Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Inteiros que se escrevem como soma de quatro quadrados.

João Luis de Figueiredo

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Trabalho financiado pela Capes

Cuiabá - MT

Julho de 2015

Inteiros que se escrevem como soma de quatro quadrados.

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por João Luis de Figueiredo e aprovada pela comissão julgadora.

Cuiabá, 15 de agosto de 2015.

Prof. Dr. Martinho da Costa Araújo
Orientador

Banca examinadora:

Prof. Dr. Martinho da Costa Araújo
Prof. Dr. José de Arimatéia Fernandes
Prof. Dr. Daniel Carlos Leite

Dissertação apresentada ao curso de Mestrado Profissional em Matemática – PROFMAT, da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

F475i Figueiredo, João Luis de.

Inteiros que se escrevem como soma de quatro quadrados / João Luis de Figueiredo. -- 2015

52 f. ; 30 cm.

Orientador: Martínho da Costa Araújo.

Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2015.

Inclui bibliografia.

1. Soma de quadrados. 2. Identidade de Lagrange. 3. Teorema Lagrange. I. Título.

Dissertação de Mestrado defendida em 10 de Agosto de 2015 e aprovada pela banca examinadora composta pelos Professores Doutores

Prof. Dr. Martinho da Costa Araújo

Prof. Dr. José de Arimatéia Fernandes

Prof. Dr. Daniel Carlos Leite

À minha querida esposa Regiane que sempre está ao meu lado, me apoiando. E certamente a minha mais nova razão de viver: Mylena Isabela.

Agradecimentos

Agradeço primeiramente a Deus que tudo realiza em minha vida. A minha família e esposa pela compreensão da minha ausência. Ao meu orientador Martinho, que sempre me encorajou nos estudos, me dando oportunidades de manter nesta perspectiva. Aos professores do PROFMAT que nos prepararam nas disciplinas, a CAPES e a SBM que incansavelmente elabora/financia projetos como este para contribuir cada vez mais ao avanço científico na área de matemática.

Não sabendo que era impossível
ele foi lá e fez.

Provérbio Chinês.

Resumo

O problema de escrever um número como soma de quadrados, principalmente números primos, é muito antigo e talvez tenha surgido das investigações de Fermat no século $XVII$. Anos mais tarde, o próprio Fermat demonstrou usando números complexos, que todo número primo da forma $4k + 1$ pode ser escrito como soma de dois quadrados. Porém mediante alguns casos, certos números não puderam ser representados neste formato, dando sequência a ideia de estabelecer mais algumas condições para que pudessem ser escritos como soma de três quadrados, até chegarmos ao aspecto geral que todo número pode ser representado como soma de quatro quadrados (Teorema de Lagrange).

Palavras chave: Soma de quadrados. Identidade de Lagrange. Teorema de Lagrange.

Abstract

The problem of writing a number as a sum of squares, mainly prime numbers, is very old and may have emerged from the investigations of Fermat in the seventeenth century. Years later, the Fermat himself demonstrated using complex numbers, that every prime number of the form $4k+1$ can be written as a sum of two squares. But through some cases, certain figures could not be represented in this format, continuing the idea of establishing some more conditions so that they could be written as the sum of three squares, until we reach the general appearance that any number can be represented as a sum of four squares (Theorem of Lagrange).

Keywords: Sum of squares. Lagrange identity. Theorem of Lagrange.

Sumário

Introdução

" O homem é aquilo que sonha ser"
(Autor desconhecido)

No primeiro momento serão apresentados alguns resultados necessários a construção da teoria.Teoremas de suma importância terão destaque nessa primeira parte como o Pequeno Teorema de Fermat, Algoritmo de Euclides e um breve estudo sobre congruências lineares. Em seguida, começaremos com o estudo da problemática de escrever números inteiros positivos como soma de dois quadrados, estabelecendo condições e tentando caracterizar aqueles que não podem ser representados desta forma, finalizando este capítulo com uma condição necessária e suficiente para termos a representação de um número como soma de dois quadrados. Por não termos todos, como soma de dois quadrados, avançamos nos estudos para investigar aqueles que podem ser escritos como soma de três quadrados, identificando suas características e principais resultados. Por fim, temos a identidade de Lagrange que nos ajudará a caracterizar de uma maneira geral que todo número é soma de quatro quadrados, também chamado de Teorema de Lagrange. Esses resultados serão organizados através de lemas de suma importância como o Lema de Thue e a caracterização dos números primos como soma de quatro quadrados, para daí então, pelo Teorema Fundamental da Aritmética, garantirmos que todos os inteiros positivos também podem ser escritos como soma de quatro quadrados.

Capítulo 1

Conceitos preliminares

1.1 Divisibilidade e Algoritmo de Euclides

Alguns resultados serão de suma importância para o desenvolvimento desta teoria. Por isso serão apresentados como conceitos preliminares. Vamos considerar o conjunto dos números naturais como sendo $\mathbb{N} = \{0, 1, 2, 3, ...\}$ e o conjunto dos números inteiros como $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$. Entende - se por $\mathbb{Z}_+ = \{0, +1, +2, +3, ...\}$ como sendo o conjunto dos inteiros não negativos e $\mathbb{Z}_+^* = \{+1, +2, +3, ...\}$ como o conjunto dos inteiros positivos.

Definição 1 *Dados dois inteiros d e a, dizemos que d divide a, representado por $d|a$, se existe $q \in \mathbb{Z}$ tal que:*

$$a = qd.$$

Lema 1 *Dados $a, b, d, x, y \in \mathbb{Z}$ temos:*

(i) Se $d|a$ e $d|b$ então $d|ax + by$.

(ii) Se $d|a$ então $a = 0$ ou $|d| \leq |a|$.

(iii) Se $d|a$ e $a|b$ então $d|b$.

Prova: (i) Se $d|a$ e $d|b$ temos que $\exists\ q_1, q_2 \in \mathbb{Z} /\ a = dq_1$ e $b = dq_2$ então

$$ax + by = (dq_1)x + (dq_2)y = d(q_1x + q_2y).$$

Como $q_1x + q_2y \in \mathbb{Z}$ segue que

$$d|ax + by.$$

(ii) Suponha que $d|a$ e $a \neq 0$. Neste caso, $a = dq, q \neq 0$, assim

$$|a| \geq 1 \Rightarrow |a| = |dq| = |d||q| \geq |d|.$$

(iii) Como $d|a$ e $a|b, \exists\ q_1, q_2 \in \mathbb{Z} \Rightarrow a = dq_1$ e $b = aq_2$ então

$$b = (dq_1)q_2 = d(q_1q_2) \Rightarrow d|b.$$

■

Definição 2 *Dados dois números inteiros a e b não simultaneamente nulos, o maior divisor comum de a e b será chamado de máximo divisor comum de a e b. Representamos o máximo divisor comum de a e b por $mdc(a, b)$.*

Observação 1

Note que para $d = mdc(a, b)$ temos:
(i) $d|a$ e $d|b$.
(ii) Se existe $c \in \mathbb{Z}$ tal que $c|a$ e $c|b$ então $c|d$.
(iii) $mdc(a, b) = mdc(b, a)$.
(iv) $mdc(a, b) = mdc(a, b - a)$, com $a < b$.

Exemplo 1 *O $mdc(2n, 2n + 1) = 1$.*

De fato, $mdc(2n, 2n + 1) = mdc(2n, (2n + 1) - (2n)) = mdc(2n, 1) = 1$.

Definição 3 *Para $x \in \mathbb{R}$, definimos a parte inteira de x como sendo o único $k \in \mathbb{Z}$ tal que*

$$k \leq x < k + 1.$$

Representamos a parte inteira de x por $\lfloor x \rfloor$.

Exemplo 2 $(i)\ \lfloor 3, 72 \rfloor = 3$ $\qquad\qquad$ $(ii)\ \left\lfloor \sqrt{2} \right\rfloor = 1$

Definição 4 *Seja S um subconjunto de $\mathbb{N}$. Dizemos que um número natural a é um menor elemento de S se possui as seguintes propriedades:*
(i) $a \in S$.
(ii) $a \leq n, \forall\ n \in S$.

Princípio da Boa Ordem: *Todo subconjunto não vazio de* $\mathbb{N}$ *possui um menor elemento.*

Teorema 1 ***(Algoritmo da divisão)*** *Dados* $a, b \in \mathbb{Z}$ *com* $b \neq 0$*, existem* $q, r \in \mathbb{Z}$ *com:*

$$a = bq + r \ e \ 0 \leq r < |b|$$

tais q e r estão unicamente determinados e são chamados o quociente e o resto da divisão de a por b.

Prova: Suponha que $b > a$ e considere, enquanto fizer sentido, os números

$$b, b - a, b - 2a, ..., b - na, ...$$

Pelo Princípio da Boa Ordem, o conjunto S formado pelos elementos acima tem um menor elemento $r = b - qa$. Vamos provar que r tem a propriedade requerida, ou seja, $r < a$.

Se $a|b$, então $r = 0$ e nada mais temos a provar. Se, por outro lado, a não divide b, então $r \neq a$, e, portanto, basta mostrar que não pode ocorrer $r > a$. De fato, se isto ocorresse, existiria um número natural $c < r$ tal que $r = c + a$. Consequentemente, sendo $r = c + a = b - qa$, teríamos

$$c = b - (q + 1)a \in S, \ com \ c < r,$$

contradição com o fato de r ser o menor elemento de S. Portanto, temos que

$$b = aq + r \ com \ r < a,$$

o que prova a existência de q e r.

