



Universidade Regional do Cariri - URCA  
Departamento de Matemática  
Programa de Mestrado Profissional em  
Matemática em Rede Nacional



# O método de Minkowski e a representação de um inteiro como soma de quadrados

Francisco Vlademir Dedes da Cruz Barros

Juazeiro do Norte - CE

2020

# O método de Minkowski e a representação de um inteiro como soma de quadrados

Francisco Vlademir Dedes da Cruz Barros

Dissertação apresentada ao Departamento de Matemática Pura e Aplicada da Universidade Regional do Cariri como parte dos requisitos exigidos para a obtenção do título de Mestre em matemática.

## **Orientador**

Prof. Dr. Jocel Faustino Norberto de Oliveira

Juazeiro do Norte - CE

2020

**Catálogo na fonte**  
**Cícero Antônio Gomes Silva – CRB-3 nº /1385**

B277

Barros, Francisco Vlademir Dedes da Cruz.

O Método de Minkowski e a Representação de um Inteiro como Soma de Quadrados./ Francisco Vlademir Dedes da Cruz Barros – Juazeiro do Norte-Ce, 2020,  
79 f.: il.;30cm.

Dissertação (Mestrado) Programa de Mestrado Profissional em Matemática em Redes - PROFMAT

Orientador: Profº.Dr. Jocel Faustino Norberto de Oliveira

1.Inteiros 2.Soma 3.Quadrado I. Título

CDD: 510

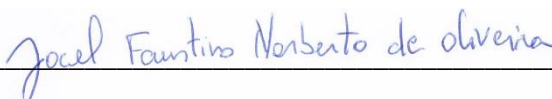
# O método de Minkowski e a representação de um inteiro como soma de quadrados

**Francisco Vlademir Dedes da Cruz Barros**

Dissertação apresentada ao Departamento de Matemática Pura e Aplicada da Universidade Regional do Cariri como parte dos requisitos exigidos para a obtenção do título mestre em matemática.

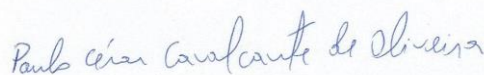
Aprovada em: 29/06/2020.

## BANCA EXAMINADORA



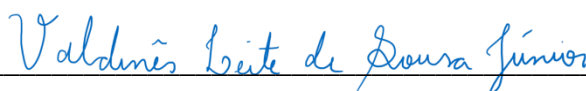
Prof. Dr. Jocel Faustino Norberto de Oliveira (Orientador)

Universidade Regional do Cariri (URCA)



Dr. Paulo César Cavalcante de Oliveira

Universidade Regional do Cariri (URCA)



Prof. Dr. Valdinês Leite de Souza Júnior

Universidade Federal do Cariri (UFCA)

*Dedico a minha esposa Edvania de Sousa Ramalho Dedes e tripla coordenada que mais amamos ( $v_1, v_2, v_3$ ), Vilker, Vinícius e Vitor, nossos filhos.*

# Agradecimentos

Agradeço a Deus, fonte de toda sabedoria, a minha família, em especial a minha esposa Edvania de Sousa Ramalho Dedes por amparo e paciência em horas difíceis, aos meus professores pelo carinho, dedicação e esforço na busca da excelência em seus trabalhos, singularmente ao professor Jocel Faustino Norberto de Oliveira, pela atenção e ajuda na realização desse trabalho. Agradeço também a Capes por seu suporte financeiro.

“A imaginação é mais importante que o conhecimento.” (Albert Einstein)

## Resumo

Neste trabalho examinamos as representações de um inteiro como uma soma de quadrados, e a proposta principal é apresentação do Método de Minkowski, que é uma ferramenta de contagem que determina quantos modos podemos ter  $n = a^2 + b^2$  com  $a$  e  $b$  co-primos. A fim de alcançar esse objetivo, revisamos algumas definições e resultados de Teoria dos Números como suporte fundamental para uma melhor compreensão desse Método. Em seguida, comprovamos a validade do resultado principal deste trabalho com bases no entendimento de noções de Álgebra linear e também de Álgebra abstrata; por isso, abordamos ideias dessas disciplinas para construir uma relação sólida entre o conceito de forma quadrática com o conceito de pontos no plano complexo. Essa relação nos permitiu deduzir resultados sobre o primeiro conceito trabalhando com o segundo, que evidentemente é mais simples de se trabalhar. E finalizamos este trabalho, resolvendo exemplos e exercícios que podem ser explorados em polos de treinamentos olímpicos para matemáticos. O assunto para resolução das questões propostas foi abordado durante toda a dissertação.

**Palavras-chave:** Inteiros, Soma, Quadrados, Minkowski.



## Abstract

In this work we examine the representations of an integer as a sum of squares, and the main proposal is to present the Minkowski Method, which is a counting tool that determines how many modes we can have  $n = a^2 + b^2$  with  $a$  and  $b$  co-prime. In order to achieve this goal, we reviewed some definitions and results of Number Theory as fundamental support for a better understanding of this Method. Then, we prove the validity of the main result of this work based on the understanding of notions of linear algebra and also of abstract algebra; therefore, we approach ideas from these disciplines to build a solid connection between the concept in a quadratic way with the concept of points in the complex plane. This connection allowed us to deduce results about the first concept working with the second, which is evidently simpler to work with. And we finished this work, solving examples and exercises that can be explored in Olympic training centers for mathematicians. The issue for resolving the proposed questions was addressed throughout the dissertation.

**Keywords:** Integers, Sum, Squares, Minkowski.

## Lista de Figuras

4.1	Semi Plano Complexo $\mathbb{H}$ e $\mathbb{H}_0$ . . . . .	56
4.2	Representantes das Formas binárias. . . . .	60
4.3	Representações próprias no $\mathbb{R}^2$ . . . . .	70
4.4	Pista de corrida . . . . .	72

## Lista de Tabelas

4.1	Tabelas de Possibilidades . . . . .	74
-----	-------------------------------------	----

# Sumário

<b>1</b>	<b>Introdução</b>	<b>13</b>
<b>2</b>	<b>Preliminares</b>	<b>16</b>
2.1	Divisibilidade . . . . .	16
2.2	Máximo Divisor Comum . . . . .	18
2.3	Teorema Fundamental da Aritmética . . . . .	22
2.3.1	Números Primos . . . . .	22
2.4	Aritmética dos Restos . . . . .	24
2.5	Congruências Lineares . . . . .	27
2.6	Congruência Quadrática . . . . .	31
2.7	Uma revisão de Álgebra Linear . . . . .	33
2.8	Algumas definições em Álgebra Abstrata . . . . .	38
<b>3</b>	<b>Soma de Quadrados</b>	<b>41</b>
3.1	Soma de Quatro Quadrados . . . . .	48
<b>4</b>	<b>O Método de Minkowski</b>	<b>55</b>
4.1	Domínio Fundamental para Ação de $SL$ sobre $\mathbb{H}$ . . . . .	55
4.2	Relação entre Formas Quadráticas Binárias e o Plano $\mathbb{H}$ . . . . .	59
4.3	Teoremas principais . . . . .	67
4.4	Questões Olímpicas e Mais Exemplos . . . . .	71

# 1 Introdução

Apesar do tema sugerir algo de fácil entendimento, soma de quadrados, informações a respeito de possibilidades e como fazê-lo, precisamos de elementos de álgebra não tão elementares assim. Abordamos a existência de representação de inteiros como soma de quadrados. A escolha do tema se justifica pelo fato de tratar de diversos conceitos em Teoria dos Números, área que está intimamente ligada às atividades de treinamento para olimpíadas de Matemática, algo diretamente relacionado à nossa atividade de docência em Matemática no ensino básico.

Para abordagem do tema, precisamos fazer uma digressão a respeito de alguns tópicos em Álgebra linear, bem como em Álgebra Abstrata, mas antes, necessitamos do embasamento teórico em Aritmética, de onde surgiu a ideia inicial para fazermos este trabalho. Essa revisão será feita na seção de preliminares, que serão usadas nos capítulos subsequentes.

Nosso trabalho é baseado no estudo do capítulo 06 do livro “Teoria dos Números”, dos autores: *Salahoddin Shokranian, Marcus Soares e Hemar Godinho* [11]. A intenção é discorrer um pouco sobre um tema bastante interessante por si só, pois engloba conceitos aprendidos na disciplina de Aritmética, do PROFMAT, de tal forma que podemos fazer um link com questões aplicadas em olimpíadas de Matemática.

Escrever um número inteiro como soma de quadrados é uma prática muito antiga. A Placa de Plimpton 322, um achado arqueológico do início do século XX, é talvez o registro mais velho da escrita de um número inteiro como soma de quadrados [4], pois esse tablete de argila escrito pelos babilônicos, data aproximadamente 3700 anos e contém uma lista de trios pitagóricos, ou seja, um número inteiro, embora ao quadrado, decomposto como soma de dois quadrados. No mesmo trabalho que comunica essa descoberta [4] defende que o uso de tais tabletas por parte desse povo antigo iria

além do ensino dos escribas, seria também aplicado para uso de construções de canais, templos e palácios.

Exploramos uma aplicação da Geometria dos Números, uma ferramenta de contagem, conhecida por **Método de Minkowski**, para contar de quantas formas podemos escrever um inteiro  $n$  como soma de dois quadrados. Inicialmente, a ideia é que podemos pensar em escrever um inteiro positivo como soma de quadrados, teoria que inicialmente foi estudada por P. Fermat. A seguir, damos um próximo passo, onde pretendemos fazer a descrição de um caso em específico, qual seja, escrever um número inteiro positivo como soma de quatro quadrados. Para encerrar esse estudo de representação de inteiro como soma de quadrados, não poderíamos deixar de apresentar a teoria de Minkowski para escrever um inteiro positivo  $m$ , como sendo soma de quadrados com parcelas formadas por números inteiros co-primos (primos entre si).

Embora tenhamos enxergado o método como uma ferramenta de Matemática avançada, as bases que alicerçam o mesmo serão conteúdo da Matemática do ensino fundamental ou médio [10] como: Divisibilidade, MMC, Algoritmo Euclidiano da Divisão e Teorema Fundamental da Aritmética

O trabalho está esquematizado da seguinte forma: No capítulo 2, iniciamos fazendo umas preliminares abordando os elementos mais básicos da aritmética, desde divisibilidade até congruência quadrática, passando pela aritmética dos restos e congruências lineares. Muitos resultados serão apresentados sem as demonstrações, que podem ser encontradas nas referências [2] e [11]. A seguir, no capítulo 3 abordamos a soma de quadrados, que possui alguns teoremas importantes e exemplos a eles relacionados. Também contém uma subseção dedicada a escrita de um inteiro como soma de quatro quadrados. No quarto e último capítulo, abordamos o Método de Minkowski, que nos permite contar as maneiras de como se escrever um número inteiro positivo como soma

de quadrados co-primos. Dividimos em quatro subseções, Domínio Fundamental para ação  $\mathbb{S}\mathbb{L}$  sobre  $\mathbb{H}$ , Relação entre Formas quadráticas binárias e o plano  $\mathbb{H}$ . As duas últimas seções são dedicadas diretamente ao método de Mikowski, sendo a subseção final apresentada com exemplos e exercícios, que de certo modo tem relação com os exercícios de treinamento para olimpíadas de Matemática.

## 2 Preliminares

### 2.1 Divisibilidade

Fato é que a divisão entre dois números naturais nem sempre tem como resposta outro natural, mas se assim não for, expressamos esta possibilidade através da relação de divisibilidade. E mesmo quando não existir uma relação de divisibilidade entre dois números naturais, podemos efetuar uma divisão com “resto pequeno” entre os mesmos, chamada de divisão euclidiana.

**Definição 1.** *Dados  $a$  e  $b \in \mathbb{N}$  com  $a \neq 0$  diremos que  $a$  divide  $b$ , escrevemos  $a|b$ , quando existir  $c \in \mathbb{N}$  tal que  $b = a \cdot c$ . E assim dizemos que  $a$  é divisor ou fator de  $b$ , ou ainda, que  $b$  é um múltiplo de  $a$ .*

**Proposição 1.** *Sejam  $a$  e  $b \in \mathbb{N}^*$  e  $c \in \mathbb{N}$  tem se que*

i)  $1|c$ ,  $a|a$  e  $a|0$ ;

ii) *Se  $a|b$  e  $b|c$  então  $a|c$ .*

*Obs:*  $\mathbb{N}^* = (\mathbb{N} - \{0\})$ .

A demonstração pode ser encontrada em [2], pág. 31.

**Proposição 2.** *Se  $a, b, c, d \in \mathbb{N}$ , com  $a \neq 0$  e  $c \neq 0$ , então*

$$a|b \text{ e } c|d \implies a \cdot c|b \cdot d.$$

A demonstração pode ser encontrada em [2], pág. 31.

**Proposição 3.** *Sejam  $a, b, c \in \mathbb{N}$ , com  $a \neq 0$  tais que  $a|(b + c)$ . Então*

$$a|b \iff a|c.$$



*Demonstração.* Uma vez que  $a|(b+c)$  então existe  $k \in \mathbb{N}$  tal que  $k \cdot a = b+c$ . Supondo que  $a|b$  então existe  $t \in \mathbb{N}$  tal que  $t \cdot a = b$  substituindo na igualdade acima temos

$$t \cdot a + c = k \cdot a,$$

por isso,  $k \cdot a > t \cdot a$ , logo,  $k > t$ . E por conta da distributividade do produto com relação a subtração, obtemos

$$c = k \cdot a - t \cdot a = (k - t) \cdot a,$$

o que implica que  $a|c$ , já que  $k - t \in \mathbb{N}$ .

A prova da recíproca é totalmente semelhante. □

De fato, uma vez que  $17|51 = 17 + 34$  e como  $17|17$ , isto implica, que  $17|34$ .

**Proposição 4.** *Sejam  $a, b, c \in \mathbb{N}$  com  $a \neq 0$  e  $c \leq b$  tais que  $a|(b - c)$ . Então.*

$$a|b \iff a|c.$$

A demonstração pode ser encontrada em [2], pág. 32.

**Proposição 5.** *Se  $a, b, c \in \mathbb{N}$  com  $a \neq 0$  e  $x, y \in \mathbb{N}$  são tais que  $a|b$  e  $a|c$ , então*

$$a|(xb + yc),$$

*e se  $yc \leq xb$ , então*

$$a|(xb - yc).$$

*Demonstração.* Como  $a|b$  e  $a|c$  então, existem  $k, t \in \mathbb{N}$  tais que  $b = k \cdot a$  e  $c = t \cdot a$ .

Logo,

$$xb \pm yc = x(k \cdot a) \pm y(t \cdot a) = (xk \pm yt)a,$$

o que prova o resultado, pois devida as circunstâncias, temos  $xk \pm yt \in \mathbb{N}$ . □

Como exemplo, temos:  $3|9$  e  $3|6$  então  $3|2 \cdot 9 + 3 \cdot 6 = 36$  e  $3|3 \cdot 9 - 3 \cdot 6 = 9$ .

**Proposição 6.** *Dados  $a, b \in \mathbb{N}^*$  temos que*

$$a|b \implies a \leq b.$$

*Demonstração.* Se  $a|b$  então existe  $c \in \mathbb{N}^*$  tal que  $b = ac$ , com  $1 \leq c$  uma vez que, a multiplicação é compatível com respeito a relação “menor igual que” então

$$1 \leq c \iff a \leq ac = b.$$

□

A recíproca da Proposição 6, não é válida, pois  $2 \leq 3$  e 2 não divide 3.

As proposições anteriores nos garante que a divisibilidade em  $\mathbb{N}^*$  é uma relação de ordem, pois:

- (i) É reflexiva;  $\forall a \in \mathbb{N}^*, a|a$  (Proposição 1);
- (ii) É transitiva: Se  $a|b$  e  $b|c$  então  $a|c$  (Proposição 1);
- (iii) É antissimétrica: Se  $a|b$  e  $b|a$  então  $a = b$  (Proposição 6).

## 2.2 Máximo Divisor Comum

**Definição 2.** *Dados  $a$  e  $b \in \mathbb{N}$  não simultaneamente nulos, diremos que  $d \in \mathbb{N}^*$  é um divisor comum de  $a$  e  $b$  quando  $d|a$  e  $d|b$ .*

E  $d$  é um máximo divisor comum (mdc) de  $a$  e  $b$  quando este satisfaz as seguintes propriedades:

- i)  $d$  é um divisor comum de  $a$  e de  $b$ ;
- ii)  $d$  é divisível por todo divisor comum de  $a$  e  $b$ .

Desta forma, temos que  $\{1, 2, 3, 6\}$  são divisores comuns a 36 e 42, destes o mdc é 6, ou seja,  $6 = \text{mdc}(36, 42)$ . Equivalentemente podemos definir  $d$  (mdc) de  $a$  e  $b$ , com a condição de ser divisor comum destes, e para qualquer  $c \in \mathbb{N}$  também divisor comum de  $a$  e  $b$  então  $c|d$ , ou seja,  $c \leq d$ . Assim sendo, com  $d = \text{mdc}(a, b)$  e  $d' = (a, b)$  então  $d \leq d'$  e  $d' \leq d$ , o mesmo que,  $d = d'$  indicando a unicidade do mdc de dois números.

Denotamos o mdc de  $a$  e  $b$  apenas por  $(a, b)$ , e uma vez que independemos da ordem em que  $a$  e  $b$  são tomados, então

$$(a, b) = (b, a).$$

De toda forma, ainda não verificamos a existência do (mdc), embora a definição pressupõem a sua existência como maior elemento do conjunto dos divisores comuns a dois números. Verificamos a propriedade (ii) da definição 2, sobre a existência do mdc, averiguando resultado subsequente.

**Lema 1. (Lema de Euclides)** *Sejam  $a, b, n \in \mathbb{N}$  com  $a < na < b$ . Se existe  $(a, b - na)$ , então  $(a, b)$  existe, e*

$$(a, b) = (a, b - na).$$

*Demonstração.* A prova segue os moldes da referência [2], pág 54.

Seja  $d = (a, b - na)$ , então  $d|a$  e  $d|(b - na)$  conseqüentemente,  $d$  divide  $b = (b - na) + na$ . Assim,  $d$  é um divisor comum de  $a$  e  $b$ . Na hipótese de que  $c$  também seja um divisor comum de  $a$  e  $b$ , então  $c$  divide  $a$  e  $b - na$ , e portanto,  $c|d$ . Isso prova que  $d = (a, b)$ . □

O Lema 1 consiste em uma ferramenta prática que determina o mdc entre dois números. Por exemplo, com 54 e 132 teremos:

$$\begin{aligned} (132, 54) &= (132 - 2 \cdot 54, 54) = (24, 54) = (24, 54 - 2 \cdot 24) = \\ &= (24, 6) = (24 - 3 \cdot 6, 6) = (6, 6) = 6. \end{aligned}$$

O exemplo mostra que tal como provamos o Lema de Euclides, poderíamos verificar que, para todo  $a, b, n \in \mathbb{N}$ , vale que

$$(a, b) = (a, b + na),$$

ou que, se  $na > b$ , então

$$(a, b) = (a, na - b).$$

Embora o Lema 1 se mostre efetivo no cálculo de mdc entre dois números, temos mais eficiência com o Algoritmo de Euclides, estabelecido na Obra, *Os Elementos*. Em notação moderna, o algoritmo seria assim descrito: com  $a, b \in \mathbb{N}$ , supondo  $a \leq b$ . Se  $a = 1$  ou  $a = b$ , ou ainda  $a|b$ , é óbvio que  $(a, b) = a$ . Suponhamos, então, que  $1 < a < b$  e que  $a$  não divide  $b$ . Logo, pela divisão euclidiana, podemos escrever

$$b = aq_1 + r_1 \text{ com } r_1 < a,$$

temos duas possibilidades

**a)**  $r_1|a$ , e, em tal caso, pelo Lema 1

$$r_1 = (a, r_1) = (a, b - q_1a) = (a, b), \text{ e terminar o algoritmo, ou}$$

**b)**  $r_1$  não divide  $a$ , e, em tal caso, podemos efetuar a divisão de  $a$  por  $r_1$ , obtendo

$$a = r_1q_2 + r_2, \text{ com } r_2 < r_1.$$

Novamente, temos duas possibilidades:

**a')**  $r_2|r_1$ , e, em tal caso, novamente, pelo Lema 1

$$r_2 = (r_1, r_2) = (r_1, a - q_2r_1) = (r_1, a) = (b - q_1a, a) = (b, a) = (a, b),$$

e paramos, pois termina o algoritmo, ou

**b')**  $r_2$  não divide  $r_1$ , e, em tal caso, podemos efetuar a divisão de  $r_1$  por  $r_2$ , obtendo

$$r_1 = r_2q_3 + r_3, \text{ com } r_3 < r_2.$$

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais  $a > r_1 > r_2 > \dots$  que não possui menor elemento, o que não é possível pela Propriedade de Boa Ordem<sup>1</sup>. Logo, para algum  $n$ , temos que  $r_n | r_{n-1}$ , que implica que  $(a, b) = r_n$ .

