UNIVERSIDADE FEDERAL RURAL DO SEMIÁRIDO
PRÓ-REITORIA DE PESQUISA E PÓS GRADUAÇÃO
CENTRO DE CIÊNCIAS EXATAS E NATURAIS
DEPARTAMENTO DE CIÊNCIAS NATURAIS, MATEMÁTICA E ESTATÍSTICA
PROGRAMA DE MESTRADO EM MATEMÁTICA PROFISSIONAL EM REDE NACIONAL

PATRÍCIO JÚNIOR DE SOUZA

UMA INTRODUÇÃO AO ESTUDO DE EQUAÇÕES DIOFANTINAS LINEARES PARA O ENSINO MÉDIO

MOSSORÓ
2020

PATRÍCIO JÚNIOR DE SOUZA

UMA INTRODUÇÃO AO ESTUDO DE EQUAÇÕES DIOFANTINAS LINEARES PARA O ENSINO MÉDIO

Dissertação apresentada ao Programa de Mestrado em Matemática Profissional em Rede Nacional da Universidade Federal Rural do Semiárido (UFERSA) como requisito para a obtenção do grau de Mestre em Matemática. Área de Concentração: Ensino de Matemática

Orientador: Prof. Dr. Antonio Gomes Nunes

MOSSORÓ

2020

© Todos os direitos estão reservados a Universidade Federal Rural do Semi-Árido. O conteúdo desta obra é de inteira responsabilidade do (a) autor (a), sendo o mesmo, passível de sanções administrativas ou penais, caso sejam infringidas as leis que regulamentam a Propriedade Intelectual, respectivamente, Patentes: Lei n° 9.279/1996 e Direitos Autorais: Lei n° 9.610/1998. O conteúdo desta obra tomar-se-á de domínio público após a data de defesa e homologação da sua respectiva ata. A mesma poderá servir de base literária para novas pesquisas, desde que a obra e seu (a) respectivo (a) autor (a) sejam devidamente citados e mencionados os seus créditos bibliográficos.

di de Souza, Patrício Júnior.
Uma introdução ao estudo de equações diofantinas lineares para o ensino médio / Patrício Júnior de Souza. - 2020.
101 f. : il.

Orientador: Antonio Gomes Nunes.
Dissertação (Mestrado) - Universidade Federal Rural do Semi-árido, Programa de Pós-graduação em , 2020.

1. Equações Diofantinas Lineares. 2. Máximo Divisor Comum. 3. Congruências. 4. Teoria dos Números. 5. Ensino Médio. I. Nunes, Antonio Gomes, orient. II. Título.

O serviço de Geração Automática de Ficha Catalográfica para Trabalhos de Conclusão de Curso (TCC´s) foi desenvolvido pelo Instituto de Ciências Matemáticas e de Computação da Universidade de São Paulo (USP) e gentilmente cedido para o Sistema de Bibliotecas da Universidade Federal Rural do Semi-Árido (SISBI-UFERSA), sendo customizado pela Superintendência de Tecnologia da Informação e Comunicação (SUTIC) sob orientação dos bibliotecários da instituição para ser adaptado às necessidades dos alunos dos Cursos de Graduação e Programas de Pós-Graduação da Universidade.

PATRÍCIO JÚNIOR DE SOUZA

UMA INTRODUÇÃO AO ESTUDO DE EQUAÇÕES DIOFANTINAS LINEARES PARA O ENSINO MÉDIO

Dissertação apresentada ao Programa de Mestrado em Matemática Profissional em Rede Nacional da Universidade Federal Rural do Semiárido (UFERSA) como requisito para a obtenção do grau de Mestre em Matemática. Área de Concentração: Ensino de Matemática

Aprovada em:

BANCA EXAMINADORA

Prof. Dr. Antonio Gomes Nunes (Orientador)
Universidade Federal Rural do Semiárido (UFERSA)

Prof. Dr. Walter Martins Rodrigues - UFERSA
Universidade Federal Rural do Semiárido (UFERSA)

Profª. Drª. Fabiane Regina da Cunha Dantas Araújo
Universidade Federal Rural do Semiárido (UFERSA)

À minha família, por sua capacidade de acreditar e investir em mim. Mãe, seu cuidado e dedicação foi que deram, em alguns momentos, a esperança para seguir. Pai, em minha memória ficaram somente boas lembranças. A todos que passaram pela minha vida e que hoje não estão conosco.

AGRADECIMENTOS

Agradeço a Deus pela vida e por tudo que podemos aprender com ela.

À minha mãe, Maria José de Souza, que sempre me incentivou e acreditou que conseguiria obter exito em minha vida por meio de meus esforços, sempre trabalhando com respeito e ética. Minha mãe foi uma grande mestre para mim, apesar de apenas saber escrever o seu nome, ensinou-me coisas que remetem aos mais altos níveis de sabedoria, ética, filosofia e educação.

À minha família, em especial, à minha irmã Patricia Regina de Souza, aos meus sobrinhos, dando um destaque à mais nova sobrinha, Ana Sofia.

Ao Prof. Dr. Antonio Gomes Nunes pelo acompanhamento e dedicação no decurso deste trabalho.

Ao Doutorando em Engenharia Elétrica, Ednardo Moreira Rodrigues, e seu assistente, Alan Batista de Oliveira, aluno de graduação em Engenharia Elétrica, pela adequação do *template* utilizado neste trabalho.

Agradeço a todos os professores do Programa de Mestrado em Matemática em Rede Nacional (PROFMAT) da UFERSA pela dedicação, flexibilidade e empatia demonstrada em várias situações, sempre compreendendo as dificuldades enfrentadas por todos os discentes.

À Coordenadoria de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pelo apoio financeiro por meio bolsa de estudos.

“Vivir es lo más peligroso que tiene la vida”

(Alejandro Sanz)

RESUMO

O trabalho tem por objetivo principal mostrar a viabilidade de aplicação do estudo de equações diofantinas lineares em turmas do Ensino Médio, para isso se faz necessário alguns conhecimentos em teoria dos números que podem ser introduzidos com embasamento em conteúdos do ensino fundamental, tais como máximo divisor comum, algoritmo de Euclides, divisibilidade e algoritmo da divisão. Alguns outros serão introduzidos é o caso do estudo das congruências que está relacionado com os restos da divisão euclidiana. Nos primeiros capítulos serão apresentados uma base em Teoria Elementar dos Números, pois são imprescindíveis na resolução das Equações Diofantinas Lineares. Será dada ênfase na resolução de equações diofantinas lineares em alguns problemas do dia a dia, no entanto, é indispensável a apresentação de métodos elementares para a resolução de alguns tipos de equações diofantinas não lineares, tais como a fatoração e o uso de desigualdades. Nosso propósito é mostrar que a introdução à resolução de problemas por meio de equações diofantinas lineares em duas incógnitas não necessita de conhecimentos avançados, possibilitando ser feito no Ensino Médio.

Palavras-chave: Equações Diofantinas Lineares.Máximo Divisor Comum.Congruências. Teoria dos Números. Ensino Médio

ABSTRACT

The main objective of this work is to show the viability of applying the study of Linear Diophantine Equations in High School classes. For that, it is necessary some knowledge of Theory of Numbers that can be introduced based on Elementary School contents, such as Greatest Common Divisor, Euclid's algorithm, divisibility and division algorithm. Some others will be introduced, such as the congruence study, which is related to the remains of the Euclidean division. In the first chapters, a basis on Elementary Theory of Numbers will be presented, as they are essential in the resolution of Linear Diophantine Equations. Emphasis will be placed on solving linear Diophantine equations in some everyday problems, however, it is essential to present elementary methods for solving some types of non-linear Diophantine equations, such as factorization and the use of inequalities. The purpose is to show that the introduction to problem solving by means of Linear Diophantine Equations in two unknowns does not require advanced knowledge, allowing it to be done in High School.

Keywords: Linear Diophantine Equations. Greatest Common Divisor. Congruences. Number's Theory. High school

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Este trabalho de pesquisa começa no capítulo 3 com um pouco de história da matemática relacionadas com os primórdios da Álgebra com os trabalhos de Diofanto, especialmente, acerca da obra *Aritmética* da qual só se conhecera uma parte, pois, outros volumes deste compêndio se perderam com a destruição da grande Biblioteca de Alexandria. Também se faz um apanhado histórico sobre grandes matemáticos e suas contribuições no estudo das equações diofantinas, dentre eles destaca-se a figura de Pierre de Fermat que deixou um desafio nas margens de uma cópia da obra Aritmética que dispunha para seu *hobby* favorito, a matemática, que intrigou as maiores mentes da humanidade por mais de 300 anos. A principal motivação para discorrer sobre o tema Equações Diofantinas é a escassez da abordagem do tema na maioria dos livros didáticos de ensino médio.

No capítulo 4 são apresentados alguns recursos teóricos da teoria dos números que alicerçam a compreensão sobre equações diofantinas, tais como o Algoritmo de Euclides, Pequeno Teorema de Fermat, Teorema Wilson e de Euler, por último, o Teorema Chinês do Resto.

O capítulo 5 é o cerne deste trabalho, nele estão propostos problemas cotidianos para motivação dos alunos e também problemas teóricos sobre equações diofantinas. Neste capítulo expõem-se técnicas de resolução de Equações Diofantinas. Demonstra-se um teorema que estabelece as condições necessárias e suficientes para que equação diofantina tenha solução, são resolvidos exemplos de equações diofantinas em duas, em três e em mais variáveis.

No capítulo 6 é proposto para o docente uma sequência didática para auxiliar na execução das aulas sobre equações diofantinas lineares que serão orientadas por duas listas de exercícios: a primeira é uma avaliação diagnóstica e a segunda é para se fazer um direcionamento do aluno no conteúdo. A estratégia se dará por meio de resolução destas listas que poderão ser complementadas com outros exercícios contextualizados.

O capítulo 7 é destinado à uma breve análise do resultado da pesquisa de campo e também a evidenciar o entendimento presente em documentos oficiais.

No capítulo 8 será exposto as considerações acerca do trabalho e quais as perspectivas de continuidade do mesmo.

2 OBJETIVOS

2.1 Objetivo Geral

Elaborar uma sequência didática através de uma pesquisa bibliográfica para inserir equações diofantinas lineares no ensino médio, sendo estas aulas aplicadas concomitantemente com o estudo de equações lineares.

2.2 Objetivos Específicos

- Fazer um breve resumo histórico acerca da vida de Diofanto e das Equações Diofantinas;
- Estudar uma base elementar em Teoria dos Números para dar suporte teórico às aulas sobre equações diofantinas;
- Estudar a solução geral para as Equações Lineares em duas variáveis;
- Estudar aplicações onde utilizam-se Equações Diofantinas Lineares em duas variáveis;
- Mostrar que a inserção do tema proposto pode ser aplicado com poucos conhecimentos teóricos, isto é, envolve conhecimentos já tratados no Ensino Fundamental;
- Propor aos professores do Ensino Médio a incorporação desse tema em suas aulas, dada a sua utilidade e a simplicidade de sua aplicação.

3 RESUMO HISTÓRICO

Neste capítulo, faz-se um breve resumo sobre alguns fatos históricos e alguns personagens, tais como Diofanto de Alexandria, do qual se dá origem ao termo *diofantina*, e seus principais trabalhos na matemática, em especial, às equações diofantinas.

3.1 Diofanto de Alexandria

Pouco se sabe sobre a vida de *Diofanto de Alexandria*, a maioria dos historiadores estimam que ele viveu no século III da era Cristã, apesar de ter sua carreira florescido em Alexandria não é conhecido o local de seu nascimento. Uma das poucas informações sobre ele é encontrado em forma de epigrama, na obra *Antologia Grega* datada por volta do quinto ou sexto século da Era Cristã.

> Deus lhe concedeu ser um menino pela sexta parte de sua vida, e somando uma duodécima parte a isto cobriu-lhe as faces de penugem; Ele lhe acendeu a lâmpada nupcial após uma sétima parte, e cinco anos após seu casamento concedeu-lhe um filho. Ai! infeliz criança tardia; depois de chegar à medida de metade da vida de seu pai, o Destino frio o levou. Depois de se consolar de sua dor durante quatro anos com a ciência dos números ele terminou sua vida. (BOYER, 1974, p. 130)

O epigrama anterior é um problema que hoje se resolve facilmente por meio da resolução de uma equação do 1º grau com uma incógnita, como segue:

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 \Rightarrow x = 84. \tag{3.1}$$

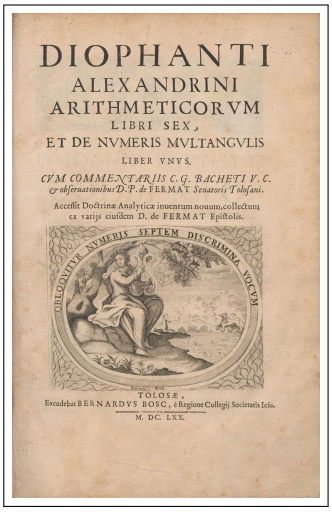
Portanto, considerando a veracidade do registro acima é possível saber que Diofanto faleceu com a idade de 84 anos.

Dentre os matemáticos que estudaram a Teoria dos Números, sem dúvida, Diofanto foi um dos mais importantes, depois dele vários gênios notáveis se debruçaram sobre problemas de Teoria dos Números, tais como Fermat, Euler, Gauss, entre outros. Sua obra *Aritmética*, escrita por volta de 250 d.C. principalmente da solução de equações indeterminadas com coeficientes inteiros. Segundo Eves (2004):

> Diofanto de Alexandria teve uma importância enorme para o desenvolvimento da álgebra e uma grande influência sobre os europeus que posteriormente se dedicaram à teoria dos números. Tal como no caso de Herão, nada se sabe com certeza acerca da nacionalidade de Diofanto e da época exata em que viveu. Apesar de haver algumas evidências tênues de que possa ter sido contemporâneo de Herão, a maioria dos historiadores tende a situá-lo no século III de nossa era. Além do fato de que sua carreira floresceu em Alexandria, nada mais de certo se sabe sobre ele, embora se encontre na Antologia grega um epigrama que se propõe a dar alguns detalhes de sua vida. (EVES, 2004, p. 207)

São conhecidos três trabalhos de Diofanto: *Aritmética*, um compêndio de treze livros dos quais apenas seis restaram, os outros se perderam, provavelmente, após o incêndio da Biblioteca de Alexandria; *Sobre os números poligonais* cuja obra também não se tem a integralidade; e, *Porismas* que se perdera totalmente. Na Europa do renascimento a matemática grega fora resgatada, as obras de Euclides, de Arquimedes, de Apolônico e de Diofanto se tornaram o centro para estudos de matemáticos do mais nível. Graças a uma tradução de *Aritmética*, feita pelo linguista francês Claude Gaspar Bachet de Méziriac (ver figura 1), Fermat teve contato com a obra de Diofanto que impulsionou um grande desenvolvimento da Teoria dos Números.

Figura 1 – Imagem da capa do livro VI da obra Aritmética de Diofanto. Tradução latina (1670) da obra Aritmética de Diofanto feita por de Méziriac.



Fonte: Wikipedia (2020).

Vários estudiosos atribuem a Diofanto de Alexandria a alcunha de "Pai da Álgebra", isso se dá ao fato dele ter difundido uma nova técnica de representação, a *sincopação*. Segundo Eves (2004), a álgebra grega se divide em três estágios no desenvolvimento da notação:

> Primeiro se tem a álgebra retórica em que os argumentos da resolução de um problema são escritos em prosa pura, sem abreviações ou símbolos específicos. A seguir vem a álgebra sincopada em que se adotam abreviações para algumas das quantidades e operações que se repetem mais frequentemente. Finalmente chega-se ao último estágio, o da álgebra simbólica, em que as resoluções se expressam numa espécie de taquigrafia matemática formada de símbolos que aparentemente nada têm a ver com os entes que representam. É razoavelmente preciso dizer que a álgebra anterior à época de Diofanto era retórica. uma das principais contribuições de Diofanto à matemática foi a sincopação da álgebra grega. A álgebra retórica, porém, continuou de maneira bastante generalizada no resto do mundo, exceto na Índia, por muitas centenas de anos. (EVES, 2004, p. 206)

Conforme afirma Eves (2004) não foi Diofanto o primeiro a trabalhar com equações

indeterminadas ou a resolver equações por meios não geométricos, no entanto, pode ter sido, de fato, o primeiro a se inclinar para a utilização de uma notação algébrica. No volume I de *Arithme* são introduzidas as abreviações que caracterizaram o período da álgebra sincopada.

Tabela 1 – Alguns símbolos e significados na notação sincopada.

Símbolo	**Significado**
ς	última letra da palavra *arithmos*, a quantidade desconhecida
Δ^{Υ}	as duas primeiras letras de *dynamis* ($\Delta\Upsilon NAMI\Sigma$), o quadrado da quantidade desconhecida
K^{Υ}	primeira letra de *kybos* ($K\Upsilon BO\Sigma$), o cubo da quantidade desconhecida
$\Delta^{\Upsilon}\Delta$	o quadrado-quadrado, a quarta potência
$\Delta^{\Upsilon}K$	o quadrado-cubo, a quinta potência
$K^{\Upsilon}K$	o cubo-cubo, a sexta potência

Fonte: Roque e Carvalho (2012).

É observado que Diofanto começa a separar as operações aritméticas com uma notação algébrica e diferindo-as das associações com a geometria, o que era forte característica da matemática grega. Ainda, segundo Roque e Carvalho (2012), a relação com a geometria era tão forte que um número com uma potência maior do que três não correspondia a nenhuma grandeza.

No entanto, segundo Boyer (1974), foi Brahmagupta, um matemático hindu que viveu em 628 da Era Cristã, na Índia central, o primeiro a determinar uma solução geral de equações no conjunto dos inteiros.

> (...) dar uma solução geral da equação linear diofantina [do tipo] $ax+by=c$, onde a, b e c são inteiros. Para que essa equação tenha soluções inteiras, o máximo divisor comum de a e b deve dividir c; e Brahmagupta sabia que se a e b são primos entre si, todas as soluções da equação são dadas por $x=p+mb$; $y=q\breve{}ma$, onde m é um número inteiro arbitrário [sendo p e q uma solução inteira particular]. (...) Brahmagupta merece muito louvor por ter dado todas as soluções inteiras da equação linear diofantina, enquanto que Diofante de Alexandria tinha se contentado em dar uma solução particular de uma equação indeterminada" (BOYER, 1974, p. 161).

4 CONHECIMENTOS PRELIMINARES EM TEORIA DOS NÚMEROS

Antes de se abordar o tema equações diofantinas é imprescindível o entendimento de novas notações, definições e teoremas particulares da *Teoria dos Números*. Neste capítulo serão apresentados alguns princípios, teoremas e proposições importantes, tais como o Princípio da Boa Ordenação (PBO), o Princípio da Indução Finita, o Algoritmo da divisão, o Algoritmo de Euclides, o Teorema Fundamental da unicidade, o Máximo Divisor Comum (MDC) e Mínimo Múltiplo Comum (MMC), algumas proposições sobre divisibilidade e Aritmética Modular.

Os critérios de divisibilidades são conteúdos geralmente tratados no 6º ano do Ensino Fundamental, conforme norteadamente sugere a Base Nacional Comum Curricular (BNCC) nas habilidades EF06MA04, EF06MA05 e EF06MA06.

> (EF06MA04) Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par).
>
> (EF06MA05) Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000.
>
> (EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor. (BRASIL, 2018, p. 301)

Portanto, faz parte das habilidades esperadas em alunos do ensino médio, visto que as competências são cumulativas.

4.1 Princípio da Boa Ordem e de Indução Finita

Dois princípios muito importantes na matemática são os Princípio da Boa Ordem - PBO - e Princípio de Indução Finita - PIF, são ferramentas frequentemente empregadas nas demonstrações de muitos teoremas ou proposições.

Princípio 4.1.1 (Princípio da Boa Ordem - PBO)**.** *Todo conjunto $A \subset \mathbb{N}$, não-vazio, contém um elemento mínimo a.*

Princípio 4.1.2 (Primeira forma do Princípio de Indução Finita - PIF)**.** *Seja $X \subset \mathbb{N}$. Se X possui as duas propriedades que seguem*

i. $1 \in X$

ii. $k+1 \in X$ *sempre que* $k \in X$

então $X = \mathbb{N}$.

Princípio 4.1.3 (Segunda forma do Princípio de Indução Finita - PIF)**.** *Seja $X \subset \mathbb{N}$. Se X possui as duas propriedades que seguem*

i. $1 \in X$

ii. $k+1 \in X$ *sempre que* $1,2,\ldots,k \in X$

então $X = \mathbb{N}$.

Apesar de o Princípio de Indução Finita sê possível demonstrá-lo a partir do Princípio da Boa Ordem não o faremos neste trabalho, a demonstração se encontra de forma clara e acessível em Santos (2006, p. 188). De antemão, vale ressaltar que o Conjunto dos Números Naturais neste trabalho está definido como $\mathbb{N} = \{1,2,3,\ldots\}$, conforme os *Axiomas de Peano*. Os axiomas de *Peano* se apresentam em Lima (2013, p. 27).

Exemplo 4.1.1. *Seja $n \in \mathbb{N}$, mostre que*

$$1+2+\ldots+n = \frac{n(n+1)}{2}$$

para todo n natural.

SOLUÇÃO: Primeiramente, devemos verificar que para $n = 1$ a sentença é verdadeira:

$$1 = \frac{1(1+1)}{2} = 1. \tag{4.1}$$

Suponhamos, pela hipótese de indução, que para n a igualdade é verdadeira

$$1+2+\ldots+n = \frac{n(n+1)}{2}. \tag{4.2}$$

Adicionando $n+1$ a ambos os membros, temos

$$1+2+\ldots+n+n+1 = \frac{n(n+1)}{2}+n+1 = \frac{(n+1)(n+2)}{2} = \frac{(n+1)\left[(n+1)+1\right]}{2}. \tag{4.3}$$

Logo, para todo n natural $1+2+\ldots+n = \frac{n(n+1)}{2}$.

Exemplo 4.1.2. *Mostre que*

$$1\cdot 2+2\cdot 3+3\cdot 4+\ldots+n(n+1) = \frac{n(n+1)(n+2)}{3}$$

para todo $n \in \mathbb{N}$.

SOLUÇÃO: Primeiramente, devemos verificar que para $n = 1$ a igualdade é verdadeira:

$$1\cdot 2 = \frac{1(1+1)(1+2)}{3} = 1\cdot 2.$$

Suponhamos, pela hipótese de indução, que para n a igualdade é verdadeira

$$1\cdot 2+2\cdot 3+3\cdot 4+\ldots+n(n+1)=\frac{n(n+1)(n+2)}{3}.$$

Somando $(n+1)(n+2)$ a ambos os membros, temos

$$\begin{aligned}1\cdot 2+2\cdot 3+3\cdot 4+\ldots+n(n+1)+(n+1)(n+2) &= \frac{n(n+1)(n+2)}{3}+(n+1)(n+2)\\ &= \frac{(n+1)(n+2)(n+3)}{3}.\end{aligned}$$

Logo, para todo n natural $1\cdot 2+2\cdot 3+3\cdot 4+\ldots+n(n+1)=\frac{n(n+1)(n+2)}{3}$.

Em alguns problemas uma certa propriedade pode ser verdadeira a partir de um certo número natural a, para isso é necessário o uso do Princípio de Indução Forte que é enunciado a seguir.

Princípio 4.1.4 (Princípio Forte de Indução)**.** *Seja $X\subset\mathbb{N}$ tal que*

i. $a\in X$*;*

ii. se $k\in X$ para $a\leq k\leq n$ então $n+1\in X$.

Então, $X=\{a,a+1,a+2,\ldots\}=\{n\in\mathbb{N}|n\geq a\}$.