Agora, vamos provar a unicidade. Note que, dados dois elementos distintos de S, a diferença entre o maior e o menor desses elementos, sendo um múltiplo de a é pelo menos a. Logo, se $r = b - aq$ e $r^{'} = b - aq^{'}$, com $r < r^{'} < a$, teríamos $r^{'} - r \geq a$, o que acarretaria $r^{'} \geq r + a \geq a$, absurdo. Portanto, $r = r^{'}$. Daí segue-se que $b - aq = b - aq^{'}$, o que implica que $aq = aq^{'}$ e, portanto, $q = q^{'}$.

■

Note que o resto da divisão de b por a é zero se, e somente se, a divide b.

Exemplo 3 *Encontre o quociente e o resto da divisão de* 19 *por* 5.

$$19 - 5 = 14, 19 - 2.5 = 9, 19 - 3.5 = 4 < 5$$

Isto não dá $q = 3$ e $r = 4$.

Exemplo 4 *O resto da divisão de* 10^n *por* 9 *é sempre* 1, $\forall\ n \in \mathbb{N}$.

Isto será feito por indução. Para $n = 0$, temos que $10^0 = 9.0 + 1$. Suponha o resultado válido para um dado k, isto é $10^k = 9q + 1$ e considere a igualdade

$$10^{k+1} = 10.10^k = (9 + 1).10^k = 9.10^k + 10^k = 9.10^k + 9q + 1 = 9.(10^k + q) + 1,$$

provando que o resultado vale para $k + 1$ e, consequentemente, vale para todo $n \in \mathbb{N}$.

Teorema 2 *(**Bachet - Bezout**) Sejam* $a, b \in \mathbb{Z}$. *Então existem* $x, y \in \mathbb{Z}$ *com*

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

Prova: O caso $a = b = 0$ é trivial (temos $x = y = 0$). Nos outros casos, considere o conjunto de todas as combinações $\mathbb{Z}$-lineares de a e b:

$$C(a, b) = \{ax + by : x, y \in \mathbb{Z}\}$$

Seja $d = ax_0 + by_0$ o menor elemento de $C(a, b)(N\tilde{a}o - vazio)$. Afirmamos que d divide todos os elementos de $C(a, b)$. De fato, dado $m = ax + by \in C(a, b)$, sejam $q, r \in \mathbb{Z}$ o quociente e o resto na divisão euclidiana de m por d, de modo que $m = dq + r$ e $0 \leq r < d$. Temos:

$$r = m - dq = a.(x - qx_0) + b.(y - qy_0) \in C(a, b)$$

Mas como $r < d$ e d é o menor elemento positivo de $C(a, b)$, segue que $r = 0 \Rightarrow d|m$. Em particular, como $a, b \in C(a, b)$ temos que $d|a$ e $d|b$, logo $d \leq mdc(a, b)$. Note ainda que se $c|a$ e $c|b$ então $c|ax_0 + by_0 \Leftrightarrow c|d$. Tomando $c = mdc(a, b)$ temos que $mdc(a, b)|d$, o que juntamente com a desigualdade $d \leq mdc(a, b)$, mostra que $d = mdc(a, b)$.

■

Proposição 1 *Se* $mdc(a,b) = 1$ *e* $a|bc$ *então* $a|c$.

Prova: Como $a|bc$ e $mdc(a,b) = 1$, existem $q, x, y \in \mathbb{Z}$ tal que, $bc = aq$ e $ax + by = 1 \Rightarrow a(cx) + (bc)y = c$. Então para todo $c \in \mathbb{Z}$ temos $a(cx) + a(qy) = c \Rightarrow a|c$.

■

1.2 Números primos e o Crivo de Eratóstenes

Definição 5 *Um número natural maior que* 1 *e que seja apenas múltiplo de* 1 *e de si próprio é chamado de número primo. Um número diferente de* 0 *e de* 1 *que não é primo é chamado de número composto.*

1.2.1 Crivo de Eratóstenes

Um método muito antigo para se obter de modo sistemático números primos é chamado de **Crivo de Eratóstenes**, devido ao matemático grego Eratóstenes. A eficiência do método é baseado na observação bem simples a seguir: Se um número natural $a > 1$ é composto, então ele é múltiplo de algum número primo p tal que $p^2 \leq a$. Equivalentemente, é primo todo número a que não é múltiplo de um número primo p tal que $p^2 < a$. De fato, se a é composto e p é o menor número primo do qual a é múltiplo, então $a = pb$, onde p e b são menores que a. Agora, sendo b primo ou composto, ele será múltiplo de um número primo q. Como a é múltiplo de b e b é múltiplo de q, pela transitividade da relação de ser múltiplo, a também é múltiplo de q e sendo p o menor primo do qual a é múltiplo, $p \leq q$. Logo, $p^2 \leq pq \leq a$. Por exemplo, para mostrar que o número $221 (= 13.17)$ é composto, bastaria testar se ele é múltiplo de algum dos números primos $p = 2, 3, 5, 7, 11$ ou 13, já que o próximo primo 17 é tal que $17^2 = 289 > 221$.

Para se obter os números primos até uma certa ordem n, escreva os números de 2 até n em uma tabela. O primeiro desses números, o 2, é primo, pois não é múltiplo de nenhum número anterior. Risque todos os demais múltiplos de 2 na tabela, pois esses não são primos. O primeiro número maior que 2 não riscado nessa nova tabela é o 3 que é primo, pois não é múltiplo de nenhum número anterior diferente de 1. Risque todos os demais múltiplos de 3 na tabela, pois esses não são primos.O primeiro número não riscado maior que 3 nessa nova tabela é o 5 que é primo, pois não é múltiplo de nenhum número anterior diferente de 1. Risque todos os demais múltiplos de 5 na tabela,

e assim por diante. Ao término desse procedimento, os números não riscados são todos os primos menores ou iguais a n. Note que o procedimento termina asssim que atingirmos um número primo p tal que $p^2 \geq n$, pois pela observação que fizemos acima, ja teríamos riscado todos os números compostos menores ou iguais a n.

A seguir é apresentado um exemplo de tabela com os números primos menores que 200.

	$\overline{2}$	$\overline{3}$	$\not{4}$	$\overline{5}$	$\not{6}$	$\overline{7}$	$\not{8}$	$\not{9}$	$\not{10}$
$\overline{11}$	$\not{12}$	$\overline{13}$	$\not{14}$	$\not{15}$	$\not{16}$	$\overline{17}$	$\not{18}$	$\overline{19}$	$\not{20}$
$\not{21}$	$\not{22}$	$\overline{23}$	$\not{24}$	$\not{25}$	$\not{26}$	$\not{27}$	$\not{28}$	$\overline{29}$	$\not{30}$
$\overline{31}$	$\not{32}$	$\not{33}$	$\not{34}$	$\not{35}$	$\not{36}$	$\overline{37}$	$\not{38}$	$\not{39}$	$\not{40}$
$\overline{41}$	$\not{42}$	$\overline{43}$	$\not{44}$	$\not{45}$	$\not{46}$	$\overline{47}$	$\not{48}$	$\not{49}$	$\not{50}$
$\not{51}$	$\not{52}$	$\overline{53}$	$\not{54}$	$\not{55}$	$\not{56}$	$\not{57}$	$\not{58}$	$\overline{59}$	$\not{60}$
$\overline{61}$	$\not{62}$	$\not{63}$	$\not{64}$	$\not{65}$	$\not{66}$	$\overline{67}$	$\not{68}$	$\not{69}$	$\not{70}$
$\overline{71}$	$\not{72}$	$\overline{73}$	$\not{74}$	$\not{75}$	$\not{76}$	$\not{77}$	$\not{78}$	$\overline{79}$	$\not{80}$
$\not{81}$	$\not{82}$	$\overline{83}$	$\not{84}$	$\not{85}$	$\not{86}$	$\not{87}$	$\not{88}$	$\overline{89}$	$\not{90}$
$\not{91}$	$\not{92}$	$\not{93}$	$\not{94}$	$\not{95}$	$\not{96}$	$\overline{97}$	$\not{98}$	$\not{99}$	$\not{100}$
$\overline{101}$	$\not{102}$	$\overline{103}$	$\not{104}$	$\not{105}$	$\not{106}$	$\overline{107}$	$\not{108}$	$\overline{109}$	$\not{110}$
$\not{111}$	$\not{112}$	$\overline{113}$	$\not{114}$	$\not{115}$	$\not{116}$	$\not{117}$	$\not{118}$	$\not{119}$	$\not{120}$
$\not{121}$	$\not{122}$	$\not{123}$	$\not{124}$	$\not{125}$	$\not{126}$	$\overline{127}$	$\not{128}$	$\not{129}$	$\not{130}$
$\overline{131}$	$\not{132}$	$\not{133}$	$\not{134}$	$\not{135}$	$\not{136}$	$\overline{137}$	$\not{138}$	$\overline{139}$	$\not{140}$
$\not{141}$	$\not{142}$	$\not{143}$	$\not{144}$	$\not{145}$	$\not{146}$	$\not{147}$	$\not{148}$	$\overline{149}$	$\not{150}$
$\overline{151}$	$\not{152}$	$\not{153}$	$\not{154}$	$\not{155}$	$\not{156}$	$\overline{157}$	$\not{158}$	$\not{159}$	$\not{160}$
$\not{161}$	$\not{162}$	$\overline{163}$	$\not{164}$	$\not{165}$	$\not{166}$	$\overline{167}$	$\not{168}$	$\not{169}$	$\not{170}$
$\not{171}$	$\not{172}$	$\overline{173}$	$\not{174}$	$\not{175}$	$\not{176}$	$\not{177}$	$\not{178}$	$\overline{179}$	$\not{180}$
$\overline{181}$	$\not{182}$	$\not{183}$	$\not{184}$	$\not{185}$	$\not{186}$	$\not{187}$	$\not{188}$	$\not{189}$	$\not{190}$
$\overline{191}$	$\not{192}$	$\overline{193}$	$\not{194}$	$\not{195}$	$\not{196}$	$\overline{197}$	$\not{198}$	$\overline{199}$	$\not{200}$

1.3 Teorema Fundamental da Aritmética

Do ponto de vista da estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, conforme veremos adiante no Teorema Fundamental da Aritmética (TFA). Na demonstração do TFA usaremos:

Segundo Princípio de Indução: *Seja* $p(n)$, *com* $n \in \mathbb{N}$ *uma sentenca aberta talque* :

(i) $p(a)$ *é verdade*;

(ii) $\forall\ r$ *com* $a \leq r < k$, $p(r)$ *verdadeira* $\Rightarrow$ $p(k)$ *verdadeira*;

Então $p(n)$ *é verdade* $\forall\ n \geq a$.

