UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Uma introdução a equações diofantinas e aproximações de números reais

Douglas Felipe Queiroz Taketomi

Dissertação de Mestrado do Programa de Pós-Graduação em Ciências de Computação e Matemática Computacional (PPG-CCMC)

ICMC USP SÃO CARLOS

Douglas Felipe Queiroz Taketomi

Uma introdução a equações diofantinas e aproximações de números reais

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Ciências de Computação e Matemática Computacional. *EXEMPLAR DE DEFESA*

Área de Concentração: Ciências de Computação e Matemática Computacional

Orientador: Prof. Dr. Sérgio Luís Zani

USP – São Carlos
Fevereiro de 2023

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

Taketomi, Douglas Felipe Queiroz
T136i Uma introdução a equações diofantinas e aproximações de números reais / Douglas Felipe Queiroz Taketomi; orientador Sérgio Luís Zani. -- São Carlos, 2023.
74 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, 2023.

1. Equações diofantinas. 2. Frações Contínuas. I. Zani, Sérgio Luís , 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

Douglas Felipe Queiroz Taketomi

An introduction to diophantine equations and approximations of real numbers

Dissertation submitted to the Instituto de Ciências Matemáticas e de Computação – ICMC-USP – in accordance with the requirements of the Computer and Mathematical Sciences Graduate Program, for the degree of Master in Science. *EXAMINATION BOARD PRESENTATION COPY*

Concentration Area: Computer Science and Computational Mathematics

Advisor: Prof. Dr. Sérgio Luís Zani

USP – São Carlos
February 2023

Dedico esse trabalho a minha vó, que sempre me incentivou a continuar meus estudos.

Obrigado vó, te amo!

AGRADECIMENTOS

Agradeço primeiramente a Deus por me dar saúde, sabedoria e força para buscar meus objetivos.

Também gostaria de agradecer a todos os professores do mestrado por todo conhecimento e sabedoria que me foram passados. Ao meu orientador Professor Dr. Sérgio Luís Zani que me deu todo o suporte para concluir esta etapa.

A todos os meus colegas de mestrado, amigos que jamais esquecerei, vocês fazem parte dessa minha conquista. Não posso deixar de agradecer à Adriana, Carlos e Meryelen por todos os momentos que passamos juntos.

Dedico também a todas as pessoas que de alguma forma contribuíram para esta conquista.

“As raízes do estudo são amargas,
mas seus frutos são doces.”
(Aristóteles)

RESUMO

TAKETOMI, H. L. **Uma introdução a equações diofantinas e aproximações de números reais**. 2023. 74 p. Dissertação (Mestrado em Ciências – Ciências de Computação e Matemática Computacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2023.

Este trabalho é uma introdução para o estudo de equações diofantinas e frações contínuas, equações que foram trabalhadas pelo matemático grego Diofanto de Alexandria, considerado o pai da Álgebra. Antes de estudar equações diofantinas, serão vistos alguns fundamentos relacionados à Teoria dos Números, incluindo propriedades, teoremas e demonstrações sobre divisibilidade, divisão euclidiana, máximo divisor comum, congruências e o algoritmo de Euclides. Em seguida, será estudado equações diofantinas lineares com duas, três e n incógnitas.E por fim, abordamos frações contínuas, onde será mostrada a relação fundamental entre números racionais e números reais, e como números racionais e irracionais podem ser representados como frações contínuas, com exemplos do número "pi" e o número de ouro.

Palavras-chave: Equações Diofantinas, Frações Contínuas.

ABSTRACT

TAKETOMI, H. L. **An introduction to diophantine equations and approximations of real numbers** . 2023. 74 p. Dissertação (Mestrado em Ciências – Ciências de Computação e Matemática Computacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2023.

This work is an introduction to the study of Diophantine equations and continued fractions, equations that were worked on by the Greek mathematician Diophantus of Alexandria, considered the father of Algebra. Before studying Diophantine equations, some fundamentals related to Number Theory will be seen, including properties, theorems and demonstrations about divisibility, Euclidean division, greatest common divisor, congruences and Euclid's algorithm. Next, linear Diophantine equations with two, three and n unknowns will be studied. And finally, we approach continued fractions, where the fundamental relationship between rational numbers and real numbers will be shown, and how rational and irrational numbers can be represented as continued fractions, with examples of the number "pi" and the number of gold.

Keywords: Diophantine Equations, Continued Fractions.

LISTA DE ABREVIATURAS E SIGLAS

CMRJ	Colégio Militar do Rio de Janeiro
ENQ	Exame Nacional de Qualificação
OBM	Olimpíada Brasileira de Matemática
PROFMAT	Mestrado Profissional em Matemática em Rede Nacional

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

Considerado por muitos como o pai da Álgebra, Diofanto de Alexandria (matemático grego) teve grande influência no desenvolvimento de diversos ramos da matemática. Diofanto nasceu por volta de 200 d.C, não se sabe ao certo sua nacionalidade, mas foi em Alexandria, no Egito, que se destacou com sua principal publicação, a obra "Arithmetica", considerado o primeiro manual de Álgebra. As equações algébricas indeterminadas foram um dos temas trabalhados em seus livros, nos quais Diofanto aceitava apenas soluções em números racionais não negativos. Essas equações, quando são aceitos apenas números racionais como soluções, ficaram conhecidas como equações diofantinas, equações que levam seu nome. (SILVA AMANDA G. DA SILVA, 2014)

Este trabalho visa auxiliar os alunos do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) com material complementar para o estudo das equações diofantinas. Mas antes de começar veremos alguns fundamentos relacionados à Teoria dos Números, área que se dedica ao estudo dos números inteiros. Mostraremos algumas propriedades, teoremas e demonstrações relacionados à divisibilidade nos inteiros, divisão euclidiana, máximo divisor comum, congruências e o algoritmo de Euclides.

No capítulo 3, relacionado às equações diofantinas lineares, estudaremos sobre as equações diofantinas com duas, três e n incógnitas, demonstraremos algumas proposições, exemplos e a solução geral de cada tipo de difantina.

O capítulo 4 falará sobre frações contínuas, em que veremos uma relação fundamental entre números racionais e números reais, que diz que números reais podem ser arbitrariamente aproximados por números racionais. Para isso faremos uso de frações contínuas. Neste mesmo capítulo mostraremos como podemos representar números racionais e irracionais como frações contínuas, dando exemplos de como podemos expressar o número "pi"e o número de ouro, denotado pelas letras gregas π e ϕ respectivamente, como frações contínuas.

Concluímos o último capítulo fazendo algumas reflexões que consideramos importantes.

CAPÍTULO

2

FUNDAMENTOS

Neste capítulo estudaremos um pouco sobre a Teoria dos Números, que é uma área da matemática que estuda as propriedades dos números inteiros. Veremos algumas propriedades e teoremas que serão importantes para darmos continuidade nos próximos capítulos.

As seguintes definições baseiam-se no livros: Aritmética de (HEFEZ, 2016), um curso com problemas e soluções de (OLIVEIRA; FERNáNDEZ, 2012) e An Introduction to the Theory of Numbers (NIVEN; MONTGOMERY, 1991).

2.1 Números Inteiros e Números Naturais

O conjunto dos números inteiros será representado pelo símbolo $\mathbb{Z}$, neste conjunto estão todos os números inteiros positivos e negativos, incluindo o número zero. O conjunto dos números inteiros é dado por:

$$\mathbb{Z} = \{\ldots, -4, -3, -2, -1,\ 0,\ 1,\ 2,\ 3,\ 4, \ldots\}.$$

O conjunto dos números naturais será representado pelo símbolo $\mathbb{N}$, esse conjunto é um subconjunto dos números inteiros, ele consiste em todos os números inteiros positivos incluindo também o número zero. O conjunto dos números naturais é dado por:

$$\mathbb{N} = \{\ 0,\ 1,\ 2,\ 3,\ 4, \ldots\}.$$

Uma das propriedades fundamentais dos números naturais é o princípio da boa ordenação, que afirma o seguinte:

Princípio da Boa Ordenação: Todo subconjunto não vazio $A \subseteq \mathbb{N}$ possui um elemento menor que todos os outros elementos deste, ou seja, existe $a \in A$ tal que $a \leqslant n$ para todo $n \in A$.

Podemos observar que o conjunto dos números inteiros não goza do princípio da boa ordenação, pois ele não é limitado inferiormente. Temos também que as operações de adição e

multiplicação de números inteiros resultam em números inteiros, mas a divisão de dois inteiros nem sempre é um inteiro.

A seguir veremos algumas propriedades referentes a adição e multiplicação de números inteiros.

i) A adição e multiplicação são bem definidas: Para todos $a, b, a', b' \in \mathbb{Z}$, se $a = a'$ e $b = b'$, então $a + b = a' + b'$ e $a \cdot b = a' \cdot b'$.

ii) A adição e multiplicação são comutativas: Para todos $a, b \in \mathbb{Z}$, $a + b = b + a$ e $a \cdot b = b \cdot a$.

iii) A adição e multiplicação são associativas: Para todos $a, b, c \in \mathbb{Z}$, $(a + b) + c = b + (a + c)$ e $(a \cdot b) \cdot c = b \cdot (a \cdot c)$.

iv) A adição e multiplicação possuem elementos neutros: Para todo $a \in \mathbb{Z}$, $a + 0 - a$ e $a \cdot 1 = a$.

v) A adição possui elementos simétricos: Para todo $a \in \mathbb{Z}$, existe $b = -a$ tal que $a + b = 0$.

vi) A multiplicação é distributiva em relação a adição: Para todos $a, b, c \in \mathbb{Z}$, tem-se $a \cdot (b + c) = a \cdot b + a \cdot c$.

vii) Fechamento de $\mathbb{Z}$: O conjunto $\mathbb{Z}$ é fechado para as operações de adição e multiplicação, ou seja, para todos $a, b \in \mathbb{Z}$, tem-se que $a + b$ e $a \cdot b \in \mathbb{Z}$

viii) Tricotomia: Dados $a, b \in \mathbb{Z}$, apenas uma das seguintes possibilidades pode ser satisfeita:

   a) $a = b$

   b) $a < b$

   c) $a > b$

ix) Princípio da Boa Ordenação: Se N é um conjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então N possui um menor elemento.

Agora iremos definir o que é o valor absoluto.

Definição 1. O valor absoluto (módulo) de um inteiro a é definido como a distância de a até 0 na reta, logo podemos chegar a conclusão que o módulo de um número é sempre positivo, pois temos que a distância é uma medida não-negativa, portanto $|a| \geqslant 0$.

$$|a| := \begin{cases} a, \text{ se } a > 0, \\ -a, \text{ se } a < 0. \end{cases}$$

Exemplo 1. A partir dessa definição podemos ver que:

i) $|7| = 7$.

ii) $|-12| = -(-12)$.

iii) Para encontrar o módulo de $|\sqrt{5}-3|$ notemos que $\sqrt{5} < 3$, logo $\sqrt{5}-3 < 0$, portanto $|\sqrt{5}-3| = -(\sqrt{5}-3) = 3-\sqrt{5}$.

2.2 Divisibilidade nos Números Inteiros

A divisão entre dois números inteiros nem sempre é exata, mas quando é possível efetuar essa divisão com exatidão, tal fato pode ser expressado através da relação de divisibilidade.

Definição 2. Dados dois números inteiros a e b, com a diferente de 0. Dizemos que b é divisível por a quando existir um número inteiro c tal que:

$$b = a \cdot c,$$

representaremos essa divisibilidade por $a \mid b$, caso a não divida b, escrevemos $a \nmid b$.

Exemplo 2. Podemos observar que:

i) $2 \mid 10$, pois podemos tomar $c = 5 \in \mathbb{Z}$ e temos $10 = 2 \cdot 5$.

ii) $5 \mid 75$, pois podemos tomar $c = 15 \in \mathbb{Z}$ e temos $75 = 5 \cdot 5$.

iii) $7 \nmid 16$, pois não existe $c \in \mathbb{Z}$ tal que $16 = 7 \cdot c$.

iv) $2 \nmid 15$, pois não existe $c \in \mathbb{Z}$ tal que $15 = 2 \cdot c$.

Agora veremos algumas propriedades da divisibilidade.

Proposição 1. Sejam a, b e c números inteiros, com a e b diferente de zero, temos que:

i) $1 \mid a$, $b \mid b$ e $b \mid 0$.

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

Demonstração. Veja que:

i) Decorre das seguintes igualdades:

$$a = 1 \cdot a,\ b = 1 \cdot b,\ 0 = b \cdot 0.$$

ii) Se $a \mid b$ e $b \mid c$, temos que existem d e f inteiros tal que $b = a \cdot d$ e $c = b \cdot f$, agora substituindo o valor de b na segunda expressão teremos que:

$$c = b \cdot f = (a \cdot d) \cdot f = a \cdot (d \cdot f),$$

como $(d \cdot f) = t \in \mathbb{Z}$, então $c = a \cdot t$ com $t \in \mathbb{Z}$. Logo temos que $a \mid c$.

□

Exemplo 3. Observemos que:

i) Se $3 \mid 6$ e $6 \mid 12$ então $3 \mid 12$, pois $3 \mid 12 = 6 \cdot 2$.

ii) Se $5 \mid 10$ e $10 \mid 60$ então $5 \mid 60$, pois $5 \mid 60 = 10 \cdot 2$.

Proposição 2. Sejam a, b e c números inteiros. Se $a \mid b$ e $a \mid c$ então a divide qualquer combinação linear entre b e c.

Demonstração. Se $a \mid b$ e $a \mid c$, temos que existem x e y inteiros tais que:

$$b = a \cdot x,$$

$$c = a \cdot y.$$

Agora tomando d e f inteiros quaisquer, podemos representar uma combinação linear de b e c na forma $b \cdot d + f \cdot c$. Substituindo os valores de a e b nessa combinação, teremos:

$$b \cdot d + f \cdot c = (a \cdot x) \cdot d + f \cdot (a \cdot y) = a \cdot (x \cdot d + f \cdot y)$$

Como $b \cdot d + f \cdot c = a \cdot (x \cdot d + f \cdot y)$, e $(x \cdot d + f \cdot y) = k \in \mathbb{Z}$, temos que $b \cdot d + f \cdot c = a \cdot k$, com $k \in \mathbb{Z}$. Logo $a \mid (b \cdot d + f \cdot c)$. □

Exemplo 4. Podemos observar que se $3 \mid 12$ e $3 \mid 30$, logo existem d e $f \in \mathbb{Z}$ tais que:

$$3 \mid 12 \cdot d + 30 \cdot f.$$

$$3 \mid 3 \cdot 4 \cdot d + 3 \cdot 10 \cdot f.$$

$$3 \mid 3 \cdot (4 \cdot d + 10 \cdot f).$$

Portanto 3 divide qualquer combinação linear entre 12 e 30.