No cálculo do mdc de 132 e 54, agora com emprego do Algoritmo de Euclides, temos:

$$\begin{aligned} (132, 54) &= (54 \cdot 2 + 24, 54) = (24, 54) = (24, 24 \cdot 2 + 6) \\ &= (24, 6) = (6 \cdot 4 + 0, 6) = (0, 6) = 6. \end{aligned}$$

Finalizamos esta seção com propriedades referentes aos números inteiros não nulos, que são importantes para verificação do Teorema 18 do capítulo 3.

**Definição 3.** Para  $a$  e  $c \in \mathbb{Z}$  diremos que estes serão primos entre si, ou co-primos quando  $(a, c) = 1$ , ou seja, quando o único divisor comum a ambos for 1.

**Proposição 7.** Dizemos que  $a$  e  $b \in \mathbb{Z}$  são co-primos se, e somente se, existirem  $b$  e  $d \in \mathbb{N}$  tais que  $ad - bc = 1$ .

A demonstração pode ser encontrada em [2], pág. 60.

Além disso, se  $b', d' \in \mathbb{Z}$  também satisfazem  $ad' + b'c = 1$ , temos

$$c(b - b') = a(d - d'), \tag{1}$$

e supondo  $(a, c) = 1$  temos que  $a | b - b'$ , isto é, existe  $t \in \mathbb{Z}$  tal que

$$b - b' = ta \quad \text{ou} \quad b = b' + ta.$$

---

<sup>1</sup>A Propriedade da boa ordem diz que todo subconjunto não-vazio de  $\mathbb{N}$  possui um menor elemento.

Substituindo essa última informação em (1), obtemos

$$cta = a(d - d');$$

assim,

$$d - d' = tc \text{ ou } d = d' + tc.$$

Reciprocamente, se  $b, d \in \mathbb{Z}$  satisfazem  $b = b' + ta$ ,  $d = d' + tc$  para algum  $t \in \mathbb{Z}$ , então  $ad - bc = ad' - b'c = 1$ ; logo, constatamos que  $b, d \in \mathbb{Z}$  satisfazem  $ad - bc = 1$  se, e somente se, existir  $t \in \mathbb{Z}$  tal que

$$b = b' + ta \text{ e } d = d' + tc.$$

## 2.3 Teorema Fundamental da Aritmética

### 2.3.1 Números Primos

**Definição 4.** *Se  $p \in \mathbb{N}$  com  $p > 1$ , dizemos que  $p$  é primo quando o conjunto de seus divisores é formado apenas por 1 e  $p$ .*

Desta forma são primos os números: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ... a lista é infinita, conforme [2], pág. 88.

Da Definição 4, temos que com  $p$  e  $q$  primos e  $a \in \mathbb{N}$ , então:

i. Se  $p|q$ , então  $p = q$ .

Pois como  $p|q$ , e sendo  $q$  primo, temos que  $p = 1$  ou  $p = q$ ; mas como,  $p$  é primo, então  $p > 1$  implicando que  $p = q$ .

ii. Se  $p$  não divide  $a$ , então  $(a, p) = 1$

Com  $(a, p) = d$ , temos que  $d|p$  e  $d|a$ . Portanto,  $d = p$  ou  $d = 1$ . Mas como  $p$  não divide  $a$ , então  $d \neq p$ ; conseqüentemente,  $d = 1$ .

Um número  $n \in \mathbb{N}$  maior que 1 quando não primo será chamado de composto, assim se  $n$  é um número composto, existe  $n_1 \in \mathbb{N}$  em que  $n_1 \neq 1$  e  $n_1 \neq n$  com  $n_1|n$ , logo, existirá também um  $n_2 \in \mathbb{N}$  tal que

$$n = n_1 n_2 \quad \text{com} \quad 1 < n_1 < n \quad \text{e} \quad 1 < n_2 < n.$$

A decomposição de um número composto em um produto entre seus fatores primos, como visto acima, é uma atividade comum entre alunos do ensino básico. Exemplo:

$$36 = 4 \cdot 9 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 \cdot 3^2 \quad \text{ou} \quad 60 = 6 \cdot 10 = 2 \cdot 3 \cdot 5 \cdot 2 = 2^2 \cdot 3 \cdot 5.$$

Desta forma, os números primos são suficientes para gerar todos os números naturais, tendo como ponto de vista uma estrutura multiplicativa. Essa é a afirmação do Teorema Fundamental da Aritmética, resultado central desta seção, que foi demonstrado de forma implícita por Euclides, que pode ser facilmente deduzido pelos resultados contidos em sua obra, *Os Elementos*.

**Proposição 8.** *Sejam  $a, b, p \in \mathbb{N}^*$ , com  $p$  primo. Se  $p|ab$ , então  $p|a$  ou  $p|b$ .*

A demonstração pode ser encontrada em [2], pág. 83.

**Corolário 1.** *Se  $p, p_1, p_2, \dots, p_n$  são números primos e  $p|p_1, p_2, \dots, p_n$  então  $p = p_i$  para algum  $i = 1, \dots, n$ .*

A demonstração pode ser encontrada em [2], pág. 83.

A verificação do resultado a seguir foi retirada da referência [2], pág. 83.

**Teorema 1. (Teorema Fundamental da Aritmética).** *Todo número natural maior que 1 ou é primo ou se escreve de modo único (menos da ordem dos fatores) como um produto de números primos.*

*Demonstração.* Usaremos a segunda forma do Princípio da Indução. Se  $n = 2$ , o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor que  $n$  e vamos provar que vale para  $n$ . Se o número  $n$  é primo, nada temos a demonstrar. Suponhamos, então, que  $n$  seja composto. Logo, existem números naturais  $n_1$  e  $n_2$ , tais que  $n = n_1 n_2$ , com  $1 < n_1 < n$  e  $1 < n_2 < n$ . Pela hipótese de indução, existem números primos  $p_1, \dots, p_r$  e  $q_1, \dots, q_s$ , tais que  $n_1 = p_1 \cdots p_r$  e  $n_2 = q_1 \cdots q_s$ . Portanto,  $n = p_1 \cdots p_r q_1 \cdots q_s$ .

Vamos provar a unicidade da escrita. Suponha, agora, que  $n = p_1 \cdots p_r = q_1 \cdots q_s$ , em que os  $p_i$  e os  $q_j$  são números primos. Como  $p_1 | q_1 \cdots q_s$ , podemos supor que seja  $q_1$ . Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s,$$

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

## 2.4 Aritmética dos Restos

Em seu livro *Disquisitiones Arithmeticae*, de 1801, o matemático Gauss nos apresenta a ideia criativa e engenhosa de uma aritmética que se trabalha com restos da divisão euclidiana por um número fixado. E essa noção simples se mostrou útil para verificações de resultados complexos, chegando a ser “uma das noções mais fecundas da aritmética” [2].

Há um série de problemas populares em Olimpíadas de Matemática que são solucionados por meio do raciocínio da aritmética com restos da divisão; principalmente os que envolvem fenômenos periódicos, como calendários, dias da semana e eventos com padrões regulares de repetições. Desta forma, ao resolver questões desse tipo, os alunos do ensino básico trabalham indiretamente com conceito de congruência.



**Definição 5.** *Seja  $m$  um número natural diferente de zero, diremos que dois números naturais  $a$  e  $b$  são congruentes módulo  $m$ , se os restos de sua divisão euclidiana por  $m$  são iguais. Quando os inteiros  $a$  e  $b$  são congruentes módulo  $m$ , escreve-se*

$$a \equiv b \pmod{m}.$$

Quando a relação  $a \equiv b \pmod{m}$  for falsa, diremos que  $a$  e  $b$  não são congruentes, ou que são incongruentes módulo  $m$ . Escrevemos, neste caso,  $a \not\equiv b \pmod{m}$ .

Assim  $14 \equiv 5 \pmod{3}$ , pois ambos, 14 e 5, deixam resto 2 ao ser dividido por 3. Por outro lado,  $15 \not\equiv 8 \pmod{2}$ , uma vez que 15 deixa resto 1 na divisão por 2 e  $2 \nmid 8$ .

A definição anterior se mostra desinteressante para seus propósitos quando  $m = 1$ , uma vez que o resto da divisão de qualquer número por 1 será sempre zero; assim consideremos sempre  $m > 1$ . É de fácil verificação que congruência módulo  $m$  é uma relação de equivalência, ou seja, esta é reflexiva, transitiva e antissimétrica, como verificamos a seguir:

**Proposição 9.** *Seja  $m \in \mathbb{N}$ , com  $m > 1$ . Para todos  $a, b, c \in \mathbb{N}$ , tem-se que*

- (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  $b \equiv c \pmod{m}$ , então  $a \equiv c \pmod{m}$ .

*Demonstração.* Em **i**, sendo  $r_1$  o resto da divisão de  $a$  por  $m$ , é simples constatar que,  $r_1 = r_1$ ; daí  $a \equiv a \pmod{m}$ .

Já em **ii** se  $a \equiv b \pmod{m}$  então  $a = q_1m + r_1$  e  $b = q_2m + r_2$  com  $r_1 = r_2$ , ou seja,  $r_2 = b - q_2m = a - q_1m = r_1$ , assim,  $b \equiv a \pmod{m}$ .

Por fim, em **iii** temos que  $r_1 = a - q_1m = b - q_2m = r_2$  e  $r_2 = b - q_2m = c - q_3m = r_3$ , o que implica,  $r_1 = a - q_1m = b - q_2m = c - q_3m = r_3$ , ou seja,  $a \equiv c \pmod{m}$ .  $\square$

O próximo resultado nos mostra uma forma mais prática de verificar a congruência entre  $a$  e  $b$  módulo  $m$ .

**Proposição 10.** *Suponha que  $a, b \in \mathbb{N}$  são tais que  $a \leq b$ . Tem-se que  $a \equiv b \pmod{m}$  se, e somente se,  $m|b - a$ .*

A demonstração pode ser encontrada em [2], pág. 111.

Usando a Proposição 10, nos exemplos anteriormente analisados, temos:

$14 \equiv 5 \pmod{3}$  pois  $(3| -9 = 5 - 14)$  e  $15 \not\equiv 8 \pmod{3}$  uma vez que  $(3 \nmid -7 = 8 - 15)$ .

Observamos então que qualquer número natural será congruente módulo  $m$  a um dos elementos de  $\{0, 1, \dots, m - 1\}$  – conjunto dos restos da divisão euclidiana por  $m$ . E mais, dois elementos distintos desse conjunto não são congruentes módulo  $m$ .

Portanto, para achar o resto da divisão de um número  $a$  por  $m$ , basta achar um elemento  $r$  do conjunto  $\{0, 1, \dots, m - 1\}$  em que  $a \equiv r \pmod{m}$ .

**Definição 6.** *Todo conjunto  $\{a_1, a_2, \dots, a_m\}$  em que os restos pela divisão por  $m$  dos seus elementos são os números  $0, 1, \dots, m - 1$ , sem repetição e numa ordem qualquer, será um sistema completo de resíduos módulo  $m$ . Conforme [2], pág. 111.*

Um sistema completo de resíduos módulo  $m$  terá  $m$  elementos, exemplo: os conjuntos  $\{15, 16, 17\}$  e  $\{21, 22, 23, 24, 25\}$  são sistemas completos de resíduos módulos 3 e 5, respectivamente.

E fica claro que, se  $a_1, a_2, \dots, a_m$  são  $m$  números naturais, dois a dois não congruentes módulo  $m$ , então eles formam um sistema completo de resíduos módulo  $m$ .

A grande utilidade e poder da noção de congruência é o fato de esta ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme o resultado a seguir:

**Proposição 11.** *Sejam  $a, b, c, d, m \in \mathbb{N}$ , com  $m > 1$ .*

(i) *Se  $a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m}$ , então  $a + c \equiv b + d \pmod{m}$*

(ii) *Se  $a \equiv b \pmod{m}$  e  $c \equiv d \pmod{m}$ , então  $ac \equiv bd \pmod{m}$*

A demonstração pode ser encontrada em [2], pág. 111.

Sendo assim, como  $8 \equiv 15 \pmod{7}$  e  $-2 \equiv 5 \pmod{7}$ , então  $6 \equiv 20 \pmod{7}$  e  $-16 \equiv 75 \pmod{7}$ .

**Corolário 2.** *Para todo  $n \in \mathbb{N}^*$ , com  $m > 1$ . Se  $a \equiv b \pmod{m}$ , então  $a^n \equiv b^n \pmod{m}$ .*

*Demonstração.* Vamos provar por indução em  $n$ , supondo  $a \equiv b \pmod{m}$ , a Proposição 11 nos garante que  $a^2 \equiv b^2 \pmod{m}$ , assim o resultado é válido para  $n = 2$ .

Supondo que para um certo  $n \in \mathbb{N}$  que  $a^n \equiv b^n \pmod{m}$  como por hipótese,  $a \equiv b \pmod{m}$ , então **ii** da Proposição 11 nos garante que  $a^{n+1} \equiv b^{n+1} \pmod{m}$ .  $\square$

**Corolário 3.** *Sejam  $a, b, m \in \mathbb{N}^*$ , com  $m > 1$ . Se  $a + b \equiv 0 \pmod{m}$ , então para todo  $n \in \mathbb{N}$ , tem-se que*

$$a^{2n} \equiv b^{2n} \pmod{m} \quad e \quad a^{2n+1} + b^{2n+1} \equiv 0 \pmod{m}.$$

A demonstração pode ser encontrada em [2], pág. 112.

## 2.5 Congruências Lineares

Analisaremos os processos de resoluções e condição de existência de congruência do seguinte tipo

$$aX \equiv c \pmod{m} \text{ ou } aX + c \equiv 0 \pmod{m},$$

a fim de garantir a existência de  $x_0$  tal que  $ax_0 \equiv c \pmod{m}$  ou  $ax_0 + c \equiv 0 \pmod{m}$ .

**Proposição 12.** *Dados  $a, c, m \in \mathbb{N}^*$  com  $m > 1$ , as congruências  $aX \equiv c \pmod{m}$  e  $aX + c \equiv 0 \pmod{m}$  possuem soluções se, e somente se,  $(a, m)|c$ .*

*Demonstração.* Suponha que a congruência  $aX \equiv c \pmod{m}$  tenha uma solução  $x_0$ , logo temos que

$$m|c - ax \text{ ou } m|ax - c,$$

então existe  $y \in \mathbb{Z}$ , tal que  $c - ax = my$  ou  $ax - c = my$ . Portanto, ao menos umas das equações a seguir admite solução

$$mY + aX = c \quad \text{ou} \quad aX - mY = c.$$

A condição sobre as equações acima é verdadeira se, e somente se,  $(a, m)|c$ . Suponha que a equação  $mY + aX = c$  admita uma solução  $x_0$  e  $y_0$ , então vale a igualdade  $ax_0 + my_0 = c$ .

Pela proposição 5, temos que  $(a, m)|a$  e  $(a, m)|m$ , assim  $(a, m)|ax_0 + my_0 \implies (a, m)|c$ .

Reciprocamente, suponha que  $(a, m)|c$ , ou seja  $c = (a, m) \cdot d$ , com  $d \in \mathbb{Z}$ . Por [2], pág. 57; existem inteiros  $k$  e  $t$ , tais que  $(a, m) = ak + mt$ .

Multiplicando a igualdade acima por  $d$ , obtemos

$$c = (a, m) \cdot d = a \cdot (kd) + m \cdot (td).$$

Logo, a equação  $aX + mY = c$  admite pelo menos a solução  $x = kd$  e  $y = td$ . O caso  $aX - mY = c$  é inteiramente análogo.  $\square$

Então a congruência  $12x \equiv 15 \pmod{9}$  admite solução, pois  $(12, 9) = 3$  e  $3|15$ . Todavia, a congruência  $12x \equiv 10 \pmod{9}$  não admite, solução uma vez que  $3 \nmid 10$ .

Uma vez determinado  $x_0$ , que é uma solução particular de  $aX \equiv c \pmod{m}$  e  $aX + c \equiv 0 \pmod{m}$ , podemos encontrar uma infinidade de soluções  $x$ , bastando apenas resolver  $x \equiv x_0 \pmod{m}$ . Assim, temos

$$ax \equiv ax_0 \equiv c \pmod{m} \text{ e } ax + c \equiv ax_0 + c \equiv 0 \pmod{m},$$

que determina uma coleção completa de soluções (módulo  $m$ ) congruentes entre si.

Então para  $12x \equiv 15 \pmod{9}$ , encontrado  $x = 2$  (uma solução), podemos determinar uma coleção completa de soluções através da congruência  $2 \equiv x \pmod{9}$ . Ou seja, todo  $x = 9n + 2$  com  $n \in \mathbb{Z}$  é solução de  $12x \equiv 15 \pmod{9}$ .

Das coleções de soluções (módulo  $m$ ), será do nosso interesse aquela em que seus termos, dois a dois, sejam incongruentes (módulo  $m$ ). Como podemos verificar no teorema logo a seguir.

**Teorema 2.** *Sejam  $a, c, m \in \mathbb{N}^*$ , com  $m > 1$  e  $(a, m) | c$  se  $x_0$  é solução minimal, isto é menor solução da congruência  $aX \equiv c \pmod{m}$  e  $aX + c \equiv 0 \pmod{m}$  então forma um sistema completo de soluções congruentes*

$$x_0, x_0 + \frac{m}{d}, x_0 + 2 \cdot \frac{m}{d}, \dots, x_0 + (d-1) \cdot \frac{m}{d},$$

em que  $d = (a, m)$ .

*Demonstração.* Vamos provar o resultado somente para congruência  $aX \equiv c \pmod{m}$ , a outra é totalmente análoga. Pela Proposição 12, sabemos que a congruência admite uma solução.

