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

# Geometria Aritmética:

# Triplas pitagóricas e números inteiros que são soma de dois quadrados

**André Martins Gonçalves**

Mestrado Profissional em Matemática: PROFMAT/SBM

Orientador: **Prof. Dr. Aldi Nestor de Souza**

Trabalho financiado pela Capes

Cuiabá - MT

dezembro de 2016

# Geometria Aritmética:

# Triplas pitagóricas e números inteiros que são soma de dois quadrados

Este exemplar corresponde à redação final da dissertação, devidamente corrigida e defendida por André Martins Gonçalves e aprovada pela comissão julgadora.

Cuiabá, 21/12/2016.

Prof. Dr. Aldi Nestor de Souza
Orientador

**Banca examinadora:**

Prof. Dr. Aldi Nestor de Souza
Prof. Dr. Junior César Alves Soares
Prof. Dr. Reinaldo de Marchi

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

**Dados Internacionais de Catalogação na Fonte.**

G635g Gonçalves, Andre Martins.
Geometria aritmética : Triplas pitagóricas e números inteiros que são soma de dois quadrados / Andre Martins Gonçalves. -- 2016
ix, 35 f. : il. color. ; 30 cm.

Orientador: Aldi Nestor de Souza.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2016.
Inclui bibliografia.

1. Ensino. 2. Matemática. 3. Álgebra. 4. Geometria Analítica. I. Título.

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

**Dissertação de Mestrado defendida em 21 de dezembro de 2016 e aprovada pela banca examinadora composta pelos Professores Doutores**

Prof. Dr. Aldi Nestor de Souza

Prof. Dr. Junior César Alves Soares

Prof. Dr. Reinaldo de Marchi

*À minha mãezinha querida,*

*Dona Flavia Maria Martins Gonçalves.*

# Agradecimentos

Agradeço, primeiramente, a Deus.

E ao meu tio-padrinho, Prof. Doutor Custódio Thomaz Kerry Martins, por seu auxílio.

Aos pais de meu amigo Renato dos Santos Resende Fortes., Jamil Resende Fortes e Tereza dos Santos de Souza.

E aos colegas Malton Will e Julio César Campanholo.

Finalmente, agradeço a toda a minha família, especialmente a minha irmã Flávia e o meu cunhado Willian.

Muito obrigado a todos.

Vale lembrar o dito português:

*Navegar é preciso,*
*viver não é preciso.*

Fernando Pessoa.

# Resumo

Esta dissertação tem como tema as triplas de números naturais que podem ser medidas dos lados de um triângulo retângulo. Esses números são caracterizados no início do trabalho, utilizando Teoria dos Números Elementar. Depois são desenvolvidos vários métodos utilizando a "Geometria Aritmética", tais como Equações Diofantinas Lineares, Teorema de Pick, Método das Tangentes e Secantes de Fermat, Curvas Projetivas, Reticulados, o Toro Plano e o Teorema de Minkowski. Por fim, utilizando esses métodos geométricos e aritméticos, faremos a caracterização dos inteiros que são soma de dois quadrados, o que corresponde aos números naturais que podem ser hipotenusa de um triângulo retângulo.

**Palavras chave:** Ensino, Matemática, Álgebra, Geometria Analítica.

# Abstract

This dissertation has as its theme the triples of natural numbers that can be the measures of the sides of a right triangle. These numbers are characterized at the beginning of the work, using Elementary Number Theory. Then several methods are developed using "Arithmetic Geometry", such as Linear Diophantine Equations, Pick Theorem, Fermat Tangent and Secant Method, Projective Curves, Reticulated, Flat Torus, and Minkowski's Theorem. Finally, using these geometric and arithmetical methods, the characterization of the integers that is the sum of two squares, which corresponds to the natural numbers that can be hypotenuse of a right triangle.

**Keywords:** Teaching, Mathematics, Algebra, Analytical Geometry.

# Sumário

# Introdução

"Deus criou os números naturais; tudo o mais é produto da mão do homem."

(Leopold Kronecker)

O presente trabalho tem como núcleo o estudo dos números inteiros sob um ponto de vista contemporâneo. Utilizamos a chamada "Geometria Aritmética"como ferramenta para estudá-los. Na Idade Moderna, René Descartes criou a Geometria Analítica, que é uma "fusão"da Geometria com a Álgebra. Isso deu espaço para aplicações da Geometria Analítica à Teoria dos Números. Na mesma época, Pierre de Fermat estava interessado nas equações diofantinas e se aprofundou bastante na Teoria dos Números. Usou a Geometria para desenvolver a Aritmética. Fermat era juiz de direito e advogado de profissão e trabalhou a Matemática como um matemático amador.

Entre os séculos XVIII e XIX, podemos destacar dois grandes matemáticos que desenvolveram muito a Geometria e a Teoria dos Números. Leonhard Euler, autor do Teorema que caracteriza os inteiros que são soma de dois quadrados, Santos (2007) prova este teorema. O presente trabalho o prova com outro ferramental. Outro grande matemático desse período foi Carl Friedrich Gauss, que provou, por exemplo, o Teorema de Reciprocidade Quadrática, um teorema de Aritmética que usa Geometria.

Hoje em dia, a pesquisa em Geometria Aritmética está presente em inúmeros trabalhos de muitos matemáticos. Ela usa todo ferramental matemático para desenvolver a Teoria dos Números, como Álgebra, Análise, Geometria Diferencial, Análise Complexa, Topologia, entre outros. Um exemplo disso foi o "Último Teorema de Fermat", provado por Andrew Wiles em 1995.

Vamos analisar as triplas de inteiros que são catetos e hipotenusa de um triângulo retângulo, além de caracterizar os números que podem ser hipotenusa. É um problema milenar que esteve presente no livro "Os Elementos"de Euclides, e é também um problema de números naturais e que pode ser explicado a estudantes do final do Ensino Fundamental e no Ensino Médio também.

No 1º Capítulo estudamos as Triplas Pitagóricas, Hefez (2013) nos dá o material para fazermos o estudo.

No 2º Capítulo, apresentamos a Geometria Aritmética. Estudamos Equações Diofantinas, o Teorema de Pick, o Método das Tangentes e Secantes de Fermat, as Curvas Projetivas, o Princípio Local-Global para cônicas, os reticulados planos, o Toro Plano e o Teorema de Minkowski. Gondim (2011) é a referência de Geometria Aritmética no qual nos baseamos.

No 3º Capítulo, caracterizamos os inteiros que são soma de dois quadrados utilizando Geometria Aritmética. Gondim (2011), novamente, é o material no qual nos beseamos. Como aplicação desse resultado, provaremos o seguinte resultado: se houver um número perfeito ímpar então ele será soma de dois quadrados.

# Capítulo 1

# As triplas pitagóricas

Primeiramente, a referência para este capítulo é (Hefez, 2013).

Um problema milenar que consiste de encontrar as soluções da equação pitagórica:

$$X^2 + Y^2 = Z^2,$$

em $\mathbb{Z}$, é conhecido desde a época de Pitágoras e ele próprio apresentou uma classe de soluções:

$$X = \frac{n^2 - 1}{2}$$

$$Y = n$$

$$Z = \frac{n^2 + 1}{2}$$

onde $n > 1$ é ímpar.

Porém, existem soluções que não são dessa forma como, por exemplo, $(8, 15, 17)$.

A equação pitagórica provém do Teorema de Pitágoras. $X$ e $Y$ são catetos e $Z$ é a hipotenusa de um triângulo retângulo.

Quando os lados de um triângulo retângulo são números naturais, dizemos que ele é um Triângulo pitagórico. As únicas soluções inteiras com uma das coordenadas nula, são $(a, 0, \pm a)$ e $(0, b, \pm b)$, com $a, b \in \mathbb{Z}$. E serão chamadas soluções triviais. Como a equação pitagórica é quadrática, basta encontrar as soluções naturais. Será o que faremos.

**Lema 1.1** *Dados dois números naturais $a$ e $b$, coprimos, se $ab$ é um quadrado perfeito, então tanto $a$ quanto $b$ são quadrados perfeitos.*

**Demonstração:**

Suponhamos que $ab = c^2$. Ponhamos $d = mdc(a, c)$. Temos que $a = a_1 d$ e $c = c_1 d$, onde $mdc(a_1, c_1) = 1$.

Daí,

$$a_1 b = c_1^2 d$$

É fácil provar que $mdc(a_1, c_1) = 1 \Rightarrow mdc(a_1, c_1^2) = 1$.

Pelo Lema de Gauss(Se $a|bc$ e $mdc(a, b) = 1$,então $a|c$), $a_1 b = c_1^2 d$ e $mdc(a_1, c_1^2) = 1 \Rightarrow c_1^2 | b$.

Logo, $b = c_1^2 l$ para algum $l \in \mathbb{N}$.

Então $la_1 = d$.

Como $d|a$ e $l|b$, temos que $mdc(d, l)|mdc(a, b)$, mas $mdc(a, b) = 1$, logo, $mdc(d, l) = 1$.

Mas $mdc(d, l) = 1, la_1 = d \Rightarrow d|a_1$, ou seja, $a_1 = \lambda d$. Substituindo, obtemos $\lambda l = 1 \Rightarrow \lambda = 1$ e $l = 1$. Daí, $b = c_1^2$ e $a_1 = d \Rightarrow a = d^2$.

■

**Definição 1.1** *Uma tripla $(a, b, c)$ de números naturais é uma tripla pitagórica se*

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

*Se $mdc(a, b, c) = 1$ então dizemos que $(a, b, c)$ é uma tripla pitagórica primitiva.*

**Observação 1.1** *As triplas pitagóricas primitivas $(a, b, c)$ dão origem a todas as triplas pitagóricas. De fato, se $(a', b', c')$ é uma tripla pitagórica, então $\left(\frac{|a'|}{d}, \frac{|b'|}{d}, \frac{|c'|}{d}\right)$, onde $d = mdc(a', b', c')$, é uma tripla pitagórica primitiva.*

Podemos, portanto, nos concentrar nas triplas primitivas.

O seguinte teorema caracteriza as triplas pitagóricas:

**Teorema 1.1** *As soluções em $\mathbb{N}$ da equação pitagórica $X^2 + Y^2 = Z^2$ expressam-se de modo único, a menos da ordem de $X$ e $Y$, como $X = l(n^2 - m^2), Y = 2lnm, Z = l(n^2 + m^2)$, onde $l, n, m \in \mathbb{N}$, com $m$ e $n$ coprimos e com paridades distintas. Reciprocamente, toda tripla, como acima, é uma tripla pitagórica.*

**Demonstração:**

Seja $(a, b, c)$ uma tripla pitagórica primitiva. Como $a, b, c$ são coprimos e $a^2 + b^2 = c^2$, temos que eles são dois a dois coprimos.

