UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
FACULDADE DE MATEMÁTICA

Juliana Matos do Nascimento

UM TEOREMA DE LAGRANGE

BELÉM - PA

2013

UNIVERSIDADE FEDERAL DO PARÁ

INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS

FACULDADE DE MATEMÁTICA

Juliana Matos do Nascimento

Trabalho de Conclusão de Curso apresentado à Faculdade de Matemática da Universidade Federal do Pará como requisito parcial para obtenção do título de Licenciada Plena em Matemática.

Orientador: Prof. Dr. João Cláudio Brandemberg Quaresma.

BELÉM - PA

2013

CERTIFICADO DE AVALIAÇÃO

JULIANA MATOS DO NASCIMENTO

UM TEOREMA DE LAGRANGE

Trabalho de Conclusão de Curso apresentado à Faculdade de Matemática da Universidade Federal do Pará como requisito parcial para obtenção do título de Licenciada Plena em Matemática, julgado pela seguinte banca examinadora:

____

Orientador : Prof. Dr. João Cláudio Brandemberg Quaresma.
Faculdade de Matemática, UFPA

____

Prof. Msc. Adam Oliveira da Silva
Faculdade de Matemática, UFPA

____

Prof. Dr^{a}. Celsa Hermínia de Melo Maranhão
Faculdade de Matemática, UFPA

DATA DA AVALIAÇÃO: _____ /_____ /______

CONCEITO: ____________________________

À Andréa Filgueiras Matos, a razão do meu viver.

Agradecimentos

Agradeço primeiramente à Andréa, minha mãe, por todo seu amor, dedicação e por sempre me dar o apoio necessário para que eu continuasse no curso, mesmo quando não havia mais forças e nem vontade para seguir em frente. Ao Hermes Matos, meu irmão querido e amado, por alegrar a minha vida. Ao Vicente Azulay, meu pai, por ser um bom pai. A todos os meus parentes que direta ou indiretamente contribuíram com a minha educação, em especial às minhas avós Marialba Matos e Júlia Azulay, minha tia Alcéia Matos e aos meus padrinhos Walter Azulay e Ana Helena.

Agradeço ao meu orientador, João Cláudio Brandemberg, pela escolha do tema, por todas as suas valiosas contribuições para a conclusão deste trabalho, por sua compreensão e serenidade, mesmo nos momentos de maior tensão, tornando esta experiência praticamente tranquila.

Aos professores Adam Silva e Celsa Maranhão, por participarem da banca deste trabalho e por suas contribuições.

À esta instituição por me proporcionar um ensino de qualidade através de seus grandes mestres, contribuindo também para o meu desenvolvimento pessoal.

À Rosinha Souza por sempre ser uma boa amiga. Às pessoas que tornaram minha passagem no curso de Matemática mais divertida e amena: Elisangela Samara, por sempre se dispor a ajudar, não somente na elaboração deste trabalho, mas com uma conversa animada ou visitas em minha casa. Helen Rodrigues, por sua ajuda nos trabalhos e por sua companhia agradável. Ao meu ex-namorado Igor Coimbra, por toda a ajuda prestada no começo da nossa amizade e durante o período de namoro e ao Ubirajara Nascimento, Bruna Nascimento e Jéssica Sirotheau.

Aos meus cachorrinhos Rex, Dudu, os gatos Cheirosa e Lorinho, pelas madrugadas em claro ao meu lado.

Resumo

Consiste em apresentar a demonstração do Teorema de Lagrange para a representação de inteiros positivos como soma de quatro quadrados inteiros, seguido de sua biografia, na qual inclui suas etapas de matemático a conde, além de abordar dois temas que auxiliaram na demonstração do teorema principal. Tais temas são: a representação de inteiros positivos como soma de dois e de três quadrados inteiros. A escolha do tema deve-se principalmente pelo fato de buscar mostrar a importância de Lagrange e suas contribuições para o desenvolvimento da Teoria dos Números, além de ter sido co-criador do Cálculo das Variações de Euler. O problema principal, presente na maior parte do trabalho, é encontrar soluções inteiras para equações diofantinas que caracterizam soma de dois, três e quatro quadrados e também mostrar as condições necessárias para que um número inteiro possa ser escrito como soma de dois e de três quadrados inteiros. Os métodos utilizados para a demonstração do Teorema de Lagrange foram as abordagens dos dois temas citados e a exposição dos teoremas referente a estes temas, além da utilização de identidades descobertas por Euler que foram de grande valia para que Lagrange concluísse sua demonstração.

Palavras-chave: Teoria dos Números - Soma de quadrados - Lagrange

Conteúdo

Introdução

Este trabalho surgiu através da vontade de obter maior conhecimento acerca das obras e da vida de um dos maiores matemáticos do século XVIII, juntamente com a ideia de expor uma de suas várias contribuições à matemática, mais especificamente, à Teoria dos Números. O Teorema de Lagrange leva o seu nome por ter sido o primeiro a provar que qualquer inteiro positivo pode ser expresso como soma de quatro quadrados inteiros. Enunciado por Bachet, em 1621 e quinze anos após "provado"por Fermat, que não publicou sua demonstração. Finalmente, em 1770, Lagrange publica a primeira demonstração baseada em um dos trabalhos de seu grande mestre: Euler.

Os conceitos que abordaremos são os da teoria dos números. Utilizaremos, principalmente, noções de congruência e divisibilidade em conjunto com algumas noções de resíduos quadráticos, justamente com o intuito de estimular o leitor a conhecer e a investigar mais sobre a disciplina Teoria dos Números.

O trabalho é dividido em três capítulos: O primeiro é composto da biografia de Joseph Louis Lagrange, onde apresentaremos sua trajetória como matemático e citaremos suas principais obras; o segundo trata exclusivamente de representação de inteiros como soma de dois e de três quadrados inteiros e as "características"dos números que podem ser escritos dessas duas formas e o último capítulo é a demonstração do teorema principal. Toda a composição do trabalho é alicerçada em obras de autores referenciados na disciplina Teoria dos Números como David Burton (2005), Emil Grosswald (1985)e na obra *Lagrange. La Elegancia Matemática* de Venancio Pardo Rego (2003).

Capítulo 1

Uma breve biografia de Lagrange

Neste capítulo, seguimos a sequência da obra de Rego (2003).

1.1 A juventude de Lagrange

Joseph Louis Lagrange (1736-1813) nasceu em 25 de janeiro de 1736 em Turim, noroeste da Itália. Fora registrado com o nome Giuseppe Ludovico Lagrangia.

Sua origem francesa veio de seu bisavô parisiense, capitão da cavalaria francesa, que então serviu ao Rei da Sardenha, Carlos Manuel II, onde morou e casou, tornando-se membro da rica família Conti em Turim. A família de Lagrange tinha uma situação financeira favorável. Seu pai, Giuseppe Francesco Ludovico, era tesoureiro do exército sardenho. Casou-se com Teresa Grosso, de família também rica e tiveram onze filhos, dos quais, somente um irmão e Lagrange, o filho mais novo, sobreviveram.

Seu pai perdeu quase toda a fortuna da família em suas especulações financeiras, o que contribuiu para que Lagrange se dedicasse aos estudos, principalmente à matemática.

No mesmo ano do nascimento de Lagrange, o matemático suíço Euler publicou uma obra importante para a física, a *Mechanica sive motus scientia analytice exposita* (Mecânica ou ciência do movimento exposta de modo analítico.

Anos mais tarde, Lagrange e Euler tornaram-se amigos e, assim como Euler, Lagrange também dedicou-se aos estudos das aplicações da análise à mecânica, tornando-se tão reconhecido quanto Euler. Lagrange mostrou interesse pelos trabalhos de Arquimedes e de Euclides. Sua família desejava que seguisse a carreira da docência ou da advocacia, mas ao conhecer uma das obras do astrônomo inglês Edmond Halley (1656-1742) se encantou a ponto de dedicar-se profundamente à matemática e em pouquíssimo tempo, de maneira solitária, conseguiu dominar a análise moderna. Seu primeiro contato com grandes matemáticos como Newton, Leibniz, Bernoulli, Euler e Clairaut foi após ter contato com a obra *Instituzioni analitiche* de Maria Gaetana Agnesi (1718-1799).

Em 1753, inicia suas investigações sobre a análise matemática e a partir daí inicia sua carreira brilhante. No ano seguinte, com 18 anos, estuda o *Methodus* de Euler e o problema dos isoperímetros presente neste livro.

Lagrange desenvolveu um cálculo formal sobre a analogia entre o binômio de Newton e as derivadas sucessivas de um produto de duas funções e a partir daí, fez questão de que chegasse ao conhecimento de Euler, que fazia parte da Academia de Ciências de Berlim, seu feito.

Após a publicação, Lagrange descobriu que seus resultados circulavam entre as correspondências de Joahann Bernoulli e Leibniz o que o aborreceu bastante, principalmente pelo fato de haver possibilidade de desconfiança acerca da verdadeira autoria do trabalho e Euler poderia desconfiar disso.

Mesmo com esses acontecimentos, Lagrange não se intimidou, pelo contrário, empenhou-se ainda mais a fim de que todas as dúvidas sobre a originalidade dos seus trabalhos cessassem e além disso, desejava que suas obras chegassem às mãos de Euler, o grande matemático da época.

Lagrange estudou a obra de Euler *(Methodus Inveniendi Lineas Curvas Maximi Minimive proprietate gaudentes sive solutio problematis isoperimatrici Latissimo Sensu Acceptl)* (1744) que, até então, somente o autor tinha domínio, pois se tratava de um novo ramo da matemática (cálculo das variações, denominada pelo próprio Euler). Ainda aos 18 anos, Lagrange obtém um resultado para o antigo problema da tautócrona (ou isócrona) através de métodos puramente analíticos pois, até então, só haviam resultados geométricos sobre o problema. Além disso, Lagrange se propôs a resolver problemas concretos através dos cálculos variacionais de Euler e a desenvolver um método mais geral e elegante.

