UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Equações diofantinas

Yuri Faleiros da Silva

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP
SÃO CARLOS

Yuri Faleiros da Silva

Equações diofantinas

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *VERSÃO REVISADA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientador: Prof. Dr. Rafael Andres Rosales Mitrowsky

USP – São Carlos
Junho de 2019

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

F187e

Faleiros, Yuri
Equações Diofantinas / Yuri Faleiros; orientador Rafael Andrés Rosales Mitrowsky. -- São Carlos, 2019.
72 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2019.

1. aritmética. 2. equações diofantinas. 3. inteiros de Gauss e de Eisenstein. 4. Ultimo Teorema de Fermat. 5. Teorema Fundamental da Aritmética. I. Rosales Mitrowsky, Rafael Andrés, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Yuri Faleiros da Silva

Diophantine equations

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of Mathematics Professional Master's Program. *FINAL VERSION*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Prof. Dr. Rafael Andres Rosales Mitrowsky

USP – São Carlos
June 2019

AGRADECIMENTOS

Como acredito em Deus, um ser ou força superior a tudo e todos, que está sempre presente, agradeço a Ele por cada milésimo de segundo em minha vida.

Agradeço aos meus pais Nilsa e Cláudio os quais me fizeram ser quem sou. Foram eles que me deram uma ótima educação o que moldou meu caráter do qual me orgulho.

À minha maravilhosa esposa Ana Laura que me ajuda e me incentiva a ir além, desde bem antes de dar início a este mestrado.

Agradeço também ao meu orientador e professor Dr. Rafael A. Rosales Mitrowsky pela dedicação e confiança.

De modo geral, agradeço aos meus colegas de turma e professores, com quem aprendi muito, pela convivência e aprendizado.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

“Independente do que você escolha ser em sua vida,
tente ao máximo ser sempre o melhor possível.”

RESUMO

FALEIROS, Y. **Equações diofantinas**. 2019. 72 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

Este trabalho descreve as soluções de algumas equações diofantinas em duas e três variáveis. O objetivo é apresentar a análise de alguns casos simples e de outros mais difíceis relativos ao Último Teorema de Fermat. Primeiramente são apresentadados os pré-requisitos necessários dentre os quais incluímos a noção de número primo, máximo divisor comum, congruência, o Algoritmo de Euclides e o Teorema Fundamental da Aritmética. Este material é desenvolvido primeiramente no anel dos inteiros racionais e posteriormente em duas extensões algébricas conhecidas como os inteiros de Gauss e de Eisenstein. A estrutura dos últimos é indispensável na resolução do primeiro caso não trivial do Último Teorema de Fermat, a saber, da equação diofantina $x^3 + y^3 = z^3$. O último capítulo apresenta algumas aplicações de problemas diofantinos e do Algoritmo de Euclides que podem ser desenvolvidos em sala de aula com alunos do sexto e do oitavo ano.

Palavras-chave: aritmética, equações diofantinas, inteiros de Gauss e de Esenstein, Último Teorema de Fermat, Teorema Fundamental da Aritmética.

ABSTRACT

FALEIROS, Y. **Diophantine equations**. 2019. 72 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2019.

This work describes the solutions to some diophantine equations in two and three variables. The objective is to present the analysis of some simple and other more difficult cases related to Fermat's Last Theorem. First, we present the necessary prerequisites which include the notion of a prime number, the maximum common divisor, congruences, Euclid's Algorithm and the Fundamental Theorem of Arithmetic. This material is first developed by using the rational integers and then presented for two algebraic extensions known as Gauss and Eisenstein integers. The structure of the latter is indispensable for the first non-trivial case of Fermat's Last Theorem, namely, the diophantine equation $x^3 + y^3 = z^3$. The last chapter presents some applications of simple diophantine equations and Euclid's algorithm which can be developed in the classroom with sixth and eight grade students.

Keywords: aritmetic, diophantine equations, Gaussian and Eisenstein integers, Fermat's Last Theorem, Fundamental Theorem of Aritmetic.

LISTA DE ILUSTRAÇÕES

LISTA DE SÍMBOLOS

$\mathbb{Q}$ — racionais

$\mathbb{Z}$ — inteiros racionais

$a \mid b$ — a divide b

$a \nmid b$ — a não divide b

$\text{mdc}(a,b,\ldots,z) = (a,b,\ldots,z)$ — máximo divisor comum de a, b, …, z

$a \equiv b \pmod{c}$ — a é congruente a b módulo c

$\mathbb{Z}[i]$ — inteiros de Gauss

$\mathbb{R}$ — números reais

$\mathbb{Z}[\rho]$ — inteiros de Eisenstein

SUMÁRIO

CAPÍTULO 1

INTRODUÇÃO

Diofanto de Alexandria foi um matemático com grande influência para o desenvolvimento da álgebra e com uma enorme importância para os europeus que futuramente se dedicaram à teoria dos números. Apesar de sua relevância na história da Matemática nessa área, não se sabe ao certo acerca de sua nacionalidade e a época precisa em que viveu, afirmam-se apenas que sua carreira aconteceu em Alexandria, no Egito. Presume-se que Diofanto nasceu em cerca de 200 d.C. e morreu em cerca de 284 d.C. Quase tudo que sabemos sobre o Diofanto encontra-se em forma de epigrama[1]. O seguinte epigrama diz a respeito da sua idade.

> "Diofanto passou $\frac{1}{6}$ de sua vida como criança, $\frac{1}{12}$ como adolescente e mais $\frac{1}{7}$ na condição de solteiro. Cinco anos depois de se casar nasceu-lhe um filho que morreu 4 anos antes de seu pai, com metade da idade (final) de seu pai" (BASHMAKOVA, 1997)

Se chamamos de x a quantidade em anos que o Diofanto viveu temos $\frac{x}{6}+\frac{x}{12}+\frac{x}{7}+5+\frac{x}{2}+4=x$ e assim $14x+7x+12x+420+42x+336=84x$, o qual leva a solução $x=84$. Se o epigrama for realmente verdadeiro, concluímos que Diofanto viveu exatamente 84 anos.

Diofanto escreveu três trabalhos: *Aritmética*[2], o mais importante deles, do qual ficaram seis dos treze livros; *Sobre Números Poligonais* do qual sobrou apenas um fragmento; e *Porismas*, que se perdeu. *Aritmética* teve muitos tradutores, mas a primeira tradução do original grego foi a de Johannes Müller von Königsberg, conhecido como Regiomontanus, em 1463. Uma versão traduzida ao inglês dos 6 livros de *Aritmética* pode ser encontrada em Heat (1910)[3]. *Aritmética* é uma abordagem crítica da teoria algébrica dos números, a qual enaltece o autor a nível de gênio em sua área, apesar de outros matemáticos também já terem realizado importantes descobertas na área. Em *Aritmética*, ele resolve 189 problemas variáveis, que são levados a equações do primeiro e segundo graus. Esse escrito representa uma grande conquista para a Matemática, visto que era um método diferente de tudo que se conhecia na época.

O primeiro livro considera equações indeterminadas em uma incógnita e os restantes, equações indeterminadas de segundo grau ou de grau maior, em duas ou três incógnitas. De acordo com Eves (2004), Diofanto realizou avanços extraordinários, exibindo em seus livros vários exemplos das melhores qualidades de um grande matemático. Não é de se espantar que

---

1 do grego ἐπίγραφὼ, é uma composição poética breve que expressa um único pensamento principal de forma engenhosa.

2 O termo 'aritmética' provém do grego ἀριθμός, que se refere aos números.

3 disponível online em <https://archive.org/details/diophantusofalex00heatiala/page/1>

sua obra *Aritmética* é vista como o primeiro manual de álgebra que usa símbolos para indicar incógnitas e potências e apresenta a resolução exata de equações indeterminadas. Eves (2004) afirma, em seus escritos, que é notável a não utilização de métodos gerais e a aplicação repetida de artifícios engenhosos ideados para as necessidades de cada problema específico. Diofanto só aceitava soluções entre os números racionais positivos recusando as negativas e/ou irracionais.

Os problemas considerados por Diofanto estão relacionados com equações algébricas indeterminadas, para as quais somente são consideradas soluções nos números racionais não negativos. Estas situações, quando consideradas sobre racionais, ficaram conhecidas hoje em dia como 'Problemas Diofantinos'. De maneira geral, um problema diofantino pode ser formulado da seguinte forma: Sejam dados m polinômios em n variáveis, $m < n$, $P_1(x_1, x_2, \ldots, x_n)$, $\ldots$, $P_m(x_1, x_2, \ldots, x_n)$, com coeficientes no corpo K. A questão fundamental consiste em determinar o conjunto das soluções racionais, $\mathfrak{S}(K)$, ao sistema

$$\begin{aligned} P_1(x_1, x_2, \ldots, x_n) &= 0, \\ &\vdots \\ P_m(x_1, x_2, \ldots, x_n) &= 0. \end{aligned}$$

Claramente o conjunto $\mathfrak{S}(K)$ depende do corpo K. A equação $x^2 + y^2 = 3$ fornece um bom exemplo disso, pois ela não apresenta soluções no corpo dos números racionais $\mathbb{Q}$, porém possui infinidade de soluções no corpo $\mathbb{Q}(\sqrt{3})$, isto é, no conjunto dos números da forma $a + b\sqrt{3}$ com $a, b \in \mathbb{Q}$. Em *Aritmética*, Diofanto considerou os problemas reduzidos a uma única equação em duas incognitas $m = 1, n = 2$, isto é ao caso

$$P(x, y) = 0.$$

Para exemplificar, consideramos o problema

$$x^2 + y^2 = 1, \tag{1.1}$$

o qual corresponde ao problema 8 do livro II em *Aritmética*. O método utilizado por Diofanto, na procura de soluções racionais em x e y da equação (1.1), constitui a essência do argumento utilizado na resolução do problema $x^2 + y^2 = z^2$, estudado adiante no Capítulo 4 desta dissertação. Segundo Bashmakova (1997), este exemplo permite expor na sua versão mais pura o "método de Diofanto". A igualdade (1.1) descreve a equação de um círculo com centro na origem e raio 1. Claramente o ponto $(1, 0)$ é uma solução racional de (1.1). Diofanto considera a substituição

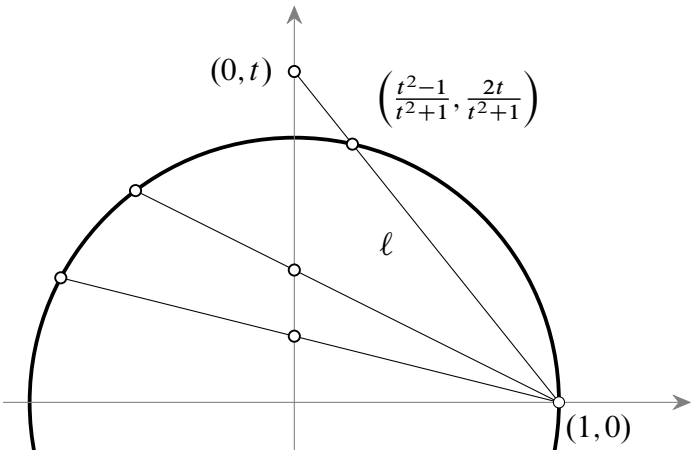
$$x = x, \qquad y = -t(x - 1) \tag{1.2}$$

correspondente a reta $\ell : y = -tx + 1$, que passa pelo ponto $(1, 0)$ e intercepta o círculo (1.1) em um segundo ponto com coordenadas

$$(x, y) = \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right). \tag{1.3}$$

Fazendo $x = 0$ em (1.2) mostra que ℓ também intercepta o eixo-y no ponto $(0,t)$. A aplicação $(0,t) \mapsto \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$ estabelece uma bijeção entre os pontos racionais do eixo-y e os pontos racionais da circunferência da forma (1.3). Com efeito, se $t \in \mathbb{Q}$, então o ponto (x,y) em (1.3) é uma solução racional de (1.1). Reciprocamente, para o ponto (x,y) da forma (1.3), existe uma reta ℓ que une esse ponto a (1,0) e é dada por uma equação com coeficientes racionais, portanto intercepta o eixo-y no ponto $(0,t)$ com $t \in \mathbb{Q}$. Uma representação desta construção é mostrada na Figura 1. Esta figura apresenta três retas definidas por $t = \frac{5}{4}$, $t = \frac{1}{2}$ e $t = \frac{1}{4}$ para as quais são obtidos respectivamente os pontos racionais $(\frac{9}{41}, \frac{40}{41})$, $(-\frac{3}{5}, \frac{4}{5})$ e $(-\frac{15}{17}, \frac{8}{17})$. Diofanto só teria considerado a solução para $t = \frac{5}{4}$.

Figura 1 – O método de Diofanto para $x^2 + y^2 = 1$.



Fonte – Realizada pelo autor.

Um outro exemplo de um problema bem famoso é o problema Diofantino determinado pela equação

$$x^n + y^n = z^n, \tag{1.4}$$

sendo n um número natural maior do que 2, isto é, $n \in \{3,4,\ldots\}$. O último Teorema de Fermat afirma que este problema não possui soluções inteiras, a não ser soluções triviais nas quais uma das variáveis x, y, z é 0. Este Teorema foi enunciado pelo Fermat em 1637, em uma nota de margem escrita na sua cópia da edição do Bachet de *Aritmética*. Como resultado na procura pela demonstração deste Teorema foram desenvolvidas novas áreas da matemática tais como a teoria algébrica dos números. A demonstração definitiva deste Teorema só foi estabelecida 358 anos depois de ser enunciado por Fermat, em dois artigos por Wiles (1995) e Wiles e Taylor (1995). O argumento do Wiles utiliza uma relação fundamental entre a equação (1.4) e curvas elípticas. Trabalhos prévios por Hellegouarch (1975), Frey (1986) e Ribet (1990) estabeleceram que o último Teorema de Fermat resultaria de uma conjectura sobre curvas elípticas conhecida como a conjectura de Taniyama-Shimura. Willes conseguiu estabelecer um caso particular desta conjectura, suficiente para lidar com o Teorema de Fermat. Uma exposição histórica dos eventos

relativos a demostração do ultimo Teorema de Fermat escrita para o publico não especializado pode ser encontrada em Singh (2006).

O resto desta dissertação está organizado da seguinte maneira. O Capítulo 2 fornece os pré-requisitos necessários para apresentar o Teorema Fundamental da Aritmética. A demostração deste teorema segue de perto o material exposto nos Capítulos II e XII em Hardy e Wright (2008). O Capítulo 3 apresenta a generalização do Teorema Fundamental a duas extensões do corpo dos números inteiros conhecidas como os inteiros de Gauss e os inteiros de Eisenstein. O Capítulo 4 considera vários problemas Diofantinos e, em particular, estuda a equação

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

a qual representa o primeiro caso não trivial do último Teorema de Fermat. O material desenvolvido no Capítulo 4 é esencial neste caso. Os Capítulos 3 e 4 estão baseados respectivamente nos Capítulos XII e XIII de Hardy e Wright (2008). Finalmente, o Capítulo 5 apresenta algumas aplicações do algoritmo de Euclides e de problemas Diofantinos mais simples, que podem ser desenvolvidos em sala de aula com os alunos do sexto e do oitavo ano.

CAPÍTULO 2

OS INTEIROS RACIONAIS

Neste capítulo apresentamos as noções de divisibilidade, primalidade, máximo divisor comum, congruência, o algoritmo da divisão de Euclides e o Teorema Fundamental da Aritmética nos inteiros racionais. O objetivo é introduzir a notação a ser utilizada e fornecer os pré-requisitos necessários para os próximos capítulos. Todos os tópicos apresentados aqui são elementares e podem ser encontrados em diversos livros. Hefez (2013), Hefez (2015), ou Santos (1998) fornecem excelentes opções. Existem várias maneiras de demonstrar o Teorema Fundamental da Aritmética. Por exemplo, nos Capítulos I e II em Hardy e Wright (2008), é apresentada uma demonstração baseada na noção de módulo. Martinez *et al.* (2010) apresenta, no Teorema 1.16, uma demonstração relativamente mais simples e suscinta. A demonstração aqui utiliza o algoritmo de Euclides de acordo com material descrito no Capítulo 12, Seção 12.5, em Hardy e Wright (2008). O motivo desta escolha é que este último argumento é facilmente estendido a outros conjuntos utilizados no estudo de equações Diofantinas.

Seja A um conjunto e "+" e "." duas operações em A chamadas de adição e multiplicação. A terna $(A,+,.)$ é um anel se as operações $+$ e $.$ satisfazem as seguintes propriedades. Para quaisquer a, b, $c \in A$: (a_1) a adição é associativa: $(a+b)+c = a+(b+c)$; (a_2) a adição é comutativa: $a+b = b+a$; (a_3) existe um elemento neutro para a adição: $\exists e \in A \ : \ e+x = x$, $\forall x \in A$; (a_4) todo elemento de A possui um simétrico: $\forall a \in A$, $\exists a' \in A \ : \ a+a' = 0$; (a_5) a multiplicação é associativa: $(a.b).c = a.(b.c)$; (a_6) a multiplicação é distributiva com relação à adição: $a.(b+c) = a.b+a.c$; $(a+b).c = a.c+b.c$

Chamamos de inteiros racionais, ou apenas inteiros, o conjunto formado pelos números

$$\ldots,-4,-3,-2,-1,0,1,2,3,\ldots$$

e denotamos o anel formado por estes números por $\mathbb{Z}$. Observamos que o número 0 é neutro para a adição e o número 1 é o elemento neutro para a multiplicação. O motivo do termo *inteiros racionais* é explicado a seguir. Dizemos que o número ξ é um número algébrico se é raíz da equação

$$c_0\xi^n + c_1\xi^{n-1} + \cdots + c_n = 0, \qquad c_0 \neq 0$$

onde c_i, $i = 1,\ldots,n$, são inteiros racionais. Em particular, quando $c_0 = 1$, chamamos ξ de inteiro algébrico. Observamos agora que o número ξ definido por $a\xi - b = 0$, é de fato o racional $\xi = b/a$. Se $a = 1$, então, ξ também é um inteiro, logo $\xi = b$ é um inteiro racional. O conjunto dos inteiros algébricos também inclui números complexos, como, por exemplo, os números

$$i = \sqrt{-1}, \tag{2.1}$$

$$\rho = e^{\frac{2}{3}\pi i} = \frac{1}{2}(-1 + i\sqrt{3}). \tag{2.2}$$

É relativamente simples verificar que ambos são inteiros algébricos pois $i^2 + 1 = 0$ e $\rho^2 + \rho + 1 = 0$.