Devemos ter dois números ímpares e $c$ não é par.

Pois, se $a$ e $b$ são ímpares, então $c^2 = 4k+2$ para algum $k \in \mathbb{N}$, o que é impossível.

Vamos supor que $a$ e $c$ são ímpares e $b$ é par.

Temos $a^2 + b^2 = c^2 \Rightarrow c^2 - a^2 = b^2 \Rightarrow \left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right) = \left(\frac{b}{2}\right)^2$.

Como $mdc(a, c) = 1$, então $mdc\left(\frac{c+a}{2}, \frac{c-a}{2}\right) = 1$.

Pelo Lema 1, existem números naturais $n$ e $m$ com $mdc(n, m) = 1$ e paridades distintas, tais que

$$\frac{c+a}{2} = n^2, \frac{c-a}{2} = m^2,$$

ou seja,

$$a = n^2 - m^2, b = 2nm, c = n^2 + m^2. \tag{1.1}$$

Reciprocamente, dados $n, m \in \mathbb{N}$, com $n > m$, $mdc(n, m) = 1$ e de paridades distintas, pondo $a = n^2 - m^2$, $b = 2nm$, $c = n^2 + m^2$, temos que $(a, b, c)$ é uma solução primitiva. De fato, $(n^2 - m^2)^2 + (2nm)^2 = (n^2 + m^2)^2$ e se um primo $p$ divide $b$ então ou $p = 2$ ou $p|n$ ou $p|m$, daí, se $p = 2$ então $p$ não divide nem $a$ nem $c$. Se $p|n$ ou $p|m$ então $p$ não divide nem $a$ nem $c$. Logo, $mdc(a, b, c) = 1$.

As soluções (1.1) são devidas a Euclides e toda solução primitiva é representada de modo único na forma (1.1).

De fato, se $n^2 - m^2 = r^2 - s^2$ e $2nm = 2rs$ e $n^2 + m^2 = r^2 + s^2$ então $n = r$ e $m = s$.

■

Uma solução $(a, b, c)$ determina $n$ e $m$ do seguinte modo:

Se $b$ é par, $b = 2nm$ e $\frac{a+c}{b} = \frac{n}{m}$.

Se $a$ é par, $a = 2nm$ e $\frac{b+c}{a} = \frac{n}{m}$.

Por exemplo, na solução $(20, 21, 29)$, basta calcular

$$\frac{21+29}{20} = \frac{50}{20} = \frac{5}{2},$$

então $n = 5$ e $m = 2$.

Dado um número natural ímpar $a > 1$ é sempre possível escrever $a = a' \cdot a''$, com $mdc(a', a'') = 1, a' < a''$ e resolver o sistema em $m$ e $n$, $n - m = a'$ e $n + m = a''$, determinando dois naturais coprimos $n$ e $m$ e de paridades distintas, com os quais obteremos a tripla pitagórica primitiva $a = n^2 - m^2$, $b = 2nm$, $c = n^2 + m^2$.

Da mesma forma, dado um número natural par $b$, para que ele seja cateto de um triângulo primitivo, $b$ deve ser múltiplo de 4. Escrevendo $b = 2b' \cdot b''$ com $b'$ par e $b''$ ímpar, e $mdc(b', b'') = 1$, tomando $n$ como o maior entre $b'$ e $b''$ e $m$ o menor dos dois, obteremos o triângulo pitagórico $a = n^2 - m^2, b = 2nm, c = n^2 + m^2$.

Logo, dado um número natural maior do que 2, existe sempre um triângulo pitagórico com um dos catetos igual a esse número natural.

Entretanto, nem todo número inteiro pode ser hipotenusa de um triângulo pitagórico. Por exemplo, $7, 9, 11$ ou $49$ não podem ser hipotenusa de um triângulo pitagórico.

## 1.1 Exemplos

1. Se $a, b$ e $c$ são lados de um triângulo pitagórico, onde $c$ é a hipotenusa, então:

   i) $\frac{(c-a)(c-b)}{2}$ e $\frac{(c+a)(c+b)}{2}$ são quadrados perfeitos.

   De fato,consideremos

   $$a = l(n^2 - m^2)$$

   $$b = 2lnm$$

   $$c = l(n^2 + m^2)$$

   onde $l, n, m \in \mathbb{N}$ e calculemos $\frac{(c-a)(c-b)}{2}$ e $\frac{(c+a)(c+b)}{2}$. Temos

   $$\frac{(c-a)(c-b)}{2} = \frac{l^2(2m^2)(n-m)^2}{2} = l^2(m^2)(n-m)^2$$

   $$\frac{(c+a)(c+b)}{2} = \frac{l^2(2n^2)(n+m)^2}{2} = l^2(n^2)(n+m)^2$$

   que são quadrados de números naturais.

   ii) um e somente um dos números $a$ ou $b$ é divisível por 3. De fato, sejam

   $$a = n^2 - m^2$$

   $$b = 2nm$$

   $$c = n^2 + m^2$$

   com $mdc(n, m) = 1$ e $n > m$, com paridades distintas.

   Se 3 divide $n$ ou divide $m$, então $3|b$ e 3 não divide $a$, pois $mdc(a, b) = 1$.

   Se 3 não divide nem $n$ e nem $m$, então 3 não divide $b$, mas $3|a$, pois $n^2 \equiv 1$ e $m^2 \equiv 1 \bmod 3$.

iii) um e somente um dos números $a$ ou $b$ é divisível por 4.

De fato, $b = 2nm$ e $m$,$n$ são de paridades distintas. Logo, $b$ é divisível por 4 e $a$ não é divisível por 4.

iv) um e somente um dos números $a, b$ ou $c$ é divisível por 5.

De fato, se 5 divide $n$ ou 5 divide $m$ então $5|b$. Como $mdc(a, b, c) = 1$, temos que 5 não divide nem $a$ nem $c$. Se 5 não divide nem $n$ nem $m$, então $n^2, m^2 \equiv \pm 1\ mod(5)$, logo, ou $a$ é divisível por 5 e $c$ não, ou $c$ é divisível por 5 e $a$ não.

v) o número $abc$ é múltiplo de 60. O triângulo não é necessariamente primitivo.

De fato, temos que $4|b$. Além disso, ou $a$ ou $b$ é divisível por 3. Também $a$ ou $b$ ou $c$ é divisível por 5. Como $mdc(4, 3, 5) = 1$, vem que $abc$ é divisível por 60.

2. Mostre que existem infinitas triplas pitagóricas $(a, b, c)$ tais que

i) $c$ é um quadrado

De fato, Seja $(a', b', c')$ uma tripla pitagórica, existem infinitas delas. Se multiplicarmos $(a', b', c')$ por $c'$ teremos a tripla pitagórica $(a, b, c)$ onde $c = (c')^2$.

ii) $c - b = 1$

De fato: seja $n = m + 1$. Temos que $c = n^2 + m^2$ e $b = 2mn$. Daí, $c - b = (n - m)^2$.

Portanto, $c - b = 1$.

3. Existem triângulos pitagóricos com área medindo 78? 96?

Para 78, é impossível, pois: Seja $a, b, c \in \mathbb{N}$ tais que $a^2 + b^2 = c^2$ com $b = 4k$, $k \in \mathbb{N}$.

A área do triângulo é $\frac{ab}{2} = 78$ e portanto, $ak = 39$.

Daí, ou $a = 1$ e $k = 39$ ou $a = 3$ e $k = 13$ ou $a = 13$ e $k = 3$ ou $a = 39$ e $k = 1$.

Temos os casos:

i) $a = 1$ e $b = 156$ e $c^2 = 24337$, impossível, pois 24337 não é quadrado perfeito.

ii) $a = 3$ e $b = 52$ e $c^2 = 2713$, impossível, pois 2713 não é quadrado perfeito.

iii) $a = 13$ e $b = 12$ e $c^2 = 313$, impossível, pois 313 não é quadrado perfeito.

iv) $a = 39$ e $b = 4$ e $c^2 = 1537$, impossível, pois 1537 não é quadrado perfeito.

Agora, para 96, fazemos o mesmo procedimento e concluímos que a solução é $a = 12$, $b = 16$ e $c = 20$.

# Capítulo 2

# Geometria Aritmética

A Aritmética é o estudo dos números inteiros. Geometria é o estudo das formas, tais como retas, polígonos e cônicas. Na Grécia Antiga, Pitágoras(500 AC), Arquimedes(300 AC), Euclides(300 AC), Diofanto(250) produziram trabalhos sobre a Aritmética.

Heath (1956) contém a Geometria e a Aritmética básicas daquele tempo.

Com o advento da Geometria Analítica, nos séculos XVII e XVIII, surgiram grandes matemáticos que usaram a Geometria no estudo da Aritmética, tais como Fermat, Euler, Gauss, Lagrange, Legendre.

A Geometria Aritmética possui vários métodos de estudo, em particular, o Método das Tangentes e Secantes de Fermat, o Teorema de Pick, as Curvas Projetivas, o Princípio Local-Global, os Reticulados no $\mathbb{R}^2$, o Toro Plano e o Teorema de Minkowski.

## 2.1 Equações Diofantinas Lineares

As equações diofantinas são equações polinomiais a coeficientes inteiros, onde se busca soluções inteiras.

Uma equação diofantina famosa é a equação do Último Teorema de Fermat, que afirma:

$$x^n + y^n = z^n$$

não tem solução não-trivial em inteiros se o número natural $n$ for maior do que 2.

Andrew Wiles (1995) provou o Último Teorema de Fermat usando muitos métodos de Geometria Aritmética.Ver (S.Singh, 2006).

A equação $x^2 + y^2 = z^2$ tem solução e já provamos isso. Ela surge com Pitágoras e Euclides dá solução a ela.

O exemplo abaixo é um problema de equação diofantina linear.

**Exemplo 2.1 (Euler)** *Um grupo de homens e mulheres gastaram, em uma taverna,* 1000 *patacas. Cada homem gastou* 19 *patacas e cada mulher,* 13*. Quantos eram os homens e quantas eram as mulheres?*

Primeiramente, aplicamos o algoritmo de Euclides para encontrar o MDC:

$$19 = 13 + 6$$

$$13 = 2 \cdot 6 + 1$$

Portanto, MDC(19,13)=1.

Fazendo os cálculos, temos $-2 \cdot 19 + 3 \cdot 13 = 1$.