No dia 12 de agosto de 1755, Lagrange envia uma carta a Euler com a resolução analítica do problema da isócrona, dando origem ao método variacional, assunto este inserido no cálculo variacional de Euler. O dito trabalho fora publicado anos mais tarde, em 1762, sob o título *Essai d'une nouvelle méthode pour detérminer les máxima et minima* *des formules integráles indéfínies* (Ensaio sobre um método para determinar os máximos e mínimos das funções integrais indefinidas). E aos 19 anos, Lagrange já era considerado o co-fundador do cálculo variacional.

O cálculo variacional de Euler e Lagrange tem aplicação na matemática, física e na economia. Euler ainda tinha algumas limitações nos desenvolvimentos de métodos variacionais, pois tratava-se de um ramo novo na matemática, mas Lagrange pôs fim à essas limitações através de um trabalho com o desenvolvimento do método de Euler de maneira formal e elegante. O dito trabalho fora enviado a Euler e junto dele, a esperança de ser reconhecido por sua originalidade. E isso aconteceu. Euler percebeu a superioridade dos métodos de Lagrange e o incentivou para que desenvolvesse ainda mais seu trabalho.

Após o reconhecimento pelo matemático suíço da genialidade de Lagrange, a sociedade matemática da época também reconheceu sua grande capacidade e seus feitos. Euler sabia reconhecer as qualidades de alguém e, com isso, foi considerado o padrinho de Lagrange, que passou a ganhar notoriedade devido ao apreço do seu mestre. Após seu primeiro grande trabalho, Lagrange se viu atraído a resolver o problema da trajetória descrita por uma partícula sob a ação de uma força central, presente na obra *Methodus inveniendi...* de Euler. O resultado obtido foi equivalente à segunda lei de Newton, com a vantagem de poder trabalhar com um grande sistema de partículas independente de saber ou não as forças que nelas atuam, mas sendo necessário conhecer a energia cinética e potencial.

Esse resultado e seu desenvolvimento, como nos anteriores, fora enviado a Euler que dessa vez não se satisfez em dar somente o reconhecimento a Lagrange, mas tratou de convencer o presidente da Academia de Ciências de Berlim a oferecer uma vaga de matemático a Lagrange na dita Academia. Mesmo com condições de trabalho inferiores às condições que Euler propôs em Berlim, Lagrange recusou a oferta, com o argumento de que deveria amadurecer mais como matemático em Turim e não viver à sombra de seu padrinho Euler.

Com apenas 20 anos, em 2 de setembro de 1753, Lagrange foi eleito membro estrangeiro da Academia de Ciências de Berlim. Com todos esses fatos ocorrendo em sua vida, Lagrange cria uma sociedade científica em Turim que, anos mais tarde, transforma-se na Academia de Ciências de Turim (1783). A Sociedade conta com uma revista editada em francês e em latim denominada *Miscellanea Taurinensia* ou *Melánges*, cuja função era publicar os trabalhos de Lagrange, além de trabalhos de outros matemáticos.

Durante três anos como membro estrangeiro da Academia de Berlim, Lagrange estuda os problemas físicos da propagação do som no ar, o problema da corda vibrante, integração de equações diferenciais em derivadas parciais surgidos a partir desses dois problemas físicos.

1.1.1 O Problema da Corda Vibrante

Por muito tempo, matemáticos como Euler, Bernoulli e D'Alembert estudaram os deslocamentos de uma corda que vibra em função do tempo e da distância. Porém, o jovem Lagrange também se propôs a dedicar-se a esse problema.

Euler e D'Alembert desenvolveram de forma independente suas proezas, mas chegaram aos mesmos resultados: uma equação diferencial em derivadas parciais. Mas D'Alembert encontrou a equação correta da corda vibrante, chamada equação de ondas unidimensional.

Enquanto Daniel Bernoulli, D'Alembert e Euler procuravam definir se eram as funções contínuas, descontínuas, ambas ou uma arbitrária que satisfazem a equação da corda vibrante, Lagrange, em 1759, publica seu trabalho sobre a propagação do som: *Recherches sur la nature et la propagation du son* (Investigações sobre a natureza e a propagação do som), onde faz considerações como as que o ar é um meio elástico e estudou a propagação do som no ar a partir da mecânica dos sistemas de partículas elásticas. Mas mesmo assim, chegou aos mesmos resultados de Euler e D'Alembert, e, além disso, concluiu que qualquer curva inicial satisfaz a equação da corda vibrante, independente da sua continuidade e da sua periodicidade. Seu desenvolvimento da expressão geral da equação da corda vibrante chega próximo da descoberta das Séries de Fourier.

Em meio às controvérsias, Lagrange levou vantagem, pois estreitou sua relação com Euler e passou a se corresponder com D'Alembert, que virou seu melhor amigo.

Aos 23 anos, Lagrange era considerado um grande matemático como os demais de sua época. No seu trabalho *Investigações sobre a natureza...*, contribui para o desenvolvimento das equações de ondas cilíndricas e esféricas.

Após os resultados obtidos sobre a propagação do som no ar, Euler, Lagrange e Bernoulli aplicaram suas teorias à prática. Analisaram os sons de diversos instrumentos nas mais variadas formas geométricas e comprovaram muitos dos resultados obtidos. Algumas equações diferenciais obtidas a partir dos sons dos instrumentos, tinham grau elevado e isso dificultava a integração utilizando somente os conhecimentos da época, dessas equações.

Os trabalhos realizados por Lagrange sobre a propagação do som no ar, foram publicados na edição do seu *Miscellanea*, volume II e depois incorporados na sua obra *Mecânica Analítica.*

1.1.2 O Problema dos Isoperímetros

Nas correspondências entre Euler e Lagrange, um dos problemas que apareciam com frequência era o dos isoperímetros. Euler conseguiu demonstrar o problema, mas Lagrange se propôs a resolvê-lo de forma analítica, já que Euler envolveu na sua resolução conceitos geométricos e analíticos, e enviou seus resultados a Euler, que se mostrou satisfeito por saber que alguém, além dele, pôde solucionar um problema que há tempos ele trabalhava e ainda afirmou que só publicaria seus resultados quando Lagrange publicasse os seus, para que também obtivesse o mérito que provavelmente teriam.

Após a publicação de Lagrange, Euler publicou seus resultados e, além disso, mencionou Lagrange como peça principal para completar a solução do problema dos isoperímetros.

Lagrange já havia se tornado conhecido no mundo científico de Turim, mas sua situação permanecia a mesma. Seus 5 anos de trabalho como matemático foram proporcionais às horas sem sono devido a tanta dedicação. Sua má alimentação contribuiria para que no futuro tivesse complicações.

Um outro importante trabalho desenvolvido por Lagrange foi o de encontrar a superfície com área mínima, onde suas fronteiras encontram-se fixas. Euler encontrou um caso especial de superfície mínima: a catenóide.

Lagrange desenvolveu uma equação para determinar a superfície mínima que foi nomeada equação das superfícies mínimas de Lagrange, publicado no volume II do *Miscellanea Taurinensia.*

Entre 1760 e 1766, Lagrange dedica-se ao estudo da teoria das equações diferenciais e à mecânica celeste. Neste último tema, as ideias originais são de Euler, publicadas no seu artigo *Princípios do movimento dos fluidos* (1752), onde o objetivo principal do artigo era encontrar a equação do fluxo uniforme de um fluido ideal.

1.1.3 Lagrange e as Equações Diferenciais

As equações diferenciais surgiram no século XVII. Ao resolver problemas de física, Newton, Huygens e os irmãos Bernoulli, já faziam uso das equações diferenciais que, na primeira metade do século XVIII, virou uma disciplina matemática. Euler já tinha bastante domínio dessa disciplina e em uma de suas obras, resolveu equações diferenciais lineares homogêneas de grau n com coeficientes constantes e, em um trabalho posterior, desenvolveu mais técnicas para resolver equações diferenciais ordinárias.

Dando continuidade ao trabalho de Euler, Lagrange estudou equações com coeficientes variáveis e descobriu que a solução de uma equação linear homogênea com coeficientes variáveis, é uma soma de soluções independentes cujas soluções dependentes são, cada uma delas, multiplicadas por uma constante arbitrária.

Dentre seus importantes trabalhos, dois artigos sobre mecânica celeste, onde são utilizadas aplicações para as leis da gravitação universal, foram premiados na Academia de Ciências de Paris. O primeiro prêmio, recebido em 1764, foi devido ao seu artigo que tratava sobre a pequena oscilação da Lua em relação ao alinhamento com a Terra. O segundo prêmio recebido, em 1762, fora oferecido através de um concurso para quem conseguisse resolver o problema dos três corpos que consiste em analisar perturbações oscilatórias de um astro relacionadas com a atração entre outros corpos celestes. O princípio utilizado em seu primeiro trabalho (Princípio da Mínima Ação), foi utilizado como base para sua obra posterior, *Mecânica Analítica*.

Após dez anos de trabalho, Lagrange pôde finalmente respirar os ares de Paris e Londres e descansar, com seus gastos custeados pelo Rei da Sardenha.

Em Paris, Lagrange foi acolhido por diversos matemáticos e filósofos iluministas como, Diderot, Voltaire, Clairaut, Condocert e Marie, mas Lagrange conheceu pessoalmente quem ele já esperava há algum tempo: D'Alembert. Desse momento, até a morte de D'Alembert, houve uma grande amizade entre os dois matemáticos. Lagrange tinha, além de Euler, D'Alembert como seu admirador.

A grande influência e apoio que Lagrange teve, seja no mundo científico, seja no mundo social ou político, foi imprescindível para que se tornasse um dos maiores matemáticos da história e tudo isso ocorreu também por causa da sua personalidade amável, embora não concordasse com algumas opiniões relacionadas à política ou religião, mas sempre manteve o respeito em seus pronunciamentos sobre esses assuntos.

Foi em Paris que suas enfermidades apareceram, em consequência da sua má alimentação e das noites em claro. Lagrange teve um problema biliar e recebeu os cuidados de D'Alembert. Após melhorar, Lagrange partiu de volta à Turim, mas antes passou por Genebra.

Algum tempo depois, a Academia de Ciências de Paris lançou outro problema sobre corpos celestes com a intenção de que, justamente Lagrange, conseguisse resolvê-lo, já que o matemático estava familiarizado com o tema. E foi o que realmente aconteceu.