Agora sim, podemos enunciar e demonstrar o Teorema Fundamental da Aritmética.

Teorema 3 *(**Teorema Fundamental da Aritmética**) Dado um número natural* $n \geq 2$, *existem um número* $r > 0$, *números primos* $p_1, p_2, ..., p_r$ *com* $p_1 < p_2 < ... < p_r$ *e números naturais não nulos* $a_1, a_2, ..., a_r$ *tais que:*

$$n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}.$$

Além disso, esta decomposição é única.

Prova: (Existência) Se $n = 2$, o resultado é obviamente verificado. Suponhamos o resultado válido para todo número natural menor que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos que n seja um número composto. Logo existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, existem números primos $p_1, p_2, ..., p_r$ e $q_1, q_2, ..., q_s$ tais que $n_1 = p_1 p_2 ... p_r$ e $n_2 = q_1 q_2 ... q_s$. Portanto $n = p_1 p_2 ... p_r q_1 q_2 ... q_s$.
(Unicidade) Suponha que $n = p_1 p_2 ... p_r = q_1 q_2 ... q_s$ onde $p_{i's}$ e $q_{j's}$ são números primos. Como $p_1 | q_1 q_2 ... q_s \Rightarrow \exists\ j / p_1 = q_j$. Digamos que seja $j = 1$. Portanto,

$$p_2 ... p_r = q_2 ... q_s$$

Como $p_2 ... p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

■

Exemplo 5

A decomposição de 1001 em fatores primos é $7 \times 11 \times 13$, enquanto $2^2 \times 3^3 \times 5^4$ é a devida representação em fatores primos de 67500.

Observação 2

Denotando por $d(m)$ o número de divisores do número natural m, segue que se:

$$m = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$$

Com $p_1, p_2, ..., p_r$ números primos e $a_1, a_2, ..., a_r$ números naturais, então:

$$d(m) = (a_1 + 1)(a_2 + 1)...(a_r + 1)$$

Exemplo 6

Como $100 = 2^2 \, . \, 5^2$, segue que $d(100) = (2 + 1)(2 + 1) = 9$. Logo 100 possui 9 divisores, a saber: $1, 2, 4, 5, 10, 20, 25, 50, 100$.

Observação 3

A fórmula acima nos mostra que um número $n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$ possui uma quantidade ímpar de divisores se, e somente se, cada a_i é par, ou seja, se, e somente se, n é um quadrado perfeito, ou seja, existe $k \in \mathbb{Z}$ tal que $k^2 = n$.

Teorema 4 *(**Euclides**) Existem infinitos números primos.*

Prova: Suponha por absurdo que os números primos sejam em número finito e seja a o produto de todos eles. O número $a+1$ não seria primo pois ele seria maior do que qualquer número primo. Logo, $a+1$ sendo composto, ele seria múltiplo de algum número primo p. Mas sendo a também múltiplo de p, teríamos que 1 seria múltiplo do número primo p, o que é um absurdo. ■

1.4 Congruências e o Pequeno Teorema de Fermat

Definição 6 *Sejam $a, b, m \in \mathbb{Z}$. Dizemos que a é congruente a b módulo m, e escrevemos:*

$$a \equiv b \ (mod \ m),$$

se $m|(a - b)$, ou seja, se a e b deixam o mesmo resto na divisão por m.

Proposição 2 *Para quaisquer $a, b, c, d, m \in \mathbb{Z}$ temos:*

(i)(Reflexiva) $a \equiv a \ (mod\ m)$.

(ii)(Simétrico) Se $a \equiv b \ (mod\ m)$ *então* $b \equiv a \ (mod\ m)$.

(iii)(Transitiva) Se $a \equiv b \ (mod\ m)$ *e* $b \equiv c \ (mod\ m)$ *então* $a \equiv c \ (mod\ m)$.

(iv)(Compatibilidade com a soma e diferença)

$$\begin{cases} a \equiv b \ (mod\ m) \\ c \equiv d \ (mod\ m) \end{cases} \Rightarrow \begin{cases} a + c \equiv b + d \ (mod\ m) \\ a - c \equiv b - d \ (mod\ m). \end{cases}$$

Em particular, se $a \equiv b \ (mod\ m)$ *então* $ka \equiv kb \ (mod\ m), \forall k \in \mathbb{Z}$.

(v) (Compatibilidade com o produto)

$$\begin{cases} a \equiv b \ (mod\ m) \\ c \equiv d \ (mod\ m) \end{cases} \Rightarrow ac \equiv bd \ (mod\ m)$$

Em particular, se $a \equiv b \ (mod\ m)$ *então* $a^k \equiv b^k \ (mod\ m), \forall k \in \mathbb{Z}$.

(vi) (Cancelamento) Se $mdc(c, m) = 1$*, então:*

$$ac \equiv bc \ (mod\ m) \Leftrightarrow a \equiv b \ (mod\ m).$$

Prova: Para o item (i) basta observar que, $m|(a - a) = 0$.

Em (ii),

$$se\ m|(a - b),\ então\ m| - (a - b) \Leftrightarrow m|(b - a).$$

Em (iii),

$$se\ m|(a - b)\ e\ m|(b - c),\ então\ m|(a - b) + (b - c) = (a - c).$$

Em (iv),

$$se\ m|(a - b)\ e\ m|(c - d),\ então \begin{cases} m|(a - b) + (c - d) \\ m|(a - b) - (c - d) \end{cases}$$

Logo, organizando as contas,

$$\begin{cases} m|(a - b + c - d) \\ m|(a - b - c + d) \end{cases} \Rightarrow \begin{cases} m|(a + c) - (b + d) \\ m|(a - c) - (b - d) \end{cases}$$

Em (v),

$$Se\ m|(a-b)+(c-d),\ então\ m|(a-b)c+(c-d)b \Leftrightarrow$$

$$m|(ac-bc+bc-bd) \Leftrightarrow m|(ac-bd).$$

Finalmente em (vi), como $mdc(c,m)=1$ temos que,

$$m|ac-bc \Leftrightarrow m|(a-b)c \Leftrightarrow m|a-b.$$

■

Lema 2 *Os números* $C_p^i = \dfrac{p!}{(p-i)!i!}$, *onde* $0<i<p$ *e* $p! = p\times(p-1)\times...\times 2\times 1$ *são todos divisíveis por p primo.*

Prova: O resultado vale para $i=1$. Podemos, então, supor $1<i<p$. Neste caso, $i!|p\times(p-1)\times...\times(p-i+1)$. Como $mdc(i!,p)=1$, decorre que $i!|(p-1)\times...\times(p-i+1)$, e o resultado se segue, pois

$$C_p^i = p\frac{(p-1)\times...\times(p-i+1)}{i!}$$

■

Teorema 5 ***(Pequeno Teorema de Fermat)*** *Seja a um inteiro positivo e p um número primo, com* $mdc(a,p)=1$ *então* $a^p \equiv a\ (mod\ p)$.

Prova: Vamos provar o resultado por indução sobre a. O resultado vale claramente para $a=1$, pois $p|0$.

Supondo o resultado válido para $a=k$, iremos prová-lo para $a=k+1$. Pela fórmula do binômio de Newton,

$$(k+1)^p-(k+1) = k^p-k+C_p^1k^{p-1}+...+C_p^{p-1}k.$$

Como, pelo Lema 2 e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, o resultado se segue.

■

Exemplo 7

O pequeno Teorema de Fermat nos diz que $47|(2^{46}-1)$.

1.5 Resíduos Quadráticos, Símbolo de Legendre e o Critério de Euler

Definição 7 *Se a congruência $x^2 \equiv a \ (mod\ m)$ tem solução, dizemos que a é um resíduo quadrático módulo m, onde $a, m, x \in \mathbb{N}$, com $m > 1$ e $mdc(a, m) = 1$. Caso contrário, dizemos que a não é um resíduo quadrático módulo m.*

Exemplo 8

A congruência $x^2 \equiv 2 \ (mod\ 3)$, não possui nenhuma solução.

Exemplo 9

Todo número natural n é resíduo quadrático módulo 2.

Exemplo 10

Se p é um número primo da forma $4k + 1$, então $p - 1$ é resíduo quadrático módulo p.

Exemplo 11

Se $p = 5$, então 1 e 4 são os elementos de $\{1, 2, 3, 4\}$ que são resíduos quadráticos módulo 5. Se $p = 7$, então $1, 2\ e\ 4$ são os elementos de $\{1, 2, 3, 4, 5, 6\}$ que são resíduos quadráticos módulo 7.

Definição 8 ***(Símbolo de Legendre)*** *Seja $p > 2$ um número primo e a um inteiro qualquer, com $mdc(a, p) = 1$; O símbolo de Legendre $\left(\frac{a}{p}\right)$ é definido por*

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

Exemplo 12

Pelo exemplo 11, $\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1$ enquanto, $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$. Por sua vez temos, $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$ e, $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$.