Proposição 3. Sejam a, b, c e d números inteiros. Se $a \mid b$ e $c \mid d$, então $a \cdot c \mid b \cdot d$.

Demonstração. Como $a \mid b$ e $c \mid d$, temos que existem x ey inteiros tais que $b = a \cdot x$ e $d = c \cdot y$.

Fazendo o produto membro a membro de b e d temos :

$b \cdot d = (a \cdot x) \cdot (c \cdot y) = (a \cdot c \cdot x \cdot y)$, como $x \cdot y = z \in \mathbb{Z}$, $b \cdot d = a \cdot c \cdot z$, portanto $a \cdot c \mid b \cdot d$. □

Exemplo 5. Podemos observar que se $2 \mid 6$ e $5 \mid 20$, então $2 \cdot 5 \mid 6 \cdot 20$, pois $10 \mid 120 = 10 \cdot 12$.

Proposição 4. Sejam a, b e c números inteiros, então:

i) Se a e b são positivos e $a \mid b$ então $0 < a \leqslant b$.

ii) Se $a \mid b$ e $b \mid a$ então $a = b$ ou $a = -b$.

Demonstração. É fácil ver que:

i) Se $a \mid b$, temos que existe $x \in \mathbb{Z}$ tal que $b = a \cdot x$, como a e b são positivos e $a \mid b$, então $x \geqslant 1$.

Logo multiplicando por a ambos lados dessa desigualdade temos que:

$$b = a \cdot x \geqslant a > 0,$$

ou seja,

$$0 < a \leqslant b.$$

ii) Se $a \mid b$ e $b \mid a$ então $|a| \mid |b|$ e $|b| \mid |a|$. Pelo item anterior temos que $|a| \leqslant |b|$ e $|b| \leqslant |a|$, ou seja, $|a| \leqslant |b| \leqslant |a|$. Logo, $|a| = |b|$ e consequentemente $a = b$ ou $a = -b$.

□

Exemplo 6. Se $6 \mid 24$, então $0 < 6 < 24$, por outro lado temos que se $9 \mid 9$, então $0 < 9 \leqslant 9$.

2.3 Divisão Euclidiana

Quando a divisão entre dois números inteiros não é exata, podemos expressar tal fato através da divisão Euclidiana. Veremos o que acontece no caso geral da divisão entre dois inteiros.

Teorema 1. Divisão Euclidiana

Dados dois inteiros a e b com b positivo existem dois únicos inteiros q e r tais que:

$$a = b \cdot q + r\ ,\ \ 0 \leqslant r < b.$$

Se $b \nmid a$, então r satisfaz a desigualdade estrita $0 < r < b$.

Deve-se observar que a é chamado de numerador, b de quociente e r é o resto dessa divisão.

Demonstração. Primeiramente demonstraremos sua existência.

Por simplicidade, tomemos a positivo. Devemos fazer três analises, para caso de $a < b$, $a = b$, $a > b$, para $a < b$, basta assumir $q = 0$ que teremos $r = a$. Caso $a = b$, basta assumir $q = 1$ que teremos $r = 0$. Agora para $a > b$ temos que $a > b > 0$, pois por hipótese b é positivo. Consideremos o seguinte conjunto,

$$K = \{a - bq \in \mathbb{Z};\ a - bq \geqslant 0\} \subseteq \mathbb{N} \cup \{0\}.$$

Como $b-a>0$, temos que o conjunto K não é vazio, pois $a-b\in K$. Pelo princípio da boa ordenação, temos que K possui um menor elemento pois $K\subseteq\mathbb{N}\cup\{0\}$, o qual será denotado pela letra r.

Podemos observar que $r=a-bq\geqslant 0$, para algum $q\geqslant 0$ e que $r<b$ pois caso contrário teríamos,

$$r=a-bq\geqslant b\Rightarrow a-b\cdot(q+1)\geqslant 0. \tag{2.1}$$

Por outro lado temos,

$$b>0\Rightarrow a-b\cdot(q+1)<a-bq. \tag{2.2}$$

Das desigualdades 2.1 e 2.2 obtemos que,

$$0\leqslant a-b\cdot(q+1)<a-bq,$$

contradizendo assim o fato de que $r=a-bq$ é o menor elemento não negativo de K.

Agora devemos provar a unicidade de r e q escolhidos. Dado b positivo e q inteiro tal que $b\cdot q\leqslant a$, temos que,

$$b\cdot q\leqslant a<b\cdot(q+1)$$

Subtraindo $b\cdot q$ da desigualdade acima, obtemos:

$$0\leqslant a-b\cdot q<b$$

Como $r=a-b\cdot q$, temos que $0\leqslant r<b$.

Vejamos agora para o caso em que $b_1<0$. Se $b_1<0$, temos que $-b_1>0$, e que existe q_1 e r_1 inteiros tais que:

$$a=(-b_1)\cdot q_1+r_1,\ \ 0\leqslant r_1<-b_1$$

Como $(-b_1)\cdot q_1\leqslant a$, temos que:

$$(-b_1)\cdot q_1\leqslant a<(-b_1)\cdot(q_1+1).$$

Somando $b_1\cdot q_1$ na desigualdade acima, obtemos:

$$0\leqslant a+b_1\cdot q_1<(-b_1)\cdot(q_1+1)+b1\cdot q1$$

$$0\leqslant a+b_1\cdot q_1<-b_1.$$

Como $r_1=a+b_1\cdot q_1$ e $-b_1=|b_1|$, pois $b_1<0$, temos da desigualdade acima que:

$$0\leqslant r_1<-b_1=|b_1|.$$

Demonstraremos agora a sua unicidade. Suponhamos que na divisão de a por b exista um outro quociente t e um outro resto s tal que:

$$a = b \cdot q + r, \;\; 0 \leqslant r < b$$

$$a = b \cdot t + s, \;\; 0 \leqslant s < b.$$

Podemos igualar as equações acima já que $a = a$, com isso obtemos:

$$b \cdot q + r = b \cdot t + s$$

$$b \cdot q - b \cdot t = s - r$$

$$b \cdot (q - t) = s - r.$$

Pela Definição 2, temos que $b \mid s - r$ e como $s < b$ e $r < b$ isso implica que $s - r < b$, portanto a única forma de $b \mid s - r$ é se $s - r = 0$ ou seja $s = r$.

Como $s - r = 0$ temos que :

$$b \cdot (q - t) = 0$$

Notemos que o produto de dois números só é zero se ao menos um deles for igual a zero, e por hipótese temos que b é positivo, logo $q - t = 0$ o que implica que $q = t$. □

Exemplo 7. Pelo Teorema acima temos que 20 dividido por 8 é igual a $20 = 8 \cdot 2 + 4$, onde 2 é denominado como quociente e 4 de resto dessa divisão.

Exemplo 8. Devemos notar que quando dividimos -20 por 8 temos $-20 = 8 \cdot (-3) + 4$ e não $-20 = 8 \cdot (-2) + (-4)$, pois o resto não deve ser maior que zero.

2.4 Máximo Divisor Comum

Sejam a, b números inteiros não nulos, temos que d será um divisor comum de a e b se $d \mid a$ e $d \mid b$.

Se o único divisor comum entre eles for igual a 1, diremos que a e b são primos entre si, ou seja, $mdc(a,b) = 1$.

Definição 3. Um número inteiro p positivo maior que 1 é dito primo, caso não haja divisor d de p satisfazendo $1 < d < p$. Se um número inteiro $a > 1$ não é primo, chamamos ele de número composto.

Assim por exemplo, temos que $2, 3, 5$ e 7 são primos, enquanto $4, 6, 8$ e 9 são números compostos.

Proposição 5. Sejam p e q números primos e r um natural diferente de zero, temos que:

i) Se $p \mid q$, então $p = q$.

ii) Se $p \nmid r$, então $mdc(p,r) = 1$.

iii) Se o $mdc(a,b) = 1$ e $a \mid bc$ então $a \mid c$.

iv) Seja p um número primo e sejam $a_1, ..., a_k \in \mathbb{Z}$. Se $p \mid a_1, ..., a_k$, então $p \mid a_i$ para algum i, $1 \leqslant i \leqslant k$.

Demonstração. i) Como $p \mid q$, temos que $p = 1$ ou $p = q$, pois q é um número primo. Entretanto sabemos que p também é um número primo, logo pela definição temos que p não pode ser igual a 1, então conclui-se que $p = q$.

ii) Temos que o $mdc(p,r) = s$ sendo s um inteiro positivo, logo podemos dizer que $s = 1$ ou $s = p$, pois p é um número primo e pela definição s só poderia assumir esses valores. Mas como $p \nmid r$, e temos que e $s \mid r$, só nos resta dizer que $s = 1$, já que s não pode ser igual a p.

iii) Como a e b são primos entre si e $a \mid bc$, temos que $a = c$ ou $a \mid c$ para algum $d \in \mathbb{N}$, tal que $a \cdot d = c$.

iv) Resolução deste item recorre ao item acima, ou seja, p vai dividir ele mesmo ou vai dividir algum número que seja múltiplo dele.

□

Teorema 2. Teorema Fundamental da aritmética

Todo n inteiro positivo maior ou igual a 2 pode ser escrito de maneira única como um produto de fatores primos, a menos da ordem dos fatores. Especificamente,

$$n = p_1 \cdot p_2 \ldots p_k$$

onde k é um inteiro maior ou igual a 1.

Demonstração. Provaremos por indução a existência da fatoração de n em números primos.

Primeiramente suponhamos que n seja um número composto, pois se n for primo não há o que demonstrar. Para n composto temos que $n = a \cdot b$ com $a, b \in \mathbb{N}$. Por hipótese a e b se decompõem como produto de números primos. Juntando as fatorações de a e b teremos uma fatoração de n em primos.

Para demostrar a unicidade dessa fatoração, tomemos por absurdo que n possui duas fatorações em primos diferentes, ou seja:

$$n = p_1 \cdot p_2 \ldots p_k = q_1 \cdot q_2 \ldots q_m$$

com $p_1 \leqslant \ldots \leqslant p_k$ e $q_1 \leqslant \ldots \leqslant q_m$.

Como $p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$, temos que $p_1 \mid q_1 \cdot q_2 \cdots q_m$, e pela Proposição 5 temos que existe $p \mid q_i$ para algum i com $1 \leqslant i \leqslant m$. Contudo temos que q_i é primo, logo $p_1 = q_i$ e $p_1 \geqslant q_1$. De forma análoga temos que $q_1 \leqslant p_1$, onde $p_1 = q_1$.

Entretanto $\dfrac{n}{p_1} = p_2 \ldots p_k = q_2 \ldots q_m$ admite uma única fatoração em primos, onde $k = m$ e $p_i = q_i$ para todo i, o que contradiz o fato de n te duas fatorações, concluindo assim a demonstração. □

Exemplo 9. Observe os seguintes números como produto de fatores primos:

i) $30 = 2 \cdot 3 \cdot 5$

ii) $700 = 2^2 \cdot 5^2 \cdot 7$

iii) $1800 = 2^3 \cdot 3^2 \cdot 5^2$

Agora iremos definir o máximo divisor comum entre dois inteiros. Euclides nos Elementos fez a seguinte definição para o máximo divisor comum:

Definição 4. Um número inteiro $d \geqslant 0$ é um máximo divisor comum de dois inteiros a e b se possuir as seguintes propriedades:

i) d é um divisor comum de a e b, isto é $d \mid a$ e $d \mid b$.

ii) d é divisível por todo divisor comum de a e b.

Exemplo 10. Observando que os divisores de 20 são dados por $D_{(20)} = \{20, 10, 5, 4, 2, 1\}$, e os divisores de 16 por $D_{(16)} = \{16, 8, 4, 2, 1\}$, temos que $D_{(20,16)} = \{4, 2, 1\}$, portanto $mdc(20, 16) = 4$.

Temos também que os divisores de 15 são dados por $D_{(15)} = \{15, 5, 3, 1\}$, e os divisores de 21 por $D_{(22)} = \{22, 11, 2, 1\}$, então $D_{(15,22)} = \{1\}$, logo $mdc(15, 22) = 1$, ou seja, eles são primos entre si.

Existem alguns casos particulares em que o mdc pode ser calculado de forma imediata, tomemos a e b um inteiro não nulo, temos que:

i) $mdc(a, 0) = |a|$.

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

iii) $mdc(a, a) = |a|$.

iv) Se a é o maior múltiplo de b, então $mdc(a, b) = b$.

Teorema 3. Sejam a, b números inteiros, então temos que,

$$mdc(a,b) = mdc(|a|,b) = mdc(a,|b|) = mdc(|a|,|b|) = x$$

Demonstração. A prova da existência do *mdc* de dois inteiros segue diretamente do segundo item da Proposição 1 e Definição 1. Como o $mdc(a,b) \mid x$, temos que $a = x \cdot c$ e $b = x \cdot d$ para c, d inteiros, logo $mdc(|a|,b) = mdc(|x \cdot c|, x \cdot d) = x$, pois x é o maior fator em comum de $mdc(|a|,b)$. O retante da prova segue de forma análoga. □

O teorema a seguir foi provado pela primeira vez por Claude-Gaspard Bachet de Méziriac (1581-1638) e depois generalizado para polinômios por Étienne Bézout (1730-1783). Ele nos mostra que sempre é possível escrever o *mdc* de dois inteiros como combinação linear destes.

Teorema 4. Teorema de Bachet - Bézout

Sejam a, b números inteiros. Então existem x, y inteiros tais que:

$$ax + by = mdc(a,b).$$

Portanto se c é um inteiro tal que $c \mid a$ e $c \mid b$, então $c \mid mdc(a,b)$.