Vamos mostrar que os números  $x_0 + i \frac{m}{d}$ , com  $i \in \mathbb{N}$ , são soluções. De fato

$$a \left( x_0 + i \frac{m}{d} \right) = ax_0 + i \frac{a}{d} m \equiv ax_0 \equiv c \pmod{m}.$$

Além disso, esses números são dois a dois incongruentes módulo  $m$ . De fato, se, para  $i, j < d$ ,

$$x_0 + i \frac{m}{d} \equiv x_0 + j \frac{m}{d} \pmod{m} \iff i \frac{m}{d} \equiv j \frac{m}{d} \pmod{m}.$$

E pelo fato de

$$\frac{m}{(a, m)} = d, \quad (\text{ver [2], pág 114})$$

segue-se que  $i \equiv j \pmod{d}$ , implicando que  $i = j$ .

Finalmente, mostraremos que todas as soluções  $x$  da congruências  $aX \equiv c \pmod{m}$  é congruentes módulo  $m$ , a  $x_0 + i \frac{m}{d}$  para algum  $i < d$ .

De fato, seja  $x$  uma solução qualquer as congruência; logo

$$ax \equiv ax_0 \pmod{m},$$

e, portanto,

$$x \equiv x_0 \pmod{\frac{m}{d}} \quad (\text{ver [2], pág. 114.})$$

Logo,  $x - x_0 = \frac{km}{d}$ . Pela divisão euclidiana, existe  $i < d$  tal que  $k = qd + i$  e, portanto,

$$x = x_0 + qm + i\frac{m}{d} \equiv x_0 + i\frac{m}{d} \pmod{m}.$$

□

A demonstração feita acima pode se encontrada em [2], pág 142.

**Exemplo 1.** *Resolva as congruências  $18X \equiv 42 \pmod{24}$  e  $4x + 3 \equiv 0 \pmod{5}$ .*

Para a primeira equação como  $d = (18, 24) = 6$ , que divide 42, temos que a congruência tem 6 soluções incongruentes módulo 24.

Em uma inspeção rápida obtemos  $x_0 = 1$ , que é a solução minimal; assim sendo, as soluções do sistema completo, módulo 24, são:

$$1, 1 + 4, 1 + 8, 1 + 12, 1 + 16, 1 + 20.$$

Já para segunda equação, temos que  $15x+6 \equiv 0 \pmod{6} \iff 15x \equiv -6 \pmod{6} \iff 15x \equiv 9 \pmod{6}$ . Tal equação terá solução, pois  $(15, 6) = 3$  e  $3|9$ , em uma verificação sobre a mesma. Achamos  $x_0 = 1$  como solução minimal e  $\{1, 1 + 2, 1 + 4\}$  como sistema completo de soluções.

**Corolário 4.** *Se  $(a, m) = 1$ , então as congruências  $aX \equiv c \pmod{m}$  e  $aX + c \equiv 0 \pmod{m}$  possuem uma única solução módulo  $m$ .*

A verificação é um caso particular do Teorema 2, quando  $d = 1$ .

**Corolário 5.** *Sejam  $m > 1$  e  $R$  um conjunto reduzido de resíduos módulo  $m$ , e  $a \in \mathbb{N}^*$  com  $(a, m) = 1$ . Então, para todo  $r \in R$ , a congruência  $rX \equiv a \pmod{m}$  possui uma única solução em  $R$ .*

*Demonstração.* Sendo  $r$  um resíduo módulo  $m$ , então  $r \equiv 1, 2, \dots, m-1 \pmod{m}$ , ou seja,  $(r, m) = 1$ . E pelo Corolário 4,  $rX \equiv a \pmod{m}$  possui solução única em  $R$ .  $\square$

Sendo  $x_0$  a única solução de  $aX \equiv 1 \pmod{m}$ , com  $(a, m) = 1$ , então  $x_0$  será chamado de inverso de  $a$ .

## 2.6 Congruência Quadrática

Nem sempre há soluções para congruências do tipo

$$X^2 \equiv a \pmod{m},$$

com  $a, m \in \mathbb{N}$  e  $m > 1$ .

Por exemplo, a congruência  $X^2 \equiv 2 \pmod{3}$  não possui solução, pois como  $x_0 \in \mathbb{Z}$ , temos uma das possibilidades:

$$x_0 \equiv 0 \pmod{3} \Rightarrow x_0^2 \equiv 0 \pmod{3};$$

$$x_0 \equiv 1 \pmod{3} \Rightarrow x_0^2 \equiv 1 \pmod{3};$$

$$x_0 \equiv 2 \pmod{3} \Rightarrow x_0^2 \equiv 4 \equiv 1 \pmod{3}.$$

Quando a congruência  $X^2 \equiv a \pmod{m}$  possui alguma solução  $a$ , esta será chamada de *resíduo quadrático* módulo  $m$ . Caso contrário,  $a$  não é *resíduo quadrático* módulo  $m$ .

Como exemplo, vimos que 2 não é resíduo quadrático módulo 3; já para qualquer  $a \in \mathbb{N}$ , este é um *resíduo quadrático* módulo 2. Ou seja, a equação  $X^2 \equiv a \pmod{2}$  com  $a \in \mathbb{N}$  sempre tem solução, pois quando  $a = 2n$ , então  $X^2 \equiv 2n \equiv 0 \pmod{2}$ , e qualquer  $x_0 = 2m$  é uma solução da congruência. Caso  $a = 2n - 1$ , basta fazer  $x_0 = 2m - 1$ , e solucionamos a congruência.

Por [2], temos como resultado válido para congruência quadrática, que se  $p$  é um número primo ímpar e  $X^2 \equiv a \pmod{p}$  possui uma solução, então haverá outra solução, de forma que, estas duas sejam as únicas soluções incongruentes entre si módulo  $p$ .

**Proposição 13.** *Sejam  $p, a \in \mathbb{N}$ , com  $p > 2$  primo e  $(p, a) = 1$ . Se a congruência  $X^2 \equiv a \pmod{p}$  possui uma solução  $x_0 \in \{0, 1, \dots, p-1\}$  então  $(x_0, p) = 1$  e  $p - x_0$  também é solução. E mais, estas são as únicas soluções em  $\{0, 1, \dots, p-1\}$*

*Demonstração.* Se  $x_0^2 \equiv a \pmod{p}$ , então  $1 = (a, p) = (x_0^2, p)$ , o que implica que  $(x_0, p) = 1$ , uma vez que,  $(p - x_0)^2 \equiv p^2 - 2px_0 + x_0^2 \equiv x_0^2 \pmod{p}$  então  $(p - x_0)^2 \equiv x_0^2 \equiv a \pmod{p}$ .

Por outro lado, com  $x_1 \in \{0, 1, 2, \dots, (p-1)\}$  e  $x_1 > x_0$ , se  $x_1^2 \equiv a \pmod{p}$  então  $x_0^2 \equiv x_1^2 \pmod{p}$ , portanto,  $p | x_1^2 - x_0^2$ , o que implica que  $p | x_1 - x_0$  ou  $p | x_1 + x_0$ . Assim temos  $x_1 = x_0$  ou  $x_1 = p - x_0$ . □

O próximo resultado é atribuído ao matemático Leonhard Euler, que o apresentou pela primeira vez em um artigo de 1748, ver [2]. Tal resultado corresponde a um critério para determinar se um número natural é ou não um *resíduo quadrático*.

**Teorema 3. (Critério de Euler).** *Seja  $p$  um número primo ímpar e  $a \in \mathbb{N}$  tal que  $(a, p) = 1$ . Tem-se que:*

- i.  $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$  se, e somente se,  $a$  é resíduo quadrático módulo  $p$ ;
- ii.  $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$  se, e somente se,  $a$  não é resíduo quadrático módulo  $p$ .

A demonstração pode ser encontrada em [2], pág. 149.

**Exemplo 2.** *Pelo Critério de Euler, a congruência  $2^{26} \equiv 1 \pmod{47}$  tem solução, pois  $7^2 \equiv 2 \pmod{47}$ .*



**Definição 7.** Se  $p$  é um número primo ímpar, define-se o símbolo de Legendre como sendo

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

Uma vez que  $a$  é solução de  $X^2 \equiv a^2 \pmod{p}$ , então  $\left(\frac{a^2}{p}\right) = 1$ . Em particular  $\left(\frac{1}{p}\right) = 1$ .

Ainda com relação ao *Símbolo de Legendre*, o próximo resultado será importante para verificações de Teoremas em Capítulos posteriores.

**Teorema 4.** Sejam  $a, b, p, \in \mathbb{N}$ , com  $p$  número primo e ímpar, se  $(a, p) = (b, p) = 1$  tem-se que:

- (i)  $a \equiv b \pmod{p}$ , então  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ ;
- (ii)  $a^{\frac{p-1}{2}} - \left(\frac{a}{p}\right) \equiv 0 \pmod{p}$ ;
- (iii)  $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ .

A demonstração pode ser encontrada em [2], pág. 151.

## 2.7 Uma revisão de Álgebra Linear

Algumas ideias e conceitos de Álgebra Linear serão aqui lembrados para dar suporte as definições e resultados que antecedem o Método de Minkowski.

**Definição 8.** (*Forma Bilinear*) Sejam  $V$  e  $W$  espaços vetoriais sobre um corpo  $K$ , com  $K = \mathbb{R}$  ou  $\mathbb{C}$ . Uma Forma bilinear será uma aplicação  $B : V \times W \rightarrow K$  que satisfaz as duas condições a seguir:

- (i)  $B(\alpha v_1 + v_2, w_1) = \alpha B(v_1, w_1) + B(v_2, w_1)$ ;

(ii)  $B(v_1, \beta w_1 + w_2) = B(v_1, w_1) + \overline{\beta} B(v_2, w_2)$ , a barra sobre  $\beta$  em (ii) denota o conjugado deste.

**Exemplo 3.** Como exemplo de Forma bilinear, conforme [1], temos o produto interno canônico.

Considerando  $V = \mathbb{R}^2$ , com  $v = (x_1, y_1)$  e  $w = (x_2, y_2)$  o produto interno  $v$  e  $w$  é

$$\langle v, w \rangle = \langle (x_1, y_1), (x_2, y_2) \rangle = x_1 \cdot x_2 + y_1 \cdot y_2.$$

Daí, segue que

$$\begin{aligned} \langle \alpha \cdot v + w, u \rangle &= \langle \alpha \cdot (x_1, y_1) + (x_2, y_2), (x_3, y_3) \rangle = \langle (\alpha \cdot x_1, \alpha \cdot y_1), (x_3, y_3) \rangle + \langle (x_2, y_2), (x_3, y_3) \rangle = \\ &= \alpha \cdot x_1 \cdot x_3 + \alpha \cdot y_1 \cdot y_3 + x_2 \cdot x_3 + y_2 \cdot y_3 = \alpha \cdot (x_1 \cdot x_3 + y_1 \cdot y_3) + (x_2 \cdot x_3 + y_2 \cdot y_3) = \\ &= \alpha \cdot \langle v, u \rangle + \langle w, u \rangle. \end{aligned}$$

A verificação da propriedade (ii) acontece de forma semelhante.

Dizemos que Forma bilinear é simétrica se  $V = W$  e  $B(v_1, v_2) = B(v_2, v_1)$ . E uma vez que  $V$  e  $W$  sejam gerados por suas respectivas bases  $B_V = (v_1, v_2, \dots, v_n)$  e  $B_W = (w_1, w_2, \dots, w_m)$ . Supondo  $v \in V$  e  $w \in W$ , temos que:

$$v = \alpha_1 \cdot v_1 + \alpha_2 \cdot v_2 + \dots + \alpha_n \cdot v_n \text{ e } w = \beta_1 \cdot w_1 + \beta_2 \cdot w_2 + \dots + \beta_m \cdot w_m,$$

se escrevem de maneira única e  $\alpha_1, \alpha_2, \dots, \alpha_n, \beta_1, \beta_2, \dots, \beta_m \in \mathbb{K}$ , que nos possibilita reformular a *Forma Bilinear* em função das coordenadas das bases dos vetores  $v$  e  $w$  como

$$\begin{aligned} B(v, w) &= B(\alpha_1 \cdot v_1 + \alpha_2 \cdot v_2 + \dots + \alpha_n \cdot v_n, \beta_1 \cdot w_1 + \beta_2 \cdot w_2 + \dots + \beta_m \cdot w_m) \\ &= B\left(\sum_{i=1}^n \alpha_i v_i, \sum_{j=1}^m \beta_j w_j\right) = \sum_{i=1}^n \sum_{j=1}^m \alpha_i \beta_j B(v_i, w_j). \end{aligned}$$

E também podemos ter  $v$  e  $w$  como matrizes colunas, pois fixadas as bases para  $B_V$  e  $B_W$ , temos

$$[v]_{B_V} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \text{e} \quad [w]_{B_W} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Então a matriz  $[B]_{B_W}^{B_V} = (b_{ij})_{n \times m}$  é a matriz mudança de base, e o produto matricial a seguir corresponde a *Forma Bilinear*  $B(v, w)$ .

$$B(v, w) = {}^t[v]_{B_V} \times [B]_{B_W}^{B_V} \times [\bar{w}]_{B_W},$$

onde

$${}^t[v]_{B_V} = \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_n \end{pmatrix} \quad \text{e} \quad [\bar{w}]_{B_W} = \begin{pmatrix} \bar{\beta}_1 \\ \bar{\beta}_2 \\ \vdots \\ \bar{\beta}_n \end{pmatrix}.$$

**Exemplo 4.** O produto interno de  $v = (x_1, y_1)$  e  $w = (x_2, y_2)$  escrito como produto matricial, fica

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}^t \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} \bar{x}_2 \\ \bar{y}_2 \end{pmatrix}.$$

**Definição 9.** (*Forma quadrática*) Dizemos que  $f : V \rightarrow K$  sendo  $V$  um espaço vetorial e  $K = \mathbb{R}$  ou  $\mathbb{C}$  é uma forma quadrática sobre  $V$  se, e somente se,

i.  $f(\alpha v) = \alpha^2 f(v), \forall \alpha \in \mathbb{K}, v \in V$

ii. A função  $B_f : V \times V \rightarrow K$ ; é definida como

$$B_f(v_1, v_2) = \frac{1}{2} [f(v_1 + v_2) - f(v_1) - f(v_2)]$$

é a *Forma Bilinear simétrica* sobre  $V \times V$ .

A Definição 9 nos permite estabelecer uma correspondência bijetora entre *Forma Quadrática* em  $V$  e as *Formas Bilineares Simétricas* sobre  $V \times V$ . Assim, para cada  $f$  existe uma  $B_f$ , tal que  $f(v) = B_f(v, v)$ .

Se  $V$  é um espaço vetorial de dimensão finita com base  $B_V = (v_1, v_2, \dots, v_n)$ , então a matriz  $F$  da *Forma Quadrática*  $f$  com relação a  $B_V$  e determinada por

$$F = (b_{ij}) = B_f(v_i, v_j) = [B_f]_{B_V}^{B_V} \quad \forall v \in V \text{ temos } f(v) = {}^t [v]_{B_V} \times F \times [\bar{v}]_{B_V},$$

desta forma, com  $V$  de dimensão  $n$  e base  $B_V$ , podemos identificar as *Formas Quadráticas* de  $V$  por matrizes simétricas  $n \times n$  com entradas em  $K$ .

**Definição 10.** (*Forma Quadrática Positiva Definida*) Uma *Forma Quadrática*  $f : \mathbb{R}^n \rightarrow \mathbb{R}$  é dita “*Positiva Definida*”, se  $f(v) > 0 \forall v \in \mathbb{R}^n$  e  $v \neq 0$ .

De agora em diante, faremos sempre  $V = \mathbb{R}^2$ , com bases canônicas fixadas e as matrizes de Formas quadráticas (binárias)  $f : \mathbb{R}^2 \rightarrow \mathbb{R}$  serão calculadas com relação a essa base. É de fácil observação que uma *Forma Quadrática Binária*, corresponde a um polinômio homogêneo de grau dois com duas indeterminadas.

**Exemplo 5.**  $f : \mathbb{R}^2 \rightarrow \mathbb{R}$  em que  $f(x, y) = x^2 - 10xy + y^2$  é uma *Forma Quadrática Binária*. Como produto matricial, temos:

$$f(v) = \begin{pmatrix} x \\ y \end{pmatrix}^t \times \begin{pmatrix} 1 & -5 \\ -5 & 1 \end{pmatrix} \times \begin{pmatrix} x \\ y \end{pmatrix}.$$

Podemos observar no Exemplo 5 que os vetores de  $\mathbb{R}^2$  são representados como matriz coluna  $2 \times 1$ . Também usaremos a notação

$$M_2(X) = \left\{ \text{matrizes } 2 \times 2 \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in X \right\}$$

e definimos o conjunto  $SL_2 = \{A \in M_2 : \det[A] = 1\}$  em que  $X$  é um conjunto (que será  $\mathbb{R}$  ou  $\mathbb{Z}$ , dependendo da situação), com o determinante da matriz  $A$  simbolizado por  $\det[A]$ .

**Definição 11.** (*Equivalência entre Formas Quadráticas*) Dizemos que  $f$  e  $g$  são Formas quadráticas equivalentes se, e somente se, suas matrizes associadas  $F$  e  $G$  forem equivalentes; para isto, devem satisfazer à equação  $G = U^t F U$  com  $U \in SL_2$ .

A cada Forma Quadrática Binária  $f$  (com matriz associada  $F$ ) ligamos ao número

$$\Delta(f) = 4 \det [F]$$

chamado de *discriminante* de  $f$ . No caso em que  $f(x, y) = ax^2 + bxy + cy^2$ , temos  $F = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$  e  $\Delta(f) = 4ac - b^2$ .

**Definição 12.** (*Representante de um inteiro  $m$* ) Para  $f$  Forma binária e  $m \in \mathbb{Z}$ . Dizemos que “ $f$  representa  $m$ ” se existir  $x_0, y_0 \in \mathbb{Z}$ , não ambos nulos, tais que  $f(x_0, y_0) = m$ . O par  $(x_0, y_0)$  é chamado de “uma representação de  $m$  por  $f$ ”. E caso  $x_0$  e  $y_0$  sejam co-primos, ou seja,  $(x_0, y_0) = 1$ , então dizemos que a representação é própria.

A partir das Definições 11 e 12 é de fácil conclusão que formas equivalentes têm o mesmo *discriminante* e representam (propriamente) o mesmo inteiro. E aqui encontramos uma conexão com o objetivo principal deste trabalho, pois estamos interessados em estudar as representações próprias de um inteiro  $m$  pela Forma  $f(x, y) = x^2 + y^2$ .

O conjunto de definições que seguem, fazem parte do ramo da Álgebra Abstrata e nos auxiliaram na tarefa de construir uma relação entre, *Formas quadráticas* e o conjunto  $\mathbb{H}$ , com  $\mathbb{H} = \{x + iy \in \mathbb{C} : y > 0\}$ . Ou seja,  $\mathbb{H}$  é o plano superior complexo.

Construiremos uma relação entre *Formas quadráticas binárias* e pontos sobre  $\mathbb{H}$ , a fim de, avaliar a *equivalência entre Formas quadráticas*, analisando a *equivalência entre os pontos* de  $\mathbb{H}$ .

## 2.8 Algumas definições em Álgebra Abstrata

**Definição 13.** (Ação de um grupo sobre um conjunto) Uma função  $\star : \mathbb{G} \times \mathbf{S} \longrightarrow \mathbf{S}$  é chamada de “ação de  $\mathbb{G}$  em  $\mathbf{S}$ ”, se satisfaz a

- i.  $e \star s = s$ , para todos  $s \in \mathbf{S}$  ( $e =$  a identidade do grupo  $\mathbb{G}$ );
- ii.  $g_1 \star (g_2 \star s) = (g_1 \cdot g_2) \star s$  para quaisquer  $g_1, g_2 \in \mathbb{G}$  e  $s \in \mathbf{S}$ , em que  $\mathbb{G}$  é um grupo e  $\mathbf{S}$  é um conjunto não vazio.