Exemplo 4.1.3. *Mostre que $n!>2^n$ para $n>4$.*

SOLUÇÃO: Primeiramente, devemos verificar que a desigualdade só é verdadeira quando $n\geq 5$, assim, verificamos que para $n=5$, temos

$$5!>2^5\Leftrightarrow 120>32. \tag{4.4}$$

Suponhamos, pela hipótese de indução, que para n a desigualdade é verdadeira, isto é,

$$n!>2^n \tag{4.5}$$

Multiplicando ambos os lados por $n+1$, temos

$$(n+1)n!>(n+1)2^n \quad\Rightarrow\quad (n+1)!>(n+1)2^n=n\cdot 2^n+2^n>2\cdot 2^n=2^{n+1}. \tag{4.6}$$

Logo, para n natural maior do que 4 é válida a desigualdade $n!>2^n$.

Seja dada uma sentença matemática $P(n)$ que dependa de uma variável natural n, a qual se torna verdadeira ou falsa quando substituímos n por um número natural qualquer. Tais sentenças serão ditas *sentenças abertas* definidas sobre $\mathbb{N}$. Assim, pode-se enunciar o Princípio Forte de Indução da seguinte maneira, que em muitas situações são mais convenientes. A proposição $P(n)$ pode ser qualquer atributo (divisibilidade, igualdade ou desigualdade).

Princípio 4.1.5 (Princípio Forte de Indução - segunda versão)**.** *Seja $P(n)$ uma proposição sobre $X = \{n \in \mathbb{N} | n \geq a;\ a \in \mathbb{N}\}$. Se*

i. $P(a)$ é verdadeira;

ii. para todo n tal que $a \leq n \leq k$, tem-se $P(n)$ verdadeira, implica que $P(k+1)$ também é verdadeira.

Então para qualquer $n \in X$, $P(n)$ é verdadeira.

É razoável a analogia entre o Princípio de Indução Finita (ou Matemática) com a derrubada de uma peça de um dominó, ao cair a primeira peça equivale que a proposição é verdadeira para um dado a (menor elemento), supondo que a k-ésima peça da sequência caia ($a \leq k \leq n$) então a $k+1$-ésima peça também cai, assim, a proposição $P(n)$ é verdadeira para todo o conjunto de peças do dominó, ou seja, todas as peças serão derrubadas.

4.2 Divisibilidade

Definição 4.2.1 (Divisibilidade)**.** *Dados dois números inteiros a e b, diz-se que a divide b, se existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$. Equivalentemente, é dito que b é múltiplo de a, ou ainda, b é divisível por a. A notação é $a|b$ (a divide b), caso contrário, a notação é $a \not| b$.*

Vale enfatizar que $a|b$ não representa uma operação em $\mathbb{Z}$, outrossim, não faz referência a uma fração. Trata-se de uma sentença que se afirma verdadeira, pois, existe k inteiro tal que $b = a \cdot k$.

Proposição 4.2.1. *Sejam $a, b \in \mathbb{Z}^*$ e $c \in \mathbb{Z}$. Tem-se que*

i. $1|a$, $a|a$ e $a|0$.

ii. se $a|b$ e $b|c$, então $a|c$.

Demonstração. (i) Observe que é imediato, pois $a = 1 \cdot a = a \cdot 1$, com isso $1|a$ e $a|a$. Outrossim, $0 = a \cdot 0$, logo $a|0$, de modo que $a \neq 0$. (ii) Então existem k_1 e k_2 inteiros tais que $b = a \cdot k_1$ e $c = b \cdot k_2$, assim, decorre que $c = (a \cdot k_1) \cdot k_2 = a \cdot (k_1 \cdot k_2)$. Logo, $a|c$. □

Exemplo 4.2.1. *Se $5|35$ e $35|700$ então $5|700$.*

Exemplo 4.2.2. *Se $n|6$ e $6|72$ então $n|72$.*

Note que neste último exemplo, fica explicito que se a e b inteiros tal que $a \leq b$, o conjunto de divisores inteiros de a está contido no conjunto dos divisores inteiros de b.

Proposição 4.2.2. *Sejam $a,b,c \in \mathbb{Z}$, com $a \neq 0$, $a|b \cdot c \Leftrightarrow a|b$ ou $a|c$.*

Demonstração. ($\Leftarrow$) Sem perda de generalidade suponha $a|b$ (pode-se facilmente tomar $a|c$, ou ainda $a|b$ e $a|c$), assim, existe k_1 inteiro tal que $b = a \cdot k_1$, então $b \cdot c = (a \cdot k_1)c = a(k_1 \cdot c)$. Logo $a|bc$.

($\Rightarrow$) Suponha que $a|bc$, então existe k_2 inteiro tal que $a \cdot k_2 = bc$, logo $a|b$ ou $a|c$. □

Exemplo 4.2.3. *Sejam $p,q \in \mathbb{Z}$, com $p \neq 0$, se $p|3q$ então $p|3$ ou $p|q$.*

Proposição 4.2.3. *Sejam $a,b,c,d \in \mathbb{Z}$, com $a \neq 0$ e $c \neq 0$, se $a|b$ e $c|d$, então $a \cdot c|b \cdot d$.*

Demonstração. Assim, existem k_1 e k_2 tais que $b = a \cdot k_1$ e $d = c \cdot k_2$. Multiplicando b por d, temos $b \cdot d = (a \cdot k_1)(c \cdot k_2) = a \cdot c(k_1 \cdot k_2)$. Logo, $a \cdot c|b \cdot d$.

□

Exemplo 4.2.4. *Se $2|4$ e $3|9$ então $6|36$.*

Exemplo 4.2.5. *Se $n|10$ então $n^2|100$.*

Proposição 4.2.4. *Sejam $a,b,c \in \mathbb{Z}$, onde $a \neq 0$, tais que $a|(b \pm c)$. Então $a|b \Longleftrightarrow a|c$.*

Demonstração. ($\Rightarrow$) Supondo, primeiramente que $a|b \pm c$, então, existe p inteiro tal que $a \cdot p = b \pm c$. Agora, se $a|b$, existe q inteiro tal que $b = a \cdot q$. Portanto, $a \cdot p = a \cdot q \pm c \Rightarrow c = a(p \mp q)$. Logo $a|c$.

($\Leftarrow$) Reciprocamente, se $a|c$ então existe q' tal que $c = a \cdot q'$, como $a|b \pm c$, logo há um inteiro p' de modo que $a \cdot p' = b \pm c$, daí $a \cdot p' \mp a \cdot q' = b \Rightarrow b = a(p' \mp q')$. Portanto, $a|b$. □

A proposição 4.2.4 poderia ser escrita de outra forma mais intuitiva: se $a|b$ e $a|c$ então $a|(b \pm c)$. Esta segunda forma chamaria atenção para um fato curioso, que é a reciproca, se $a|(b \pm c)$ então $a|b$ e $a|c$? A resposta é negativa. Vamos tomar um exemplo simples, $7|(11+3)$, porém, $7 \not| 11$ e $7 \not| 3$, explicar-se-á melhor situações análogas fazendo uso da aritmética modular que será abordado na seção 4.8.

Exemplo 4.2.6. *Se $5|n$ e $5|(n+m)$ então $5|m$.*

Exemplo 4.2.7. *Se $a|(p^2+n)$ e $a|n$ então $a|p^2$.*

Proposição 4.2.5. *Sejam $a,b,c \in \mathbb{Z}$, onde $a \neq 0$, tais que $a|b$ e $a|c$, então $a|(mb+nc)$ para todo $m,n \in \mathbb{Z}$.*

Demonstração. Então existem k_1 e k_2 inteiros tais que $a \cdot k_1 = b$ e $a \cdot k_2 = c$, assim, $mb + nc = mak_1 + nak_2 = a(mk_1 + nk_2)$. Logo, $a|(mb + nc)$ para quaisquer $m, n \in \mathbb{Z}$. □

Exemplo 4.2.8. *Particularmente, quando $m = n = 1$ temos: se $a|b$ e $a|c$ então $a|b + c$.*

Exemplo 4.2.9. *Particularmente, quando $m = 1$ e $n = -1$ temos: se $a|b$ e $a|c$ então $a|b - c$.*

Exemplo 4.2.10. *Verifique que $n+1|(n^2+1)$ para algum $n \in \mathbb{Z}$.*

Deve-se usar o item 1 da proposição 4.2.1, $n+1|n+1$, e considerar que $n+1|(n^2+1)$, destarte, existem dois inteiros a e b, donde

$$n+1|[a(n+1) + b(n^2+1)],$$

tomando $a = -n$ e $b = 1$, temos que $n+1|1-n$. Agora, aplicamos a proposição 4.2.4, se $n+1|n+1$ e $n+1|1-n$ então $n+1|2$. O que possibilita a determinação de n, a escolha de a e b foi a mais conveniente para o nosso propósito. Portanto, $n+1 = \pm 1$ e $n+1 = \pm 2$, consequentemente, $n = \{-3, -2, 0, 1\}$.

Proposição 4.2.6. *Dados $a, b \in \mathbb{Z}^*$, se $a|b$ e $b|a$ então $|a| = |b|$.*

Demonstração. Então existem p e q inteiros tais que $b = ap$ e $a = bq$, daí, temos $b = bqp \Rightarrow qp = 1$. Sem perda de generalidade, podemos afirmar que $q|1$, ou seja, $q = \pm 1$. Logo, $a = \pm b \Rightarrow |a| = |b|$. □

Proposição 4.2.7. *Dados $a, b \in \mathbb{Z}$, onde $a \neq 0$, temos que, se $a|b$ então $|a| \leq |b|$.*

Demonstração. Então existe k inteiro tal que $b = ak$, com isso temos $|b| = |ak| = |a| \cdot |k| \geq |a|$. □

Problema 4.1. *Mostre que para todo $n \in \mathbb{N}$, $n^2|(n+1)^n - 1$.*

Proposição 4.2.8. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b|(a^n - b^n)$.*

Demonstração. A prova se dá por indução sobre n. Para $n = 1$, é evidente, pois $a^1 - b^1 = a - b$. Por hipótese, $a - b|(a^n - b^n)$, assim, existe $k \in \mathbb{Z}$ tal que $a^n - b^n = (a-b)k$. Com isso devemos provar que $a - b|(a^{n+1} - b^{n+1})$. Com efeito,

$$\begin{aligned} a^{n+1} - b^{n+1} &= aa^n - ba^n - bb^n + ba^n \\ &= (a-b)a^n + (a^n - b^n)b. \end{aligned}$$

Logo, para todo $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, $a - b|(a^n - b^n)$. □

Proposição 4.2.9. *Sejam $a,b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a+b|(a^{2n+1}+b^{2n+1})$.*

Demonstração. A prova também se dá por indução sobre n. Para $n=0$, é evidente, pois $a^1+b^1 = a+b$, para $n=1$, temos $a^3+b^3 = (a+b)\left(a^2-ab+b^2\right)$. Por hipótese, $a+b|(a^{2n+1}+b^{2n+1})$. Com isso devemos provar que $a+b|(a^{2n+3}-b^{2n+3})$. Reescrevendo, temos

$$\begin{aligned} a^{2n+3}+b^{2n+3} &= a^2a^{2n+1}-b^2a^{2n+1}+b^2b^{2n+1}+b^2a^{2n+1} \\ &= (a^2-b^2)a^{2n+1}+b^2(a^{2n+1}+b^{2n+1}). \end{aligned}$$

Logo, para todo $a,b \in \mathbb{Z}$ e $n \in \mathbb{N}$, $a+b|(a^{2n+1}-b^{2n+1})$. □

Proposição 4.2.10. *Sejam $a,b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a+b|(a^{2n}-b^{2n})$.*

Demonstração. Por indução, para $n=1$, temos $a^2-b^2 = (a-b)(a+b)$. Suponha, por hipótese, que $a+b|(a^{2n}-b^{2n})$. Reescrevendo

$$\begin{aligned} a^{2n+2}+b^{2n+2} &= a^2a^{2n}-b^2a^{2n}-b^2b^{2n}+b^2a^{2n} \\ &= (a^2-b^2)a^{2n}+b^2(a^{2n}-b^{2n}). \end{aligned}$$

Portanto, $a+b|(a^{2n}-b^{2n})$, para todo $a,b \in \mathbb{Z}$ e $n \in \mathbb{N}$. □

4.3 O Algoritmo da Divisão

O Algoritmo da Divisão (ou também conhecido *Algoritmo da Divisão Euclidiana*) tem essa denominação em homenagem ao grande matemático grego *Euclides de Alexandria* do qual não se tem muitas informações acerca, no entanto, a maioria dos estudiosos concluem que a sua obra mais magistral, "O Elementos", data por volta de 300 a.C., esta obra foi uma compilação em vários livros de proposições, postulados, definições e teoremas em diversas áreas conhecidas da matemática que foram ensinadas de forma oral e empírica de gerações anteriores e de outros povos. O *Algoritmo da Divisão* foi escrito no início do livro VII de "Os Elementos", além dele muitas outras proposições e teoremas podem ter sido apenas condensadas nesta obra, Euclides pode ter apenas "reeditado". Segundo Eves (2004), a obra "Os Elementos"que chegou até os tradutores do ocidente por volta do século XII foi por meio de traduções feitas para o árabe, onde se supõe que seu trabalho tenha chegado ao ocidente com ligeiras modificações que não corromperam a essência da obra. Euclides foi brilhante em vários campos da matemática, tanto na Geometria quanto na Teoria dos Números, o rigor lógico introduzido em seus trabalhos é um

divisor de água entre as proto-matemáticas e a matemática formal e axiomática que conhecemos atualmente.

Antes de ser apresentado o Algoritmo da Divisão, há um teorema de grande importância o *Teorema de Eudoxius*, erroneamente atribuído a Arquimedes como *Princípio de Arquimedes*.

Teorema 4.3.1 (Teorema de Eudoxius)**.** *Dados dois inteiros a e b, $b \neq 0$, então a é um múltiplo de b ou se encontra entre dois múltiplos de b. Assim, se $b > 0$ temos*

$$b \leq a < (q+1)b$$

e se $b < 0$ temos

$$qb \leq a < (q-1)b.$$

Demonstração. Vamos analisar três situações:

- se $a = bk$ para algum k inteiro, então, a é múltiplo de b e não há nada a provar.
- se $a \neq bk$, onde $a > 0$ e $b > 0$ inteiros, pelo princípio 4.1.1 (Princípio da Boa Ordem), existe $x \in \mathbb{Z}$ menor inteiro tal que $a < xb$. Assim, $(x-1)b < a$, portanto, $(x-1)b < a < xb$. Pondo $q = x-1$, obtemos $qb < a < (q+1)b$.
- se $a \neq bk$, onde $a < 0$ e $b < 0$, por outro lado, $-a > 0$ e $-b > 0$, novamente pelo princípio 4.1.1 (Princípio da Boa Ordem), existe $x \in \mathbb{Z}$ menor inteiro tal que $-a < -xb$, com isso temos $-(x-1)b < -a < -xb \Rightarrow xb < a < (x-1)b$, tomando $x = q$, conclui-se que $qb < a < (q-1)b$.

Além das três situações acima há duas outras situações, $a < 0$ e $b > 0$ ou $a > 0$ e $b < 0$ que podem ser mostradas de forma análoga às que estão acima. □

Decerto que o Algoritmo de Euclides tenha sido influenciado pelos paradigmas da matemática grega, visto que os números a serem considerados eram apenas os positivos. O Algoritmo é uma importante ferramenta até os dias atuais, abaixo está transcrito como se encontra em Santos (2006, p. 4):

Teorema 4.3.2 (Algoritmo da Divisão)**.** *Dados dois inteiros a e b, $b > 0$, existe um único par de inteiros q e r tais que*

$$a = qb + r,$$

com $0 \leq r < b$ ($r = 0 \Leftrightarrow b|a$). Onde q é chamado de quociente e r de resto da divisão de a por b.

Demonstração. Pelo Teorema de Eudoxius, como $b > 0$, existe q satisfazendo:

$$qb \leq a < (q+1)b$$

o que implica $0 \leq a - qb$ e $a - qb < b$. Desta forma, se definirmos $r = a - qb$, teremos, garantida, a existência de q e r. A fim de mostrarmos a unicidade, vamos supor a existência de outro par q_1 e r_1 verificando:

$$a = q_1 b + r_1 \qquad \text{com} \qquad 0 \leq r_1 < b.$$

Disto temos $(qb+r) - (q_1 b + r_1) = 0 \Rightarrow b(q - q_1) = r_1 - r$, o que implica $b|(r_1 - r)$. Mas, como $r_1 < b$ e $r < b$, temos $|r_1 - r| < b$ e, portanto, como $b|(r_1 - r)$ devemos ter $r_1 - r = 0$ o que implica $r = r_1$. Logo $q_1 b = qb \Rightarrow q_1 = q$, uma vez que $b \neq 0$. □

Observação: Embora no enunciado do algoritmo exista a restrição $b > 0$, isto não é necessário e, utilizando-se o Teorema de Eudoxius teríamos encontrado q e r também para $b < 0$. Podemos, pois, anunciar o Algoritmo da Divisão de Euclides da seguinte forma: Dados dois inteiros a e b, $b \neq 0$ existe um único par de inteiros q e r tais que $a = qb + r$ com $0 \leq r < |b|$.

Essa última do algoritmo da divisão euclidiana é usada por Hefez (2013), o mesmo autor emprega o Teorema de Eudoxius como um colorário do algoritmo.

Exemplo 4.3.1. *O quociente e o resto da divisão de* 73 *por* 13 *são* $q = 5$ *e* $r = 8$*. No entanto, na divisão* -73 *por* 13 *temos o quociente* $q = -6$ *e o resto* $r = 5$*, visto que* $0 \leq r < |b|$*.*

Exemplo 4.3.2. *O quociente e o resto da divisão de* 63 *por* 9 *são* $q = 7$ *e* $r = 0$*. Quando dividimos* -63 *por* 9 *temos o quociente* $q = -7$ *e o resto* $r = 0$*.*

Quando se menciona algoritmo tem-se em mente um roteiro, um procedimento estruturado de acordo com um sequência lógica pré-determinadas. Apesar desses serem mais utilizadas atualmente em linguagens computacionais, desde os primeiros povos que desenvolveram suas proto-matemáticas os algoritmos foram bastante empregados. No dicionário online Priberam temos as seguintes difinições:

> *al·go·rit·mo*
> (latim medieval algorismus ou algorithmus, do árabe al-Huuarizmi, nome de um matemático árabe do século IX) substantivo masculino 1. [Matemática] .Sequência finita de instruções não ambíguas utilizadas para resolver um problema ou fazer um cálculo.
>
> 2. [Matemática] Processo de cálculo.
>
> 3. [Informática] Conjunto de regras e operações bem definidas e não ambíguas, que, aplicadas a um conjunto de dados e num número finito de etapas, conduzem à solução de um problema.
>
> "algoritmo", in Dicionário Priberam da Língua Portuguesa [em linha], 2008-2020, <https://dicionario.priberam.org/algoritmo> [consultado em 14-02-2020].

Em Coutinho (2005, p. 20) temos o algoritmo da divisão escrito em pseudocódigo, isto é, escrito em linguagem convencional (diferente de alguma linguagem de programação de máquina, tais como C/C++, Fortran, Pascal, java, lisp etc).

> **Algoritmo de divisão.**
> **Entrada:** inteiros positivos a e b.
> **Saída:** inteiros não-negativos q e r tais que $a = bq + r$ e $0 \leq r < b$.
> **Etapa 1:** Comece fazendo $Q = 0$ e $R = a$.
> **Etapa 2:** Se $R < b$ escreva o quociente é Q e o resto é R e pare; senão vá para a Etapa 3.
> **Etapa 3:** Se $R \geq b$ subtraia b de R, incremente Q de 1 e volte à Etapa 2.
> (COUTINHO, 2005, p. 20)

Dessarte, podemos obter outra proposição acerca da divisibilidade.

Proposição 4.3.1. *Sejam a e b inteiros, $b \neq 0$, temos que b divide a se, e somente se, o resto da divisão entre a e b é $r = 0$.*

Demonstração. ($\Rightarrow$) Supondo que $b|a$ e $r \neq 0$, então existe $q \in \mathbb{Z}$ tal que $a = bq$, assim pelo teorema 4.3.2, temos $a = bq + r$. Logo $r = 0$ (absurdo!) ($\Leftarrow$) A recíproca é imediata, se $r = 0$ então $a = bq + r = bq$, logo $b|a$. □

4.4 Sistema de Numeração

Sabe-se que atualmente o sistema de numeração mundialmente utilizado é o *sistema decimal*, porém, não foi o primeiro a ser utilizado pelo homem. Como escreveu Eves (2004, p. 28 - 29):

> O sistema vigesimal (base 20) também foi amplamente usado, e remonta aos dias em que o homem andava descalço. Esse sistema foi usado por índios americanos, mais conhecido pelo bem desenvolvido sistema de numeração maia. As palavras-número francesas *quatre-vingt* (oitenta) em vez de *huitante* e *quatre-vingt-dix* (noventa) em vez de *nonante* são traços da base 20 dos celtas. Também se encontram traços no gaélico, no dinamarquês e no inglês. Os groenlandeses usam "um homem" para 20, "dois homens" para 40 e assim por diante. em inglês há a palavra *score* (uma vintena), frequentemente usada.
>
> O sistema sexagesimal (base 60) foi usado pelos babilônios, sendo ainda empregado na medida do tempo e de ângulos em minutos e segundos. (EVES, 2004, p. 28 - 29)

Atualmente os computadores e outras máquinas utilizam os sistemas binários (base 2) ou hexadecimal (base 16). Eves (2004, p. 35) o atual sistema de numeração é posicional, formado pelos algarismos hindu-arábicos (0,1,2,3,4,5,6,7,8 e 9), no entanto, não foi o primeiro e único, os babilônios entre os anos de 3000 a.C e 2000 a.C. usavam um sistema posicional na base 60 (sexagesimal).

Vale ressaltar ainda que bem antes da criação do zero pelo hindus, havia outras formas para representar as lacunas que ficavam sem algarismos, isto é, o zero foi criado como um símbolo e não como quantificador.

Em Eves (2004) podemos observar uma representação para o algarismo zero no sistema de numeração maia que era essencialmente vigesimal (base 20).

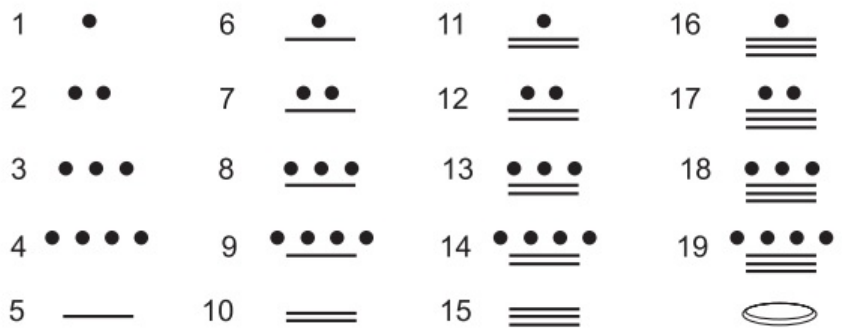


Figura 2 – Tábua da representação do sistema de numeração maia, sistema de base vigesimal. Fonte: (EVES, 2004).

Ainda segundo Eves (2004) a palavra *zero* vem da palavra latina *zephirum* derivada da palavra *sifr* que é uma tradução árabe para *sunya* que significa "vazio"ou "vácuo"em hindu. Os ábacos, por exemplo, até hoje conservam a representação do zero por uma lacuna.

A seguir é apresentado um importante teorema que garante a representação de um número natural em qualquer base dada, ver Hefez (2013).