Multiplicando tudo por 1000, temos $-2000 \cdot 19 + 3000 \cdot 13 = 1000$

Fazendo $x$ para o número de homens e $y$ para o número de mulheres, temos

$$x = -2000 + 13t$$

$$y = 3000 - 19t.$$

Para que $x > 0$ e $y > 0$ ao mesmo tempo, temos: $t = 154$ ou $t = 155$ ou $t = 156$ ou $t = 157$.

Logo, existem quatro respostas possíveis para este problema: 2 homens e 74 mulheres ou 15 homens e 55 mulheres ou 28 homens e 36 mulheres ou 41 homens e 17 mulheres.

Veremos abaixo que uma solução geral para a equação diofantina $19x+13y = 1000$ é

$$x = 2 + 13t$$

e

$$y = 74 - 19t$$

onde $t \in \mathbb{Z}$.

Consideremos o conjunto $\mathbb{Z}^2 \subset \mathbb{R}^2$, ou seja, os pontos inteiros do plano.

Seja $l$ a reta dos pontos $(x, y) \in \mathbb{R}^2$ tais que $bx + cy = a$, onde $a, b, c \in \mathbb{Z}$.

$v = (c, -b)$ é um vetor diretor de $l$.

Se $(x_0, y_0) \in \mathbb{Z}^2$ é um ponto de $l$, então:

$(x_k, y_k) = (x_0 + kc, y_0 - kb)$ está em $l$ para todo $k \in \mathbb{Z}$.

Seja $d = mdc(b, c)$.

Se $d$ não divide $a$ então $l$ não possui ponto inetiro.

Pois: se $(x, y)$ é um ponto inteiro então $d \mid b, d \mid c \Rightarrow d \mid a$.

Se $d \mid a$, então:

$a = d\alpha$

$b = d\beta$

$c = d\gamma$

e temos $\beta x + \gamma y = \alpha$, com $\beta$ e $\gamma$ primos entre si.

**Proposição 2.1** *Seja $l$ a reta dada acima, $bx + cy = a$, com $a, b, c \in \mathbb{Z}$. Suponhamos que a reta $l$ possua um ponto inteiro $(x_0, y_0)$. Seja $w = (\gamma, -\beta)$ o vetor diretor de $l$, com $\beta, \gamma \in \mathbb{Z}$ e $\beta, \gamma$ coprimos. Então todos os pontos inteiros de $l$ são:*

$$(x_k, y_k) = (x_0 + k\gamma, y_0 - k\beta) \tag{2.1}$$

*onde $k \in \mathbb{Z}$.*

**Demonstração:**

$v = (c, -b)$ é um vetor diretor de $l$. Se $d = mdc(b, c)$ então $w = \left(\frac{c}{d}, \frac{-b}{d}\right)$ também é vetor diretor de $l$. Pondo:

$\gamma = \frac{c}{d}$ e $\beta = \frac{b}{d}$,

$\beta$ e $\gamma$ são coprimos e $w = (\gamma, -\beta)$.

Fazendo

$$(x_k, y_k) = (x_0 + k\gamma, y_0 - k\beta) \tag{2.2}$$

onde $k \in \mathbb{Z}$, temos: $bx_k + cy_k = bx_0 + cy_0 + kb\gamma - kc\beta = bx_0 + cy_0 = a$. Logo $(x_k, y_k) \in l$.

Provemos que entre $P_k = (x_k, y_k)$ e $P_{k+1} = (x_{k+1}, y_{k+1})$ não existe outro ponto inteiro de $l$.

$Q$ é um ponto entre $P_k$ e $P_{k+1}$.

E $P_{k+1}I$ e $QJ$ são paralelos ao eixo Oy, $P_kI$ é paralelo ao eixo Ox.

Temos que:

$|P_{k+1}I| = |\beta|$, onde $|P_{k+1}I|$ é o comprimento do segmento $P_{k+1}I$,

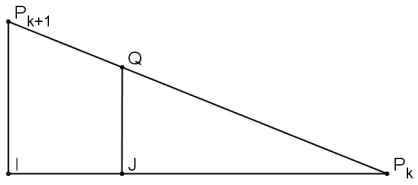


Figura 2.1: Triângulo retângulo paralelo aos eixos.

$|P_kI| = |\gamma|$

Sejam $|P_kJ| = s$ e $|QJ| = t$.

$$\frac{s}{t} = \frac{|\gamma|}{|\beta|}.$$

$s < |\gamma|$ e $t < |\beta|$, mas $s|\beta| = t|\gamma|$.

$mdc(\beta, \gamma) = 1 \Rightarrow \beta \mid t, \gamma \mid s$.Absurdo.

Logo, os únicos pontos inteiros de $l$ são os $P_k$ para $k \in \mathbb{Z}$.

■

**Teorema 2.1 (Algoritmo de Euclides)** *Sejam $b > c > 0$ números inteiros. Então existe um algoritmo efetivo para encontrar o $mdc(b, c)$ a partir de um número finito de sucessivas divisões com resto.*

**Demonstração:**

Fazemos $r_{-1} = b$ e $r_0 = c$.

Temos que $b = cq_0 + r_1$, com $r_1 < c$.

É fácil provar que $mdc(b, c) = mdc(c, r_1)$

Fazendo as mesmas divisões euclidianas, se o resto não for zero, $r_k = r_{k+1}q_{k+1} + r_{k+2}$, com $r_{k+2} < r_{k+1}$ e $mdc(r_k, r_{k+1}) = mdc(r_{k+1}, r_{k+2})$.

Vale que $b > c > r_1 > ... > r_k > r_{k+1} > ....$ Mas todos os restos são maiores do que ou iguais a zero.

Pelo Princípio da Boa Ordem (Qualquer subconjunto não-vazio de $\mathbb{N}$ tem um menor elemento),

$\exists n \in \mathbb{N} | r_{n+1} = 0$.

$mdc(r_{n-1}, r_n) = r_n$.

Logo, $mdc(b, c) = r_n$.

■

**Teorema 2.2 (Algoritmo estendido de Euclides e Lema de Bèzout)** *Sejam $b$ e $c$ inteiros tais que $b > c > 0$ e $mdc(b, c) = d$. Então existem $x, y \in \mathbb{Z}$ tais que $bx + cy = d$.*

**Demonstração:**

Depois de realizar o Algoritmo de Euclides com $b$ e $c$, obtemos os $r_k$ e os $q_k$.

Para $k = -1$,temos $x_{-1} = 1$ e $y_{-1} = 0$, donde $b \cdot 1 + c \cdot 0 = r_{-1} = b$.

Para $k = 0$, temos $x_0 = 0$ e $y_0 = 1$, donde $b \cdot 0 + c \cdot 1 = r_0 = c$.

Suponhamos $k > 0$. E

$bx_{k-2} + cy_{k-2} = r_{k-2}$ $bx_{k-1} + cx_{k-1} = r_{k-1}$.

Como $r_{k-2} = r_{k-1}q_k + r_k$, vem que:

$r_k = b(x_{k-2} - q_k x_{k-1}) + c(y_{k-2} - q_k y_{k-1})$

E assim, por recorrência, obtemos os $x_k$ e os $y_k$.

O Algoritmo para quando $r_{n+1} = 0$.

Logo $d = mdc(b, c) = r_n = bx_n + cy_n$. ■

**Teorema 2.3 (Euclides)** *Sejam $a, b, c \in \mathbb{Z}$ , a equação diofantina $bx + cy = a$, e $d = mdc(b, c)$.*

*Se $d$ não divide $a$ então não há solução para a equação em $x$ e $y$ inteiros.*

*Se $d \mid a$ então há pelo menos uma solução $(x_0, y_0) \in \mathbb{Z}^2$ e todas as soluções são:*

$$(x_k, y_k) = (x_0 + \gamma k, y_0 - \beta k) \tag{2.3}$$

*Onde $\beta = \dfrac{b}{d}$ e $\gamma = \dfrac{c}{d}$ são coprimos.*

**Demonstração:** Se $d$ não divide $a$ então foi provado que $bx + cy = a$ não tem solução em $(x, y)$ inteiros. Se $d|a$ então pelo Teorema 2.2, podemos encontrar $(x_0, y_0)$ e pela Proposição 2.1, vem a tese. ■

## 2.2 Áreas e Teorema de Pick

Seja $ABCD$ um paralelogramo com vértices em $\mathbb{Z}^2$.

Sejam $v = \overrightarrow{AB}$ e $w = \overrightarrow{AC}$.

Consideremos $v = (a, b)$ e $w = (c, d)$.

No $\mathbb{R}^3$, $v = (a, b, 0)$ e $w = (c, d, 0)$.

Pois podemos identificar $\mathbb{R}^2 \cong \{(x, y, z) \in \mathbb{R}^3 | z = 0\}$.

Temos que $v \times w = (0, 0, ad - bc)$ é o produto vetorial.

Ou seja, $|v \times w| = |det(v, w)|$ é o determinante de uma matriz que tem colunas $v$ e $w$.

Sabemos que a área de $ABCD$ é $A = |det(v, w)| = |v \times w|$.

Seja $v = (a, b) \in \mathbb{Z}^2$ e $d = mdc(a, b)$.

**Definição 2.1** $\Delta(v) = \{det(v, w) | w \in \mathbb{Z}^2\}$ *é o conjunto das áreas algébricas de paralelogramos com uma das bases sendo o vetor* $v$ *.*

**Teorema 2.4** *:* $\Delta(v) = d\mathbb{Z}$ *é o conjunto dos múltiplos de* $d$*.*

**Demonstração:** $\Delta(v) = \{ax + by | x, y \in \mathbb{Z}\}$, pois $v = (a, b)$

$\exists (x_0, y_0) \in \mathbb{Z}^2 | ax_0 + by_0 = d$ (Bèzout).

$z \in \Delta(v) \Rightarrow d \mid z$.

$d \mid z \Rightarrow (ax_0 + by_0)q = z \Rightarrow z \in \Delta(v)$.

Logo, $\Delta(v) = d\mathbb{Z}$.

■

Introduziremos agora o teorema de Pick, que é um interessante resultado que calcula a área de um polígono de vértices inteiros , a partir de uma contagem dos pontos de coordenadas inteiras no interior e na fronteira do polígono.