Para cada  $s \in \mathbf{S}$ , o conjunto  $\mathbb{G} \star s = \{g \star s : g \in \mathbb{G}\}$  é a “órbita do elemento  $s$ ”.

**Definição 14.** (Equivalência entre os elementos de  $\mathbf{S}$ ) Dizemos que  $s_1, s_2 \in \mathbf{S}$  são equivalentes quando existe  $g \in \mathbb{G}$  tal que

$$g \star s_1 = s_2$$

e quando a igualdade acima for satisfeita, dizemos que  $s_1$  e  $s_2$  são equivalentes.

**Definição 15.** (Domínio Fundamental da Ação) Dizemos que  $\mathbb{F}$  é um domínio fundamental da ação de  $\mathbb{G}$  sobre  $\mathbf{S}$  quando  $\mathbb{F} \subset \mathbf{S}$  e

- i.  $\forall s \in \mathbf{S}, \exists g \in \mathbb{G}; g \star s \in \mathbb{F}$ ;
- ii. Dados  $s_1 \in \mathbf{S}$  e  $g_1 \in \mathbb{G}$ , se  $s_1 \in \mathbb{F}$  e  $g_1 \star s_1 \in \mathbb{F}$ , então  $g_1 = e$ , em que “ $e$ ” é o elemento neutro de  $\mathbb{G}$ .

Em resumo, o domínio fundamental  $\mathbb{F}$  contém um ponto de cada órbita de  $\mathbf{S}$ . Agora faremos  $\mathbb{G} = SL_2(\mathbb{Z})$  e  $\mathbf{S} = \mathbb{H}$ , e vamos definir a seguinte ação

$$\star : SL_2(\mathbb{Z}) \times \mathbb{H} \longrightarrow \mathbb{H}$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \star z_1 = \frac{az_1 + b}{cz_1 + d} = z_2 = x_2 + iy_2.$$

A ação está bem definida, vejamos inicialmente que  $cz_1 + d \neq 0$ . Como  $z_1 = x_1 + iy_1$ , temos que  $cz_1 + d = (cx_1 + d) + icy_1$ , e se  $c = 0$  então  $d \neq 0$ , uma vez que,  $(\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1)$  daí  $cz_1 + d \neq 0$ . Se  $c \neq 0$ , então  $cy_1 \neq 0$  (já que  $y_1 > 0$ ) e novamente teremos  $cz_1 + d \neq 0$ .

Além disso, verificamos que a “Ação de  $SL_2(\mathbb{Z})$  em  $\mathbb{H}$ ” resulta em um elemento de  $\mathbb{H}$ , pois como  $z\bar{z} = |z|^2$ , temos

$$\begin{aligned} z_2 &= \frac{az_1 + b}{cz_1 + d} = \frac{(az_1 + b)(c\bar{z}_1 + d)}{|cz_1 + d|^2} = \frac{(acz_1\bar{z}_1 + bd) + adz_1 + bc\bar{z}_1}{|cz_1 + d|^2} \\ &= \frac{acz_1\bar{z}_1 + bd + (ad + bc)x_1}{|cz_1 + d|^2} + \frac{(ad - bc)y_1}{|cz_1 + d|^2}i \end{aligned}$$

logo,  $y_2 = \frac{y_1}{|cz_1 + d|^2} > 0$ , pois  $ad - bc = 1$ . Portanto,  $z_2 \in \mathbb{H}$ .

E por fim, a “Ação de  $SL_2(\mathbb{Z})$  sobre  $\mathbb{H}$ ”, como foi determinada, satisfaz as propriedades **i** e **ii** da Definição 13.

(i)  $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \star z_1 = z_1$ , para qualquer  $z_1 \in \mathbb{H}$ .

(ii) Com  $U_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  e  $U_2 = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$  pertencentes a  $SL_2(\mathbb{Z})$  e  $z_1 \in \mathbb{H}$ ,

verifica-se que

$$\begin{aligned}
U_1 \star (U_2 \star z_1) &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \star \left[ \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \star z_1 \right] = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \star \frac{a'z_1 + b'}{c'z_1 + d'} \\
&= \frac{a \frac{a'z_1 + b'}{c'z_1 + d'} + b}{c \frac{a'z_1 + b'}{c'z_1 + d'} + d} = \frac{(aa' + bc')z_1 + (ab' + bd')}{(a'c + cd')z_1 + (cb' + db')} \\
&= \begin{pmatrix} (aa' + bc') & (ab' + bd') \\ (a'c + cd') & (cb' + db') \end{pmatrix} \star z_1 = \left[ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \right] \star z_1 \\
&= (U_1 \cdot U_2) \star z_1.
\end{aligned}$$

Uma vez bem definida a Ação de  $SL_2(\mathbb{Z})$  sobre  $\mathbb{H}$ , então  $z_1$  e  $z_2$  são equivalentes se, e somente se, existir  $U \in SL_2(\mathbb{Z})$ , tal que  $U \star z_1 = z_2$ .

Reforçamos o comentário sobre o conceito de Equivalência entre os pontos em  $\mathbb{H}$ , que será de fundamental importância na verificação dos resultados do Capítulo 4.



### 3 Soma de Quadrados

Por se tratar de um tema milenar, a escrita de um número como soma de quadrado já foi abordada por diversos matemáticos em diferentes níveis de abstração. Desde os agrimensores egípcios, que com conhecimento empírico sobre ternos pitagóricos, mediam terrenos próximo ao Nilo, após as cheias. Até chegar aos gregos como Pitágoras e Diofanto, que metodizaram o problema, possibilitando a abordagem de grandes matemáticos como: Euler, Fermat e Gauss.

Mais recentemente, no século XIX, o matemático Herman Minkowski analisou o problema geometricamente, através da Teoria Geométrica dos Números, criada pelo próprio, para resolver problemas da Teoria dos Números [11].

Neste capítulo, analisamos as condições necessárias e suficientes, para decompor um inteiro como Soma de Quadrados. Apesar de não evidenciarmos como fazer tal decomposição, ainda assim, encontramos resultados difíceis de verificar e ao mesmo tempo com diversas aplicações.

**Definição 16.** *Para  $m$ , número inteiro positivo, dizemos que o mesmo poderá ser escrito como soma de quadrados se existirem  $a$  e  $b$  inteiros, tais que  $m = a^2 + b^2$ .*

**Lema 2.** *Sejam  $m$  e  $n$  dois inteiros positivos em que  $m = a^2 + b^2$  e  $n = c^2 + d^2$ , então  $m \cdot n = A^2 + B^2$ .*

*Demonstração.* Se  $m = a^2 + b^2$  e  $n = c^2 + d^2$ , então

$$\begin{aligned} m \cdot n &= (a^2 + b^2) \cdot (c^2 + d^2) = a^2 \cdot c^2 + a^2 d^2 + b^2 c^2 + b^2 d^2 = \\ &= (ac)^2 + 2abcd + (bd)^2 + (ad)^2 - 2abcd + (bc)^2 = \\ &= (ac)^2 + 2(ac)(bd) + (bd)^2 + (ad)^2 - 2(ad)(bc) + (bc)^2 = (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

Fazendo  $A = ac + bd$  e  $B = ad - bc$ , temos  $m \cdot n = A^2 + B^2$ . □

O próximo resultado nos diz, quando um número inteiro não poderá ser escrito como soma de quadrados. Dessa forma, constatamos que, para  $m \in \mathbb{Z}$  e  $m = 4k + 3$ ,  $m$  não pode ser decomposto como tal soma.

**Teorema 5.** *Se  $m$  é inteiro positivo da forma  $4k + 3$ , então não podemos escrevê-lo como soma de quadrados.*

*Demonstração.* Para qualquer  $a$  inteiro, temos se  $a = 2k_1$  implica que  $a^2 = 4k_1^2 = 4k$ .

E se  $a = 2k_1 - 1$ , então  $a^2 = 4k_1^2 - 4k_1 + 1 = 4k + 1$ . Avaliando todas as possibilidades para  $a$  e  $b$ , temos:

$$m = a^2 + b^2 = 4k_1^2 + 4k_2^2 = 4k \text{ (} a \text{ e } b \text{ pares);}$$

$$m = a^2 + b^2 = 4k_1^2 + 4k_2^2 - 4k_1 - 4k_2 + 2 = 4k + 2 \text{ (} a \text{ e } b \text{ ímpares);}$$

$$m = a^2 + b^2 = 4k_1^2 + 4k_2^2 - 4k_1 - 1 = 4k + 1 \text{ (} a \text{ e } b \text{ forem de paridades distintas).}$$

Assim, concluímos que não podemos ter  $m = a^2 + b^2 = 4k + 3$ . □

**Teorema 6.** *Seja  $p > 0$  primo e  $n$  pertencente aos naturais se  $n \cdot p = a^2 + b^2$ , então  $p = a^2 + b^2$ .*

*Demonstração.* Para  $n_0 \in \mathbb{N}$ , que é o menor valor, tal que,  $n_0 \cdot p = a^2 + b^2$ , devemos mostrar que  $n_0 = 1$ .

Usando o raciocínio contra positivo, iremos supor  $n_0 = 2$ , que é o menor natural tal que,  $2 \cdot p = a^2 + b^2$ , uma vez que  $2 = 1^2 + 1^2$ . Sendo assim, o Lema 2 garante que  $2p \cdot 2 = 4p = (a + b)^2 + (a - b)^2 = A^2 + B^2$ .

Uma vez que  $2 \cdot p$  é par, podemos ter  $a = 2 \cdot n_1$  e  $B = 2 \cdot n_2$ . Assim,  $4p = (a+b)^2 + (a-b)^2 = 4(n_1+n_2)^2 + 4(n_1-n_2)^2$ , ou seja,  $p = (n_1+n_2)^2 + (n_1-n_2)^2 = A_1^2 + B_1^2$ .

E quando  $a = 2n_1 - 1$  e  $b = 2n_2 - 1$ , temos  $4p = (a + b)^2 + (a - b)^2 = 4(n_1 + n_2 - 1)^2 + 4(n_1 - n_2 - 1)^2$ ; ou seja,  $p = (n_1 + n_2 - 1)^2 + (n_1 - n_2 - 1)^2 = A_2^2 + B_2^2$ .

Os dois caso contradizem a hipótese de  $n_0 = 2$  ser o menor número natural, tal que  $n_0 \cdot p = a^2 + b^2$ .

Supondo agora que com  $n_0 \geq 3$  temos  $n_0 \cdot p = a_1^2 + b_1^2$ , sendo  $a_1 \equiv r_1 \pmod{n_0}$  e  $b_1 \equiv r_2 \pmod{n_0}$ . Em outras palavras,  $r_1$  e  $r_2$  são restos da divisão de  $a_1$  e  $b_1$  por  $n_0$ , respectivamente. Escolhendo

$$0 < |r_1|, |r_2| \leq \left(\frac{n_0}{2}\right), \quad (2)$$

e como  $a_1 \equiv r_1 \pmod{n_0}$  e  $b_1 \equiv r_2 \pmod{n_0}$ , logo  $a_1^2 \equiv r_1^2 \pmod{n_0}$  e  $b_1^2 \equiv r_2^2 \pmod{n_0}$ . Pelo item **iii** da Proposição 11, temos  $n_0 \cdot p \equiv a_1^2 + b_1^2 \equiv r_1^2 + r_2^2 \equiv 0 \pmod{n_0}$ .

Assim, existe um  $n$  natural, em que  $n \cdot n_0 = r_1^2 + r_2^2$ , e a escolha em (2) resulta em:

$$n \cdot n_0 = r_1^2 + r_2^2 \leq 2 \cdot \left(\frac{n_0}{2}\right)^2 \implies n \leq \frac{n_0}{2}.$$

O Lema 2 nos garante que

$$\begin{aligned} n_0 \cdot p \cdot n_0 \cdot n &= n_0^2 \cdot n \cdot p = (a_1^2 + b_1^2) \cdot (r_1^2 + r_2^2) \\ &= (a_1 \cdot r_1 + b_1 \cdot r_2)^2 + (a_1 \cdot r_2 - b_1 \cdot r_1)^2 = A^2 + B^2. \end{aligned} \quad (3)$$

Multiplicando as congruências  $a_1 \equiv r_1 \pmod{n_0}$  e  $b_1 \equiv r_2 \pmod{n_0}$ , por  $r_1$  e  $r_2$ , respectivamente, obtemos  $a_1 r_1 \equiv r_1^2 \pmod{n_0}$  e  $b_1 r_2 \equiv r_2^2 \pmod{n_0}$ . Somando os resultado da multiplicação, temos  $a_1 r_1 + b_1 r_2 \equiv r_1^2 + r_2^2 \equiv 0 \pmod{n_0}$ . Ou seja,  $A \equiv 0 \pmod{n_0}$ .

De modo semelhante, podemos mostrar que  $B \equiv a_1 \cdot r_2 - b_1 \cdot r_1 \equiv r_1 r_2 - r_1 r_2 \equiv 0 \pmod{n_0}$ , o que nos permite concluir que existem  $a$  e  $b \in \mathbb{N}$ , em que  $A = a \cdot n_0$  e  $B = b \cdot n_0$ . Substituindo os valores de  $A$  e  $B$  em (3), temos

$$n_0^2 \cdot p \cdot n = A^2 + B^2 = (a \cdot n_0)^2 + (b \cdot n_0)^2 \iff n \cdot p = a^2 + b^2.$$

Entretanto, como  $n \leq \frac{n_0}{2} < n_0$  contraria novamente a suposição inicial, em que  $n_0$  é o

menor valor que satisfaz  $n_0 \cdot p = a^2 + b^2$ , assim  $n_0$  não pode ser 2 e não pode ser maior igual a 3 então  $n_0 = 1$ .  $\square$

Os Teoremas 5 e 6 ajudarão na verificação do próximo resultado, que elucidará as condições necessárias e suficiente em que um número primo  $p > 2$  possa ser escrito como soma de quadrados. Também somos auxiliados pelo Teorema 4, verificado no Capítulo 2.

**Teorema 7.** *Para  $p > 2$  número primo temos que  $p = a^2 + b^2$  se, e somente se,  $p = 4 \cdot k + 1$ .*

*Demonstração.* Pelo Teorema 5, se  $p$  primo pode ser escrito como soma de quadrados, então este não poderá ser da forma  $4 \cdot k + 3$ ; e uma vez que  $p$  não é par, pois  $p > 2$ , então resta ao mesmo ser da forma  $4 \cdot k + 1$ , finalizando a verificação da primeira parte do Teorema.

Para a recíproca do Teorema, temos por base que  $p = 4 \cdot k + 1$ , o Teorema 4 garante que

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

fazendo  $a = -1$  temos

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

Como supomos  $p = 4 \cdot k + 1$  então  $\frac{p-1}{2} = 2k$ , uma vez que  $p$  é ímpar; assim existe  $a_1 \in \mathbb{Z}$  tal que  $a_1^2 \equiv -1 \pmod{p} \iff n \cdot p = 1^2 + a^2$ , e o Teorema 6 garante que  $p = a^2 + b^2$ .  $\square$

Com os resultados examinados, até o momento, somos capazes de identificar quando um primo  $p > 2$  poderá ou não ser escrito como soma de quadrados, porém nada falamos sobre como chegar a tal decomposição. Todavia restringiremos nosso intervalo de busca por  $a$  e  $b$ , pois, uma vez que  $p = a^2 + b^2$  então  $a$  e  $b \in (0, \sqrt{p})$ .

**Exemplo 6.** *Determine  $a$  e  $b$  tais que  $137 = a^2 + b^2$ .*

Como observado anteriormente,  $a$  e  $b \in (0, \sqrt{137})$ , assim numa análise sobre os inteiros entre 1 e 11, obtemos 4 e 16, que é solução para o problema, visto que  $137 = 4^2 + 11^2$ .

O próximo resultado verificará a unicidade dos valores de  $a$  e  $b$  no intervalo  $(0, \sqrt{p})$ , em que  $a^2 + b^2 = p$ .

**Teorema 8.** *Com  $p > 2$  (número primo da forma  $4 \cdot k + 1$ ), existem únicos  $a$  e  $b$  em  $(0, \sqrt{p})$  tais que  $p = a^2 + b^2$ .*

*Demonstração.* Supondo que exista  $c$  e  $d$  em  $(0, \sqrt{p})$  em que  $p = c^2 + d^2 = a^2 + b^2$ , então  $a^2 \equiv -b^2 \pmod{p}$  e  $d^2 \equiv -c^2 \pmod{p}$ . Assim  $a^2 \cdot d^2 \equiv b^2 \cdot c^2 \equiv 0 \pmod{p}$ , que resulta em  $a \cdot d \equiv b \cdot c \pmod{p}$  ou  $a \cdot d \equiv -b \cdot c \pmod{p}$ .

Desta forma, existem  $k_1, k_2 \in \mathbb{Z}$  tais que  $k_1 p = ad + bc$  ou  $k_2 p = ad - bc$ . Como  $a, b, c, d \in (0, \sqrt{p})$ , então  $a \cdot d < p$  e  $b \cdot c < p$ . Isso é equivalente a  $a \cdot d + b \cdot c < 2 \cdot p$  e nesse caso podemos ter  $ad + bc = p$  ou  $ad - bc = 0$ .

1º caso: Para  $ad - bc = 0$  implica em  $ad = bc$  e uma vez que  $p = a^2 + b^2$  pode ser entendido como Equação Diophantina de coeficientes  $a$  e  $b$ , então  $(a, b)|p$ , o mesmo que  $(a, b) = 1$ .

Como  $ad = bc$  temos que  $a|c$  e  $b|d$ , ou seja,  $c = k \cdot a$  e  $d = k \cdot b$ . Com isso  $p = c^2 + d^2 = k^2(a^2 + b^2)$ , temos  $k = 1$  ou  $k = -1$ , mas como  $a, b, c$  e  $d \in (0, \sqrt{p})$ , então não podemos ter  $k = -1$ , o que implica em  $a = c$  e  $b = d$ .

2º caso: Se  $ad + bc = p$  então

$$\begin{aligned} p^2 &= (a^2 + b^2) \cdot (c^2 + d^2) = a^2 c^2 + a^2 d^2 + b^2 c^2 + b^2 d^2 = (a^2 d^2 + b^2 c^2) + (a^2 c^2 + b^2 d^2) = \\ &= (a^2 d^2 + 2(ad)(bc) + b^2 c^2) + (a^2 c^2 - 2(ac)(bd) + b^2 d^2) = (ad + bc)^2 + (ac - bd)^2 = \\ &= p^2 + (ac - bd)^2 \iff (ac - bd)^2 = 0, \text{ que equivale a } ac - bd = 0 \iff ac = bd \text{ e, a partir} \end{aligned}$$

daqui, procedendo de maneira semelhante ao (1º caso), obtemos novamente  $a = d$  e  $b = c$  finalizando assim a demonstração.  $\square$

Logo em seguida anunciamos o principal resultado desta seção que é uma generalização do Teorema 7 para todo número inteiro.

