Johny Andrade da Cunha

SOMAS DE QUADRADOS E TRIÂNGULOS RETÂNGULOS COM LADOS INTEIROS

Itabaiana

Agosto de 2019

Johny Andrade da Cunha

SOMAS DE QUADRADOS E TRIÂNGULOS RETÂNGULOS COM LADOS INTEIROS

Dissertação submetida ao Corpo Docente do Programa de Mestrado Profissional em Matemática da Universidade Federal de Sergipe como requisito para a obtenção do título de Mestre em Matemática.

Universidade Federal de Sergipe

Departamento de Matemática

Programa de Pós-Graduação

Orientador: Prof. Me. Samuel Brito Silva

Itabaiana

Agosto de 2019

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA PROFESSOR ALBERTO CARVALHO
UNIVERSIDADE FEDERAL DE SERGIPE

C972s Cunha, Johny Andrade da.
Somas de quadrados e triângulos retângulos com lados inteiros / Johny Andrade da Cunha; orientação: Samuel Brito Silva. – Itabaiana, 2019.
57 f.; il.

Dissertação (Mestrado em Matemática) – Universidade Federal de Sergipe, 2019.

1. Matemática. 2. Geometria plana. 3. Triângulo. I. Silva, Samuel Brito. II. Título.

CDU 513.1

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Somas de Quadrados e Triângulos Retângulos com Lados Inteiros

por

Johny Andrade da Cunha

Aprovada pela banca examinadora:

Samuel Brito Silva
Prof. Samuel Brito Silva - UFS
Orientador

Mateus Alegri
Prof. Mateus Alegri - UFS
Primeiro Examinador

Jussineide da Fonseca Nascimento Fontes
Profa. Jussineide Da Fonseca Nascimento Fontes - IFS
Segundo Examinador

São Cristóvão, 02 de Agosto de 2019

Dedicatória.

Sou grato a Deus e a todos aqueles que estavam ao meu lado e que em nenhum momento me deixaram fraquejar ou desistir desse trabalho

Agradecimentos

Quero agradecer primeiramente a Deus por ter me dado força em um momento tão complicado na minha vida.

Meus pais José Luiz da Cunha e Maria Edilene Andrade da Cunha que sempre me incentivaram e apoiaram nos estudos.

A minha esposa Jessica Silva Santos pela compreensão e paciência ao logo deste percurso, aos meus filhos Maria Tayná e John Vitor.

Meus irmãos Valdenusia, Junior, Mônica e Simone.

Ao meu orientador Prof. Mestre Samuel Brito Silva, pela atenção e ideias para este trabalho.

Ao Professor Dr. Mateus Alegri pelo incentivo e inspiração ao longo do curso.

E por fim a todos os que contribuíram direta e indiretamente no desenvolvimento do presente trabalho.

Resumo

Nesta dissertação iremos fornecer ferramentas para responder quando um número inteiro pode ser escrito como uma soma de quadrados. Usando estas ferramentas, conseguiremos determinar dado um número inteiro x maior que 2, quantos triângulos retângulos com lados inteiros, tendo x como um de seus catetos, existem. Determinaremos também todos os triângulos retângulos que tem x como hipotenusa, em função da decomposição de x em fatores primos.

Palavras-chaves: Triângulos retângulos, números inteiros, soma de quadrados.

Abstract

In this dissertation we will provide tools to answer when an integer can be written as a sum of squares. Using these tools, we will be able to determine given an integer x greater than 2, how many triangles rectangles with integer sides, having x as one of their legs, exist. We will also determine all triangles rectangles that have x as hypotenuse, as a function of the decomposition of x in prime factors.

Key-words:

Rectangles triangles, integers, sum of squares.

Sumário

Introdução

Certamente, a maioria de nós já se deparou com o desafio de encontrar os catetos de um triângulo retângulo que possua hipotenusa igual a 5 u.c., por exemplo, e quase que automaticamente pensou na solução $x = 4$ e $y = 3$. Este é um caso muito fácil de resolver, por ser tratar de um caso de triângulo retângulo com lados inteiros que sempre apareciam em nossos exercícios e exemplos no ensino básico. Mas, existem algumas perguntas mais gerais a serem feitas em problemas deste tipo. Algumas destas perguntas são: "Dado um número inteiro x maior do que 2, sempre existe um triângulo retângulo com lados inteiros que tenha x como um de seus catetos? e se existem, quantos são?". Ou ainda, "fixando um número inteiro z como sendo a hipotenusa de um triângulo retângulo, existem triângulos retângulos com lados inteiros com hipotenusa z? Se existem, quantos são?".

Observe que as perguntas acima podem ser reformuladas matematicamente da seguinte maneira: Dado um número inteiro n, existem inteiros x, y tais que $n = x^2 + y^2$? Ou seja, n pode ser escrito como uma soma de quadrados? Esta e outras perguntas serão respondidas ao longo do texto.

Esta dissertação foi dividida em três capítulos. No primeiro capítulo, intitulado "Teoria Básica", definimos os principais termos utilizados ao longo do texto e apresentamos resultados básicos sobre divisibilidade e congruências. Além disso, estudamos alguns anéis especias que possuem propriedades que nos auxiliarão nas demonstrações dos resultados do capítulo 2. Estes anéis são: o *Anel dos Inteiros de Gauss*, *Anel dos Quatérnios* e o *Anel dos Inteiros de Hurwitz*.

No segundo capítulo, intitulado *Representação de Inteiros Como Soma de Quadrados*, utilizamos as ferramentas do primeiro capítulo para caracterizar os inteiros que podem ser escritos como soma de quadrados. Mostraremos os casos em que um inteiro pode ser escrito como soma de dois, três ou quatro quadrados.

E finalmente no terceiro capítulo, intitulado *Triângulos Retângulos com Lados Inteiros*, usando alguns dos resultados obtidos no segundo capítulo, respondemos às perguntas supracitadas. Verificamos que dado um inteiro x maior do que 2, sempre existe um triângulo retângulo com lados inteiros tendo x como um de seus catetos. E além disso, através da decomposição de x em fatores primos, determinamos quantos destes triângulos existem. Por fim, destacamos também neste capítulo a condição necessária e suficiente para que dado um inteiro z exista um triângulo retângulo com lados inteiros tendo z como hipotenusa.

1 Teoria Básica

Neste capítulo, iremos apresentar alguns resultados e definições básicas que nos auxiliarão no entendimento e nas demostração do restante do trabalho.

1.1 Divisibilidade

Definição 1.1. *Dados dois números inteiros a e b, diremos que a divide b, escrevendo $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = ca$. Nesse caso, diremos também que a é um divisor ou um fator de b, ou ainda, que b é um múltiplo de a ou que b é divisível por a. Caso não exista esse inteiro, diremos que a não divide b, e denotaremos por $a \nmid b$.*

Definição 1.2. *Sejam dados dois inteiros a e b, distintos ou não. Um número inteiro d será dito um divisor comum de a e b se $d \mid a$ e $d \mid b$.*

Definição 1.3. *Diremos que um número inteiro $d \geq 0$ é o máximo divisor comum (mdc) de a e b (denotado por (a, b)), se possuir as seguintes propriedades:*

i. d é um divisor comum de a e b;

ii. d é divisível por todo divisor comum de a e b.

Proposição 1.1. *Se a, b, c, m e n são inteiros, $c \mid a$ e $c \mid b$ então $c \mid (ma + nb)$.*

Demonstração: Se $c \mid a$ e $c \mid b$, então $a = r_1 c$ e $b = r_2 c$ para alguns r_1 e r_2 inteiros. Multiplicado-se estas duas equações respectivamente por m e n teremos $ma = mr_1 c$ e $nb = nr_2 c$. Somando-se membro a membro e usando a propriedade distributiva dos números inteiros obtemos $ma + nb = (mr_1 + nr_2)c$, o que nos diz que $c \mid (ma + nb)$.

□

Exemplo 1.1. *Como $3 \mid 21$ e $3 \mid 42$, então $3 \mid (5.15 + 3.42)$.*

Teorema 1.1. *(Algoritmo da Divisão em $\mathbb{Z}$) Dados $a, b \in \mathbb{Z}, b > 0$, existe um único par de inteiros q e r que satisfazem*

$$a = qb + r, \ com \ 0 \leq r < b.$$

q é chamado quociente e r resto da divisão de a por b.

Demonstração: Seja b um número inteiro positivo não nulo. Se $a \in \mathbb{Z}$, então a é múltiplo de b ou está situado entre dois múltiplos consecutivos de b, isto é $qb \leq a < (q+1)b$. Somando $-qb$ em todos os termos da desigualdade obtemos $qb - qb \leq a - qb < qb + b - qb$ então $0 \leq a - qb < b$. Desta forma, tomando $r = a - qb$, segue que $a = qb + r$, em que $0 \leq r < b$.

Suponhamos agora, que existam q_1, q_2, r_1, r_2, onde $q_1 \neq q_2$ e $r_1 \neq r_2$ e que satisfaçam às igualdades: $a = q_1 b + r_1$, com $0 \leq r_1 < b$ e $a = q_2 b + r_2$, com $0 \leq r_2 < b$. Se $b > r_1$ e $b > r_2$ então $b >\mid r_2 - r_1 \mid$ e $a = bq_1 + r_1 = bq_2 + r_2$. Dessa forma, $b(q_2 - q_1) = r_2 - r_1$. Tomando $k = (q_2 - q_1)$, segue que $r_2 - r_1 = kb$, com $k \in \mathbb{Z}$ e daí $b \mid (r_2 - r_1)$. Portanto $b \leq\mid r_2 - r_1 \mid$, o que é um absurdo, pois contradiz $b >\mid r_2 - r_1 \mid$. Logo, $r_2 = r_1$. Concluímos que $(q_2 - q_1)b = 0$. Sendo $b \neq 0$, temos que $(q_2 - q_1) = 0$ e concluímos que $q_1 = q_2$.

Na equação $a = qb + r$, com $0 \leq r < b$, os inteiros, q e r são chamados respectivamente de quociente e resto da divisão de a por b. Vale lembrar que b somente é divisor de a se $r = 0$. Neste caso, temos que $a = bq$ e o quociente q na divisão exata de a por b pode ser indicado também por $\frac{a}{b}$.

□

O algoritmo euclidiano possui uma grande importância no conjunto dos números inteiros. Este algoritmo também é válido em outros anéis denominados como euclidianos.

Lema 1.1. *(Bézout)Seja d o máximo divisor comum de a e b, então existem inteiros n_0 e m_0 tais que $d = n_0 a + m_0 b$.*

Demonstração: Seja o conjunto $B = \{na + mb \mid n, m \in \mathbb{Z}\}$. Sejam $n_0, m_0 \in \mathbb{Z}$ tais que $c = n_0 a + m_0 b$ é o menor inteiro positivo pertencente a B, vamos provar que $c \mid a$ e $c \mid b$. Para tanto suponhamos que $c \nmid a$.

Pelo algoritmo da divisão existem q e r inteiros, tais que $a = qc + r, 0 < r < c$. Tomando $r = a - qc = a - q(n_0 + m_0 b) = a(1 - n_0 q) + b(-m_0 q)$, ou seja, r é um número inteiro positivo e $r \in B$ uma vez que, $(1 - n_0 q)$ e $(-m_0 q) \in \mathbb{Z}$. Daí, temos que $r \geq c$. Mas do Teorema 1.1, $r < c$, o que é um absurdo. Logo, $c \mid a$. Analogamente mostramos que $c \mid b$. Assim, c é um divisor comum, e como $d = (a, b)$, temos que $c \leq d$.

Resta ainda mostrar que $d = n_0 a + m_0 b$. Vejamos que, se $d = (a, b)$ então $d \mid a$ e $d \mid b$, o que implica que $a = k_1 d$ e $b = k_2 d$ para algum $k_1, k_2 \in \mathbb{Z}$. Ainda tomando $c = n_0 a + m_0 b = n_0(k_1 d) + m_0(k_2 d) = d(n_0 k_1 + m_0 k_2)$, resulta em $d \mid c$. Além disso, $c \neq 0$ então $\mid d \mid \leq\mid c \mid$ e como não é possível termos $d < c$, uma vez que $d = (a, b)$ então $d = c$, ou seja, $d = n_0 + m_0 b$.

□

Teorema 1.2. *Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Demonstração: Como $(a, b) = 1$ pelo Lema de Bézout existem inteiros n e m tais que $na+mb = 1$. Multiplicando-se dois lados desta igualdade por c temos: $n(ac)+m(bc) = c$. Como $a \mid ac$ e, por hipótese, $a \mid bc$ então, pela Proposição 1.1, $a \mid c$.

□

Proposição 1.2. *Para todo inteiro positivo t, $(ta, tb) = t(a, b)$*

Demonstração: Pela demostração do Lema de Bézout (ta, tb) é o menor valor positivo de $mta + ntb$ (m e n inteiros), que é igual a t vezes o menor valor positivo de $ma + nb = (a, b)$, ou seja $t(ma + nb) = t(a, b)$.

□

Proposição 1.3. *Se $c > 0$ e a e b são divisíveis por c, então*

$$(\frac{a}{c}, \frac{b}{c}) = \frac{1}{c}(a, b).$$

Demonstração: Como a e b são divisíveis por c temos que a/c e b/c são inteiros. Basta, então substituir na Proposição 1.2"a" por a/c e "b" por b/c tomando $t = c$.

□

Corolário 1.1. *Se $(a, b) = d$, temos que $(\frac{a}{d}, \frac{b}{d}) = 1$*

Demonstração: No que acabamos de demonstrar c é um divisor comum de a e b. Se tomarmos c como sendo o máximo divisor comum d, temos que:

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

Portanto, $(\frac{a}{d}, \frac{b}{d}) = 1$.

□

Proposição 1.4. *Sejam a e b inteiros e $d = (a, b)$. Se $d \nmid c$ então a equação $ax + by = c$ não possui nenhuma solução inteira. Se $d \mid c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por*

$$x = x_0 + (b/d)k$$

$$y = y_0 - (a/d)k$$

onde k é um inteiro.

Demonstração: Se $d \nmid c$, então a equação $ax+by = c$, não possui solução, pois como $d \mid a$ e $d \mid b$, d deveria dividir c, o qual é uma combinação linear de a e b. Suponhamos, que $d \mid c$. Pelo Lema de Bézout existem inteiros n_0 e m_0, tais que

$$an_0 + bm_0 = d. \tag{1.1}$$

Como $d \mid c$, existe um inteiro k tal que $c = kd$. Se multiplicamos, ambos os membros de (1.1) por k, teremos $a(n_0k) + b(m_0k) = kd = c$. Isto nos diz que o par (x_0, y_0) com $x_0 = n_0k$ e $y_0 = m_0k$ é uma solução de $ax + by = c$. É visível a verificação de que os pares da forma

$$x = x_0 + (b/d)k$$
$$y = y_0 - (a/d)k$$

são soluções, uma vez que

$$\begin{aligned} ax + by &= a(x_0 + (b/d)k) + b(y_0 - (a/d)k) \\ &= ax_0 + \tfrac{ab}{d}k + by_0 - \tfrac{ab}{d}k \\ &= ax_0 + by_0 = c. \end{aligned}$$

O que acabamos de mostrar é que, conhecida uma solução particular (x_0, y_0) podemos, a partir dela, gerar infinitas soluções. Precisamos, agora, mostrar que toda solução da equação $ax + by = c$ é da forma $x = x_0 + (b/d)k$, $y = y_0 - (a/d)k$. Vamos supor que (x, y) seja uma solução, isto é, $ax + by = c$. Mas, como $ax_0 + by_0 = c$, obtemos, subtraindo membro a membro, que

$$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0$$

o que implica $a(x - x_0) = b(y_0 - y)$. Como $d = (a, b)$ pelo corolário da Proposição 1.3,

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

Portanto, dividindo-se os dois membros da última igualdade por d, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \tag{1.2}$$

Logo, pelo Teorema 1.2, $(b/d) \mid (x - x_0)$ e, portanto, existe um inteiro k satisfazendo $x - x_0 = k(b/d)$, ou seja $x = x_0 + (b/d)k$. Substituindo este valor de x na equação (1.2) temos $y = y_0 - (a/d)k$, o que conclui a demonstração.

□

1.2 Congruência

Definição 1.4. *Se a, b e m são inteiros, dizemos que a é congruente a b módulo m com $(m > 0)$ se $m \mid (a - b)$. Denotamos isto por $a \equiv b \ (mod\ m)$. Se $m \nmid (a - b)$ dizemos que a é incongruente à b módulo m e denotamos $a \not\equiv b \ (mod\ m)$.*

Exemplo 1.2. $14 \equiv 4 \ (mod\ 5)$ *pois* $5 \mid (14 - 4)$. *Como* $7 \nmid 9$ *e* $9 = 24 - 15$ *temos que* $24 \not\equiv 15 \ (mod\ 7)$.

Proposição 1.5. *Se a e b são inteiros, temos que $a \equiv b \ (mod\ m)$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração: *Se $a \equiv b \ (mod\ m)$, então $m \mid (a - b)$ o que implica na existência de um inteiro k tal que $a - b = km$. A reciproca é trivial pois da existência de um k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, que $m \mid a - b$, isto é, $a \equiv b \ (mod\ m)$.*

Proposição 1.6. *Se a, b, m e d são inteiros, com $m > 0$, então as seguintes sentenças são verdadeiras:*

1. $a \equiv a \ (mod\ m)$;
2. *Se* $a \equiv b \ (mod\ m)$, *então* $b \equiv a \ (mod\ m)$;
3. *Se* $a \equiv b \ (mod\ m)$ *e* $b \equiv d \ (mod\ m)$, *então* $a \equiv d \ (mod\ m)$.