Teorema 4.4.1. *Dados $n, b \in \mathbb{N}$, com $b > 1$, existem números naturais $a_0, a_1, \ldots, a_n$ menores do que b, univocamente determinados, tais que $n = a_0 + a_1 b + a_2 b^2 + \ldots + a_k b^k$.*

Demonstração. Vamos provar utilizando a segunda forma do Princípio da Indução Finita (Princípio 4.1.3) sobre n. Se $n = 0$, basta tomar $k = 0$. Se $n = 1$, basta tomar $k = 1$. Supondo que o resultado seja verdadeiro para todo natural menor do que n, vamos prová-lo para n. Pelo algoritmo da divisão, existem q e r únicos tais que $n = bq + r$, com $r < b$.

Como $q < a$, pela hipótese de indução, segue-se que existem números naturais m e $d_0, d_1, \ldots, d_m$, com $d_i < b$ para todo i tais que

$$q = d_o + d_1 b + \ldots + d_m b^m.$$

Assim, segue que

$$a = bq + r = b(d_o + d_1 b + \ldots + d_m b^m) + r,$$

comparando os resultados, temos $r = a_0$, $n = m+1$ e $a_j = d_{j-1}$ para $j = 1, \ldots, n$.

A unicidade dos a_j se dá pela unicidade do resto, dada pelo teorema 4.3.2. □

O teorema acima é a aplicação do algoritmo da divisão euclidiana sucessivas vezes, como segue:

$$\begin{aligned} a &= bq_0 + r_0, \quad r_0 < b \\ q_0 &= bq_1 + r_1, \quad r_1 < b \\ q_1 &= bq_2 + r_2, \quad r_2 < b \\ &\vdots \quad \vdots \\ q_{n-1} &= bq_n + r_n, \quad r_2 < b \end{aligned}$$

Como $a > q_0 > q_1 > \ldots q_{n-1} > q_n = 0$, para $q_{n-1} < b$. Portanto, os algarismos de um número natural n em uma base $b > 1$ são formados pelos restos de uma divisão sucessiva de n por b, assim, podemos escrever $n = r_n r_{n-1} \ldots r_1 r_0$.

Exemplo 4.4.1. *Escreva o número 2020 na base 5.*

Fazendo as divisões euclidianas sucessivas, temos:

$$\begin{aligned} 2020 &= 5 \times 404 + 0 \\ 404 &= 5 \times 80 + 4 \\ 80 &= 5 \times 16 + 0 \\ 16 &= 5 \times 3 + 1 \\ 3 &= 5 \times 0 + 3. \end{aligned}$$

Então, $2020 = 3 \times 5^4 + 1 \times 5^3 + 0 \times 5^2 + 4 \times 5 + 0$. *Assim, a representação do número 2020 na base* 5 *é* $(31040)_5$.

Exemplo 4.4.2. *Escreva o número 2020 na base 5.*

Fazendo as divisões euclidianas sucessivas, temos:

$$\begin{aligned} 2020 &= 5\times 404+0 \\ 404 &= 5\times 80+4 \\ 80 &= 5\times 16+0 \\ 16 &= 5\times 3+1 \\ 3 &= 5\times 0+3. \end{aligned}$$

Então, $2020 = 3\times 5^4+1\times 5^3+0\times 5^2+4\times 5+0$. *Assim, a representação do número 2020 na base* 5 *é* $(31040)_5$.

Exemplo 4.4.3. *Represente o número 523 na base 2.*

Fazendo as divisões euclidianas sucessivas, temos:

$$\begin{aligned} 523 &= 2\times 261+1 \\ 261 &= 2\times 130+1 \\ 130 &= 2\times 65+0 \\ 65 &= 2\times 32+1 \\ 32 &= 2\times 16+0 \\ 16 &= 2\times 8+0 \\ 8 &= 2\times 4+0 \\ 4 &= 2\times 2+0 \\ 2 &= 2\times 1+0 \\ 1 &= 2\times 0+1 \end{aligned}$$

Então, $523 = 1\times 2^9+0\times 2^8+0\times 2^7+0\times 2^6+0\times 2^5+0\times 2^4+1\times 2^3+0\times 2^2+1\times 2+1$.

Representa-se 523 na base binária da seguinte maneira: $523 = (1000001011)_2$

Exemplo 4.4.4. *Considere 73 na base 10; em qual base ele se escreve 243?*

Seja a representação de 73 numa base n igual a 243*, basta equacionar*

$$\begin{aligned} 2\cdot n^2+4\cdot n+3 &= 73 \\ 2n^2+4n-70 &= 0 \\ 2\left(n^2+2n-35\right) &= 0 \\ 2\left(n+7\right)\left(n-5\right) &= 0. \end{aligned}$$

Como a base $n>1$, então, a base é $n=5$.

Quando se escreve um inteiro n forma $n=a_kb^k+a_{k-1}b^{k-1}+\ldots+a_1b+a_0$, diz-se que é a expansão relativa à base b, onde todos $a_i<b$, com $i=1,\ldots,k$. Se $b=10$, diz-se expansão decimal.

4.5 Critérios de divisibilidade

Com base nas definições, teoremas e proposições anteriores pode-se provar a validade de algumas "regras"de divisibilidade, por exemplo: os critérios de divisibilidade por 2, 3, 4, 5, 7, 9 e 10. Vale ressaltar que há muitos algoritmos específicos para verificar a divisibilidade para diversos números primos.

Proposição 4.5.1 (Divisibilidade por 2)**.** *Seja N um número inteiro com $k+1$ algarismos (quando N é escrito por um único algarismo, tem-se o caso $N=a_0$), 2 divide N se, e somente se, ele tem o algarismo das unidades par (0,2,4,6 ou 8).*

Demonstração. Escrevendo a expansão de N relativa à base 10, temos

$$N=a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_1\cdot 10+a_0.$$

Pela proposição 4.2.5 $2|\left(a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_1\cdot 10\right)$, pois, 2 divide as potências de 10. Se $2|N$, então, pela proposição 4.2.4, $2|a_0$.

A reciproca é imediata pela proposição 4.2.4, se $2|a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_1\cdot 10$ e $2|a_0$, logo $2|N$. □

Proposição 4.5.2 (Divisibilidade por 4)**.** *Seja N um número inteiro, 4 divide N se, e somente se, o número formado pelos algarismo da dezena e da unidade é divisível por 4.*

Demonstração. Escrevendo a expansão de N relativa à base 10, temos

$$N=a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_1\cdot 10+a_0.$$

Pela proposição 4.2.5 $4|\left(a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_2\cdot 10^2\right)$, pois, 4 divide as potências de 10^j para $j\geq 2$. Se $4|N$, então, pela proposição 4.2.4, $4|a_1a_0$.

A reciproca é análoga à da proposição 4.5.1, pela proposição 4.2.4, se $4|a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_2\cdot 10^2$ e $4|a_1a_0$, logo $4|N$. □

Aplicando o *Princípio da Indução Finita (ou Matemática)* pode-se verificar que se $2^k|N$ então $2^k|a_{k-1\ldots a_1a_0}$. Particularmente, a "regra"de divisão (algoritmo) ensinado geralmente no 6º ano do ensino fundamental diz que um número é divisível por 8 se os três últimos algarismos formam um número divisível por 8, isto é, o algoritmo é válido quando se tem pelo menos quatro algarismos. Quando o número tiver três ou menos algarismos deve ser verificado pelo *Algoritmo da Divisão*.

Proposição 4.5.3 (Divisibilidade por 3)**.** *Um número inteiro N é divisível por* 3 *se, e somente se, a soma de seus algarismos é divisível por 3.*

Demonstração. Tomando N um número inteiro escrito na base 10, temos

$$N=a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_1\cdot 10+a_0.$$

Note que $9|\left(10^k-1\right)$ como $3|9$ então $3|\left(10^k-1\right)$. Reescrevendo N, convenientemente, temos

$$\begin{aligned}N &= a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_1\cdot 10+a_0\\ N &= a_k\cdot\left(10^k-1\right)+a_{k-1}\cdot\left(10^{k-1}-1\right)+\ldots+a_1\cdot\left(10^1-1\right)+\left(a_k+a_{k-1}+\ldots+a_1+a_0\right).\end{aligned}$$

Se $3|N$ e $3|\sum_{j=1}^{k}\left(10^j-1\right)$ então $3|\left(a_k+a_{k-1}+\ldots+a_1+a_0\right)$.

A recíproca é imediata. □

Proposição 4.5.4 (Divisibilidade por 9)**.** *Um número inteiro N é divisível por* 9 *se, e somente se, a soma de seus algarismos é divisível por 9.*

Demonstração. Tomando N um número inteiro escrito na base 10, temos

$$\begin{aligned}N &= a_k\cdot 10^k+a_{k-1}\cdot 10^{k-1}+\ldots+a_1\cdot 10+a_0\\ N &= a_k\cdot\left(10^k-1\right)+a_{k-1}\cdot\left(10^{k-1}-1\right)+\ldots+a_1\cdot\left(10^1-1\right)+\left(a_k+a_{k-1}+\ldots+a_1+a_0\right).\end{aligned}$$

Note que $9|9|\sum_{j=1}^{k}\left(10^j-1\right)$. Se $9|N$ então $9|\left(a_k+a_{k-1}+\ldots+a_1+a_0\right)$.

Reciprocamente, se $9|\sum_{j=1}^{k}\left(10^j-1\right)$ e $9|\left(a_k+a_{k-1}+\ldots+a_1+a_0\right)$ então $9|N$. □

Proposição 4.5.5 (Divisibilidade por 5)**.** *Um número inteiro N é divisível por* 5 *se, e somente se, o algarismo da unidade é* 0 *ou* 5*.*

Demonstração. Como 5 divide qualquer combinação linear das potências de 10, se $5|N$, então 5 divide o último algarismo, que só pode ser 0 ou 5.

Reciprocamente, se $5|\sum_{j=1}^{k} a_j \cdot 10^j$ e $5|a_0$ então $5|N$. □

Proposição 4.5.6 (Divisibilidade por 10)**.** *Um número inteiro N é divisível por* 10 *se, e somente se, o algarismo das unidades é* 0*.*

Demonstração. Escrevendo $N = 10k + i$, onde k é um natural e i é o algarismo das unidades, se $10|N$ então $10|i$, logo $i = 0$. Reciprocamente, se $i = 0$ é evidente que $10|N$. □

Proposição 4.5.7 (Divisibilidade por 11)**.** *Um número inteiro* $N = a_k a_{k-1} \ldots a_1 a_0$ *é divisível por* 11 *se, e somente se,* $\left(\sum_{j=0}^{p} a_{2j} + 10 \cdot a_{2j+1}\right)$, $p \in \mathbb{N}$*, é múltiplo de 11.*

Demonstração. Representando N na expansão decimal, temos

$$N = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10^1 + a_0$$

Note que $10^2 = 11 \cdot 9 + 1$ e $10^3 = 11 \cdot 90 + 10$, por meio recursivo, pode-se verificar que quando o expoente da potência de dez é par o resto da divisão por 11 é 1 e quando é ímpar o resto é 10. Assim, pode-se escrever N da seguinte forma

$$\begin{aligned} N &= a_{2p+1} \cdot \left(10^{2p+1} - 10\right) + a_{2p} \cdot \left(10^{2p} - 1\right) + a_{2p-1} \cdot \left(10^{2p-1} - 10\right) + \ldots + a_2 \cdot \left(10^2 - 1\right) \\ &+ \left(10 \cdot a_{2p+1} + a_{2p} + 10 \cdot a_{2p-1} + \ldots + a_2 + 10 \cdot a_1 + a_0\right) \end{aligned}$$

Como $10^{2j+1} - 10$ e $11|10^{2j} - 1$ são múltiplos de 11, então, se $11|N$, logo

$$11|\left(10 \cdot a_{2p+1} + a_{2p} + 10 \cdot a_{2p-1} + \ldots + a_2 + 10 \cdot a_1 + a_0\right).$$

A recíproca é trivial. □

Proposição 4.5.8 (Divisibilidade por 7)**.** *Um número inteiro* $N = 10k + i$*, onde* i *é o algarismo da unidade, é divisível por* 7 *se, e somente se, o número obtido pela subtração entre o número formado pela exclusão do algarismo da unidade e o dobro deste algarismo é um múltiplo de 7, isto é,* $k - 2i$ *é múltiplo de 7.*

Demonstração. Supondo que $7|(10k+i)$ então existe $p \in \mathbb{Z}$ tal que $10k+i = 7p$, com isso, $i = 7p-10k$, portanto, $k-2i = 21k-14p = 7(3k-2p)$, logo, $7|k-2i$. A reciproca se prova de maneira análoga, se $7|(k-2i)$ então existe $q \in \mathbb{Z}$ de modo que $k-2i = 7q$, o que implica em $k = 7q+2i$, o que leva a $10k+i = 70q+21i = 7(10q+3i)$. □

O algoritmo para verificar a divisibilidade por 7 tem sua aplicação recursiva, isto é, pode-se aplicar diversas vezes até se obter $k-2i$ suficientemente pequeno para facilitar a verificação.

Exemplo 4.5.1. *Verifique que 476 é múltiplo de 7.*

Basta retirar o último algarismo (da unidade) e se obtém 47*, subtraindo pelo dobro de 6, temos:* $47-12 = 35$ *que é múltiplo de 7 (divisível por 7).*

Exemplo 4.5.2. *Verifique que 7 divide* 7539*.*

Escrever $7539 = 753 \times 10+3$*, assim,* $k = 753$ *e* $i = 3$*. Mas, neste caso já devemos a aplicar a recursividade do algoritmo.*

n (laço)	k	i	$k-2i$
1	*753*	*9*	*735*
2	*73*	*5*	*63*
3	*6*	*3*	*0*

Veja que $k-2i$ *do laço 1 será obtido k e i do laço 2 e assim sucessivamente, no exemplo acima bastaria até o laço 2, visto que 63 é múltiplo de 7. No entanto, foi útil seguir até zero para mostrar que caso o número seja divisível por 7 atingirá o seu menor múltiplo não negativo, zero.*

4.6 O Máximo Divisor Comum (M.D.C.) e o Algoritmo de Euclides

Quando se fala em máximo divisor comum é natural a proposição de problemas do dia-a-dia, como segue:

Problema 4.6.1. *João é carpinteiro e dispõe de dois pedaços de madeiras, um com 40 cm e outro com 25 cm de comprimento, de mesma largura e espessura. João deseja cortá-lo em pedaços menores de modo que eles tenham o maior comprimento em números inteiros. Qual deve ser o comprimento, em cm, de cada pedaço?*

Nesta seção será mostrado alguns resultados importantes sobre o *Máximo Divisor Comum*. Além de exemplos do dia a dia em que temos aplicação dos conhecimentos em *Máximo Divisor Comum*.

Definição 4.6.1. *O máximo divisor comum d de dois números inteiros a e b, denotado por* $d = (a,b)$*, é o maior número inteiro positivo que divide a e b.*

Teorema 4.6.1. *Seja d o máximo divisor comum de a e b, então existem inteiros* m_0 *e* n_0 *tais que* $d = am_0 + bn_0$.

Demonstração. Seja $C = \{c = am + bn,\ a,b,m,n \in \mathbb{Z}\}$ o conjunto de todas as combinações lineares de a e b com $c = am_0 + bn_0$ sendo o menor inteiro positivo pertencente ao conjunto C. Deve-se provar que $c|a$ e $c|b$. Suponha que $c \nmid a$, isto é, existem q e r tais que $a = qc + r$ com $0 < r < c$, portanto, $r = a - qc = a - q(am_0 + bn_0) = a(1 - qm_0) + b(qn_0)$, o que mostra $r \in C$, absurdo, visto que $r < c$ e c é o menor elemento de C. Logo $c|a$ e de forma análoga se prova que $c|b$.

Como d divide a e b, existem inteiros k_1 e k_2 tais que $a = dk_1$ e $b = dk_2$, então $c = am_0 + bn_0 = d(ak_1 + bk_2)$ o que implica que $d|c$. Sabendo-se que $d \leq c$ e $d < c$ é absurdo, então, $d = am_0 + bn_0$. □

Proposição 4.6.1. *Dados a, b e k inteiros,* $(ka,kb) = k \cdot (a,b)$.

Demonstração. Pelo Teorema 4.6.1 existem m e n inteiros tais que

$$(ka,kb) = m(ka) + n(kb) = k(am + bn) = k \cdot (a,b).$$

□

Proposição 4.6.2. *Se* $c > 0$ *e c divide a e b, então*

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

Demonstração. Se c divide a e b então existem k_1 e k_2 inteiros tais que $a = ck_1$ e $b = ck_2$, assim, existem m_0 e n_0 inteiros tais que

$$(k_1,k_2) = m_0k_1 + n_0k_2.$$

Multiplicando ambos os lados por c, temos

$$c(k_1,k_2) = m_0ck_1 + n_0ck_2 = am_0 + bn_0 = (a,b).$$

Segue-se que

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

□

Corolário 4.6.1. *Se* $(a,b)=d$*, temos que* $\left(\frac{a}{d},\frac{b}{d}\right)=1$.

Demonstração. A demonstração é imediata pela Proposição 4.6.2, pois é um caso particular, isto é, quando $c=d$, segue que

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

□

Um conceito muito importante na matemática que surgiu ainda nos trabalhos de Euclides foi o de *Números Primos*, apesar de hoje se ter uma vasta teoria sobre eles, ainda resistem alguns mistérios tais como a obtenção de uma função que mapeie todos os números primos, um desafio que intrigou as maiores mentes da matemática. As correspondências entre Christian Goldbach e Leonhard Euler deram origem ao que hoje conhece-se por *Conjectura de Goldbach*. O crivo de Eratóstenes talvez tenha sido a primeira intrigante descoberta sobre esses números que apresenta um definição breve e sucinta.

Definição 4.6.2. *Um número inteiro n (*$n>1$*) possuindo somente dois divisores naturais* 1 *e n é chamado de* número primo*. Se* $n>1$ *não é primo dizemos que é* composto*.*

Definição 4.6.3. *Os inteiros a e b são relativamente* primos entre si *quando* $(a,b)=1$.

Teorema 4.6.2. *Para a, b, c e x inteiros, com* $c>0$*, temos* $(a,bx)=c\cdot(a,b)$.

Demonstração. Seja $d=(a,b)$ então existem k_1 e k_2 inteiros tais que $a=dk_1$ e $b=dk_2$, pelo Teorema 4.6.1 existem inteiros p_0 e q_0 tais que

$$(a,bx)=ap_0+bxq_0=dk_1p_0+dk_2q_0=(k_1p_0+k_2q_0)d.$$

Tomando $c=k_1p_0+k_2q_0$, temos $(a,bx)=c\cdot(a,b)$. O valor do máximo divisor comum é limitado pelo maior entre a e b, ou seja, $(a,bx)\leq\max\{a,b\}$. □

Teorema 4.6.3. *Para a, b e x inteiros temos* $(a,b)=(a,b+ax)$.

Demonstração. Sejam $d = (a,b)$ e $f = (a, b+ax)$ então existem inteiros m e n tais que $d = am + bn$. Note que $d = a(m-nx) + (b+ax)n$ que pelo Teorema 4.6.1 implica que existem $m-nx$ e n inteiros tais que f é uma combinação linear deles. Por outro lado, é evidente que $d|f$, como d e f são positivos segue $d = f$. □

Teorema 4.6.4. *Se a e b são inteiros e $a = bq + r$ onde q e r são inteiros, com $0 \leq r < b$, então $(a,b) = (b,r)$.*

Demonstração. Seja $a = bq + r$, se d é divisor de b e r então d divide a. Rescrevendo $r = bq - a$, é imediato que para todo d que divide a e b também divide r. Portanto, os conjuntos de divisores dos dois pares de inteiros são iguais, logo $(a,b) = (b,r)$. □

Teorema 4.6.5 (Algoritmo de Euclides)**.** *Sejam $r_0 = a$ e $r_1 = b$ inteiros não-negativos com $b \neq 0$. Se o algoritmo da divisão for aplicado sucessivamente para se obter*

$$r_i = q_{i+1} r_{r+1} + r_{r+2} \quad , \quad 0 \leq r_{i+2} < r_{r+1}$$

para $i = 0, 1, \ldots, n-1$ e $r_{n+1} = 0$ então $(a,b) = r_n$, o último resto não-nulo.

Demonstração. A prova se dá aplicando o algoritmo da divisão (Teorema 4.3.2), inicialmente, para dividir $r_0 = a$ por $r_1 = b$, assim, tem-se $r_0 = q_1 r_1 + r_2$. Recursivamente, pode-se determinar a divisão r_1 por r_2 obtendo $r_1 = q_2 r_2 + r_3$ e assim, sucessivamente, até obter $r_{n+1} = 0$. A sequência formada pelo restos da divisão sucessiva é decrescente, isto é, $r_i > r_{i+1}$ para $i = 0, 1, \ldots, n$, portanto, após um número finito de divisões sucessivas o algoritmo para, pois chega a um resto nulo. Segue abaixo a sequência de restos obtidos com a aplicação do algoritmo da divisão sucessivas vezes:

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 \quad , \quad 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 \quad , \quad 0 < r_3 < r_2 \\
r_2 &= q_3 r_3 + r_4 \quad , \quad 0 < r_4 < r_3 \\
&\vdots \quad \vdots \quad \vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n \quad , \quad 0 < r_n < r_{n-1} \\
r_{n-1} &= q_n r_n + 0 \quad , \quad r_{n+1} = 0 < r_n.
\end{aligned}$$

Pelo Teorema 4.6.4 na sequência acima, conclui-se que $(r_{n-1}, r_n) = (r_{n-2}, r_{n-1}) = \ldots = (r_0, r_1) = (a,b) = r_n$. Portanto, o máximo divisor comum de a e b é o último resto não nulo da sequência de divisões sucessivas. □

O Algoritmo de Euclides é uma ferramenta muito importante para nossos propósitos neste trabalho, visto que o cálculo do máximo divisor comum é um passo indispensável na resolução de equações diofantinas lineares. Particularmente, é comum o uso do *Algoritmo de Euclides Estendido* que é uma versão em que se faz uso de recorrências de modo a explicitar uma combinação linear entre dois números iniciais, a e b.

O máximo divisor comum pode ser estendido para mais do que um par de números, na verdade, pode ser estendido para uma sequência de n inteiros. Segue abaixo o caso do cálculo do máximo divisor comum para três números inteiros, a prova para n inteiros é obtido por indução (será omitido aqui).

Proposição 4.6.3. *Sejam a, b e c inteiros temos* $(a,b,c) = ((a,b),c)$.

Demonstração. Se $(a,b,c) = d$ então existem inteiros k_1, k_2 e k_3 tais que $a = dk_1$, $b = dk_2$ e $c = dk_3$. Com isso, $(a,b) = d$, assim, temos

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

□

Quando se fala em Máximo Divisor Comum também vem em mente o Mínimo Múltiplo Comum, decerto, há uma relação intrínseca entre eles, que será exposto daqui a pouco, no entanto, é preciso entender o conceito de fatoração explicitado pelo *Teorema Fundamental da Álgebra* que não será demonstrado aqui, visto que seu resultado é muito conhecido e se encontra nas obras Santos (2006), Coutinho (2005) e Moreira *et al.* (2011).

Teorema 4.6.6 (Teorema Fundamental da Aritmética)**.** *Seja* $n \geq 2$ *um número natural. Podemos escrever n de uma única forma como um produto*

$$n = p_1 \cdot \ldots \cdot p_m$$

onde $m \geq 1$ *é um natural e* $p_1 \leq \ldots \leq p_m$ *são primos.*

Em suma, o Teorema Fundamental da Aritmética afirma que para qualquer número n natural maior ou igual a 2 pode ser escrito como um produto de potências de números primos, ou seja, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$, onde p_i é um primo e α_i é um inteiro não negativo. Fica entendido que a ordem dos fatores primos não importa e que todo número possui uma única fatoração em potência de primos, com isso, pode-se expressar o máximo divisor comum pela seguinte proposição.