Dizemos que um subconjunto $S \subset \mathbb{Z}$ é limitado inferiormente se existir $a \in \mathbb{Z}$ tal que $a \leq x$ para todo $x \in S$. Diremos que $a \in S$ é o menor elemento de S se $a \leq x$ para todo $x \in S$. Com estes pré-requisitos estamos prontos para enunciar a seguinte propriedade de $\mathbb{Z}$.

Princípio da Boa Ordenação. Se $S \subset \mathbb{Z}$ é não vazio e limitado inferiormente, então S possui um menor elemento.

2.1 Divisibilidade em $\mathbb{Z}$

Denotamos os elementos de $\mathbb{Z}$ por letras do alfabeto latino $a, b, \ldots$. Sejam a e b dois números inteiros com $a \neq 0$. Dizemos que a é um divisor de b se, e somente se, existir algum número inteiro k tal que

$$b = ak.$$

Neste caso dizemos que b é um múltiplo de a ou que b é divisível por a. Utilizamos a notação $a \mid b$ caso a divida b e $a \nmid b$ caso a não divida b. Observamos que para qualquer inteiro racional a, $1 \mid a$ e $-1 \mid a$, e para qualquer $a \neq 0$, $a \mid a$.

Uma unidade (a respeito da multiplicação) em $\mathbb{Z}$ é um número que divide todos os outros elementos de $\mathbb{Z}$. Consideramos formalmente a seguinte definição.

Definição 1 (Unidade)**.** O números ± 1[1] são denominados as unidades de $\mathbb{Z}$. Usaremos o símbolo ϵ para representar unidades em todo o texto.

Definição 2 (Número primo)**.** Dizemos que $p \in \mathbb{Z}$ é primo quando existem exatamente quatro divisores inteiros de p: ± 1 e $\pm p$.

Chamamos de número composto, um número inteiro que não seja primo e não seja uma unidade. Por exemplo, os números 12, 34 e -35 são compostos.

Proposição 1. *Sejam a, b, c inteiros racionais. Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração. Se $a \mid b$, então existe um inteiro k_1 tal que $b = ak_1$. Se $b \mid c$, logo existe um inteiro k_2 tal que $c = bk_2$. Substituindo b temos $a = ck_2k_1$. □

Proposição 2. *Se a, b e c são inteiros com $a \neq 0$ tais que $a \mid b$ e $a \mid c$, então $a \mid (b \pm c)$.*

[1] Utilizamos $\pm a$ para denotar os inteiros a ou $-a$.

Demonstração. Se $a \mid b$, então existe algum inteiro m tal que $b = ma$ e se $a \mid c$, há algum inteiro n tal que $c = na$. Fazendo a adição entre b e c temos

$$b + c = ma + na \Rightarrow b + c = a(m + n)$$

o qual mostra que $(b + c)$ é um múltiplo de a e, por isso, $a \mid (b + c)$. A demonstração de $a \mid (b - c)$ é completamente análoga. □

Proposição 3. *Sejam a, b e c números inteiros com $a \neq 0$, se $a \mid b$ e $a \mid c$, então $a \mid (xb + yc)$ para x e y inteiros.*

Demonstração. Se $a \mid b$, então existe algum inteiro m tal que $b = ma$ e se $a \mid c$, existe algum inteiro n tal que $c = na$. Substituindo em $xb + yc$ temos

$$xb + yc = x(ma) + y(na) = (xm + yn)a.$$

Dessa forma provamos que a é um múltiplo de $(xb + yc)$ e logo $a \mid (xb + yc)$. □

2.2 Máximo Divisor Comum

Dados os números inteiros a e b não nulos, dizemos que c é divisor comum de a e b se, e somente se, $c \mid a$ e $c \mid b$. Diremos que o inteiro $c > 0$ é o maximo divisor comum entre os inteiros a e b se, e somente se,

i) c for um divisor comum de a e b, e

ii) todos os divisores comuns de a e b também dividem c.

Assim, o máximo divisor comum de a e b é denotado por $\text{mdc}(a, b)$ ou simplesmente (a, b).

Esta definição é estendida da seguinte forma. Um inteiro k é o máximo divisor comum entre os inteiros, não todos nulos, a_1, a_2, a_3, ... e a_n se, e somente se,

i) k for um divisor comum de a_1, a_2, a_3, ... e a_n, e

ii) todos os divisores comuns de a_1, a_2, a_3, ... e a_n também dividem k.

Desta forma $k = (a_1, a_2, a_3, ..., a_n)$.

Exemplo 1. Apresentamos neste exemplo como determinar $(30, 45)$. Primeiramente encontraremos todos os divisores de 30 e 45:

Divisores de 30: ± 1, ± 2, ± 3, ± 5, ± 6, ± 10, ± 15 e ± 30;

Divisores de 45: ± 1, ± 3, ± 5, ± 9, ± 15 e ± 45.

Analisando os divisores desses dois números percebemos que o maior destes é o número 15, dessa forma $(30, 45) = 15$.

Percebe-se que ± 1, ± 3, ± 5 e ± 15 são divisores de $(30, 45) = 15$, o que nos mostra a segunda condição para ser um máximo divisor comum.

O máximo divisor comum apresenta as seguintes propriedades básicas.

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

ii) $(1,a) = (-1,a) = 1$.

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

Os seguintes lemas serão utilizados para descrever o algoritmo de Euclides apresentado na seguinte seção.

Lema 1. *Sejam a, b e n inteiros. Se* $(a,b-na)$ *existe, então*

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

Demonstração. Seja $c = (a,b-na)$, logo $a = ck_1$ e $b-na = ck_2$, com k_1 e k_2 inteiros. Assim, substituindo $b-nck_1 = ck_2$ temos, $b = c(k_2+nk_1)$ e, logo, $c \mid b$. Suponhamos agora que $(a,b) = d$, pela Proposição 3 temos $d \mid xa+yb$. Para x e y inteiros, usando $x = -n$ e $y = 1$ mostramos que $d \mid (b-na)$ e, dessa forma, $d \mid c$. Por outro lado, como c divide a e b, temos que $c \mid d$ e logo $d = c$. □

Lema 2 (Relação de Bézout). *Sejam a, b inteiros não nulos tais que* $(a,b) = c$*, então existem* x *e* y *inteiros os quais satisfazem* $ax+by = c$.

Demonstração. Seja S definido por

$$S = \{ax+by \mid x,y \in \mathbb{Z}\},$$

onde a e b são inteiros dados. Todo elemento de S é inteiro e, por hipótese, $(a,b) = c$, ou seja, $c \mid a$ e $c \mid b$ fazendo com que c divida todo elemento de S, uma vez que $c \mid (ax+by)$.

Utilizando apenas os elementos não negativos de S, pelo Princípio da Boa Ordenação, existe um menor elemento positivo em S que chamaremos de $c' = ax'+by'$. Pelo fato de $c \mid a$ e $c \mid b$, observamos que $c \mid c'$, e, assim, $c \leq c'$. Provaremos, a seguir, que $c = c'$

Supondo que $c' \nmid a$, podemos escrever $a = qc'+r$, com $q,r \in Z$ e $0 < r < c'$, isto será demonstrado ainda neste capítulo no Teorema 1. Reescrevendo, temos $r = a-qc' = a-q(ax'+by') = a(1-qx')+b(-qy')$ e, dessa maneira, r também é um elemento de S, o que gera uma contradição, pois c' é o menor elemento positivo de S e r também elemento de S tal que $0 < r < c'$. Logo concluímos que $c' \mid a$ e, de maneira análoga, que $c' \mid b$, fazendo com que c' seja um divisor comum entre a e b. Por definição, todos os divisores comuns de a e b também dividem $c = (a,b)$ e, assim, $c' \mid c \Rightarrow c' \leq c$, provando que $c = c'$. □

Lema 3. *Sejam a, b e n inteiros não nulos, então vale*

$$(na,nb) = |n|(a,b).$$

Observação: O valor absoluto para n é necessário, pois por definição $(a,b) > 0$.

Demosntração do Lema 3. Pelo Lema 2, existem inteiros x e y tais que $(a,b) = (ax+by)$. Multiplicando por n temos $n(a,b) = n(ax+by) = (nax+nby)$. Por outro lado, $(na,nb) = (nax+nby)$, assim, $(na,nb) = |n|(a,b)$. □

Lema 4. *Sejam a e b inteiros tais que $a \mid b$. Então $(a,b) = |a|$.*

Demonstração. Se $a \mid b$ então $b = ak$, para algum inteiro k. Suponha que $(a,b) = c$. Sabemos que $(a,b) = (a,ak) = c$ e pelo Lema 3, $c = (a,ak) = |a|(1,k) = |a|$. □

Lema 5. *Sendo a e b números inteiros, ambos não nulos, tem-se*

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

Demonstração. Pelo Lema 3 temos

$$(a,b)\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = \left((a,b)\frac{a}{(a,b)}, (a,b)\frac{b}{(a,b)}\right) = (a,b).$$

Como $(a,b)1 = (a,b)$, provamos que

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

□

Definição 3. Dois números inteiros a e b são ditos primos entre si ou coprimos, quando os únicos divisores comuns entre eles forem as unidades ± 1, ou seja, $(a,b) = 1$.

Proposição 4. *Sendo a, b e c inteiros não todos nulos, temos que $(a,b,c) = (a,(b,c))$.*

Demonstração. Seja $k = (a,(b,c))$, logo $k \mid a$ e $k \mid (b,c)$, o que implica em que $k \mid b$ e $k \mid c$, por definição, fazendo com que k seja um divisor comum de a, b e c. Por outro lado, sendo d um divisor comum de a, b e c, temos que $d \mid a$ e $d \mid (b,c)$, implicando que $d \mid k$. Assim provamos que k divide a, b e c e que qualquer outro divisor comum de a, b e c divide k, logo

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

□

2.3 Algoritmo de Euclides

Sejam $a \neq 0$ e b dois inteiros tais que $a \nmid b$. Euclides diz no seu livro Os Elementos, sem enunciar, o seguinte fato explicitamente: é sempre possível efetuar a divisão de b por a obtendo um resto inteiro não negativo. Lembrando que Euclides, em seu tempo, só tratava de números naturais.

Teorema 1 (Divisão Euclidiana). *Sejam a e b dois inteiros racionais com $b \neq 0$, existem dois únicos inteiros q e r, sendo $0 \leq r < |b|$, tais que*

$$a = qb + r.$$

No caso em que $r = 0$, tem-se $a = qb$, isto é, $b \mid a$.

Demonstração. Como a e b são inteiros, existe algum inteiro k tal que $k \leq \frac{a}{|b|} < k+1$, já que se trata de números inteiros. Multiplicando toda essa desigualdade por $|b|$, lembrando que $|b| > 0$, temos

$$k|b| \leq a < k|b| + |b|.$$

Observando a parte $k|b| \leq a$, podemos reescrevê-la como $0 \leq a - k|b|$ e a parte $a < k|b| + |b|$ pode ser reescrita como $a - k|b| < |b|$. Como $a - k|b|$ é um número inteiro podemos tomar $r = a - k|b|$ e, assim, $0 \leq r < |b|$. Dessa forma $a = k|b| + r$. Convenientemente podemos tomar $q = k\frac{|b|}{b} \in \mathbb{Z}$ para obtermos $k|b| = qb$ e, logo, encontramos $a = qb + r$, sendo q e r inteiros, com $0 \leq r < |b|$. □

O procedimento descrito a seguir é conhecido como o algoritmo de divisão de Euclides. Considere a e b inteiros positivos, onde $a > b$. Se $b \mid a$, pelo Lema 4, $(a,b) = |b|$. Suponhamos, agora, que $1 < b < a$ e que $b \nmid a$. O Teorema 1 permite escrever

$$a = q_1 b + r_1, \tag{2.3}$$

com q_1 e r_1 naturais, sendo $0 < r_1 < b$. Devemos considerar as seguintes possibilidades:

i) Se $r_1 \mid b$, temos pelo Lema 4 que $(b, r_1) = r_1$. De (2.3) e utilizando o Lema 1, temos

$$r_1 = (r_1, b) = (a - q_1 b, b) = (a, b),$$

e, dessa forma, o algoritmo termina, pois r_1 é o maior divisor de a e de b.

ii) Se $r_1 \nmid b$, podemos utilizar o Teorema 1 e assim teremos

$$b = r_1 q_2 + r_2,$$

com $0 < r_2 < r_1$. E novamente, neste caso, temos duas opções as serem analisadas:

ii.a) Se $r_2 \mid r_1$, temos pelo Lema 4 que $(r_1, r_2) = r_2$ e, pelo Lema 1, que

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

e paramos já que r_2 é o maior divisor comum de a e b.

ii.b) Se $r_2 \nmid r_1$, pelo Teorema 1 temos

$$r_1 = r_2 q_3 + r_3,$$

com $0 < r_3 < r_2 < r_1$.

O procedimento descrito possui fim, pois como resultado é gerada uma sequência decrescente de números inteiros não negativos $r_1 > r_2 > \ldots > 0$. Existe, portanto, um inteiro $n > 0$ tal que $r_1 > \ldots > r_n$, sendo r_n o menor resto possível da divisão de a por b tal que $r_n \mid r_{n-1}$ e

$$r_n = (r_n, r_{n-1}) = (r_{n-1}, r_{n-2}) = \cdots = (r_2, r_1) = (r_1, b) = (b, a).$$

O algoritmo de Euclides fornece, portanto, uma maneira de se calcular (a,b). O seguinte exemplo mostra como é possível obtermos o máximo divisor comum entre 200 e 188. Temos neste caso que

$$\begin{aligned} 200 &= 1 \cdot 188 + 12 \\ 188 &= 15 \cdot 12 + 8 \\ 12 &= 1 \cdot 8 + 4 \end{aligned}$$

Como $4 \mid 8$, temos que $(200, 188) = 4$.

No teorema a seguir provaremos, de outra forma, que $(a,b) = r_n$. Este resultado corresponde ao Teorema 207 em Hardy e Wright (2008).

Teorema 2. *Seja $r_1 > \ldots > r_n$ a sequência dos restos obtidos ao considerar o algoritmo de Euclides na divisão de a por b. Nesse caso $(a,b) = r_n$.*

Demonstração. Suponhamos que $(a,b) = d$, sabemos que $a = q_1 b + r_1$ e, como $d \mid a$ e $d \mid b$, assim $d \mid r_1$. Por outro lado $b = q_2 r_1 + r_2$ e, como $d \mid b$ e $d \mid r_1$, temos que $d \mid r_2$. Continuando este processo até r_n veremos que $d \mid r_n$ e logo concluimos que $d \leq r_n$. De forma similar, sabendo que $r_n \mid r_{n-1}$, temos que

$$r_n \mid r_{n-1} \Rightarrow r_n \mid r_{n-2} \Rightarrow r_n \mid r_{n-3} \Rightarrow \cdots \Rightarrow r_n \mid r_1 \Rightarrow r_n \mid b \Rightarrow r_n \mid a.$$

Se $r_n \mid a$ e $r_n \mid b$, então $r_n \mid d$ e, assim, $r_n \leq d$. Mas concluímos tamém que $d \leq r_n$ e, dessa forma, encontramos $r_n = d = (a,b)$. □

2.4 Teorema Fundamental da Aritmética

O seguinte teorema ocupa uma posição central na Teoria dos Números. É de fato o ponto de partida para a análise do último Teorema de Fermat no caso $n = 3$, estudado no Capítulo 4.

Teorema 3. *Todo inteiro $n > 1$, pode ser representado de uma única forma em um produto de números primos, além, é claro, da ordem dos fatores.*

A demonstração deste teorema depende de dois resultados preliminares, enunciados nos seguintes dois teoremas. Estes correspondem, respectivamente, aos Teoremas 208 e 209 em Hardy e Wright (2008).

Teorema 4. *Se $d \mid a$ e $d \mid b$, então $d \mid (a,b)$.*

Demonstração. A demonstração está baseada no algoritmo de Euclides e, em particular, no Teorema 2. Usando o Teorema 1 temos $a = q_1 b + r_1$. Por hipótese $d \mid a$ e $d \mid b$ portanto $d \mid r_1$. Novamente, utilizando o Teorema 1 podemos expressar b como $b = q_2 r_1 + r_2$. Temos como hipótese $d \mid b$ o qual junto a $d \mid r_1$ implica em $d \mid r_2$. Continuando este processo sucessivamente obtemos

$$d \mid r_1 \Rightarrow d \mid r_2 \Rightarrow d \mid r_3 \Rightarrow \ldots \Rightarrow d \mid r_n = (a,b),$$

sendo a última igualdade válida pelo Teorema 2. □

Teorema 5. *Se $(a,b) = 1$ e $b \mid ca$, então $b \mid c$.*

Demonstração. Utilizando o algoritmo de Euclides e multiplicando cada uma das equações obtidas ao aplicar a divisão Euclidiana por c obtemos

$$\begin{aligned} ca &= cq_1 b + cr_1 \\ &\vdots \\ cr_{n-2} &= cq_n r_{n-1} + cr_n \\ cr_{n-1} &= cq_{n+1} r_n, \end{aligned}$$

o qual corresponde ao algoritmo iniciado pela divisão de ca por cb em lugar de a por b. Assim, pelo Teorema 2, $(ca,cb) = cr_n$. Por outro lado, $r_n = (a,b) = 1$ o qual implica $(ca,cb) = c$. Se utilizamos $b \mid ca$, válido por hipótese, junto a $b \mid cb$, pelo Teorema 4 concluímos que $b \mid (ca,cb) = c$. □

Se p é primo, então ou $p \mid a$ ou $(a,p) = 1$. No último caso, se também supormos que $p \mid ac$, pelo Teorema 5, então obtemos $p \mid c$. Desta forma concluímos que $p \mid ac$ implica em $p \mid a$ ou $p \mid c$. Esse é a seguinte Proposição.

