**UNIVERSIDADE FEDERAL DO CEARÁ**

**CENTRO DE CIÊNCIAS**

**DEPARTAMENTO DE MATEMÁTICA**

**PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL**

**GEORGE DA COSTA EUZÉBIO**

# O RETICULADO INTEIRO E ALGUMAS APLICAÇÕES

**FORTALEZA**

**2020**

GEORGE DA COSTA EUZÉBIO

# O RETICULADO INTEIRO E ALGUMAS APLICAÇÕES

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em rede nacional, da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática.
Área de Concentração: Álgebra

Orientador: Prof. Dr. Antonio Caminha Muniz Neto

FORTALEZA

2020

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

---

E91r Euzébio, George da Costa.
O reticulado inteiro e algumas aplicações / George da Costa Euzébio. – 2020.
39 f. : il. color.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2020.
Orientação: Prof. Dr. Antonio Caminha Muniz Neto.

1. Reticulado inteiro. 2. Frações de Farey. 3. Círculos de Ford. 4. Teorema de Hurwitz. I. Título.
CDD 510

GEORGE DA COSTA EUZÉBIO

# O RETICULADO INTEIRO E ALGUMAS APLICAÇÕES

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em rede nacional, da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática.
Área de Concentração: Álgebra

Aprovada em: 28/02/2020

BANCA EXAMINADORA

---

Prof. Dr. Antonio Caminha Muniz Neto (Orientador)
Universidade Federal do Ceará (UFC)

---

Prof. Dr. Francisco Yure Santos do Nascimento
Universidade Federal do Ceará

---

Prof. Dr. Ulisses Lima Parente
Universidade Estadual do Ceará

À minha filha Ana Sophia, para que um dia possa seguir meus passos.

"A Matemática, vista corretamente, possui não apenas verdade, mas também suprema beleza."

(BERTRAND RUSSELL)

## RESUMO

O presente trabalho tem como objetivo principal apresentar o Teorema de Hurwitz sobre a aproximação de números irracionais através de números racionais utilizando uma constante associada ao valor de $\sqrt{5}$ para as aproximações. Para isso, serão relembrados inicialmente alguns conhecimentos sobre Teoria dos Números, tais como divisibilidade e congruências modulares, bem como alguns teoremas acerca de números primos e inteiros que podem ser escritos como soma de dois quadrados. Posteriormente, serão apresentados o reticulado dos números inteiros e algumas das propriedades de seus pontos, assim como alguns teoremas geométricos sobre tais pontos. Em uma última parte será desenvolvida a sequência de Farey em conjunto com os círculos de Ford, para apresentação dos teoremas sobre aproximação de irracionais por racionais e, assim, demonstrarmos o teorema de Hurwitz.



**Palavras-chave:** Reticulado inteiro. Frações de Farey. Círculos de Ford. Teorema de Hurwitz

**ABSTRACT**

The present work aims at presenting Hurwitz's theorem on rational approximations of irrational numbers, using a constant associated with the value of $\sqrt{5}$ for the approximations. For this, some knowledge about Number Theory, such as divisibility and modular congruences, will be developed, as well as some theorems about primes and integers that can be written as a sum of two squares. Subsequently, we shall present the lattice points of the plane, together with some of their basic properties, as well as some geometric results involving them. In the last part, the Farey sequences will be developed in conjunction with Ford's circles. This machinery is needed for presentation of theorems about approximation of irrationals by rationals and, thus, allow the presentation of the proof of Hurwitz's Theorem.

**Keywords:** Lattice points. Farey's sequence. Ford's circles. Hurwitz's Theorem

**SUMÁRIO**

# 1 ALGUNS PRELIMINARES DE TEORIA DOS NÚMEROS

No presente capítulo será apresentado o reticulado dos números inteiros, ou seja, os pontos do plano cartesiano que possuem coordenadas inteiras e suas propriedades. Para isso serão apresentadas algumas noções pertinentes à **Teoria dos Números** como divisibilidade, ideais, números relativamente primos e congruências modulares. Seguimos, essencialmente, (NETO, 2013), na qual as demonstrações não apresentadas podem ser encontradas.

## 1.1 Divisibilidade, Ideais e MDC

Começamos com a seguinte

**Definição 1.1.1** (Divisibilidade)**.** *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$, dizemos que b divide a (escrevemos $b \mid a$) quando existe um inteiro c tal que $a = bc$. Nesse caso, também podemos dizer que b é divisor de a ou que a é um múltiplo de b.*

A proposição a seguir coleciona alguns resultados elementares sobre divisibilidade, os quais serão utilizados livremente ao longo dessa dissertação.

**Proposição 1.1.1.** *Dados inteiros não nulos a, b e c, são válidas as seguintes propriedades sobre divisibilidade*

*(i)* $a \mid a$, *para todo* $a \in \mathbb{Z}$.

*(ii) Se* $a \mid 1$, *então* $a = \pm 1$.

*(iii) Se* $a \mid b$, *então* $|a| \leq |b|$.

*(iv) Se* $a \mid b$ *e* $b \mid a$, *então* $|a| = |b|$

*(v) Se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$.

*(vi) Se* $a \mid b$ *e* $a \mid c$, *então* $a \mid (mb + nc)$, *para todos os inteiros m, n.*

Para demonstrarmos nosso primeiro teorema a respeito de divisibilidade, faremos uso de um axioma conhecido como o

**Princípio da Boa Ordenação (PBO)**: Se $X \subset \mathbb{N}$ é um conjunto não vazio, então $X$ possui um menor elemento. Em outras palavras, $\exists\, n_0$ em $X$ o qual todo $x \in X$ satisfaz $n_0 \leq x$.

**Teorema 1.1.1** (Algoritmo da Divisão)**.** *Dados inteiros a e b, com $b > 0$, existem únicos inteiros q e r tais que $a = qb + r$ e $0 \leq r < |b|$.*

*Demonstração.* Seja $X = \{a - qb; q \in \mathbb{N}, a - qb \geq 0\}$, um subconjunto de $\mathbb{Z}$. Temos que $X$ é não vazio, pois quando $q = 0$ temos $a - 0\dot{b}$, portanto, $a \in X$. Pelo **PBO**, o conjunto $X$ possui um menor elemento $r_0$, tal que $r_0 = a - q_0 b$ para algum $q_0 \in \mathbb{Z}$. Se $r_0 \geq b$, então

$$a - (q_0 + 1)b = r_0 - b \geq 0$$

garante que $r_0 - b \in X$, com $r_0 - b < r_0$, contrariando a minimalidade de $r_0$. Portanto, existem $r, q \in \mathbb{Z}$, com $0 \leq r < b$, tais que $a = qb + r$.

Para a unicidade, consideraremos a existência de inteiros $q'$ e $r'$ tais que

$$a = qb + r = q'b + r'.$$

Então,

$$b(q - q') = r - r' \implies b \mid (r - r');$$

mas, como $0 \leq r, r' < b$, devemos ter $r - r' = 0$, ou seja, $r = r'$, o que por sua vez garante que $q = q'$. ■

O teorema anterior, que, como observamos, é conhecido como o Algoritmo da Divisão, tem uma grande importância em Teoria dos Números, pois garante a existência de um quociente $q$ e um resto $r$ na divisão de um inteiro dado $a$ por um inteiro não nulo e também dado $b$. Mais à frente, veremos a importância do resto em uma divisão quando definirmos uma nova relação, chamada de *congruência modular*. Para seguirmos com nosso propósito, necessitaremos trabalhar com a noção de ideal e suas propriedades.

**Definição 1.1.2.** *Um conjunto não vazio I de inteiros é dito um* ***ideal*** *quando a seguinte condição for satisfeita:*

$$\alpha, \beta \in I \implies m\alpha + n\beta \in I, \ \ \forall m, n \in \mathbb{Z}.$$

**Proposição 1.1.2.** *Os ideais de $\mathbb{Z}$ são os conjuntos da forma $m\mathbb{Z} = \{n \in \mathbb{Z}; m \mid n\}$, para algum $m \in \mathbb{N}$.*

*Demonstração.* Mostremos primeiro que $m\mathbb{Z}$ é ideal de $\mathbb{Z}$. Para tanto, dados inteiros $\alpha, \beta \in m \cdot \mathbb{Z}$, temos que $m \mid \alpha$ e $m \mid \beta$. Então, conforme foi visto na seção anterior, $m \mid (r\alpha + s\beta)$, para todos $r, s \in \mathbb{Z}$, de sorte que $r\alpha + s\beta \in m\mathbb{Z}$. Portanto $m\mathbb{Z}$ é um ideal.

Agora, seja $I$ um ideal de $\mathbb{Z}$. Se $I = \{0\}$, então $I = 0\mathbb{Z}$. Se $I \neq \{0\}$, então, como $x \in I \Leftrightarrow -x \in I$, temos que $I$ contém inteiros positivos. Tome, pelo PBO, o menor inteiro positivo $m$ em $I$. Como $I$ é ideal, temos claramente que $I$ contém os múltiplos de $m$, isto é, $m\mathbb{Z} \subset I$. Reciprocamente, se $x \in I$, o algoritmo da divisão garante a existência de $q, r \in \mathbb{Z}$ tais que $x = mq + r$, com $0 \leq r < m$. Então, como $r = 1 \cdot x + (-q)m$, com $m, x \in I$, temos (novamente pelo fato de $I$ ser ideal) que $r \in I$. Portanto, a minimalidade de $m$ garante que $r = 0$ e, daí, que $x \in mZ$. Assim, $I \subset m\mathbb{Z}$. ■

O conjunto $m\mathbb{Z}$ é também conhecido como o conjunto dos múltiplos do inteiro $m$ e servirá de auxílio para demonstramos o próximo resultado. Para tanto, precisamos da seguinte

**Definição 1.1.3.** *Chamamos de* ***máximo divisor comum*** *(abreviamos* ***mdc****) dos inteiros não nulos* $a_1$, $a_2$,..., $a_n$, *denotado* $\text{mdc}(a_1, a_2, \ldots, a_n)$, *ao maior dos divisores comuns de* $a_1$, $a_2$,..., $a_n$. *Os inteiros* $a_1$, $a_2$, ..., $a_n$ *são ditos* ***relativamente primos*** *quando* $\text{mdc}(a_1, a_2, \ldots, a_n) = 1$.

**Teorema 1.1.2** (Bézout)**.** *Dados inteiros não nulos* $a_1$, $a_2$, ..., $a_n$, *se*

$$S = \Big\{ \sum_{i=1}^{n} a_i x_i;\ x_i \in \mathbb{Z}, \textit{para } 1 \leq i \leq n \Big\},$$

*temos que* $S = d\mathbb{Z}$, *onde* $d = \text{mdc}(a_1, a_2, \ldots, a_n)$. *Em particular, existem inteiros* $r_1$, $r_2$, ..., $r_n$ *tais que*

$$\text{mdc}(a_1, a_2, \ldots, a_n) = a_1 r_1 + a_2 r_2 + \ldots + a_n r_n.$$

*Demonstração.* É imediato verificar que $S$ é um ideal de $\mathbb{Z}$. Também, $S$ contém inteiros positivos, como, por exemplo, $a_1^2 = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n$, com $x_1 = a_1$ e $x_2 = \ldots = x_n = 0$. Logo, existe um inteiro positivo $d$ tal que $S = d\mathbb{Z}$. Em particular, $d = a_1 r_1 + a_2 r_2 + \ldots + a_n r_n$, para certos inteiros $r_1$, $r_2$, ..., $r_n$; também, como $a_i \in S \Rightarrow a_i \in d\mathbb{Z}$, temos que $d \mid a_1, a_2, \ldots, a_n$.