Proposição 4.6.4. *Sejam* $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ *e* $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}$*, onde* p_i *são primos, então* $(a,b) = \prod_1^n p_i^{\min\{\alpha_i,\beta_i\}}$.

Demonstração. Dados dois inteiros positivos a e b temos duas situações: i) a e b são primos entre si, neste caso $(a,b) = \prod_{i=1}^n p_i^{\min\{\alpha_i,\beta_i\}} = \prod_1^n p_i^0 = 1$. ii) a e b não são primos entre si, assim, existe pelo menos um p_i em comum nas duas fatorações, por conseguinte, o máximo divisor será o produto de todas as potências de primos em comum com o menor expoente entre eles, isto é, $(a,b) = \prod_{i=1}^n p_i^{\min\{\alpha_i,\beta_i\}}$. □

Exemplo 4.6.1. *Determine o máximo divisor comum entre 120 e 36.*

***Solução**: Basta decompor os números e observar quais são as potências de fatores primos com maior expoente em comum:* $120 = 2^3 \times 3 \times 5$ *e* $36 = 2^2 \times 3^2$*. Pela Proposição 4.6.4, temos* $(120,36) = 2^2 \times 3 = 12$.

A Proposição 4.6.4 é um algoritmo muito prático para a obtenção do máximo divisor e também para determinar a quantidade de divisores naturais de um número natural.

Proposição 4.6.5. *Seja* $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_m^{\alpha_m}$*, onde* p_i *são primos e* α_i *inteiros não negativos, então* $d(n) = \prod_1^m (\alpha_i + 1) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_m + 1)$*, onde* $d(n)$ *é a quantidade de divisores naturais de n.*

Demonstração. A prova se dá por indução em m. Para $m = 1$, temos $n = p_1^{\alpha_1}$, assim, os divisores naturais são $1, p_1, p_1^2, \ldots, p_1^{\alpha_1}$, isto é, $d(n) = \alpha_1 + 1$. Quando $m = 2$ temos $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$, consequentemente, temos como divisores naturais $1, p_1, p_1^2, \ldots, p_1^{\alpha_1}, p_2, p_2p_1, p_2p_1^2, \ldots, p_2^{\alpha_2}p_1^{\alpha_1}$, assim, $d(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1)$. Tomando sucessivas vezes, até m, é fácil concluir que $d(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_m + 1)$. □

Exemplo 4.6.2. *Determine a quantidade de divisores naturais de* 528.

***Solução**: Tomando a decomposição em fatores primos de* 528*, temos:*

$$528 = 2^4 \times 3 \times 11.$$

Assim, a quantidade de divisores naturais é $d(528) = (4+1) \cdot (1+1) \cdot (1+1) = 20$.

Exemplo 4.6.3. *Determine a quantidade de divisores naturais de* 5200 *que são quadrados perfeitos.*

***Solução**: Tomando a decomposição em fatores primos de* 5200*, temos:*

$$5200 = 2^3 \times 3^3 \times 5^2.$$

Assim, a quantidade de divisores naturais é $d(528) = (3+1)\cdot(3+1)\cdot(2+1) = 48$.

No entanto se deseja contar somente os divisores quadrados perfeitos, outrossim, deve-se reagrupar os expoentes aos pares, de maneira genérica pode-se determinar por $Q(n) = p_1^{\lfloor \frac{\alpha_1}{2} \rfloor} \cdot p_2^{\lfloor \frac{\alpha_2}{2} \rfloor} \cdot \ldots \cdot p_m^{\lfloor \frac{\alpha_m}{2} \rfloor}$*., então,*

$$d(Q(n)) = \left(\lfloor \frac{\alpha_1}{2} \rfloor + 1\right)\left(\lfloor \frac{\alpha_2}{2} \rfloor + 1\right) \cdot \ldots \cdot \left(\lfloor \frac{\alpha_m}{2} \rfloor + 1\right).$$

No caso, temos $Q(5200) = 2^{\lfloor \frac{3}{2} \rfloor} \cdot 3^{\lfloor \frac{3}{2} \rfloor} \cdot \cdot 5^{\lfloor \frac{2}{2} \rfloor}$*, logo,* $d(Q(n)) = 2 \cdot 2 \cdot 2 \cdot 2 = 8$*, ou seja, o número 5200 tem 8 divisores quadrados perfeitos.*

Apesar de ter ficado claro pela definição 4.6.2 que todo número primo possui somente dois divisores naturais (1 e o próprio número), pode-se verificar pela proposição 4.6.5.

4.7 Mínimo Múltiplo Comum

Definição 4.7.1. *O Mínimo Múltiplo Comum de dois inteiros positivos a e b é o menor inteiro positivo que é divisível por a e b. Vamos denotá-lo por [a,b].*

Proposição 4.7.1. *Se* $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ *e* $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}$*, onde* $p_1, p_2, \ldots, p_n$ *são os primos que ocorrem nas fatorações de a e de b, então*

$$[a,b] = \prod_{i=1}^{n} p_i^{\max\{\alpha_i, \beta_i\}}$$

Demonstração. Pela definição 4.7.1, $[a,b]$ é um múltiplo de a e b, para ser múltiplo deve possuir na forma fatorada todos os fatores primos que estejam na fatoração de a e de b com os maiores expoentes possíveis, portanto, $[a,b] = p_1^{\max\{\alpha_1,\beta_1\}} \cdot p_2^{\max\{\alpha_2,\beta_2\}} \cdot \ldots \cdot p_n^{\max\{\alpha_n,\beta_n\}} = \prod_{i=1}^{n} p_i^{\max\{\alpha_i,\beta_i\}}$. □

Teorema 4.7.1. *Sejam a e b inteiros positivos temos,* $[a,b] \cdot (a,b) = a \cdot b$.

Demonstração. Se $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ e $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}$, então $a \cdot b = p_1^{\alpha_1+\beta_1} \cdot \ldots \cdot p_n^{\alpha_n+\beta_n}$. Como $\alpha_i + \beta_i = \min\{\alpha_i, \beta_i\} + \max\{\alpha_i, \beta_i\}$, portanto, chegamos a

$$a \cdot b = \left(p_1^{\min\{\alpha_1,\beta_1\}} \cdot p_2^{\min\{\alpha_2,\beta_2\}} \cdot \ldots \cdot p_n^{\min\{\alpha_n,\beta_n\}}\right)\left(p_1^{\max\{\alpha_1,\beta_1\}} \cdot p_2^{\max\{\alpha_2,\beta_2\}} \cdot \ldots \cdot p_n^{\max\{\alpha_n,\beta_n\}}\right).$$

Logo $a \cdot b = [a,b] \cdot (a,b)$. □

Corolário 4.7.1. *Sejam a e b primos entre si, então* $[a,b] = a \cdot b$.

Demonstração. Se $(a,b) = 1$, pelo Teorema 4.7.1 é imediato que $[a,b] = a \cdot b$. □

4.8 Congruência

Nesta seção será tratada uma importante relação na teoria dos números, a *congruência*. O tema foi abordado por Gauss em um dos seus celebres trabalhos em Teoria dos Números, *Disquisitiones Arithmeticae* publicado em 1801 já continha até a mesma notação que é utilizada até os dias atuais. São mostrados alguns resultados importante, no entanto, não será mostrado as provas referentes.

Definição 4.8.1. *Sejam a, b e m números inteiros dizemos que a é* congruente *a b módulo m* $(m > 0)$ *se* $m|(a-b)$. *Denota-se por* $a \equiv b(mod\ m)$. *Se* $m \nmid (a-b)$ *dizemos que a é incongruente a b módulo m e é denotado por* $a \not\equiv b(mod\ m)$.

Exemplo 4.8.1. $26 \equiv 1(mod\ 5)$, *pois* $5|(26-1)$. *Note que* 1 *é o resto da divisão de* 26 *por* 5.

Exemplo 4.8.2. $37 \equiv 4(mod\ 11)$, *pois* $11|(37-4)$.

A proposição a seguir mostra que a *congruência* possui as propriedades reflexiva, antissimétrica e transitiva, ou seja, é uma relação de equivalência.

Proposição 4.8.1. *Seja* $m \in \mathbb{N}$. *Para todos* $a,b,c \in \mathbb{Z}$, *tem-se que*

i. $a \equiv a(mod\ m)$;

ii. *se* $a \equiv b(mod\ m)$, *então* $b \equiv a(mod\ m)$;

iii. *se* $a \equiv b(mod\ m)$ *e* $b \equiv c(mod\ m)$, *então* $a \equiv c(mod\ m)$.

Teorema 4.8.1. *Se a, b, c e m são inteiros tais que* $a \equiv b(mod\ m)$ *então*

i. $a + c \equiv b + c(mod\ m)$;

ii. $a - c \equiv b - c(mod\ m)$;

iii. $ac \equiv bc(mod\ m)$.

Teorema 4.8.2. *Se a, b, c e m e* $ac \equiv bc(mod\ m)$, *então* $a \equiv b(mod\ m/d)$ *onde* $d = (c,m)$.

Definição 4.8.2. *Se r e s são dois inteiros com* $r \equiv s(mod\ m)$, *dizemos que s é um resíduo de r módulo m.*

Definição 4.8.3. *O conjunto dos inteiros* $\{r_1, r_2, \ldots, r_n\}$ *é um sistema completo de resíduos módulo m se*

1. $r_i \not\equiv r_j (mod\ m)$ *para* $i \neq j$;
2. *para todo inteiro n existe um* r_i *tal que* $n \equiv r_i (mod\ m)$.

Proposição 4.8.2. *Se a, b, k e m são inteiros com* $k > 0$ *e* $a \equiv b (mod\ m)$, *então* $a^k \equiv b^k (mod\ m)$.

Proposição 4.8.3. *Se* $a \equiv b (mod\ m_1)$, $a \equiv b (mod\ m_2)$, $\ldots, a \equiv b (mod\ m_k)$ *onde* $a, b, m_1, m_2, \ldots, m_k$ *são inteiros com* m_i *positivos,* $i = 1, 2, \ldots, k$, *então*

$$a \equiv b (mod\ [m_1, m_2, \ldots, m_k])$$

onde $[m_1, m_2, \ldots, m_k]$ *é o mínimo múltiplo comum de* $m_1, m_2, \ldots, m_k$.

Há várias ocasiões que é mais conveniente analisar os restos da divisão, pois, estes seguem às "regras"da *aritmética modular* que são as propriedades de congruência. Por exemplo, determinar o algarismo das unidades do número $2^{77} + 3^{80}$.

4.8.1 Congruência Linear

Definição 4.8.4. *Denomina-se* congruência linear *em uma variável uma congruência da forma* $ax \equiv b (mod\ m)$ *onde x é uma incógnita.*

Definição 4.8.5. *Diz-se que uma solução* x_0 *de* $ax \equiv b (mod\ m)$ *é única módulo m quando qualquer outra solução* x_1 *for congruente a* x_0 *módulo m.*

Definição 4.8.6. *Uma solução* $\overline{a}$ *de* $ax \equiv 1 (mod\ m)$ *é chamada de um inverso de a módulo m.*

Proposição 4.8.4. *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se, e somente se,* $a \equiv 1 (mod\ p)$ *e* $a \equiv -1 (mod\ p)$.

4.8.2 Os Teoremas de Euler, Fermat, Wilson e o Teorema Chinês do Resto

Aqui são destacados os referidos teoremas pelas relevantes importâncias em seus resultados.

Teorema 4.8.3 (Teorema de Wilson)**.** *Se p é primo, então* $(p-1)! \equiv -1 (mod\ p)$.

Demonstração. Para $p = 2$ e $p = 3$ é fácil verificar a validade. A congruência do tipo $ax \equiv 1 (mod\ p)$ tem uma única solução para todo $a \in \{1, 2, 3, \ldots, p-1\}$, e como, destes elementos

somente 1 e $p-1$ são seus próprios inversos módulo p, pode-se agrupá-los em $\frac{p-3}{2}$ pares cujo produto seja congruente a 1 módulo p. Multiplicando todas as congruências, membro a membro, obtém-se

$$2 \times 3 \times 4 \times \ldots \times (p-2) \times (p-1) \equiv (p-1)(mod\ p).$$

Logo $(p-1)! \equiv -1(mod\ p)$, visto que $p-1 \equiv -1(mod\ p)$. □

Teorema 4.8.4 (Pequeno Teorema de Fermat)**.** *Seja p é primo. Se* $p \nmid a$ *então* $a^{p-1} \equiv 1(mod\ p)$.

Demonstração. Seja $\{0,1,2,\ldots,p-1\}$ um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívuca com um subconjunto de $\{0,1,2,\ldots,p-1\}$. Considere os números $a, 2a, 3a, \ldots, (p-1)a$, como $(a,p) = 1$ nenhum deles é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak(mod\ p)$ implic $j \equiv k(mod\ p)$, só é possível se $j = k$. Logo, cada um deles é congruente a exatamente um dentre os elementos $1,2,3,\ldots,p-1$. Multiplicando estas congruências, membro a membro, tem-se

$$\begin{aligned} a \cdot 2a \cdot \ldots (p-1)a &\equiv 1 \cdot 2 \cdot \ldots \cdot (p-1)(mod\ p) \\ a^{p-1}(p-1)! &\equiv (p-1)!(mod\ p). \end{aligned}$$

Como $p \nmid (p-1)!$, daí decorre que $p|(a^{p-1}-1)$, portanto, $a^{p-1} \equiv 1(mod\ p)$. □

Teorema 4.8.5 (Euler)**.** *Se m é um inteiro positivo e a um inteiro com* $(a,m) = 1$*, então*

$$a^{\phi(m)} \equiv 1(mod\ m).$$

Demonstração. Ver Santos (2006, p. 43-44). □

A prova do Teorema 4.8.5 será omitida aqui, pois seria necessário alguns conceitos que se distanciam do objetivo deste trabalho.

A função $\phi(n)$ de Euler pode ser apresentada de maneira simplificada como sendo a função que conta quantos números tem de 1 a $n-1$ que são primos com n. Por exemplo, $\phi(10) = 4$, pois os números $1,3,7,9$ são primos com 10. Em Santos (2006, p. 72-73) estão disponíveis mais propriedades desta importante função aritmética.

Exemplo 4.8.3. $2^6 \equiv 1(mod\ 7)$

Exemplo 4.8.4. $5^2 \equiv 1(mod\ 6)$

Exemplo 4.8.5. $7^8 \equiv 1(mod\ 16)$

Teorema 4.8.6 (Teorema Chinês do Resto)**.** *Se* $(a_i, m_i) = 1$, $(m_i, m_j) = 1$ *para* $i \neq j$ *e* c_i *inteiro, então o sistema*

$$\begin{cases} a_1X & \equiv & b_1(mod\ m_1) \\ a_2X & \equiv & b_2(mod\ m_2) \\ a_3X & \equiv & b_3(mod\ m_3) \\ \vdots & \vdots & \vdots \\ a_rX & \equiv & b_r(mod\ m_r) \end{cases}$$

possui solução e a solução é única módulo m, onde $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$*. O sistema de congruências acima é equivalente*

$$\begin{cases} X & \equiv & c_1(mod\ n_1) \\ X & \equiv & c_2(mod\ n_2) \\ X & \equiv & c_3(mod\ n_3) \\ \vdots & \vdots & \vdots \\ X & \equiv & c_r(mod\ n_r) \end{cases}$$

Com $(n_i, n_j) = 1$ *para* $i \neq j$ *e* $n = n_1 \cdot n_2 \cdot \ldots \cdot n_r$*. Tendo como solução*

$$x = N_1y_1c_1 + \ldots + N_ry_rc_r,$$

onde $N_i = N/n_i$ *e* y_i *é solução de* $N_iY \equiv 1(mod\ n_i)$, $i = 1, \ldots, r$.

O teorema chinês do resto é aplicado para resolver sistemas de congruências lineares que recaem problemas que envolvem restos, como é mostrado no exemplo a seguir.

Exemplo 4.8.6. *Ache o menor número natural que deixa restos 1, 3 e 5 quando dividido por 5, 7 e 9, respectivamente.*

***Solução**: Primeiramente, equaciona-se o sistema*

$$\begin{cases} X & \equiv & 1(mod\ 5) \\ X & \equiv & 3(mod\ 7) \\ X & \equiv & 5(mod\ 9) \end{cases}$$

Segundo passo é obter $N = 5 \cdot 7 \cdot 9 = 315$, *assim,* $N_1 = 315/5 = 63$, $N_2 = 315/7 = 45$ *e* $N_3 = 315/9 = 35$. *Para determinar* y_i *devemos resolver algumas congruências lineares separadamente:*

$$\begin{cases} 63y_1 & \equiv & 1(mod\ 5) \Rightarrow y_1 = 2 \\ 45y_2 & \equiv & 1(mod\ 7) \Rightarrow y_2 = 5 \\ 35y_3 & \equiv & 1(mod\ 9) \Rightarrow y_3 = 8 \end{cases}$$

Portanto,

$$\begin{aligned} x &= 63 \cdot 2 \cdot 1 + 45 \cdot 5 \cdot 3 + 35 \cdot 8 \cdot 5 = 2201 \\ x &\equiv 2201(mod\ 315) \equiv 311(mod\ 315). \end{aligned}$$

Então $x = 311 + 315t$, $t \in \mathbb{Z}$, *quando* $t = 0$ *se tem* 311 *como o menor natural que satisfaz ao sistema de congruências.*

Exemplo 4.8.7. *Resolva o sistema a seguir em* $\mathbb{Z}$

$$\begin{cases} 2x & \equiv & 1(mod\ 5) \\ 5x & \equiv & 3(mod\ 11) \\ 7x & \equiv & 2(mod\ 17) \end{cases}$$

Solução*: Deve-se determinar um sistema de congruências equivalente na forma do sistema*

$$\begin{cases} X & \equiv & c_1(mod\ n_1) \\ X & \equiv & c_2(mod\ n_2) \\ X & \equiv & c_3(mod\ n_3) \end{cases}$$

Assim, tem-se

$$\begin{cases} 8 \cdot 2x & \equiv & 8 \cdot 1(mod\ 5) \\ 9 \cdot 5x & \equiv & 9 \cdot 3(mod\ 11) \\ 5 \cdot 7x & \equiv & 5 \cdot 2(mod\ 17) \end{cases} \Rightarrow \begin{cases} x & \equiv & 3(mod\ 5) \\ x & \equiv & 5(mod\ 11) \\ x & \equiv & 10(mod\ 17) \end{cases}$$

Agora se obtem $N = 5 \cdot 11 \cdot 17 = 935$, *assim,* $N_1 = 935/5 = 187$, $N_2 = 935/11 = 85$ *e* $N_3 = 935/17 = 55$. *Para determinar* y_i *devemos resolver algumas congruências lineares separadamente:*

$$\begin{cases} 187y_1 & \equiv & 1(mod\ 5) \Rightarrow y_1 = 7 \\ 85y_2 & \equiv & 1(mod\ 11) \Rightarrow y_2 = 3 \\ 55y_3 & \equiv & 1(mod\ 17) \Rightarrow y_3 = 13 \end{cases}$$

Portanto,

$$\begin{aligned} x &= 85 \cdot 7 \cdot 5 + 187 \cdot 3 \cdot 3 + 55 \cdot 13 \cdot 10 = 11808 \\ x &\equiv 11808(mod\ 935) \equiv 588(mod\ 935). \end{aligned}$$

Então $x = 588 + 935t$, $t \in \mathbb{Z}$.

5 EQUAÇÕES DIOFANTINAS

Neste capítulo fica definido o que é equação diofantina e como resolvê-las, especialmente, as lineares que é o principal objetivo. Será mostrado aqui como resolver as equações diofantinas em duas variáveis. A definição a seguir pode ser consultada em Ribeiro (2014, p. 26).

Definição 5.0.1. *Uma equação diofantina é uma equação do tipo*

$$f(x_1, x_2, \ldots, x_n) = 0 \tag{5.1}$$

onde f é uma função n-variável com $n \geq 2$ e coeficientes inteiros. As soluções de 5.1 são as n-uplas $(a_1, a_2, \ldots, a_n)$ em que $a_i \in \mathbb{Z},\ 1 \leq i \leq n$. Este tipo de equação recebe a denominação diofantina *em homenagem a Diofanto, que em seus trabalhos restringira seus resultados a números racionais positivos ou inteiros positivos.*

As equações diofantinas nem sempre tem solução nos inteiros, a exemplo: $x^n + y^n = z^n$, para $n \geq 3$, não tem soluções inteiras, até 1994, a assertiva era uma conjectura, pois nenhum matemático tinha provado se havia ou não soluções inteiras, tudo começou quando Pierre de Fermat escreveu nas margens de um exemplar de *Aritmética* de Diofanto que teria uma prova que afirmaria a não existência de soluções inteiras para tal proposição, no entanto, não escrevera pois não caberia. A maioria dos matemáticos da atualidade creem que foi um blefe de Fermat afim de irritar seus rivais, em especial, Descartes. Fermat mantinha segredo em todos os seus trabalhos sobre matemática, a qual se dedicava como um passatempo. Apenas em 1994, um matemático britânico Andrew Wiles, professor da Universidade de Princeton, demonstrou a validade da conjectura, assim, passou a ser denominado *O Último Teorema de Fermat*, em Singh (2018) são dados pormenores acerca de fatos históricos deste grande marco na história da matemática.

5.1 Alguns métodos elementares para resolução de equações diofantinas

No trabalho de Ribeiro (2014) há a proposta do uso de fatoração e de inequações para resolução de alguns tipos de equações diofantinas não lineares, algo extremamente viável para aluno de ensino médio, no entanto, vale ressaltar que se exige muita habilidade e as limitações, visto que certas questões exigem estratégias muito sofisticadas.

Os *ternos pitagóricos* são soluções da equação diofantina $a^2 + b^2 = c^2$, onde a e b são catetos e c é a hipotenusa de um triângulo retângulo. Para as equações pitagóricas há infinitas soluções inteiras, a ideia para determinar a existência de soluções inteiras é analisar que todo

quadrado perfeito deixa resto igual a 0 ou 1 quando dividido por 4, no entanto, apenas isso não basta para de fato resolver, é recomendada a leitura de Neto (2012, p. 52).

5.1.1 Método da fatoração para resolução de equações diofantinas

Exemplo 5.1.1 (Extraído de Círculos Matemáticos: A experiência russa)**.** *Resolva em* $\mathbb{Z}$

$$(2x+y)(5x+3y) = 7.$$

Solução*: Note que* $2x+y$ *e* $5x+3y$ *são números que estão na forma fatorada. Como a solução está no conjunto dos números inteiros, tem-se quatro possibilidades o que dá quatro sistemas de equações em x e em y. Daí,*

$$\begin{cases} 2x+y &= -1 \\ 5x+3y &= -7 \end{cases} \textit{ ou } \begin{cases} 2x+y &= 1 \\ 5x+3y &= 7 \end{cases}$$
$$\begin{cases} 2x+y &= -7 \\ 5x+3y &= -1 \end{cases} \textit{ ou } \begin{cases} 2x+y &= 7 \\ 5x+3y &= 1 \end{cases}$$

Resolvendo os quatro sistemas, obtém-se as soluções inteiras, $S = \{(4,-9);(-4,9);(20,-33);(-20,33)\}$.

Exemplo 5.1.2 (Extraído de Círculos Matemáticos: A experiência russa)**.** *Resolva em* $\mathbb{Z}$

$$xy = x+y+3.$$

Solução*: Nesta questão a estratégia para resolver é fatorar por agrupamento, escrever x em termos de y e explorar as propriedades de divisibilidade.*

$$\begin{aligned} xy = x+y+3 &\Rightarrow xy-x = y+3 \\ x(y-1) = y+3 &\Rightarrow x = \frac{y+3}{y-1} = 1+\frac{4}{y-1} \end{aligned}$$

Veja que $x \in \mathbb{Z} \iff (y-1)|4$*, ou seja,* $y-1 = \pm 1$ *ou* $y-1 = \pm 2$ *ou* $y-1 = \pm 4$*. Obtém-se o seguinte conjunto solução,* $S = \{(5,2);(2,5);(0,-3);(-3,0);(3,3);(-1,-1)\}$.