Proposição 5 (Primeiro Teorema de Euclides). *Sendo a e b inteiros e p primo, se $p \mid ab$ então $p \mid a$ ou $p \mid b$.*

Estamos praticamente prontos para demonstrarmos o Teorema 3. Só falta rever a noção da forma padrão na fatoração de um número em primos. Suponhamos que o inteiro positivo n possa ser fatorado como $n = p_1 p_2 \cdots p_k$ onde $p_1, p_2, \ldots, p_k$ são números primos não necessariamete diferentes nem ordenados de acordo com uma ordem específica. Se ordenamos estes números em forma crescente e associarmos conjuntos de primos iguais em fatores únicos, obtemos, após de uma mudança na notação, a seguinte representação para n,

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \qquad a_1 > 0,\ a_2 > 0,\ \ldots\ a_k > 0,\ p_1 < p_2 < \ldots < p_k.$$

Chamamos esta última de forma padrão de n.

Demonstração do Teorema 3. Uma extensão imediata da Proposição 5 fornece o seguinte resultado,

$$p \mid abc...l \Rightarrow p \mid a \text{ ou } p \mid b \text{ ou } p \mid c \text{ ou } \ldots \text{ ou } p \mid l.$$

Se a, b, ..., l são primos, então p é um destes números. Suponhamos que n possua duas decomposições em primos, isto é,

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = q_1^{b_1} q_2^{b_2} \cdots q_j^{b_j}.$$

Nesse caso temos necessariamente que $p_i \mid q_1^{b_1} q_2^{b_2} \cdots q_j^{b_j}$ para cada i, portanto a cada p corresponde exatamente um dos q e vice-versa. Assim $k = j$ e, uma vez que todos os números p e q estejam organizados em ordem crescente, $p_i = q_i$ para cada i.

Cogitamos que $a_i > b_i$. Se dividirmos ambas as formas padrão de n por $p_i^{b_i}$ obtemos

$$p_1^{a_1} \cdots p_i^{a_i - b_i} \cdots p_k^{a_k} = p_1^{b_1} \cdots p_{i-1}^{b_{i-1}} p_{i+1}^{b_{i+1}} \cdots p_k^{b_k}.$$

O lado esquerdo desta última identidade é divisível por p_i, porém o lado direito não é divisível por p_i, o que gera uma contradição. De maneira análoga $b_i > a_i$ também gera uma contradição e assim provamos que $a_i = b_i$ para cada i. Isto conclui a demonstração do Teorema 3. □

O número 1 não é considerado primo, pois senão este teorema seria falso uma vez que podemos inserir qualquer quantidade de unidades dentre os fatores.

Apresentamos a seguir uma forma equivalente de enunciarmos o Teorema 3, a qual permite estender este resultado de maneira natural aos conjuntos a serem considerados no próximo capítulo. Mas antes, temos a definição de um associado.

Definição 4 (Associado). Seja x um inteiro, dizemos que o produto entre x e uma unidade é um associado de x, assim, os associados de x são os números x e $-x$.

Teorema 6 (Teorema Fundamental da Aritmética em $\mathbb{Z}$). *Qualquer inteiro diferente de* ± 1 *ou* 0 *pode ser expresso como um produto de primos de maneira única, exceto em relação à ordem dos primos e o uso dos associados desses primos.*

Teorema 7. *Considerando a, b, c e x inteiros tais que $ab = c^x$ e $(a,b) = 1$, existem inteiros s e t tais que $a = s^x$ e $b = t^x$.*

Este teorema será utilizado na Seção 4.2.

Demonstração. Desconsideraremos os casos em que $a = 1$ ou $b = 1$, pois assim o teorema seria trivial. Pelo Teorema 6, temos que $c = p_1^{d_1} p_2^{d_2} p_3^{d_3} ... p_m^{d_m}$, com $d_1 > 0$, $d_2 > 0$, ... e $d_m > 0$ sendo cada um dos p_j, com $1 \leq j \leq m$, um número primo. Assim, segue que $c^x = p_1^{xd_1} p_2^{xd_2} p_3^{xd_3} ... p_m^{xd_m}$ e, dessa forma, cada $p_j^{xd_j}$ é uma potência de expoente x. Por outro lado, ainda pelo Teorema 6, temos da mesma forma que $a = s_1^{e_1} s_2^{e_2} s_3^{e_3} ... s_n^{e_n}$, com $e_1 > 0$, $e_2 > 0$, ... e

$e_n > 0$ sendo cada um dos $s_k^{e_k}$, com $1 \leq k \leq n$, um primo e que $b = t_1^{f_1} t_2^{f_2} t_3^{f_3} ... t_q^{f_q}$, com $f_1 > 0$, $f_2 > 0$, ... e $f_q > 0$ sendo cada um dos $s_l^{f_l}$, com $1 \leq l \leq q$, um primo. Sabemos que

$$c^x = p_1^{xd_1} p_2^{xd_2} p_3^{xd_3} ... p_m^{xd_m} = ab = s_1^{e_1} s_2^{e_2} s_3^{e_3} \ldots s_n^{e_n} \cdot t_1^{f_1} t_2^{f_2} t_3^{f_3} \ldots t_q^{f_q}.$$

Como $(a,b) = 1$, nenhum dos $s_k^{e_k}$ é igual a um dos $t_l^{f_l}$ e, assim, cada um dos $p_j^{xd_j}$ será igual a um $s_k^{e_k}$ ou um $t_l^{f_l}$, fazendo com que e_k e f_l também sejam potências de expoente x, provando assim o Teorema 7. □

A seguinte propriedade do mdc é aplicação elementar do Teorema Fundamental da Aritmética. Esta será utilizada adiante no estudo de certos problemas Diofantinos.

Lema 6. *Sejam a e b inteiros, não ambos nulos, tais que* $(a,b) = 1$*, então para qualquer inteiro positivo k tem-se* $(a^k, b^k) = 1$.

Demonstração. Considere as fatorações em números primos de a e b,

$$a = p_1 p_2 ... p_m \quad \text{e} \quad b = q_1 q_2 ... q_n.$$

Como $(a,b) = 1$, nenhum dos primos p_i pode ser igual a algum dos primos q_j, portanto $p_i^k \neq q_j^k$ para quaisquer $1 \leq i \leq m$, $1 \leq j \leq n$ e qualquer inteiro positivo k. Dessa forma a^k e b^k não possuem primos em comum nas suas fatorações, o que implica em $(a^k, b^k) = 1$. □

2.5 Congruências

Definição 5. Sejam a, b e c inteiros. Quando os restos das divisões de a por c e de b por c são iguais, dizemos que a e b são congruentes módulo c e escreve-se

$$a \equiv b \pmod{c}. \tag{2.4}$$

Exemplo 2. O resto da divisão de 41 por 5 é igual 1 e o resto da divisão de 26 por 5 também é igual a 1, logo $41 \equiv 26 \pmod 5$.

Proposição 6. *Sejam a, b e c três inteiros, com* $c \neq 0$*. Temos que* $a \equiv b \pmod c$ *se, e somente se,* $c \mid (a-b)$.

Demonstração. Considere as divisões Euclidianas de a e b por c, $a = cq_1 + r_1$, com $0 \leq r_1 < c$ e $b = cq_2 + r_2$, com $0 \leq r_2 < c$. Temos que

$$a - b = c(q_1 - q_2) + (r_1 - r_2). \tag{2.5}$$

Para dizermos que $a \equiv b \pmod c$, r_1 e r_2 devem ser iguais e, assim, $a - b = c(q_1 - q_2) + 0$. Isso ocorre se, e só se, $c \mid (a-b)$. □

Exemplo 3. Temos que $15 \equiv 21 \pmod 6$, e $6 \mid (15-21)$.

Proposição 7. *Sendo $a \equiv b \pmod c$, existe algum k inteiro tal que $a = ck + b$.*

Demonstração. Utilizando a Proposição 6 temos que $a - b = c(q_1 - q_2)$. Pela divisão Euclidiana $(q_1 - q_2)$ deve ser inteiro e, assim, trocando $(q_1 - q_2)$ por k, temos $a = ck + b$. □

Proposição 8. *Sendo a, b, c, d e x inteiros tais que $a \equiv b \pmod x$ e $c \equiv d \pmod x$, então $(a + c) \equiv (b + d) \pmod x$.*

Demonstração. Pela Proposição 6 sabemos que $x \mid (b - a)$ e $x \mid (d - c)$. Desta forma $x \mid (b - a) + (d - c) = (b + d) - (a + c)$ e, logo $(a + c) \equiv (b + d) \pmod x$. □

Proposição 9. *Sendo a, b, c, d e x inteiros tais que $a \equiv b \pmod x$ e $c \equiv d \pmod x$, então $ac \equiv bd \pmod x$.*

Demonstração. Para isto, devemos demonstrar que $x \mid (bd - ac)$. Sabemos, pela Proposição 6, que $x \mid (b - a)$ e $x \mid (d - c)$, assim podemos afirmar que $x \mid d(b - a)$ e $x \mid a(d - c)$. Logo, $x \mid d(b - a) + a(d - c) = (bd - ac)$. □

CAPÍTULO 3

OS INTEIROS DE GAUSS E DE EISENSTEIN

Este capítulo apresenta algumas propriedades elementares de dois conjuntos conhecidos como os inteiros de Gauss e de Eisenstein. O primeiro foi considerado por Gauss na sua pesquisa sobre reciprocidade biquadrática. Maiores detalhes podem ser encontrados nas memórias de Gauss tituladas *Theoria residuorum biquadraticorum*, *Werke*, ii. 67-148 (GAUSS, 1876). Gauss foi o primeiro matemático a utilizar números complexos de maneira consistente. Os inteiros de Eisenstein foram introduzidos por Eisenstein e Jacobi nos seus trabalhos sobre reciprocidade cúbica.

Os resultados apresentados neste capítulo são pré-requisitos para o estudo do problema diofantino $x^3 + y^3 = z^3$ considerado no Capítulo 4.

3.1 O anel $\mathbb{Z}[i]$

Chamamos de inteiros Gaussianos o conjunto definido como

$$\{\, \xi = a + bi \ : \ a, b \in \mathbb{Z},\ i = \sqrt{-1}\,\}.$$

É imediato que os inteiros racionais estão incluídos nesse conjunto, basta tomar $b = 0$.

Sejam $\xi = a + bi$ e $\zeta = c + di$ dois inteiros Gaussianos. As operações de adição, subtração, multiplicação e divisão são definidas pelas operações correspondentes aos números complexos, isto é,

Adição: $\xi + \zeta = (a + c) + (b + d)i$

Subtração: $\xi - \zeta = (a + c) - (b + d)i$

Multiplicação: $\xi\zeta = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i$

Divisão:

$$\frac{\xi}{\zeta} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) - (ad - bc)i}{c^2 + d^2} \tag{3.1}$$

Observe que a adição e multiplicação sempre geram um inteiro em $\mathbb{Z}[i]$ e que 0 e 1 são neutros, nessa ordem, para adições e multiplicações. Isto faz do conjunto dos inteiros Gaussianos um anel, usualmente denotado por $\mathbb{Z}[i]$. Analogamente às definições para os números complexos, consideramos o conjugado do número $\xi = a + bi$ como sendo o inteiro $\bar{\xi} = a - bi$. Para dois inteiros Gaussianos ξ, ζ quaisquer, desta definição decorre que $\overline{\xi + \zeta} = \bar{\xi} + \bar{\zeta}$. Denotamos a

parte real de ξ por $\Re\mathrm{e}(\xi)$ e a parte imaginária por $\Im\mathrm{m}(\xi)$. Apresentamos a seguir duas definições essenciais para desenvolver a Teoria dos inteiros Gaussianos.

Definição 6 (**Divisibilidade**)**.** Sejam η, ξ dois inteiros Gaussianos com $\eta \neq 0$. Escrevemos $\eta \mid \xi$, se existe algum inteiro Gaussiano ζ tal que

$$\xi = \eta\zeta.$$

Usando a Definição 6, são imediatas as seguintes propriedades

$$\begin{gathered} \alpha \mid \beta \ \text{ e } \ \beta \mid \gamma \ \Rightarrow \ \alpha \mid \gamma \qquad (3.2) \\ \alpha \mid \gamma_1, \ \alpha \mid \gamma_2, \ \ldots, \ \alpha \mid \gamma_n \ \Rightarrow \ \alpha \mid (\beta_1\gamma_1 + \beta_2\gamma_2 + \ldots + \beta_n\gamma_n). \end{gathered}$$

Definição 7 (**Unidade**)**.** De forma análoga ao considerado no anel dos inteiros racionais, uma unidade ϵ é um inteiro que divide qualquer inteiro $\xi \in \mathbb{Z}[i]$.

Também podemos dizer que a unidade ϵ é qualquer inteiro que divida o número 1, pois 1 divide qualquer ξ e assim (3.2) implica em $\epsilon \mid \xi$. Além das unidades ± 1, $\mathbb{Z}[i]$ também possui como unidades os números $\pm i$. De fato, para o inteiro $\xi = a + bi$ temos

$$\begin{aligned} \frac{\xi}{i} &= \frac{(a+bi)}{i} = \frac{(a+bi)(-i)}{i(-i)} = b - ai, \\ \frac{\xi}{-i} &= \frac{(a+bi)}{-i} = \frac{(a+bi)i}{-i\,i} = -b + ai. \end{aligned}$$

Qualquer inteiro Gaussiano ξ possui, portanto, oito divisores triviais

$$\pm 1, \pm\xi, \pm i, \ \text{ e } \ \pm i\xi.$$

Introduzimos a seguir uma norma em $\mathbb{Z}[i]$ a qual será utilizada para descrever as unidades e os primos neste corpo.

Definição 8. Para qualquer inteiro $\xi = a + bi$, definimos a sua norma como sendo a função $\| \ \| : \mathbb{Z}[i] \to \mathbb{Z}$ dada por $\xi \mapsto \|\xi\| = \xi\bar{\xi} = a^2 + b^2$.

É interessante observar que a norma utilizada aqui é diferente da utilizada comumente em análise, sendo esta última definida como $(\xi\bar{\xi})^{1/2}$ e denotada por $|\xi|$. Um dos motivos da escolha feita aqui é que $\|\xi\| \in \mathbb{Z}$.

Lema 7. *O produto entre as normas de dois ou mais inteiros Gaussianos é igual à norma do produto entre os inteiros.*

Demonstração. Para dois inteiros Gaussianos quaisquer da forma $\xi = a + bi$ e $\zeta = c + di$ temos que

$$\|\xi\|\|\zeta\| = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2.$$

Por outro lado,

$$\begin{aligned}\|\xi\zeta\| &= \|(a+bi)(c+di)\| = \|(ac-bd)+(ad+bc)i\| \\ &= (ac-bd)^2+(ad+bc)^2 = a^2c^2+b^2d^2+a^2d^2+b^2c^2\end{aligned}$$

e, assim, $\|\xi\|\|\zeta\| = \|\xi\zeta\|$. □

Lema 8. *A norma de uma unidade em $\mathbb{Z}[i]$ é 1 e qualquer inteiro cuja norma é 1, também é uma unidade.*

Demonstração. Se ϵ é uma unidade, então $\epsilon \mid 1$ e, dessa forma, $1 = \epsilon\zeta$ para algum ζ inteiro Gaussiano. Sabemos também que $\|1\| = 1$. Do Lema 7 obtemos

$$\|\epsilon\zeta\| = 1 \Rightarrow \|\epsilon\|\|\zeta\| = 1,$$

e, assim, $\|\epsilon\| \mid 1$. Como sabemos que uma norma é um inteiro racional não negativo e que o único desses que divide 1 é o próprio 1, segue que $\|\epsilon\| = 1$. Suponhamos agora, que $\alpha = a+bi$ seja um inteiro Gaussiano tal que $\|\alpha\| = 1$. Neste caso temos que

$$1 = a^2+b^2 = \alpha\bar{\alpha},$$

logo $\alpha|1$ e assim, utilizando (3.2), deduzimos que α é uma unidade. □

Teorema 8. *As unidades em $\mathbb{Z}[i]$ são os números $\epsilon = i^\ell$, $\ell = 0,1,2,3$.*

Demonstração. Suponha $\epsilon = a+bi$ uma unidade. Do Lema 8 temos que $\|\epsilon\| = 1$ e assim $a^2+b^2 = 1$. Como a e b são inteiros racionais temos apenas duas opções para ϵ,

i) Se $a = \pm 1$ e $b = 0$, então $\epsilon = 1 = i^0$ ou $\epsilon = -1 = i^2$,

ii) Se $a = 0$ e $b = \pm 1$, logo $\epsilon = i = i^1$ ou $\epsilon = -i = i^3$.

Isto conclui a demonstração. □

Definição 9 (Associado). Seja ξ um inteiro e ϵ uma unidade. Dizemos que $\epsilon\xi$ é um associado de ξ. Os associados de ξ são, portanto, os números

$$\xi,\ -\xi,\ i\xi \text{ e } -i\xi.$$

Os associados de uma unidade também são claramente unidades. Assim, se $\xi \mid \eta$, temos que $\xi\epsilon_1 \mid \eta\epsilon_2$, sendo ϵ_1 e ϵ_2 unidades quaiquer, pois $\epsilon_1 \mid \epsilon_2$ e $\epsilon_2 \mid \epsilon_1$. Logo qualquer associado de ξ divide um associado qualquer de η.

3.1.1 Os primos em $\mathbb{Z}[i]$

Definição 10 (Primos). A definição a seguir é similar à definição de primo em $\mathbb{Z}$. Um primo nos inteiros complexos é um número que possui exatamente oito divisores, sendo eles os seus associados e as unidades. Assim, se π é um primo em $\mathbb{Z}[i]$, seus únicos divisores são

$$\pm 1, \pm i, \pm \pi \text{ e } \pm i\pi.$$

Os associados de um primo são também primos em $\mathbb{Z}[i]$.

