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

Algumas Propriedades dos Ternos Quase Pitagóricos

Jessé Garcia De Faria

Mestrado Profissional em Matemática: PROFMAT/SBM

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

Trabalho financiado pela Capes

Cuiabá - MT

Abril de 2014

Algumas Propriedades dos Ternos Quase Pitagóricos

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por Jessé Garcia de Faria e aprovada pela comissão julgadora.

Cuiabá, 25 de abril de 2014.

Prof. Dr. Martinho da Costa Araujo
Orientador

Banca examinadora:

Prof. Dr. Martinho da Costa Araujo
Prof. Dr. José de Arimatéia Fernandes
Prof. Dr. Eduardo Rogério Fávaro

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

.

Dados Internacionais de Catalogação na Fonte.

F224a Faria, Jessé Garcia de.
Algumas Propriedades dos Ternos Quase Pitagóricos / Jessé Garcia de Faria. -- 2014
52 f. ; 30 cm.

Orientador: Martinho da Costa Araujo.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2014.
Inclui bibliografia.

1. Terno Quase Pitagórico. 2. Números Complexos. 3. Grupo. 4. Divisão Euclidiana. 5. Números Primos. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Dissertação de Mestrado defendida em 11 de abril de 2014 e aprovada pela banca examinadora composta pelos Professores Doutores

Prof. Dr. Martinho da Costa Araujo

Prof. Dr. José de Arimatéia Fernandes

Prof. Dr. Eduardo Rogério Fávaro

A DEUS e a meus pais.

Agradecimentos

A **DEUS**, que sempre está comigo.

À **Minha familia**, em especial meus pais, a quem procuro me espelhar.

Aos **Meus colegas da turma**, que inspiram, motivação e dedicação.

Aos **Professores do Profmat**

Aos **Meu Orientador** Prof. Dr. Martinho da Costa Araujo.

Voltei-me e vi debaixo do sol que
não é dos ligeiros a carreira,
nem dos valentes a peleja,
nem tão pouco dos sábios o pão,
nem ainda dos prudentes a riqueza
nem dos entendidos o favor,
mas que o tempo e a sorte pertence a
todos.

(Eclesiastes 9:11).

Resumo

O presente trabalho consiste no estudo do conjunto $\mathbb{T}_m$, formado por ternos (x, y, z), onde x, y e z são números inteiros que satisfazem a equação $x^2 + my^2 = z^2$ (m é um número inteiro positivo livre de quadrados), tais ternos são chamados ternos quase pitagóricos. Com a finalidade de identificar algumas propriedades entre ternos, ultilizamos o conjunto quociente de $\mathbb{T}_m$ obtido pela relação de equivalência $\sim$. Denotamos tal conjunto quociente por $\mathbb{T}_{[m]}$, onde cada classe deste conjunto é gerado por um terno (a, b, c) que satisfaz a equação acima e $mdc(a, b) = 1$, tais ternos são chamados ternos quase pitagóricos primitivos. Na parte principal deste trabalho está definida uma operação no conjunto $\mathbb{T}_{[m]}$ e com essa operação está demonstrado que $\mathbb{T}_{[m]}$ é um grupo. Tal demonstração foi desenvolvida ultilizando uma elegante relação entre um terno quase pitagórico (x, y, z) e um número complexo $w = \frac{x}{z} + i\frac{y\sqrt{m}}{z}$, cuja representação gráfica coincide com um ponto da circunferencia unitária com centro na origem do plano complexo. Para obter esta relação foi lançado mão de duas ferramentas essenciais, a função norma e uma certa função injetora ϕ.

Palavras chave: Divisão Euclidiana, Grupo, Máximo Divisor Comum, Número Complexo, Número Primo, Terno quase pitagórico.

Abstract

This present work consists in the study of $\mathbb{T}_m$ set. Comprising triplet (x, y, z) which x, y and z are integers which satisfy the equation $x^2 + my^2 = z^2$ (m is a positive integer devoid of squares) these triplets are called almost Pythagoreans. In order to identify some prospeteis among the triplet use we the $\mathbb{T}_m$ quociente set obtained by the equivalence relation $\sim$. We denote such quociente set $\mathbb{T}_{[m]}$, where which class of this set is generate by a triplet (a, b, c) which satisfies the above equation and $mdc(a, b) = 1$, such triplet are called almost primitive Pythagoreans. At the principal part of this work is defined an operation in the $\mathbb{T}_{[m]}$ set and with this operations is demonstrated that $\mathbb{T}_{[m]}$ is a group. This demonstrations was developed using and elegant relations between a triplet almost Pythagorean (x, y, z) and a complex number $w = \frac{x}{z} + i\frac{y\sqrt{m}}{z}$, whose graphical representation coincides with a point unit circle centered at the origin of the complex plane. To obtain this relation was used two essential tools, norma function and a certain function injection ϕ.

Keywords: Euclidian division, group, greatest common divisor, complex number, prime number, triplet almost Pythagorean.

Sumário

Lista de Figuras

Introdução

> "A melhor maneira que o homem dispõe para se aperfeiçoar, é aproximar-se de Deus."
>
> (Pitágoras)

Estudar o conjunto solução de uma equação matemática, por mais simples que seja, nos permite extrair características essenciais da equação e assim podermos analisar e concluir sobre determinados problemas que tal equação modela.

O desafio deste trabalho é estudar o conjunto solução da equação $x^2 + my^2 = z^2$ com $x, y, z, m \in \mathbb{Z}$ e m livre de quadrados, descobrir se existe solução e caso exista, encontrar propriedades do conjunto solução desta equação. Note que esta equação se assemelha a equação de pitágoras associada a triângulos retângulos, o que difere é apenas o coeficiente inteiro m livre de quadrados. Dessa maneira, ao falarmos da equação $x^2 + my^2 = z^2$, estramos tratando de uma familia de equações:

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

$$x^2 + 3y^2 = z^2$$

$$x^2 + 5y^2 = z^2$$

$$x^2 + 6y^2 = z^2$$

$$x^2 + 7y^2 = z^2$$

$$\dots$$

E embora tenhamos denominado por **terno quase pitagórico** um terno (a, b, c), com a, b e c inteiro, satisfazendo uma equação do tipo $x^2 + my^2 = z^2$, não encontramos evidências de que Pitágoras tenha estudado esse tipo de equação, a justificativa para

essa denominação é o fato de tal equação se assemelhar com a equação do Teorema de Pitágoras. Além disso, em nossas pesquisas, não encontramos referências bibliograficas sobre o assunto principal deste texto, grande parte do teor deste trabalho segue de maneira específica o que foi feito no artigo (1), o que justifica a terminologia e a notação original que adotamos neste texto. Outro fato que vale destacar é que algumas das propriedades que identificamos no segundo capítulo foram enunciadas e provadas sem evidências de ja terem sido estudadas anteriormente.

Este pequeno trabalho é composto por dois capítulos, o primeiro está reservado a abordagem de conceitos matemáticos básicos e fundamentais para o desenvolvimento do segundo capítulo. Trataremos neste capítulo o conceito de grupo e subgrupo, explorando alguns exemplos importantes para este texto, faremos também um estudo sobre aritmética dos inteiros, onde o foco principal é o teorema do algorítmo euclidiano, definição e propriedades do máximo divisor comum e o Teorema Fundamental da Aritmética. Este capítulo traz uma abordagem objetiva, o que implica ao leitor uma prévia noção dos conceitos nele apresentado.

No segundo, e último capítulo, apresentaremos de fato os resultados em que estamos interessados, definiremos o cojunto $\mathbb{T}_m$ dos ternos quase pitagóricos que estudaremos, apresentaremos diversas propriedades deste conjunto, bem como exemplos importantes para a identificação deste conjunto. Na segunda etapa definiremos uma relação sobre este conjunto e provaremos que esta relação é de equivalência, sendo possível então particionar o conjunto dos ternos quase pitagóricos em classes ($[(a,b,c)]$) e definiremos uma operação sobre este conjunto de classes ($\mathbb{T}_{[m]}$), que denotaremos $\star$. Com esta operação provaremos que o conjunto dos ternos quase pitagóricos é um grupo abeliano, faremos isto utilizando a função norma de um número complexo para estabelecermos uma elegante associação, de uma solução da equação $x^2 + my^2 = z^2$ com um número complexo $w = \dfrac{x}{z} + i\dfrac{y\sqrt{m}}{z}$(a esta altura já teremos analisado que $z \neq 0$). Demonstraremos então o seguinte resultado:

Teorema 0.0.1 *Seja S_1 o conjunto dos números complexos que formam a circunferência unitária no plano complexo.*

*A função $\phi : \mathbb{T}_{[m]} \longrightarrow S_1$, definida por $\phi[(x,y,z)] = e^{i\theta} = \dfrac{x}{z} + i\dfrac{y\sqrt{m}}{z}$ é **injetora**. Além disso:*

$$\phi\big([(x,y,z)] \star [(a,b,c)]\big) = \phi[(x,y,z)] \cdot \phi[(a,b,c)], \quad \forall [(x,y,z)], [(a,b,c)] \in \mathbb{T}_{[m]}. \tag{1}$$

Este resultado nos garante que esta associação é eficiente, pois mostra que a operação $\star$ que definiremos em $\mathbb{T}_{[m]}$ é compatível com a multiplicação de números complexos.

Logo após esse resultado, passaremos ao trabalho de demonstrar que o conjunto das classes de ternos quase pitagóricos munido da operação $\star$ é um grupo abeliano, encerrando este estudo.

Capítulo 1

Noções de Álgebra e Aritmética

Neste capítulo apresentaremos um breve apanhado dos conceitos de Álgebra (mais precisamente de teoria de grupos) e de Aritmética dos inteiros, que serão necessários para o desenvolvimento do terceiro capítulo deste trabalho. De início informamos ao leitor que, durante o texto, as demonstrações de alguns resultados foram omitidas, com o objetivo de não cansar o leitor.

1.1 Um Pouco de Teoria de Grupos

Definição 1.1.1 *Seja $\mathcal{G} \neq \emptyset$ um conjunto munido de uma operação:*

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

*A dupla $(\mathcal{G}, *)$ será chamada de **Grupo** quando essa operação satisfizer as condições seguintes:*

[$*1$] **Associatividade**; isto é: $a * (b * c) = (a * b) * c, \ \forall \ a, \ b, \ c \in \mathcal{G}$.

[$*2$] Existe um **Elemento Neutro** $e_{\mathcal{G}}$ para $*$. Ou seja, existe $e_{\mathcal{G}} \in \mathcal{G}$, tal que

$$a * 0_{\mathcal{G}} = e_{\mathcal{G}} * a = a, \ \forall \ a \in \mathcal{G}.$$

[$*3$] Todo elemento de $\mathcal{G}$ possui **simétrico**; isto é, dado $a \in \mathcal{G}$, existe $a' \in \mathcal{G}$ tal que

$$a * a' = a' * a = 0_{\mathcal{G}}.$$

Observação 1.1.1 *De agora em diante, quando não restarem dúvidas quanto à operação considerada, cometeremos um pequeno abuso de notação, e escreveremos "grupo $\mathcal{G}$" ao invés de "grupo $(\mathcal{G}, *)$".*

Definição 1.1.2 *Um Grupo $\mathcal{G}$ será chamado* ***Grupo Comutativo*** *ou* ***Grupo Abeliano*** *quando cumprir a seguinte propriedade:*

[$*4$] A operação $*$ é **Comutativa**; isto é: $a * b = b * a, \ \forall \ a, \ b \in \mathcal{G}$.

Vamos agora aos exemplos:

Exemplo 1.1.1 *Entre os grupos mais importantes, estão os grupos numéricos aditivos. Eis alguns deles: (i) O grupo $(\mathbb{Z}, +)$ dos números inteiros; (ii) o grupo $(\mathbb{Q}, +)$ dos números racionais; (iii) o grupo $(\mathbb{R}, +)$ dos números reais. Em cada um desses gupos, consideremos a operação de adição usual nesses conjuntos. Todos esses grupos também são grupos abelianos.*

Exemplo 1.1.2 *Agora usando a operação de multiplicação usual nos conjuntos numéricos, temos como exemplo de grupo multiplicativo: (i) o grupo abeliano $(\mathbb{Q}-\{0\}, \cdot)$ dos números racionais; (ii) o grupo abeliano $(\mathbb{R} - \{0\}, \cdot)$ dos números reais. Observe que o conjunto $\mathbb{Z} - \{0\}$ munido da operação de multiplicação não é um grupo, pois esta operação não satisfaz a condição [$\star 3$] da definição(1.1.1).*

Daremos um enfoque agora no conjunto $\mathbb{C} = \{a + bi; \ a, b \in \mathbb{R}\}$ dos números complexos.

