que os mesmos são quadrados perfeitos.

(a) 273.5XY (b) 290.5XY (c) 540.2XY (d) 703.9XY

(10) Verifique através do MTC e propriedades de potências se o número $734.449^{537.925}$ representa um quadrado perfeito (Questão de Paridade).

(11) Sabendo que 10.243.249 é a **"**Concatenação**"** de dois quadrados perfeitos com a mesma ordem de grandeza, mostre que ele próprio não é número quadrado.

(12) Dado um produto de quatro números inteiros positivos e consecutivos, determine o menor inteiro positivo que devemos somar a este produto, a fim de que o mesmo se transforme em quadrado perfeito e calcule sua raiz quadrada.

(13) Faça uma investigação para descobrir o único quadrado perfeito de oito dígitos, cuja representação em sistema decimal começa com o arranjo 3518**.**

(14) Mostre que um número quadrado e sua raiz têm sempre mesma paridade.

(15) Henrique gosta muito de estudar Matemática. Ele resolve fazer uma experiência à qual exige a soma de um número quadrado com a sua raiz, encontrando 546.879 como resposta. Mostre que ele cometeu algum equívoco.

(16) Paulo escolhe aleatoriamente um inteiro positivo numa lista com 100 naturais consecutivos. Demonstre que a Probabilidade de ele escolher um quadrado perfeito nesse contexto em particular nunca é superior aos 10%**.**

(17) Calcule a raiz quadrada de 29 com aproximação de três casas decimais.

(18) Calcule a soma dos primeiros 64 números quadrados perfeitos ímpares.

(19) Mostre que nenhum dos membros de uma sequência "elementar" como (11, 111, 1111, 11111, 111111,...) é um número quadrado perfeito. Sugestão: verificar a ausência de terminação característica em todos os seus elementos.

(20) Mostre que nenhum dos membros de uma sequência "elementar" como (22, 222, 2222, 22222, 222222,...) é um número quadrado perfeito. Sugestão: verificar a ausência de terminação característica em todos os seus elementos.

(21) Mostre que nenhum dos membros de uma sequência “elementar” como (33, 333, 3333, 33333, 333333,...) é um número quadrado perfeito. Sugestão: verificar a ausência de terminação característica em todos os seus elementos.

(22) Mostre que nenhum dos membros de uma sequência “elementar” como (44, 444, 4444, 44444, 444444,...) é um número quadrado perfeito. Sugestão: observe a terminação da quarta parte de cada um dos membros da sequência.

(23) Mostre que nenhum dos membros de uma sequência “elementar” como (55, 555, 5555, 55555, 555555,...) é um número quadrado perfeito. Sugestão: verificar a ausência de terminação característica em todos os seus elementos.

(24) Mostre que nenhum dos membros de uma sequência “elementar” como (66, 666, 6666, 66666, 666666,...) é um número quadrado perfeito. Sugestão: verificar a ausência de terminação característica em todos os seus elementos.

(25) Mostre que nenhum dos membros de uma sequência “elementar” como (77, 777, 7777, 77777, 777777,...) é um número quadrado perfeito. Sugestão: verificar a ausência de terminação característica em todos os seus elementos.

(26) Mostre que nenhum dos membros de uma sequência “elementar” como (88, 888, 8888, 88888, 888888,...) é um número quadrado perfeito. Sugestão: verificar a ausência de terminação característica em todos os seus elementos.

(27) Mostre que nenhum dos membros de uma sequência “elementar” como (99, 999, 9999, 99999, 999999,...) é um número quadrado perfeito. Sugestão: verificar a ausência de terminação característica em todos os seus elementos.

(28) Demonstre que todo número quadrado perfeito maior do que nove admite pelo menos dois dígitos distintos quando representado em sistema decimal**.**

(29) Demonstre pelo algoritmo da divisão euclidiana que todo número quadrado perfeito admite somente uma das formas algébricas $5m, 5m + 1\ ou\ 5m + 4$.

(30) Demonstre que se um número quadrado tem 2n dígitos na sua representação decimal, então a sua raiz quadrada tem exatamente n dígitos.

(31) Resolva a equação $(x_4x_3)^2 + (x_2x_1)^2 = x_4x_3x_2x_1$ no conjunto dos números inteiros positivos. A solução detalhada pode ser vista no apêndice.