Exemplo 5.1.3 (Extraído de Círculos Matemáticos: A experiência russa)**.** *Resolva em* $\mathbb{Z}$

$$\frac{1}{a}+\frac{1}{b}+\frac{1}{c} = 1.$$

***Solução**: Nesta questão o primeiro passo é obter o máximo divisor comum entre os denominadores e a estratégia segue com as propriedades de divisibilidade em $\mathbb{Z}$.*

$$\begin{aligned} \frac{ab+ac+bc}{abc} &= 1 \\ ab+ac+bc &= abc \\ a(b+c) &= bc(a-1) \\ \frac{a}{a-1} &= \frac{bc}{b+c} = k \end{aligned}$$

Veja que $k \in \mathbb{Z} \iff (a-1)|a$, como $a = (a-1)+1$ segue que $(a-1)|1$, ou seja, $a-1 = \pm 1$ o que implica em $a = 2$ ou $a = 0$, no entanto, $a \neq 0$, portanto $a = 2$. Assim, obtém-se os valores para b e c.

$$\begin{aligned} \frac{bc}{b+c} = 2 &\Rightarrow bc = 2b+2c \\ bc-2b = 2c &\Rightarrow b(c-2) = 2c \\ b &= \frac{2c}{c-2} \end{aligned}$$

Analogamente, $b \in \mathbb{Z} \iff (c-2)|2c$, como $(c-2)|2c$ então $(c-2)|2$ ou $(c-2)|c$, mas note que $c = (c-2)+2$, portanto, basta $(c-2)|2$, assim, vem que $c-2 = \pm 2$ ou $c-2 = \pm 1$. Portanto $c_1 = 1$, $c_2 = 3$, $c_3 = 4$, respectivamente, $b_1 = -2$, $b_2 = 6$ e $b_3 = 4$. Logo, as soluções são as ternas $(2,-2,1),(2,6,3),(2,4,4)$.

5.1.2 Usando inequações para resolver equações diofantinas

Nem sempre é possível resolver apenas usando fatoração, em certos casos é conveniente limitar um intervalo de valores inteiros ou naturais afim de resolver ou pelo menos refinar o espaço amostral das prováveis soluções.

Exemplo 5.1.4. *Determine as soluções da equação*

$$3(xy+xz+yz) = 4xyz.$$

***Solução**:Reescrevendo a equação, temos*

$$\frac{xy+xz+yz}{xyz} = \frac{4}{3},$$

que equivale a

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z} = \frac{4}{3}.$$

Sem perda de generalidade podemos assumir que $x \leq y \leq z$. Isto implica que

$$\frac{3}{x} \geq \frac{4}{3} \Rightarrow x \leq \frac{9}{4} \Rightarrow x \in \mathbb{Z}.$$

Se $x = 1$, temos

$$\frac{1}{y} + \frac{1}{z} = \frac{1}{3} \Rightarrow \frac{2}{y} \geq \frac{1}{3} \Rightarrow y \leq 6 \Rightarrow y \in \{1,2,3,4,5,6\}.$$

Substituindo os valores obtemos as soluções (1, 4, 12) e (1, 6, 6).

Caso $x = 2$, temos

$$\frac{1}{y} + \frac{1}{z} = \frac{5}{6} \Rightarrow \frac{2}{y} \geq \frac{5}{6} \Rightarrow y \leq \frac{12}{5} \Rightarrow y \in \{2\}.$$

Assim obtemos as soluções (2,2,3). Portanto, as soluções são $(1,4,12), (1,6,6)$ e $(2,2,3)$.

Exemplo 5.1.5. *Resolva a equação em $\mathbb{Z}$,*

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

***Solução**: A equação acima é conhecida como equação de Pell, pois é do tipo $x^2 - Ay^2 = 1$, com x e y inteiros e A é um inteiro positivo diferente de um quadrado perfeito, ver Souza (2017, p. 61). Porém, é possível resolvê-la por métodos elementares como segue:*

$$\begin{aligned} x^2 - 2y^2 &= 1 \\ 2(x^2 - y^2) &= 1 + x^2 \\ 2\left[(x-y)(x+y)\right] &= (x^2 - 1) + 2 \\ 2\left[(x-y)(x+y) - 1\right] &= (x-1)(x+1) \end{aligned}$$

Analisando o segundo membro da equação, quando $x = \pm 1 \Rightarrow y = 0$. Assim, temos duas soluções $(-1,0)$ e $(1,0)$. Note que o resultado do segundo membro deve ser par, com isso vamos considerar duas situações: x par ou x ímpar.

Caso x par, isto é, $x = 2k$, com $k \in \mathbb{Z}$, teríamos $(2k+1)(2k-1) = 2q$, q inteiro, logo absurdo. Caso x ímpar, isto é, $x = 2k+1$, temos

$$\begin{aligned} 2\left[(x-y)(x+y)-1\right] &= (x-1)(x+1) \\ 2\left((2k+1)^2-y^2-1\right) &= 2(2k)(k+1) \\ 4k^2+4k-y^2 &= 2k^2+2k \\ 2k^2+2k-y^2 &= 0 \\ y &= \pm\sqrt{2k(k+1)} \end{aligned}$$

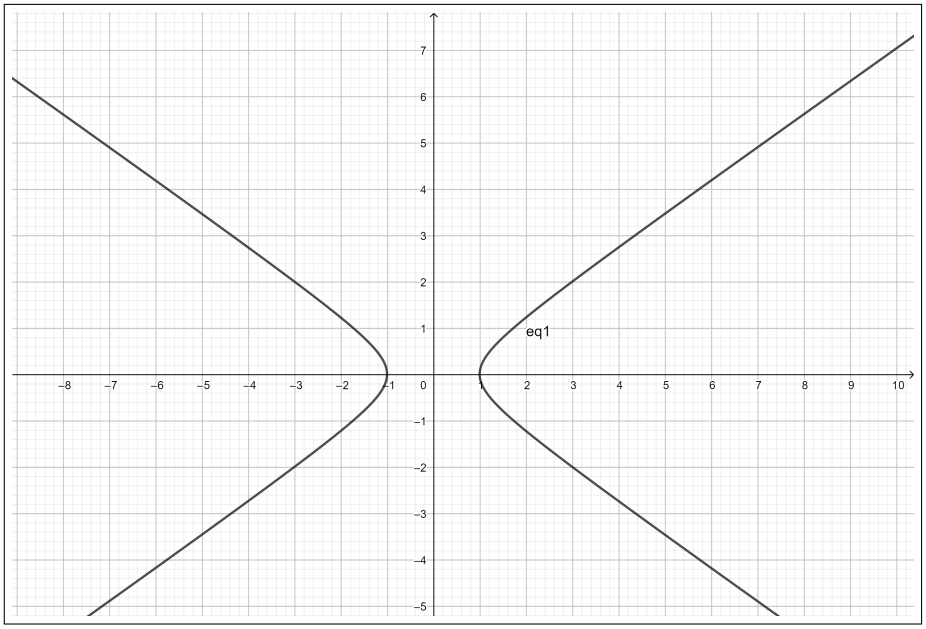
Quando x é ímpar encontramos um par de possíveis valores para y, mas devemos escolher y inteiro, note que y é inteiro se, e somente se, a decomposição seja do tipo $y = p^2$*, portanto, devemos ter* $2k = k+1$*, então* $k = 1$*. Portanto,* $x = 3$ *e* $y = \pm 2$*. No entanto, se elevarmos ao quadrado a igualdade* $y = \pm\sqrt{2k^2+2k}$*, obtemos*

$$2k^2+2k = 4 \Rightarrow 2(k^2+k-2) = 0 \Rightarrow 2(k+2)(k-1) = 0.$$

Assim, encontramos $k = -2$*, então,* $x = -3$ *e* $y = \pm 2$*.*

Logo, o conjunto solução desta equação em $\mathbb{Z}$ *é (-3,-2),(-3,2), (-1,0),(1,0),(3,-2) e (3,2).*

Figura 3 – Gráfico da solução da equação $x^2 - 2y^2 = 1$.



Fonte: elaborado pelo autor (2020).

5.2 Equações Diofantinas Lineares

5.2.1 Equações Diofantinas em duas variáveis

Esta subseção se detém a mostrar o caso mais simples de equações diofantinas lineares, com duas incógnitas, visto sua proximidade com problemas relacionados com equações lineares que são exploradas junto ao conteúdo de sistemas de equações lineares no Ensino Médio.

Teorema 5.2.1 (Existência de soluções)**.** *A equação diofantina $ax+by=c$ tem solução inteira se, e somente se, o máximo divisor comum de a e b, $(a,b)=d$, divide c.*

Demonstração. Seja (x_0,y_0) solução particular da equação $ax+by=c$. Como d divide a e divide b, ele também divide ax_0+by_0, e com isso divide c. De modo recíproco, se d divide c, então $c=d\cdot k$, para algum k inteiro. Por outro lado, sabemos que existem inteiros m e n, tais que $d=am+bn \Rightarrow d\cdot k=(am+bn)\cdot k=a(mk)+b(nk)$. E assim, então, existe (mk,nk) que é solução da equação. Pondo $x_0=mk$ e $y_0=nk$, assim

$$ax_0+by_0=amk+bnk=c.$$

Por outro lado,

$$ax+by=c \Rightarrow ax+by=ax_0+by_0 \Rightarrow a\left(x-x_0+\frac{b}{d}k\right)+b\left(y-y_0-\frac{a}{d}k\right)=0.$$

Logo as soluções são $x=x_0+\frac{b}{d}k$ e $y=y_0-\frac{a}{d}k$. Há ainda uma quantidade infinita de soluções se c for um múltiplo de d. Caso contrário, a equação Diofantina $ax+by=c$ não possui solução. □

Como consequência temos o seguinte corolário que a prova é imediata, portanto, adotamos como postulado.

Corolário 5.2.1. *Se $(a,b)=1$, isto é, se a e b são relativamente primos (ou primos entre si), então a equação $ax+by=c$ sempre tem soluções inteiras, qualquer que seja c.*

Vejamos agora alguns exemplos com situações que podem ser resolvidas por meio de equações diofantinas lineares em duas variáveis.

Exemplo 5.2.1. *João sacou R$ 150 em um caixa eletrônico que dispunha de cédulas de R$ 20 e R$ 50, quais são as possibilidades de saques que ele pode fazer?*

***Solução**: Este problema pode ser resolvido por meio de resolução gráfica, sem a necessidade de aplicar equações diofantinas lineares visto que apresenta um pequeno número*

de soluções, no entanto, vamos mostrar que é uma estratégia viável. Seja a equação linear $20x+50y=150$ *uma equação diofantina, pois, as soluções do problema devem ser números inteiros positivos (números racionais não satisfazem devido à natureza do problema). Note que* $(20,50)=10$ *que divide* 150*, assim, sabemos que há infinitas soluções inteiras, porém, para o caso só nos interessam as positivas. Aplicamos o algoritmo de Euclides, para determinar uma solução particular (podemos obter uma solução particular por inspeção).*

Pelo Algoritmo de Euclides:

$$\begin{aligned} 50 &= 20\cdot 2+10 \\ 20 &= 10\cdot 2+0 \end{aligned}$$

Assim, $20\cdot(-2)+50\cdot 1=10$*, multiplicando por* 15*, obtemos uma solução particular* (x_0,y_0)*:*

$$50\cdot 15+20\cdot(-30)=150.$$

Portanto, a solução geral da equação é dada por

$$\begin{cases} x &= -30+5k \\ y &= 15-2k \end{cases}$$

com k inteiro. Porém, devemos impor as restrições $x\geq 0$ *e* $y\geq 0$*, ou seja,*

$$\begin{cases} -30+5k\geq 0 &\Rightarrow\ k\geq 6 \\ 15-2k\geq 0 &\Rightarrow\ k\leq \frac{15}{2} \end{cases}$$

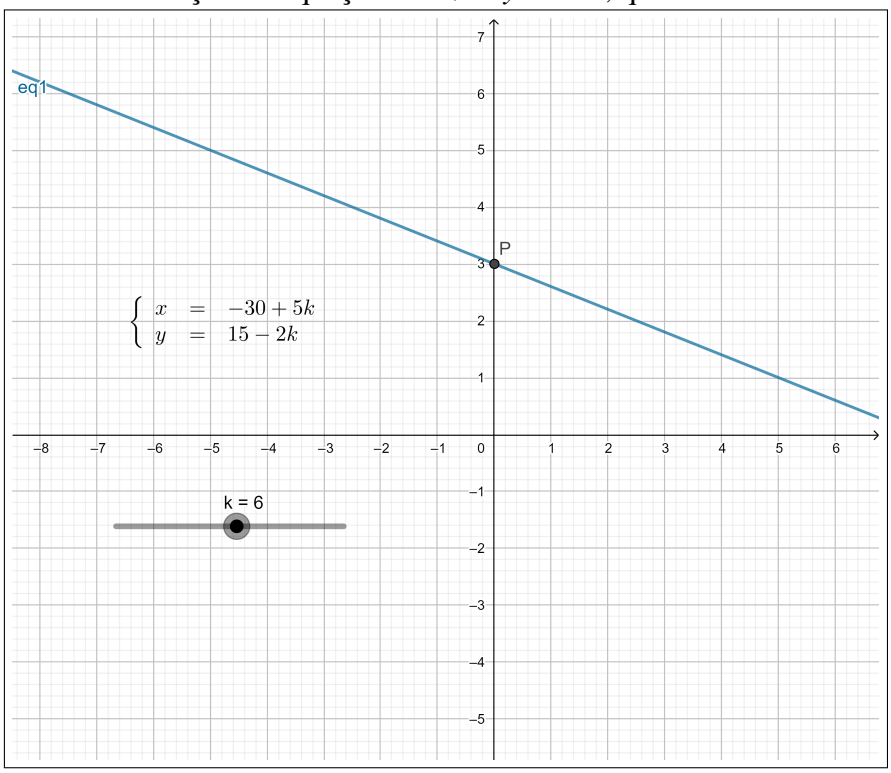
então $k\in\{6,7\}$*. Se* $k=6$ *a solução é* $(0,3)$*, ou seja, 3 cédulas de R$ 50. Se* $k=7$ *a solução é* $(5,1)$*, isto significa, 5 cédulas de R$ 20 e 1 de R$ 50. Logo, só há duas maneiras de sacar o valor mencionado com cédulas de R$ 20 e R$50. Utilizando o Geogebra obtém-se o gráfico em que situa os pares ordenados sobre a reta que é o gráfico da equação no plano cartesiano (figura 4 e figura 5).*

Problema 5.2.1. *(Proposto por Euler) Uma pessoa comprou cavalos e bois. Foram pagos 31 escudos por cavalo e 20 escudos por boi e sabe-se que todos os cavalos custaram 7 escudos a menos do que todos os bois. Quantos cavalos e quantos bois foram comprados?*

Solução: Deve-se antes de qualquer coisa modelar o problema em forma de equação. Seja x o número de bois e y o número de cavalos comprados, temos a seguinte equação

$$20x-31y=7. \tag{5.2}$$

Figura 4 – Gráfico da solução da equação $20x + 50y = 150$, quando $k = 6$.



Fonte: elaborado pelo autor (2020).

Como $(20, -31) = (20, 31) = 1$, logo existem x e y inteiros tais que satisfaçam a equação 5.2. Aplicando o Algoritmo de Euclides, temos que

$$\begin{aligned} 31 &= 20 \cdot 1 + 11 \\ 20 &= 11 \cdot 1 + 9 \\ 11 &= 9 \cdot 1 + 2 \\ 9 &= 2 \cdot 4 + 1 \end{aligned}$$

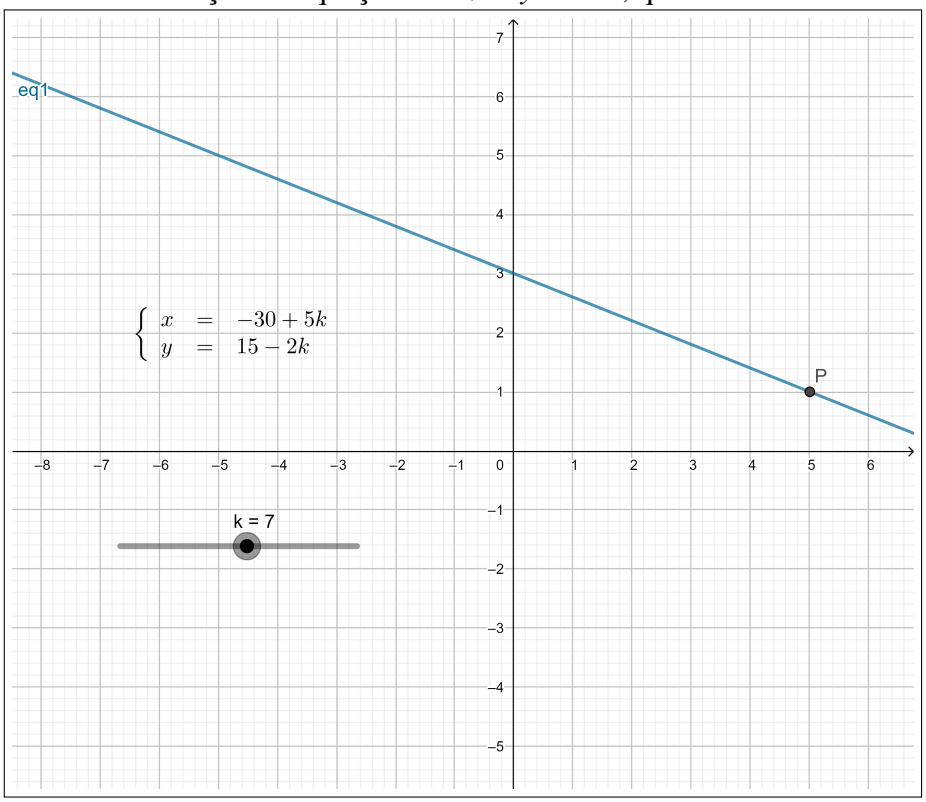
Isolando os restos do algoritmo e fazendo as substituições convenientes, obtemos

$$1 = 9 - 4 \cdot 2 = 9 - 4(11 - 9) = 5 \cdot 9 - 4 \cdot 11 = 5(20 - 9) - 4 \cdot 11 =$$
$$5 \cdot 20 - 9 \cdot 11 = 5 \cdot 20 - 9(31 - 20) = 14 \cdot 20 - 9 \cdot 31 = 20(14) - 31(9) = 1$$

Multiplicando a expressão acima por 7, chega-se a $20(98) - 31(63) = 7$. Como $98 = 31(3) + 5$, obtemos $20(5) - 31(3) = 7$.

Portanto, $x_0 = 5$ e $y_0 = 3$ são solução particular (e minimal) da equação diofantina. A solução geral é dada pelo conjunto de pares ordenados $S = \{(5 + 31k, 3 + 20k) | k \in \mathbb{Z}_+\}$. As soluções possíveis só surgem para $k \geq 0$, assim, podemos listar algumas soluções na tabela a seguir:

Figura 5 – Gráfico da solução da equação $20x+50y=150$, quando $k=7$.



Fonte: elaborado pelo autor (2020).

k	$x=5+31k$	$y=3+20k$
0	5	3
1	36	23
2	67	43
$\vdots$	$\vdots$	$\vdots$
n	$5+31n$	$3+20n$

Problema 5.2.2. *Em um pátio do DETRAN, sabe-se que há 400 pneus retirados de carros e motos que foram apreendidos no mês de Setembro. Quantos veículos de cada categoria foram apreendidos sabendo que a diferença entre os dois números é a menor possível?*

Solução: Seja p o número de carros e q o número de motos presentes neste pátio. Sabemos que cada carro possui quatro pneus e cada moto, dois pneus. Deste modo o problema pode ser representado pela equação

$$4p+2q=400.$$

A equação acima possui solução pois $(4,2)=2$ divide 400. Ela mesma pode ser reescrita como

$$2p+q=200.$$

Esta última também possui soluções pois os coeficientes são co-primos, assim, devemos tomar uma solução particular, de pronto, temos $2(1)+1(-1)=1$. Multiplicando por 200 segue que

$$2(200)+1(-200)=2(50)+1(100).$$

Assim $p_0=50$ e $q_0=100$ são soluções particulares da equação. Com efeito, as soluções são do tipo $p=50+t$ e $q=100-2t$, com $t\in\mathbb{Z}$. A própria natureza do problema impõe a restrição da não negatividade, por isso, $p=50+t>0$ e $q=100-2t>0$, assim, $-50<t<50$. A diferença entre o número de carros e motos é dado por $|p-q|=|(50+t)-(100-2t)|=|3t-50|$, pois $p-q>0$ ou $p-q<0$. Por último, deve-se verificar qual é o menor valor assumido por $|3t-50|$, como t é inteiro não é possível $|3t-50|=0$, por conseguinte, testamos $|3t-50|=1$, ou seja, $3t-50=1$ ou $3t-50=-1$, para o primeiro caso obtemos $t=17$ já no segundo t não é inteiro. Então, temos como solução $p=67$ e $q=66$.

Problema 5.2.3. *Uma certa quantidade de maçãs é dividida em 37 montes de igual número. Após serem retiradas 17 frutas, as restantes são acondicionadas em 79 caixas, cada uma com a mesma quantidade. Quantas maçãs foram colocadas em cada caixa? Quantas maçãs tinha cada monte?*

Solução: Seja m a quantidade de maçãs. A quantidade m foi dividida em 37 montes, ou seja, $m=37x$, com x sendo o número de maçãs em cada monte.

Por outro lado, se forem retiradas do total 17 frutas, o restante pode ser guardadas em 79 caixas, ou seja, $m-17=79y$, sendo y o número de maçãs em cada caixa. Substituindo o valor de m da primeira igualdade na segunda obtemos $37x-79y=17$.

Basta agora calcularmos a solução para esta equação, uma vez que ela admite solução já que $(37,79)=1$. Nesse sentido, temos, pelo Algoritmo de Euclides, que

$$\begin{aligned} 79 &= 37\cdot 2+5 \\ 37 &= 5\cdot 7+2 \\ 5 &= 2\cdot 2+1 \end{aligned}$$

Consequentemente, temos

$$1 = 5-2(2)=5-2(37-5(7))=5(15)-37(2)=(79-37(2))(15)-37(2)$$
$$=(-32)37-(-15)79$$

Multiplicando a igualdade acima por 17 e aplicando a divisão euclidiana, obtemos

$$(-544)37-(-255)79=((-7)79+9)37-(-255)79=(9)37-(4)79.$$

Portanto, a solução minimal $x_0=9$ e $y_0=4$. Assim, a solução geral é dada por $S=\{(9-79t,4-37t)|t\in\mathbb{N}\}$. O único valor possível é $t=0$. De imediato, em cada monte foram colocadas 9 maçãs e em cada caixa, 4 maçãs.