O seguinte teorema fornece um critério bastante útil para verificarmos se um inteiro Gaussiano é primo.

Teorema 9. *Se a norma de um inteiro Gaussiano ξ é um primo em $\mathbb{Z}$, então ξ é um primo em $\mathbb{Z}[i]$.*

Demonstração. Suponhamos que $\|\xi\| = p$, que p é um primo em $\mathbb{Z}$, e que $\xi = \eta\zeta$. Assim,

$$p = \|\xi\| = \|\eta\zeta\| = \|\eta\|\|\zeta\|.$$

Como p é um primo em $\mathbb{Z}$, temos as situações em que $\|\eta\| = 1$ e $\|\zeta\| = p$ ou $\|\eta\| = p$ e $\|\zeta\| = 1$. Supondo que $\|\eta\| = 1$ temos que η é uma unidade ϵ qualquer. Logo $\xi = \epsilon\zeta$, fazendo com que ζ seja um associado de ξ e, portanto, ξ é divisível apenas pelas unidades e por seus associados, o que faz de ξ um primo, análogo para o outro caso. □

Exemplo 4. O inteiro $2+i$ é primo, pois $\|2+i\| = 2^2 + 1^2 = 5$, e 5 é um primo em $\mathbb{Z}$.

Não podemos afirmar que a recíproca seja verdadeira, ou seja, que qualquer primo em $\mathbb{Z}$ será um primo em $\mathbb{Z}[i]$. Um bom exemplo disto é o inteiro racional 17, já que $17 = (4+i)(4-i)$, provando dessa forma que além dos oito divisores triviais há mais dois divisores para 17.

Teorema 10. *Qualquer inteiro não nulo e diferente das unidades é divisível por um primo.*

Demonstração. Se γ é um inteiro não primo, temos que

$$\gamma = \alpha_1\beta_1, \text{ com } \|\alpha_1\| > 1 \text{ e } \|\beta_1\| > 1.$$

Segue que $\|\gamma\| = \|\alpha_1\|\|\beta_1\|$ e também que $1 < \|\alpha_1\| < \|\gamma\|$. Se α_1 não é um primo, então

$$\alpha_1 = \alpha_2\beta_2, \text{ com } \|\alpha_2\| > 1 \text{ e } \|\beta_2\| > 1 \quad \Rightarrow \quad \|\alpha_1\| = \|\alpha_2\|\|\beta_2\|, \text{ com } 1 < \|\alpha_2\| < \|\alpha_1\|.$$

Se α_2 não é primo, então

$$\alpha_2 = \alpha_3\beta_3, \text{ com } \|\alpha_3\| > 1 \text{ e } \|\beta_3\| > 1 \quad \Rightarrow \quad \|\alpha_2\| = \|\alpha_3\|\|\beta_3\|, \text{ com } 1 < \|\alpha_3\| < \|\alpha_2\|.$$

Continuaremos este processo até encontrar algum α_r que seja primo, e isto acontecerá, pois

$$\|\gamma\| > \|\alpha_1\| > \|\alpha_2\| > ... > \|\alpha_r\| > 1$$

é uma sequência decrescente de inteiros racionais não negativos. Considerando que α_r seja o primeiro primo da sequência $\gamma, \alpha_1, \alpha_2, ...$ e α_r, temos

$$\gamma = \beta_1\alpha_1 = \beta_1\beta_2\alpha_2 = ... = \beta_1\beta_2\beta_3...\beta_r\alpha_r,$$

e, portanto, $\alpha_r \mid \gamma$. □

Teorema 11. *Qualquer inteiro não nulo e diferente das unidades em $\mathbb{Z}[i]$ é um produto de números primos.*

Demonstração. Seja γ um inteiro Gaussiano não nulo e diferente de qualquer uma das unidades em $\mathbb{Z}[i]$. O Teorema 10 garante a existência um primo π_1 tal que $\pi_1 \mid \gamma$ e assim de γ_1 tal que

$$\gamma = \pi_1\gamma_1, \quad \text{e} \ \|\gamma_1\| < \|\gamma\|.$$

O número γ_1 pode ou não ser uma unidade. No segundo caso, utilizando o mesmo argumento da a análise para γ, obtemos

$$\gamma_1 = \pi_2\gamma_2, \quad \text{e} \ \|\gamma_2\| < \|\gamma_1\|.$$

Repetindo este processo obtemos uma sequência decrescente $\|\gamma\|, \|\gamma_1\|, \ldots$ de números positivos em $\mathbb{Z}$. Existe, portanto, um índice r para o qual $\|\gamma_r\| = 1$, logo, do Lema 8, γ_r é necessariamente uma unidade. Desta forma, concluímos que

$$\gamma = \pi_1\pi_2\cdots\pi_{r-1}\theta_r,$$

no qual $\theta_r = \epsilon\pi_r$ é um número associado de π_r e também um primo. □

3.1.2 Teorema Fundamental da Aritmética em $\mathbb{Z}[i]$

O Teorema 11 mostra que qualquer inteiro $\gamma \in \mathbb{Z}[i]$ pode ser expresso como um produto de números primos, isto é,

$$\gamma = \pi_1\pi_2\ldots\pi_r.$$

O teorema apresentado a seguir, garante a unicidade desta representação, a não ser pela ordem dos fatores.

Teorema 12 (Teorema Fundamental da Aritmética em $\mathbb{Z}[i]$). *Todo inteiro Gaussiano não nulo e diferente de uma unidade, pode ser representado como um produto de primos e, desconsiderando a ordem entre os primos e as associações desses primos, esta representação é única.*

Este teorema será provado através dos três próximos teoremas, os quais, por sua vez, consideram um argumento análogo ao utilizado em $\mathbb{Z}$, baseado no Algoritmo de Euclides.

Teorema 13. *Sejam γ e $\gamma_1 \neq 0$ dois inteiros em $\mathbb{Z}[i]$. Existe um inteiro $\kappa \in \mathbb{Z}[i]$ tal que*

$$\gamma = \kappa\gamma_1 + \gamma_2, \text{ com } \|\gamma_2\| < \|\gamma_1\|.$$

Na demonstração vamos provar mais do que isso, de fato mostraremos que $\|\gamma_2\| < \frac{1}{2}\|\gamma_1\|$. Mesmo assim, o fato crucial para a demonstração do Teorema 12 é o que está no enunciado deste teorema. Se c e c_1 são inteiros racionais, com $c_1 \neq 0$, então pelo Teorema 1 existe um inteiro racional k tal que $c = c_1k + c_2$, com $0 \leq c_2 < c_1$. É sobre isso que depende a construção do Algoritmo de Euclides e o Teorema 13 fornece uma base para uma construção similar em $\mathbb{Z}[i]$.

Demonstração (do Teorema 13). Visto que $\gamma_1 \neq 0$, temos

$$\frac{\gamma}{\gamma_1} = R + Si,$$

sendo R e S números reais. Na verdade, R e S são números racionais o qual pode ser verificado pela fórmula (3.1). Sejam x e y dois inteiros racionais tais que

$$|R-x| \leq \frac{1}{2} \quad \text{e} \quad |S-y| \leq \frac{1}{2}.$$

Tais inteiros sempre existem, pois $\mathbb{Q}$ é denso nos números reais $\mathbb{R}$, logo sempre é possível escolhermos dois inteiros $x, y \in \mathbb{Z} \subset \mathbb{R}$, arbitrariamente próximos dos números $R, S \in \mathbb{Q}$. Assim, que

$$\left|\frac{\gamma}{\gamma_1} - (x+iy)\right| = |R+Si-x-iy| = |(R-x)+i(S-y)| = \sqrt{(R-x)^2+(S-y)^2}$$

pois para qualquer número complexo $z = a + bi$, por definição $|z| = (a^2+b^2)^{\frac{1}{2}}$. Utilizando os limitantes superiores para $|R-x|$ e $|S-y|$ obtemos $(R-x)^2 \leq \frac{1}{4}$ e $(S-y)^2 \leq \frac{1}{4}$, portanto

$$\left|\frac{\gamma}{\gamma_1} - (x+iy)\right| \leq \frac{1}{\sqrt{2}}.$$

Se agora escolhemos

$$\kappa = x+iy, \quad \text{e} \quad \gamma_2 = \gamma - \kappa\gamma_1,$$

temos

$$|\gamma_1|\left|\frac{\gamma}{\gamma_1} - \kappa\right| \leq \frac{1}{\sqrt{2}}|\gamma_1|,$$

ou seja, $|\gamma - \kappa\gamma_1| \leq 2^{-\frac{1}{2}}|\gamma_1|$, portanto $|\gamma_2| \leq 2^{-\frac{1}{2}}|\gamma_1|$. Isto implica em $\|\gamma_2\| \leq 2^{-1}\|\gamma_1\|$, pois por definição da norma em $\mathbb{Z}[i]$, para qualquer inteiro Gaussiano ξ, $\|\xi\| = |\xi|^2$. □

Aplicamos agora o Teorema 13 sucessivas vezes para obtermos um análogo ao Algoritmo de Euclides para a divisão de γ por $\gamma_1 \in \mathbb{Z}[i]$. Sejam γ e $\gamma_1 \neq 0$ dados, logo existe κ tal que

$$\gamma = \gamma_1\kappa + \gamma_2, \text{ com } \|\gamma_2\| < \|\gamma_1\|.$$

Se $\gamma_2 \neq 0$, então existe κ_1 tal que

$$\gamma_1 = \kappa_1\gamma_2 + \gamma_3, \text{ com } \|\gamma_3\| < \|\gamma_2\|$$

e assim por diante. A sequência $\|\gamma_1\|, \|\gamma_2\|, \|\gamma_3\|, \ldots$ gerada com este procedimento é uma sequência decrescente de inteiros racionais não negativos, logo há um número natural n tal que $\|\gamma_{n+1}\| = 0 \Rightarrow \gamma_{n+1} = 0$, e os dois últimos passos desse processo serão

$$\gamma_{n-2} = \kappa_{n-2}\gamma_{n-1} + \gamma, \text{ com } \|\gamma_n\| < \|\gamma_{n-1}\|$$

e

$$\gamma_{n-1} = \kappa_{n-1}\gamma_n + \gamma_{n+1} \Rightarrow \gamma_{n-1} = \kappa_{n-1}\gamma_n.$$

Observamos agora que, analogamente ao resultado do Teorema 2, γ_n é um divisor comum de γ e γ_1 e que todos os divisores comuns de γ e γ_1 também são divisores de γ_n. Isto motiva a seguinte definição.

Definição 11. Seja ζ o divisor comum de γ e de γ_1 tal que todo divisor comum de γ e γ_1, é também um divisor de ζ. Dizemos neste caso que ζ é o maior divisor comum de γ e γ_1 e o denotamos por $\zeta = (\gamma, \gamma_1)$.

De acordo com esta definição, γ_n é o máximo divisor comum de γ e γ_1, ou seja, $\gamma_n = (\gamma, \gamma_1)$. Observamos que, em geral, uma versão do Teorema 4 em $\mathbb{Z}[i]$ decorre da Definição 11, isto é, se $\zeta \mid \gamma$ e $\zeta \mid \gamma_1$ então $\zeta = (\gamma, \gamma_1)$. Embora, diferentemente do que ocorre em $\mathbb{Z}$, um máximo divisor comum em $\mathbb{Z}[i]$ não é único já que seus associados também serão máximos divisores comuns. Para verificarmos isso, suponhamos que η e ζ sejam os máximos divisores comuns de α e β, então, pela definição, $\eta \mid \zeta$, $\zeta \mid \eta$ e assim $\zeta = \phi\eta$ e $\eta = \theta\zeta$, com ϕ e θ inteiros. Portanto $\phi\theta = 1$, assim $\phi \mid 1$ o que mostra que ϕ é uma unidade. Como ϕ é uma unidade, η é um associado de ζ, pois $\zeta = \phi\eta$. Logo podemos dizer que um máximo divisor comum é único, exceto pela ambiguidade entre seus associados.

Note que a definição de máximo divisor comum nos inteiros racionais é diferente da definição nos inteiros Gaussianos. Em $\mathbb{Z}$ o máximo divisor comum é um inteiro racional positivo. Uma forma alternativa de definirmos o máximo divisor comum de dois números em $\mathbb{Z}[i]$ é aquele número que, dentre os divisores comuns, possui a maior norma.

O seguinte resultado é análogo ao Teorema 5.

Teorema 14. *Se $(\gamma, \gamma_1) = 1$ e $\gamma_1 \mid \beta\gamma$, então $\gamma_1 \mid \beta$.*

Demonstração. Multiplicando $(\gamma, \gamma_1) = 1$ por β temos $(\beta\gamma, \beta\gamma_1) = \beta$. Por hipótese $\gamma_1 \mid \beta\gamma$ e, como $\gamma_1 \mid \beta\gamma_1$, temos que $\gamma_1 \mid (\beta\gamma, \beta\gamma_1) = \beta$. □

Se π é um primo e $(\pi, \gamma) = \mu$, então $\mu \mid \pi$ e $\mu \mid \gamma$. Se μ é uma unidade temos $(\pi, \gamma) = \pm 1$ ou $(\pi, \gamma) = \pm i$, ou se μ não é uma unidade temos que μ é um associado de π e logo $\pi \mid \gamma$. Se tomarmos $\gamma_1 = \pi$ no Teorema 14, obtemos uma analogia ao Primeiro Teorema de Euclides, Proposição 5.

Teorema 15. *Se π é um primo e $\pi \mid \beta\gamma$, então $\pi \mid \beta$ ou $\pi \mid \gamma$.*

Com estes requisitos, estamos prontos para a demonstração do Teorema Fundamental em $\mathbb{Z}[i]$. O argumento utilizado na prova é igual ao utilizado na demonstração do Teorema 6, apresentado no final da Seção 2.4.

3.2 Os inteiros de Eisenstein

O conjunto conhecido como os inteiros de Einsenstein é definido como

$$\{a + b\rho \,|\, a, b \in \mathbb{Z}\},$$

sendo ρ o número complexo determinado pela expressão (2.2). Considerando $\xi = a + b\rho$ e $\zeta = c + d\rho$ dois inteiros de Eisenstein, as operações de adição, subtração e multiplicação são definidas pelas operações correspondentes aos números complexos, isto é,

Adição: $\xi + \zeta = (a + c) + (b + d)\rho$

Subtração: $\xi - \zeta = (a + c) - (b + d)\rho$

Multiplicação: $\xi\zeta = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)\rho$

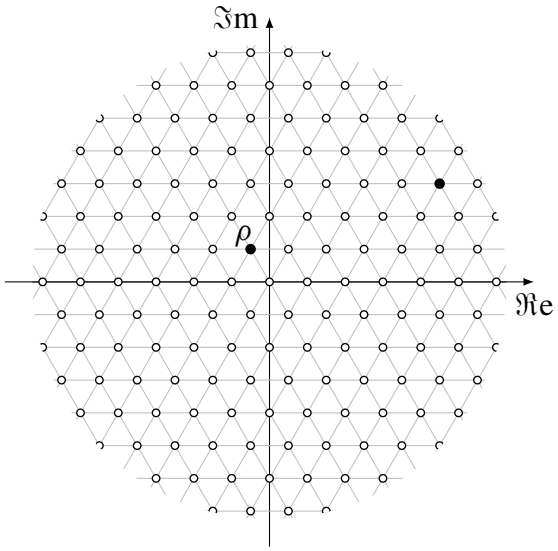
Os resultados da adição e da multiplicação sempre geram um inteiro de Eisenstein e 0 e 1 são neutros, nessa ordem, para adições e multiplicações. Isto faz desse conjunto um anel e o denotamos por $\mathbb{Z}[\rho]$.

Definição 12 (Divisibilidade). Sejam α, β dois inteiros de Einsestein com $\alpha \neq 0$. Escrevemos $\alpha \mid \beta$ se existir algum inteiro η em $\mathbb{Z}[\rho]$ tal que

$$\beta = \eta\alpha.$$

Ao longo desta seção utilizamos o termo inteiro para um inteiro em $\mathbb{Z}[\rho]$. Tipicamente utilizamos letras gregas para denotar elementos em $\mathbb{Z}[\rho]$ e $\mathbb{Z}[i]$ e as letras a, b, ... para os elementos de $\mathbb{Z}$. Uma representação dos elementos de $\mathbb{Z}[\rho]$ no plano complexo é apresentada na Figura 2. Além do ponto ρ, essa Figura também apresenta em destaque o inteiro $6 + 3\rho$.

Figura 2 – Representação do conjunto $\mathbb{Z}[\rho]$ no plano complexo.



Fonte – Realizada pelo autor.

O número ρ apresenta as seguintes duas propriedades

$$\rho^2 + \rho + 1 = 0 \tag{3.3}$$

$$\rho^3 = 1. \tag{3.4}$$

Essas serão utilizadas constantemente ao longo desta seção e posteriormente na Seção 4.2.3 do Capítulo 4.

A seguir introduziremos a definição de norma em $\mathbb{Z}[\rho]$.

Definição 13. Seja $\xi = a + b\rho$. A função $\| \ \| : \mathbb{Z}[\rho] \to \mathbb{Z}[i]$,

$$\xi \mapsto \|\xi\| = (a + b\rho)(a + b\rho^2) = a^2 - ab + b^2,$$

é uma norma em $\mathbb{Z}[\rho]$.

Demonstração. Observamos primeiro que a expressão para a norma de ξ pode ser fatorada como

$$\|\xi\| = \left(a - \frac{1}{2}b\right)^2 + \frac{3}{4}b^2,$$

o qual mostra que $\|\xi\| > 0$ se $\xi \neq 0$ e $\|\xi\| = 0$ se, e somente se, $\xi = 0$. Só resta mostrar a desigualdade triangular. Esta desigualdade pode ser obtida seguindo passos análogos a aqueles descritos na demonstração do Definição 8. □

Observamos agora que se ξ é um inteiro Gaussiano da forma $a + b\rho$, então

$$|\xi|^2 = \|\xi\|, \tag{3.5}$$

pois $|a+b\rho|^2 = a^2 - ab + b^2 = \|a+b\rho\|$. Portanto, para quaisquer inteiros Gaussianos $\alpha, \beta, \ldots$, temos

$$\|\alpha\|\|\beta\| = \|\alpha\beta\|, \qquad \|\alpha\|\|\beta\|\cdots = \|\alpha\beta\cdots\|.$$

Para verificarmos isto, basta observar que $\|\alpha\|\|\beta\| = |\alpha|^2|\beta|^2 = |\alpha\beta|^2 = \|\alpha\beta\|$.