Exemplo 1.1.3 *Definindo sobre $\mathbb{C}$ a seguinte operação de adição:*

$$\begin{aligned} + \quad : \quad \mathbb{C} \times \mathbb{C} \quad &\longrightarrow \quad \mathbb{C} \\ (a + bi, c + di) &\longmapsto (a + bi) + (c + di) := (a + c) + (b + d)i \end{aligned}$$

Podemos provar, sem muito trabalho, que $(\mathbb{C}, +)$ é um grupo abeliano.

Exemplo 1.1.4 *Definindo sobre $\mathbb{C} - \{0\}$ a seguinte operação de multiplicação:*

$$\begin{aligned} \cdot \quad : \quad \mathbb{C} \times \mathbb{C} \quad &\longrightarrow \quad \mathbb{C} \\ (a + bi, c + di) &\longmapsto (a + bi)(c + di) := (ac - bd) + (ad + bc)i \end{aligned}$$

Temos, $(\mathbb{C} - \{0\}, \cdot)$ é um grupo abeliano.

De fato sejam $\alpha = a+bi,\ \beta = c+di,\ \gamma = e+fi \in \mathbb{C}-\{0\}$; isto é, $a, b, c, d, e, f, \in \mathbb{R}$. Utilizaremos repetidas vezes o conhecido fato de que $(\mathbb{R} - \{0\}, \cdot)$ é um grupo.

[$*1$] A multiplicação é **Associativa**; isto é: $\alpha(\beta\gamma) = (\alpha\beta)\gamma,\ \forall\ \alpha,\ \beta,\ \gamma \in \mathbb{C}$. De fato, temos, por um lado:

$$\begin{aligned} \alpha(\beta\gamma) &= (a+bi)[(c+di)(e+fi)] = (a+bi)[(ce-df)+(cf+de)i] \\ &= [a(ce-df)-b(cf+de)]+[a(cf+de)+b(ce-df)]i \\ &= [ace-adf-bcf-bde]+[acf+ade+bce-bdf]i \end{aligned} \tag{1.1}$$

Enquanto que, por outro lado:

$$\begin{aligned} (\alpha\beta)\gamma &= [(a+bi)(c+di)](e+fi) = [(ac-bd)+(ad+bc)i](e+fi) \\ &= [(ac-bd)e-(ad+bc)f]+[(ad+bc)e+(ac-bd)f]i \\ &= [ace-adf-bcf-bde]+[acf+ade+bce-bdf]i \end{aligned} \tag{1.2}$$

Por (1.1) e (1.2) e pela propriedade transitiva das igualdades fica estabelecida a veracidade de [$*1$].

[$*4$] A multiplicação é **Comutativa**; isto é: $\alpha\beta = \beta\alpha,\ \forall\ \alpha,\ \beta \in \mathbb{C}$.

Com efeito:

$$\begin{aligned} \alpha\beta &= (a+bi)(c+di) = (ac-bd)+(ad+bc)i \\ &= (ca-db)+(cb+da)i = (c+di)(a+bi) \\ &= \beta\alpha. \end{aligned}$$

[$*2$] Existe um **elemento neutro** para multiplicação; isto é, existe $1 = 1+0i \in \mathbb{C}$ tal que $\alpha \cdot 1 = 1 \cdot \alpha = \alpha,\ \forall\ \alpha \in \mathbb{C}$.

De fato:

$$\begin{aligned} \alpha \cdot 1 &= (a+bi)(1+0i) \\ &= (a\cdot 1 - b\cdot 0)+(a\cdot 0+b\cdot 1)i = (a-0)+(b+0)i \\ &= a+bi = \alpha. \end{aligned}$$

Por [$*4$], temos também $1 \cdot \alpha = \alpha$.

[∗3] Todo elemento de $\mathcal{C} - \{0\}$ possui **simétrico**; isto é, dado $\alpha \in \mathcal{C} - \{0\}$, existe $\alpha' \in \mathcal{C} - \{0\}$ tal que $\alpha * \alpha' = \alpha' * \alpha = 1$.

De fato, tomando $\alpha' = \dfrac{a - bi}{a^2 + b^2} = \dfrac{a}{a^2 + b^2} - \dfrac{b}{a^2 + b^2} i$ temos:

$$\begin{aligned}
\alpha \cdot \alpha' &= (a + bi)\left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i\right) \\
&= (a \cdot \frac{a}{a^2 + b^2} + b \cdot \frac{b}{a^2 + b^2}) + \left(-a \cdot \frac{b}{a^2 + b^2} + b \cdot \frac{a}{a^2 + b^2}\right) i \\
&= \cdot \frac{a^2 + b^2}{a^2 + b^2} + \left(- \cdot \frac{ab}{a^2 + b^2} + \cdot \frac{ab}{a^2 + b^2}\right) i \\
&= 1 + 0i = 1.
\end{aligned}$$

1.1.1 Propriedades Imediatas de um Grupo

A condição [∗2] impõe a **existência** de um *elemento neutro* para a a operação $*$, a fim de que $(\mathcal{G}, *)$ seja um grupo. A seguir, demonstraremos que, em um grupo $(\mathcal{G}, *)$, este *elemento neutro* é **único**. A **unicidade** de um elemento é de grande relevância em Matemática, uma vez que nos dá a certeza de que, ao adotarmos um símbolo para esse elemento, não estaremos introduzindo uma notação inconsistente. Nas proposições seguintes, estabeleceremos alguns resultados de unicidade.

Proposição 1.1.1 *Em um grupo $\mathcal{G}$, o elemento neutro é único.*

Demonstração: De fato, se e e e' são dois elementos neutros para a operação $*$ em um grupo $\mathcal{G}$, então $e = e + e' = e'$. Aqui, a primeira igualdade se deve à hipótese de que e' é um elemento neutro para a operação $*$ em $\mathcal{G}$; e a segunda ao fato de que e é também um elemento neutro. ■

Proposição 1.1.2 *O simétrico de um elemento $a \in \mathcal{G}$ é único.*

Demonstração: De fato, se b e b' são simétricos de a, então

$$b = b * e = b * (a * b') = (b * a) * b' = e * b' = b'.$$

■

A unicidade demonstrada acima permite denotarmos o (único) elemento *simétrico* a' de a num grupo aditivo por $-a$ e num grupo multiplicativo por a^{-1}.

No exemplo (1.1.1), todos os grupos citados possui como elemento neutro o número 0 (zero), já no exemplo (1.1.2), todos os grupos citados possui como elemento neutro o número 1 (um).

1.1.2 Subgrupos

Definição 1.1.3 *Seja $(\mathcal{G}, *)$ um grupo. Dizemos que um subconjunto não-vazio $\mathcal{H} \subset \mathcal{G}$ é um subgrupo de $\mathcal{G}$ quando:*

(i) $\mathcal{H}$ é fechado para a operação $*$. Isto é, se $a, b \in \mathcal{H}$ então $a * b \in \mathcal{H}$;

(ii) $(\mathcal{H}, *)$ também é um grupo (aqui $*$ significa a restrição da operação de $\mathcal{G}$ aos elementos de $\mathcal{H}$).

Provaremos agora uma proposição que fornece um condição necessária e suficiente para que um subconjunto $\mathcal{H} \neq \emptyset$ de um grupo $\mathcal{G}$ seja um subgrupo de $\mathcal{G}$ (aqui e para o que segue estamos admitindo $*$ como operação).

Proposição 1.1.3 *Seja $\mathcal{H}$ um subconjunto não-vazio do grupo $\mathcal{G}$. Então as seguines afirmações são equivalentes:*

(i) $\mathcal{H}$ é um subgrupo de $(\mathcal{G}, *)$.

(ii) $[H_1]$ $e \in \mathcal{H}$ *(e é o elemento neutro de $\mathcal{G}$);*

$[H_2]$ $a * b \in \mathcal{H},\ \forall a, b \in \mathcal{H}$;

$[H_3]$ $a' \in \mathcal{H},\ \forall a \in \mathcal{H}$.

(iii) $\mathcal{H} \neq \emptyset$ e $a * b' \in \mathcal{H},\ \forall a, b \in \mathcal{H}$.

Demonstração: $[(i) \Rightarrow (ii)]$ Segue imediatamente da definição 1.1.1, da unicidade do elemento neutro e unicidade do simétrico.

$[(ii) \Rightarrow (iii)]$ De $[H_1]$ segue que $\mathcal{H} \neq \emptyset$. Agora se $a, b \in \mathcal{H}$ então por $[H_3]$ temos que $b' \in \mathcal{H}$, o que implica por $[H_2]$ que $a * b' \in \mathcal{H}$.

$[(iii) \Rightarrow (i)]$ Devemos provar que $(\mathcal{H}, *)$ é um grupo, isto é temos que provar $[*1]$, $[*2]$ e $[*3]$ da definição 1.1.1.

De fato, note que $[*1]$ é evidente pois $*$ já é associativa para todos elementos de $\mathcal{G}$, em particular para os elementos de $\mathcal{H}$. Tomando agora $x_0 \in \mathcal{H}$ temos que $e = x_0 * x_0' \in \mathcal{H}$, provando $[*2]$. Por fim $x_0' = e * x_0' \in \mathcal{H}$. Concluindo assim que $(\mathcal{H}, *)$ é um grupo.

■

Exemplo 1.1.5 *Se $\mathcal{G}$ é um grupo, então $\{e\}$ e $\mathcal{G}$ são subgrupos de $\mathcal{G}$, chamados* ***subgrupos triviais*** *de $\mathcal{G}$.*

Exemplo 1.1.6 *$(2\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$, onde $2\mathbb{Z}$ é conjunto dos inteiros múltiplos de 2. De maneira mais geral, se n é um número inteiro qualquer então, $(n\mathbb{Z}, +)$ é um subgrupo de $(\mathbb{Z}, +)$.*

Exemplo 1.1.7 *Seja $S_1 = \{\cos\theta + i\sin\theta;\ 0 \leq \theta < 2\pi\}$ o subconjunto de $\mathbb{C}$ que representa os pontos da circunferência unitária (raio igual a 1) com centro na origem do plano complexo (plano XOY). Afirmamos que $(S_1, \cdot)$ é um subgrupo de $(\mathbb{C} - \{0\}, \cdot)$ abordado no exemplo (1.1.4).*

De fato, S_1 não é vazio, pois $1 = \cos 2\pi + i\sin 2\pi$, e se $w_1 = \cos\alpha + i\sin\alpha$ e $w_2 = \cos\beta + i\sin\beta$ são elementos de S_1 então $w_2' = \cos\beta - i\sin\beta$.

Logo $w_1 \cdot w_2 \in S_1$, pois:

$$\begin{aligned} w_1 \cdot w_2' &= (\cos\alpha + i\sin\alpha)\cdot(\cos\beta - i\sin\beta) \\ &= (\cos\alpha\cos\beta - \sin\alpha\sin\beta) + i(\sin\alpha\cos\beta - \cos\alpha\sin\beta) \\ &= \cos(\alpha - \beta) + i\sin(\alpha - \beta) \end{aligned}$$

O que implica, pela proposição acima, que $(S_1, \cdot)$ é um subgrupo de $(\mathbb{C} - \{0\}, \cdot)$.

1.2 Um Pouco de Aritmética dos Inteiros

Nesta seção faremos um breve apanhado dos conceitos de Aritmética dos Inteiros que serão úteis para este trabalho, portanto muitas definições e resultados interessantes ficarão de fora deste texto, por fugir do objetivo do trabalho. Imaginamos que o leitor ja tenha uma noção dos conceitos básicos pré-requisitados, caso não tenha, recomendamos a leitura de (8),(13) ou (14).

Começaremos nossa abordagem pelo conjunto dos inteiros positivos (conjunto $\mathbb{N} = \{1, 2, 3, ...\}$ dos números naturais), apresentando uma indispensável ferramenta na demonstração de muitos teoremas: O Princípio da Indução Finita.

1.2.1 Princípio da Indução

Embora esses próximos conceitos possam ser extendidos, com algumas hipóteses adicionais, a todo o conjunto dos números inteiros, será suficiente para este texto apresentarmos como segue.

