UNIVERSIDADE FEDERAL DA PARAÍBA
Centro de Ciências Exatas e da Natureza
Departamento de Matemática
Mestrado Profissional em Matemática em Rede Nacional

Números Inteiros Como Soma de Quadrados [†]

por

João Evangelista Cabral dos Santos

sob orientação do

Prof. Dr. Bruno Henrique Carvalho Ribeiro

Trabalho de conclusão de curso apresentado ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Agosto/2013

João Pessoa - PB

[†]O presente trabalho foi realizado com apoio da CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior.

S237n Santos, João Evangelista Cabral dos.
Números inteiros como soma de quadrados / João Evangelista Cabral dos Santos.- João Pessoa, 2013.
69f. : il.
Orientador: Bruno Henrique Carvalho Ribeiro
Dissertação (Mestrado) – UFPB/CCEN
1. Matemática. 2. Números inteiros. 3. Último teorema de Fermat. 4. Soma de quadrados.

UFPB/BC CDU: 51(043)

Números Inteiros Como Soma de Quadrados

por

João Evangelista Cabral dos Santos

Trabalho de conclusão de curso apresentado ao Corpo Docente do Mestrado Profissional em Matemática em Rede Nacional PROFMAT CCEN-UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de concentração: Matemática.

Aprovada por:

Bruno Henrique Carvalho Ribeiro -UFPB (Orientador)

Abiel Costa Macedo - UFPE

Flank David Morais Bezerra - UFPB

Agosto/2013

Agradecimentos

Quero agradecer primeiramente a Deus, meus pais, minha esposa e filhos pela compreensão e ao meu orientador pela atenção e ideias para este trabalho.

Dedicatória

A todos os que se alegram com o nosso sucesso.

Resumo

Este trabalho tem como objetivo fazer uma pesquisa bibliográfica sobre o tema da representação de inteiros como soma de quadrados, para os casos onde temos soma de dois, três e quatro quadrados. A ideia é estudar condições para que possamos garantir quando um número inteiro positivo poderá ser representado como uma soma de dois e quatro quadrados. O foco central está na demonstração do teorema dos quatro quadrados de Lagrange, apesar de termos ido um pouco adiante estudando a técnica do descenso infinito de Fernat e o caso n=3 do último teorema de Fermat. Por fim, trabalhamos com a elaboração de uma sequência didática que pode ser utilizada nas séries finais do ensino fundamental e no ensino médio, cujo conteúdo abordado nesta sequência são os principais teoremas do capítulo 2 que remete a representação de inteiros como soma de quadrados.

Palavras Chave: Números inteiros, último teorema de Fermat, soma de quadrados.

Abstract

This paper is a survey on representation of integers as sums of squares for the cases where we have the sum of two, three and four squares. The idea is to study conditions so that we can ensure the representation of numbers that are written as the sum of two and four square. The central focus is the statement of the theorem of Lagrange four squares, although we have gone a little further studying Fermat' s technique of infinite descense and the case n = 3 of Fermat's last theorem. Finally, we work with the development of a didactic sequence that can be used in the final grades of elementary school and middle school, addressing Chapter 2 of this dissertation.

Keywords: Whole numbers, Fermat's last theorem, the sum of squares.

Sumário

Introdução

A ideia de representar um número natural como soma de quadrados surge naturalmente ao tentarmos encontrar triângulos retângulos de lados inteiros. É um problema antigo e um dos primeiros a estudá-lo foi Diofanto de Alexandria, o qual escreve em sua obra prima intitulada *aritmética* . Séculos mais tarde o matemático chamado Bachet faz a tradução da obra de Diofanto para o latim e por isso este problema foi inicialmente conhecido como conjectura de Bachet. Mas foi Eduard Waring que fez várias afirmações sobre este tema inclusive que todo número natural pode ser representado como soma de no máximo quatro quadrados. Matemáticos de várias épocas mostraram interesse em demonstrar este e outros resultados que Waring havia enunciado, entre eles, Fermat e Lagrange, e isto gerou muita contribuição para a matemática da época. Mas, foi apenas no ano de 1909 que o matemático Hilbert demonstrou que para cada inteiro positivo s, há um inteiro positivo $g(s)$, que independe de n, tal que n pode ser expresso como a soma de no máximo $g(s)$ s-ésimas potências positivas.

No primeiro capítulo faremos uma breve introdução a teoria dos resíduos quadráticos, definindo e demonstrando resultados relevantes para o andamento desta pesquisa.

No segundo capítulo, tratamos do tema central da pesquisa que é a representação de inteiros como soma de quadrados. Não faremos aqui um estudo aprofundado sobre este tema, trataremos apenas dos casos particulares para a soma de dois, três e

quatro quadrados, visto que o caso mais geral que foi demosntrado por Hilbert foge ao propósito. Veremos resultados importantes para caracterizar números inteiros que podem ser representados como soma de dois e quatro quadrados. Finalmente, falaremos dos dois resultados centrais deste trabalho que são: o teorema dos quatro quadrados de Lagrange e o teorema da unicidade de Euler. Fomos um pouco mais adiante e ainda fizemos duas seções bem interessantes: uma sobre a técnica do descenso infinito de Fermat, onde fizemos um exemplo para podermos compreender melhor sua utilização, na outra seção, relembramos um pouco da história do útltimo teorema de Fermat e finalizamos fazendo um caso particular do mesmo, o caso $n = 3$, para termos mais ou menos a ideia de como é a demonstração deste Teorema.

No terceiro e último capítulo elaboramos uma sequência didática baseada na teoria exposta no capítulo 2. Ela está dividida em duas partes, a primeira aborda os principais resultados do capítulo 2, enquanto a segunda parte é uma aplicação a geometria destes conhecimentos. A atividade pode ser aplicada nas séries finais do ensino fundamental II e no ensino médio podendo ter ótimo rendimento entre os alunos visto que ela vai de um nível mais elementar para o nível mais complexo.

Capítulo 1

Alguns Resultados Importantes

Neste capítulo faremos uma breve introdução no estudo dos resíduos quadráticos, enunciando e demonstrando alguns resultados importantes que servirão de base para resultados posteriores.

1.1 Resíduos Quadráticos

O interesse maior no estudo dos resíduos quadráticos está em estudar as soluções para a congruência $x^2 \equiv a \pmod{m}$. Quando m é um primo ímpar e $(a, m) = 1$ ((a, b) é a notação para o máximo divisor comum entre a e b), a congruência, caso tenha solução, terá exatamente duas soluções incongruentes, é o que mostraremos no teorema abaixo.

Teorema 1.1 *Para p primo ímpar e a um inteiro não divisível por p, a congruência abaixo, caso tenha solução, tem exatamente duas soluções incongruentes módulo p.*

$$x^2 \equiv a \pmod{p}$$

Demonstração: Seja x_1 solução da congruência acima, podemos concluir que $-x_1$ também é solução pois, $(-x_1)^2 = (x_1)^2 \equiv a \pmod{p}$. Temos que mostrar que

estas soluções são incongruentes. Suponhamos por absurdo que x_1 e $-x_1$ sejam congruentes módulo p, ou seja, $x_1 \equiv -x_1 \pmod{p}$, daí $x_1 + x_1 \equiv -x_1 + x_1 \pmod{p}$ portanto, $2x_1 \equiv 0 \pmod{p}$. Temos que p é ímpar e não divide x_1 e sabendo que x_1 é diferente de zero, podemos concluir que não é possível ocorrer a congruência $2x_1 \equiv 0 \pmod{p}$, pois p não divide a e além disso $x_1^2 \equiv a \pmod{p}$ daí podemos garantir que p nãzo divide x_1^2 e portanto não divide x_1, assim podemos concluir que x_1 e $-x_1$ são incongruentes móduo p. A nossa meta agora é mostrar que existem apenas estas duas soluções incongruentes módulo p. Assim, seja y uma solução de $x^2 \equiv a \pmod{p}$, então $y^2 \equiv a \pmod{p}$, como x_1 é solução teremos que $x_1^2 \equiv a \pmod{p}$, portanto $x_1^2 \equiv y^2 \equiv a \pmod{p}$ e assim, $x_1^2 - y^2 \equiv 0 \pmod{p}$, onde podemos concluir $(x_1 + y)(x_1 - y) \equiv 0 \pmod{p}$, como p é primo temos que $p \mid x_1 + y$ ou $p \mid x_1 - y$, o que é o mesmo que $x_1 + y \equiv 0 \pmod{p}$ ou $x_1 - y \equiv 0 \pmod{p}$ daí $y \equiv -x_1 \pmod{p}$ ou $y \equiv x_1 \pmod{p}$. Portanto, caso exista soluções, só existem apenas duas soluções incongruentes módulo p.

□

Definição 1.1 *O conjunto $A = \{r_1, r_2, \ldots, r_s\}$ é um sistema de resíduos módulo p se:*

1. *r_i não for congruente a r_j módulo p para $i \neq j$*
2. *Para todo inteiro n, existe um r_i tal que $n \equiv r_i \pmod{p}$.*

Definição 1.2 *Sejam a e p inteiros com $(a, p) = 1$. Dizemos que a é resíduo quadrático módulo p se a congruência $x^2 \equiv a \pmod{p}$ tiver solução. Caso a congruência não tenha solução, dizemos que a não é resíduo quadrático módulo p ou que a é um resíduo não-quadrático.*

Teorema 1.2 *Seja p um primo ímpar. Dentre os números $\{1,\ 2,\ 3, \ldots,\ p-1\}$, veja que $\frac{p-1}{2}$ são resíduos quadráticos e $\frac{p-1}{2}$ não são.*

Demonstração:

Vamos considerar os quadrados dos números de 1 a $p-1$. Assim, $(1)^2 \equiv 1 \pmod{p}$, ou seja, 1 é resíduo quadrático da congruência $x^2 \equiv 1 \pmod{p}$, mas observemos que $(-1)^2 = (1)^2 \equiv 1 \pmod{p}$, ou seja, -1 também é solução desta congruência e, além disso, temos que $-1 \equiv p + (-1) = p - 1 \pmod{p}$, onde $p-1$ também é solução da congruência, pois $(p-1)^2 = p^2 - 2p + 1$, portanto $(p-1)^2 \equiv 1 \pmod{p}$, logo pelo teorema 1.1 concluímos que 1 e $p-1$ são as únicas soluções incongruentes de $x^2 \equiv 1 \pmod{p}$, entre os números $1, 2, 3, \ldots, p-1$.

Consideremos agora o 2^2 que será congruente a algum número k diferente de 1, da mesma forma $(-2)^2$ também o é. Observando que $-2 \equiv p + (-2) = p - 2 \pmod{p}$, novamente pelo teorema 1.1 concluímos que 2 e $p-2$ são as únicas soluções incongruentes de $x^2 \equiv k \pmod{p}$ dentre os números $i = 1, 2, 3, \ldots, p-1$.

Se tomarmos agora 3^2 e este será congruente a algum q diferente de 1 e de k, analagomente ao que foi mostrado temos que $(-3)^2$ também será congruente a q e além disso, $-3 \equiv p-3 \pmod{\ }$ então -3 e $p-3$ são as únicas soluções incongruentes de $x^2 \equiv q \pmod{p}$ dentre os números $i = 1, 2, 3, \ldots, p-1$.

Temos como resíduos quadráticos os números 1, k e q das congruências $x^2 \equiv 1 \pmod{p}$, $x^2 \equiv k \pmod{p}$ e $x^2 \equiv q \pmod{p}$ sendo suas respectivas soluções os pares $(1, p-1)$, $(2, p-2)$ e $(3, p-3)$. Se continuarmos procedendo desta maneira teremos $\frac{p-1}{2}$ pares de soluções

$$(1, p-1), (2, p-2), (3, p-3), \ldots, \left(\frac{p-1}{2}, \frac{p-1}{2}\right)$$

onde cada par é solução para uma dentre as $\frac{p-1}{2}$ congruências associadas a $\frac{p-1}{2}$ resíduos quadráticos.

□

Teorema 1.3 *Para p primo, a congruência $x^2 \equiv -1 \pmod{p}$ tem solução se, e somente se, $p = 2$ ou $p \equiv 1 \pmod{4}$.*

Demonstração:

Caso p=2: de fato, para $x = 1$ a congruência $x^2 \equiv -1 \pmod 2$ tem solução, sabemos que $2 \equiv 0 \pmod 2$, daí adicionando -1 a congruência, obtemos $2+(-1) \equiv 0+(-1) \pmod 2$ assim, $1 \equiv -1 \pmod 2$ e daí $1^2 \equiv -1 \pmod 2$, o que nos mostra que realmente $x = 1$ é solução da congruência. Resta agora mostrar que existe uma solução para $p \equiv 1 \pmod 4$.

Sendo p primo pelo teorema de Wilson, vide apêndice, podemos garantir que $(p-1)! \equiv -1 \pmod p$, como $p > 2$ é primo então $p-1$ é par, logo $(p-1)!$ tem uma quantidade par de fatores, ou seja, $p-1$ fatores exatamente. Daí poderemos escrever o teorema de Wilson da seguinte forma

$$(p-1)! = (p-1)\cdot(p-2)\cdot\ldots(p-k)\ldots\left(\frac{p+1}{2}\right)! \equiv -1 \pmod p,$$

observemos que há neste momento $\frac{p-1}{2}$ fatores, de fato, observemos que os fatores $((p-1),(p-2),\ldots),(p-k),\ldots 3,2,1)$ formam uma P.A de razão -1, daí o termo

$$\begin{aligned} a_{\frac{p-1}{2}} &= (p-1)+\left(\frac{p-1}{2}-1\right)(-1) \\ &= p-1+1-\frac{1-p}{2} \\ &= p-\frac{1-p}{2} \\ &= \frac{2p+1-p}{2} \\ &= \frac{p+1}{2}. \end{aligned}$$

Ainda podemos escrever

$$(p-1)! = (p-1)\cdot(p-2)\cdot\ldots\cdot(p-k)\cdot\ldots\cdot\left(\frac{p+1}{2}\right)! \equiv -1 \pmod p$$

como,

$$((p-1)\cdot(p-2)\cdot\ldots\cdot(p-k)\cdot\ldots\cdot\left(\frac{p+1}{2}\right))\cdot$$
$$(\left(\frac{p-1}{2}\right)\ldots k\ldots 4\cdot 3\cdot 2\cdot 1)\equiv -1 \pmod{p}. \quad (1.1)$$

