UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

FRANCISCO ERILSON FREIRE DE OLIVEIRA

SOBRE VÁRIAS DEMONSTRAÇÕES DO PEQUENO TEOREMA DE FERMAT E AS INTER-RELAÇÕES ENTRE AS ÁREAS DA MATEMÁTICA

FORTALEZA

2019

FRANCISCO ERILSON FREIRE DE OLIVEIRA

SOBRE VÁRIAS DEMONSTRAÇÕES DO PEQUENO TEOREMA DE FERMAT E AS INTER-RELAÇÕES ENTRE AS ÁREAS DA MATEMÁTICA

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Orientador: Prof. Dr. José Ederson Melo Braga

FORTALEZA

2019

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

O47s Oliveira, Francisco Erilson Freire de.
Sobre Várias Demonstrações do Pequeno Teorema de Fermat e as Inter-relações entre as Áreas da Matemática / Francisco Erilson Freire de Oliveira. – 2019.
60 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2019.
Orientação: Prof. Dr. José Ederson Melo Braga.

1. Pequeno Teorema de Fermat. 2. Demonstrações Clássicas. 3. Demonstrações Alternativas. 4. História da Matemática. 5. Inter-relações da Matemática. I. Título.

CDD 510

FRANCISCO ERILSON FREIRE DE OLIVEIRA

SOBRE VÁRIAS DEMONSTRAÇÕES DO PEQUENO TEOREMA DE FERMAT E AS INTER-RELAÇÕES ENTRE AS ÁREAS DA MATEMÁTICA

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática. Área de Concentração: Ensino de Matemática.

Aprovada em: 28/06/2019.

BANCA EXAMINADORA

Prof. Dr. José Ederson Melo Braga (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. José Alberto Duarte Maia
Universidade Federal do Ceará (UFC)

Prof. Dr. Eurípedes Carvalho da Silva
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Dedico este trabalho a meu bom Deus, criador do Céu e da Terra. A ele toda honra e glória. A minha amada esposa Edwirgens e meus queridos filhos Erick e Laís. Finalmente aos meus pais e irmãos, Maria do Socorro, Miguel Maia, Fátima Freire e Julio Edison.

AGRADECIMENTOS

A DEUS, pelo dom da vida e por me dar forças para prosseguir nos estudos, mesmo nos momentos mais difíceis.

À minha família. Em especial a Denise Edwirgens dos Santos Andrade (minha esposa), Francisco Erick Andrade Oliveira e Laís Andrade Oliveira (meus filhos), Maria do Socorro Freire de Oliveira (minha mãe), Miguel Maia de Oliveira (meu pai), Antonia de Fátima Freire de Oliveira e Julio Edison Freire de Oliveria (meus irmãos).

Aos meus queridos amigos Francisco Robério Pereira Magalhães e Marineide Ferreira Magalhães, que com seus esforços me ajudaram nos momentos mais difíceis, possibilitando minha dedicação aos estudos relativos ao Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, da Universidade Federal do Ceará - UFC.

Aos professores do PROFMAT da UFC.

Ao meu orientador, Professor Dr. José Ederson Melo Braga, pelas excelentes aulas ministradas no PROFMAT - UFC, pelo empenho dedicado, pela confiança que depositou em mim e pelas sugestões e preciosas contribuições para a produção deste trabalho.

Ao Professor Dr. José Alberto Duarte Maia, pelas inúmeras contribuições relativas aos conteúdos estudados durante o curso do PROFMAT, que mesmo em horários além das aulas, sempre esteve disponível para contribuir com a minha aprendizagem e pela cordial aceitação em participar da banca examinadora.

Ao caro professor Dr. Eurípedes Carvalho da Silva que, em detrimento de seus afazeres pessoais e profissionais, aceitou cordialmente nosso convite para participar da banca examinadora.

Ao Professor Dr. Esdras Soares de Medeiros Filho, pelo apoio e contribuições às pesquisas iniciais das demonstrações abordadas nesta dissertação.

Ao Professor Dr. Ângelo Papa Neto (IFCE), pelas valiosas contribuições acerca da apresentação das principais fontes de pesquisa sobre Teoria dos Números, utilizadas nesta dissertação.

A todos os meus colegas da turma do PROFMAT - UFC (ENA 2017). Destaco Antonio Erivan Bezerra Ferreira, Thedy Barbosa Bezerra, Maria Elisa de Castro Guimarães e Keyson Gondim Gomes, pelo apoio e parceria durante o curso.

Aos meus professores do curso de Licenciatura em Matemática do Instituto Federal de Educação, Ciência e Tecnologia do Ceará - IFCE, Campus Canindé, que sempre me proferiram

palavras de estímulo relativo ao estudo da Matemática e me possibilitaram a crença da construção de uma educação de qualidade. Avulto a Professora Ma. Luciana de Oliveira Souza Mendonça, Professora Dra. Ana Cláudia Gouveia de Sousa, Professor Me. Diego Ponciano de Oliveira Lima, Professor Me. Diego Eloi Misquita Gomes, Professor Me. Francisco Ricardo Nogueira de Vasconcelos, Professor Clodomir Silva Lima Neto e Professor Genilson Gomes da Silva.

Ao meu colega e grande amigo Luiz Augustavo Almeida Feitoza, por todas as contribuições relativas à esta dissertação, pelas valiosas ajudas durante minha graduação e pós-graduação e pela parceria que perdura desde o curso de Licenciatura em Matemática, do IFCE Campus Canindé.

À minha colega e amiga Maria Eliandra Sousa Maciel, contemporânea da Licenciatura em Matemática, do IFCE Campus Canindé e do Mestrado Profissional em Matemática em Rede Nacional, da UFC, pelas valiosas contribuições à esta dissertação, principalmente ao capítulo "Um Pouco de História".

Ao meu chefe e amigo Professor Me. Luiz Fernando de Oliveira dos Santos, por realizar a correção ortográfica desta dissertação, bem como por envidar todos os esforços relativos à conciliação de minhas atribuições profissionais e estudantis, viabilizando assim o meu progresso no PROFMAT.

Aos meus alunos da turma de Olimpíadas de Matemática do Nivel II, do Colégio Militar de Fortaleza, dos anos de 2017, 2018 e 2019, por todas as indagações que me fizeram e fazem buscar ainda mais o conhecimento, possibilitando assim uma melhor ação docente durante as aulas preparatórias para olimpíadas.

À gestão do Colégio Militar de Fortaleza, por ter me disponibilizado momentos de estudo semanal para dedicação ao PROFMAT.

"Tomai sobre vós o meu jugo, e aprendei de mim, que sou manso e humilde de coração; e encontrareis descanso para as vossas almas."

(Mateus 11:29)

RESUMO

A proposta desta dissertação é apresentar diferentes demonstrações para um dos mais importantes teoremas em Teoria dos Números, a saber, o Pequeno Teorema de Fermat. Nosso interesse neste pleito é mostrar as inter-relações existentes entre as mais diversas áreas da Matemática. Nosso trabalho, em certo sentido, não deixa de ser também uma pesquisa bibliográfica. Fazemos um breve levantamento sobre a história de Pierre de Fermat, elencando algumas de suas várias contribuições para a Matemática, em especial para a Teoria dos Números. Damos sequência, no terceiro capítulo, apresentando as demonstrações mais conhecidas para o Pequeno Teorema de Fermat. No quarto capítulo, começamos as demonstrações alternativas, apresentando, primeiramente, uma por Análise Combinatória, consequentemente utilizando ideias introdutórias de Teoria dos Grafos e concluindo com uma demonstração que utiliza como principal conteúdo a Série de Taylor. No capítulo seguinte, trazemos uma demonstração utilizando as ideias de Sistemas Dinâmicos e, em seguida, desenvolvemos uma demonstração via Teoria dos Grupos. Por fim, trazemos nossas considerações acerca do trabalho desenvolvido, ressaltando as contribuições de Pierre de Fermat para a Matemática, as inter-relações existentes entre as mais diversas áreas desta Ciência e a importância da utilização das demonstrações matemáticas para os alunos da Educação Básica.

Palavras-chave: Pequeno Teorema de Fermat. Demonstrações Clássicas. Demonstrações Alternativas. História da Matemática. Inter-relações da Matemática.

ABSTRACT

The purpose of this dissertation is to present different proofs for one of the most important theorems in Number Theory, namely Fermat's Little Theorem. Our interest in this issue is to show the interrelationships between the most diverse areas of Mathematics. Our work, in certain sense, is also a bibliographical research. We make a brief survey on the history of Pierre de Fermat, listing some of his various contributions to Mathematics, especially in Number Theory. In the third chapter, we present the most popular proofs for the Fermat's Little Theorem. In the fourth chapter, we begin the alternative proofs, first presenting one by Combinatorial Analysis, in the sequence using introductory ideas of Graph Theory and concluding with a proof that uses Taylor's series as main tool. In the next chapter, we bring a proof using the ideas of Dynamical Systems and then we develop a proof by Group Theory. Finally, we bring our considerations about the work developed, highlighting the contributions of Pierre de Fermat to Mathematics, the interrelationships existing between the most diverse areas of this Science and the importance of the use of the mathematical proofs for the students of Basic Education.

Keywords: Fermat's Little Theorem. Classical Proofs. Alternative Proofs. History of Mathematics. Inter-relations of Mathematics.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A motivação pessoal desta dissertação surgiu do interesse em relacionar a Matemática estudada durante as aulas do PROFMAT com a Matemática da Educação Básica, concernente aos conteúdos de aulas preparatórias para Olimpíadas de Matemática do Nível II, que abarcam alunos do 8^o e do 9^o ano do Ensino Fundamental (EF), mais especificamente no tocante ao assunto do Pequeno Teorema de Fermat, o qual vez por outra pode ser utilizado para simplificar e agilizar a resolução de um problema matemático durante a realização de uma prova olímpica.

Assim, considerando a Matemática uma área de conhecimento rica em inter-relações entre os conteúdos e que tais relações se apresentam das mais diversas formas - desde as mais simples ideias de contagem até os mais complexos e sofisticados ramos de estudo. A Matemática consegue estabelecer relações entre conhecimentos que, observados de forma simplória, inicialmente, parecem nem existir, e nos possibilita visualizar a demonstração do Pequeno Teorema de Fermat por meio dos mais diversos conteúdos matemáticos estudados durante a Educação Básica, como também no ensino Superior.

Desta forma, o presente trabalho tem como objetivo apresentar algumas demonstrações do Pequeno Teorema de Fermat, que é um dos mais importantes teoremas da Teoria dos Números, de modo a mostrar as inter-relações existentes entre as mais diversas áreas da Matemática.

Para tanto, lançaremos mão da utilização dos mais diversos métodos de demonstrações, bem como de conteúdos distintos, apresentando, assim, demonstrações alternativas às que são mais conhecidas. Reconhecemos que algumas dessas demonstrações contribuem muito para com as habilidades dos alunos em resolverem determinados problemas durante a participação em provas olímpicas do Nível II, pois utilizamos conteúdos concernentes a este nível.

Ressaltamos que os Parâmetros Curriculares Nacionais (PCN) apresentam as provas e demonstrações como uma das competências a ser trabalhada durante as aulas de Matemática do Ensino Fundamental (BRASIL, 1998).

Anteriormente a cada demonstração, quando julgado necessário, para uma melhor compreensão do leitor, traremos algumas informações e resultados preliminares acerca do assunto que será abordado.

Vale salientar que algumas demonstrações expressas neste trabalho não são pertinentes de se apresentar aos alunos da Educação Básica, tendo em vista que precisam de uma estrutura cognitiva mais amadurecida, bem como do conhecimento de conteúdos que não convêm

serem trabalhados neste nível de ensino.

O Pequeno Teorema de Fermat foi formulado pelo advogado francês Pierre de Fermat e consiste no seguinte:

$$\textit{Se } a, p \in \mathbb{Z}\textit{, com } p \textit{ primo e } MDC(a,p) = 1\textit{, então } a^{p-1} \equiv 1 \ (mod\ p).$$

Tal enunciado, atualizando a linguagem, foi declarado em uma carta a Frenicle de Bessy em 18 de outubro de 1640.

Uma prova baseada em Indução Finita, através do Teorema Binomial, foi dada por Leibniz (1646-1716), um contemporâneo de Fermat. No entanto, tal prova foi escrita em um manuscrito inédito e sem data, descoberto apenas em 1894, nos arquivos da Biblioteca de Hannover. Leibniz escreveu neste manuscrito que já sabia da prova antes de 1683.

Em 1729, Goldbach (1690-1764) perguntou a Leonhard Euler (1707-1783) se ele poderia verificar uma das muitas afirmações sem provas dadas por Fermat. Isso levou Euler a estudar os trabalhos de Fermat, especialmente, os relativos a Teoria dos Números. Em 1736, Euler publicou uma prova do Pequeno Teorema de Fermat, que era essencialmente a prova de Leibniz usando o Teorema Binomial. Sua segunda prova, publicada em 1747, foi uma variação do mesmo tema, baseada na Indução. No entanto, em 1758, Euler publicou uma terceira prova, que evitou o uso do Teorema Binomial e empregou essencialmente o ponto de vista da moderna Teoria dos Grupos. Com base em sua terceira prova, Euler publicou uma generalização do resultado de Fermat em 1760.

Embora Fermat não tenha deixado nenhuma evidência escrita de sua prova, uma tentativa de reconstrução desta, apresentada por André Weil (1906-1998), sugere que Fermat possa ter começado com uma prova semelhante a de Leibniz, mas depois concebida mesma ideia de Teoria dos Grupos formuladas por Euler (CHAN; NORRISH, 2012).

Assim, para conhecermos um pouco mais sobre os fatos que ocorreram durante a vida de Pierre de Fermat, no **Capítulo 2** trazemos uma breve história dessa personalidade, elencando seus principais estudos, bem como algumas de suas várias contribuições para a Matemática, em especial para a Teoria dos Números.

No **Capítulo 3**, apresentamos as demonstrações mais conhecidas para o Pequeno Teorema de Fermat, iniciando com a primeira demonstração publicada, escrita por Leonhard Euler e traduzida por Gonçalves e Haddad (2009), seguida do seu enunciado com características da época. Em seguida trazemos uma demonstração ancorada nos mesmos conhecimentos

utilizados por Euler, porém numa linguagem contemporânea. Por fim, seguimos apresentando uma demonstração mais direta utilizando apenas as ideias da Teoria dos Números.

Essas primeiras demonstrações, com exceção da prova dada por Euler, são as mais conhecidas, como também as mais fáceis de se encontrar nos livros textos de Aritmética. Pelo exposto, para não nos limitar às demonstrações de fácil acesso, nos capítulos seguintes apresentamos algumas demonstrações alternativas para o Pequeno Teorema de Fermat. Tais demonstrações expressam com clareza que os mais diversos ramos da Matemática possuem várias interseções.

A partir desta ideia, e munidos da teoria necessária, no **Capítulo 4**, trazemos uma demonstração utilizando os conceitos da **Análise Combinatória**, esta apresentada primeiramente por Julius Petersen (1839-1910), o qual fez uso das ideias de construções de colares a partir de contas de miçangas coloridas. Consequentemente apresentamos uma demonstração utilizando ideias introdutórias de **Teoria dos Grafos**. Concluímos o capítulo com uma demonstração que utiliza como principal conteúdo a **Série de Taylor**.

No **Capítulo 5**, trazemos uma demonstração utilizando as ideias de **Sistemas Dinâmicos** e em seguida desenvolvemos uma demonstração via **Teoria dos Grupos** que, de acordo com Yorgey (2017), explicar essa prova para um matemático profissional, provavelmente, levaria apenas uma única sentença. Porém, a teoria de base que dá suporte a esta demonstração requer uma atenção especial, pois é necessário utilizar resultados como o Lema de Bézout e, principalmente, o teorema de Lagrange. Este último é o que nos possibilita imbricar a Teoria dos Grupos com a Aritmética durante a demonstração.