Proposição 3 *(**Critério de Euler**) Seja $p > 2$ um primo e a um inteiro qualquer. Então:*

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

Prova: Para $a \equiv 0\ (mod\ p)$ temos evidentemente o resultado. Suponha que p não divide a. Pelo Pequeno Teorema de Fermat, temos $a^{p-1} \equiv 1\ (mod\ p)$, donde

$$(a^{\frac{p-1}{2}} - 1).(a^{\frac{p-1}{2}} + 1) \equiv 0\ (mod\ p) \Leftrightarrow$$

$$p|a^{\frac{p-1}{2}} - 1 \ ou\ p|a^{\frac{p-1}{2}} + 1 \Leftrightarrow a^{\frac{p-1}{2}} \equiv \pm 1\ (mod\ p).$$

Assim devemos mostrar que $a^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ se, e só se, a é um resíduo quadrático módulo p. Se a é um residuo quadrático, então existe $x \in \mathbb{N}$ com $mdc(p, x) = 1$ tal que $a \equiv x^2\ (mod\ p)$. Novamente pelo Pequeno Teorema de Fermat temos que:

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1\ (mod\ p).$$

■

Exemplo 13

Como $x^2 \equiv 2\ (mod\ 47)$ tem solução para $x = 7$, segue que $47|2^{46} - 1$.

Exemplo 14

Pelo Critério de Euler temos

$$\left(\frac{3}{5}\right) \equiv 3^{\frac{5-1}{2}} \equiv 3^2 \equiv -1\ (mod\ 5).$$

Proposição 4 *O símbolo de Legendre possui as seguintes propriedades:*

(i) Se $a \equiv b\ (mod\ p)$ então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) $\left(\frac{a^2}{p}\right) = 1$, *se p não divide a.*

(iii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & se \quad p \equiv 1\ (mod\ 4) \\ -1 & se \quad p \equiv 3\ (mod\ 4) \end{cases}$

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

Prova: Os itens (i) e (ii) seguem da definição, e (iii) segue do critério de Euler:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \ (mod\ p) \Leftrightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}},$$

já que $p > 2$ e ambos os lados da congruência são iguais a ± 1. Da mesma forma, para demonstrar (iv), aplicando o critério de Euler temos:

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

O que mostra que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right).\left(\frac{b}{p}\right)$, pois novamente ambos os lados da congruência são iguais a ± 1.

■

Exemplo 15 $\left(\frac{2}{7}\right) \equiv 2^{\frac{7-1}{2}} = 2^3 = 8 \equiv 1 \ (mod\ 7)$.

Exemplo 16 *O número* $2^{2^5} + 1$ *é um número composto.*

De fato, esse número corresponde a $n = 5$ dos chamados números de Fermat que são da forma:

$$F_n = 2^{2^n} + 1.$$

Fermat afirmou que esses números, para qualquer valor natural de n, são primos e deu como exemplos:

$$F_0 = 3, F_1 = 5, F_3 = 257 \ e \ F_4 = 65537$$

que são efetivamente números primos. No entanto, o número $F_5 = 2^{2^5} + 1 = 4294967297$ era muito grande para se verificar se era primo ou não.

Euler, estudando a forma dos divisores de um número do tipo F_n, chegou a conclusão de que se F_5 fosse composto, ele deveria ser divisível pelo primo 641.

Com efeito, note que $\left(\frac{-1}{641}\right) = 1$, pois 641 é um número primo da forma $4k + 1$. Logo, -1 é um resíduo quadrático módulo 641. Disto segue que,

$$\exists \ x \in \mathbb{N} / \ x^2 \equiv -1 \ (mod\ 641).$$

Afirmamos que $x = 2^{16}$.

Para isso, observe que $641 = 5 \times 2^7 + 1$, logo

$$5 \times 2^7 \equiv -1 \ (mod\ 641).$$

Elevando a quarta potência ambos os membros da congruência acima, obtemos

$$5^4 \times 2^{28} \equiv 1 \ (mod\ 641). \tag{1.1}$$

Por outro lado, da igualdade $641 = 625 + 16 = 5^4 + 2^4$, obtemos que

$$5^4 \equiv -2^4 \ (mod\ 641). \tag{1.2}$$

Juntando (1.1) e (1.2), obtemos $-2^{32} \equiv 1 \ (mod\ 641)$, ou seja, $(2^{16})^2 \equiv -1 \ (mod\ 641)$, o que implica que $F_5 = 2^{32} + 1 \equiv 0 \ (mod\ 641)$, donde 641 divide F_5. Portanto, F_5 não é um número primo.

Capítulo 2

Inteiros que são soma de dois quadrados

Aqui serão apresentados os primeiros resultados sobre soma de quadrados. Definições da soma de dois quadrados e de exemplos gerais na tentativa de estabelecer conjecturas, assim como apresentar o Lema de Thue e sua demonstração que dará condições para a caracterização de Fermat para números primos.

2.1 Soma de dois quadrados e os semigrupos multiplicativos

Definição 9 *Considere um número inteiro $m > 0$. Dizer que m pode ser escrito como soma de dois quadrados, garante a existência de inteiros não negativos a e b tal que:*

$$m = a^2 + b^2.$$

Dizemos que m está escrito na forma da soma de dois quadrados.

Exemplo 17

Como $a^2 = a^2 + 0^2$, qualquer quadrado perfeito é soma de dois quadrados.

Definição 10 *Um conjunto S de números inteiros não negativos é um semigrupo multiplicativo se, e somente se, ele tem o produto de cada par de seus elementos, como elemento de S, isto é: $x, y \in S \Rightarrow xy \in S$.*

Exemplo 18

Seja P o conjunto dos números pares e Imp o conjunto dos números ímpares. É fato que tais conjuntos denotam semigrupos multiplicativos.

Agora temos um importante resultado.

Proposição 5 *Se S é um semigrupo multiplicativo de inteiros não negativos tal que todos os primos pertencem a S, então os inteiros maiores que* 1 *pertencem a S.*

Prova: Temos apenas outro modo de enunciar o Teorema Fundamental da Aritmética que afirma que todos os números naturais maiores que 1 ou são primos ou um produto de primos.

■

O próximo resultado garante que se dois números inteiros positivos são representados como soma de dois quadrados, então seu produto também será.

Proposição 6 *O conjunto $Q_2 = \{a^2 + b^2 : a, b \in \mathbb{Z}_+\}$ da soma de dois quadrados é um semigrupo multiplicativo.*

Prova: Com efeito, considere $x, y \in Q_2$, logo existem inteiros não negativos a, b, c *e* d tais que:

$$x = a^2 + b^2 \text{ } e \text{ } y = c^2 + d^2$$

Note que $xy = (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2$, ou seja, $xy \in Q_2$.

■

O resultado de Q_2 ser um semigrupo multiplicativo é necessário para identificarmos se o número inteiro é ou não soma de dois quadrados a partir de seus fatores, e usando o Teorema Fundamental da Aritmética poderemos caracterizar todos aqueles que podem expressos dessa forma. Por isso, ainda precisamos caracterizar os números primos que sejam soma de dois quadrados.

2.2 Soma de dois quadrados e os divisores primos

Vamos mostrar agora algumas condições sobre os divisores primos de um número que é soma de dois quadrados. Notemos inicialmente que

$$2 = 1^2 + 1^2.$$

Quanto aos primos ímpares, temos o seguinte resultado:

Proposição 7 *Sejam a e b dois números inteiros tais que $mdc(a,b) = 1$ e seja p um número primo ímpar tal que $p|a^2 + b^2$, então p é da forma $4k + 1$.*

Prova: Note que p não divide a e nem b e que $a^2 + b^2 \equiv 0\ (mod\ p)$ garante que $a^2 \equiv -b^2 (mod\ p)$. Elevando a potência $\frac{p-1}{2}$ temos que:

$$(a^2)^{\frac{p-1}{2}} \equiv (-b^2)^{\frac{p-1}{2}}\ (mod\ p) \Rightarrow a^{p-1} \equiv (-1)^{\frac{p-1}{2}}.\ b^{p-1}\ (mod\ p)$$

E pelo pequeno teorema de Fermat obtemos que $(-1)^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$. Logo $\frac{p-1}{2}$ é um número par e portanto, $p \equiv 1\ (mod\ 4)$.

■

Proposição 8 *Nenhum inteiro da forma $4k + 3$ é soma de dois quadrados.*

Prova: Seja a um inteiro qualquer. Logo temos $a = 2t$ ou $a = 2t + 1$, $t \in \mathbb{Z}$. Donde tem - se:

$$a^2 \equiv (2t)^2 \equiv 4t^2 \equiv 0\ (mod\ 4)\ ou$$

$$a^2 \equiv (2t + 1)^2 \equiv 4(t^2 + t) + 1 \equiv 1\ (mod\ 4)$$

Logo para qualquer inteiro b, temos $a^2 + b^2 \equiv 0, 1\ ou\ 2\ (mod\ 4)$. O que nos faz concluir que nenhum inteiro que é representado como soma de dois quadrados é da forma $4k + 3$.