Demonstração:

1. *Como* $m \mid 0$, *então* $m \mid (a - a)$, *ou seja* $a \equiv a \ (mod\ m)$.
2. *Se* $a \equiv b \ (mod\ m)$, *então* $a = b + mk_1$ *para algum inteiro* k_1. *Logo,* $b = a - mk_1$ *o que implica pela Proposição* 1.5 *que* $b \equiv a \ (mod\ m)$.
3. *Se* $a \equiv b \ (mod\ m)$ *e* $b \equiv d \ (mod\ m)$, *então existem* k_1 *e* k_2 *tais que* $a - b = k_1 m$ *e* $b - d = k_2 m$. *Assim, somando estas duas últimas equações teremos* $a - d = (k_1 + k_2)\, m$ *resulta em* $a \equiv d \ (mod\ m)$.

A proposição acima nos garante que a relação de congruência nos inteiros é uma relação de equivalência.

Teorema 1.3. *Se a, b, c e m são inteiros tais que $a \equiv b \ (mod\ m)$, então:*

1. $a + c \equiv b + c \ (mod\ m)$;
2. $a - c \equiv b - c \ (mod\ m)$;
3. $ac \equiv bc \ (mod\ m)$;

Demonstração:

1. *Como* $a \equiv b \ (mod\ m)$*, temos que* $a - b = km$ *para algum inteiro* k *e, portanto, como* $a - b = (a + c) - (b + c)$ *temos* $a + c \equiv b + c \ (mod\ m)$.

2. *Como* $(a - c) - (b - c) = a - b$ *e, por hipótese* $a - b = km$*, temos que* $a - c \equiv b - c \ (mod\ m)$.

3. *Como* $a - b = km$*, então* $ac - bc = ckm$*, implica que* $m \mid (ac - bc)$ *e, portanto,* $ac \equiv bc \ (mod\ m)$.

□

Teorema 1.4. *Se* a, b, c, d *e* m *são inteiros tais que* $a \equiv b \ (mod\ m)$ *e* $c \equiv d \ (mod\ m)$*, então*

1. $a + c \equiv b + d \ (mod\ m)$;

2. $a - c \equiv b - d \ (mod\ m)$;

3. $ac \equiv bd \ (mod\ m)$;

Demonstração:

1. *De* $a \equiv b \ (mod\ m)$ *e* $c \equiv d \ (mod\ m)$ *temos* $a - b = km$ *e* $c - d = k_1 m$ *para certos inteiros* k *e* k_1*. Somando as duas equações teremos* $(a + c) - (b + d) = (k + k_1)m$ *o que implica que* $a + c \equiv b + d \ (mod\ m)$.

2. *Usando a hipótese, temos as equações* $a - b = km$ *e* $c - d = k_1 m$*, obtendo assim* $(a-b)-(c-d) = (a-c)-(b-d) = (k-k_1)m$*, o que implica em* $a-c \equiv b-d \ (mod\ m)$.

3. *Multiplicando ambos os lados de* $a - b = km$ *por* c *e multiplicando ambos os lados da equação* $c - d = k_1 m$ *por* b*, teremos* $ac - bc = ckm$ *e* $bc - bd = bk_1 m$*. Basta, agora, somarmos membro a membro estas últimas igualdades, obtendo* $ac - bc + bc - bd = ac - bd = (ck + bk_1)m$*, o que implica em* $ac \equiv bd \ (mod\ m)$.

□

Teorema 1.5. *Se* a, b, c *e* m *são inteiros e* $ac \equiv bc \ (mod\ m)$*, então* $a \equiv b \ (mod\ m/d)$ *onde* $d = (c, m)$.

Demonstração: De $ac \equiv bc \ (mod\ m)$ temos que $ac - bc = c(a-b) = km$ para certo inteiro k. Se dividirmos os dois membros por d, teremos $(c/d)(a-b) = k(m/d)$. Logo, $(m/d) \mid (c/d)(a-b)$ e, como $(m/d, c/d) = 1$, pelo Teorema 1.2, $(m/d) \mid (a-b)$ o que implica $a \equiv b \ (mod\ m/d)$.

□

Definição 1.5. *O conjunto dos inteiros $A = \{r_1, r_2, ..., r_s\}$ é um sistema completo de resíduos módulo m se*

(1) $r_i \not\equiv r_j \ (mod\ m)$ *para* $i \neq j$

(2) *Para todo inteiro n existe um r_i tal que $n \equiv r_i \ (mod\ m)$.*

Proposição 1.7. *Sejam a, b e m inteiros tais que $m > 0$ e $(a, m) = d$. No caso que $d \nmid b$ a congruência $ax \equiv b \ (mod\ m)$ não possui nenhuma solução e quando $d \mid b$, possui exatamente d soluções incongruentes módulo m.*

Demonstração: Pela Proposição 1.5 sabemos que o inteiro x é solução , $ax \equiv b \ (mod\ m)$ se, e somete se, existir um inteiro y tal que $ax = b + ym$, ou seja, $b = ax - ym$. Da Proposição 1.4 sabemos que esta equação não possui nenhuma solução caso $d \nmid b$, e que $d \mid b$ ela possui infinitas soluções dadas por $x = x_0 - (\frac{m}{d})k$ 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 $ax \equiv b \ (mod\ m)$ irá possuir infinitas soluções dadas por $x = x_0 - (\frac{m}{d})k$.

Desejamos saber a quantidade de soluções incongruentes. Daí, estudaremos as condições para as quais $x_1 = x_0 - (\frac{m}{d})k_1$ e $x_2 = x_0 - (\frac{m}{d})k_2$ são congruentes módulo m. Se x_1 e x_2 forem congruentes, então $x_0 - \frac{m}{d}k_1 \equiv x_0 - (\frac{m}{d})k_2 \ (mod\ m)$, assim

$$x_0 - x_0 - (\frac{m}{d})k_1 \equiv x_0 - x_0 - (\frac{m}{d})k_2 \ (mod\ m)$$

daí

$$-(\frac{m}{d})k_1 \equiv -(\frac{m}{d})k_2 \ (mod\ m) \Rightarrow (\frac{m}{d})k_1 \equiv (\frac{m}{d})k_2 \ (mod\ m)$$

Como $(\frac{m}{d}) \mid m$, pois $m = d.(\frac{m}{d})$, temos que $(\frac{m}{d}, m) = \frac{m}{d}$, pelo Teorema 1.5 podemos fazer o cancelamento $(\frac{m}{d})$ na congruência anterior, logo $k_1 \equiv k_2 \ (mod\ m)$. Note que m foi substituído por $d = m/(m/d)$.

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

□

Definição 1.6. *Dizemos que uma solução x_0 de $ax \equiv b \ (mod\ m)$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m.*

Definição 1.7. *Uma solução $\bar{a}$ de $ax \equiv 1\ (mod\ m)$ é chamado de um inverso de a módulo m.*

Teorema 1.6. *(Wilson) Seja $p \in \mathbb{N}$ um número primo. Então, $(p-1)! \equiv -1(mod\ p)$.*

Demonstração: Como $(2-1) \equiv 1 \equiv -1\ (mod\ 2)$ o resultado é válido para $p = 2$. Pela Proposição 1.7, a congruência $ax \equiv 1\ (mod\ p)$ tem uma única solução para todo a no conjunto $\{1, 2, 3, ..., p-1\}$ e como, deste elementos, somente 1 e $p-1$ são seus próprios inversos módulo p, podemos agrupar os números $2, 3, 4, ..., p-2$ em $\frac{p-3}{2}$ pares cujo produto seja congruente a 1 módulo p. Se multiplicarmos estas congruência membro a membro, teremos, pelo Teorema 1.4 (item 3), $2 \times 3 \times 4 \times ..... \times p-2 \equiv 1\ (mod\ p)$. Multiplicando-se ambos os lados desta congruência por $p-1$ teremos

$$2 \times 3 \times 4 \times ... \times (p-2) \times (p-1) \equiv (p-1) \equiv -1\ (mod\ p)$$

isto é $(p-1)! \equiv -1\ (mod\ p)$ uma vez que $p-1 \equiv -1\ (mod\ p)$.

□

Definição 1.8. *Sejam $a, m \in \mathbb{Z}, m > 2$ e $(a, m) = 1$. Dizemos que a é um resíduo quadrático módulo m se a equação $x^2 \equiv a \mod m$ tiver solução.*

Teorema 1.7. *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*

$$x^2 \equiv a\ (mod\ p).$$

Demonstração: Seja x_1 solução da congruência acima, podemos concluir que $-x_1$ também é solução pois, $(-x_1)^2 = (x_1)^2 \equiv a\ (mod\ p)$.Temos que mostrar que estas soluções são incongruentes. Suponhamos por absurdo que x_1 e $-x_1$ sejam congruentes módulo p, ou seja, $x_1 \equiv -x_1\ (mod\ p)$, daí $x_1 + x_1 \equiv -x_1 + x_1 (mod\ p)$, portanto, $2x_1 \equiv 0\ (mod\ p)$.

Temos que p é primo ímpar e não divide x_1 pois, se $p \mid x_1$, temos que $p \mid x_1^2$ e como estamos supondo que $x_1^2 \equiv a\ (mod\ p)$ temos que $x_1^2 - a = pq$, para algum q inteiro. O que implicaria que $p \mid a$ contradizendo a hipótese. Logo $p \nmid x_1$. e sabendo que x_1 é diferente de zero pois se $x_1 = 0$ e $x_1^2 \equiv a\ (mod\ p)$ implica $x_1^2 - a = pq$ para algum q inteiro, logo $-a = pq$ e, portanto, $p \mid a$, contradizendo a hipótese. Podemos concluir que não é possível ocorrer a congruência $2x_1 \equiv 0\ (mod\ p)$, pois p não divide a e além disso $x_1^2 \equiv a\ (mod\ p)$ daí podemos garantir que p não divide x_1^2 e portanto não divide x_1, assim podemos concluir que x_1 e $-x_1$ são incongruentes módulo p. A nossa meta agora e mostrar que existem apenas estas duas soluções incongruentes módulo p.

Assim, seja y uma solução de $x^2 \equiv a\ (mod\ p)$, então $y^2 \equiv a\ (mod\ p)$ como x_1 é solução teremos que $x_1^2 \equiv a\ (mod\ p)$, portanto $x_1^2 \equiv y^2 \equiv a\ (mod\ p)$ e assim, $x_1^2 - y^2 \equiv$

$0\ (mod\ p)$, onde podemos concluir $(x_1 + y)(x_1 - y) \equiv 0\ (mod\ p)$, como p é primo temos que $p \mid x_1 + y$ ou $p \mid x_1 - y$ sendo o mesmo que $x_1 + y \equiv 0\ (mod\ p)$ ou $x_1 - y \equiv 0\ (mod\ p)$ daí $y \equiv -x_1\ (mod\ p)$ ou $y \equiv x_1\ (mod\ p)$. Portanto, caso exista soluções, serão apenas duas soluções incongruentes módulo p.

Proposição 1.8. *Seja p um número primo ímpar. Dentre os números $\{1, 2, \ldots, p-1\}$, $\frac{p-1}{2}$ são resíduos quadráticos módulo p e $\frac{p-1}{2}$ não são.*

Demonstração: Serão considerados os quadrados dos números de 1 a $p - 1$. Logo, $(1)^2 \equiv 1\ (mod\ p)$, ou seja, 1 é resíduo quadrático da congruência $x^2 \equiv 1\ (mod\ p)$, notemos que $(-1)^2 = (1)^2 \equiv 1\ (mod\ p)$,ou seja, -1 também é solução desta congruência e, além disso, temos que $-1 \equiv p + (-1) = p - 1\ (mod\ p)$, onde $(p - 1)$ também é solução da congruência, pois $(p-1)^2 = p^2 - 2p + 1$, portanto $(p-1)^2 \equiv 1\ (mod\ p)$, logo pelo Teorema 1.7 concluímos que 1 e $p-1$ são as únicas soluções incongruentes de $x^2 \equiv 1(mod\ p)$, entre os números $1, 2, ..., p - 1$.

Consideremos agora 2^2 que será congruente a algum número k diferente de 1, da mesma forma $(-2)^2$ também é. Note que $-2 \equiv p + (-2) = p - 2\ (mod\ p)$, novamente usando o Teorema 1.7 concluímos que 2 e $p - 2$ são as únicas soluções incongruentes de $x^2 \equiv k\ (mod\ p)$ dentre os números $i = 1, 2, 3, ..., p - 1$.

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

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

$$(1, p-1)(2, p-2)(3, p-3), ..., (\frac{p-1}{2}, \frac{p-1}{2})$$

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

□

1.3 O anel dos inteiros de Gauss

Ao estudar questões de teoria dos números relacionadas à reciprocidade cúbica e biquadrática, Gauss (1777-1855) percebeu que essa investigação se tornava mais simples

trabalhando em um subconjunto dos números complexos onde a parte real e a parte imaginária eram dadas por números inteiros. Este subconjunto é denominado anel dos inteiros de Gauss em sua homenagem. Veremos que o problema de caracterizar os inteiros primos que são soma de dois quadrados é equivalente a um certo problema de fatoração neste anel.

Definição 1.9. *Um anel $(A, +, .)$ é um conjunto A com pelo menos dois elementos, munido de uma operação denotada por "$+$" (chamada adição) e de uma operação denotada por "." (chamada multiplicação) que satisfazem as condições seguintes:*

A.1) *A adição é associativa, isto é,*

$$\forall x, y, z \in A, (x + y) + z = x + (y + z).$$

A.2) *Existe um elemento neutro com respeito à adição, isto é,*

$$\exists 0 \in A \text{ tal que}, \forall x \in A, 0 + x = x \text{ e } x + 0 = x.$$

A.3) *Todo elemento de A possui um inverso com respeito à adição, isto é,*

$$\forall x \in A, \exists z \in A \text{ tal que } x + z = 0 \text{ e } z + x = 0.$$

A.4) *A adição é comutativa, isto é,*

$$\forall x, y \in A,\ x + y = y + x.$$

M.1) *A multiplicação é associativa, isto é,*

$$\forall x, y, z \in A, (x.y).z = x.(y.z).$$

M.2) *A adição é distributiva relativamente à multiplicação, isto é,*

$$\forall x, y, z \in A\, x.(y + z) = x.y + x.z.$$

Se além das propriedades acima, também for satisfeita a propriedade (M.3) abaixo, o anel é dito ser um Anel Comutativo.

M.3) *A multiplicação é comutativa, isto é,*

$$\forall x, y \in A\, x.y = y.x.$$

Quando um anel satisfaz a propriedade (AM) abaixo ele é dito ser um Anel com unidade.

(AM) Existe um elemento neutro com respeito à multiplicação, isto é,

$$\exists 1 \in A \text{ tal que} \forall z \in A, 1.x = x \text{ e } x.1 = x.$$

Definição 1.10. *Seja $A, +, .$ um anel e B um subconjunto não vazio de A. Suponhamos que B seja fechado as operações $+$ e $.$ de A, isto é,*

1. $x, y \in B \Rightarrow x + y \in B$
2. $x, y \in B \Rightarrow x.y \in B$

Asim podemos também considerar a soma e o produto como operações em B. Se $B, +, .$ for um anel com as operações de A dizemos que B é um subanel de A.

Exemplo 1.3. *$(\mathbb{Z}, +, .)$ é um anel, onde $+$ e $.$ são a adição e a multiplicação usuais dos inteiros. A operação $.$ é comutativa e 1 é o elemento neutro para esta operação.*

Exemplo 1.4. *$(\mathbb{Q}+, .), (\mathbb{R}, +, .)$ e $(\mathbb{C}, +, .)$ são anéis, onde $+$ e $.$ são a adição e a multiplicação usuais. Em cada caso, a operação $.$ é comutativa e 1 é a identidade.*

Exemplo 1.5. *Para todo $n \geq 0$, seja $n\mathbb{Z} = \{na; a \in \mathbb{Z}\}$. Com as operações induzidas pelas operações de $\mathbb{Z}$, temos que $(n\mathbb{Z}, +, .)$ é um anel, onde a operação $.$ é comutativa e não tem identidade para esta operação, se $n \neq 1$.*

Definição 1.11. *O anel dos inteiros de Gauss é definido como sendo o conjunto:*

$$\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}.$$

Com as seguintes operações:

Adição - $z_1 + z_2 = (a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i$

Multiplicação - $z_1.z_2 = (a_1 + b_1 i).(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i$

Definição 1.12. *Um anel $(D, +, .)$ é chamado domínio ou domínio de integridade se ele satisfaz a seguinte condição:*

M.4) O produto de quaisquer dois elementos não nulos de D é um elemento não nulo, isto é,

$$\forall x, y \in D \backslash \{0\}, x.y \neq 0.$$

Um anel $(K, +, .)$ é chamado corpo se ele satisfaz a seguinte condição:

M.4′) Todo elemento diferente de zero de k possui um inverso com respeito à multiplicação, isto é,

$$\forall x \in K \backslash \{0\}, \exists y \in K \text{ tal que } x.y = 1.$$

Definição 1.13. *Um domínio euclidiano* $(D, +, ., \varphi)$ *é um domínio de integridade* $(D, +, .)$ *tal que exite uma função*

$$\varphi : D\backslash\{0\} \longrightarrow \mathbb{N} = \{0, 1, 2...\}$$

que satisfaz as propriedades seguintes:

$1)\forall a, b \in D, b \neq 0$, *existem* $t, r \in D$ *tais que*

$$a = bt + r \ com \begin{cases} \varphi(r) < \varphi(b) \\ ou\ r = 0, \end{cases}$$

$2)\varphi(a) \leq \varphi(ab), \forall a, b \in D\backslash\{0\}$.