Exemplo 5.2.2. *Um laboratório dispõe de 2 máquinas para examinar amostras de sangue. Uma delas examina 40 amostras de cada vez enquanto a outra examina 28. De quantos modos diferentes essas máquinas podem ser acionadas para examinar 1200 amostras? (Adaptado de Rocque e Pitombeira (1991, p. 39))*

***Solução**: Primeiro equacionamos o problema, Seja x_1 o número de exames feitos pela máquina 1 e x_2 o número de exames feitos pela máquina 2, assim, temos*

$$40x_1+28x_2=1200.$$

Aplicando o algoritmo de Euclides, temos

$$\begin{aligned}40 &= 28\cdot 1+12\\ 28 &= 12\cdot 2+4\\ 12 &= 4\cdot 3+0\end{aligned}$$

Reescrevendo as divisões sucessivas acima, temos

$$\begin{aligned}12 &= 40\cdot 1+28\cdot(-1)\\ 4 &= 28\cdot 1+12\cdot(-2)\\ 4 &= 28\cdot 1+(40\cdot 1+28\cdot(-1))(-2)\\ 4 &= 40\cdot(-2)+28\cdot 3\end{aligned}$$

Multiplicando a última igualdade por 300*, obtemos uma solução particular:*

$$40\cdot(-600)+28\cdot(900)=1200.$$

Assim, temos como solução geral $x_1=-600+7k$ e $x_2=900-10k$, $k\in\mathbb{Z}$, é evidente pela natureza do problema que $x_1\geq 0$ e $x_2\geq 0$, consequentemente, devemos resolver o sistema

$$\begin{cases}x_1 &= -600+7k\geq 0\\ x_2 &= 900-10k\geq 0\end{cases}$$

assim, temos $k \in \{86, 87, 88, 89, 90\}$. *Então, temos como solução os pares (2,40), (9,30), (16,20), (23,10), (30,0).*

O exemplo acima poderia ser implementada acrescentando o custo de cada máquina por exame realizado e daí poderíamos formular um problema de programação linear (minimização/maximização), problemas deste tipo são comuns em situações reais. São frequentes os problemas em economia ou em engenharias em que há a restrição de que as soluções sejam inteiras positivas, a disciplina de Pesquisa Operacional trás muitas questões, das mais variadas áreas, nesse sentido Pommer e Pommer (2013) trás uma vivência de sala de aula que motiva.

> Em outra circunstância, ao lecionar Fundamentos de Matemática em cursos de bacharelado em Ciências Sociais, havia recomendação para a contextualização da disciplina com os temas característicos desta área. Durante a revisão bibliográfica, encontramos inúmeras situações e ilustrações de conceitos básicos presentes na área de Microeconomia que estão em interface com o ensino da Matemática. Mais especificamente, emergiram alguns exemplos que representavam soluções inteiras, implicitamente relacionadas as Equações Diofantinas Lineares. Vale ressaltar que algumas dessas situações referem-se a questões cujo contexto consideramos próximos à realidade do cidadão comum. Pommer e Pommer (2013, p. 168)

Infelizmente, as equações diofantinas são tratadas geralmente em cursos superiores específicos da área de ciências exatas, matemática ou computação, no entanto, necessita de conhecimentos que estão acessíveis a alunos do ensino fundamental ou médio, é evidente que se abordado com a devida sensibilidade se logrará exito.

5.2.2 Equações Diofantinas em três variáveis

Na subseção anterior vimos como resolver equações diofantinas em duas variáveis, agora se faz necessário abordar casos com três variáveis, é salutar que é possível resolver equações diofantinas com três ou mais incógnitas, mas se recorre ao caso com duas variáveis e para isso é necessário um recurso algébrico interessante que nos remete a um caso análogo que é o do Máximo Divisor Comum. É sugerida a leitura de Souza (2017, p. 33).

Dizemos que uma equação diofantina é linear de três variáveis se ela é escrita da forma $ax + by + cz = k$, onde a, b, x, y, z são inteiros, no qual os coeficientes a, b e c não são nulos. Vimos na proposição 5.2.1 que uma equação diofantina linear de duas variáveis $ax + by = c$ possui solução se, se somente se, (a,b) divide c. De forma similar, as equações diofantinas de três variáveis admitem solução se, e somente se, o termo a direita da igualdade é divisível pelo máximo divisor comum dos coeficientes a, b e c. Enunciamos esse resultado na seguinte proposição.

Proposição 5.2.1. *A equação diofantina $ax+by+cz=k$ com a, b, c números inteiros não nulos e k um inteiro qualquer admite solução se, e somente se, $(a,b,c)|k$.*

Demonstração. Seja $(a,b)=d_1$. Logo existem t_1, t_2 inteiros tais que $at_1+bt_2=d_1$. Como $(a,b,c)=(d_1,c)=d$, existem t, z_0 inteiros de modo que $d=d_1t+cz_0$. Logo,

$$d=d_1t+cz_0=(at_1+bt_2)t+cz_0=at_1t+bt_2t+cz_0.$$

Tomando $x_0=t_1t$ e $y_0=t_2t$ temos que

$$ax_0+by_0+cz_0=d.$$

Assim, a equação $ax+by+cz=k$ admite solução, pois, $d|k$, ou seja, $k=dq$, para algum q inteiro. Então,

$$a(x_0q)+b(y_0q)+c(z_0q)=dq=k$$

onde x_0q, y_0q e z_0q são soluções particulares dessa equação. □

Em uma equação do formato $ax+by+cz=k$, podemos considerar $p=ax+by$ e resolver a equação de duas variáveis $p+cz=k$. A partir desta, determinamos a solução geral, ou seja, o valor de z e o valor de p ($p=p_0+ct$ e $z=z_0-t$). Na sequência basta resolvermos $ax+by=p_0+ct$ que obteremos os respectivos valores das incógnitas x e y.

Problema 5.2.4. *Gabriel guarda em um cofre moedas de 5, 10 e 25 centavos. Ele resgatou o valor de R$ 10,00 e foram contadas 50 moedas. Quantas moedas de cada valor estavam no cofre?*

Solução: Note que devemos escrever a quantia expressa em Reais (R$) para centavos, afim de evitarmos o cálculo de máximo divisor comum para número racionais que é abordado em Ripoll *et al.* (2006). Sejam x, y e z as quantidades de moedas de 5, 10 e 25 centavos, respectivamente. Pode-se equacionar o problema com a seguinte equação diofantina

$$5x+10y+25z=1000. \tag{5.3}$$

Como $(5,10,25)=5$ e $5|1000$, então, a equação 5.3 possui solução. Podemos reescrevê-la da seguinte maneira

$$x+2y+5z=200. \tag{5.4}$$

Tomando $p = x + 2y$, temos

$$p + 5z = 200.$$

Pelo Teorema 5.2.1 a equação acima admite solução, pois $(1,5) = 1$ divide 200. Sendo $p_0 = 20$ e $z_0 = 36$ uma solução particular. Logo, as soluções inteiras são da forma $p = 20 - 5t$ e $z = 36 + t$, com $t \in \mathbb{Z}$.

Como visto anteriormente, $x + 2y = p = 20 - 5t$. Desta forma, devemos encontrar as soluções inteiras da equação

$$x + 2y = 20 - 5t \tag{5.5}$$

Para que a equação acima admita soluções inteiras, 1 deve dividir $20 - 5t$. Note que é imediato verificar que $1|(20 - 5t)$ para todo t inteiro. Logo, existem x e y inteiros tais que

$$x + 2y = 1, \tag{5.6}$$

na qual podemos tomar como solução particular $x_0 = -1$ e $y_0 = 1$.

Multiplicando a equação 5.6 por $20 - 5t$, obtem-se

$$1(5t - 20) + 2(20 - 5t) = 20 - 5t \tag{5.7}$$

Desta última obtém-se $x = -20 + 5t + 2t_1$, $y = 20 - 5t - t_1$ e $z = 36 + t$.

O problema nos impõe outra condição que deve ser equacionada, deixamos por último por conveniência do método utilizado. A soma dos números de moedas é 50, isto é, $x + y + z = 50$. Com isso, temos

$$\begin{aligned} (-20 + 5t + 2t_1) + (20 - 5t - t_1) + (36 + t) &= 36 + t + t_1 = 50 \\ &\Rightarrow \quad t + t_1 = 14 \end{aligned}$$

Substituindo $t_1 = 14 - t$, temos

$$\begin{cases} x &= 8 + 3t \geq 0 \\ y &= 6 - 4t \geq 0 \\ z &= 36 + t \geq 0 \end{cases}$$

Como o problema só admite soluções inteiras positivas devemos ter $t = 0$ ou $t = 1$. Por inspeção, conclui-se que $t = 1$, assim,a solução é $x = 11$, $y = 2$ e $z = 37$. Então, no cofre tinha 11 moedas de 5 centavos, 2 moedas de 10 centavos e 37 moedas de 25 centavos.

5.2.3 Equações Diofantinas de n variáveis

Uma equação diofantina de n variáveis é uma equação da forma

$$a_1x_1 + a_2x_2 + a_3x_3 + ... + a_nx_n = k \tag{5.8}$$

com $a_i \in \mathbb{Z}$ e $a_i \neq 0$ para $i = 1,2,3,\ldots,n$. Aplicando os mesmos recursos algébricos que foram utilizados para resolução as equações diofantinas de com variáveis, também deve-se atentar para a condição de existência de solução para a equação 5.8.

Proposição 5.2.2. *A equação diofantina $a_1x_1 + a_2x_2 + ... + a_nx_n = k$, $a_i \in \mathbb{Z}$, $a_i \neq 0$ para $\forall i = 1,2,\ldots,n$, com $k \in \mathbb{Z}$ admite solução se, e somente se, $(a_1,a_2,...,a_n)|k$.*

Demonstração. Pelo Teorema 4.6.1, vimos que existem $x_1,x_2,\ldots,x_n$ inteiros tais que

$$C(a_1,a_2,\ldots,a_n) = \sum_{i=1}^{n} a_ix_i = (a_1,a_2,\ldots,a_n).$$

Portanto, é evidente que a equação acima tem solução se, e somente se, $k \in C(a_1,a_2,\ldots,a_n)$ que implica em $(a_1,a_2,\ldots,a_n)|k$. □

Exemplo 5.2.3. *Determinar a solução geral em $\mathbb{Z}$ da equação diofantina $3x+6y-10z+2w = 50$.*

Solução: Reduziremos a equação inicial em uma outra com duas variáveis, tomando $k^{(1)} = 3x+6y-10z$, temos $k_1 + 2w = 50$. Note que $(1,2) = 1$, assim, a equação $k^{(1)} + 2w = 1$ possui solução em inteiros, tomando como solução particular $k_0^{(1)} = 3$ e $w_0 = -1$. Multiplicando por 50, temos

$$\begin{cases} k^{(1)} = 150 - 2t_0 \\ w = -50 + t_0 \end{cases}$$

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

Refazendo o mesmo processo algébrico do qual obtemos $k^{(1)}$ e z, escrevemos $k^{(2)} = 3x+6y$, então

$$k^{(2)} - 10z = k^{(1)} = 150 - 2t_0.$$

A equação acima possui solução, pois o máximo divisor comum dos coeficientes da equação divide $150-2t_0$ para todo $t_0 \in \mathbb{Z}$. De fato, existe uma combinação linear na qual determinamos

uma solução particular.

$$150 - 2t_0 = 1(-10 + 8t_0) - 10(-16 + t_o).$$

Então, $k^{(2)} = -10 + 8t_0 - 10t_1$ e $z = -16 + t_0 - t_1$, com $t_0, t_1 \in \mathbb{Z}$.

Por consequência, chegou-se a

$$3x + 6y = -10 + 8t_0 - 10t_1. \tag{5.9}$$

Para que haja solução devemos ter $3|(-10 + 8t_0 - 10t_1) \Leftrightarrow 3|(-1 + 2t_0 - t_1)$, logo existe p inteiro tal que $-1 + 2t_0 - t_1 = 3p$. Na equação 5.9 o máximo divisor comum dos coeficientes é igual a 3, dividindo ambos os membros da equação diofantinas por 3, chega-se a

$$x + 2y = -3 + 2t_0 - 3t_1 + p.$$

Como $x_0 = 3 - 2t_0 + 3t_1 - p$ e $y_0 = -3 + 2t_0 - 3t_1 + p$. Então,

$$\begin{cases} x = 3 - 2t_0 + 3t_1 - p + 2q \\ y = -3 + 2t_0 - 3t_1 - q. \end{cases}$$

Logo a solução geral em $\mathbb{Z}$ é dada pelo conjunto $S = \{(3 - 2t_0 + 3t_1 - p + 2q, -3 + 2t_0 - 3t_1 - q, -16 + t_0 - t_1, -50 + t_0) | t_0, t_1, p, q \in \mathbb{Z}\}$. Pode-se obter soluções ao atribuirmos valores para t_0 e t_1, respeitando a condição $3|(-1 + 2t_0 - t_1)$, feito isso, devemos equacionar um sistema de equações para determinar os valores de p e q.

6 METODOLOGIA

6.1 Caracterização da Escola

Foi elaborada uma sequência didática para ser trabalhada com duas turmas regulares no turno matutino do 2º ano do ensino médio na Escola Estadual Coronel Solon, na qual sou professor responsável de cinco turmas do ensino médio, a escola está situada no município de Grossos-RN, na zona urbana. Grossos, é um município litorâneo situado na microrregião oeste do estado do Rio Grande do Norte. Segundo, o Instituto Brasileiro de Geografia e Estatística (IBGE) no censo de 2017 a população do município era de 10.386 habitantes. A economia do município é baseada na extração e industrialização do sal marinho, assim, como os municípios de Areia Branca, Macau, Tibau e Icapuí, este último situado no estado do Ceará, faz parte da *costa branca*. A Escola Estadual Coronel Solon é a única instituição no município que oferta o ensino médio desde 04/04/1994, por meio do decreto estadual 12.105/94 a "Escola Estadual Coronel Solon, Ensino de 1º Grau"foi transformada em "Escola Estadual Coronel Solon, Ensino de 1º e 2º Graus", conforme a Lei 5.692/71 da LDB. Sobre a criação se sabe que ocorreu em meados dos anos 1950, outrora, denominado Grupo Escolar era responsável pela educação primária de filhos de salineiros, pescadores e de agricultores que migraram de outras cidades do interior do estado para trabalharem nas salinas da região. Segundo, o INEP (Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira) a nota do IDEB (Índice de Desenvolvimento da Educação Básica) do ano 2015 desta instituição foi de 2,8, porém, a projeção era de 4,0, no entanto, devido à baixa participação do corpo discente nesta avaliação externa não houve divulgação oficial pela autarquia responsável (ver anexo B).

6.2 Sequência didática para o uso da decomposição em fatores primos para a obtenção do Máximo Divisor Comum e Mínimo Múltiplo Comum

A ideia consiste em aplicar as aulas em duas turmas do 2º ano do Ensino Médio que são compostas por cerca de 30 alunos cada. A sequência didática foi elaborada de modo a simplificar a aplicação em sala de aula, contudo, deve-se enfatizar no desenvolvimento de habilidades básicas tais como divisibilidade, máximo múltiplo comum e mínimo múltiplo comum que se relacionam diretamente ao tema proposto. Nas primeiras aulas serão relembrados os algoritmos para obtenção do máximo divisor comum e mínimo múltiplo comum, alguns exercícios serão

resolvidos em sala de aula e outros propostos, estes primeiros serão abordados de uma maneira algorítmica, da mesma forma que geralmente é abordada no ensino fundamental, no decorrer das aulas exploratórias é recomendado que o professor insira problemas que exigem contextualização com situações cotidianas, afim de tornar o tema algo mais palpável na perspectiva pedagógica. A proposta de resolução de problemas em matemática contextualizados com situações cotidianas é um dos grandes desafios no geral para a maioria dos alunos e dos professores.

Os materiais que serão utilizados nas aulas: lousa, pincel para lousa, notebook, projetor, Geogebra, planilhas eletrônicas.

No primeiro momento deve-se realizar uma avaliação diagnóstica quanto ao domínio de alguns conteúdos que serão explorados no decorrer das aulas sobre equações diofantinas lineares. A avaliação diagnóstica deve ser composta com exercícios sobre Algoritmo da divisão, decomposição em fatores primos (Ver *Teorema Fundamental da Aritmética*), máximo divisor comum e mínimo múltiplo comum. Diante da análise feita pelo professor sobre a situação da turma, deve-se escolher em fazer uma breve revisão com a resolução de exercícios da própria avaliação diagnóstica ou na continuação da sequência didática com a próxima parte dos conteúdos auxiliares. O tempo estimado para a Avaliação Diagnóstica será de 4 aulas de 50 minutos, ver Apêndice A.

6.3 Sequência didática para resolução de Equações Diofantinas Lineares

A proposta do ensino de equações diofantinas lineares está intimamente ligada a um processo de discretização do estudo de sistemas lineares, portanto, é mister estimular a *priori* nos discentes formas alternativas de soluções, o método das tentativas e erros deve ser estimulada, se for oportuno pode-se mostrar o *Método da falsa posição* e sua aplicabilidade na resolução de equações de 1º grau. A motivação utilizada para introduzir este tema pouco explorado no ensino médio se dá pelo pouco espaço que a matemática discreta assume no ensino de matemática na educação básica.

Ao prosseguir com a transposição didática serão apresentadas a definição de equação linear em duas incógnitas e o método de resolução por tentativa e erro, aquele em que se atribui um valor para uma incógnita e se equaciona para obter a outra. Posto isto, é oportuno discorrer sobre a quantidade infinita de soluções reais e conjecturar sobre a infinitude das soluções inteiras e inteiras não negativas.

Antes de resolver equações diofantinas lineares faz-se necessário uma sondagem

sobre resolução de inequações de 1º grau com uma incógnita, caso necessário, será feita uma revisão com resolução de exercícios direcionados. Esta última habilidade é importante quando se tem que resolver equações diofantinas lineares com valores inteiros positivos.

É importante solicitar a fixação de alguns conceitos teóricos para dar suporte na estratégia de resolução das equações diofantinas lineares, dentre eles é o domínio do algoritmo de Euclides e do teorema de Bezout. A lista de atividades dirigidas para a resolução de equações diofantinas encontra-se no Apêndice B. O tempo destinado para a transposição didática será flexibilizada em função da necessidade de tempo para o domínio dos conteúdos específicos, estimou-se em aproximadamente 8 aulas de 50 minutos.

A depender dos resultados obtidos com o ensino de equações diofantinas lineares pode-se prosseguir com a resolução de alguns tipos de equações diofantinas não lineares, o que demandará mais tempo e conhecimentos teóricos que estão contidos no Capítulo 4. A inserção de meios computacionais para auxiliar na resolução dos problemas é algo que deve ser incentivado e orientado pelo docente.

6.4 Opinião de professores de matemática sobre a inserção do tema no Ensino Médio

Foi realizado um questionário eletrônico com questões de opinião acerca da inserção do tópico *equações diofantinas lineares* no ensino médio e questões para identificação do perfil docente (sexo, faixa etária, tempo de magistério e formação acadêmica).

7 RESULTADOS

Devido à suspensão das aulas presenciais na rede estadual de educação no estado do Rio Grande do Norte não se deu a aplicação em sala com os alunos. Havia a possibilidade de ser aplicada em modo não presencial, no entanto, constatou-se pouca participação dos discentes nas aulas remotas o que

7.1 Resultados do questionário

Quanto ao questionário, ele foi aplicado em 23 professores de matemática por meio de formulário eletrônico feito no *Formulários Google* e enviado para eles através de mensagem pelo *whatsapp*. As primeiras perguntas foram para traçar um perfil dos professores entrevistados. Ver o resultado do questionário no Apêndice C.

Observado o resultado do questionário, a maioria, 18 entre os 23 entrevistados concordam em inserir o tema no ensino médio. A maioria dos professores tem domínio sobre o objeto de estudo. Isto corrobora com a ideia do presente trabalho, visto que se embasa em conhecimento adquiridos no ensino fundamental, no entanto, é observada certa deficiência nestes conteúdos que remetem à teoria dos números devido à natureza abstrata. É válido citar um trecho das Orientações Curriculares para o Ensino Médio

> A contextualização não pode ser feita de maneira ingênua, visto que ela será fundamental para as aprendizagens a serem realizadas – o professor precisa antecipar os conteúdos que são objetos de aprendizagem. Em outras palavras, a contextualização aparece não como uma forma de "ilustrar" o enunciado de um problema, mas como uma maneira de dar sentido ao conhecimento matemático na escola. BRASIL (2006, p. 83)

A Matemática é uma disciplina que exige abstrações do aluno, pois exige concentração e disciplina para seu aprendizado, no entanto, não podemos dissociar o ensino-aprendizagem da Matemática aos conhecimentos de mundo do indivíduo, dando relevância às suas percepções e experiências do seu cotidiano. Neste sentido as Orientações Curriculares para o Ensino Médio ainda recomenda:

> Para isso, a escola deve buscar novas formas de se organizar, considerando que os conteúdos disciplinares não se esgotam em si mesmos, mas significam o acesso ao saber cultural e à aquisição de ferramentas para o entendimento da sociedade em que vivemos, destacando-se as que capacitam os indivíduos para viverem em um mundo tecnológico e informatizado. Nesse sentido, pode ser interessante propiciar momentos de trabalho em duplas e em pequenos grupos, que possibilitam a participação ativa dos alunos, o confronto de ideias e a adoção de consensos. (BRASIL, 2006, p. 91)

Neste sentido os Parâmetros Curriculares Nacionais (PCNs) recomendam que haja incitação ao desenvolvimento do pensamento algébrico.

> o estudo da Álgebra constitui um espaço bastante significativo para que o aluno desenvolva e exercite sua capacidade de abstração e generalização, além de lhe possibilitar a aquisição de uma poderosa ferramenta para resolver problemas. (BRASIL, 1998, p. 117)

8 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

O presente trabalho objetivou uma proposta de fortalecimento dos estudos em teoria elementar dos números a nível de ensino fundamental e médio, também inserindo novo conceitos. Toda fundamentação teórica se mostrou direcionada ao tema equações diofantinas. As atividades propostas nas sequências didáticas justificaram a necessidade do embasamento teórico diante dos problemas aplicados. Portanto, uma ponderação entre o abstrato e o palpável se mostram uma proposta coerente. Ainda neste delinear, faz-se mister a abordagem e contextualização histórica de tópicos em Teoria dos Números. Deve-se dar ênfase às aplicações das equações diofantinas lineares com duas variáveis, no entanto pode-se dar continuidade com aplicações de equações diofantinas lineares com três variáveis e a resolução por meio de fatoração e desigualdades. Há a ideia para que o material produzido neste trabalho seja aproveitado como material de preparação para as Olimpíadas de Matemática em relação aos conteúdos de teoria dos números. Para o aprimoramento e adaptações deste texto, sugere-se a leitura de algumas obras citadas nas Referências Bibliografia, tais como Hefez (2006), Hefez (2013), Moreira *et al.* (2011),Dutenhefner e Cadar (2017), Fomin *et al.* (2010), Neto (2012), Santos (2006) e Ripoll *et al.* (2006)(artigo).

REFERÊNCIAS

BORGES, F. V. de A. **Equações Diofantinas Lineares em Duas Incógnitas e Suas Aplicações**. 63 p. Dissertação (Mestrado) — Universidade Federal de Goiás, Goiânia, abril 2013. Disponível em: <https://repositorio.bc.ufg.br/tede/bitstream/tede/3124/5/Borges%2c%20F%c3%a1bio%20Vieira%20de%20Andrade.pdf>. Acesso em: 02 out. 2019.

BOYER, C. B. **História da Matemática**. 1ª ed.. ed. São Paulo: Edgard Blucher, 1974.

BRASIL. **Parâmetros Curriculares Nacionais: Matemática**. Brasília, 1998.

BRASIL. **Parâmetros Curriculares Nacionais (PCNs) - Ensino Médio**. Brasília, 1999.

BRASIL. **Orientações Curriculares Para o Ensino Médio; volume 2 – Ciências da Natureza, Matemática e suas Tecnologias**. Brasília, 2006. 135 p.

BRASIL. **Base Nacional Comum Curricular - BNCC**. Brasília, 2018. 595 p. Disponível em: <http://basenacionalcomum.mec.gov.br/images/BNCC_EI_EF_110518_versaofinal_site.pdf>. Acesso em: 02 fev. 2020.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. 2ª ed.. ed. Rio de Janeiro: IMPA, 2005. 226 p.