Observemos que $(p-1)!$ está dividido em duas partes, onde cada uma tem $\frac{p-1}{2}$ fatores. Poderemos reescrever agrupando os fatores aos pares, daí ficaremos com, $1\cdot(p-1)\cdot 2\cdot(p-2)\cdot\ldots\cdot k(p-k)\cdot\ldots\cdot(\frac{p-1}{2})\cdot(\frac{p+1}{2})\equiv -1 \pmod{p}$. Note que ainda podemos escrevê-la como o produtório, abaixo:

$$\prod_{k=1}^{\frac{p-1}{2}} k(p-k)\equiv -1 \pmod{p}. \quad (1.2)$$

Façamos a seguinte afirmação, $k(p-k)\equiv -k^2 \pmod{p}$, que é de fácil justificativa, pois

$$\begin{aligned} n = k(p-k) &= kp-k^2 \\ &= kp+(-k^2) \\ &= k(p-k)\equiv -k^2 \pmod{p}, \end{aligned}$$

assim,

$$\prod_{k=1}^{\frac{p-1}{2}} k(p-k)\equiv \prod_{k=1}^{\frac{p-1}{2}}(-k^2)\equiv -1 \pmod{p},$$

portanto $\prod_{k=1}^{\frac{p-1}{2}}(-k^2)\equiv -1 \pmod{p}$, note que

$$\begin{aligned}\prod_{k=1}^{\frac{p-1}{2}}(-k^2) &= (-1^2)\cdot(-2^2)\ldots\cdot(-\left(\frac{p-1}{2}\right)^2) \\ &= (-1)\cdot(-1)\cdot\ldots\cdot(-1)(1^2)\cdot(2^2)\ldots\cdot\left(\frac{p-1}{2}\right)^2 \\ &= (-1)^{\frac{p-1}{2}}\left(1\cdot 2\ldots\cdot\frac{p-1}{2}\right)^2 \\ &= (-1)^{\frac{p-1}{2}}\left(\prod_{k=1}^{\frac{p-1}{2}}k\right)^2 \equiv -1 \pmod p). \end{aligned} \tag{1.3}$$

Como $p \equiv 1 \pmod 4$, podemos afirmar que $\frac{p-1}{2}$ é par. De fato, sendo $p \equiv 1 \pmod 4$ existe s inteiro tal que $p = 4s+1$ logo $p-1 = 4s$, sendo p um primo maior do que dois então este é impar, portanto $p-1$ é, par, então ao dividirmos ambos os membros da equação por 2 teremos $\frac{p-1}{2} = 2s$, o que no diz que $\frac{p-1}{2}$ é par. Daí, $(-1)^{\frac{p-1}{2}} = 1$, logo, $(\prod_{k=1}^{\frac{p-1}{2}}k)^2 \equiv -1 \pmod p$ o que nos diz que

$$x = \prod_{k=1}^{\frac{p-1}{1}} = 1\cdot 2\cdot 3\cdot\ldots\cdot\frac{p-1}{2} = \left(\frac{p-1}{2}\right)!$$

é uma solução de $x^2 \equiv -1 \pmod p$. Vamos supor agora que a congruência $x^2 \equiv -1 \pmod p$ tenha solução e que $p > 2$, pois $x^2 \equiv -1 \pmod 2$ tem solução $x = 1$. Elevando a congruência a potência $\frac{p-1}{2}$ obtemos

$$(x^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

que é o mesmo que

$$x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

.

Como $x^2 \equiv -1 \pmod p$, nós podemos dizer que $p \nmid x^2$ e daí $p \nmid x$, portanto pelo pequeno teorema de Fermat, vide apendice, $(x)^{p-1} \equiv 1 \pmod p$, aí teremos

$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ o que nos permite afirmar que $\frac{p-1}{2}$ é par, daí existe j inteiro tal que $\frac{p-1}{2} = 2j$, o que podemos ainda como $p-1 = 4j$ e assim termos $p = 4j+1$ o que acarreta $p \equiv 1 \pmod{4}$, e assim concluímos a nossa demonstração.

□

Definição 1.3 *Para p um primo ímpar e a um inteiro não divisível por p, definimos o Símbolo de Legendre $(\frac{a}{p})$ por:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{se } a \text{ é um resíduo quadrático de } p; \\ -1, & \text{se } a \text{ não é um resíduo quadrático de } p. \end{cases}$$

Teorema 1.4 *(Critério de Euler) Se p for um primo ímpar e a um inteiro não-divisível por p, então:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Demonstração:

Supondo que, $(\frac{a}{p}) = 1$, ou seja, a congruência $x^2 \equiv a \pmod{p}$ tem solução. Seja y tal solução, daí teremos que $y^2 \equiv a \pmod{p}$ implicando em $y^2 - a \equiv 0 \pmod{p}$, assim, concluímos que p divide $y^2 - a$, mas p não divide a, portanto não pode dividir y, logo $(y,p) = 1$ e pelo pequeno teorema de Fermat temos que $y^{p-1} \equiv 1 \pmod{p}$, assim $(y^2)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}$ então $a^{\frac{p-1}{2}} \equiv y^{p-1} \equiv 1 \pmod{p}$, portanto $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ e assim $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \equiv 1$ e isto conclui o caso em que $(\frac{a}{p}) = 1$.

Vamos considerar agora o caso em que $(\frac{a}{p}) = -1$, isto é, tomemos a um resíduo não-quadrático de p e seja c um dos inteiros $\{1, 2, 3, \ldots, p-1\}$. Lembrando um pouco das congruências linear, sabemos que existe uma solução c' de $cx \equiv a \pmod{p}$, onde c' está no conjunto mencionado. Observemos que $c' \neq c$, pois se $c = c'$ teríamos $c^2 \equiv a \pmod{p}$, mas isto nos diz que a é resíduo quadrático, o que contradiz o fato de que $(\frac{a}{p}) = -1$. Daí podemos dividir os inteiros de 1 até $p-1$ em $\frac{p-1}{2}$ pares, c e c', onde $cc' \equiv a \pmod{p}$, o que nos dá $\frac{p-1}{2}$ congruências.

$$\begin{aligned} c_1 c_1^{'} &\equiv a \pmod{p} \\ c_2 c_2^{'} &\equiv a \pmod{p} \\ \vdots \qquad & \qquad \vdots \\ c_{\frac{p-1}{2}} c_{\frac{p-1}{2}}^{'} &\equiv a \pmod{p} \end{aligned}$$

Multiplicando obtemos

$$c_1 c_1^{'} c_2 c_2^{'} \ldots c_{\frac{p-1}{2}} c_{\frac{p-1}{2}}^{'} \equiv a^{\frac{p-1}{2}} \pmod{p}$$

podemos escrever ainda da seguinte maneira

$$(p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}$$

Pelo teorema de Wilson obtemos

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

como queríamos.

□

Teorema 1.5 *O Símbolo de Legendre é uma função multiplicativa de a, ou seja :*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

para a e b inteiros não-divisíveis por p.

Demonstração: Usando o critério de Euler, concluímos que :

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod{p}$$

Lembrando que

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}}$$

e

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p} \text{ e } \left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} \pmod{p},$$

e assim, podemos concluir que

$$(ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}.$$

Portanto,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

□

Corolário 1.1 $\left(\frac{a^2}{p}\right) = 1$

Demonstração:

Usando o teorema 1.5 e considerando $a = b$ aliado ao fato de que $(\frac{a}{p}) = \pm 1$, temos

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right)$$

como $(\frac{a}{p}) = \pm 1$, temos que se $(\frac{a}{p}) = 1$, então

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1 \cdot 1 = 1$$

agora, se $(\frac{a}{p}) = -1$, teremos

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = (-1)\cdot(-1) = 1$$

concluindo assim a demonstração.

□

Teorema 1.6 *Para p primo ímpar, temos:*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & se\ p \equiv 1 \pmod 4; \\ -1, & se\ p \equiv 3 \pmod 4. \end{cases}$$

Demonstração: Sabemos do Critério de Euler que :

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

Da expressão acima podemos concluir que $(\frac{-1}{p}) = 1$ se $\frac{p-1}{2}$ for par e $(\frac{-1}{p}) = -1$ quando $\frac{p-1}{2}$ ímpar. Se p for um primo ímpar, existem apenas duas possibilidades para p, em termos de congruência módulo 4, $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$. Se $p \equiv 1 \pmod 4$, existe s inteiro tal que $p = 4s + 1$ onde $p - 1 = 4s$ e assim termos $\frac{p-1}{2} = 2s$, ou seja, $\frac{p-1}{2}$ é par. Se $p \equiv 3 \pmod 4$, existe k inteiro tal que $p = 4k + 3$ podendo ser escrito da seguinte forma $p-1 = 2(2k+1)$ concluíndo que $\frac{p-1}{2} = 2k+1$, ou seja, $\frac{p-1}{2}$ é ímpar. Portanto, quando $p \equiv 1 \pmod 4$ temos $(\frac{-1}{p}) = 1$ e quando $p \equiv 3 \pmod 4$ tem-se $(\frac{-1}{p}) = -1$.

□

Proposição 1.1 *sejam a, b e m inteiros tais que $m > 0$ e $(a, m) = d$. No caso que $d \nmid b$ a congruência $ax \equiv b \pmod m$ não possui nenhuma solução e quando $d \mid b$ possui exatamente d soluções incongruentes módulo m.*

Demonstração: como a e b são inteiros, $ax \equiv b \pmod m$ se, e somente se, existir y tal que $ax = b + ym$, ou seja, $b = ax - ym$. Sabemos que se $d \nmid b$ então a

equação $ax - my = b$ não tem solução, já se $d \mid b$ teremos que a equação $ax - my = b$ possui infinitas soluções que são da forma $x = x_0 - (\frac{m}{d})k$ e $y = y_0 - (\frac{a}{d})k$ onde (x_0, y_0) é uma solução particular da equação $ax - my = b$. Portanto, a congruência $ax \equiv b \pmod{m}$ irá possuir infinitas soluções dadas por $x = x_0 - (\frac{m}{d})$. Desejamos saber a quantidade de soluções incongruentes. Daí estudaremos as condições para as quais $x_1 = x_0 - (\frac{m}{d})$ e $x_2 = x_0 - (\frac{m}{d})$ são congruentes módulo m. Se x_1 e x_2 forem congruentes então $x_0 - (\frac{m}{d})k_1 \equiv x_0 - (\frac{m}{d})k_2 \pmod{m}$, assim

$$x_0 - x_0 - \left(\frac{m}{d}\right) k_1 \equiv x_0 - x_0 - \left(\frac{m}{d}\right) k_2 \pmod{m}$$

daí

$$-\left(\frac{m}{d}\right) k_1 \equiv -\left(\frac{m}{d}\right) k_2 \Rightarrow \left(\frac{m}{d}\right) k_1 \equiv \left(\frac{m}{d}\right) k_2.$$

Como $(\frac{m}{d}) \mid m$, de fato $m = d \cdot (\frac{m}{d})$, temos que $(\frac{m}{d}, m) = \frac{m}{d}$, portanto podemos cancelar $(\frac{m}{d})$ na congruência anterior, portanto $k_1 \equiv k_2 \pmod{m}$.

Daí as soluções incongruentes são da forma $x = x_0 - (\frac{m}{d})k$, onde k percorre um sistema completo de resíduos módulo d.

□

Teorema 1.7 *Para todo primo p existem inteiros a, b e c, não todos nulos, tais que a congruência seguinte se verifica*

$$a^2 + b^2 + c^2 \equiv 0 \pmod{p}.$$

Demonstração: Para $p = 2$, tomando $a = b = 1$ e $c = 0$, teremos $1^2 + 1^2 + 0^2 = 2 \equiv 0 \pmod{2}$. Ao considerarmos $p \equiv 1 \pmod{4}$ tomaremos $b = 1$, $c = 0$ e a como sendo uma solução da congruência $x^2 \equiv -1 \pmod{p}$. Daí, $b^2 = 1^2 = 1$, $c^2 = 0^2 = 0$ e $a^2 \equiv -1 \pmod{p}$, assim, $a^2 + b^2 + c^2 \equiv -1 + 1 + 0 = 0 \pmod{p}$. Agora, supondo que $p \equiv 3 \pmod{4}$ tomaremos $c = 1$ e iremos mostrar que exite solução para a congruência

$$a^2 + b^2 \equiv -1 \pmod{p}$$

Pelo teorema 1.2, sabemos que para um número p primo ímpar teremos $\frac{p-1}{2}$ resíduos quadráticos e $\frac{p-1}{2}$ resíduos não quadráticos dentre os números 1, 2, 3, ..., $p-1$. E ainda se q for um resíduo quadrático, então a congruência:

$$x^2 \equiv q \pmod{p}$$

tem solução se p for primo. Iremos supor que d é o menor resíduo positivo não-quadrático módulo p. Sabemos que 1 é resíduo quadrático pois, $2 \equiv 0 \pmod 2$ o que resulta em $1 \equiv -1 \pmod 2$ e assim temos $1^2 \equiv -1 \pmod 2$, então $d \geq 2$. Pelo teorema 1.6 concluímos que se $p \equiv 3 \pmod 4$ existe k_1 inteiro tal que $p = 4k_1 + 3$ a qual podemos escrever como segue $p = 4k_1 + 3 - 4 + 4 = 4(k_1 + 1) - 1$ e daí $p \equiv -1 \pmod 4$, então $(\frac{-1}{p}) = -1$, sabendo que d não é resíduo quadrático então $(\frac{d}{p}) = -1$. Pelo teorema 1.5,

$$\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{d}{p}\right) = (-1)(-1) = 1$$

A expressão acima nos informa que $-d$ é um resíduo quadrático módulo p, ou seja, a congruência $x^2 \equiv -d \pmod p$ tem solução. Então seja b tal que $b^2 \equiv -d \pmod p$. Devemos encontrar a conveniente tal que $a^2 \equiv d-1 \pmod p$, daí, $a^2+b^2 \equiv -d + d - 1 = -1 \pmod p$. Observemos que $a^2 \equiv d - 1 \pmod p$ tem solução, pois $d \geq 2$ e $d - 1 < d$ sendo d o menor resíduo não quadrático positivo módulo p temos que $a^2 \equiv d-1 \pmod p$ tem solução pois p é primo e $d-1$ é um resíduo quadrático. Logo,

$$a^2 + b^2 \equiv -1 \pmod{p}$$

tem solução e assim, a congruência

$$a^2 + b^2 + c^2 \equiv 0 \pmod{p}$$

é verificada.

□

Capítulo 2

Representação de Inteiros como Soma de Quadrados

2.1 O Problema de Waring

Um dos mais importantes matemáticos gregos, conhecido como o "Pai da Álgebra"já desconfiava que todos os números inteiros positivos poderiam ser escritos como soma de no máximo quatro quadrados. Este matemático era Diofanto de Alexandria que nasceu em 22 de Setembro de 250 a.C e morreu 84 anos depois. O problema ficou inicialmente conhecido como conjectura de Bachet o qual fez a tradução para o latim do trabalho mais conhecido de Diofanto intitulado *Aritmética*. Muitos matemáticos se interressaram por este problema inclusive Fermat, mas todos não tiveram êxito em demonstrá-lo. Em 1770 o matemático inglês Edward Waring afirmou que todo inteiro pode ser representado como soma de no máximo 4 quadrados, no máximo 9 cubos e no máximo 19 quartas potências. A pesar de não ter demonstrado nenhuma dessas afirmações ele, através de muitos exemplos, conjecturou que para todo número inteiro positivo s existe um inteiro positivo $g(s)$, tal que todo inteiro n positivo pode ser expresso em no máximo $g(s)$ s-ésimas potências

positivas.

O matemático italiano Joseph Louis Lagrange, em 1770 demonstra que todo inteiro pode ser escrito como soma de no máximo quatro quadrados, em 1859 é que foi demonstrado que o fato de que todo inteiro é soma de no máximo 9 cubos. No ano de 1909 o matemático Hilbert demonstra que para cada s inteiro positivo existe $g(s)$, que não depende de n, de modo que todo inteiro n pode ser escrito como soma de no máximo $g(s)$ s-ésimas potências. Como foi dito, ele apenas demonstrou a existência de $g(s)$ não explicitou nenhuma fórmula para o mesmo.