Por fim, no **Capítulo 6**, trazemos nossas considerações acerca do trabalho desenvolvido, momento no qual ressaltamos as contribuições de Fermat para o desenvolvimento da Ciência Matemática, bem como a importância de seu Pequeno Teorema para a Teoria dos Números; pontuamos a necessidade de utilização das demonstrações matemáticas para os alunos, ancorado nas diversas técnicas empregadas no decorrer deste trabalho, visando dar maiores subsídios para a compreensão dos assuntos trabalhados em sala; e reforçamos as inter-relações existentes entre os variados ramos da Matemática e a possibilidade de utilização destas durante as aulas na Educação Básica.

2 UM POUCO DE HISTÓRIA

O que o mundo antigo conheceu foi, em grande parte, esquecido por conta do estado de inatividade intelectual vivenciado durante a alta Idade Média. Só depois do século XII a Europa Ocidental tornou-se novamente consciente da Matemática. O renascimento da erudição clássica foi estimulado pelas traduções latinas do grego e, em especial, do árabe.

A latinização das versões árabes do grande tratado de Euclides, os Elementos, apareceu pela primeira vez em 1120. Porém, esta não foi uma tradução fiel dos Elementos, tendo sofrido traduções sucessivas e imprecisas do grego - primeiro para o árabe, depois para o castelhano e finalmente para o Latim - feito por copistas não interessados no conteúdo da obra. No entanto, esta cópia foi muito utilizada e, mesmo com o seu acúmulo de erros, serviu de base para todas as edições conhecidas na Europa até 1505, quando o texto grego foi recuperado.

Com a tomada de Constantinopla (atual Istambul) pelos turcos em 1453, os estudiosos bizantinos, que haviam servido como os principais guardiões da Matemática, trouxeram as antigas obras-primas do aprendizado grego para o Ocidente.

É relatado que uma cópia do que resistiu da *Arithmetica* de Diofanto de Alexandria, um trabalho sobrevivente da Biblioteca de Alexandria, queimada em 646 d.C, foi encontrada na biblioteca do Vaticano, por volta de 1462, por Johannes Müller (mais conhecido como Regiomontanus). Presume-se que tenha sido levado a Roma pelos refugiados de Bizâncio. Regiomontanus observou que: "Nesses livros a própria flor da aritmética permanece oculta", e tentou interessar a outros ao traduzi-la (BURTON, 2002).

Não obstante a atenção que foi chamada à obra, ela permaneceu praticamente fechada até 1572, quando a primeira tradução e edição impressa foi trazida pelo professor alemão Wilhelm Holzmann, o qual escreveu sob a forma grega de seu nome, Xylander.

A Aritmética tornou-se totalmente acessível aos matemáticos europeus quando Claude Gaspar Bachet - tomando emprestado liberalmente de Xylander - publicou em 1621 o texto original grego da *Arithmetica* de Diofanto, junto com uma tradução em latim contendo notas e comentários.

A edição latina de Bachet provavelmente traz a distinção de ser o trabalho que causou grande encanto à Fermat e o inspirou a se dedicar e desenvolver a Teoria dos Números, área da Matemática em que ele obteve maior destaque.

Poucos períodos foram tão frutíferos para a Matemática quanto o século XVII. Só o norte da Europa produziu tantos homens de notável capacidade quanto surgiram no milênio

anterior. Numa época em que nomes como Desargues, Descartes, Pascal, Wallis, Bernoulli, Leibniz e Newton estavam se tornando famosos, um certo funcionário público francês, Pierre de Fermat (1601?-1665), era um igual entre esses estudiosos brilhantes.

De acordo com Eves (2011), há controvérsias em relação à data de nascimento de Pierre de Fermat, pois

> Segundo um registro aparentemente confiável, Fermat nasceu em Beaumont de Lomagne, perto de Toulouse, a 17 de agosto de 1601. Sabe-se que morreu em Castres ou Toulouse a 12 de janeiro de 1665. Em sua laje tumular, originalmente na igreja dos agostinianos em Toulouse e depois transferida para o museu local, consta a data precedente como a da morte de Fermat, com 57 anos de idade. Devido a esse conflito de datas costuma-se escrever (1601? -1665) para nascimento e morte de Fermat. De fato, por várias razões, seu ano de nascimento, a julgar pelas informações de vários escritores, varia de 1590 a 1608. (EVES, 2011, p. 389, 390)

O pai de Pierre de Fermat, Dominique Fermat, era um rico comerciante de pele de animais e ascendeu ao status de cônsul da cidade de Beaumont. A mãe, Claire de Long, pertencia a uma família aristocrata. O casal possuía uma boa situação financeira. Além de Fermat, tiveram mais três filhos.

O'Connor e Robertson (1996), afirmam que embora haja pouca evidência sobre a educação escolar de Fermat, esta deve ter sido no mosteiro franciscano local. Quando mais velho, frequentou a Universidade de Toulouse na França, antes de se mudar para Bordeaux. De Bordeaux foi para Orléans, onde estudou Direito na Universidade local. Acredita-se que a posição social da família tenha contribuído para a escolha de sua carreira profissional.

Fermat, o "Príncipe dos Amadores", foi o último grande matemático a desenvolver seus estudos como uma linha lateral para uma carreira não científica. Era um advogado e magistrado ligado ao parlamento provincial de Toulouse na França e, por isso, buscava refúgio da controvérsia na abstração da Matemática.

Em Bordeaux, Fermat iniciou suas investigações mais sérias em relação à Matemática. Nesse mesmo período, ele foi bastante influenciado pelo trabalho do matemático francês Viète, o qual já havia feito obras relacionadas à álgebra. Ele conheceu o trabalho de François Viète (1540-1603) por meio de uma biblioteca que d'Espagnet, um grande amigo seu, havia herdado.

Segundo Burton (2002), Fermat, evidentemente, não tinha nenhum treinamento matemático específico e não demonstrou interesse em seu estudo até os 30 anos. Para ele, o estudo da Matemática era apenas um hobby a ser cultivado no tempo de lazer e, mesmo não

sendo um “matemático profissional”, nenhum praticante de sua época fez maiores descobertas ou contribuiu de forma mais eficaz para o avanço desta disciplina.

Durante o trabalho de advogado na cidade de Toulouse, Fermat conheceu Carcavi que também era advogado. Além do coleguismo da profissão, a Matemática foi outro fator aproximador entre os dois, pois Carcavi também tinha grande interesse por esta área. Com essa proximidade, Fermat apresentou a Carcavi algumas de suas descobertas e investigações.

Um tempo depois, Carcavi viajou para Paris como bibliotecário real. Nesse período, Mersenne estava a encorajar outros matemáticos a se comunicarem mais abertamente. Ele unia um grupo de grandes cientistas para trocar e divulgar novas descobertas. Numa época em que não existiam grandes meios de comunicação e divulgação, Mersenne servia como um meio de distribuição de informação. Ele se correspondia com grandes cientistas contemporâneos como: Descartes, Pascal, Galileu e Torricelli.

Além das correspondências, Mersenne organizava encontros entre estes cientistas e viajava à Europa frequentemente, para encontros mais individuais. Foi então que Carcavi entrou em contato com Mersenne, informando-lhe todas as descobertas de Fermat. Mersenne ficou muito interessado pelos trabalhos que Fermat já havia desenvolvido. O curioso é que Mersenne se interessou inicialmente por um trabalho de Fermat, relativo às aplicações físicas da Matemática, relacionado a corpos em queda.

Neste período, Galileu já havia construído trabalhos acerca de corpos em queda. O primeiro contato de Fermat com Mersenne foi baseado nas observações que ele tinha em relação ao trabalho de Galileu, além de comentar um pouco sobre seus trabalhos em espirais e também sobre sua restauração da obra de Apollonius, *De Locis Planis*.

O trabalho de Fermat em espirais foi incitado pela observação do trajeto dos corpos em queda livre e construído através de métodos do trabalho Sobre Espirais de Arquimedes, porém Fermat utilizou métodos generalizados dos de Arquimedes. Hoje temos as Espirais de Fermat, que é a nomeação que utilizamos para as conhecidas espirais parabólicas.

Apesar do interesse de Mersenne no trabalho de Fermat ter sido exposto primeiramente em um trabalho ligado à Física, é notório que o maior interesse de Fermat não estava nessa área. O maior encanto de Fermat estava ligado à Matemática, principalmente no que diz respeito à criação de teoremas.

Neste primeiro contato com Mersenne, Fermat também demonstrou uma de suas principais características, a de desafiar seus colegas na busca de soluções de problemas propostos

por ele, enviando dois problemas referentes a máximos e mínimos.

Mersenne logo transmitiu a seu grupo as descobertas de Fermat. Roberval e Mersenne, ao se depararem com os dois problemas propostos por Fermat, acharam que as técnicas conhecidas por eles, até aquele momento, não eram suficientes para solucioná-los. Foi então que eles resolveram entrar em contato com Fermat, a fim de que ele expusesse seus métodos. Fermat enviou seus trabalhos sobre máximos e mínimos e tangentes a linhas curvas, a restauração da *De Locis Planis* e suas investigações de geometria referentes à álgebra, para auxiliá-los.

Mersenne e Fermat passaram a se corresponder regularmente e Mersenne logo se tornou grande amigo e colaborador de Fermat. Mersene era o principal incentivador para que Fermat publicasse suas descobertas e trabalhos, porém Fermat sempre se recusava a publicar.

O domínio de seis línguas (incluindo grego antigo e latim) foi o que lhe proporcionou a restauração da obra *De Locis Planis* devido a Apollonius, com o auxílio da Coleção de Pappus e da álgebra de Viète. Neste trabalho, Fermat identificou a forte relação que existia entre conceitos geométricos e termos algébricos e, além disso, acredita-se que este trabalho o inspirou a chegar ao princípio fundamental da Geometria Analítica (o termo real foi proposto apenas no início do século XIX).

O resultado da restauração de Fermat foi o tratado *Ad locus planos et sólidos isagoge* (Introdução aos lugares planos e sólidos), só publicado após sua morte. Fermat foi, assim, um dos inventores da Geometria Analítica, juntamente com René Descartes, seu contemporâneo.

Segundo Eves (2011, p. 389), enquanto *"Descartes partia de um lugar geométrico e então encontrava sua equação, Fermat partia da equação e então estudava o lugar correspondente. São esses os dois aspectos recíprocos do princípio fundamental da geometria analítica."*.

Durante esse tempo, Fermat também realizou relevantes descobertas sobre máximos e mínimos. Ele se interessou tanto pela geometria, que, além das descobertas acerca do cálculo de pontos máximos e mínimos, Fermat ingressou em um estudo acerca de tangentes a uma curva, desenvolvendo com isso, uma técnica para o cálculo dessas tangentes, estabelecendo, assim, as bases técnicas do Cálculo Diferencial.

De acordo com Singh (2001), por séculos acreditou-se que Isaac Newton havia inventado o Cálculo de forma independente e sem ter conhecido o trabalho de Fermat. Porém, em 1934, Louis Trenchard Moore encontrou uma nota que deu a Fermat o crédito que ele merece. Nesta nota, Newton escreveu que seu Cálculo havia sido desenvolvido com base no "método de

monsieur Fermat para estabelecer tangentes".

EVES (2011) afirma que Fermat desenvolveu um trabalho pioneiro não só no que se refere à diferenciação, mas também no que se refere à integração, pois, no transcorrer de seu trabalho, chegou a resultados equivalentes à integração de expressões como $x^n, sen(\theta), sen^2(\theta)$ e $\theta sen(\theta)$.

Outra área da Matemática na qual Fermat esteve profundamente envolvido é a Teoria da Probabilidade. Ele e Pascal lançaram os alicerces para este assunto. A Teoria da Probabilidade, na época, um novo ramo da Matemática, resultou da troca de cartas entre Fermat e Pascal por volta de 1654. Aliás, Pascal foi outro incentivador para que Fermat publicasse seu trabalho, mas Fermat continuava a afirmar que não era necessário.

Segundo EVES (2011), o problema que incitou os estudos de Fermat e Pascal nesta área foi o "Problema dos Pontos", que pede que se determine como deve ser divididas as apostas entre dois jogadores igualmente hábeis, os quais interromperam um jogo de azar, sabendo-se a contagem de pontos no momento em que interromperam e a quantidade de pontos necessários para cada um ganhar o jogo.

O problema já havia intrigado vários matemáticos anteriormente como: Pacioli, Cardano e Tartaglia. O problema foi encaminhado por Antoine Gombaud a Pascal, que o repassou para Fermat. Os dois solucionaram o problema corretamente, porém de formas distintas.

Pascal utilizou para a construção da solução o seu "triângulo aritmético", hoje conhecido como triângulo de Pascal. Ele utilizou-se das ideias de combinações simples, característica própria de seu triângulo. Fermat, por sua vez, em uma carta a Pascal, apresentou seu método utilizando considerações sobre Análise Combinatória, chegando a utilizar as ideias de arranjos. Para conhecimento das soluções, tanto a de Pascal como a de Fermat, ambas relativas ao problema acima, recomendamos a leitura de (EVES, 2011).

Fermat e Pascal não publicaram suas ideias acerca da Teoria da Probabilidade, ficando todas registradas nas correspondências trocadas. Somente em 1657 apareceu um estudo mais profundo da teoria das probabilidades, quando o matemático holandês Christiaan Huygens (1629-1695), incitado pelo problema e embasado nas correspondências entre Fermat e Pascal, publicou a obra "Sobre o Raciocínio em Jogos de Azar".

Apesar de todas essas contribuições, o verdadeiro amor de Fermat pela Matemática, residia, sem dúvida, na Teoria dos Números, da qual resgatou do reino da superstição e do ocultismo onde há muito tempo estava aprisionada. Suas contribuições aqui sobressaem a todas

as outras. Podemos, inclusive, dizer que o renascimento do interesse pelo lado abstrato da Teoria dos Números começou com Fermat.

Em um fragmento de uma carta escrita em 1643, cujo destinatário é supostamente Mersenne, Fermat descreveu uma técnica sua para fatorar grandes números. Essa técnica representou a primeira melhoria real em relação ao método clássico de tentar encontrar um fator de n dividindo por todos os primos não excedendo $\frac{y}{n}$.

O esquema de fatoração de Fermat tem em sua essência a observação de que a busca por fatores de um inteiro ímpar n (porque potências de 2 são facilmente reconhecíveis e removidas no início da fatoração) é equivalente a obter soluções x e y; da equação $n = x^2 - y^2$ (ORE, 1948). Dessa forma, Fermat escreveu que

(i) *todo primo ímpar pode ser expresso como a diferença de dois quadrados de uma só maneira;*

Fermat é responsável por um considerável impulso da aritmética e, dentro deste campo, volta seu interesse principalmente para os números primos e propriedades de divisibilidade. Diante do seu fascínio com os números primos, além do teorema já citado, também fez investigações como:

(ii) *um primo da forma* $4n+1$ *pode ser representado como a soma de dois quadrados;*

(iii) *um número primo de forma* $4n+1$ *é apenas uma vez a hipotenusa de um triângulo retângulo de lados inteiros, seu quadrado é duas vezes, seu cubo é três vezes, e assim por diante.*

Fermat também conjecturou, em uma carta a Frenicle de Bessy, que: *para todo inteiro positivo, o número* $f_n = 2^{2^n} + 1$ *é primo*. Porém, Euler, aproximadamente 100 anos depois, ao se deparar com essa indagação, mostrou que f_5 (a saber: 4.294.967.297) não é primo, pois

$$f_5 = 2^{32} + 1 = 641 \cdot 6700417,$$

verificando que a conjectura proposta por Fermat era incorreta. Tal resultado, atualmente, é conhecido como número de Fermat (DICKSON, 1952).