Demonstração. Considere a seguinte combinação linear:

$$C_{a,b} = \{ax + by \,;\;\; x, y \in \mathbb{Z}\}.$$

Para x e y iguais a zero, temos que o zero também está contido em $C_{a,b}$.

Agora iremos pegar o menor elemento x_0 e y_0 contidos em $C_{a,b} \geqslant 0$, tais que $\gamma = ax_0 + by_0$.

Primeiro iremos provar que $\gamma \mid a$.

Suponhamos por absurdo que $\gamma \nmid a$, logo pela divisão Euclidiana, existem inteiros q e r, tais que $a = \gamma \cdot q + r$ com $0 < r < \gamma$.

Substituindo o valor de γ na equação acima iremos obter:

$$a = (ax_0 + by_0) \cdot q + r$$

Isolando r e reorganizando a equação de forma estratégica teremos que:

$$r = a - q \cdot (ax_0 + by_0)$$
$$r = a \cdot (1 - qx_0) + b \cdot (-qy_0).$$

Com isso temos que r está contido em $C_{a,b}$, o que contradiz a hipótese de que γ ser o menor inteiro positivo contido em $C_{a,b}$.

Para provar que $\gamma \mid b$, vamos seguir de forma análoga a $\gamma \mid a$. Suponhamos por absurdo que $\gamma \nmid b$, logo pela divisão Euclidiana, existem inteiros s e t, tais que $b = \gamma \cdot s + t$ com $0 < t < \gamma$.

Substituindo o valor de γ em na equação acima iremos obter:

$$b = (ax_0 + by_0) \cdot s + t$$

Isolando t e reorganizando a equação de forma estratégica teremos que:

$$t = b - s \cdot (ax_0 + by_0)$$

$$t = a \cdot (-sx_0) + b \cdot (1 - sy_0)$$

Com isso temos que t está contido em $C_{a,b}$, o que contradiz a hipótese de que γ ser o menor inteiro positivo contido em $C_{a,b}$.

Só nos resta provar que $\gamma = d$. Como $d = (a,b)$, existem a_1, b_1 inteiros, tais que $a = d \cdot a_1$ e $b = d \cdot b_1$, logo substituindo esses valores em $\gamma = ax_0 + by_0$ teremos:

$$\gamma = (da_1) \cdot x_0 + (db_1) \cdot y_0.$$

Deixando d em evidência:

$$\gamma = d \cdot (a_1 x_0 + b_1 y_0).$$

Portanto $d \mid \gamma$, logo temos que $d \leqslant \gamma$. Contudo temos que $d < \gamma$ é impossível pois d é o máximo divisor comum de a e b, chegando a conclusão que $d = \gamma = ax_0 + by_0$, terminando assim a demonstração. □

2.5 Congruências

Este tópico é destinado ao estudo da Relação de Congruência. Grande parte dos resultados sobre congruência foram introduzidos por Gauss $(1777 - 1855)$ em um trabalho publicado em 1801 (Disquisitiones Arithmeticae) quando tinha apenas 24 anos.

A Relação de Congruência consiste em um estudo dos restos, onde dois números a e b são ditos congruentes entre si, se possuírem o mesmo resto.

Definição 5. Sejam $a, b, n \in \mathbb{Z}$. Dizemos que a é congruente a b módulo n, se $n \mid a - b$, ou seja, se a e b deixam o mesmo resto na divisão por n. Denotamos essa congruência como:

$$a \equiv b \mod n.$$

Caso a não seja congruente a b módulo n, denotamos por $a \not\equiv b \mod n$

Exemplo 11. De acordo com a definição acima, podemos escrever:

i) $16 \equiv 2 \mod 7$, pois $7 \mid 16-2$, ou seja, 2 e 16 deixam o mesmo resto na divisão por 7.

ii) $-1 \equiv 7 \mod 8$, pois $8 \mid 7-(-1) = 8$ ou seja, -1 e 7 deixam o mesmo resto na divisão por 8.

iii) $3 \not\equiv 5 \mod 6$, pois $6 \nmid 5-3$, ou seja, 3 e 5 não deixam o mesmo resto na divisão por 8.

iv) $x \equiv -x \mod 2$, pois $2 \mid x-(-x) = 2x$, ou seja, x e $-x$ deixam o mesmo resto na divisão por 2.

Proposição 6. Dados a, b, c e $n \in \mathbb{Z}$, sendo $n > 1$ temos:

i) Reflexiva: $a \equiv a \mod n$.

ii) Simétrica: $a \equiv b \mod n$ então $b \equiv a \mod n$.

iii) Transitiva: $a \equiv b \mod n$ e $b \equiv c \mod n$, então $a \equiv c \mod n$.

Demonstração. Podemos observar que:

i) Como $a \equiv a \mod n$, então $n \mid (a-a) = 0$, ou seja, $n \mid 0$, o que é verdade pois $n \cdot 0 = 0$.

ii) Se $a \equiv b \mod n$, então $n \mid -(a-b)$, que é a mesma coisa de dizer que $n \mid (b-a)$, portanto, $n \mid (b-a)$.

Temos por exemplo que $3 \equiv 13 \mod 10$, pois $10 \mid 3-13 = -10$, então $13 \equiv 3 \mod 10$, pois $10 \mid 13-3 = 10$.

iii) Se $a \equiv b \mod n$, então $n \mid a-b$, isso implica que $a-b = k_1 \cdot n$ com $k_1 \in \mathbb{Z}$.

Se $b \equiv c \mod n$, então $n \mid b-c$, isso implica que $b-c = k_2 \cdot n$ com $k_2 \in \mathbb{Z}$.

Somando a equação $a-b = k_1 \cdot n$ mais a equação $b-c = k_2 \cdot n$ teremos que:

$$(a-b)+(b-c) = k_1 \cdot n + k_2 \cdot n$$

$$a-b+b-c = n \cdot (k_1+k_2)$$

$$a-c = n \cdot (k_1+k_2).$$

Como $k_1+k_2 = k_3 \in \mathbb{Z}$, podemos reescrever a equação como:

$$a-c = n \cdot k_3.$$

Logo temos que $n \mid (a-c)$, ou seja $a \equiv c \mod n$.

□

Temos por exemplo que $18 \equiv 3 \mod 5$ e $3 \equiv 23 \mod 5$, então $18 \equiv 23 \mod 5$.

Agora veremos uma maneira de verificar se dois números são congruentes módulo n sem precisar efetuar a divisão Euclidiana em ambos os números por n.

Proposição 7. Sejam a, b e $n \in \mathbb{Z}$, com $n > 1$. Tem-se que $a \equiv b \mod n$ se, e somente se $m \mid a - b$.

Demonstração. Iniciaremos provando que se $a \equiv b \mod n$, então $n \mid a - b$.

Pela divisão Euclidiana, temos que ao dividirmos a e b por n, teremos:

$$a = n \cdot k_1 + r_1, \ \ 0 \leqslant r_1 < k_1.$$

$$b = n \cdot k_2 + r_2, \ \ 0 \leqslant r_2 < k_2.$$

Subtraindo as equações acima, iremos obter que:

$$a - b = (n \cdot k_1 + r_1) - (n \cdot k_2 + r_2).$$

$$a - b = n \cdot (k_1 + k_2) + (r_1 - r_2).$$

Para que $n \mid (a - b)$, teremos que ter $r_1 - r_2 = 0$, ou seja, $r_1 = r_2$.

Agora basta provar que se $n \mid a - b$, então $a \equiv b \mod n$.

Se $n \mid (a - b)$, então $a - b = n \cdot k_3$, com $k_3 \in \mathbb{Z}$, ou seja, $a \equiv b \mod n$, concluindo assim a demonstração. □

Proposição 8. Sejam a, b, c, d e $n \in \mathbb{Z}$, com $n > 1$.

i) Se $a \equiv b \mod n$ e $c \equiv d \mod n$, então $a + c \equiv b + d \mod n$.

ii) Se $a \equiv b \mod n$ e $c \equiv d \mod n$, então $a \cdot c \equiv b \cdot d \mod n$.

Demonstração. Podemos observar que:

i) Se $a \equiv b \mod n$, então $n \mid (a - b)$, logo temos que $a - b = k_1 \cdot n$, com $k_1 \in \mathbb{Z}$.

Se $c \equiv d \mod n$, então $n \mid c - d$, logo temos que $c - d = k_2 \cdot n$, com $k_2 \in \mathbb{Z}$.

Somando as duas igualdades acima, teremos:

$$(a - b) + (c - d) = k_1 \cdot n + k_2 \cdot n$$

$$(a + c) - (b + d) = (k_1 + k_2) \cdot n$$

$$(a + c) - (b + d) = k_3 \cdot n \ , \ \ k_3 \in \mathbb{Z}.$$

Com isso temos que $n \mid (a + c) - (b + d)$, portanto, da definição de congruência, temos que,

$$a + c \equiv b + d \mod n.$$

ii) Se $a \equiv b \mod n$ então $n \mid a-b$, logo $a-b = k_1 \cdot n$, com $k_1 \in \mathbb{Z}$. Agora multiplicando ambos os membros dessa equação por c, teremos:

$$a \cdot c - b \cdot c = k_1 \cdot n \cdot c. \tag{2.3}$$

Se $c \equiv d \mod n$, então $n \mid c-d$, logo $c-d = k_2 \cdot n$, com $k_2 \in \mathbb{Z}$. Agora multiplicando ambos os membros dessa equação por b, teremos:

$$c \cdot b - d \cdot b = k_2 \cdot n \cdot b. \tag{2.4}$$

Somando a Equação 2.3 com a Equação 2.4 (sugestão apenas):

$$a \cdot c + b \cdot c - b \cdot c - d \cdot b = k_1 \cdot n \cdot c + k_2 \cdot n \cdot b$$

$$a \cdot c - d \cdot b = n \cdot (k_1 \cdot c + k_2 \cdot b)$$

$$a \cdot c - d \cdot b = n \cdot k_3 \ , \ \ k_3 \in \mathbb{Z}.$$

Portanto, temos que $n \mid a \cdot c - d \cdot b$, logo $a \cdot c \equiv d \cdot b \mod n$.

□

2.6 Algoritmo de Euclides

Para realizar o cálculo do $mdc(a,b)$ quando a e b assumem valores respectivamente "pequenos"não se exige muito trabalho, mas quando se trata em encontrar o $mdc(a,b)$ com a e b relativamente "grandes"o cálculo acaba se tornando um pouco exaustivo, para determinar o mdc nesses casos podemos fazer o uso de uma ferramenta chamada de Algoritmo de Euclides que é um método bastante eficiente para determinar o máximo divisor comum nesses casos.

Primeiramente veremos o próximo lema que é a base para a obtenção do máximo divisor comum utilizando o Algoritmo de Euclides.

Proposição 9. Sejam a e b inteiros positivos tais que $a = b \cdot q + r$. Então $mdc(a,b) = mdc(b,r)$

Demonstração. Se $mdc(a,b) = d$, então $d \mid a$ e $d \mid b$. Logo d divide qualquer combinação linear entre a e b, ou seja $d \mid (a - b \cdot q) = r$. Portanto $d \mid r$, assim $d \mid mdc(b,r)$. Da mesma forma, se definirmos $mdc(b,r) = c$, teremos que $c \mid (b \cdot q + r) = a$ ou seja $c \mid a$, assim $d \mid mdc(a,b)$. Portanto temos que $d \mid c$ e $c \mid d$, mas como ambos são positivos temos que $d = c$ □

Agora podemos enunciar o Algoritmo de Euclides.

Teorema 5. Algoritmo de Euclides

Dados a e b números inteiros positivos não nulos, realizando sucessivamente a divisão euclidiana obteremos o $mdc(a,b)$.

$$a = b \cdot q + r \ , \ \ 0 \leqslant r < b$$

$$b = r \cdot q_1 + r_1 \ , \ \ 0 \leqslant r_1 < r$$

$$r = r_1 \cdot q_2 + r_2 \ , \ \ 0 \leqslant r_2 < r_1$$

$$r_1 = r_2 \cdot q_3 + r_3 \ , \ \ 0 \leqslant r_3 < r_2$$

$$...$$

$$r_{n-2} = r_{n-1} \cdot q_n + r_n \ , \ \ 0 \leqslant r_n < r_{n-1}$$

$$r_{n-1} = r_n \cdot q_{n+2}$$

O algoritmo para quando encontramos r_n, o último resto não nulo, assim $r_n = mdc(a,b)$.

Demonstração. Pela resultado anterior temos que:

$$mdc(a,b) = mdc(b,r) = mdc(r,r_1) = mdc(r_1,r_2) = ... = mdc(r_{n-1},r_n)$$

Como $r_n \cdot q_{n+2} = r_{n-1}$ temos que $r_n \mid r_{n-1}$, então $mdc(r_{n-1},r_n) = r_n$.

Portanto o $mdc(a,b) = mdc(r_{n-1},r_n) = r_n$.

Agora veremos na prática como esse algoritmo funciona. □

Exemplo 12. Calcule o $mdc(1800,76)$.

Demonstração. Realizando as divisões sucessivas, temos:

$$1800 = 76 \cdot 23 + 52$$

$$76 = 52 \cdot 1 + 24$$

$$52 = 24 \cdot 2 + 4$$

$$24 = 4 \cdot 6.$$

Assim, temos $mdc(1800,76) = mdc(76,52) = mdc(52,24) = mdc(24,4) = 4$. □

Exemplo 13. Calcule o $mdc(1003,106)$.

Demonstração. Realizando as divisões sucessivas, temos:

$$1001 = 106 \cdot 9 + 47$$

$$106 = 47 \cdot 2 + 12$$

$$47 = 12 \cdot 3 + 11$$

$$12 = 11 \cdot 1 + 1$$

$$11 = 1 \cdot 11 + 0$$

Assim, temos $mdc(1001, 106) = mdc(106, 47) = mdc(47, 12) = mdc(12, 11) = 1$. □

CAPÍTULO

3

EQUAÇÕES DIOFANTINAS LINEARES

Este capítulo é dedicado ao estudo de equações diofantinas. Tais equações receberam esse nome em homenagem ao grande matemático grego Diofanto de Alexandria. Sua importância foi tão grande na área da matemática que ele foi considerado por muitos como pai da Álgebra e da Teoria dos Números. Veremos alguns teoremas e proposições que serão aplicados em questões retirados das provas nacionais, como o Exame Nacional de Qualificação (ENQ) do PROFMAT e Olimpíada Brasileira de Matemática (OBM) que tem como finalidade oferecer uma visão prática dos conceitos teóricos aplicados na resolução de equações diofantinas.