Exemplo 1.6. $(\mathbb{Z}, +, .)$ *é um domínio*

Exemplo 1.7. $(\mathbb{Z}[i], +, .)$ *é um domínio.*

Demonstração. *Sejam* $X, Y \in \mathbb{Z}[i]$, *onde* $X = a+bi$ *e* $Y = c+di$, *queremos mostrar que,*

$X.Y = 0$ *então* $X = 0$ *ou* $Y = 0$.

Suponha então que $Y \neq 0$, *ou seja,* c *ou* $d \neq 0$. *Logo,*

$X.Y = (a + bi)(c + di) = 0$

dai,

$ac + adi + bci - bd = 0$, *logo* $ac = bd$ *e* $ad = -bc$, *assim multiplicando a primeira equação por* c *e a segunda por* d *obtemos*

$ac^2 = cbd$ *e* $ad^2 = -cbd$, *com a soma das duas equações possuirmos*

$a(c^2 + d^2) = 0$, *por hipótese* c *ou* d *são diferente de* 0,

logo, $c^2 + d^2 \neq 0$, *então* $a = 0$. *Se* $c \neq 0$, *temos que*

$ad = -bc$, *como* $a = 0$, *logo*

$0 = -bc$ *ou seja* $b = 0$.

Portanto, $X = 0$.

□

Teorema 1.8. *(Algorítmo de Euclides para* $\mathbb{Z}$ *)*

Seja $|\ | : \mathbb{Z} \longrightarrow \mathbb{N}$ *a função valor absoluto. Então:*

i. $(\mathbb{Z}, +, ., |\ |)$ *é um domínio euclidiano, isto é,*

- $(\mathbb{Z}, +, .)$ *é um domínio,*

- $\forall a, b \in \mathbb{Z}, B \neq 0$, *existem* $t, r \in \mathbb{Z}$ *tais que*

$$a = bt + r \text{ com} \begin{cases} \mid r \mid < \mid b \mid \\ ou\ r = 0, \end{cases}$$

- $\forall a, b \in \mathbb{Z}\backslash\{0\}, \mid a \mid \leq \mid ab \mid$.

ii. Tais elementos t *e* r *podem ser efetivamente calculados.*

iii 1. *Em geral , tais inteiros* t *e* r *não são únicos.*

2. *É sempre possível escolher* $r \geq 0$*, e isso de maneira única.*

Demonstração. (i) e (ii): Que $(\mathbb{Z}, +, .)$ é um domínio, já que foi visto.

Se $b \in \mathbb{Z}\backslash\{0\}$, temos $\mid b \mid \geq 1$, e consequentemente

$$\mid a \mid \leq \mid a \mid\mid b \mid = \mid ab \mid, \forall a \in \mathbb{Z}.$$

Agora, sejam $a, b \in \mathbb{Z}, b \neq 0$. Procuramos elementos t e $r \in \mathbb{Z}$ tais que $a = bt + r$ com r "pequeno"e positivo (afim de obter $(iii.2)$), isto é, procuramos $t \in \mathbb{Z}$ tal que $a - bt$ seja "pequeno"e positivo.

Vamos prova no caso $b > 0$ e $a \geq 0$. Neste caso, temos $b \geq 1$ e existe um único inteiro t tal que

$$tb \leq a \ e \ (t+1)b > a.$$

Observamos que este inteiro t é necessariamente tal que $0 \leq t \leq a$, de modo que calculando $0b, 1b, 2b, 3b, ..., ab$, vamos efetivamente encontrá-lo. Tome $r = a - tb($ que pode ser efetivamente calculando pois a e b são dados e t foi calculado); temos $a = bt + r$ com $r \geq 0$; além disto, de $(t+1)b > a$, obtemos $\mid r \mid = r = a - tb < b = \mid b \mid$. Os outros casos será de forma análoga.

Tratamos agora o problema da unicidade. Se existem elementos $t_1, r_1, t_2, r_2 \in \mathbb{Z}$ tais que

$a = bt_1 + r_1 = bt_2 + r_2$ com $\begin{cases} 0 \leq r_1 < \mid b \mid \\ 0 \leq r_2 < \mid b \mid \end{cases}$, então temos $\mid b \mid\mid t_1 - t_2 \mid = \mid b(t_1 - t_2) \mid =$ $\mid r_2 - r_1 \mid < \mid b \mid$, logo $\mid t_1 - t_2 \mid = 0$ e portanto, $t_1 = t_2$ e $r_1 = r_2$. Falta agora verificar $(iii.1)$. De fato, podemos escrever o número 3 das seguintes formas

$$3 = 2.1 + 1 \ (t = 1, r = 1)$$

$$3 = 2.2 + (-1) \ (t = 2, r = -1),$$

isto é, temos duas possibilidades para a divisão de 3 por 2.

□

Definição 1.14. *Se D é um anel e $a \in D$, então um elemento $b \in D$ é um divisor ou fator de a (em D), se existe $c \in D$ tal que $a = bc$.*

Definição 1.15. *Um elemento $a \in D$ é invertível (em D) se existe $b \in D$ tal que $ab = 1$. Denotaremos por D^* o conjunto dos elementos invertíveis de D*

Exemplo 1.8. $\{a \in \mathbb{Z} \mid a \text{ é } invertível\} = \{1, -1\}$

Definição 1.16. *Seja $N : \mathbb{Z}[i] \to \mathbb{N}$, a função norma onde $N(a + bi) = a^2 + b^2$.*

Exemplo 1.9. $\{\alpha \in \mathbb{Z}[i] \mid \alpha \text{ é } invertível\} = \{\alpha \in \mathbb{Z}[i] \mid N(\alpha) = 1\} = \{\pm 1, \pm i\}$.

De fato, considere $\alpha = a + bi \in \mathbb{Z}[i]$ um elemento invertível. Assim, $N(\alpha) = a^2 + b^2 = 1$. As únicas soluções inteiras que satisfazem esta última igualdade são $a = \pm 1$ e $b = 0$, concedendo assim, $\alpha = \pm 1$, ou $a = 0$ e $b = \pm 1$ o que nos dá $\alpha = \pm i$.

Definição 1.17. *Dois elementos $a, b \in D$ são associados (em D) se existe $u \in D$, u invertível em D, tal que $a = ub$.*

Exemplo 1.10. *Dado $a \in \mathbb{Z}, \{b \in \mathbb{Z} \mid b \text{ é associado a } a\} = \{a, -a\}$*

Definição 1.18. *Um elemento $a \in D \backslash \{0\}$ é irredutível (em D) se as duas condições seguintes são satisfeitas:*

1. *a não é invertível em D.*
2. *a não possui fatoração não-trivial em D, isto é,*

   $\forall b, c \in D$ tais que $a = bc$ então b ou c é invertível em D.

Observe que os únicos divisores de um elemento irredutível a são os elementos associados de a em D e os elementos invertíveis de D.

Exemplo 1.11. $\{a \in \mathbb{Z} \mid a \text{ é } irredutível\} = \{\pm p \mid p \text{ } primo\}$.

1.4 O anel dos quatérnios

Definição 1.19. *O anel dos quatérnios é definido como sendo o conjunto $Q = \{a + bi + cj + dk; a, b, c, d \in \mathbb{R}\}$. A operação de soma é definida coordenada a coordenada e para o produto será usada $i^2 = j^2 = k^2 = ijk = -1$.*

Estas igualdades têm os seguintes resultados $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$ e por fim $ik = -j$. Assim, as leis que definem as operações em Q são:

$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = a+a'+(b+b')i+(c+c')j+(d+d')k$

e

$(a+bi+cj+dk).(a'+b'i+c'j+d'k) = aa'-bb'-cc'-dd'+(ab'+ba'+cd'-c'd)i+(ac'-bd'+ca'+db')j+(ad'+bc'-cb'+da')k.$

Q é um anel de divisão, também conhecido como corpo não comutativo. Mas, se $a \in \mathbb{R}$ e $\alpha \in Q$ então a e α comutam, ou seja, $\alpha a = a\alpha$. Claramente, $\mathbb{C} = \{a+bi; a,b \in \mathbb{R}\} = \{a+bi+0j+0k; a,b \in \mathbb{R}\} \subset Q$.

Se $\alpha = a+bi+cj+dk \in Q$, definimos o conjugado de α como $\overline{\alpha} = a-bi-cj-dk$ e a norma de α como:

$N(\alpha) = \alpha.\ \overline{\alpha} = (a+bi+cj+dk).(a-bi-cj-dk)$

$= a^2-abi-acj-adk+abi-bi^2-bi.cj-bi.dk+acj-cj.bi-c^2j^2-cj.dk+adk-dk.bi-ckdj-dk^2$

$= a^2-abi+abi-acj+acj-adk+adk+b^2-bcij+bcij-bdik+bdik+c^2-cdjk+cdjk+d^2$

$= a^2+b^2+c^2+d^2 \neq 0$, no caso em que $\alpha \neq 0$, usando a relação de Hamilton que $ik=-ki$, $ij=-ji$ e $jk=-kj$.

Segue da definição de norma que se $\alpha \neq 0$, assim:

$N(\alpha) = \alpha.\overline{\alpha},\ \alpha^{-1} = \frac{\overline{\alpha}}{N(\alpha)}$.

Lema 1.2. . *A conjugação em Q satisfaz às seguintes propriedades:*

1. Se $\alpha \in Q$, então $\overline{\overline{\alpha}} = \alpha$.
2. Se $\alpha,\ \beta \in Q$ e $r,s \in \mathbb{R}$, então $\overline{r\alpha+s\beta} = r\overline{\alpha}+s\overline{\beta}$.
3. Se $\alpha,\beta \in Q$, então $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$.

Demonstração:

1. Seja $\alpha \in Q$, então:
   $\overline{\overline{\alpha}} = \overline{\overline{(\alpha)}} = \overline{(a-bi-cj-dk)} = a+bi+cj+dk = \alpha$
2. Sejam $\alpha,\beta \in Q$ e $r,s \in \mathbb{R}$, então:
   $\overline{r\alpha+s\beta} = \overline{r(a_1+b_1i+c_1j+d_1k)+s(a_2+b_2i+c_2j+d_2k)}$
   $= \overline{(ra_1+rb_1i+rc_1j+rd_1k)+(sa_2+sb_2i+sc_2j+sd_2k)}$
   $= ra_1-rb_1i-rc_1j-rd_1k+sa_2-sb_2i-sc_2j-sd_2k$
   $= r(a_1-b_1i-c_1j-d_1k)+s(a_2-b_2i-c_2j-d_2k) = r\overline{\alpha}+s\overline{\beta}.$

3. Sejam $\alpha, \beta \in Q$, então:

   $\overline{\alpha\beta} = \overline{(a+bi+cj+dk)(a'+b'i+c'j+d'k)}$

   $= \overline{aa'+ab'i+ac'j+ad'k+ba'i+bb'i^2+bc'ij+bd'ik+ca'j+cb'ji+cc'j^2+cd'jk}$
   $\overline{+da'k+db'ki+dc'kj+dd'k^2}$

   $= aa'-ab'i-ac'j-ad'k-ba'i+bb'i^2+bc'ij+bd'ik-ca'j+cb'ji+cc'j^2+cd'jk-$
   $da'k+db'ki+dc'kj+dd'k^2$

   $= a'a-b'ia-c'ja-d'ka-a'bi+b'bi^2+c'jbi+d'kbi-a'cj+b'icj+c'cj^2+d'kcj-$
   $a'dk+b'idk+c'jdk+d'dk^2$

   $= (a'-b'i-c'j-d'k)(a-bi-cj-dk)$

   $= \overline{\beta}\overline{\alpha}$

   □

Lema 1.3. *A norma em Q satisfaz às seguintes propriedades:*

1. Se $\alpha \in Q$, então $N(\alpha) \in \mathbb{R}, N(\alpha) \geq 0$ e $N(\alpha) = 0 \Longleftrightarrow \alpha = 0$
2. Se $\alpha, \beta \in Q$, então $N(\alpha\beta) = N(\alpha)N(\beta)$.

Demonstração:

1. Seja $\alpha \in Q$ então:

   $N(\alpha) = \alpha\overline{\alpha} = a^2+b^2+c^2+d^2 \geq 0 \in \mathbb{R}$.

   Seja $N(\alpha) = 0$ então,

   $a^2+b^2+c^2+d^2 = 0$, note que $a^2+b^2+c^2+d^2 \in \mathbb{R}$, assim a única possibilidade será quando $a = b = c = d = 0$, então $\alpha = a+bi+cj+dk = 0+0i+0j+0k = 0$

   Reciprocamente, seja $\alpha = 0$ e como $\alpha = a+bi+cj+dk = 0$, ou seja $a = b = c = d = 0$, logo teremos que:

   $N(\alpha) = a^2+b^2+c^2+d^2 = 0^2+0^2+0^2+0^2 = 0$, ou seja, $N(\alpha) = 0$.

2. Seja $\alpha, \beta \in Q$, usando o Lema 1.2, temos:

$$\begin{aligned} N(\alpha\beta) &= (\alpha\beta)(\overline{\alpha\beta}) \\ &= \alpha(\beta\overline{\beta})\overline{\alpha} \\ &= \alpha N(\beta)\overline{\alpha} \\ &= \alpha\overline{\alpha}N(\beta) \\ &= N(\alpha)N(\beta) \end{aligned}$$

   □

Definição 1.20. *Dizemos que $m \in \mathbb{Z}, m \neq 1$, é livre de quadrados quando o único quadrado que divide m é 1. Isto é, $x^2 \mid m$ implica que $x^2 = 1$.*

Exemplo 1.12. *(a) $m = -1$ é livre de quadrados.*

(b) Todo número primo p é livre de quadrados.

1.5 Anéis quadráticos

Definição 1.21. *Seja $\alpha \in \mathbb{C}$. Dizemos que α é um inteiro algébrico se α anula um polinômio mônico $f(x) = a_n X^n + a_{n-1} X^{n-1} + ... + a_0 \in \mathbb{Z}[X]$.*

Definimos então os inteiros de $\mathbb{Q}[\sqrt{m}]$ como sendo o conjunto dos inteiros algébricos que estão em $\mathbb{Q}[\sqrt{m}]$. Assim, para cada inteiro m livre de quadrado o conjunto dos inteiros de $\mathbb{Q}[\sqrt{m}]$. é um anel chamado anel quadrático.

Definição 1.22. *Os elementos de $\mathbb{Z}[\theta]$ podem ser escritos de uma das seguintes formas*

1. *$a + b\theta$, com $a, b \in \mathbb{Z}$; ou*
2. *$\frac{a}{2} + \frac{b}{2}\sqrt{m}$ com $a, b \in \mathbb{Z}$ e de mesma paridade, isto é, $a \equiv b \ (mod\ 2)$.*

$$\theta = \begin{cases} \frac{1+\sqrt{m}}{2} se\ m \equiv 1 \ (mod\ 4), \\ \sqrt{m} \ se\ m \equiv 2, 3 \ (mod\ 4). \end{cases}$$

Assim, para cada inteiro m livre de quadrado, $\mathbb{Z}[\theta]$ é anel quadrático formado pelos inteiros $\mathbb{Q}[m]$.

Exemplo 1.13. *$\mathbb{Z}[i]$ é um exemplo com $m = -1 \equiv 3 \ (mod\ 4)$ e $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ com $m = -3 \equiv 1 \ (mod\ 4)$.*

Teorema 1.9. *Se $m < 0$, existe um algorismo da divisão em $\mathbb{Z}[\theta]$, isto é, $\mathbb{Z}[\theta]$ é um anel euclidiano, quando $m = -1, -2, -3, -7, -11$.*

Demonstração: Dados $\alpha, \beta \in \mathbb{Z}[\theta], \beta \neq 0$, queremos encontrar $q, r \in \mathbb{Z}[\theta]$ tais que $\alpha = q\beta + r$ com $N(r) < N(\beta)$. Mas,

$$N(r) = N(\alpha - q\beta) = N((\frac{\alpha}{\beta} - q)\beta) = N(\frac{\alpha}{\beta} - q)N(\beta)$$

e portanto basta mostrar que se $\gamma \in \mathbb{Q}[\theta] = \mathbb{Q}[\sqrt{m}]$, o corpo das frações de $\mathbb{Z}[\theta]$, existe $q \in \mathbb{Z}[\theta]$ tal que $N(\gamma - q) < 1$.

Quando $m \equiv 2,3 \ (mod\ 4)$, isto é, quando $m = -1, -2$, se $\gamma = a + b\sqrt{m}$ com $a, b \in \mathbb{Q}$, tomamos $x, y \in \mathbb{Z}$ tais que $\mid a - x \mid \leq \frac{1}{2}$ e $\mid b - y \mid \leq \frac{1}{2}$. Assim, se $q = x + y\sqrt{m}$,

$$N(\gamma - q) = N(a - x + (b - y)\sqrt{m}) \leq (a - x)^2 - m(b - y)^2 \leq \frac{1}{4} + \mid m \mid \frac{1}{4} < 1.$$

Quando $m \equiv 1 \ (mod\ 4)$, isto é, quando $m = -3, -7, -11$, se, como acima $\gamma = a + b\sqrt{m}$ com $a, b \in \mathbb{Q}$,tomamos $y = \frac{v}{2}$ com $v \in \mathbb{Z}$ tal que $\mid b - y \mid \leq \frac{1}{4}$ e depois $x = \frac{u}{2}$ com $u \in \mathbb{Z}, u \equiv v \ (mod\ 2)$, tal que $\mid a - x \mid \leq \frac{1}{2}$. Sabemos que $m \equiv 1 \ (mod\ 4)$, u e v têm que ter a mesma paridade .