**Teorema 9.** *Se  $n \in \mathbb{N}$  e  $n = N^2 \cdot m$ , em que  $m$  é livre de quadrados (ou seja, não existirá nenhum  $p_0$  primo, com  $p_0^2$  dividindo  $m$ ), então  $n = a^2 + b^2$  se, e somente se, os fatores primos de  $m$  não forem do tipo  $4 \cdot k + 3$ .*

*Demonstração.* A princípio vamos supor  $m$  sem fatores primos do tipo  $4k + 3$ . Para  $m = 1$ , podemos ter  $n$  como soma de quadrados, pois  $n = N^2 + 0^2$ . E se  $m > 1$ , teremos que  $m = p_1 \cdot p_2 \dots p_r$  (uma vez que  $m$  é livre de quadrados), salvo o caso em que um dos  $p_i = 2$  todos os primos serão da forma  $4k + 1$ . No entanto, primos desta forma podem ser decompostos como soma de quadrados segundo o Teorema 7; e com  $2 = 1^2 + 1^2$ , o Lema 2 garante que existem  $a$  e  $b$  inteiros, tais que  $m = a^2 + b^2$ . Basta fazer  $A = N \cdot a$  e  $B = N \cdot b$ , que temos  $n = N^2 \cdot m = N \cdot (a^2 + b^2) = A^2 + B^2$ .

Para recíproca, se existem  $a$  e  $b$  inteiros tais que  $n = N^2 \cdot m = a^2 + b^2$ . No caso de  $m = 1$ , então este não será da forma  $4k + 3$  e encerramos. Mas se  $m > 1$  com um fator primo  $p$ , se  $d = (a, b)$  então existem  $t, r \in \mathbb{Z}$ , tais que  $a = td$  e  $b = rd$  com  $(r, t) = 1$ , daí  $d^2 \cdot (r^2 + t^2) = N^2 \cdot m$ . Uma vez que  $m$  é livre de quadrados, concluímos que  $d^2 | N^2$ , e portanto

$$r^2 + t^2 = \left( \frac{N^2}{d^2} \right) \cdot m = M \cdot p, \quad (4)$$

para algum inteiro positivo  $M$ . Escrevendo (4) como uma congruência módulo  $p$ , temos

$$r^2 + t^2 \equiv 0 \pmod{p}, \quad (5)$$

no entanto, como  $(r, t) = 1$  então  $(r, p) = 1$  ou  $(t, p) = 1$ . Se  $(r, p) = 1$  então existem  $r_1$

e  $r_2$  inteiros, tais que  $r_1 \cdot r + r_2 \cdot p = 1$ , ou seja,  $r_1 \cdot r \equiv 1 \pmod{p}$ . Assim, multiplicando (5) por  $r_1^2$ , obtemos  $(r \cdot r_1)^2 + (t \cdot r_1)^2 \equiv 1 + (t \cdot r_1)^2 \equiv 0 \pmod{p}$ , ou seja,  $(t \cdot r_1)^2 \equiv -1 \pmod{p}$  ou  $\left(\frac{-1}{p}\right) = 1$ . E pelo Teorema 4, a última igualdade, implica  $p = 2$  ou  $p = 4k + 1$ , nos fazendo concluir que  $m$  não tem fatores  $4k + 3$ . Analogamente, chegaríamos ao mesmo resultado ao supor  $(t, p) = 1$ .  $\square$

**Corolário 6.** *Com  $n \in \mathbb{N}$  vale que  $n = a^2 + b^2$  se, e somente se, os fatores primos de  $n$  da forma  $4 \cdot k + 3$  aparecerem com índice par.*

*Demonstração.* Sendo  $n = a^2 + b^2$ , o Teorema 9 garante que podemos ter  $n = N^2 \cdot m$  com  $m$  livre de quadrados, assim fatores do tipo  $4 \cdot k + 3$  que eventualmente fizerem parte de  $n$  estão em  $N^2$ .

Reciprocamente o natural  $n$  está elevado a uma potência par com  $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \dots \cdot p_r^{\alpha_r}$  em que  $p_i = 4 \cdot k + 3$  para  $1 \leq i \leq r$ . Então podemos representar o produto dos  $p_i$ 's por  $p^{2k}$  e os demais por  $m$ . Desta forma, com  $N = p^k$ , temos que  $n = N^2 \cdot m$  com  $m$  livre de quadrados e sem fatores do tipo  $4 \cdot k + 3$ , assim a recíproca do Teorema 9 nos garante que  $n = a^2 + b^2$ .  $\square$

**Exemplo 7.** *É possível decompor como uma soma de quadrados 490 e 693?*

Mesmo sem necessariamente saber quais os valores dos fatores que satisfazem as decomposições  $490 = a^2 + b^2$  e  $693 = c^2 + d^2$  pelo Corolário 6, somente 490 poderá ser escrito como uma soma de quadrados, pois  $490 = 2 \cdot 5 \cdot 7^2$ . Já  $693 = 3^2 \cdot 7 \cdot 11$  por apresentar 7 e 11 entre seus fatores primos não poderá assim ser escrito.

O Corolário 6 parece ser um “xeque-mate” no problema de constatar se um inteiro positivo pode ser escrito como soma de quadrados, pois basta apenas uma simples análise sobre os fatores primos  $p_i$  que o compõem. Porém quanto maior o valor dos inteiros, mais difícil fatorá-los, tornando inviável a análise anteriormente citada. Essa

inviabilidade abre uma janela para o avanço nesse campo matemático em busca de uma ferramenta que aprimore o processo.

Para finalizar, analisamos um resultado sobre a decomposição de um número positivo em uma diferença de quadrados.

**Proposição 14.** *Para  $a, b, n \in \mathbb{Z}$  com  $n$  positivo, temos que*

$$n = a^2 - b^2 \iff n \not\equiv 2 \pmod{4}.$$

*Demonstração.* Para qualquer inteiro par, vimos que  $a^2 \equiv 0 \pmod{4}$  e quando  $a$  é ímpar então  $a^2 \equiv 1 \pmod{4}$ , daí  $n = a^2 - b^2 \equiv 0 \pmod{4}$  se  $a$  e  $b$  tem mesma paridade, ou  $n \equiv a^2 - b^2 \equiv 1 \pmod{4}$ , ou mesmo  $n \equiv a^2 - b^2 \equiv 3 \pmod{4}$  quando  $a$  e  $b$  são de paridade distintas. Em todo caso, temos  $n \not\equiv 2 \pmod{4}$ .

Para recíproca, se  $n \not\equiv 2 \pmod{4}$  então teremos uma das possibilidades:

(i)  $n \equiv 1 \pmod{4}$

(ii)  $n \equiv 3 \pmod{4}$

(iii)  $n \equiv 0 \pmod{4}$ .

Se vale (i) e (ii) então serão pares os números  $n + 1$  e  $n - 1$  e podemos escrever  $n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$  como uma diferença de quadrados. E caso valha (iii), então  $n = \left(\frac{n}{4} + 1\right)^2 - \left(\frac{n}{4} - 2\right)^2$ . □

### 3.1 Soma de Quatro Quadrados

É mesmo admirável que, após muitos resultados da seção anterior, buscando condições que garantam decompor um número como soma de quadrados, descobrimos que qualquer inteiro positivo pode ser escrito como soma de quatro quadrados. Após nos empenharmos bastante, a fim de garantir a existência de  $a$  e  $b \in \mathbb{Z}$  tal que para  $m > 0$  inteiro temos  $m = a^2 + b^2$ . Não parece ser natural que dado qualquer  $m$  nas condições citadas existam sempre  $a, b, c$  e  $d \in \mathbb{Z}$  tais que:



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

Iniciaremos com um resultado análogo ao Lema 2 para o caso de decomposição de um inteiro em uma soma de quatro quadrados.

**Lema 3.** *Se  $m$  e  $n \in \mathbb{Z}^+$  podem ser escritos como soma de quatro quadrados, então  $m \cdot n$  também poderá ser escrito como soma de quatro quadrados.*

*Demonstração.* Sejam  $a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2$ , e tome  $m = a_1^2 + b_1^2 + c_1^2 + d_1^2$  e  $n = a_2^2 + b_2^2 + c_2^2 + d_2^2$ , então

$$\begin{aligned} m \cdot n &= (a_1^2 + b_1^2 + c_1^2 + d_1^2) \cdot (a_2^2 + b_2^2 + c_2^2 + d_2^2) \\ &= a_1^2 a_2^2 + a_1^2 b_2^2 + a_1^2 c_2^2 + a_1^2 d_2^2 + b_1^2 a_2^2 + b_1^2 b_2^2 + b_1^2 c_2^2 + b_1^2 d_2^2 \\ &\quad + c_1^2 a_2^2 + c_1^2 b_2^2 + c_1^2 c_2^2 + c_1^2 d_2^2 + d_1^2 a_2^2 + d_1^2 b_2^2 + d_1^2 c_2^2 + d_1^2 d_2^2 \\ &= (a_1 \cdot a_2)^2 + (b_1 \cdot b_2)^2 + (c_1 \cdot c_2)^2 + (d_1 \cdot d_2)^2 \\ &\quad + (a_1 \cdot b_2)^2 + (a_2 \cdot b_1)^2 + (c_1 \cdot d_2)^2 + (c_2 \cdot d_1)^2 \\ &\quad + (a_1 \cdot c_2)^2 + (b_1 \cdot d_2)^2 + (a_2 \cdot c_1)^2 + (b_2 \cdot d_1)^2 \\ &\quad + (a_1 \cdot d_2)^2 + (b_1 \cdot c_2)^2 + (b_2 \cdot c_1)^2 + (a_2 \cdot d_1)^2, \end{aligned}$$

o que fizemos até o momento foi distribuir o produto e associar as parcelas da soma em ordem conveniente. Continuando, somaremos cada linha às parcelas abaixo, de modo a completar o quadrado em cada linha. A igualdade será preservada pois o resultado da soma adicionada é zero

$$\begin{aligned} &2(a_1 a_2 b_1 b_2 + a_1 a_2 c_1 c_2 + a_1 a_2 d_1 d_2 + b_1 b_2 c_1 c_2 + b_1 b_2 d_1 d_2 + c_1 c_2 d_1 d_2) \\ &+ 2(-a_1 a_2 b_1 b_2 + a_1 b_2 c_1 d_2 - a_1 b_2 c_2 d_1 - a_2 b_1 c_1 d_2 + a_2 b_1 c_2 d_1 - c_1 c_2 d_1 d_2) \\ &+ 2(-a_1 b_1 c_2 b_2 - a_1 a_2 c_1 c_2 + a_1 b_2 c_2 d_1 + a_2 b_1 c_1 d_2 - b_1 b_2 d_1 d_2 - a_2 b_2 c_1 d_1) \\ &+ 2(a_1 b_1 b_2 d_2 - a_1 b_2 c_1 d_2 - a_1 a_2 d_1 d_2 - b_1 b_2 c_1 c_2 - a_1 b_2 c_1 d_2 + a_2 b_2 c_1 d_1). \end{aligned}$$

Completando quadrados temos

$$(a_1a_2 + b_1b_2 + c_1c_2 + d_1d_2)^2 = a^2$$

$$(a_1b_2 + a_2b_1 - c_1d_2 + c_2d_1)^2 = b^2$$

$$(a_1c_2 - b_2d_1 - a_1c_2 + b_2d_1)^2 = c^2$$

$$(a_1d_2 + b_2c_1 - b_2c_1 - a_2d_1)^2 = d^2,$$

ou seja,  $m \cdot n = m = a^2 + b^2 + c^2 + d^2$ . □

De acordo com o Lema 3, mostrar que  $m \in \mathbb{Z}$  e  $m > 0$  pode ser representado como soma de quatro quadrados, isso é mesmo que mostrar que qualquer primo pode ser assim representado. Pois o Teorema 1 (TFA), nos garante que qualquer inteiro é escrito como produto de primos.

Antes de chegar a tal conclusão sobre  $p > 0$  primo, faremos no próximo Teorema o uso do Princípio da Casa dos Pombos que em uma de suas versões, muito conhecida, diz que: *Ao distribuir  $n+1$  pombos em  $n$  casas, necessariamente colocaremos ao menos dois pombos em umas das casas.*

Geralmente o recurso anunciado é utilizado para demonstrações de existência de determinado elemento ou de uma característica do mesmo. Veremos em que condições ele foi aplicado no próximo resultado.

**Lema 4.** *Seja  $p > 2$  primo então existem inteiros  $x_0$  e  $y_0$  no intervalo  $[0, \frac{p-1}{2}]$  soluções da equação:*

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}.$$

*Demonstração.* Tomamos  $S_1 = 1+k^2$  ( em que  $k = 0, 1, 2, \dots, \frac{p-1}{2}$ ) e  $S_2 = -l^2$  (em que  $l = 0, 1, 2, \dots, \frac{p-1}{2}$ ) como conjuntos das soluções inteiras da equação  $x^2+y^2+1 \equiv 0 \pmod{p}$  em  $[0, \frac{p-1}{2}]$ .

Mostraremos que, em  $S_1$  ou  $S_2$ , dois elementos distintos são incongruentes módulo  $p$ , pois com  $1 + k_1^2$  e  $1 + k_2^2$ , distintos, em  $S_1$  e supondo  $1 + k_1^2 \equiv 1 + k_2^2 \pmod{p}$ , então  $k_1^2 - k_2^2 \equiv (k_1 + k_2) \cdot (k_1 - k_2) \equiv 0 \pmod{p}$ ; e uma vez que,  $k_1$  e  $k_2 \in [0, \frac{p-1}{2}]$  vale uma das possibilidades

$$0 \leq k_1 + k_2 \leq (p-1) \quad \text{ou} \quad -(p-1) \leq k_1 - k_2 \leq (p-1).$$

Com  $0 \leq k_1 + k_2 \leq (p-1)$ , temos  $k_1 + k_2 \equiv 0 \pmod{p} \iff 1 + k_1^2 = 1 + k_2^2$  se  $-(p-1) \leq k_1 - k_2 \leq (p-1)$ , então  $k_1 - k_2 \equiv 0 \pmod{p} \iff 1 + k_1^2 = 1 + k_2^2$ .

Em todo caso, contrariamos a suposição  $1 + k_1^2 \neq 1 + k_2^2$  mostrando que em  $S_1$  dois elementos distintos são incongruentes.

Da mesma forma, com  $-l_1^2 \neq -l_2^2$  em  $S_2$  se  $-l_1^2 \equiv -l_2^2 \pmod{p}$ , então  $-l_1^2 = -l_2^2$ . Logo, em  $S_2$ , dois elementos distintos são incongruentes entre si.

Nota-se que  $S_1$  e  $S_2$  são disjuntos, pois temos apenas elementos positivos em um e no outro apenas elementos negativos; assim, a quantidade de elementos da união dos dois conjuntos é

$$n(S_1 \cup S_2) = n(S_1) + n(S_2) = \left(1 + \frac{p-1}{2}\right) + \left(1 + \frac{p-1}{2}\right) = p + 1.$$

E com uso, do Princípio de Casas dos Pombos, ao distribuir os  $p + 1$  elementos, os “pombos”, em suas “casas”, que são os possíveis restos na divisão por  $p$ , há ao menos dois elementos em  $S_1 \cup S_2$  com o mesmo resto na divisão por  $p$  (dois pombos na mesma casa). Em resumo, existem  $1 + x_0^2$  e  $-y_0^2$  em  $S_1$  e  $S_2$  respectivamente, tais que  $1 + x_0^2 \equiv -y_0^2 \pmod{p}$  se, e somente se,  $1 + x_0^2 + y_0^2 \equiv 0 \pmod{p}$ .  $\square$

**Corolário 7.** Com  $p > 2$  primo então  $\exists k \in \mathbb{Z}_+$  com  $k < p$  e  $k \cdot p = a^2 + b^2 + c^2 + d^2$ .

*Demonstração.* O Lema 4 nos garante a existência de  $x_0$  e  $y_0$  em  $(0, \frac{p}{2})$ , tais que  $1 + x_0^2 + y_0^2 \equiv 0 \pmod{p}$ , o que equivale a  $x_0^2 + y_0^2 + 1 + 0 = k \cdot p$ .

Basta-nos apenas verificar que  $k < p$ , como  $x_0$  e  $y_0 \in (0, \frac{p}{2})$  e  $p > 2$ , então

$$k \cdot p = x_0^2 + y_0^2 + 1^2 < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2 \iff k < p.$$

□

**Teorema 10.** Para todo  $p$  número primo, temos que  $p = a^2 + b^2 + c^2 + d^2$ .

*Demonstração.* Para  $p = 2$  é fácil ver que  $2 = 1^2 + 1^2 + 0^2 + 0^2$ . Como Corolário 7 nos garante que  $k \cdot p = a^2 + b^2 + c^2 + d^2$  com  $k < p$ ; e este  $k$  sendo menor inteiro, em que tal decomposição é possível, devemos mostrar que  $k = 1$ .

Vamos inicialmente supor que  $k$  é par, e podemos concluir que uma das situações acontece: Para  $a, b, c$  e  $d$  são todos pares ou todos ímpares ou dois pares e dois ímpares, em todo caso, vale que

$$a \equiv b \pmod{2} \text{ e } c \equiv d \pmod{2}$$

e assim,  $\frac{(a-b)}{2}, \frac{(a+b)}{2}, \frac{(c-d)}{2}, \frac{(c+d)}{2} \in \mathbb{Z}$ . Com isso, vale a igualdade

$$\left(\frac{1}{2} \cdot k\right) \cdot p = \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2.$$

Porém como  $k$  é par, temos então que  $\frac{1}{2} \cdot k$  é inteiro e, assim, a igualdade acima contraria o fato de  $k$  ser o menor valor em que tal decomposição seria possível.

Supondo  $k$  ímpar com  $k \geq 3$ , nos permite escolher  $x, y, z$  e  $w \in \mathbb{Z}$ , tais que

$$a \equiv x \pmod{k}, \quad b \equiv y \pmod{k}, \quad c \equiv z \pmod{k} \text{ e } d \equiv w \pmod{k}$$

com

$$|x|, |y|, |z| \text{ e } |w| < \frac{k}{2}.$$

Essa escolha é sempre possível, pois caso  $|x| \geq k$ , então escolheríamos  $x - k < \frac{k}{2}$  como resto da divisão de  $a$  por  $k$ .

Nossa suposição garante que  $kp = a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k}$ ; conseqüentemente, existe  $n \in \mathbb{Z}$ , tal que  $n \cdot k = x^2 + y^2 + z^2 + w^2$ .

A forma como escolhemos  $x, y, z$  e  $w$  nos permite deduzir que  $0 \leq n \cdot k = x^2 + y^2 + z^2 + w^2 \leq 4 \cdot \left(\frac{k}{2}\right)^2 = k^2$ , ou seja,  $n \neq 0$ ; pois se  $n = 0$ , teríamos  $x = y = z = w = 0$  e assim  $k|a$ ,  $k|b$ ,  $k|c$  e  $k|d$ , equivalente a  $k^2|k \cdot p \implies k|p$ , o que seria um absurdo, pois  $1 < k$  e  $p$  é um número primo.

Assim temos que  $0 < n \cdot k < k^2$  equivalente a  $0 < n < k$ , como

$$k^2 \cdot np = (a^2 + b^2 + c^2 + d^2) \cdot (x^2 + y^2 + z^2 + w^2) = A^2 + B^2 + C^2 + D^2,$$

o Lema 3, garante que

$$A = ac + bxcz + dw, B = ay - bx + cw - dz, C = az - bw - dx + cz \text{ e } D = aw + bz - cy - dx.$$

Desta forma, vale que  $\frac{A}{k}, \frac{B}{k}, \frac{C}{k}$  e  $\frac{D}{k} \in \mathbb{Z}$ , e vale a igualdade a seguir

$$n \cdot p = \left(\frac{A}{k}\right)^2 + \left(\frac{B}{k}\right)^2 + \left(\frac{C}{k}\right)^2 + \left(\frac{D}{k}\right)^2 \quad (6)$$

com  $0 < n < k$ . A equação 6 contraria novamente o fato de  $k$  ser o menor valor que, multiplicado por  $p$ , pode ser escrito como soma de quatro quadrados. Assim concluímos que a única possibilidade é  $k = 1$  finalizando a demonstração.  $\square$

O Principal resultado desta seção, o Teorema de Euler, comprova a afirmação supracitada, que todo inteiro positivo pode ser escrito como soma de quatro quadrados.