3.1 Equações Diofantinas com Duas Incógnitas

Nesta seção veremos equações diofantinas da forma:

$$ax + by = c.$$

Temos que a, b e c são números inteiros e a e b não são ambos nulos. Procuraremos apenas os pares (x, y) de inteiros que são soluções de $ax + by = c$.

Proposição 10. A equação diofantina $ax + by = c$ possui solução nos inteiros se, e somente se, $d \mid c$, com $d = mdc(a, b)$.

Demonstração. Iniciaremos provando a primeira parte. Tomemos por hipótese que exista uma solução para a equação diofantina $ax + by = c$, e a solução seja o par (x_0, y_0) de inteiros. Substituindo esses valores na equação diofantina temos que,

$$ax_0 + by_0 = c.$$

Como o $mdc(a, b) = d$, então $d \mid a$ e $d \mid b$, logo pela Proposição 2, temos que d divide qualquer combinação linear entre a e b, ou seja $d \mid ax_0 + by_0 = c$; portanto, temos que $d \mid c$.

Agora mostremos que a recíproca é verdadeira. Por hipótese temos que $d = mdc(a,b) \mid c$, então existe um f inteiro tal que $f \cdot d = c$. Pelo Teorema 4 (Bachet - Bézout), existem x_0 e y_0 inteiros tais que $ax_0 + by_0 = d$. Agora multiplicando por f ambos os lados da igualdade teremos,

$$(ax_0) \cdot f + (by_0) \cdot f = d \cdot f.$$

Como $d \cdot f = c$ temos que:

$$(ax_0) \cdot f + (by_0) \cdot f = c.$$

Sendo assim a equação diofantina admite a solução $x = x_0 \cdot f$ e $y = y_0 \cdot f$.

Proposição 11. Se x_0 e y_0 são uma solução particular da equação $ax+by=c$, onde $mdc(a,b) = 1$, então sua solução geral é dada pelas seguintes expressões em que t é um inteiro:

$$x = x_0 + tb \qquad e \qquad y = y_0 - ta.$$

Demonstração. Se (x_0, y_0) é solução de $ax + by = c$ então,

$$ax_0 + by_0 = c.$$

Como $ax + by = c$ e $ax_0 + by_0 = c$, podemos igualar as duas equações,

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

Consequentemente,

$$a \cdot (x - x_0) = b \cdot (y_0 - y).$$

Como $mdc(a,b) = 1$, logo $a \mid (y_0 - y)$, então sabemos que existe um t inteiro tal que $y_0 - y = t \cdot a$, portanto $y = y_0 - t \cdot a$.

Agora substituindo o valor de y na igualdade anterior obtemos:

$$a \cdot (x - x_0) = b \cdot (y_0 - (y_0 - ta))$$

$$a \cdot (x - x_0) = b \cdot (ta).$$

Dividindo por a ambos os lados da igualdade teremos,

$$bt = x - x_0.$$

Logo $x = x_0 + tb$, o que mostra que são soluções para a equação diofantina.

Agora mostremos que a recíproca é verdadeira. Para isso iremos substituir o valores de x e y encontrados na equação $ax+by=c$.

$$a\cdot(x_0+tb)+b\cdot(y_0-ta)=c.$$

Fazendo a distributiva obtemos:

$$ax_0+atb+by_0-bta=c.$$

Logo,

$$ax_0+by_0=c.$$

Então temos que os pares (x_0,y_0) de inteiros são uma solução particular da equação diofantina $ax+by=c$, assim concluímos a demonstração. □

Veremos agora alguns exemplos de equações diofantinas em que serão aplicados alguns teoremas e proposições que forma vistas até o momento.

Exemplo 14. Iremos mostrar um método para resolver a equação diofantina $22x+14y=100$.

Demonstração. Pela Proposição 10 temos que a equação diofantina possui solução, visto que $mdc(22,14)=2\mid 100$, portanto existe solução nos inteiros que satisfaz essa equação.

Dividindo por 2 ambos os lados da equação $22x+14y=100$, obtemos a equação equivalente:

$$11x+7y=50.$$

Aplicando o Algoritmo de Euclides, encontraremos uma solução particular (x_0,y_0) :

$$11=7\cdot 1+4$$

$$7=4\cdot 1+3$$

$$4=3\cdot 1+1.$$

Isolando os restos dessas igualdades teremos que:

$$4=11-7\cdot 1$$

$$3=7-4\cdot 1$$

$$1=4-3\cdot 1. \tag{3.1}$$

Agora substituindo de forma estratégica as igualdades acima em 3.1 teremos:

$$1=4-(7-4\cdot 1)\cdot 1=4\cdot 2-7.$$

Continuando,

$$1 = 4 \cdot 2 - 7 = (11 - 7 \cdot 1) \cdot 2 - 7 = 11 \cdot 2 - 7 \cdot 3.$$

Multiplicando a igualdade acima por 50 iremos encontrar uma solução particular da equação diofantina $11x + 7y = 50$

$$11 \cdot (2 \cdot 50) + 7 \cdot (3 \cdot 50) = 1 \cdot 50$$

$$11 \cdot 100 + 7 \cdot (-150) = 50$$

Como $x_0 = 100$ e $y_0 = -150$ é solução particular da equação, pela Proposição 11 temos que as soluções são iguais a $x = x_0 + tb$ e $y = y_0 - ta$, logo as soluções da equação diofantina $22x + 14y = 100$ podem ser encontradas por:

$$x = 100 + 7t \quad \text{e} \quad y = -150 - 11t; \qquad t \in \mathbb{Z}.$$

□

No caso do exemplo anterior, ao fazermos t percorrer todos os números inteiros, encontraremos as infinitas soluções dessa equação diofantina, mas existem casos em que procuramos uma quantidade restrita de soluções, vejamos a seguir:

Exemplo 15. Duas crianças sobem uma escada, uma subiu os degraus pulando-os de 3 em 3, assim restaram apenas 2 degraus para que ela chegasse no final da escada, já a outra criança subiu os degraus pulando-os de 2 em 2, restando assim apenas um degrau no final da escada. Determine quantos degraus essa escada possuía, sabendo que a quantidade de degraus é um número múltiplo de 7 e estão compreendidos entre 50 e 90.

Demonstração. Temos da primeira criança que a quantidade de degraus é um número que quando multiplicado por 3 deixa resto 2, então se chamarmos de d a quantidade de degraus teremos que $d = 3x + 2$, logo da segunda criança temos que a quantidade de degraus é um número que quando multiplicado por 2 deixa resto 1, ou seja, $d = 2y + 1$. Igualando essas duas equações temos:

$$3x + 2 = 2y + 1.$$

Logo,

$$3x - 2y = -1.$$

Pela Proposição 10 temos que a equação diofantina $3x - 2y = -1$, possui solução, pois $mdc(3,2) = 1 \mid (-1)$. É fácil ver que $x_0 = 1$ e $y_0 = 2$ são uma solução particular para essa equação. Logo as soluções da equação diofantina $3x - 2y = -1$ podem ser encontradas por:

$$x = 1 - 2t \quad \text{e} \quad y = 2 - 3t; \qquad t \in \mathbb{Z}.$$

Para concluir este exercício teremos que encontrar todos os valores de d que sejam múltiplos de 7 e estão compreendidos entre 50 e 90. Como $d = 3x+2$ e $d = 2y+1$, ao substituirmos x ou y encontrados, teremos que,

$$d = 5 - 6t.$$

Buscamos soluções que estão compreendidas entre 50 e 90 portanto,

$$50 < 5 - 6t < 90.$$

Subtraindo 5 unidades dessa desigualdade,

$$45 < -6t < 85.$$

Agora dividindo por -6 teremos que,

$$-7,5 < t < 14,16\ldots$$

Temos que t está compreendido entre os inteiros -7 e 14. Logo os valores possíveis para $d = (47,53,59,65,71,77,83,89)$.

Como a quantidade de degraus é um número divisível por 7, temos que a única solução possível é de $d = 77$. □

No exemplo anterior percebemos que achar uma solução particular para a equação diofantina $3x - 2y = -1$ foi fácil, pois os coeficientes da equação são relativamente baixos, entretanto existem casos em que encontrar uma solução particular se torna algo mais difícil, isso pode ocorrer quando os coeficientes da equação diofantina são relativamente altos, e as vezes encontrar uma solução particular usando o Algoritmo de Euclides se tornar muito mais trabalhoso. Portanto iremos mostrar outro método para encontrar uma solução particular de uma equação diofantina no próximo exemplo.

Exemplo 16. Encontre as soluções da equação diofantina $7x + 19y = 120$.

Demonstração. Pela Proposição 10, percebemos que existe solução para essa equação, pois $mdc(7,19) = 1 \mid 120$. Agora iremos resolver esse problema utilizando congruências lineares. Para isso precisamos escrever a equação diofantina $ax + by = c$ como uma congruência do tipo:

$$ax \equiv c \mod b.$$

Resolver a equação $ax + by = c$ equivale a resolver a congruência $ax \equiv c \mod b$, ou seja, encontrar a classe de equivalência $[x]$ tal que $a \cdot x \equiv c \mod b$.

Usando o módulo 7 na equação $7x + 19y = 120$, teremos:

$$\overline{5} \cdot \overline{Y} \equiv \overline{1} \mod 7; \qquad y \in \mathbb{Z}.$$

Como $\overline{5}\cdot\overline{3} \equiv \overline{15} \equiv \overline{1} \mod 7$, temos que se multiplicarmos a congruência anterior pela classe de equivalência $\overline{3}$ temos:

$$\overline{3}\cdot\overline{5}\cdot\overline{Y} \equiv \overline{3}\cdot\overline{1} \mod 7.$$

Portanto,

$$\overline{15}\cdot\overline{Y} \equiv \overline{3} \mod 7.$$

Como $\overline{15} \equiv \overline{1} \mod 7$, podemos substituir, logo:

$$\overline{Y} \equiv \overline{3} \mod 7.$$

Logo temos que:

$$y = 3 + 7t; \qquad y,\ t \in \mathbb{Z}.$$

Agora substituindo o valor de y na equação principal $7x + 19y = 120$ encontraremos o valor de x em função da variável t.

$$7x + 19\cdot(3 + 7t) = 120.$$

Fazendo a distributiva,

$$7x + 57 + 133t = 120.$$

logo temos que,

$$7x = 63 - 133t.$$

Daí temos que $x = 9 - 19t$.

Portanto as soluções da equação diofantina $7x + 19y = 120$ podem ser encontradas por:

$$x = 9 - 19t \quad e \quad y = 3 + 7t; \qquad t \in \mathbb{Z}.$$

□

Exemplo 17. (ENQ-2022.2, 2022) Resolva a congruência $17x \equiv 82 \mod 165$.

Demonstração. Da congruência temos que $17x = 82 + 165y$, portanto,

$$17x - 165y = 82.$$

Pela Proposição 10 temos que a equação diofantina $17x - 165y = 82$ possui solução, pois $mdc(17, 165) = 1 \mid 82$.

Aplicando o Algoritmo de Euclides, encontraremos uma solução particular (x_0, y_0) :

$$165 = 17\cdot 9 + 12$$

$$17 = 12 \cdot 1 + 5$$

$$12 = 5 \cdot 2 + 2$$

$$5 = 2 \cdot 2 + 1.$$

Isolando os restos dessas igualdades teremos que:

$$12 = 165 - 17 \cdot 9. \tag{3.2}$$

$$5 = 17 - 12 \cdot 1. \tag{3.3}$$

$$2 = 12 - 5 \cdot 2. \tag{3.4}$$

$$1 = 5 - 2 \cdot 2. \tag{3.5}$$

Substituindo de forma estratégica a Equação 3.4 na Equação 3.5 teremos:

$$1 = 5 - 2 \cdot 2 = 5 - (12 - 5 \cdot 2) \cdot 2 = 5 \cdot 5 - 12 \cdot 2.$$

Agora substituindo a Equação 3.3 na equação acima:

$$1 = 5 \cdot 5 - 12 \cdot 2 = 5 \cdot (17 - 12 \cdot 1) - 12 \cdot 2 = 5 \cdot 17 - 12 \cdot 7.$$

Efetuando a substituição da Equação 3.2 na equação acima:

$$1 = 5 \cdot 17 - 12 \cdot 7 = 5 \cdot 17 - (165 - 17 \cdot 9) \cdot 7$$

$$17 \cdot 68 - 165 \cdot 7 = 1.$$

Multiplicando a igualdade acima por 82 iremos encontrar uma solução particular da equação diofantina $17x - 165y = 82$.

$$17 \cdot (68 \cdot 82) - 165 \cdot (7 \cdot 82) = 1 \cdot 82$$

$$17 \cdot 5576 - 165 \cdot 574 = 82.$$

Temos que $x_1 = 5576$ e $y_1 = 574$ é uma solução particular de $17x - 165y = 82$. E pela Proposição 11, temos que a solução geral da equação diofantina é igual a:

$$x = 5576 - 165t \quad \text{e} \quad y = 574 - 17t\ ; \qquad t \in \mathbb{Z}.$$

□

Exemplo 18. (ENQ-2017.1, 2017) Resolva a congruência $13x \equiv 1 \ mod\ 2436$.

Demonstração. Da congruência temos que acima temos que $13x = 1 + 2436y$, portanto,

$$13x - 2436y = 1.$$

Pela Proposição 10 temos que a equação diofantina $13x - 2436y = 1$, possui solução, pois $mdc(13, 2436) = 1 \mid (1)$.