Iremos estudar resultados que caracterizam os números inteiros que possuem representação como soma de dois quadrados, demosntraremos o teorema de Lagrange o qual caracteriza os inteiros que podem ser representados como soma de quatro quadrados e falaremos um pouco sobre o resultado de Euler o qual caracteriza os primos que podem ser representados de forma única como soma de dois quadrados, além de estudarmos resultados que mostram quando um número não é escrito como soma de três quadrados chegando a falar um pouco sobre a técnica do descenso infinito de Fermat e fazendo um caso particular do último teorema de Fermat.

2.2 Soma de dois Quadrados

Iremos estudar alguns resultados que nos permitirão caracterizar todos os inteiros que podem ser escritos como uma soma de dois quadrados, ou seja, todos os valores inteiros de n de modo que

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

apresenta solução em inteiros. Mostraremos a seguir um resultado que garante o seguinte: se dois números podem ser escritos como soma de dois quadrados o produto entre eles também o pode.

Lema 2.1 *Se u e v são cada um uma soma de dois quadrados, então o produto uv também é.*

Demonstração: Como u e v podem ser representados como soma de dois quadrados então existem a, b, c e d inteiros tais que $u = a^2 + b^2$ e $v = c^2 + d^2$, devemos mostrar que uv também pode ser representado por uma soma de dois quadrados, ou seja, que existem s e t inteiros tais que $uv = s^2 + t^2$. Daí,

$$\begin{aligned} uv = (a^2 + b^2)(c^2 + d^2) &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2. \end{aligned}$$

Agora vamos somar e subtrair $2(ad)(bc)$. Obtendo,

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

e finalmente temos

$$\begin{aligned} uv &= (ac)^2 + 2(ac)(bd) + (bd)^2 + (ad)^2 - 2(ad)(bc) + (bc)^2 \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

Encontramos s e t de modo que $uv = s^2 + t^2$, que é justamente o que queríamos provar.

□

O teorema abaixo nos fornece condições para identificar primos que se representam como soma de dois quadrados.

Teorema 2.1 *Sendo p um número primo a equação $x^2 + y^2 = p$ possui solução inteira se, e somente se, $p = 2$ ou $p \equiv 1 \pmod 4$.*

Demonstração: Supondo primeiramente que $p = 2$ ou $p \equiv 1 \pmod 4$, devemos mostrar que a equação $x^2 + y^2 = p$, onde p é primo, possui solução inteira.

De fato, se $x = 1$ e $y = 1$ temos $p = 2 = 1^2 + 1^2$, assim $p = 2$ resolve o nosso problema. Basta mostrar que $p \equiv 1 \pmod 4$ tem que ocorrer. Sabemos que para todo primo ímpar p, $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$. Lembremos do seguinte fato, para todo inteiro a, $a^2 \equiv 0 \pmod 4$ ou $a^2 \equiv 1 \pmod 4$, este fato é fácil de ser mostrado, sendo a um inteiro qualquer, sabemos que os possíveis restos da divisão de a por quatro são, 0, 1, 2 e 3. Daí, $a \equiv 0, 1, 2$, ou $3 \pmod 4$, assim, $a \equiv 0 \pmod 4$ onde obtemos $a^2 \equiv 0^2 = 0 \pmod 4$, da mesma forma sendo $a \equiv 1 \pmod 4$ teremos $a^2 \equiv 1^2 = 1 \pmod 4$, $a \equiv 2 \pmod 4$ então $a^2 \equiv 2^2 = 4 \equiv 0 \pmod 4$ e finalmente,$a \equiv 3 \pmod 4$ então $a^2 \equiv 3^2 = 9 \equiv 1 \pmod 4$, portanto temos que $a^2 \equiv 0$ ou $1 \pmod 4$. Sabendo que $a^2 \equiv 0 \pmod 4$ ou $a^2 \equiv 1 \pmod 4$ e $x^2 + y^2 = p$ podemos concluir que $p \equiv 1 \pmod 4$, de fato; o que devemos mostrar é que a congrência $p \equiv 3 \pmod 4$ sendo p primo não é possível de acontecer, supondo, $x^2 \equiv y^2 \equiv 0 \pmod 4$ teremos $x^2 + y^2 \equiv 0 + 0 \pmod 4$ logo $p \equiv 0 \pmod 4$, da mesma forma se $x^2 \equiv y^2 \equiv 1 \pmod 4$ então $x^2 + y^2 \equiv 1 + 1 \pmod 4$ teremos $p \equiv 2 \pmod 4$ e finalmente se $x^2 \equiv 0 \pmod 4$ e $y^2 \equiv 1 \pmod 4$, assim $x^2 + y^2 \equiv 0 + 1 \pmod 4$ obtemos $p \equiv 1 \pmod 4$. Portanto, a única congruência possível de ocorrer é $p \equiv 1 \pmod 4$.

Supondo que $p = 2$ ou $p \equiv 1 \pmod 4$ mostraremos que todo p satisfazendo $p \equiv 1 \pmod 4$ pode ser escrito como soma de dois quadrados. Lembre que para $p = 2$ já sabemos que este pode ser escrito como uma soma de dois quadrados, $2 = 1^2 + 1^2$.

Tomemos agora um primo p que satisfaz $p \equiv 1 \pmod 4$ e usando o teorema 1.3, podemos concluir que existe x inteiro, tal que $x^2 \equiv -1 \pmod p$. Vamos definir a seguinte função $f(u, v) = u + xv$ e consideremos $m = [\sqrt{p}]$. Sabendo que $\sqrt{p}$ não é um inteiro, temos que $m < \sqrt{p} < m + 1$. Tomemos os pares (u, v) de inteiros onde $0 \leq u \leq m$ e $0 \leq v \leq m$, onde observando os intervalos concluímos que u

pode assumir $m+1$ valores e v também. Daí o número total de pares ordenados (u,v) é $(m+1)^2$. Como $m+1 > \sqrt{p}$ temos que $(m+1)^2 > (\sqrt{p})^2$, dái obtemos que $(m+1)^2 > p$, assim o número total de pares é superior a p. Sabemos que um sistema completo de resíduos módulo p tem exatamente p elementos, se considerarmos $f(u,v)$ módulo p teremos mais números do que classes de resíduos, daí pelo princípio da casa dos pombos existem pelo memos dois pares distintos (u_1,v_1) e (u_2,v_2) com coordenadas satisfazendo $0 \leq u_i \leq m$ e $0 \leq v_i \leq m$ onde $(i = 1,2)$, para os quais $f(u_1,v_1) \equiv r \pmod{p}$ e $f(u_2,v_2) \equiv r \pmod{p}$, ou seja, $f(u_1,v_1) \equiv f(u_2,v_2) \pmod{p}$, o que é equivalente a $u_1 + xv_1 \equiv u_2 + xv_2 \pmod{p}$, isto é,

$$u_1 + xv_1 - u_2 \equiv u_2 + xv_2 - u_2 \pmod{p}$$

e assim ficamos com

$$u_1 + xv_1 - u_2 \equiv xv_2 \pmod{p},$$

daí

$$u_1 + xv_1 - u_2 - xv_1 \equiv xv_2 - xv_1 \pmod{p},$$

o que resulta em

$$u_1 - u_2 \equiv xv_2 - xv_1 \pmod{p}$$

logo

$$u_1 - u_2 \equiv -x(v_2 - v_1) \pmod{p}$$

elevando a congruência acima ao quadrado obtemos

$$(u_1 - u_2)^2 \equiv (-x)^2(v_2 - v_1)^2 \equiv x^2(v_2 - v_1)^2 \pmod{p}, \tag{2.2}$$

portanto, $(u_1-u_2)^2 \equiv -1(v_2-v_1)^2 \pmod{p}$, pois $x^2 \equiv -1 \pmod{p}$. Chamando $a = u_1 - u_2$ e $b = v_1 - v_2$, teremos $a^2 \equiv -b^2 \pmod{p}$ adicionando b^2 a congruência teremos $a^2 + b^2 \equiv -b^2 + b^2 \pmod{p}$ o que resulta em $a^2 + b^2 \equiv 0 \pmod{p}$, assim concluímos que $p/a^2 + b^2$. Como os pares (u_1, v_1) e (u_2, v_2) são distintos então a e b não são ambos nulos, isto é, $a^2 + b^2 > 0$. Sendo u_1 e u_2 inteiros do intervalo $[0, m]$ temos que $a = u_1 - u_2$ pertence ao intervalo $-m \leq a \leq m$, da mesma forma $b = v_1 - v_2$ e $-m \leq b \leq m$. Como $m < \sqrt{p}$ concluímos que $|a| \leq m < \sqrt{p}$, analogamente $|b| \leq m < \sqrt{p}$. Daí $|a|^2 < (\sqrt{p})^2 = p$ da mesma forma $|b|^2 < (\sqrt{p})^2 = p$, assim $a^2 + b^2 < p + p = 2p$. Como $p/a^2 + b^2$ e $0 < a^2 + b^2 < 2p$, concluímos que o único múltiplo inteiro de p neste intervalo é ele mesmo, daí $a^2 + b^2 = p$.

□

O próximo resultado resultado mais geral do que o anterior e nos permite identificar inteiros que podem ter representação como soma de dois quadrados.

Teorema 2.2 *Um inteiro n pode ser representado como soma de dois quadrados se, e somente se, tiver fatoração da forma.*

$$n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} ... q_s^{\beta_s}$$

onde $p_i \equiv 1 \pmod{4}$ e $q_j \equiv 3 \pmod{4}$, $i = 1,\ 2, ...,\ r,\ j = 1,\ 2, ...,\ s$ e todos os expoentes β_j são pares.

Demonstração: Supondo que n tem fatoração $n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} ... q_s^{\beta_s}$, devemos mostrar que n pode ser representado como soma de dois quadrados, ou seja, devemos tentar escrever cada fator de n como uma soma de dois quadrados. Observemos que o primo $2 = 1^2 + 1^2$, podemos concluir que 2^{α} também pode ser representado como uma soma de dois quadrados, sabemos do teorema 2.1 que todos os p_i podem ser representados como soma de dois quadrados, assim, os $p_i^{\alpha_i}$ podem

ser representados por uma soma de dois quadrados, consequentemente $p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}$ também. Basta mostrarmos que os $q_j^{\beta_j}$ podem ser representados por uma soma de dois quadrados. Temos por hipótese que todos os β_i são pares, ou seja, existe $\beta_i^{'}$ tal que $\beta_i = 2\beta_i^{'}$, logo $q_j^{\beta_j} = (q_j)^{2\beta_i^{'}} = (q_j^2)^{\beta_i^{'}}$. Note que podemos escrever $q_j^2 = q_j^2 + 0^2$, ou seja, podemos escrever q_j^2 como soma de dois quadrados, daí de forma anóloga os $q_j^{\beta_j}$ podem ser escritos como soma de dois quadrados, portando usando o lema 2.1 no produto $2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}...p_r^{\alpha_r}q_1^{\beta_1}q_2^{\beta_2}...q_s^{\beta_s}$, concluímos que n pode ser escrito como soma de dois quadrados.

Agora, vamos considerar que n possa ser escrito como soma de dois quadrados e que existe um β_j que seja ímpar, sem perda de generalidade vamos considerar β_1 como sendo tal ímpar. Consideremos que $d = (a, b)$ onde a e b satisfazem a equação $a^2 + b^2 = n$. Sendo $d = (a, b)$ então $d \mid a$ e $d \mid b$, assim, existem k_1 e k_2 tais que $a = k_1 d$ e $b = k_2 d$. Observemos que

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b) = \frac{1}{d}d = 1,$$

logo,

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \left(\frac{k_1 d}{d}, \frac{k_2 d}{d}\right) = (k_1, k_2) = 1.$$

Podemos afirmar que $d^2|n$, de fato, sabendo que $d|a$ e $d|b$ então $a = k_1 d$ e $b = k_2 d$ e a e b satisfazem a equação $a^2 + b^2 = n$, logo

$$\begin{aligned} n &= (k_1 d)^2 + (k_2 d)^2 \\ &= k_1^2 d^2 + k_2^2 d^2 \\ &= d^2(k_1^2 + k_2^2) \\ &= kd^2, \end{aligned}$$

daí podemos afirmar que $d^2|n$ e além disso se dividirmos ambos os lados da igualdade por d^2 obtemos

$$\frac{k_1^2d^2}{d^2} + \frac{k_2^2d^2}{d^2} = \frac{kd^2}{d^2}.$$

o que resulta em

$$k = k_1^2 + k_2^2$$

Sendo β_1 ímpar e tendo $n = kd^2$ onde $k = \dfrac{n}{d^2}$, concluímos que o expoente de q_1 em k deve ser ímpar, pois os números k e $\dfrac{n}{d^2}$ têm a mesma decomposição primária. Como o expoente de q_1 é ímpar, então existe s inteiro tal que $k = q_1^{2s+1}\gamma$ e assim podemos escrever $k = q_1^{2s}q_1^1\gamma = q_1q_1^{2s}\gamma$, ou seja, $q_1|k$ e sabendo que $(k_1, k_2) = 1$ podemos observar $(q_1, k_1) = (q_1, k_2) = 1$. Vamos verificar que $(q_1, k_1) = 1$, temos os seguintes dados $(k_1, k_2) = 1$ e $q_1|k$, de $(k_1, k_2) = 1$ garantimos a existência de x e y tais que $xk_1 + yk_2 = 1$, elevando ambos os lados desta igualdade ao quadrado, obtemos

$$\begin{aligned}(xk_1 + yk_2)^2 &= (xk_1)^2 + 2(xk_1)(yk_2) + (yk_2)^2\\ &= x^2k_1^2 + 2xk_1yk_2 + y^2k_2^2\\ &= 1.\end{aligned}$$

Guardemos esta informação por enquanto, temos ainda que $q_1|k$, ou seja, existe s inteiro de modo que $k = q_1s$, mas por outro lado $k = k_1^2 + k_2^2$, logo, $k_1^2 + k_2^2 = q_1s$ e assim segue que $k_2^2 = q_1s - k_1^2$, lembremos também que $b = k_2d$, onde $d = (a, b)$, por isso, $k_1 = \dfrac{b}{d}$ agora vamos substituir estes valores em $x^2k_1^2 + 2xk_1yk_2 + y^2k_2^2 = 1$ e obteremos que

$$\begin{aligned}x^2k_1^2 + 2xk_1yk_2 + y^2k_2^2 &= x^2k_1^2 + 2xk_1y\left(\frac{b}{d}\right) + y^2(q_1s - k_1^2)\\ &= x^2k_1^2 + 2xk_1y\left(\frac{b}{d}\right) + y^2q_1s - y^2k_1^2\\ &= 1,\end{aligned}$$

vamos juntar os termos que contém k_1 e os que contém q_1, assim ficaremos com $x^2k_1^2 + 2xk_1y\left(\frac{b}{d}\right) - y^2k_1^2 + y^2q_1s = 1$, vamos por em evidência na expressão k_1 e q_1, daí

$$\left(x^2k_1 + 2xy\left(\frac{b}{d}\right) - y^2k_1\right)k_1 + (y^2s)q_1 = 1, \tag{2.3}$$

observemos que $t = x^2k_1 + 2xy\left(\frac{b}{d}\right) - y^2k_1$ e $u = y^2s$ são números inteiros, portanto a expressão $tk_1 + uq_1 = 1$ no diz que q_1 e k_1 são prinos entre si, ou seja, $(q_1, k_1) = 1$, analogamente podemos mostrar que $(q_1, k_2) = 1$.