**Definição 2.2** *: Um polígono plano é simples se não possui "furos"e se suas arestas só se intersectam nos vértices.*

**Teorema 2.5 (Pick)** *Seja* $\mathcal{P} \subset \mathbb{R}^2$ *um polígono simples cujos vértices pertencem a* $\mathbb{Z}^2$*. Defina* $F$ *o número de pontos inteiros na fronteira de* $\mathcal{P}$ *(vértices e arestas) e* $I$ *o número de pontos inteiros no interior de* $\mathcal{P}$*. Então a área do polígono* $\mathcal{P}$ *é*

$$A(P) = \frac{1}{2}F + I - 1 \tag{2.4}$$

Antes de apresentar a demonstração deste teorema, vamos apresentar alguns exemplos como ilustração. Considere o triângulo descrito na figura a seguir.

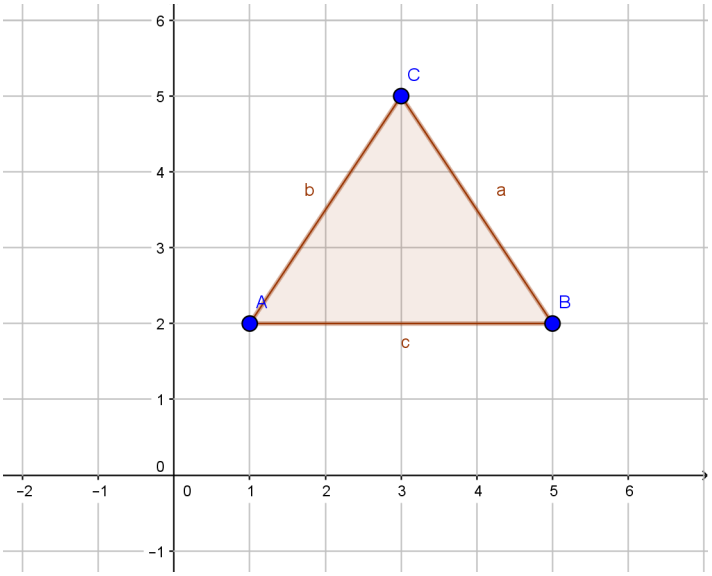


Figura 2.2: Exemplo do teorema de Pick, num triângulo.

A área deste triângulo é 6, usando a geometria que conhecemos desde o colégio. Pela Fórmula de Pick, $A = \frac{1}{2}F + I - 1 = \frac{1}{2}6 + 4 - 1 = 6$.

Agora vamos considerar um trapézio conforme a figura:

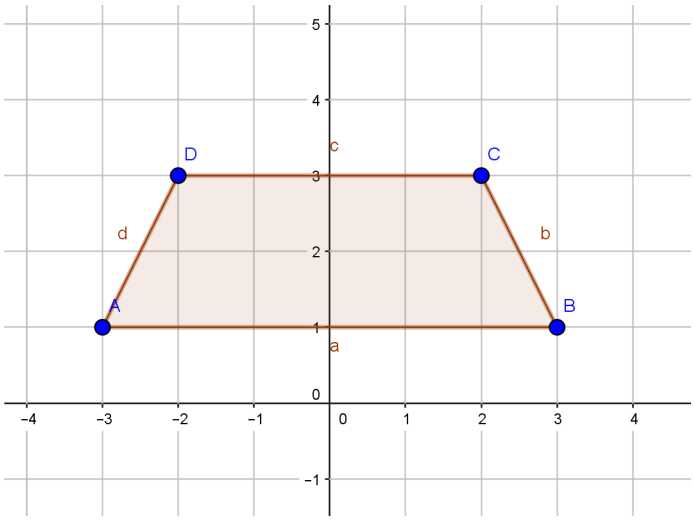


Figura 2.3: Exemplo do teorema de Pick, num trapézio.

A área do trapézio é $\frac{1}{2}(4+6)\cdot 2 = 10$. Usando a fórmula de Pick, temos $A = \frac{1}{2}\cdot 12 + 5 - 1 = 10$.

Iremos agora demonstrar o Teorema de Pick.

**Demonstração:**

Definamos $Pick(P) = \frac{1}{2}F + I - 1$ como sendo o número de Pick associado ao polígono simples $\mathcal{P}$.

Consideremos dois polígonos simples $P_1$ e $P_2$ com vértices em $\mathbb{Z}^2$ que estão concatenados, isto é, $P_1$ e $P_2$ têm uma aresta em comum como na figura abaixo:

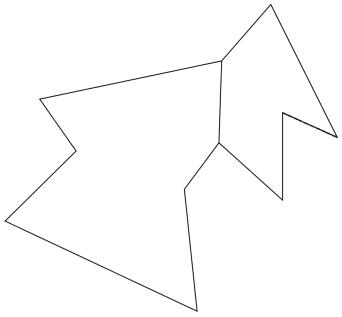

Figura 2.4: teorema de Pick e concatenações

Dizemos que $P = P_1 \oplus P_2$ é a concatenação de $P_1$ e $P_2$.

Provemos que $Pick(P) = Pick(P_1) + Pick(P_2)$

Consideremos que a aresta comum a $P_1$ e $P_2$ tem $k+2$ pontos inteiros, onde $k$ são interiores a aresta.

Sejam $I, I_1, I_2$ o número dos pontos inteiros interiores a $P, P_1, P_2$, respectivamente.

Sejam $F, F_1, F_2$ o número dos pontos inteiros da fronteira de $P, P_1, P_2$, respectivamente.

Temos que

$$I = I_1 + I_2 + k$$

e

$$F = F_1 + F_2 - 2(k+2) + 2.$$

Então:

$$Pick(P) = \frac{1}{2}(F_1 + F_2 - 2(k+2) + 2) + I_1 + I_2 + k - 1 =$$

$$= \frac{1}{2}F_1 + I_1 - 1 + \frac{1}{2}F_2 + I_2 - 1 = Pick(P_1) + Pick(P_2).$$

Agora, todo polígono simples com vértices inteiros pode ser dividido em triângulos cujos vértices são vértices do polígono.

Um triângulo qualquer com vértices inteiros pode ser inserido num retângulo horizontal de vértices inteiros. O triângulo está contido nesse retângulo horizontal e podemos dividir o retângulo em triângulos retângulos com bases paralelas aos eixos conjuntamente ao triângulo em questão.

Daí a área de um triângulo com bases paralelas aos eixos será a metade de um retângulo formado por quadrados $1 \times 1$.

Se a fórmula de Pick vale num quadrado $1 \times 1$, então por concatenação, vale no retângulo, e no triângulo, e no polígono.

Mas no quadrado $1 \times 1$, temos que $A = 1$,$F = 4$,$I = 0$.
Então, $1 = \frac{1}{2}4 + 0 - 1 \Rightarrow A = \frac{1}{2}F + I - 1$.
Logo, o Teorema de Pick é verdadeiro. ■

**Observação 2.1** *Podemos olhar para a Fórmula de Pick de outra forma:* $I = A - \frac{1}{2}F + 1$, *ou seja, a partir da área e dos pontos na fronteira, podemos calcular o número de pontos inteiros interiores.*

**Proposição 2.2** *: Seja* $\mathcal{P} = A_0A_1A_2...A_{n-1}A_n$, *com* $A_0 = A_n$, *um polígono simples no plano com vértices inteiros. Defina* $v_i = \overrightarrow{A_{i-1}A_i} = (a_i, b_i)$ *e* $d_i = mdc(a_i, b_i)$. *Então o número de pontos inteiros na fronteira de* $\mathcal{P}$ *é igual a*

$$F = \sum_{i=1}^{n} d_i$$

.

**Demonstração:**
Pela Proposição 1 acima demonstrada, temos que se $P, Q$ são pontos inteiros e $v = \overrightarrow{PQ} = (a, b)$ com $mdc(a, b) = 1$ então os únicos pontos inteiros do segmento $PQ$ são $P$ e $Q$.

Mas se $d = mdc(a, b) > 1$ então $PQ$ tem $d + 1$ pontos inteiros, pois pode ser dividido em $d$ segmentos iguais cada um com a propriedade de que as coordenadas do vetor são coprimas, onde só os extremos são inteiros.

Logo, no interior de $A_{i-1}A_i$, há $d_i - 1$ pontos inteiros.
Ou seja, $F = \sum_{i=1}^{n} d_i - n + n = \sum_{i=1}^{n} d_i$. ■

## 2.3 Método das Tangentes e Secantes de Fermat

Uma curva algébrica plana em $\mathbb{R}^2$ é um conjunto da forma:

$$C = \{(x, y) \in \mathbb{R}^2 | f(x, y) = 0\}$$

onde $f(x, y)$ é um polinômio com coeficientes reais.

Uma cônica é uma curva algébrica plana cujo polinômio possui grau 2.

Se ela for um conjunto vazio ou um conjunto de um número finito de pontos, ela é uma cônica degenerada.

As formas canônicas, com coeficientes inteiros, das cônicas são as seguintes:

1. Parábola: $C = \{(x, y) \in \mathbb{R}^2 | ax^2 + by = 0\}$ com $a, b \in \mathbb{Z}$ e $a, b \neq 0$.

2. Hipérbole: $C = \{(x, y) \in \mathbb{R}^2 | ax^2 - by^2 = c\}$ com $a, b, c \in \mathbb{Z}$ e $a, b, c > 0$.

3. Elipse: $C = \{(x, y) \in \mathbb{R}^2 | ax^2 + by^2 = c\}$ com $a, b, c \in \mathbb{Z}$ e $a, b, c > 0$.

4. Círculo: $C = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = c\}$ com $c \in \mathbb{Z}$ e $c > 0$, quando na elipse $a = b$.