Assim, se $q = x + y\sqrt{m}$, então

$$N(\gamma - q) = N(a - x + (b - y)\sqrt{m}) \leq (a - x)^2 - m(b - y)^2 \leq \frac{1}{4} + \mid m \mid \frac{1}{4} < 1.$$

e o Teorema está demonstrado.

□

1.6 O anel dos quatérnios inteiros de Hurwitz

O anel dos quatérnios inteiros de Hurwitz, subanel do anel dos quatérnios, pode ser apresentado de duas formas diferentes:

Sejam $H = \{(a\xi + bi + cj + dk); a, b, c, d \in \mathbb{Z}\}$ e $H' = \{\frac{1}{2}(a' + b'i + c'j + d'k); a', b', c', d' \in \mathbb{Z}$ *e* $a' \equiv b' \equiv c' \equiv d' (mod\ 2)\}$. Seja $\xi = \frac{1}{2}(1 + i + j + k)$.

Lema 1.4. *Afirmamos que* $H = H'$.

Demonstração: De fato, se $\alpha = a\xi + bi + cj + dk \in H$, então

$$\begin{aligned} \alpha &= \frac{a}{2}(1 + i + j + k) + bi + cj + dk \\ &= \frac{a}{2} + i(\frac{a}{2} + b) + j(\frac{a}{2} + c) + k(\frac{a}{2} + d) \\ &= \frac{1}{2}[a + i(a + 2b) + j(a + 2c) + k(a + 2d)], \end{aligned}$$

e estes coeficientes satisfazem $a \equiv 2b + a \equiv 2c + a \equiv 2d + a \ (mod\ 2)$. Então, $\alpha \in H'$.

Reciprocamente, se $\alpha = \frac{1}{2}(a' + b'i + c'j + d'k) \in H'$ assim,

$$\begin{aligned} \alpha &= \frac{1}{2}a' + \frac{1}{2}b'i + \frac{1}{2}c'j + \frac{1}{2}d'k \\ &= \frac{1}{2}a' + \frac{1}{2}a'i - \frac{1}{2}a'i + \frac{1}{2}a'j - \frac{1}{2}a'j + \frac{1}{2}a'k - \frac{1}{2}a'k + \frac{1}{2}b'i + \frac{1}{2}c'j + \frac{1}{2}d'k \\ &= \frac{a'}{2}(1 + i + j + k) + \frac{b' - a'}{2}i + \frac{c' - a'}{2}j + \frac{d' - a'}{2}k, \end{aligned}$$

então $\alpha = a'\xi + \frac{b'-a'}{2}i + \frac{c'-a'}{2}j + \frac{d'-a'}{2}k$ e como a', b', c' e d' tem a mesma paridade, $\frac{b'-a'}{2}, \frac{c'-a'}{2}, \frac{d'-a'}{2} \in \mathbb{Z}$ e $\alpha \in H$.

□

Como acabamos de demostrar que $H' = H$, passaremos a denotá-lo o anel dos quatérnios inteiros de Hurwitz por H.

Lema 1.5. *H é um subanel de Q*

Demonstração: De fato, seja $A = a_1\xi + b_1i + c_1j + d_1k$ e $B = a_2\xi + b_2i + c_2j + d_2k$ dois elementos de H onde ($a_1, b_1, c_1, d_1, a_2, b_2, c_2$ *e* $d_2 \in \mathbb{Z}$), logo, podemos deduzir que:

i. $S \neq \emptyset$ pois, $\xi = 3i + j + 2k \in H$

ii. $A - B = a_1\xi + b_1i + c_1j + d_1k - (a_2\xi + b_2i + c_2j + d_2k)$

$= (a_1 - a_2)\xi + (b_1 - b_2)i + (c_1 - c_2)j + (d_1 - d_2)k$

$= a'\xi + b'i + c'j + d'k \in H.$

iii. $A.B = (a_1\xi + b_1i + c_1j + d_1k).(a_2\xi + b_2i + c_2j + d_2k)$

$= (a_1a_2\xi^2 - b_1b_2 - c_1c_2 - d_1d_2) + (a_1b_2\xi + b_1a_2\xi + c_1d_2 - c_2d_1)i + (a_1c_2\xi - b_1d_2 + a_2c_1\xi + d_1d_2)j + (a_1d_2\xi + b_1c_2 - c_1b_2 + d_1a_2\xi)k$

$= \xi((a_1a_2\xi - \frac{1}{\xi}b_1b_2 - \frac{1}{\xi}c_1c_2 - \frac{1}{\xi}d_1d_2)) + (a_1b_2\xi + b_1a_2\xi + c_1d_2 - c_2d_1)i + (a_1c_2\xi - b_1d_2 + a_2c_1\xi + d_1d_2)j + (a_1d_2\xi + b_1c_2 - c_1b_2 + d_1a_2\xi)k$

$= a"\xi + b"i + c"j + d"k \in H$

Portanto, H é um sub-anel de Q.

□

Se $\alpha = \frac{1}{2}(a+bi+cj+dk) \in H$, assim α é a raiz o polinômio mônico $X^2 - aX + N(\alpha) \in \mathbb{Z}[X]$.

De fato, $X^2 - aX + N(\alpha) = (\alpha)^2 - a\alpha + N(\alpha)$

$= (\frac{1}{2}(a + bi + cj + dk))^2 + a(a + bi + cj + dk) + \frac{1}{4}(a^2 + b^2 + c^2 + d^2)$

$= \frac{1}{4}[a^2 - b^2 - c^2 - d^2 + (ab + abcd - cd)i + (ac - bd + ac + bd)j + (ad + ad + bc - bc)k] + \frac{1}{4}(a^2 + b^2 + c^2 + d^2)$

$= \frac{1}{4}a^2 - \frac{1}{4}b^2 - \frac{1}{4}c^2 - \frac{1}{4}d^2 + \frac{1}{2}abi + \frac{1}{2}acj + \frac{1}{2}adk - \frac{1}{2}abi - \frac{1}{2}a^2 - \frac{1}{2}acj - \frac{1}{2}adk + \frac{1}{4}a^2 + \frac{1}{4}b^2 + \frac{1}{4}c^2 + \frac{1}{4}d^2 = 0.$

Note que o anel dos inteiros de Gauss, $\mathbb{Z}[i] = \{a + bi, a, b \in Z\}$, é um subanel de H. Com efeito, se $a + bi \in \mathbb{Z}[i]$, então $a + bi = \frac{2a}{2} + \frac{2b}{2}i + 0j + 0k \in H$. Assim, sejam $A = a_1 + b_1i$ e $B = a_2 + b_2i$. Daí,

i. $A - B = a_1 + b_1 i - a_2 - b_2 i = \frac{2}{2}(a_1 - a_2) + \frac{2}{2}(b_1 - b_2) + 0j + 0k \in \mathbb{Z}[i]$.

ii. $A.B = (a_1 + b_1 i).(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i = \frac{2}{2}a' + \frac{2}{2}b'i + 0j + 0k \in \mathbb{Z}[i]$.

Portanto, $\mathbb{Z}[i]$ é um subanel de H.

Lema 1.6. *Se $\alpha \in H$ então $N(\alpha) \in \mathbb{N}$.*

Demonstração: Considere $\alpha = \frac{1}{2}(a + bi + cj + dk) \in H$ da definição de H' temos a mesma paridade. Se a, b, c, d são todos pares, então a^2, b^2, c^2, d^2 são todos divisíveis por 4 e portanto $N(\alpha) = \frac{1}{4}(a^2 + b^2 + c^2 + d^2) \in \mathbb{N}$. Se a, b, c, d são todos ímpares, então $a^2 \equiv b^2 \equiv c^2 \equiv d^2 \equiv 1 \ mod\ 4$, logo $a^2 + b^2 + c^2 + d^2$ é divisível por 4 e portanto $N(\alpha) = \frac{1}{4}(a^2 + b^2 + c^2 + d^2) \in \mathbb{N}$.

□

Lema 1.7. *Seja $\alpha \in H$. Logo, α é inversível se, e somente se, $N(\alpha) = 1$.*

Demonstração: Se α é inversível, então $\alpha\alpha^{-1} = 1$ e portanto $N(\alpha)N(\alpha^{-1}) = N(\alpha\alpha^{-1}) = N(1) = 1$. Pelo Lema 1.6, $N(\alpha) \in \mathbb{N}$ resulta que $N(\alpha) = N(\alpha^{-1}) = 1$. Reciprocamente, se $N(\alpha) = 1$ então $\alpha\bar{\alpha} = 1$, logo $\alpha^{-1} = \bar{\alpha}$.

□

Lema 1.8. *H possui exatamente 24 elementos inversíveis.*

Demonstração: *Considere $\alpha = \frac{1}{2}(a + bi + cj + dk) \in H$ um elemento inversível. Pelo Lema 1.7, $N(\alpha) = \frac{1}{4}(a^2 + b^2 + c^2 + d^2) = 1$. Portanto, as soluções possíveis desta equação são:*

1. *Um dos valores a^2, b^2, c^2 ou d^2 é igual a 4 e os demais são nulos, resultando 8 elementos inversíveis: $\pm 1, \pm i \pm j$ e $\pm k$.*
2. *$a^2 = b^2 = c^2 = d^2 = 1$ pelo princípio fundamental da contagem, tem-se 16 elementos inversíveis da forma $\frac{1}{2}(a + bi + cj + dk)$ com $a, b, c, d \in \{1, -1\}$*

□

Proposição 1.9. *Existe um algoritmo da divisão em H, isto é, dados $\alpha, \beta \in H, \beta \neq 0$, existem $q, r \in H$ tais que $\alpha = q\beta + r$ com $N(r) < N(\beta)$.*

Demonstração: Começamos como na demonstração do Teorema 1.9. Dados $\alpha, \beta \in H, \beta \neq 0$, queremos encontrar $q, r \in H$ tais que $\alpha = q\beta + r$ com $N(r) < N(\beta)$. Mas,

$$N(r) = N(q\beta - \alpha) = N((\frac{\alpha}{\beta} - q)\beta) = N(\frac{\alpha}{\beta} - q)N(\beta),$$

e com $\frac{\alpha}{\beta} \in Q$ o anel dos quatérnios, basta mostrar que se $\gamma \in Q$, existe $q \in H$ tal que $N(\gamma - q) < 1$.

Seja $\gamma = u + vi + xj + yk \in Q$. Escolhemos $a \in \mathbb{Z}$ tal que $\mid u - \frac{a}{2} \mid \leq \frac{1}{4}$ e escolhemos $b, c, d \in \mathbb{Z}$ com $a \equiv b \equiv c \equiv d \ (mod\ 2)$, tais que $\mid v - \frac{b}{2} \mid \leq \frac{1}{2}$, $\mid x - \frac{c}{2} \mid \leq \frac{1}{2}$ e $\mid y - \frac{d}{2} \mid \leq \frac{1}{2}$. Assim, se $q = \frac{1}{2}(a + bi + cj + dk)$, então

$$N(\gamma - q) = N((u + vi + xj + yk - \tfrac{1}{2}(a + bi + cj + dk))$$
$$= N(u - \tfrac{a}{2} + (v - \tfrac{b}{2})i + (x - \tfrac{c}{2})j + (y - \tfrac{d}{2})k)$$
$$= (u - \tfrac{a}{2})^2 + (v - \tfrac{b}{2})^2 + (x - \tfrac{c}{2})^2 + (y - \tfrac{d}{2})^2$$
$$\leq (\tfrac{1}{4})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 = \tfrac{1}{16} + \tfrac{1}{4} + \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{13}{16} < 1,$$

□

Definição 1.23. *Sabemos que I é um ideal a esquerda de H se na multiplicação é exigido apenas que $\forall \alpha \in H$ e $\beta \in I, \alpha\beta \in I$.*

Definição 1.24. *Dizemos que I é um ideal principal de A quando existe $a \in A$ tal que*

$$I = aA = \{ab;\ b \in A\}$$

:

Lema 1.9. *Todo ideal I à esquerda de H é principal.*

Demonstração: Podemos supor $I \neq (0)$. Seja $\beta \in I$ tal que $\beta \neq 0$ e $N(\alpha) \geq N(\beta), \forall \alpha \in I, \alpha \neq 0$. Pelo algoritmo da divisão existem $q, r \in H$ tais que $\alpha = q\beta + r$ com $N(r) < N(\beta)$. Então, como $r \in I$ pela escolha de β, temos que ter $r = 0$ e portanto $\alpha \in I$.

□

Definição 1.25. *Dizemos que um elemento $\alpha \in H$ é central se $\alpha\beta = \beta\alpha, \forall \beta \in H$.*

Exemplo 1.14. *Todo elemento $\alpha \in \mathbb{Z}$ é central.*

Definição 1.26. *Dizemos que um elemento central α é primo se $\alpha \mid \beta\gamma \Longrightarrow \alpha \mid \beta$ ou $\alpha \mid \gamma$.*

Lema 1.10. *Todo elemento $\alpha \in H$ central e irredutível é primo.*

Demonstração: Seja $\alpha \in H$ central e irredutível. Suponha que $\alpha \mid \beta\gamma$ e que $\alpha \nmid \beta$. Seja $\delta \in H$ tal que $\alpha\delta = \beta\gamma$. Considere o ideal à esquerda $I = (\alpha, \beta)$. Como α é irredutível e I é principal, resulta que $I = (\alpha)$ ou $I = H$.

De fato, como $(q) = I = (\alpha, \beta)$, e como $\alpha \in (\alpha, \beta) = I = (q)$, assim $\alpha \in (q)$

$\Longrightarrow \alpha = nq$, ou seja, $n = 1$ e $q = \alpha$ ou $n = \alpha$ e $q = 1$

$\Longrightarrow I = (\alpha)$

Portanto, temos que $I = (1) \Rightarrow I = H$. Por outro lado como $\alpha \nmid \beta, \beta \notin (\alpha)$ e $I = H$. Assim, como $1 \in I$, existem $u, v \in H$ tais que $1 = u\alpha + v\beta$. Multiplicando à direita por γ, temos $\gamma = u\alpha\gamma + v\beta\gamma = u\alpha\gamma + v\alpha\delta$. Como α é central α comuta com γ e com δ. Assim, $\gamma = u\gamma\alpha + v\delta\alpha = (u\alpha + v\delta)\alpha$ e $\alpha \mid \gamma$, concluindo nossa demonstração.

□

2 REPRESENTAÇÃO DE INTEIROS COMO SOMA DE QUADRADOS

Historicamente, um problema que recebeu uma boa dose de atenção é o de representar números inteiros como a soma de quadrados. Entre os matemáticos que estudaram este problema estavam Mohamed Ben Alhocain (século X), Leonardo da Pisa (mais conhecido como Fibonacci, 1175-1230), Vieta (1540-1603) e Xylander (século XVI, editor e comentarista da Diophantus). Bachet (1581-1638), famoso por sua edição própria de Diophantus, fez algumas observações sobre esse problema, mas parece ter sido Girard (1595-1632) que primeiro declarou corretamente as condições necessárias e suficientes para que a equação $n = x^2 + y^2$ possua soluções inteiras.

Pouco depois, Fermat (1601-1665), muito provavelmente de forma independente, afirmou, como condição sobre n, que $n \equiv 1 \ (mod \ 4)$ e que quando n é dividido por seu maior fator quadrado, o quociente não deve conter nenhum primo $q \equiv 3 \ (mod \ 4)$. Não há indicação de que Girard tenha (ou mesmo tenha alegado ter) uma prova para sua declaração, enquanto Fermat alegou ter uma "prova irrefutável"de sua autoria, e enquanto ele nunca tornou público, o conteúdo de suas cartas (para Descartes e para Mersenne) deixa quase nenhuma dúvida de que ele tinha uma prova e que isso foi baseado em um método de sua própria autoria chamado "método do descenso infinito".

Um pouco mais adiante, o matemático Eduard Waring (1734-1789) estudou com mais intensidade este problema fazendo varias outras afirmações. Ele chegou a afirmar que um número inteiro pode ser representado por no máximo quatro quadrados, nove cubos e no máximo 19 quartas potências. Foi Lagrangre quem conseguiu demonstrar o problema de Waring para o caso em que a soma pode ser representado por no máximo quatro quadrados.

Neste trabalho estudaremos critérios para definir quando um inteiro pode ser escrito como soma de dois, três ou quatro quadrados.

2.1 Soma de dois quadrados

Nesta seção 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.

$$x^2 + y^2 = n,$$

apresenta solução em inteiros.

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

Demonstração: Sejam u e v cada um uma soma de dois quadrados. Assim, existem a, b, c e d inteiros tais que $u = a^2 + b^2$ e $v = c^2 + d^2$, nosso objetivo é mostrar que uv também pode ser representado por uma soma de dois quadrados, ou seja, que existem s e t inteiros tais que $uv = s^2 + t^2$. Note que,

$uv = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$

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

Agora, vamos somar e subtrair $2(ac)(bd)$. Obtendo,

$uv = (a^2 + b^2)(c^2 + d^2)$

$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 + 2(ac)(bd) - 2(ac)(bd)$

e finalmente temos:

$uv = (ac)^2 + 2(ac)(bd) + (bd)^2 + (ad)^2 - 2(ac)(bd) + (bc)^2$

$uv = ((ac) + (bd))^2 + ((ad) - (bc))^2$

Encontramos $s = (ac) + (bd)$ e $t = (ad) - (bc)$ de modo que $uv = s^2 + t^2$.

□

Teorema 2.1. *Seja $p \in \mathbb{N}$ um número primo. As seguintes afirmações são equivalentes*

1. *$p = 2$ ou $p \equiv 1 \ (mod\ 4)$.*
2. *A equação $x^2 \equiv -1 \ (mod\ p)$ tem solução.*
3. *p é redutível em $\mathbb{Z}[i]$.*
4. *p é soma de dois quadrados.*

Demonstração: $1 \Rightarrow 2$: Se $p = 2$, basta tomar $x = 1$ e teremos $1^2 \equiv 1 \equiv -1 \ (mod\ 2)$.