Usando a proposição 1.1, garantimos que existe x de modo que $k_1x \equiv k_2 \mod q_1$ e como $q_1 \mid k$, portanto $k \equiv 0 \mod q_1$, mas lembremos que $k = k_1^2 + k_2$, então

$$k_1^2 + k_2^2 \equiv k_1^2 + k_2^2 - k_2^2 \equiv 0 - k_2^2 \equiv -k_2^2 \mod q_1.$$

Como $k_1x \equiv k_2 \mod q_1$, temos que elevenado ao quadrado esta congrência obtemos $k_1^2x^2 \equiv k_2^2 \mod q_1$. Agora somando as congruências $k_1^2 \equiv -k_2^2 \mod q_1$ e $k_1^2x^2 \equiv k_2^2 \mod q_1$, ficamos com

$$k_1^2x^2 + k_1^2 = k_1^2(x^2 + 1) \equiv -k_2^2 + k_2^2 \equiv 0 \mod q_1.$$

Façamos a seguinte afirmação, $q_1 \nmid k_1^2$, de fato, sendo $(q_1, k_2) = 1$, temos que $q_1 \nmid k_1$, portanto não divide k_1^2.

Vamos mostrar este fato, para isso usaremos a demonstração pela contrapositiva, ou seja, suponhamos que $q_1 \mid k_1^2$, dái $q_1 \mid k_1k_1$, como q_1 é primo então $q_1 \mid k_1$ ou $q_1 \mid k_1$, portanto $q_1 \mid k_1$ e assim, mostramos que $q_1 \nmid k_1^2$. Como q_1 é primo e $q_1 \mid k_1^2(x^2 + 1)$ então $q_1 \mid k_1^2$ ou $q_1 \mid (x^2 + 1)$, mas $q_1^2 \nmid k_1^2$ portanto, $q_1 \mid (x^2 + 1)$, ou seja, $x^2 \equiv -1 \mod q_1$. Observemos que a equação $x^2 \equiv -1 \mod q_1$ possui solução para $q_1 \equiv 3 \pmod 4$ o que contradiz o proposição 1.1, portanto todos os $\beta_j's$ são pares.

□

2.3 Soma de Três Quadrados

O que faremos nesta seção é exibir dois exemplos de números que não podem ser escritos como uma soma de três quadrados.

O primeiro exemplo que se segue nos diz que todo inteiro que deixa resto 7 quando dividido por 8 não pode ser escrito como uma soma de três quadrados.

Teorema 2.3 *Todo inteiro da forma* $8a + 7$ *com* $a \in \mathbb{Z}$ *não pode ser representado como a soma de três quadrados.*

Demonstração: Tomemos n inteiro. Sabemos que ao dividirmos n por 8 podemos obter como resto algum dos seguintes números 0, 1, 2, 3, 4, 5, 6 ou 7, portanto, $a \equiv 0 \pmod 8$ ou $a \equiv 1 \pmod 8$, $a \equiv 2 \pmod 8$, $a \equiv 3 \pmod 8$, $a \equiv 4 \pmod 8$, $a \equiv 5 \pmod 8$, $a \equiv 6 \pmod 8$, $a \equiv 7 \pmod 8$.

Daí,

$$
\begin{aligned}
a^2 &\equiv 0^2 = 0 \pmod 8 \\
a^2 &\equiv 1^2 = 1 \pmod 8 \\
a^2 &\equiv 2^2 = 4 \pmod 8 \\
a^2 &\equiv 3^2 = 9 \equiv 1 \pmod 8 \\
a^2 &\equiv 4^2 = 16 \equiv 0 \pmod 8 \\
a^2 &\equiv 5^2 = 25 \equiv 1 \pmod 8 \\
a^2 &\equiv 6^2 = 36 \equiv 4 \pmod 8 \\
a^2 &\equiv 7^2 = 49 \equiv 1 \pmod 8.
\end{aligned}
$$

Concluímos assim, que $a^2 \equiv 0$, 1 ou 4 $\pmod 8$. Agora, observemos que realizando todas as combinações possíveis para as somas dos quadrados não é possível obter $a^2 + b^2 + c^2 \equiv 7 \pmod 8$. De fato, vamos descrever todas as posssibilidades para a soma $a^2 + b^2 + c^2$.

$$a^2 + b^2 + c^2 \equiv 0 + 0 + 0 = 0 \equiv 0 \pmod 8$$
$$a^2 + b^2 + c^2 \equiv 0 + 0 + 1 = 1 \equiv 1 \pmod 8$$
$$a^2 + b^2 + c^2 \equiv 0 + 0 + 4 = 4 \pmod 8$$
$$a^2 + b^2 + c^2 \equiv 0 + 1 + 1 = 2 \pmod 8$$
$$a^2 + b^2 + c^2 \equiv 0 + 1 + 4 = 5 \pmod 8$$
$$a^2 + b^2 + c^2 \equiv 0 + 4 + 4 = 8 \equiv 0 \pmod 8$$
$$a^2 + b^2 + c^2 \equiv 1 + 1 + 1 = 3 \pmod 8$$
$$a^2 + b^2 + c^2 \equiv 1 + 1 + 4 = 6 \pmod 8$$
$$a^2 + b^2 + c^2 \equiv 4 + 4 + 1 = 9 \equiv 1 \pmod 8$$
$$a^2 + b^2 + c^2 \equiv 4 + 4 + 4 = 12 \equiv 4 \pmod 8.$$

Portanto, podemos perceber que não há como termos $a^2 + b^2 + c^2 \equiv 4 \pmod 8$ ou $a^2 + b^2 + c^2 \equiv 5 \pmod 8$ ou $a^2 + b^2 + c^2 \equiv 6 \pmod 8$ ou $a^2 + b^2 + c^2 \equiv 7 \pmod 8$. Mas, o que nos interessa saber é que não é possível haver a congruência $a^2 + b^2 + c^2 \equiv 7 \pmod 8$.

□

Proposição 2.1 *Seja $n \in \mathbb{N}$ da forma $n = 4^k(8m + 7)$ com k,$m > 0$. Então n jamais é soma de três ou menos quadrados.*

Demonstração: Vamos demonstrar por indução em k, vejamos primeiramente que para $k = 0$, teremos que $n = (8m + 7)$, vamos supor por absurdo que existam a_0,b_0 e c_0 inteiros positivos tais que $n = (8m+7) = a_0^2+b_0^2+c_0^2$. Sendo $n = (8m+7)$ então $n \equiv 7 \pmod 8$ e ainda podemos dizer que $n \equiv 1 \pmod 2$. Recordemos que ao dividirmos a por 8 podemos obter agum desses números como resto 0, 1, 2, 3, 4, 5, 6 ou 7, assim da demonstração do teorema anterior podemos concluir que $a \equiv 0$,

1, 2, 3, 4, 5, 6 (mod 8) e portanto, $a^2 \equiv 0$, 1 ou 4 (mod 8). Assim, não é possível termos $n \equiv 7$ (mod 8), daí n não pode ser escrito como soma de três quadrados.

Agora supomos que $4^{k-1}(8m+7)$ não seja escrito como uma soma de três quadrados, devemos mostrar que $4^k(8m+7)$ não pode ser escrito como soma de três quadrados. Sendo $k \geq 1$ e supondo que n possa escrito como soma de três quadrados, ou seja, existem a_0,b_0 e c_0 inteiros não positivos tais que $n = 4^k(8m+7) = a_0^2+b_0^2+c_0^2$, podemos concluir que $4 \mid n$, ou seja, n é par, de fato, $n = 4^k(8m+7) = 44^{k-1}(8m+7) = 2^2 4^{k-1}(8m+7)$. Assim, podemos concluir que a, b e c são todos pares. De fato, sendo n par então para a soma $n = a_0^2 + b_0^2 + c_0^2$ temos duas possibilidades :

1. Dois quadrados são ímpares e um é par;

2. Todos os quadrados são pares.

A primeira não pode ocorrer, pois $n = a_0^2+b_0^2+c_0^2 \equiv 1^2+1^2+0^2 = 2$ (mod 4), ou seja, dessa forma 4 não divide n o que é um absurdo. Assim, a única opção possivel é a segunda, ou seja, todos os quadrados são pares, daí podemos concluir que a, b e c são todos pares. De fato, sendo a^2 par então a também é par, para mostrarmos isto usaremos a demonstração por contrapositiva, se um número inteiro positivo não é par então é ímpar ou seja, sendo a ímpar devemos mostrar que a^2 é também impar e de fato isto é verdade, portanto podemos concluir que a afirmação feita é verdadeira. Sendo a, b e c todos pares então existem u, v e w inteiros positivos tais que $a = 2u$, $b = 2v$ e $c = 2w$, logo

$$\begin{aligned} 4^k(8m+7) &= a_0^2 + b_0^2 + c_0^2 \\ &= (2u)^2 + (2v)^2 + (2w)^2 \\ &= 4u^2 + 4v^2 + 4w^2 \\ &= 4(u^2 + v^2 + w^2), \end{aligned}$$

Ao dividirmos a igualdade acima por 4, obtemos

$$4^{k-1}(8m+7) = u^2 + v^2 + w^2 \tag{2.4}$$

ora mas isto contradiz a hipótese de indução, portanto $n = 4^k(8m+7)$ não pode ser escrito como uma soma de três quadrados.

□

2.4 Soma de Quatro Quadrados

Como foi dito no início deste trabalho o matemático inglês Waring, afirmou que todo número inteiro positivo é a soma de no máximo 4 quadrados. Nesta seção iremos demonstrar esta afirmação feita por Waring, mas antes demonstremos um resultado análogo ao lema 2.1 da seção anterior que garante que se dois números podem ser representados por uma soma de 4 quadrados então o produto entre eles também o pode.

Lema 2.2 *Para quaisquer a, b, c e d inteiros, temos que*

$$(a^2+b^2+c^2+d^2)\cdot(r^2+s^2+t^2+v^2) = (ar+bs+ct+dv)^2 + (as-br-cv+dt)^2 + (at+bv-cr-ds)^2 + (av-bt+cs-dr)^2.$$

Demonstração: Vamos desenvolver ambos os lados da igualdade e assim obteremos o resultado desejado. Desenvolvendo o lado esquerdo temos que

$$\begin{aligned}(a^2+b^2+c^2+d^2)\cdot(r^2+s^2+t^2+v^2) = \\ a^2r^2 + a^2s^2 + a^2t^2 + a^2v^2 + b^2r^2 + b^2s^2 + b^2t^2 + b^2v^2 \\ + c^2r^2 + c^2s^2 + c^2t^2 + c^2v^2 + d^2r^2 + d^2s^2 + d^2t^2 + d^2v^2. \end{aligned} \tag{2.5}$$

Vamos agora desenvolver o lado direito da igualdade e comparar com o resultado obtido no lado esquerdo. Vamos fazer isto em 4 etapas, desenvolvendo cada quadrado separadamente, assim,

$$(ar+bs+ct+dv)^2 =$$
$$(ar+bs)^2 + 2(ar+bs)(ct+dv) + (ct+dv)^2 =$$
$$a^2r^2 + 2arbs + b^2s^2 + 2(arct + ardv + bsct + bsdv) + c^2t^2 + 2ctdv + d^2v^2 =$$
$$a^2r^2 + b^2s^2 + c^2t^2 + d^2v^2 + 2arct + 2ardv + 2bsct + 2bsdv + 2arbs + 2ctdv. \quad (2.6)$$

Da mesma forma,

$$(as-br-cv+dt)^2 =$$
$$(as-br)^2 + 2(as-br)(-cv+dt) + (-cv+dt)^2 =$$
$$a^2s^2 - 2asbr + b^2r^2 + 2(-ascv + asdt + brcv - brdt) + c^2v^2 + 2cvdt + d^2t^2 =$$
$$a^2s^2 + b^2r^2 + c^2v^2 + d^2t^2 - 2ascv + 2asdt + 2brcv - 2brdt - 2asbr + 2cvdt. \quad (2.7)$$

De modo análogo,

$$(at+bv-cr-ds)^2 =$$
$$(at+bv)^2 + 2(at+bv)(-cr-ds) + (-cr-ds)^2 =$$
$$a^2t^2 + 2atbv + b^2v^2 + 2(-atcr - atds - bvcr - bvds) + c^2r^2 + 2crds + d^2s^2 =$$
$$a^2t^2 + b^2v^2 + c^2v^2 + d^2s^2 - 2atcr - 2atds - 2bvcr - 2bvds + 2atbv + 2crds. \quad (2.8)$$

E Finalmente,

$$(av - bt + cs - dr)^2 =$$
$$(av - bt)^2 + 2(av - bt)(cs - dr) + (cs - dr)^2 =$$
$$a^2v^2 - 2avbt + b^2t^2 + 2(avcs - avdr - btcs + btdr) + c^2s^2 - 2csdr + d^2r^2 =$$
$$a^2v^2 + b^2t^2 + c^2s^2 + d^2r^2 + 2avcs - 2avdr - 2btcs + 2btdr - 2avbt - 2csdr. \quad (2.9)$$

Agora, somando (2.6) + (2.7) + (2.8) + (2.9), obtemos

$$(ar+bs+ct+dv)^2+(as-br-cv+dt)^2+(at+bv-cr-ds)^2+(av-bt+cs-dr)^2 =$$
$$a^2r^2 + a^2s^2 + a^2t^2 + a^2v^2 + b^2r^2 +$$
$$b^2s^2 + b^2t^2 + b^2v^2 + c^2r^2 + c^2s^2 +$$
$$c^2t^2 + c^2v^2 + d^2r^2 + d^2s^2 + d^2t^2 + d^2v^2, \quad (2.10)$$

portanto ambos os lados dão o mesmo resultado, daí concluímos que

$$(a^2 + b^2 + c^2 + d^2) \cdot (r^2 + s^2 + t^2 + v^2) = (ar + bs + ct + dv)^2 + (as - br - cv + dt)^2$$
$$+ (at + bv - cr - ds)^2 + (av - bt + cs - dr)^2. \quad (2.11)$$

□

Teorema 2.4 *Todo inteiro positivo possui representação como soma de quatro quadrados.*

Demonstração: Sabemos que todo primo possui tal representação. Lembremos que $2 = 1^2 + 1^2 + 0^2 + 0^2$, assim tomemos p um primo ímpar, pelo teorema 1.7, existem a, b e c tais que $a^2 + b^2 + c^2 \equiv 0 \pmod{p}$, ou seja, existe M inteiro tal que $a^2 + b^2 + c^2 = Mp$, podemos escrever a congruência $a^2 + b^2 + c^2 \equiv 0 \pmod{p}$ da seguinte forma $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{p}$ onde $d = 0$, pela equação anterior e considerando o conjunto formado pelos números que podem ser escritos como soma de quatro quadrados, podemos garantir pelo principio da boa ordenação que este conjunto tem um menor elemento, pois ele não é vazio. Consideremos m tal elemento mínimo, assim, $a^2 + b^2 + c^2 = mp$. Como nas equações acima estamos trabalhando módulo p e a, b e c estão elevados ao quadrado, podemos tomar $|a|$, $|b|$ e $|c|$ no intervalo $[0, \frac{p}{2})$. Logo

$$a < \frac{p}{2},\ b < \frac{p}{2},\ c < \frac{p}{2} \text{ e } d < \frac{p}{2},$$

daí

$$a^2 < \left(\frac{p}{2}\right)^2,\ b^2 < \left(\frac{p}{2}\right)^2,\ c^2 < \left(\frac{p}{2}\right)^2 \text{ e } d^2 < \left(\frac{p}{2}\right)^2,$$

somando as desigualdades acima obtemos

$$a^2 + b^2 + c^2 + d^2 = mp < 4\left(\frac{p}{2}\right)^2 = 4\frac{p^2}{4} = p^2.$$

Mas, $mp < p^2$ logo $m < p$. Sabendo que $a^2 + b^2 + c^2 = mp$ e $m < p$ basta que mostremos que $m = 1$, ou seja, mostrar que $a^2+b^2+c^2 = mp$, daí teremos concluído que todo primo ímpar pode ser representado como soma de quatro quadrados. Para isto, vamos mostrar que a suposição de $m > 1$ irá nos conduzir a existência de um certo m', onde $m' < m$ e $a^2 + b^2 + c^2 + d^2 = m'p$ o que é um contradição, visto que

m foi escolhido como elemento minimal, de modo que mp tenha representação como soma de quatro quadrados.