Seja, agora, $d'$ um divisor comum de $a_1$, $a_2$, ..., $a_n$, digamos com $a_i = d' q_i$ para $1 \leq i \leq n$. Então,

$$\begin{aligned} d &= a_1 r_1 + a_2 r_2 + \ldots + a_n r_n \\ &= d' q_1 r_1 + d' q_2 r_2 + \ldots + d' q_n r_n \\ &= d' (q_1 r_1 + q_2 r_2 + \ldots + q_n r_n), \end{aligned}$$

de sorte que $d' \mid d$ e, em particular, $d' \leq d$. Assim, $d$ é o mdc de $a_1$, $a_2$, ..., $a_n$. ■

A seguir temos alguns corolários do teorema anterior.

**Corolário 1.1.1.** *Sejam $a_1, a_2, \ldots, a_n$ inteiros não nulos e $d$ seu* $\text{mdc}(a_1, a_2, \ldots, a_n)$. *Se $d' \in \mathbb{N}$, então $d' \mid a_1, a_2, \ldots, a_n$ se, e somente se, $d' \mid d$.*

**Corolário 1.1.2.** *Sejam $a_1, a_2, \ldots, a_n$ inteiros não nulos e $d = \text{mdc}(a_1, a_2, \ldots, a_n)$. Então, $d = 1$ se, e somente se, existem inteiros $r_1, r_2, \ldots, r_n$ tais que $a_1 r_1 + a_2 r_2 + \ldots + a_n r_n = 1$.*

**Corolário 1.1.3.** *Sejam $a_1, a_2, \ldots, a_n$ inteiros não nulos. Se $d = \text{mdc}(a_1, a_2, \ldots, a_n)$, então* $\text{mdc}\left(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}\right) = 1$.

A próxima consequência do Teorema 1.1.2 é suficientemente importante para que também a chamemos de

**Teorema 1.1.3** (Euclides)**.** *Sejam $a, b, c$ inteiros tais que $a, c \neq 0$ e $a \mid bc$. Se* $\text{mdc}(a, c) = 1$, *então $a \mid b$.*

*Demonstração.* Pelo Teorema de Bézout, existem inteiros $r$ e $s$ tais que $1 = ra + sc$. Multiplicando essa igualdade por $b$, obtemos $b = r(ba) + s(bc)$. Como $a \mid ba$ e, por hipótese, $a \mid bc$, concluímos que $a \mid b$. ■

**Proposição 1.1.3.** *Sejam $a$ e $b$ inteiros não nulos tais que* $\text{mdc}(a, b) = 1$. *Se $c$ é um inteiro tal que $a \mid c$ e $b \mid c$, então $ab \mid c$.*

*Demonstração.* Como $a \mid c$, existe $q \in \mathbb{Z}$ tal que $c = aq$. Como $b \mid c = aq$ e, por hipótese, $\text{mdc}(a, b) = 1$, o resultado anterior garante que $b \mid q$, digamos, $q = br$, com $r \in \mathbb{Z}$. Portanto, $c = aq = a(br) = (ab)r$, o que nos leva a concluir que $ab \mid c$. ■

**Definição 1.1.4.** *Um inteiro positivo $p$ diz-se **primo** quando possui exatamente dois divisores positivos, a saber* $1$ *e $p$. Em particular, $p > 1$.*

Um inteiro $a > 1$ que não é um primo, é chamado de **composto**. Nesse caso, $a$ pode ser escrito como produto de dois números inteiros maiores que 1.

**Proposição 1.1.4.** *Seja $p$ um primo e sejam $a$ e $b$ inteiros não nulos.*

*(i) Se $p \nmid a$, então* $\text{mdc}(a, p) = 1$.

*(ii) Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

*Demonstração.*
(i) Se $p \nmid a$, então, como $p$ é primo, o único divisor comum de $a$ e $p$ é 1. Portanto, $\text{mdc}(a, p) = 1$.

(ii) Se $p \mid a$, então o teorema está provado. Caso contrário, pelo item (i) temos que $\text{mdc}(a, p) = 1$. Portanto, pelo teorema de Euclides, $p \mid b$. ■

**Corolário 1.1.4.** *Se $p \mid a_1 a_2 \dots a_n$, então $p \mid a_k$ para algum $k$, $1 \leq k \leq n$.*

*Demonstração.* O resultado segue imediatamente do item (ii) da proposição anterior, usando indução sobre o número de fatores do produto $a_1 a_2 \dots a_n$. ■

**Teorema 1.1.4.** *Todo inteiro $n > 1$ possui um divisor primo.*

*Demonstração.* Se $n$ é primo, então nada há para demonstrar. Se $n > 1$ não é primo, então, como todo inteiro possui uma quantidade finita de divisores maiores que 1 (o que está garantido pela propriedade (iii) de divisibilidade), podemos tomar $k$ como o menor desses divisores. Se $k$ não é primo, então podemos decompô-lo como um produto de dois inteiros menores que $k$ e maiores que 1. Um qualquer desses fatores seria, então, um divisor de $n$ menor que $k$ e ainda maior que 1, contrariando a minimalidade de $k$. Portanto, $k$ deve ser primo. ■

Pelo teorema anterior, podemos concluir que todo número pode ser escrito como um produto finito de números primos. Por sua importância, apresentamos esse fato como um

**Corolário 1.1.5** (Euclides)**.** *Todo inteiro $n > 1$ pode ser escrito com um produto de números primos.*

*Demonstração.* Argumentemos por indução. Se $n$ é primo, nada há a fazer. Se $n > 1$ não é primo, tome um divisor primo $p$ de $n$. Aplicando a hipótese de indução a $\frac{n}{p}$ (que é menor que $n$ e maior que 1), concluímos que $\frac{n}{p} = p_1 \dots p_k$, para certos primos $p_1, \dots, p_k$. Portanto,

$$n = p \cdot \frac{n}{p} = p p_1 \dots p_k,$$

um produto de primos. ■

A seguir, temos mais um importante resultado devido a Euclides.

**Teorema 1.1.5** (Euclides)**.** *O conjunto dos números primos é infinito.*

*Demonstração.* Seja $P$ o conjunto dos números primos. Se há uma quantidade finita de números primos, então $P = \{p_1, p_2, \ldots, p_n\}$, para certos primos $p_1$, ..., $p_n$. Seja $m = p_1 p_2 \ldots p_n + 1$. Pelo teorema anterior, $m$ deve possuir um número primo como divisor, digamos $p$. Por sua vez, esse primo $p$ não está listado no conjunto $P$, pois $m$ deixa resto 1 quando dividido por $p_k$, para todo índice $1 \leq k \leq n$. Mas isso contradiz o fato de que $P$ é o conjunto de todos os primos. Logo, $P$ não pode ser finito. ■

Antes de demonstramos o Teorema 1.1.6, que é considerado a pedra angular da Teoria dos Números, precisamos da seguinte generalização imediata do item (ii) da Proposição 1.1.4.

**Lema 1.1.1.** *Se $a_1, a_2, \ldots, a_n \in \mathbb{N}$ e $p$ é um primo tal que $p \mid a_1 a_2 \ldots a_n$, então existe $1 \leq i \leq n$ tal que $p \mid a_i$. Em particular, se $a_1, a_2, \ldots, a_n$ forem todos primos, então existe $1 \leq i \leq n$ tal que $p = a_i$.*

**Teorema 1.1.6** (Fundamental da Aritmética)**.** *Todo inteiro $n > 1$ pode ser escrito como um produto de potências de números primos distintos. Além disso, essa decomposição é única, a menos de uma permutação de seus fatores.*

*Demonstração.* Pelo Corolário 1.1.5, todo inteiro $n > 1$ pode ser escrito como um produto de primos. Então, agrupando os primos repetidos, temos que $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, com $p_1$, ..., $p_k$ primos dois a dois distintos e $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$. Isso garante a existência da decomposição.

Para a unicidade, suponhamos que $n$ admite uma outra decomposição como acima, digamos

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}.$$

Suponhamos também, sem perda de generalidade, que $p_1 < \ldots < p_k$ e $q_1 < \ldots < q_l$.

Como $p_1 \mid n$, temos que $p_1 \mid q_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}$. Pelo lema anterior, existe $1 \leq j \leq l$ tal que $p_1 = q_j$. Por outro lado, como $q_1 \mid n$, temos que $q_1 \mid p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ e, novamente pelo lema anterior, existe $1 \leq i \leq k$ tal que $q_1 = p_i$. Desse modo,

$$p_1 = q_j \geq q_1 = p_i \geq p_1,$$

o que implica que $p_1 = q_1$. Daí

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} = p_1^{\beta_1} q_2^{\beta_2} \ldots q_l^{\beta_l}.$$

Mostraremos, agora, que $\alpha_1 = \beta_1$. De fato, se $\alpha_1 < \beta_1$, então

$$p_2^{\alpha_2} \dots p_k^{\alpha_k} = p_1^{\beta_1 - \alpha_1} q_2^{\beta_2} \dots q_l^{\beta_l},$$

de modo que $p_1 \mid q_2^{\alpha_2} \dots q_l^{\alpha_l}$. Argumentando como anteriormente, existiria $2 \leq i \leq l$ tal que $p_1 = q_i$, o que é um absurdo. Analogamente, se $\alpha_1 > \beta_1$ teremos um absurdo similar, de sorte que $\alpha_1 = \beta_1$.

Assim, temos a igualdade

$$\frac{n}{p_1^{\alpha_1}} = p_2^{\alpha_2} \dots p_k^{\alpha_k} = q_2^{\beta_2} \dots q_l^{\beta_l}.$$

Raciocinando por indução (e aplicando a hipótese de indução a $\frac{n}{p_1^{\alpha_1}}$), concluímos que $k-1 = l-1$ (logo, $k = l$) e $p_i = q_i$, $\alpha_i = \beta_i$ para $2 \leq i \leq k$. ■

## 1.2 Congruência modular

Passaremos, agora, a estudar um novo tipo de relação conhecida como **congruência modular**. Assim como a definição de ideais, a noção de congruência modular nos ajudará fortemente com alguns resultados a respeito dos números inteiros, especialmente quando tentarmos descobrir quais são os inteiros que podem ser escritos como soma de quadrados.

**Definição 1.2.1.** *Dados inteiros $a, b, m$, com $m > 1$, dizemos que* ***a é congruente a b, módulo m*** *e escrevemos $a \equiv b \pmod{m}$, quando $m \mid (a-b)$.*

O resultado a seguir revela a importância do conceito de congruência.