**Proposição 2.3 (Método das Tangentes e Secantes de Fermat)** *Sejam $C$ uma cônica, $P \in C$, e $l$ uma reta que não passa por $P = P_1$. Seja $\overline{l}$ a reta paralela a $l$ passando por $P$ e $C \cap \overline{l} = \{P_1, P_2\}$ ( não necessariamente distintos). Defina, ainda, $\overline{P} = T_P C \cap l$. Temos a função:*

$$\begin{aligned} \varphi : \ C - \{P_1, P_2\} &\longrightarrow \quad l - \{\overline{P}\} \\ Q \quad &\longmapsto \ R(Q) = PQ \cap l \end{aligned}$$

*$\varphi$ é bijetiva e*

$$\begin{aligned} \varphi^{-1} : \ l - \{\overline{P}\} &\longrightarrow \quad C - \{P_1, P_2\} \\ R \quad &\longmapsto \ Q(R) = PR \cap C \end{aligned}$$

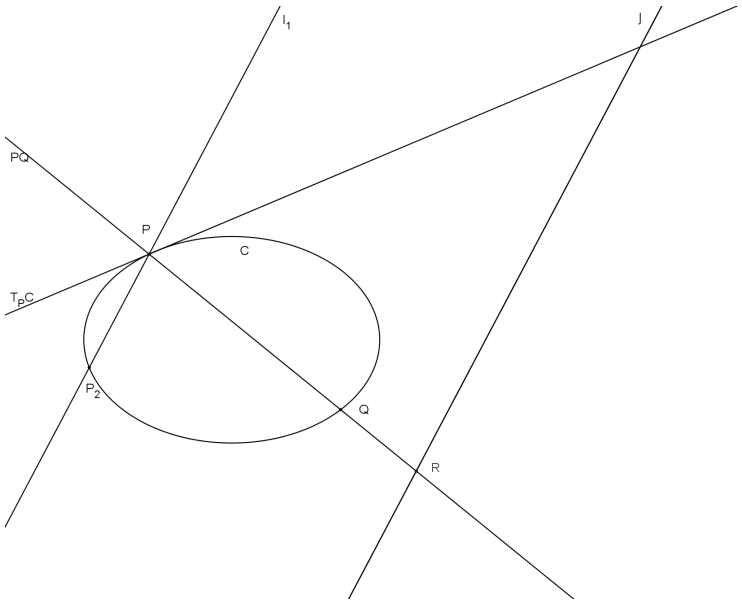


Figura 2.5: Secantes e tangentes.

**Demonstração:** De fato, para cada $Q \in C - \{P_1, P_2\}$, a reta $PQ$ não é paralela a $l$ (a única paralela a $l$ passando por $P$ é $P_1P_2$) Assim a intersecção $PQ \cap l = R(Q) = R$ define o ponto $R(Q)$. E para que $\varphi^{-1}$ pudesse ser definida, tivermos que excluir o ponto $\overline{P}$, caso contrário, a reta $P\overline{P}$ seria tangente a $C$. ■

**Teorema 2.6** *: Sejam $C \subset \mathbb{R}^2$ uma cônica com coeficientes racionais e $P \in C$ um ponto racional. Considere $l \subset \mathbb{R}^2$ uma reta com coeficientes racionais paralela a $T_PC$ (não coincidente). Então a função*

$$\begin{array}{rccc} \varphi: & C - \{P\} & \longrightarrow & l \\ & Q & \longmapsto & R(Q) = PQ \cap l \end{array}$$

*está bem definida, é bijetiva e leva pontos racionais de $C$ em pontos racionais de $l$.*

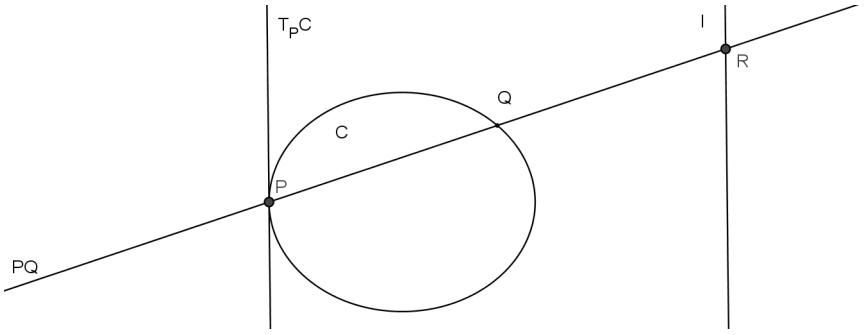


Figura 2.6: Tangente.

**Demonstração:** É fácil provar que $\varphi$ está bem definida e que é bijetora, como na Proposição anterior.

Como $P$ é um ponto racional, se $Q$ é racional então a reta $PQ$ tem coeficientes racionais. Mas $l$ tem coeficientes racionais, logo, $R(Q)$ é racional.

Se $R(Q) = R$ é racional, a reta $PR$ é do tipo $y = mx + n$ com $m, n \in \mathbb{Q}$ e $Q \in C \cap PR$.

Mas $C$ é do tipo $ax^2 + by^2 = c$ com $a, b, c \in \mathbb{Q}$.

Então $x_P$ e $x_Q$ são soluções de uma equação $\alpha x^2 + \beta x + \gamma = 0$, com $\alpha, \beta, \gamma \in \mathbb{Q}$.

Mas $P$ é racional. Logo, $Q$ é racional. ■

**Corolário 2.1** *: Se uma cônica com coeficientes racionais possui pelo menos um ponto racional, então possui infinitos pontos racionais.*

**Demonstração:** Teorema anterior.

**Exemplo 2.2** *Sejam* $C = \{(x, y) \in \mathbb{R} | x^2 + y^2 = 1\}$, $P = (-1, 0)$ *e* $l = \{(0, t) | t \in \mathbb{R}\}$. *Vamos parametrizar a circunferência com o parâmetro* $t$. *Seja*

$$\begin{aligned} \varphi : \ C - \{P\} &\longrightarrow \quad l \\ Q \quad &\longmapsto \ R(Q) = PQ \cap l \end{aligned}$$

*onde* $T_P C$ *é a reta* $x = -1$.

*Temos que* $\dfrac{y}{x+1} = t$.

*Portanto* $\varphi(x, y) = \left(0, \dfrac{y}{x+1}\right)$.

*Mas* $y = t(x + 1)$ *e* $x^2 + y^2 = 1$ *nos dá* $x^2 + t^2(x + 1)^2 = 1$, *ou seja,*

$$(1 + t^2)x^2 + 2t^2x + t^2 - 1 = 0.$$

*Como* $x = -1$ *é uma solução da equação e o produto das soluções é* $\dfrac{t^2-1}{1+t^2}$, *temos que a outra solução é* $x = \dfrac{1-t^2}{1+t^2}$.

*Daí,* $y = t(x + 1) \Rightarrow y = t(\dfrac{2}{1+t^2}) \Rightarrow y = \dfrac{2t}{1+t^2}$.

*e a parametrização fica:* $\varphi^{-1}(t) = \left(\dfrac{1-t^2}{1+t^2}, \dfrac{2t}{1+t^2}\right)$.

**Exemplo 2.3** *:* $C : x^2 + y^2 = 2$, $P = (1, 1)$, $l_t : y - 1 = t(x - 1)$.

*Temos que* $y = 1 + t(x - 1)$.

*De* $x^2 + y^2 = 2$ *vem que* $x^2 + [1 + t(x - 1)]^2 = 2$.

*Daí,* $x^2+1+2t(x-1)+t^2(x-1)^2-2 = 0 \Rightarrow (1+t^2)x^2+(2t-2t^2)x+(t^2-2t-1) = 0$.

$x = 1$ *é solução da equação quadrática acima.*

*O produto das soluções é* $\dfrac{t^2-2t-1}{1+t^2}$.

*Logo,* $x_t = \dfrac{t^2-2t-1}{1+t^2}$.

*E* $y_t = 1 + t(x - 1) = 1 + t\left(\dfrac{-2t-2}{1+t^2}\right) = \dfrac{-t^2-2t+1}{1+t^2}$.

*Portanto, a parametrização da circunferência fica:*

$t \longmapsto \left(\dfrac{t^2-2t-1}{1+t^2}, \dfrac{-t^2-2t+1}{1+t^2}\right)$.

**Teorema 2.7** *Seja* $C \subset \mathbb{R}^2$ *a cônica de equação* $ax^2 + by^2 = c$ *com* $a, b, c \in \mathbb{Q}$. *Se* $P_0 = (x_0, y_0)$ *é um ponto racional de* $C$, *então todos os outros pontos racionais de* $C$ *são da forma*

$$\left(\frac{bt^2x_0 - 2bty_0 - ax_0}{bt^2 + a}, \frac{-bt^2y_0 - 2atx_0 + ay_0}{bt^2 + a}\right) \tag{2.5}$$

*em que* $t \in \mathbb{Q}$, $bt^2 + a \neq 0$, *exceto* $(x_0, -y_0)$. *Ou seja, o conjunto dos pontos racionais de* $C$ *pode ser parametrizado a partir de* $P_0$.

**Demonstração:** Vamos parametrizar usando a reta $l_t : y - y_0 = t(x - x_0)$ para cada $t$ nas condições dadas.

Então $y = y_0 + t(x - x_0)$ e $ax^2 + by^2 = c$.

Obteremos a equação em $x$:

$$(a + bt^2)x^2 + (-2bt^2x_0 + 2bty_0)x + (bt^2x_0^2 - 2btx_0y_0 - ax_0^2) = 0$$

. Temos que $x_0$ é uma solução e a outra é $x_t$.

Logo, $x_0x_t = x_0\dfrac{bt^2x_0 - 2bty_0 - ax_0}{bt^2 + a} \Rightarrow x_t = \dfrac{bt^2x_0 - 2bty_0 - ax_0}{bt^2 + a}$.

Agora, $y_t = y_0 + t(x_t - x_0) \Rightarrow y_t = \dfrac{-bt^2y_0 - 2atx_0 + ay_0}{bt^2 + a}$.

Pelo Método das Secantes e Tangentes de Fermat, vem a tese. ■

## 2.4 Homogeneização e Desomogeneização: Curvas Projetivas

**Definição 2.3** *Um polinômio* $F$ *em mais de uma variável é homogêneo se todos os seus monômios são de mesmo grau, digamos,* $n$.

$F(\lambda P) = \lambda^n F(P)$ *e se* $\lambda \neq 0$ *então* $F(P) = 0 \Leftrightarrow F(\lambda P) = 0$.

**Definição 2.4** *A relação de equivalência em* $\mathbb{R}^3 - \{0\}$*:* $v \equiv w \Leftrightarrow v = \lambda w, \lambda \neq 0$ *é necessária para definir plano projetivo.*

**Definição 2.5** *O plano projetivo* $\mathbb{P}^2(\mathbb{R})$ *é definido pelo quociente de* $\mathbb{R}^3$ *pela relação de equivalência acima.*

*Se a classe de* $v = (X, Y, Z)$ *possui* $Z \neq 0$, *então* $(X, Y, Z) \equiv (x, y, 1)$, *caso contrário, dizemos que* $v$ *representa um ponto no infinito.*

*Assim,* $\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup l_\infty$. *Onde* $l_\infty$ *representa a "reta no infinito", ou seja,* $\mathbb{P}^1(\mathbb{R})$.

Se $f(x, y)$ é um polinômio de duas variáveis de grau $n$, então podemos obter um polinômio homogêneo $F(X, Y, Z)$ fazendo $x = \dfrac{X}{Z}$ e $y = \dfrac{Y}{Z}$ e cancelando os denominadores, considerando $F(X, Y, Z) = 0$.