Capítulo IX

Dois números quadrados e uma nova equação algébrica

Sabe-se pelo teorema de Lagrange que todo número inteiro pode ser obtido mediante uma soma de até quatro quadrados. Nesse sentido, duas perguntas surgem naturalmente quando se admite uma diminuição do número de quadrados a serem somados nesse contexto de relevância indiscutível para a teoria elementar dos números; notadamente no sentido histórico desse profícuo campo de pesquisa. Dentre elas: Quais os números inteiros que são soma de três quadrados? Por incrível que pareça, tem-se aqui uma pergunta muito mais simples em relação à primeira onde esta figurou como um enorme desafio para vários matemáticos. De fato, observando-se os números com até dois dígitos que não admitem uma representação do último tipo, chega-se a uma conclusão extremamente interessante. Para obtê-los, somamos os primeiros números quadrados, três a três.

{0, 1, 2, 3, 4, 5, 6, **7**, 8, 9, 10, 11, 12, 13, 14, **15**, 16, 17, 18, 19, 20, 21, 22, **23**, 24, 25, 26, 27, 28, 29, 30, **31**, 32, 33, 34, 35, 36, 37, 38, **39**, 40, 41, 42, 43, 44, 45, 46, **47**, 48, 49, 50, 51, 52, 53, 54, **55**, 56, 57, 58, 59, 60, 61, 62, **63**, 64, 65, 66, 67, 68, 69, 70, **71**, 72, 73, 74, 75, 76, 77, 78, **79**, 80, 81, 82, 83, 84, 85, 86, **87**, 88, 89, 90, 91, 92, 93, 94, **95**, 96, 97, 98, 99}.

Observando os números acima com um pouco mais de atenção, percebe-se que eles formam uma progressão aritmética de razão oito. Como não temos intenção de aprofundar a discussão desse problema, mas fornecer os primeiros indícios que permitem descobrir a solução do mesmo; adiante-se apenas que esse padrão elementar será preservado mesmo na hipótese de se aumentar o repertório inicial de números quadrados. Quer dizer, realizando a mesma experiência com mais quadrados, os resultados serão semelhantes. Em outras palavras, haverá somente uma ampliação daquela progressão. Assim, enunciaremos sem a demonstração:

9.1: Proposição. A condição necessária e suficiente para que um inteiro positivo seja soma de três quadrados perfeitos é não admitir a forma algébrica $8m + 7$.

Exemplo: Verifique se 678.945 se escreve como uma soma de três quadrados. Sol. O número é da forma $8m + 1 \neq 8m + 7$ assim, a resposta é certamente negativa.

A próxima pergunta que faremos, ainda a respeito do primeiro problema, consiste na identificação dos números inteiros que são soma de dois quadrados perfeitos. Infelizmente, neste caso, a solução é bem mais difícil. Assim, serão fornecidos apenas os primeiros indícios através dos quais é possível enxergar a solução que depende essencialmente da fatoração nos primos. Faremos uma experiência semelhante tomando o mesmo repertório de números quadrados, mas somando os arranjos dois a dois. Depois, voltaremos a nossa atenção para a fatoração primária de algumas das somas em questão, buscando naturalmente alguma regularidade.

{0, 1, 4, 9, 16, 25, 36, 49, 64, 81}

Tomando como base a experiência anterior, não será mais exibida a relação com os resultados das somas mencionadas, visando simplificar a exposição em questão. Vamos tomar algumas dessas somas e colocar em evidência a sua fatoração, buscando ao menos uma propriedade em comum. Assim, é interessante mencionar um resultado fundamental que resolve o problema citado para os números primos:

9.2: Proposição. Todo primo da forma $4t + 1$ se escreve, de forma única uma como soma de dois números quadrados perfeitos.

9.3: Proposição. Nenhum primo da forma $4t + 3$ se escreve como uma soma de dois números quadrados. A demonstração elementar será deixada a cargo do leitor.

Teorema. Se dois inteiros podem ser escritos como soma de dois quadrados, então o seu produto admite essa mesma representação. (Identidade de Fibonacci)

$$(\boldsymbol{a^2 + b^2}).(\boldsymbol{c^2 + d^2}) = (\boldsymbol{ad - bc})^2 + (\boldsymbol{ac + bd})^2 \ (\boldsymbol{I})$$

Agora, devemos voltar a atenção para o Teorema Fundamental da Aritmética segundo o qual todo inteiro ou é primo ou escreve de forma única como produto de primos. Agora, estamos em condições de tomar resultados particulares resultantes da soma de dois quadrados e atentar para alguns detalhes da sua fatoração.