O desafio consistia em encontrar uma solução para o problema dos n corpos, para $n = 6$ e tratava sobre a atração entre os quatro satélites de Júpiter, pois naquela época não tinha conhecimento que Júpiter possui mais de vinte satélites. A grande questão explorada é o fato de que o sistema de gravitação de Júpiter pode ser comparado com o sistema solar, de uma forma reduzida. Lagrange chegou a resultados satisfatórios, embora não tenha conseguido resolver o problema para $n = 6$.

Os cinco prêmios recebidos da Academia de Ciências de Paris foram referentes à mecânica celeste. Seus trabalhos sobre mecânica celeste e equações diferenciais foram publicados no Volume III do *Miscellanea Taurinensia*.

Em 1755, Lagrange tomou conhecimento, através de D'Alembert, que o Rei Frederico estava disposto a substituir Euler por D'Alembert no cargo de diretor da seção de matemática da Academia de Ciências de Berlim, mas o matemático não aceitou a oferta, alegando que os conhecimentos de Euler eram insubstituíveis, mas falou ao rei sobre Lagrange e Frederico ofereceu o posto a Lagrange que também recusou, pois jamais passaria por cima do mestre que tanto lhe ajudou.

Algumas semanas mais tarde, Euler pediu demissão do seu posto de diretor mas, antes disso, recomendou ao rei que pusesse Lagrange no seu lugar e o rei aceitou, enviando novamente a proposta ao matemático, que dessa vez aceitou o convite.

Em outubro, Lagrange chega à Berlim e dois meses depois, no dia 6 de novembro de 1766, toma posse de seu cargo.

1.2 A Passagem por Berlim

O rei Frederico recebeu Lagrange com muito entusiasmo, o que não foi motivo para o matemático de Turim se empolgar, pois Lagrange já tinha conhecimento do tratamento concedido a Euler após o rei tomar antipatia pelo "ciclope suíço", apelido recebido pelo rei após Euler perder a visão de um dos olhos antes de ficar totalmente cego. Euler considerava a Rússia como seu país de adoção e partiu para a corte rival de Catarina II, na Rússia.

O rei Frederico II tinha influência francesa em sua educação, e simpatizava com os ideais filosóficos. Tornou-se amigo de Diderot e Voltaire, além de D'Alembert.

As funções de Lagrange eram a leitura de uma memória mensal publicadas de tempos em tempos no Compêndio da Academia de Berlim, além da direção dos trabalhos matemáticos produzidos na Academia. Como não tinha função docente, a etapa em Berlim fora a mais produtiva em toda a sua carreira matemática, chegando a produzir mais de cento e cinquenta memórias, pois passou também a ter uma vida mais regrada com horários fixos para produzir seus trabalhos e para alimentar-se regularmente.

Onze meses após sua chegada em Berlim, casou-se com sua prima Vittoria Conti, dividindo opiniões, pois acreditava-se que seu matrimônio influenciaria na produção de suas obras. Mas, segundo o próprio matemático, seu casamento era apenas por conveniência e para receber cuidados de uma esposa dedicada.

1.2.1 Lagrange e a Teoria dos Números

Lagrange teve um papel muito importante na Teoria dos Números, pois resolveu vários teoremas que ainda estavam em aberto por anos, alguns até por séculos, como por exemplo, a equação de Pell, que Euler, por muito tempo, havia tentando resolver:

$$x^2 - Ay^2 = 1$$

com $A, x, y \in \mathbb{Z}, y \neq 0, A \neq b^2$ e $b \in \mathbb{Z}$, utilizando o algoritmo das frações contínuas. Lagrange agradeceu os esforços do matemático suíço que, sem eles, seria difícil chegar a uma solução do problema.

Em 1770, Euler lança sua obra *Álgebra* que, segundo Lagrange, a única coisa interessante presente na obra é um tratado sobre equações diofantinas. Após a tradução, que estava em alemão, Lagrange inseriu notas na obra que continham demonstrações interessantes sobre dois teoremas que ele seria o primeiro a provar.

Uma dessas demonstrações, presente em seu *Memórias de Berlim* (1770), consistia em encontrar as soluções inteiras da equação diofantina [1]

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2 \tag{1.1}$$

que Euler tentou provar sem sucesso.

O segundo teorema, cuja demonstração foi publicada em uma de suas memórias da Academia de Ciências de Berlim, diz o seguinte:

Teorema 1.2.1. *Se p é um primo, então $(p-1)!+1$ é múltiplo de p.*[2]

Em 17775, Lagrange funda a teoria das formas quadráticas binárias. Outros importantes resultados demonstrados por Lagrange foram:

Teorema 1.2.2. *Uma congruência de grau m*

$$Ax^m + Bx^{m-1} + Cx^{m-2} + \cdots + Mx + N \equiv 0 (mod p)$$

onde p é primo e $(A,p)=1$, não pode ser resolvida por mais de m maneiras diferentes ou não pode ter mais de m raízes incongruentes módulo p.

e

Teorema 1.2.3. *Se um número pode ser representado por uma forma binária, por exemplo*

$$N = ax^2 + bxy + cy^2$$

Então N pode ser representado por formas equivalentes por meio de mudança de variáveis da forma

$$x = \alpha x' + \beta y'$$
$$y = \chi x' + \delta y'$$

Em Berlim, seu último trabalho em teoria dos números foi o artigo intitulado: *Sobre alguns problemas de análise diofantina* (1771). Anos mais tarde, já em Paris, publicou o

[1] A equação (1.1) será o teorema principal demonstrado neste trabalho.

[2] Enunciado pela primeira vez por Edward Waring (1734-1793), cuja demonstração encontra-se no livro [4] de José Plínio de Oliveira dos Santos.

trabalho sobre frações contínuas: *Ensaio de análise numérica sobre a transformação de frações.*

1.2.2 Análise Algébrica

Entre 1767 e 1777, Lagrange estudou problemas que envolvessem resolução de equações. Seus trabalhos neste período foram: um ensaio sobre o melhoramento do método de Cramer para eliminação de parâmetros na resolução de sistemas de equações lineares (1769), *Sobre a resolução de equações numéricas* (1769), *Apêndice à memória sobre a resolução de equações numéricas* (1770), neste último, verifica que somente os números irracionais quadráticos podem ser representados por frações contínuas periódicas. Nas duas outras obras, Lagrange aplica o método das frações contínuas. Também em 1770, Lagrange lança o trabalho *Novo método para resolver as equações literais por meio de séries*, sugerido pelo matemático Lambert, já que havia dado início a um trabalho com o mesmo tema.

Em sua memória, Lagrange analisa as soluções de equações de grau m, tal que $2 \leqslant m \leqslant 4$, $m \in \mathbb{Z}$, utilizando métodos de resoluções por meio de radicais e também afirmou que equações de grau n, com $n > 4$. $n \in \mathbb{Z}$, são impossíveis de resolver através de radicais.

Embora equações de grau superior a quatro não possam ser solúveis através de radicais, muitas equações de grau arbitrário podem ser resolvidas dessa maneira. Cabia agora investigar as condições para que uma equação pudesse ou não ser resolvida por meio de radicais. Através dos estudos dessas condições, que Lagrange pôde disseminar a teoria dos grupos de permutação ou grupos de substituição.

Lagrange ainda publicou mais duas memórias sobre resolução de equações algébricas. A primeira, *Sobre a forma das raízes imaginárias das equações* (1773), tratava sobre sua demonstração (dada primeiramente por Euler e D'Alembert) sobre a equação polinomial $f(x) = 0$ com coeficientes reais ou complexos, cuja equação admite pelo menos uma raiz real ou complexa, mas Lagrange não conseguiu dar uma prova completa. Sua segunda memória,*Investigações sobre a determinação do número de raízes imaginárias nas equações literais*, era um complemento da primeira.

1.2.3 Mecânica Celeste

Durante sua vida em Berlim, Lagrange também publicou memórias no campo da mecânica celeste, além de participar de premiações da Academia de Ciência de Paris sobre este tema.

Seu primeiro trabalho em Berlim, nesta área, foi *Investigações sobre o movimento de um corpo que é atraído para dois centros fixos* (1767), constituído por uma generalização dos trabalhos de Euler referentes à mecânica celeste.

Ainda em 1767, Lagrange foi convidado a participar de um concurso na Academia de Ciências de Paris, que aconteceria no ano seguinte. D'Alembert o convidou, pois tinha conhecimento que se tratava de um assunto que Lagrange dominava (A teoria da Lua), mas Lagrange não aceitou, pois Euler também concorreria ao prêmio e o matemático de Turim não queria concorrer com seu mestre.

No concurso de 1770, Lagrange também não concorreu, devido a uma enfermidade, mas publicou um trabalho intitulado *Memória sobre a passagem de Vênus em 3 de junho de 1769*, que envolve astronomia pura. Já em 1772, participa do concurso com o trabalho: *Ensaio sobre o problema dos três corpos*, inovador pois, até então, só havia conhecimento sobre os resultados do problema dos dois corpos. Mesmo não mostrando soluções gerais para o problema dos três corpos, Lagrange obteve resultados particulares muito interessantes que serviram de base para estudos futuros por George William Hill (1838-1924) e Jules-Henri Poincaré (1854-1912). Por decisão unânime, Lagrange e Euler ganham o prêmio de cinco mil libras, cada um.

Em 1774, a Academia de Ciências de Paris ofereceu outra premiação. A problemática era: *A possibilidade de explicação sobre a equação secular da Lua pela atração de todos os corpos celestes ou pelo efeito da não-esfericidade da Terra e da Lua*. Lagrange participou com o trabalho: *Sobre a equação secular da Lua*, que lhe rendeu outro prêmio.

Entre 1776 e 1782, as memórias de Lagrange sobre o estudo da mecânica celeste, estiveram presentes em artigos da Academia de Ciências de Paris e na Academia de Ciências de Berlim.

Em 1780, participa de mais outra premiação com o trabalho *Investigações sobre a teoria das perturbações que os cometas podem sofrer pela ação dos planetas*, conseguindo o prêmio duplo de quatro mil libras. Esta foi sua última participação em premiações, pois não voltaria mais a concorrer em outro concurso.