**Definição 2.6** *Seja $f(x, y)$ um polinômio com coeficientes reais e $C \subset \mathbb{R}^2$ a curva associada. O polinômio homogêneo $F$, associado a $f$, é chamado homogeneização de $f$ onde $\overline{C} = \{(x : y : z) \in \mathbb{P}^2; F(x : y : z) = 0\}$ é a curva projetiva associada.*

**Proposição 2.4** *Seja $f(x, y)$ um polinômio com coeficientes racionais e $F(X, Y, Z)$ a homogeneização de $f$. Existe uma bijeção entre as soluções racionais de $f$ e as soluções inteiras, sem fator comum e com $Z \neq 0$ de $F$ (a menos de sinal).*

**Demonstração:** Consideremos $(x, y)$ uma solução racional de $f(x, y) = 0$ e multipliquemos $(x, y, 1)$ pelo mmc das frações $x$ e $y$, irredutíveis. Obteremos $(X, Y, Z)$ que, a menos de sinal, é uma solução em inteiros coprimos de $F(X, Y, Z)$.

Reciprocamente, se $F(X, Y, Z)$ é um polinômio homogêneo em três variáveis, fazemos $X = xZ$ e $Y = yZ$ e cancelamos $Z^n$. Para cada solução em inteiros de $F(X, Y, Z) = 0$ com $Z \neq 0$, obtemos uma solução racional de $f(x, y)$. ■

**Exemplo 2.4** *Consideremos a circunferência $x^2 + y^2 = 3$. Veremos que ela não possui ponto racional.*
*Homogeneizando, temos $X^2 + Y^2 = 3Z^2$ com $X, Y, Z$ dois a dois primos entre si.*
*Sejam*

$$X \equiv a$$

$$Y \equiv b$$

$$Z \equiv c$$

*módulo* 3.
$a^2 + b^2 \equiv 0 \ mod\ 3$.
*Se* $3|a$ *mas* 3 *não divide* $b$ *então* $a^2 + b^2 \equiv 1$, *absurdo.*
*Idem se* 3 *não divide* $a$ *e* $3|b$.
*Se* 3 *não divivir nem* $a$ *nem* $b$, *então* $a^2 \equiv b^2 \equiv 1$, *o que é absurdo.*
*Logo,* $a \equiv b \equiv 0 \ mod\ 3$.
*Dessa forma:*

$$X = 3m$$

$$Y = 3n$$

*Portanto,* $9m^2 + 9n^2 = 3Z^2$. *Ou seja,* $Z^2 = 3m^2 + 3n^2$. *Logo,* $3|Z$, *absurdo.*

**Exemplo 2.5 (Curva Elíptica)** *Uma curva elíptica pode ser dada pela equação*

$$y^2 = x^3 - n^2 x, n \in \mathbb{N}.$$

*Sua homogeneização é obtida por* $x = \frac{X}{Z}$ *e* $y = \frac{Y}{Z}$ *onde*

$$\left(\frac{Y}{Z}\right)^2 = \left(\frac{X}{Z}\right)^3 - n^2 \left(\frac{X}{Z}\right)$$

*ou seja,*

$$Y^2 Z = X^3 - n^2 X Z^2$$

*Temos que* $(0:1:0)$ *é um ponto no infinito da curva projetiva.*

Finalizamos essa seção enunciando, sem demonstração, um importante resultado devido a Hasse e a Minkowski que caracteriza quando uma cônica possui um ponto racional, chamado de Princípio Local-Global para cônicas, que se encontra em (Gondim, 2011):

**Teorema 2.8 (Hasse-Minkowski)** *Seja* $C \subset \mathbb{R}^2$ *uma cônica com coeficientes racionais e* $\overline{C} \subset \mathbb{P}^2$ *a curva projetiva associada (com coeficientes inteiros). Uma condição necessária e suficiente para a existência de um ponto racional em* $C$ *é que sua equação homogênea possua solução módulo* $p^e$ *para todo natural primo* $\mathbf{p}$ *e para cada* $\mathbf{e} > \mathbf{0}$.

**Exemplo 2.6** *Consideremos uma curva dada por*

$$x^2 + 3x^2 y + 6xy + 1 = 0.$$

*Usemos* $p = 3$ *e o anel* $\mathbb{Z}_3$.
*Temos:*

- *Se* $x \equiv 0 \ mod\ 3$ *então* $x^2 + 3x^2 y + 6xy + 1 \equiv 1 \ mod\ 3$.
- *Se* $x \equiv 1 \ mod\ 3$ *então* $x^2 + 3x^2 y + 6xy + 1 \equiv 2 \ mod\ 3$.
- *Se* $x \equiv 2 \ mod\ 3$ *então* $x^2 + 3x^2 y + 6xy + 1 \equiv 2 \ mod\ 3$.

*Logo, pelo Teorema de Hasse-Minkowski acima, a curva dada não possui ponto racional.*

## 2.5 Reticulados no Plano

**Definição 2.7** *: Sejam $v_1, v_2 \in \mathbb{R}^2$ dois vetores linearmente independentes.*

$L = \{m_1v_1 + m_2v_2 | m_1, m_2 \in \mathbb{Z}\}$ *é chamado um reticulado no plano* $\mathbb{R}^2$.

$D = \{a_1v_1 + a_2v_2 | 0 \leq a_1, a_2 < 1\}$ *é chamado um domínio fundamental para* $L$.

**Lema 2.1** *$L$ é um subgrupo aditivo de $\mathbb{R}^2$.*

*A prova disso é imediata. Encontra-se em (Gondim, 2011).*

**Definição 2.8** *$X \subset \mathbb{R}^2$ é discreto se todos os seus pontos são isolados, isto é*

$$\forall p \in X, \exists \delta > 0 | D(p, \delta) \cap X = \{p\}$$

**Lema 2.2** *Os subgrupos aditivos discretos de $\mathbb{R}$ são isomorfos a $\mathbb{Z}$.*

**Demonstração:** Seja $G$ tal subgrupo. Suponhamos que $G \neq \{0\}$.

$\exists m > 0$ menor elemento positivo de $G$, pois $G$ é discreto.

Portanto, $m\mathbb{Z} \subset G$.

Seja $g \in G$ qualquer. Se $g \notin m\mathbb{Z}$ então $\exists x \in \mathbb{Z} | mx < g < m(x + 1)$.

Daí, $0 < g - mx < m$. Mas $g - mx \in G$. Absurdo. Logo, $G = m\mathbb{Z}$.

A referência usada é (Gondim, 2011). ■

**Observação 2.2** *Os subgrupos aditivos de $\mathbb{R}$ que não são discretos são bem mais complicados. Por exemplo, $\mathbb{Q} \subset \mathbb{R}$ é subgrupo aditivo e é denso.*

**Proposição 2.5** *Seja $G \subset \mathbb{R}^2$ um subgrupo aditivo. Então são equivalentes:*

1. *$G$ é um reticulado*

2. *$G \subset \mathbb{R}^2$ é discreto*

**Demonstração:** $G$ é um reticulado $\Rightarrow$ $G$ é discreto:

Seja $G = \{av + bw | a, b \in \mathbb{Z}\}$ onde $v, w \in \mathbb{R}^2$ não são múltiplos.

Provemos que $O \in G$ é ponto isolado.

Tomemos $\delta = \frac{1}{2} min\{\|v\|, \|w\|, \|v + w\|\}$.

Onde $||v||$ é a norma euclidiana de $v$, isto é, se $v = (x, y)$ então $||v|| = \sqrt{(x^2 + y^2)}$.

$0 \in D(0, \delta)$ e $D(0, \delta) \cap G = \{0\}$.

Reciprocamente, provemos que $G$ é discreto $\Rightarrow$ $G$ é um reticulado.

Seja $v \in G$ o vetor não-nulo de menor norma (euclidiana).

Seja $w \in G$ o ponto mais próximo da reta $l = \{\lambda v | \lambda \in \mathbb{R}\}$ (não contido na reta).

Afirmamos que $G = \{av + bw | a, b \in \mathbb{Z}\}$.

Seja $u \in G$ e consideremos os pontos $u - mw \in G$ tal que $m \in \mathbb{Z}$.

Tomemos as retas paralelas a $l$ que contêm $mw$ para cada $m \in \mathbb{Z}$.

Se $u$ não estiver em nenhuma dessas retas, existirá $m \in \mathbb{Z}$ tal que $u - mw$ estará entre $l$ e a reta paralela a $l$ que passa por $w$.

Daí, $u - mw$ é mais próximo de $l$ que $w$. Contradição.

Logo, $u - mw \in l$. E $G$ é um reticulado. ■

**Exemplo 2.7** *Consideremos $L = \mathbb{Z}^2 \subset \mathbb{R}^2$ o reticulado padrão.*

$$B_1 = \{(1,0), (0,1)\}$$

$$B_2 = \{(2,1), (1,1)\}$$

*são conjuntos de geradores de $L$.*

$$(2,1) = 2(1,0) + 1(0,1)$$

$$(1,1) = 1(1,0) + 1(0,1)$$

*e*

$$(1,0) = 1(2,1) - 1(1,1)$$

$$(0,1) = -1(2,1) + 2(1,1)$$

*Logo, o reticulado é o mesmo, $L$.*

**Proposição 2.6** *Seja $L \subset \mathbb{R}^2$ um reticulado. Sejam $D$ e $E$ domínios fundamentais para $L$ tais que:*
*O domínio $D$ é gerado por $\{v_1, v_2\}$ e o domínio $E$ é gerado por $\{u_1, u_2\}$.*
*Então $A(D) = A(E)$.*

**Demonstração:**

$$u_1 = a_1 v_1 + a_2 v_2$$

$$u_2 = b_1 v_1 + b_2 v_2$$

A matriz mudança de base é:

$$M = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$$

Seja $N$ a outra matriz mudança de base.

Temos que $M \cdot N = I_2$.

Então: $det(M)det(N) = 1 \Rightarrow det(M) = \pm 1$.

Daí: $A(E) = \|u_1 \times u_2\| = |det(u_1, u_2)| = |det(a_1v_1 + a_2v_2, b_1v_1 + b_2v_2)| = |det(M)|A(D) = A(D)$.