Aplicando o Algoritmo de Euclides, encontraremos uma solução particular (x_0, y_0) :

$$2436 = 13 \cdot 187 + 5$$

$$13 = 5 \cdot 2 + 3$$

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1.$$

Isolando os restos dessas igualdades teremos que:

$$5 = 2436 - 13 \cdot 187. \tag{3.6}$$

$$3 = 13 - 5 \cdot 2. \tag{3.7}$$

$$2 = 5 - 3 \cdot 1. \tag{3.8}$$

$$1 = 3 - 2 \cdot 1. \tag{3.9}$$

Substituindo de forma estratégica a Equação 3.8 na Equação 3.9 teremos:

$$1 = 3 - (5 - 3 \cdot 1) \cdot 1 = 3 \cdot 2 - 5 \cdot 1.$$

Agora substituindo a Equação 3.7, na equação acima:

$$1 = 3 \cdot 2 - 5 \cdot 1 = (13 - 5 \cdot 2) \cdot 2 - 5 \cdot 1 = 13 \cdot 2 - 5 \cdot 5$$

Efetuando a substituição da Equação 3.6 na equação acima:

$$1 = 13 \cdot 2 - 5 \cdot 5 = 13 \cdot 2 - (2436 - 13 \cdot 187) \cdot 5$$

$$13 \cdot 937 - 2436 \cdot 5 = 1$$

Temos que $x_1 = 937$ e $y_1 = 5$ é uma solução particular de $13x - 2436y = 1$. E pela Proposição 11, temos que a solução geral da equação diofantina é igual a:

$$x = 937 - 2436t \quad \text{e} \quad y = 5 - 13t \; ; \qquad t \in \mathbb{Z}.$$

□

Exemplo 19. (OBM, 1999) Contando-se os alunos de uma classe de 4 em 4 sobram 2 e contando-se de 5 em 5 sobram 1. Sabendo-se que 15 alunos são meninas e que nesta classe o número de meninas é maior que o número de meninos, o número de meninos é igual a?

Demonstração. Temos que a quantidade de alunos é um número que quando multiplicado por 4 deixa resto 2. Assim se chamarmos de d a quantidade de alunos teremos que $d = 4x+2$ para algum inteiro x. Agora da segunda informação temos que a quantidade de crianças é um número que quando multiplicado por 5 deixa resto 1, ou seja, $d = 5y+1$ para algum inteiro y. Igualando essas duas equações temos:

$$4x+2 = 5y+1.$$

Logo,

$$4x-5y = -1.$$

Pela Proposição 10 temos que a equação diofantina $4x-5y = -1$, possui solução, pois $mdc(4,5) = 1 \mid (-1)$. É fácil ver que $x_0 = 1$ e $y_0 = 1$ são uma solução particular para essa equação. Logo as soluções da equação diofantina $4x-5y = -1$ podem ser encontradas por:

$$x = 1-5t \quad e \quad y = 1-4t; \qquad t \in \mathbb{Z}. \tag{3.10}$$

Para concluir este exercício temos que 15 alunos são meninas e que a quantidade de meninas é maior do que a quantidade de meninos, logo a quantidade de alunos esta compreendida entre $15 \leqslant d < 30$, a princípio pode só ter meninas neta sala. Como $d = 4x+2$ e $d = 5y+1$, ao substituirmos x ou y encontrados na Equação 3.10, teremos que,

$$d = 6-20t.$$

Buscamos soluções que estão compreendidas entre 15 e 30 portanto,

$$15 \leqslant 6-20t < 30.$$

Subtraindo 6 unidades dessa desigualdade,

$$9 \leqslant -20t < 24.$$

Agora dividindo por -20 teremos que,

$$-0,4 > t \geqslant -1,2...$$

Temos que t é um inteiro, logo os valores possíveis para $t = -1$. Como a quantidade de alunos é igual a $d = 6-20t$:

$$d = 6-20\cdot(-1)$$

$$d = 6 + 20 = 26.$$

Como temos 15 meninas na sala, o total de meninos é igual a $26 - 15 = 11$. Portanto, essa sala possui 11 meninos. □

Exemplo 20. (OBM, 2003)Você possui muitos palitos de 6 cm e 7 cm de comprimento. Para fazer uma fila de palitos com comprimento total de 2 metros, o número mínimo de palitos que você precisa utilizar é?

Demonstração. Iremos precisar de x de palitos de 6 cm e de y palitos de 7 cm para termos 2 metros de palitos, que é igual a 200 cm. Logo, temos que resolver a seguinte equação:

$$6x + 7y = 200. \tag{3.11}$$

Pela Proposição 10 temos que a equação diofantina $6x + 7y = 200$, possui solução, pois $mdc(6,7) = 1 \mid (200)$. Para facilitar na resolução dessa equação, iremos trabalhar com uma equação mais simples, para depois retornarmos na original. Pelo Teorema 4 (Bachet - Bézout), temos que existem x_0 e y_0 inteiros tais que:

$$6x_0 + 7y_0 = 1.$$

Uma solução particular para essa equação é $x_0 = -1$ e $y_0 = 1$, logo temos que:

$$6 \cdot (-1) + 7 \cdot 1 = 1.$$

Agora multiplicando ambos os lados dessa igualdade por 200, encontraremos uma solução particular da Equação 3.11:

$$6 \cdot (-1) \cdot (200) + 7 \cdot (1) \cdot (200) = 1 \cdot (200)$$

$$6 \cdot (-200) + 7 \cdot (200) = 200.$$

Portanto $x_1 = -200$ e $y_1 = 200$ são uma solução particular da Equação 3.11. E pela Proposição 11, temos que a solução geral da equação $6X + 7Y = 200$ é igual a:

$$x = -200 + 7t \quad e \quad y = 200 - 6t\ ; \qquad t \in \mathbb{Z}. \tag{3.12}$$

Como estamos em busca da quantidade mínima de palitos para conseguirmos ter 200 cm de palitos, teremos que ter a quantidade mínima de palitos de 6 cm.

Temos que a incógnita x nos mostra q quantidade de palitos de 6 cm. Logo para que $x = -200 + 7t$ seja o menor número natural, teremos que assumir $t = 29$.

$$x = -200 + 7 \cdot 29 = -200 + 203 = 3$$

Com $t = 29$, teremos que a quantidade de palitos de 7 cm sera igual:

$$y = 200 - 6 \cdot 29 = 200 - 174 = 26$$

Portanto a quantidade minima de palitos usados para termos 2 metros será igual a $3 + 26 = 29$ palitos. □

Exemplo 21. (ENQ-2018.2, 2018) Considere a equação diofantina linear $5x + 3y = 2018$. Escreva a solução geral em $\mathbb{Z}$.

Demonstração. Pela Proposição 10, temos que a equação diofantina $5x + 3y = 2018$ possui solução, pois $mdc(5,3) = 1 \mid 2018$.Para facilitar na resolução dessa equação, iremos trabalhar com uma equação mais simples, para depois retornarmos na original. Pelo Teorema 4 (Bachet - Bézout), temos que existem x_0 e y_0 inteiros tais que:

$$5x_0 + 3y_0 = 1.$$

Uma solução particular para essa equação é $x_0 = 2$ e $y_0 = -3$, logo temos que:

$$5 \cdot 2 + 3 \cdot (-3) = 1.$$

Agora multiplicando ambos os lados dessa equação por 2018, teremos:

$$5 \cdot 2 \cdot 2018 + 3 \cdot (-3) \cdot 2018 = 1 \cdot 2018$$

$$5 \cdot 4036 + 3 \cdot (-6054) = 2018.$$

Logo,

$$x_0 = 4036$$

$$y_0 = -6054$$

Como (x_0, y_0) é uma solução particular da equação, pela Proposição 11 temos que as soluções são iguais a $x = x_0 + tb$ e $y = y_0 - ta$. Logo temos que a solução geral da equação diofantina $5x + 3y = 2018$ em $\mathbb{Z}$ é dada por:

$$x = 4036 + 3t \quad \text{e} \quad y = -6054 - 5t; \qquad t \in \mathbb{Z}.$$

□

Exemplo 22. (ENQ-2019.1, 2019) Determine o menor número natural c para o qual a equação difantina $5x + 7y = c$, tenha exatamente 4 soluções em $\mathbb{N} \cup \{0\}$. Determine, explicitamente, as 4 soluções obtidas anteriormente.

Pela Proposição 10, temos que a equação diofantina $5x+7y=c$ possui solução, pois $mdc(5,7)=1 \mid c$. Para facilitar na resolução dessa equação, iremos trabalhar com uma equação mais simples, para depois retornarmos na original. Pelo Teorema 4 (Bachet - Bézout), temos que existem x_0 e y_0 inteiros tais que:

$$5x_0+7y_0=1.$$

Uma solução particular para essa equação é $x_0=-4$ e $y_0=3$, logo temos que:

$$5\cdot(-4)+7\cdot 3=1.$$

Agora multiplicando ambos os lados dessa equação por c, teremos:

$$5\cdot(-4)\cdot c+7\cdot 3\cdot c=1\cdot c$$

$$5\cdot(-4c)+7\cdot 3c=c.$$

Portanto $x_1=-4c$ e $y_1=3c$ é uma solução particular da equação $5X+7Y=c$. E pela Proposição 11, temos que a solução geral da equação $5X+7Y=c$ é igual a:

$$x=-4c+7t \quad e \quad y=3c-5t\ ; \qquad t\in\mathbb{Z}. \tag{3.13}$$

Como procuramos soluções em $\mathbb{N}\cup\{0\}$, temos que:

$$x=-4c+7t\geq 0 \quad e \quad y=3c-5t\geq 0$$

$$x=-4c\geq -7t \quad e \quad y=3c\geq 5t.$$

Dividindo a primeira inequação por -7 e a segunda inequação por 5 teremos:

$$x=\frac{-4c}{-7}\geq\frac{-7t}{-7} \quad e \quad y=\frac{3c}{5}\geq\frac{5t}{5}$$

$$x=\frac{4c}{7}\leq t \quad e \quad y=\frac{3c}{5}\geq t.$$

Logo,

$$\frac{4c}{7}\leq t\leq\frac{3c}{5}; \qquad t\in\mathbb{Z}. \tag{3.14}$$

Como queremos quatro soluções, temos que:

$$\frac{3c}{5}-\frac{4c}{7}\geq 3.$$

Resolvendo essa inequação teremos:

$$\frac{21c-20c}{35}\geq\frac{105}{35}$$

$$\frac{c}{35} \geq \frac{105}{35}$$
$$c \geq 105.$$

Considerando $c = 105$ e substituindo na Equação 3.14 encontraremos o intervalo em que t se encontra.

$$\frac{4 \cdot 105}{7} \leq t \leq \frac{3 \cdot 105}{5}; \qquad t \in \mathbb{Z}$$
$$\frac{420}{7} \leq t \leq \frac{315}{5}; \qquad t \in \mathbb{Z}$$
$$60 \leq t \leq 63; \qquad t \in \mathbb{Z}.$$

Portanto, exatamente quatro soluções correspondentes a $t = 60, 61, 62$ e 63. E para que a equação diofantina $5x + 7y = c$ tenha exatamente 4 soluções em $\mathbb{N} \cup \{0\}$, o menor número natural que c pode assumir é 105.

$$5X + 7Y = 105.$$

Para determinar as quatro soluções, basta substituir os valores de c e t na Equação 3.13.

$$x = -4c + 7t \quad \text{e} \quad y = 3c - 5t\ ; \qquad t \in \mathbb{Z}.$$

Logo as soluções da equação diofantina são $(0,15), (7,10), (14,5), (21,0)$, terminando assim o exemplo.

3.2 Equações Diofantinas com Três Incógnitas

Uma equação diofantina com três incógnitas é da forma:

$$ax + by + cz = p$$

onde a, b, c e p são números inteiros e a, b e c não são todos nulos. Procuraremos apenas ternos (x, y, z) de inteiros que são soluções de $ax + by + cz = p$.

De modo semelhante a equação diofantina com duas incógnitas temos que:

Proposição 12. A equação diofantina $ax + by + cz = p$ possui solução nos inteiros se, e somente se, $d \mid p$, com $d = mdc(a, b, c)$.

Demonstração. Iniciaremos provando a primeira parte, tomemos por hipótese que exista uma solução para a equação diofantina $ax + by + cz = p$, e a solução seja o terno (x_0, y_0, z_0) de inteiros. Substituindo esses valores na equação diofantina temos que,

$$ax_0 + by_0 + cz_0 = p$$

Como o $mdc(a,b,c) = d$ então $d \mid a$, $d \mid b$ e $d \mid c$, logo pela Proposição 2, temos que d divide qualquer combinação linear entre a, b e c, ou seja $d \mid ax_0 + by_0 + cz_0 = p$, portanto temos que $d \mid p$.

Agora veremos se a recíproca é verdadeira, por hipótese temos que $d = mdc(a,b,c) \mid p$, então existe um f inteiro tal que $f \cdot d = p$. Pelo Teorema de Bézout, existem x_0, y_0 e z_0 inteiros tais que $ax_0 + by_0 + cz_0 = d$. Agora multiplicando por f ambos os lados dessa igualdade teremos:

$$(ax_0) \cdot f + (by_0) \cdot f + (cz_0) \cdot f = d \cdot f$$

Como $d \cdot f = p$ temos que:

$$(ax_0) \cdot f + (by_0) \cdot f + (cz_0) \cdot f = p$$

Sendo assim a equação diofantina admite a solução $x = x_0 \cdot f$, $y = y_0 \cdot f$ e $z = z_0 \cdot f$. □

Proposição 13. Se (x_0, y_0, z_0) é uma solução particular da equação $ax + by + cz = p$, então sua solução geral é dada pelas seguintes expressões sendo k_0, r_0 e t números inteiros.