DUTENHEFNER, F.; CADAR, L. **Encontros de Aritmética**. Rio de Janeiro: IMPA, 2017. 121 p.

EVES, H. **Introdução à história da matemática**. Campinas: Editora da UNICAMP, 2004.

FOMIN, D.; GENKIN, S.; ITENBERG, I. **Círculos Matemáticos: A Experiência Russa**. Rio de Janeiro: IMPA, 2010. 292 p.

HEFEZ, A. **Elementos de aritmética**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2006.

HEFEZ, A. **Indução matemática**. Rio de Janeiro: IMPA, 2009.

HEFEZ, A. **Aritmética I**. Rio de Janeiro: SBM, 2013.

HEFEZ, A. **Iniciação a Aritmética**. 1ª. ed. Rio de Janeiro: IMPA, 2015.

LIMA, E. L. **Números e Funções Reais**. 1ª. ed. Rio de Janeiro: IMPA, 2013. 297 p. ISBN 978-85-85818-81-4.

LIMA, R. V. **Equações Diofantinas**. São João Del-Rei: [s.n.], 2017. 54 p. Disponível em: <https://www.ufsj.edu.br/portal2-repositorio/File/comat/tcc_Ricardo.pdf>. Acesso em: 15 dez. 2019.

MARTOS, S. P. **A prova dos noves e estimativas de erros**. 57 p. Dissertação (Mestrado) — Universidade Estadual de Maringá, Centro de Ciências Exatas, Departamento Matemática. Programa de Mestrado Profissional em Matemática, Maringá-PR, Abril 2018. Disponível em: <http://repositorio.uem.br:8080/jspui/bitstream/1/5539/1/000228657.pdf>. Acesso em: 13 dez. 2019.

MOREIRA, C. G. T. de A.; MARTINEZ, F. E. B.; SALDANHA, N. C.; TENGAN, E. Introdução à teoria dos números: Funções aritméticas. **II Coloquio da Região Sul**, Londrina, 2011.

NETO, A. C. M. **Tópicos de Matemática Elementar, vol. 5: Teoria dos Números (Coleção do professor de matemática)**. Rio de Janeiro: SBM, 2012. 263 p.

POMMER, W. M.; POMMER, C. P. C. R. Equações diofantinas lineares no ensino médio: um tema mobilizador de estratégias aritméticas & algébricas. **Cadernos da Pedagogia**, São Carlos, v. 6, p. 166–184, 2013. ISSN 1982-4440.

RIBEIRO, R. **Equações Diofantinas: uma abordagem para o Ensino Médio**. 43 p. Dissertação (Mestrado) — Universidade de Brasília, Instituto de Ciências Exatas, Departamento de Matemática, Programa de Mestrado Profissional em Matemática em Rede Nacional, Brasília, junho 2014. Disponível em: <https://repositorio.unb.br/bitstream/10482/17328/1/2014_RildoRibeiro.pdf>. Acesso em: 05 out. 2019.

RIPOLL, C. C.; RIPOLL, J. B.; SANT'ANA, A. A. O mínimo múltiplo comum e o máximo divisor comum generalizados. **Revista Matemática Universitária**, Sociedade Brasileira de Matemática, Rio de Janeiro, v. 40, p. 59–74, 2006.

ROCQUE, G. de L.; PITOMBEIRA, J. B. Uma equação diofantina e suas resoluções. **Revista do Professor de Matemática**, SBM, Rio de Janeiro, v. 19, 1991. Disponível em: <http://rpm.org.br/cdrpm/19/9.htm>. Acesso em: 18 dez. 2019.

ROQUE, T. **História da matemática: Uma visão crítica, desfazendo mitos e lendas**. 1ª. ed. Rio de Janeiro: Editora Zahar, 2012.

ROQUE, T.; CARVALHO, J. B. P. **Tópicos de História da Matemática**. 2ª ed.. ed. Rio de Janeiro: SBM, 2012. 467 p.

SANTOS, J. P. O. **Introdução à Teoria dos Números**. 3ª. ed. Rio de Janeiro: IMPA, 2006. 198 p. ISBN 85-244-0142-7.

SAVóIS, J. N.; FREITAS, D. Método para resolver equações diofantinas com coeficientes no conjunto dos números racionais. **Ciência e Natura - Ed. Especial PROFMAT**, Revista do Centro de Ciências Naturais e Exatas - UFSM, Santa Maria-RS, v. 37, p. 47–57, 2015.

SINGH, S. **O Último Teorema de Fermat: a história do enigma que confundiu as mais brilhantes mentes do mundo durante 358 anos**. 3ª. ed. Rio de Janeiro: BestBolso, 2018.

SOUZA, R. S. de. **Equações Diofantinas Lineares, Quadráticas e Aplicações**. 75 p. Dissertação (Mestrado) — Universidade Estadual Paulista Júlio de Mesquita Filho, Instituto de Geociências e Ciências Exatas, Rio Claro - SP, Março 2017. Disponível em: <https://igce.rc.unesp.br/Home/Pos-Graduacao44/programasdepos/souza_rs_me_rcla.pdf>. Acesso em: 13 nov. 2019.

VANSAN, A. H. Equações diofantinas: um projeto para a sala de aula e o uso do geogebra. **Ciência e Natura - Ed. Especial PROFMAT**, Revista do Centro de Ciências Naturais e Exatas - UFSM, Santa Maria, v. 37, p. 532–554, 2015. ISSN 0100-8307.

APÊNDICE A – AVALIAÇÃO DIAGNÓSTICA

Governo do Estado do Rio Grande do Norte
Secretaria da Educação, da Cultura, do Esporte e do Lazer - SEEC
12ª Diretoria Regional de Educação e Cultura - 12ª DIREC
Escola Estadual Coronel Solon. Ensino Fundamental e Médio.
Rua Manoel Firmino, 127 - Centro - Grossos/RN, CEP: 59.675-000. Telefone: (84) 3327 3561
Nome do discente: _____
SÉRIE/ANO: _____ CURSO:_____ TURNO: _____ TURMA: _____
Data: ___ de _____ de 20___
PROFESSOR: PATRÍCIO J. DE SOUZA

Avaliação diagnóstica

1. Aplicando o *algoritmo da divisão* determine o quociente q e o resto r das divisões de a por b:

(a) $a = 12$ e $b = 3$
(b) $a = 26$ e $b = 5$
(c) $a = 108$ e $b = 7$
(d) $a = 224$ e $b = 13$
(e) $a = 2450$ e $b = 23$
(f) $a = -400$ e $b = 360$
(g) $a = -100$ e $b = 7$
(h) $a = -125$ e $b = -5$
(i) $a = 241$ e $b = -17$

2. Faça a decomposição em *fatores primos* dos seguintes números naturais:

(a) 24
(b) 72
(c) 27
(d) 224
(e) 1735
(f) 400
(g) 225
(h) 13005
(i) 999333

3. Determine a quantidade de divisores naturais de cada número inteiro positivo abaixo:

(a) 12
(b) 28
(c) 36
(d) 81
(e) 144
(f) 386

4. (Extraído do Caderno de Exercícios - Conjuntos e Quantidades de Divisores no Portal da Matemática) Uma professora leva para a sala de aula uma caixa com 24 bombons. Ela quer distribuir estes bombons de maneira que cada aluno receba a mesma quantidade de bombons e também que não sobre nem um bombom com ela. Quantas são as possíveis quantidades de alunos em sala para que isso aconteça?

5. Calcule o *Máximo Divisor Comum* aplicando dois métodos: pela decomposição em fatores primos e pelo Algoritmo de Euclides. (Notação: $(a,b) = \text{MDC}(a,b)$.)

(a) $(12,9)$
(b) $(24,40)$
(c) $(28,42,147)$
(d) $(54,128,36)$
(e) $(36,108,216)$
(f) $(171,855,882)$

6. Calcule o *Mínimo Múltiplo Comum* aplicando dois métodos: pela decomposição em fatores primos ou pela relação $a \cdot b = (a,b) \cdot [a,b]$. (Notação: $(a,b) = \text{MDC}(a,b)$ e $[a,b] = \text{MMC}(a,b)$.)

(a) $[12,9]$

(b) $[24,40]$

(c) $[15,36,54]$

(d) $[40,28,20]$

(e) $[36,108,216]$

(f) $[54,16,82]$

7. (Extraído do Colégio Militar de Fortaleza - 2014) Da rodoviaria da cidade de Alegrelândia, saem ônibus de 75 em 75 minutos para a cidade de Vila Feliz e de 2 em 2 horas com destino a cidade de Boa Esperança. Em um determinado dia, às 8 horas da manhã, dois ônibus saem juntos, um para cada cidade. Qual e a diferença entre o numero de viagens realizadas para Vila Feliz e para Boa ´ Esperança ate o próximo horário em que dois ônibus sairão juntos novamente da rodoviária de Alegrelândia, um para cada cidade?

(a) 3

(b) 5

(c) 6

(d) 8

(e) 9

8. Uma parede retangular de 480 cm de comprimento por 300 cm de altura deve ser coberta com azulejos quadrados. Deseja-se utilizar a menor quantidade possível de azulejos, qual deve ser a medida inteira, em centímetros, do seu lado? (Deve ser desprezada a espessura do rejunte)

9. Numa corrida de fórmula 1 se verificou que os tempos médios de uma volta de três pilotos foram: piloto A, 72 segundos; piloto B, 80 segundos; piloto C, 70 segundos. Se todos largaram no inicio da primeira volta juntos, depois de quantas voltas completas eles irão cruzar novamente a linha de chegada juntos?

10. Resolva as operações com frações abaixo:

(a) $\dfrac{2}{5}+\dfrac{1}{3}$

(b) $\dfrac{4}{3}-\dfrac{2}{7}+\dfrac{1}{5}$

(c) $\dfrac{4}{5}+\dfrac{4}{3}\cdot\dfrac{9}{7}$

(d) $2+\left(\dfrac{2}{3}\right)^2-\dfrac{7}{3}$

(e) $1-\left(\dfrac{2}{5}-\dfrac{1}{3}\right)^2$

APÊNDICE B – LISTA DE EXERCÍCIOS DIRIGIDOS PARA RESOLUÇÃO DE EQUAÇÕES DIOFANTINAS LINEARES

Governo do Estado do Rio Grande do Norte
Secretaria da Educação, da Cultura, do Esporte e do Lazer - SEEC
12ª Diretoria Regional de Educação e Cultura - 12ª DIREC
Escola Estadual Coronel Solon. Ensino Fundamental e Médio.
Rua Manoel Firmino, 127 - Centro - Grossos/RN, CEP: 59.675-000. Telefone: (84) 3327 3561
Nome do discente: _____
SÉRIE/ANO: ____ CURSO:_____ TURNO: _____ TURMA: _____
Data: ___ de _____ de 20___
PROFESSOR: PATRÍCIO J. DE SOUZA

Lista de Exercícios Dirigidos para resolução de equações diofantinas lineares

1. Determine uma solução em números inteiros para cada equação linear a seguir:

(a) $2x+3y=5$
(b) $-x+5y=6$
(c) $4x-3y-5=0$
(d) $2x+8y=3$
(e) $7x+56y=-28$
(f) $x+y+z=5$
(g) $10x-7y+2z=0$
(h) $\frac{2}{3}x-\frac{5}{4}y=0$
(i) $\frac{1}{4}x+\frac{7}{3}y=1$

2. Dadas as equações lineares esboce o gráfico com todas as soluções em $\mathbb{Z}_+$:

(a) $x+2y=7$
(b) $4x+7y=28$
(c) $3x+12y=24$
(d) $5x+10y=11$
(e) $x+y+2z=3$
(f) $3x+y+z=5$

3. Resolva as inequações do 1º grau em $\mathbb{R}$:

(a) $2x+3<7$
(b) $3x-7>5$
(c) $3-2x\leq 7$
(d) $8-2t\geq 1$
(e) $1+4t<5$
(f) $10-8t\geq -6$

4. Resolva os sistemas de inequações do 1º grau em $\mathbb{Z}$:

(a) $\begin{cases} 2x+3 & < & 15 \\ 3x-7 & > & 5 \end{cases}$
(b) $\begin{cases} 3x-7 & < & 5 \\ 3-2x & \leq & 7 \end{cases}$
(c) $\begin{cases} 8-2t & \geq & 1 \\ 1+4t & > & 5 \end{cases}$
(d) $\begin{cases} 10-8t & \geq & -6 \\ t & \geq & -1 \end{cases}$

5. Determine uma solução particular das equações diofantinas a seguir aplicando o Teorema de Euclides Estendido:

(a) $15X+36Y=18$
(b) $90X+28y=22$
(c) $40X+65Y=50$
(d) $24x+18y=6$
(e) $7x-56y=28$
(f) $35X-15Y=75$

6. Resolva em $\mathbb{Z}$ as equações:

(a) $28X + 22Y = 32$

(b) $40X + 65Y = 135$

(c) $8X + 13Y = 23$

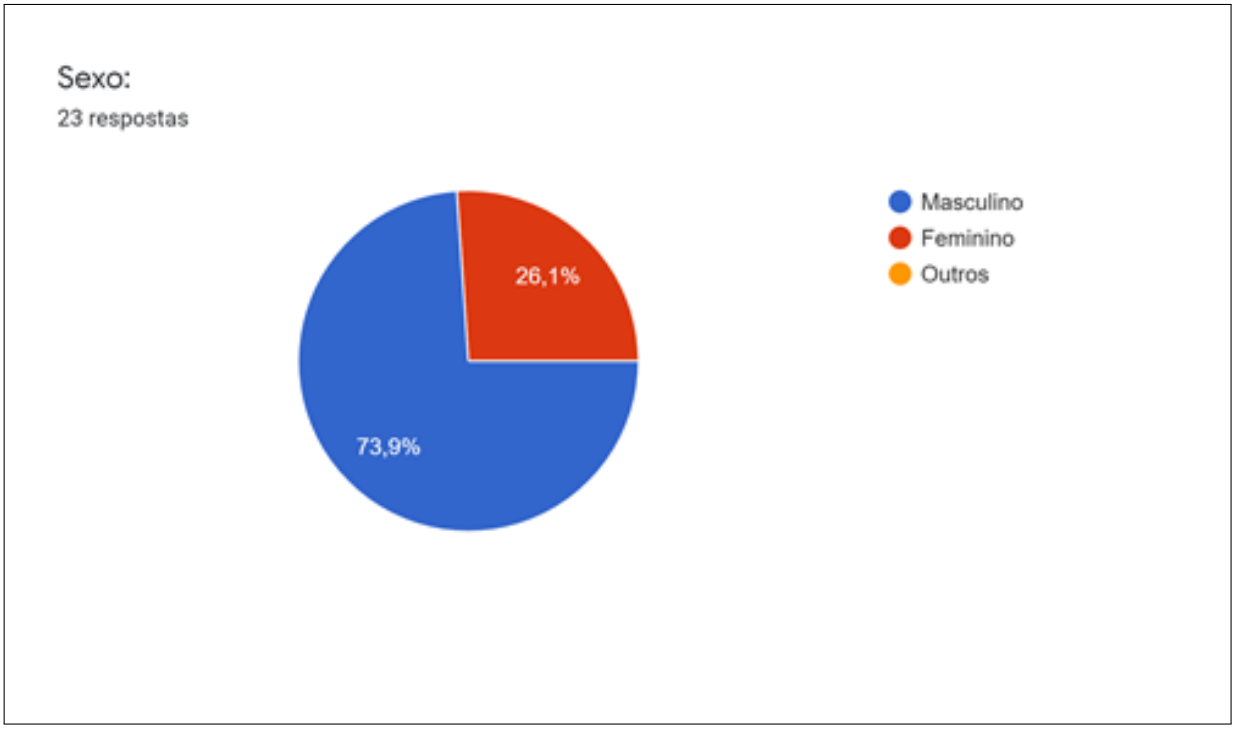
(d) $51X - 36Y = -9$

7. José sacou R$ 100 em um caixa eletrônica que dispunha de cédulas de 10 e 20 reais. Considerando que as quantidades de cédulas dos dois valores seja maior do que 10, de quantas maneiras José poderá receber o seu valor solicitado? (Encontre as soluções graficamente e por meio da resolução de equações diofantinas lineares)

8. Numa criação de coelhos e galinhas, contaram-se 400 pés. Quantas são as galinhas e quantos são os coelhos, sabendo que a diferença entre esses dois números é a menor possível?

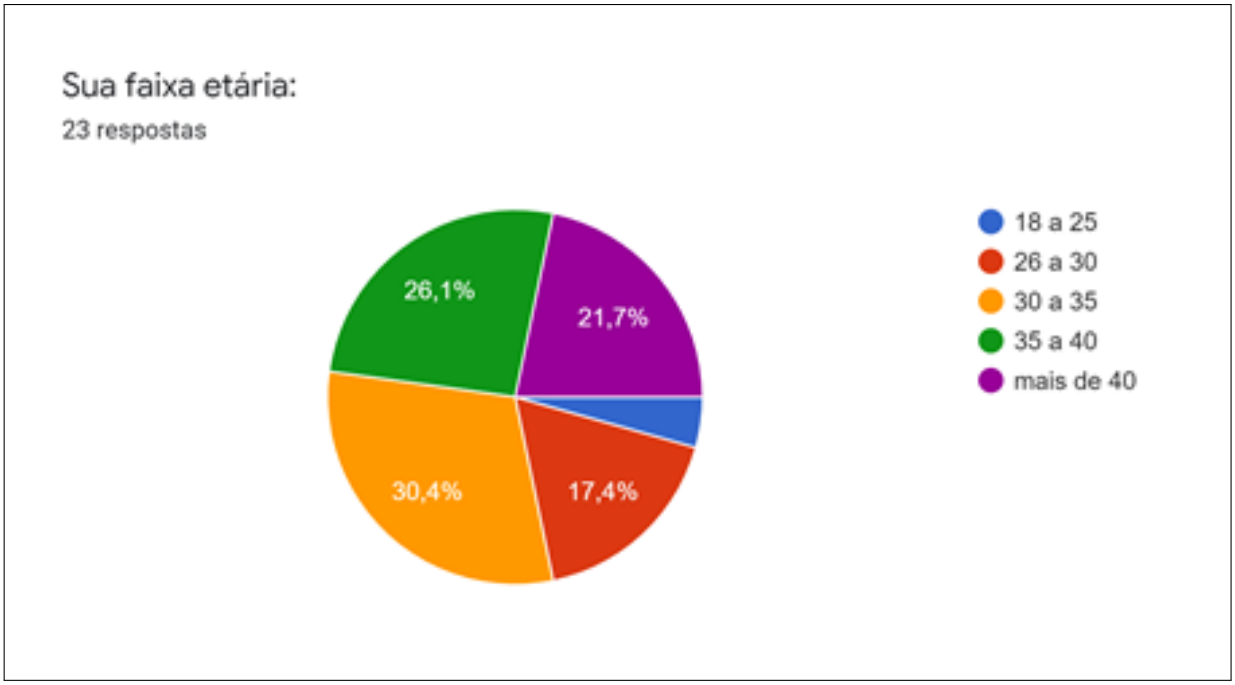
APÊNDICE C – QUESTIONÁRIO APLICADO AOS PROFESSORES

Figura 6 – Gráfico indicando o sexo dos entrevistados, 17 do sexo masculino e 6 do sexo feminino.



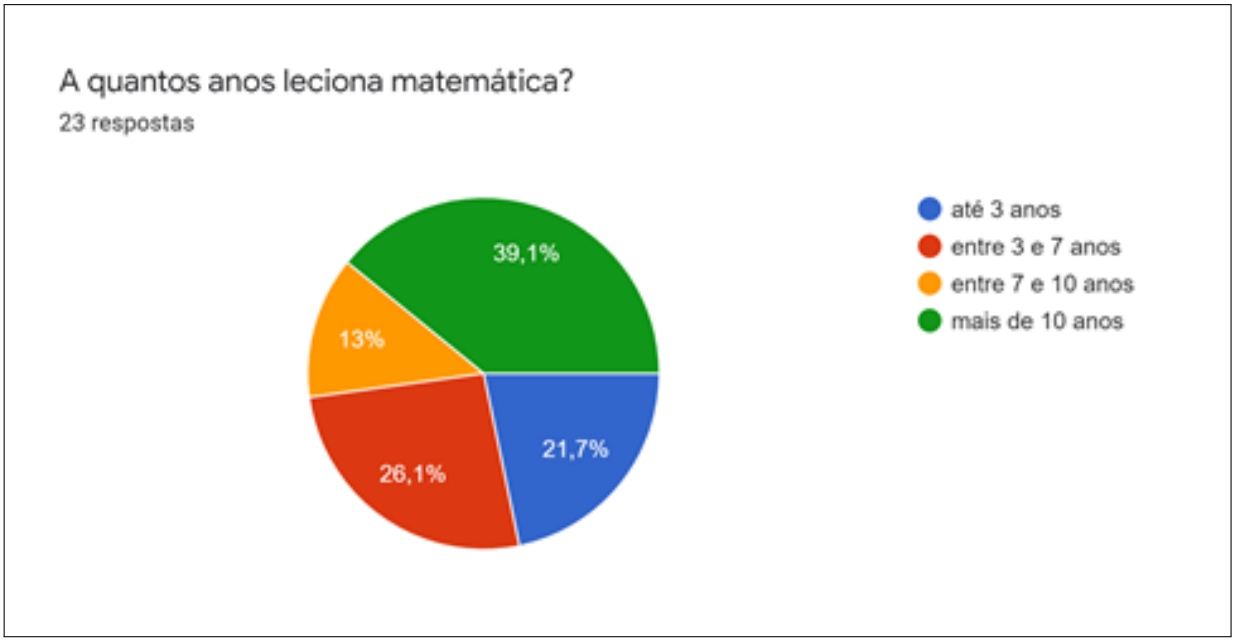
Fonte: elaborado pelo autor (2020).

Figura 7 – Faixa etária.



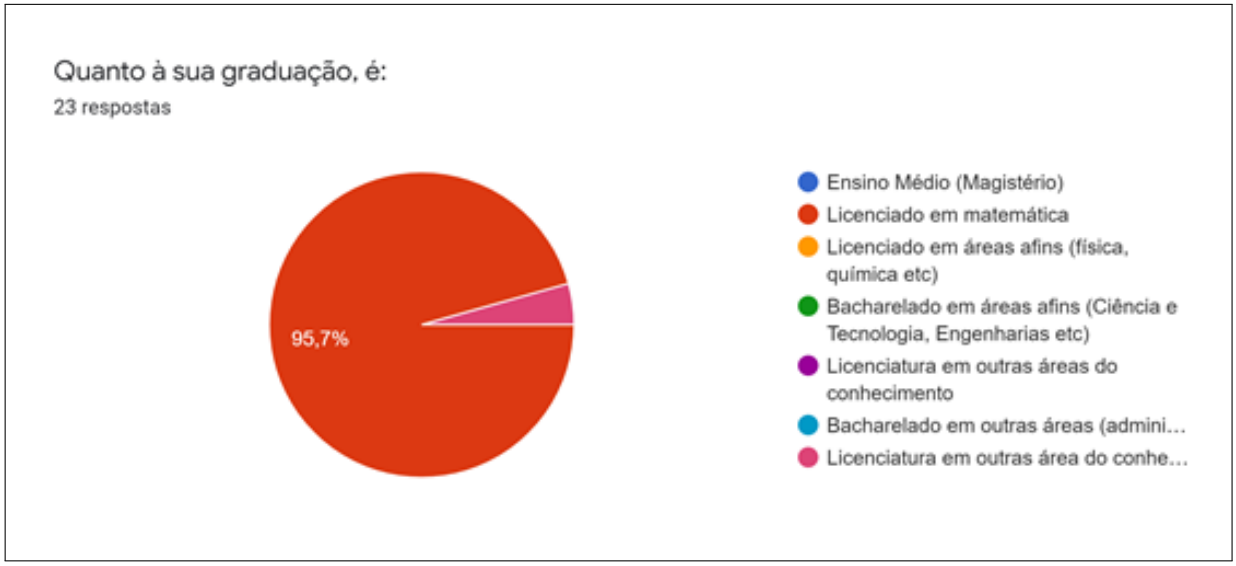
Fonte: elaborado pelo autor (2020).