Axioma 1.2.1 (Princípio da Indução) *Seja $\mathcal{A}$, um subconjunto não-vazio de $\mathbb{N}$. Se:*

(i) $1 \in \mathcal{A}$*;*

(ii) $n + 1 \in \mathcal{A}$ *sempre que* $n \in \mathcal{A}$*.*

Então $\mathcal{A} = \mathbb{N}$*.*

Usaremos este Axioma para demonstrar a seguinte afirmação.

Teorema 1.2.1 (Princípio da Boa Ordenação) *Todo subconjunto de $\mathbb{N}$, não-vazio possui um menor elemento.*

Demonstração: Sejam $I_n = \{p \in \mathbb{N};\ 1 \leq p \leq n\}$ e $\mathcal{X} \subset \mathbb{N}$, um conjunto formado pelos elementos $n \in \mathbb{N}$ tais que $I_n \subset \mathbb{N} - \mathcal{A}$.

Se $1 \in \mathcal{A}$, então claramente 1 é o menor elemento de $\mathcal{A}$.

Agora se $1 \notin \mathcal{A}$, então $1 \in \mathcal{X}$, tendo em vista que $I_1 = \{1\} \subset \mathbb{N} - \mathcal{A}$. Porém $\mathcal{X} \neq \mathbb{N}$, pois $\mathcal{A} \neq \emptyset$ e $\mathcal{X} \subset \mathbb{N}$.

Logo o princípio da indução não pode ser aplicado a $\mathcal{X}$, o que implica que o item (ii) do axioma 1.2.1 não vale em $\mathcal{X}$, isto é: existe um $n_0 \in \mathcal{X}$ tal que $n_0 + 1 \notin \mathcal{X}$.

Assim como $I_n \subset \mathbb{N} - \mathcal{A}$, temos que todos os números inteiros de 1 a n_0 pertencem a $\mathcal{X}$ e como $n_0 + 1 \notin \mathcal{X}$, temos que $n_0 + 1 \in \mathcal{A}$ e $I_n = \mathcal{X}$.

Portanto $a = n_0 + 1$ é o menor elemento de $\mathcal{A}$. ■

Na realidade o Princípio da Indução e o Princípio da Boa Ordenação (PBO) são afirmações equivalentes, e nesse sentido poderíamos ter assumido o PBO como axioma e o utilizado para demonstrar o Princípio da Indução. Enunciaremos abaixo uma segunda versão do Axioma da Indução que equivale também as duas anteriores (a verificação disto fica a cargo do leitor).

Teorema 1.2.2 (Princípio da Indução Forte) *Seja $\mathcal{A}$, um subconjunto não-vazio de $\mathbb{N}$. Se:*

(i) $1 \in \mathcal{A}$*;*

(ii) $n+1 \in \mathcal{A}$ *sempre que* $1, 2, 3, ..., n \in \mathcal{A}$.

Então $\mathcal{A} = \mathbb{N}$.

Estes resultados acima (versões do princípio da indução) nos fornecem métodos para demonstrar e até enunciar algumas definições em matemática. Veja o exemplo abaixo.

Exemplo 1.2.1 *Vamos verificar que* $s_n = 1 + 2 + 3 + 4 + ... + n = \dfrac{n(n+1)}{2}$ *vale para todo número inteiro positivo.*

Lançando mão do princípio da indução, provaremos inicialmente o item (i) (isto é, se $n = 1$ *então* $s_1 = \dfrac{1 \cdot 2}{2}$*).*

De fato $s_1 = 1 = \dfrac{1 \cdot 2}{2}$.

Agora para provar (ii), supomos que $s_k = 1 + 2 + 3 + 4 + ... + k = \dfrac{k(k+1)}{2}$, *para um certo* $k \in \mathbb{Z}^+$ *e vamos mostrar que a expressão vale também para* $k+1$ *(isto é,* $s_{k+1} = 1 + 2 + 3 + 4 + ... + k + (k+1) = \dfrac{(k+1)[(k+1)+1]}{2}$.

De fato:

$$\begin{aligned} s_{k+1} = 1 + 2 + 3 + 4 + ... + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{k^2 + k + 2k + 2}{2} \\ &= \frac{k(k+1) + 2(k+1)}{2} \\ &= \frac{(k+1)(k+2)}{2} = \frac{(k+1)[(k+1)+1]}{2}. \end{aligned}$$

Conluímos por indução que $s_n = 1 + 2 + 3 + 4 + ... + n = \dfrac{n(n+1)}{2}$, $\forall n \in \mathbb{Z}^+$.

Os conceitos abordados nesta seção, são conceitos inerentes a caracterização do conjunto dos números naturais formulada por Giuseppe Peano em 1889, onde figura o Axioma da Indução.

1.2.2 Algorítmo da Divisão Euclidiana

A partir de agora abordaremos, de fato, conceitos referentes a propriedades dos números inteiros iniciando o estudo da divisibilidade de números inteiros tendo como principal resultado o Algorítmo da Divisão Euclidiana. Admitimos que $(\mathbb{Z}, +)$ é um grupo e que a multiplicação em $\mathbb{Z}$ só não satisfaz a condição $[*3]$ da definição de grupo.

Definição 1.2.1 *Sejam $a, b \in \mathbb{Z}$. Dizemos que b é **divisor** (ou **fator**) de a quando existe $c \in \mathbb{Z}$, tal que $a = bc$. Dizemos também que "b divide a", ou "a é múltiplo de b", ou ainda, "a é divisível por b". Denotamos por $b \mid a$. Quando b não é um divisor de a, denotamos $b \nmid a$.*

Exemplo 1.2.2 *O inteiro 2 é um fator de 6 em $\mathbb{Z}$. Basta notar que $2 \cdot 3 = 6$ e $3 \in \mathbb{Z}$.*

Proposição 1.2.1 *Sejam $a, b, c, d, n_1, n_2, ..., n_s$ números inteiros. As seguintes afirmações são verdadeiras:*

(i) $a \mid 0$ e $a \mid a$;

(ii) Se $a \mid b$ e $b \mid c$, então $a \mid c$;

(iii) Se $a \mid b$ e $c \mid d$, então $ac \mid bd$. Em particular, se $a \mid b$, então $ca \mid cb$;

(iv) Se $a \mid (b + c)$ e $a \mid b$, então $a \mid c$;

(v) Se $a \mid n_1$, $a \mid n_2, ...,$ $a \mid n_s$, então $a \mid (c_1 n_1 + c_2 n_2 + ... + c_s n_s)$ para todos inteiros $c_1, c_2, ..., c_s$;

(vi) Se $a \mid b$ e $b \mid a$, então $a = \pm b$.

Demonstração: Veja (8),(13) ou (14). ■

Para enunciar o resultado principal desta seção e para sua demonstração necessitamos definir a função **Valor Absoluto** e demonstrar uma proposição chamada **Propriedade Arquimediana de** $\mathbb{Z}$.

Definição 1.2.2 (Função Valor Absoluto) *A função $|\cdot|$ definida por:*

$$|\cdot| \ : \ \mathbb{Z} \longrightarrow \mathbb{Z}^+ \cup \{0\}$$
$$a \longmapsto |a| = \begin{cases} a, & a \geq 0 \\ -a, & a < 0 \end{cases}.$$

*é chamada **Valor Absoluto** em $\mathbb{Z}$.*

Proposição 1.2.2 *Sejam a, b, r números inteiros. Então:*

(i) $|ab| = |a| \cdot |b|$;

(ii) $-|a| \leq a \leq |a|$;

(iii) $|a| \leq r \quad \Leftrightarrow \quad -r \leq a \leq r$;

(iv) $|a + b| \leq |a| + |b|$;

(v) $0 \leq |a| \ \ \forall\ a \in \mathbb{Z}$;

(vi) $|a| = b \geq 0 \ \Rightarrow\ a = \pm b$.

Demonstração: Veja (8) ou (13). ■

Proposição 1.2.3 (Propriedade Arquimediana de $\mathbb{Z}$) *Dados dois números inteiros a e b, com $b \neq 0$, existe um inteiro n tal que $nb \geq a$.*

Demonstração: Como $b \neq 0$, temos que $|ab| \geq |a| \geq a$ (verifique!). Daí, quando $b > 0$, basta tomar $n = |a|$; daí, $nb = |a| \cdot b = |a||b| = |ab| \geq |a| \geq a$. Por outro lado, se $b < 0$, basta tomar $n = -|a|$, o que acarreta $nb = (-|a|) \cdot b = |a|(-b) = |a||b| = = |ab| \geq |a| \geq a$. ■

Agora vamos ao teorema que estabelece um método de divisão para números inteiros.

Teorema 1.2.3 (Algoritmo de Euclides para $\mathbb{Z}$) *Seja $|\cdot| \ : \ \mathbb{Z} \longrightarrow \mathbb{Z}^+$ a função valor absoluto. Dados $a, b \in \mathbb{Z}$, com $b \neq 0$, existem $t, r \in \mathbb{Z}$ tais que $a = bt + r$, onde $0 \leq r < |b|$. Além disso, t e r são univocamente determinados por essas duas condições. Os inteiros t e r acima são chamados (respectivamente) **quociente** e **resto** da divisão euclidiana de a por b.*

Demonstração: Para a demonstração, sejam $a, b \in \mathbb{Z}$, com $b \neq 0$ e consideremos o conjunto $\mathcal{S} = \{x \in \mathbb{Z}^+;\ x = a - bn,\ n \in \mathbb{Z}\}$.

É claro que $\mathcal{S}$ é limitado inferiormente. Além disso, afirmamos que $\mathcal{S} \neq \emptyset$. Com efeito, existe, em decorrência da Propriedade Arquimediana, um inteiro n_0 tal que $n_0(-b) \geq -a$. Desse modo, obtemos $x_0 = a - bn_0 \geq 0$, com $n_0 \in \mathbb{Z}$, o que significa que $x_0 = a - bn_0 \in \mathcal{S}$.

Assim, $\mathcal{S}$ está nas hipóteses do Princípio da Boa Ordenação, implicando assim a existência de $r := \min \mathcal{S}$. Como $r \in \mathcal{S}$, temos que $r = a - bt \geq 0$, para algum $t \in \mathbb{Z}$. Resta provar que $r < |b|$.

Suponhamos que ocorresse $r \geq |b|$; isto é, $r = |b| + s$, para algum $s \in \mathbb{Z}$, tal que $0 \leq s < r$. Teríamos, então, $a = bt + r = bt + |b| + s = b(t \pm 1) + s$, e, conseqüentemente, $s = a - b(t \pm 1) \in \mathcal{S}$, pois $(t \pm 1 \in \mathbb{Z})$, e $s \geq 0$. Assim, s seria um elemento de $\mathcal{S}$ menor do que $r := \min \mathcal{S}$. Contradição.

Para demonstrar a unicidade de t e r, suponhamos que:

$$a = bt_1 + r_1 = bt_2 + r_2, \tag{1.3}$$

onde $t_1, t_2, r_1, r_2 \in \mathbb{Z}$ e $0 \leq r_1 < |b|$ e $0 \leq r_2 < |b|$.

Multiplicando a primeira desigualdade por (-1), obtemos $-|b| < -r_1 \leq 0$. Daí, somando membro a membro as desigualdades $0 \leq r_2 < |b|$ e $-|b| < -r_1 \leq 0$, encontramos $-|b| < r_2 - r_1 < |b|$, o que equivale a $|r_2 - r_1| < |b|$.

Dessa última desigualdade e de (1.3), obtemos:

$$b(t_1-t_2) = r_2-r_1 \Rightarrow |b||t_1-t_2| = |r_2-r_1| < |b| \Rightarrow |t_1-t_2| < 1 \Rightarrow |t_1-t_2| = 0 \Rightarrow t_1-t_2 = 0.$$

Logo, $t_1 = t_2$, o que implica em $r_2 - r_1 = b(t_1 - t_2) = b \cdot 0 = 0$; isto é, $r_1 = r_2$.

■

Observe que, a função valor absoluto é que garante a unicidade do resto (em consequência disso a unicidade do quociente), pois se exigíssemos apenas $0 \leq r < b$, obteríamos dois possíveis quocientes e dois restos, como por exemplo na divisão de 3 por 2 obteríamos: $3 = 2 \cdot 1 + 1$, onde $r = 1$ e $t = 2$ e $3 = 2 \cdot 2 - 1$ onde $r = -1$ e $t = 2$.