**Teorema 11.** (Euler) *Qualquer inteiro positivo  $n$  pode ser escrito como soma de quatro quadrados, ou seja, existem  $a, b, c, d \in \mathbb{Z}$ , tais que  $n = a^2 + b^2 + c^2 + d^2$ .*

A verificação é consequência direta dos Teoremas 1 e 10, e do Lema 3.

Semelhante ao tratamento dado à fatoração de um inteiro positivo em uma soma de quadrados, também não falamos como fatorar um inteiro  $n > 0$  como  $a^2 + b^2 + c^2 + d^2$ , embora, para esse caso, temos a vantagem de saber que ao menos um desses fatores está em  $(0, \frac{\sqrt{n}}{2})$ , pois se  $a = b = c = d = \frac{\sqrt{n}}{2}$  então

$$a^2 + b^2 + c^2 + d^2 = 4 \cdot \left(\frac{\sqrt{n}}{2}\right)^2 = n.$$

A decomposição de valores pequenos de  $n$ , como soma de quatro quadrados, é uma atividade que se encaixa à realidade dos alunos do ensino básico. Por exemplo:

**Exemplo 8.** *Fatore 29 como soma de quatro quadrados.*

Como foi comentado, ao menos um dos fatores estará no intervalo  $\left(0, \frac{\sqrt{29}}{2}\right)$ , ou seja, menor que 3; e ao fatorarmos como soma de quatro quadrados, o número 29, encontramos mediante sucessivas tentativas os seguintes valores:

$$29 = 0^2 + 2^2 + 3^2 + 4^2 = 0^2 + 0^2 + 2^2 + 5^2.$$

Ao tratarmos questões como essas em turmas mais experientes, podemos propor uma miscelânea com o conteúdo da Análise Combinatória. Assim, no Exemplo 8, também poderíamos pedir ao aluno que o mesmo exiba o número de sequências que podemos formar com os algarismos dos fatores da soma como quatro quadrados. Desta forma, temos 12 sequências com 4 algarismos para  $29 = 0^2 + 0^2 + 2^2 + 5^2$ , a saber:

0025, 0052, 0250, 0520, 0205, 0502, 2500, 5200, 2050, 5020, 2005 e 5002.

## 4 O Método de Minkowski

O Método de Minkowski, tema central do nosso trabalho, é uma ferramenta que nos permite contar de quantas maneiras podemos escrever o número inteiro e positivo  $m$  como soma de quadrados, em que os fatores  $a$  e  $b$  da soma são co-primos. Ou seja

$$m = a^2 + b^2 \text{ com } (a, b) = 1.$$

E então usaremos definições estabelecidas no Capítulo 2 no intuito de evidenciar o Método, tomando por destaque a noção de equivalência entre pontos do plano  $\mathbb{H}$ , assim como a equivalência entre formas quadráticas binárias positivas.

Relacionaremos de forma bijetora estes dois conceitos para obtermos um processo sistemático que nos permitirá decidir sobre a equivalência de formas quadráticas, analisando pontos sobre  $\mathbb{H}$  (plano superior complexo).

Essa não é a única forma de chegar ao resultado sobre o número de maneiras de decompor o número inteiro e positivo  $m$  como soma de quadrados. Mas essa forma nos permite admitir generalizações, além de ser dotada de muita beleza e engenhosidade. As demonstrações dos resultados deste capítulo foram tiradas de [11].

### 4.1 Domínio Fundamental para Ação de $SL$ sobre $\mathbb{H}$

**Teorema 12.** *Para  $\mathbb{H}_0 \subset \mathbb{H}$ , definido como*

$$\mathbb{H}_0 = \left\{ z = x + iy \in \mathbb{H}, \text{ tais que } -\frac{1}{2} \leq x < \frac{1}{2} \text{ e } |z| > 1 \text{ ou } -\frac{1}{2} \leq x \leq 0 \text{ e } |z| = 1 \right\},$$

( a parte em destaque, na figura 4.1).

*Então, conforme a Definição 15,  $\mathbb{H}_0$  é um domínio fundamental para a ação de  $SL_2(\mathbb{Z})$  sobre  $\mathbb{H}$ .*

*Demonstração.* Vamos inicialmente demonstrar que para  $z_0, w_0 \in \mathbb{H}_0$  não existirá  $\Gamma \in SL_2(\mathbb{Z})$  tal que  $z_0 \star \Gamma = w_0$ ; em outras palavras, dois pontos em  $\mathbb{H}_0$  não serão

equivalentes. Logo após, mostramos que para todo  $z \in \mathbb{H}$  existe um  $\Gamma \in SL_2(\mathbb{Z})$  que  $z \star \Gamma \in \mathbb{H}_0$ , e, conforme com a Definição 15, isso finalizará a demonstração.

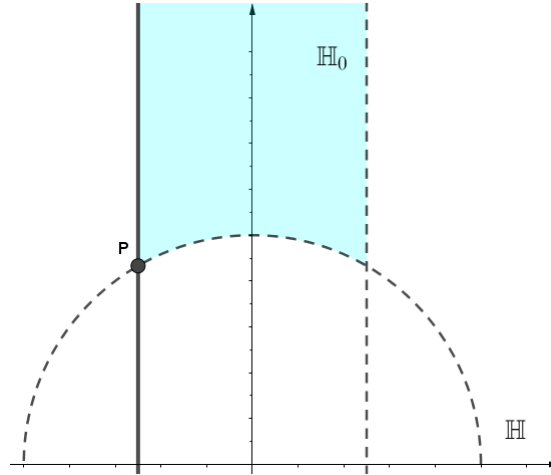


Figura 4.1: Semi Plano Complexo  $\mathbb{H}$  e  $\mathbb{H}_0$ .

Fixado  $\Gamma_1 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ , vamos associar a cada  $z \in \mathbb{H}$  com

$$z' = z \star \Gamma_1 = \frac{az + b}{cz + d}.$$

O modo como foi definido  $z' \in \{\mathbb{C} ; |cz + d| = 1\}$ , esse está em um círculo  $C_1$  de centro  $\left(\frac{-d}{c}, 0\right)$  e raio  $\frac{1}{|c|} \leq 1$ , uma vez que  $c \in \mathbb{Z}$ . Observamos também que

$$cz' - a = c \frac{az + b}{cz + d} - a = \frac{bc - ad}{cz + d} = \frac{-1}{cz + d},$$

assim, se  $z \in C_1$  então  $z' \notin C_1$ . Mais interessante que isso, é observar que se  $z$  é exterior a  $C_1$ , então  $z'$  será interior a  $C_2 = |cz' + a|$ , ou seja  $|cz + d| > 1 \implies |cz' + a| < 1$ .

Observe que os círculos  $C_1$  e  $C_2$  ou estão centrados em pontos inteiros com raios iguais a 1 ou estão centrados em pontos racionais (veja que  $(d, c) = 1$ ) com raio menor ou igual à  $\frac{1}{2}$ . O que nos permite concluir que, com exceção dos pontos do arco  $\mathbf{A} = \{z = x + yi \in \mathbb{H} : |z| = 1 \text{ e } -\frac{1}{2} \leq x \leq 0\}$ , todos os demais pontos  $z$  de  $\mathbb{H}_0$  serão exteriores a qualquer círculo  $C_1$ , que é unicamente determinado pela escolha de  $\Gamma_1$ , portanto os pontos  $z'$  são interiores a  $C_2$  e conseqüentemente  $z' = z \star \Gamma_1 \notin \mathbb{H}_0$ .



O arco  $\mathbf{A}$ , por sua vez, é exterior a todos os círculos  $C_1$ , exceto

$$\lambda_1 = \{z \in \mathbb{C}; |z| = 1\} \quad \text{e} \quad \lambda_2 = \{z \in \mathbb{C}; |z + 1| = 1\}.$$

O círculo  $\lambda_1$  está associado à transformação  $T : \mathbb{H} \rightarrow \mathbb{H}$  do tipo

$$T(z) = z' = \frac{az + b}{z}.$$

Por sua vez, a transformação  $T$  está associada a uma matriz de  $SL_2(\mathbb{Z})$ . Fazendo  $b = -1$ , temos

$$z' = \frac{az - 1}{z} = a - \frac{1}{z} \implies |z' - a| = \frac{1}{z}.$$

Se  $z \in \mathbf{A}$ , temos  $|z| = 1$ , logo  $|z' - a| = 1$  e  $z' \notin \mathbb{H}_0$ , haja vista que  $a \in \mathbb{Z}$ . Contudo a afirmação  $z' \notin \mathbb{H}_0$  não será verdadeira se  $a = 0$  ou  $a = -1$ , pois quando  $a = 0$  teremos a transformação  $W(z) = -\frac{1}{z}$ , que leva o arco  $\mathbf{A}$  no arco  $\mathbf{B} = \{z = x + yi \in \mathbb{H} : |z| = 1 \text{ e } 0 \leq x \leq \frac{1}{2}\}$ . Além do mais,  $\mathbf{A} \cap \mathbf{B} = \{i\}$  e  $W(i) = \frac{-1}{i} = \frac{-1}{i} \cdot \frac{-i}{-i} = \frac{i}{-i^2} = \frac{i}{1} = i$ .

No entanto, quando for o caso de  $a = -1$ , será a transformação  $T_1(z) = \frac{-(z+1)}{z}$  que levará o arco  $\mathbf{A}$  no arco  $\mathbf{C} = \{z = x + yi \in \mathbb{H} : |z + 1| = 1 \text{ e } -1 \leq x \leq -\frac{1}{2}\}$ , assim  $\mathbf{A} \cap \mathbf{C} = \{\rho\}$ , em que  $\left(\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}\right)$  e  $T_1(\rho) = \rho$ .

Por outro lado, o círculo  $\lambda_2 = |z + 1| = 1$  está associado a uma transformação do tipo

$$z' = \frac{az + b}{z + 1} = \frac{az + (a - 1)}{z + 1} = a - \frac{1}{z + 1}.$$

A segunda igualdade é obtida pelo fato de  $\det \begin{pmatrix} a & b \\ 1 & 1 \end{pmatrix} = a - b = 1$ , e desta forma,

temos

$$-\frac{1}{z + 1} = z' - a \implies z = -\left(\frac{z' - (a - 1)}{z' - a}\right)$$

como resultado se  $z \in \mathbf{A}$ , logo  $|z| = 1$  e  $|z' - (a - 1)| = |z' - a|$ . Uma vez que  $z' = x' + iy'$

temos então que

$$|x' - (a - 1) + iy'|^2 = |x' - a + iy'|^2 \implies [x' - (a - 1)]^2 + (y')^2 = (x' - a)^2 + (y')^2,$$

daí concluímos que  $x' = a - \frac{1}{2}$ .

Assim,  $z'$  não pertencerá a  $\mathbb{H}_0$ , a menos que  $a = 0$ , e neste caso temos que a transformação  $T_2(z) = \frac{-1}{z+1}$  leva o arco  $\mathbf{A}$  sobre o segmento  $\mathbf{L} = \{z = x + iy \in \mathbb{H} : x = -\frac{1}{2} \text{ e } \frac{1}{2} \leq y \leq \frac{\sqrt{3}}{2}\}$ . Desta forma,  $\mathbf{A} \cap \mathbf{L} = \{\rho\}$  e  $T_2(\rho) = \rho$ .

Evidenciamos que não existe  $w \in \mathbf{A}$  tal que para alguma matriz  $U \in SL_2(\mathbb{Z})$  tenhamos  $w$  e  $U \star w \in \mathbf{A}$  com  $U \star w \neq w$ . Em resumo, dois pontos distintos de  $\mathbb{H}_0$  não são equivalentes.

Para completar a demonstração, precisamos mostrar que para qualquer  $w \in \mathbb{H}$ , existe  $T \in SL_2(\mathbb{Z})$ , tal que  $T \star w \in \mathbb{H}_0$ . Se adotarmos a notação

$$S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ e } W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$S$  é o gerador do grupo  $SL_2(\mathbb{Z})$ , isto é, para qualquer  $U \in SL_2(\mathbb{Z})$ , existe  $n \in \mathbb{Z}$  tal que  $U = S^n$ . Podemos mostrar que para qualquer  $w \in \mathbb{H}$ , existem  $n_1, \dots, n_k \in \mathbb{Z}$  tais que  $S_k^{n_k} W S_{k-1}^{n_{k-1}} W \dots W S_2^{n_2} W S_1^{n_1} \star w \in \mathbb{H}_0$ . E isso completa a prova.  $\square$

**Teorema 13.** *O ponto  $\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$  é aplicado por si mesmo pelas transformações*

$$I(z) = z, T_1 = -\frac{z+1}{z}, T_2 = -\frac{1}{z+1}$$

*e por nenhuma outra. O ponto "i" é aplicado por si mesmo pelas transformações*

$$I(z) = z, W(z) = \frac{-1}{z}$$

*e por nenhuma outra. Qualquer outro ponto de  $\mathbb{H}_0$  diferente de  $i$  e de  $\rho$  só é aplicado sobre si mesmo pela transformação identidade  $I(z) = z$ .*

A demonstração pode ser deduzida a partir do Teorema 12.

**Teorema 14.** *Seja  $U \in \Gamma$ . Existem  $n_1, \dots, n_k \in \mathbb{Z}$  tais que  $U = W^\epsilon S_k^{n_k} W \dots W S_2^{n_2} W S_1^{n_1}$ , com  $\epsilon = 0$  ou  $2$ .*

*Demonstração.* Seja  $U \in \Gamma$ . Tome  $w \in \mathbb{H}_0$  tal que  $w \notin \mathbf{A}$ . Para o ponto  $U^{-1} \cdot w \in \mathbb{H}$ , o Teorema 12 nos diz que existem  $n_1, \dots, n_k \in \mathbb{Z}$  tais que,  $S_k^{n_k} W \dots W S_1^{n_1} \cdot (U^{-1} \star w) \in \mathbb{H}_0$ , ou seja,  $S_k^{n_k} W S_{k-1}^{n_{k-1}} W \dots W S_1^{n_1} \cdot U^{-1} \star w \in \mathbb{H}_0$ .

Pelo Teorema 13, a única alternativa para esta situação é  $S_k^{n_k} W \dots W S_1^{n_1} U^{-1} = \pm I_2$ , e assim  $U = \pm I_2 \cdot S_k^{n_k} W \dots W S_1^{n_1} = W^\epsilon S_k^{n_k} W W S_1^{n_1}$  (veja que  $W^2 = -I_2$  e  $W^0 = I_2$ ), o que completa a demonstração.  $\square$

Em resumo, o Teorema 14 nos diz que  $SL_2(\mathbb{Z})$  é finitamente gerado por  $S$  e  $W$ . A reunião dos últimos Teoremas nos fornece uma ferramenta prática para decidir quando dois pontos de  $\mathbb{H}$  são equivalente, pois com  $w_1$  e  $w_2 \in \mathbb{H}$  determinamos  $\tilde{w}_1$  e  $\tilde{w}_2 \in \mathbb{H}_0$ , tais que  $w_i$  seja equivalente a  $\tilde{w}_i$  ( $i = 1, 2$ ). Além do mais, o Teorema 12 nos garante que para  $w \in \mathbb{H}$  existirá um número finito de translações (transformações do tipo  $S^n \cdot w$ ) e reflexões (transformações do tipo  $W \cdot w$ ) aplicados a  $w$ , que nos leva obter  $\tilde{w} \in \mathbb{H}_0$  tal que  $\tilde{w}$  é equivalente a  $w$ ; então  $w_1$  é equivalente a  $w_2$  se, e somente se,  $\tilde{w}_1 = \tilde{w}_2$ .

## 4.2 Relação entre Formas Quadráticas Binárias e o Plano $\mathbb{H}$

Nesta seção vamos efetivamente deduzir resultados sobre formas quadráticas binárias, trabalhando sobre os pontos de  $\mathbb{H}$ . Definiremos também a representação própria de um inteiro para finalmente apresentar e provar o resultado principal do nosso trabalho, o Método de Minkowski, que corresponde a um Corolário de um Teorema mais geral.

Inicialmente, lembremos-nos que

$$f(x, y) = ax^2 + bxy + cy^2 \text{ é uma Forma quadrática binária com } a, b, c \in \mathbb{R}.$$

A Forma será positiva quando  $a > 0$  e  $\Delta = 4ac - b^2 > 0$ . A verificação deste fato é relativamente fácil quando a matriz  $F$  (associada à Forma) é  $2 \times 2$ . A generalização com uma matriz  $n \times n$  (pode ser vista em [3]) que será um caso particular de um Teorema que estabelece a afirmação de  $f$  ser positiva definida se, e somente se, todos os menores principais de ( $F$  matriz de  $f$ ) forem positivos.

Fixando o  $\Delta > 0$ , podemos associar a nossa  $f$  com um polinômio quadrático  $p(z) =$

$az^2 + bz + c$ , que tem zeros  $\frac{-b \pm \sqrt{-\Delta}}{2a}$  e  $\frac{-b \pm \sqrt{\Delta}.i}{2a}$ . Chamaremos de  $w_f$  o zero deste polinômio que pertence a  $\mathbb{H}$ , ou seja,  $w_f = \frac{-b \pm \sqrt{\Delta}.i}{2a}$ . Reciprocamente, se  $z_0 = x_0 + iy_0 \in \mathbb{H}$ , existe um único número positivo  $u$  tal que a forma quadrática associada ao polinômio quadrático  $p(z) = u(z - z_0)(z - \bar{z}_0)$  que tem *discriminante*  $\Delta$  (basta tomar  $u = \frac{\sqrt{\Delta}}{2y_0}$ ). Assim, existe uma correspondência bijetora entre formas quadráticas binárias positivas de discriminante  $\Delta > 0$  e pontos do plano superior  $\mathbb{H}$ , conforme o exemplo da figura 4.2 para as formas binárias:  $f(x, y) = x^2 + y^2$  e  $g(x, y) = 10x^2 - 6xy + y^2$ .

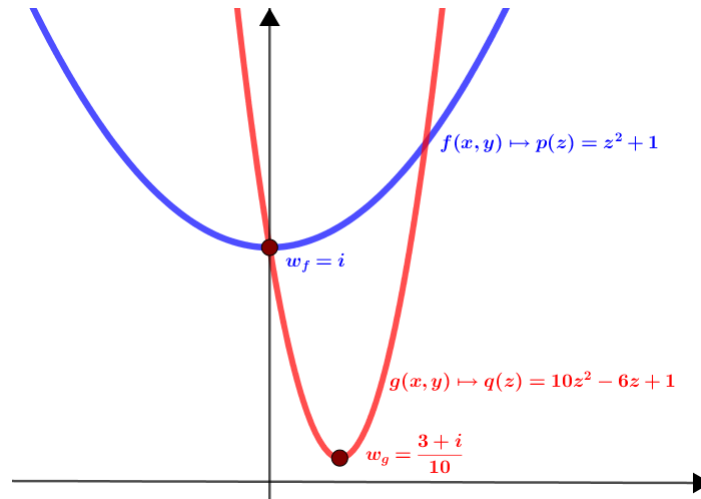


Figura 4.2: Representantes das Formas binárias.