O Lema 8 e os Teoremas 9, 10 e 11 permanecem verdadeiros em $\mathbb{Z}[\rho]$ e as demonstrações são as mesmas, excetuando a forma para a norma em $\mathbb{Z}[\rho]$. As unidades em $\mathbb{Z}[\rho]$ diferem daquelas em $\mathbb{Z}[i]$.

Lema 9. *As unidades em $\mathbb{Z}[\rho]$ são os números ± 1, $\pm\rho$ e $\pm\rho^2$.*

Demonstração. Da definição da norma em $\mathbb{Z}[\rho]$ e o Lema 8, as unidades ϵ satisfazem

$$\|\epsilon\| = a^2 - ab + b^2 = 1.$$

As únicas soluções para esta equação são:

i) $a = \pm 1$ e $b = 0$, então temos $\epsilon = \pm 1$;

ii) $a = 0$ e $b = \pm 1$, então temos $\epsilon = \pm\rho$;

iii) $a = 1$ e $b = 1$, então temos $\epsilon = (1+\rho)$ ou $-\rho^2$;

iv) $a = -1$ e $b = -1$, então temos $\epsilon = -(1+\rho)$ ou ρ^2. □

Além de estabelecer a noção correta de unidade, a norma apresentada na Definição 13 fornece um critério bastante útil para identificar os primos em $\mathbb{Z}[\rho]$.

Proposição 10. *Qualquer número inteiro cuja norma seja um primo em $\mathbb{Z}$, será um primo em $\mathbb{Z}[\rho]$.*

A demonstração desta proposição é igual a demonstração do resultado análogo em $\mathbb{Z}[i]$, isto é, do Teorema 9.

Por exemplo, o número $1-6\rho$ é um primo, pois $\|1-6\rho\| = 31$. O contrário é falso. Por exemplo, se consideramos o número primo 2,

$$2 = (a+b\rho)(c+d\rho) \Rightarrow 4 = (a^2 - ab + b^2)(c^2 - cd + d^2)$$

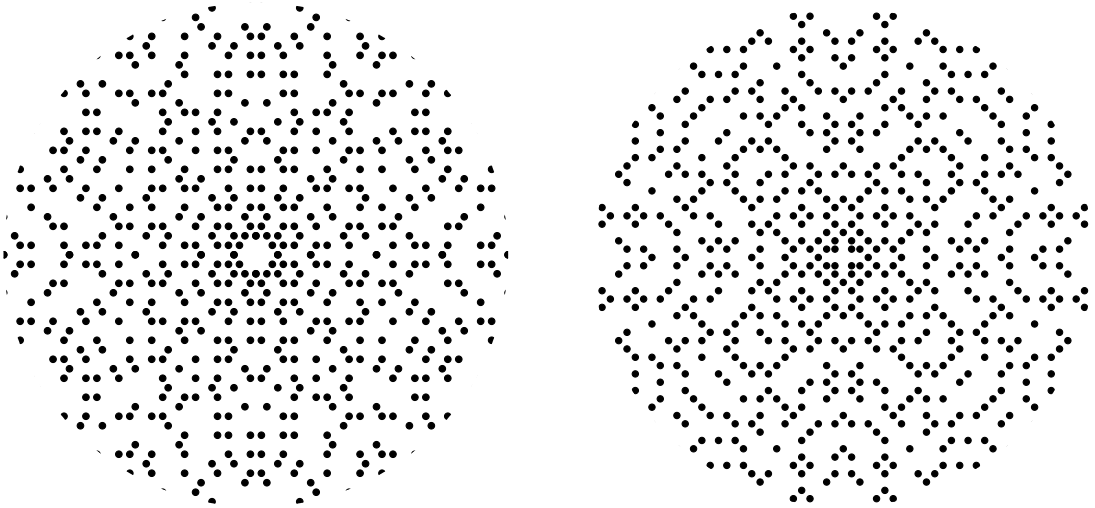
do qual resulta que ou $a+b\rho$ ou $c+d\rho$ é uma unidade, ou

$$a^2 - ab + b^2 = \pm 2, \qquad (2a-b)^2 + 3b^2 = \pm 8,$$

que é impossível. Apenas para comparação, a Figura 3 apresenta a distribuição no plano complexo dos primos em $\mathbb{Z}[i]$ e $\mathbb{Z}[\rho]$, próximos da origem. A identificação dos primos em $\mathbb{Z}[\rho]$ nesta figura está baseada no critério exposto na Proposição 10.

O Teorema Fundamental da Aritmética também é verdadeiro em $\mathbb{Z}[\rho]$. A demonstração deste fato depende do seguinte resultado, análogo ao resultado em $\mathbb{Z}[i]$ descrito pelo Teorema 13.

Figura 3 – Distribuição dos primos em $\mathbb{Z}[\rho]$ (esquerda) e $\mathbb{Z}[i]$ no plano complexo



Fonte – Realizada pelo autor, baseado no código em *Mathematica* segundo Pegg (2016).

Teorema 16. *Dados quaisquer inteiros γ e γ_1, com $\gamma_1 \neq 0$, existe um inteiro κ tal que*

$$\gamma = \kappa\gamma_1 + \gamma_2, \text{ com } \|\gamma_2\| < \|\gamma_1\|.$$

Demonstração. Sejam $\gamma = a + b\rho$ e $\gamma_1 = c + d\rho$, logo

$$\frac{\gamma}{\gamma_1} = \frac{a+b\rho}{c+d\rho} = \frac{(a+b\rho)(c+d\rho^2)}{(c+d\rho)(c+d\rho^2)} = \frac{(ac+bd-ad)+(bc-ad)\rho}{c^2-cd+d^2} = R + S\rho,$$

sendo R e S números reais. Podemos encontrar inteiros racionais x e y tais que

$$|R-x| \leq \frac{1}{2} \quad \text{e} \quad |S-y| \leq \frac{1}{2}.$$

Assim

$$\begin{aligned}\left|\frac{\gamma}{\gamma_1} - (x+y\rho)\right|^2 &= |(R-x)+(S-y)\rho|^2 = \|(R-x)+(S-y)\rho\| \\ &= (R-x)^2 - (R-x)(S-y) + (S-y)^2 \leq \left(\frac{1}{2}\right)^2 + \frac{1}{2}\frac{1}{2} + \left(\frac{1}{2}\right)^2 = \frac{3}{4}\end{aligned}$$

sendo que a segunda igualdade decorre de (3.5). Se agora tomamos $\kappa = x + y\rho$ e $\gamma_2 = \gamma - \kappa\gamma_1$, a cota superior permite escrever

$$\|\gamma_1\|\left\|\frac{\gamma}{\gamma_1} - \kappa\right\|^2 \leq \frac{3}{4}\|\gamma_1\| \Rightarrow \|\gamma - \kappa\gamma_1\|^2 \leq \frac{3}{4}\|\gamma_1\| < \|\gamma_1\|. \qquad \square$$

Teorema 17 (Teorema Fundamental da Aritmética em $\mathbb{Z}[\rho]$). *Todo inteiro em $\mathbb{Z}[\rho]$, exceto as unidades e o número 0, pode ser representado como um produto de números primos. Além da ordem entre os primos e do uso dos associados desses primos, o produto é único.*

A demonstração do Teorema 17 é análoga à demonstração do Teorema Fundamental da Aritmética em $\mathbb{Z}[i]$. O argumento é igual ao apresentado no final da Seção 2.4, munidos da forma equivalente para a divisão Euclideana em $\mathbb{Z}[\rho]$ fornecida pelo Teorema 16.

As próximas conclusões que tiraremos aqui serão de fundamental importância para a Seção 4.2.3. Observamos que a definição de congruência em $\mathbb{Z}[\rho]$ é igual a definição em $\mathbb{Z}$.

Lema 10. *Para $a, b \in \mathbb{Z}$ quaisquer, tem-se*

$$(a \pm b\rho)(a \pm b\rho^2) = a^2 \mp ab + b^2, \qquad (a \pm b)(a \pm b\rho)(a \pm b\rho^2) = a^3 \pm b^3.$$

Demonstração. Cada uma das identidades é demonstrada desenvolvendo o produto dos fatores correspondentes e utilizando as propriedades de ρ em (3.3) e (3.4). Para o primeiro dos produtos temos

$$(a \pm b\rho)(a \pm b\rho^2) = a^2 \pm ab(\rho^2 + \rho) + b^2\rho^3 = a^2 \mp ab + b^2,$$

e para o segundo,

$$(a \pm b)(a \pm b\rho)(a \pm b\rho^2) = (a \pm b)(a^2 \mp ab + b^3) = a^3 \pm b^3. \qquad \square$$

Lema 11. *O número*

$$\lambda = 1 - \rho \tag{3.6}$$

é primo em $\mathbb{Z}[\rho]$.

Demonstração. A norma de λ é $\|\lambda\| = 1^2 - 1(-1) + (-1)^2 = 3$, um número primo em $\mathbb{Z}$. O resultado segue ao aplicarmos a Proposição 10. $\square$

Proposição 11. *3 é um associado de λ^2.*

Demonstração. $\lambda^2 = 1 - 2\rho + \rho^2 = -2\rho + (1 + \rho^2) = -3\rho.$ $\square$

Lema 12. *Ao dividirmos um inteiro de $\mathbb{Z}[\rho]$ por λ os possíveis restos são 0, 1 ou -1.*

Demonstração. Da definição de ρ obtemos

$$(1 - \rho)(1 - \rho^2) = 1 - \rho^2 - \rho + \rho^3 = 1 + (-\rho^2 - \rho) + 1 = 1 + 1 + 1 = 3$$

o qual implica em $\lambda \mid 3$.

Qualquer inteiro quando dividido por 3 deixa resto 0, 1 ou 2. Porém, como $3 \equiv 0 \pmod 3$ $\Rightarrow 2 \equiv -1 \pmod 3$, podemos dizer que qualquer inteiro, quando dividido por 3, deixa resto 0, 1 ou -1.

Seja $a + b\rho$ um inteiro qualquer, temos

$$\frac{a + b\rho}{\lambda} \Rightarrow \frac{a + b\rho}{1 - \rho}. \tag{3.7}$$

Multiplicando numerador e denominador pelo inteiro $(1-\rho^2)$ encontramos

$$\frac{(a+b\rho)(1-\rho^2)}{(1-\rho)(1-\rho^2)} \Rightarrow \frac{(a+b\rho)(1-\rho^2)}{3}. \tag{3.8}$$

E, assim, teremos um inteiro $(a+b\rho)(1-\rho^2)$ qualquer que dividido por 3, tem resto 0, 1 ou -1. □

Lema 13. *Os números* $\pm(1-\rho)$, $\pm(1-\rho^2)$, *e* $\pm\rho(1-\rho)$ *são todos associados de* λ.

Demonstração. É suficiente observar que

$$\pm(1-\rho) = \pm\lambda, \qquad \pm(1-\rho^2) = \mp\lambda\rho^2, \qquad \pm\rho(1-\rho) = \pm\lambda\rho. \qquad \square$$

CAPÍTULO 4

EQUAÇÕES DIOFANTINAS

Este capítulo é dedicado ao estudo de alguns problemas Diofantinos. Primeiramente são considerados problemas determinados por equações lineares em duas e três variáveis. Algumas destas situações são de fato incluídas no caderno do oitavo ano do aluno do Estado de São Paulo. Posteriormente são considerados alguns problemas não lineares correspondentes aos casos $n = 2, 3$ e 4 do Último Teorema de Fermat. A demonstração do teorema para $n = 4$ é relativamente simples, mas é suficiente para demonstrar o teorema para qualquer inteiro par maior ou igual do que 4. O argumento para o caso $n = 3$ é o mais elaborado e utiliza a estrutura de $\mathbb{Z}[\rho]$ apresentada no Capítulo 3. O primeiro passo neste sentido consiste em observar que o número $x^3 + y^3$ pode ser fatorado em $\mathbb{Z}[\rho]$ de maneira única como

$$(x + y)(x + \rho y)(x + \rho^2 y).$$

A unicidade desta fatoração é garantida pelo Teorema 17. A prova do caso $n = 3$ foi desenvolvida por Euler durante um período de 27 anos, desde 1753 até 1770. A prova do Euler, incompleta em certo ponto, foi terminada por Legendre. A demonstração apresentada aqui segue o material relativo ao Teorema 227 em Hardy e Wright (2008).

4.1 Equações lineares

Nesta seção veremos apenas dois tipos de equações diofantinas lineares: as que possuem duas e três variáveis. Nesta seção, a palavra inteiro será utilizada apenas para os elementos do anel $\mathbb{Z}$.

4.1.1 Equações lineares em duas variáveis

Consideramos como primeiro exemplo de um problema diofantino as equações do tipo $ax + by = c$, com $a, b, c \in \mathbb{Z}$, em que, as soluções para x e y são inteiras.

Proposição 12. *Sejam a, b e c números inteiros não nulos. A equação $ax + by = c$ admite soluções inteiras para x e y se, e somente se, $(a, b) \mid c$.*

Demonstração. Seja $(a, b) = d$, logo, como $d \mid a$ e $d \mid b$, existem r e s inteiros tais que, $a = dr$ e $b = ds$. Substituindo em $ax + by = c$, temos $drx + dsy = c$, portanto $d(rx + sy) = c$. Dessa forma concluimos que $d \mid c$.

Seja $d = (a,b)$ e suponho que $d \mid c$. Então $c = dt$ para algum $t \in \mathbb{Z}$, mas existem inteiros r e s tais que $ar + bs = d$. Logo $art + bst = dt$, ou seja, $x_0 = rt$ e $y_0 = st$ é uma solução de $ax + by = c$. □

Podemos agora dividir $ax + by = c$ por (a,b), em que, $r = \frac{a}{d}$, $s = \frac{b}{d}$, $t = \frac{c}{d}$, obtendo assim $rx + sy = t$. Observa-se que $(r,s) = 1$ pelo Lema 3 e $1 \mid t$, logo $rx + sy = t$ tem soluções inteiras para x e y, pela Proposição 12. Existindo soluções inteiras que a satisfaçam, podemos sempre dividir $ax + by = c$ por (a,b), encontrando assim $a_1x + b_1y = c_1$ em que $(a_1,b_1) = 1$ ainda pelo Lema 3. Podemos, então, nos restringir a equações da forma $ax + by = c$ em que $(a,b) = 1$.

Teorema 18. *Dada a equação $ax + by = c$, em que a, b e c são inteiros, a e b ambos não nulos e $(a,b) = 1$, considere que x_0, y_0 é uma de suas soluções. Então, as soluções inteiras para x, y são da forma*

$$x = x_0 + bt, \qquad y = y_0 - at$$

com t sendo qualquer número inteiro.

Demonstração. Como x_0, y_0 é uma das soluções, temos a seguinte igualdade

$$ax + by = ax_0 + by_0.$$

Também temos

$$ax - ax_0 = by_0 - by \Rightarrow a(x - x_0) = b(y_0 - y),$$

em que os dois membros da igualdade continuam sendo inteiros. Dividindo a última expressão por b temos

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

Como $(a,b) = 1$, temos que $b = 1$ ou $b \nmid a$, do contrário, se $b \mid a$, teríamos $(a,b) = b$. Lembrando que $(y_0 - y)$ é um número inteiro, b deve dividir $a(x - x_0)$, assim, se $b = 1$ ele divide qualquer inteiro e, se $b \nmid a$, então $b \mid (x - x_0)$. Assim, concluimos que b é um divisor de $(x - x_0)$, seguindo o exposto na Seção 2.1, temos que $(x - x_0) = tb$, com $t \in \mathbb{Z}$, seguindo que

$$x = x_0 + tb.$$

Por outro lado, se $(x - x_0) = tb$, podemos substituir em $a(x - x_0) = b(y_0 - y)$ obtendo $atb = b(y_0 - y)$. Dividindo por b, temos $at = y_0 - y$, logo

$$y = y_0 - at.$$ □

4.1.2 Equações lineares em três variáveis

Uma equação linear com três variáveis é da forma

$$ax + by + cz = d, \qquad \text{para} \quad a,b,c \in \mathbb{Z} \setminus \{0\},\ d \in \mathbb{Z}.$$

Teorema 19. *A equação $ax + by + cz = d$ com a, b e c inteiros não nulos e d inteiro, possui soluções inteiras em x, y e z se, e somente se, $(a,b,c) \mid d$, ou seja, existe algum inteiro q tal que $d = (a,b,c)q$.*

Demonstração. Considere $(a,b,c) = k$ e $(a,b) = k_1$, analisando primeiro (a,b) existem w_1 e w_2 inteiros tais que $aw_1 + bw_2 = k_1$ e, dessa forma, $(a,b,c) = ((a,b),c) = (k_1,c) = k$, logo existem w e z_0 tais que $k_1 w + cz_0 = k$. Substituindo k_1 obtemos

$$(aw_1 + bw_2)w + cz_0 = k \Rightarrow aw_1 w + bw_2 w + cz_0 = k.$$

Trocando k por (a,b,c) e multiplicando os dois lados por um inteiro q, encontramos

$$a(w_1 wq) + b(w_2 wq) + c(z_0 q) = (a,b,c)q = d,$$

nas quais $(w_1 wq)$, $(w_2 wq)$ e $(z_0 q)$ são soluções particulares de x, y e z respectivamente. □

Teorema 20. *A equação $ax + by + cz = d$, em que $(a,b,c) \mid d$, com a, b e c inteiros não nulos e d inteiro, possui soluções*

$$x = x_0(k_0 - cq) + bt, \quad y = y_0(k_0 - cq) - at, \quad e \quad z = (a,b)q + r_0,$$

sendo k_0, r_0, q e t inteiros.