1.2.3 Máximo Divisor Comum

Definição 1.2.3 *Dados dois inteiros a e b, chama-se* ***máximo divisor comum de*** *a* ***e*** *b o inteiro d, que satisfaz as seguintes condições:*

(1) Se $a = b = 0$ então $d = 0$;

(2) Se $a \neq 0$ ou $b \neq 0$ então d é caracterizado pelas propriedades:

(i) $d \mid a$ e $d \mid b$;

(ii) Para cada $x \in \mathbb{Z}$, se $x \mid a$ e $x \mid b$ então $x \mid d$. Neste caso, temos $x \leq d$.

Observação 1.2.1 *Se d é o máximo divisor comum de a e b, denotamos $d = mdc(a, b)$. De maneira mais geral podemos definir $mdc(a_1, a_2, ..., a_n)$ para $a_1, a_2, ..., a_n \in \mathbb{Z}$.*

Exemplo 1.2.3 *Os divisores comuns de 24 e 84 são $\pm1, \pm2, \pm3, \pm4, \pm6$ e ±12. Portanto, $mdc(24, 84) = 12$. Analogamente, olhando os conjuntos de divisores comuns, concluímos que $mdc(35, 45) = 5$, $mdc(17, 25) = 1$, $mdc(0, -8) = 8$ e $mdc(-9, -15) = 3$.*

Definição 1.2.4 *Dois inteiros a e b são ditos* ***primos entre si*** *quando $mdc(a,b) = 1$.*

A proposição seguinte garante a existência do $mdc(a,b)$ em $\mathbb{Z}$, para a e b não simultaneamente nulos. Além disso, fornece uma caracterização extremamente útil para esse $mdc(a,b)$.

Proposição 1.2.4 *Sejam a e b números inteiros, não simultaneamente nulos. Então, existe $d := mdc(a,b)$ em $\mathbb{Z}$. Além disso; $d := mdc(a,b) = \min\{ma + nb > 0;\ m,n \in \mathbb{Z}\}$.*

Demonstração: Consideremos o conjunto $\mathcal{L} = \{ma + nb > 0;\ m,n \in \mathbb{Z}\} \subset \mathbb{Z}$. Inicialmente, note que $\mathcal{L} \neq \emptyset$. De fato, como $a \neq 0$ ou $b \neq 0$, concluímos que o inteiro $|a| + |b| > 0$ pertence a $\mathcal{L}$. Além disso, é fácil ver que $\mathcal{L}$ é limitado inferiormente. Logo, pelo Princípio da Boa Ordenação, existe $d := \min \mathcal{L}$.

Resta mostrar que $d = mdc(a,b)$.

Com efeito, por um lado, como $d \in \mathcal{L}$, podemos escrever $d = m_0a + n_0b > 0$, com $m_0, n_0 \in \mathbb{Z}$. Por outro lado, efetuando a divisão euclidiana de a por d, obtemos $t, r \in \mathbb{Z}$ tais que $a = dt + r$, com $0 \leq r < d$. Daí:

$$r = a - dt = a - (m_0a + n_0b)t = (1 - m_0t)a + (n_0t)b. \tag{1.4}$$

Isso nos permite concluir que $r = 0$. De fato, se fosse $r > 0$, teríamos $r \in \mathcal{L}$, o que não pode ocorrer, uma vez que isso implicaria em $r < d := \min \mathcal{L}$. Em vista de (1.4), e do fato que $r = 0$, podemos concluir que $a = dt$, e, portanto, $d \mid a$.

Um raciocínio análogo (efetuando a divisão euclidiana de b por d) nos permite concluir que $d \mid b$. Logo, $d \mid a$ e $d \mid b$, e a condição (i) da definição de mdc está demonstrada.

Para mostrarmos que a condição (ii) também ocorre, seja $x \in \mathbb{Z}$ tal que $x \mid a$ e $x \mid b$. Então, existem $u, v \in \mathbb{Z}$ tais que $a = ux$ e $b = vx$. Devemos provar que $x \mid d$.

Com efeito, uma vez que $d \in \mathcal{L}$, podemos escrever $d = m_0a + n_0b$, com $m_0, n_0 \in \mathbb{Z}$. Daí:

$$d = m_0a + n_0b = m_0(ux) + n_0(vx) = (m_0u + n_0v)x,$$

o que significa que $x \mid d$, como queríamos. ■

Corolário 1.2.1 *Sejam $a, b \in \mathbb{Z}$ e $d = mdc(a, b)$. Então, existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$. Em particular, se $a, b \in \mathbb{Z}$ são primos entre si, então existem $r, s \in \mathbb{Z}$ tais que $ra + sb = 1$.*

Demonstração: Segue imediatamente do Teorema anterior. ■

Proposição 1.2.5 *Dados inteiros a, b e c, se $a \mid bc$, e a e b são primos entre si, então $a \mid c$.*

Demonstração: Como a e b são primos entre si, pelo corolário (1.2.1) existem certos inteiros r e s, tais que $ra + sb = 1$. Logo, multiplicando a igualdade acima por c obtemos $rac + sbc = c$. Assim, $a \mid rac$ e $a \mid sbc$ (pois $a \mid bc$). Logo $a \mid (rac + sbc)$, e portanto $a \mid c$.
■

Proposição 1.2.6 *Dados inteiros a, b não-nulos. Se $d = mdc(a, b)$ então $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si.*

Demonstração: De fato, se $d = mdc(a, b)$ então, pelo corolário 1.2.1, existem inteiros r e s tais que $d = ra + sb$ e como $d \mid a$ e $d \mid b$ temos que $1 = r \cdot \frac{a}{d} + s \cdot \frac{b}{d}$.

O que implica que $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si. ■

1.2.4 Números Primos

Esta seção que encerra o nosso pequeno passeio pela Aritmética, aborda um dos conceitos mais importantes e enigmáticos de toda a Matemática, os números primos. Esses números atraíram, desde os tempos remotos, a atenção dos maiores matemáticos existentes. Grandes esforços já foram depositados no estudo desses números, pois eles estão envolvidos em muitos problemas famosos, inclusive uma grande parte destes ainda resistem há muitos anos. Nestas linhas voltaremos nossa atenção, única e exlusivamente, ao papel fundamental que os números primos desempenham, ou seja, ao de "decompor todos os números inteiros maiores do que 1 em produto de fatores primos".

Definição 1.2.5 *Um número inteiro $p \neq 0$ é chamado **primo** quando:*

(i) $p \notin \{-1, 1\}$;

(ii) Os únicos divisores de p são ± 1 e $\pm p$.

Note que, pela definição acima podemos afirmar que: p é primo se, e somente se, seus únicos divisores positivos são 1 e $|p|$.

Um número inteiro $n \notin \{-1, 0, 1\}$ que não é primo, é chamado **composto**. Isto significa que n possui um divisor $x \neq 0$ com $x < |n|$.

Provaremos agora uma proposição que é consequência imediata da definição de número primo. Na verdade este resultado que provaremos é equivalente a tal definição, sendo em muitos textos utilizado como definição.

Proposição 1.2.7 *Sejam a, b e p números inteiros com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração: Para esta demonstração suponhamos que p é um número primo tal que $p \mid ab$ e $p \nmid a$, com isso mostraremos que $p \mid b$.

De fato se $p \nmid a$ então $mdc(a, p) = 1$ e pelo corolário (1.2.1) existem inteiros r e s, tais que $ra + sp = 1$.

Multiplicando ambos os membros da igualdade acima por b, temos: $rab + spb = b$.

E como $p \mid ab$, temos que $p \mid (rab + spb)$. Logo $p \mid b$.

■

Por fim enunciaremos e demonstraremos o principal teorema desta seção que permite decompor um número inteiro em um produto de fatores primos, como dito anteriormente.

Corolário 1.2.2 *Sejam p, $a_1, a_2, ..., a_n$ números inteiros com $n \geq 2$ e p primo.*

Se $p \mid (a_1 \cdot a_2 \cdots a_n)$ então $p \mid a_i$ para algum índice $i \in \{1, 2, ..., n\}$.

Demonstração: A demonstração se faz por indução sobre n. O leitor interessado pode consultar (13). ■

Teorema 1.2.4 (Teorema Fundamental da Aritmética) *Todo inteiro $n \neq 0$ pode ser escrito na forma:*

$$n = u \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_k \tag{1.5}$$

onde $u \in \{-1, 1\}$ e $p_1 \leq p_2 \leq p_3 \leq ... \leq p_k$ são primos positivos. Além disso essa expressão é única.

Demonstração: É suficiente provar o caso $u = 1$, isto é, faremos a demonstração para inteiros positivos. Reduzimos assim a expressão (1.5) a $n = p_1 \cdot p_2 \cdot p_3 \cdots p_k$ onde $p_1 \leq p_2 \leq p_3 \leq ... \leq p_k$ são primos positivos.

A demonstração se faz utilizando o segundo princípio da indução sobre n.

Supondo então que todo número inteiro m, com $1 \leq m < n$ pode ser escrito da forma acima como produto de números primos (hipótese de indução). Afirmamos que n também pode.

De fato, se n é primo, nada temos para fazer. Mas se n é composto, então existem inteiros m_1 e m_2, com $1 \leq m_1 < n$ e $1 \leq m_2 < n$, tais que $n = m_1 \cdot m_2$. Logo pela hipótese de indução existem $q_1 \leq q_2 \leq q_3 \leq ... \leq q_r$ e $q'_1 \leq q'_2 \leq q'_3 \leq ... \leq q'_s$ primos positivos tais que:

$$m_1 = q_1 \cdot q_2 \cdot q_3 \cdots q_r \quad e \quad m_2 = q'_1 \cdot q'_2 \cdot q'_3 \cdots q'_s.$$

Portanto:

$$n = n = m_1 \cdot m_2 = (q_1 \cdot q_2 \cdot q_3 \cdots q_r)(q'_1 \cdot q'_2 \cdot q'_3 \cdots q'_s). \tag{1.6}$$

e reorganizando os números primos $q_1 \leq q_2 \leq q_3 \leq ... \leq q_r$ e $q'_1 \leq q'_2 \leq q'_3 \leq ... \leq q'_s$ em (1.6) podemos escrever,

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k,$$

com $p_1 \leq p_2 \leq p_3 \leq ... \leq p_k$ são primos positivos e $k = r + s$, como queríamos.

Para provarmos a unicidade desta decomposição, supomos

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_k = p'_1 \cdot p'_2 \cdot p'_3 \cdots p'_t \tag{1.7}$$

onde $p_1 \leq p_2 \leq p_3 \leq ... \leq p_k$ e $p'_1 \leq p'_2 \leq p'_3 \leq ... \leq p'_t$ são primos positivos.

Novamente pelo segundo princípio da indução sobre k, temos que se $k = 1$ então que $p_1 = p'_1 \cdot p'_2 \cdot p'_3 \cdots p'_t$.

Logo $p'_i \mid p_1$ para $i \in \{1, 2, ..., t\}$ e como p'_i e p_1 são primos temos que $p'_i = p_1$, implicando assim $k = 1 = t$.

Supomos agora que a unicidade acontece sempre que tivermos um produto de r fatores primos, onde $1 \leq r < k$. Vamos provar, a partir disso, que a unicidade vale para um inteiro positivo formado por um produto de k fatores primos.

De fato, se $p_1 \cdot p_2 \cdot p_3 \cdots p_k = p'_1 \cdot p'_2 \cdot p'_3 \cdots p'_t$, com $k \geq 2$ então p_1 divide algum p'_i e como os dois são números primos, temos que $p'_i = p_1$. Sem perda de generalidade podemos supor $p'_1 = p_1$.

Assim na equação (1.7) podemos cancelar $p'_1 = p_1$, obtendo:

$$p_2 \cdot p_3 \cdots p_k = p'_2 \cdot p'_3 \cdots p'_t.$$

Note que no primeiro membro da equação acima temos $k-1$ fatores primos e pela hipótese de indução o produto $p_2 \cdot p_3 \cdots p_k$ é único. Portanto $k-1 = t-1 \implies k = t$ e assim $p'_i = p_i,\ \forall i \in \{1, 2, ..., k\}$, encerrando a demonstração. ■

Este teorema tem uma importância muito grande para o estudo do conjunto dos números inteiros, esperamos que o leitor ja tenha uma noção de suas aplicações. Com este teorema encerramos este capítulo e agora estamos em condições de abordar o assunto principal deste trabalho.

Capítulo 2

Os Ternos Quase Pitagóricos

Neste capítulo apresentaremos de fato a definição do conjunto dos ternos quase pitagóricos, que é o alvo do estudo deste trabalho, bem como elencaremos algumas propriedades desse conjunto explorando uma relação entre os seus elementos e os números complexos.