**Proposição 1.2.1.** *Dois inteiros a e b são congruentes módulo m se, e somente se, deixam o mesmo resto na divisão por m.*

*Demonstração.* Pelo algoritmo da divisão, temos $a = mq_1 + r_1$ e $b = mq_2 + r_2$, com $0 \leq r_1, r_2 < m$. Assim,

$$a - b = m(q_1 - q_2) + (r_1 - r_2),$$

de sorte que $m \mid (a-b)$ se, e somente se, $m \mid (r_1 - r_2)$. Mas, como $0 \leq |r_1 - r_2| < m$, segue que $m \mid (a-b)$ se, e somente se, $r_1 = r_2$. ■

A seguir, listamos algumas propriedades importantes do conceito de congruência. Assim como com as propriedades de divisibilidade, elas são de fácil demonstração e, portanto, suas provas serão omitidas.

(i) $a \equiv a \pmod{m}$.

(ii) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

(iii) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a+c \equiv b+d \pmod{m}$ e $ac \equiv bd \pmod{m}$.

(iv) Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$.

Com o auxílio dessa formalização inicial de congruências, demonstraremos a seguir alguns teoremas que nos ajudarão a descrever precisamente quais números naturais podem ser escritos como somas de dois quadrados.

**Definição 1.2.2.** *Dados inteiros a, b e m, com $m > 1$, dizemos que* ***a é o inverso de b, módulo m*** *se a congruência $ab \equiv 1 \pmod{m}$ se verificar.*

**Teorema 1.2.1.** *Sejam dados inteiros a e m, com $m > 1$. Se $\text{mdc}(a,m) = 1$, então a possui um único inverso, módulo m.*

*Demonstração.* Como $\text{mdc}(a,m) = 1$, o Teorema de Bézout garante a existência de inteiros $b$ e $c$ tais que $ab + cm = 1$. Desse modo, considerando que $ab + cm \equiv 1 \pmod{m}$ e $m \equiv 0 \pmod{m}$, as propriedades de congruências listadas acima dão facilmente $ab \equiv 1 \pmod{m}$.

Suponha, agora, que tenhamos $ab_1 \equiv 1 \pmod{m}$ e $ab_2 \equiv 1 \pmod{m}$. Então, $ab_1 \equiv ab_2 \pmod{m}$ e, daí, $m \mid a(b_1 - b_2)$. Mas, como $\text{mdc}(a,m) = 1$, sabemos que essa divisibilidade implica $m \mid (b_1 - b_2)$ ou, o que é o mesmo, $b_1 \equiv b_2 \pmod{m}$. ■

A noção de inverso módulo $m$ permite apresentar uma demonstração simples do

**Teorema 1.2.2** (Wilson)**.** *Se p é um número primo, então $(p-1)! \equiv -1 \pmod{p}$.*

*Demonstração.* Se $p = 2, 3$, o teorema é de verificação é imediata. Suponha, pois, que $p > 3$.

Se $X = \{1, 2, \ldots, p-1\}$, então o teorema anterior garante que todos os elementos de $X$ possuem um único inverso módulo $p$. Além disso, 1 e $p-1$ são os únicos elementos que coincidem com seus inversos.

De fato, se $a \in X$ é tal que $a^2 \equiv 1 \pmod{p}$, então $p \mid (a+1)(a-1)$ e, como $p$ é primo, temos que $p \mid (a+1)$ ou $p \mid (a-1)$. Se $p \mid (a+1)$, então $a \equiv -1 \equiv p-1 \pmod{p}$; por outro lado, se $p \mid (a-1)$, então $a \equiv 1 \pmod{p}$.

Agora, arranje os fatores do produto $(p-1)! = 1 \cdot 2 \ldots (p-1)$ de modo que cada $a \in X \setminus \{1, p-1\}$ fique adjacente a seu inverso multiplicativo, módulo $p$. Assim fazendo,

obtemos

$$(p-1)! = 1 \cdot (p-1) \cdot a_1 b_1 \cdot \ldots \cdot a_k b_k,$$

com $k = \frac{p-3}{2}$ e $a_i b_i \equiv 1 \pmod{p}$ para $1 \leq i \leq \frac{p-3}{2}$. Então, olhando a igualdade acima módulo $p$, obtemos

$$(p-1)! \equiv 1(-1) \equiv -1 \pmod{p}.$$

■

A seguir, colecionamos outro resultado elementar, mas muito importante, sobre congruências.

**Teorema 1.2.3** (Pequeno Teorema de Fermat)**.** *Sejam $p$ um primo e $a$ um inteiro tal que $p \nmid a$. Então, $a^{p-1} \equiv 1 \pmod{p}$.*

*Demonstração.* Para $1 \leq k \leq p-1$, é claro que $p \nmid ka$. Também, se $la \equiv ka \pmod{p}$, para certos $1 \leq l < k \leq p-1$, então teríamos que $p \mid a(l-k)$ e, como $\text{mdc}(a,p) = 1$, viria que $l \equiv k \pmod{p}$, o que é um absurdo. Portanto, $1 \leq l < k \leq p-1$ implica $la \not\equiv ka \pmod{p}$.

Segue do parágrafo anterior que os inteiros $a, 2a, \ldots, (p-1)a$ formam um conjunto de $p-1$ inteiros dois a dois incongruentes módulo $p$. Assim, $a, 2a, \ldots, (p-1)a$ são congruentes módulo $p$, em alguma ordem, aos inteiros 1, 2, ..., $p-1$, de forma que

$$a \cdot 2a \ldots (p-1)a \equiv 1 \cdot 2 \ldots (p-1) \pmod{p}.$$

Então,

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

e, como $(p-1)!$ e $p$ são relativamente primos, concluímos com o auxílio da Proposição 1.1.3 que $a^{p-1} \equiv 1 \pmod{p}$. ■

De agora, até o final desta seção, analisamos o problema da representação de um natural como soma de dois quadrados. Para tanto, precisamos da seguinte

**Definição 1.2.3.** *Dado $x \in \mathbb{R}$, sua **parte inteira**, denotada $\lfloor x \rfloor$, é definida por $\lfloor x \rfloor = \max\{n \in \mathbb{Z}; n \leq x\}$. Em outros termos, $\lfloor x \rfloor = n \Leftrightarrow n \leq x < n+1$.*

Na demonstração do resultado a seguir, utilizaremos do **princípio da casa dos pombos**: *se $A$ e $B$ são conjuntos finitos tais que $|A| > |B|$ e $f : A \to B$ é uma função qualquer, então existem $a, a' \in A$ distintos, tais que $f(a) = f(a')$.*

**Teorema 1.2.4** (Thue)**.** *Seja $p$ um primo. Para qualquer inteiro $a$ tal que $p \nmid a$, existem $x, y \in \{1, 2, \ldots, \lfloor\sqrt{p}\rfloor\}$ tais que $ax \equiv y \pmod{p}$.*

*Demonstração.* O conjunto $S = \{0, 1, 2, \ldots, \lfloor\sqrt{p}\rfloor\} \times \{0, 1, 2, \ldots, \lfloor\sqrt{p}\rfloor\}$ tem $(\lfloor\sqrt{p}\rfloor + 1)^2$ pares ordenados. Como $\sqrt{p} < \lfloor\sqrt{p}\rfloor + 1$, temos $p < (\lfloor\sqrt{p}\rfloor + 1)^2$; portanto, $S$ possui mais de $p$ elementos.

Seja, agora, $A = \{ax - y; (x, y) \in S\}$ e consideremos dois casos separadamente: (i) Se existirem pares ordenados distintos $(x_1, y_1), (x_2, y_2) \in S$ tais que $ax_1 - y_1 = ax_2 - y_2$, então $ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$. (ii) Se $ax_1 - y_1 \neq ax_2 - y_2$ para todos os pares ordenados distintos $(x_1, y_1), (x_2, y_2) \in S$, então $|A| = |S| > p$. Daí, pondo $B = \{0, 1, 2, \ldots, p-1\}$, temos $|A| > p = |B|$; definindo $f : A \to B$ como a função que associa ao número $ax - y$ o resto de sua divisão por $p$, o princípio da casa dos pombos garante a existência de pares ordenados distintos $(x_1, y_1), (x_2, y_2) \in S$ tais que $ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$.

A partir de $ax_1 - y_1 \equiv ax_2 - y_2 \pmod{p}$, obtemos $a(x_1 - x_2) \equiv y_1 - y_2 \pmod{p}$. Sendo $x = |x_1 - x_2|$ e $y = |y_1 - y_2|$, temos $(x, y) \in S$. Podemos excluir a possibilidade que $x = 0$ ou $y = 0$, desse modo $x, y \in 1, 2, \ldots, \lfloor\sqrt{p}\rfloor$

Supondo primeiro que $x = |x_1 - x_2| = 0$, então $x_1 = x_2$. Assim $a(x_1 - x_2) = 0 \equiv y_1 - y_2 \pmod{p}$. Desde que $y_1, y_2 \in 1, 2, \ldots, \lfloor\sqrt{p}\rfloor$, sabemos que $y_1, y_2 < p$, portanto, devemos ter $y_1 = y_2$, contrariando $(x_1, y_1) \neq (x_2, y_2)$.

Supondo agora $y = |y_1 - y_2| = 0$, então $y_1 = y_2$. Desse modo, $a(x_1 - x_2) \equiv 0 \pmod{p}$. Se $p \nmid a$, então $x_1 - x_2 \equiv 0 \pmod{p}$. Seguindo a mesma lógica anterior, concluímos que $x_1 = x_2$, também contrariando $(x_1, y_1) \neq (x_2, y_2)$. Portanto devemos ter $ax \equiv \pm y \pmod{p}$ ■

A seguinte consequência do Teorema de Thue é o primeiro passo para investigar os inteiros que podem ser escritos como soma de dois quadrados.

**Teorema 1.2.5.** *Se existe um inteiro $a$ tal que $a^2 + 1 \equiv 0 \pmod{p}$, então $p$ pode ser escrito como soma de dois quadrados.*

*Demonstração.* Inicialmente, se existe um inteiro $a$ tal que $a^2 + 1 \equiv 0 \pmod{p}$, então $p \nmid a$, pois se $p \mid a$, então $a^2 \equiv 0 \pmod{p}$, ou seja, $a^2 + 1 \equiv 1 \pmod{p}$. Pelo Teorema de Thue, existem $x, y \in \{1, 2, \ldots, \lfloor\sqrt{p}\rfloor\}$ tais que $ax \equiv y \pmod{p}$; logo, $a^2x^2 \equiv y^2 \pmod{p}$. Por outro lado, a congruência $a^2 + 1 \equiv 0 \pmod{p}$ implica $a^2x^2 + x^2 \equiv 0 \pmod{p}$. Então, $y^2 + x^2 \equiv a^2x^2 + x^2 \equiv 0 \pmod{p}$, de sorte que existe um inteiro $k$ tal que $x^2 + y^2 = kp$. Resta mostrar que $k = 1$. Para isso, como

$1 \leq x, y < \sqrt{p}$, temos que

$$2 \leq x^2 + y^2 < 2\left(\sqrt{p}\right)^2 = 2p,$$

isto é, $2 \leq kp < 2p$. Então, $kp = p$, de sorte que $k = 1$. ■

**Teorema 1.2.6** (Euler)**.** *Um número primo $p > 2$ pode ser escrito como soma de dois quadrados se, e somente se, $p \equiv 1 \pmod 4$.*

*Demonstração.* Uma vez que todo inteiro $n$ é congruente a 0, 1, 2 ou 3, módulo 4, é imediato verificar que $n^2 \equiv 0$ ou $1 \pmod 4$, sendo congruente a 0 se e só se $n$ for par. Assim, se $p > 2$ é primo (logo, ímpar) e $p = x^2 + y^2$, então

$$p = x^2 + y^2 \equiv 0, 1 \text{ ou } 2 \pmod 4 \Rightarrow p \equiv 1 \pmod 4.$$

Reciprocamente, suponha que $p \equiv 1 \pmod 4$. A fim de mostrar que $p$ pode ser escrito como soma de dois quadrados, é suficiente, pelo teorema anterior, mostrar que existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -1 \pmod p$. Para tanto, usando o fato de que $p - l \equiv -l \pmod p$ para todo $l \geq 1$, obtemos

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

Agora, o Teorema 1.2.2 nos dá $(p-1)! \equiv -1 \pmod p$. Portanto, sendo $a = 1 \cdot 2 \ldots \left(\frac{p-1}{2}\right)$ e $p = 4k + 1$, os cálculos acima fornecem $-1 \equiv (-1)^{2k} a^2 \pmod p$. Isso é o mesmo que $a^2 \equiv -1 \pmod p$, conforme desejado. ■

Precisamos, agora, do seguinte resultado auxiliar.