Se $p \equiv 1 \ (mod\ 4)$, usando o Teorema 1.6, temos que $(4n)! = (p-1)! \equiv -1 \ (mod\ p)$. Note que,

$(4n) = p - 1$ para algum $n \in \mathbb{Z}$,

$(4n)! = 1 \times 2 \times 3 \times 4 \times ... \times 2n \times (2n + 1) \times (2n + 2) \times ... \times 4n =$

$1 \times (p - 1) \times 2 \times (p - 2) \times (3) \times (p - 3) \times ..... \times (2n) \times (p - 2n)$

o que nos dá

$$(4n)! = \prod_{k=1}^{2n} k(p-k) \equiv \prod_{k=1}^{2n} -k^2 \equiv (\prod_{k=1}^{2n} k)^2 \ (mod\ p).$$

Assim, fazendo $b = (\prod_{k=1}^{2n} k)$, temos que:

$$(-1) \equiv (p-1)! \equiv (4n)! \equiv (\prod_{k=1}^{2n} k)^2 \equiv b^2 \ (mod\ p)$$

e a equação $x^2 \equiv -1 \ (mod\ p)$ tem solução.

$2 \Rightarrow 3$: Considere b uma solução da equação $x^2 \equiv -1 \ (mod\ p)$. Então $p|(b^2+1)$, em $\mathbb{Z}[i]$, $p|(b+i)(b-i)$. Se p fosse irredutível em $\mathbb{Z}[i]$, como $\mathbb{Z}[i]$ é um anel euclidiano, p seria um elemento primo e logo $p|(b+i)$ ou $p|(b-i)$. Se $p|(b+i)$ pelo critério de divisibilidade existirá $c+di \in \mathbb{Z}[i]$ tal que $b+i = p(c+di)$. Assim dessa igualdade segue que $1 = pd$, o que não é possível, pois p é primo e $d \in \mathbb{Z}$.

$3 \Rightarrow 4$: Como p é redutível, $p = (a+bi)(c+di)$, com $(a+bi)$ e $(c+di)$ não são inversíveis. Logo, $N(a+bi) = a^2+b^2 \neq 1$ e $N(c+di) = c^2+d^2 \neq 1$. Como $p \times p = p^2 = N(p) = N((a+bi)(c+di)) = N(a+bi)N(c+di) = (a^2+b^2)(c^2+d^2)$, assim $p = a^2+b^2 = c^2+d^2$, isto é, p é soma de dois quadrados.

$4 \Rightarrow 1$ Seja $x \in \mathbb{Z}$. O valor de x possui duas possibilidades se x é impar logo $x^2 \equiv (1 \ mod\ 4)$ e se x é par, $x^2 \equiv 0 \ (mod\ 4)$. Suponha que $p = a^2+b^2$. Assim, $a^2+b^2 \equiv 0$ ou $a^2+b^2 \equiv 1$ ou $a^2+b^2 \equiv 2 \ (mod\ 4)$. Como p é primo, $a^2+b^2 \equiv 0 \ (mod\ 4)$ não acontece, e $a^2+b^2 \equiv 2 \ (mod\ 4)$ só acontece se $p = 2$. Portanto, $p = 2$ ou $p \equiv 1 \ (mod\ 4)$.

□

Teorema 2.2. *Os elementos irredutíveis de $\mathbb{Z}[i]$ são:*

1. *$\pm p, \pm pi$, com p primo em $\mathbb{N}$ tal que $p \equiv 3 \ (mod\ 4)$.*
2. *$a+bi$, com $a^2+b^2 = p$, p número primo em $\mathbb{N}$.*

Demonstração: Os elementos listados no item 1 são irredutíveis em $\mathbb{Z}[i]$ pelo Teorema 2.1. Considere $a+bi \in \mathbb{Z}[i]$ um elemento no item 2. Assim, $a^2+b^2 = p$ sendo $p \in \mathbb{N}$ número primo. Se $a+ib$ são redutíveis, logo $a+bi = \alpha\beta$, como $\alpha, \beta \in \mathbb{Z}[i]$ não inversíveis. Logo, $p = a^2+b^2 = N(a+bi) = N(\alpha\beta) = N(\alpha)N(\beta)$. Neste caso temos que $N(\alpha) = 1$ ou $N(\beta) = 1$, isto é, α ou β é inversível o que é considerado uma contradição.

Vamos agora mostrar que não existem outros elementos irredutíveis em $\mathbb{Z}[i]$. Suponha que $a+bi \in \mathbb{Z}[i]$ é irredutível e que não é do item 2. Logo, a^2+b^2 não é primo em $\mathbb{Z}$, isto é, irredutível $\mathbb{Z}[i]$, isto é, $a^2+b^2 = mn$ com $m \neq 1$ ou $n \neq 1$. É fácil ver que $a-bi$ também é irredutível em $\mathbb{Z}[i]$. Com efeito se $a-bi$ fosse redutível teríamos $a-bi = uv$ e $a+bi = \overline{uv}$ e assim teríamos que $a+bi$ seria também redutível. Como

$(a+bi)(a-bi) = a^2+b^2 = mn$ e $a+bi$ e $a-bi$ são irredutíveis, podemos supor que $a+bi = \alpha m$, com α inversível, isto é, $\alpha = \pm 1$ ou $\alpha = \pm i$. Como $a+bi$ é irredutível em $\mathbb{Z}[i]$, m é irredutível em $\mathbb{Z}$, isto é, m é primo em $\mathbb{Z}$, e $a+bi$ é um elemento do tipo 1.

□

Pelo Teorema 1.9, $\mathbb{Z}[i]$ é um anel euclidiano. Como todo anel euclidiano é um anel fatorial, temos então o seguinte resultado.

Teorema 2.3. *Todo elemento não nulo e não inversível de $\mathbb{Z}[i]$ é escrito de maneira única a menos de elementos inversíveis - como produto de elementos irredutíveis.*

Observações:

1. A maneira de escrever um número primo como a soma de dois quadrados $p = a^2+b^2$ com $a \geq b > 0$ é única. Com efeito note que $p = a^2+b^2 = c^2+d^2$, assim $(a+bi)(a-bi) = (c+di)(c-di)$ como estes quatros elementos são irredutíveis então $(a+bi) = \alpha(c+di)$ ou $(a+bi) = \alpha(c-di)$ como α é inversível, isto é, $\alpha = \pm 1$ ou $\alpha = \pm i$. Portanto, $a = \pm c$ e $b = \pm d$ ou $a = \pm d$ e $b = \pm c$.

2. Como $1-i = -i(1+i)$, $1+i$ e $1-i$ são associados. Usando a última igualdade, temos $2 = 1^2+1^2 = (1+i)(1-i) = -i(1+i)^2$.

3. Quando $p \equiv 1 \ mod\ 4$ escrevemos $p = a^2+b^2$. Como p é impar então a e b tem paridade distintas assim supondo $a > b > 0$. Logo, verificamos que $a+bi$ e $a-bi$ não são associados.

Proposição 2.1. *. Seja p um número primo tal que $p \equiv 3\ (mod\ 4)$, $d \in \{1,2,...,p-1\}$ é um resíduo quadrático módulo p, então $p-d$ não é.*

Demonstração: Observamos que $d \neq p-d$, pois caso contrário $2d = d+p-d = p$. Suponha que p e $p-d$ sejam resíduos quadrático módulo p. Então existem $x, y \in \{1,2,...,p-1\}$ tais que $x \neq d$ e $y \neq p-d$, $x^2 \equiv d\ mod\ p$ e $y^2 \equiv p-d\ (mod\ p)$. Assim, $x^2+y^2 \equiv d+p-d \equiv p \equiv 0\ (mod\, p)$ e portanto $p \mid (x^2+y^2)$. Logo, em $\mathbb{Z}[i]$, $p \mid (x+iy)(x-iy)$, e como pelo Teorema 2.2, p é irredutível em $\mathbb{Z}[i]$, $p \mid (x+iy)$ ou $p \mid (x-iy)$. Suponha que $p \mid (x+iy)$. Logo, existe $a+bi \in \mathbb{Z}[i]$ uma vez que $p(a+bi) = x+iy$ e portanto $p \mid x$ e $p \mid y$ o que não é possível pois se este fato acontecer teríamos $y < p$ e $x < p$, porém $x, y \in \{1,2,...,p-1\}$.

□

Teorema 2.4. *Sendo p um primo a equação $x^2+y^2 = p$ possui solução inteira se, e somente se, $p = 2$ ou $p \equiv 1\ (mod\ 4)$.*

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 que* $p = 2 = 1^2 + 1^2$*, assim para* $p = 2$ *o nosso problema está resolvido. Logo, faltar mostrar no caso de* $p \equiv 1 \pmod 4$ *.*

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 por* a *por quatro são* $0, 1, 2$ *e* 3*.*

Daí, $a \equiv 0, 1, 2,$ *ou* $3 \pmod 4$*. Assim, se* $a \equiv 0 \pmod 4$ *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* $1 \pmod 4$*.*

Agora observe que já possuímos o fato de que $a^2 \equiv 0 \pmod 4$ *ou* $a^2 \equiv 1 \pmod 4$ *e* $x^2 + y^2 = p$ *conclui-se que* $p \equiv 1 \pmod 4$*, de fato; o que devemos mostrar é que a congruência* $p \equiv 3 \pmod 4$ *sendo* p *primo não é possível de acontecer, como já foi visto temos que as únicas possibilidades para* x *e* y *serão* 0 *ou* 1*, assim suponhamos que,* $x^2 \equiv y^2 \equiv 0 \pmod 4$ *teremos* $x^2 + y^2 \equiv 0 + 0 \pmod 4$*, logo* $p \equiv 0 \pmod 4$*, da mesma forma será feita para* $x^2 \equiv y^2 \equiv 1 \pmod 4$ *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 todo* $p = 2$ *já sabemos que este poder ser escrito como uma soma de dois quadrados,* $2 = 1^2 + 1^2$*.*

Tomemos agora um p *primo que satisfaz* $p \equiv 1 \pmod 4$ *e usado o Teorema* 2.1 *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 observamos 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* $(m+1)^2 > (\sqrt{p})^2$*, daí obtemos que* $(m + 1)^2 > p$*, assim o total de pares é superior a* p*.*

Sabemos que um sistema completo de resídios módulos p *tem exatamente* p *elementos, se consideramos* $f(u, v)$ *módulo* p *teremos mais números do que classes de resíduos, daí pelo princípio da casa dos pombos existem pelo menos 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,*

$u_1 + xv_1 - u_2 \equiv u_2 + xv_2 - u_2 \ (mod\ p)$

$u_1 + xv_1 - u_2 \equiv xv_2 \ (mod\ p)$

daí, $u_1 + xv_1 - u_2 - xv_1 \equiv xv_2 - xv_1 \ (mod\ p)$*, resultando em*

$u_1 - u_2 \equiv xv_2 - xv_1 \ (mod\ p)$*, assim*

$u_1 - u_2 \equiv -x(v_1 - v_2) \ (mod\ p)$

elevando a potência 2 *a congruência acima temos*

$(u_1 - u_2)^2 \equiv (-x)^2(v_1 - v_2)^2 \ (mod\ p) \equiv x^2(v_1 - v_2)^2 \ (mod\ p).$

Portanto, $(u_1 - u_2)^2 \equiv -1(v_1 - v_2)^2 \ (mod\ p)$*, pois* $x^2 \equiv -1 \ (mod\ p)$*. Chamando* $a = u_1 - u_2$ *e* $b = v_1 - v_2$*, teremos* $a^2 \equiv -b^2 \ (mod\ p)$ *adicionando* b^2 *a congruência teremos* $a^2 + b^2 \equiv -b^2 + b^2 \ (mod\ p)$ *o que se resulta em* $a^2 + b^2 \equiv 0 \ (mod\ p)$*, assim concluímos que* $p \mid a^2 + b^2$*. Como os pares* (u_1, v_1) *e* (u_2, v_2) *são distintos então* a *e* b*, ambos inteiros não 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 o 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* $\mid a \mid \leq m < \sqrt{p}$*, analogamente* $\mid b \mid \leq m < \sqrt{p}$*. Daí* $\mid a \mid^2 < \sqrt{p}^2 = p$ *da mesma forma* $\mid b \mid^2 < \sqrt{p}^2 = p$*, assim* $a^2 + b^2 < p + p = 2p$*. Como* $p \mid a^2 + b^2$ *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 mais geral do que o anterior nos permite identificar inteiros que podem ser representados como a soma de dois quadrados.

Teorema 2.5. *Um inteiro* n *pode ser representado como a 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 $p_i \equiv 1 \ (mod\ 4)$ *e* $q_j \equiv 3 \ (mod\ 4)$*,* $i = 1, 2...., r, j = 1, 2, ..., s$ *e todos os expoentes* β_j *são pares.*

Demonstração: Considerando n com fatoração $n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} ... q_s^{\beta_s}$, queremos mostrar que n pode ser representado como a soma de dois quadrados, ou seja, tentaremos escrever cada fator n como a soma de dois quadrados.

Note que o primo $2 = 1^2 + 1^2$, assim aplicando o Lema 2.1 várias vezes chegamos ao seguinte resultado 2^{α} também pode ser representado como a soma de dois quadrados, conhecemos do Teorema 2.4 que todos p_i serão representados como soma de dois quadrados, logo $p_i^{\alpha_i}$ pode ser representado como a soma de dois quadrados, usando o Lema 2.1 novamente, $p_1^{\alpha_1} p_2^{\alpha_2} ... p_r^{\alpha_r}$ também.

Falta mostrar que os $q_j^{\beta_j}$ podem ser representados por uma soma de dois quadrados. Por hipótese temos que todos β_i são pares, ou seja, exite β_i' de modo que $\beta_i = 2\beta_i'$, assim $q_j^{\beta i} = (q_j)^{2\beta_i'} = (q_j^2)^{\beta_i'}$. Podemos escrever $q_j^2 = q_j^2 + 0$, isto é, podemos escrever q_j^2 como a soma de dois quadrados, logo 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 a soma de dois quadrados.

Vamos considerar que n possa ser escrito como a soma de dois quadrados e que existe um β_j que seja ímpar, sem perda de generalidade vamos considerar β_1 como sendo ímpar. Consideremos que $d = (a, b)$ onde a e b satisfazem a equação $a^2 + b^2 = n$. Como $d = (a, b)$ então $d \mid a$ e $d \mid b$, logo existem r_1 e r_2 tais que $a = r_1 d$ e $b = r_2 d$. Notemos que

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

então,

$$(\frac{a}{d}, \frac{b}{d}) = (\frac{r_1 d}{d}, \frac{r_2 d}{d}) = (r_1, r_2) = 1$$

Notemos que $d^2 \mid n$,pois $d \mid a$ e $d \mid b$, logo $a = r_1 d$ e $b = r_2 d$ e a e b satisfazem a equação $a^2 + b^2 = n$, então

$$\begin{aligned} n &= (r_1 d)^2 + (r_2 d)^2 \\ &= r_1^2 d^2 + r_2^2 d^2 \\ &= d^2(r_1^2 + r_2^2) \\ &= r d^2, \end{aligned}$$

com $r = r_1^2 + r_2^2$

Sendo β_1 ímpar e tendo $n = rd^2$ onde $r = \frac{n}{d^2}$, concluímos que o expoente de q_1 em r deve ser ímpar, pois os números r e $\frac{n}{d^2}$ têm a mesma decomposição primária. Como o expoente de q_1 é ímpar, então existe s inteiro tal que $r = q_1^{2s+1}\gamma$ e assim escrevemos $r = q_1^{2s} q_1^1 \gamma = q_1^1 q_1^{2s} \gamma$, ou seja, $q_1 \mid r$ e sabendo que $(r_1, r_2) = 1$ podemos observar $(q_1, r_1) = (q_1, r_2) = 1$. Vamos verificar que $(q_1, r_1) = 1$, temos os seguintes dados $(r_1, r_2) = 1$ e $q_1 \mid r$, de $(r_1, r_2) = 1$ garantimos a existência de x e y tais que $xr_1 + yr_2 = 1$, elevando ambos lados da igualdade ao quadrado, teremos:

$$\begin{aligned} (xr_1 + yr_2)^2 &= (xr_1)^2 + 2(xr_1)(yr_2) + (yr_2)^2 \\ &= x^2 r_1^2 + 2xr_1 yr_2 + y^2 r_2^2 \\ &= 1. \end{aligned}$$

Guardemos esta informação por enquanto, temos ainda que $q_1 \mid r$, ou seja, existe s inteiro de modo que $r = q_1 s$, mas por outro lado $r = r_1^2 + r_2^2$, logo $q_1 s = r_1^2 + r_2^2$ e assim segue que $r_2^2 = q_1 s - r_1^2$, lembremos também que $b = r_2 d$, onde $d = (a, b)$, por isso, $r_2 = \frac{b}{d}$ agora vamos substituir estes valores em $x^2 r_1^2 + 2xr_1 yr_2 + y^2 r_2^2 = 1$ e obteremos que

$$\begin{aligned} x^2r_1^2 + 2xr_1yr_2 + y^2r_2^2 &= x^2r_1^2 + 2xr_1y(\tfrac{b}{d}) + y^2(q_1s - r_1^2) \\ &= x^2r_1^2 + 2xr_1y(\tfrac{b}{d}) + y^2q_1s - y^2r_1^2 \\ &= 1, \end{aligned}$$

vamos juntar os termos que contém r_1 e os que contém q_1, assim ficaremos com $x^2r_1^2 + 2xr_1y(\frac{b}{d}) + y^2q_1s - y^2r_1^2 = 1$. Colocando em evidência obtemos r_1 e q_1,

$$(x^2r_1 + 2xy(\frac{b}{d}) - y^2r_1)r_1 + (y^2s)q_1 = 1,$$

observamos que $t = x^2r_1 + 2xy(\frac{b}{d}) - y^2r_1$ e $u = y^2s$ são números inteiros, portanto a expressão $tr_1 + uq_1 = 1$ nos diz que q_1 e r_1 são primos entre si, ou seja, $(q_1, r_1) = 1$, analogamente podemos mostrar que $(q_1, r_2) = 1$.