2.1 Definição e Algumas Propriedades

Definição 2.1.1 *Sejam $x, y, z \in \mathbb{Z}$. O terno (x, y, z) é chamado* ***Terno quase pitagórico*** *quando satisfaz a equação*

$$x^2 + my^2 = z^2 \tag{2.1}$$

onde $m \in \mathbb{N}$ é livre de quadrado.

Antes de darmos exemplos, faremos algumas observações iniciais:

Se $x = 0$ então $x^2 + my^2 = z^2 \ \Rightarrow \ my^2 = z^2$, e pelo teorema fundamental da aritmética temos que, m é um quadrado perfeito, contrariando a definição 2.1.

Agora supondo $z = 0$ então $x^2 + my^2 = z^2 \ \Rightarrow \ x^2 = -my^2$ e como x^2 e my^2 são positivos, a única opção que resta é $x = y = 0$.

Com isso afirmamos que $x = 0$ se, e somente,se quando $z = 0$. Nesse caso temos $y = 0$ também.

Portanto para o que segue desconsideraremos o caso $x = z = 0$, que pelo feito acima é o mesmo que desconsiderar o terno $(0, 0, 0)$.

Exemplo 2.1.1 *O terno* $(1, 2, 3)$*, satisfaz a equação* $x^2 + 2y^2 = z^2$*, portanto é um terno quase pitagórico. Bem como* $(2, 4, 6)$ *e* $(3, 6, 9)$ *também são.*

Proposição 2.1.1 *Se* (x_0, y_0, z_0) *é um terno quase pitagórico, então* (ax_0, ay_0, az_0) *também o é, para todo* $a \in \mathbb{Z} - \{0\}$*.*

Demonstração: De fato, se (x_0, y_0, z_0) é um terno quase pitagórico, então pela Definição 2.1 temos $x_0^2 + my_0^2 = z_0^2$ e assim multiplicando em ambos os membros dessa equação um inteiro a qualquer, não-nulo, obtemos:

$$(ax_0)^2 + m \cdot (ay_0)^2 = a^2(x_0^2 + m \cdot y_0^2) = a^2 z_0^2 = (az_0)^2.$$

Portanto (ax_0, ay_0, az_0) é um terno quase pitagórico, para todo $a \in \mathbb{Z} - \{0\}$. ■

Desse modo se conseguirmos encontrar um terno quase pitagórico, podemos então, através deste, gerar infinitos outros ternos quase pitagóricos. A proposição a seguir nos fornece uma forma de encontrar um terno quase pitagórico, além de mostrar que existe uma infinidade destes ternos.

Proposição 2.1.2 *Se* $a, b, c \in \mathbb{Z} - \{0\}$*, então* $(a^2 - mb^2\ ,\ 2ab\ ,\ a^2 + mb^2)$ *é um terno quase pitagórico, para todo* $m \in \mathbb{N}$ *livre de quadrados.*

Demonstração: De fato:

$$\begin{aligned}(a^2 - mb^2)^2 + m(2ab)^2 &= (a^2)^2 - 2ma^2b^2 + (mb^2)^2 + 4ma^2b^2 \\ &= (a^2)^2 + 2ma^2b^2 + (mb^2)^2 \\ &= (a^2 + mb^2)^2\end{aligned}$$

O que implica que $(a^2 - mb^2\ ,\ 2ab\ ,\ a^2 + mb^2)$ é um terno quase pitagórico. ■

Proposição 2.1.3 *Seja* (x, y, z) *um terno quase pitagórico. Se* $d = mdc(x, y)$ *então* $\left(\frac{x}{d}, \frac{y}{d}, \frac{z}{d}\right)$ *é um terno quase pitagórico.*

Demonstração: De fato se (x, y, z) é um terno quase pitagórico, então $x^2 + my^2 = z^2$. Agora supondo $d = mdc(x, y)$, temos que $d \mid x \ \Rightarrow\ d^2 \mid x^2$ e também que $d \mid y \ \Rightarrow\ d^2 \mid my^2$.

Logo $d^2 \mid (x^2 + my^2) \ \Rightarrow\ d^2 \mid z^2 \ \Rightarrow\ d \mid z$.

Isto é, existem $x', y', z' \in \mathbb{Z}$ tais que:

$$x = x'd, \quad y = y'd, \quad z = z'd \quad e \quad mdc(x', y') = 1.$$

Substituindo as igualdades acima em $x^2 + my^2 = z^2$, obtemos:

$$x^2 + my^2 = z^2 \quad \Leftrightarrow \quad x'^2d^2 + my'^2d^2 = z'^2d^2 \quad \Leftrightarrow \quad x'^2 + my'^2 = z'^2.$$

Como $x' = \dfrac{x}{d}$, $y' = \dfrac{y}{d}$, $z' = \dfrac{z}{d}$, concluímos que $\left(\dfrac{x}{d}, \dfrac{y}{d}, \dfrac{z}{d}\right)$ é um terno quase pitagórico, além disso mdc(x',y')=1. ■

Esta proposição nos permite enunciar a seguinte:

Definição 2.1.2 *Sejam $x, y, z \in \mathbb{Z}$ satisfazendo $x^2 + my^2 = z^2$. Quando $mdc(x, y) = 1$ o terno (x, y, z) é denominado* ***terno quase pitagórico primitivo****.*

Com isso podemos pensar na possibilidade de estudar o conjunto de todos os ternos quase pitagóricos, utilizando apenas os ternos quase pitagóricos primitivos, pois pelas proposições acima podemos gerar qualquer terno quase pitagórico utlizando um terno quase pitagórico primitivo conveniente.

Exemplo 2.1.2 *No exemplo 2.1.1 temos $(1, 2, 3)$ é um terno quase pitagórico primitivo referente a equação $x^2 + 2y^2 = z^2$ e tal terno gera os outros ternos quase pitagóricos $(2, 4, 6) = (2 \cdot 1, 2 \cdot 2, 2 \cdot 3)$ e $(3, 6, 9) = (3 \cdot 1, 3 \cdot 2, 3 \cdot 3)$. Pela Proposição (2.1.1) afirmamos que $(t, 2t, 3t)$ é um terno quase pitagórico, para todo $t \in \mathbb{Z}$.*

De posse da Proposição 2.1.2, podemos afirmar que existem infinitos ternos quase pitagóricos primitivos do tipo $(a^2 - mb^2\ ,\ 2ab\ ,\ a^2 + mb^2)$ quando $m = 2$. Para demonstrar esta afirmação basta tomar inteiros a e b, com a impar e b par de modo que $mdc(a, b) = 1$. Assim $(a^2 - 2b^2\ ,\ 2ab\ ,\ a^2 + 2b^2)$ é um terno quase pitagórico primitivo referente a equação $x^2 + 2y^2 = z^2$.

De fato se $d = mdc(a^2 - 2b^2\ ,\ a^2 + 2b^2)$, então d é ímpar, pois $d \mid (a^2 - 2b^2)$ e $d \mid (a^2 + 2b^2)$ que são ímpares.

Logo $d \mid (a^2 - 2b^2 + a^2 + 2b^2)$ e $d \mid (a^2 + 2b^2 - a^2 + 2b^2)$, isto é $d \mid 2a^2$ e $d \mid 2^2b^2$, mas como d é ímpar $d \mid a^2$ e $d \mid b^2$.

Portando d divide o número ímpar a^2, também divide o número par b^2 e como $mdc(a, b) = 1$ obtemos $d = 1$.

Agora se $d' = mdc(a^2 - 2b^2\ ,\ 2ab)$ então $d' \mid (a^2 - 2b^2)$ e $d' \mid 2ab$, o que implica que $d' \mid [(a^2 - 2b^2)^2 + (2ab)^2]$, isto é $d' \mid (a^2 + 2b^2)$.

Logo $d' \mid (a^2 - 2b^2)$ e $d' \mid (a^2 + 2b^2)$.

Mas ja provamos acima que $mdc(a^2 - 2b^2\ ,\ a^2 + 2b^2) = 1$, portanto $d' = 1$, isto é $mdc(a^2 - 2b^2\ ,\ 2ab) = 1$.

Exemplo 2.1.3 *Vamos procurar ternos quase pitagóricos primitivos referente a equação* $x^2 + 2y^2 = z^2$*, seguindo os passos acima.*

1. *Tomando* $a = 5$ *e* $b = 2$*, temos* $(5^2 - 2 \cdot 2^2\ ,\ 2 \cdot 5 \cdot 2\ ,\ 5^2 + 2 \cdot 2^2) = (17, 20, 33)$.

2. *Tomando* $a = 7$ *e* $b = 4$*, temos* $(7^2 - 2 \cdot 4^2\ ,\ 2 \cdot 7 \cdot 4\ ,\ 7^2 + 2 \cdot 4^2) = (17, 56, 81)$.

3. *Tomando* $a = 9$ *e* $b = 4$*, temos* $(9^2 - 2 \cdot 4^2\ ,\ 2 \cdot 9 \cdot 4\ ,\ 9^2 + 2 \cdot 4^2) = (49, 72, 123)$.

Neste trabalho estamos interessados nos ternos com componentes inteiras, porém o conjunto solução das equações do tipo $x^2 + my^2 = z^2$ possui ternos compostos por números reais, o que nos instiga a esboçar o gráfico de uma equação desse tipo afim de observar o seu comportamento. Veja como exemplo um pedaço do gráfico da equação $x^2 + 2y^2 = z^2$.

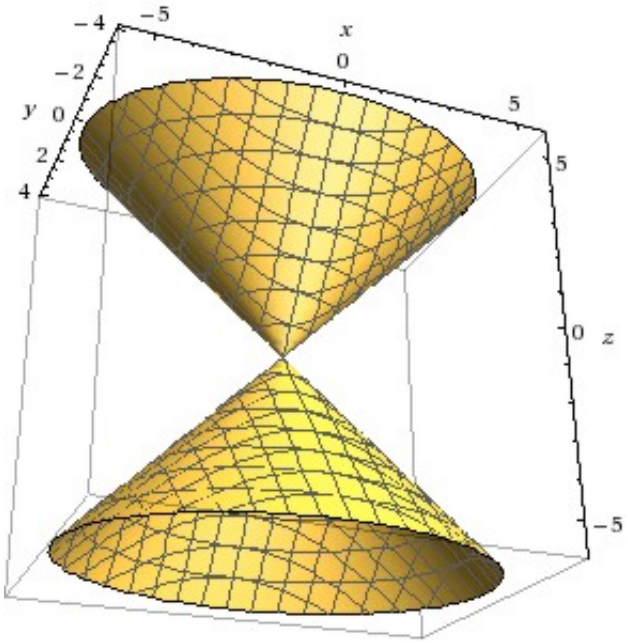

Figura 2.1: Gráfico da equação $x^2 + 2y^2 = z^2$ no espaço tridimensional

Observe que o gráfico é simétrico em relação ao plano XOY, e assim quando formos analisar o comportamento das soluções desta equação podemos considerar os ternos

com $z > 0$, isto é considerar apenas o cone positivo do gráfico. Note também que, como estamos admtindo $z \neq 0$, temos:

$$x^2 + my^2 = z^2 \implies \left(\frac{x}{z}\right)^2 + m\left(\frac{y}{z}\right)^2 = 1 \implies (x')^2 + m(y')^2 = 1.$$

Onde $x' = \dfrac{x}{z}$ e $y' = \dfrac{y}{z}$, são números racionais de mesmo denominador.

Isto é, nossa equação inicial se transfoma na equação de uma elipse no plano cartesiano XOY, onde cada terno quase pitagórico está relacionado a um ponto de coordenadas racionais sobre esta elipse. Veja o gráfico da equação $x^2 + 2y^2 = z^2$ no plano XOY.

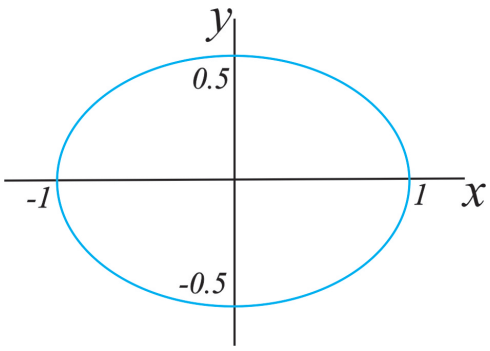

Figura 2.2: Gráfico da equação $x^2 + 2y^2 = z^2$ no plano cartesiano

Neste trabalho utilizaremos dessas ideias acima apenas para visualização. Nosso trabalho se voltará para a relação de um terno quase pitagórico com um ponto do plano complexo.