**Lema 1.2.1** (Euler)**.** *Se a e b são inteiros positivos que podem ser escritos como somas de dois quadrados, então o produto ab também pode ser escrito como soma de dois quadrados.*

*Demonstração.* Sejam $a = x^2 + y^2$ e $b = z^2 + t^2$, com $x, y, z, t \in \mathbb{Z}_+$. Então,

$$\begin{aligned}ab &= (x^2 + y^2)(z^2 + t^2) = x^2z^2 + x^2t^2 + y^2z^2 + y^2t^2 \\ &= (x^2z^2 + 2xyzt + y^2t^2) + (x^2t^2 - 2xyzt + y^2z^2) \\ &= (xz + yt)^2 + (xt - yz)^2.\end{aligned}$$

■

Para o que segue, é conveniente termos a próxima definição a nosso dispor.

**Definição 1.2.4.** *Um inteiro $a$ é **livre de quadrados** se, para todo inteiro $m > 1$, tivermos que $m^2 \nmid a$.*

**Teorema 1.2.7.** *Um inteiro positivo $n$ pode ser escrito como soma de dois quadrados se, e somente se, cada fator primo $p$ de $n$ tal que $p \equiv 3 \pmod 4$ ocorre com expoente par na fatoração de $n$.*

*Demonstração.* Seja $n = 2^{\alpha} p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_1} \dots q_l^{\beta_l}$ a decomposição de $n$ em fatores primos com $\alpha, \alpha_i, \beta_j \geq 0$, $p_i \equiv 1 (\text{mod } 4)$ e $q_j \equiv 3 (\text{mod } 4)$, para todos $1 \leq i \leq k$ e $1 \leq j \leq l$.

Inicialmente, afirmamos que se $\beta_j$ for par para todo $1 \leq j \leq l$, então $n$ pode ser escrito como soma de dois quadrados. De fato, pelo Teorema 1.2.6 cada $p_i$ pode ser escrito como soma de dois quadrados. Temos ainda que se $\alpha$ for par, então $2^{\alpha} = (2^{\alpha/2})^2 + 0^2$. Por outro lado, se $\alpha$ for ímpar, então $2^{\alpha} = (2^{(\alpha-1)/2})^2 + (2^{(\alpha-1)/2})^2$. Para encerrar, como cada $\beta_j = 2c_j$, com $c_j \in \mathbb{Z}$ para $1 \leq j \leq l$, então $q_j^{\beta_j} = (q_j^{c_j})^2 + 0^2$. Assim, aplicando o lema anterior várias vezes, concluímos que $n$ pode ser escrito como soma de dois quadrados.

Reciprocamente, para mostrar que cada $\beta_j$ é par se $n$ puder ser escrito como soma de dois quadrados, é suficiente assumir que $n$ pode ser escrito como soma de quadrados e mostrar que, se $\beta_j \geq 1$, então $\beta_j \geq 2$ e $\frac{n}{q_j^2}$ também pode ser escrito como soma de dois quadrados. Suponha, pois, que $n = c^2 + d^2$, com $c, d \in \mathbb{Z}$, de sorte que $c^2 + d^2 \equiv 0 (\text{mod } q_j)$. Se $d \not\equiv 0 (\text{mod } q_j)$, então $\text{mdc}(d, q_j) = 1$, de sorte que $d$ é invertível módulo $q_j$. Sendo $f$ o inverso de $d$ módulo $q_j$, temos que $c^2 + d^2 \equiv 0 (\text{mod } q_j) \Rightarrow (cf)^2 + 1 \equiv 0 (\text{mod } q_j)$. Portanto, os teoremas 1.2.5 e 1.2.6 garantem que $q_j \equiv 1 (\text{mod } 4)$, contrariando a hipótese de que $q_j \equiv 3 (\text{mod } 4)$. Assim, devemos ter $d \equiv 0 (\text{mod } q_j)$ e, analogamente, $c \equiv 0 (\text{mod } q_j)$. Então, concluímos que $n = c^2 + d^2 \equiv 0 (\text{mod } q_j^2)$, (logo, $\beta_j \geq 2$) e $\frac{n}{q_j^2} = \left(\frac{c}{q_j}\right)^2 + \left(\frac{d}{q_j}\right)^2$. ■

Para concluirmos esta seção, mostraremos que todo primo da forma $4k+1$ é escrito como soma de dois quadrados de uma única maneira.

**Teorema 1.2.8.** *Se $p$ é um primo da forma $4k+1$, então existem únicos inteiros $x, y$ tais que $x < y$ e $p = x^2 + y^2$.*

*Demonstração.* Suponha que existam inteiros positivos $a, b, x, y$ tais que $p = a^2 + b^2 = x^2 + y^2$. É imediato que $a$, $b$, $x$ e $y$ são todos primos com $p$ e menores que $\sqrt{p}$.

Pelo teorema 1.2.4 podemos tomar inteiros $1 \leq c, z < p$ tais que $xz \equiv y \pmod{p}$ e $ac \equiv b \pmod{p}$. Afirmamos que $c = z$ ou $c + z = p$. De fato, como $xz \equiv y \pmod{p}$, temos

$$p = x^2 + y^2 \equiv x^2 + (xz)^2 = x^2(z^2 + 1) \pmod{p},$$

e, daí, $z^2 \equiv -1 \pmod{p}$. De modo análogo, obtemos $c^2 \equiv -1 \pmod{p}$, de sorte que $p \mid (z^2 - c^2)$; assim, $p \mid (z - c)$ ou $p \mid (z + c)$. Como $1 \leq c, z < p$ implica $-p < z - c < z + c < 2p$, concluímos que $z - c = 0$ ou $z + c = p$.

Se $c = z$, as congruências $xz \equiv y \pmod{p}$ e $ac \equiv b \pmod{p}$ garantem que

$$bxz \equiv acy \equiv ayz \pmod{p},$$

logo, $bx \equiv ay \pmod{p}$. Mas, como $0 < a, b, x, y < \sqrt{p}$, temos $0 < bx, ay < p$ e, consequentemente, $bx = ay$. Desse modo,

$$p = x^2 + y^2 = x^2 + \left(\frac{bx}{a}\right)^2 = \left(\frac{x}{a}\right)^2 (a^2 + b^2) = \left(\frac{x}{a}\right)^2 p,$$

de sorte que $\frac{x}{a} = 1$ e, portanto, $x = a$. Daí, $bx = ay$ implica $y = b$.

Se $z + c = p$, podemos argumentar de forma análoga à acima para concluir sucessivamente que $bx \equiv -ay \pmod{p}$ e $bx + ay = p$. Então,

$$(ax - by)^2 + p^2 = (ax - by)^2 + (bx + ay)^2 = (a^2 + b^2)(x^2 + y^2) = p^2$$

implica $ax - by = 0$, ou seja, $ax = by$. Por fim,

$$\begin{aligned} p &= bx + ay \\ xp &= bx^2 + axy = bx^2 + by^2 = b(x^2 + y^2) \\ xp &= bp \end{aligned} \tag{1.1}$$

Portanto, temos que $x = b$ e podemos concluir que $y = a$. ■

# 2 O RETICULADO DOS NÚMEROS INTEIROS

Um **reticulado** é o conjunto dos pontos do plano que têm coordenadas inteiras em relação a um sistema ortogonal de coordenadas fixado.

Esse conjunto de pontos será de extrema importância para trabalharmos nossos resultados a seguir, principalmente as propriedades da sequência de Farey no próximo capítulo. Para mostrarmos a importância do reticulado, veremos agora um teorema de extrema importância e que nos ajuda a calcular a área de qualquer polígono apenas usando pontos desse conjunto.

## 2.1 O Teorema de Pick

Para demonstrarmos o teorema de Pick, o demonstraremos inicialmente para um triângulo cujos vértices são pontos do reticulado e não há pontos do reticulado em seu interior. Desse modo, seguiremos com a definição.

**Definição 2.1.1.** *Chamamos de **triângulo primitivo** todo triângulo de vértices em pontos do reticulado que não possuem pontos do reticulado em seu interior ou lados.*

Mostraremos inicialmente que a área de um triângulo primitivo é igual a $1/2$. Para isso, relembraremos a seguinte fórmula de cálculo da área usada em geometria analítica para um triângulo de vértices $(x_1,y_1)$, $(x_2,y_2)$, $(x_3,y_3)$.

$$\frac{1}{2}\begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} = \frac{1}{2}\left|(x_1y_2 + x_2y_3 + x_3y_1 - x_1y_3 - x_2y_1 - x_3y_2)\right|.$$

Como os vértices são pontos do reticulado, então cada valor de $x$ e $y$ acima é um número inteiro, portanto a expressão em parêntesis é um inteiro. Garantimos que o resultado acima é pelo menos $1/2$, uma vez que a expressão em parêntesis será nula somente se os três pontos forem colineares, mas como estamos tratando de um triângulo de coordenadas inteiras, então a expressão em parêntesis é pelo menos 1. Para mostrarmos que a área do triângulo primitivo é exatamente $1/2$, colocaremos um triângulo $T$ em um retângulo $R$ como mostra a figura a seguir. Como podemos observar na imagem, e generalizando, cada retângulo $R$ possuirá 4 pontos do reticulado como vértices, $l-4$ pontos em seus lados que não são vértices, onde $l$ é a quantidade de pontos nos lados do retângulo, e $k$ pontos no seu interior. Particionando $R$ em $n$ triângulos primitivos, teremos que a soma de todos os ângulos desses triângulos será dada por $n180^\circ$. Por outro lado,

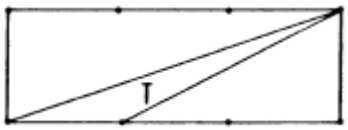


Figura 1 – O triângulo T.

os quatro vértices do retângulo somam 360°, cada ponto nos lados, que não são vértices, soma 180° e cada ponto no interior do retângulo soma 360°. Portanto, temos que

$$n180^\circ = 360^\circ k + 180^\circ(l-4) + 360^\circ,$$

ou seja,

$$n = 2k + l - 2.$$

A fórmula acima nos garante que a quantidade de triângulos primitivos na partição de $R$ depende somente da quantidade de pontos nos lados e no interior do retângulo.