Usando esta bijeção, chamamos o ponto  $w_f = \frac{-b + \sqrt{\Delta}.i}{2a}$  descrito acima como representante da Forma  $f$ . Vale também ressaltar que a demonstração do próximo teorema é uma tarefa mais trabalhosa do que necessariamente difícil de provar. Esse Teorema irá conectar Formas binárias com  $\Delta > 0$  fixo aos seus representantes.

**Teorema 15.** *Sejam  $f$  e  $g$  formas quadráticas binárias positivas definidas e de discriminante  $\Delta > 0$ . Sejam  $w_f$  e  $w_g$  os pontos de  $\mathbb{H}$  que são os pontos de  $f$  e  $g$  (obtidos*

como antes) e  $F$  e  $G$  as matrizes de  $f$  e  $g$ , respectivamente. Então, existe  $T \in SL_2(\mathbb{Z})$  tal que  $T \star w_f = w_g$  se, e somente se,  $G = {}^tTFT$ .

*Demonstração.* Sendo  $f(x, y) = a_1x^2 + a_2xy + a_3y^2$  e  $g(x, y) = nx^2 + mxy + ly^2$  duas formas quadráticas como no enunciado com matrizes correspondentes:

$$F = \begin{pmatrix} a_1 & \frac{a_2}{2} \\ \frac{a_2}{2} & a_3 \end{pmatrix} \text{ e } G = \begin{pmatrix} n & \frac{m}{2} \\ \frac{m}{2} & l \end{pmatrix},$$

e representantes:  $w_f = \frac{-b \pm \sqrt{\Delta}}{2a}$ ,  $w_g = \frac{-m \pm \sqrt{\delta}}{2n}$  com  $\Delta = b^2 - 4ac$  e  $\delta = m^2 - 4nl$ .

Com  $f$  equivalente a  $g$ , é notório que existirá  $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$  tal que  ${}^tTFT = G$ , ou seja,

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} a_1 & \frac{a_2}{2} \\ \frac{a_2}{2} & a_3 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} n & \frac{m}{2} \\ \frac{m}{2} & l \end{pmatrix},$$

o que equivale a

$$\begin{aligned} n &= a_1a^2 + a_2ac + a_3c^2 \\ m &= 2a_1ab + a_2(ad + bc) + 2a_3cd \\ l &= a_1b^2 + a_2bd + a_3d^2. \end{aligned} \tag{7}$$

Feito isso, será apenas um esforço computacional substituir os valores de  $n, m$  e  $l$  da equação 7 em

$$w_g = \frac{-m \pm \sqrt{\delta}}{2n},$$

e aplicando  $\star$ , obtemos:

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \star w_g = \frac{aw_g + c}{bw_g + d} = \frac{-b \pm \sqrt{\Delta}}{2a} = w_f.$$

A recíproca se dá de maneira semelhante, bastando apenas seguir o caminho inverso da primeira parte. □

O que este Teorema nos diz , em outras palavras, é que duas formas quadráticas binárias  $f$  e  $g$  positivas definidas e de *discriminante*  $\Delta > 0$  são equivalentes se, e somente se, seus representantes forem equivalentes.

Como por exemplo as formas binárias  $f(x, y) = x^2 + y^2$  e  $g(x, y) = 10x^2 - 6xy + y^2$  da figura 4.2, em que:

$$F = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ e } G = \begin{pmatrix} 10 & -3 \\ -3 & 1 \end{pmatrix}, \text{ com } T = \begin{pmatrix} -1 & 0 \\ 3 & -1 \end{pmatrix} \in SL_2(\mathbb{Z}), \text{ temos que,}$$

$$\begin{pmatrix} -1 & 3 \\ 0 & -1 \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} -1 & 0 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} 10 & -3 \\ -3 & 1 \end{pmatrix} \text{ e como seus representantes são}$$

respectivamente:  $w_f = i$  e  $w_g = \frac{3+i}{10}$ , é fácil verificar que  $\begin{pmatrix} -1 & 0 \\ 3 & -1 \end{pmatrix} \star i = \frac{3+i}{10}$ . A ideia de representante em  $\mathbb{H}$  para cada Forma binária nos leva a seguinte definição:

**Definição 17.** (*Forma reduzida*) Uma Forma quadrática binária  $f$  positiva definida com  $\Delta > 0$  será chamada de Forma reduzida se o seu representante  $w_f$  pertence a  $\mathbb{H}_0$ .

Vimos que Formas quadráticas equivalentes contêm Formas reduzidas e estas constituem um sistema completo de representantes para a relação de equivalência, definida entre as Formas quadráticas binárias positivas de *discriminante*  $\Delta$ .

Verificamos algumas condições que uma forma reduzida  $f(x, y) = ax^2 + bxy + cy^2$  deve cumprir. Sendo  $w_f = \frac{-b + \sqrt{\Delta}.i}{2a} = \frac{-b}{2a} + \frac{\sqrt{\Delta}.i}{2a}$  e  $|w_f|^2 = \frac{b^2 + \Delta}{4a^2} = \frac{c}{a}$ , como devemos ter  $w_f \in \mathbb{H}_0$ , então

$$-\frac{1}{2} \leq \frac{-b}{2a} < \frac{1}{2} \text{ e } \frac{c}{a} > 1 \text{ ou } -\frac{1}{2} \leq \frac{-b}{2a} \leq 0 \text{ e } \frac{a}{c} = 1.$$

Simplemente, temos que a Forma  $f(x, y) = ax^2 + bxy + cy^2$  está reduzida se, e somente se,

$$-a < b \leq a < c \text{ ou } 0 \leq b \leq a = c. \quad (8)$$

Doravante designaremos apenas por “ $\Delta$ -forma positiva inteira” as Formas quadrá-

ticas  $f(x, y) = ax^2 + bxy + cy^2$  positivas definidas, com  $a, b, c \in \mathbb{Z}$  e  $\Delta = 4ac - b^2$ , fixo.

**Teorema 16.** *Existe apenas um número finito de  $\Delta$ -formas positivas inteiras que são reduzidas.*

*Demonstração.* Seja  $f(x, y) = ax^2 + bxy + cy^2$  uma Forma nas condições do Teorema pela equação (8) logo  $4a^2 \leq 4ac = \Delta + b^2 \leq \Delta + a^2$  e  $0 < a \leq \sqrt{\Delta/3}$ . Assim, temos um número finito de possibilidade para  $a$  (já que  $a \in \mathbb{Z}$  e  $\Delta > 0$  está fixado). Como  $|b| \leq a$  (também pelas condições em (8)) então haverá um número finito de possibilidades para  $b$ . Finalmente, para cada par  $a$  e  $b$  existe no máximo um número inteiro positivo  $c$  tal que  $4ac - b^2 = \Delta$ .  $\square$

Uma parte do processo, na busca da nossa ferramenta específica de contagem (o Método de Minkowski), é inferir que a contagem de  $\Delta$ -formas positivas inteiras reduzidas é o mesmo que contar as classes de equivalência das mesmas, pois como observado, em cada classe de equivalência, encontramos exatamente uma Forma reduzida.

Por exemplo, para  $\Delta = 3$ , devemos ter  $0 < a \leq 1$ ; logo  $a = 1$ , resulta em

$$\Delta = 4ac - b^2 \iff 3 = 4c - b^2$$

de  $|b| \leq 1$ , e assim temos  $b = 0$  ou  $b = 1$ . Para  $b = 0$  deveríamos encontrar um inteiro positivo  $c$  tal que  $4c = 3$ , o que não é possível. Para  $b = 1$  encontramos  $c = 1$  e a Forma  $x^2 + xy + y^2$  é a única 3-forma positiva inteira e reduzida. De maneira semelhante, o leitor pode mostrar que só existe uma classe de *discriminante* 4 e sua forma reduzida é  $x^2 + y^2$ . Como representante de  $x^2 + y^2$ , temos “ $i$ ” de  $x^2 + xy + y^2$  é “ $\rho$ ”.

**Definição 18.** *(Unidade de  $f$ )* Seja  $f$  uma Forma quadrática positiva definida (não necessariamente inteira) e  $F$  sua matriz associada, uma “unidade de  $f$ ” é uma matriz  $U \in SL_2(\mathbb{Z})$  tal que  ${}^tUFU = F$ .

Podemos notar a partir desta definição que, para cada forma  $f$ , o conjunto  $\mathbf{U}(f)$  de todas as unidades de  $f$  é um subgrupo de  $SL_2(\mathbb{Z})$ .

O Teorema 15 nos mostra que se  $f$  é uma Forma quadrática binária positiva definida de discriminante  $\Delta$  e  $w_f$  é o representante de  $f$  em  $\mathbb{H}$ , então  $U \in SL_2(\mathbb{Z})$  é uma unidade de  $f$  se, e somente se,  $U \star w_f = w_g$ . Em conjunto com o Teorema 13, temos condições de verificar o próximo resultado.

**Teorema 17.** *Seja  $a > 0$ ; as Unidades da forma  $f(x, y) = a(x^2 + y^2)$  serão apenas*

$$\pm I_2 \quad \text{e} \quad \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

E as unidades da forma  $g(x, y) = a(x^2 + xy + y^2)$  serão somente

$$\pm I_2, \pm \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{e} \quad \pm \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Toda forma binária reduzida distinta dessas duas possui como unidade apenas  $\pm I_2$ .

**Observações:** É imediato verificar as seguintes propriedades:

(1) Se  $f$  e  $g$  são formas equivalentes e  $T \in SL_2(\mathbb{Z})$  é tal que  $G = {}^tTFT$  ( $T$  e  $G$  matrizes de  $f$  e  $g$  respectivamente) então  $\mathbf{U}(g) = T^{-1}\mathbf{U}(f)T$  (isto é, se  $U \in \mathbf{U}(g)$  logo  $TUT^{-1} \in \mathbf{U}(f)$  e reciprocamente, se  $V \in \mathbf{U}(f) \implies T^{-1}VT \in \mathbf{U}(g)$ ). Portanto, conhecendo o grupo das unidades das formas reduzidas, identificamos o grupo das unidades de qualquer forma quadrática binária positiva.

(2) Seja  $f(x, y) = a_1x^2 + a_2xy + a_3y^2$  uma forma quadrática binária com matriz associada  $F$  com  $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$  e  $g$  é a forma associada à matriz  $G = {}^tUFU$ , então uma computação simples mostra que  $g(x, y) = nx^2 + mxy + ly^2$  em que

$$n = a_1a^2 + a_2ac + a_3c^2; \quad m = 2a_1ab + a_2(ad + bc) + 2a_3cd; \quad l = a_1b^2 + a_2bd + a_3d^2. \quad (9)$$

Conforme o Teorema 15, em particular, se  $f$  é uma  $\Delta$ -forma positiva inteira e  $a, c$



é uma representação própria de um inteiro positivo  $n$  por  $f$ , então a forma  $g$  acima é uma  $\Delta$ -forma positiva inteira equivalente a  $f$  e cuja matriz associada traz  $n$  na posição  $1 \times 1$  conforme as equações em (9). Prosseguindo mais um pouco nesta análise, se  $a, c$  é uma representação própria de  $n$  por  $f$ , temos  $(a, c) = 1$ ; e pela proposição 7, no capítulo 2, existem  $b', d' \in \mathbb{Z}$  (não únicos) tais que, quaisquer  $b, d \in \mathbb{Z}$  que satisfaçam  $ad - bc = 1$  são da forma  $b = b' + at$  e  $d = d' + ct$  ( $t \in \mathbb{Z}$ ). Substituindo em (9), encontramos

$$\begin{aligned} m &= 2a_1a(b' + at) + a_2(ad' + act + b'c + act) + 2a_3c(d' + ct) \\ &= 2a_1ab' + a_2(ad' + b'c) + 2a_3cd' + 2nt. \end{aligned}$$

Por isso  $m$  é determinado por uma congruência quadrática módulo  $4n$ .

Existe exatamente um valor de  $t \in \mathbb{Z}$  tal que  $0 \leq m < 2n$ . Assim, ao se fazer a representação própria de  $n$  por  $f$ , estamos associando um número  $m \in \mathbb{Z}$  em que  $0 \leq m < 2n$  e  $m^2 \equiv -\Delta \pmod{4n}$  (lembre que  $g$  também é uma  $\Delta$ -forma e  $\Delta = 4nb_3 - m^2$ ). Não parece claro que este  $m$  associado a  $a$  e  $c$  seja único, uma vez que  $b'$  e  $d'$  não são únicos. Considere então  $b' e' d'' \in \mathbb{Z}$ , tais que quaisquer  $b ec \in \mathbb{Z}$  que satisfaçam  $ad - bc = 1$  sejam do forma  $b = b'' + ar, d = d'' + cr$  com  $r \in \mathbb{Z}$ . Substituindo essa nova informação em (9), obtemos

$m = 2a_1ab'' + a_2(ad'' + b''c) + 2a_3cd'' + 2nr$ . Como  $ad'' - b''c = 1$ , existe  $t_1 \in \mathbb{Z}$  tal que

$$d'' = d' + t_1c, \quad e \quad b'' = b' + t_1a$$

e daí,

$$m = 2a_1ab' + a_2(ad' + b'c) + 2a_3cd' + 2n(r + t_1)$$

de modo que para termos  $0 \leq m < 2n$ , a única possibilidade é tomarmos  $r + t_1 = t$ , como antes. Assim o número  $m$ , satisfazendo  $m^2 \equiv -\Delta \pmod{4n}$  e  $0 \leq m < 2n$  que associamos à representação própria  $(a, c)$ , independe dos  $b'$  e  $d'$  considerados.

Portanto, através da fórmula (9), à cada representação própria de  $n$  por  $f$ , há um único inteiro  $m$  tal que  $0 \leq m < 2n$  e  $m^2 \equiv -\Delta \pmod{4n}$ , e conseqüentemente, há uma única  $\Delta$ -forma  $g(x, y) = nx^2 + mxy + ly^2$  equivalente a  $f$ . Em resumo, justificamos o seguinte resultado:

**Teorema 18.** *Suponha que  $(a, c)$  seja uma representação própria de um inteiro positivo  $n$  pela  $\Delta$ -forma positiva inteira  $f(x, y) = a_1x^2 + b_1xy + c_1y^2$ . Então existem únicos inteiros  $b$  e  $d$ , tais que  $ad - bc = 1$  e a transformação  $\mathbf{F} \rightarrow {}^tUFU = G$  leva  $f$  para*

$$g(x, y) = nx^2 + mxy + ly^2,$$

em que  $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  e  $m$  é determinado de maneira única, tal que  $0 \leq m < 2n$ ,

$$m^2 \equiv -\Delta \pmod{4n} \tag{10}$$

e ainda,

$$l = \frac{m^2 + \Delta}{4n}. \tag{11}$$

Assim, a cada representação própria de  $n$  por  $f$ , associamos uma única raiz  $m$  de (10) tal que  $0 \leq m < 2n$ , e que uma única  $\Delta$ -forma  $g$  equivalente com  $f$  tem o primeiro coeficiente  $n$  e o segundo coeficiente  $m$ . Queremos investigar sobre uma recíproca apropriada para este Teorema, que nos forneça uma maneira de contar as representações próprias de  $n$ . O Teorema a seguir nos dá um método eficaz de contar o número de tais representações de um inteiro positivo  $n$  por uma  $\Delta$ -forma  $f$ . Antes de enunciá-lo, vamos observar que se  $m$  é raiz de (10) e  $0 \leq m < 2n$ , então  $4n - m$  também é raiz de (10) e  $2n < 4n - m \leq 4n$  de modo que nos referimos a  $m$  como raiz principal da congruência

$$m^2 \equiv -\Delta \pmod{4n} \text{ se, e somente se, } 0 \leq m < 2n.$$

Já reunimos todas as condições para apreciar o teorema final e suas conseqüências.

### 4.3 Teoremas principais

O que chamamos de método de Minkowski é um resultado que diz quantas representações próprias de um inteiro como soma de quadrados podemos encontrar a partir de uma congruência que envolve  $\Delta$ -formas positivas inteiras. O teorema a seguir é mais geral e o método de Minkowski sairá como consequência imediata dele.

**Teorema 19.** *Seja  $u(f)$  o número de unidades da  $\Delta$ -forma positiva inteira e  $n \in \mathbb{Z}^+$ .*

*Para cada raiz principal  $m$  da equação*

$$m^2 \equiv -\Delta \pmod{4n},$$

*determinamos  $l$  pela equação*

$$l = \frac{m^2 + \Delta}{4n}.$$

*Então, o número de representações próprias de  $n$  por  $f$  será o produto entre  $u(f)$  com números das formas  $g(x, y) = nx^2 + mxy + ly^2$  equivalentes a  $f$ .*

*Demonstração.* Iremos desenvolver a forma  $g$  como apresentada no enunciado e por meio das raízes principais de (10) verificar:

- i.** Se  $g$  e  $f$  não forem equivalentes, então não haverá representação própria de  $n$  por  $f$  associada à raiz principal  $m$ ;
- ii.** Se  $g$  é equivalente com  $f$ , então existem  $u(f)$  representações próprias de  $n$  por  $f$  associadas à raiz principal  $m$ .

Uma representação própria de  $n$  por  $f$ , quando existe, associa-se a uma única raiz principal  $m$  da equação 10. Assim, as formas  $g$  e  $f$  seriam necessariamente equivalentes. É importante destacar que não analisamos se as diferentes representações próprias de  $n$  por  $f$  podem ser associadas à mesma raiz principal  $m$ , o que veremos ser possível (pois, construímos uma função que, a cada representação própria de  $n$  por  $f$ , associa

uma raiz principal de  $m$  em (10); mas esta função, quando pode ser definida, não é injetora e em geral também não é sobrejetora).

Em relação a **ii**, se  $g$  é equivalente com  $f$ , existe

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \text{ tal que } G = {}^tTFT.$$

De fato, observe que contar as representações próprias de  $n$  por  $f$ , corresponde a contar as matrizes  $T \in SL_2(\mathbb{Z})$  tais que  $G = {}^tTFT$ , pois dada  $(a, c)$  uma representação própria de  $n$  por  $f$ , o teorema 18 nos garante que existem únicos  $b, d \in \mathbb{Z}$ ; tais que, se

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ então } G = {}^tTFT$$

( $G$  associada à raiz principal  $m$ , que está fixada, uma vez que fixamos  $g$ ), e reciprocamente, é óbvio que se

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ satisfaz } G = {}^tTFT,$$

então  $(a, c)$  é uma representação própria de  $n$  por  $f$ . Seja então  $T_0 \in SL_2(\mathbb{Z})$  tal que  $G = {}^tT_0FT_0$ , vamos mostrar que  $T \in SL_2(\mathbb{Z})$  é tal que  ${}^tTFT = G$  se, e somente se,  $T = UT_0$  para alguma matriz de  $U \in \mathbf{U}(f)$ ; ou seja,  $T = UT_0$  para alguma matriz  $U$  (unidade da Forma  $f$ ).

Inicialmente, se  $U \in \mathbf{U}(f)$ , temos

$${}^t(UT_0)F(UT_0) = {}^tT_0{}^tUFUT_0 = {}^tT_0FT_0 = G.$$

Logo  $UT_0 = T$  satisfaz  ${}^tTFT = G$ . Reciprocamente, seja  $T \in SL_2(\mathbb{Z})$  satisfazendo  ${}^tTFT = G$ . Então

$${}^tTFT = {}^tT_0FT_0,$$

e daí

$${}^t(TT_0^{-1})F(TT_0^{-1}) = F,$$

ou seja,  $TT_0^{-1} = U \in \mathbf{U}(f)$ .