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

Demonstração. Iniciaremos reescrevendo a equação $ax + by + cz = p$ como

$$ax + by = p - cz \tag{3.15}$$

Como por hipótese existe solução para equação, temos que $(a,b) \mid f = (p - cz)$ com f inteiro. E pela divisão euclidiana sabemos que z pode ser escrito como $(a,b) \cdot q + r$, sendo r e q inteiros, com $0 \leq r < (a,b)$

Escrevendo z dessa maneira e substituindo em $p - cz$ teremos:

$$p - cz = p - c \cdot ((a,b) \cdot q + r)$$

$$p - cz = (p - cr) - cq \cdot (a,b) \tag{3.16}$$

Como $(a,b) \mid (p - cz) = (p - cr) - cq \cdot (a,b)$ e sabemos que $(a,b) \mid -cq \cdot (a,b)$, logo temos que $(a,b) \mid (p - cr)$. Então existe um k inteiro tal que $(p - cr) = (a,b) \cdot k$, isolando p nessa igualdade teremos:

$$p = (a,b) \cdot k + cr$$

Essa equação admite soluções inteiras para k e r, sendo $((a,b),c) = (a,b,c)$ e que por hipótese temos que $(a,b,c) \mid p$. Logo podemos encontrar k_0 e r_0 tal que

$$(a,b) \cdot k_0 + cr_0 = p \tag{3.17}$$

$$(p - cr_0) = (a,b) \cdot k_0$$

Agora substituindo k e r por k_0 e r_0 na Equação 3.16:

$$p - cz = (p - cr) - cq \cdot (a,b)$$

$$p - cz = (p - cr_0) - cq \cdot (a,b) \tag{3.18}$$

Da Equação 3.17 temos que $(a,b) \cdot k_0 = p - cr_0$, logo substituindo na Equação 3.18 teremos

$$p - cz = (a,b) \cdot (k_0 - cq)$$

Da Equação 3.15 temos que $ax + by = p - cz$, portanto

$$ax + by = (a,b) \cdot (k_0 - cq)$$

Agora buscamos (x_0, y_0) tais que $ax_0 + by_0 = (a,b)$. Multiplicando os ambos lados dessa igualdade por $(k_0 - cq)$ obtemos:

$$a(x_0(k_0 - cq)) + b(y_0(k_0 - cq)) = (a,b) \cdot (k_0 - cq) \tag{3.19}$$

Essa equação possui solução já que $(a,b) \mid (a,b) \cdot (k_0 - cq)$ e pela Proposição 11 temos que a solução geral dessa equação diofantina é dada pelas seguintes expressões em que t é um inteiro:

$$x = x_0 \cdot (k_0 - cq) + bt \quad \text{e} \quad y = y_0 \cdot (k_0 - cq) - at$$

E como foi dito no início da demonstração, temos que $z = (a,b) \cdot q + r_0$, terminando assim a demonstração. □

Para ficar mais claro a compreensão, vamos ver um exemplo:

Exemplo 23. Qual a solução geral da equação diofantina $7x + 35y + 11z = 213$.

Demonstração. Pela Proposição 12, temos que a equação possui solução, pois temos que o $mdc(7,35,11) = 1 \mid 213$. Iniciaremos a demonstração reescrevendo a equação $7x + 35y + 11z = 213$, como:

$$7x + 35y = 213 - 11z \tag{3.20}$$

Usando o mesmo raciocínio utilizado acima, temos que a Equação 3.20 só possui solução se $(7,35) = 7 \mid (213 - 11z)$. E pela divisão euclidiana sabemos que z pode ser escrito como $z = 7 \cdot q + r$, sendo r e q inteiros, com $0 \leq r < 7$.

Logo, também podemos escrever 213 como $213 = 7 \cdot 30 + 3$.

Temos daí que:

$$213 - 11z = 7 \cdot 30 + 3 - 11 \cdot (7q + r)$$

$$213 - 11z = 7 \cdot 30 + 3 - 11 \cdot 7q \cdot -11r$$

$$213 - 11z = 7 \cdot (30 - 11q) + 3 - 11r$$

Portanto para que $7 \mid (213 - 11z) = 7 \cdot (30 - 11q) + 3 - 11r$, teremos que encontrar um valor para r, tal que $7 \mid (3 - 11r)$, com $0 \leq r < 7$, o único valor possível é $r = 6$. Temos então que $z = 7 \cdot q + 6$.

Substituindo z na Equação 3.20 teremos:

$$7x + 35y = 213 - 11 \cdot (7q + 6)$$

$$7x + 35y = 213 - 77q - 66$$

$$7x + 35y = 147 - 77q$$

Dividindo ambos os lados da última equação por 7, teremos uma equação equivalente:

$$1x + 5y = 21 - 11q \tag{3.21}$$

Para facilitar na resolução dessa equação, iremos resolver uma equação mais simples, para depois retornarmos na original, ou seja, tomemos que:

$$1x + 5y = 1$$

Uma solução particular para essa equação é $x_0 = -4$ e $y_0 = 1$, portanto:

$$1 \cdot (-4) + 5 \cdot 1 = 1$$

Agora multiplicando ambos os lados da equação por $21 - 11q$, teremos:

$$1 \cdot (-4) \cdot (21 - 11q) + 5 \cdot 1 \cdot (21 - 11q) = 1 \cdot (21 - 11q)$$

$$1 \cdot (84 - 44q) + 5 \cdot (21 - 11q) = 21 - 11q$$

Portanto $x_1 = 84 - 44q$ e $y_1 = 21 - 11q$ é uma solução particular da Equação 3.21.

E pela Proposição 11, temos que a Equação 3.21 possui solução geral igual a:

$$x = -84 + 44q + 5t \quad e \quad y = 21 - 11q - t \quad \text{com } t, t_1 \in \mathbb{Z}$$

Como $z = 7q + 6$ temos que a solução geral da equação $7x + 35y + 11z = 213$ é igual:

$$\begin{cases} x = -84 + 44q + 5t \\ y = 21 - 11q - t \\ z = 7q + 6 \end{cases} \text{, com } q \text{ e } t \in \mathbb{Z}.$$

□

Agora vamos ver outra forma de resolver uma equação diofantina com três incógnitas.

Exemplo 24. Encontre a solução geral da equação diofantina $3x + 5y + 7z = 34$.

Demonstração. Pela Proposição 12, temos que a equação possui solução, pois temos que o $mdc(3,5,7) = 1 \mid 34$. Iniciaremos a demonstração assumindo que $3x + 5y = p$, logo podemos escrever a equação original como:

$$p + 7z = 34 \tag{3.22}$$

Como $p_0 = 6$ e $z_0 = 4$ é uma solução particular da Equação 3.22 e temos que o $mdc(1,7) = 1$, pela Proposição 11 sua solução geral é dada por:

$$p = 6 + 7t \quad \text{e} \quad z = 4 - t; \qquad t \in \mathbb{Z}$$

No início da demonstração assumimos que $3x + 5y = p$, logo podemos igualar esse valor com a igualdade acima.

$$3x + 5y = 6 + 7t \tag{3.23}$$

Pela Proposição 10 temos que a Equação 3.23 possui solução, pois $mdc(3,5) = 1$ e $1 \mid (6 + 7t)$.

Aplicando o Algoritmo de Euclides em $(3,5)$:

$$5 = 3 \cdot 1 + 2$$

$$3 = 2 \cdot 1 + 1$$

Agora isolando os restos dessas igualdades teremos:

$$2 = 5 - 3 \cdot 1$$

$$1 = 3 - 2 \cdot 1$$

Substituindo as igualdades acima uma nas outras, ou seja:

$$1 = 3 - (5 - 3 \cdot 1) \cdot 1$$

$$1 = 3 \cdot 2 + 5 \cdot (-1).$$

Multiplicando de forma estratégica a última igualdade por $6 + 7t$, acharemos uma solução particular da Equação 3.23:

$$(6 + 7t) \cdot 1 = 3 \cdot 2 \cdot (6 + 7t) + 5 \cdot (-1) \cdot (6 + 7t).$$

Reorganizando teremos:

$$6 + 7t = 3 \cdot (12 + 14t) + 5 \cdot (-6 - 7t)$$

$$3 \cdot (12 + 14t) + 5 \cdot (-6 - 7t) = 6 + 7t.$$

Pela Proposição 11, temos que a Equação 3.23 possui solução geral igual a:

$$x = 12 + 14t + 5t_1 \quad \text{e} \quad y = -6 - 7t - 3t_1 \quad , \text{com } t,\ t_1 \in \mathbb{Z}.$$

Como $z = 4 - t$ temos que a solução geral da equação $3x + 5y + 7z = 34$ é igual:

$$\begin{cases} x = 12 + 14t + 5t + 1 \\ y = -6 - 7t - 3t_1 \qquad , \text{com } t \text{ e } t_1 \in \mathbb{Z}. \\ z = 4 - t \end{cases}$$

□

3.3 Equações Diofantinas com N Incógnitas

Definição 6. Uma equação diofantina é qualquer equação polinomial com coeficientes inteiros com uma ou mais incógnitas. Ou seja, uma equação diofantina é da forma:

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = b \tag{3.24}$$

onde $a_1, \cdots, a_n$ são inteiros dados, chamados coeficientes, b que também é um inteiro dado, é chamado constante e $x_1, \cdots, x_n$ são as incógnitas.

3.3.1 Solução Geral

Para encontrar a solução geral da equação diofantina de n variáveis, utilizaremos o mesmo método utilizado para resolver equações diofantinas com três variáveis, ou seja, devemos reduzir a equação $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n = b$ em uma equação diofantina com duas variáveis.

Para isso, teremos que substituir $n-1$ variáveis, por uma outra variável qualquer, mas diferente das já existentes. Após realizar esse processo basta encontrar a solução geral da equação gerada. Temos que a solução geral de uma equação diofantina linear de n variáveis terá $n-1$ parâmetros.

Proposição 14. Seja a equação diofantina $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n = b$ onde $a_1 + a_2, \cdots, a_n$ sejam inteiros não nulos simultaneamente, a solução geral pode ser encontrada utilizando mesmo método para resolver equações com três variáveis, ou seja, reduzindo a equação diofantina em uma equação de duas variáveis $n-1$ vezes.

Demonstração. Consideremos a equação diofantina $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n = b$ tal que $mdc(a_1, a_2, ..., a_n) = d \mid b$ para algum $d \in \mathbf{N}$.

Iniciaremos a demonstração assumindo que $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_{n-1} \cdot x_{n-1} = k^{(1)}$ com $k^{(1)}$ inteiro. Agora podemos reescrever a Equação 3.24 como:

$$k^{(1)} + a_n \cdot x_n = b \tag{3.25}$$

Podemos observar que $mdc(1, a_n) = 1$, pela Proposição 10 temos que existem infinitas soluções para essa equação diofantina, pois $1 \mid b$. Logo pela Proposição 11, temos que as soluções são do tipo:

$$\begin{cases} k^{(1)} = k_1 + a_n \cdot t_1 \\ x_n = x'_n - t_1 \end{cases}, \text{com } t_1 \in \mathbb{Z}.$$

□

Onde $(k_1, x_{(n)})$ é uma solução particular da Equação 3.25 .

O próximo passo é resolver a equação $k^{(1)} = k_1 + a_n \cdot t_1$, que pode ser reescrita como:

$$a_1 \cdot x_1 + a_2 \cdot x_2 + ... + a_{n-1} \cdot x_{n-1} = k_1 + a_n \cdot t_1 \tag{3.26}$$

Temos que a Equação 3.26 só possui solução se $(a_1, a_2, \cdots, a_{n-1}) \mid (k_1 + a_n \cdot t_1)$, tomemos então, $t_1 = t'_{(1)}$ de modo que $(a_1, a_2, \cdots, a_{n-1}) \mid (k_1 + a_n \cdot t'_{(1)})$, mas para isso devemos observar que quando $t_1 = t'_{(1)}$, a variável x_n devera ser escrita como $x_n = x'_{(n)} - t'_{(1)}$. Devemos ter que $t'_1 = (a_1, a_2, \cdots, a_{n-1}) \cdot q_1 + r_1$, com $0 \leq r_1 < (a_1, a_2, \cdots, a_{n-1})$, onde r_1 é um número inteiro determinado e q_1 é inteiro um qualquer. Então ao substituir o valor de $t'_{(1)}$ na Equação 3.26, teremos que:

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_{n-1} \cdot x_{n-1} = k_1 + a_n \cdot ((a_1, a_2, \cdots, a_{n-1}) \cdot q_1 + r_1)$$

Logo,

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_{n-1} \cdot x_{n-1} = a_n \cdot (a_1, a_2, \cdots, a_{n-1}) \cdot q_1 + k_1 + a_n \cdot r_1$$

Portanto,

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_{n-1} \cdot x_{n-1} = a_n \cdot (a_1, a_2, \cdots, a_{n-1}) \cdot q_1 + s_1 \ \text{, com } \ s_1 = k_1 + a_n \cdot r_1.$$

Agora iremos seguir de forma análoga ao passo anterior, ou seja, tomemos $k^{(2)} = a_1 x_1 + \cdots + a_{(n-2)}, logo:$

$$k^{(2)} + a_{(n-1)} \cdot x_{n-1} = a x_1 + \cdots + a_{n-1} \cdot x_{n-1} = s_1 + a_n \cdot (a_1, \cdots, a_{n-1}) \cdot q_1. \tag{3.27}$$

Como $mdc(1, a_{n-1}) = 1 \mid (s_1 + a_n(a_1, \cdots, a_{n-1}))$, pela Proposição 10 temos que a Equação 3.27 possui solução. Logo pela Proposição 11, temos que as soluções são do tipo,

$$\begin{cases} k^{(2)} = k_2 + a_{n-1} \cdot t_2 \\ x_{n-1} = x'_{(n-1)} - t_2 \end{cases} \text{, com } t_2 \in \mathbb{Z}.$$

onde (k_2, x'_{n-1}) são uma solução particular da Equação 3.27.

Agora devemos resolver a seguinte equação:

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_{n-2} \cdot x_{n-2} = k_2 + a_{n-1} \cdot t_2. \tag{3.28}$$

Temos que a Equação 3.28 só possui solução se $(a_1, a_2, \cdots, a_{n-2}) \mid (k_2 + a_{n-1} \cdot t_2)$, tomemos então, $t_2 = t'_{(2)}$ de modo que $(a_1, a_2, \cdots, a_{n-2}) \mid (k_1 + a_n \cdot t'_{(1)})$. Onde $t'_2 = (a_1, \cdots, a_{n-2}) \cdot q_2 + r_2$, com $0 \leq r_2 < (a_1, \cdots, a_{n-2})$, onde r_2 é um número inteiro determinado e q_2 é inteiro um qualquer. Então ao substituir o valor de $t'_{(2)}$ na Equação 3.28, teremos que:

$$a_1 \cdot x_1 + \cdots + a_{n-2} \cdot x_{n-2} = s_2 + a_{n-1} \cdot (a_1, \cdots, a_{n-2}) \cdot q_2 \ \text{, com } \ s_2 = k_2 + a_{n-1} \cdot r_2. \tag{3.29}$$

Seguindo de forma análoga, ou seja, tomando $k^{(3)} = a_1 x_a + \cdots + a_{n-3}$ e tomando os passos anteriores, iremos repetir esse processo $n-2$ vezes, no qual serão determinados os valores das x_f variáveis, com $f = 3, \cdots, n \in \mathbb{Z}$.