Agora particionaremos o retângulo $R$ em $n$ triângulos primitivos de área $\frac{1}{2}$ cada, primeiro dividindo-o em quadrados com vertíces nos pontos do reticulado e posteriormente traçando as diagonais desse quadrado, como mostra a figura abaixo. Como os $n$ triângulos

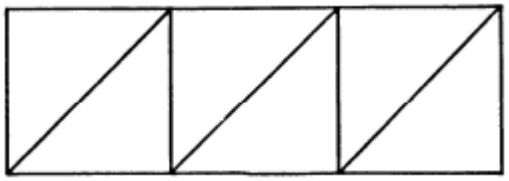

Figura 2 – Partição de R.

possuem área igual a $\frac{1}{2}$, podemos concluir que

$$\text{Área de } R = \frac{n}{2}$$

Considerando $T_1, T_2, \ldots, T_n$ sendo os $n$ triângulos em nossa partição inicial, para a obtenção da expressão $n = 2k + l - 2$, e denotando $(T_i)$ como sendo a área do triângulo $T_i$, temos que

$$(T_i) \geq \frac{1}{2}, \quad para\, i = 1, 2, \ldots, n \tag{2.1}$$

Por outro lado, como $T_i$ preenche $R$,

$$\sum_{i=1}^{n} (T_i) = (T_1) + (T_2) + \ldots + (T_n) = \frac{n}{2} \tag{2.2}$$

E pelas equações (2.1) e (2.2) podemos concluir que

$$(T_1) = (T_2) = \ldots = (T_n) = \frac{1}{2},$$

em particular temos que $(T) = \frac{1}{2}$

**Teorema 2.1.1** (Pick)**.** *Seja R um polígono qualquer com vértices em pontos do reticulado inteiro. Suponha que haja q pontos do reticulado no interior de R e p pontos nos lados desse polígono, excluindo os vértices. Então,*

$$\textit{Área de } R = q + \frac{p}{2} - 1.$$

*Demonstração.* Para demonstrarmos esse teorema faremos uso do reticulado inteiro.

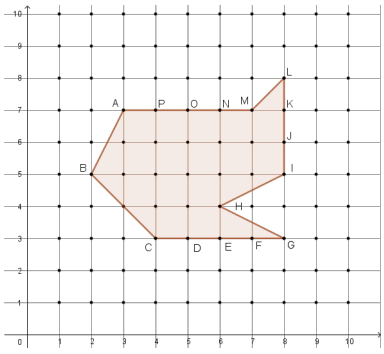


Figura 3 – O polígono $R$.

Desse modo, se há $q$ pontos interiores em $R$ e $p$ pontos nos lados de $R$, então cada ponto interior é também vértice de um triângulo primitivo e cada um desses vértices possui um ângulo de $360^\circ$, portanto, há $q360^\circ$. Cada ponto no lado, que não é um vértice do polígono $R$, também é vétrice de um triângulo primitivo e cada um desses pontos possui um ângulo de $180^\circ$, portanto, há $(p-v)180^\circ$. Por último, como a soma dos ângulos internos de um polígono é dado por $(v-2)180^\circ$, então o número $n$ de triângulos primitivos que dividem $R$ é

$$\begin{aligned} 180^\circ n &= q360^\circ + (p-v)180^\circ + (v-2)180^\circ \\ &= q360^\circ + p180^\circ - v180^\circ + v180^\circ - 360^\circ \\ &= q360^\circ + p180^\circ - 360^\circ \end{aligned} \tag{2.3}$$

e, ao dividirmos por $360^\circ$ ambos os lados de (2.3), obtemos

$$\frac{n}{2} = q + \frac{p}{2} - 1,$$

portanto,

$$\text{Área de } R = q + \frac{p}{2} - 1$$

■

Para a demonstração desse teorema assumimos sem prova a existência da decomposição de um polígono em triângulos primitivos. Para a demonstração de que existe tal decomposicão, pode-se consultar o apêndice do capítulo 5 de (HONSBERGER, 1970, p. 35).

Existe uma relação entre o teorema de Pick e a relação de Euler para poliedros, bem como um equivalente a esse teorema para o cáculo do volume de poliedros. Essas informações podem ser encontradas em (MENESES, ).

## 2.2 Outros resultados interessantes

### *2.2.1 O Teorema de Browkin*

O Teorema de Browkin afirma que, para todo inteiro positivo $n$, existe um quadrado no plano que contém exatamente $n$ pontos do reticulado em seu interior. Para demonstrarmos esse resultado, mostraremos inicialmente que dois pontos distintos do reticulado não possuem o mesmo valor pela função

$$f(x,y) = \left|x + y\sqrt{3} - \frac{1}{3}\right| + \left|x\sqrt{3} - y - \frac{\sqrt{3}}{3}\right|.$$

Sejam dois pontos distintos $(a,b),\ (c,d)$ do reticulado, vamos supor inicialmente que $f(a,b) = f(c,d)$. Ao tirarmos o módulo na igualdade $f(a,b) = f(c,d)$ obtemos inteiros $p,\ q,\ r,\ s \in \{-1,1\}$ tais que

$$p\left(a + b\sqrt{3} - \frac{1}{3}\right) + q\left(a\sqrt{3} - b - \frac{\sqrt{3}}{3}\right) = r\left(c + d\sqrt{3} - \frac{1}{3}\right) + s\left(c\sqrt{3} - d - \frac{\sqrt{3}}{3}\right)$$

agora separando a parte racional da parte irracional, teremos

$$pa - \frac{p}{3} - qb - rc + \frac{r}{3} + sd = \sqrt{3}\left(rd + sc - \frac{s}{3} - pb - qa + \frac{q}{3}\right) \tag{2.4}$$

para obtermos a igualdade na equação (2.4), devemos ter

$$pa - qb - rc + sd + \frac{r-p}{3} = 0 \tag{2.5}$$

assim como,

$$rd + sc - pb - qa + \frac{q-s}{3} = 0 \tag{2.6}$$

como os termos nas equações (2.5) e (2.6) representam inteiros, então as frações $\frac{r-p}{3}$ e $\frac{q-s}{3}$ se reduzem a inteiros de modo que os denominadores devem ser iguais a $2,\ 0,\ -2$, devido a escolha de $p,\ q,\ r,\ s$, portanto, a única opção é

$$r-p=0 \quad e \quad q-s=0 \implies p=r \quad e \quad q=s$$

As equações (2.5) e (2.6) se reduzem a

$$pa-qb-rc+sd=0 \quad e \quad rd+sc-pb-qa=0$$

Desse modo, ao multiplicarmos a primeira por $p$ e a segunda por $q$ e subtraindo a segunda da primeira obtemos

$$\begin{aligned} p^2(a-c)+q^2(a-c)&=0 \\ (a-c)(p^2+q^2)&=0 \end{aligned} \tag{2.7}$$

e como $p,q \in \{-1,1\}$, então (2.7) nos dá $2(a-c)=0 \implies a=c$, que consecutivamente nos mostra que $b=d$.

Para concluir a nossa demonstração primeiro temos que entender qual a interpretação geométrica de $f(x,y)$. De fato, os comprimentos $d_1,\ d_2$ do ponto $(x,y)$ do reticulado para as retas $L_1:\ x+y\sqrt{3}-\frac{1}{3}=0$ e $L_2:\ x\sqrt{3}-y-\frac{\sqrt{3}}{3}=0$, respectivamente. Assim,

$$|d_1|=\left|\frac{x+y\sqrt{3}-\frac{1}{3}}{\sqrt{1+3}}\right| \implies 2\,|d_1|=\left|x+y\sqrt{3}-\frac{1}{3}\right|$$

Analogamente, obtemos

$$2\,|d_2|=\left|x\sqrt{3}-y-\frac{\sqrt{3}}{3}\right|$$

então a função $f(x,y)=2\,|d_1|+2\,|d_2|$, ou seja, $f$ define o perímetro do quadrilátero formado por $d_1,\ d_2,\ L_1\ e\ L_2$. Agora tomando a sequência de pontos $p_1,\ p_2,\ldots,p_n,\ldots$ do reticulado ordenados por $f$, onde $p-1$ é o ponto onde f atinge seu menor valor no reticulado, $p_2$ é o segundo e assim em diante, e usaremos a notação $a_n$ para representar o valor de $p_n$ por $f$. Consideraremos as funções $h(x,y)=x(1+\sqrt{3})+y(\sqrt{3}-1)-\frac{1}{3}-\frac{1}{\sqrt{3}}$ e $g(x,y)=x(1-\sqrt{3})+y(1+\sqrt{3})-\frac{1}{3}+\frac{1}{\sqrt{3}}$ e considerando as quatro retas

$$h(x,y)=\pm a_{n+1} \quad e \quad g(x,y)=\pm a_{n+1}$$

temos que obviamente $h(x,y)=a_{n+1}$ é paralela a $h(x,y)=-a_{n+1}$, assim como $g(x,y)=a_{n+1}$ é paralela a $g(x,y)=-a_{n+1}$, como mostra a figura 4 abaixo. Como observado na figura e também

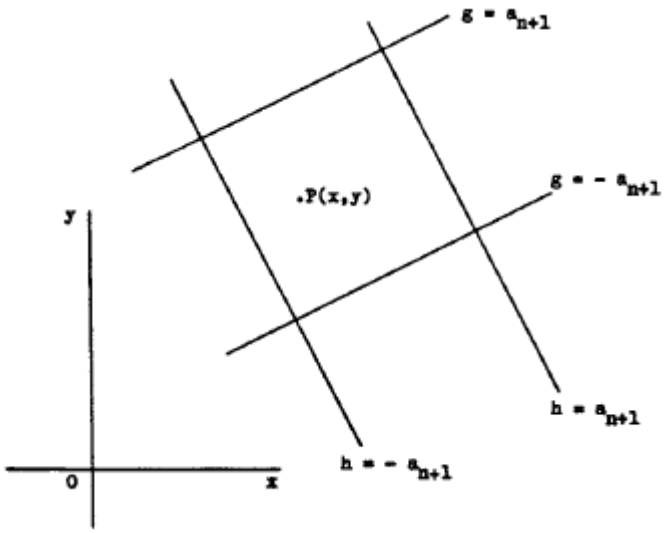


Figura 4 – O quadrado formado pelas retas $h(x,y) = \pm a_{n+1}$ e $g(x,y) = \pm a_{n+1}$.

analisando os coeficientes angulares de $h(x,y)$ e $g(x,y)$, vemos que suas retas são perpendiculares, formando assim um quadrado.