Acredita-se que Fermat teria capacidade suficiente de perceber este erro, levando a considerar que ele tenha cometido falhas ao fazer os testes. Tal fato fica explicado quando observamos o fragmento da carta enviada à Frenicle de Bessy em outubro de 1640, pois nesta, ele confessa não ter provado tal resultado e que verificou a primalidade dos números por meio de

fatorações. Fermat escreveu:

> Mas aqui está o que mais admiro: é que estou quase convencido de que todos os números progressivos aumentados pela unidade, dos quais os expoentes são números da progressão dupla, são números primos, [...] Não tenho a prova exata disso, mas excluí tantos divisores por demonstrações infalíveis, e tenho luzes tão grandes, que estabelecem meu pensamento, que teria dificuldade em negar o que disse. (FERMAT,1640, n.p. *apud* TANNERY; HENRY, 1894, p.206, **tradução nossa**)

Além das propriedades dos números primos e da divisibilidade, Fermat elencou vários outros resultados relativos aos números inteiros, estudados por grandes Matemáticos. Dentre esses resultados, escreveu teoremas relativos às potências de números inteiros.

Fermat inferiu que (iv) *"todo inteiro não negativo pode ser representado como soma de no máximo quatro quadrados"*. Tal teorema foi demonstrado por Lagrange em 1770. Além disso, Fermat também escreveu que (v) *"a área de um triângulo nunca pode ser um quadrado perfeito inteiro quando esse triângulo possui lados inteiros"*. Lagrange também determinou este resultado posteriormente.

Fermat ainda escreveu os seguintes teoremas:

(vi) *Há uma única solução inteira de* $x^2+2=y^3$ *e apenas duas de* $x^2+4=y^3$.

(vii) *Não existem inteiros positivos* x,y,z *tais que* $x^4+y^4=z^2$.

(viii) *Não existem inteiros positivos* x,y,z,n*, onde* $n>2$*, de modo que* $x^n+y^n=z^n$.

O teorema (viii) é conhecido como o Último Teorema de Fermat. Tal teorema foi um dos achados responsável pela fama de Fermat, consagrando-o na Teoria dos Números e na Matemática. Junto ao Último Teorema, Fermat afirmou que tinha uma demonstração verdadeiramente adimirável, porém, como de costume, Fermat não a apresentou.

Dentre os vários matemáticos que buscaram solucionar o teorema podemos destacar: Euler (1707-1783), Legendre (1752-1833), Sophie Germain (1776-1831), Gabriel Lamé (1795-1870), Dirichlet (1805-1859) e Kummer (1810-1893).

A repercussão do teorema foi tão grande que Paul Wolfskehl (1856-1906), um médico e matemático alemão, em seu testamento estabeleceu que a quantia de 100.000 marcos (equivalente hoje a aproximadamente 225.700,00 reais) fosse paga à pessoa que primeiro demonstrasse corretamente o Último Teorema de Fermat e decidiu que a Royal Society of Science in Göttingen mantivesse em confiança o dinheiro e servisse como juiz para a atribuição do prêmio (BARNER, 1997).

Como consequencia desse prêmio, diversos matemáticos e amadores se empenharam na busca por uma demonstração. O resultado foi que o Último Teorema de Fermat ganhou o título de problema matemático com maior número de demonstrações incorretas publicadas. Somente em 1995 foi apresentada uma demonstração correta para o resultado, devida a Andrew Wiles (1953-).

Após a demonstração de Wiles, muitos pesquisadores afirmaram que seria impossível Fermat saber de fato como demonstrar o seu teorema, haja vista, para a demonstração que conhecemos hoje, serem utilizadas técnicas matemáticas muito avançadas, algumas descobertas depois da época de Fermat.

Burton (2002) afirma que mesmo se Fermat possuísse uma prova geral para tal teorema, esta deveria possuir uma falha. De fato, o próprio Fermat pode ter descoberto este erro posteriormente, pois não há referência à prova em suas correspondências com outros matemáticos.

Fermat, no entanto, deixou uma demonstração, de modo elementar, de seu último teorema para os casos $n = 3$ e $n = 4$. Para resolver estes problemas e muitos outros em aritmética, Fermat estabeleu um método próprio, intitulado Método da Descida Infinita (conhecido atualmente como Descida Infinita de Fermat ou mesmo Princípio da Descida Infinita - PDI), que traduz uma forma de indução (CARNEIRO, 1996).

Em resumo, o método pode ser descrito da seguinte forma: assume-se que é possível apresentar uma solução do problema em questão nos inteiros positivos. Dessa solução, se constrói uma nova solução em inteiros positivos menores, o que leva a uma solução ainda menor, e assim por diante. Como os inteiros positivos não podem ser diminuídos indefinidamente, segue-se que a suposição inicial deve ser falsa e, portanto, nenhuma solução é possível. A solução do Último Teorema de Fermat para o caso $n = 3$ pode ser encontrado em (USPENSKI; HEASLET, 1939) e para o caso $n = 4$ em (BURTON, 2002).

Carneiro (1996) afirma que na maioria das apresentações do conjunto dos números inteiros, hoje em dia, o PDI aparece "traduzido" como o Princípio da Boa Ordenação (PBO): *Todo conjunto não vazio de números naturais possui um menor elemento.* Boyer (1974) atribui à Fermat a criação do PBO.

Percebemos, assim, que existe uma forte equivalência entre o PDI e o PBO. Lima (1976), por sua vez, demonstra que o Princípio da Boa Ordenação e o Princípio de Indução Finita (PIF) são equivalentes, restando-nos inferir que o PDI, PBO e o PIF são equivalentes entre si.

Mesmo com todas essas descobertas, Fermat preferia o prazer que derivava da própria pesquisa Matemática a qualquer reputação que esta pudesse lhe trazer. De fato, ele publicou apenas um manuscrito principal durante sua vida e apenas cinco anos antes de sua morte, usando as iniciais M.P.E.A.S. Recusando-se categoricamente a colocar seu trabalho em forma final, frustando vários esforços de outros para disponibilizar os resultados impressos em seu nome.

Em compensação pela falta de interesse em publicação, Fermat continuou mantendo volumosas correspondências com matemáticos contemporâneos. A maior parte do pouco que sabemos sobre suas investigações é encontrada nas cartas a amigos com quem ele trocou problemas e a quem relatou seus sucessos. Seus amigos fizeram o melhor que puderam para divulgar os talentos de Fermat, passando essas cartas de mão em mão ou fazendo cópias, que foram distribuídas pelo continente.

Dentre esses enunciados, porém, não menos importante, encontra-se o conhecido "Pequeno Teorema de Fermat", apresentado pela primeira vez numa carta a Frenicle de Bessy em 18 de outubro de 1640 da seguinte forma:

> Todo número primo mede infalivelmente uma das potências -1 de alguma progressão, e o expoente da dita potência é submúltiplo do dado primo -1; e depois de encontrar a primeira potência que satisfaz o problema, todas aquelas cujos expoentes são múltiplos do expoente da primeira, ainda satisfazem o problema. [...] E essa proposição é geralmente verdadeira para todas as progressões e para todos os números primos; Eu lhe enviaria a demonstração, se não tivesse medo de ser muito longa. (FERMAT,1640, n.p. *apud* TANNERY; HENRY, 1894, p.209, **tradução nossa**)

A partir dessa afirmação foi formulado o famoso Pequeno Teorema de Fermat como conhecemos atualmente. Tal teorema versa o seguinte:

Dados $a \in \mathbb{Z}$ e p primo. Se p não divide a, então p divide $a^{p-1} - 1$.

Note que Fermat escreveu algo além do que consta no teorema da forma como o conhecemos, pois ele indicou a ideia do que chamamos atualmente de Ordem de um número módulo p, deixando claro que reconhecia a possibilidade de existirem números menores do que $p-1$ que satisfazem a questão. Em outras palavras, Fermat reconhecia que dados $a, b, p \in \mathbb{Z}$ com p primo e $b < p$, temos que se $p \mid a^b - 1$, então $b \mid p-1$.

Segundo Burn (2002), o Pequeno Teorema de Fermat foi desenvolvido a partir de estudos relativos aos números perfeitos de Euclides. Fermat escreveu à Mersenne, em junho de 1640, sobre esses números e evidenciou que sabia dos resultados clássicos. Um número perfeito tem como característica a soma de seus divisores impróprios ser igual à ele mesmo.

As investigações de números perfeitos de Fermat começou a partir de um teorema de Euclides, se $1+2+4+8+\ldots+2^n$ é um número primo p, então $2^n p$ é um número perfeito (isto é, igual à soma dos seus divisores impróprios, 6 = 1 + 2 + 3 e 28 = 1 + 2 + 4 + 7 + 14 são ambos números perfeitos).

Para construir sobre eles, Fermat investigou os fatores primos dos números, que eram um a menos do que uma potência de 2. O pequeno teorema de Fermat é uma generalização, para potências de outros números, de resultados obtidos por potências de 2. Assim, Fermat afirmou que, para um número primo p, 2^p-2 tem um fator $2p$. O fator 2 é óbvio, já o fator p não é.

A alegação de que 2^p-2 tem um fator p é um caso especial do Pequeno Teorema de Fermat. Assim, o que percebemos é uma coleção de ideias, que estavam disponíveis para Fermat e teriam sido suficientes para provar que 2^p-2 tem um fator p para qualquer número primo p. O método pressupõe familiaridade com o triângulo de Pascal. Porém, este só foi dado por Pascal em 1654. Mesmo assim já era conhecido até certo ponto por várias centenas de anos antes disso.

Além das cartas enviadas, Fermat costumava inserir notas matemáticas nas margens de qualquer livro que estivesse usando. Ele escreveu muitos de seus famosos teoremas em Teoria dos Números, inclusive o já citado Último Teorema de Fermat, sobre as margens de sua cópia pessoal da tradução latina da *Arithmetica* de Diofanto. Estes foram descobertos por seu filho Clément-Samuel cinco anos após a morte de Fermat.

Seu filho, após tal descoberta, trouxe uma nova edição da *Arithmetica* incorporando as célebres notas de Fermat inseridas nas margens. Como havia pouco espaço disponível, o hábito de Fermat era anotar alguns resultados e omitir todos os passos que levaram à conclusão. A comunidade matemática desejou muitas vezes que as margens da *Arithmetica* fossem mais amplas ou que Fermat tivesse sido um pouco menos reservado sobre seus métodos.

Para Eves (2011, p. 390), *"Fermat enriqueceu tantos ramos da matemática com tantas contribuições importantes que é considerado o maior matemático francês do século XVII"*. Dentre as célebres descobertas encontra-se nosso objeto de estudo, o "Pequeno Teorema de Fermat", do qual abordaremos mais nos próximos capítulos, apresentando algumas demonstrações utilizando-se dos mais variados conteúdos matemáticos.

3 DEMONSTRAÇÕES USUAIS DO PEQUENO TEOREMA DE FERMAT

Neste capítulo, nossa intenção é apresentar as demonstrações mais usadas atualmente para o Pequeno Teorema de Fermat. Porém, antes dessas, trazemos a primeira demonstração que foi publicada por Leonhard Euler em 1736 e traduzida por Gonçalves e Haddad (2009), mantendo as características de linguagem e de argumentação da época.

3.1 Prova dada por Euler

Antes de passar à demonstração propriamente dita, vale salientar que no texto existem algumas palavras que se referem a outros termos, dos quais utilizamos hoje. Assim, fazemos uma compilação de algumas palavras utilizadas por Euler, seguidas de seu significado atual:

$$mede \longrightarrow divide$$
$$duplo\ menor \longrightarrow metade$$
$$etc \longrightarrow \ldots$$
$$congruente \longrightarrow igual$$

Euler também faz uso de forma liberal do sinal de igualdade junto das argumentações, assim devemos compreender como sendo a expressão "igual a". É citado em alguns momentos a palavra série, esta, por sua vez, normalmente possui um número finito de termos.

A partir deste ponto, apresentamos, de forma fiel, a demonstração de Euler para o Pequeno Teorema de Fermat. Passemos aos argumentos realizados por Euler.[1]

A proposição, então, que aqui tomei para ser demonstrada, é a seguinte:

Significando $\boldsymbol{p}$ *um número primo, a fórmula* $a^{p-1} - 1$ *sempre poderá ser dividida por* $\boldsymbol{p}$*, a menos que* $\boldsymbol{a}$ *possa ser dividido por* $\boldsymbol{p}$*.*[2]

Convém, em primeiro lugar, conduzir a verificação do caso $a = 2$, pelo qual mais facilmente o trânsito para (coisas) mais gerais do que ele pode ser produzido. A ser demonstrada, então, será a proposição seguinte:

---

[1] Pelo fato do restante desta seção ser, literalmente, a primeira prova para o Pequeno Teorema de Fermat, a demonstração deve, eventualmente, aparentar falta de estilo do autor, porém, isso é devido à própria linguagem e recursos da época.

[2] Teorema 3.1.1.

Significando $\boldsymbol{p}$ *um número primo ímpar qualquer, a fórmula* $2^{p-1}-1$ *sempre poderá ser dividida por* $\boldsymbol{p}$.[3]

DEMONSTRAÇÃO[4]

No lugar de 2, seja posto 1+1, e será

$$(1+1)^{p-1} = 1+\frac{p-1}{1}+\frac{(p-1)(p-2)}{1\cdot 2}+\frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3}$$

$$+ \frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4}+etc.,$$

de cuja série o número de termos é = p e, portanto, ímpar. Além disso, qualquer termo, ainda que tenha aspecto de fração, dará um número inteiro; de fato, cada numerador, como é suficientemente claro, pode ser dividido por seu denominador. Então a série com o primeiro termo removido será

$$(1+1)^{p-1}-1 = 2^{p-1}-1 = \frac{p-1}{1}+\frac{(p-1)(p-2)}{1\cdot 2}+\frac{(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3}$$

$$+ \frac{(p-1)(p-2)(p-3)(p-4)}{1\cdot 2\cdot 3\cdot 4}+etc.,$$

o número dos quais é = $p-1$ e, por isso, par. Então agrupam-se cada dois termos em uma soma, com o que o número de termos faça-se o duplo menor; será

$$2^{p-1}-1 = \frac{p(p-1)}{1\cdot 2}+\frac{p(p-1)(p-2)(p-3)}{1\cdot 2\cdot 3\cdot 4}+\frac{p(p-1)(p-2)(p-3)(p-4)(p-5)}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6}+etc.,$$

de cuja série o último termo, por causa do número ímpar p, será

$$\frac{p(p-1)(p-2)\cdot\ldots\cdot 2}{1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)} = p$$

Mas é evidente que os termos individuais são divisíveis por p; pois, como p é número primo e maior do que qualquer fator dos denominadores, em nenhuma parte poderá ser eliminado pela divisão. Por essa razão, se p for um número primo ímpar, $2^{p-1}-1$ sempre poderá ser dividida por ele. C.Q.D.

DE OUTRO MODO[5]

[3] Proposição 3.1.1.
[4] Prova da Proposição 3.1.1.
[5] Euler apresentou, de uma outra forma, a prova da Proposição 3.1.1.

Se $2^{p-1}-1$ pode ser dividida por um número primo p, também seu dobro 2^p-2 poderá ser dividido e reciprocamente. De sua parte, é

$$2^p=(1+1)^p=1+\frac{p}{1}+\frac{p(p-1)}{1\cdot 2}+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}+\ldots+\frac{p}{1}+1$$

cuja série, truncada do primeiro e último termos, dá

$$\frac{p}{1}+\frac{p(p-1)}{1\cdot 2}+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}+\ldots+p=2^p-2.$$

É claro, também, que qualquer termo dessa série é divisível por p, uma vez que p é número primo. Por essa razão, também 2^p-2 sempre poderá ser dividida por p e, por causa disso, também $2^{p-1}-1$ por p, a menos que seja $p=2$. *C.Q.D.*

Como, então, $2^{p-1}-1$ pode ser dividida pelo número primo ímpar p, é fácil entender que também esta fórmula $2^{m(p-1)}-1$ pode ser dividida por p, denotando m um número inteiro qualquer. Por isso, também as fórmulas seguintes todas $4^{p-1}-1$, $8^{p-1}-1$, $16^{p-1}-1$ etc. poderão ser divididas pelo número primo p. Está, então, demonstrada a verdade do teorema geral para todos os casos, nos quais a é qualquer potência de dois e p qualquer número primo além de dois.