Vamos supor que $m > 1$ teremos dois casos a considerar: m sendo par e m sendo ímpar. Tomando m ímpar e $m > 1$. Podemos escolher dentro do intervalo $[0, \frac{m}{2}]$, números a_1, b_1, c_1 e d_1 tais que $a_1 \equiv a \pmod{m}$, $b_1 \equiv b \pmod{m}$, $c_1 \equiv c \pmod{m}$ e $d_1 \equiv d \pmod{m}$. Então, teremos $a_1^2 \equiv a^2 \pmod{m}$, $b_1^2 \equiv b^2 \pmod{m}$, $c_1^2 \equiv c^2 \pmod{m}$ e $d_1^2 \equiv d^2 \pmod{m}$ e portanto, $a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}$, assim podemos garantir que existe $m' > 0$ tal que $a_1^2 + b_1^2 + c_1^2 + d_1^2 = mm'$ onde, $|a_1| < \frac{m}{2}$, $|b_1| < \frac{m}{2}$, $|c_1| < \frac{m}{2}$ e $|d_1| < \frac{m}{2}$, portanto $a_1^2 < \frac{m^2}{4}$, $b_1^2 < \frac{m^2}{4}$, $c_1^2 < \frac{m^2}{4}$ e $d_1^2 < \frac{m^2}{4}$ e daí $a_1^2 + b_1^2 + c_1^2 + d_1^2 < 4\frac{m^2}{4}$ onde $m'm < m^2$ e portanto $m' < m$. Se fizermos $m' = 0$ então $a_1^2 + b_1^2 + c_1^2 + d_1^2 = 0$, a soma de quatro números positivos dando zero só acontece se $a_1 = b_1 = c_1 = d_1 = 0$ assim, $a \equiv b \equiv c \equiv d \equiv 0 \pmod{m}$ o que conduz a afirmarmos que $m^2 \mid mp$. De fato, sendo $a \equiv b \equiv c \equiv d \equiv 0 \pmod{m}$ existem k_1, k_2, k_3, k_4 inteiros tais que $a = k_1 m$, $b = k_2 m$, $c = k_3 m$ e $d = k_4 m$, assim substituindo em $a^2 + b^2 + c^2 + d^2 = mp$, obtemos

$$\begin{aligned}(k_1m)^2 + (k_2m)^2 + (k_3m)^2 + (k_4m)^2 &= k_1^2m^2 + k_2^2m^2 + k_3^2m^2 + k_4^2m^2 \\ &= m^2(k_1^2 + k_2^2 + k_3^2 + k_4^2) \\ &= mp.\end{aligned}$$

Da equação acima podemos concluir que $m^2 \mid mp$. Observemos também que $m^2 \mid mp$ implica $m \mid p$, ora mas isto é uma contradição pois escolhemos $1 < m < p$ e sendo p primo os únicos divisores do mesmo seriam 1 e p que estão fora do intervalo que m pertence. Assim, concluímos que $m' \neq 0$. Tendo $a^2 + b^2 + c^2 + d^2 = mp$ e $a_1^2 + b_1^2 + c_1^2 + d_1^2 = m'm$ teremos que

$$(mp)(m^{'}m) = (a^2+b^2+c^2+d^2)(a_1^2+b_1^2+c_1^2+d_1^2) =$$
$$(aa_1+bb_1+cc_1+dd_1)^2+(ab_1-ba_1-cd_1+dc_1)^2+$$
$$(ac_1+bd_1-ca_1-db_1)^2+(ad_1-bc_1+cb_1-da_1)^2,$$

pelo lema 2.2.

Sabendo que $a \equiv a_1$, $b \equiv b_1$, $c \equiv c_1$ e $d \equiv d_1 \pmod{m}$ e $a^2 \equiv aa_1$, $b^2 \equiv b_1$, $c^2 \equiv$ e $d^2 \equiv dd_1$, podemos afirmar que as quatro expressões que estão elevadas ao quadrado do lado direito da multiplicação de $mpm^{'}m$ são múltiplos de m. De fato, vamos analisar por expresão, sendo $a^2 \equiv aa_1$, $b^2 \equiv bb_1$, $c^2 \equiv cc_1$ e $d^2 \equiv dd_1$, temos que ao somarmos estas congruências obtemos $aa_1+bb_1+cc_1+dd_1 \equiv a^2+b^2+c^2+d^2 \equiv 0 \pmod{m}$. Portanto $(aa_1+bb_1+cc_1+dd_1)^2$ é um mútiplo de m. Vamos analisar a expressão $(ab_1-ba_1-cd_1+dc_1)^2$. Observe que $a \equiv a_1 \pmod{m}$, então $a \equiv r_1 \pmod{m}$ e $a_1 \equiv r_1 \pmod{m}$, analogamete teremos $b \equiv r_2 \pmod{m}$ e $b_1 \equiv r_2 \pmod{m}$,$c \equiv r_3 \pmod{m}$ e $c_1 \equiv r_3 \pmod{m}$, $d \equiv r_4 \pmod{m}$ e $d_1 \equiv r_4 \pmod{m}$. Assim, $ab_1 \equiv r_1r_2 \pmod{m}$, $-ba_1 \equiv -r_1r_2 \pmod{m}$, $-cd_1 \equiv -r_3r_4 \pmod{m}$ e $dc_1 \equiv r_3r_4 \pmod{m}$. Portanto, $ab_1-ba_1-cd_1+dc_1)^2 \equiv 0+0 \equiv 0 \pmod{m}$, ou seja, $(ab_1-ba_1-cd_1+dc_1)^2$ é um múltiplo de m. Analogamente fazemos com as outras expressões e concluímos que são mútiplas de m. Mostrado isto, podemos afirmar que existem inteiros $\overline{a}$, $\overline{b}$, $\overline{c}$ e $\overline{d}$, tais que

$$\begin{aligned}(\overline{a}m)^2+(\overline{b}m)^2+(\overline{c}m)^2+(\overline{d}m)^2 &= \overline{a}^2m^2+\overline{b}^2m^2+\overline{c}^2m^2+\overline{d}^2m^2\\ &= m^2(\overline{a}^2+\overline{b}^2+\overline{c}^2+\overline{d}^2)\\ &= m^2pm^{'}.\end{aligned}$$

Daí, obtemos $\overline{a}^2+\overline{a}^2+\overline{c}^2+\overline{d}^2 = pm^{'}$ onde $m^{'}$ é menor do que m. Falta provarmos que, no caso m par poderemos encontrar $\overline{m} < m$ de modo que $\overline{m}p$ seja escrito como

soma de quatro quadrados. De fato, sendo m par teremos que mp também é par, pois p é um primo ímpar, assim $a^2+b^2+c^2 = mp$ é par, ora mas há três possibilidades para que isto aconteça. Os inteiros a, b, c e d são todos pares, ou todos ímpares ou dois pares e dois ímpares, sendo que em qualquer um dos casos mencionados é possível escolhermos a, b, c e d tais que $a \equiv b \pmod 2$ e $c \equiv d \pmod 2$. Sabendo que m é par temos que

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

é par, então dividindo a equação anterior por dois temos

$$\frac{a^2 + b^2 + c^2 + d^2}{2} = \frac{mp}{2}$$

Podemos escrevê-la da seguinte forma

$$\begin{aligned}\frac{2(a^2 + b^2) + 2(c^2 + d^2)}{4} &= \frac{2(a^2 + b^2)}{4} + \frac{2(c^2 + d^2)}{4} \\ &= \frac{mp}{2},\end{aligned}$$

agora vamos somar e subtrair da expressão anterior $\frac{2ab}{4}$ e $\frac{2cd}{4}$, ficaremos com,

$$\begin{aligned}a^2 + b^2 + c^2 + d^2 &= \frac{2(a^2 + b^2)}{4} + \frac{2(c^2 + d^2)}{4} \\ &= \frac{a^2 + b^2}{4} - \frac{2ab}{4} + \frac{2ab}{4} + \frac{a^2 + b^2}{4} + \frac{c^2 + d^2}{4} + \frac{c^2 + d^2}{4} - \frac{2cd}{4} + \frac{2cd}{4} \\ &= \frac{mp}{2}.\end{aligned}$$

Portanto,

$$\begin{aligned}\frac{a^2 - 2ab + b^2}{4} + \frac{a^2 + 2ab + b^2}{4} + \frac{c^2 - 2cd + d^2}{4} + \frac{c^2 + 2cd + d^2}{4} = \\ \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2 = \frac{mp}{2}. \quad (2.12)\end{aligned}$$

Se tomarmos $\overline{m} = \frac{m}{2} < m$, teremos caído em uma contradição mais uma vez pois lembremos que tomamos m o menor inteiro positivo tal que mp é soma de quatro quadrados. Portanto, podemos concluir que $m = 1$ e teremos demonstrado o que queríamos.

□

2.5 Um Teorema de Unicidade de Euler

A nossa meta nesta seção é de mostrar que certos primos possuem representação única como soma de dois quadrados, para isso vamos ver alguns resultados preliminares.

Proposição 2.2 *Se um primo $p = c^2 + d^2$ e se existir $q > 1$ tal que $pq = a^2 + b^2$, $(a, b) = 1$, então q é a soma dos quadrados de dois inteiros relativamente primos.*

Demonstração: É claro que se tivermos $p = c^2 + d^2$, p sendo primo então $(c, d) = 1$. Sendo $pq = a^2 + b^2$, temos

$$\begin{aligned} c^2b^2 - a^2b^2 &= c^2b^2 + a^2c^2 - a^2c^2 - a^2b^2 \\ &= c^2(a^2 + b^2) - a^2(c^2 + b^2) \\ &= c^2pq - a^2p \\ &= p(c^2q - a^2) = pk. \end{aligned}$$

Logo;

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

Daí, concluímos que $p \mid (bc+ad)(bc-ad)$, como p é primo temos $p \mid (bc+ad)$ ou $p \mid (bc-ad)$. Observemos que $bc-ad \neq 0$, de fato, se $bc=ad$ e como $(a,b)=(c,d)=1$ temos que $a=b$ e $c=d$, assim, $p=2a^2$ e $pq=2a^2$e portanto $p=pq$ o que implica $q=1$, o que é um absurdo pois $q>1$. Se $p \mid (bc-ad)$ teremos que existe t inteiro tal que $bc-ad=tp$. Sejam;

$$r = b - tc$$

e

$$s = a + td$$

Ao multilpicar a primeira das equações acima por c e a segunda por d ficaremos com

$$cr = c(b-tc) = cb - tc^2$$

e

$$ds = d(a+td) = da + td^2.$$

Sutraindo as equações acima obteremos

$$\begin{aligned} cr - ds &= c(b-tc) - d(a+td) = (cb - tc^2) - (da + td^2) \\ &= (cb - da) - t(c^2 + d^2) \\ &= tp - tp = 0. \end{aligned}$$

Logo, $cr = ds$, ou seja, $r = d\frac{s}{c}$. Como $(c,d)=1$ e $r = d\dfrac{s}{c}$ temos que $n = \dfrac{s}{c}$ deve ser inteiro. Sendo $s = c\dfrac{s}{c}$ devemos ter $r = dn$ e $s = cn$.

Observemos que $pq = a^2 + b^2$, $a = s - td$ e $b = r + tc$ temos ainda $a = nc - td$ e $b = nd + tc$, portanto

$$\begin{aligned} pq = (nc - td)^2 + (tc + nd)^2 &= n^2c^2 - 2(nc)(td) + t^2d^2 + t^2c^2 + 2(tc)(nd) + n^2d^2 \\ &= n^2c^2 + t^2d^2 + t^2c^2 + n^2d^2 = t^2d^2 + n^2d^2 + n^2c^2 + t^2c^2 \\ &= d^2(t^2 + n^2) + c^2(t^2 + n^2) \\ &= (t^2 + n^2)(c^2 + d^2). \end{aligned}$$

Lembremos que $p = c^2 + d^2$. Daí, $pq = p(t^2 + n^2) \Rightarrow q = t^2 + n^2$. Notemos que $(t, n) = 1$, de fato observe que $r = b - tc$ e $s = a + td$, $r = nd$ e $s = nc$. Sabendo que $(a, b) = 1$, então existem x e y inteiros tais que $xa + yb = 1$ e temos que $a = nc - td$ e $b = nd + tc$, logo

$$\begin{aligned} x(nc - td) + y(nd + tc) &= xnc - xtd + ynd + ytc \\ &= ytc - xtd + xnc + ynd \\ &= (yc - xd)t + (xc + yd)n = 1. \end{aligned}$$

Portanto $(t, n) = 1$. O caso $p \mid (bc + ad)$ é análogo ao que fizemos anteriormente, isto é, se $bc + ad = kp$, então

$$r = b - kc$$

e

$$s = a - kd$$

Multiplicando a primeira equação por c e a segunda por d obtemos que

$$cr = cb - kc^2$$

e

$$ds = ad - kd^2$$

e portanto, ao somarmos ambas as equações teremos que $cr + ds = cb + ad - kc^2 - kd^2 = kp - kp = 0$. Disto, concluímos que $cr = -ds$ onde $r = dn$ e $s = -cn$ tomando $n = -\frac{s}{c}$. Substituindo estes valores em $r = b - kc$ e $s = a - kd$ obtemos,

$$\begin{aligned} pq = a^2 + b^2 &= (-cn + kd)^2 + (dn + kc)^2 \\ &= c^2n^2 - 2(cn)(kd) + k^2d^2 + d^2n^2 + 2(dn)(kc) + k^2c^2 \\ &= c^2n^2 + k^2d^2 + d^2n^2 + k^2c^2 \\ &= d^2(k^2 + n^2) + c^2(n^2 + k^2) \\ &= (k^2 + n^2)(c^2 + d^2) = p(k^2 + n^2), \end{aligned}$$

e assim, $q = k^2 + n^2$. Para mostrarmos que $(k, n) = 1$ fazemos de modo análogo ao que fizemos no cas anterior. Portanto temos mostrado o que desejávamos.