Pois

$$det(a_1v_1 + a_2v_2, b_1v_1 + b_2v_2) =$$

$$det(a_1v_1, b_1v_1) + det(a_1v_1, b_2v_2) + det(a_2v_2, b_1v_1) + det(a_2v_2, b_2v_2) =$$

$$a_1b_2det(v_1, v_2) - b_1a_2det(v_1, v_2) =$$

$$(a_1b_2 - b_1a_2)det(v_1, v_2)$$

■

## 2.6 O Toro plano

**Definição 2.9** *Seja $L \subset \mathbb{R}^2$ um reticulado plano.*
*$\mathbb{R}^2/L$ é o quociente do grupo aditivo $\mathbb{R}^2$ pelo subgrupo abeliano $L$.*
*$\mathbb{R}^2/L$ é chamado de toro plano.*

**Definição 2.10** *Seja $S^1 = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 = 1\}$ o círculo unitário, munido de sua estrutura de grupo multiplicativo. $T = S^1 \times S^1$ é chamado de toro em $\mathbb{R}^3$.*

Consideremos a função:

$$\begin{array}{rccc} \varphi: & \mathbb{R}^2 & \longrightarrow & T = S^1 \times S^1 \\ & (a_1v_1 + a_2v_2) & \longmapsto & (e^{2\pi i a_1}, e^{2\pi i a_2}) \end{array}$$

Afirmação:

i) $\varphi$ é um homomorfismo de grupos.

ii) $Ker(\varphi) = L = \{a_1v_1 + a_2v_2 | a_1, a_2 \in \mathbb{Z}\}$.

iii) $\mathbb{R}^2/L \cong T$.

Justificativa:

$\varphi((a_1+b_1)v_1+(a_2+b_2)v_2) = (e^{2\pi i(a_1+b_1)}, e^{2\pi i(a_2+b_2)}) =$

$$= (e^{2\pi i a_1}, e^{2\pi i a_2}) \cdot (e^{2\pi i b_1}, e^{2\pi i b_2}) =$$

$$= \varphi(a_1v_1+a_2v_2)\varphi(b_1v_1+b_2v_2)$$

$\varphi(a_1v_1+a_2v_2) = (1,1)$ se, e somente se, $a_1, a_2 \in \mathbb{Z}$ se,e somente se, $a_1v_1+a_2v_2 \in L$.

$\varphi$ é sobrejetora, pois dado $(z,w) \in S^1 \times S^1$, temos $|z| = 1$ e $|w| = 1$, logo $z = e^{2\pi ix}$ e $w = e^{2\pi iy}$ com $x, y \in \mathbb{R}$.

Então pelo Teorema do isomorfismo, ver(Gonçalves, 1995) nas páginas 144 e 145, temos $\mathbb{R}^2/L \cong T$.

■

**Definição 2.11** *Seja $L$ um reticulado plano, $X \subset T \cong \mathbb{R}^2/L$ uma região do toro e $D$ domínio fundamental para $L$. Definimos a área de $X$ como*

$$A(X) = A(\varphi|_D^{-1}(X))$$

**Proposição 2.7** *Se $Y \subset \mathbb{R}^2$ é limitada e existe $A(Y)$ e se $A(\varphi(Y)) \neq A(Y)$ então $\varphi|_Y$ não é injetiva.*

**Demonstração:**

Provemos que se $\varphi|_Y$ é injetiva então $A(\varphi(Y)) = A(Y)$.

Temos que $Y = \bigcup Y_i$ onde $Y_i = Y \cap (D + w_i)$ são disjuntos. Fazendo $Z_i = Y_i - w_i \subset D$, eles são disjuntos, pela injetividade de $\varphi|_Y$, logo:

$$A(\varphi(Y)) = A(\varphi(\bigcup Y_i)) = A(\varphi(\bigcup Z_i)) = \sum A(Z_i) = \sum A(Y_i) = A(Y).$$

■

**Proposição 2.8** *Dados um reticulado $L \subset \mathbb{Z}^2$ e $D$ um domínio fundamental para $L$.*

*Então $A(D) = |\mathbb{Z}^2/L|$ que corresponde ao número de pontos inteiros em um domínio fundamental.*

**Demonstração:** Temos que $\mathbb{Z}^2/L \cong D$, pois dois pontos do plano $\mathbb{Z}^2$ são congruentes mod $L$ se e somente se sua diferença está em $L$. Cada ponto de $D$ é um representante de uma classe de equivalência e essas são todas as classes de equivalência.

Pelo Teorema de Pick, a área de $D$ é $A(D) = \frac{1}{2}F + I - 1$ e vai dar exatamente o número de pontos inteiros de $D$, porque $D$ é um paralelogramo onde são tiradas duas arestas e $A(D)$ fica $\frac{1}{2}(F-2) + I$. Logo, $A(D) = |\mathbb{Z}^2/L|$. ■

## 2.7 Teorema de Minkowski

**Teorema 2.9 (Minkowski)** *Sejam $L$ um reticulado de $\mathbb{R}^2$, $D$ um domínio fundamental para $L$ e $X \subset \mathbb{R}^2$ um conjunto limitado, simétrico e convexo tal que*

$$A(X) > 4A(D)$$

*então $X$ contém um ponto não-nulo de $L$.*

**Demonstração:** Duplicando $L$, obtém-se um reticulado $2L$, com domínio fundamental $2D$ cuja área é $4A(D)$.

Seja $T = \mathbb{R}^2/2L$.

Temos que $A(T) = A(2D) = 4A(D)$.

Seja $\varphi : \mathbb{R}^2 \longrightarrow T$ a função da Definição 11.

$A(\varphi(X)) \leq A(T) = 4A(D) < A(X)$.

Logo, $\varphi|_X$ não é injetiva.

Existem $x_1 \neq x_2$ em $X$ tais que $\varphi(x_1) = \varphi(x_2)$.

Então $x_1 - x_2 \in Ker(\varphi) = 2L$.

Ou seja, $\frac{x_1 - x_2}{2} \in L$.

Por $X$ ser simétrico, como $x_2 \in X$, temos $-x_2 \in X$.

Como $X$ é convexo, $\frac{1}{2}x_1 + \frac{1}{2}(-x_2) \in X$.

Logo, $\frac{x_1 - x_2}{2} \in L \cap X$ é um ponto não-nulo do reticulado $L$ que pertence a $X$.

■

# Capítulo 3

# Soma de dois quadrados

Toda hipotenusa de um triângulo pitagórico pode ser expressa por uma soma de quadrados de números inteiros ou por um múltiplo de uma soma de quadrados de inteiros. O Teorema principal deste capítulo pode ser provado apenas com Teoria dos Números elementar. Como ilustração do que desenvolvemos até aqui, provaremos esse resultado usando a geometria aritmética.

**Teorema 3.1** *Seja $n \in \mathbb{Z}$ um inteiro positivo. Então $n$ é soma de dois quadrados de racionais se, e somente se, $n$ é soma de dois quadrados de inteiros.*

**Demonstração:** Se $n$ é soma de dois quadrados de inteiros, então $n$ é soma de dois quadrados de racionais, já que $\mathbb{Z} \subset \mathbb{Q}$.

Provemos que se $n = p_1^2 + p_2^2$ com $p_1, p_2 \in \mathbb{Q}$ e $p_1 \notin \mathbb{Z}$ ou $p_2 \notin \mathbb{Z}$ então $n$ será soma de dois quadrados de inteiros.

Sejam $P = (p_1, p_2) \in \mathbb{R}^2$ e a circunferência $C : x^2 + y^2 = n$.

Temos que $P \in C$.

Seja $M = (m_1, m_2) \in \mathbb{Z}^2$ tal que $|m_i - p_i| < \frac{1}{2}$ para $i = 1, 2$.

Seja $l$ a reta que passa por $M$ e por $P$.

Temos que $l$ não é tangente a $C$, pois:

Se o triângulo $OPM$ fosse retângulo em $P$, então $OM^2 = OP^2 + PM^2$ com $OM \in \mathbb{Z}$ e $OP^2 = n$.

Mas $0 \neq PM^2 = (m_1 - p_1)^2 + (m_2 - p_2)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$.

Então $0 < OM^2 - OP^2 = PM^2 \leq \frac{1}{2}$. Absurdo.

Logo, $l$ é secante a $C$. E $l$ passa por $P$ e $M$ e encontra $C$ no ponto $Q$, outro extremo da corda $PQ$.

$C$ e $l$ têm coeficientes racionais. Pelo Método de Fermat, $Q = (q_1, q_2) \in \mathbb{Q}^2$.

Seja $d$ o mmc das frações irredutíveis $p_1$ e $p_2$ que definem $P$.

Defina $c = d \cdot PM < d$.

Temos que $c = d[(m_1 - p_1)^2 + (m_2 - p_2)^2] = d[m_1^2 + m_2^2 + n - 2(p_1 m_1 + p_2 m_2)] \in \mathbb{Z}$.

Vamos mostrar que $c$ elimina os denominadores de $q_1$ e $q_2$.

Seja $Q = P + t(M - P) = (p_1 + t(m_1 - p_1), p_2 + t(m_2 - p_2))$ onde $t \in \mathbb{Q}^*$.

Temos que $Q \cdot Q = n$ e $P \cdot P = n$.

Seja $v = M - P = (m_1 - p_1, m_2 - p_2)$.

$n = (P + tv) \cdot (P + tv) \Rightarrow 2tP \cdot v + t^2 v \cdot v = 0 \Rightarrow t = -\dfrac{2P \cdot v}{v \cdot v}$.

$v \cdot v = (m_1 - p_1)^2 + (m_2 - p_2)^2 = \dfrac{c}{d}$.

$P \cdot v = p_1(m_1 - p_1) + p_2(m_2 - p_2) = p_1 m_1 + p_2 m_2 - n$.

Então $t = -\dfrac{2(p_1 m_1 + p_2 m_2 - n)}{\frac{c}{d}} = \dfrac{2d(n - p_1 m_1 - p_2 m_2)}{c}$.

$ct = d(2n - 2(p_1 m_1 + p_2 m_2))$.

Mas $\dfrac{c}{d} = m_1^2 - 2p_1 m_1 + p_1^2 + m_2^2 - 2p_2 m_2 + p_2^2$.

$-2p_1 m_1 - 2p_2 m_2 = \dfrac{c}{d} - m_1^2 - m_2^2 - n$.

Daí, $ct = d[\dfrac{c}{d} + n - m_1^2 - m_2^2] = c + d(n - m_1^2 - m_2^2)$.

Vamos avaliar $cq_i$ para $i = 1, 2$.

$$cq_i = c(p_i + t(m_i - p_i)) = cp_i + (ct)(m_i - p_i) =$$

$$= cp_i + [c + d(n - m_1^2 - m_2^2)](m_i - p_i) =$$

$$= cp_i + cm_i - cp_i + d(n - m_1^2 - m_2^2)(m_i - p_i) =$$

$$= cm_i + d(n - m_1^2 - m_2^2)(m_i - p_i) \in \mathbb{Z}$$

Logo, se $P$ é um ponto racional do círculo, com mmc entre os denominadores $p_1, p_2$ mínimo, então obtemos $Q$ com mmc menor.