Em 1782, publica uma obra *Teoria da oscilação da Lua e de outros fenômenos que dependem da forma esférica do planeta*, sobre a oscilação da Lua, que na verdade é uma edição melhorada de sua primeira obra publicada ainda em Turim, sobre o assunto referente.

1.2.4 Equações Diferenciais

Além dos problemas presentes em mecânica geral e mecânica celeste, existiam os problemas solúveis através de equações diferenciais. Para estes problemas, Lagrange utilizava alguns métodos de resolução, até perceber que alguns problemas físicos necessitavam de métodos mais específicos de resolução utilizando equações diferenciais. Lagrange e Euler se propuseram a pesquisar profundamente o estudo das equações diferenciais que matemáticos do século seguinte deram continuidade. Suas produções em Berlim sobre este tema ocorreram entre 1768 e 1787.

Em 1783, foi criada a Academia de Ciências de Turim e a revista *Recueil de l'Academia*, inspiradas nos trabalhos de Lagrange durante sua etapa em Turim: a Sociedade Científica de Turim e a *Miscellanea Taurinensia*. Na Academia de Ciências de Turim, Lagrange foi nomeado presidente de honra, devido à todas suas conquistas no meio científico da Europa e como agradecimento, Lagrange enviou um trabalho sobre cálculo diferencial para ser publicado na *Recueil de l'Academia*.

Seus trabalhos foram precursores de estudos que formaram hoje as equações elípticas.

Em 1773, Lagrange publica um trabalho *Sobre a integração das equações em derivadas parciais de primeira ordem*, sendo complementado com o trabalho publicado em 1779, *Em relação à diferentes problemas de análise relacionados à teoria das integrais particulares*, onde mostra um método encontrado para integrar equações lineares em derivadas parciais de primeira ordem. Seu outro trabalho de 1785, *Método geral para integrar equações não-lineares em derivadas parciais de primeira ordem*, consiste em reduzir o problema de integrar a equação não linear do tipo

$$q - Q(x, y, z, p) = 0$$

ao de integrar uma equação linear do tipo

$$-Q_p\frac{\partial p}{\partial x}+\frac{\partial p}{\partial y}+(Q-pQ_p)\frac{\partial p}{\partial z}-Q_x-pQ_z=0$$

Estes trabalhos podem ser considerados como o estudo mais aprofundado do século XVIII sobre equações diferenciais de primeira ordem em derivadas parciais.

Ainda em Berlim, Lagrange publica trabalhos sobre equações diferenciais ordinárias de ordem superior, onde mostra métodos de variação de parâmetros ou variação de constantes referentes ao estudo das perturbações dos movimentos dos planetas.

Seus dois últimos trabalhos durante a passagem por Berlim, coincidiram com a redação da sua grande obra *Mecânica Analítica*. O primeiro trabalho consiste num estudo mais aprofundado sobre mecânica dos fluidos e o segundo foi uma continuação do trabalho publicado em Turim sobre transmissão de som e equações de ondas. Depois de Newton, Lagrange foi um dos maiores matemáticos a estudar com afinco temas sobre mecânica.

Seu interesse por geometria era pouco, porém, seu amigo Monge conseguiu encantá-lo com sua Geometria Diferencial. Em 1775, publicou um artigo *Soluções analíticas de alguns problemas sobre as pirâmides triangulares*, onde as resoluções utilizadas constituem hoje a álgebra pura, como os determinantes, quadrado de um determinante, matriz ortogonal, entre outros.

No dia 15 de setembro de 1782, Lagrange termina de redigir o seu *Mecânica Analítica*.

Entre cartas a D'Alembert e Euler, é possível perceber a preocupação de Lagrange em relação ao futuro de suas produções pois seus estudos já haviam sido bastante explorados e, caso não se criassem novas vertentes matemáticas, seu trabalho teria que ser abandonado.

Lagrange já estava com 45 anos e seus níveis de produção científica decaíram não só pela idade, mas pelo fato de sua esposa encontrar-se gravemente enferma. Embora não muito empolgado no início com o seu casamento com Vittoria, Lagrange passou a sentir carinho pela esposa com quem conviveu por 13 anos. Em meados de 1783, Vittoria morre e Lagrange entra em depressão, afastando-se de todos. No mesmo ano, Lagrange sofre duas perdas irreparáveis. No dia 18 de setembro, morre Euler, seu mestre e amigo (mesmo sem nunca conhecê-lo pessoalmente). No dia 29 de outubro, morre seu amigo D'Alembert que antes de morrer encoraja Lagrange a não desistir de seu trabalho.

Euler e Lagrange construíam a parte mais importante da matemática do século XVIII, além de desenvolverem as obras de Newton.

Após isso, Lagrange recebeu propostas, inclusive da Academia de Ciências de Turim, para sair de Berlim, mas recusou o convite, pois sentia muita gratidão por Frederico II, que sempre lhe tratou bem e valorizou seu trabalho, além do mais, Lagrange vivia em um dos maiores berços da ciência da época. Mas em agosto de 1786, Frederico II morre, deixando seu sobrinho Guilherme II no poder. Guilherme não se importava com a evolução da ciência, além de ter antipatia por qualquer assunto relacionado à França.

Dessa vez Lagrange se viu fortemente tentado a sair de Berlim e assim o fez, quando recebeu a proposta para um cargo na Academia de Ciências de Paris do rei Luís XVI. Para Lagrange, a situação seria proveitosa, pois a Academia de Ciências de Paris era referência da ciência européia, teria também a companhia de seus amigos Laplace e Legendre. Outro motivo seria a sua descendência francesa, da qual Lagrange sempre deixou claro.

Embora alguns cientistas da época tenham se prejudicado em razão da situação que ocorria na Prússia, o mesmo não aconteceu com Lagrange que teve direito a uma pensão até o ano de 1792, pois houve mudanças no cenário político da Prússia. No entanto, o contrato firmado com a Academia de Ciências de Paris se manteve-se até a sua morte.

No dia 18 de maio de 1787, Lagrange parte rumo à Paris, levando lembranças dos vinte e um anos de trabalho realizados em Berlim.

1.3 O Conde Lagrange

Em julho de 1787, Lagrange chega em Paris e no mesmo mês, no dia 29, ingressou como veterano aposentado da Academia de Ciências, já que, desde maio de 1772, é membro estrangeiro.

Lagrange estava totalmente diferente da época de sua primeira visita em Paris. Encontrava-se triste. Dos amigos presentes em sua primeira visita, somente Marie e Condocert estavam vivos. Pôde conhecer pessoalmente seus amigos de correspondência Legendre e Laplace e fez amizade com Lavoisier, Carnot, Coloumb, Delambre e Monge.

Lavoisier e a rainha Antonieta cuidaram de Lagrange e mantiveram-no longe de alvoroços, já que encontrava-se triste e desmotivado até mesmo com a matemática.

Em sua mala trouxe a obra *Mecânica Analítica* a fim de editá-la. A edição foi feita por Joseph-François Marie (1738-1801) e lançada no começo de 1788, sendo muito elogiada.

Mecânica Analítica é dividida em duas partes: *Estática* e *Dinâmica* e em cada uma destas duas partes há subseções sobre corpos sólidos e fluidos. A obra consiste em resolver questões presentes na mecânica através de métodos puramente analíticos, utilizando somente conceitos algébricos e além disso, Lagrange desenvolveu equações para a resolução dos problemas presentes.

Até então, não havia um princípio geral da mecânica sobre um número qualquer de forças em um sistema mecânico qualquer, mas Lagrange conseguiu este feito com o seu *Princípio das Velocidades Virtuais* ou *Princípio dos Deslocamentos Virtuais*, enunciado pela primeira vez por Johann Bernoulli, em 1717.

Durante os embates políticos que ocorriam na França durante o século XVIII, Lavoisier e Condocert morrem.

Lagrange foi nomeado presidente da Comissão para a Unificação das Medidas, impulsionando a adoção do sistema métrico decimal, contrariando os defensores do sistema de base 12.

O astrônomo Pierre-Charles Lemonnier (1715-1799), amigo de Lagrange, tinha uma filha que, ao saber da melancolia do matemático de Turim, se comoveu e o pediu em casamento. No dia 13 de maio de 1792, Renée-Françoise Adélaide Lemonnier (1767-1833) e Lagrange casaram-se, devolvendo a ele a vontade de trabalhar e produzir.

Porém, no dia 21 de janeiro de 1793, Luís XVI e Maria Antonieta no dia 17 de outubro do mesmo ano, foram executados.

No dia 8 de agosto de 1793, a Convenção Nacional exige o fechamento das academias, alegando não haver necessidade de "sábios"e após três meses, Lavoisier e Laplace são mandados embora da Comissão de Pesos e Medidas, mas Lagrange é estranhamente mantido em seu cargo.

No mês seguinte, o Comitê de Bem Estar Público ordenou que estrangeiros de países inimigos fossem deportados, além de terem seus bens apreendidos. Preocupados por Lagrange ter mantido uma grande amizade com o rei Frederico, além de ter mantido uma boa relação com Maria Antonieta, os amigos de Lagrange o propuseram que o mesmo voltasse à Berlim, mas receberam uma resposta negativa. Então, Lavoisier, que tinha influência política, intercede por Lagrange a um dos membros da Comissão do Bem Estar para que o matemático permaneça em seu cargo e seu pedido é aceito.

Infelizmente, Condocert comete suicídio no dia 24 de março de 1794 e Lavoisier, o amigo que tanto lhe ajudou, foi guilhotinado no dia 8 de maio do mesmo ano.

Em julho de 1794, o clima encontra-se mais ameno, devido à morte dos comandantes da época do Terror. As produções científicas voltam a todo vapor.

No dia 30 de outubro de 1794, é criada a *l'École Normale* com a finalidade de proporcionar um ensino uniforme, além de formar professores e mestres.

Lagrange foi designado para desempenhar a função de professor principal e Laplace, professor adjunto.

No dia 11 de março de 1794, foi fundada a *l'École Centrale des Travaux Publics* que, após certo período, foi renomeada para *École Polytechinique*, sendo prestigiada até hoje. Lá, Lagrange ensinou análise até 1799.