□

Proposição 2.3 *Se pq é soma de dois quadrados de dois inteiros relativamente primos e q não é a soma de dois quadrados de inteiros relativamente primos, então p possui um fator primo que não é a soma de dois quadrados.*

Demonstração: Suponhamos por absurdo que $p = p_1p_2 \dots p_n$ onde cada primo p_j $(j = 1, 2, \dots, n)$ é a soma soma de dois quadrados. Como $p_1(p_2 \dots p_nq) = pq$ é a soma de dois quadrados de inteiros primos entre si e pela proposição 2.2 temos a garantia que $p_2 \dots p_nq$ é a soma de dois quadrados de inteiros relativamente primos entre si. Repetindo mais uma vez este processo temos que $p_2(p_3 \dots p_nq) = p_2 \dots p_nq$ é a soma de dois quadrados de interios relativamente primos entre si e novamente usando a proposição 2.2 temos a garantia que $p_3 \dots p_nq$ é a soma de dois quadrados de inteiros prims entre si. Procedendo sempre desta forma chegaremos a conclusão

de que q é a soma de dois quadrados de interios relatiamente primos, ora, mas isto contradiz a nossa hitótese de que q não pode ser escrito como soma de dois quadrados de inteiros primos entre si. Este absurdo foi obtido quando supomos que todos os fatores primos de p poderiam ser escritos como soma de dois quadrados, daí um destes fatores não pode ser escrito como tal.

□

Proposição 2.4 *Se um primo p divide a^2+b^2 com $(a,b)=1$, então p é a soma de dois quadrados.*

Demonstração: Suponhamos por absurdo que p não seja soma de dois quadrados. Sabemos que $p \nmid a$ e $p \nmid b$, de fato, vamos supor por absurdo que $p \mid a$, como a e b são primos entre si podemos concluir que $p \nmid b$, sabemos por hipótese que $p \mid a^2+b^2$, ou seja, existe k inteiro de modo que $p \mid a^2+b^2 = pk$o que implica $b^2 = pk - a^2$, como supomos que $p \mid a$, temos que existe u inteiro tal que $a = pu$, daí $a^2 = p(pu^2)$ e assim $p \mid a^2$, daí $b^2 = pk - a^2 = pk - p(pu^2) = p(k - pu^2)$ o que acarreta $p \mid a^2$ e assim $p \mid a$, ora mas isto é um absurdo pois sabemos que $p \nmid a$. O que nos leva a conclusão de que $p \nmid a$, da mesma forma se supormos que $p \mid b$ pelos mesmo argumentos feito para o caso anterior conluíremos que $p \nmid a$ e de forma análoga concluíremos que $p \nmid b$. Vamos utilizar o seguinte argumento: dados a e b inteiros com $b \neq 0$, mostrar que existem inteiros q e r satisfazendo $a = qb \pm r$, onde $0 \leq r \leq \frac{b}{2}$. De fato, pelo algorítmo de Euclides existem q e s de modo que $a = qb+s$, onde $0 \leq s < b$. Se $0 \leq r \leq \frac{b}{2}$, daí podemos tomar $r = s$ e teremos $0 \leq r \leq \frac{b}{2}$, agora se $s > \frac{b}{2}$, podemos escrever $a = qb + r - b + b = qb + b + r - b = q(b+1) + r - b$, observemos $s > \frac{b}{2}$, ao subtrairmos b teremos o seguinte

$$\frac{b}{2} - b \leq s - b < b - b \Rightarrow -\frac{b}{2} \leq s - b \leq 0 \Rightarrow 0 < -(s-b) \leq \frac{b}{2},$$

chamando $r = s - b$, assim, poderemos escrever $a = q'b - r$. Daí, usando o resultado que acabamos de mostrar, existem q_1, q_2, r_1 e r_2 satisfazendo

$$a = q_1 p \pm r_1,\ 0 < r_1 \leq \frac{p}{2}$$

$$b = q_2 p \pm r_2,\ 0 < r_2 \leq \frac{p}{2}$$

Assim, isolando r_1 e r_2 e logo em seguida elevando ao quadrado obtemos:

$$\pm r_1 = a - pq_1 \Rightarrow r_1^2 = (a - pq_1)^2$$

$$\pm r_2 = a - pq_2 \Rightarrow r_2^2 = (a - pq_2)^2$$

Somando estas equações teremos que

$$r_1^2 + r_2^2 = a^2 - 2pq_1 + p^2q_1^2 + b^2 - 2pq_2 + p^2q_2^2$$

daí podemos escrevê-la da seguinte maneira

$$\begin{aligned} r_1^2 + r_2^2 &= a^2 + b^2 + (-2pq_1 + p^2q_1^2 - 2pq_2 + p^2q_2^2) \\ &= a^2 + b^2 + pm, \end{aligned} \tag{2.13}$$

onde $m = -2q_1 + pq_1^2 - 2q_2 + pq_2^2$, lembremos do fato que $p \mid a^2 + b^2$, ou seja, existe s inteiro de modo que $a^2 + b^2 = ps$, assim, $r_1^2 + r_2^2 = ps + pm = p(s + m) = pM$, lembremos ainda que $r_1 \leqslant \frac{p}{2}$ e $r_2 \leqslant \frac{p}{2}$, daí $r_1^2 \leqslant \frac{p^2}{4}$ e $r_2^2 \leqslant \frac{p^2}{4}$, portanto, $r_1^2 + r_2^2 \leqslant \frac{p^2}{4} + \frac{p^2}{4} = \frac{p^2}{2}$, agora podemos escrever que $pM \leqslant \frac{p^2}{2}$. Vamos mostrar que sendo r_1 e r_2 menores do que p, tomando qualquer divisor comum de r_1 e r_2 então este divisor comum dividirá M. De fato, seja k um divisor comum de r_1 e r_2 então existem inteiros de modo que $r_1 = ks$ e $r_2 = kt$, substituindo em $r_1^2 + r_2^2$, temos que

$$r_1^2 + r_2^2 = k^2s^2 + k^2t^2 = Mp \Rightarrow k^2(s^2 + t^2) = Mp \Rightarrow k^2 \mid Mp,$$

mas lembremos que $k \leq r_1 < p$ então $k < p$, sendo p primo e $k < p$ não é possível p está na decomposição primária de k, logo $k \nmid p$, assim, podemos dizer que $(k, p) = (k^2, p) = 1$, portanto temos $k^2 \mid Mp$ e $(k^2, p) = 1$ e assim $k^2 \mid M$ implica $k \mid M$. Caso seja necesário uma simplificação por k^2 teremos

$$r_1^2 + r_2^2 = Mp \Rightarrow \frac{r_1^2 + r_2^2}{k^2} = \frac{Mp}{k^2} \Rightarrow a_1^2 + b_1^2 = np,$$

onde $(\frac{r_1}{k}, \frac{r_2}{k}) = 1$ o que nos diz que $(a_1, b_1) = 1$. Da proposição 2.3 podemos, ter a certeza de que n possui um fator primo o qual chamaremos de p_1 de modo que este não seja soma de dois quadrados e que $p_1 \leq \frac{p}{2}$. Ao repetirmos este processo tomando p_1 ao invés de p obteremos um primo p_2, onde $p_2 < p_1 \leq \frac{p}{2}$, que não é soma de dois quadrados, ora mas isto é um absurdo pois np é soma de dois quadrados de números relativamente primos como é mostrado na proposição 2.2.

□

Teorema 2.5 *Todo primo da forma $4n + 1$ possui representação única como soma de dois quadrados.*

Demonstração: O teorema 1.1 diz que -1 é um resíduo quadrático de qualquer primo $p \equiv 1 \pmod 4$ o que quer dizer que existe um inteiro a tal que $a^2 \equiv -1 \pmod p$ para primos $p \equiv 1 \pmod 4$. Existindo tal a inteiro de modo que $a^2 \equiv -1 \pmod p$ então $a^2 + 1 \equiv 0 \pmod p$ o que implica $p \mid a^2 + 1$ e utilizando a proposição 2.4 podemos concluir que p é a soma de dois quadrados. Bem, acabamos de concluir que de fato p é soma de dois quadrados, vamos agora mostrar que a representação de p como soma de dois quadrados é única. Supondo que existem duas representações distintas para p, ou seja, $p = a^2 + b^2 = c^2 + d^2$. Sabemos que sendo p um número ímpar então um dos números a e b é ímpar e o outro deve ser par, da mesma forma procedemos para c e d.

Temos que

$$c^2 + b^2 = c^2 + d^2 \Rightarrow a^2 - c^2 = d^2 - b^2 \Rightarrow (a + c)(a - c) = (d + b)(d - b).$$

Consideremos $r = (a - c, d - b)$, daí existe m inteiro tal que $a - c = mr$ e existe n inteiro de modo que $d - b = nr$ onde $(m, n) = 1$, de fato, sabendo que

$$r = (a - c, d - b) = (mr, nr).$$

então

$$r = (mr, nr) \Rightarrow \frac{1}{r}r = \frac{1}{r}(mr, nr) \Rightarrow \left(\frac{mr}{r}, \frac{nr}{r}\right) = 1 \Rightarrow (m, n) = 1$$

Portanto, $m(a + c) = n(d + b)$. Sabendo que $(m, n) = 1$ e considerando $s = (a + c, d + b)$, podemos concluir que $a + c = ns$ e $d + b = ms$. Sendo a e c ambos pares ou ímpares teremos que r e s são pares. De fato, se a e c são ambos pares temos que $a - c = mr = 2k - 2s = 2(k - s)$ e $a + c = ns = 2t - 2y = 2(t - y)$, ou seja, mr e ns são pares então há as seguintes possibilidades m e r pares e n e s pares ou m par e r ímpar e n par e s ímpar ou m ímpar e r par e n ímpar e s par, observemos que as duas primeiras possibilidades não podem ocorrer pois $(m, n) = 1$ restando então a terceira e por ela concluímos que r e s são pares. Da mesma forma, se considerarmos a e c ímpares faremos de forma análoga ao anterior. Se apenas um deles é par consequentemente o utro é ímpar, digamos a é par e c é ímpar então $a - c = mr = 2k - (2s + 1) = 2(k - s) - 1$ e $a + c = ns = 2t - (2y + 1) = 2(t - y) - 1$ o que nos leva a conclusão de que mr e ns são ímpares assim, m é ímpar e r é ímpar e n é ímpar e s é ímpar daí concluímos que r e s são ambos ímpares e também concluímos neste caso que m e n também são ímpares. Temos que

$$\begin{aligned}(r^2 + s^2)(m^2 + n^2) &= m^2r^2 + n^2r^2 + m^2s^2 + n^2s^2 \\ &= (a - c)^2 + (d + b)^2 + (d - b)^2 + (a + c)^2.\end{aligned}$$

Assim,

$$\begin{aligned}(a - c)^2 + (d + b)^2 + (d - b)^2 + (a + c)^2 = \\ a^2 - 2ac + c^2 + a^2 + 2ac + c^2 + d^2 + 2db + b^2 + d^2 - 2db + b^2 = \\ 2(a^2 + b^2) + 2(c^2 + d^2). \quad (2.14)\end{aligned}$$

Portanto,

$$\begin{aligned}\frac{(r^2+s^2)(m^2+n^2)}{4} &= \frac{a^2+b^2}{2}+\frac{c^2+d^2}{2}\\ &= \frac{p}{2}+\frac{p}{2}=p.\end{aligned} \tag{2.15}$$

Podemos tirar as seguintes conclusões sobre a expressão acima, sendo r e s ambos pares p será o produto de $\frac{r^2+s^2}{2}$ e $\frac{m^2+n^2}{2}$ e estes são maiores do que 1. Agora sendo r e s ímpares não podemos ter ambos iguais a 1, pois caso fosse possível teríamos $a-c=m$, $a+c=n$, $d-b=n$ e $d+b=m$ somando as duas primeiras e as duas últimas obtemos que $a=\frac{m+n}{2}$ e $d=\frac{m+n}{2}$, portanto $a=d$, sendo $a=d$ e subtraindo a segunda pela primeira e a quarta pela terceira, obtemos $b=\frac{m-n}{2}$ e $c=\frac{m-n}{2}$, o que acarreta $b=c$. Mas, isto não é possível pois as duas representações de p são distintas, ou seja, $a\neq d$ e $c\neq b$. Quando r e s são ímpares p, será o produto de $\frac{r^2+s^2}{2}$ e $\frac{m^2+n^2}{2}$ e estes fatores são diferentes de 1. Mas, observemos que p é um primo ímpar e de modo algum poderá ser escrito como as expressões ditas anteriormente, portanto podemos concluir que a representação de p é única.

□

2.6 Descenso Infinito de Fermat

Considerando a equação $f(x_1,x_2,\ldots,x_n)=0$ o método do descenso infinito consiste em verificar a não existência de soluções inteiras positivas ou mostrar sob certas condições todas as soluções inteiras desta equação. Ao considerarmos o conjunto solução $A=\{(x_1,\ldots,x_n)\in\mathbb{Z}|f((x_1,\ldots,x_n)=0\}$ e supondo que este seja não vazio, desejamos construir uma função $\phi: A\to\mathbb{N}$ e consideraremos uma solução $(x_1,x_2,\ldots,x_n)\in A$ onde $\phi(x_1,x_2,\ldots,x_n)$ é a menor possível. A partir desta encontraremos uma outra menor do que ela e portanto teremos assim uma contradição o que nos levarará que o conjunto solução da equação é vazio.

Façamos o exemplo abaixo e tentemos compreender esta técnica elaborada por Fermat.

Exemplo: (Fermat). Demonstrar que a equação $x^4 + y^4 = z^2$ não possui soluções inteiras positivas. $\diamond$

Suponhamos que $x^4 + y^4 = z^2$ possui uma solução inteira onde $x, y, z > 0$. Portanto, existe uma solução (a, b, c) onde podemos consirear c mínimo. Temos a e b primos entre si. De fato, se $d = (a, b) > 1$ poderíamos substituir (a, b, c) por $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2})$ e este terno é solução da equação, veja que $(\frac{a}{d})^4 + (\frac{b}{d})^4 = \frac{a^4+b^4}{d^4}$. Note que o terno (a, b, c) é solução de $x^4 + y^4 = z^2$ então $(\frac{a}{d})^4 + (\frac{a}{d})^4 = \frac{a^4+b^4}{d^4} = \frac{c^2}{d^4}$, ou seja, o terno $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2})$ é solução da equação e $\frac{c}{d^2} < c$ o que contradiz a minimilidade de c. Sabemos que $(a^2)^2 + (b^2)^2 = c^2$ temos assim que o terno (a^2, b^2, c) é um terno pitagórico primitivo e daí existem números inteiros positivos m e n que são primos entre si de modo que

$$a^2 = m^2 - n^2,\ b^2 = 2mn \text{ e } c = m^2 + n^2.$$

Notemos que $a^2 + n^2 = m^2$ satisfaz a relação de Pitágoras e portanto a terna ordenada (a, n, m) é uma terna pitagorica primitiva e assim podemos concluir que m é impar. De fato, note que m é ímpar pois a e n não podem ser ambos pares, devido a e n serem primos. Portanto supomos que a é ímpar, n não pode ser ímpar pois caso contrário

$$a = 2k + 1 \Rightarrow a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 \Rightarrow a^2 \equiv 1 \pmod 4$$

e

$$n = 2s + 1 \Rightarrow n^2 = 4s^2 + 4s + 1 \Rightarrow n^2 \equiv 1 \pmod 4,$$

assim,

$$a^2 + n^2 = m^2 \equiv 1 + 1 = 2 \pmod 4$$

o que não é possível pois todo número ao quadrado quando dividido por 4 deixa resto 0 ou 1, portanto n^2 é par e consequentemente m^2 é ímpar e daí podemos concluir que m é ímpar. Assim, de $b^2 = 2mn$ concluímos que b é par e consequentemente n também. Observemos ainda que $b^2 = (2n)m$ é um quadrado perfeito e $(2n, m) = 1$, de fato, $(2n, m) = 1$, pois $(n, m) = 1$ implica $(2n, m) = (2, m)$ onde $(2, n) = 1$ ou 2, vamos mostrar que não pode ocorrer $(2, m) = 2$, pois neste caso $2 \mid m$ o que nos diz que m é par, mas sabemos que m é ímpar assim $(2n, m) = (2, m) = 1$. Sendo $b^2 = (2n)m$ quadrado perfeito temos que $2n$ e m também o são. De fato, suponhmamos que $2n$ não é um quadrado perfeito e então existe um fator primo $p_i^{\alpha_i}$ de $2n$ que aparece uma quantidade ímpar de vezes no produto, ou seja, α_i é ímpar e como $(2n, m) = 1$ este fator não aparece em m, sabendo que $b^2 = (2n)m$ é um quadrado perfeito então o fator p_i deve aparecer uma quantidade par de vezes, mas isto é um absurdo, o que nos leva a conclusão de que $2n$ e m são ambos quadrados perfeitos.