Podemos finalmente demonstrar o

**Teorema 2.2.1** (Browkin)**.** *Para todo inteiro positivo n existe um quadrado no plano que contém exatamente n pontos do reticulado em seu interior.*

*Demonstração.* Se um ponto $(x,y)$ do reticulado possui valor por $h(x,y)$ de modo que $|h(x,y)| < a_{n+1}$, então o ponto $(x,y)$ está entre as retas paralelas $h(x,y) = a_{n+1}$ e $h(x,y) = -a_{n+1}$. Vemos similarmente que $|g(x,y)| < a_{n+1}$ se, e somente se, o ponto $(x,y)$ está entre as retas paralelas $g(x,y) = a_{n+1}$ e $g(x,y) = -a_{n+1}$. Portanto, o ponto $(x,y)$ pertencerá ao quadrado se, e somente se, as duas desigualdades forem satisfeitas

$$|h(x,y)| < a_{n+1} \quad e \quad |g(x,y)| < a_{n+1} \tag{2.8}$$

o que equivale dizer que

$$\left|\frac{h(x,y)+g(x,y)}{2}\right| + \left|\frac{h(x,y)-g(x,y)}{2}\right| < a_{n+1} \tag{2.9}$$

uma vez que $|h(x,y)+g(x,y)| = \pm(h(x,y)+g(x,y))$ e $|h(x,y)-g(x,y)| = \pm(h(x,y)-g(x,y))$. Desse modo, considerando os casos em que temos $h(x,y), g(x,y), h(x,y), -g(x,y), -h(x,y), g(x,y)$

e $-h(x,y), -g(x,y)$, ao retirarmos os módulos, teremos que

$$\left|\frac{h(x,y)+g(x,y)}{2}\right| + \left|\frac{h(x,y)-g(x,y)}{2}\right| = \pm h(x,y)$$

$$ou \tag{2.10}$$

$$\left|\frac{h(x,y)+g(x,y)}{2}\right| + \left|\frac{h(x,y)-g(x,y)}{2}\right| = \pm g(x,y)$$

assim concluindo que (2.8) é equivalente a (2.9)

Substituindo a expressão para $h(x,y)$ e $g(x,y)$ e simplificando obtemos que $|f(x,y)| < a_{n+1}$, portanto, $(x,y)$ pertence ao quadrado se, e somente se, $|f(x,y)| < a_{n+1}$ e como os pontos $p_1,\ p_2, \ldots,\ p_n$ estão ordenados, como mencionado anteriormente, esses $n$ pontos satisfazem a condição acima e temos exatamente $n$ pontos no interior do quadrado. ■

### *2.2.2 O Teorema de Schinzel*

O teorema de Schinzel se baseia no número $r(n)$ de soluções inteiras $(x,y)$ da equação

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

onde

$$r(n) = 4(d_1 - d_3)$$

sendo $d_1$ a quantidade de divisores de $n$ da forma $4k+1$ e $d_3$, a quantidade de divisores de $n$ da forma $4k+3$. Usaremos esse resultado sem demonstração. Utilizaremos também a caracterização dos inteiros que podem ser escritos como soma de dois quadrados.

**Teorema 2.2.2.** *Para todo inteiro positivo n, existe um círculo no plano passando por exatamente n pontos do reticulado.*

*Demonstração.* Consideraremos os casos em que $n$ é par ou $n$ é ímpar separadamente, mostrando que

(i) Para $n = 2k$, o círculo de centro $(\frac{1}{2}, 0)$ e raio $\frac{1}{2} \cdot 5^{\frac{(k-1)}{2}}$ passa exatamente por $n$ pontos do reticulado;

(ii) Para $n = 2k+1$, o círculo com centro $(\frac{1}{3}, 0)$ e raio $\frac{1}{3} \cdot 5^k$ passa por exatamente por $n$ pontos do reticulado.

Então, para cada número par $2k$, consideraremos as soluções inteiras da equação

$$x^2 + y^2 = 5^{k-1} \tag{2.11}$$

Todos os divisores de $5^{k-1}$ são potências de 5, portanto, são da forma $4k+1$. Como de $5^0$ a $5^{k-1}$ há $k$ potências de 5, então o número de soluções de (2.11) é dado por

$$r(5^{k-1}) = 4(k-0) = 4k$$

e essas soluções são dadas por $2k$ pares $(x,y)$ e $2k$ pares $(y,x)$. E como $5^{k-1}$ é ímpar, então no par $(x,y)$ um dos valores é par e o outro ímpar. Desse modo, para cada ponto $(p,q)$ do reticulado que pertence ao círculo de centro $(\frac{1}{2},0)$ e raio $\frac{1}{2}\cdot 5^{\frac{(k-1)}{2}}$, temos que $(q,p)$ não pertence ao círculo. De fato,

$$\begin{gathered}\left(p-\frac{1}{2}\right)^2+(q-0)^2=\frac{5^{k-1}}{4}\\ (2p-1)^2+(2q)^2=5^{k-1}\end{gathered} \tag{2.12}$$

e temos que (2.11) e (2.12) nos dão que as soluções procuradas são da forma $x=2p-1$ e $y=2q$, portanto, a primeira coordenada ímpar e a segunda par. Isso nos mostra que, das $4k$ soluções da equação 2.11, só podemos considerar as $2k$ soluções da forma $(x,y)=(2p-1,2q)$, concluindo que há exatamente $n=2k$ pontos do reticulado no círculo.

Considerando agora que para cada número ímpar $2k+1$, o número de soluções inteiras de

$$x^2+y^2=5^{2k} \tag{2.13}$$

é $r(5^{2k})=4(2k+1-0)=8k+4$, então as $8k+4$ soluções são os pontos que possuem uma das formas

$$(x,y),\ (x,-y),\ (-x,y),\ (-x,-y),\ (y,x),\ (y,-x),\ (-y,x),\ (-y,-x) \tag{2.14}$$

Se um dos termos é nulo, então as soluções reduzem-se apenas a quatro números dessa lista, assim como se $x=y$. Como o lado direito de (2.13) é igual a $5^{2k}$, devemos ter uma das entradas de $(x,y)$ par e a outra ímpar, portanto, $x\neq y$. Entretanto, se uma das entradas de $(x,y)$ é zero, teremos as quatro soluções

$$(0,5^{2k}),\ (0,-5^{2k}),\ (5^{2k},0),\ (-5^{2k},0) \tag{2.15}$$

e, consequentemente, as $8k+4$ soluções são $8k$ do tipo (2.14) e quatro do tipo (2.15).

Agora, considerando o ponto $(p,q)$ do reticulado sobre o círculo com centro $(\frac{1}{3},0)$ e raio $\frac{1}{3}\cdot 5^k$, temos que

$$\begin{gathered}\left(p-\frac{1}{3}\right)^2+(q-0)^2=\frac{5^{2k}}{9};\\ (3p-1)^2+(3q)^2=5^{2k}.\end{gathered} \tag{2.16}$$

De 2.13 e 2.16 temos $x = 3p - 1$ e $y = 3q$, ou seja, $x \equiv -1 \pmod 3$ e $y \equiv 0 \pmod 3$. Como

$$5^{2k} \equiv 25^k \equiv 1^k \equiv 1 \pmod 3,$$

segue de (2.14) que as únicas possíveis soluções de (2.13) são $(x,y)$ e $(x,-y)$ e de (2.15) a única possívei soluçõe é $(-5^k,0)$, se $k$ é ímpar, onde $-5^k \equiv 1 \pmod 3$, ou $(5^k,0)$, se $k$ é par, onde $5 \equiv 1 \pmod 3$. Portanto, totalizam $2k+1$ soluções. Assim, o círculo passa por $2k+1$ pontos do reticulado. ■

### *2.2.3 O Teorema de Kulikowiski*

O Teorema de Kulikowiski estende o Teorema de Schinzel do plano para o espaço.

**Teorema 2.2.3.** *Para todo inteiro positivo n, existe uma esfera contendo exatamente n pontos do reticulado em sua superfície.*

*Demonstração.* Inicialmente, pelo Teorema 2.2.2, o plano $z = 0$ possui um círculo

$$(x-a)^2 + (y-b)^2 = c^2$$

contendo exatamente $n$ pontos do reticulado. Consequentemente uma esfera que contenha esse círculo tem pelo menos $n$ pontos em sua superfície.

Agora, considere a esfera de equação

$$(x-a)^2 + (y-b)^2 + (z-\sqrt{2})^2 = c^2 + 2$$

ou, o que é o mesmo,

$$(x-a)^2 + (y-b)^2 + z^2 - 2z\sqrt{2} = c^2. \tag{2.17}$$

Mostremos que ela possui exatamente $n$ pontos de coordenadas inteiras em sua superfície.

Pela demonstração do Teorema 2.2.2, temos que $a,b,c$ são números racionais tais que $a = \frac{1}{2}$ ou $\frac{1}{3}$, $b = 0$ e $c$ é o raio da esfera. Desse modo, os valores inteiros de $(x,y,z)$ nos dão valores racionais na equação (2.17), exceto em $-2z\sqrt{2}$. Portanto, não há inteiros $x,y,z$ que satisfaçam a equação, a menos que $z = 0$. Como visto anteriormente, há exatamente $n$ pontos da esfera que pertencem ao reticulado e ao plano $z = 0$. ■

# 3 FRAÇÕES DE FAREY

Nessa parte do trabalho, falaremos sobre uma sequência específica, cujas propriedades nos ajudarão a demonstrar teoremas geométricos a partir de propriedades artiméticas dos números inteiros. Essa sequência, conhecida como sequência de Farey, possui uma história bastante curiosa, segundo (HARDY; WRIGHT, 1938). Apesar da sequência levar seu nome, Farey não era matemático, mas um geólogo e conjecturou, na *Philosophical Maragzine* de 1816, o item (ii) do Teorema 3.1.2 que fora demonstrado por Cauchy. Porém, em 1802, Haros havia apresentado uma demonstração para todo o Teorema 3.1.2.

## 3.1 Sequências de Farey

Construiremos uma tabela onde cada linha apresentará a $n$-ésima sequência de Farey, que será representada por $F_n$. A construção se dará do seguinte modo: na primeira linha escreveremos as frações $0/1$ e $1/1$. Para $n = 2,3,\ldots$, usaremos a seguinte regra: para a $n$-ésima linha da tabela escreveremos a $(n-1)$-ésima linha, mas inserindo as frações $\frac{a+a'}{b+b'}$ entre as frações $\frac{a}{b}$ e $\frac{a'}{b'}$, quando $b+b' \leq n$. Na tabela abaixo, mostramos $F_n$ para $1 \leq n \leq 7$.