Devido a extinção das academias durante a época do Terror, foi criado o Instituto Nacional, em 27 de setembro de 1795, e Lagrange foi nomeado presidente da primeira classe do diretório que envolvia as ciências físicas e matemáticas.

Embora Lagrange não tivesse tanto entusiasmo para a carreira docente, pois estava há mais de trinta anos sem lecionar, ensinava seus alunos de Paris de maneira muito disciplinada.

Suas notas de aula também eram repletas de novas descobertas. Com isso, Lagrange as utilizou para lançar mais um artigo (*As lições elementares sobre matemática distribuídas na l'École Normale*). Um de seus resultados envolvendo aproximação de funções foi o método chamado Interpolador de Lagrange.

No ano de 1797, Lagrange lança seu trabalho *Teoria das Funções Analíticas*, uma versão melhorada do seu trabalho de 1792 com o mesmo tema. Nele, Lagrange desenvolve conceitos sobre teoria das funções contribuindo com seu formalismo algébrico para o cálculo diferencial e integral. Um teorema muito importante presente nesta obra é o **Teorema do Valor Médio** do cálculo diferencial. Em 1801, Lagrange complementa esta obra através de um tratado (*Lições sobre o cálculo de funções*) onde adianta alguns estudos sobre equações diferenciais ordinárias e geometria diferencial.

1.3.1 O Período Napoleônico

Entre 1796 e 1798, Napoleão Bonaparte toma o poder do Norte da Itália das mãos dos austríacos que, até então, a governavam. Os franceses sempre tiveram orgulho por ter Lagrange em seu meio científico e o domínio de Piamonte influenciou mais ainda na permanência de Lagrange no Instituto Nacional e, além disso, foi nomeado professor de análise da l'École Polytechinique.

No dia 9 de novembro de 1799, o general Napoleão toma o poder da França, iniciando uma nova forma de poder: Consulado, de 1799 à 1804 e Império, de 1804 à 1815.

Muitos matemáticos apoiavam Napoleão, pois este era a favor do desenvolvimento das ciências. Monge, Laplace e Fourier, já eram seus amigos de longa data. Para Napoleão, Lagrange era considerado a "mais altas das pirâmides das ciências matemáticas", além de oferecer ao matemático sua mais sincera amizade e respeito.

Durante a última década de vida de Lagrange, suas produções diminuíram. Seus dois últimos trabalhos foram uma segunda edição do *Mecânica Analítica* publicada em 1811 e o *Tratado sobre resolução das equações numéricas de grau arbitrário* (uma compilação de suas obras dos anos de 1769 e 1770 sobre o mesmo tema), publicada em 1798.

Em 1808, o imperador Napoleão nomeia Lagrange conde do império. Além de Lagrange, Monge, Laplace e Carnot foram nomeados para o mesmo cargo.

Lagrange já tinha mais de 70 anos, sem filhos, mas com sucessores na matemática, como Cauchy e Gauss. Este último correspondia-se através de cartas com Lagrange. Já Cauchy teve a oportunidade de conhecer Lagrange pessoalmente.

Em meados de abril de 1813, Lagrange encontra-se enfermo e recebe a última visita de seus amigos e dois dias após essa visita, no dia 10 de abril de 1813, morre, aos 77 anos. Seus restos mortais encontram-se no Panteão ao lado de grandes personagens da história.

Lagrange recebeu homenagens em diversas universidades do reino da Itália, enquanto que no reino da Prússia nada foi feito, devido aos conflitos entre a França.

Capítulo 2

Soma de Dois e de Três Quadrados

Neste capítulo seguimos Burton (2005) e Grosswald (1985).

2.1 Soma de Dois Quadrados

Dado um inteiro $m > 0$, tal que m pode ser representado por

$$m = x^2 + y^2 \tag{2.1}$$

queremos encontrar as soluções inteiras da equação diofantina acima.

Alguns números (quadrados perfeitos) podem ser facilmente verificados como soma de dois quadrados, levando em consideração que o número zero pode ser elevado ao quadrado. Por exemplo:

$$4 = 2^2 + 0^2,\ 9 = 3^2 + 0^2 \text{ e } 16 = 4^2 + 0^2$$

mas números da forma $m = x_1^2 + 0^2$ não são interessantes para mostrarmos, já que recaem na representação de inteiros como um quadrado apenas e outros são clássicos ternos pitagóricos como: $25 = 4^2 + 3^2$, $10^2 = 6^2 + 8^2$ e $13^2 = 12^2 + 5^2$.

2.1.1 Algumas evidências sobre soma de dois quadrados inteiros

Determinar se a equação diofantina (2.1) tem solução não será uma tarefa simples, para isso, reuniremos uma série de lemas e teoremas para que saibamos identificar quais números inteiros positivos podem ser representados como soma de dois quadrados e como encontrar suas soluções inteiras para os termos x e y.

Um lema importante mostrado por Diofanto (325-409 a.C) é o seguinte:

Lema 2.1.1.

$$(a^2+b^2)\cdot(c^2+d^2) = (ac+bd)^2+(ad-bc)^2 = (ac-bd)^2+(ad+bc)^2 \qquad (2.2)$$

Demonstração. $(a^2+b^2)\cdot(c^2+d^2) = a^2c^2+a^2d^2+b^2c^2+b^2d^2 = a^2c^2+2abcd+b^2d^2+a^2d^2-2abcd+b^2c^2 = (ac+bd)^2+(ad-bc) = (ac-bd)^2+(ad+bc)^2$ □

A identidade (2.2) nos mostra que dados $m = a^2+b^2$ e $n = c^2+d^2$, se dois números inteiros positivos são representados como soma de dois quadrados, então o seu produto também será uma soma de dois quadrados.

Por exemplo,

$$5 = 2^2+1^2$$

e

$$13 = 3^2+2^2$$

$$\begin{aligned}
65 = 5\cdot 13 &= (2^2+1^2)\cdot(3^2+2^2)\\
&= (2\cdot 3+1\cdot 2)^2+(2\cdot 2-1\cdot 3)^2\\
&= (6+2)^2+(4-3)^2\\
&= 8^2+1^2\\
&= (2\cdot 3-1\cdot 2)^2+(2\cdot 2+1\cdot 3)^2\\
&= (6-2)^2+(4+3)^2\\
&= 4^2+7^2
\end{aligned}$$

Muitos matemáticos como Mohamed Ben Alhocain (Séc. X), Leonardo de Pisa (conhecido como Fibonacci, 1175-1230), Vieta (1540-1603) e Xylander (Séc. XVI) estudaram o problema (2.1). Bachet (1581-1638) também fez algumas observações sobre o referido problema, mas quem aparentemente declarou condições corretas e suficientes para a solubilidade em números inteiros da equação diofantina $m = x^2+y^2$ foi Girard (1595-1632).

Tais condições são:

- m tem que ser um quadrado (quando $m^2 = m^2 + 0^2$);
- ou um primo $p \equiv 1(mod \quad 4)$;
- ou um produto de tais números (evidente em (2.2));

Exemplo: $4 \cdot 5 = 20 = (2^2 + 0^2) \cdot (2^2 + 1^2) = 4^2 + 2^2$.

Podemos perceber que a declaração principal de Girard e que queremos mostrar é a de que um primo p ímpar só pode ser representado como soma de dois quadrados se, e somente se, $p \equiv 1(mod \quad 4)$.

Vejamos o exemplo do número $17 = 4^2 + 1^2$ que é um primo da forma $p = 4k + 1$, e 11 que não pode ser expresso como soma de dois quadrados, pois não satisfaz a condição estabelecida.

Provavelmente de forma independente, Fermat (1601-1665) também fez uma afirmação sobre representação de inteiros como soma de dois quadrados. A condição seria que se m é da forma $m = 4k + 1$, então, quando dividido pelo seu maior fator, o quociente não poderia conter qualquer primo $q \equiv 3(mod \quad 4)$. Embora Fermat tenha afirmado em suas cartas a Descartes e Mersenne que possuía uma "prova irrefutável", nunca houve nenhuma publicação de sua autoria de uma demonstração sobre esta afirmação.

2.1.2 Os teoremas necessários

Segundo David Burton (2005) e Emil Grosswald (1985), são necessários alguns resultados para verificarmos se um inteiro positivo pode ou não ser expresso como soma de dois quadrados.

Teorema 2.1.2. *Se $n \equiv 3(mod \quad 4)$, tal que $n \in \mathbb{Z}_+^*$, então não existem inteiros a e b, tais que $n = a^2 + b^2$.*

Demonstração. Seja a um inteiro qualquer. Temos que $a = 2k$ ou $a = 2k - 1$ e isso implica que $a^2 = 4k^2$ ou $a^2 = 4(k^2 - k) + 1$, ou seja, $a^2 \equiv 0(mod \quad 4)$ ou $a^2 \equiv 1(mod \quad 4)$, logo, para qualquer inteiro b, temos que $a^2 + b^2 \equiv 0, 1$ ou $2(mod \quad 4)$. O que nos faz concluir que nenhum inteiro que é representado como soma de dois quadrados é da forma $4k + 3$. □

Agora provaremos a declaração de Girard, que diz que qualquer primo p só pode ser representado como soma de dois quadrados se $p \equiv 1 (mod \quad 4)$, para isso, teremos que provar primeiramente um lema do matemático norueguês Axel Thue (1863-1922) e este lema necessita do Princípio da Casa dos Pombos ou Princípio da Gaveta de Dirichlet (1805-1859).

Definição (Dirichlet)**.** *Princípio da Casa dos Pombos ou Princípio da Gaveta: Dados n objetos e m gavetas, tal que $n > m$, então se colocarmos os n objetos nas m gavetas, pelo menos uma gaveta conterá mais de um objeto.*

Em termos mais matemáticos, o princípio afirma que se um conjunto n é a união de m subconjuntos e se $n > m$, então um subconjunto tem mais de um elemento.