Sendo então, $2n$ e m quadrado perfeitos então existem s e t positivos de modo que $2n = 4s^2$ e $m = t^2$. Por outro lado sabendo que $a^2 + n^2 = m^2$, então existirão inteiros positivos i e j primos entre si onde

$$a = i^2 - j^2,\ n = 2ij \text{ e } m = i^2 + j^2.$$

Daí, $s^2 = \frac{n}{2} = ij$, logo i e j são quadrados perfeitos, digamos $i = u^2$ e $j = v^2$. Portanto, teremos $m = i^2 + j^2$, $i = u^2$, $j = v^2$ e $m = t^2$, assim, $t^2 = u^4 + v^4$, de fato $m = (t)^2 + (j)^2 = (u^2)^2 + (v^2)^2 = u^4 + v^4 = t^2$, isto é, (u, v, t) é outra solução da equação original. Porém,

$$t \leq t^2 = m \leq m^2 < m^2 + n^2 = c \Rightarrow t < c$$

e lembremos que $t \neq 0$, pois $m \neq 0$.

2.7 O Último Teorema de Fermat

Este sem dúvida alguma é um dos mais belos teoremas de todos os tempos, o qual desafiou matemáticos extraordinários através dos seus 300 anos em que ficou sem uma demostração. Pierre de Fermat era considerado um matemático amador, mesmo sendo o seu trabalho de alta qualidade. Quando Fermat morreu, seu filho encontra algumas anotações do pai e em uma dessas anotações estava escrito o seguinte :"é impossível para um cubo ser escrito como a soma de dois cubos ou uma quarta potência ser escrita como soma de duas quartas potências ou, em geral, para qualquer número que é uma potência maior do que a segunda, ser escrito a soma de duas potências com o mesmo expoente". Ele também escreveu que tinha encontrado uma demonstração para esta afirmação, porém não tinha como escrvê-la naquelas margens. Muitos matemáticos importantes se dedicaram a solucionar este "último teorema de Fermat", mas nenhum deles teve êxito, mas destas inúmeras tentativas surgiram teorias importantes em matemática, como por exemplo a teoria dos anéis comutativos, dentre outros. Este teorema virou uma lenda no mundo da matemática, chegando a existir até um prêmio para quem o demonstrasse. A façanha coube ao matemático Andrew Wiles um, professor da universidade de Princenton, o qual na verdade demonstrou a conjectura de Taniyama-Shimura, ficando assim demonstrado o último teorema de Fermat.

Para ilustrar o quanto este problema é difícil acompanharemos a demonstração do teorema de Fermat para caso onde $n = 3$, que foi originalmente feita por Euler, mas não estava completa. Assim vejamos primeiramente o lema abaixo:

Lema 2.3 *Todas as soluções de* $s^3 = a^2+3b^2$ *em inteiros positivos tais que* $(a, b) = 1$ *e* s *é ímpar são dadas por*

$$s = m^2 + 3n^2,\ a = m^3 - 9mn^2,\ b = 3m^2n - 3n^3$$

com $m + n$ *ímpar e* $(m, 3n) = 1$.

Demonstração: Vamos primeiramente mostrar que s, a e b assim definidas satisfazem a equação $s^3 = a^2 + 3b^2$, vejamos que

$$\begin{aligned} s^3 = (m^2 + 3n^2)^3 &= (m^2)^3 + 3(m^2)(3n^2) + 3(m^2)(3n^2) + (3n^2)^3 \\ &= m^6 + 9m^4n^2 + 27m^2n^4 + 27n^6 \end{aligned} \tag{2.16}$$

e

$$\begin{aligned} a^2 + 3b^2 &= (m^3 - 9mn^2)^2 + 3(3m^2n - 3n^3)^2 \\ &= (m^3)^2 - 2(m^3)(9mn^2)^2 + 3((3m^2n)^2 - 2(3m^2n)(3n^3) + (3n^3)^2) \\ &= m^6 + 9m^4n^2 + 27m^2n^4 + 27n^6. \end{aligned} \tag{2.17}$$

portanto, verificamos que $s^3 = a^2 + 3b^2$. Observemos que

$$\begin{aligned} (a, b) = (m^3 - 9mn^2, 3m^2n - 3n^3) &= (m(m^2 - 9n^2), 3n(m^2 - n^2)) \\ &= (m^2 - 9n^2, m^2 - n^2) \\ &= (8n^2, m^2 - n^2). \end{aligned} \tag{2.18}$$

Podemos fazer as seguintes proposições :

- n par e m é ímpar;
- n par e m par;
- n ímpar e m par;
- n ímpar e m ímpar.

Mas, lembremos que por hipótese que $m + n$ é par então apenas as suposições abaixo são possíveis de ocorrer:

- n par e m é ímpar;
- n ímpar e m par.

Em ambos os casos teremos que $(8n^2, m^2 - n^2) = 1$. Suponhamos agora que a terna (a, b, s) é uma solução da equação, consideremos então p primo de modo que $p \mid s$, sendo $(a, b) = 1$ e ainda s ímpar temos $p \nmid a$,$p \nmid b$ e $p > 3$. De $s^3 = a^2 + 3b^2$ temos $a^2 = s^3 - 3b^2$, note que $p \mid s$, assim $a^2 = p^3t^3 - 3b^2 = p(p^2t^3) - 3b^2 \Rightarrow a^2 \equiv -3b^2 \pmod{p}$, temos então pela lei da reciprocidade quadrática

$$\left(-\frac{3}{p}\right) = 1 \Leftrightarrow \left(\frac{p}{3}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{6}.$$

De fato, sendo $\left(-\frac{3}{p}\right) = 1$, temos que

$$\begin{aligned}\left(-\frac{3}{p}\right) = \left(-\frac{1}{p}\right)\left(\frac{3}{p}\right) = 1 &\Leftrightarrow \left(-\frac{1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}} = 1 \\ &\Leftrightarrow \left(-\frac{1}{p}\right)\left(-\frac{1}{p}\right) = 1 \\ &\Leftrightarrow \left(-\frac{1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{4}. \qquad (2.19)\end{aligned}$$

Sabemos que existem números m_1 e n_1 de modo que $p = m_1^2 + 3n_1^2$, assim $p^3 = (m_1^2+3n_1^2)^3 = m_1^6+9m_1^4n_1^2+27m_1^2+27n_1^6$, onde $p^3 = c^2+3d^2$ onde $c = m_1^3-9m_1n_1^2$ e $d = 3m_1^2n_1 - 3n_1^3$. Sabemos que existem inteiros m_1 e n_1 tais que $p = m_1^2 + 3n_1^2$ e assim, $p^3 = c^2+3d^2$ onde $c = m_1^3-9m_1n_1^2$ e $d = 3m_1^2n_1-3n_1^3$. Podemos observar que $(p, m_1) = (p, n_1) = 1$ e ainda $p > 3$, logo $(p, c) = (p, d) = 1$, como na demonstração acima de $(a, b) = 1$. Utilizando o método da indução sobre o número de divisores de primos de s. Se $s = 1$ teremos pelo caso anterior que o problema está resolvido, vamos supor agora que este resultado seja válido para todo s que tenha extamente k fatores primos, digamos $s = pt$ onde p é primo $p > 3$, observemos que $t^3p^6 = s^3p^3$, daí

$$t^3p^6 = s^3p^3 = (a^2 + 3b^2)(c^2 + 3d^2) = (ac \pm 3bd)^2 + 3(ad \mp bc)^2$$

onde podemos observar que

$$(ad + bc)(ad - bc) = (ad)^2 - (bc)^2 = d^2(a^2 + 3b^2) - b^2(c^2 + 3d^2) = p^3(t^3d^2 - b^2),$$

logo $p^3 \mid (ad+bc)(ad-bc)$. Se p divide os dois fatores, temos que $p \mid ad$ e $p \mid bc$. Lembremos ainda que $(p, c) = (p, d) = 1$ o que acarreta $p \mid a$ e $p \mid b$, ora mas isto contradiz a hipótese $(a, b) = 1$, logo, p^3 divide extamente um dos fatores, e tomando adequadamente os sinais vamos ter

$$u = \frac{ac \pm 3bd}{p^3} \text{ e } u = \frac{ad \mp bc}{p^3}$$

como sendo números inteiros tais que $t^3 = u^2 + 3v^2$, como t tem k fatores primos segue por hipótese de indução que

$$t = m_2^2 + 3n_2^2 \text{ , } u = m_2^3 - 9m_2n_2^2 \text{ e } v = 3m_2^2n_2 - 3n_2^3.$$

Agora, dado que $a = uc + 3vd$ e $b = \pm(ud - vc)$, então substituindo t,u,v, c e d em termos de m_i e n_i $(i = 1, 2)$ em s, a e b e fazendo $m = m_1m_2 + 3n_1n_2$, $n = m_1n_2 - m_2n_1$, onde obtemos o que desejávamos mostrar.

□

Proposição 2.5 *A equação diofantina $x^3 + y^3 = z^3$ não possui soluções inteiras com $xyz \neq 0$.*

O método utilizado para a demonstração deste caso particular é basicamente o método do descenso infinito de Fermat.

Demonstração: vamos supor que (x, y, z) é solução de $x^3 + y^3 = z^3$ onde $x, y, z > 0$ e de modo que xyz seja mínimo. Como qualquer fator comum de dois destes números é também fator comum do terceiro x, y e z são primos relativos dois

a dois e em particular um destes será par. observe que $x = y$ não é possível de ocorrer, pois se fosse teríamos que $x^3 + x^3 = z^3$ implica $2x^3 = z^3$, observe que do lado direito o expoente da maior potência de 2 é um múltiplo de 3 enquanto do lado esquerdo teremos não. Assim, vamos supor que x e y são ímpares e z é par podemos então escrever $x = p + q$ e $y = p - q$, onde $p > 0$ e $q > 0$ primos entre si (pois x e y também são primos entre si e de diferente paridades). Daí,

$$\begin{aligned} x^3 + y^3 &= (x + y)(x^2 - xy + y^2) \\ &= 2p((p + q)^2 - (p + q)(p - q) + (p - q)^2) \\ &= 2p(p^2 + 3q^2). \end{aligned} \tag{2.20}$$

Portanto, $2p \mid p^2+3q^2$ é um cubo perfeito. De forma análoga supondo z ímpar e x ou y é par, podemos supor sem a perda de generalidade que y é ímpar, e substituindo $z = q + p$ e $y = q - p$, teremos

$$\begin{aligned} x^3 = z^3 - y^3 &= 2p(p + q)^2 + (p + q)(p - q) + (q - p)^2 \\ &= 2p(p^2 + 3q^2). \end{aligned} \tag{2.21}$$

Como $p^2 + 3q^2$ é ímpar e $2p(p^2 + 3q^2)$ é um cubo perfeito, temos que p será par. Calculando o máximo divisor comum de p e de $p^2 + 3q^3$ obtemos

$(p, p^2 + 3q^2) = (p, 3q^2) = (p, 3)$, assim, $(p, p^2 + 3q^2) = 1$ ou $(p, p^2 + 3q^2) = 3$.

No primeiro, existem naturais a e b tais que $a^3 = 2p$ e $b^3 = p^2 + 3q^2$, neste caso sabemos que existem inteiros m e n com paridades diferentes e primos relativos, de modo que

$$b = m^2 + 3n^2,\ p = m^3 - 9mn^2,\ q = 3m^2n - 3n^3.$$

Logo, $a^3 = 2m(m-3n)(m+3n)$, observemos que os números $2m$, $(m-3n)(m+3n)$ são primos relativos, logo existem inteiros e, f e g tais que $2m = e^3$, $m - 3n = f^3$

e $m + 3n = g^3$. Em particular, teremos que $f^3 + g^3 = e^3$, como $efg = a^3 = 2p \leq x + y < xyz$, teremos uma solução menor, o que contradiz a escolha de x, y e z. No caso $3 \mid p$, então $p = 3r$ com $(r, q) = 1$, logo $z^3 = 18r(3r^2 + q^2)$ ou $x^3 = 18r(3r^2 + q^2)$ ou $x^3 = 18r(3r^2 + q^2)$ e assim, existem inteiros positivos a e b tais que $18r = a^3$ e $3r^2 + q^2 = b^3$. Novamente existirão inteiros m e n tais que

$$b = m^2 + 3n^2 \ , \ q = m^3 - 9mn^2 \text{ e } r = 3m^2n - 3n^3.$$

Daí, segue que $a^3 = 27(2n)(m-n)(m+n)$, de igual forma teremos que os números $2n$, $m - n$ e $m + n$ são primos relativos, portanto existem inteiros positivos e, f e g tais que $2n = e^3$, $m - n = f^3$, $m + n = g^3$. Assim, $e^3 + f^3 = g^3$, que também contradiz o fato de que (x, y, z) é mínimo.

□

Capítulo 3

Uma Proposta de Atividade para o Ensino Médio

Neste capítulo pretendemos fazer uma proposta de atividade para o ensino médio, versando sobre a teoria exposta capítulo 2. Faremos primeiramente a apresentação da atividade que está dividida em duas partes e posteriormente faremos a análise e solução para a mesma. Essa atividade tem por objetivo fazer com que o aluno do ensino médio compreenda os teoremas que caracterizam a representação de dois e quatro quadrados. Através de tentativas e erros ele irá perceber que mesmo sendo estes teoremas que aparentemente são difíceis para o nível escolar em que estão, é possível que estes alunos possam compreender e usar os resultados destes teoremas, até com certa facilidade em alguns casos. O que da motivação para estes alunos, fazendo assim que percebam que mesmo teorias que até certo ponto são avançadas para o nível escolar deles, podem produzir resultados simples e de fácil entendimento. Isto faz com que o aluno vá perdendo o medo que tem da matemática, deixando de considerá-la como um bicho de sete cabeças e tornando-a mais prazerosa de estudar.