Tendo demonstrado agora aquele teorema[6], com a ajuda dele demonstraremos também o seguinte.

TEOREMA[7]

Denotando p um número primo qualquer além do 3, esta fórmula $3^{p-1}-1$ *sempre poderá ser dividida por ele.*

DEMONSTRAÇÃO[8]

Se $3^{p-1}-1$ pode ser dividida por um número primo p exceto 3, então 3^p-3 pode ser dividida por p, desde que p seja um número primo qualquer, e reciprocamente. É verdade que

$$3^p=(1+2)^p=1+\frac{p}{1}\cdot 2+\frac{p(p-1)}{1\cdot 2}\cdot 4+\frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}\cdot 8+\ldots+\frac{p}{1}\cdot 2^{p-1}+2^p$$

de cuja série os termos individuais exceto o primeiro e o último poderão ser divididos por p, uma vez que p é número primo. Então pode ser dividida por p esta fórmula 3^p-2^p-1, que é igual a esta

$$3^p-3-2^p+2.$$

[6] Euler se referiu à Proposição 3.1.1.
[7] Proposição 3.1.2.
[8] Prova da Proposição 3.1.2.

Mas $2^p - 2$ sempre pode ser dividida pelo número primo p; então também $3^p - 3$. Por isso, $3^{p-1} - 1$ sempre pode ser dividida pelo p, desde que p seja um número primo exceto 3. $C.Q.D.$

Do mesmo modo, será possível progredir a partir deste valor do próprio a para o seguinte, maior por uma unidade. Mas porque quero produzir uma demonstração mais elegante e mais genuína do teorema geral, exponho o seguinte

TEOREMA[9]

Denotando p um número primo, se $a^p - a$ pode ser dividida por p, então também a fórmula $(a+1)^p - a - 1$ poderá ser dividida pelo mesmo $\boldsymbol{p}$.

DEMONSTRAÇÃO[10]

Seja resolvida $(1+a)^p$ conforme o costume em série; será

$$(1+a)^p = 1 + \frac{p}{1}\cdot a + \frac{p(p-1)}{1\cdot 2}\cdot a^2 + \frac{p(p-1)(p-2)}{1\cdot 2\cdot 3}\cdot a^3 + \ldots + \frac{p}{1}\cdot a^{p-1} + a^p,$$

de cuja série os termos individuais, exceto o primeiro e o último, podem ser divididos por p, uma vez que p é um número primo. Por essa razão, $(1+a)^p - a^p - 1$ admite a divisão por p; mas esta fórmula é congruente com esta $(1+a)^p - a - 1 - a^p + a$. Mas $a^p - a$ por hipótese pode ser dividida por p, logo também $(1+a)^p - a - 1$. $C.Q.D.$

Como, então, dado que $a^p - a$ pode ser dividida pelo número primo p, também esta fórmula $(a+1)^p - a - 1$ admite a divisão por p, segue-se também que $(a+2)^p - a - 2$, e mesmo $(a+3)^p - a - 3$ e genericamente $(a+b)^p - a - b$ podem ser divididas por p. Dado ainda $a = 2$, como já demonstramos que $2^p - 2$ pode ser dividida por p, é claro que a fórmula $(b+2)^p - b - 2$ deve admitir a divisão por p, qualquer que seja o número inteiro substituído no lugar de b.

Então p mede a fórmula $a^p - a$ e, consequentemente, também esta $a^{p-1} - 1$, a menos que seja $a = p$ ou múltiplo do próprio p. E essa é a demonstração do teorema geral[11], que tomei para apresentar.

3.2 Por Indução Finita utilizando Binomial

A demonstração que apresentaremos a seguir é essencialmente a mesma que foi dada por Euler, porém utilizando linguagem contemporânea. Esta é a mais tradicional e configura como uma das mais apresentadas nos livros textos de Aritmética.

[9] Teorema 3.1.2.
[10] Prova do Teorema 3.1.2.
[11] Euler refere-se ao Teorema 3.1.1.

Vale salientar que esta demonstração é pertinente de se apresentar a alunos que estudem para olimpíadas de Matemática do Nível II, visto que é necessário uma quantidade relativamente pequena de conteúdos para proceder com a demonstração.

Assim, inicialmente, visando uma melhor compreensão desta demonstração, é que apresentamos as seguintes definições.

Definição 3.2.1 (Princípio de Indução Finita) *Seja P(n) uma propriedade descrita em termos de números naturais n maior que ou igual a um número natural (n_0) fixado. Se P(n) satisfaz as duas condições abaixo*
i) $P(n_0)$ é válida
ii) A validade de P(n) implicar na validade de P(n+1),
Então, a propriedade P(n) é válida para todo $n \geq n_0$.
Quando $n_0 = 1$ então P(n) é válida para todo $n \in \mathbb{N}$.

Para a próxima definição, precisamos compreender o seguinte teorema.

Teorema 3.2.1 (Algorítmo da Divisão de Euclides) *Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$, chamados respectivamente de quociente e resto, tais que*

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

Separaremos a demonstração, do Algorítmo da Divisão de Euclides, em dois casos.
Demonstração: Caso 1: Para $b > 0$, considere o conjunto $S = \{a - bt;\ t \in \mathbb{Z},\ a - bt \geq 0\}$. Note que S é não vazio pois $a - (-|a|b) = a + |a|b \geq a + |a| \geq 0$. Claramente S possui um menor elemento $r = a - bq$. Para mostrar que $r < |b| = b$, note que $r = b \Rightarrow a = (1+q)b \Rightarrow r = 0 \Rightarrow b = 0$, que é um absurdo. $r > b \Rightarrow \exists k; r = b + k$, onde $0 < k < r$. Assim $b + k = a - bq \Rightarrow k = a - (q+1)b \in S$, o que é um absurdo, pois r é o menor elemento de S. Logo $0 \leq r < |b|$.
Mostraremos agora que q e r são unicamente determinados. Suponha que $a = bq + r = bq' + r'$, com $0 \leq r, r' \leq |b| = b$. Neste caso $0 \leq |r - r'| < b$. Por outro lado, $bq' + r' = bq + r \Rightarrow b(q' - q) = r - r' \Rightarrow b|q - q'| = |r - r'|$. Se fosse $r \neq r'$, teríamos $|q - q'| \geq 1$. Daí $b \leq b|q - q'| = |r - r'| < b$, o que é um absurdo. Portanto $r = r'$ e, consequentemente, $q = q'$.
Caso 2: Para $b < 0$, aplicamos o caso anterior com $a, |b|$. Assim existem únicos $q, r \in \mathbb{Z}$ tais que $a = |b|q + r$, com $0 < r \leq |b|$. Se pomos $q_1 = -q$, então $a = bq_1 + r$, com $0 < r \leq |b|$. Claramente, q_1 é unicamente determinado. □

Definição 3.2.2 (Relação de Congruência) *Sejam a, b e m inteiros, com m > 0, dizemos que a é congruente a b módulo m se* $m \mid (a-b)$ *e denotamos por* $a \equiv b \pmod{m}$. *Se* $m \nmid (a-b)$, *dizemos que a é incongruente a b módulo m e denotamos por* $a \not\equiv b \pmod{m}$.

Note que $a \equiv b \pmod{m}$ é equivalente a dizer que b é o resto da divisão de a por m.

Definição 3.2.3 (Fatorial) *Seja* $n \in \mathbb{N} \cup \{0\}$ *definimos o fatorial de n como*

$$n! = \begin{cases} 1, & \text{se } n = 0 \\ n \cdot (n-1)!, & \text{se } n \neq 0 \end{cases},$$

n! lê-se: n fatorial.

Definição 3.2.4 (Binomial) *Para todo* $n \in \mathbb{N}$ *e todo* $k \in \mathbb{N} \cup \{0\}$ *com* $0 \leq k \leq n$ *temos*

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Número este que chamamos de coeficiente binomial de classe k do número n, ou, simplesmente, coeficiente binomial n sobre k.

Até aqui temos todos os tópicos necessários para provar o Pequeno Teorema de Fermat em sua segunda formulação, porém, para apresentar o Teorema em sua forma mais tradicional, ainda precisamos do lema que segue.

Lema 3.2.1 (Lei do Corte) *Se* $ax \equiv ay \pmod{n}$ *e MDC(a,n)=1, então* $x \equiv y \pmod{n}$.

Demonstração: Pela hipótese, temos que $\exists q \in \mathbb{Z}$, tal que $ax = nq + ay$, daí

$$\begin{aligned} nq &= ax - ay \\ &= a(x-y) \end{aligned}$$

Assim, temos que $n \mid a(x-y)$, mas como o $MDC(a,n) = 1$, segue $n \mid (x-y)$, garantindo que

$$x \equiv y \pmod{n}.$$

□

Pelo exposto estamos prontos para provar o seguinte teorema.

Teorema 3.2.2 (Pequeno Teorema de Fermat: 2ª Formulação) *Dados p primo e $a \in \mathbb{Z}$, temos que $a^p \equiv a \ (mod\ p)$.*

Demonstração: Do desenvolvimento binomial, temos que,

$$\begin{aligned}(a+1)^p &= \sum_{k=0}^{p} \binom{p}{k} a^{p-k} 1^k \\ &= \sum_{k=0}^{p} \frac{p!}{k!(p-k)!} a^{p-k} \\ &= a^p + pa^{p-1} + p\frac{p-1}{2}a^{p-2} + \ldots + pa + 1.\end{aligned}$$

Logo,

$$(a+1)^p \equiv a^p + 1 \ (\text{mod } p) \tag{3.1}$$

pois, $pa^{p-1} + p\frac{p-1}{2}a^{p-2} + \ldots + pa \equiv 0 \ (\text{mod } p)$, ou note que $\binom{p}{k} \equiv 0 \ (\text{mod } p)$, para $0 < k < p$. Assim, subtraindo $a+1$ em ambos os membros da congruência (3.1), obtemos

$$\begin{aligned}(a+1)^p - (a+1) &\equiv a^p + 1 - (a+1) \ (\text{mod } p) \\ &\equiv a^p - a \ (\text{mod } p) \end{aligned} \tag{3.2}$$

Agora usaremos o Princípio de Indução Finita para concluir o resultado.

Primeiro verificamos em (3.2) se, para $a = 1$, $a^p - a$ é divisível por p, o que é verdadeiro, pois $1^p - 1 = 0$.

Suponhamos que $a^p - a$ é divisível por p. Assim, pela congruência (3.2), $(a+1)^p - (a+1)$ também será divisível por p e, portanto, pelo Princípio de Indução Finita, temos que

$$a^p \equiv a \ (\text{mod } p).$$

O que prova o resultado na sua segunda versão.

Agora, se a não for múltiplo de p, ou seja, $MDC(a, p) = 1$, podemos escrever a congruência da seguinte forma,

$$a \cdot a^{p-1} \equiv a \cdot 1 \ (\text{mod } p).$$

E pelo Lema (3.2.1) temos o resultado na sua forma clássica, ou seja,

$$a^{p-1} \equiv 1 \ (\text{mod } p).$$

□

3.3 Por Congruência Linear

Seguindo na linha das demonstrações pertinentes a serem apresentadas aos alunos da Educação Básica, trazemos a demonstração que utiliza essencialmente os conteúdos da Teoria dos Números. Esta demonstração pode ser facilmente apresentada aos alunos do 8º e do 9º ano do EF, pois, para a sua compreensão, o aluno só precisa de alguns conceitos de divisibilidade e restos de divisões escritos na forma de congruências, que já foi definida na seção anterior. Vale salientar que, antes de apresentar tal demonstração aos alunos, é necessário um trabalho introdutório das propriedades de divisibilidade pertinentes à Aritmética. Abordaremos, agora, a definição que julgamos importante para a compreensão da demonstração.

Definição 3.3.1 (Sistema Reduzido de Resíduos) *Seja p um número primo. Dizemos que um conjunto de $p-1$ números inteiros $a_1, a_2, \ldots, a_{p-1}$ é um Sistema Reduzido de Resíduos (srr) módulo p se os a_i representam todos as classes de congruências não nulas módulo p.*

Por exemplo, $1, 2, \ldots, p-1$ formam um srr módulo p, pois são todos os restos não nulos possíveis de se obter quando dividimos um número inteiro por p.

Precisamos ainda do seguinte lema para conseguir proceder com a demonstração.

Lema 3.3.1 *Dados p primo e a inteiro de tal modo que MDC(p,a)=1 e dado o conjunto $\boldsymbol{A} := \{an;\ \forall\ n \in \mathbb{N}$ com $n < p\}$. O conjunto dos restos das divisões dos elementos de $\boldsymbol{A}$ por p forma um srr módulo p.*

Demonstração: Como n é diferente de zero e estritamente menor do que p, então temos exatamente $p-1$ valores possíveis. Agora suponha que haja dois múltiplos de a, digamos, ia e ja que tenham o mesmo resto quando divididos por p. Nós podemos escrever isso como

$$ia \equiv\ ja \pmod{p}.$$

Subtraindo ja de ambos os lados e fatorando a, descobrimos que

$$a(i-j) \equiv 0 \pmod{p}$$

isto é, $a(i-j)$ é divisível por p. Como p divide o produto de dois números, ele deve dividir um dos números (ou ambos). Mas como a não é divisível por p, daí p deve dividir $i-j$. Mas i e j são ambos menores que p, portanto, a diferença deles deve estar estritamente entre $-p$ e p. O único múltiplo de p estritamente entre $-p$ e p é zero, então $i-j=0$, isto é, $i=j$. Então a

única maneira de ter $ia \equiv ja \pmod{p}$ é se $i = j$. Mostrando assim que todos os múltiplos de a a partir a até $(p-1)a$ possuem diferentes restos quando divididos por p. Finalmente, uma vez que existem exatamente $p-1$ múltiplos de a no nosso conjunto e $p-1$ possíveis restos não nulos $(mod\, p)$, concluímos que cada resto aparece exatamente uma vez. Provando assim que o conjunto dos restos das divisões dos elementos de **A** por p se configura como um srr módulo p.□

Agora estamos prontos para provar nosso resultado.

Teorema 3.3.1 *Se p é um primo e a é um inteiro não divisível por p, então*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Demonstração: Admitindo as hipóteses, ou seja, supondo que p seja um número primo e a seja um inteiro não divisível por p. Agora, considerando o conjunto $\mathbf{A} = \{a, 2a, 3a, \ldots, (p-1)a\}$. Devido ao Lema (3.3.1), nenhum dos elementos de **A** é divisível por p e quaisquer dois deles são incongruentes (mod p). Dessa forma, o conjunto formado pelos restos das divisões dos elementos de **A** por p consiste num srr. Assim, podemos multiplicar todos os elementos de **A** e obter a seguinte congruencia

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p},$$

isto é, o produto de todos os múltiplos de a tem o mesmo resto que o fatorial de $(p-1)$ quando dividido por p. Agora, podemos fatorar os $(p-1)$ números do lado esquerdo, e ficamos

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Como $(p-1)!$ é o produto de vários números que são todos menores que p, temos que $MDC(p, (p-1)!) = 1$. Assim, pela (Lei do Corte) temos

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

□

4 DEMONSTRAÇÕES ALTERNATIVAS: PARTE I

Neste capítulo apresentaremos três demonstrações alternativas para o Pequeno Teorema de Fermat. A primeira utilizando as ideias de Análise Combinatória, a partir da construção de colares; a segunda aplicando as ideias de Teoria dos Grafos; e a terceira utilizando a Série de Taylor. Tais demonstrações encontram-se embasadas, respectivamente, em (SANTOS, 2009), (YEGNANARAYANAN, 2005) e (BISHOP, 2008).