■

2.3 Princípio das Gavetas e Lema de Thue

Já mostramos que todos os números primos impares que dividem $a^2 + b^2$ com $mdc(a,b) = 1$ são da forma $4k + 1$ e que o produto de números que são soma de dois quadrados também o é. Assim seria interessante provar o reciproco desta afirmação; Mas para isto, precisamos que todos os primos da forma $4k+1$ sejam soma de dois quadrados. Pesquisando os primeiros casos, vemos que:

$$5 = 2^2 + 1^2 \qquad 13 = 3^2 + 2^2 \qquad 17 = 4^2 + 1^2$$

$$29 = 5^2 + 2^2 \qquad 37 = 6^2 + 1^2 \qquad 41 = 5^2 + 4^2$$

Note que alguns números primos da forma $4k+1$ são soma de dois quadrados. Afirmamos que isto vale para todos os números primos desta forma. De fato, para mostrar esta afirmação precisamos antes dos seguintes resultados:

Princípio da Casa dos Pombos ou das Gavetas: *Dados n objetos e m gavetas, onde $n > m$, se colocarmos os n objetos nas m gavetas, pelo menos uma gaveta conterá mais de um objeto.*

Lema 3 ***(Thue)*** *Sejam $a, m \in \mathbb{Z}_+$ e $mdc(a, m) = 1$. Então a congruência*

$$ax \equiv y \ (mod\ m)$$

admite uma solução x_0, y_0, onde:

$$0 < |x_0| < \sqrt{m} \quad e \quad 0 < |y_0| < \sqrt{m}$$

Prova: No caso em que $m = 1$, para qualquer valor de a teremos $x = y = 1$ satisfazem as condições. Suponhamos que m seja um número natural maior que 1. Seja $q = \lfloor \sqrt{m} \rfloor$. Então $q+1 > \sqrt{m}$ e portanto $(q+1)^2 > m$. Consideremos todos os números da forma $ax - y$ onde x e y tomam os valores $0, 1, 2, ..., q$. Observe que estamos considerando $(q+1)^2$ números. Como só existem m restos possíveis ao dividir um número por m, o príncipio das gavetas nos garante que existem dois desses números, que têm o mesmo resto quando divididos por m. Sejam $ax_1 - y_1$ e $ax_2 - y_2$ tais números, isto é:

$$ax_1 \equiv y_1 \ (mod\ m) \ e \ ax_2 \equiv y_2 \ (mod\ m)$$

Portanto, sua diferença $a(x_1 - x_2) - (y_1 - y_2)$ é divisível por m. Se $x_1 = x_2$ então $y_1 - y_2$ será divisível por $m \Rightarrow y_1 = y_2$. Contradição, pois (x_1, y_1) é diferente de (x_2, y_2). Se $y_1 = y_2$ então $a(x_1 - x_2)$ será divisível por m, o que também é uma contradição, pois $mdc(a, m) = 1$, caso não fossem, p dividiria $(x_1 - x_2)$ e $x_1 = x_2$ o que não pode acontecer. Assim, $x_1 - x_2 \neq 0$ e $y_1 - y_2 \neq 0$. Podemos supor, sem perda de generalidade que $x_1 - x_2 > 0$ e, neste caso, tomamos $x_0 = x_1 - x_2$ e $y_0 = |y_1 - y_2|$ e concluimos a prova do lema.

■

2.4 Caracterização da soma de dois quadrados para números primos

Teorema 6 *Um número p primo e ímpar é expresso como soma de dois quadrados se, e somente se,* $p \equiv 1 \ (mod\ 4)$.

Prova: Suponha que p pode ser escrito como uma soma de dois quadrados, ou seja, $p = a^2 + b^2$. Como p é primo, então p não divide a nem b. Então $mdc(a, p) = mdc(b, p) = 1$. Logo pela teoria das conguências lineares, existe um inteiro c tal que:

$$bc \equiv 1 \ (mod\ p),\ com\ 0 < |c| < \sqrt{p}$$

Ou seja, $bc = pt + 1$, onde $t \in \mathbb{Z}$. Módulo p, $(ac)^2 + (bc)^2 = pc^2$ torna - se:

$$(ac)^2 + (pt + 1)^2 = pc^2 \Rightarrow (ac)^2 = p(c^2 - pt^2 - 2t) - 1$$

$$(ac)^2 \equiv -1 \ (mod\ p)$$

Logo (-1) é um resíduo quadrático módulo p, daí $\left(\frac{-1}{p}\right) = 1$. Mas isso somente acontece se $p \equiv 1 \ (mod\ 4)$.

Reciprocamente, supondo que a é um inteiro tal que $a^2 \equiv -1 \ (mod\ p)$, como (-1) é um residuo quadrático, por hipótese, de $p \equiv 1 \ (mod\ 4)$, então a congruência:

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

tem uma solução $x_0 = a, y_0 = -1$. Além disso, temos também:

$$-1 \equiv a^2 \ (mod\ p) \Rightarrow -x_0^2 \equiv (ax_0)^2 \ (mod\ p)$$

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

$$x_0^2 + y_0^2 \equiv 0 \ (mod\ p) \Rightarrow x_0^2 + y_0^2 = kp,\ com\ 1 \leq k \in \mathbb{Z}.$$

Como $0 < |x_0| < \sqrt{p}$ e $0 < |y_0| < \sqrt{p}$ obtemos $0 < x_0^2 + y_0^2 < 2p$, o que implica dizer que $k = 1$. Logo $x_0^2 + y_0^2 = p$, o que conclui a demonstração.

■

O seguinte resultado mostra que a decomposição de um primo como soma de dois quadrados de fato é única.

Teorema 7 *Seja p um número primo da forma $4k+1$. Então p pode ser escrito de forma única como soma de dois quadrados.*

Prova: De fato, suponha que

$$p = a^2 + b^2 = c^2 + d^2, \ com \ a, b, c, d < \sqrt{p}.$$

Note que necessariamente temos $mdc(a, b) = mdc(c, d) = 1$. Afirmamos que, a menos de ordem, estas somas são iguais. Com efeito, se

$$a^2 + b^2 \equiv 0 \ (mod \ p) \ e \ c^2 + d^2 \equiv 0 \ (mod \ p),$$

tem-se:

$$a^2 \equiv -b^2 \ (mod \ p) \ e \ d^2 \equiv -c^2 \ (mod \ p)$$

Então:

$$(ad)^2 \equiv (bc)^2 \ (mod \ p) \Rightarrow (ad)^2 - (bc)^2 \equiv 0 \ (mod \ p)$$

$$(ad - bc)(ad + bc) \equiv 0 \ (mod \ p)$$

Logo

$$p|(ad - bc) \ ou \ p|(ad + bc)$$

pois p é primo. No primeiro caso, sabemos que:

$$|ad - bc| \leq max\{ad, bc\} < p.$$

Donde segue que

$$p|ad - bc \Longleftrightarrow ad - bc = 0 \Longleftrightarrow ad = bc.$$

Então

$$a|bc, \ com \ mdc(a, b) = 1 \Rightarrow a|c,$$

digamos que $c = ak$. Ou seja,

$$ad = bc = b(ak) \Rightarrow d = bk.$$

Logo temos,

$$p = c^2 + d^2 \Rightarrow$$

$$\Rightarrow p = (ak)^2 + (bk)^2 \Rightarrow$$

$$\Rightarrow p = a^2k^2 + b^2k^2 \Rightarrow p = (a^2 + b^2)k^2 \Rightarrow k = 1.$$

Neste caso, temos que $a = c$ e $b = d$. Analogamente, se $p|ad + bc$ e como $0 < ad + bc < 2p$ tem-se que $ad + bc = p$, logo

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

E assim $ac - bd = 0$ o que resulta que $ac = bd$. Seguindo os mesmos raciocínios teremos que $a = d$ e $b = c$. ■

2.5 Dois quadrados - Contando soluções

Observação 4

Podemos perceber que qualquer primo $p \equiv 1\ (mod\ 4)$ pode ser escrito como soma de dois quadrados em oito formas. Com efeito, para $p = 13$, temos:

$$13 = 3^2 + 2^2 = (-3)^2 + 2^2 = 3^2 + (-2)^2 = (-3)^2 + (-2)^2 =$$

$$= 2^2 + 3^2 = 2^2 + (-3)^2 = (-2)^2 + 3^2 = (-2)^2 + (-3)^2.$$

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

Definição 11 *Representaremos por $V(m)$ o número de soluções de*

$$x^2 \equiv -1\ (mod\ m). \tag{2.1}$$

Observação 5

Para obter a quantidade de soluções de (2.1) consultar [3] página 77 - Teorema 88.

Exemplo 19

$V(5) = 2$, pois as soluções de $x^2 \equiv -1 \ (mod\ 5)$ são 2 e 3 apenas

$$2^2 \equiv -1 \ (mod\ 5) \qquad\qquad 3^2 \equiv -1 \ (mod\ 5).$$

Exemplo 20

$V(130) = 4$, pois as soluções são $47, 57, 73\ e\ 83$, de fato

$$47^2 \equiv -1 \ (mod\ 130) \qquad\qquad 83^2 \equiv -1 \ (mod\ 130)$$
$$57^2 \equiv -1 \ (mod\ 130) \qquad\qquad 73^2 \equiv -1 \ (mod\ 130).$$

Teorema 8 *O número de soluções de $m = a^2 + b^2$, com $mdc(a, b) = 1$ é $4V(m)$.*

Prova: Não demonstraremos este resultado. Para o leitor interessado consultar [3], página 165 - Teorema 161.

■

Exemplo 21

Como $V(5) = 2$, o número de soluções da equação $5 = a^2 + b^2$, com $mdc(a, b) = 1$ é

$$4V(5) = 4 \times 2 = 8.$$

Exemplo 22

Por sua vez, como $V(130) = 4$, existem 16 soluções para a equação $130 = a^2 + b^2$.

Definição 12 *Denotaremos por $n_2(m)$ o número de modos de representar um inteiro positivo m como soma de dois quadrados.*

Exemplo 23

Como podemos representar o número 4 nas quatro seguintes somas de dois quadrados $(\pm 2)^2 + 0^2$ e $0^2 + (\pm 2)^2$, temos $n_2(4) = 4$.