Lema 2.1.3 (Lema de Thue)**.** *Sejam $a, p \in \mathbb{Z}_+$ e $(a, p) = 1$, então a congruência $ax \equiv y (mod \quad p)$ admite uma solução x_0, y_0, tal que*

$$\begin{cases} 0 < |x_0| < \sqrt{p} \\ 0 < |y_0| < \sqrt{p} \end{cases}$$

Demonstração. Seja $k = \lfloor \sqrt{p} \rfloor + 1$ e considere o conjunto de inteiros
$S = \{ax - y | 0 \leq x \leq k - 1, 0 \leq y \leq k - 1\}$

Como $ax - y$ assume $k^2 > p$ possíveis valores, pois $k > \sqrt{p}$, o Princípio da Casa dos Pombos garante que pelo menos dois membros de S devem ser congruentes módulo p e digamos que esses números sejam $ax_1 - y_1$ e $ax_2 - y_2$. Então
$ax_1 - y_1 \equiv ax_2 - y_2 (mod \quad p) \Leftrightarrow a(x_1 - x_2) \equiv y_1 - y_2 (mod \quad p)$.

Seja $x_0 = x_1 - x_2$ e $y_0 = y_1 - y_2$, segue que x_0 e y_0 fornecem uma solução para a congruência $ax \equiv y (mod \quad p)$. Se $x_1 = x_2$, então $y_1 - y_2$ será divisível por p, o que implica $y_1 = y_2$, mas (x_1, y_1) e (x_2, y_2) são diferentes, uma contradição. Se $y_1 = y_2$ então $a(x_1 - x_2)$ será divisível por p, o que também é uma contradição, pois a e p são primos entre si, caso não fossem, p dividiria $(x_1 - x_2)$ e $x_1 = x_2$, o que não pode acontecer. Logo

$$\begin{cases} 0 < |x_0| \leq k - 1 < \sqrt{p} \\ 0 < |y_0| \leq k - 1 < \sqrt{p} \end{cases}$$

(BURTON, 2005) □

Com estes resultados, vamos demonstrar o Teorema de Girard, embora tal resultado muitas vezes seja referido como teorema de Fermat, mas a primeira prova foi dada por Euler.

Teorema 2.1.4 (Girard, Euler)**.** *Um número p primo e ímpar, é expresso como uma soma de dois quadrados se, e somente se,* $p \equiv 1(mod \quad 4)$

Demonstração. Suponha que p pode ser escrito como uma soma de dois quadrados, ou seja, $p = a^2 + b^2$. Como p é primo, então $p \nmid a$ e $p \nmid b$. (Se $p \mid a$ então $p \mid b^2$, e assim $p \mid b$ levando à contradição que $p^2 \mid p$). Logo, pela teoria das congruências lineares, existe um inteiro c, tal que:

$$bc \equiv 1(mod \quad p)$$

O que implica dizer que $bc = pk + 1$, onde $k \in \mathbb{Z}$. Módulo p, a relação $(ac)^2 + (bc)^2 = pc^2$ torna-se:

$$\begin{aligned}
(ac)^2 + (bc)^2 &= pc^2 \\
(ac)^2 + (pk+1)^2 &= pc^2 \\
(ac)^2 + (p^2k^2 + 2pk + 1) &= pc^2 \\
(ac)^2 &= pc^2 - (p^2k^2 + 2pk + 1) \\
(ac)^2 &= p(c^2 - pk^2 - 2k) - 1 \\
(ac)^2 &\equiv (-1)(mod \quad p)
\end{aligned}$$

fazendo (-1) um resíduo quadrático de p, no caso em que $p \equiv 1(mod \quad 4)$ o que implica que (utilizando o símbolo de Legendre) $\left(\frac{-1}{p}\right) = 1$. Supondo que a é um inteiro tal que $a^2 \equiv -1(mod \quad p)$, como (-1) é resíduo quadrático, por hipótese, de $p \equiv 1(mod \quad 4)$, então a congruência

$$ax \equiv y(mod \quad p)$$

tem uma solução x_0, y_0, para que a conclusão do lema de Thue seja válida. Temos como resultado

$$-x_0^2 \equiv a^2x_0^2 \equiv (ax_0)^2 \equiv y_0^2(mod \quad p)$$

ou

$$x_0^2 + y_0^2 \equiv 0(mod \quad p)$$

ou seja

$$x_0^2 + y_0^2 = kp$$

para $k \in \mathbb{Z}$ tal que $k \geq 1$. Na medida em que $0 < |x_0| < \sqrt{p}$ e $0 < |y_0| < \sqrt{p}$, obtemos $0 < x_0^2 + y_0^2 < 2p$, o que implica dizer que $k = 1$. Logo, $x_0^2 + y_0^2 = p$, o que conclui a demonstração. $\square$

Considerando $a^2 = (-a)^2$, temos o seguinte corolário:

Corolário 2.1.5. *Qualquer primo p da forma $4k+1$, tem somente uma representação como soma de dois quadrados inteiros, independente da ordem e do sinal dos elementos da soma.*

Demonstração. Suponha que $p = a^2 + b^2 = c^2 + d^2$, onde a, b, c, $d \in \mathbb{Z}_+$. Reescrevemos, $a^2d^2 - b^2c^2 = p(d^2 - b^2) \equiv 0(mod \quad p)$, então $ad \equiv bc(mod \quad p)$ ou $ad \equiv -bc(mod \quad p)$. Como a, b, c e d são todos menores do que $\sqrt{p}$, então

$$ad - bc = 0$$

ou

$$ad + bc = p$$

Se a segunda igualdade se mantém, então, $ac = bd$, pois

$$\begin{aligned} p^2 = (a^2 + b^2)(c^2 + d^2) &= (ad + bc)^2 + (ac - bd)^2 \\ &= p^2 + (ac - bd)^2 \end{aligned}$$

e assim, $ac - bd = 0$. O que resulta que

$$ad = bc \text{ ou } ac = bd$$

Suponha que $ad = bc$, então $a|bc$, com $(a, b) = 1$, o que implica que $a|c$; digamos que $c = ka$. Ou seja, $ad = bc = b(ka)$, logo $d = bk$. Mas

$$p = c^2 + d^2 = k^2a^2 + b^2k^2 = k^2(a^2 + b^2)$$

o que implica que $k = 1$. Neste caso, temos que $a = c$ e $b = d$. Analogamente, utilizando os mesmo argumentos, $ac = bd$ implicará que $a = d$ e $b = c$. Em qualquer um dos casos, as representações do primo p serão idênticas. $\square$

Podemos perceber que qualquer primo $p \equiv 1 (mod \quad 4)$ pode ser escrito como soma de dois quadrados em oito formas. Por exemplo, para $p = 5$, temos:

$$\begin{aligned} 5 &= 2^2 + 1^2 = (-2)^2 + 1^2 = 2^2 + (-1)^2 = (-2)^2 + (-1)^2 \\ &= 1^2 + 2^2 = (-1)^2 + 2^2 = 1^2 + (-2)^2 = (-1)^2 + (-2)^2 \end{aligned}$$

Mas nenhuma dessas oito representações diferem devido à ordem de seus termos ou pelo sinal deles. Logo, as representações não são distintas.

Alguns números, que não são primos, mas da forma $4k+1$ não podem ser representados como soma de dois quadrados inteiros, como o número 21. Para sabermos quais são esses números, veremos mais uma condição.

Teorema 2.1.6. *Seja $m = n_0^2 n$, , onde n é livre de quadrados, ou seja, não existe um primo p tal que p^2 divida n, então a equação diofantina $m = x^2 + y^2$ tem solução se, e somente se n não tem fatores primos da forma $4k + 3$.*

Demonstração. Primeiramente vamos supor que n não tem fatores primos da forma $4k+3$. Se $n = 1$, então $m = n_0^2 + 0^2$ que é soma de dois quadrados. Se $n > 1$, então n pode ser escrito como $n = p_1p_2 \cdots p_r$, pois n é livre de quadrados, onde os $p_r's$ podem ser iguais a 2 ou da forma $4k + 1$. Pelo teorema 2.1.4 $4k + 1$, pode ser escrito como soma de dois quadrados e 2 também pode ser escrito como soma de dois quadrados. Pelo lema 2.2, o produto de dois inteiros que é representado como soma de dois quadrados é igual à soma de dois quadrados. Deste modo, podemos multiplicar os fatores primos de n de modo que $n = a^2 + b^2$. Como $m = n_0^2 n$, isso implica que

$$m = n_0^2(a^2 + b^2) = n_0^2a^2 + n_0^2b^2 = (n_0a)^2 + (n_0b)^2$$

que é soma de dois quadrados.

Agora assumiremos que $m = x^2 + y^2 = n_0^2 n$. Supondo que $n > 1$, e seja p um fator primo de n. Se $(x, y) = d$, então, existe $t, r \in \mathbb{Z}$, tais que $x = rd$ e $y = td$ e $(r, t) = 1$. Então,

$$d^2(r^2 + t^2) = n_0^2 n$$

como n é livre de quadrados, então $d^2 | n_0^2$. Logo

$$r^2 + t^2 = \left(\frac{n_0^2}{d^2}\right) n = sp \tag{2.3}$$

para s positivo. A equação (2.3) mostra-nos que

$$r^2 + t^2 \equiv 0 (mod \quad p) \tag{2.4}$$

Agora a condição $(r, t) = 1$ implica que devemos ter r ou t relativamente primo com p. Suponhamos que $(r, p) = 1$, então existem inteiros r' e $r"$ tais que

$$r'r + r"p = 1$$

ou

$$r'r \equiv 1 (mod \quad p) \tag{2.5}$$

Agora, multiplicando a equação (2.4) por $(r')^2$, teremos:

$$\begin{aligned} (r')^2(r^2 + t^2) &\equiv 0 \cdot (r')^2 (mod \quad p) \\ (r'r)^2 + (tr')^2 &\equiv 0 (mod \quad p) \end{aligned} \tag{2.6}$$

mas de 2.5, temos que

$$\begin{aligned} (r'r)^2 &\equiv 1^2 (mod \quad p) \\ (r'r)^2 &= pk + 1 \end{aligned} \tag{2.7}$$

onde $k \in \mathbb{Z}$. Substituindo 2.7 em 2.6, temos:

$$\begin{aligned} pk + 1 + (tr')^2 &\equiv 0(mod \quad p) \\ (tr')^2 + 1 &= ps - pk \\ (tr')^2 + 1 &\equiv 0(mod \quad p) \end{aligned}$$

onde $s \in \mathbb{Z}$. Então $\left(\dfrac{-1}{p}\right) = 1$, ou seja, -1 é resíduo quadrático de p e isso só ocorre no caso em que $p = 2$ ou p é da forma $4k+1$. Então n_0 não possui fatores da forma $4k+3$.