4.1 Por Análise Combinatória

Nesta seção trazemos a primeira demonstração alternativa para o Pequeno Teorema de Fermat, utilizando assuntos introdutórios da Análise Combinatória, essencilamente o Princípio Fundamental da Contagem e a Combinação Simples.

O conteúdo de Análise Combinatória, apesar de ser concernente ao EM, também é abordado em Olimpíadas de Matemática do Nível II, 8º e 9º anos do EF. Por este motivo, damos uma atenção especial para esta demonstração, pois acreditamos na possibilidade de ser apresentada para ambos os grupos de alunos citados, desde que sejam trabalhados os pré-requisitos de conteúdos necessários. Tal demonstração também pode ser apresentada de forma lúdica, como propõe (SANTO, 2017).

Assim, para conseguirmos uma melhor compeensão dos leitores passamos à definição necessária para a demonstração.

Definição 4.1.1 (Princípio Fundamental da Contagem) *Se há d_1 modos de tomar uma decisão D_1, d_2 modos de tomar a decisão D_2 e assim por diante, até d_n modos de tomar a decisão D_n, então o número de modos de tomar sucessivamente tais decisões é*

$$d_1 \cdot d_2 \cdot d_3 \cdot \ldots \cdot d_n.$$

Vamos a demonstração do Pequeno teorema de Fermat.

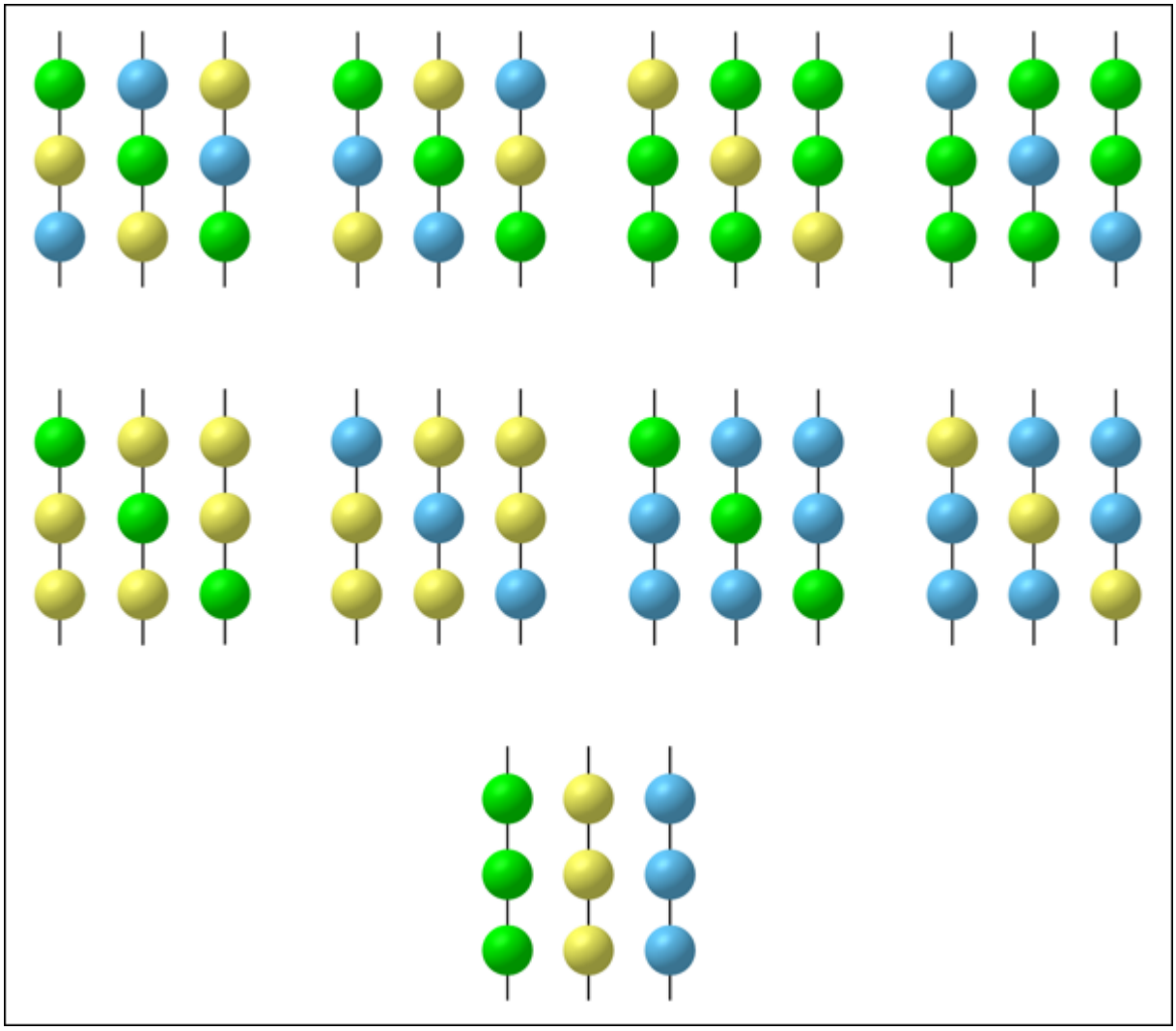
Para construirmos essa demonstração, partiremos da necessidade de se formar correntes, cada uma com p contas coloridas, e que possuímos um total de n cores para uso ilimitado. Nesse contexto, pelo Princípio Fundamental da Contagem, conseguimos formar n^p correntes diferentes. Veja que para a primeira conta c_1 temos n cores possíveis, para a conta c_2 também temos n cores possíveis e assim segue até a p-ésima conta c_p. Descobrindo assim, que a quantidade

de correntes é

$$\underbrace{n \cdot n \cdot \ldots \cdot n}_{p \text{ vezes}} = n^p.$$

Observe a Figura 1 abaixo, que ilustra o total de correntes quando temos $n = 3$ e $p = 3$.

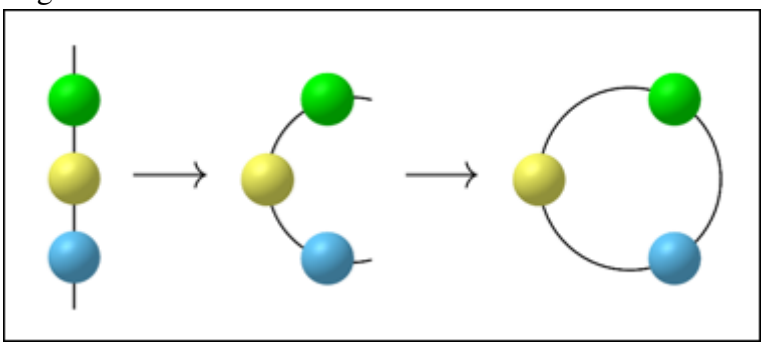
Figura 1 – Todas as correntes quando $n = 3$ e $p = 3$



Fonte: Elaborada pelo autor.

Como podemos usar a mesma cor para todas as contas e temos um total de n cores, então conseguiremos formar n correntes que possuam uma única cor. Com isso, como temos n^p correntes, quando separarmos as n correntes que possuem apenas uma cor, ficamos com $n^p - n$ correntes que possuem pelo menos uma conta com uma cor diferente das outras. Se de cada corrente formada, juntarmos suas extremidades, formaremos braceletes. Veja na Figura 2, com uma das correntes do exemplo dado.

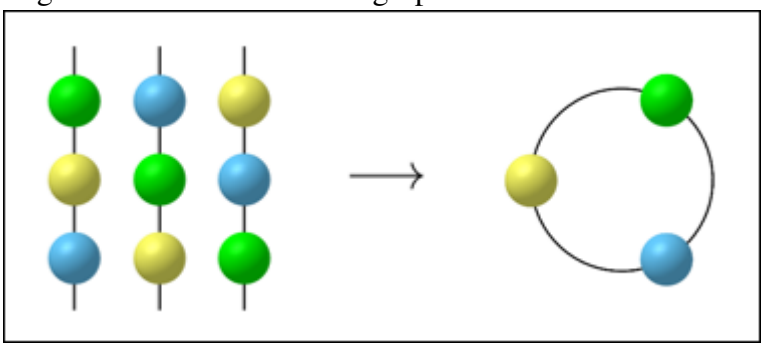
Figura 2 – Bracelete de uma corrente



Fonte: Elaborada pelo autor.

Note que se pegarmos uma corrente aleatória e movermos a conta que está na parte inferior e colocarmos na parte superior da corrente, montaremos uma corrente diferente (sabemos que essa nova corrente está dentro do conjunto das $n^p - n$ que poderemos formar, porém ela será diferente da corrente que escolhemos aleatoriamente), mas o bracelete resultante permanecerá o mesmo.

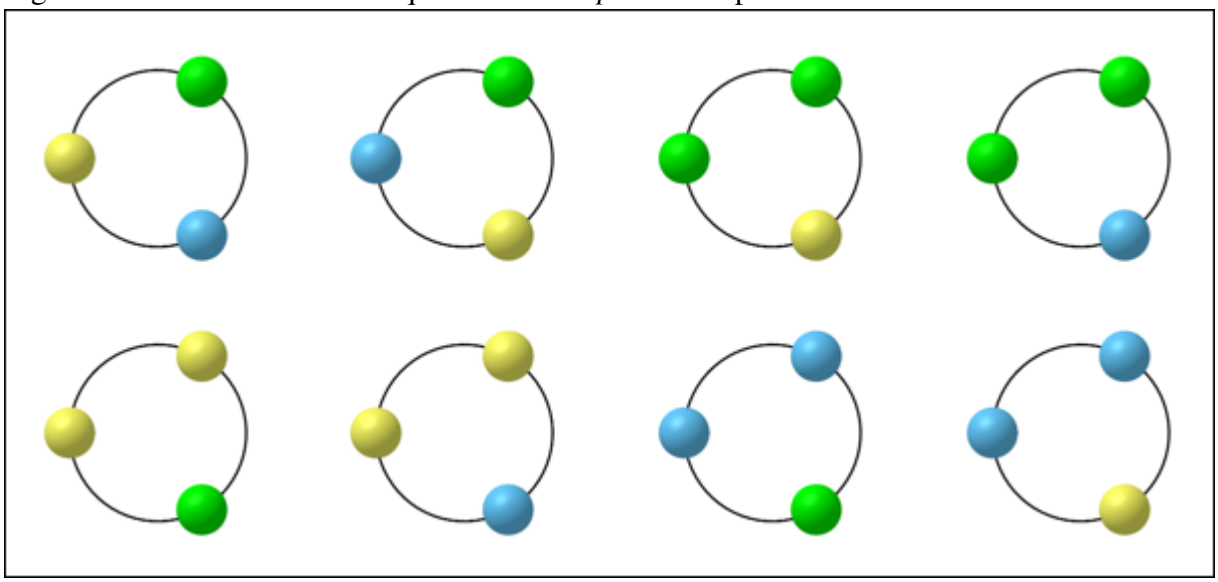
Figura 3 – Bracelete de um grupo de correntes diferentes



Fonte: Elaborada pelo autor.

Pelo exemplo dado inicialmente, quando $n = 3$ e $p = 3$, conseguimos formar 27 correntes, das quais apenas 3 formam um grupo das que possuem uma única cor e 24 são as que possuem pelo menos uma conta com uma cor diferente das outras. Podemos dividir essas 24 correntes em 8 grupos de 3 correntes multicoloridas que podem ser obtidas uma da outra, por uma ou mais repetições do processo que descrevemos (mover a conta que está na parte inferior e colocar na parte superior). Note que na Figura 1 dispomos os 8 primeiros grupos da forma descrita acima. Observe que para cada um desses oito grupos distintos corresponde um bracelete diferente. Veja a Figura 4 abaixo.

Figura 4 – Todos os braceletes quando $n = 3$ e $p = 3$ com pelo menos uma conta de cor diferente

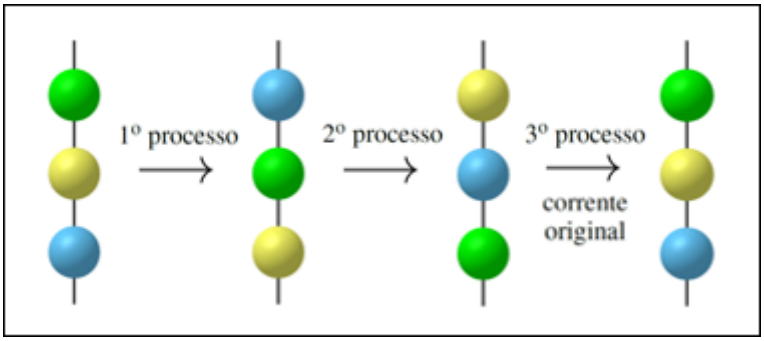


Fonte: Elaborada pelo autor.

Chamaremos de k o menor número de vezes que podemos repetir o processo descrito até que obtenhamos novamente a corrente original. Como separamos as correntes que possuem apenas uma cor, podemos ver que $k > 1$. Dessa forma, se escolhermos uma corrente e fizermos k vezes o processo, obteremos a corrente original, se fizermos mais k vezes, ou seja $2k$ vezes, obteremos novamente a corrente original e de forma semelhante para $3k$, $4k$, $5k$, etc.

Pelo algoritmo de Euclides (Definição 3.2.1), há q e r, tais que $p = qk + r$, com $0 \leq r < k$. Como uma corrente é reproduzida após qk passos (processos) e é também reproduzida após p passos, serão necessários r passos, após o qk-ésimo passo para se obter uma reprodução da colocação inicial. Como $r < k$ e k é o menor número inteiro positivo de passos necessários para a obtenção de uma reprodução, vemos que r deve ser igual a zero. Logo $p = qk$ e, portanto, $k = p$ uma vez que $k > 1$ e p é primo. Observe que no exemplo $n = 3$ e $p = 3$ precisamos de no mínimo três repetições do processo descrito para obtermos a corrente original.

Figura 5 – Processos para obtenção da corrente original



Fonte: Elaborada pelo autor.

Sendo assim, as $n^p - n$ correntes podem ser organizadas em grupos de p correntes cada (como fizemos na Figura 1 com o exemplo dado) e, como já mostrado, cada um desses grupos gera um bracelete diferente.

Chamando o número de braceletes de B, podemos concluir que quando multiplicamos B por p encontramos o número de correntes que não são formadas de uma única cor. Como sabemos, o número de correntes que não são formadas com contas de uma única cor é $n^p - n$. Portanto, $pB = n^p - n$, isto é $p \mid (n^p - n)$.

4.2 Por Teoria dos Grafos

Os matemáticos, normalmente, estão cientes do significado da Teoria dos Grafos aplicada a outras áreas da ciência e até mesmo a problemas sociais. Essas áreas incluem Química Orgânica, Física do Estado Sólido, Redes de Comunicações, Ciência da Computação, representação de rede de rotas de transporte (aplicativos de mapas, por exemplo), entre outros.

No entanto, nem todos percebem que os poderosos métodos combinatórios encontrados na Teoria dos Grafos também podem ser usados para provar resultados significativos e bem conhecidos em uma variedade de áreas da Matemática Pura. Um desses resultados, que é o Pequeno Teorema de Fermat, apresentamos neste trabalho e, assim como a demonstração anterior, também vislumbramos a possibilidade de apresetação desta para os alunos de olimpíadas.

As idéias básicas e o ponto de partida da Teoria dos Grafos foram introduzidos por Leonhard Euler no século XVIII, quando resolveu o conhecido "problema das sete pontes de Königsberg". Para detalhes sobre o surgimento desse ramo da Matemática, bem como do problema citado, indicamos a leitura de (ASSIS, 2016).