Teorema 9 $n_2(m) = 4\sum_{d^2|m} V\left(\frac{m}{d^2}\right)$

Prova: Se os pares a, b forem classificados de acordo com os valores de $mdc(a,b) = d$ onde $d^2|m$, então o resultado segue do teorema 8, uma vez que para $mdc(a,b) = d$, $m = a^2 + b^2$ é equivalente a afirmação

$$\left(\frac{m}{d}\right) = a_1^2 + b_1^2, \ com \ a_1 = \frac{a}{d}, b_1 = \frac{b}{d} \ e \ mdc(a_1, b_1) = 1.$$

■

Observação 6

Outras maneiras de representar $n_2(m)$ são:

$$(i) \ n_2(m) = 4\sum_{d|m} X(d) \ onde \ X(d) = \begin{cases} 0 & para \quad d \equiv 0 \ (mod \ 2) \\ 1 & para \quad d \equiv 1 \ (mod \ 4) \\ -1 & para \quad d \equiv 3 \ (mod \ 4) \end{cases}$$

$$(ii) \ n_2(m) = 4\sum_{d|m} (-1)^{\frac{d-1}{2}}, \ com \ d \ ímpar.$$

2.6 Caracterização de soma de dois quadrados para qualquer inteiro

Observação 7

Alguns números que não são primos, mas são da forma $4k+1$ não podem ser representados como soma de dois quadrados de inteiros, como o número 21 por exemplo. Desta forma, teremos que estabelecer mais algumas condições para sabermos quais são esses números.

Definição 13 *Um número inteiro n é dito livre de quadrados, se a decomposição de n em fatores primos tem somente primos distintos.*

Teorema 10 *Seja $m = n_0^2 n$, onde n é livre de quadrados. Então m é soma de dois quadrados se, e somente se, n não tem fatores primos da forma $4k + 3$.*

Prova: Suponha que n não tem fatores primos da forma $4k + 3$. Se $n = 1$, então $m = n_0^2 \times 1 = n_0^2 + 0^2$ que é trivialmente soma de dois quadrados. Se $n > 1$, então n pode ser escrito como:

$$n = p_1 p_2 ... p_r$$

pois n é livre de quadrados e os $p_i^{,}s$ podendo ser somente iguais a 2 ou a $4k+1$. Pelo teorema (6), temos que os primos $p = 4k+1$ podem ser escritos como soma de dois quadrados, assim como o número 2. Logo pela proposição (6) segue que n pode ser escrito como soma de dois quadrados, digamos $n = a^2 + b^2$. Como $m = n_0^2 n$, isso implica que:

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

Garantindo que m é soma de dois quadrados. Por sua vez, considere que m seja uma soma de dois quadrados, digamos $m = a^2 + b^2 = n_0^2 n$ com a, b inteiros. Se n=1, nada temos a demonstrar. Supondo $n > 1$, considere p um fator primo de $n(= fp)$. Se $mdc(a, b) = d$, então existe $r, t \in \mathbb{Z}$, tais que:

$$a = rd \; e \; e \; b = td \; com \; mdc(r, t) = 1$$

Então:

$$a^2 + b^2 = n_0^2 n$$

$$(rd)^2 + (td)^2 = n_0^2 n$$

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

Donde segue que

$$d^2 | n_0^2 n,$$

como n é livre de quadrados, segue que

$$d^2 | n_0^2$$

$$n_0^2 = ed^2, e \in \mathbb{Z}$$

logo

$$r^2 + t^2 = en$$

Como $n = fp$ e considerando $g = ef$ tem-se que:

$$r^2 + t^2 = e(fp) = (ef)p = gp \; , g \; positivo$$

logo temos

$$r^2 + t^2 \equiv 0 \ (mod\ p)$$

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

$$r'r + t'p = 1$$

Ou módulo p, $r'r \equiv 1 \ (mod\ p)$. Mas como $(r')^2(r^2 + t^2) \equiv 0 \ (mod\ p)$ tem-se:

$$(r't)^2 \equiv -1 \ (mod\ p)$$

Ou seja, (-1) é residuo quadrático módulo p ou simplesmente $\left(\frac{-1}{p}\right) = 1$ o que é equivalente a dizer que $p = 2$ ou $p = 4k + 1$.
Então n não possui fatores primos da forma $4k + 3$.

■

Consequentemente temos mais uma caracterização de números inteiros que podem ser escritos como soma de dois quadrados.

Corolário 1 *Seja n um inteiro positivo tal que:*

$$n = 2^{\alpha} p_1^{a_1} ... p_r^{a_r} q_1^{b_1} ... q_s^{b_s} \ onde \ \begin{cases} p_i & \equiv & 1 \ (mod\ 4), & 1 \leq i \leq r \\ q_j & \equiv & 3 \ (mod\ 4), & 1 \leq j \leq s \end{cases}$$

Então

$$n \text{ é soma de dois quadrados} \iff b_j \text{ são números pares.}$$

Prova: Queremos mostrar que n é soma de dois quadrados. Suponha para isso que b_j sejam números pares para todo j tal que $1 \leq j \leq k$. Logo

$$q_j^{b_j} = q_j^{2t} = (q_j^t)^2,$$

ou seja

$$q_j^{b_j} = (q_j^t)^2 + 0^2$$

é soma de dois quadrados.

Além disso, os primos 2 e os da forma $4k+1$ são soma de dois quadrados, logo o produto

$$n = 2^{\alpha} p_1^{a_1} ... p_r^{a_r} q_1^{b_1} ... q_s^{b_s}$$

é uma soma de dois quadrados.

Agora assumiremos que $n = a^2 + b^2$. Seja $mdc(a, b) = d$, temos

$$a = a_1 d \ e \ b = b_1 d, \ com \ mdc(a_1, b_1) = 1.$$

então

$$n = (a_1 d)^2 + (b_1 d)^2 = d^2 n_1$$

onde $n_1 = a_1^2 + b_1^2$.

Agora dado um q primo da forma $4k+3$, tal que, ao decompormos n em fatores primos, q tenha um expoente impar. Então temos que $q | n_1$, mas q não divide a_1 e b_1, e como

$$a_1^2 + b_1^2 \equiv 0 \ (mod \ q)$$

tem - se que

$$a_1^2 \equiv -b_1^2 \ (mod \ q).$$

Pelos resultados de residuos quadráticos, temos

$$\left(\frac{a_1^2}{q}\right) = \left(\frac{-b_1^2}{q}\right),$$

e como $q \nmid a_1$ temos $\left(\frac{a_1^2}{q}\right) = 1$, logo

$$\left(\frac{-b_1^2}{q}\right) = \left(\frac{-1}{q}\right) \times \left(\frac{b_1^2}{q}\right) = 1$$

Mas $\left(\frac{-1}{q}\right) = 1 \iff q \equiv 1 \ (mod \ 4)$. Ou seja, q não pode ser da forma $4k+3$, contradição. Logo, os expoentes dos primos impares da forma $4k+3$ são todos pares.

■

Capítulo 3

Inteiros que são soma de três quadrados

3.1 Soma de três quadrados

Na impossibilidade de escrever alguns números inteiros como soma de dois quadrados, como por exemplo o número 67, considerou - se o fato de estabelecer mais alguns critérios para que se pudesse expressar tais números como soma de dois quadrados. Deseja-se nesta sessão enunciar algumas condições para que um inteiro positivo possa ou não ser escrito como soma de três quadrados. O número 67, já citado, não é uma soma de dois quadrados por ser um primo ímpar da forma $4k + 3$. No entanto, tal número pode ser expresso como:

$$67 = 7^2 + 3^2 + 3^2,$$

ou seja, como soma de três quadrados. De fato, temos alguns exemplos de números que não podem ser expressos como soma de dois quadrados, mas são escritos como soma de três quadrados:

$$11 = 3^2 + 1^2 + 1^2$$
$$14 = 3^2 + 2^2 + 1^2$$
$$105 = 10^2 + 2^2 + 1^2.$$

Brevemente enunciaremos algumas condições neste sentido, visto que ainda existirão números que não poderão ser escritos como soma de três quadrados.

Lema 4 *Todo inteiro positivo da forma* $8k+7,\ k \in \mathbb{Z}$ *não pode ser escrito como soma de três quadrados.*

Prova: Com efeito, módulo 8, o número inteiro m é congruente a

$$0, 1, 2, 3, 4, 5, 6 \ ou\ 7 \Rightarrow m^2 \equiv 0, 1 \ ou\ 4 \ (mod\ 8).$$

Logo temos que:

$$a^2 + b^2 + c^2 \equiv 0, 1, 2, 3, 4, 5 \ ou\ 6 \ (mod\ 8) \ com\ a, b, c \in \mathbb{Z}$$

Portanto, não existe inteiros que sejam soma de três quadrados da forma $8k+7$.

■

Teorema 11 ***(Legendre-Gauss)*** *Uma condição necessária e suficiente para que um inteiro m seja uma soma de três quadrados, é que m* ***não*** *seja da forma* $4^n(8k+7)$*, para todo* $n \in \mathbb{N}$ *e* $k \in \mathbb{Z}$*.*

Prova: Vamos provar a primeira parte do teorema:

(i) Se m é uma soma de três quadrados, então m **não** é da forma $4^n(8k+7)$ para todo $n \in \mathbb{N}$ e $k \in \mathbb{Z}$.

Suponha que

$$m = 4^n(8k+7) = a^2 + b^2 + c^2 \tag{3.1}$$

Onde a, b *e* c são inteiros. Seja $n = n_0$ o menor valor com o qual m é representado. Note que $n_0 > 0$, pois se tivessémos $n_0 = 0$, seguiria que $m = 4^0(8k+7) \equiv 7\ (mod\ 8)$, o que pelo **lema 4** não pode ser representado como soma de três quadrados. Agora, como m é par e $4|m$ segue que a, b *e* c são também números pares. Sejam $a = 2A, b = 2B$ *e* $c = 2C$. E dividindo a equação (3.1) por 4 temos

$$m = 4^{n_0-1}(8k+7) = A^2 + B^2 + C^2 \tag{3.2}$$

Implicando que $n = n_0 - 1 < n_0$ é o menor valor com o qual m é representado. Isto é uma contradição pelo definição de n_0. Portanto, m não pode ser representado como soma de três quadrados.