$F_1$: $\frac{0}{1}\ \frac{1}{1}$

$F_2$: $\frac{0}{1}\ \frac{1}{2}\ \frac{1}{1}$

$F_3$: $\frac{0}{1}\ \frac{1}{3}\ \frac{1}{2}\ \frac{2}{3}\ \frac{1}{1}$

$F_4$: $\frac{0}{1}\ \frac{1}{4}\ \frac{1}{3}\ \frac{1}{2}\ \frac{2}{3}\ \frac{3}{4}\ \frac{1}{1}$

$F_5$: $\frac{0}{1}\ \frac{1}{5}\ \frac{1}{4}\ \frac{1}{3}\ \frac{2}{5}\ \frac{1}{2}\ \frac{3}{5}\ \frac{2}{3}\ \frac{3}{4}\ \frac{4}{5}\ \frac{1}{1}$

$F_6$: $\frac{0}{1}\ \frac{1}{6}\ \frac{1}{5}\ \frac{1}{4}\ \frac{1}{3}\ \frac{2}{5}\ \frac{1}{2}\ \frac{3}{5}\ \frac{2}{3}\ \frac{3}{4}\ \frac{4}{5}\ \frac{5}{6}\ \frac{1}{1}$

$F_7$: $\frac{0}{1}\ \frac{1}{7}\ \frac{1}{6}\ \frac{1}{5}\ \frac{1}{4}\ \frac{2}{7}\ \frac{1}{3}\ \frac{2}{5}\ \frac{3}{7}\ \frac{1}{2}\ \frac{4}{7}\ \frac{3}{5}\ \frac{2}{3}\ \frac{5}{7}\ \frac{3}{4}\ \frac{4}{5}\ \frac{5}{6}\ \frac{6}{7}\ \frac{1}{1}$

Figura 5 – A sequência de Farey.

Como podemos observar, cada uma das linhas da tabela possui primeiro termo igual a $\frac{0}{1}$ e último igual a $\frac{1}{1}$. A seguir, apresentaremos alguns resultados que trazem propriedades

gerais dos termos dessa sequência.

**Teorema 3.1.1.** *Se $n > 1$, então não há dois termos consecutivos de $F_n$ possuindo o mesmo denominador.*

*Demonstração.* De fato, temos que se $b > 1$ e $\frac{c}{b}$ é o termo sucessor de $\frac{a}{b}$ em $F_n$, então $a+1 \leq c < b$, portanto,

$$\frac{a}{b} < \frac{a}{b-1} < \frac{a+1}{b} \leq \frac{c}{b} \tag{3.1}$$

nos mostra que $\frac{a}{b-1}$ está entre $a/b$ e $c/b$, contradizendo o fato de $\frac{a}{b}$ e $\frac{c}{b}$ serem consecutivos em $F_n$. ■

**Teorema 3.1.2.** *Se $a/b$, $c/d$ são frações consecutivas de $F_n$, então $bc - ad = 1$*

*Demonstração.* Vemos facilmente que é verdade para $n = 1$.Supondo ser verdade para a $(n-1)$-ésima linha. Qualquer fração consecutiva da $n$-ésima linha é uma das opções $a/b$, $a'/b'$ ou $a/b$, $(a+a')/(b+b')$ ou $(a+a')/(b+b')$, $a'/b'$, onde $a/b$ e $a'/b'$ são frações consecutivas da $(n-1)$-ésima linha. Como $a'b - ab' = 1$, temos que $b(a+a') - a(b+b') = a'b - ab' = 1$, asim como $a'(b+b') - b'(a+a') = a'b - ab' = 1$. O que concretiza a prova por indução. ■

**Corolário 3.1.1.** *Cada $a/b$ na tabela é uma fração própria, ou seja,* $\text{mdc}(a,b) = 1$

**Corolário 3.1.2.** *As frações de cada linha $F_n$ estão dispostas em ordem crescente.*

**Teorema 3.1.3.** *Se $\frac{a}{b}$ e $\frac{c}{d}$ são dois termos de $F_n$, de modo que não exista outro termo de $F_n$ entre essas frações, então*

$$\left|\frac{a}{b} - \frac{a+c}{b+d}\right| = \frac{1}{b(b+d)} \leq \frac{1}{b(n+1)},$$

*e*

$$\left|\frac{c}{d} - \frac{a+c}{b+d}\right| = \frac{1}{d(b+d)} \leq \frac{1}{d(n+1)}$$

*Demonstração.* Temos que

$$\left|\frac{a}{b} - \frac{a+c}{b+d}\right| = \frac{|ad-bc|}{b(b+d)} = \frac{1}{b(b+d)} \leq \frac{1}{b(n+1)}$$

devido ao teorema 3.1.2 e ao fato de que $b+d \geq n+1$. A segunda expressão pode ser demonstrada analogamente. ■

## 3.2 Os círculos de Ford

Nesta seção, utilizaremos frações de Farey para apresentar um novo ente matemático chamado de **Círculos de Ford**. Tais círculos são criados a partir da escolha de dois inteiros $p,q$ primos entre si, onde cada círculo $C(p,q)$ criados por esses dois inteiros terá raio igual a $\frac{1}{2q^2}$ e será centrado no ponto

$$\left(\frac{p}{q},\pm\frac{1}{2q^2}\right)$$

A figura abaixo apresenta um exemplo dos círculos de Ford e nela podemos observar a sequência de círculos tangentes entre si. É obvio que existem círculos que não se tangenciam, mostraremos a frente quando há a tangência entre esses círculos.

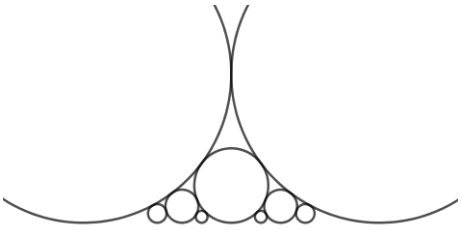

Figura 6 – Os círculos de Ford.

A sequência de Ford se assemelha a sequência de Farey pelo fato de trabalharmos com frações próprias, ou seja, em que $mdc(p,q)=1$. Devido a esse fato, usaremos os teoremas já demonstrados a respeito das propriedades da sequência de Farey, mas antes iremos enunciar a tangência dos círculos como um teorema.

**Teorema 3.2.1.** *Sejam $C(p,q)$ e $C(p',q')$ dois círculos de Ford. Se $p/q,\ p'/q'$ são termos consecutivos da sequência de Farey, então $C(p,q)$ e $C(p',q')$ são tangentes.*

*Demonstração.* De fato, começaremos calculando a distância entre os centros de $C(p,q)$ e $C(p',q')$, assim

$$d^2=\left(\frac{p}{q}-\frac{p'}{q'}\right)^2+\left(\frac{1}{2q^2}-\frac{1}{2q'^2}\right)^2 \tag{3.2}$$

Agora calculando a soma dos raios de $C(p,q)$ e $C(p',q')$ temos

$$s=\frac{1}{2q^2}+\frac{1}{2q'^2} \tag{3.3}$$

e, por último, calculando a diferença entre (3.2) e o quadrado de (3.3) obtemos que

$$\begin{aligned} d^2 - s^2 &= \left(\frac{p}{q} - \frac{p'}{q'}\right)^2 + \left(\frac{1}{2q^2} - \frac{1}{2q'^2}\right)^2 - \left(\frac{1}{2q^2} + \frac{1}{2q'^2}\right)^2 \\ &= \left(\frac{p}{q}\right)^2 - 2\frac{pp'}{qq'} + \left(\frac{p'}{q'}\right)^2 - \frac{4}{4q^2q'^2} \\ &= \frac{p^2q'^2}{q^2q'^2} - 2\frac{pp'qq'}{q^2q'^2} + \frac{p'^2q^2}{q^2q'^2} - \frac{1}{q^2q'^2} \\ &= \frac{(pq' - p'q)^2 - 1}{q^2q'^2} \end{aligned} \tag{3.4}$$

E como é sabido, pelo teorema 3.1.2 (i), que se $p/q,\ p'/q'$ são termos consecutivos de $F_n$, então $pq' - p'q = 1$, e a expressão em 3.4 se reduz a

$$d^2 - s^2 = 0 \Rightarrow |d| = |s|$$

portanto, $d = s$ garante que $C(p,q)$ e $C(p',q')$ são tangentes. ■

O fato de $p/q,\ p'/q'$ serem termos consecutivos de $F_n$ é o que garante a tangência. Assim, podemos usar a sequência de Farey para criar os círculos de Ford. Os círculos de Ford possuem grande importância, pois suas tangencias ao eixo-x constroem os números racionais.

# 4 O TEOREMA DE HURWITZ

## 4.1 Aproximações de irracionais por racionais

**Teorema 4.1.1.** *Se n é um inteiro positivo e x um número real, existe uma fração $\frac{a}{b}$ tal que*

$$\left|x-\frac{a}{b}\right| \leq \frac{1}{b(n+1)}$$

*Demonstração.* Pelo teorema 3.1.3, temos que

$$\left|\frac{a}{b}-\frac{a+c}{b+d}\right| = \frac{1}{b(b+d)} \leq \frac{1}{b(n+1)} \tag{4.1}$$

Sendo um número real $x$ tal que $\frac{a}{b} < x < \frac{a+c}{b+d}$. Então, ainda pelo teorema 3.1.3, temos que

$$\left|x-\frac{a}{b}\right| \leq \left|\frac{a}{b}-\frac{a+c}{b+d}\right| \leq \frac{1}{b(n+1)} \tag{4.2}$$

e a expressão (4.2) nos mostra o que desejávamos. ■

Agora, com uso do teorema anterior, demonstraremos o nosso primeiro teorema acerca da aproximação de números irracionais a partir de números racionais. Tal teorema é devido à Dirichlet e históricamente foi o primeiro teorema sobre aproximação de números irracionais, devido a isso estamos o apresentando neste trabalho.

**Teorema 4.1.2** (Dirichlet)**.** *Se $\xi$ é um número irracional, então há uma infinidade de frações $\frac{a}{b}$ tais que*

$$\left|\xi-\frac{a}{b}\right| < \frac{1}{b^2}$$

*Demonstração.* Pelo teorema 4.1.1, para qualquer inteiro $n > 0$ podemos achar um $a_n$ e um $b_n$, com $0 < b_n \leq n$, tais que

$$\left|\xi-\frac{a_n}{b_n}\right| \leq \frac{1}{b_n(n+1)} \tag{4.3}$$

e supondo que (4.3) é válida para uma quantidade finita de inteiros, deve existir um $k$ tal que

$$\left|\xi-\frac{a_n}{b_n}\right| \geq \left|\xi-\frac{a_k}{b_k}\right| \tag{4.4}$$

e como $\xi$ é um número irracional, afirmamos que

$$\left|\xi-\frac{a_k}{b_k}\right| > 0,$$

ou seja, podemos achar um $n$ suficientemente grande tal que

$$\frac{1}{n+1} < \left|\xi-\frac{a_k}{b_k}\right|.$$

Portanto,

$$\left|\xi - \frac{a_k}{b_k}\right| \leq \left|\xi - \frac{a_n}{b_n}\right| \leq \frac{1}{b(n+1)} \leq \frac{1}{n+1} < \left|\xi - \frac{a_k}{b_k}\right| \tag{4.5}$$

o que é um absurdo, logo devemos ter uma infinidade de inteiros $n$ para os quais é válido

$$\left|\xi - \frac{a_n}{b_n}\right| < \frac{1}{b_n(n+1)} < \frac{1}{b_n^2} \tag{4.6}$$

■

O resultado acima nos mostra que se tomarmos uma fração com denominador 10, então a aproximação do número irracional terá um "erro"menor que um centésimo, caso o denominador seja 1000, então a aproximação racional terá um erro menor que um miilionésimo. Portanto, quanto maior o denominador, mais próxima será a nossa aproximação racional.