{2, 5, 10, 17, 26, 37, 50, 65, 82, 8, 13, 20, 29, 40, 53, 85, 18, 25, 34, 45, 58, 73, 90, 32, 41, 52, 80, 97, 61, 74, 89, 106, 72, 100, 117, 98, 113, 130, 128, 145}.

Como o problema está resolvido para os primos, estes serão descartados do conjunto. Quer dizer, somente os números compostos nos interessam. Para tornar a nossa experiência mais interessante, recomenda-se a observação dos expoentes de cada fator primo nos aspectos de paridade, segundo as categorias: $4t + 1\ e\ 4t + 3$.

Compostos Pares:

$10 = 2\,x\,5,\quad 26 = 2\,x\,13,\quad 50 = 2\,x\,5^2,\quad 82 = 2\,x\,41,\quad 8 = 2^3, 20 = 2^2x\,5,\quad 40 = 2^3x\,5,\quad 18 = 2\,x\,3^2,\quad 34 = 2\,x\,17,\quad 58 = 2\,x\,29\quad 90 = 2\,x\,3^2\,x\,5,\quad 32 = 2^5,\quad 52 = 2^2\,x\,13,\ 80 = 2^4\,x\,5,\ 74 = 2\,x\,37,\ 100 = 2^2x\,5^2,\ 106 = 2\,x\,53,\ 98 = 2\,x\,7^2,\ 128 = 2^7, 130 = 2\,x\,5\,x\,13.$

Veja que todos os fatores primos da forma $4t + 3$ admitem seus expoentes pares.

Compostos Ímpares:

$65 = 5\,x\,13, 85 = 5\,x\,17, 25 = 5^2, 45 = 3^2\,x\,5, 117 = 3^2\,x\,13, 145 = 5\,x\,29.$

Veja que todos os fatores primos da forma $4t + 3$ admitem seus expoentes pares.

Teorema (Gauss-Legendre). Um número inteiro positivo é soma de dois quadrados, se, e somente se, são pares os expoentes dos fatores primos da forma $4t + 3$.

Apresentação do Problema Fundamental.

Quando somamos dois números quadrados, suas raízes não costumam reaparecer no resultado da operação. De fato, $25^2 + 36^2 = 1.521$, $29^2 + 43^2 = 2.690$, $37^2 + 49^2 = 3.770$, etc. Essa é a regra geral, mas que pode nos surpreender quando analisada.

Refletindo sobre essa questão aparentemente simples, deve-se fazer a seguinte pergunta: Será que existem pares de números quadrados, cujas raízes reaparecem no final da soma? Visando facilitar a busca pela resposta, adotaremos uma restrição segundo a qual os números quadrados devem possuir a mesma ordem de grandeza. Uma interessante equação surge naturalmente atrelada a essa fantástica pergunta**:**

$$\boldsymbol{(x_4x_3)^2 + (x_2x_1)^2 = x_4x_3x_2x_1}\ \textbf{(Caso n = 2)}$$

Em outras palavras, a equação acima admite solução nos inteiros positivos?

Depois de muita simulação, dado o entusiasmo pessoal provocado pela minha curiosidade, mergulhei numa busca pela resposta dessa questão, movido tanto pela paixão quanto pela intuição, visto que ainda não tinha me deparado com equações desse tipo. Assim, passei a acreditar na possibilidade de que esta seria mais uma das minhas contribuições como matemático amador, fato que se mostrou verdadeiro depois de alguns meses quando finalmente, cercados de limitações computacionais, foi possível superar o problema, mediante a conclusão de uma resposta positiva.

Além disso, sendo possível exibir todas as soluções correspondentes, respeitadas as hipóteses adotadas inicialmente, do contrário, a complexidade computacional seria imensamente maior. Agora, podemos nos dar ao luxo de ser mais objetivos, devido aos vários comentários feitos até o momento. Além de todas as proposições mencionadas que sem dúvidas, servirão como suporte indispensável para compreensão geral da solução dessa classe de problemas.

Solução. Fazendo $x_4x_3 = a\ e\ x_2x_1 = b$ em (II), resulta $a^2 + b^2 = 100a + b$.