(ii) Se m **não** é da forma $4^n(8k+7)$ para todo $n \in \mathbb{N}$ e $k \in \mathbb{Z}$, então m é uma soma de três quadrados.

A prova desta afirmação será omitida por está fora do objetivo deste trabalho. O leitor interessado pode consultar [3], página 194 - Teorema 187.

■

Exemplo 24

Os primeiros números que não são soma de três quadrados são:
Considere $n = 0$ e $k \in \mathbb{N}$ em $4^n(8k + 7)$

$$7, 15, 23, 31, ...$$

Considere $n = 1$ e $k \in \mathbb{N}$ em $4^n(8k + 7)$

$$28, 60, 92, 124, ...$$

E assim por diante.

Observação 8

Na sessão anterior, tínhamos o fato de que o produto de dois ou mais números que eram expressos como soma de dois quadrados, também resultava numa representação de uma soma de dois quadrados. Todavia, em relação a soma de três quadrados isso não acontece. Com efeito:

$$19 = 3^2 + 3^2 + 1^2$$

$$21 = 4^2 + 2^2 + 1^2.$$

No entanto, o produto $19 \times 21 \equiv 7$ $(mod\ 8)$, não sendo representado na forma de soma de três quadrados. Em geral temos:

Proposição 9 *Todo número inteiro da forma mn onde* $m \equiv 3$ $(mod\ 8)$ *e* $n \equiv 5$ $(mod\ 8)$*, não são expressos na forma de soma de três quadrados.*

Prova: De fato, o produto $mn \equiv 15 \equiv 7$ $(mod\ 8)$.

■

Capítulo 4

Inteiros que são somas de quatro quadrados

4.1 Identidade de Lagrange e soma de quatro quadrados

Como nem todos os inteiros positivos podem ser soma de dois quadrados ou ainda expressos como soma de três quadrados, houve a necessidade de ampliar os conceitos de representação de inteiros como soma de quadrados. Alguns matemáticos como Fermat, Descartes e Euler tentaram demonstrar uma afirmação conjecturada pelo matemático Bachet de Méziriac:

"Todo inteiro é representável como soma de quatro quadrados de inteiros."

Euler fez afirmações relevantes sobre esta conjectura descrita em uma carta de 1730 para Goldbach, e afirmou que a maior dificuldade estava em mostrar que números da forma $n^2 + 7$ podem ser escritos como soma de quatro quadrados. No entanto, o primeiro matemático a verificar a veracidade dessa conjectura foi Lagrange. Vamos dar condições para que esta demonstração seja exibida.

O próximo resultado garante que se os inteiros m e n podem ser escritos como soma de quatro quadrados, então seu produto mn também é uma soma de quatro quadrados.

Lema 5 *O conjunto* $Q_4 = \{a^2+b^2+c^2+d^2 : a, b, c, d \in \mathbb{Z}_+\}$ *da soma de quatro quadrados é um semigrupo multiplicativo.*

Prova: Para este resultado, usamos uma relação denominada Identidade de Lagrange: $\forall\ x, y, z, w, a, b, c, d \in \mathbb{Z}_+$ temos:

$$(x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = r^2 + s^2 + t^2 + u^2,$$

onde,

$$\begin{aligned} r &= xa + yb + zc + wd \\ s &= xb - ya + zd - wc \\ t &= xc - yd - za + wb \\ u &= xd + yc - zb - wa. \end{aligned}$$

Basta desenvolver de ambos os lados e depois comparar os resultados.

■

Lema 6 *Se dois números podem ser escritos como soma de três quadrados, então o produto deles pode ser escrito como soma de quatro quadrados.*

Prova: Fazendo uso das identidades para os inteiros:

$$m = x^2 + y^2 + z^2 \ e \ n = a^2 + b^2 + c^2,$$

assim como as parcelas

$$(yc - zb), (za - xc), (xb - ya), (xa + yb + zc),$$

temos:

$$mn = (yc - zb)^2 + (za - xc)^2 + (xb - ya)^2 + (xa + yb + zc)^2.$$

■

4.2 Quatro quadrados - Contando soluções

Em geral, existem mais de uma maneira para escrever um número m como a soma de quatro quadrados. Assim é interessante saber se existem outras maneiras de escrever um número m como a soma de quatro quadrados após achar uma representação.

Definição 14 *A função* $\sigma : \mathbb{N} \to \mathbb{N}$ *dada por*

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

fornece a soma dos divisores positivos de m*.*

Exemplo 25

Os divisores positivos de 6 são $1, 2, 3$ e 6. Logo

$$\sigma(6) = 1 + 2 + 3 + 6 = 12.$$

Exemplo 26

Da mesma forma, os divisores de 14 são $1, 2, 7$ e 14. Então

$$\sigma(14) = 1 + 2 + 7 + 14 = 24.$$

Observação 9

Números naturais m tais que $\sigma(m) = 2m$, são chamados de números perfeitos. Neste caso, seguindo dos dois exemplos anteriores, apenas o número 6 é um número perfeito.

Teorema 12 *Seja* $n_4(m)$ *o número de modos de escrever* $m \in \mathbb{Z}, m > 0$*, como soma de quatro quadrados. Temos:*
(i) Se m *é ímpar, então* $n_4(m) = 8\sigma(m)$*.*
(ii) Se m *é par e* $m = 2^\alpha u$*, com* u *ímpar, então* $n_4(2^\alpha u) = 24\sigma(u)$*.*

Prova: Não provaremos este resultado e estamos incluindo o mesmo aqui como informação adicional. O leitor interessado pode encontrar esta demonstração em [3], página 180 - Teorema 172, com a observação de que estamos usando $n_4(m) = Q(m)$.

■

Uma estratégia para escrever um número m como soma de quatro quadrados é escolher o primeiro termo igual ao maior quadrado perfeito contido em m e tentar representar a diferença como soma de três quadrados. Para isso, procuramos o maior quadrado nessa diferença, e assim por diante.

Exemplo 27 *Escrever os números* 55 *e* 217 *como a soma de quatro quadrados usando a estratégia acima.*

$$55 = 7^2 + 6 = 7^2 + 2^2 + 2 = 7^2 + 2^2 + 1^2 + 1^2$$
$$217 = 14^2 + 21 = 14^2 + 4^2 + 5 = 14^2 + 4^2 + 2^2 + 1^2.$$

Exemplo 28

Note que os divisores de 1001 são $1, 7, 11, 13, 77, 91, 133$ e 1001, logo

$$\sigma(1001) = 1 + 7 + 11 + 13 + 77 + 91 + 133 + 1001 = 1334.$$

Como 1001 é ímpar, temos

$$n_4(1001) = 8\sigma(1001) = 8 \times 1334 = 10672.$$

4.3 Soma de quatro quadrados e números primos

Teorema 13 *Um número inteiro* $\boldsymbol{m}$ *é soma de quatro quadrados se, e somente se,* $\boldsymbol{2m}$ *também é.*

Prova: Considere que existam $a, b, c, d \in \mathbb{Z}$ tais que:

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

Disto segue que:

$$2m = 2a^2 + 2b^2 + 2c^2 + 2d^2$$
$$2m = a^2 + b^2 + a^2 + b^2 + c^2 + d^2 + c^2 + d^2$$
$$2m = (a^2 + 2ab + b^2) + (a^2 - 2ab + b^2) + (c^2 + 2cd + d^2) + (c^2 - 2cd + d^2)$$
$$2m = (a + b)^2 + (a - b)^2 + (c + d)^2 + (c - d)^2.$$

Garantindo que $2m$ é uma soma de quatro quadrados.

Sendo $2m$ uma soma de quatro quadrados, existem $x, y, z, w \in \mathbb{Z}$ tais que:

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

Como $x^2+y^2+z^2+w^2$ é par segue que temos quatro parcelas impares ou quatro parcelas pares ou duas parcelas impares e duas parcelas pares. Então sem perda de generalidade, podemos supor que x^2+y^2 e z^2+w^2 são somas pares. Logo,

$$m = \frac{(x^2+y^2)}{2} + \frac{(z^2+w^2)}{2}$$

Mas $\forall\ a, b \in \mathbb{Z}$ tem - se: $\dfrac{(a^2+b^2)}{2} = \dfrac{(a+b)^2}{2} + \dfrac{(a-b)^2}{2}$

Então segue que:

$$m = \frac{(x+y)^2}{2} + \frac{(x-y)^2}{2} + \frac{(z+w)^2}{2} + \frac{(z-w)^2}{2}.$$

Deixando claro que m é soma de quatro quadrados. ■

Observação 10

É fato que também $\dfrac{(x+y)^2}{2}$ *e* $\dfrac{(x-y)^2}{2}$ são inteiros, assim como $\dfrac{(z+w)^2}{2}$ e $\dfrac{(z-w)^2}{2}$. Pois como $x^2+y^2+z^2+w^2$ é par, temos que duas a duas parcelas possuem a mesma paridade.

Teorema 14 *Seja p um primo ímpar. Então a congruência:*

$$x^2 + y^2 + 1 \equiv 0\ (mod\ p)$$

tem uma solução x_0, y_0 onde $0 \leq x_0, y_0 \leq \dfrac{p-1}{2}$.