Iremos repetir o processo até chegarmos na seguinte equação:

$$a_1 \cdot x_1 + \cdots + a_2 \cdot x_2 = s_{n-2} + a_3 \cdot (a_1, a_2) \cdot q_{n-2} \ \text{, com } \ s_{n-2} = k_{n-2} + a_4 \cdot r_{n-2}.$$

Determinando r_{n-3} modo que $t_{n-3} = t'_{n-3} \cdot (a_1, a_2, a_3))$ e $(a_1, a_2, a_3) \mid (k_{n-3} + a_4 \cdot t_{n-3})$.

Resolvendo $a_1 \cdot x_1 + \cdots + a_2 \cdot x_2 = s_{n-3} + a_4 \cdot (a_1, a_2) \cdot q_{n-3}$, teremos,

$$x_1 = x'_1 + \frac{a_2}{(a_1, a_2)} \cdot t_{n-1}$$

$$x_2 = x_2 - \frac{a_1}{(a_1, a_2)} \cdot t_{n-1}$$

com $t_n - 1 \quad \in \mathbb{Z}$.

Chegamos à conclusão que a solução geral da equação diofantina $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n = b$, será dada por:

$$x_1 = x_1' + \frac{a_2}{(a_1, a_2)} \cdot t_{n-1}$$

$$x_2 = x_2' - \frac{a_1}{(a_1, a_2)} \cdot t_{n-1}$$

$$x_3 = x_3' - t_{n-2}'$$

$$\cdots$$

$$x_n = x_n' - t_1'$$

□

CAPÍTULO

4

FRAÇÕES CONTÍNUAS

Nesta seção faremos um breve estudo sobre frações contínuas, onde veremos como representar números racionais e números irracionais, através de uma sequência de números inteiros.

Considerado um dos mais belos temas da Matemática Elementar, as frações contínuas é um dos melhores instrumentos de investigação da natureza aritmética dos números irracionais.

Representaremos o conjunto dos números racionais com o símbolo $\mathbb{Q}$, nesse conjunto estão todos os números que podem ser escrito na forma de fração, onde o numerador e o denominador são números inteiros. O conjunto dos números racionais é dado por:

$$\mathbb{Q} = \{\frac{p}{q}, \text{ p e q } \in \mathbb{Z}, \text{ com } q \neq 0\}.$$

O conjunto dos números irracionais será representado pelo símbolo $\mathbb{I}$, nesse conjunto estão os números que não podem ser representados como uma fração. Este conjunto é composto pelas dízimas não periódicas. Temos como exemplo o número "pi"e o número de ouro que são denotados pelas letras gregas π e ϕ respectivamente, e as raízes não exatas, como é o caso da $\sqrt{2}$ e $\sqrt{3}$.

O conjunto dos números reais será representado pelo símbolo $\mathbb{R}$, nesse conjunto estão todos os números racionais e irracionais, ou seja, $\mathbb{R} = \mathbb{Q} \cup \mathbb{I}$.

Exite uma relação fundamental entre os números racionais e os números reais que nos diz que $\mathbb{Q}$ é denso em $\mathbb{R}$, ou seja, números reais podem ser arbitrariamente bem aproximados por números racionais.

Veremos agora como podemos realizar tais aproximações.

4.1 Frações Contínuas Finitas e Infinitas

Iniciaremos vendo como funciona o algoritmo das frações contínuas simples e algumas definições baseadas em (PAULINO, 2020).

Dado um número real x, existe um único $\lfloor x \rfloor \in \mathbb{Z}$, denominado o maior inteiro menor do que ou igual a x e um único real $x \in [0,1)$, que é denominado como sendo a parte fracionária de x, e denotado por$\{x\}$, tais que

$$x = \lfloor x \rfloor + \{x\}, \text{ com } \lfloor x \rfloor \in \mathbb{Z} \text{ e } 0 \leqslant \{x\} < 1.$$

Se x não for um número inteiro, temos que $\{x_1\} \neq 0$, logo definido $x_1 = \dfrac{1}{\{x\}}$, teremos que:

$$x = \lfloor x \rfloor + \frac{1}{x_1} = \lfloor x \rfloor + \frac{1}{\dfrac{1}{\{x\}}}.$$

Se x_1 não for inteiro, então $\{x_1\} \neq 0$, logo definindo $x_2 = \dfrac{1}{\{x_1\}}$, teremos que:

$$x = \lfloor x \rfloor + \frac{1}{\lfloor x_1 \rfloor + \dfrac{1}{x_2}}.$$

O processo só termina se para algum $k \geqslant 1 \in \mathbb{N}$ ocorrer $\{x_k\} = 0$ para algum $k \geqslant 1$, caso contrário, o processo continua.

Uma das vantagens da representação por frações contínuas é que além de não dependermos de escolhas artificiais de base, o reconhecimento de racionais é mais simples que na representação decimal que estamos habituados.

Definição 7. Dado $x \in \mathbb{R}$, definimos como fração contínua simples de x a sequência (a_n), definida por $a_n := \lfloor \alpha_n \rfloor$, para $n \in \mathbb{N}$, em que α_n é obtido recursivamente por

$$\begin{cases} \alpha_0 = x \\ \alpha_{n+1} = \dfrac{1}{\{\alpha_n\}} = \dfrac{1}{\alpha_n - a_n} \end{cases}, \text{ com } \alpha_n \notin \mathbb{Z}.$$

i) Caso $\alpha_n = x_n$, ou seja $\{\alpha_n\} = 0$, a sua representação em frações contínuas é finita.

$$ax_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{k-1} + \dfrac{1}{a_k}}}}} := [a_0; a_1, a_2, \ldots, a_{k-1}, a_k]. \tag{4.1}$$

ii) Caso contrário teremos,

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \cfrac{1}{a_{a-1} + \cfrac{1}{a_k + \ldots}}}}} = [a_0; a_1, a_2, \ldots, a_{k-1}, a_k, \ldots]. \tag{4.2}$$

Teorema 6. Qualquer fração contínua simples finita representa um número racional. Reciprocamente temos que qualquer número racional pode ser representado por uma fração contínua simples finita.

Demonstração. A primeira parte da demonstração sai de forma imediata, pois se trata de uma fração contínua simples finita, ou seja, uma fração contínua simples finita (Equação 4.1).

Para provar a recíproca, consideremos $\frac{a}{b} \in \mathbb{Q}$. Pelo algoritmo da divisão, temos que,

$$\frac{a}{b} = q_0 + \frac{r_0}{b}, \text{ onde } 0 \leqslant r_0 < b \text{ e } q_0 = \frac{a}{b}.$$

Se $r_0 = 0$ temos que $\frac{a}{b}$ é um número inteiro, logo não há nada para provar, mas caso $r_0 \neq 0$, então da faremos:

$$\frac{a}{b} = q_0 + \frac{1}{\frac{b}{r_0}}, \text{ com } 0 < r_0 < b.$$

Fazendo o mesmo para $\frac{b}{r_0}$ teremos que,

$$\frac{b}{r_0} = q_1 + \frac{r_1}{r_0}.$$

Se $r_1 \neq 0$, temos $\frac{a}{b} = q_0 + \frac{1}{q_1} = [q_0; q_1]$, terminando a prova. Caso $r_1 \neq 0$, repetimos o mesmo processo com a fração $\frac{r_1}{r_0}$. Esse procedimento só vai parar quando $r_n = 0$ para algum n, o que ocorre, porque $b > r_0 > r_1 > \cdots$ é uma sequência decrescente de inteiros positivos. Logo temos,

$$\begin{gathered}
\frac{a}{b} = q_0 + \frac{r_0}{b}, \ 0 < r_0 < b, \\
\frac{b}{r_0} = q_1 + \frac{r_1}{r_0}, \ 0 < r_1 < r_0, \\
\cdots \\
\frac{r_{n-3}}{r_{n-2}} = q_{n-2} + \frac{r_{n-1}}{r_{n-2}}, \ 0 < r_{n-1} < r_{n-2}, \\
\frac{r_{n-2}}{r_{n-1}} = q_{n-1}, \ r_n = 0.
\end{gathered}$$

Portanto,

$$\frac{a}{b} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots + \cfrac{1}{q_{n-1}}}}}.$$

□

4.2 Representação de Racionais como Frações Contínuas

Veremos alguns exemplos de como representar números racionais como frações contínuas.

O próximo exemplo é uma questão retirada da prova do Colégio Militar do Rio de Janeiro (CMRJ).

Exemplo 25. (CMRJ, 2008) Temos que a fração $\frac{37}{13}$ pode ser escrita sob a forma $2 + \cfrac{1}{x + \cfrac{1}{y + \frac{1}{z}}}$.

Descubra quais são os valores de (x, y, z).

Demonstração. Iniciaremos efetuando a divisão de $\frac{37}{13}$. Pela divisão euclidiana, temos que $37 = 13 \cdot 2 + 11$, portanto:

$$\frac{37}{13} = 2 + \frac{11}{13}.$$

Manipulando o resultado para que fique com a cara da equação que desejamos, ou seja, podemos escrever $2 + \frac{11}{13} = 2 + \frac{1}{\frac{13}{11}}$. Pela Divisão Euclidiana, temos que $13 = 11 \cdot 1 + 2$, portanto:

$$\frac{13}{11} = 1 + \frac{2}{11}.$$

Logo temos que:

$$\frac{37}{13} = 2 + \frac{11}{13} = 2 + \frac{1}{\frac{13}{11}} = 2 + \frac{1}{1 + \frac{2}{11}}.$$

Manipulando o resultado anterior mais uma vez, ou seja, podemos escrever $1 + \frac{2}{11} = 1 + \frac{1}{\frac{11}{2}}$.

Logo temos que:

$$\frac{37}{13} = 2 + \cfrac{1}{1 + \frac{2}{11}} = 2 + \cfrac{1}{1 + \cfrac{1}{\frac{11}{2}}}.$$

Pela divisão euclidiana, temos que $11 = 2 \cdot 5 + 1$. Portanto,

$$\frac{11}{2} = 5 + \frac{1}{2}.$$

Então podemos concluir que:

$$\frac{37}{13} = 2 + \cfrac{1}{1 + \cfrac{1}{5 + \cfrac{1}{2}}}.$$

Chegamos a conclusão que (x, y, z) são iguais a $(1, 5, 2)$. □

Agora vamos ver uma forma mais prática e rápida para encontramos a fração contínua de um número racional.

Iremos usar o algoritmo de Euclides realizando divisões sucessivas e organizando os resultados obtidos dentro de uma tabela que possui apenas três linhas, a primeira linha será destinada aos quocientes da divisão, o primeiro número da segunda linha é o numerador e o segundo o denominador do racional que estamos calculando, a terceira linha será destinada aos restos da divisão. Conforme vamos realizando sucessivas divisões iremos preencher essa tabela sempre colocando os quocientes obtidos na primeira linha, os restos na terceira linha e copiando os mesmos na segunda linha para poder continuar a divisão.

Vejamos na prática como fica essa tabela.

Temos que $37 = 2 \cdot 13 + 11$, portanto:

Q	2	
37	13	11
R	11	

Como $13 = 1 \cdot 11 + 2$, teremos que:

Q	2	1	
37	13	11	2
R	11	2	

Continuando as divisões teremos que $11 = 5 \cdot 2 + 1$, logo:

Q	2	1	5	2
37	13	11	2	1
R	11	2	1	0

Agora com esses resultados já conseguimos escrever $\frac{37}{13}$ como frações contínuas, ou seja, $\frac{37}{13} = [2; 1, 5, 2]$. Note que todos esses valores obtidos se encontram na primeira linha da tabela acima.

Exemplo 26. Represente como fração contínua os seguintes racionais:

i) $\frac{62}{27}$.

ii) $\frac{1320}{35}$.

Demonstração. Utilizaremos o método acima para resolução deste exercício.

i) Aplicando o algoritmo de Euclides sucessivamente no racional $\frac{62}{27}$ e preenchendo a tabela de forma ordenada, teremos que:

Q	2	3	2	1	2
62	27	8	3	2	1
R	8	3	2	1	0

Portanto a fração contínua do racional $\frac{62}{27}$ é igual:

$$\frac{62}{27} = 2 + \cfrac{1}{3 + \cfrac{1}{2 + \cfrac{1}{1 + \frac{1}{2}}}} = [2;3,2,1,2].$$

ii) Aplicando o algoritmo de Euclides sucessivamente no racinal $\frac{1320}{35}$ e preenchendo a tabela de forma ordenada, teremos que:

Q	37	1	2	2
1320	35	25	10	5
R	25	10	5	0

Portanto a fração contínua do racional $\frac{1320}{35}$ é igual:

$$\frac{1320}{35} = 37 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{2}}} = [37;1,2,2].$$

□

Exemplo 27. Obtenha os seguintes racionais a partir de suas expansões por frações contínuas simples:

i) $\frac{a}{b} = [2;5,4,3]$.

ii) $\frac{c}{d} = [0;2,3]$.

iii) $\frac{e}{f} = [2;1,3,4]$.