Usando a Proposição 1.7, garantimos que existe x de modo que $r_1x \equiv r_2 \ (mod\ q_1)$. Como $q_1 \mid r$, concluímos que $r \equiv 0 \ (mod\ q_1)$; Além disso $r = r_1^2 + r_2^2$, implicar em

$$r \equiv r_1^2 + r_2^2 \equiv 0 \ (mod\ q_1)$$

$$r_1^2 + r_2^2 - r_2^2 \equiv 0 - r_2^2 \equiv -r_2^2 \ (mod\ q_1)$$

.

Como $r_1x \equiv r_2 \ (mod\ q_1)$, aplicando a potência 2 na congruência temos $r_1^2x^2 \equiv r_2^2 \ (mod\ q_1)$. Agora utilizando a congruência anterior $r_1^2 \equiv -r_2^2 \ (mod\ q_1)$ e somando as duas últimas temos

$$r_1^2x^2 + r_1^2 = r_1^2(x^2 + 1) \equiv r_2^2 - r_2^2 \equiv 0 \ (mod\ q_1)$$

.

Portanto, $q_1 \mid r_1^2(x^2 + 1)$. Agora, usaremos o fato de que $(q_1, r_1) = 1$ para mostrar que $q_1 \nmid r_1^2$.

Para tanto, usaremos a demonstração pela contrapositiva. Suponhamos que $q_1 \mid r_1^2$, daí $q_1 \mid r_1r_1$. Como q_1 é primo temos $q_1 \mid r_1$ ou $q_1 \mid r_1$, portanto $q_1 \mid r_1$. O que contradiz o fato de $(q_1, r_1) = 1$.

Como q_1 é primo e $q_1 \mid r_1^2(x^2 + 1)$ então $q_1 \mid r_1^2$ ou $q_1 \mid (x^2 + 1)$, mas $q_1 \nmid r_1^2$ assim, $q_1 \mid (x^2 + 1)$, ou seja, $x^2 - 1 \equiv 0 \ (mod\ q_1)$ ou que vale $x^2 \equiv -1 \ (mod\ q_1)$. Notemos que a equação $x^2 \equiv -1 \ (mod\ q_1)$ possui solução para $q_1 \equiv 3 \ (mod\ 4)$ o que contradiz o Teorema 2.1, portanto todos os $\beta_j's$ são pares.

□

2.2 Soma de três quadrados

Nesta seção caracterizaremos os números inteiros que não podem serem escritos como a soma de três quadrados.

Teorema 2.6. *Qualquer inteiro escrito como $n \equiv 7 \ (mod\ 8)$ não pode ser representado como a soma de três quadrados.*

Demonstração: *Se $n \equiv 7 \ (mod\ 8)$, então n pode ser escrito como $n = 8k + 7$, com $k \in \mathbb{Z}$. Sendo a soma de um número par com número ímpar $8k + 7$, logo n é necessariamente, ímpar.*

Suponha, agora que $n = x_1^2 + x_2^2 + x_3^2$ com $x_1, x_2, x_3 \in \mathbb{Z}$. Então

$$7 \equiv n \equiv x_1^2 + x_2^2 + x_3^2 \ (mod\ 8),$$

ou seja, $7 \equiv s_1 + s_2 + s_3 \ (mod\ 8)$, como os possíveis restos r na divisão de um número n por 8 são $0, 1, 2, 3, 4, 5, 6$ ou 7, temos que

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

Concluímos assim, que $s_1, s_2, s_3 \in \{0, 1, 4\}$. Então, a congruência $7 \equiv s_1 + s_2 + s_3 \ (mod\ 8)$, indica que $s_1 + s_2 + s_3$ deve ser ímpar, pois como vimos o nosso n e ímpar. Logo o número de parcelas são ímpares, então $s_1 + s_2 + s_3$ é 1 ou 3. Como os únicos possíveis valores para s_1, s_2 e s_3 são $0, 1, 4$, temos então que

$$s_1 + s_2 + s_3 = 1 + 1 + 1 = 3,$$

$$s_1 + s_2 + s_3 = 1 + 0 + 4 = 5,$$

$$s_1 + s_2 + s_3 = 0 + 1 + 0 = 1,$$

$$s_1 + s_2 + s_3 = 1 + 4 + 4 = 9 \equiv 1 \ (mod\ 8).$$

Como em nenhuma dessas situações obtemos o resultado 7, n não pode ser escrito como soma de três quadrados.

□

Proposição 2.2. *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: *Será utilizado indução em k para prova este fato, notemos que o resultado vale para $k = 0$, daí temos que $n = 4^0(8m + 7) = (8m + 7)$. Vamos provar por absurdo que existem x_0, y_0, z_0 inteiros positivos tais que $n = (8m + 7) = x_0^2 + y_0^2 + z_0^2$. Sendo $n = 8m + 7$ então $n \equiv 7 \pmod 8$ e ainda podemos dizer que $n \equiv 1 \pmod 2$. Note que, quando dividimos a por 8 deixa os restos de $0, 1, 2, 3, 4, 5, 6, 7$ logo usando o teorema anterior podemos concluir que $a \equiv 0, 1, 2, 3, 4, 5, 6, 7 \pmod 8$ então, $a^2 \equiv 0, 1$ ou $4 \pmod 8$. Portanto, não possível termos $n \equiv 7 \pmod 8$, assim n não será representado como a soma de três quadrados.*

Supondo que $4^{k-1}(8m + 7)$ não será escrito como a soma de três quadrados, resta mostrar que $4^k(8m+7)$ não escrito como a soma de três quadrados. Como $k \geq 1$ e supondo por contradição que n possa ser escrito como a soma de três quadrados, ou seja, existem x_0, y_0, z_0 inteiros não positivos tais que $n = x_0^2 + y_0^2 + z_0^2 = 4^k(8m + 7)$ podemos concluir que $4 \mid n$, ou seja, n é par, de fato, $n = 4^k(8m + 7) = 4.4^{k-1}(8m + 7) = 2^2 4^{k-1}(8m + 7)$. Vamos mostra que, x_0, y_0, z_0 são todos pares. De fato, sendo n par então $n = x_0^2 + y_0^2 + z_0^2$ tem as seguintes possibilidades:

1. *Dois quadrados são ímpares e um seja par;*

2. *Todos os três quadrados sejam pares.*

Observemos que a primeira possibilidade não irá ocorrer, pois $n = x_0^2 + y_0^2 + z_0^2 \equiv 1^2 + 1^2 + 0^2 = 2 \pmod 4$, ou seja, dessa forma 4 não divide n o que é um absurdo. Então, resta o caso de que todos três quadrados são pares, ou seja, x_0, y_0, z_0 são todos pares.

Sendo x_0, y_0, z_0 todos pares então existem u, v, w inteiros positivos tais que $x_0 = 2u, y_0 = 2v, z_0 = 2w$, logo

$$\begin{aligned} 4^k(8m + 7) &= x_0^2 + y_0^2 + z_0^2 \\ &= (2u)^2 + (2v)^2 + (2w)^2 \\ &= 4u^2 + 4v^2 + 4w^2 \\ &= 4(u^2 + v^2 + w^2), \end{aligned}$$

Fazendo a divisão por 4, obtemos

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

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

□

2.3 Soma de quatro quadrados

Como foi abordado na introdução o matemático Waring fez a afirmação que todo número inteiro não negativo poderia ser representado como a soma de até quatro quadrados. Mostraremos aqui a vericidade da afirmação de Waring.

Proposição 2.3. *Seja p um número primo tal que $p \equiv 3\ (mod\ 4)$. Então existem $a, b \in \mathbb{Z}$ tais que $p \mid (1 + a^2 + b^2)$.*

Demonstração: Seja $d \in \{1, 2, ..., p-1\}$ o menor inteiro tal que d não é resíduo módulo p. Observamos que $d > 1$, já que 1 é resíduo quadrático módulo p. Assim, usando a contrapositiva da Proposição 2.1, temos que $d-1$ e $p-d$ são resíduos quadráticos módulo p e portanto existem $a, b \in \mathbb{Z}$ tais que $a^2 \equiv d-1\ (mod\ p)$ e $b^2 \equiv p-d\ (mod\ p)$. Portanto, $(1 + a^2 + b^2) \equiv 1 + d - 1 + p - d \equiv 0\ (mod\ p)$. Portanto, $p \mid (1 + a^2 + b^2)$.

□

Proposição 2.4. *. Seja $p \in \mathbb{Z}$ um número primo. Então p é redutível em H.*

Demonstração: Se $p = 2$ ou $p \equiv 1\ (mod\ 4)$, então, usando o Teorema 2.1, p é redutível em $\mathbb{Z}[i]$ e, a fortiori, em H. Se $p \equiv 3\ (mod\ 4)$, pela Proposição 2.3, existem $a, b \in \mathbb{Z}$ tais que $p \mid (1 + a^2 + b^2)$. Logo, $p \mid (1 + ai + bj)(1 - ai - bj)$. Suponha que p seja irredutível em H. Então, Lema 1.10, p é primo em H e consequentemente $p \mid (1 + ai + bj)$ ou $p \mid (1 - ai - bj)$. Em qualquer uma das duas possibilidades, existe um inteiro $x \in \mathbb{Z}$ tal que $px = 1 + ai + bj$ daí tem-se $1 = px$, o que não é possível.

□

Lema 2.2. *Sejam $x, y \in \mathbb{N}$. Suponha que x e y sejam a soma de quatro quadrados. Então xy é soma de quatro quadrados.*

Demonstração: Suponha que $x = a^2 + b^2 + c^2 + d^2$ e $y = (a')^2 + (b')^2 + (c)'^2 + (d)'^2$. E considerem $\alpha = a + bi + cj + dk$ e $\beta = a' + b'i + c'j + d'k$ elementos de H.

Então, $xy = (a^2 + b^2 + c^2 + d^2)((a')^2 + (b')^2 + (c')^2 + (d')^2) = N(\alpha)N(\beta) = N(\alpha.\beta)$ é a soma de quatro quadrados.

□

Lema 2.3. *Seja $n \in N$ tal que $2n$ é a soma de quatro quadrados. Então n é a soma de quatro quadrados.*

Demonstração: Suponha que $2n = a^2 + b^2 + c^2 + d^2$. Existe três possibilidades: todos serem pares, todos serem ímpares ou dois serem pares e dois ímpares. Vamos supor então que a e b como c e d tenham a mesma paridade. Temos que $n = \frac{a^2+b^2}{2} + \frac{c^2+d^2}{2}$.

Mas, $\frac{a^2+b^2}{2} = (\frac{a+b}{2})^2 + (\frac{a-b}{2})^2 = (a')^2 + (b')^2$, onde $a' = \frac{a+b}{2}$ e $b' = \frac{a-b}{2}$. Com a e b têm mesma paridade, $a', b' \in \mathbb{Z}$. Analogamente, existem $c', d' \in \mathbb{Z}$ tais que $\frac{c^2+d^2}{2} = (c')^2 + (d')^2$. Portanto, $n = \frac{a^2+b^2}{2} + \frac{c^2+d^2}{2} = (a')^2 + (b')^2 + (c')^2 + (d')^2$ é uma soma de quatro quadrados.

□

Teorema 2.7. *Todo número inteiro é soma de quatro quadrados.*

Demonstração: O Teorema Fundamental da Aritmética afirma que todo número inteiro maior que 1 decompõe-se em produto de primos(de maneira única, a menos da ordem). Logo mostramos que todo primo é soma de quadrados, pelo Lema 2.2, concluímos que todo número inteiro é soma de quatro quadrados. No caso em questão, os inteiros positivos. Se $p = 2$ ou $p \equiv 1$ $(mod\ 4)$, assim p é soma de dois quadrados portanto é soma de quatro quadrados.

Suponha agora que $p \equiv 3$ $(mod\ 4)$. Pela Proposição 2.4, p é redutível em H. Logo, existem, $\alpha, \beta \in H$ tais que $p = \alpha\beta$ como $N(\alpha) > 1$ e $N(\beta) > 1$. Como $p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$, temos necessariamente $N(\alpha) = p$ e $N(\beta) = p$. Seja $\alpha = \frac{1}{2}(a + bi + cj + dk)$. Então, $p = N(\alpha) = \frac{1}{4}(a^2 + b^2 + c^2 + d^2)$ e $4p = a^2 + b^2 + c^2 + d^2$, isto é, $4p$ é soma de quatro quadrados. Aplicando duas vezes o Lema 2.3, concluímos que p é soma de quatro quadrados.

□

3 TRIÂNGULOS RETÂNGULOS COM LADOS INTEIROS

A história de problemas envolvendo triângulos retângulos remonta até a remota antiguidade. Segundo Høyrup (2002, p. 385) o Teorema de Pitágoras foi usado em nove problemas encontrados em textos matemáticos babilônicos, que datam de uns mil anos antes do nascimento do próprio Pitágoras, o que nos leva a um anacronismo.

Este capítulo tem como finalidade estudar os triângulos retângulos com lados inteiros, os quais chamaremos, a partir de agora, apenas de triângulos retângulos.

Se x, y, z são números inteiros não negativos, dizemos que (x, y, z) é um terno pitagórico quando satisfaz a equação $x^2 + y^2 = z^2$. Apresentaremos aqui dois teoremas que nos dão condições necessárias e suficientes para que um terno (x, y, z) seja um terno pitagórico. Utilizando um destes resultados mostramos que se $x \geq 3$, existe pelo menos um triângulo retângulo com cateto x. Mostramos também como encontrar todos eles e quantos são em função da decomposição de x em fatores primos.

Já para a hipotenusa, mostraremos que existe um triângulo retângulo com hipotenusa z se, e somente se, z é divisível por um primo $p \equiv 1 \ mod \ 4$. Concluiremos mostrando como encontrar todos eles e quantos são em função da decomposição de z em fatores primos.

3.1 Ternos pitagóricos

Dado um terno pitagórico (x, y, z) se $(x, y) = 1$ daí temos que $(x, y) = (y, z) = 1$ dizemos que (x, y, z) é um terno pitagórico primitivo. Se (x, y, z) é um terno pitagórico e k é um número inteiro positivo, então (kx, ky, kz) também é um terno pitagórico. Com efeito $(kx)^2+(ky)^2 = k^2(x^2+y^2) = k^2z^2 = (kz)^2$. Se (x, y, z) é um terno pitagórico e $x = kx_1, y = ky_1$ e $z = kz_1$, então (x_1, y_1, z_1) também será um terno pitagórico. Com efeito, $(kx_1)^2 + (ky_1)^2 = k^2(x_1^2+y_1^2) = x^2+y^2 = z^2 = (kz_1)^2 = k^2z_1^2$ e como $k \neq 0$ resulta que $x_1^2+y_1^2 = z_1^2$. Assim, conhecendo os ternos pitagóricos primitivos, conhecemos todos eles. Então, como $(3, 4, 5)$ é um terno Pitagórico são, também as ternas $(12, 16, 20), (18, 24, 30), (21, 28, 35)$.

Teorema 3.1. *(x, y, z), é um terno pitagórico se, e somente, se existem inteiros u, v tais que $u > v > 0, u$ e v tem a mesma paridade, uv é um quadrado perfeito, $x = \sqrt{uv}, y = \frac{u-v}{2}$ e $z = \frac{u+v}{2}$.*

Demonstração: Suponha que (x, y, z) é um terno pitagórico. Como $z^2 = x^2 + y^2, x^2 = z^2 - y^2 = (z + y)(z - y)$. Sejam $u = z + y, v = z - y$. Então u e v são inteiros tais que $u > v > 0$,u e v tem a mesma paridade uv é um quadrado perfeito, somando as equações temos que, $u + v = 2z$, ou seja, $z = \frac{u+v}{2}$, fazendo a substituição temos:

$x = \sqrt{uv}, y = \frac{u-v}{2}$.

Reciprocamente, suponha que u e v satisfazem às condições do teorema. Como u e v tem a mesma paridade e $u > v > 0$ então $y = \frac{u-v}{2}$ e $z = \frac{u+v}{2}$ são inteiros positivos. Como uv é um quadrado perfeito, $x = \sqrt{uv}$ também é um inteiro positivo. Assim,

$x^2 + y^2 = (\sqrt{uv})^2 + (\frac{u-v}{2})^2 = \frac{4uv+u^2-2uv+v^2}{4} = \frac{u^2+2uv+v^2}{2} = (\frac{u+v}{2})^2 = z^2$. Portanto, (x, y, z) é um terno pitagórico.

□

Observação: Note que os pares (u, v) e (u', v') distintos podem determinar o mesmo triângulo retângulo $(9, 1)$ e $(8, 2)$, note que:

Para o par $(9, 1)$ será, $x = \sqrt{1.9} = \sqrt{9} = 3$ e $y = \frac{9-1}{2} = \frac{8}{2} = 4$

Para o par $(8, 2)$ será, $x = \sqrt{2.8} = \sqrt{16} = 4$ e $y = \frac{8-2}{2} = \frac{6}{2} = 3$

Assim estes pares determinam o triângulo retângulo cujos os catetos são 3 e 4.