Prova: Considere os dois conjuntos:

$$A_1 = \{1+0^2, 1+1^2, ..., 1+(\frac{p-1}{2})^2\}\ e\ A_2 = \{0^2, -1^2, ..., -(\frac{p-1}{2})^2\}$$

Note que em A_1 não existe $1+x_1^2 \equiv 1+x_2^2\ (mod\ p)$, com $x_1 \neq x_2$, pois se existisse, teríamos $x_1^2 \equiv x_2^2\ (mod\ p) \Rightarrow x_1^2 - x_2^2 \equiv 0\ (mod\ p)$ e $(x_1+x_2)(x_1-x_2) \equiv 0\ (mod\ p)$, e teríamos $x_1 \equiv -x_2\ (mod\ p)$ ou $x_1 \equiv x_2\ (mod\ p)$. Este último caso só seria possível se $x_1 = x_2$, o que é uma contradição. Do mesmo modo, não existem dois elementos em A_2 que sejam congruentes módulo p. A_1 e A_2 contém $2(1+\dfrac{p-1}{2}) = p+1$ inteiros e pelo príncipio da casa dos pombos, algum inteiro em A_1 deve ser congruente módulo p a algum inteiro em A_2. Logo existem x_0, y_0 tais que:

$$1 + x_0^2 \equiv -y_0^2\ (mod\ p),\ com\ 0 \leq x_0, y_0 \leq \frac{p-1}{2}$$

■

Teorema 15 *Seja p um primo ímpar, então existe um inteiro k, tal que:*

$$1 \leq k < p \text{ e } kp \text{ seja soma de quadrados.}$$

Prova: Já sabemos que a congruência: $x_0^2 + y_0^2 + 1 \equiv 0 \ (mod\ p)$, tem solução com $0 \leq x_0, y_0 \leq \frac{p-1}{2} < \frac{p}{2}$. Então:

$$\exists\ k \in \mathbb{Z} : x_0^2 + y_0^2 + 1^2 + 0^2 = kp$$

Além disso, temos que:

$$1 \leq kp < \frac{p^2}{4} + \frac{p^2}{4} + 1 = \frac{p^2}{2} + 1 < p^2 \Rightarrow 1 \leq kp < p^2 \Rightarrow 1 \leq k < p.$$

■

4.4 Teorema de Lagrange

Teorema 16 *Qualquer primo p pode ser escrito como a soma de quatro quadrados.*

Prova: Com efeito, se $p = 2$ temos

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

Considere então que $p > 2$, e seja k o menor inteiro positivo tal que:

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

com $1 \leq k < p$. Queremos mostrar que $k = 1$.

De fato, se k fosse par teriamos x, y, z *e* w dois a dois de mesma paridade. Logo pelo teorema 13, $(\frac{k}{2})p$ também poderia ser representado como soma de quatro quadrados, o que contraria o fato de k ser um valor mínimo.

Tome $k > 1$.

Agora considere os restos a, b, c *e* d obtidos através da divisão de x, y, z *e* w por k, no intervalo $(\frac{-k}{2}, \frac{k}{2})$. Isto é, escrevemos:

$$x = q_1 k + a$$
$$y = q_2 k + b$$
$$z = q_3 k + c$$
$$w = q_4 k + d,$$

desta forma, $|a|, |b|, |c|, |d| < \frac{k}{2}$ e além disso,

$$\begin{aligned} x &\equiv a \ (mod\ k) \\ y &\equiv b \ (mod\ k) \\ z &\equiv c \ (mod\ k) \\ w &\equiv d \ (mod\ k), \end{aligned}$$

logo temos:

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 = kp \equiv 0 \ (mod\ k)$$

então

$$a^2 + b^2 + c^2 + d^2 = nk, \ com\ n \geq 0.$$

Se $n = 0$ temos,

$$a = b = c = d = 0 \Rightarrow x \equiv y \equiv z \equiv w \equiv 0 \ (mod\ k)$$

logo

$$k|x, y, z, w \Rightarrow k^2|x^2 + y^2 + z^2 + w^2 = kp \Rightarrow k|p,$$

contradição, pois $1 < k < p$.

Considere $n \geq 1$. Agora como

$$1 \leq nk = a^2 + b^2 + c^2 + d^2 < 4(\frac{k}{2})^2 = k^2,$$

temos que $nk < k^2 \Rightarrow n < k$, ou seja, $1 \leq n < k$.

Para terminarmos a demonstração, vamos mostrar que np também é uma soma de quatro quadrados, sendo assim chegaremos a uma contradição, garantindo assim que $k = 1$.

Com efeito,

$$k^2(np) = (kp)(nk) = (x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = r^2 + s^2 + t^2 + u^2$$

onde r, s, t, u estão de acordo com a Identidade de Lagrange. Disto segue que:

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

portanto, $k|r,s,t,u \Rightarrow k^2|r^2+s^2+t^2+u^2$.

Considere $m \in \mathbb{Z}$ *com* $k^2m = r^2+s^2+t^2+u^2$, logo:

$$k^2(np) = k^2m \Rightarrow np = m$$

Mas $m = (\frac{r}{k})^2 + (\frac{s}{k})^2 + (\frac{t}{k})^2 + (\frac{u}{k})^2 = np$, mostrando assim que np é soma de quatro quadrados. Logo $k = 1$, então:

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

■

Finalmente, temos condições de demonstrar o principal resultado deste trabalho.

Teorema 17 *(**Teorema de Lagrange**) Todo inteiro positivo pode ser representado como soma de quatro quadrados.*

Prova: Consideraremos $m > 1$.

Se m for um número primo, pelo teorema 16 nada há para se demonstrar.

Agora se m for um número composto, o Teorema Fundamental da Aritmética nos garante a existência de primos $p_1, p_2, ..., p_r$, tais que:

$$m = p_1p_2...p_r$$

Como Q_4 é um semigrupo multiplicativo, segue que qualquer m é uma soma de quatro quadrados.

■

Considerações finais

Grande parte de nossos alunos de ensino básico, infelizmente não são orientados de maneira científica em sua formação. Afirmo isso, mediante o fato de, em sua maioria, os resultados serem apresentados na ordem "Conceito, Exemplos e Exercícios", nos inúmeros livros didáticos tidos e entendidos como referência em nosso país. Geralmente neste sentido, não se têm muito tempo para o praticar voluntário das definições pelos alunos, pois estes já se veem, assim como o seu professor, na necessidade de cumprir a matriz curricular. Seria interessante se porventura algumas vezes, pudéssemos apresentar a temática no sentido inverso dos fatos: Exercícios, exemplos e conceitos, pois desta forma, penso que o conhecimento seria melhor descoberto. Neste trabalho, há uma tentativa de se incentivar isso, através da apresentação de exemplos e resolução de exercícios. Deseja - se elaborar através da Teoria dos Números, afirmações percebidas pelos alunos e alunas, e possíveis respostas a estas, incentivando desta forma o pensamento científico. Além disso, considerando a possibilidade do estudo direcionado no Ensino Fundamental e Médio sobre Aritmética, inclusive sobre algumas relações algébricas, tem - se no presente estudo uma forma diferenciada de se abordar diversos assuntos tais como: Quadrados perfeitos, o estudo particular de Binômios e os próprios Números Primos e assim como propriedades e conceitos não ainda apresentados, porém de fácil acesso ao entendimento, como por exemplo, as Congruências. O estudo de quadrados ou soma de quadrados é apenas um ponto de partida para esses estudos. O entendimento de um lema, proposição e teoremas através de conjecturas, ajudará o discente a entender o formalismo com o qual a matemática, como também outras áreas, são pesquisadas e escritas. A todo momento, refleti sobre escolher um tema de fácil acesso a esses níveis de ensino para, a partir dele, incentivar uma proposta de construção de conceitos matemáticos através de resolução de exercícios. O Teorema de Lagrange segue essas perspectivas, pois inicia- se na caraterização dos números primos que podem ser escritos como soma de quadrados,

para daí pela impossibilidade de escrever todos os números inteiros positivos como soma de dois quadrados ou ainda de três quadrados, definirmos e provarmos o resultado mais abrangente. A continuidade desta pesquisa, se dará através da prática efetiva dos seus resultados. A de se considerar que não foi dado destaque a quantas soluções temos em relação a uma equação do tipo $m = a^2 + b^2 + c^2$, pois embora este difícil problema tenha solução, iríamos desviar muito do nosso objetivo. Grande parte das pesquisas sobre soma de três quadrados estão sendo feitas mediante a classificação dos números inteiros positivos que não podem ser escritos dessa forma. Poderia haver uma continuidade do trabalho nesse sentido, realizando a tentativa de se caracterizar diretamente os números inteiros possitivos que podem ser escritos como soma de três quadrados. Considero que tomar como referência tais apresentações/abordagens ajudará na construção do perfil acadêmico/científico que todos (os professores) esperam ver nos alunos e alunas quando chegam na universidade. Enfim, o maior proveito de tudo certamente está em mudar, para melhor, o que nós entendemos por Educação e não simplesmente fazer parte dela.

Referências Bibliográficas

[1] Herstein, I. N. - *Topics in Algebra*, 2nd ed, Chicago: University of Chicago, 1975.

[2] S.C. Coutinho - *Números Inteiros e Criptografia RSA*, Coleção Computação e Matemática, SBM e IMPA - 2000.

[3] LANDAU, EDMUND Georg Hermann. - *Teoria Elementar dos Números*, Rio de Janeiro, Editora Ciência Moderna, 2002.

[4] ABRAMO Hefez - *Elementos de Aritmética*, 2ª ed. Textos Universitários, SBM - 2005.

[5] Garcia, Arnaldo e Lequain, Yves - *Elementos de Algebra*, 4 ed, Rio de Janeiro: IMPA, 2006.

[6] J.P.O Santos. - *Introdução á Teoria dos Números*, 3ª ed. Coleção Matemática Universitária, IMPA - 2010.

[7] MOREIRA, Carlos Gustavo MARTINEZ, Fabio e SALDANHA, Nicolau - *Tópicos de Teoria dos números*, Rio de Janeiro: SBM, 2012.

[8] Wong, Michel - *Representing Integers as Sums of Squares.*

[9] Cooper, Cristhopher D. H. - *Number Theory*, 2a Edition 2013.

[10] Clark, Peter L. - *Representations of Integers by Quadratic Forms.*