Dessa forma, passemos às definições necessárias para a demonstração do Pequeno Teorema de Fermat com viés na Teoria dos Grafos.

Definição 4.2.1 *Um grafo não direcionado $G = (V,E)$ é um par em que V é um conjunto, chamado de vértices de G, e E é um conjunto de subconjuntos de 2 elementos de V, chamados de arestas de G. Uma aresta $e \in E$ é denotada por $e = xy$, onde x e y são os vértices de e. O grau de um vértice v é o número de arestas incidentes com v.*

Definição 4.2.2 *Uma trilha de comprimento n em um grafo G é uma sequência de vértices $x_0, x_1, ..., x_n$ com $x_i \in V$, tal que para $i = 0, 1, \ldots, n-1$, $x_i x_{i+1}$ é uma aresta de G e, além disso, todas as arestas $x_i x_{i+1}$ são distintas. Se $x_0 = x_n$, então a trilha será fechada. Quando todos os*

vértices da sequência são distintos, a trilha é percorrida por um caminho. Uma trilha fechada, cujos vértices são distintos, exceto para x_0 e x_n, é chamada de ciclo.

Definição 4.2.3 *Um grafo G é conexo se quaisquer dois vértices de G forem unidos por uma trilha em G. Caso contrário, G será desconexo. Os componentes de G são os subgrafos conexos máximos de G.*

Com tais definições, estamos prontos para proceder com a segunda demonstração alternativa para o Pequeno Teorema de Fermat.

Demonstração: Considere o Grafo $G = (V,E)$, onde V é o conjunto de todas as sequências $(a_1, a_2, \ldots, a_p)$ de números naturais tais que $1 \leq a_i \leq a$, com $a_i \neq a_j$ para algum $i \neq j$. Como existe pelo menos um par $a_i \neq a_j$, para conseguirmos contar quantos elementos possuem em V, basta contar a quantidade de possibilidades para todo $a_i = a_j$ e subtrair da quantidade total de possibilidade de formação do conjunto $(a_1, a_2, \ldots, a_p)$. Assim, V possui $a^p - a$ elementos, pois a^p é a quantidade de possibilidades sem nenhuma restrição e a é a quantidade de possibilidades de todos os a_i serem iguais, a saber:

$$a \text{ conjuntos} \begin{cases} (1,1,\ldots,1) \\ (2,2,\ldots,2) \\ \quad\vdots \\ (a,a,\ldots,a) \end{cases}$$

Sejam $u, v \in V$ de tal forma que $u = (u_1, u_2, u_p)$ e $v = (u_p, u_1, \ldots, u_{p-1})$. Assim, temos que $uv \in E$ (lembre-se que uv representa uma aresta de G). Nessas condições, cada vértice de G é de grau 2, pois incidem exatamente duas arestas em cada um deles. Desta forma, cada componente de G é um ciclo de comprimento p. Portanto, o número de componentes de G deve ser $\frac{a^p - a}{p}$. Mostrando que $p \mid (a^p - a)$.

4.3 Por Série de Taylor

Segundo Serpa (2012), uma das provas mais modernas para o Pequeno Teorema de Fermat se vale das ideias da Série de Taylor, publicada no ano de 2008, com base na publicação de Brook Taylor (1717).

O interessante é que tal demonstração, apesar de ser moderna, é ancorada em técnicas matemáticas antigas, pois utiliza apenas a já citada Série de Taylor, o Teorema Binomial, a

Progressão Geométrica e o Princípio de Indução Finita. Em outras palavras, a prova não é o resultado de ferramentas matemáticas hodiernas, contudo era perfeitamente acessível aos matemáticos antes mesmo da demonstração dada por Euler (BISHOP, 2008).

Para conseguirmos construir tal demonstração, definamos primeiro a Série de Taylor.

Definição 4.3.1 (Série de Taylor) *A série de Taylor da função $f(x)$ em torno do ponto $x = a$ é dada da seguinte forma*

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(a)}{n!}(x-a)^n.$$

Associadamente, temos o polinômio de Taylor de ordem n em torno de $x = a$, da função f(x) diferenciável n-vezes no ponto, é dado por

$$p(x) = f(a)\frac{(x-a)^0}{0!} + f'(a)\frac{(x-a)^1}{1!} + f''(a)\frac{(x-a)^2}{2!} + \ldots + f^n(a)\frac{(x-a)^n}{n!}.$$

Do Cálculo I, temos que o Polinômio de Taylor é o Polinômio de grau n que melhor aproxima o gráfico de uma dada função no entorno de um ponto p que pertence ao seu domínio.

Também precisaremos do conceito de Progressões Geométicas.

Definição 4.3.2 *Uma Progressão Geométrica (PG) é uma sequência numérica em que cada termo, a partir do segundo, é obtido pelo produto do termo anterior por uma constante (q), e esta constante chamamos de razão da progressão geométrica.*

Para concluir as ferramentas necessárias a nossa demonstração, precisamos compreender como se dá a soma dos n primeiros termos de uma PG. Assim enunciamos o seguinte lema.

Lema 4.3.1 *A soma dos n primeiros termos de uma Progressão Geométrica (a_n), de razão $q \neq 1$ é dada por*

$$S_n = a_1 \cdot \frac{q^n - 1}{q - 1}.$$

Demonstração: Admita a soma dos termos da Progressão Geométrica

$$S_n = a_1 + a_2 + a_3 \ldots + a_{n-1} + a_n. \tag{4.1}$$

Multiplicando ambos os membros pela razão (q) obtemos

$$qS_n = a_2 + a_3 + a_4 \ldots + a_n + a_{n+1}. \tag{4.2}$$

Subtraindo a quação (4.1) da equação (4.2) temos

$$qS_n - S_n = a_{n+1} - a_1$$
$$S_n(q-1) = a_1 q^n - a_1$$
$$S_n = a_1 \cdot \frac{q^n - 1}{q-1}.$$

Agora estamos prontos para proceder com a prova do Pequeno Teorema de Fermat.

Demonstração: O caso $p = 2$ é facilmente verificado, dessa forma consideremos que p é um primo ímpar. Seja,

$$f(x) = x^{p-1} - 1. \tag{4.3}$$

Faremos o desenvolvimento em série de Taylor da função em torno de $x = 1$, porém antes é importante percebermos que

$$\begin{aligned}
f(x) &= x^{p-1} - 1 \\
f(1) &= 1^{p-1} - 1 = 0 \\
f'(x) &= (p-1)x^{p-2} \\
f'(1) &= (p-1) \\
f''(x) &= (p-1)(p-2)x^{p-3} \\
f''(1) &= (p-1)(p-2) \\
&\vdots
\end{aligned}$$

Se desenvolvermos em série de Taylor a função em torno de $x = 1$, obtemos

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

Agora, vamos considerar os valores de x divisíveis por p. Nesses valores de x, $f(x)$ é igual a um múltiplo de $p-1$ (basta substituir em 4.3), logo $f(x)$ não é divisível por p. Dessa forma, tome $x = pq + r$, com $r \in \mathbb{Z}$ e $0 < r < p$. Então a equação $f(x) = x^{p-1} - 1 \pmod p$, pode ser escrita como

$$f(pq+r) \equiv f(r) \pmod p$$

Logo, basta considerarmos os valores de x tais que $0 < x < p$.

Por indução temos que, quando $x = 1$, $f(x)$ é divísível por p, pois $f(1) = 0$ e $p \mid 0$. Suponhamos então que $f(n)$ é divisível por p para algum $n \in \mathbb{N}$ e vamos verificar que $f(n+1)$ também é. Temos

$$f(n+1) = (p-1)n + \frac{1}{2!}(p-1)(p-2)n^2 + \ldots + \frac{1}{(p-1)!}(p-1)!n^{p-1}. \tag{4.4}$$

Como

$$\binom{p-1}{k} = \frac{(p-1)!}{k!(p-k-1)!} = \frac{(p-1)(p-2)\ldots(p-k)(p-k-1)!}{k!(p-k-1)!}$$

$$\Rightarrow \binom{p-1}{k} = \frac{(p-1)(p-2)\ldots(p-k)}{k!} \equiv \frac{(-1)(-2)\ldots(-k)}{k!} \equiv \frac{(-1)^k k!}{k!} \equiv (-1)^k (\text{mod } p),$$

da equação (4.4) resulta

$$f(n+1) \equiv -n + n^2 - n^3 + \ldots + (-n)^k \ (\text{mod } p).$$

Note que $f(n+1)$ é congruente à soma de uma progressão geométrica de razão $-n$. Logo, podemos reduzir a última congruência da seguinte forma

$$f(n+1) \equiv \frac{-n+n^p}{1+n} \ (\text{mod } p).$$

Fatorando esta última congruência temos

$$f(n+1) \equiv \frac{n(-1+n^{p-1})}{1+n} \ (\text{mod } p).$$

Como $0 < n < p$, então $1+n$ não é divisível por p. Por hipótese, $n^{p-1} - 1$ é divisível por p, o que prova o resultado por indução.

5 DEMONSTRAÇÕES ALTERNATIVAS: PARTE II

Neste capítulo, apresentaremos mais duas demonstrações alternativas para o Pequeno Teorema de Fermat. A primeira, utilizando as ideias de Sistemas Dinâmicos e a segunda, os conceitos introdutórios da Teoria dos Grupos, utilizando-se também do Lema de Bézout.

5.1 Via Sistemas Dinâmicos

À primeira vista, o assunto dos sistemas dinâmicos parece não ter relação com a teoria dos números, pois nesta área da Matemática, estudamos como as quantidades mudam no tempo quando governadas por equações diferenciais ou relações de recorrência.

O estudo relativo aos Sistemas Dinâmicos foi introduzido pelo matemático francês Henri Poincaré (1854-1912) que Segundo Viana (2012), é considerado por muitos como o último matemático que compreendeu com profundidade e deu notáveis contribuições à maioria das disciplinas matemáticas e também a áreas afins do conhecimento, tais como a Física e a Filosofia.

Assim, o objetivo dessa seção é a prova do Pequeno Teorema de Fermat num viés de Sistemas Dinâmicos. Uma prova utilizando deste assunto, porém, com uma abordagem que privilegia a Geometria pode ser encontrada em (IGA, 2003). Assim, passemos aos pré-requisitos necessários para proceder com a demonstração.

Aqui, usaremos a ideia de pontos periódicos de um Sistema Dinâmico definido por funções da forma

$$f : [0,1] \longrightarrow [0,1]$$

contínuas.

Definição 5.1.1 *Dizemos que um ponto $x \in [0,1]$ é $n \in \mathbb{N}$ periódico se $f^n(x) = x$ e $\forall k < n$, $k \in \mathbb{N}$, $f^k(x) \neq x$.*

Observe que $f^n(x)$ representa a composição de f por ela mesma n vezes. Feitas tais considerações podemos enunciar o Teorema desejado:

Teorema 5.1.1 (Fermat) *Seja p um primo e a um inteiro. Então*

$$a^p \equiv a \ (mod\ p).$$

A prova deste Teorema é baseada em três lemas relacionados à seguinte função:
Seja $n \in \mathbb{N}$ defina a função

$$\begin{array}{rcl} T_n : [0,1] & \longrightarrow & [0,1] \\ x & \longmapsto & \begin{cases} nx - \lfloor nx \rfloor, & \text{se } x \neq 1 \\ 1, & \text{se } x = 1. \end{cases} \end{array}$$

onde $\lfloor\ \rfloor : \mathbb{R} \longrightarrow \mathbb{R}$ é a função tal que $\forall y \in \mathbb{R}$

$$\lfloor y \rfloor = max\{z \in \mathbb{Z};\ z \leq y\},$$

conhecida como função piso ou função maior inteiro.

Vamos aos lemas necessários para a prova do Teorema de Fermat.

Lema 5.1.1 *Seja $n \in \mathbb{N} \setminus \{1\}$. Então T_n tem n pontos fixos.*

Vale lembrar que $f : [0,1] \longrightarrow [0,1]$ tem um ponto fixo se existe $x \in [0,1]$ tal que $f(x) = x$.
Demonstração: Primeiramente, observe que 0 e 1 são pontos fixos de T_n. Agora tome $x \in (0,1)$. Neste caso, se x é ponto fixo de T_n temos:

$$\begin{array}{rcl} T_n(x) = x & \iff & nx - \lfloor nx \rfloor = x \\ & \iff & nx - x = \lfloor nx \rfloor \\ & \iff & x = \dfrac{\lfloor nx \rfloor}{n-1} \end{array} \tag{5.1}$$

Isto prova que $x \in \mathbb{Q}$ e é da forma

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

e como $x \in (0,1)$ os valores possíveis para k são:

$$k = 1, 2, 3, \ldots, n-2. \tag{5.2}$$

Note que se $n = 2$ o resultado está provado, pois 0 e 1 são pontos fixos.
Logo, assuma $n \geq 3$.

Por fim, observe que para todo k em (5.2) obtemos um ponto fixo para T_n. De fato, note que

$$\frac{\lfloor nx \rfloor}{n-1} = \frac{\left\lfloor n \cdot \dfrac{k}{n-1} \right\rfloor}{n-1} = \frac{\left\lfloor \dfrac{n}{n-1} \cdot k \right\rfloor}{n-1} \tag{5.3}$$

e veja que $\frac{n}{n-1} \cdot k \leq k$, do contrário, isto é, se

$$\frac{n}{n-1} \cdot k \geq k+1$$

então

$$nk \geq (k+1)(n-1) = kn - k + n - 1$$

donde obtemos

$$k+1 \geq n$$

o que é absurdo, pois estamos assumindo $k \leq n-2$.

De (5.3) segue que

$$\frac{\lfloor nx \rfloor}{n-1} = \frac{\left\lfloor \frac{n}{n-1} \cdot k \right\rfloor}{n-1} = \frac{k}{n-1} = x,$$

ou seja, de (5.1) x é ponto fixo de T_n.

Logo, os pontos fixos de T_n são:

$$0, \frac{1}{n-1}, \frac{2}{n-1}, \ldots, \frac{n-2}{n-1}.$$

que são em um total de n. □

Enunciemos e provemos agora o segundo lema.

Lema 5.1.2 *Para todo $z \in \mathbb{Z}$ e $x \in \mathbb{R}$,*

$$\lfloor x+z \rfloor = \lfloor x \rfloor + z.$$

Demonstração: Temos,

$$\lfloor x+z \rfloor \leq x+z < \lfloor x+z \rfloor + 1 \leq x+z+1 \tag{5.4}$$

Também,

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \tag{5.5}$$

De (5.4) temos:

$$x+z-1 < \lfloor x+z \rfloor \leq x+z \tag{5.6}$$

e substituindo (5.5) em (5.6) obtemos:

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

ou seja,

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

Como os três números acima são inteiros consecutivos, segue que

$$\lfloor x + z \rfloor = \lfloor x \rfloor + z.$$

Isto prova o lema. □

Consideremos agora o último lema.

Lema 5.1.3 *Sejam m, n* $\in \mathbb{N}$. *Então,* $\forall x \in [0,1]$, *temos*

$$\big(T_m \circ T_n\big)(x) = T_{mn}(x).$$

Demonstração: Se $x = 1$ o resultado é óbvio. Tomemos $x \in [0,1)$. Temos

$$\begin{aligned} \big(T_m \circ T_n\big)(x) &= T_m\big(T_n(x)\big) \\ &= T_m\big(nx - \lfloor nx \rfloor\big) \\ &= m\big(nx - \lfloor nx \rfloor\big) - \big\lfloor m\big(nx - \lfloor nx \rfloor\big)\big\rfloor \\ &= mnx - m\lfloor nx \rfloor - \big\lfloor mnx - m\lfloor nx \rfloor\big\rfloor \end{aligned}$$

como $m \in \mathbb{N}$, temos que $-m\lfloor nx \rfloor \in \mathbb{Z}$. Dessa forma, pelo Lema (5.1.2) temos

$$\begin{aligned} \big(T_m \circ T_n\big)(x) &= (mn)x - m\lfloor nx \rfloor - \big(\lfloor mnx \rfloor - m\lfloor nx \rfloor\big) \\ &= (mn)x - \big\lfloor (mn)x \big\rfloor \\ &= T_{mn}(x), \end{aligned}$$

como queríamos demonstrar. □

Agora, para concluirmos os pré-requisitos necessários para provar o Teorema de Fermat, precisamos definir o conceito de órbita de um ponto em relação a uma função.