□

Teorema 2.1.7. *Seja $m \in \mathbb{Z}_+^*$, então m só será representado como uma soma de dois quadrados se, e somente se, todo fator primo de m da forma $q \equiv 3(mod \quad 4)$ tiver expoente par.*

Exemplo: $245 = 7^2 \cdot 5 = 14^2 + 7^2$

Demonstração. $\Leftarrow$ Se assumirmos que m é da forma $2^f \cdot p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r} \cdot \cdot q_2^{2l_2} \cdots q_s^{2l_s}$, com $p_j \equiv 1(mod \quad 4)$ e $q_j \equiv 3(mod \quad 4)$, todos primos. Como sabemos, $2 = (1^2 + 1^2)$ e todos os primos da forma $4k+1$ podem ser representados como soma de dois quadrados e $q_j^{2l_s} = (q_j^2)^{l_s}$ o que quer dizer que $q_j^2 = q_j^2 + 0^2$, que é uma soma de dois quadrados. Pelo lema (2.1), um produto de números representados por soma de dois quadrados é uma soma de dois quadrados, então m pode ser representado como uma soma de dois quadrados se qualquer primo da forma $4k+3$ estiver elevado ao quadrado.

$\Rightarrow$ Agora, assumiremos que $m = x^2 + y^2$. Seja $(x, y) = d$, temos que $x = x_1 d$ e $y = y_1 d$ (com $(x_1, y_1) = 1$), então, $m = (x_1 d)^2 + (y_1 d)^2 = d^2(x_{1^2} + y_1^2) = d^2 m_1$, onde $m_1 = x_1^2 + y_1^2$. Agora, dado um q primo da forma $4k+3$, tal que, ao decompormos m em fatores primos q tenha um expoente ímpar. Então temos que $q | m_1$, mas $q \nmid x_1$ e $q \nmid y_1$. Como $-y_1^2 \equiv x_1^2(mod \quad q)$, pelos estudos de resíduos quadráticos, temos que:

- Se $-y_1^2 \equiv x_1^2(mod \quad q) \Rightarrow \left(\dfrac{x_1^2}{q}\right) = \left(\dfrac{-y_1^2}{q}\right)$.

  Como

  $q \nmid x_1 \Rightarrow \left(\dfrac{x_1^2}{q}\right) = 1$, logo $\left(\dfrac{-y_1^2}{q}\right) = \left(\dfrac{-1}{q}\right) \cdot \left(\dfrac{y_1^2}{q}\right)$, mas $\left(\dfrac{-1}{q}\right) = 1 \Leftrightarrow q \equiv 1(mod \quad 4)$.

Daí segue que $q \equiv 1 (mod \quad 4)$, o que é uma contradição.

□

2.2 Soma de Três Quadrados

Como está evidente, alguns números inteiros positivos não podem ser expressos como soma de dois quadrados. Tendo em vista esta impossibilidade, fora preciso criar um outro modo para representar inteiros como soma de quadrados. Desta vez, utilizaremos a soma de três quadrados inteiros e, assim como na seção que trata sobre soma de dois quadrados, enunciaremos algumas condições para que um inteiro positivo possa ou não ser expresso como soma de três quadrados. Abaixo, temos alguns exemplos de números que não podem ser expressos como soma de dois quadrados, mas são como soma de três:
$14 = 3^2 + 2^2 + 1^2$, $11 = 3^2 + 1^2 + 1^2$ e $67 = 7^2 + 3^2 + 3^2$

Para darmos início ao nosso breve estudo sobre representação de inteiros positivos como soma de três quadrados, enunciaremos o seguinte teorema:

Teorema 2.2.1. *A equação diofantina* $m = x^2 + y^2 + z^2$ $(x, y, z \in \mathbb{Z}$ *e* $m \in \mathbb{Z}_+^*)$, *tem solução se, e somente se,* m *não é da forma* $4^n(8k + 7)$, *onde* $n \geq 1$ *e* $k \geq 0$.

Primeiramente vamos provar o seguinte teorema:

Teorema 2.2.2. *Nenhum inteiro positivo da forma* $8k + 7$, $k \in \mathbb{Z}$, *pode ser escrito como soma de três quadrados.*

Demonstração. Módulo 8, o número inteiro a é congruente a $0, 1, 2, 3, 4, 5, 6$ ou 7 (Pela teoria das congruências), logo, $a^2 \equiv 0, 1$ ou $4 (mod \quad 8)$, então, $a^2 + b^2 + c^2 \equiv 0, 1, 2, 3, 4, 5$ ou $6 (mod \quad 8)$, para $a, b, c \in \mathbb{Z}$. Portanto, é impossível a representação de um inteiro positivo da forma $8k + 7$ como soma de três quadrados inteiros.

□

Demonstração. **(Teorema (2.2.1))**: Seja a um inteiro. Módulo 4, temos que $a \equiv 0$ ou 1, logo, para que $x^2 + y^2 + z^2$ seja da forma $4^n(8k + 7)$, temos que ter x, y e z pares, então $x = 2x_1$, $y = 2y_1$ e $z = 2z_1$, assim:

$$\begin{aligned} x^2+y^2+z^2 &= 4^n(8k+7) = 4(x_1^2+y_1^2+z_1^2) \\ &= 4^{n-1}(8k+7) \end{aligned}$$

Como $n \geq 1$, então, se tivermos $n-1 \geq 1$, implicaria que $8k+7$ poderia ser escrito como soma de três quadrados, o que é uma contradição, como foi mostrado anteriormente. Logo, o número $4^n(8k+7)$ não pode ser escrito como soma de três quadrados inteiros.

$\square$

Alguns exemplos de números que não podem ser representados como soma de três quadrados:
$7 = 8 \cdot 0 + 7$ e $60 = 4^1(8 \cdot 1 + 7)$ *Observação:* A "volta"deste teorema (mostrar que se um inteiro m não for da forma $4^n(8k+3)$ então m pode ser representado como soma de três quadrados) não é trivial e exige conceitos nada elementares, como gêneros de classes, gêneros binários e até ternários. Por esta razão, vamos suprimir esta demonstração neste trabalho.

Diferentemente do caso de multiplicação entre dois números representados como soma de dois quadrados e que veremos no próximo capítulo a multiplicação de dois números representados como soma de quatro quadrados, o produto de dois números representados como soma de três quadrados não é uma soma de três quadrados.

Vejamos o exemplo:
$3 = 1^2 + 1^2 + 1^2$ e $5 = 2^2 + 1^2 + 0^2$
Seu produto
$3 \cdot 5 = 15 \equiv 7(mod \quad 8)$ que, como vimos, não tem representação como soma de três quadrados.

De fato, os números $m \equiv 3(mod \quad 8)$ e $n \equiv 5(mod \quad 8)$ podem ser representados como soma de três quadrados. Pela teoria das congruências, seu produto $m \cdot n \equiv 7(mod \quad 8)$, logo $m \cdot n$ não pode ser representado como soma de quadrados.

Capítulo 3

Soma de Quatro Quadrados

Para a demonstração do Teorema de Lagrange, seguimos a obra de Burton (2005) e artigos da internet. No capítulo anterior, vimos que nem todos os inteiros positivos podem ser escritos como soma de dois e de três quadrados, como por exemplo o número 7. Por isso, houve a necessidade de ampliar os conceitos de representação de inteiros como soma de quadrados. Há muito tempo, Bachet de Méziriac mencionou que *"todo inteiro positivo é representável como soma de quatro quadrados inteiros"*. Diofanto nunca mencionou publicamente este teorema, mas suas considerações sobre representação de inteiros positivos como soma de dois e de três quadrados puderam ser interpretadas por Bachet e Xylander como uma indicação de conhecimento da representatividade de inteiros como soma de quatro quadrados.

Ainda que Bachet tenha enunciado o teorema sobre soma de quatro quadrados, o mesmo não conseguiu exibir uma demonstração geral, apenas mostrou por indução que o teorema era válido para inteiros de 1 até 325.

Alguns matemáticos tentaram demonstrar, sem sucesso, o teorema mencionado por Bachet, entre eles, Descartes e Euler. Fermat afirmou ter uma prova baseada no seu método da descida, mas nunca a tornou pública. Euler fez afirmações relevantes sobre o teorema descrito e em uma carta de 1730 para Goldbach afirmou que a maior dificuldade estava em mostrar que números da forma $n^2 + 7$ podem ser escritos como soma de quatro quadrados.

Finalmente, o primeiro matemático a verificar este teorema, como mencionado no Capítulo 1, foi Lagrange.

Assim, vamos buscar a demonstração deste teorema devido a Lagrange sobre a representação de inteiros positivos como soma de quatro quadrados.

Primeiramente utilizaremos um lema e três teoremas que serão a base do Teorema de Lagrange.

Lema 3.0.3 (Euler). *Se os inteiros m e n são expressos como soma de quatro quadrados, então o seu produto $m \cdot n$ também é uma soma de quatro quadrados.*

Ou seja, se $m = a_1^2 + a_2^2 + a_3^2 + a_4^2$ e $n = b_1^2 + b_2^2 + b_3^2 + b_4^2$, então

$$\begin{aligned} m \cdot n &= (a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\ &= (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 \\ &+ (a_1b_3 - a_2b_4 - a_3b_1 + a_4b_2)^2 + (a_1b_4 + a_2b_3 - a_3b_2 - a_4b_1)^2 \end{aligned}$$

Para verificarmos a validade deste lema, basta multiplicarmos os termos e compararmos os resultados.