Reagrupando os termos semelhantes e pela técnica de completar quadrados:

$$(2a - 100)^2 + (2b - 1)^2 = 10.001 \quad \text{(III)}$$

A grande questão agora é verificarmos se o número do segundo membro pode ser escrito mediante soma de dois quadrados. Além disso, quantas são as representações possíveis na hipótese de uma resposta positiva? (a e b mesma ordem de grandeza). Como a fatoração primária de $10.001 = 73\ x\ 137$ e ambos os fatores são da forma $4t + 1$, concluímos pelo teorema de Gauss-Legendre que 10.001 pode ser obtido mediante uma soma de dois quadrados. Para isso, reescrevemos cada um dos fatores primos que integram aquela fatoração canônica:

$73 = 8^2 + 3^2\ \ e\ 137 = 11^2 + 4^2$. Assim, temos $10.001 = (8^2 + 3^2)x(11^2 + 4^2)$.

Apoiados na identidade de Fibonacci, encontraremos ambos os quadrados.

$$(a^2 + b^2).(c^2 + d^2) = (ad - bc)^2 + (ac + bd)^2\ (I)$$

Assim, concluímos que 10.101 = 76^2 + 65^2. Voltando a equação III, resulta:

$2a - 100 = 76 \Longrightarrow a = 88$. Por outro lado, $2a - 100 = -76 \Longrightarrow a = 12$.

$2b - 1 = 65 \Longrightarrow b = 33$. Por outro lado, $2b - 1 = -33 \Longrightarrow b = -16 \notin \mathbb{Z}$.

Logo, concluímos que o problema fundamental admite as duas soluções seguintes:

$$\mathbf{88^2 + 33^2 = 8.833}\ \boldsymbol{e}\ \mathbf{12^2 + 33^2 = 1.233}$$

Ampliando a discussão para as próximas ordens de grandeza, fica claro que o problema se mostra ainda mais interessante, dada a simetria das equações resultantes. O fato é que se pode fazer referência a uma família de equações caracterizadas pela soma de dois números quadrados com a mesma ordem de grandeza nas quais ambas as raízes quadradas reaparecem no resultado da operação. Seguindo essa linha de raciocínio, visando principalmente não deixar dúvidas de que tais resultados são de minha autoria, apresentarei as soluções das duas próximas equações que podem ser resolvidas de forma semelhante.

A decisão de apresentar essas descobertas, guardadas há bastante tempo, foi motivada em parte para prestar uma homenagem ao meu orientador, sem o qual não teria transformado o meu texto em algo que pudéssemos chamar de uma tese de mestrado, já que mais parecia um livro, devido à sua linguagem corrida. Tudo isso, levando-se em conta que a sua principal linha de pesquisa é a álgebra, outra área fascinante da Matemática, sendo impossível não se apaixonar pela mesma. Tenho quase certeza de que mesmo com toda a sua experiência, ele ainda não havia tomando conhecimento da existência dessa classe de equações algébricas.

Resumo da equação para o caso n = 3:

$(\mathrm{x_6x_5x_4})^2 + (\mathrm{x_3x_2x_1})^2 = \mathrm{x_6x_5x_4x_3x_2x_1}$: $[(990)^2 + (100)^2 = 990.100]$

$(2a - 1.000)^2 + (2b - 1)^2 = 1.000.001 = 101\ x\ 9.901 = 980^2 + 199^2$

Resumo da equação para o caso n = 4:

$(x_8x_7x_6x_5)^2 + (x_4x_3x_2x_1)^2 = x_8x_7x_6x_5x_4x_3x_2x_1$

$(2a - 10.000)^2 + (2b - 1)^2 = 100.000.001 = (4.705)^2 + (8.824)^2$

$(9.412)^2 + (2.353)^2 = 94.122.353$

Capítulo X

Conclusões

Toda essa análise culminou com a criação de uma poderosa ferramenta para a identificação de números quadrados perfeitos e cálculo de suas raízes, denominada de o Método das Terminações Características (MTC) que permite ainda obter aproximações de irracionais quadráticos via números racionais, mediante decimais exatos na hipótese de uma resposta negativa. Agora, uma das conclusões mais importantes é a de que tanto os números primos**,** quanto as suas fatorações primárias podem ser descartadas desse contexto. Isso significa romper com uma prática que há décadas vem dominando o ambiente escolar como uma espécie de amarra, apesar das outras utilidades que lhe podem ser atribuídas como o cálculo da quantidade de divisores assim como a tomada de decisão sobre a representação de um natural como uma soma de dois quadrados com a determinação ainda das diferentes formas de efetuarmos essa expansão (Teoria Aditiva dos Números).