Definição 5.1.2 *Dada $f : [0,1] \longrightarrow [0,1]$ e $x_0 \in [0,1]$. A órbita de x_0 em relação a f é o conjunto que descreve a evolução de x_0, isto é,*

$$\{x_0,\ f(x_0),\ f^2(x_0), \dots\} = \{f^n(x_0);\ n \in \mathbb{N}\}.$$

Denotaremos este conjunto por

$$O_f(x_0).$$

Note agora que se $x_0 \in [0,1]$ é n-periódica, então

$$f^n(x_0) = x_0$$

e daí, $\forall m \in \mathbb{N}$, $\exists k, r \in \mathbb{N} \cup \{0\}$ tal que

$$m = nk + r, \quad r < n.$$

Daí,

$$f^m(x_0) = f^{nk+r}(x_0) = f^r(x_0),$$

isto prova que $O_f(x_0)$ tem apenas n elementos, a saber,

$$x_0,\ f(x_0),\ f^2(x_0), \dots,\ f^{n-1}(x_0).$$

Neste caso, dizemos que o comprimento da órbita $O_f(x_0)$ é n.

Com estas informações, podemos seguir com a prova do Teorema principal.

Demonstração (Pequeno Teorema de Fermat): Podemos supor, sem perda de generalidade, que $a \in \big(\mathbb{N} \setminus \{1\}\big)$. Então para o primo p, considere x um ponto p-periódico de T_a. Neste caso,

$$T_a^p(x) = x.$$

Pelo Lema (5.1.3) temos que $T_a^p(x) = T_{a^p}(x)$, daí,

$$T_{a^p}(x) = x.$$

Pelo Lema (5.1.1), segue que

$$T_a \text{ tem } a \text{ pontos fixos}$$

e

$$T_{a^p} \text{ tem } a^p \text{ pontos fixos.}$$

Note ainda que todo ponto fixo de T_a é também ponto fixo de T_{a^p}. De fato,

$$T_{a^p}(x) = T_{a^{p-1}}\big(T_a(x)\big) = T_{a^{p-1}}(x) = \ldots = T_a(x) = x.$$

Agora, desde que p seja primo, o resto dos pontos p-periódicos de T_{a^p} tem período mínimo p sob T_a, isto é, não existe x_0 ponto p-periódico de T_a e $n < p$ tal que

$$T_a^n(x) = x.$$

Esses pontos restantes indicados acima são exatamente

$$a^p - a \text{ pontos.}$$

Ora, cada um dos pontos $a^p - a$ indicados acima tem uma órbita de comprimento p. Segue daí que existem

$$\frac{a^p - a}{p}$$

órbitas de comprimento p para f. Logo, como o número de órbitas é um número natural, segue que

$$a^p - a \text{ é divisível por } p$$

donde

$$a^p \equiv a \pmod{p}.$$

□

Isto conclui a prova do Pequeno Teorema de Fermat usando conceitos de Sistemas Dinâmicos.

5.2 Via Teoria dos Grupos

Como vimos até aqui, existem variadas demonstrações para o Pequeno Teorema de Fermat, e a Teoria dos Grupos nos fornece uma muito elegante. A teoria mencionada envolve o estudo de estruturas algébricas conhecidas como grupos, que tem aplicações em muitos campos da Matemática.

Assim, nesta seção, temos como objetivo demonstrar o Pequeno Teorema de Fermat utilizando os conceitos da Teoria dos Grupos. Para tanto, iniciaremos com alguns fatos sobre

grupos e, em seguida, enunciaremos e demonstraremos o Lema de Bézout, de modo que tenhamos as ferramentas necessárias à abordagem do objeto desta investigação. A demonstração que apresentaremos agora é baseada na publicação de (MOMKUS, 2011).

Definição 5.2.1 *Chamamos de Grupo um conjunto G, não vazio, com uma operação binária*

$$\begin{aligned} *: \quad G \times G &\longrightarrow G \\ (a,b) &\longmapsto a*b \end{aligned}$$

se tal conjunto satisfaz as seguintes condições:

1. *G é fechado para a operação binária $*$, ou seja, para todo $a,b \in G$*

$$a*b \in G.$$

2. *A operação $*$ é associativa, ou seja, quaisquer que sejam $a,b,c \in G$, tem se que*

$$(a*b)*c = a*(b*c);$$

3. *Para todo $a \in G$, existe um elemento identidade em G, ou seja, $\exists e \in G$ tal que*

$$e*a = a = a*e;$$

4. *Para cada $a \in G$, existe $a^{-1} \in G$ chamado inverso de a na operação $*$ tal que*

$$a*a^{-1} = e = a^{-1}*a.$$

Definição 5.2.2 *Dizemos que G é um Grupo Abeliano se para todos $a,b \in G$, a operação $*$ é comutativa, ou seja, também satisfaz a seguinte condição:*

$$a*b = b*a.$$

Pelas definições acima, temos que o conjunto dos números inteiros, munido da operação de adição $(\mathbb{Z},+)$ é um Grupo Abeliano. Normalmente utilizamos a notação multiplicativa $(.)$ quando falamos sobre grupos gerais e a notação aditiva $(+)$ quando falamos sobre Grupos Abelianos. Nesta dissertação, assumiremos que todos os Grupos são Abelianos, então, utilizaremos $+$ como a operação binária.

Definição 5.2.3 *Um Subgrupo H é um subconjunto não vazio de um Grupo G que é um grupo sob a operação indicada. Denotamos um Subgrupo por $H \leq G$.*

Proposição 5.2.1 *Seja G um Grupo. Um subconjunto não vazio $H \subseteq G$ é um Subgrupo se, e somente se, para todos $a, b \in H$,*

$$a - b \in H.$$

Demonstração: Seja $a \in H$. Se $a - b \in H$, para todos $a, b \in H$ então

$$a - a = 0 \in H,$$

satisfazendo a condição (3) dos critérios para ser um Grupo. Observe que

$$0 - a = -a \in H,$$

assim, a condição (4) é satisfeita.
Para todos $a, b \in H$, temos que

$$a - (-b) = a + b \in H,$$

mostrando que a condição (1) também é válida. Note que H herda a associatividade de G.
Desse modo, mostramos que para todos $a, b \in H$ temos que $a - b \in H$, o que implica $H \leq G$. □

Note que um Subgrupo é essencialmente um Grupo, pois, como verificadas acima, todas as condições de Grupo são satisfeitas.

Um exemplo de um Subgrupo de $(\mathbb{Z}, +)$ é o conjunto dos números pares $2\mathbb{Z}$. De fato, todo subconjunto da forma $n\mathbb{Z}$ são Subgrupos. Vamos mostrar, posteriormente, que esses são os únicos Subgrupos de $(\mathbb{Z}, +)$.

Sendo um Grupo G e um Subgrupo $H \leq G$, definimos uma relação de equivalência $\sim_H$ em G por $g \sim_H g'$, se $g - g' \in H$.

Definição 5.2.4 *As Classes de H em G são dadas por*

$$g + H = \{f \in G;\ g \sim_H f\} = \{f \in G;\ f = g + h,\ h \in H\}.$$

Definição 5.2.5 *Se um Grupo G é finito, chama-se Ordem de G, denotado por $|G|$, a quantidade de elementos do conjunto G, ou seja, é a sua Cardinalidade. Um grupo infinito diz-se ter Ordem infinita e representa-se por $|G| = \infty$.*

Definição 5.2.6 *Seja G um Grupo e $g \in G$. Chamamos de Ordem do elemento g, denotado $Ord(g)$, ou mesmo $|g|$, o menor inteiro positivo n tal que $g + g + \ldots + g$ adicionado n vezes é igual a zero, ou seja, $ng = 0$. Se não existir tal n, então dizemos que a Ordem de g é infinita.*

Proposição 5.2.2 *Seja um Subgrupo $H \leq G$. Então, H é ele mesmo uma Classe e todas as Classes de H possuem mesma Cardinalidade, portanto segue-se que $|H| = |g+H|$ para todo $g \in G$.*

Demonstração: Seja $g \in G$. Definimos uma função $\phi_g : H \longrightarrow g+H$ por

$$\phi_g(h) = g+h.$$

Vamos mostrar que tal aplicação é bijetiva, e, desse modo, cada conjunto possui a mesma quantidade de elementos.

Dado algum $f \in g+H$, sabemos que, pela definição de Classe, existe algum h tal que $f = g+h = \phi_g(h)$. Consequentemente, se $f \in g+H$, então existe algum $h \in H$ tal que $\phi_g(h) = f$, mostrando que a função ϕ_g é sobrejetiva.

Agora, tome $h_1, h_2 \in H$. Se $\phi_g(h_1) = \phi_g(h_2)$, então $g+h_1 = g+h_2$. Subtraindo g em ambos os membros temos que $h_1 = h_2$. Mostrando assim que a função também é injetiva. Portanto, a função ϕ_g é bijetiva, o que acarreta em $|H| = |g+H|$ para todo $g \in G$. □

Além disso, como G é um Grupo, ele deve conter a identidade 0, portanto, o próprio H deve ser uma Classe porque podemos ter $0+H = H$.

Definição 5.2.7 *Sejam G um Grupo Abeliano e $H \leq G$. Definimos o Grupo Quociente G/H por $\{g+H; g \in G\}$. A operação binária é uma operação de Classes. A adição é definida por*

$$(g_1+H)+(g_2+H) = (g_1+g_2)+H.$$

Proposição 5.2.3 *Esta adição de Classes é bem definida.*

Demonstração: Sejam $g_1+H = g_1'+H$ e $g_2+H = g_2'+H$. Segue-se que $g_1' \in g_1+H$ e $g_2' \in g_2+H$. Assim, existem $h_1, h_2 \in H$ tal que $g_1' = g_1+h_1$ e $g_2' = g_2+h_2$. Então, temos que dois elementos pertencem a mesma Classe se, e somente se, a diferença deles pertence a H. Precisamos mostrar que se g_1-g_1', $g_2-g_2' \in H$, então $(g_1+g_2)-(g_1'+g_2') \in H$. Note que, como os Grupos são Comutativos, temos $(g_1+g_2)-(g_1'+g_2') = (g_1-g_1')+(g_2-g_2')$. Portanto, temos que ambos g_1-g_1', $g_2-g_2' \in H$, então, pela definição de um Subgrupo, a soma deles deve estar em H. □

Definição 5.2.8 *Seja X um conjunto. Uma partição de X é qualquer coleção P de subconjuntos não vazios de X dotada da seguinte propriedade: todo elemento de X pertence a um e apenas um dos elementos de P.*

Proposição 5.2.4 *O conjunto de todas as classes de H em G forma uma partição de G.*

Demonstração: Para as classes formarem uma partição de G, elas devem satisfazer duas condições:

1. Precisamos mostrar que a união de todas as classes é igual a G. Assim, tomemos a união de todas as classes. Se $g \in G$, então $g \in g+H$, então todo g está em alguma classe e $G = \bigcup_i g_i + H$.
2. Precisamos mostrar que se pegarmos $g_1,\ g_2 \in G$ temos que ou $g_1 + H = g_2 + H$ ou $(g_1+H)\bigcap(g_2+H) = \varnothing$, ou seja, as classes de H são disjuntas. Assumindo que as classes não são disjuntas, então $(g_1+H)\bigcap(g_2+H) \neq \varnothing$. Como a interseção não é vazia, então deve existir algum $f \in G$ tal que $f \in g_1+H$ e $f \in g_2+H$. Pela definição de classes, também sabemos que existem alguns $h_1, h_2 \in H$ tal que $g_1+h_1 = f = g_2+h_2$.

Portanto, para todo $h \in H$, $g_1+h = g_2+(h_2-h_1+h)$. Como $h_2-h_1+h \in H$, temos que $g_1+h \in g_2+H$ e $g_1+H \subseteq g_2+H$. Podemos repetir este mesmo procedimento para mostrar que $g_2+H \subseteq g_1+H$. Desse modo, $g_1+H = g_2+H$, mostrando que o conjunto de todas as classes de H em G formam uma partição de G. □

Agora que definimos as classes e demonstramos algumas de suas propriedades, podemos seguir para um dos mais importantes teoremas envolvendo Grupos, o teorema de Lagrange.

O teorema de Lagrange é essencial para o entendimento de Grupos e muitos outros conceitos matemáticos. Este teorema conecta a Teoria dos Grupos finitos à Aritmética, por isso é muito útil para conectar essas duas áreas.

Teorema 5.2.1 (Lagrange) *Para todo Grupo finito G, a ordem de todo subgrupo H de G divide a ordem de G.*

Demonstração: Seja G um Grupo e H um Subgrupo de G, com $g+H$ representando uma classe de H em G. Sabemos, da Proposição (5.2.4) que as Classes de $g+H$ particionam G e cada classe deve ter a mesma ordem que H. Seja n o número de Classes de H em G, e seja q a ordem de H. Como G é a união disjunta de suas classes e cada classe tem q elementos, existem qn elementos em G, então q divide a ordem de G. □

Passamos agora as características dos subgrupos de $(\mathbb{Z},+)$.

Proposição 5.2.5 *Um subconjunto de $(\mathbb{Z},+)$ é um subgrupo se, e somente se, o subconjunto for da forma $n\mathbb{Z}$ para algum inteiro positivo n.*

Demonstração: Tome um subconjunto $H \subseteq \mathbb{Z}$ que é da forma $n\mathbb{Z}$. Vamos mostrar que este é um subgrupo de $(\mathbb{Z},+)$. Sejam $a,b \in H$. Da Proposição (5.2.1), podemos mostrar que H é um subgrupo se $a-b \in n\mathbb{Z}$. Como $a,b \in n\mathbb{Z}$, eles também podem ser escritos como $a = na'$ e $b = nb'$ com $a',b' \in n\mathbb{Z}$. Desse modo, a$-b = na' - nb' = n(a'-b') \in n\mathbb{Z}$. Consequentemente, todo subconjunto da forma $n\mathbb{Z}$ são subgrupos do grupo $(\mathbb{Z},+)$.

Agora, tome um subgrupo $H \leq (\mathbb{Z},+)$. Precisamos mostrar que $H = n\mathbb{Z}$. Se $H = \{0\}$ então temos que $H = 0\mathbb{Z}$. Caso contrário, tomaremos apenas os elementos positivos de H que estão contidos em $\mathbb{N}$. Seja $H_+ = \{h \in H; h > 0\}$. Observe que H_+ não é vazio, pois H não é vazio e contém os elementos diferentes de zero. Como $\mathbb{N}$ é bem ordenado, isso significa que existe um elemento mínimo que está contido em H_+. Seja n o menor elemento em H_+. Note que $H \leq (\mathbb{Z},+)$, então segue que H é fechado para a adição e, consequentemente

$$\{nx; x \in \mathbb{Z}\} \subseteq H.$$

Portanto, $n\mathbb{Z} \leq H$. Agora precisamos mostrar que $H \leq n\mathbb{Z}$.