Demonstração. Podemos reescrever a equação $ax + by + cz = d$ como

$$ax + by = d - cz.$$

Pela Proposição 12 sabemos que existem soluções inteiras para x e y se, e somente se, $(a,b) \mid (d - cz)$. Pela divisão Euclidiana sabemos que z pode ser escrito como $(a,b)q + r$, sendo r e q inteiros, com $0 \leq r < (a,b)$ e, assim, obtemos

$$\begin{aligned} d - cz &= d - c((a,b)q + r) \\ &= (d - cr) - cq(a,b). \end{aligned}$$

Observamos agora que $(a,b) \mid d - cz = (d - cr) - cq(a,b)$, o que implica em $(a,b) \mid (d - cr)$. Existe, portanto, um k inteiro tal que $(d - cr) = (a,b)k$, e também

$$(a,b)k + cr = d.$$

Esta última equação admite soluções inteiras para k e r, sendo $((a,b),c) = (a,b,c)$ que, por hipótese, divide d. Dessa forma podemos encontrar algum k_0 e r_0 tal que $(a,b)k_0 + cr_0 =$

$d \Rightarrow (d - cr_0) = (a,b)k_0$. Agora substituimos k e r por k_0 e r_0, respectivamente, e obtemos as observações

$$\begin{aligned} ax + by &= d - cz \\ &= d - c((a,b)q + r_0) \\ &= (d - cr_0) - cq(a,b) \\ &= (a,b)(k_0 - cq). \end{aligned}$$

Neste momento, basta encontrar inteiros x_0 e y_0 tais que $ax_0 + by_0 = (a,b)$ e multiplicar os dois lados dessa equação por $(k_0 - cq)$ para obtermos a equação

$$a(x_0(k_0 - cq)) + b(y_0(k_0 - cq)) = (a,b)(k_0 - cq).$$

Observe que essa possui soluções inteiras, pois $(a,b) \mid (a,b)(k_0 - cq)$ e, pelo Teorema 18, temos que

$$x = x_0(k_o - cq) + bt \text{ e } y = y_0(k_0 - cq) - at, \text{ com } t \in \mathbb{Z}.$$

Como foi dito no início da demonstração, $z = (a,b)q + r_0$, provando, assim, o Teorema 20. □

Exemplo 5. Vamos encontrar agora as soluções gerais para a equação $4x + 5y + 6z = 10$, lembrando que $(4,5,6) \mid 10$.

Primeiramente a reescrevemos na forma $4x + 5y = 10 - 6z$, observa-se que há solução para qualquer $z \in \mathbb{Z}$ já que $(4,5) \mid 10 - 6z$. Como $(4,5) = 1$, encontraremos agora algum x_0 e y_0 tal que $4x_0 + 5y_0 = 1$, o que é simples, usaremos $x_0 = -1$ e $y_0 = 1$. Em seguida, multiplicamos os dois lados dessa última equação por $(10 - 6z)$ obtendo

$$4(-10 + 6z) + 5(10 - 6z) = 1(10 - 6z).$$

Logo, pelo Teorema 18, temos que $x = -10 + 6z + 5t$ e $y = 10 - 6z - 4t$, com z e t sendo inteiros. Vamos utilizar, apenas para testar essa solução, $z = 7$ e $t = -1$. Dessa forma, temos

$$\begin{aligned} x &= -10 + 6(7) + 5(-1) = 27, \\ y &= 10 - 6(7) - 4(-1) = -28 \text{ e} \\ z &= 7. \end{aligned}$$

Substituindo em $4x + 5y + 6z = 10$ encontramos

$$4(27) + 5(-28) + 6(7) = 108 - 140 + 42 = 10.$$

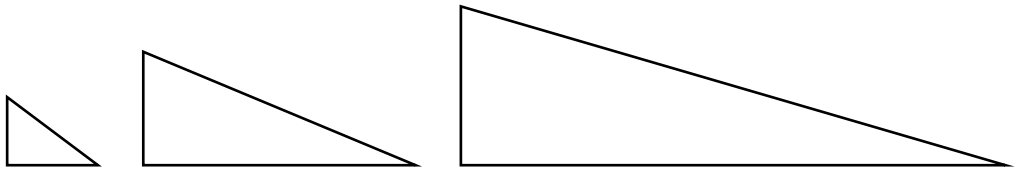
4.2 Equações não lineares

4.2.1 A equação $x^2 + y^2 = z^2$

Nesta seção apresentamos a forma genérica de todas as soluções em $\mathbb{Z}$ para a equação Pitagórica $x^2 + y^2 = z^2$. A soluções (x,y,z) desta equação são conhecidas como ternas Pitagó-

ricas. Para exemplificar, a Figura 4 apresenta três triângulos com lados de comprimentos dados pelas ternas $(3,4,5)$, $(5,12,13)$ e $(7,24,25)$.

Figura 4 – Três ternas Pitagóricas



Fonte – Realizada pelo autor.

Teorema 21. *Sejam x, y e z números inteiros. As soluções da equação*

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

são dadas por

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2$$

onde a e b são dois inteiros. Existe uma correspondência um a um entre os diferentes valores de a, b e os diferentes valores de x, y, z.

Demonstração. Seja d o máximo divisor comum entre x e y, isto é, d é o maior inteiro tal que

$$\frac{x}{d} = r \Rightarrow x^2 = d^2 r^2 \quad \text{e} \quad \frac{y}{d} = s \Rightarrow y^2 = d^2 s^2,$$

com r e $s \in \mathbb{Z}$. Observamos que $d \mid x$ e $d \mid y$ e isso implica em $d \mid z$. Assim, existe algum inteiro t tal que $\frac{z^2}{d^2} = t^2$. Dividindo $x^2 + y^2 = z^2$ por d^2 teremos

$$r^2 + s^2 = t^2. \tag{4.1}$$

Como $(x, y) = d$, pelo Lema 5, temos que $(r, s) = 1$ e, pelo Lema 6, $(r^2, s^2) = 1$.

Devemos estudar a paridade de r e s, o qual leva a consideração dos seguintes casos.

CASO 1: Suponhamos que ambos r e s sejam números pares. Um número par ao quadrado somado a outro par ao quadrado resulta em um número par, logo $\text{mdc}(r, s, t) \geq 2$, porém, segundo (4.1) este último é impossível. Concluímos assim que r e s não são ambos pares.

CASO 2: r e s são ambos ímpares. Neste caso $r = (2m + 1)$ e $s = (2n + 1)$, com m e $n \in \mathbb{N}$

$$r^2 = (2m+1)^2 = (4m^2 + 4m + 1) \equiv 1 \pmod 4$$
$$s^2 = (2n+1)^2 = (4n^2 + 4n + 1) \equiv 1 \pmod 4$$

e assim,

$$t^2 = r^2 + s^2 \equiv 2 \pmod 4,$$

mas isto é um absurdo pois, t^2 é um quadrado perfeito e todo quadrado perfeito, quando dividido por 4, deixa resto 1 ou 0, por exemplo $(2g)^2 = 4g^2 \equiv 0 \pmod 4$ e $(2h+1)^2 = (4h^2+4h+1) \equiv 1 \pmod 4$, com $g,h \in \mathbb{Z}$. Ambos r e s não são, portanto, ímpares.

CASO 3: Vamos assumir, sem perda de generalidade, que r é ímpar e s é par. Logo t^2 também é ímpar, pois r^2+s^2 é ímpar. Por outro lado, é possível reescrevermos (4.1) como

$$r^2 = t^2 - s^2 = (t+s)(t-s), \tag{4.2}$$

o qual permite deduzir o mdc de $(t+s)$ e $(t-s)$. Supondo que o $\text{mdc}(s,t) = c$, com $c \in \mathbb{Z}$, temos que $c \mid t$ e $c \mid s$, assim $c^2 \mid t^2$, $c^2 \mid s^2$ e $c^2 \mid (t^2-s^2) \Rightarrow c^2 \mid r^2$, porém, como o $(r,s) = 1$, $c^2 = 1$, logo o $\text{mdc}(s,t) = 1$. Suponhamos agora que $((t+s),(t-s)) = f$, com $f \in \mathbb{Z}$, temos que $f \mid (t+s)$ e $f \mid (t-s)$, logo $f \mid [(t+s)+(t-s)] \Rightarrow f \mid 2t$ e $f \mid [(t+s)-(t-s)] \Rightarrow f \mid 2s$. Assim $f \mid (2s,2t) = 2(s,t) = 2\cdot 1$. Concluímos, então, como 2 é primo, que f poderia ser 2 ou 1. Como t é ímpar e s é par temos que $(t+s)$ e $(t-s)$ são ímpares. Por outro lado, como $f \mid (t+s)$, um número ímpar, concluimos que $f = 1$, chegando à conclusão de que o $((t+s)),(t-s)) = 1$. Observamos agora, pelo Teorema 7, que $(t+s)$ e $(t-s)$ são quadrados perfeitos, já que seu produto em (4.2) resulta em um quadrado perfeito. Assim, sejam

$$(t+s) = a^2 \qquad \text{e} \qquad (t-s) = b^2,$$

com a e b inteiros, isolamos t e s e substituímos em (4.2), encontrando

$$r^2 = \Big(\frac{a^2+b^2}{2}\Big)^2 - \Big(\frac{a^2-b^2}{2}\Big)^2.$$

Desenvolvendo essa expressão, chegamos a $r^2 = a^2b^2$ e assim $r = ab$. As soluções inteiras para $x^2+y^2 = z^2$ são da forma

$$(dr)^2 + (ds)^2 = (dt)^2 \Rightarrow \big[d(ab)\big]^2 + \Big[d\Big(\frac{a^2-b^2}{2}\Big)\Big]^2 = \Big[d\Big(\frac{a^2+b^2}{2}\Big)\Big]^2.$$

Multiplicando por 4 e dividindo por d^2 temos $(2ab)^2 + (a^2-b^2)^2 = (a^2+b^2)^2$ e, assim, concluímos que $x = 2ab$, $y = a^2-b^2$ e $z = a^2+b^2$. □

Apresentamos agora a forma genérica de todas as soluções inteiras para o caso particular da equação $x^2+y^2 = z^2$, em que x e y são coprimos, ou seja, $(x,y) = 1$.

Corolário 1. *Sejam x, y e z números inteiros com o $(x,y) = 1$, então as soluções da equação*

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

são dadas por

$$x = 2ab, \quad y = a^2-b^2, \quad z = a^2+b^2$$

onde a e b são dois inteiros, com $mdc(a,b) = 1$ e paridades opostas. Existe uma correspondência um a um entre os diferentes valores de a, b e os diferentes valores de x, y, z.

Demonstração. Do Teorema 21 temos que

$$x = 2ab, \quad y = a^2 - b^2 \quad \text{e} \quad z = a^2 + b^2.$$

Suponha que exista um máximo divisor comum c, diferente de 1, entre a e b, logo $a = cg$, $b = ch$. Assim,

$$x = 2cgch = 2c^2gh \quad \text{e} \quad y = (cg)^2 - (ch)^2 = c^2(g^2 - h^2).$$

Dessa forma, $c^2|x$ e $c^2|y$, o que é absurdo, pois $(x, y) = 1$. Concluimos que $(a, b) = 1$. O fato de a e b serem de paridade oposta é demonstrado seguindo o mesmo argumento utilizado para mostrar que r e s possuem paridade oposta no Teorema 21. □

4.2.2 A equação $x^4 + y^4 = z^4$

A procura de soluções inteiras não nulas para $x^4 + y^4 = z^4$ é relativamente simples e a demonstração decorre do que foi estudado no Teorema 21. Observamos que se o Último Teorema de Fermat é válido para algum n, então também vale para qualquer múltiplo de n, pois $x^{nk} + y^{nk} = z^{nk}$ é de fato igual a

$$(x^k)^n + (y^k)^n = (z^k)^n.$$

A demonstração do caso $n = 4$ é suficiente para mostrarmos que o teorema vale para qualquer n par tal que $n > 2$.

Teorema 22. *A equação*

$$x^4 + y^4 = z^4$$

não possui soluções inteiras não nulas em x, y e z.

Demonstração. Seja d o máximo divisor comum entre x e y, isto é, d é o maior inteiro tal que

$$\frac{x}{d} = r \Rightarrow x^4 = d^4r^4 \quad \text{e} \quad \frac{y}{d} = s \Rightarrow y^4 = d^4s^4,$$

com r e s sendo inteiros. O fato de que $d \mid x$ e $d \mid y$ implica em $d \mid z$ e, assim, existe algum inteiro t tal que $\frac{z^4}{d^4} = t^4$. Dividindo $x^4 + y^4 = z^4$ por d^4 teremos

$$r^4 + s^4 = t^4. \tag{4.3}$$

Como $(x, y) = d$, pelo Lema 5, segue que $(r, s) = 1$ e, usando o Lema 6, $(r^4, s^4) = 1$.

Substituindo t^2 por u temos

$$(r^2)^2 + (s^2)^2 = u^2, \qquad \text{com} \quad |r| > 0, |s| > 0 \text{ e } |u| > 0.$$

Dessa forma, $|u|$ deve ser o menor inteiro possível para que essa equação tenha solução já que o $(r,s) = 1$, pois, caso contrário, seria possível dividir e reduzir a equação novamente. Pelo Corolário 1 temos que

$$r^2 = 2ab, \quad s^2 = a^2 - b^2 \quad \text{e} \quad u = a^2 + b^2$$

com a e b tendo paridade oposta e $(a,b) = 1$.

Devemos analisar a paridade de a e b. Suponhamos, sem perda de generalidade, que b é ímpar, ou seja $b = 2k+1$, logo a é da forma $a = 2k'$, com k e k' inteiros, e

$$s^2 = (2k')^2 - (2k+1)^2 = 4k'^2 - 4k^2 - 4k - 1,$$

portanto $s^2 \equiv -1 \pmod 4$ o que é absurdo, já que quadrados só deixam resto 1 ou 0 quando divididos por 4. Concluímos que b é par e pode ser escrito como $b = 2c$, com $c \in \mathbb{Z}$. Assim,

$$r^2 = 4ac \quad \Rightarrow \quad \left(\frac{r}{2}\right)^2 = ac$$

e, como o $(a,b) = 1$ pelo Corolário 1, temos que $(a,c) = 1$ implicando que a e c devem ser quadrados. Escrevemos $a = g^2$, $c = f^2$, com g e f inteiros, logo

$$s^2 = a^2 - b^2 = (g^2)^2 - (2f^2)^2 \quad \Rightarrow \quad (2f^2)^2 + s^2 = (g^2)^2.$$

Novamente pelo Colorário 1, aplicado a última equação, $2f^2 = 2pv$, $s = p^2 - v^2$ e $g^2 = p^2 + v^2$, com $(p,v) = 1$. Pelo Teorema 7 podemos escrever $p = m^2$ e $v = n^2$, e como $f^2 = pv$, segue que

$$g^2 = p^2 + v^2 = (m^2)^2 + (n^2)^2 \quad \Rightarrow \quad m^4 + n^4 = g^2,$$

mas, $g \leq g^2 = a < a^2 + b^2 = u$ e, assim, $|u|$ não é o menor inteiro para $r^4 + s^4 = u^2$, o que não é possível. Provamos, então, por uma contradição que $r^4 + s^4 = t^4$ não possui soluções inteiras não nulas, e isso implica que $d^4(r^4 + s^4) = d^4t^4 \Rightarrow x^4 + y^4 = z^4$ também não tem. □

4.2.3 A equação $x^3 + y^3 = z^3$

Um primeiro passo para provarmos que a equação (1.4) não possui soluções x, y, z inteiras quando $n = 3$, consiste em escrevermos

$$(x+y)(y+\rho y)(x+\rho^2 y) = z^3,$$

o qual resulta ao aplicarmos o Lema 10 e o Teorema 17. Posteriormente deve ser analisada a estrutura de cada um dos fatores envolvendo o número ρ em $\mathbb{Z}[\rho]$. Observamos que se o Último Teorema de Fermat no caso $n = 3$ não possui soluções em $\mathbb{Z}[\rho]$, então, também não existem soluções nos inteiros racionais, pois $\mathbb{Z} \subset \mathbb{Z}[\rho]$. O seguinte teorema corresponde ao Teorema 227 em Hardy e Wright (2008).

Teorema 23. *Sejam ξ, η e ζ inteiros não nulos em $\mathbb{Z}[\rho]$. A equação*

$$\xi^3 + \eta^3 + \zeta^3 = 0,$$

não possui soluções inteiras em $\mathbb{Z}[\rho]$. Em particular, não existem soluções inteiras para $x^3 + y^3 = z^3$, exceto as soluções triviais nas quais um dos números x, y, z é 0.

O Teorema 23 será provado em vários passos seguindo os Teoremas 24-27.

Teorema 24. *Sejam $\lambda = 1-\rho$, o número primo definido no Lema 11, e $\omega \in \mathbb{Q}(\rho)$. Se $\lambda \nmid \omega$ então*

$$\omega^3 \equiv \pm 1 \ (mod\ \lambda^4),$$

Demonstração. Seguindo o Lema 12, ao dividirmos um número por λ os restos possíveis são 0 quando o número for divisível por λ ou $\pm$ 1 no caso contrário. Como $\lambda \nmid \omega$ temos que

$$\omega \equiv \pm 1 \ (\text{mod } \lambda).$$

Considerando $\pm\omega = \alpha$, temos $\alpha \equiv 1 \ (\text{mod } \lambda)$ e, assim, $\lambda \mid (\alpha - 1)$. Dessa forma, existe algum $\beta \in \mathbb{Z}[\rho]$ tal que

$$\alpha = \lambda\beta + 1.$$

Este último é consequência da Proposição 7.