A partir da analise feita após o grafico da figura 2.1, denotaremos o conjunto dos ternos quase pitagóricos por:

$$\mathbb{T}_m = \{(x, y, z) \in \mathbb{Z}^3;\ \ x^2 + my^2 = z^2,\ x \neq 0\ e\ z > 0\}.$$

2.2 Classe de Ternos Quase Pitagóricos

As proposições demonstradas na seção anterior, nos permite pensar em "dividir"o conjunto $\mathbb{T}_m$ em um conjunto de classes, onde cada classe gerada por um terno quase pitagórico primitivo. Nesta seção mostraremos que isso é possível e para isto, definimos a seguinte relação.

Definição 2.2.1 *Definimos sobre $\mathbb{T}_m$ a relação binária, que denotaremos por $\sim$, da seguinte maneira:*

$$(x,y,z) \sim (a,b,c) \ . \equiv . \ \exists \ r,s \in \mathbb{Z} - \{0\} \ \ tais \ que \ \ r(x,y,z) = s(a,b,c).$$

Proposição 2.2.1 *A Relação $\sim$ definida sobre $\mathbb{T}_m$ é uma relação de equivalência.*

Demonstração: Sejam (a,b,c), (d,e,f), (u,v,w) pertencentes a $\mathbb{T}_m$, temos que:

1. ($\sim$ é reflexiva): Com efeito $(a,b,c) = 1 \cdot (a,b,c) \implies (a,b,c) \sim (a,b,c)$.

2. ($\sim$ é simétrica): Se $(a,b,c) \sim (d,e,f)$ então pela definição existem $r,s \in \mathbb{Z} - \{0\}$ tais que $r(a,b,c) = s(d,e,f)$ e como a relação de igualdade é uma relação simétrica temos que $s(d,e,f) = r(a,b,c)$. Logo $(d,e,f) \sim (a,b,c)$.

3. ($\sim$ é transitiva): Se $(a,b,c) \sim (d,e,f)$ e $(d,e,f) \sim (u,v,w)$ então pela definição da relação $\sim$, existem $p,q,r,s \in \mathbb{Z} - \{0\}$ tais que:

   $$p(a,b,c) = q(d,e,f) \ \ e \ \ r(d,e,f) = s(u,v,w).$$

   Multiplicando membro a membro a primeira igualdade por r e a segunda por q, obtemos:

   $$pr(a,b,c) = qr(d,e,f) \ \ e \ \ qr(d,e,f) = qs(u,v,w).$$

   Logo $pr(a,b,c) = qs(u,v,w)$, o que significa que $(a,b,c) \sim (u,v,w)$.

Desse modo concluímos que a relação $\sim$ é uma relação de equivalência sobre $\mathbb{T}_m$.

■

Uma vez que a relação $\sim$ é uma relação de equivalência sobre $\mathbb{T}_m$, faz sentido considerarmos o conjunto-quociente $\mathbb{T}_m/\sim$ de $\mathbb{T}_m$ pela relação $\sim$. De agora em diante, denotaremos esse conjunto-quociente por $\mathbb{T}_{[m]}$, e cada elemento de $\mathbb{T}_{[m]}$ será denominado **classe de ternos quase pitagóricos**.

Dado $(a,b,c) \in \mathbb{T}_m$, a classe de ternos quase pitagóricos determinada por (a,b,c) consiste no conjunto $\{(x,y,z) \in \mathbb{T}_m; \ (x,y,z) \sim (a,b,c)\}$. Tal conjunto será doravante denotado por $[(a,b,c)]$. Cada elemento de (a,b,c) é dito um **representante** de $[(a,b,c)]$. É evidente que cada classe $[(a,b,c)]$ possui uma infinidade de representantes, porém pelas

Proposições 2.1.1 e 2.1.3 podemos escolher um terno quase pitagórico primitivo dessa classe para a representação da classe.

Proposição 2.2.2 *Em cada classe* $[(a,b,c)]$ *de* $\mathbb{T}_{[m]}$*, existe apenas um único terno quase pitagórico primitivo.*

Demonstração: Seja (a,b,c) um terno quase pitagórico primitivo, por definição temos $mdc(a,b)=1$. Note inicialmente que os ternos quase pitagóricos primitivos com $b=0$, são $(1,0,1)$ e $(-1,0,1)$ que estão em classes diferentes e além disso é facil ver que são os únicos primitivos de suas classes.

Supondo agora $b\neq 0$, se $(d,e,f)\in[(a,b,c)]$ é um terno quase pitagórico primitivo então, pela definição 2.2.1 existem $r,s\in\mathbb{Z}-\{0\}$ tais que $(rd,re,rf)=(sa,sb,sc)$, isto é:

$$\begin{cases} rd=sa \\ re=sb \\ rf=sc \end{cases} \implies \begin{cases} rdb=sab \\ rea=sba \\ rf=sc \end{cases}.$$

Subtraindo membro a membro, a segunda igualdade da primeira (na ultima chave), obtemos $rdb-rea=0$, o que implica $db=ea$. Assim $d\mid ea$ e como $mdc(d,e)=1$ temos $d\mid a$, do mesmo modo obtemos $a\mid bd$ e como $mdc(a,b)=1$ afirmamos que $a\mid d$. Neste caso temos $d\mid a$ e $a\mid d$ e pela propriedade (vi) da proposição 1.2.1 concluímos que $d=\pm a$. Analogamente se obtém $e=\pm b$.

Logo, $a^2+mb^2=d^2+me^2 \implies c^2=f^2$, e como estamos considerando apenas os ternos com a terceira componente positiva, conluímos que $c=f$.

Portanto o terno (d,e,f) pode ser um dos ternos $(-a,-b,c)$, $(-a,b,c)$, $(a,-b,c)$ ou (a,b,c). Mas os três primeiros ternos não pertencem a classe de $[(a,b,c)]$ e como $(d,e,f)\in[(a,b,c)]$, concluímos que $(d,e,f)=(a,b,c)$ como queríamos. ■

Proposição 2.2.3 *Seja* $[(a,b,c)]\in\mathbb{T}_{[m]}$*, com* $mdc(a,b)=1$*. Se* $(x,y,z)\in[(a,b,c)]$ *então* $(x,y,z)=t(a,b,c)$*, para algum* $t\in\mathbb{Z}-\{0\}$*.*

Demonstração: De fato sejam $(x,y,z)\in[(a,b,c)]$ e $mdc(a,b)=1$, temos pela definição da relação $\sim$ que existe $r,s\in\mathbb{Z}-\{0\}$ tais que:

$$r(x,y,z)=s(a,b,c).$$

Seja $d = mdc(r, s)$, temos que existe $t, u \in \mathbb{Z} - \{0\}$ tas que $r = du$ e $s = dt$.

Note que $mdc(r', s') = 1$.

Assim: $r(x, y, z) = s(a, b, c) \implies du(x, y, z) = dt(a, b, c)$.

Logo $u(x, y, z) = t(a, b, c)$, o que implica que $(ux, uy, uz) = (ta, tb, tc)$ e consequentemente $ux = ta$ e $uy = tb$.

Desse modo temos que $u \mid ta$, mas como u e t são primos entre si, pela 1.2.3 segue que $u \mid a$.

Análogamente obtemos que $u \mid b$.

Concluindo então que $u = 1$, pois a e b são primos entre si.

Portanto $u(x, y, z) = t(a, b, c) \implies (x, y, z) = t(a, b, c)$. ■

Assim se (a, b, c) é um terno quase pitagórico primitivo então podemos representar

$$[(a, b, c)] = \{(x, y, z) \in \mathbb{T}_m; (x, y, z) = (ta, tb, tc), \forall t \in \mathbb{Z} - \{0\}\}.$$

2.2.1 Operação em $\mathbb{T}_{[m]}$

Observe inicialmente que, se (x, y, z) e (a, b, c) são ternos quase pitagóricos, então valem $x^2 + my^2 = z^2$ e $a^2 + mb^2 = c^2$.

Multiplicando essas duas igualdades membro a membro, temos:

$$\begin{aligned}
(zc)^2 = z^2 \cdot c^2 &= (x^2 + my^2) \cdot (a^2 + mb^2) && (2.2)\\
&= x^2a^2 + mx^2b^2 + my^2a^2 + m^2y^2b^2 && (2.3)\\
&= x^2a^2 - 2xamyb + m^2y^2b^2 + mx^2b^2 + 2xamyb + my^2a^2 && (2.4)\\
&= (xa - myb)^2 + m(xb + ya)^2. && (2.5)
\end{aligned}$$

Isto mostra que o produto de dois inteiros da forma $x^2 + my^2$ é também dessa forma, nos inspirando a definir uma operação sobre $\mathbb{T}_{[m]}$, que denotaremos por $\star$, da seguinte maneira:

$$\begin{array}{rcccl}
\star & : & \mathbb{T}_{[m]} \times \mathbb{T}_{[m]} & \longrightarrow & \mathbb{T}_{[m]} \\
 & & \big([(x, y, z)], [(a, b, c)]\big) & \longmapsto & [(x, y, z)] \star [(a, b, c)] := [(xa - myb, xb + ya, zc)]
\end{array}$$

Mostraremos agora que esta operação está bem definida em $\mathbb{T}_{[m]}$, isto é, o composto $[(x, y, z)] \star [(a, b, c)]$ não se altera quando mudamos os representantes das classes, mas

precisamente mostraremos que:

Proposição 2.2.4 *Se* (x, y, z), (a, b, c), (x', y', z') *e* (a', b', c') *são ternos quase pitagóricos tais que* $mdc(x, y) = mdc(a, b) = 1$, $[(x, y, z)] = [(x', y', z')]$ *e* $[(a, b, c)] = [(a', b', c')]$, *então* $[(x, y, z)] \star [(a, b, c)] = [(x', y', z')] \star [(a', b', c')]$.

Demonstração: De fato sejam (x, y, z), (a, b, c), (x', y', z') e (a', b', c'), ternos quase pitagóricos tais que:

$$mdc(x, y) = mdc(a, b) = 1, \quad [(x, y, z)] = [(x', y', z')] \quad e \quad [(a, b, c)] = [(a', b', c')].$$

Temos $(x', y', z') = (rx, ry, rz)$ e $(a', b', c') = (sa, ab, ac)$ e daí:

$$[(x', y', z')] \star [(a', b', c')] = [(rx, ry, rz)] \star [(sa, ab, ac)] = [(rxsa - mrysb, rxsb + rysa, rzsc)].$$

Logo:

$$[(rx, ry, rz)] \star [(sa, ab, ac)] = [(rs(xa - myb), rs(xb + ya), rs(zc))] = [(xa - myb, xb + ya, zc)].$$

■

Nosso objetivo agora é mostrar que $(\mathbb{T}_{[m]}, \star)$ é um **grupo abeliano**, o que pode ser feito somente manipulando a operação $\star$, como na definição. Porém neste trabalho, mais especificamente na próxima seção, apresentaremos uma ferramenta bastante elegante e eficiente para realizar esta tarefa.

2.3 Ternos Quase Pitagóricos e os Números Complexos

Nesta seção apresentaremos uma relação entre um elemento de $\mathbb{T}_m$ e um número complexo, mas especificamente um número complexo sobre a circunferência unitária com centro na origem do plano complexo. Tal relação nos permite visualizar geometricamente algumas propriedades de uma classe $[(a, b, c)] \in \mathbb{T}_{[m]}$, bem como facilitar alguns trabalhos computacionais.

Mas para tal feito é necessário que definamos uma certa função cujo domínio é $\mathbb{C}$, e que toma valores em $\mathbb{R}^+$: a chamada *Função Norma*. Além de defini-la, ressaltaremos algumas de suas propriedades.

Definição 2.3.1 (Função Norma) *A função $\mathcal{N}$ definida por*

$$\begin{aligned} \mathcal{N} \ : \ \mathbb{C} &\longrightarrow \mathbb{R}^+ \\ a+bi &\longmapsto a^2+b^2 \end{aligned}$$

é chamada de ***Função Norma*** *em $\mathbb{C}$.*

A proposição seguinte encerra propriedades importantes da Função Norma, que utilizaremos no transcorrer deste texto.