Suponha que existe $g \in H$ tal que $g \neq n\mathbb{Z}$. Pelo algoritmo da divisão, existe $nq + r = g$ tal que $0 < r < n$. Como H é um subgrupo e $g, nq \in H$, então $g - nq = r \in H$. Isto é uma contradição, porque $0 < r < n$ e já assumimos que n é o menor elemento em H_+. Portanto, $H \leq n\mathbb{Z}$ e segue que $H = n\mathbb{Z}$, que conclui a prova. □

Agora podemos usar as informações que temos sobre subgrupos de $(\mathbb{Z},+)$ para nos ajudar a provar o lema de Bézout.

O lema de Bézout é um conceito muito importante para provar o Pequeno Teorema de Fermat. Tal lema envolve tanto a Teoria dos Números quanto a Teoria dos Grupos.

Lema 5.2.1 (Bézout) *Sejam a, b inteiros tais que pelo menos um seja diferente de zero. Então, existem dois inteiros x e y tais que $MDC(a;b) = ax + by$.*

Demonstração: Seja o conjunto das combinações lineares de inteiros a e b chamado L. Esse conjunto deve ser um subconjunto do Grupo $(\mathbb{Z},+)$. Vamos mostrar que L também é um subgrupo de $(\mathbb{Z},+)$.

Sejam $x,y,z,w \in \mathbb{Z}$. Vamos pegar dois elementos $(xa+yb),(wa+zb) \in L$.

Observe que

$$\begin{aligned}(xa+yb)-(wa+zb) &= xa-wa+yb-zb \\ &= (x-w)a+(y-z)b\end{aligned}$$

Já sabemos que $(\mathbb{Z},+)$ é Grupo, portanto, para todo $x,y,z,w \in \mathbb{Z}$, temos $(x-w),(y-z) \in \mathbb{Z}$. Portanto, $(x-w)a+(y-z)b \in L$, assim, pela Proposição (5.2.1), L é um subgrupo de $(\mathbb{Z},+)$.

Como L é um subgrupo de $(\mathbb{Z},+)$, sabemos, da Proposição (5.2.5), que L deve ser da forma $n\mathbb{Z}$, em outras palavras, para todo $x,y \in \mathbb{Z}$,

$$xa+yb \in n\mathbb{Z}.$$

Consequentemente, $n \in L$ e existe $z \in \mathbb{Z}$ tal que $xa+yb=nz$. Tal resultado deve valer para todos $x,y \in \mathbb{Z}$. Podemos tomar $x=0$ e $y=1$ para mostrar que existe $z_1 \in \mathbb{Z}$ tal que $0\cdot a+1\cdot b=b=nz_1$ e segue que $n \mid b$. Podemos repetir o mesmo procedimento com $x=1$ e $y=0$ para mostrar que existe z_2 tal que $1\cdot a+0\cdot b=a=nz_2$ que significa $n \mid a$. Agora que $n \mid a$ e $n \mid b$, sabemos que

$$n \mid MDC(a,b).$$

Pela definição do máximo divisor comum, o $MDC(a,b)$ divide ambos a e b. Como $n \in L$, temos que n pode ser escrito como uma combinação linear dos inteiros a e b, assim $MDC(a,b)$ deve dividir n. Segue que $n=MDC(a,b)$. □

Agora que temos provado o teorema de Lagrange e o lema de Bézout, temos, então, as ferramentas necessárias para provar o Pequeno Teorema de Fermat, usando a Teoria dos Grupos.

Teorema 5.2.2 *Dado um inteiro a e um número primo p, o número a^p-a é divisível por p, isto é,*

$$a^p \equiv a\ (mod\ p)$$

Demonstração: Tome o conjunto $G=\{\mathbb{Z}/p\mathbb{Z}\}-\{0\}=\left\{\overline{1},\overline{2},\ldots,\overline{p-1}\right\}$, onde $\overline{a}$ representa o conjuntos dos números que deixam resto igual a a quando divididos por p. Tomemos esse conjunto (G), módulo p, sobre a operação binária de multiplicação.

Definimos multiplicação como

$$(a \bmod p)\cdot(b \bmod p) \equiv ab\ (\bmod p).$$

Observe que as propriedades associativa e comutativa são herdadas de $\mathbb{Z}$. Podemos verificar se G é fechado para essa operação, verificando se o produto de qualquer elemento em G não é equivalente a 0 mod p, o que nos permitirar dizer que nenhum divisor de p está em G. Sabemos que p é primo, consequentemente seus únicos divisores são 1 e p. Desse modo, não há como o produto de quaisquer dois elementos ser congruente a 0 mod p.

Podemos usar o lema de Bézout (Lema 5.2.1) para mostrar que os elementos de G são, de fato, invertíveis. Se tomarmos $g \in G$ e o número primo p, eles devem ser relativamente primos, uma vez que p é um número primo. Isto implica que o $MDC(g,p) = 1$. Desse modo, pelo lema de Bézout, existem inteiros x, y tais que

$$gx + py = MDC(g,p) = 1.$$

Quando colocamos isso em termos de aritmética modular, obtemos

$$gx \equiv 1 \pmod{p}.$$

Como resultado, x deve ser um inverso de g, satisfazendo, assim, a condição (4) de um Grupo. Assim, G se configura como um Grupo, pois satisfaz todas as condições necessárias. Observe que $|G| = p - 1$.

Seja $a \in G$, e $k = Ord(a)$. Podemos gerar um subgrupo $H \leq G$, a partir do inteiro a, tal que $H = \left\{a, a^2, a^3, \ldots, a^k\right\}$ Segue-se da definição da ordem de um elemento que

$$a^k \equiv 1 \pmod{p}.$$

Mostrando que H contém a identidade. Seja $m, n \in \mathbb{N}$ tais que $m, n \leq k$. O inverso do elemento a^n está contido em H, pois

$$a^n \cdot a^{k-n} \equiv a^k \equiv 1 \pmod{p}.$$

Note que $a^{k-n} \in H$, pois $n \leq k$. O produto de dois elementos a^m, $a^n \in H$ é dado por

$$a^m \cdot a^n = a^{m+n},$$

e sabemos que $a^{m+n} \in H$, porque se $m + n > k$, existirá $u, r \in \mathbb{N}$ tais que $r < k$ e $m + n = uk + r$. Então,

$$\begin{aligned} a^{m+n} &= a^{uk+r} \\ &= a^{uk} \cdot a^r \\ &= (a^k)^u \cdot a^r \\ &\equiv 1^u \cdot a^r \ (mod p) \\ &\equiv a^r \ (mod p) \end{aligned}$$

Desse modo, temos todos os requisitos para inferir que H é um subgrupo de G. Note que $|H| = k$.

Pelo teorema de Lagrange, sabemos que $|H|$ divide $|G|$, então segue-se que k divide $(p-1)$. Em outras palavras, existe $n \in \mathbb{Z}$ tal que

$$p - 1 = kn.$$

Agora podemos olhar a^{p-1} em termos de k.

$$\begin{aligned} a^{p-1} &= a^{kn} \\ &= (a^k)^n \\ &\equiv 1^n \ (mod p) \\ &\equiv 1 \ (mod p) \end{aligned}$$

Daí, temos que $a^{p-1} \equiv 1 \ (\text{mod } p)$. Quando multiplicarmos cada membro por a, obtemos

$$a^p \equiv a \ (\text{mod } p),$$

o que conclui a prova. □

6 CONSIDERAÇÕES FINAIS

Com base nas várias demonstrações apresentadas é que reforçamos as inter-relações existente entre os diversos ramos da Matemática, pois, além dos conteúdos imenentemente pertencentes à Teoria dos Números, conseguimos construir outras demonstrações para o Pequeno Teorema Fermat, ancorado nas ideias de Número Binomial, por meio do Princípio de Indução Finita; Análise Combinatória; Teoria dos Grafos; Série de Taylor; Sistemas Dinâmicos; e Teoria dos Grupos.

Para além dos nossos objetivos, conforme apresentado no decorrer do texto, percebemos que Pierre de Fermat deu contribuições bastante significativas para o desenvolvimento da Matemática, se destacando o princípio fundamental da Geometria Analítica, desenvolvido em paralelo com René Descartes; as bases técnicas do Cálculo Diferencial e Integral, utilizadas posteriormente por Isaac Newton; os alicerces para Teoria da Probabilidade juntamente com Pascal; e principalmente a Teoria dos Números, do qual apresentou diversos teoremas e conjecturas que engrandeceram esta área.

Dentro da Teoria dos Números, encontra-se nosso objeto de estudo, o Pequeno Teorema de Fermat, que cumpre um papel importantíssimo neste ramo da Matemática, pelo fato dele ter sido formulado com base no estudo sobre os Números Perfeitos que é fundamentado na investigação de fatores primos, que devido ao Teorema Fundamental da Aritmética se configura como a base desta área da Matemática.

De acordo com o conteúdo da carta de Fermat a Frenicle de Bessy, da qual, a partir de uma das explanações foi formulado o Pequeno Teorema Fermat como o conhecemos atualmente, percebemos que tal teorema não reflete no todo o que Fermat indagou, pois durante a leitura dessa passagem fica claro que ele se referia a potências de submúltiplo do dado primo subtraído de uma unidade, ou seja, dados $a, p \in \mathbb{Z}$, com p primo e $MDC(a,p) = 1$, temos que $p \mid a^{p-1} - 1$, podendo existir $b \in \mathbb{N}$ menor do que $p-1$ que satisfaz $p \mid a^b - 1$.

Outro aspecto que nos faz enfatizar a importância de Fermat para a Matemática é o fato do Princípio de Indução Finita, que é uma das ferramentas mais importantes e poderosas da Matemática, possuir uma forte equivalência com o conhecido Método da Descida Infinita que foi formulado e utilizada largamente por ele.

Ressaltamos a importância da utilização das demonstrações matemáticas para os alunos da Educação Básica, por meio das variadas técnicas, pois objetiva dar maiores subsídios de compreensão ampla dos assuntos trabalhados em sala.

Nesse sentido, acreditamos que as primeiras demonstrações do Pequeno Teorema de Fermat, apresentadas neste trabalho, possam ser utilizadas como referências, em cursos de Teoria dos Números voltados para turmas olímpicas da Educação Básica.

Consideramos ainda que o trabalho como um todo, constitui-se em uma referência a mais no tocante ao estudo da Teoria dos Números em nível de graduação e pós-graduação, bem como de tópicos relativos a História da Matemática.

Por fim, esperamos que esta dissertação motive professores da Educação Básica a buscarem desenvolver, em suas aulas, assuntos que reforçam as relações existentes entre os mais variados ramos da Matemática, assim como desperte o interesse em trabalhar as demonstrações dos conteúdos abordados.

REFERÊNCIAS

ASSIS, J. S. M. **Grafos Eulerianos no Ensino Médio.** 2016. 42 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional: PROFMAT) — Instituto de Matemática Pura e Aplicada - IMPA, Rio de Janeiro, 2016.

BARNER, K. Paul Wolfskehl and the Wolfskehl Prize. **Notices of the AMS**, v. 44, n. 10, p. 1294–1303, 1997.

BISHOP, R. E. On Fermat's Little Theorem. **VIGRE at the University of Chicago**, 2008. Disponível em: <www.math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/>. Acesso em: 20 mai. 2019.

BOYER, C. B. **História da Matemática**. São Paulo: Edgar Blücher, 1974.

BRASIL. Secretaria de Educação Fundamental. **Parâmetros Curriculares Nacionais:** Matemática. Brasília, MEC/SEF, 1998.

BURN, B. Fermat's Little Theorem - Proofs That Fermat Might Have Used. **The Mathematical Gazette**, v. 86, n. 507, p. 415–422, 2002. Disponível em: <www.jstor.org/stable/3621133>. Acesso em: 10 mai. 2019.

BURTON, D. M. **Elementary Number Theory**. Boston: McGraw-Hill, 2002.

CARNEIRO, J. P. Q. O Princípio da Descida Infinita de FERMAT. **Revista do Professor de Matemática (RPM)**, Rio de Janeiro: SBM, n. 32, 1996.

CHAN, H.-L.; NORRISH, M. A String of Pearls: Proofs of Fermat's Little Theorem. In: **International Conference on Certified Programs and Proofs**. Springer, Berlin, Heidelberg, 2012. p. 188–207.

DICKSON, L. E. **History of the Theory of Numbers**: Divisibility and primality. New York: Chelsea Publishing company, 1952. v. 1.

EVES, H. **Introdução à história da matemática**. Howard Eves; tradução Hygino H. Domingues. 5ª ed. - Campinas, SP: Editora da Unicamp, 2011.

GONÇALVES, C. H. B.; HADDAD, T. A. S. "Demonstração de Certos Teoremas Referentes a Números Primos", de Leonhard Euler: Tradução e Comentários. **Revista Brasileira de História da Matemática**, Rio Claro, v. 9, n. 17, p. 93–99, 2009. Disponível em: <www.rbhm.org.br/vo9-no17.html>. Acesso em: 28 abr. 2019.

IGA, K. A Dynamical Systems Proof of Fermat's Little Theorem. **Mathematics magazine**, Taylor & Francis, v. 76, n. 1, p. 48–51, 2003.

LIMA, E. L. **Curso de análise**. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada - IMPA, 1976. v. 1.

MOMKUS, J. Introductory Group Theory and Fermat's Little Theorem. **VIGRE at the University of Chicago**, 2011. Disponível em: <www.math.uchicago.edu/~may/VIGRE/VIGREREU2011.html>. Acesso em: 15 mai. 2019.

O'CONNOR, J. J.; ROBERTSON, E. F. Biography of Pierre de Fermat. **MacTutor History of Mathematics archive**, St Andrews: School of Mathematics and Statistics of the University of St Andrews, Scotland, 1996. Disponível em: <https://www-history.mcs.st-andrews.ac.uk/Biographies/Fermat.html>. Acesso em: 22 mai. 2019.

ORE, O. **Number Theory and its History**. New York: McGraw-Hill Book Company, 1948.

SANTO, M. A. T. d. E. **Aspectos de duas demonstrações do Pequeno Teorema de Fermat.** 2017. 70 f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional: PROFMAT) — Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, São Paulo, 2017.

SANTOS, J. P. d. O. **Introdução à Teoria dos Números**. 3 ed. Rio de Janeiro: IMPA, 2009.

SERPA, C. Do Pequeno Teorema de Fermat às Famílias Gerais de Congruências. **Gazeta de Matemática**, n. 167, 2012. Disponível em: <www.gazeta.spm.pt/fichaartigo?id=368>. Acesso em: 18 mai. 2019.

SINGH, S. **O Último Teorema de Fermat:** a história do enigma que confundiu as maiores mentes do mundo durante 358 anos / Simon Singh; tradução de Jorge Luiz Calife. - 8ª ed. - Rio de Janeiro: Record, 2001.

TANNERY, P.; HENRY, C. **Oeuvres de Fermat**. Paris: Gauthier-Villars et fils, 1894. v. 2.

TAYLOR, B. **Methodus Incrementorum Directa & Inversa**. Londini: Impensis Gulielmi Innys, 1717.

USPENSKI, J.; HEASLET, M. **Elementary Number Theory**. New York: McGraw-Hill Book Company, 1939.

VIANA, M. Henri Poincaré e a Gênese dos Sistemas Dinâmicos. **VI Simpósio Nacional / Jornadas de Iniciação Científica**, Rio de Janeiro, IMPA, 2012. Disponível em: <www.youtube.com/watch?v=12ibbpfDrHo>. Acesso em: 14 mai. 2019.

YEGNANARAYANAN, V. Graph theory to pure mathematics: Some illustrative examples. **Resonance**, Springer India, in co-publication with Indian Academy of Sciences, v. 10, n. 1, p. 50–59, 2005.

YORGEY, B. Fermat's Little Theorem: proof by group theory. **The Math Less Traveled**, 2017. Disponível em: <www.mathlesstraveled.com/2017/12/21/fermats-little-theorem-proof-by-group-theory/>. Acesso em: 20 mai. 2019.