## 4.2 O teorema de Hurwitz

**Lema 4.2.1.** *Se x e y são inteiros positivos, então apenas uma das duas desiguladades*

$$\frac{1}{xy} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2} + \frac{1}{y^2}\right), \qquad \frac{1}{x(x+y)} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2} + \frac{1}{(x+y)^2}\right)$$

*pode ser válida.*

*Demonstração.* Essas duas desigualdades podem ser escritas como

$$\sqrt{5}xy \geq y^2 + x^2, \quad \sqrt{5}x(x+y) \geq (x+y)^2 + x^2.$$

Somando essas igualdades, obtemos $\sqrt{5}(x^2+xy) \geq 3x^2 + 2xy + 2y^2$, portanto, $2y^2 - 2(\sqrt{5}-1)xy + (3-\sqrt{5})x^2 \leq 0$. Multiplicando-as por 2 e reescrevendo-as, temos

$$4y^2 - 4(\sqrt{5}-1)xy + (5 - 2\sqrt{5} + 1)x^2 \leq 0,$$

ou seja, $(2y - (\sqrt{5}-1)x)^2 \leq 0$. Para $x$ e $y$ inteiros positivos a desigualdade anterior é impossível, pois $\sqrt{5}$ é irracional. ■

**Teorema 4.2.1** (Hurwitz)**.** *Dado qualquer número irracional $\xi$, existem uma infinidade de números racionais $\frac{p}{q}$ para os quais*

$$\left|\xi - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2} \tag{4.7}$$

*Demonstração.* Seja $n$ um inteiro positivo. Existem duas frações consecutivas $a/b$ e $c/d$ em $F_n$, de modo que $a/b < \xi < c/d$. Provaremos que pelo menos uma das frações $a/b, \quad c/d, \quad (a+c)/(b+d)$ servirá como $p/q$ em (4.7). Mostraremos isso por contradição. Assumindo inicialmente que $\xi < (a+c)/(b+d)$, vamos supor que

$$\xi - \frac{a}{b} \geq \frac{1}{b^2\sqrt{5}}, \quad \frac{a+c}{b+d} - \xi \geq \frac{1}{(b+d)^2\sqrt{5}}, \quad \frac{c}{d} - \xi \geq \frac{1}{d^2\sqrt{5}}.$$

Adicionando a primeira com a terceira desiguladade e a primeira com a segunda desigualdade, obteremos

$$\frac{c}{d} - \frac{a}{b} \geq \frac{1}{d^2\sqrt{5}} + \frac{1}{b^2\sqrt{5}}, \quad \frac{a+c}{b+d} - \frac{a}{b} \geq \frac{1}{(b+d)^2\sqrt{5}} + \frac{1}{b^2\sqrt{5}}$$

Portanto,

$$\frac{1}{bd} = \frac{cb-ad}{bd} = \frac{c}{d} - \frac{a}{b} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{b^2} + \frac{1}{d^2}\right)$$

e

$$\frac{1}{b(b+d)} = \frac{(a+c)b-(b+d)a}{b(b+d)} \geq \frac{1}{\sqrt{5}}\left(\frac{1}{b^2} + \frac{1}{(b+d)^2}\right).$$

Essas duas desigualdades contradizem o lema 4.2.1, portanto, pelo menos uma das frações $a/b, \quad c/d, \quad (a+c)/(b+d)$ servem como $p/q$ em (4.7). De maneira análoga pode-se demonstrar o caso em que $\xi > (a+c)/(b+d)$. Desse modo, mostramos a existência de alguma fração $p/q$ satisfazendo ao teorema. Para mostrarmos a infinidade de frações $p/q$ satisfazendo o nosso teorema, uma vez que $p/q$ depende da escolha de $n$ como mostrado acima. Desse modo, faremos uso do teorma 3.1.3, onde teremos

$$\left|\xi - \frac{p}{q}\right| < \left|\frac{c}{d} - \frac{a}{b}\right| = \left|\frac{c}{d} - \frac{a+c}{b+d}\right| + \left|\frac{a+c}{b+d} - \frac{a}{b}\right| \leq \frac{1}{d(n+1)} + \frac{1}{b(n+1)} \leq \frac{2}{n+1},$$

onde $a/b < \xi < c/d$. Agora vamos supor que alguma fração $p_1/q_1$ satisfaz (4.7). Então $\left|\xi - \frac{p_1}{q_1}\right|$ é positiva e podemos escolher $n > 2/\left|\xi - \frac{p_1}{q_1}\right|$. A sequência de Farey de ordem $n$ produz uma fração $p/q$ satisfazendo (4.7) de tal modo que

$$\left|\xi - \frac{p}{q}\right| \leq \frac{2}{n+1} < \left|\xi - \frac{p_1}{q_1}\right|.$$

Isso nos mosrta a existência de uma infinidade de números racionais $p/q$ que satisfaz (4.7) desde que, dado um racional, podemos encontrar outro que está próximo de $\xi$. ■

**Teorema 4.2.2.** *No teorema 4.2.1, a constante $\sqrt{5}$ é o valor que otimiza a expressão. Em outras palavras, o teorema não é válido caso o $\sqrt{5}$ seja trocado por qualquer outro número real $m > \sqrt{5}$.*

*Demonstração.* Precisamos exibir um $\xi$ para o qual $\sqrt{5}$ não pode ser substituído para grandes valores. Portanto, tomemos $\xi = (1+\sqrt{5})/2$, então

$$(x-\xi)\left(x-\frac{1-\sqrt{5}}{2}\right) = x^2 - x - 1.$$

Para inteiros $p, q$ com $q > 0$, temos que

$$\begin{aligned} \left|\frac{p}{q}-\xi\right|\left|\frac{p}{q}-\xi+\sqrt{5}\right| = \\ \left|\left(\frac{p}{q}-\xi\right)\left(\frac{p}{q}-\xi+\sqrt{5}\right)\right| = \\ \left|\frac{p^2}{q^2}-\frac{p}{q}-1\right| = \frac{1}{q^2}|p^2-pq-q^2| \end{aligned} \tag{4.8}$$

■

a expressão a esquerda em (4.8) é diferente de zero, uma vez que $\xi$ e $\sqrt{5}-\xi$ são irracionais. A expressão $\left|p^2-pq-q^2\right|$ é um inteiro não negativo. Portanto

$$\left|\frac{p}{q}-\xi\right|\left|\frac{p}{q}-\xi+\sqrt{5}\right| \geq \frac{1}{q^2} \tag{4.9}$$

agora supondo que tenhamos uma sequência infinita de números racionais $p_i/q_i$, com $q_i > 0$, e um número real positivo $m$ de modo que

$$\left|\frac{p_i}{q_i}-\xi\right| < \frac{1}{m{q_j}^2}. \tag{4.10}$$

então $q_i\xi - \frac{1}{mq_i} < p_i < q_i\xi + \frac{1}{mq_i}$, e isso implica que existe apenas um número finito de $p_i$ correspondente a cada $q_i$. Desse modo, temos que $q_i \to \infty$ quando $i \to \infty$. Assim, por (4.8),(4.2) e pela desigualdade triangular, temos que

$$\frac{1}{{q_i}^2} \leq \left|\frac{p_i}{q_i}-\xi\right|\left|\frac{p_i}{q_i}-\xi+\sqrt{5}\right| < \frac{1}{mq_i^2}\left(\frac{1}{mq_i^2}+\sqrt{5}\right)$$

ou seja,

$$m < \frac{1}{mq_i^2}+\sqrt{5}$$

e, portanto,

$$m \leq \lim_{i\to\infty}\frac{1}{mq_i^2}+\sqrt{5} = \sqrt{5}.$$

# 5 CONCLUSÃO

Então concluí-se que o reticulado dos números inteiros apresenta propriedades que o torna uma ferramenta importante para a demonstração de teoremas geométricos e, como podemos ver em (MENESES, ), também constitui uma ferramenta pedagógica poderosa para a compreensão do cálculo de áreas de polígonos utilizando malhas quadriculadas com o uso do teorema de Pick.

Pode-se observar também em (NORTHSHIELD, ) que os círculos de Ford são entes geométricos importantes devido as suas tangências, pois tais tagências constroem geometricamente o conjunto dos números racionais, podendo assim ser um referêncial geométrico para se trabalhar o conjunto dos números racionais com alunos de nível médio. No trabalho citado, podemos verificar a existência das tangências das esferas de Ford, ou seja, uma equivalência entre as tangências dos círculos de Ford.

Concluí-se também, como mostra (HONSBERGER, 1970), que ao associarmos as frações da sequência de Farey às coordenadas dos pontos do reticulado inteiro, podemos não somente demonstrar as propriedades de tal sequência e mostrar a existência dos círculos de Ford, mas também podemos trabalhar com aproximação de números irracionais por números racionais, desenvolvendo assim os teoremas de aproximação, conforme (NIVEN; ZUCKERMAN, 1960). Isso torna o cálculo do valor aproximado de números irracionais uma opção viável para alunos de nível médio, uma vez que pode-se auxiliar na resolução de algum problema que envolva o uso de números irracionais.

## REFERÊNCIAS


BHASKAR, J. Sum of two squares. 2015. Disponível em: <https://www.math.uchicago.edu/ may/VIGRE/VIGRE2008/REUPapers/Bhaskar.pdf>. Acesso em: 23 dez. 2019. 2008.

CONWAY, J. H.; GUY, R. K. **The Book of Numbers**. 1. ed. New York: Copernicus, 1995. v. 1.

ERDOS, P.; SURANYI, J. **Topics in the Theory of Numbers**. 1. ed. EUA: Springer, 2000. v. 1.

HARDY, G. H.; WRIGHT, E. M. **An Introducton to Theory of Numbers**. 4. ed. New York: Oxford University Press, 1938. v. 1.

HONSBERGER, R. **Ingenuity in Mathematics**. 4. ed. EUA: Mathematical Association of America, 1970. v. 23.

HONSBERGER, R. **Mathematical Gems**. 1. ed. EUA: Mathematical Association Of America, 1973. v. 1.

MENESES, P. de O. **Teorema de Pick e teorema espacial tipo-Pick: Demonstrações e aplicações no ensino médio**. 2016. 84 f. Dissertação (Mestrado em Matemática em Rede Nacional) – Centro de Ciências, Universidade Federal do Ceará, Fortaleza, 2016.

NETO, A. C. M. **Tópicos de Matemática Elementar**. 2. ed. Rio de Janeiro: SBM, 2013. v. 5.

NIVEN, I.; ZUCKERMAN, H. S. **An introduction to the Theory of Numbers**. 5. ed. New York: John Wiley Sons Inc, 1960. v. 1.

NORTHSHIELD, S. Ford circles and spheres. 2008. Disponível em: <https://arxiv.org/abs/1503.00813v1>. Acesso em: 23 dez. 2019.

ROBERTS, J. **Elementary Number Theory: A Problem Oriented Approach**. 1. ed. Massachusetts: THE MIT PRESS, 1977. v. 1.

ZUKIN, D. The farey sequence and its niche(s). 2016. Disponível em: <https://www.whitman.edu/Documents/Academics/Mathematics/2016/Zukin.pdf> . Acesso em: 23 dez.2019.