Assim, se  $g(x, y) = nx^2 + mxy + ly^2$  é equivalente com  $f$ , existem  $u(f)$  matrizes  $T \in SL_2(\mathbb{Z})$  tais que  ${}^tTFT = G$ ; e, portanto, existem  $u(f)$  representações próprias de  $n$  por  $f$  associadas à raiz principal  $m$ . Isso prova o item **ii**.

Para concluir a demonstração, basta ver que, se existe apenas uma  $\Delta$ -forma positiva inteira reduzida (para um dado *discriminante*  $\Delta$ ), as Formas  $f$  e  $g$  são necessariamente equivalentes, de modo que toda raiz principal de (10) está associada a alguma representação. Portanto, há  $u(f)$  representações próprias de  $n$  por  $f$ .  $\square$

Quando *discriminante*  $\Delta$  aceitar apenas uma  $\Delta$ -forma positiva inteira reduzida temos um caso particular em que o número de representações próprias de  $n$  por  $f$  é  $u(f)$  vezes o número de raízes principais de (10). Finalmente anunciaremos e comprovaremos o principal resultado desse trabalho e, como já havíamos dito antes, não foi o caminho mais curto até o mesmo, mas um dos mais belos em um sentido que está bem fundamentado numa teoria sólida, que nos permite garantir a sua veracidade.

**Corolário 8. (O Método de Minkowski)** *O número de representações próprias de um inteiro positivo  $n$  como soma de dois quadrados é quatro vezes o número de soluções da congruência*

$$u^2 \equiv -1 \pmod{n}.$$

*Demonstração.* Para  $f(x, y) = x^2 + y^2$ , temos  $\Delta = 4$ , e já sabemos que só existe uma 4-forma positiva inteira reduzida e que  $u(f) = 4$ . Logo, pelo Teorema 19, o número de representações próprias de  $n$  por  $f$  será quatro vezes o número de raízes principais da congruência

$$m^2 \equiv -4 \pmod{4n}.$$

Para satisfazer tal equação,  $m$  precisa ser par; ou seja,  $m = 2m_1$  com  $0 \leq m_1 < n$ , portanto

$$4m_1^2 \equiv -4 \pmod{4n}$$

ou,

$$m_1^2 \equiv -1 \pmod{n} \text{ e } 0 \leq m_1 < n,$$

exatamente como afirma o corolário. □

**observação 1.** *É interessante observar que o Método de Minkowski nos diz que o número de representações próprias de um inteiro positivo como soma de quadrado corresponde sempre a um múltiplo de quatro. Por exemplo, 2 tem quatro representações, 5 tem oito representações e 65 terá dezesseis, ou seja, quando  $n \in \mathbb{Z}_+$  pode escrito como  $a^2 + b^2$ , tais que  $(a, b) = 1$ , então haverá  $4 \cdot m$  pares distintos  $a$  e  $b$  satisfazendo a essa condição com  $m \in \mathbb{Z}$ .*

*E plotando esses pontos de coordenadas  $(a, b)$  sobre  $\mathbb{R}^2$ , obtemos polígonos com  $4 \cdot m$  lados, um efeito visual interessante, conforme a figura 4.3 que apresenta sobre o  $\mathbb{R}^2$  os pontos das representações próprias dos seguintes inteiros:*

$$\{2, 5, 10, 13, 17, 25, 26, 29, 34, 37, 41, 50, 53, 58, 61, 65 \text{ e } 85\}.$$

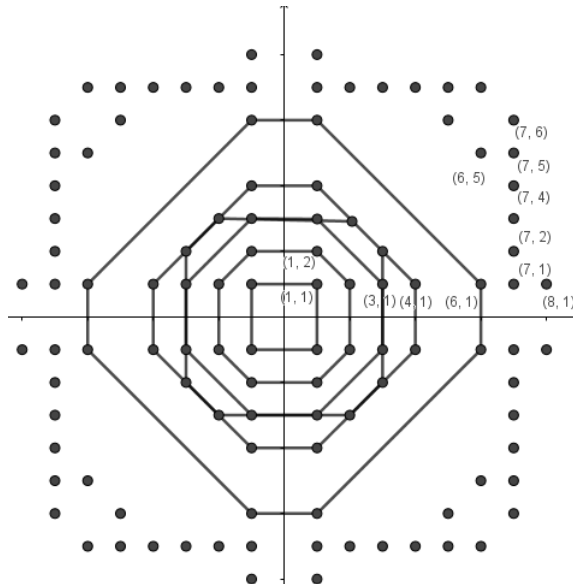


Figura 4.3: Representações próprias no  $\mathbb{R}^2$ .

Assim encerramos este capítulo. Para os leitores que tenham interesse em aprofundar as ideias aqui introduzidas, indicamos a leitura de [11] para maiores informações sobre o assunto. Na seção a seguir, apresentaremos alguns exemplos que possam abordar o nosso tema, mesmo que não diretamente usando o método de Minkowski, tratamos de somas de quadrados e questões a isso relacionadas.

#### 4.4 Questões Olímpicas e Mais Exemplos

Contextualizações das questões de Matemática é uma prática comum, que visa o despertar de interesse dos discentes na resolução de problemas. Há uma diversidade de exercícios de Matemática, porém destacamos aqueles, que advêm dos bancos de competições olímpicas, porque prendem a atenção dos alunos estimulando e intrigando a mente deles, além do mais, esses desafios despertam prazer ao serem resolvidos, diferenciando das atividades trabalhadas nos livros didáticos, por isso é importante ter acesso a questões e problemas bem estruturados.

Como fonte de material didático de qualidade, o banco de questões da OBMEP (Olimpíadas Brasileira de Matemática das Escolas Públicas, disponibilizado em seu site “ [www.obmep.org.br](http://www.obmep.org.br) ”) tem desafios e problemas que estimulam a criatividade dos alunos. Selecionamos alguns destes, principalmente os de aritmética, para comentar sobre a resolução dos mesmos, também trabalhamos exemplos de aplicação do Método de Minkowski para uma melhor assimilação do assunto.

**Exemplo 9.** *(Banco de Questões OBMEP) O personagem histórico mexicano Benedito Juárez nasceu na primeira metade do século XIX (o século XIX vai do ano 1801 ao ano 1900) Sabendo que Benedito Juárez completa  $x$  anos no ano  $x^2$ , qual foi o ano do seu nascimento ?*

*Demonstração.* Inicialmente podemos decompor 1900 em seus fatores primos e obtemos

$2^2 \cdot 5^2 \cdot 19 = 50 \cdot 38$ , assim podemos estimar os quadrados perfeitos mais próximos de 1801 e 1900:

$$44 \cdot 44 = 1936$$

$$43 \cdot 43 = 1849$$

$$42 \cdot 42 = 1764$$

Sendo  $x$  a idade de Benedito Juárez no ano  $x^2$ . Então  $x$  não pode ser 42, pois caso contrário Benedito não teria nascido no século XIX. Testando o ano 1849, sendo a idade de Benedito 43, o mesmo teria nascido em  $1806 = 1849 - 43$  uma vez que 1806 pertence ao século XIX este será o ano de nascimento de Benedito Juárez. Observamos que de 44 em diante a subtração do número pelo seu quadrado será maior que 1901. Sendo 43 de fato única resposta possível.  $\square$

**Exemplo 10.** (Banco de Questões da OBMEP) A figura abaixo representa o traçado de uma corrida

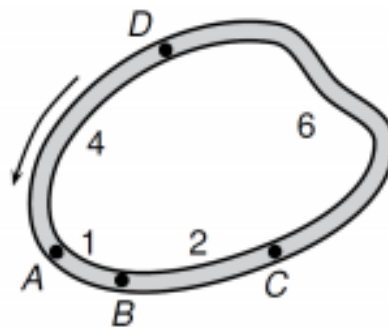


Figura 4.4: Pista de corrida

Os pontos  $A$ ,  $B$ ,  $C$  e  $D$  são usadas para partidas e chegadas de todas as corridas. As distâncias entre pontos vizinhos em quilômetros estão indicadas na figura e as corridas são realizadas no sentido indicado pela flecha. Por exemplo, uma corrida de  $17\text{Km}$



*pode ser realizada com partida em D e chegada em A.*

- a) *Quais pontos de partidas e chegada de uma corrida de 14 km?*
- b) *E para uma corrida de 100 km quais são esses pontos?*
- c) *Mostre que é possível realizar uma corrida com extensão igual a qualquer número inteiro em quilômetro.*

*Demonstração.* a) A volta completa da pista tem uma extensão de 13km logo podemos trabalhar congruência módulo 13, uma vez que,  $14 \equiv 1 \pmod{13}$  então nossa corrida teria seu início em A finalizando em B.

b) Semelhante ao item anterior, observamos inicialmente que  $100 \equiv 9 \pmod{13}$ .

Respeitando o sentido da corrida para somar 9Km, o início seria em A e final em D. E pelo fato do quociente de 100 por 13 ser 7 deduzimos que a corrida teria sete voltas completas iniciando em A, para em seguida terminar em D.

c) Como observados nos itens anteriores, a ideia da solução do problema baseia-se em dar uma certa quantidade de voltas. Uma vez que a pista tem uma extensão de 13Km verificaremos todas as corridas cuja a extensão corresponde a um possível resto na divisão euclidiana por 13. Ou seja, um sistema completo de resíduos módulo 13.

Dispomos os resultados na tabela 4.1, **Primeiro caso:** A extensão é múltipla de 13 neste caso basta escolher qualquer ponto começar e terminar a corrida nesse ponto e número de voltas completas corresponde ao quociente entre a extensão da corrida por 13;

**Segundo caso:** A extensão não é múltiplo de 13, neste caso, calculamos quociente e resto da divisão da extensão por 13. O resto será um dos elementos do conjunto  $\{1, 2, 3, \dots, 11, 12\}$  e a tabela acima nos fornecerá os pontos de partidas e chegadas da corrida. Enquanto o número de voltas será igual ao quociente da divisão.

Extensão em Km	Ponto de Partida	Ponto de Chegada
1	A	B
2	B	C
3	A	C
4	D	A
5	D	B
6	C	D
7	D	C
8	B	D
9	A	D
10	C	A
11	C	B
12	B	A
13	qualquer um	o mesmo da partida

Tabela 4.1: Tabelas de Possibilidades

**Exemplo 11.** *Uma questão bem famosa sobre separação de um número como a soma de dois outros é a Conjectura de Goldbach. Há uma versão moderna dessa especulação que leva o nome do matemático prussiano Cristian Goldbach que propôs por meio de cartas para Leonhard Euler, em 1742, diz que:*

*“ Todo número inteiro par maior que 2 pode ser escrito como soma de primos”*

Para números pequenos a afirmação é simples de verificar:

$$4 = 2 + 2$$

$$6 = 3 + 3$$

$$8 = 3 + 5$$

$$10 = 3 + 7$$

$$12 = 5 + 7 \dots$$

Esse teste direto ou jocoso, como é conhecido, foi aprimorado para computadores que já testaram números na ordem de  $10^{18}$ , porém isso não soluciona o problema.

A Conjectura de Goldbach é um sublime caso em que o enunciado e compreensão do problema são imediatos, porém, a demonstração é assombrosamente difícil, é por isso que ainda hoje não foi demonstrada, no entanto houve significativo desenvolvimento na Matemática, especificamente na Teoria dos Números nas investidas para solucionar o problema.  $\square$

**Exemplo 12.** *Verifiquemos quais dos números a seguir podem ser escritos como soma de quadrados: 234, 572 e 1521.*

*Demonstração.* Inicialmente vamos decompor em seus fatores primos nossos valores e obtemos

$$234 = 2 \cdot 3^2 \cdot 13, \quad 572 = 2^2 \cdot 11 \cdot 13 \quad \text{e} \quad 1521 = 3^2 \cdot 13^2.$$

Como exposto no corolário 6, poderemos decompor 234 e 1521 como uma soma de quadrados, porém como 572 apresentou um fator primo do tipo  $4k + 3$  elevado a uma potência ímpar, o 11 não poderá assim ser escrito.  $\square$

**Exemplo 13.** *Ainda com relação aos valores 234 e 1521, vamos escrevê-los como  $a^2 + b^2$  com  $a, b \in \mathbb{Z}$ .*

*Demonstração.* Em nossa busca por  $a$  e  $b$  há uma restrição; conforme mostra o resultado do Teorema 8, ao intervalo  $(0, \sqrt{234})$  e também  $(0, \sqrt{1521})$ . Essas restrições facilitam a nossa busca, e assim por tentativas obtemos os seguintes valores

$$234 = 3^2 + 15^2 \quad \text{e} \quad 1521 = 15^2 + 36^2.$$

$\square$

**Exemplo 14.** *Mostre que os números da forma  $2^n$ , com  $n \in \mathbb{N}$ , podem ser escritos como soma de dois quadrados.*

*Demonstração.* Utilizando o método de indução finita sobre  $n$ , o caso base  $n = 1$  é óbvio, pois

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

Supondo que para um certo  $n \in \mathbb{N}$  existam  $a$  e  $b$  inteiros em que

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

como  $2^{n+1} = 2 \cdot 2^n$  por nossa hipótese de indução sobre  $n$ , temos:

$$2^{n+1} = 2 \cdot 2^n = 2 \cdot (a^2 + b^2) = (a + b)^2 + (a - b)^2.$$

Fazendo  $A = a + b$  e  $B = a - b$  temos  $2^{n+1} = A^2 + B^2$ , como queríamos provar.  $\square$

**Exemplo 15.** *Vamos mostrar que  $n \in \mathbb{N}$ , não poderá ser escrito como soma de quadrados quando  $n \equiv 3 \pmod{9}$  ou  $n \equiv 6 \pmod{9}$ .*

*Demonstração.* Como visto na seção 2.5

$$n \equiv 3 \pmod{9} \implies 9|n - 3 \implies n - 3 = 9a \implies n = 9 \cdot a + 3 \text{ com } a \in \mathbb{Z}.$$

Assim temos  $n = 9a + 3 = 3 \cdot (3a + 1)$ , uma vez que há um fator primo 3 em  $n$ , se mostrarmos que não há outro, então o Teorema (9) garante que  $n$  não poderá ser escrito como soma de quadrados. E como  $3 \cdot a + 1 \neq 3k$  qualquer que seja  $a$  e  $k \in \mathbb{Z}$  então o caso  $n \equiv 3 \pmod{9}$  está verificado.

Agora com  $n \equiv 6 \pmod{9}$  temos que

$$n \equiv 6 \pmod{9} \implies 9|n - 6 \implies n - 6 = 9 \cdot a \implies n = 9 \cdot a + 6 \text{ com } a \in \mathbb{Z},$$

desta forma,  $n = 9 \cdot a + 6 = 3 \cdot (a \cdot 3 + 2)$  e uma vez que  $3 \cdot a + 2 \neq 3k$ , qualquer que seja,  $a$  e  $k \in \mathbb{Z}$ , concluímos por argumentos semelhantes ao caso anterior que  $n$  não poderá ser escrito como soma de quadrados.  $\square$

**Exemplo 16.** *De posse do Método de Minkowski, contaremos o número de representações próprias de 10 e 65.*

*Demonstração.* Como  $10 = 5 \cdot 2$  e  $65 = 5 \cdot 13$  e pelo Corolário 6 estes podem ser escrito como soma de quadrados.

Segue também que  $u^2 \equiv -1 \pmod{10}$  apresenta duas soluções  $\{3, 7\}$  logo serão 8 as representações próprias do 10 conforme Corolário 8.

Pelos mesmos argumentos temos 16 representações próprias do 65, pois

$$u^2 \equiv -1 \pmod{65},$$

apresenta quatro soluções  $\{8, 18, 47, 57\}$ . De fato

$$\begin{aligned} 10 &= (1)^2 + (3)^2 = (1)^2 + (-3)^2 = (-1)^2 + (3)^2 = (-1)^2 + (-3)^2 \\ &= (3)^2 + (1)^2 = (3)^2 + (-1)^2 = (-3)^2 + (1)^2 = (-3)^2 + (-1)^2 \end{aligned}$$

da mesma forma

$$\begin{aligned} 65 &= (1)^2 + (8)^2 = (1)^2 + (-8)^2 = (-1)^2 + (8)^2 = (-1)^2 + (-8)^2 \\ &= (8)^2 + (1)^2 = (8)^2 + (-1)^2 = (-8)^2 + (1)^2 = (-8)^2 + (-1)^2 \end{aligned}$$

e ainda temos

$$\begin{aligned} 65 &= (4)^2 + (7)^2 = (4)^2 + (-7)^2 = (-4)^2 + (7)^2 = (-4)^2 + (-7)^2 \\ &= (7)^2 + (4)^2 = (7)^2 + (-4)^2 = (-7)^2 + (4)^2 = (-7)^2 + (-4)^2 \end{aligned}$$

□

É pelo envolvimento e entrega dos participantes e professores que as competições de Matemáticas, nos proporcionam questões tão bem elaboradas em todos os níveis. Isso reforça a importância da continuidade de projetos como da OBMEP, assim como, uma ampliação do uso do material disponibilizado pelo programa em sala de aula, instigando a criatividade dos alunos, despertando afeição e diminuindo a repulsa pela disciplina Matemática.

## Referências

- [1] **Boldrini, José Luiz et al** . Álgebra Linear, São Paulo: Harbra, 1984.
- [2] **Hefez, Abramo**. Elementos da Aritmética, Rio de Janeiro: SBM , Rio de Janeiro 2011.
- [3] **Hoffman, Kenneth. Kunze, Ray**. Álgebra Linear. Formas Bilineares Simétricas: Livros Técnicos e Científicos, Rio de Janeiro,1979.
- [4] **Manfield, Daniel F. Wilderger, N. J.** . Plimpton 322 is Babylonian exact sexagesimal trigonometry: Elsevier Inc , número 44, p. 395-419, August, Sydney, 2017.
- [5] **Morgado, José. Franco de**. Algumas equações diofantinas. Boletim da SBM, número 15, p24-35, Jan/Fev, 1990. Disponível em: <<http://natilus.s.uc.pt/psbm/revista/15/024-035.300.pdf>>. Acesso em 12 de Dez 2019.
- [6] **Natário. José**. Espaço Tempo de Minkowski: A Física como Geometria. Gazeta Matemática, número 162, p 34-36, Nov. 2010. Disponível em:< <http://gazeta.spm.pt/getArtigo?gid=305> >. Acesso em 20 de Fev 2020.
- [7] **OBMEP**. Banco de Questões. Disponível em: < <http://www.obmep.org.br/banco.htm>> Acesso em: 20 de Mar 2020.
- [8] **O'Connor, J. J. Robertson, E. F.**, Hermann Minkowski. Disponível em:<https://mathshistory.st-andrews.ac.uk/Biographies/Minkowski/>. Acesso em 29 de Fev 2019.

- [9] **Oliveira, A. J. Franco de.** Breve introdução histórica e alguns problemas e conjecturas. Boletim da SBM, número 6, p 49-64, outubro, 1993. Disponível em:<<http://nailus.s.uc.pt/psbm/revista/6/049-064.300.pdf>>. Acesso em 10. Dez 2020.
- [10] **Santos, João E. C. dos** .Números Inteiros Como Soma de Quadrados, 2013. 60f. (Mestrado em Educação Matemática) - Universidade Federal da Paraíba, João Pessoa, 2013.
- [11] **Shokranian, Salahoddin. et al.** Teoria dos Números : UnB, Brasília 1999.