Observamos agora que $\pm(\omega^3 \mp 1) = \alpha^3 - 1$, pois $\pm\omega = \alpha \Rightarrow \pm\omega^3 - 1 = \alpha^3 - 1$. Dessa forma, utilizando o Lema 10 obtemos

$$\begin{aligned}
\pm(\omega^3 \mp 1) = \alpha^3 - 1 &= (\alpha-1)(\alpha-\rho)\big(\alpha-\rho^2\big) \\
&= (\alpha-1)(\alpha-1+1-\rho)\big(\alpha-1+1-\rho^2\big) \\
&= \lambda\beta(\lambda\beta+1-\rho)(\lambda\beta+1-\rho^2) \\
&= \lambda\beta\big(\lambda\beta+(1-\rho)\big)(\lambda\beta+(1-\rho)(1+\rho)) \\
&= \lambda\beta(\lambda\beta+\lambda)(\lambda\beta+\lambda(1+\rho)) \\
&= \lambda^3\beta(\beta+1)(\beta-\rho^2),
\end{aligned}$$

lembrando que $\rho^2 + \rho + 1 = 0$.

Como $(\rho-1)/\lambda = -1$, da Proposição 6 obtemos

$$\rho \equiv 1 \ (\text{mod } \lambda),$$

e das Proposições 8 e 9 encontramos

$$\begin{aligned}
-\rho^2 \equiv -1 \ (\text{mod } \lambda) &\Rightarrow (\beta-\rho^2) \equiv (\beta-1) \ (\text{mod } \lambda) \\
&\Rightarrow (\beta+1)(\beta-\rho^2) \equiv (\beta+1)(\beta-1) \ (\text{mod } \lambda) \\
&\Rightarrow \beta(\beta+1)(\beta-\rho^2) \equiv \beta(\beta+1)(\beta-1) \ (\text{mod } \lambda). \qquad (4.4)
\end{aligned}$$

Do Lema 12, o resto da divisão de qualquer inteiro em $\mathbb{Z}[\rho]$ por λ é 0, 1 ou -1 e, com isso, necessariamente algum dos inteiros β, $(\beta+1)$ ou $(\beta-1)$ terá resto 0 quando dividido por λ, isto é, $\lambda \mid \beta(\beta+1)(\beta-1)$ o que implica que $\lambda^4 \mid \lambda^3\beta(\beta+1)(\beta-1)$. Devido a (4.4) observe que λ também divide $\beta(\beta+1)(\beta-\rho^2)$ implicando que $\lambda^4 \mid \lambda^3\beta(\beta+1)(\beta-\rho^2)$. Com isso podemos afirmar que

$$\begin{aligned}\lambda^3\beta(\beta+1)(\beta-\rho^2) \equiv 0 \pmod{\lambda^4} &\Rightarrow \pm(\omega^3 \mp 1) \equiv 0 \pmod{\lambda^4} \\ &\Rightarrow \pm\omega^3 - 1 \equiv 0 \pmod{\lambda^4} \\ &\Rightarrow \pm\omega^3 \equiv 1 \pmod{\lambda^4} \Rightarrow \omega^3 \equiv \pm 1 \pmod{\lambda^4}.\end{aligned}$$

□

Teorema 25. *Sejam α, β e γ tais que $\alpha^3+\beta^3+\gamma^3 = 0$. Um dos números α, β ou γ é divisível por λ.*

Demonstração. Vamos supor o contrário, ou seja, que $\lambda \nmid \alpha$, $\lambda \nmid \beta$ e $\lambda \nmid \gamma$. Dessa forma, do Teorema 24, temos $\alpha^3 \equiv \pm 1 \pmod{\lambda^4}$, $\beta^3 \equiv \pm 1 \pmod{\lambda^4}$ e $\gamma^3 \equiv \pm 1 \pmod{\lambda^4}$, ou, pela Proposição 8, que

$$\alpha^3+\beta^3+\gamma^3 = 0 \equiv \pm 1 \pm 1 \pm 1 \pmod{\lambda^4}.$$

Chegamos, assim, em dois casos.

Caso 1: Se forem apenas dois sinais iguais, temos $0 \equiv \pm 1 \pmod{\lambda^4}$, ou seja, $\lambda^4 \mid \pm 1$. Mas como λ não é uma unidade, ou seja, $\lambda \nmid \pm 1$, $\lambda^4 \nmid 1$ e logo $\lambda^4 \nmid \pm 1$.

Caso 2: Se os sinais forem todos iguais, temos $0 \equiv \pm 3 \pmod{\lambda^4}$, ou seja, $\lambda^4 \mid \pm 3$. Vimos na Proposição 11 que $\lambda^2 = -3\rho$, então $\lambda^4 = 9\rho^2$. Analisando este caso

$$\lambda^4 \mid \pm 3 \Rightarrow \qquad 9\rho^2 \mid \pm 3 \Rightarrow \qquad 3\rho^2 \mid \pm 1.$$

Isso é uma contradição, pois $3 \nmid \pm 1$. Mostramos, assim, que é impossível λ não dividir nenhum de α, β ou γ e assim pelo menos um deles deve ser divisível por λ.

Suponhamos que $\lambda \mid \gamma$. Seja θ tal que $(\lambda, \theta) = 1$ e

$$\gamma = \lambda^n\theta$$

com $n \in \mathbb{Z}$ e $n \geq 1$, como vimos no Capítulo 2. Temos agora

$$\alpha^3+\beta^3+\lambda^{3n}\theta^3 = 0$$

com $(\alpha, \beta) = 1$, $n \geq 1$, $\lambda \nmid \alpha$, $\lambda \nmid \beta$ e $\lambda \nmid \theta$. □

Teorema 26. *Se α, β e θ satisfazem a equação, então $n \geq 2$.*

Demonstração. Pelos Teoremas 24 e 25, sendo ϵ uma unidade, temos

$$-\epsilon\lambda^{3n}\theta^3 = \alpha^3 + \beta^3 \equiv \pm 1 \pm 1 \pmod{\lambda^4}$$

Se os sinais dos dois números ± 1 à direita da congruência são iguais, temos $-\epsilon\lambda^{3n}\theta^3 \equiv \pm 2 \pmod{\lambda^4}$, o que é impossível, pois $\lambda \nmid 2$. Logo os sinais das quantidades ± 1 são diferentes, isto é,

$$-\epsilon\lambda^{3n}\theta^3 \equiv 0 \pmod{\lambda^4}.$$

Dessa forma, $\lambda^4 \mid \lambda^{3n}\theta^3$ e, como $\lambda \nmid \theta$, sobra a opção em que

$$\lambda^4 \mid \lambda^{3n}. \tag{4.5}$$

Concluímos que $n \geq 2$. □

Teorema 27. *Se*

$$\alpha^3 + \beta^3 + \epsilon\lambda^{3n}\theta^3 = 0$$

é possível para $n = m > 1$, com m inteiro, então também é possível para $n = m - 1$.

Este teorema, após sua demonstração, entrará em contradição com o Teorema 26 que diz que $n \geq 2$, já que se $n = m - 1$, n poderá ser um inteiro menor que 2. Assim, provaremos imediatamente o Teorema 23, pois se $n = 1$, um número menor que 2, λ^{3n} não será divisível por λ^4 em 4.5, contradizendo o argumento do Teorema 25.

Demonstração do Teorema 27. Por hipótese $-\epsilon^{3m}\theta^3 = \alpha^3 + \beta^3$, logo

$$-\epsilon^{3m}\theta^3 = (\alpha + \beta)(\alpha + \beta\rho)(\alpha + \beta\rho^2).$$

Consideramos primeiro as diferenças entre os fatores do lado direito da expressão à direita da última igualdade. Para a diferença entre o primeiro e o segundo fator temos

$$(\alpha + \beta) - (\alpha + \beta\rho) = \beta(1 - \rho) = \beta\rho,$$

entre o primeiro e o terceiro

$$(\alpha + \beta) - (\alpha + \beta\rho^2) = \beta(1 - \rho^2) = \beta(1 + \rho)(1 - \rho) = \beta\rho^2\lambda,$$

e entre o segundo e o terceiro

$$(\alpha + \beta\rho) - (\alpha + \beta\rho^2) = \beta\rho(1 - \rho) = \beta\rho\lambda.$$

Os números $\beta\lambda$, $\beta\rho^2\lambda$ e $\beta\rho\lambda$ são associados de $\beta\lambda$. Observe que cada um deles é divisível por λ, mas não por λ^2. Dessa forma, os três fatores da direita em (3.5) são divisíveis por λ. Como $m \geq 2$, segue que $3m > 3$ e um desses fatores deve ser divisível por λ^2 e os outros dois por λ,

porém, não por λ^2, devido as suas diferenças. Suponhamos então que $(\alpha+\beta)$ seja divisível por λ^2, assim temos

$$(\alpha+\beta)=\lambda^{3m-2}k_1, \qquad (\alpha+\beta\rho)=\lambda k_2, \qquad (\alpha+\beta\rho^2)=\lambda k_3,$$

e os números k_1, k_2 e k_3 não são divisíveis por λ. Determinamos a seguir o valor dos números (k_1,k_2), (k_1,k_3) e (k_2,k_3). Se $\delta \mid k_2$ e $\delta \mid k_3$, então δ divide a diferença k_2-k_3. Por outro lado,

$$\lambda k_2-\lambda k_3=(\alpha+\beta)-(\alpha+\beta\rho^2)$$

e, portanto,

$$\lambda(k_2-k_3)=\beta\rho(1-\rho)\Rightarrow k_2-k_3=\beta\rho.$$

Substituindo em $(\alpha+\beta\rho)=\lambda k_2$ temos

$$\alpha+(k_2-k_3)=\lambda k_2 \;\Rightarrow\; \alpha=(1-\rho)k_2-k_2+k_3 \;\Rightarrow\; \alpha=k_3-\rho k_2,$$

e, multiplicando por ρ

$$\rho k_3-\rho^2 k_2=\rho\alpha.$$

Assim δ divide α e β, mas $(\alpha,\beta)=1$ e, logo, $\delta=1$. Dessa forma, lembrando que $\delta \mid k_2$ e $\delta \mid k_3$, como $\delta=1$ temos $(k_2,k_3)=1$. De maneira similar conclui-se que $(k_1,k_3)=1$ e $(k_1,k_2)=1$.

Fazendo as substituições em (3.5) temos

$$-\epsilon\theta^3=k_1k_2k_3.$$

Como já sabemos, $(k_1,k_2)=(k_1,k_3)=(k_2,k_3)=1$ e o produto $k_1k_2k_3$ é igual a $-\epsilon\theta^3$, um cubo. Logo, pelo Teorema 7, esses três números também são cubos. Assim podemos usar $k_1=\tau^3$, $k_2=\phi^3$, $k_3=\psi^3$ e obtemos $(\alpha+\beta)=\epsilon_1\lambda^{3m-2}\tau^3$, $(\alpha+\beta\rho)=\epsilon_2\lambda\phi^3$ e $(\alpha+\beta\rho^2)=\epsilon_3\psi^3$, cujos τ, ϕ e ψ não possuem fatores em comum e não são divisíveis por λ.

Lembrando que $(\rho^2+\rho+1)=0$ e multiplicando por $(\alpha+\beta)$ obtemos

$$\alpha\rho^2+\alpha\rho+\alpha+\beta\rho^2+\beta\rho+\beta=0,$$

portanto,

$$(\alpha+\beta)+\rho(\alpha+\beta\rho)+\alpha\rho^2+\beta\rho=0.$$

Multiplicando $\alpha\rho^2+\beta\rho$ por ρ^3, lembrando que $\rho^3=1$, obtemos $\alpha\rho^5+\beta\rho^4\Rightarrow\rho^2(\alpha+\beta\rho^2)$. Logo

$$(\alpha+\beta)+\rho(\alpha+\beta\rho)+\rho^2(\alpha+\beta\rho^2)=0$$

o qual implica em

$$\epsilon_1\lambda^{3m-2}\tau^3+\rho\epsilon_2\lambda\phi^3+\rho^2\epsilon_3\lambda\psi^3=0.$$

Dividindo por $\lambda\rho\epsilon_2$, temos

$$\epsilon_5\lambda^{3(m-1)}\tau^3+\phi^3+\epsilon_4\psi^3=0, \tag{4.6}$$

em que

$$\epsilon_5 = \frac{\epsilon_1}{\epsilon_2 \rho} \qquad \text{e} \qquad \epsilon_4 = \frac{\epsilon_3 \rho}{\epsilon_2}$$

são unidades, lembrando que ρ é uma unidade em $\mathbb{Z}[\rho]$. Como $m \geq 2$ temos $\epsilon_5 \lambda^{3(m-1)} \tau^3 \equiv 0 \pmod{\lambda^2}$ e

$$0 = \phi^3 + \epsilon_4 \psi^3 \equiv 0 \pmod{\lambda^2}. \tag{4.7}$$

Mas $\lambda \nmid \phi$ e $\lambda \nmid \psi$ e, assim, pelo Teorema 24

$$\phi^3 \equiv \pm 1 \pmod{\lambda^4}$$

e

$$\psi^3 \equiv \pm 1 \pmod{\lambda^4},$$

então $\phi^3 + \epsilon_4 \psi^3 \equiv \pm 1 \pm \epsilon_4 \pmod{\lambda^4}$.

Como ϵ_4 é uma unidade em $\mathbb{Z}[\rho]$, ele é igual a ± 1, $\pm\rho$ ou $\pm\rho^2$. Vamos analisar as opções. Se $\epsilon_4 = \pm\rho$, temos $\pm 1 \pm 1 \equiv 0 \pmod{\lambda^4}$. Os sinais não podem ser iguais, pois $\lambda \nmid 1 + \rho$ e $\lambda \nmid -1 - \rho$. Logo ϵ_4 não é $\pm\rho$. De forma similar observamos que ϵ_4 também não é $\pm\rho^2$. Concluimos, então, que $\epsilon_4 = \pm 1$.

Se $\epsilon_4 = 1$, temos

$$\epsilon_5 \lambda^{3(m-1)} \tau^3 + \phi^3 + \psi^3 = 0,$$

uma equação do tipo (3.4) onde $n = m - 1$. Se $\epsilon_4 = -1$, trocamos ψ^3 por $-\psi^3$ e temos outra equação do tipo (3.4) com $n = m - 1$, provando assim o Teorema 27 e, portanto, o Teorema 23. □

CAPÍTULO 5

PROBLEMAS FINAIS

Esse capítulo apresenta algumas situações-problema que podem ser trabalhadas em sala de aula com os alunos do sexto e do oitavo ano. Os problemas considerados incluem algumas aplicações de equações diofantinas lineares estudadas no Capítulo 4, assim como, a noção elementar do máximo divisor comum revisada no Capítulo 2. Propomos a revisão do algoritmo de Euclides como pré-requisito teórico para abordar ambos assuntos em sala de aula.

5.1 Alguns casos no Caderno do Aluno do Estado de São Paulo

No sexto ano, na Situação de Aprendizagem 2 do volume 1 no caderno do aluno do estado de São Paulo (SÃO PAULO, 2014) são trabalhados alguns temas referentes ao conjunto dos números naturais tais como os números primos, múltiplos e divisores de um número natural, máximo divisor comum e mínimo múltiplo comum. São trabalhadas algumas competências e habilidades referentes a esses assuntos, uma delas é saber resolver problemas envolvendo a ideia de máximo divisor comum. Especificamente, a atividade 7 pede para que o aluno encontre todos os divisores naturais de alguns números. A atividade 8 pede para que o aluno encontre todos os divisores comuns a dois números naturais. Enfim, nas atividades 9 e 10, é solicitado que o estudante encontre o maior divisor comum entre dois números. Nenhum método geral é mencionado e, portanto, é esperado que o professor introduza o assunto e apresente a teoria necessária. Claramente, o algoritmo de Euclides pode ser apresentado com este objetivo. O seguinte exemplo ilustra o assunto.

Problema 1. Temos dois tubos de PVC que devem ser cortados em pedaços iguais. O primeiro deles mede 24 metros, e o segundo, 40 metros. Determine o maior tamanho que deve ter cada pedaço de modo que os dois tubos sejam utilizados inteiramente, sem sobras.

Resolução. Buscamos para este problema cortar os tubos em pedaços de mesmo tamanho, divisores comuns entre 40 e 24, e sendo a maior medida possível, por isso buscamos o máximo divisor comum entre 24 e 40. Utilizando o Algoritmo de Euclides temos

$$40 = 1 \cdot 24 + 16$$
$$24 = 1 \cdot 16 + 8,$$

como $8 \mid 16$ o algoritmo termina e concluímos que o maior divisor comum entre 24 e 40 é 8. ◇

Para facilitar o entendimento dos cálculos do aprendiz consideramos a Tabela 1, a qual apenas é uma maneira de organizar os cálculos do algoritmo de Euclides para um aluno de sexto ano.

Tabela 1 – Máximo Divisor Comum

maior n°	menor n°	r_1	r_2	...	$r_{(n-1)}$	r_n
r_1	r_2	r_3	r_4	...	0	

O número r_1 é o resto da divisão entre o maior e menor dos dois números. O número r_2 é o resto da divisão entre o menor dos dois números e r_1. O número r_3 é o resto da divisão entre r_1 e r_2. Suponhamos que este processo seja repetido n vezes até obtermos os númeor r_{n-1} e r_n tais que $r_n \mid r_{n-1}$. Neste caso, r_n é o valor que procuramos. Os cálculos para o problema dos tubos de PVC são apresentados na Tabela 2. Concluímos, assim, que $(40, 24) = 8$.

Tabela 2 – Máximo Divisor Comum de 40 e 24

40	24	16	8
16	8	0	

5.1.1 Oitavo ano, Volume 2, Situação de Aprendizagem 4

Voltando agora para o oitavo ano, no volume 2 do caderno do aluno, a Situação de Aprendizagem 4 é toda sobre equações diofantinas lineares, como as vistas em 4.1, porém, apenas com números inteiros não negativos. Neste momento os alunos já trabalharam em situações recentes sobre equações lineares e sistemas de equações lineares no plano cartesiano. Com as atividades desta situação de aprendizagem deseja-se que o estudante consiga no fim, como competências e habilidades, identificar regularidades e padrões, organizar informações em tabelas e ter um raciocínio lógico-dedutivo em problemas algébricos. No início desta situação são propostos os seguintes problemas.