Considerando todos triângulos retângulos com cateto x. Observando que para $x = 1$ e $x = 2$, não existem triângulos com esse cateto. De fato, não existem inteiros positivos u e v, tais que $u > v > 0$, de modo que u e v tem a mesma paridade, uv é um quadrado perfeito e $x^2 = uv$, isto é, $uv = 4$ ou $uv = 1$.

Proposição 3.1. *Se $x \geq 3$, existem um triângulo retângulo com cateto x.*

Demonstração: Se x é ímpar, tomamos $u = x^2$ e $v = 1$, pois satisfaz o Teorema 3.1, onde:

$u > v > 0$ têm a mesma paridade e $u.v$ e um quadrado perfeito.

$x = \sqrt{u.v} = \sqrt{x^2.1} = \sqrt{x^2} = x$, $y = \frac{u-v}{2} = \frac{x^2-1}{2}$ e

$z^2 = x^2 + y^2 = (x)^2 + (\frac{x^2-1}{2})^2 = x^2 + \frac{x^4-2.x^2+1}{4} = (\frac{x^2+1}{2})^2$

Se x é par, tomemos $u = \frac{x^2}{2}$ e $v = 2$ aplicando novamente o Teorema 3.1 tem-se que

$u > v > 0$ têm a mesma paridade e $u.v$ e um quadrado perfeito.

$x = \sqrt{u.v} = \sqrt{\frac{x^2}{2}.2} = \sqrt{x^2} = x$, $y = \frac{u-v}{2} = \frac{\frac{x^2}{2}-2}{2} = \frac{x^2-4}{4}$ e

$z^2 = x^2 + y^2 = (x)^2 + (\frac{x^2-4}{4})^2 = x^2 + \frac{x^4-8.x^2+16}{16} = (\frac{x^2+4}{4})^2$

□

Teorema 3.2. *Sejam x, y e z inteiros positivos. Então são equivalentes:*

1. $(x, y) = 1$ e $x^2 + y^2 = z^2$

2. $x = 2ab, y = a^2 - b^2$ ou vice-versa e $z = a^2 + b^2$, com a e b inteiros tais que $a > b > 0, (a, b) = 1$ e a e b tem paridade distinta.

Demonstração: $1 \Rightarrow 2$) Usando o Teorema 3.1, existem u e v tais que $u > v > 0$, onde u e v têm a mesma paridade, uv é um quadrado perfeito, $x = \sqrt{u.v}, y = \frac{u-v}{2}$ e $z = \frac{u+v}{2}$.

Suponhamos que u e v sejam ambos pares. Assim, escrevendo $u = 2m$ e $v = 2n$ de modo que $x = \sqrt{uv} = \sqrt{2m.2n} = 2\sqrt{m.n}$ e $y = \frac{u-v}{2} = \frac{2m-2n}{2} = m - n$. Com $(x, y) = 1$, resulta que $(m, n) = 1$. Como efeito, se $d = (m, n)$, como $u = 2m$ e $v = 2n$ assim temos que $y = m - n$ daí $d \mid y$. Por outro lado, $x^2 = 4mn$, usando o fato de que $(x, y) = 1$, temos $xm + yn = 1$ o que resulta $x^2m + y(xn) = x$, ou seja, $d \mid x^2m + y(xn)$, logo $d \mid x$. Portanto, $d \mid (x, y)$ assim temos que $d = 1$.

Além disso, m e n têm paridade distinta, pois caso contrário, $2 \mid x$ e $2 \mid y$, o que contradiz o fato de $(x, y) = 1$. Como $x^2 = 4mn$ e $(m, n) = 1$ resulta que m e n são quadrados perfeitos e portanto existem $a, b \in \mathbb{Z}$, $a > b > 0$ tais que $m = a^2$ e $n = b^2$ e a e b têm paridade diferente. Além disso, $x = 2\sqrt{mn} = 2\sqrt{a^2b^2} = 2ab$, $y = m - n = a^2 - b^2$ e como

$$\begin{aligned} z^2 &= x^2 + y^2 \\ &= (2ab)^2 + (a^2 - b^2)^2 \\ &= 4a^2b^2 + a^4 - 2a^2b^2 + b^4 \\ &= a^4 + 2a^2b^2 + b^4 \\ &= (a^2 + b^2)^2 \end{aligned}$$

daí temos, $z = a^2 + b^2$.

Suponhamos agora que u e v sejam ambos ímpares. Mostraremos que $(x, y) = 1$, resulta que $(u, v) = 1$. Com efeito, se $d = (u, v)$ então $d \mid u$ e $d \mid v$, de forma análoga que já foi feito, $d \mid x$ e $d \mid y$ e como $(x, y) = 1$ temos que $d = 1$. Como $x^2 = uv$ e $(u, v) = 1$, resulta que u e v são quadrados perfeitos e portanto existem $m, n \in \mathbb{Z}$,$m > n > 0$ tais que $u = m^2$ e $v = n^2$. Como u e v são ímpares, m e n também são ímpares. Logo,

$$\begin{aligned} y &= \tfrac{u-v}{2} \\ &= \tfrac{m^2-n^2}{2} \\ &= 2.(\tfrac{m+n}{2})(\tfrac{m-n}{2}) \\ &= 2ab. \end{aligned}$$

Além disso,

$$\begin{aligned} x &= \sqrt{u.v} \\ &= mn \\ &= (\tfrac{m+n}{2})^2 - (\tfrac{m-n}{2})^2 \\ &= a^2 - b^2 \end{aligned}$$

e como

$$\begin{aligned} z^2 &= x^2 + y^2 \\ &= (a^2 - b^2)^2 + (2ab)^2 \\ &= (a^2 + b^2)^2, \end{aligned}$$

daí temos que $z = a^2 + b^2$.

Resta mostrar que a e b têm paridade distinta. Se $m \equiv n \equiv 1 \ (mod\ 4)$ ou $m \equiv n \equiv 3 \ (mod\ 4)$, então $m + n \equiv 2 \ (mod\ 4)$ e $m - n \equiv 0 \ (mod\ 4)$ de modo que $a = \frac{m+n}{2}$ é ímpar e $b = \frac{m-n}{2}$ é par. Se $m \equiv 1 \ (mod\ 4)$ e $n \equiv 3 \ (mod\ 4)$ ou $n \equiv 1 \ (mod\ 4)$ e $m \equiv 3 \ (mod\ 4)$, então $m + n \equiv 0 \ (mod\ 4)$ e $m - n \equiv 2 \ (mod\ 4)$, de modo que $a = \frac{m+n}{2}$ é par e $b = \frac{m-n}{2}$ é ímpar.

$2 \Rightarrow 1)$ Como $x = 2ab$, $y = a^2 - b^2$ e $z^2 = a^2 + b^2$, temos que $z = x^2 + y^2$. Resta mostrar que $(x, y) = 1$. Observe que $x = 2ab$ é par enquanto que $y = a^2 - b^2$ é ímpar, uma vez que a e b têm paridade diferente. Suponha que $(x, y) \neq 1$ e seja p um número primo ímpar tal que $p \mid x$ e $p \mid y$ daí temos que $p \mid 2ab$, ou seja, $p \mid a$ ou $p \mid b$, como $p \mid y$ temos que $p \mid a^2 - b^2$, ou seja, $p \mid (a + b)$ ou $p \mid (a - b)$, consequentemente temos $p \mid a$ e $p \mid b$. Assim, $(a, b) \neq 1$, uma contradição.

□

3.2 Triângulos retângulos com um cateto fixo

Agora, trataremos determinadamente de todos os triângulos retângulos com um cateto fixo. Pela Proposição 3.1 para $x = 1$ ou $x = 2$, não existem triângulos retângulos com esse cateto.

Para determinar todos os triângulos retângulos com cateto x, tomamos todas decomposições $x^2 = uv$, com $u > v$ e u e v com a mesma paridade.

Como foi demonstrado pela Proposição 3.1, será trabalhado agora com um cateto fixo x, tomamos todas as decomposições $x^2 = uv$, com $u > v$ e u e v com a mesma paridade, existirá duas possibilidades para x ser par ou ímpar.

Se x é ímpar, escrevemos $x = p_1^{r_1} p_2^{r_2} ... p_k^{r_k}$, como os $p_i's$ primos ímpares distritos e $r_i > 0$ para $i = 1, 2, 3, ..., k$. Lembramos todos divisores de número ímpar são ímpares. Como $x^2 = p_1^{2r_1} p_2^{2r_2} ... p_k^{2r_k}$ daí x^2 tem $(2r_1 + 1)(2r_2 + 1)(2r_3 + 1)...(2r_k + 1)$ divisores que

formam os pares (u, v) tais que $x^2 = uv$. Porém, pelo Teorema 3.1, só estamos interessados nos pares (u, v) de modo que $u > v$. Logo, o par (x, x) será desprezado, e dos demais, apenas a metade satisfaz a condição $u > v$. Então, levando em conta que para cada par (u, v) acima com $u > v$ existem um triângulo retângulo com cateto x, se x é um número ímpar, existem

$$m = \frac{(2r_1 + 1)(2r_2 + 1)(2r_3 + 1)...(2r_k + 1) - 1}{2}$$

triângulos retângulos não semelhantes com cateto x.

Suponha agora que x é par. Escrevemos $x = 2^{r_1}p_2^{r_2}...p_k^{r_k}$ com os $p_i's$ primos ímpares e $r_i > 0$, para todo $i = 1, 2, 3, ..., k$. Assim, $x^2 = uv$ é par e u e v têm a mesma paridade resta que u e v são ambos pares. Escrevendo $u = 2u'$ e $v = 2v'$ daí $x^2 = uv = (2u')(2v')$, ou seja, $\frac{x^2}{4} = u'v'$, logo consideremos os pares (u', v') divisores de $\frac{x^2}{4}$ tais que $\frac{x^2}{4} = u'v'$ e $u' > v'$. Como $x^2 = 2^{2r_1}p_2^{2r_2}...p_k^{2r_k}$ assim, $\frac{x^2}{4} = \frac{2^{2r_1}}{4}p_2^{2r_2}...p_k^{2r_k}$, ou seja, $\frac{x^2}{4} = 2^{2r_1-2}p_2^{2r_2}...p_k^{2r_k}$ então $\frac{x^2}{4}$ tem $(2r_1 - 1)(2r_2 + 1)...(2r_k + 1)$ divisores que formam os pares (u', v') tais que $\frac{x^2}{4} = u'v'$. Usando o Teorema 3.1, só estamos interessados nos pares (u', v') tais que $u' > v'$. Logo, o par $(\frac{x}{2}, \frac{x}{2})$ deve ser desprezado, e dos demais, apenas a metade satisfaz a condição $u' > v'$, isto é, $u > v$ existe um triângulo retângulo com cateto x, se x é um número par, existem

$$m = \frac{(2r_1 - 1)(2r_2 + 1)(2r_3 + 1)...(2r_k + 1) - 1}{2}$$

triângulos retângulos não semelhantes com o cateto x.

Portanto, mostramos o seguinte Teorema.

Teorema 3.3. *Seja x um inteiro tal que $x \geq 3$. Escrevemos $x = p_1^{r_1}p_2^{r_2}...p_k^{r_k}$ se x é ímpar e $x = 2^{r_1}p_2^{r_2}...p_k^{r_k}$ se x é par, com $p_i's$ primos ímpares distintos e $r > 0$. Então existem m triângulos retângulos não semelhantes com cateto x, onde*

$$m = \frac{(2r_1 + 1)(2r_2 + 1)(2r_3 + 1)...(2r_k + 1) - 1}{2}$$

com x ímpar, e

$$m = \frac{(2r_1 - 1)(2r_2 + 1)(2r_3 + 1)...(2r_k + 1) - 1}{2}$$

com x par.

Proposição 3.2. *Existem infinitos triângulos retângulos com um de seus catetos e a hipotenusa números consecutivos.*

Demonstração: Tomando cada número ímpar $x, x \geq 3$, consideremos $u = x^2$ e $v = 1$. Logo, pelo Teorema 3.1, $z = \frac{u+v}{2} = \frac{x^2+1}{2} = \frac{x^2-1}{2} + 1 = \frac{u-v}{2} + 1 = y + 1$.

□

3.3 Exemplos

Exemplo 3.1. *Seja* $x = 12 = 2^2 \times 3$ *Será encontrado todos os triângulos retângulos com um dos catetos igual à* 12. *Como* 12 *é par, determinamos inicialmente todos os pares* (u', v') *tais que* $\frac{12^2}{4} = 36 = u'v'$ *como* $u' > v'$. *São eles* $(36, 1), (18.2), (12, 3), (9, 4)$. *Os valores para* $u = 2u', v = 2v', x = \sqrt{uv}, y = \frac{u-v}{2}$ *e* $z = \frac{x+y}{2}$ *estão calculados na tabela abaixo:*

u'	*v'*	*u*	*v*	*x*	*y*	*z*
36	*1*	*72*	*2*	*12*	*35*	*37*
18	*2*	*36*	*4*	*12*	*16*	*20*
12	*3*	*24*	*2*	*12*	*9*	*15*
9	*4*	*18*	*8*	*12*	*5*	*13*

Note que todos os casos temos $z^2 = x^2 + y^2$ *e que o numero de triângulos retângulos, 4, está de acordo com o Teorema* 3.3, *pois*

$$m = \frac{(4-1).(2+1)-1}{2} = \frac{3.3-1}{2} = \frac{8}{2} = 4.$$

Exemplo 3.2. *Seja* $x = 45 = 3^2 \times 5$

Será encontrado todos os triângulos retângulos com um dos catetos igual a 45. *Como* 45 *é ímpar, determinamos inicialmente todos os pares* (u, v) *tais que* $45^2 = 2025 = uv$ *com* $u > v$. *São eles* $(2025, 1), (675, 3), (405, 5), (225, 9), (135, 45), (81, 25)$ *e* $(75, 27)$. *Os valores para* $x = \sqrt{uv}, y = \frac{u-v}{2}$ *e* $z = \frac{x+y}{2}$ *estão calculados na tabela abaixo:*

u	*v*	*x*	*y*	*z*
2025	*1*	*45*	*1012*	*1013*
675	*3*	*45*	*336*	*339*
405	*5*	*45*	*200*	*205*
225	*9*	*45*	*108*	*117*
135	*15*	*45*	*60*	*75*
81	*25*	*45*	*28*	*53*
75	*27*	*45*	*24*	*51*

Assim, todos os casos possíveis de triângulos retângulos com o cateto fixo $x = 45$ *é* 7, *usando o Teorema* 3.3, *pois*

$$m = \frac{(4+1).(2+1)-1}{2} = \frac{5.3-1}{2} = \frac{14}{2} = 7.$$

Exemplo 3.3. *Seja* $x = 147 = 3 \times 7^2$

Encontraremos todos os triângulos retângulos com um dos catetos igual a 147. *Como este número é ímpar, então iremos encontrar todos os pares* (u, v) *tais que* $147^2 =$

$21609 = uv$, *como* $u > v$. *São eles* $(21609, 1), (7203, 3), (3087, 7), (2401, 9), (1029, 21), (441, 49)$ *e* $(343, 63)$. *Os valores para* $x = \sqrt{uv}, y = \frac{u-v}{2}$ *e* $z = \frac{x+y}{2}$ *estão calculados na tabela abaixo:*

u	v	x	y	z
21609	*1*	*147*	*10804*	*10805*
7203	*3*	*147*	*3600*	*3603*
3087	*7*	*147*	*1540*	*1547*
2401	*9*	*147*	*1196*	*1205*
1029	*21*	*147*	*504*	*525*
441	*49*	*147*	*196*	*245*
343	*63*	*147*	*140*	*203*

Assim, todos os casos possíveis de triângulos retângulos com o cateto fixo $x = 147$ *é* 7, *para comprovar isso, iremos trabalhar com o Teorema* 3.3

$$m = \frac{(2+1).(4+1)-1}{2} = \frac{3.5-1}{2} = \frac{14}{2} = 7.$$

3.3 Triângulos retângulos com a hipotenusa fixa

Agora, determinaremos os números inteiros positivos z que são hipotenusa de um triângulo retângulo. Assim, vamos encontrar todos os triângulos retângulos que possui z como a hipotenusa e quantos são eles, em função da decomposição de z em fatores primos.

Como foi demonstrado no Teorema 3.1, o qual determina as soluções de $x^2+y^2 = z^2$ pode ser reescrito como o produto de dois números inteiros: $x^2 = (z+y)(z-y) = uv$.

Para determinarmos os inteiros z que são hipotenusa de um triângulo retângulo, não é possível escrever z^2 como produto de dois inteiros em função de x e y, porém de modo similar ao da resolução da equação de grau 2 com discriminante negativo, que irá recair no conjunto dos números complexos onde encontramos as nossas raízes, a dependerão das variáveis x e y: $z^2 = x^2 + y^2 = (x + yi)(x - yi)$. Como $x, y \in \mathbb{Z}$.

Como foi estudado, onde foi utilizado a decomposição de z em fatores irredutíveis de $\mathbb{Z}[i]$ demostramos nossos resultados.

Teorema 3.4. *Seja* z *um número inteiro positivo. Então existe um triângulo retângulo com a hipotenusa* z *se, e somente se,* z *é divisível por um número primo* p *tal que* $p \equiv 1$ $(mod\ 4)$.