Demonstração. Para obter o racional a partir de sua expansão por frações contínuas basta efetuar as operações de soma de frações.

i) $\frac{a}{b} = [2;5,4,3] = 2 + \cfrac{1}{5 + \cfrac{1}{4 + \frac{1}{3}}} = 2 + \cfrac{1}{5 + \cfrac{1}{\frac{13}{3}}} = 2 + \cfrac{1}{5 + \frac{3}{13}} = 2 + \cfrac{1}{\frac{68}{13}} = 2 + \frac{13}{68} = \frac{149}{68}.$

ii) $\frac{c}{d} = [0;2,3] = 0 + \cfrac{1}{2 + \frac{1}{3}} = 0 + \frac{1}{\frac{7}{3}} = \frac{3}{7}.$

iii) $\frac{e}{f} = [2;1,3,4] = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{4}}} = 2 + \cfrac{1}{1 + \cfrac{1}{\frac{13}{4}}} = 2 + \cfrac{1}{1 + \frac{4}{13}} = 2 + \cfrac{1}{\frac{17}{13}} = 2 + \frac{13}{17} = \frac{47}{17}.$

□

4.3 Representação de Irracionais como Frações Contínuas

Veremos agora como fica a representação de um irracional como frações contínuas.

Exemplo 28. Represente os cinco primeiros elementos de π.

Demonstração. Iremos precisar de uma calculadora para resolução desse exercício. Como $\pi = 3,141592...$, podemos escrevê-lo como $\pi = 3 + 0,141592....$ Logo,

$$\pi = 3 + 0,141592... = 3 + \frac{1}{(0,1415...)^{(-1)}}.$$

Com o auxílio uma calculadora podemos ver que o $(0,141592...)^{-1} = 7,062513....$,

$$\pi = 3 + 0,1415... = 3 + \frac{1}{7,062513...}. \tag{4.3}$$

Podemos escrever $7,062513...$ como $7 + 0,062513...$, portanto,

$$\pi = 3 + \frac{1}{7 + 0,062513} = 3 + \cfrac{1}{7 + \cfrac{1}{(0,062513...)^{-1}}}.$$

Como $(0,062513...)^{-1} = 15,996594...$, podemos substituir na equação,

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{(0,062513...)^{-1}}} = 3 + \cfrac{1}{7 + \cfrac{1}{15,996594...}}. \tag{4.4}$$

Novamente iremos repetir o processo usado até o momento, ou seja, iremos separar a parte inteira de $15,996594$ que é 15 e depois calcular o inverso da parte fracionária que é igual a $(0,996594...)^{-1} = 1,003417$.

$$\pi = 3+\frac{1}{7+\frac{1}{15+(0,996594...)}} = 3+\frac{1}{7+\frac{1}{15+\frac{1}{(0,996594...)^{-1}}}} = 3+\frac{1}{7+\frac{1}{15+\frac{1}{1,003417...}}}.$$

Repetindo o processo de separar a parte inteira do último quociente e depois substituir a parte fracionária pelo seu inverso, como $(0,003417...)^{-1} = 292,6345...$ teremos,

$$\pi = 3+\frac{1}{7+\frac{1}{15+\frac{1}{1,003417...}}}$$

$$\pi = 3+\frac{1}{7+\frac{1}{15+\frac{1}{1+\frac{1}{(0,003417...)^{-1}}}}}$$

$$\pi = 3+\frac{1}{7+\frac{1}{15+\frac{1}{1+\frac{1}{292,6345...}}}}.$$

Realizando o processo mais uma vez, teremos que,

$$\pi = 3+\frac{1}{7+\frac{1}{15+\frac{1}{1+\frac{1}{292,6345...}}}}$$

$$\pi = 3+\frac{1}{7+\frac{1}{15+\frac{1}{1+\frac{1}{292+0,6345}}}}$$

$$\pi = 3+\frac{1}{7+\frac{1}{15+\frac{1}{1+\frac{1}{292+\frac{1}{(0,6345...)^{-1}}}}}}.$$

Como π é uma dizima não periódica, ou seja, $\pi \in \mathbb{I}$, esse processo não tem fim, logo,

$$\pi = 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cfrac{1}{\ddots}}}}} = \lfloor 3; 7, 15, 1, 292, \ldots \rfloor.$$

□

Obervação: Uma boa aproximação para π em racionais, devida a Arquimedes é de $\frac{22}{7} = 3,14285714\ldots$, conseguimos encontrar esse valor facilmente na Equação 4.3.

$$\pi = 3 + 0,1415926... = 3 + \frac{1}{7,062513...} \simeq 3 + \frac{1}{7} = \frac{21+1}{7} = \frac{22}{7}.$$

Outra aproximação muito conhecida de π é de $\frac{355}{113}$ pode ser encontrado na Equação 4.4,

$$\pi = 3 + \frac{1}{7 + \cfrac{1}{(0,062513...)^{-1}}} = 3 + \frac{1}{7 + \cfrac{1}{15,996594...}} \simeq 3 + \frac{1}{7 + \cfrac{1}{16}} = 3 + \frac{1}{\cfrac{112+1}{16}}$$

$$= 3 + \frac{1}{\cfrac{113}{16}} = 3 + \frac{16}{113} = \frac{339+16}{113} = \frac{355}{113} = 3,1415929203\ldots.$$

Se continuarmos os cálculos iremos encontrar cada vez mais melhores aproximações para o número π.

Exemplo 29. Represente a fração contínua do número de ouro, ou seja, represente a fração contínua do número irracional $\phi = \frac{\sqrt{5}+1}{2}$.

Demonstração. Podemos observar que $2 > \frac{\sqrt{5}+1}{2} > 1$, pois temos que $\sqrt{5} = 2,236\ldots$, logo pelo algoritmo das frações contínuas podemos escrever ϕ como,

$$\phi = \alpha_0 = \frac{\sqrt{5}+1}{2} = \lfloor \frac{\sqrt{5}+1}{2} \rfloor + \{\frac{\sqrt{5}+1}{2}\} = 1 + (\frac{\sqrt{5}+1}{2} - 1) = 1 + \frac{\sqrt{5}-1}{2}.$$

Agora fazendo o inverso da parte fracionária podemos escrever,

$$\phi = 1 + \frac{\sqrt{5}-1}{2} = 1 + \frac{1}{\cfrac{2}{\sqrt{5}-1}}.$$

Como $\alpha_1 = \frac{2}{\sqrt{5}-1} = \frac{2\cdot(\sqrt{5}+1)}{(\sqrt{5}-1)\cdot(\sqrt{5}+1)} = \frac{2\cdot(\sqrt{5}+1)}{2} = \frac{\sqrt{5}+1}{2}$, chegamos a conclusão que $\alpha_0 = \alpha_1$, logo o processo ira se repetir implicando que $\alpha_n = \alpha_0 = \frac{\sqrt{5}+1}{2}$ e

$a_n = a_0 = 1$ para todo $n \in \mathbb{N}$. Logo chegamos a conclusão que a representação de ϕ em frações contínuas é um processo infinito, no qual temos,

$$\phi = \frac{\sqrt{5}+1}{2} = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \ddots}}} = [1;1,1,1,\ldots].$$

□

Exemplo 30. Represente a fração contínua do irracional $\sqrt{2}$.

Demonstração. Podemos observar que $2 > \sqrt{2} > 1$, pois temos que $\sqrt{2} = 1,414213\ldots$, logo pelo algoritmo das frações contínuas podemos escrever $\sqrt{2}$ como,

$$\alpha_0 = \sqrt{2} = \lfloor \sqrt{2} \rfloor + \{\sqrt{2}\} = 1 + (\sqrt{2} - 1).$$

Logo podemos escrever $\sqrt{2}$ como,

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\cfrac{1}{\sqrt{2}-1}}.$$

Portanto,

$$\sqrt{2} = 1 + \frac{1}{\cfrac{1}{\sqrt{2}-1}} = 1 + \frac{1}{\cfrac{1\cdot(\sqrt{2}+1)}{(\sqrt{2}-1)\cdot(\sqrt{2}+1)}} = 1 + \frac{1}{\cfrac{\sqrt{2}+1}{2-1}} = 1 + \frac{1}{\cfrac{\sqrt{2}+1}{1}} = 1 + \frac{1}{\sqrt{2}+1}.$$

Aplicando o algoritmo das frações contínuas no quociente encontrado,

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{\lfloor(\sqrt{2}+1)\rfloor + \{\sqrt{2}+1\}} = 1 + \frac{1}{2 + (\sqrt{2}+1-2)} = 1 + \frac{1}{\sqrt{2}+1}.$$

Aplicando o algoritmo das frações contínuas novamente:

$$\sqrt{2}+1 = \lfloor \sqrt{2}+1 \rfloor + \{\sqrt{2}+1\} = 2 + (\sqrt{2}+1) - 2 = 2 + \sqrt{2} - 1.$$

Logo temos que,

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2+\sqrt{2}-1} = 1 + \frac{1}{\sqrt{2}+1}.$$

Fazendo o inverso da parte fracionária,

$$\sqrt{2} = 1 + \frac{1}{2+\sqrt{2}-1} = 1 + \frac{1}{2 + \cfrac{1}{\cfrac{1}{\sqrt{2}-1}}} = 1 + \frac{1}{2 + \cfrac{1}{\cfrac{1\cdot(\sqrt{2}+1)}{(\sqrt{2}-1)\cdot(\sqrt{2+1})}}} = 1 + \frac{1}{2 + \cfrac{1}{\cfrac{\sqrt{2}+1}{1}}}.$$

Portanto temos que,

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{\frac{\sqrt{2}+1}{1}}} = 11 + \frac{1}{2 + \frac{1}{\sqrt{2}+1}}.$$

Como $\sqrt{2}-1$ tem como inverso $\sqrt{2}+1$ e $\alpha_1 = \alpha_2 = \frac{1}{\sqrt{2}-1}$ o processo ira se repetir implicando que $\alpha_n = \alpha_1 = \frac{1}{\sqrt{2}-1}$, sendo apenas $\alpha_0 = \sqrt{2}$, logo,

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \ldots}} = [1;,2,2,2,\ldots].$$

□

CAPÍTULO

5

CONSIDERAÇÕES FINAIS

É notável a importância que Diofanto teve no desenvolvimento da matemática, principalmente na álgebra, onde foi o precursor da estruturação da simbologia algébrica que estudamos até hoje.

O objetivo deste trabalho é fornecer um material complementar para o estudo das equações diofantinas, conteúdo que é ministrado durante a disciplina de Aritmética do Mestrado PROFMAT. Nesta dissertação apresentamos algumas proposições, teoremas e suas demonstrações, que são necessários para ajudar a encontrar a solução geral de equações diofantinas com duas ou mais incógnitas.

Frações contínuas é um tema que não é trabalhado no PROFMAT. À primeira vista parece ser um conteúdo complicado, mas podemos ver como é fácil representar números reais em frações contínuas.

Tendo em vista que os conteúdos fundamentais vistos nesta dissertação são estudados durante a Educação Básica, seria interessante trabalhar com as equações diofantinas na Educação Básica, visto que já é uma disciplina prevista no currículo de Matemática do Estado de São Paulo, tendo assim a possibilidade de se aprofundar no tema (SILVA, 2019).

Frações contínuas também seria um tema interessante para trabalhar com turmas do ensino fundamental, deixando um pouco a teoria de lado e trabalhando na resolução de exercícios, os alunos aprenderão mais sobre a adição de frações e o inverso de um número.

Esperamos que o objetivo deste trabalho seja alcançado, que possa servir como material de apoio, contribuindo para um melhor entendimento do assunto por parte do leitor.

REFERÊNCIAS

CMRJ. **Exame Nacional de Qualificação**. 2008. Disponível em: <http://www.professorwaltertadeu.mat.br/GABProfWalterTadeuCMRJ1ano2008.pdf>. Acesso em: 15-12-2022. Citado na página 62.

ENQ-2017.1. **Exame Nacional de Qualificação**. 2017. Disponível em: <http://sbm.org.br/profmat/wp-content/uploads/sites/4/sites/4/2021/10/ENQ20171_Gabarito.pdf>. Acesso em: 06-08-2022. Citado na página 43.

ENQ-2018.2. **Exame Nacional de Qualificação**. 2018. Disponível em: <https://profmat-sbm.org.br/wp-content/uploads/sites/4/sites/4/2021/10/ENQ-20182-gabarito.pdf>. Acesso em: 20-08-2022. Citado na página 47.

ENQ-2019.1. **Exame Nacional de Qualificação**. 2019. Disponível em: <https://profmat-sbm.org.br/wp-content/uploads/sites/4/sites/4/2021/10/ENQ-20191-Gabarito-1-1.pdf>. Acesso em: 20-08-2022. Citado na página 47.

ENQ-2022.2. **Exame Nacional de Qualificação**. 2022. Disponível em: <https://profmat-sbm.org.br/wp-content/uploads/sites/4/sites/4/2022/08/ENQ-2022.2_Gabarito_com_Pautas.pdf>. Acesso em: 19-07-2022. Citado na página 42.

HEFEZ, A. **Aritmética - Coleção PROFMAT**. 2. ed. Rio de Janeiro: SBM, 2016. ISBN 978-85-8337-105-2. Citado na página 21.

NIVEN, H. S. Z. I.; MONTGOMERY, H. L. **An Introduction to the Theory of Numbers**. 5. ed. Estados Unidos da América: Courier Companies, 1991. ISBN 0-471-62546-9. Citado na página 21.

OBM. **Olimpíada Brasileira de Matemática**. 1999. Disponível em: <https://www.obm.org.br/content/uploads/2017/02/1fase-N2.doc>. Acesso em: 25-08-2022. Citado na página 45.

____. **Olimpíada Brasileira de Matemática**. 2003. Disponível em: <https://www.obm.org.br/content/uploads/2017/02/1faseOBM_2003-N1.doc>. Acesso em: 25-08-2022. Citado na página 46.

OLIVEIRA, K. I. M.; FERNáNDEZ, A. J. C. **Iniciação à Matemática: um curso com problemas e soluções**. 2. ed. Rio de Janeiro: SBM, 2012. ISBN 978-85-8337-114-4. Citado na página 21.

PAULINO, R. A. F. **Frações contínuas: fundamentação teórica e possíveis abordagens na Educação Básica**. [S.l.], 2020. Citado na página 60.

SILVA, A. C. da. **As equações diofantinas lineares no currículo da educação básica**. [S.l.], 2019. Citado na página 71.

SILVA AMANDA G. DA SILVA, O. F. A. d. O. J. A. S. Equações diofantinas lineares: estratégicas para resolução de problemas indeterminados. **XXXV CNMAC**, v. 3, n. 1, 2014. Citado na página 19.


ICMC
USP
SÃO CARLOS