3.1 Apresentação da Atividade Proposta

Faremos aqui a apresentação da atividade proposta, ela está baseada no teorema 2.1, Lema 2.1, teorema 2.2 e teorema 2.5, apresentados e demonstrados no capítulo 2. Os Exercícios foram retirados de [2] na página 138 e foram adptados de modo a se encaixarem nos propósitos desta sequência didática, que é justamente fazer com que o aluno compreenda a essência dos principais teoremas citados no capítulo 2.

Atividade Proposta

1^{a} Parte

- Observe os primos 11, 17, 19, 23, 29 e 31. Quais destes podemos representar como soma de dois quadrados. Por exemplo, podemos escrever os números primos 5 e 13 como soma de dois quadrados da seguinte forma: $5 = 2^2 + 1^2$ e $13 = 3^2 + 2^2$.

- Agora façamos a divisão de cada primo acima por 4 e observemos o valor dos restos. A partir da observação dos restos é possível dizermos alguma coisa sobre estes números?

- Os números 6, 8, 10 , 16, 36 podem ser representados como uma soma de dois quadrados?

- Observe que os números 13 e 29 podem ser representados por uma soma de dois quadrados. Podemos a partir da multiplicação destes dois números produzir um outro número que pode ser representado por uma soma de dois quadrados? Em caso afirmativo dê a sua representação?

- será que existe outra representação como soma de dois quadrados para os primos 13 e 29? E para qualquer outro primo que possa ser representado por uma soma de dois quadrados ?

- Será possível representar o número 29 como soma de quatro quadrados ? Em caso afirmativo dê esta representação.

2ª Parte

- Dizer se existe um triângulo retângulo isósceles de lados inteiros.

3.2 Solução e Comentário de cada Item

1ª Parte

- Observe os primos 11, 17, 19, 23, 29 e 31. Quais destes podemos representar como soma de dois quadrados. Por exemplo, podemos escrever os números primos 5 e 13 como soma de dois quadrados da seguinte forma: $5 = 2^2 + 1^2$ e $13 = 3^2 + 2^2$.

Neste exercício primeiramente é deixado o aluno livre de modo que este por meio de tentativas vá solucionando o exercício, nesse processo acertos e erros vão ser bastante comuns, visto que o aluno ainda não conhece o resultado do teorema 2.1. Possivelmente a maioria dos alunos não conseguirão resolver esta atividade com êxito num primeiro momento, mas depois da apresentação do resultado geral ficará mais simples o seu entendimento pleno por parte do aluno. Destes números os que podem ser representados por uma soma de dois quadrados são 17 e 29, as suas representações são $17 = 4^2 + 1^2$ e $29 = 5^2 + 2^2$. Este exercíco serve para que o aluno tenha o primeiro contato com a ideia de representar um número como uma soma de dois quadrados e preparar terreno para a introdução do resultado geral.

- Agora façamos a divisão de cada primo acima por 4 e observemos o valor dos restos. A partir da observação dos restos é possível dizermos alguma coisa sobre estes números?

Nesta etapa da atividade é necesário que o aluno divida os primos do item anterior por 4, e observe as coincidências entre os restos dos mesmos, observar que o resto dos números que não puderam ser escritos como uma soma de dois quadrados é 3 e dos que puderam ser escritos é 1, isto da margem para que os alunos possam conjecturar algo a respeito da representação de números como soma de dois quadrados. Depois dos alunos tentarem e tirarem as suas próprias conclusões é hora do professor apresentar o teorema 2.1 de modo a adequá-lo a linguagem do ensino médio, podendo ser escrito da seguite forma "um número primo é escrito como uma soma de dois quadrados se for dois ou deixar resto 1 ao ser dividido por 4".

- Os números 6, 8, 10 , 16, 36 e 27 podem ser representados como uma soma de dois quadrados?

Neste item os alunos agora devem verificar se sendo agora um número não primo quais as condições para que estes possam ser representados por uma soma de dois quadrados, o caminho natural a seguir por esses alunos depois das estapas passadas é tentar fazer por tentativas, pois os resultados anteriores não ajudam muito. Neste caso, aparece o teorema 2.2 que fala na decomposição de um número que é representado por uma soma de dois quadrados, neste teorema é explicitado como é a fatoração de números dessa natureza, assim depois que os alunos tentarem por meio de tentativas, o professor deve explicar o teorema 2.2 aos alunos, ou seja, dizer na fatoração de um número que pode ser representado por uma soma de dois quadrados deve aparecer uma potência do fator primo 2, potências de fatores primos que podem ser representados por uma soma de dois quadrados e caso apareça outro fator primo que não seja como o dito anteriormente o expoente deste tem que ser par.

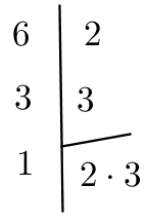


Figura 3.1:

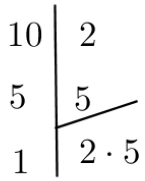


Figura 3.2:

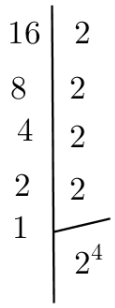


Figura 3.3:

Nas figuras 3.1, 3.2 e 3.3, temos as fatorações dos números 6, 10 e 16 respectivamente, observemos que nenhum destes números obedece as condições do teorema 2.2, pois na fatoração do 6, não há fator primo congruente a 1 módulo 4, analogamente na fatoração do 10, já o número 16 podemos escrever a fatoração do mesmo da seguinte forma de modo a se adequar ao teorema: $16 = 2^4 = 2^4 \cdot 13^0 \cdot 7^0$, observe que esta fatoração cumpre as condições do teorema 2.2, portanto podemos escrever 16, como soma de dois quadrados $16 = 4^2 + 0^2$. Vamos ver agora as fatorações dos números 8 e 36 e 27

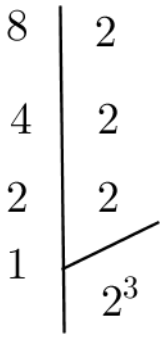


Figura 3.4:

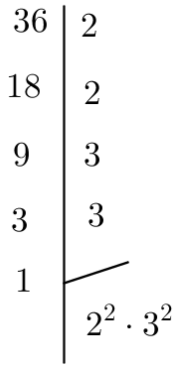


Figura 3.5:

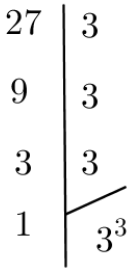


Figura 3.6:

Note que os números 8 e 36 podem ser representados como uma soma de dois quadrados pois suas fatorações se enquadram nos moldes do teorema 2.2, já o número $27 = 3^3$ não pode ser representado pois o fator primo que é congruo a 3 módulo 4 possui expoente ímpar. Portanto, os números que podem ser escritos como soma de dois quadrados são $8 = 2^2 + 2^2$, $36 = 6^2 + 0^2$ e $16 = 4^2 + 0^2$.

- Observe que os números 13 e 29 podem ser representados por uma soma de dois quadrados. Podemos a partir da multiplicação destes dois números produzir um outro número que pode ser representado por uma soma de dois quadrados? Em caso afirmativo dê a sua representação?

Nesta etapa o aluno já deve conhecer O teorema 2.1 e saber de fato que os números 13 e 29 podem ser representados por uma soma de dois quadrados, o objetivo desta tarefa é fazer com que o aluno observe que se dois números são representados por uma soma de dois quadrados, então podemos gerar outro número da mesma natureza fazendo a multiplicação entre eles. Num primeiro momento não falamos no resultado do lema 2.1 e deixamos os alunos tentarem verificar este resultado, alguns podem tentar usar o teorema 2.1 ao fazerem a multiplicação dos números 13 e 29, mas não terão êxito pois o número gerado não é primo, então restará para eles a tentativa de escever o resultado da multipliação como uma soma de dois quadrados , depois deles tentarem por alguns minutos e tirarem suas própias conlusões ai é que o professor entra com o resultado do lema 2.1 comprovando que realmente a multipliação de dois números que são soma de dois quadrados é um número que é soma de dois quadrados. É até possível que o professor caso deseje fazer a demonstração deste lema para os alunos, pois as ferramentas matemáticas envolidas são de conhecimento dos alunos do ensino médio e assim torna o entendimento deste resultado mais simples. Portato, teremos que $13 = 3^2 + 2^2$ e $29 = 5^2 + 2^2$, assim pelo lema 2.1 temos que $(29)(13) = (5^2+2^2)(3^2+2^2) = (5\cdot 3+2\cdot 2)^2+(5\cdot 2-2\cdot 3)^2 \Rightarrow 377 = 19^2+4^2$.

- será que existe outra representação como soma de dois quadrados para os primos 13 e 29? E para qualquer outro primo que possa ser representado por uma soma de dois quadrados ?

Neste momento é deixado novamente aos alunos a por tentativas verificarem se há como obter outra representação como soma de dois quadrados para os primos 13 e 29. Notemos que $13 = 3^2 + 2^2$ e se tentarmos encontrar outra representação para este número não teremos êxito, pois pelo teorema 2.5 os primos que deixam resto 1 ao serem divididos por 4 possuem representação única como soma de dois quadrados. No primeiro momento, os alunos não terão esta informação, tirarão suas conclusões por meio de tentativas, ou seja, acertos e erros, posteriormente é que o professor deve falar sobre este Teorema.

- Será possível representar o número 29 como soma de quatro quadrados ? Em caso afirmativo dê esta representação

Bem, este item visa fazer com que o aluno venha a descobrir que qualquer número inteiro positivo pode ser representado por uma soma de quatro quadrados, que é justamente o resultado do teorema de Lagrange, posteriormente as tentativas dos alunos o professor faz a apresentação deste resultado. Aqui faremos por tentativas mesmo e chegaremos que $29 = 5^2 + 2^2 + 0^2 + 0^2$.

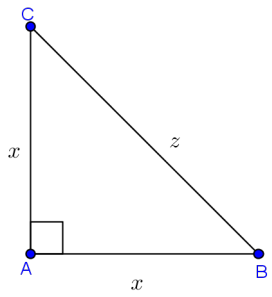
Esta é a primeira etapa da atividade, e o objetivo é fazer com que o aluno se familiarize com os resultados básicos da teoria desenvolvida no capítulo 2.

Vamos agora para a segunda parte da atividade, que é constituida de um único item , uma aplicação da teoria dos números a geometria.

2^{a} Parte

- Dizer se existe um triângulo retângulo isósceles de lados inteiros.

Vamos a solução e comentários sobre este problema. Devemos verificar se existe um triângulo isósceles retângulo de modo que os lados do mesmo sejam inteiros, ou seja, devemos verificar se existem x e z inteiros de modo que $z^2 = x^2 + x^2$ que é a relação de pitágoras, veja a figura abaixo.



Vamos supor que existam tais x e y inteiros de modo a satisfazer a relação de pitágoras, assim, $z^2 = x^2 + x^2$, notemos que z^2 não pode ser primo pois, tem 1, p e p^2 como divisores. Assim temos que analisar o caso

- z^2 não primo;

Se z^2 não é primo e tendo $z^2 = x^2 + x^2$ observemos que do lado direito temos uma quantidade par de fatores 2 e do lado esquerdo há uma quantidade ímpar de fatores 2, portanto temos aqui uma contradição, daí concluímos que sendo z^2 um número não primo não há como termos um triângulo retângulo isósceles de lados inteiros.

Daí, não há possibilidade de existir um triângulo isósceles retângulo de lados inteios. Essa etapa da atividade é mais elaborada e exige conhecimentos um pouco mais aprofundados do aluno, fazendo-se assim uma atividade bem interressante para se trabalhar como preparação para as olímpiadas de matemática.

Apêndice A

Resultados Complementares

Trazemos aqui resultados de complementação do texto.

Teorema A.1 *(Teorema de Wilson) Se p é primo, então* $(p-1)! \equiv -1 \pmod{p}$.

Teorema A.2 *(Pequeno Teorema de Fermat) Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{N}$.*

Corolário A.1 *Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^p - 1$.*

Teorema A.3 *(Propriedade da Boa Ordem) Todo subconjunto não vazio de $\mathbb{N}$ possui um menor elemento.*

Teorema A.4 *(Princípio de Indução Matemática). Sejam $a \in \mathbb{N}$ e seja $p(n)$ uma sentença aberta em n. Suponha que*

1. *$p(a)$ é verdade, e que*
2. *$\forall n \geq a$, $p(n) \Rightarrow p(n+1)$ é verdade,*

então, $p(n)$ é verdade para todo $n \geq a$.

Teorema A.5 *(O principio da casa dos pombos) Se* $n+1$ *pombos são colocados em* n *gaiolas, então pelo menos uma gaiola deverá conter* 2 *ou mais pombos.*

Para o leitor interessado em maiores detalhes sobre a demonstração dos quatro primeiros teoremas deste apêndice consultar [2], a demonstração do princípio de indução matemática está em [3] e a demonstração do princípio da casa dos pombos está em [11].

Referências Bibliográficas

[1] **MARTINEZ, Fabio brochero at al**.*Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*, Rio de Janeiro: IMPA, 2011.

[2] **SANTOS, José Plínio de Oliveira**. *Introdução à Teoria dos Números*. Rio de Janeiro: IMPA, 2007.

[3] HEFEZ, Abramo. *Elementos de Aritmética*. Rio de Janeiro, 2011.

[4] **LIMA, Elon Lages**. *Analise Real, volume 1*. Coleção matemática universitária. p. 185-204, Outubro, 2008.

[5] **SANZ, Antonio Pérez**. *Los números poligonales: Una caja de sorpresas con mucha historia*. La Gaceta,331-337, Madri, 1996. Disponível em: <http://dmle.cindoc.csic.es/pdf/GACETARSME200003205.pdf>. Acesso em: 28 Mar.2013.

[6] **SOARES, Stela Zumerle**. *Soma de Quadrados*. FAMAT em Revista. Uberlândia-MG, número 9, p.217-230, Outubro, 2007.Disponível em:<http://www.portal.famat.ufu.br>. Acesso em: 28 Mar.2013.

[7] **CORY, Leo**.*El Teorema de Fermat y sus Historias*. LA GACETA DE LA RSME, Vol. 9.2 (2006), p. 1-42. Disponível

em:<http://www.tau.ac.il/corry/publications/articles/pdf/Fermat20-20Real20Sociedad.pdf>. Acesso em:28. Abr. 2013.

[8] **OLIVEIRA, A. J. Franco de**.*Breve introdução histórica e alguns problemas e conjecturas*.Boletim da SPM, número 6, p.49-64, outubro, 1993. Disponível em:<http://nautilus.s.uc.pt/bspm/revistas/6/049-064.300.pdf>. Acesso em:29.Mar.2013.

[9] **MORGADO, José. Franco de**.*Algumas equações diofantinas*.Boletim da SPM, número 15, p.24-35, Janeiro/Fevereiro, 1990. Disponível em: <http://nautilus.s.uc.pt/bspm/revistas/15/024-035.300.pdf>. Acesso em: 04. Abr. 2013.

[10] **GROSSWALD, Emil. Franco de**.*Representations of integers as sums of squares*.New York, p.13-19, 1985. Disponível em: <http://www-ti.informatik.unituebingen.de/borchert/ArithmeticalCircuits/Grosswald.pdf>. Acesso em: 25.Mai. 2003.

[11] **SANTOS, José Plínio O., Mello, Margarida P., e Murari, Idani T.C.**.*Introdução à Análise Combinatória*.Rio de Janeiro: Editora Ciência Moderna Ltda, 2007.