Demonstração: Seja p um número primo tal que $z = pz_1$ com $p \equiv 1$ $(mod\ 4)$. Usando o Teorema 2.1, temos que existem inteiros positivos a e b tais que $p = a^2 + b^2 =$

$N(a+bi)$. Logo,

$$\begin{aligned} p^2 &= N(a+bi)^2 \\ &= N((a+bi)^2) \\ &= N(a^2-b^2+2abi) \\ &= (a^2-b^2)^2+(2ab)^2. \end{aligned}$$

Supondo que $a > b > 0$, temos que $a^2 - b^2 > 0$ e $2ab > 0$. Assim,

$$\begin{aligned} z^2 &= p^2 z_1^2 \\ &= ((a-b)^2+(2ab)^2)(z_1^2) \\ &= ((a-b)^2 z_1^2+(2ab)^2)(z_1^2) \\ &= ((a-b)z_1)^2+(2abz_1)^2. \end{aligned}$$

Reciprocamente, suponha que z não seja divisível por nenhum primo p tal que $p \equiv 1\ (mod\ 4)$ e que $x^2+y^2=z^2$ com $x, y \in \mathbb{N}$, $x, y > 0$. Assim, a decomposição de z em fatores primos é da forma $z = 2^v q_1^{s_1} q_2^{s_2} ... q_l^{s_l}$ como $q_j \equiv 3\ (mod\ 4)$. Sendo $z^2 = (x+yi)(x-yi)$ e como $N(x+yi) = N(x-yi)$, logo tomando a decomposição de z^2 em elementos irredutíveis de $\mathbb{Z}[i]$ usando o Teorema 2.2 temos que $x+yi = u(1+i)^{(2v)} q_1^{s_1} q_2^{s_2} ... q_l^{s_l} = u((1+i)^2)^v q_1^{s_1} q_2^{s_2} ... q_l^{s_l} = u(2i)^v q_1^{s_1} q_2^{s_2} ... q_l^{s_l}$ com u inversível em $\mathbb{Z}[i]$. Então, $x+yi$ é um número real ou número imaginário puro, implicando, que $y = 0$ ou $x = 0$, que seria uma contradição.

□

É fácil ver que, como p é primo, a e b são primos entre si. Assim, pelo Teorema 3.2, $a^2 - b^2$ e $2ab$ são primos entre si. Seja $p = a^2 + b^2$ ou seja $a^2 = p - b^2$ assim, $d = (b, a^2) = (b, p - b^2)$ sendo d que irá dividir uma combinação $d \mid (b.b) + p - b^2$ ficando assim, $d \mid p$, então temos $d = 1$ ou $d = p$, porém $a, b < p$ então a única possibilidade será $d = 1$ sendo um caso particular do lema a seguir.

Lema 3.1. . *Sejam $p_1, ..., p_k$ número primos distintos tais que $p_j \equiv 1\ (mod\ 4)$. Suponha que $p_j = a_j^2 + b_j^2$ com $a_j, b_j \in \mathbb{Z}$ e seja $\alpha = x+yi = (a_1+b_1 i)^{n_1}(a_2+b_2 i)^{n_2}(a_3+b_3 i)^{n_3}...(a_k+b_k i)^{n_k}$. Então x e y são primos entre si em $\mathbb{Z}$.*

Demonstração: Primeiro observamos que, pelo Teorema 2.1 podemos escrever $p_j = a_j^2 + b_j^2$. Logo, usando os Teoremas 2.2 e 2.3 temos que $(a_1 + b_1 i)^{n_1}(a_2 + b_2 i)^{n_2}(a_3 + b_3 i)^{n_3}...(a_k + b_k i)^{n_k}$ é a decomposição (única) de α divisíveis por 2 ou por um primo q tal que $q \equiv 3\ (mod\ 4)$, pois $1 + i$ e q não aparecem na decomposição de α e x e y pois $\alpha = x + yi = (a_1 + b_1 i)^{n_1}(a_2 + b_2 i)^{n_2}(a_3 + b_3 i)^{n_3}...(a_k + b_k i)^{n_k}$ não podem ser ambos divisíveis por um primo p tal que $p \equiv 1\ (mod\ 4)$, porque para cada $a + bi$ que aparece na decomposição de α, o seu conjugado complexo não aparece nesta decomposição. Tiramos a conclusão de que x e y são primos entre si.

□

Agora iremos ver como encontrar todos os triângulos com a hipotenusa z.

Teorema 3.5. *Seja $z = p_1^{t_1} p_2^{t_2} ... p_k^{t_k} w$. Suponha que os números primos p_j são distintos, que $p_j \equiv 1 \ (mod\ 4)$ e que w não é divisível por nenhum primo p tal que $p \equiv 1 \ (mod\ 4)$. Então existem*

$$\sum_{m=1}^{k} 2^{m-1} \Big(\sum_{1 \leq j_1 < j_2 < ... < j_m \leq k} t_{j_1} t_{j_2} ... t_{j_m} \Big)$$

triângulos retângulos não semelhantes com hipotenusa z.

Demonstração: Seja $z = z_1 z_2$, onde todos primos p_j que dividem z_1 são tais que $p_j \equiv 1 \ (mod\ 4)$ e todos aqueles q_j que dividem z_2 são tais que $q_j = 2$ ou $q_j \equiv 3 \ (mod\ 4)$. Como foi feito na demonstração do Teorema 3.4, que como consequência dos Teoremas 2.2 e 2.3, x e y têm que ser múltiplos de z_2. Portanto, o que realmente importa na determinação dos triângulos retângulos hipotenusa z são os primos p_j que dividem z_1.

Considerando d um divisor de z_1, $z = dz_3$. Vamos obter x_1, y_1 primos entre si tais que $x_1^2 + y_1^2 = d^2$ e tomando $x = x_1 z_3$ e $y = y_1 z_3$ teremos que

$$\begin{aligned} x^2 + y^2 &= (x_1 z_3)^2 + (y_1 z_3)^2 \\ &= (x_1)^2 (z_3)^2 + (y_1)^2 (z_3)^2 \\ &= (x_1^2 + y_1^2) z_3^2 \\ &= d^2 z_3^2 \\ &= (dz_3)^2 \\ &= z^2. \end{aligned}$$

Logo, podemos supor que $z = p_1^{t_1} p_2^{t_2} ... p_k^{t_k} w$ com $p_j \equiv 1 \ (mod\ 4)$ e vamos encontrar x e y primos entre si tais que $x^2 + y^2 = z^2$.

Iremos trabalhar primeiramente para o caso particular para $k = 1$. Suponha então $z = p^t$, como $p = a^2 + b^2 = (a + bi)(a - bi)$. Logo

$$\begin{aligned} z^2 &= p^{2t} \\ &= N(p^t) \\ &= N((a + bi)^t) N((a - bi)^t) \\ &= N((a + bi)^t) N((a + bi)^t) \\ &= N((a + bi)^{2t}). \end{aligned}$$

Portanto, se $(a + bi)^{2t} = x + yi$ então como $N(a + bi)^{2t} = N(x + yi) = x^2 + y^2$, logo $z^2 = x^2 + y^2$ e, pelo Lema 3.1, x e y são primo entre si. Já no caso de x ou y serem

negativos, trocamos o sinal para obter o valor do cateto. Podemos escolher

$$\begin{aligned} z^2 &= p^{2t} \\ &= N(p^2) \\ &= N((a+bi)^t)N((a-bi)^t) \\ &= N((a-bi)^t)N((a-bi)^t) \\ &= N((a-bi)^{2t}). \end{aligned}$$

Mas, pela propriedade da conjugação complexa $(a-bi)^{2t} = x-yi$, assim obtemos o mesmo triângulo retângulo.

Porém, não podemos trocar alguns dos fatores $a+bi$ por $a-bi$ sem trocar todos eles porque, assim, neste caso, os inteiros x e y são ambos divisíveis por p. Ainda mais, devido à decomposição única dos elementos de $\mathbb{Z}[i]$ em produto de elementos irredutíveis, sendo assim, não é possível encontrar outro triângulo retângulo não semelhante a este com catetos primos entre si. Portanto, temos um triângulo retângulo com hipotenusa z e catetos x e y primos entre si.

Suponha agora que $k > 1, p_j = a_j^2 + b_j^2 = (a+bi)(a-bi)$ e $\alpha_j = a_j + b_j i$. Considere $\alpha = x + yi$ um dos número complexos $\beta_1\beta_2\beta_3...\beta_k$ onde $\beta_j = \overline{\alpha_j}^{2t_j}$ ou $\beta_j = \alpha_j^{2t_j}$. Assim, $N(\alpha) = z^2$, ou seja, $x^2 + y^2 = z^2$ e pelo Lema 3.1 x e y são primos entre si. Contando agora o total de triângulos. Existem 2^k possibilidades para escolha de α, porém, estamos contando mais dois a dois, um é o conjugando, gerando o mesmo triângulo retângulo. Logo, temos o total de $\frac{2^k}{2} = 2^{k-1}$ triângulos retângulos com catetos x e y primos entre si, tais que $x^2 + y^2 = z^2$. Analisando para o caso $k = 1$ só possuirá um triângulo retângulo com catetos primos entre si não semelhante a estes já obtido.

Considere $z = p_1^{t_1}p_2^{t_2}p_3^{t_3}...p_k^{t_k}$ com $p_j \equiv 1\ (mod\ 4)$. Vamos contar quantos são os triângulos retângulos com hipotenusa z.

Tomemos um divisor $d = p_{j_1}^{s_{j_1}}p_{j_2}^{s_{j_2}}p_{j_3}^{s_{j_3}}...p_{j_k}^{s_{j_k}}$ de z com expoentes positivos, $z = dz_1$. Sendo que este divisor terá 2^{m-1} triângulos retângulos com catetos primos entre si e sua hipotenusa d. Fazendo a multiplicação z_1 a expressão ficará $z = dz_1 = p_{j_1}^{s_{j_1}}p_{j_2}^{s_{j_2}}p_{j_3}^{s_{j_3}}...p_{j_m}^{s_{j_m}}z_1$, obtemos, portanto 2^{m-1} triângulos retângulos com hipotenusa z. Como estes primos $p_{j_1}p_{j_2}...p_{j_m}$ são $t_{j_1}t_{j_2}...t_{j_m}$ divisores. Variando $j_1j_2....j_m$ com $1 \leq j_1 \leq j_2 \leq .... \leq j_m \leq k$, como observamos que

$$\sum_{1 \leq j_1 < j_2 < ... < j_m \leq k} t_{j_1}t_{j_2}...t_{j_m}$$

divisores possuindo exatamente m primos distintos. Assim, fazendo a variação do m de 1 até k.

□

Agora analisando um caso particular em que $z = p_1p_2p_3...p_kw$ obteremos uma fórmula atraente.

Corolário 3.1 Suponha que $z = p_1p_2p_3...p_kw$ e que as condições do Teorema 3.5 estejam satisfeitas. Então existem

$$\sum_{m=1}^{k} 2^{m-1}\binom{k}{m}$$

triângulos retângulos não semelhantes com hipotenusa z e catetos inteiros.

3.5 Exemplos

Exemplo 3.4. $z = 425 = 5^2 \times 17$

Primeiro passo é verificar os restos de 5 e 17 quando dividimos por 4, que nesse caso será 1. São dois divisores com os primos 5 e 17.

- Para 5 temos $2^{2-1} = 2$ triângulos retângulos.
- Para 17 temos $2^{2-1} = 2$ triângulos retângulos.
- São 2 divisores com primo 5, daí $2^{2-1} = 2$ triângulos retângulos.
- São 1 divisores com primo 17, daí $2^{1-1} = 1$ triângulos retângulos.

Portanto, temos 2+2+2+1 = 7 triângulos retângulos não semelhantes a hipotenusa 425, ou poderia usar o Teorema 3.5 onde $p_1 = 5^2, p_2 = 17$ e $w = 1$, logo

$$(2^{2-1}).(2.1) + (2^{2-2}).(2+1) = 7$$

Como $5 = 2^2 + 1^2 = (2+i)(2-i)$ e $17 = 4^2 + 1^2 = (4+i)(4-i)$, sejam

$\alpha_1 = (2+i)^4(4+i)^2 = (-7+24i)(8i+15) = -297+304i,$

$\alpha_2 = (2+i)^4(4-i)^2 = (-7+24i)(-8i+15) = 87+416i,$

$\alpha_3 = 5(2+i)^2(4+i)^2 = 5(3+4i)(8i+15) = 65+420i,$

$\alpha_4 = 5(2+i)^2(4-i)^2 = 5(3+4i)(-8i+15) = 385+180i,$

$\alpha_5 = 17(2+i)^4 = 17(-7+24i) = -119+408i,$

$\alpha_6 = 25(4+i)^2 = 25(8i+15) = 375+200i,$

$\alpha_7 = 85(2+i)^2 = 85(3+4i) = 225+340i,$

Como $N(\alpha_j) = 425^2$, temos então

$$\begin{aligned} 297^2 + 304^2 &= 425^2 \\ 87^2 + 416^2 &= 425^2 \\ 65^2 + 420^2 &= 425^2 \\ 385^2 + 180^2 &= 425^2 \\ 119^2 + 408^2 &= 425^2 \\ 375^2 + 200^2 &= 425^2 \\ 225^2 + 340^2 &= 425^2 \end{aligned}$$

e encontramos os 7 triângulos retângulos com hipotenusa 425.

Exemplo 3.5. $z = 237133 = 13 \times 17 \times 29 \times 37$

São $2^{4-1} = 8$ triângulos retângulos com catetos x e y primos entre si.

Como $13 = 3^2 + 2^2 = (3+2i)(3-2i)$, $17 = 4^2 + 1^2 = (4+i)(4-i)$, $29 = 5^2 + 2^2 = (5+2i)(5-2i)$ e $37 = 6^2 + 1^2 = (6+i)(6-i)$, sejam

$\alpha_1 = (3+2i)^2(4+i)^2(5+2i)^2(6+i)^2 = (5+12i)(15+8i)(21+20i)(35+12i) = -219835 + 88908i$,

$\alpha_2 = (3+2i)^2(4+i)^2(5+2i)^2(6-i)^2 = (5+12i)(15+8i)(21+20i)(35-12i) = -119035 + 205092i$,

$\alpha_3 = (3+2i)^2(4+i)^2(5-2i)^2(6+i)^2 = (5+12i)(15+8i)(21-20i)(35+12i) = 78085 + 223908i$,

$\alpha_4 = (3+2i)^2(4+i)^2(5-2i)^2(6-i)^2 = (5+12i)(15+8i)(21-20i)(35-12i) = 199045 + 128892i$,

$\alpha_5 = (3+2i)^2(4-i)^2(5+2i)^2(6+i)^2 = (5+12i)(15-8i)(21+20i)(35+12i) = -48635 + 232092i$,

$\alpha_6 = (3+2i)^2(4-i)^2(5+2i)^2(6-i)^2 = (5+12i)(15-8i)(21+20i)(35-12i) = 104005 + 213108i$,

$\alpha_7 = (3+2i)^2(4-i)^2(5-2i)^2(6+i)^2 = (5+12i)(15-8i)(21-20i)(35+12i) = 229445 + 59892i$,

$\alpha_8 = (3+2i)^2(4-i)^2(5-2i)^2(6-i)^2 = (5+12i)(15-8i)(21-20i)(35-12i) = 217925 + 93492i$,

Como $N(\alpha_j) = 237133^2$, assim

$$\begin{aligned}
219835^2 + 88908^2 &= 237133^2 \\
119035^2 + 205092^2 &= 237133^2 \\
78085^2 + 223908^2 &= 237133^2 \\
199045^2 + 128892^2 &= 237133^2 \\
48635^2 + 232092^2 &= 237133^2 \\
104005^2 + 213108^2 &= 237133^2 \\
229445^2 + 59892^2 &= 237133^2 \\
217925^2 + 93492^2 &= 237133^2.
\end{aligned}$$

REFERÊNCIAS BIBLIOGRÁFICAS

[1] EVES, H. (2002). Introdução à História da Matemática. Unicamp, 3 edição.

[2] ANDRADE, José Fernandes Silva. Tópicos especiais em álgebra. Rio de Janeiro: SBM, 2013.

[3] SHOKRANIAN, Salahoddin. Teoria dos Números. 2. ed. Brasília: Editora Universidade de Brasílias, 1999.

[4] HEFEZ, Abramo. Aritmética. Rio de Janeiro: SBM, 2013

[5] SANTOS, José Plínio de Oliveira. Introdução à teoria dos Números. Rio de Janeiro: IMPA, 2007

[6] JUNIOR, Gustavo Oliveira Lima. Números Inteiros, Congruências e Somas de Quadrados. Monografia (Pós-Graduação em Matemática) – UFC. Fortaleza-CE, 2013.

[7] GONÇALEVS, Adilson. Introdução à álgebra. 5. ed. Rio de Janeiro: IMPA, 2007.

[8] GARCIA, Arnaldo. Elementos de Álgebra. 3. ed. Rio de Janeiro: IMPA, 2005.

[9] ALVES, Lislene Heloisa; BALDON, Natália Silvério; PEREIRA, Bruno Alves; PINTO, Ana Carolina Neves; OLIVEIRA, Luiz Fernando Campos de; SILVA, Viviane Reis. Inteiros que são soma de dois quadrados. UNICAMP. Campinas, 2011.

[10] SANTOS, João Evangelista Cabral dos. Números Inteiros como Soma dos Quadrados. Dissertação (Dissertação em matemática) – UFPB. João Pessoa-PB, 2013.

[11] LANG, Serge. Undergraduate algebra. 3. ed. Library of Congress Cataloging in Publication – 1927. New Haven, USA.

[12] HØYRUP, Jens.Lengths, Widths, Surfaces: A Portrait of Old Babylonian Algebra and Its Kin. New York, Berlin, Heidelberg: Springer, 2002.

[13] GROSSWALD, Emil. Representations of integers as sums of squares. Temple University. College of Liberal Arts.Springer-Verlag, New Work 1985.