Problema 2. Para agrupar 13 ônibus em filas de 3 ou 5 em uma garagem, quantas filas de cada tipo serão formadas?

Problema 3. Quantas quadras de vôlei e quantas quadras de basquete são necessárias para que 80 alunos joguem simultaneamente? E se forem 77 alunos? (Dado: um time de basquete é formado por 5 jogadores; um de vôlei, por 6.)

Problema 4. Um laboratório dispõe de duas máquinas para examinar amostras de sangue. Uma delas examina 15 amostras de cada vez, enquanto a outra examina 25. Quantas vezes essas máquinas devem ser acionadas para examinar 2 000 amostras?

Problema 5. Um caixa eletrônico disponibiliza para saque apenas notas de R$ 20,00, R$ 50,00 e R$ 100,00. Se um cliente deseja sacar R$ 250,00, de quantas maneiras diferentes ele poderá receber suas notas?

Problema 6. Deseja-se adquirir peças dos tipos A, B e C cujos preços unitários são R$ 1,00, R$ 10,00 e R$ 20,00, respectivamente. Se dispomos de R$ 200,00 para a compra, quantas e quais são as possibilidades de compra que podemos fazer?

Estes problemas são desenvolvidos por meio de sete atividades, sendo que em duas delas são utilizadas tabelas de maneira análoga ao explicado na resolução do problema 1. Em minha opinião são ótimas questões para se introduzir o problema de equações com soluções inteiras, porém, o caderno não apresenta exemplos envolvendo inteiros negativos e nem problemas com números relativamente grandes, onde é necessário um método geral para encontrar todas as soluções inteiras possíveis. Após a realização bem sucedida da situação de aprendizagem 4 podemos trabalhar com os alunos alguns problemas mais desafiadores incluindo equações, de duas variáveis, com coeficientes relativamente grandes.

No caderno do professor, onde temos várias orientações e respostas para os problemas do caderno do aluno, há uma breve explicação sobre o que vimos na Proposição 12. Esta última pode ser apresentada e demonstrada em sala de aula para que os alunos entendam que, nem sempre, é possível termos soluções inteiras. Também no caderno do professor é mostrado apenas um método através do algoritmo de Euclides para encontrar uma *primeira* solução, mas, para uma equação bastante fácil de se obter uma solução trivial, nada muito desafiador para o aluno. Apresentamos a seguir algumas questões que podem ser desenvolvidas em sala de aula após a realização dessa situação de aprendizagem, com o intuito de desafiar os alunos.

5.1.2 Questões sobre equações diofantinas lineares

Questão 1. Encontre a solução geral para a equação $550x + 343y = 4$.

Resolução. Vamos encontrar uma solução para a equação $550x + 343y = 4$, sabendo que $(550, 343) \mid 4$. Utilizando o algoritmo de Euclides temos

$$550 = 1 \cdot 343 + 207 \tag{5.1}$$
$$343 = 1 \cdot 207 + 136 \tag{5.2}$$
$$207 = 1 \cdot 136 + 71 \tag{5.3}$$
$$136 = 1 \cdot 71 + 65 \tag{5.4}$$
$$71 = 1 \cdot 65 + 6 \tag{5.5}$$
$$65 = 10 \cdot 6 + 5 \tag{5.6}$$
$$6 = 1 \cdot 5 + 1 \tag{5.7}$$

O que prova que $(550,343) = 1 \mid 4$. O interessante aqui são todas as linhas deste algoritmo. Temos, pela última linha (5.7), que $1 = 6 - 1 \cdot 5$ e já pela linha (5.6) temos que $5 = 65 - 10 \cdot 6$, substituindo o número 5 encontramos $1 = 6 - 1(65 - 10 \cdot 6)$. Pela linha (5.5), $6 = 71 - 1 \cdot 65$ e substituindo novamente na igualdade $1 = 6 - 1(65 - 10 \cdot 6) = -65 + 11 \cdot 6$ encontramos $1 = -65 + 11(71 - 1 \cdot 65)$. Fazendo sucessivamente essas substituições da última até a primeira linha temos

$$\begin{aligned}
1 = 6 - 1 \cdot 5 &\Rightarrow 1 = 6 - 1(65 - 10 \cdot 6) \\
&\Rightarrow 1 = -65 + 11 \cdot 6 \\
&\Rightarrow 1 = -65 + 11(71 - 65) \\
&\Rightarrow 1 = 11 \cdot 71 - 12 \cdot 65 \\
&\Rightarrow 1 = 11 \cdot 71 - 12(136 - 71) \\
&\Rightarrow 1 = -12 \cdot 136 + 23 \cdot 71 \\
&\Rightarrow 1 = -12 \cdot 136 + 23(207 - 136) \\
&\Rightarrow 1 = 23 \cdot 207 - 35 \cdot 136 \\
&\Rightarrow 1 = 23 \cdot 207 - 35(343 - 207) \\
&\Rightarrow 1 = -35 \cdot 343 + 58 \cdot 207 \\
&\Rightarrow 1 = -35 \cdot 343 + 58(550 - 343) \\
&\Rightarrow 1 = 550(58) + 343(-93)
\end{aligned}$$

Multiplicando a última igualdade por 4 encontramos

$$4 = 550(232) + 343(-372),$$

portanto, uma das soluções de $4 = 550x + 343y$ é $x = 232$ e $y = -372$. Finalmente, utilizando o Teorema 18, obtemos

$$x = 232 + 343t \quad \text{e} \quad y = -372 - 550t, \quad \text{para todo } t \in \mathbb{Z}. \qquad \diamond$$

Para simplificar os cálculos, apresentamos a seguir o Algoritmo de Euclides Estendido. Considere a Tabela 3 onde registramos os resultados do Algoritmo de Euclides.

Considere a equação $ax + by = (a,b)$ com a e b inteiros. Os números q_1 e r_1 são, nessa ordem, o quociente e o resto da divisão de a por b, já os números q_2 e r_2 são, nessa ordem, o quociente e o resto da divisão de b por r_1, em seguida, os números q_3 e r_3 são, nessa ordem, o quociente e o resto da divisão de r_1 por r_2. Como visto na Seção 2.3, repetimos este processo até obtermos r_{i-1} e r_i tais que $r_i \mid r_{i-1}$, ou seja, $r_{i+1} = 0$ e, usando o Teorema 2, concluímos que $(a,b) = r_i$.

Os números m_i e n_i obedecem a relação $r_i = am_i + bn_i$. Para calcularmos os valores da coluna m, temos $m_1 = 1 - (0 \cdot q_1)$, $m_2 = 0 - (m_1 \cdot q_2)$ e todos os outros são da forma

Tabela 3 – Algoritmo de Euclides Estendido

Restos	Quocientes	m	n
a		1	0
b		0	1
r_1	q_1	m_1	n_1
r_2	q_2	m_2	n_2
$\dots$	$\dots$	$\dots$	$\dots$
r_{i-1}	q_{i-1}	m_{i-1}	n_{i-1}
r_i	q_i	m_i	n_i
r_{i+1}	q_{i+1}	m_{i+1}	n_{i+1}

Tabela 4 – Questão 1

Restos	Quocientes	m	n
550		1	0
343		0	1
207	1	1	-1
136	1	-1	2
71	1	2	-3
65	1	-3	5
6	1	5	-8
5	10	-53	85
1	1	58	-93
0	5	-343	550

$m_{i+1} = m_{i-1} - (m_i \cdot q_{i+1})$. Já os valores da coluna n, temos $n_1 = 0-(1\cdot q_1)$, $n_2 = 1-(n_1 \cdot q_2)$ e todos os outros são da forma $n_{i+1} = n_{i-1} - (n_i \cdot q_{i+1})$.

A seguir, apresentamos como é aplicado este método na resolução Questão 1. A tabela resultante para este problema é apresentada na Tabela 4.

Pela penúltima linha da tabela encontramos $550(58) + 343(-93) = 1$, multiplicamos esta igualdade por 4 e obtemos $550(232) + 343(-372) = 4$, encontrando uma solução inicial. Novamente, utilizando o Teorema 18, temos

$$x = 232 + 343t \quad \text{e} \quad y = -372 - 550t, \quad \text{para todo } t \in \mathbb{Z}.$$

Questão 2 (OBMEP 2015)**.** Considere dois tambores de capacidade suficientemente grande, um deles vazio e o outro cheio de líquido. Determine se é possível colocar exatamente um litro do líquido do tambor cheio, no vazio, usando dois baldes, um com capacidade de 5 litros e o outro com capacidade de 7 litros.

Resolução. Chamando de x a quantidade de vezes que devemos usar o balde com capacidade de 5 litros e de y a quantidade de vezes que devemos usar o balde com capacidade de 7 litros,

obtemos a seginte equação

$$5x + 7y = 1.$$

Agora, basta observarmos que $(5,7) \mid 1$, o que verifica ser possível pela Proposição 12. E uma das maneiras possíveis é usar o balde de capacidade de 5 litros três vezes ($x = 3$) para colocar o líquido no tambor vazio, obtendo-se 15 litros e, em seguida, usamos o balde com capacidade de 7 litros duas vezes ($y = -2$) para retirar o líquido do tambor que inicialme estava vazio, restando, assim, apenas um litro. ◇

Questão 3. Dois tipos de refrigerantes A e B em determinado supermercado custam 8 e 5 reais respectivamente. Maria comprou alguns refrigerantes do tipo A e alguns do tipo B. Verifique se é possível que sua compra tenha ficado em 32 reais.

Resolução. Usando x para indicar a quantidade de refrigerantes do tipo A e y para indicar a quantidade de refrigerante do tipo B, temos a equação $8x + 5y = 32$. Observe que $(8,5) \mid 32$ e assim sabemos que existem soluções inteiras para x e y. Uma solução trivial seria $x = 4$ e $y = 0$, pelo Teorema 18 temos

$$x = 4 + 5t \text{ e } y = 0 - 8t, \text{ com } t \in \mathbb{Z}.$$

Por outro lado, devemos nos certificar se existe alguma solução inteira positiva, sabendo que não há quantidade nula ou negativa de refrigerantes. Logo, para $x > 0$,

$$4 + 5t > 0 \Rightarrow t > 0,8$$

e para $y > 0$ temos

$$0 - 8t > 0 \Rightarrow t < 0,$$

o que nos mostra que não há solução inteira onde x e y são positivos e, assim, não é impossível que essa compra tenha ficado em 32 reais. ◇

Questão 4. Mariana precisou sacar em um caixa eletrônico 250 reais. No caixa utilizado só havia notas de 20 e 5 reais. De quantas maneiras diferentes, se tratando da quantidade de cédulas, era possível realizar este saque?

Resolução. Usando x para a quantidade de notas de 20 reais e y para a de 5 reais, temos a equação

$$20x + 5y = 250.$$

Vamos simplificar esta equação divindo por 5 e obtendo $4x + y = 50$. Uma solução trivial pode ser $x = 10$ e $y = 10$, assim, pelo Teorema 18, temos $x = 10 + t$ e $y = 10 - 4t$, com $t \in \mathbb{Z}$. As soluções deste problema devem ser inteiras e não negativas, assim, para $x \geq 0 \Rightarrow 10 + t \geq 0 \Rightarrow t \geq -10$; e para $y \geq 0 \Rightarrow 10 - 4t \geq 0 \Rightarrow t \leq 2,5$. Deste modo $t = -10, -9, -8, ..., 1e2$, um total de 13 maneiras diferentes. ◇

Questão 5. Se em nosso país existissem apenas cédulas de 5 e de 2 reais seria possível efetuar um pagamento de qualquer valor inteiro? E com notas apenas de 5 e 20 reais?

Resolução. Para a primeira pergunta a resposta é sim, pois $(5,2) = 1$ e em uma equação do tipo $5x + 2y = c$, com $c \in \mathbb{Z}$, $(5,2) \mid c$. Já para a segunda pergunta teríamos uma equação do tipo $5x + 20y = c$, com $c \in \mathbb{Z}$. Para obtermos solução, sabemos que $(5,20) = 5$ deve dividir c, então não há como efeturar qualquer pagamento inteiro para segunda pergunta, apenas valores múltiplos de 5. ◇

Questão 6 (Euler)**.** Divida 100 em 2 parcelas positivas, de modo que uma seja divisível por 7 e a outra por 11.

Resolução. A parcela divisível por 11 é do tipo $11x$, com $x \in \mathbb{Z}$, e a parcela divisível por 7 é tipo $7y$, com $y \in \mathbb{Z}$ e, assim, obtemos a equação $11x + 7y = 100$. Observe que $11(2) + 7(-3) = 1$, multiplicando por 100 obtemos $11(200) + 7(-300) = 100$ e encontramos uma solução inteira para a equação. Pelo Teorema 18, $x = 200 + 7t$ e $y = -300 - 11t$, com $t \in \mathbb{Z}$. Procuramos por parcelas positivas, então,

$$200 + 7t \geq 0 \Rightarrow t \geq \frac{-200}{7} \approx -28,6 \text{ e}$$
$$-300 - 11t \geq 0 \Rightarrow t \leq \frac{-300}{11} \approx -27,3.$$

Logo o único valor inteiro para t é -28 e, assim, $x = 200 + 7(-28) = 4$ e, portanto, a parcela divisível por 11 é 44 e outra parcela, divisível por 7, é 56. ◇

Questão 7. Para pintar sua casa Estênio verificou que eram necessários 128 litros de tinta. Ele comprou alguns litros de tinta branca, que eram vendidos em latas de 4 litros, e comprou também alguns litros de tinta azul que eram vendidos em latas de 20 litros, totalizando a quantidade necessária. Sabendo que a quantidade de latas compradas era um múltiplo de 7, quantas latas de tinta azul foram compradas?

Tabela 5

t	0	1	2	3	4	5
x	2	7	12	17	22	27
y	6	5	4	3	2	1
$x+y$	8	12	16	20	24	28

Resolução. Utilizando x e y para indicar as quantidades de latas de tinta branca e azul, respectivamente, temos a equação $4x + 20y = 128$ e, para facilitar os cálculos, divimos por 4 e encontramos $x + 5y = 32$. Uma solução trivial é $x = 2$ e $y = 6$, logo as soluções são do tipo,

pelo Teorema 18, $x = 2 + 5t$ e $y = 6 - t$, com $t \in \mathbb{Z}$. Como x e y são inteiros positivos, temos que

$$2 + 5t > 0 \Rightarrow t > -0,4 \text{ e}$$
$$6 - t > 0 \Rightarrow t < 6.$$

A partir disso, podemos construir a Tabela 5. Como a quantidade de latas compradas $(x + y)$ era múltipla de 7, a solução está na última coluna em que $x = 27$ e $y = 1$, logo, foi comprada apenas uma lata de tinta azul. ◇

REFERÊNCIAS

BASHMAKOVA, I. G. **Diophantus and Diophantine Equations**. Washington, DC: Mathematical Association of America, 1997. (Dolciani Mathematical Expositions, 20). Citado nas páginas 19 e 20.

EVES, H. **Introdução à História da Matemática**. 1. ed. [S.l.]: UNICAMP, 2004. Citado nas páginas 19 e 20.

FREY, G. Links between stable elliptic curves and certain diophantine equations. **Annales Universitatis Saraviensis**, v. 1, p. 1–40, 1986. Citado na página 21.

GAUSS, C. F. **Werke: 2**. Königlichen Gesellschaft der Wissenschaften, 1876. Disponível em: <https://books.google.com.br/books?id=3LCkdxX2DEcC>. Citado na página 35.

HARDY, G. H.; WRIGHT, E. M. **An Introduction to the Theory of Numbers**. 6a. ed. Oxford: Oxford University Press, 2008. Citado nas páginas 22, 23, 29, 49 e 56.

HEAT, T. L. **Diophantos of Alexandria: A study in the history of Greek algebra**. Cambridge, UK: Cambridge University Press, 1910. Citado na página 19.

HEFEZ, A. **Aritmética**. Rio de Janeiro, IMPA: Sociedade Brasileira de Matemática, 2013. (Coleção PROFMAT). Citado na página 23.

____. **Iniciação à Aritmética**. 1. ed. Rio de Janeiro, IMPA: Sociedade Brasileira de Matemática, 2015. (PIC-OBEMEP). Citado na página 23.

HELLEGOUARCH, Y. Points d'ordre $2p^h$ sour les courbes elliptiques. **Acta Arith.**, XXVI, p. 253–263, 1975. Citado na página 21.

MARTINEZ, F. B. B.; MOREIRA, C. G.; SALDANHA, N. C.; TENGAN, E. **Teoria dos Números: : um passeio com primos e outros números familiares pelo mundo inteiro**. 2. ed. Rio de Janeiro, Brasil: IMPA, 2010, 2010. Citado na página 23.

PEGG, E. **The Hippasus Primes**. 2016. <https://community.wolfram.com/groups/-/m/t/965609>. Acesado em 20-11-2018. Citado na página 45.

RIBET, K. On modular representations of Gal($\bar{Q}/Q$) arising from modular forms. **Inventiones Mathematicae**, v. 100, n. 2, p. 431–476, 1990. Citado na página 21.

SANTOS, J. P. O. **Introdução à Teoria dos Números**. Rio de Janeiro, IMPA: Sociedade Brasileira de Matemática, 1998. (Coleção Matemática Universitária). Citado na página 23.

SINGH, S. **O último teorema de Fermat**. [S.l.]: Record, 2006. Citado na página 22.

SÃO PAULO, Secretaria do Estado da Educação. **Matemática do Ensino Fundamental, 9 ano. Caderno do Professor de Matemática**. São Paulo: SEE, 2014. v. 1. Citado na página 63.

WILES, A. Modular elliptic curves and Fermat's Last Theorem. **Ann. Math**, v. 141, n. 3, p. 443–551, 1995. Citado na página 21.

WILES, A.; TAYLOR, R. Ring-theoretic properties of certain Hecke algebras. **Ann. Math**, v. 141, n. 3, p. 553–572, 1995. Citado na página 21.


ICMC
USP
SÃO CARLOS