Insistimos que o MTC, devido à sua inerente capacidade de distinguir quadrados de não quadrados como nenhum outro algoritmo representa uma estratégia inovadora, divulgada em primeira mão, através da qual somos capazes de efetivamente resolver ambos os problemas elencados, sem a constante preocupação com a presença dos primos que representa o pior dos cenários na Teoria dos Números. Duas outras importantes aplicações da fatoração primária devem ser mencionadas, até mesmo pelo fato de serem amplamente conhecidas por alunos e professores: Refiro-me ao Mínimo Múltiplo Comum (MMC) e ao Máximo Divisor Comum (MDC). Agora, vale lembrar que ainda nesse caso, não podemos garantir de forma alguma, tratar-se da melhor estratégia com vistas à resolução destes dois problemas. Na verdade, segundo a Aritmética Clássica, sabemos que o MMC x MDC de dois ou mais inteiros positivos coincide com o produto desses mesmos números (Teorema).

Bibliografia

BARBOSA, Ruy Madsen. **Descobrindo Padrões Pitagóricos: Geométricos e Numéricos.** São Paulo, Atual Editora, 1993.

BONJORNO, José Roberto. Matemática **(Coleção Fazendo a Diferença)**. Título IV – 1ed. – São Paulo. FTD, 2006.

BOYER, Carl Benjamin. **História da Matemática. 2ªed**. . São Paulo, Edgard Blücher 1996.

CARVALHO, João Bosco Pitombeira de. **A Raiz Quadrada ao Longo dos Séculos.** V Bienal SBM UFPB, 2010.

DANTE, Luiz Roberto. **Didática da resolução de problemas**. São Paulo: Ática, 1989.

Eduardo S. G. Leandro & Gabriel A. Guedes. **Densidade de Shnirel 'Man, Teorema de Man e a Conjectura de Goldbach**. III Bienal da SBM, UFG 2006.

LANG, serg. **Álgebra para Graduação**. Rio de Janeiro: Editora Ciência Moderna 2008.

LIMA, E. L. P; CARVALHO, C. P.; WAGNER, E.; MORGADO, A.C. **A Matemática do Ensino Médio**, vol. 1. Coleção do Professor de Matemática. Rio de janeiro: Publicação da Sociedade Brasileira de Matemática, 1996.

LOPES, Maria Aparecida. **Introdução à Teoria dos Números e dos Números Primos**. UEPB, 2011.

MACHADO, Nilson José. **Matemática e língua materna**. São Paulo: Cortez, 1990.

MACIEL, Jarbas. **Elementos de Teoria Geral dos Sistemas.** Petrópolis, Editora Vozes: 1974.

Meu professor de Matemática e outras Histórias. Coleção do Professor de Matemática, Rio de Janeiro: Publicação da Sociedade brasileira de Matemática, 1991.

POLYA, George. **A arte de resolver problemas**. Trad. Heitor Lisboa de Araújo. Rio de janeiro: Interciência, 1978.

RIBENBOIM, Paulo. **Seis Décadas de Matemática**. Revista Matemática Universitária, edição – 45,1996.

SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números.** 3ed. Rio de janeiro: IMPA, 2009.

SINGH, Simon. **O Último Teorema de Fermat**. 10ªed. Rio de Janeiro: Record, 2004.

Apêndice

Tabela 5: números quadrados perfeitos com nove algarismos distintos não nulos.

139.854.276	**152.843.769**	**157.326.849**
215.384.976	**245.893.761**	**254.817.369**
326.597.184	**361.874.529**	**375.468.129**
382.945.761	**385.297.641**	**412.739.856**
523.814.769	**529.874.361**	**537.219.684**
549.386.721	**587.432.169**	**589.324.176**
597.362.481	**615.387.249**	**627.953.481**
653.927.184	**672.935.481**	**697.435.281**
714.653.289	**735.982.641**	**743.816.529**
842.973.156	**847.159.236**	**923.187.456**

A tabela acima contém todos os números quadrados entre as permutações simples dos algarismos 1, 2, 3, 4, 5, 6, 7, 8 e 9. Segundo o Princípio Fundamental da contagem, são 362.880. Sem dúvidas, a construção de uma tabela como essa, cuja autoria não se conhece, exigiu muito esforço computacional, haja vista a extensão de cada permutação assim como as dificuldades para percorrer tamanha quantidade. Infelizmente, todas as permutações em questão admitem a mesma forma algébrica compatível com os números quadrados, conforme a terceira etapa do MTC. Nesse sentido, vejamos de que forma MTC pode auxiliar na construção da referida tabela, notadamente no que diz respeito às suas terminações características. Como se trata de permutações simples sem a presença do zero, somente 17 classes devem ser consideradas. Cada qual admite parcelas adjacentes com sete dígitos. Sendo assim, resultam agora 85.680 permutações, sem dúvidas, um valor ainda expressivo, mas que indica uma incrível redução de $\cong 76\%$ do total.