Utilizaremos o outro seguinte resultado:

Teorema 3.0.4 (Euler). *Seja p um primo ímpar. Então a congruência $x^2 + y^2 + 1 \equiv 0(mod \quad p)$ tem uma solução x_0, y_0, onde $0 \leq x_0, y_0 \leq \dfrac{p-1}{2}$.*

Demonstração. A ideia é considerar os dois seguintes conjuntos

$$S_1 = \left\{ 1 + 0^2, 1 + 1^2, 1 + 2^2, \cdots, 1 + \left(\frac{p-1}{2}\right)^2 \right\}$$

$$S_2 = \left\{ -0^2, -1^2, -2^2, \cdots, -\left(\frac{p-1}{2}\right)^2 \right\}$$

Podemos perceber que não existem dois elementos em S_1 que sejam congruentes módulo p. Ou seja, não existe $1 + x_1^2 \equiv 1 + x_2^2(mod \quad p)$, com $x_1 \neq x_2$, pois se existisse, teríamos $x_1^2 \equiv x_2^2(mod \quad p) \Rightarrow x_1^2 - x_2^2 \equiv 0(mod \quad p)$ e $(x_1 + x_2)(x_1 - x_2) \equiv 0(mod \quad p)$, e teríamos $x_1 \equiv -x_2(mod \quad p)$ ou $x_1 \equiv x_2(mod \quad p)$. Este último caso só seria possível se $x_1 = x_2$, o que é uma contradição. Do mesmo modo, não existem dois elementos em S_2 que sejam congruentes módulo p. S_1 e S_2 contém $2\left(1 + \dfrac{p-1}{2}\right) = p + 1$ inteiros e pelo Princípio da Casa dos Pombos, algum inteiro em S_1 deve ser congruente módulo p a algum inteiro em S_2. Logo, existem x_0, y_0 tais que

$$1 + x_0^2 \equiv -y_0^2(mod \quad p)$$

com $0 \leq x_0, y_0 \leq \dfrac{p-1}{2}$. $\square$

Teorema 3.0.5. *Se p um primo ímpar, então existe um número k, tal que $1 \leq k < p$ e kp seja soma de quatro quadrados.*

Demonstração. Segue do Teorema (3.0.4) que a congruência $1 + x^2 \equiv -y^2 (mod \quad p)$ tem solução $x_0, y_0 < \dfrac{p}{2}$. Portanto,

$$x_0^2 + y_0^2 + 1^2 + 0^2 = kp, \qquad 0 < kp < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2 \tag{3.1}$$

então, $k < p$. $\square$

Teorema 3.0.6. *Qualquer primo p pode ser escrito como a soma de quatro quadrados.*

Demonstração. Consideraremos $p \neq 2$ pois, para $p = 2$, temos

$$2 = 1^2 + 1^2 + 0^2 + 0^2$$

Sem perda de generalidade, assumiremos $p > 2$ e, seja k o menor inteiro positivo, tal que

$$kp = x^2 + y^2 + z^2 + w^2$$

Pelos dois teoremas anteriores, tal k existe e, além disso, $1 \leq k < p$. Nosso objetivo é mostrar que $k = 1$. Para isso, faremos as seguintes afirmações:

Afirmação 1: k é ímpar.

Prova: Assumimos que k seja par, então x, y, z e w são todos pares, todos ímpares ou dois pares e dois ímpares, pois $par^2 = par$ e $ímpar^2 = ímpar$. Arrumando os termos, temos $x + y$ e $z + w$ pares. Então,

$$\frac{1}{2}(kp) = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 \tag{3.2}$$

todos os termos entre parênteses são inteiros e como $x+y = 2l \Rightarrow x-y = 2l-2y = 2(l-y)$, que também é par. Da mesma forma, $z + w$ é par. Isso mostra-nos a representação de $\left(\dfrac{k}{2}\right)p$ como soma de quatro quadrados inteiros, contrariando a minimalidade de k e levando-nos à uma contradição.

Afirmação 2: $k = 1$

Prova: Assumiremos $k \neq 1$.

A **Afirmação 1** implica que $k \geq 3$. Então, existem $a, b, c, d \in \mathbb{Z}$, tais que

$$a \equiv x \qquad b \equiv y \qquad c \equiv z \quad e \quad d \equiv w (mod \quad k) \tag{3.3}$$

com $0 \leq |a|, |b|, |c|, |d| < \frac{k}{2}$. (Para encontrarmos a, por exemplo, temos que $x \equiv r(mod \quad k)$, com $0 \leq r \leq k-1$. Considere $a = r$ se $r < \frac{k}{2}$ e $a = r - k$, se $r > \frac{k}{2}$).
Assim,

$$a^2 + b^2 + c^2 + d^2 = nk \tag{3.4}$$

para algum $n \geq 0$. Ou seja,

$$0 \leq nk < 4\left(\frac{k}{2}\right)^2 = k^2 \Rightarrow n < k$$

Além disso, $n \neq 0$, caso contrário, $a = b = c = b = 0$ e 3.3 implicaria que k dividiria cada x, y, z, w e ainda, $k^2 | kp \Rightarrow k | p$, o que é uma contradição, pois $1 < k < p$.

Conclusão: $0 < n < k$.

É facilmente verificado que

$$\begin{aligned} k^2 np = (kp)(kn) &= (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) \\ &= r^2 + s^2 + t^2 + u^2 \end{aligned}$$

onde

$$\begin{aligned} r &= xa + yb + zc + wd \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 (mod \quad k) \\ s &= xb - ya + zd - wc \equiv ab - ba + cd - dc \equiv 0 (mod \quad k) \\ t &= xc - yd - za + wa \equiv ac - bd + cd - dc \equiv 0 (mod \quad k) \\ u &= xd + yc - zd - wa \equiv ad + bc - cd - da \equiv 0 (mod \quad k) \end{aligned}$$

A primeira equivalência é assegurada por 3.3 e a segunda por 3.4. Portanto,

$r \equiv s \equiv t \equiv u \equiv 0 (mod \quad k)$ e segue que

$$np = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2$$

onde os termos entre parênteses são inteiros. Desde que $0 < n < k$, isso contradiz a nossa minimalidade escolhida para k. Portanto, $k = 1$.

Para finalizar, temos $k = 1$ e segue que nosso primo p pode ser expresso como

$$p = x^2 + y^2 + z^2 + w^2 \tag{3.5}$$

como queríamos.

□

Agora temos suporte para mostrar o teorema principal deste trabalho.

Teorema 3.0.7 (O Teorema de Lagrange). *Qualquer inteiro $n \in \mathbb{Z}_+^*$ pode ser representado como soma de quatro quadrados, ou seja, a equação diofantina*

$$n = a^2 + b^2 + c^2 + d^2$$

tem solução inteira, considerando que qualquer a, b, c, d possa ser igual a zero.

Demonstração. Consideraremos $n > 1$. Sabendo que n pode ser decomposto em fatores primos, temos que $n = p_1 \cdot p_2 \cdots p_r$, onde os $p_i's$ são primos. Pelo Teorema (3.0.6), qualquer primo pode ser escrito como soma de quatro quadrados e pelo Lema (3.0.3), o produto de $p_1 \cdot p_2 \cdots p_r$ é uma soma de quatro quadrados, então, n é uma soma de quatro quadrados. □

Considerações Finais

Percebemos no decorrer do trabalho que Lagrange foi merecidamente considerado um dos maiores matemáticos do século XVIII pois, além deste problema, conseguiu conjecturar novos problemas e provar muitas outras questões que levaram dezenas e até centenas de anos para serem concluídas, sem falar nas suas obras valiosíssimas que enriqueceram ainda mais os campos da mecânica, física, astronomia e claro, da matemática. Não poderíamos deixar de citar a contribuição de Euler para a ascensão de Lagrange e para a demonstração do "Teorema dos quatro quadrados". Suas obras, seu reconhecimento e sua influência foram fundamentais para que Lagrange se tornasse a "mais alta pirâmide da matemática".

Durante o trabalho percebemos também que demonstrar o Teorema de Lagrange, apesar da aparente simplicidade do problema, requer recursos e conceitos mais aprofundados em teoria dos números que só surgiram anos após o seu enunciados e daí entendemos um dos motivos da demonstração ter sido dada mais de cem anos após sua conjectura.

A utilização de conceitos sobre representação de inteiros positivos como soma de dois e de três quadrados inteiros foi crucial para a conclusão deste trabalho, já que o nosso teorema principal utiliza alguns métodos propostos nos teoremas da representação de inteiros positivos como soma de dois quadrados e resolvemos incluí-los para permitir que o leitor acompanhe o desenvolvimento da construção das hipóteses sobre representação de inteiros positivos como soma de quadrados e também para auxiliar no entendimento do Teorema de Lagrange.

Enfatizamos aqui, as grandes observações de Lagrange à teoria dos números que, com absoluta certeza, foi um dos protagonistas no desenvolvimento da Teoria dos Números.

Referências

[1] BURTON, David M., *Elementary Number Theory*, 6ª ed. [Nova Iorque] McGraw-Hill. [2005].

[2] GROSSWALD, Emil., *Representations of Integers as a Sum of Squares*, 1ª ed. [Nova Iorque] Springer-Verlag. [1985].

[3] REGO, Venancio P., *Lagrange. la Elegancia Matemática.* 1 ed. [Espanha] NIVOLA libros y ediciones. [2003].

[4] SANTOS, José Plínio de Oliveira, *Introdução à Teoria dos Números.* 2 ed. [Rio de Janeiro] Instituto de Matemática Pura e Aplicada. [1998].

[5] SEVERINO, Mike e SWICEGOOD, Grant, *Class Notes: Linear Algebra with an Introduction to Quadratic Forms over Fields*
Disponível em: <http://www.math.umt.edu/mckinnie/f10/notes/09012010.pdf> Data de acesso: 23, nov. 2013.

[6] TIJDEMAN, Robert, *Combinatorial and Analytic Number Theory* [2007]
Disponível em: <http://www.math.leidenuniv.nl/~hfinkeln/seminarium/multiplicatieve_functies.pdf> Data de acesso: 23, nov. 2013.

[7] VELANI, Sanju *Number Theory*
Disponível em: <http://www.mathematik.uni-kl.de/~taylor/PDF/York/NumberTheory.pdf> Data de acesso: 23, nov. 2013.