Proposição 2.3.1 *Seja $\mathcal{N}$ a Função Norma em $\mathbb{C}$. Então:*

(i) $\mathcal{N}(\alpha) \geq 0, \ \forall \ \alpha \in \mathbb{C}$;

(ii) $\mathcal{N}(\alpha) = 0$, se, e somente se, $\alpha = 0$;

(iii) $\mathcal{N}(\alpha) = \alpha\bar{\alpha}$, para todo $\alpha \in \mathbb{C}$, onde $\bar{\alpha}$ denota o ***conjugado*** *de α;*

(iv) $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta), \ \forall \ \alpha, \beta \in \mathbb{C}$; isto é, a Função Norma preserva a multiplicação.

Demonstração: Por questão de objetividade, provaremos aqui apenas a afirmação (iv). As demais podem ser demonstradas sem muito esforço pelo leitor, ou então consultar (3) e (6).

(iv) Dados dois números complexos $\alpha = a + bi$ e $\beta = c + di$ quaisquer, temos:

$$\begin{aligned} \mathcal{N}(\alpha\beta) &= \mathcal{N}\big((a+bi)(c+di)\big) \\ &= \mathcal{N}\big((ac-bd)+(bc+ad)i\big) = (ac-bd)^2+(bc+ad)^2 \\ &= a^2c^2 - 2acbd + b^2d^2 + b^2c^2 + 2bcad + a^2d^2 \\ &= a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2 \\ &= a^2(c^2+d^2) + b^2(c^2+d^2) \\ &= (a^2+b^2)(c^2+d^2) \\ &= \mathcal{N}(\alpha)\cdot\mathcal{N}(\beta) \end{aligned}$$

■

De posse dessa função norma, note que se $(x, y, z) \in \mathbb{T}_m$, então:

$$z^2 = x^2 + my^2 = (x + y\sqrt{-m})(x - y\sqrt{-m}) = \mathcal{N}(x + y\sqrt{-m}).$$

Assim podemos associar cada terno quase pitagórico (x, y, z) a um número complexo pertencente ao conjunto:

$$\mathbb{Z}[\sqrt{-m}] = \{x + y\sqrt{-m} / \quad x, y \in \mathbb{Z}\} \subset \mathbb{C}.$$

O leitor mais interessado, pode verificar que $\mathbb{Z}[\sqrt{-m}]$ é um subanel do anel $\mathbb{C}$, sob as operações de adição e multiplicação usuais de números complexos.

Denotaremos, a partir de agora, os números desse conjunto por $x+iy\sqrt{m}$ e assim sua representação geométrica no plano complexo será:

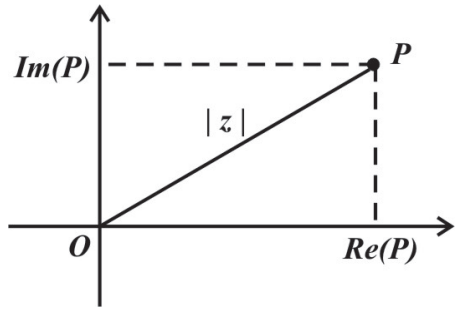

Figura 2.3: Representação no plano complexo

Onde $\quad P = x + iy\sqrt{m}, \quad Re(P) = x, \quad Im(P) = y\sqrt{m} \quad$ e

$$|z| = \sqrt{\mathcal{N}(x + iy\sqrt{m})} = \sqrt{x^2 + my^2}.$$

Exemplo 2.3.1 *De acordo com o exemplo 2.1.1, o terno* $(1, 2, 3)$ *é uma das soluções da equação* $x^2 + 2y^2 = z^2$*, logo podemos associá-lo ao número complexo* $1 + i2\sqrt{2}$*.*

Do mesmo modo associamos:

$(2, 4, 6) \quad a \quad 2 + i4\sqrt{2} = 2(1 + i2\sqrt{2}) \quad e \quad (3, 6, 9) \quad a \quad 3 + i6\sqrt{2} = 3(1 + i2\sqrt{2}).$

Generalizando este exemplo identificamos que todos os elementos de uma classe $[(a, b, c)] \in \mathbb{T}_{[m]}$ está disposto geometricamente sobre a reta que passa pelo segmento $\overline{OP}$ no plano complexo, onde O é a origem do plano complexo e $P = a + ib\sqrt{m}$. Isso nos faz conluir que as classes $[(a, b, c)] \in \mathbb{T}_{[m]}$ são duas a duas disjuntas, pois cada classe

representa uma reta no plano complexo passando pela origem e desse modo o único ponto pertencente a interseção dessas retas é o ponto $O = 0 + i0\sqrt{m}$ que é associado ao terno $(0, 0, 0) \notin \mathbb{T}_m$.

Consideremos agora a circunferência unitária S_1, observamos que os números complexos $x + iy\sqrt{m}$ referentes aos ternos quase pitagóricos (x, y, z) estão no exterior de S_1 com exceção do terno $(1, 0, 1)$, que está sobre S_1.

Assim $p = x + iy\sqrt{m}$ pode ser associado a um ponto W sobre a circunferência unitária S_1 no plano complexo onde $W = \overline{OP} \cap S_1$ representado pelo número complexo $w = \cos\theta + i\sin\theta = e^{i\theta}$, sendo θ o ângulo com vértice em O formado pelo eixo OX e o segmento $\overline{OP}$ tal que $0 < \theta \leq 2\pi$.

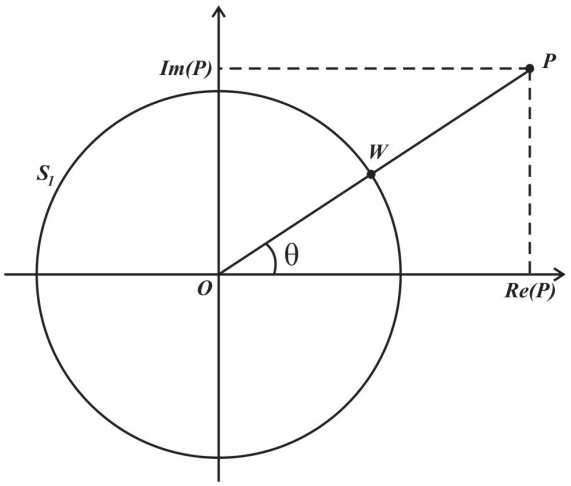

Figura 2.4: Circunferência unitária

Como w é um número complexo que representa um ponto sobre S_1, temos que $|w| = 1$.

Assim, se $p = x + iy\sqrt{m}$ é um número complexo associado pelo terno quase pitagórico (x, y, z) então p é multiplo de p, isto é $p = x + iy\sqrt{m} = w \cdot k$, para algum $k \in \mathbb{Z}^+$.

Logo, aplicando a função norma e ultilizando o fato de que esta função preserva a multiplicação, obtemos:

$$z^2 = x^2 + my^2 = \mathcal{N}(P) = \mathcal{N}(w \cdot k) = \mathcal{N}(w) \cdot \mathcal{N}(k) = 1 \cdot k^2 = k^2.$$

Implicando assim que $|k| = |z|$. Mas como z e k são positivos, temos que $k = z$. Portanto $w = e^{i\theta} = \dfrac{x}{z} + i\dfrac{y\sqrt{m}}{z}$.

Observe agora que se $(x, y, z) \in [(a, b, c)]$, onde (a, b, c) é o terno quase pitagórico primitivo desta classe, então $(x, y, z) = (ta, tb, tc)$ para algum $t \in \mathbb{Z}^+$. Pelo feito acima associamos o terno (x, y, z) ao seguinte número complexo em S_1:

$$W = \frac{x}{z} + i\frac{y\sqrt{m}}{z} = \frac{ta}{tc} + i\frac{tb\sqrt{m}}{tc} = \frac{a}{c} + i\frac{b\sqrt{m}}{c}.$$

Em outras palavras, podemos associar todos os ternos da classe ao número complexo em S_1, associado pelo terno quase pitagórico primitivo representante da classe.

Antes de enunciar o próximo resultado (que é o resultado principal desta seção), é importante lembrar que S_1 é um subgrupo multiplicativo de $\mathbb{C}$, onde a multiplicação em questão se refere a multiplicação usual de números complexos. Portanto no enunciado seguinte vamos admitir S_1 sendo um grupo multiplicativo.

Teorema 2.3.1 *Seja S_1 o conjunto dos números complexos que formam a circunferência unitária no plano complexo.*

*A função $\phi : \mathbb{T}_{[m]} \longrightarrow S_1$, definida por $\phi[(x, y, z)] = e^{i\theta} = \dfrac{x}{z} + i\dfrac{y\sqrt{m}}{z}$ é **injetora**. Além disso:*

$$\phi\big([(x, y, z)] \star [(a, b, c)]\big) = \phi[(x, y, z)] \cdot \phi[(a, b, c)], \quad \forall [(x, y, z)], [(a, b, c)] \in \mathbb{T}_{[m]}. \tag{2.6}$$

Demonstração: Sejam $[(a, b, c)]$ e $[(x, y, z)]$ elementos de $\mathbb{T}_{[m]}$, tais que $mdc(x, y) = 1$ e $mdc(a, b) = 1$. Temos que:

$\phi[(a, b, c)] = e^{i\alpha} = \dfrac{a}{c} + i\dfrac{b\sqrt{m}}{c}$ e $\phi[(x, y, z)] = e^{i\beta} = \dfrac{x}{z} + i\dfrac{y\sqrt{m}}{z}$.

Assim

$$\begin{aligned}
\phi\big([(x, y, z)] \star [(a, b, c)]\big) &= \phi[(xa - myb, xb + ya, zc)] \\
&= \frac{xa - myb}{zc} + i\frac{(xb + ya)\sqrt{m}}{zc} \\
&= \frac{xa - myb + ixb\sqrt{m} + iya\sqrt{m}}{zc} \\
&= \frac{x(a + ib\sqrt{m}) + iy\sqrt{m}(ib\sqrt{m} + a)}{zc} \\
&= \frac{(x + iy\sqrt{m})(a + ib\sqrt{m})}{zc} \\
&= \frac{(x + iy\sqrt{m})}{z} \cdot \frac{(a + ib\sqrt{m})}{c} \\
&= \phi[(x, y, z)] \cdot \phi[(a, b, c)]
\end{aligned}$$

Logo a função ϕ cumpre (2.6). Com isso, provando futuramente que $(\mathbb{T}_{[m]}, \star)$ é um grupo, dizemos que ϕ é um homomorfismo de grupo.

Além disso se $\phi[(x,y,z)] = \phi[(a,b,c)]$, então:

$$\phi[(x,y,z)] = \phi[(a,b,c)] \implies \frac{x}{z} + i\frac{y\sqrt{m}}{z} = \frac{a}{c} + i\frac{b\sqrt{m}}{c}.$$

Pela igualdade de números complexos temos, $\dfrac{x}{z} = \dfrac{a}{c}$ e $\dfrac{y\sqrt{m}}{z} = \dfrac{b\sqrt{m}}{c}$.

Logo $xc = za$ e $yc = zb$. Isolando z na primeira igualdade e substituindo na segunda obtemos $ya = xb$.

Agora como $mdc(x,y) = 1$, existem $r, s \in \mathbb{Z}$ tais que $1 = xr + ys$.

Daí obtemos:

$$a = a(xr + ys) = (ax)r + (ay)s = (ax)r + (xb)s = x(ar + bs). \tag{2.7}$$

Do mesmo modo:

$$c = c(xr + ys) = (cx)r + (cy)s = (za)r + (zb)s = z(ar + bs). \tag{2.8}$$

Da ultima igualdade e do fato de que $yc = zb$ segue que:

$$yc = zb \;\Rightarrow\; yz(ar + bs) = zb \;\Rightarrow\; y(ar + bs) = b \tag{2.9}$$

Portanto: $(ar + bs) \mid a$ e $(ar + bs) \mid b$.

Mas como $mdc(a,b) = 1$, chegamos a conclusão de que $ar + bs = 1$. Tendo em vista as igualdades (2.7), (2.8) e (2.9) acima, isto implica que $a = x$, $c = z$, $y = b$, isto é:

$$(x,y,z) = (a,b,c).$$

Concluíndo a demonstração de que ϕ também é injetora.

■

Desse modo, efetuar a operação $[(x,y,z)] \star [(a,b,c)]$ em $\mathbb{T}_{[m]}$ é equivalente a multiplicar os seus respectivos elementos associados em S_1.