Se não existisse um ponto inteiro, chegaríamos a uma contradição, pela Descida Infinita de Fermat.

Ou seja existe um ponto inteiro de $C$.

■

## 3.1 Inteiros de Gauss

**Definição 3.1** *O subconjunto de* $\mathbb{C}$*, definido por* $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ *é chamado de inteiros gaussianos.*

**Definição 3.2** *A conjugação em* $\mathbb{Z}[i]$ *é definida da seguinte forma:*

$$\overline{a + bi} = a - bi.$$

**Proposição 3.1** *A conjugação em* $\mathbb{Z}[i]$ *satisfaz:*

*i)* $\overline{z + w} = \overline{z} + \overline{w}$

*ii)* $\overline{zw} = \overline{z} \cdot \overline{w}$

*iii)* $z\overline{z} \geq 0$

*iv)* $z\overline{z} \in \mathbb{Z}$

**Demonstração:** Sejam $z = a + bi$ e $w = c + di$.

$\overline{z} = a - bi$ e $\overline{w} = c - di$.

$z+w = (a+c)+(b+d)i \Rightarrow \overline{z + w} = (a+c)-(b+d)i = (a-bi)+(c-di) = \overline{z}+\overline{w}$.

$zw = (ac - bd) + (ad + bc)i \Rightarrow \overline{zw} = (ac - bd) - (ad + bc)i = \overline{z} \cdot \overline{w}$.

$z\overline{z} = a^2 + b^2 \geq 0$ e $z\overline{z} \in \mathbb{Z}$. ■

**Definição 3.3** *Norma de* $z = a + bi$.

$$N(z) = z\overline{z} = a^2 + b^2 \in \mathbb{Z}$$

**Proposição 3.2** *Sejam* $z, w \in \mathbb{Z}[i]$. *Então* $N(zw) = N(z)N(w)$.

**Demonstração:**

$$zw = (ac - bd) + (ad + bc)i \Rightarrow N(zw) = (ac - bd)^2 + (ad + bc)^2 =$$

$$= a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2c^2 =$$

$$= a^2(c^2 + d^2) + b^2(c^2 + d^2) = (a^2 + b^2)(c^2 + d^2) = N(z)N(w)$$

Ou seja, o produto de duas somas de quadrados é ainda uma soma de dois quadrados. ■

## 3.2 Soma de dois Quadrados

**Observação 3.1** $\mathbb{N}$ *é o conjunto dos números inteiros positivos.*

Consideramos, agora, para um $n \in \mathbb{N}$ a equação $x^2 + y^2 = n$ em $\mathbb{N}$. Queremos saber quais números naturais são soma de dois quadrados de naturais. Ou seja, quais números naturais podem ser hipotenusa de um triângulo retângulo de lados inteiros.

**Lema 3.1** *Se $p \equiv 1$ (mod 4) e $p$ é um número primo então existe $u \in \mathbb{Z}_p$ tal que $u^2 \equiv -1$ (mod p), onde $\mathbb{Z}_p$ é o conjunto das classes residuais módulo p.*

**Demonstração:** Pelo Pequeno Teorema de Fermat, $a^{p-1} = \overline{1}$ em $\mathbb{Z}_p$, com $a \neq \overline{0}$.

Mas $p = 4k + 1 \Rightarrow p - 1 = 4k$.

Agora, se $a \neq \overline{0}$ então $a^{4k} = \overline{1}$.

Além disso, a equação em $\mathbb{Z}_p$: $x^{4k} - \overline{1} = \overline{0}$ tem $p - 1$ soluções.

Daí, $(x^{2k} + \overline{1})(x^{2k} - \overline{1}) = \overline{0} \Rightarrow x^{2k} + \overline{1} = \overline{0}$ ou $x^{2k} - \overline{1} = 0$.

E $x^{2k} - \overline{1} = \overline{0}$ possui no máximo $2k$ soluções.

Logo, $\exists x \in \mathbb{Z}_p | x^{2k} + \overline{1} = \overline{0}$.

Então existe $w \in \mathbb{Z}$ tal que $w^{2k} \equiv -1$ (mod p).

Seja $u = w^k$.

$u^2 \equiv -1$ (mod p). ■

**Teorema 3.2 (Fermat-Euler)** *Um primo $p > 0$ é soma de dois quadrados de inteiros se, e somente se, $p = 2$ ou $p$ é da forma $4k + 1, k \in \mathbb{N}$.*

**Demonstração:** $2 = 1^2 + 1^2$ é soma de dois quadrados de inteiros.

Se $p \neq 2$ e $p \neq 4k + 1 \forall k \in \mathbb{Z}$ então $p = 4k + 3$.

Então se $a^2 + b^2 = p \equiv 3$ (mod 4), temos que $a^2, b^2$ são congruentes a 0 ou 1 (mod 4), gerando uma impossibilidade.

Logo, se $p \equiv 3$ (mod 4) então $p$ não é soma de dois quadrados de inteiros.

Provemos que se $p \equiv 1$(mod 4) então $p$ é soma de dois quadrados de inteiros.

$\exists u \in \mathbb{Z}_p | u^2 = \overline{-1}$, pelo Lema anterior.

Seja $L = \{(a, b) \in \mathbb{Z}^2 | \overline{b} = \overline{ua} \in \mathbb{Z}_p\}$.

$$\begin{array}{rccc} \varphi: & \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}_p \\ & (x, y) & \longmapsto & \overline{y - ux} \end{array}$$

$\varphi$ é um homomorfismo. $Ker(\varphi) = L$ e

$\mathbb{Z}^2/L \cong \mathbb{Z}_p$.

$D \cong \mathbb{Z}^2/L \cong \mathbb{Z}_p$.

$A(D) = p$.

Seja o círculo $X \in \mathbb{R}^2$ limitado, simétrico e convexo:

$X = \{(x, y) \in \mathbb{R}^2 | x^2 + y^2 \leq \frac{3p}{2}\}$

$A(X) = \pi r^2 = \pi\frac{3p}{2} > 4p = 4A(D)$

Pelo Teorema de Minkowski, existe $(a, b) \neq 0$ tal que $(a, b) \in L \cap X$.

$0 \neq a^2 + b^2 \leq r^2 = \frac{3p}{2} < 2p$.

Analisando $a^2 + b^2$ mod p, sabendo que $u^2 \equiv -1$ (mod p), obtemos:

$a^2 + b^2 \equiv a^2 + u^2a^2 \equiv a^2 - a^2 \equiv 0$ (mod p)

Logo, $a^2 + b^2 = p$. ■

**Teorema 3.3** *Seja $n > 0$ inteiro.*

*$n$ é soma de dois quadrados de inteiros se, e somente se, na fatoração de $n$ ocorrem os primos 2 e os primos $p = 4k+1$ com expoente arbitrário e os primos $p = 4k+3$ ocorrem com expoente par.*

**Demonstração:** Suponhamos que $n = a^2 + b^2$ e $n$ possua algum fator primo da forma $p = 4k + 3$ cujo expoente é ímpar.

Seja $d = mdc(a, b)$.

$d^2 | a^2 + b^2 = n$.

$p|n$ com multiplicidade ímpar.

$p|\frac{n}{d^2} = m$.

Sejam $a = du$ e $b = dv$, com $mdc(u, v) = 1$ e $p|m$.

Temos que $u^2 + v^2 = m$.

Seja $mdc(u, p) = 1$ e $uw \equiv 1$ (mod p).

$u^2 + v^2 \equiv 0$ (mod p) $\Rightarrow (vw)^2 \equiv -1$ (mod p).

Mas $p = 4k + 3$.

Daí, $p = 2q + 1$ com $q$ ímpar.

E $p - 1 = 2q$.

$(vw)^{2q} \equiv (-1)^q \equiv -1$ (mod p).

Portanto $(vw)^{p-1} \equiv -1$. Absurdo.

Provemos agora que se $n$ tem na sua fatoração os primos 2 e os primos $4k+1$ com expoente qualquer e os primos $4k+3$ com expoentes pares então $n = a^2 + b^2$ para algum $a \in \mathbb{Z}$ e algum $b \in \mathbb{Z}$.

$2 = 1^2 + 1^2$ é soma de dois quadrados, se 2 estiver com expoente par, já é um quadrado.Se 2 estiver com expoente ímpar, será um quadrado multiplicado por $1^2 + 1^2$, que é uma soma de quadrados. Para os primos da forma $4k+1$, temos que o produto de duas somas de quadrado é uma soma de quadrados.

As potências dos primos $4k+3$ são de expoente par, logo, são quadrados de inteiros.

O produto de uma soma de quadrados por um quadrado é uma soma de quadrados.

Logo, $n$ é soma de quadrados. ■

Como aplicação desse último resultado, provaremos o seguinte fato:

**Teorema 3.4** *Se existe um número perfeito ímpar, então ele é soma de quadrados.*

**Demonstração:** Um número perfeito é tal que $S(n) = 2n$, onde $S(n)$ é a soma de todos os divisores positivos de $n$.

Como $n$ é ímpar, todos os seus divisores são ímpares.

Se $n$ não for soma de quadrados, então existe um fator primo $p$ de $n$ congruente a 3 módulo 4 com expoente ímpar, pelo Teorema 26.

Daí, $S(p^{2k+1}) = 1+p+p^2+p^3+...+p^{2k}+p^{2k+1} \equiv 0(mod 4)$, pois $1+p \equiv 0(mod 4)$, $p^2 + p^3 = p^2(1+p)$,..., $p^{2k} + p^{2k+1} = p^{2k}(1+p)$.

Mas $S(p^{2k+1})|S(n) \Rightarrow 4|S(n)$. E $S(n) = 2n$, com $n$ ímpar. Absurdo.

Logo, $n$ é soma de quadrados. ■

# Referências Bibliográficas


Gonçalves, A. (1995). *Introdução à Álgebra*. IMPA, R.Janeiro.

Gondim, R. (2011). Aritmética em retas e cônicas. In *I Colóquio de Matemática do Nordeste, Sergipe, 2011*, Sergipe, Brasil.

Heath, T. (1956). *The Thirteen Books of Elements*. Dover, New York.

Hefez, A. (2013). *Aritmetica*. SBM, R.Janeiro.

Santos, J. (2007). *Introdução à Teoria dos Números*. IMPA, R.Janeiro.

S.Singh (2006). *O Ultimo Teorema de Fermat*. Editora Record, R.Janeiro.