Tabela 4: Termos gerais das classes de números quadrados

Classe	Termo Geral
$R(01)$	$a_m = \begin{cases} (25m-24)^2 & ,se\ m = 2t-1. \\ (25m-1)^2 & ,se\ m = 2t. \end{cases}$
$R(121)$	$a_m = \begin{cases} (25m-14)^2 & ,se\ m = 2t-1. \\ (25m-11)^2 & ,se\ m = 2t. \end{cases}$
$R(441)$	$a_m = \begin{cases} (25m-4)^2 & ,se\ m = 2t-1. \\ (25m-21)^2 & ,se\ m = 2t. \end{cases}$
$R(361)$	$a_m = \begin{cases} (25m-6)^2 & ,se\ m = 2t-1. \\ (25m-19)^2 & ,se\ m = 2t. \end{cases}$
$R(81)$	$a_m = \begin{cases} (25m-16)^2 & ,se\ m = 2t-1. \\ (25m-9)^2 & ,se\ m = 2t. \end{cases}$
$R(04)$	$a_m = \begin{cases} (25m-23)^2 & ,se\ m = 2t-1. \\ (25m-2)^2 & ,se\ m = 2t. \end{cases}$
$R(324)$	$a_m = \begin{cases} (25m-7)^2 & ,se\ m = 2t-1. \\ (25m-18)^2 & ,se\ m = 2t. \end{cases}$
$R(144)$	$a_m = \begin{cases} (25m-13)^2 & ,se\ m = 2t-1. \\ (25m-12)^2 & ,se\ m = 2t. \end{cases}$
$R(64)$	$a_m = \begin{cases} (25m-17)^2 & ,se\ m = 2t-1. \\ (25m-8)^2 & ,se\ m = 2t. \end{cases}$
$R(484)$	$a_m = \begin{cases} (25m-3)^2 & ,se\ m = 2t-1. \\ (25m-22)^2 & ,se\ m = 2t. \end{cases}$

Classe	Termo Geral
$R(09)$	$a_m = \begin{cases} (25m-22)^2 & ,se\ m = 2t-1. \\ (25m-3)^2 & ,se\ m = 2t. \end{cases}$
$R(529)$	$a_m = \begin{cases} (25m-2)^2 & ,se\ m = 2t-1. \\ (25m-23)^2 & ,se\ m = 2t. \end{cases}$
$R(49)$	$a_m = \begin{cases} (25m-18)^2 & ,se\ m = 2t-1. \\ (25m-7)^2 & ,se\ m = 2t. \end{cases}$
$R(169)$	$a_m = \begin{cases} (25m-12)^2 & ,se\ m = 2t-1. \\ (25m-13)^2 & ,se\ m = 2t. \end{cases}$
$R(289)$	$a_m = \begin{cases} (25m-8)^2 & ,se\ m = 2t-1. \\ (25m-17)^2 & ,se\ m = 2t. \end{cases}$
$R(16)$	$a_m = \begin{cases} (25m-21)^2 & ,se\ m = 2t-1. \\ (25m-4)^2 & ,se\ m = 2t. \end{cases}$
$R(36)$	$a_m = \begin{cases} (25m-19)^2 & ,se\ m = 2t-1. \\ (25m-6)^2 & ,se\ m = 2t. \end{cases}$
$R(256)$	$a_m = \begin{cases} (25m-9)^2 & ,se\ m = 2t-1. \\ (25m-16)^2 & ,se\ m = 2t. \end{cases}$
$R(576)$	$a_m = \begin{cases} (25m-1)^2 & ,se\ m = 2t-1. \\ (25m-24)^2 & ,se\ m = 2t. \end{cases}$
$R(196)$	$a_m = \begin{cases} (25m-11)^2 & ,se\ m = 2t-1. \\ (25m-14)^2 & ,se\ m = 2t. \end{cases}$
$R(25)$	$a_m = (10m-5)^2$