Além do mais, se $\phi[(x,y,z)] = \dfrac{x}{z} + i\dfrac{y\sqrt{m}}{z}$ e $\phi[(a,b,c)] = \dfrac{a}{c} + i\dfrac{b\sqrt{m}}{c}$ formam os

ângulos α e β com o eixo OX, então:

$$\phi\Big([(x,y,z)] \star [(a,b,c)]\Big) = \phi[(x,y,z)] \cdot \phi[(a,b,c)] = e^{i\alpha} \cdot e^{i\beta} = e^{i(\alpha+\beta)}$$

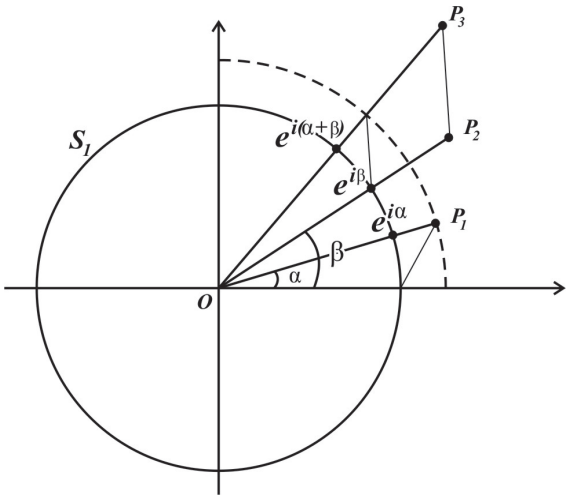

Figura 2.5: Produto de números complexos

2.4 $(\mathbb{T}_{[m]}, \star)$ é um Grupo Abeliano

Esta seção é dedicada apenas a verificar que $(\mathbb{T}_{[m]}, \star)$ é um grupo abeliano, utilizando para tanto a função ϕ definida na seção anterior, e também utilizaremos constantemente os resultados demonstrados no Teorema 2.3.1.

Teorema 2.4.1 $(\mathbb{T}_{[m]}, \star)$ *é um Grupo Abeliano. Isto é a operação* $\star$ *é assossiativa, comutativa, existe um elemento neutro para a operação* $\star$ *em* $\mathbb{T}_{[m]}$ *e todos elementos de* $\mathbb{T}_{[m]}$ *possui um simétrico em relação a operação* $\star$*.*

Demonstração: Para a demonstração observe atentamente que usaremos a todo o momento o resultado do teorema 2.3.1, isto é, a função ϕ é um homomorfismo injetor e também utilizaremos o fato de que S_1 é um grupo multiplicativo.

Sejam então $[(x,y,z)]$, $[(a,b,c)]$ e $[(d,e,f)]$ pertencente a $\mathbb{T}_{[m]}$, temos que:

$$\phi[(x,y,z)] = e^{i\alpha}, \quad \phi[(a,b,c)] = e^{i\beta}, \quad \phi[(d,e,f)] = e^{i\gamma}.$$

[⋆1] **Associatividade:** Dado $[(x,y,z)]$, $[(a,b,c)]$ e $[(d,e,f)]$ pertencente a $\mathbb{T}_{[m]}$, temos:

$$\begin{aligned}\phi\Big(\big([(x,y,z)]\star[(a,b,c)]\big)\star[(d,e,f)]\Big) &= (e^{i\alpha}\cdot e^{i\beta})\cdot e^{i\gamma}\\ &= e^{i\alpha}\cdot(e^{i\beta}\cdot e^{i\gamma})\\ &= \phi\Big([(x,y,z)]\star\big([(a,b,c)]\star[(d,e,f)]\big)\Big).\end{aligned}$$

Como ϕ é injetora temos:

$$\big([(x,y,z)]\star[(a,b,c)]\big)\star[(d,e,f)] = [(x,y,z)]\star\big([(a,b,c)]\star[(d,e,f)]\big).$$

[⋆4] **Comutatividade:** Dado $[(x,y,z)]$, $[(a,b,c)]$ pertencente a $\mathbb{T}_{[m]}$, temos:

$$\begin{aligned}\phi\Big([(x,y,z)]\star[(a,b,c)]\Big) &= e^{i\alpha}\cdot e^{i\beta}\\ &= e^{i\beta}\cdot e^{i\alpha}\\ &= \phi\Big([(a,b,c)]\star[(x,y,z)]\Big).\end{aligned}$$

Como ϕ é injetora temos: $[(x,y,z)]\star[(a,b,c)] = [(a,b,c)]\star[(x,y,z)]$.

[⋆2] **Existe um elemento neutro:** Com efeito $[(1,0,1)]$ é o elemento neutro, pois

$$\phi\Big([(x,y,z)]\star[(1,0,1)]\Big) = e^{i\alpha}\cdot e^{0} = e^{i\alpha} = \phi[(x,y,z)].$$

Mas sendo ϕ uma função injetora, temos $[(x,y,z)]\star[(1,0,1)] = [(x,y,z)]$ e como vale [⋆2], vale também $[(1,0,1)]\star[(x,y,z)] = [(x,y,z)]$.

[⋆3] **Todo elemento de $\mathbb{T}_{[m]}$ possui simétrico:** De fato $[(x,-y,z)]$ é o elemento simétrico de $[(x,y,z)]$, pois se $\phi[(x,y,z)] = \dfrac{x}{z} + i\dfrac{y\sqrt{m}}{z} = e^{i\alpha}$, então:

$$\phi[(x,-y,z)] = \frac{x}{z} - i\frac{y\sqrt{m}}{z} = e^{i(-\alpha)} = e^{i(2\pi-\alpha)}.$$

Logo

$$\phi\Big([(x,y,z)]\star[(x,-y,z)]\Big) = \phi[(x,y,z)]\cdot\phi[(x,-y,z)] = e^{i\alpha}\cdot e^{i(-\alpha)} = e^{0} = \phi[(1,0,1)].$$

Como ϕ é injetora temos que $[(x,y,z)] \star [(x,-y,z)] = [(1,0,1)]$ e por $[\star 2]$ segue que $[(x,-y,z)] \star [(x,y,z)] = [(1,0,1)]$.

Portanto está provado que $(\mathbb{T}_{[m]}, \star)$ é de fato um grupo abeliano. ■

Note que, geometricamente $[\star 4]$ está relacionado com a simetria dos pontos de S_1 em relação ao eixo real do plano complexo.

Considerações finais

.

O leitor deve ter notado que não nos preocupamos em determinar (caracterizar) o conjunto dos ternos quase pitagóricos e sim em identificar padrões e propriedades dos elementos deste conjunto. No decorrer do último capítulo foi comprovada a existência de infinitos ternos quase pitágóricos que foram particionados em classes dando origem ao conjunto $\mathbb{T}_{[m]}$, mostramos também que cada classe deste conjunto é determinada por um único terno quase pitagórico primitivo. A fim de mostrar que $(\mathbb{T}_{[m]}, \star)$ é um grupo abeliano (resultado principal deste trabalho), adotamos a estratégia de associar um terno quase pitagórico a um número complexo pertencente ao conjunto $\mathbb{Z}[\sqrt{-m}]$. Essa associação foi possível após visualizar uma forma de escrever a equação $x^2 + my^2 = z^2$ como produto de dois números complexos, a saber $z^2 = (x + y\sqrt{-m})(x - y\sqrt{-m})$. Estudar esta fatoração em $\mathbb{Z}[\sqrt{-m}]$ instiga trabalhos futuros no sentido de encontrar expressões que determinam o conjunto solução de uma equação do tipo $x^2+my^2 = z^2$, durante este estudo suspeitamos que tais expressões sejam as descritas no enunciado da Proposição (2.1.2).

Um outro fato curioso que pode fomentar ideias de trabalhos futuros é fruto de alguns testes que efetuamos durante o estudo e a formulação deste trabalho, observe que tomando $m = 3$ temos a equação $x^2 + 3y^2 = z^2$ e claramente $(1, 1, 2)$ é um dos ternos que satisfazem essa equação e como seus componentes são primos entre si, este terno representa uma classe. Observamos que ao efetuar sucessivamente a operação $[(x, y, z)] \star [(a, b, c)] := [(xa - myb, xb + ya, zc)]$ usando a classe $[(1, 1, 2)]$, após um certo número de vezes, tal operação nos dá como resultado a classe $[(1, 0, 1)]$, que é o elemento neutro da operação $\star$, veja:

$$[(1, 1, 2)] \star [(1, 1, 2)] = [(-2, 2, 4)];$$

$$[(1, 1, 2)] \star [(-2, 2, 4)] = [(-8, 0, 8)];$$

$$[(1,1,2)] \star [(-8,0,8)] = [(-8,-8,16)];$$

$$[(1,1,2)] \star [(-8,8,16)] = [(16,-16,32)]$$

$$[(1,1,2)] \star [(16,-16,32)] = [(64,0,64)] \in [(1,0,1)]$$

$$[(1,1,2)] \star [(64,0,64)] = [(64,64,128)];$$

$$[(1,1,2)] \star [(64,64,128)] = [(-128,128,256)];$$

$$[(1,1,2)] \star [(-128,128,256)] = [(-512,0,512)];$$

$$[(1,1,2)] \star [(-512,0,512)] = [(-512,512,1024)];$$

$$[(1,1,2)] \star [(-512,512,1024)] = [(1024,-1024,2048)];$$

$$[(1,1,2)] \star [(1024,-1024,2048)] = [(4096,0,4096)] \in [(1,0,1)].$$

O leitor pode verificar que este ciclo se repete por mais vezes para este exemplo, e isso nos motiva a estudar específicamente o conjunto $\mathbb{T}_{[3]}$ com o objetivo de verificar se $(\mathbb{T}_{[3]},\star)$ é um grupo cíclico. E mais, caso a afirmação anterior se estabeleça, podemos desenvolver um estudo para quais valores de m acontece uma relação semelhante a esta observada acima.

Referências Bibliográficas

[1] ARAUJO, Martinho C., e Nacismento, Thais S.. *Propriedades dos Ternos Pitagóricos*. V Bienal de Matemática. SBM. 2010

[2] BOYER, Carl B.. *História da Matemática*. Segunda Edição. Editora Edgard Blücher. São Paulo-SP. 2001.

[3] DOMINGUES, Hygino H. & IEZZI, Gelson. *Álgebra Moderna*. Atual Editora. São Paulo-SP. 2003.

[4] DOMINGUES, Hygino H. *Fundamentos de Aritmética*. Atual Editora. São Paulo-SP. 1991.

[5] EVES, Howard.. *Introdução à História da Matemática.* 3ª edição. Unicamp. Campinas-SP. 2002.

[6] GARCIA, Arnaldo & LEQUAIN, Yves. *Álgebra: Um curso de Introdução*. Projeto Euclides. Instituto de Matemática Pura e Aplicada. 1988.

[7] GONÇALVES, Adilson. *Introdução a Álgebra*. Projeto Euclides. 5ª edição. Instituto de Matemática Pura e Aplicada. Rio de Janeiro-RJ. 2012.

[8] HEFEZ, Abramo. *Curso de Álgebra*. Coleção Matemática Universitária. Volume I. 4ª edição. Instituto de Matemática Pura e Aplicada. Rio de Janeiro - RJ. 2010.

[9] HEFEZ, Abramo. *Elementos da Aritmética*. Textos Universitários. Sociedade Brasileira de Matemática. 2ª edição. Rio de Janeiro-RJ. 2011.

[10] IEZZI, Gelson. *Fundamentos de Matemática Elementar*. Volume 6. Atual. São Paulo-SP. 1993.

[11] MARTINEZ,Fabio B. MOREIRA, Carlos G. SALDANHA, Nicolau. TENGAN, Edurado.Teoria dos Números: , *Um passeio com primos e outros números familiares pelo mundo inteiro*.Projeto Euclides. IMPA, Rio de Janeiro - 2011.

[12] MUNIZ NETO, Antonio Caminha. Tópicos de Matemática Elementar. Volume 5. *Teoria dos Números*. Coleção Professor de Matemática, SBM. Rio de Janeiro - 2012.

[13] SAMPAIO, João C. V.. *Notas do Curso de Estruturas Algébricas*. Disponível no Site: http://www.dm.ufscar.br/ sampaio/algebra.html. UFSCar. 2013.

[14] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números*. Coleção Matemática Universitária. Instituto de Matemática Pura e Aplicada. 1998.

[15] TAUSSKY, Olga, *Sums of squares*, The American Mathematical Monthly. Volume 77. Paginas 805-830. California. 1970