Figura 8 – Tempo de docência em matemática.



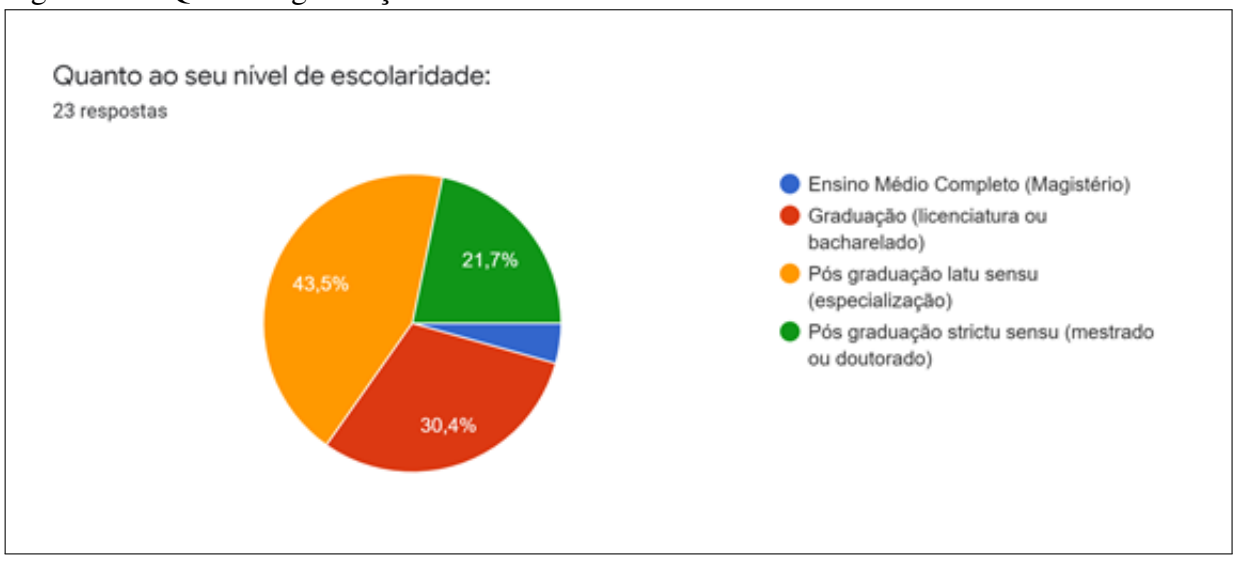
Fonte: elaborado pelo autor (2020).

Figura 9 – Quanto ao tipo de graduação.



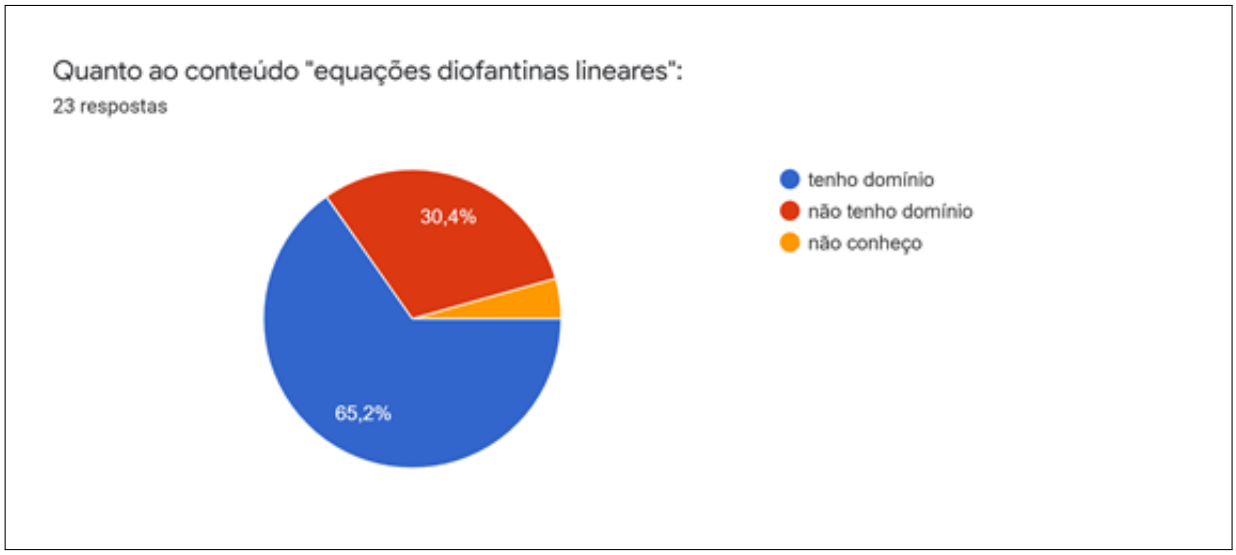
Fonte: elaborado pelo autor (2020).

Figura 10 – Quanto à graduação



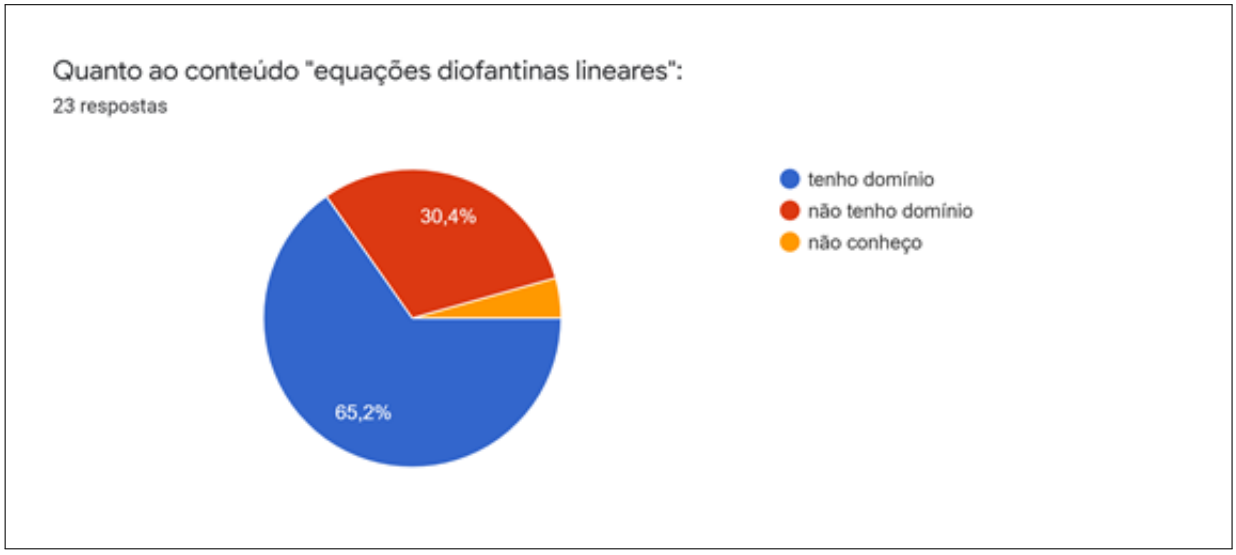
Fonte: elaborado pelo autor (2020).

Figura 11 – Quanto ao domínio do conteúdo "equações diofantinas lineares".



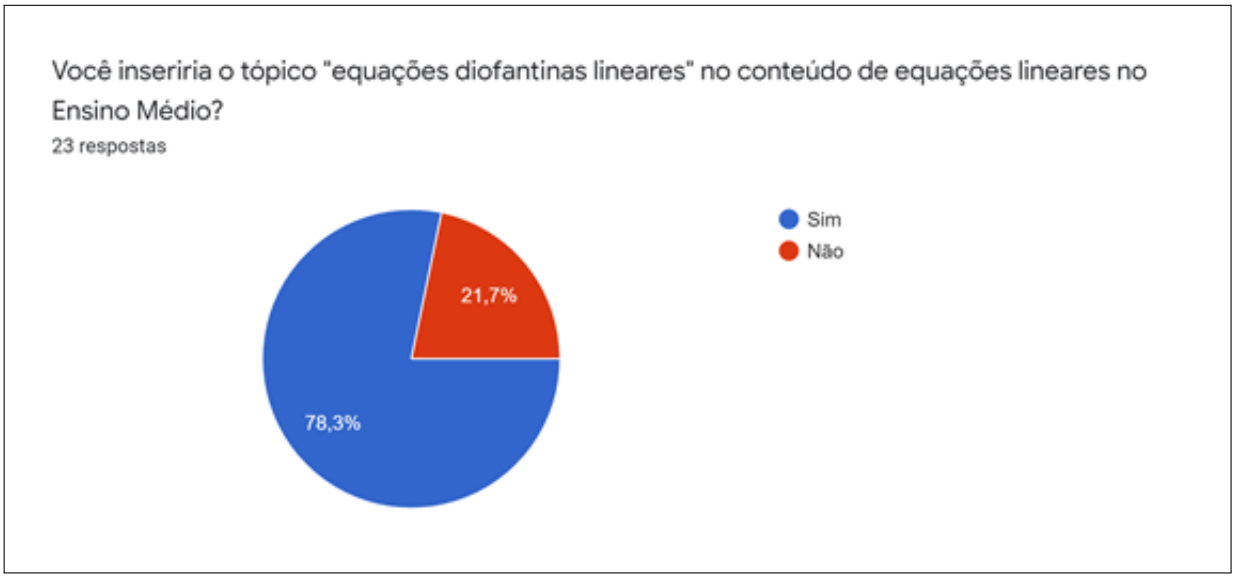
Fonte: elaborado pelo autor (2020).

Figura 12 – Quanto ao domínio do conteúdo "equações diofantinas lineares".



Fonte: elaborado pelo autor (2020).

Figura 13 – Quanto à inserção do conteúdo "equações diofantinas lineares"no ensino médio.



Fonte: elaborado pelo autor (2020).

ANEXO A – O MÍNIMO MÚLTIPLO COMUM E O MÁXIMO DIVISOR COMUM GENELARIZADOS

O presente artigo trata sobre os conceitos de mínimo múltiplo e máximo divisor comum no conjunto dos racionais e irracionais, além da aplicabilidade da forma generalizada.

Pode-se fazer uma descrição sucinta do arquivo anexado.

MATEMÁTICA UNIVERSITÁRIA
nº 40 – junho/2006 – pp. 59–74

O Mínimo Múltiplo Comum e o Máximo Divisor Comum Generalizados

CYDARA C. RIPOLL, JAIME B. RIPOLL, ALVERI A. SANT'ANA

1 Introdução

Na disciplina "Tecnologia de Informação e Comunicação em Educação Matemática", do Mestrado Profissionalizante em Ensino de Matemática da UFRGS, os alunos foram solicitados a explorar o programa GraphEquation, e lá calcularam o mínimo múltiplo comum entre números reais, obtendo, por exemplo[1],

$$\operatorname{lcm}\left(\frac{1}{2}\,,\,\frac{3}{4}\right)=\frac{3}{2}. \tag{1}$$

Paralelamente, na disciplina de Fundamentos de Matemática B, lhes era dito que o mínimo múltiplo comum entre dois racionais (ou reais) pode ser sempre tomado igual a 1, simplesmente porque $\mathbb{Q}$ (ou $\mathbb{R}$) é um corpo. Estas duas informações geraram, naturalmente, uma confusão entre os alunos, ocasionando um debate entre estes e seus professores. Considerando a polêmica ensejada por esta discussão, bem como certas

[1] lcm =least common multiple=mínimo múltiplo comum

questões levantadas como, por exemplo, a da utilidade da noção do mmc entre reais, escrevemos o presente trabalho, com os seguintes objetivos:

i) esclarecer em que sentido as duas afirmações acima estão corretas;

ii) abordar questão similar com relação ao máximo divisor comum;

iii) apresentar exemplos de aplicações para o máximo divisor comum e o mínimo múltiplo comum entre números reais.

Começamos relembrando os conceitos e algumas propriedades do mínimo múltiplo comum e do máximo divisor comum entre inteiros.

Definição 1.1. *Dizemos que um inteiro v é* ***múltiplo*** *de um inteiro u, ou que u é um* ***divisor*** *de v, se*

$$v = tu \tag{2}$$

para algum inteiro t. Dizemos que ℓ é ***múltiplo comum*** *de dois inteiros u e v se ℓ é múltiplo de u e de v. Finalmente, dizemos que M é o* ***mínimo múltiplo comum entre*** *u e v, e escrevemos $M = \mathsf{mmc}(u, v)$, se:*

i) $M > 0$,

ii) M é múltiplo comum de u e v,

iii) M é o menor dos múltiplos comuns, no sentido de que se M' é um múltiplo comum de u e v e $M' > 0$ então $M \leq M'$.

Definição 1.2. *Dados dois inteiros u e v, dizemos que um natural D é o* ***máximo divisor comum entre*** *u e v, e escrevemos $D = \mathsf{mdc}(u, v)$, se:*

i) D é um divisor comum de u e v, isto é, D é divisor tanto de u quanto de v,

ii) D é o maior dos divisores comuns, no sentido de que se D' é um divisor comum de u e v então $D' \leq D$.

Propriedades do mmc e do mdc:

As provas das propriedades a seguir podem ser encontradas em [2]:

1. Sempre existem o mmc e o mdc entre dois inteiros u e v.
2. Dados dois inteiros u e v, tem-se

$$uv = \mathsf{mmc}(u, v) \times \mathsf{mdc}(u, v) \tag{3}$$

3. Para quaisquer inteiros u, v, w,

$$\mathsf{mmc}(uw, vw) = |w|\mathsf{mmc}(u, v) \tag{4}$$

e

$$\mathsf{mdc}(uw, vw) = |w|\mathsf{mdc}(u, v) \tag{5}$$

Embora as noções de mmc e de mdc sejam introduzidas principalmente para o estudo dos números inteiros, elas admitem uma extensão para pares de reais comensuráveis, como mostramos a seguir.

2 Números reais comensuráveis, mmc e mdc generalizados

A noção de comensurabilidade, historicamente, foi introduzida e utilizada como uma forma de comparar o tamanho de dois segmentos de reta:

Definição 2.1. *Dizemos que dois segmentos de reta são* ***comensuráveis*** *quando ambos podem ser obtidos através de um número inteiro de emendas de um mesmo segmento de reta.*

Os gregos da Antigüidade acreditaram, por muito tempo, que dois quaisquer segmentos de reta eram sempre comensuráveis. Entre 450 e 400 a.C., contudo, provou-se que o segmento diagonal de um quadrado não era comensurável com o seu lado. Isto gerou uma forte crise na Matemática grega, chamada Crise dos Incomensuráveis, que só foi resolvida depois de muitos anos de discussão; discussão esta que levou à formulação precisa do problema da comensurabilidade em termos de *medida* de segmentos de retas e que se encerrou com a criação dos números reais absolutos.

Embora sendo um conceito geométrico, a comensurabilidade pode ser equivalentemente definida como uma relação entre dois números reais quaisquer:

Definição 2.2. *Dois números reais r e s são* ***comensuráveis*** *se existem inteiros não nulos m, n tais que*

$$mr = ns. \tag{6}$$

Exemplos:

1. Dois racionais são sempre comensuráveis.
2. Dois irracionais podem ser comensuráveis: por exemplo, $\sqrt{2}$ e $2\sqrt{2}$.
3. Dois reais quaisquer nem sempre são comensuráveis: basta tomar um racional e um irracional, mas também a maioria de pares de irracionais, como, por exemplo, $\sqrt{2}$ e $\sqrt{3}$. De fato, se existissem naturais m e n tais que

$$m\sqrt{2} = n\sqrt{3} \tag{7}$$

então, elevando ao quadrado a expressão acima, teríamos

$$2m^2 = 3n^2. \tag{8}$$

Considerando a fatoração em primos de inteiros, temos em (8) um absurdo, pois é ímpar o número de vezes que o primo 2 aparece na fatoração em primos de $2m^2$, enquanto que é par o número de vezes que 2 aparece na fatoração em primos de $3n^2$. Assim, concluímos que não existem naturais m e n para os quais (7) seja verdadeira.

A noção de comensurabilidade de dois números reais motiva uma primeira extensão da definição de múltiplo e divisor, como segue:

Definição 2.3. *Dizemos que um número real r é um* ***múltiplo inteiro*** *de um real s, ou que s é um* ***divisor inteiro*** *de r, se existe um inteiro a tal que $r = as$.*

Decorre das definições de comensurabilidade e de múltiplo inteiro de um real o seguinte fato:

Proposição 2.4. *Sejam r e s dois reais não nulos. As seguintes afirmações são equivalentes:*

a) r e s são comensuráveis;

b) o quociente r/s é um número racional;

c) existe um real t que é múltiplo inteiro comum de r e de s;

d) existe um real u que é divisor inteiro comum de r e de s.

Prova. *(a)⇒(b):* Se r e s são comensuráveis então existem $m, n \in \mathbb{Z}^*$ tais que $mr = ns$. Conseqüentemente,

$$\frac{r}{s} = \frac{n}{m} \in \mathbb{Q}.$$

(b)⇒(c): Suponhamos que $r/s \in \mathbb{Q}$, digamos,

$$\frac{r}{s} = \frac{n}{m}.$$

então, multiplicando a igualdade acima por sm obtemos que $t := mr = ns$ é um múltiplo inteiro comum de r e de s.

(c)⇒(d): Seja $t \in \mathbb{R}$ um múltiplo inteiro comum de r e de s, digamos, $t = mr = ns$, com $m, n \in \mathbb{Z}^*$. Então o número

$$u := \frac{r}{n} = \frac{s}{m}$$

é um divisor inteiro comum de r e de s.

(d)⇒(a): Seja u um divisor inteiro comum de r e de s, digamos, $r = un$ e $s = um$,com $m, n \in \mathbb{Z}^*$. Então $mr = ns$. ■

Considerando a proposição anterior, ficam naturais as seguintes definições:

Definição 2.5. *Sejam r e s dois reais comensuráveis não nulos.*

Dizemos que t é o ***mínimo múltiplo comum generalizado entre*** *r e s, e escrevemos*

$$t = \mathsf{mmcg}(r, s),$$

se:

a) $t > 0$,

b) t é um múltiplo inteiro comum de r e s,

c) se t' é múltiplo inteiro comum de r e s e $t' > 0$, então $t \leq t'$.

Dizemos que u é o ***máximo divisor comum generalizado entre*** *r e s, e escrevemos*

$$u = \mathsf{mdcg}(r, s),$$

se:

a) u é um divisor inteiro comum de r e s

b) se u' é divisor inteiro comum de r e de s então $u' \leq u$.

No teorema que segue obtemos uma fórmula para o mmcg e para o mdcg entre dois reais comensuráveis quaisquer.

Teorema 2.6. *Sejam r e s dois reais comensuráveis não nulos. Então*

$$\mathsf{mmcg}(r, s) = |vr| = |us| \quad e \quad \mathsf{mdcg}(r, s) = \left|\frac{r}{u}\right| = \left|\frac{s}{v}\right|,$$

onde u/v é a forma irredutível do racional r/s.

Prova. Consideraremos aqui apenas o caso r e s positivos. Observamos inicialmente que se a, b, c, d são inteiros tais que

$$ar = bs \quad \text{e} \quad cr = ds$$

então

$$\frac{b}{a} = \frac{d}{c},$$

e este número nada mais é do que o número r/s. Assim, os menores naturais a, b que satisfazem $ar = bs$ são claramente obtidos quando tomamos o numerador e o denominador da fração irredutível que representa o racional r/s. Daí, pela Definição 2.5, se u/v é tal fração irredutível,

$$\mathsf{mmcg}(r, s) = vr = us \quad \text{e} \quad \mathsf{mdcg}(r, s) = \frac{r}{u} = \frac{s}{v},$$

o que completa prova do teorema. ∎

No caso de r e s serem números racionais, as fórmulas dadas no teorema acima podem ser reescritas em termos das representações destes racionais em frações irredutíveis:

Corolário 2.7. *Sejam r, s racionais não nulos e sejam a, b, c, d inteiros tais que a/b e c/d são as representações para r e s, respectivamente, na forma de fração irredutível. Então*

$$\mathsf{mmcg}(r,s) = \frac{\mathsf{mmc}(a,c)}{\mathsf{mdc}(b,d)} \quad e \quad \mathsf{mdcg}(r,s) = \frac{\mathsf{mdc}(a,c)}{\mathsf{mmc}(b,d)}. \tag{9}$$

Prova. Novamente aqui provamos apenas para o caso r e s positivos. Como $\mathsf{mdc}(a,b) = 1 = \mathsf{mdc}(b,d)$, temos

$$\frac{r}{s} = \frac{a/b}{c/d} = \frac{ad}{bc} = \frac{a'd'}{b'c'},$$

onde

$$a' = \frac{a}{\mathsf{mdc}(a,c)}, \quad b' = \frac{b}{\mathsf{mdc}(b,d)}, \quad c' = \frac{c}{\mathsf{mdc}(a,c)}, \quad d' = \frac{d}{\mathsf{mdc}(b,d)}.$$

É claro então que a fração $a'd'/b'c'$ é irredutível, e portanto, pelo Teorema 2.6, temos

$$\begin{aligned}\mathsf{mmcg}(r,s) = rb'c' &= \frac{a}{b}\frac{b}{\mathsf{mdc}(b,d)}\frac{c}{\mathsf{mdc}(a,c)} \\ &\overset{(3)}{=} \frac{\mathsf{mmc}(a,c)}{\mathsf{mdc}(b,d)},\end{aligned}$$

e

$$\begin{aligned}\mathsf{mdcg}(r,s) = \frac{r}{a'd'} &= \frac{a}{b}\frac{\mathsf{mdc}(a,c)}{a}\frac{\mathsf{mdc}(b,d)}{d} \\ &\overset{(3)}{=} \frac{\mathsf{mdc}(a,c)}{\mathsf{mmc}(b,d)},\end{aligned}$$

o que completa a prova. ■

Observação 2.8. *A hipótese "na forma de fração irredutível" no Corolário 2.7 é imprescindível, isto é, a fórmula (9) quando aplicada a frações não irredutíveis não proporciona necessariamente o* $\mathsf{mmcg}(r,s)$ *e o* $\mathsf{mdcg}(r,s)$, *como nos mostra o exemplo a seguir. Seja* $r = 10/6$ *e* $s = 1/7$ *então*

$$\frac{\mathsf{mmc}(10,1)}{\mathsf{mdc}(6,7)} = 10 \neq 5 = \frac{\mathsf{mmc}(5,1)}{\mathsf{mdc}(3,7)} = \mathsf{mmcg}(r,s)$$

e

$$\frac{\mathsf{mdc}(10,1)}{\mathsf{mmc}(6,7)} = \frac{1}{42} \neq \frac{1}{21} = \frac{\mathsf{mdc}(5,1)}{\mathsf{mmc}(3,7)} = \mathsf{mdcg}(r,s)$$

Exemplos:

1) Da observação acima obtemos $\mathsf{mmcg}\left(\frac{10}{6}, \frac{1}{7}\right) = \mathsf{mmcg}\left(\frac{5}{3}, \frac{1}{7}\right) = 5.$

e $\mathsf{mdcg}\left(\frac{10}{6}, \frac{1}{7}\right) = \mathsf{mdcg}\left(\frac{5}{3}, \frac{1}{7}\right) = \frac{\mathsf{mdc}(5,1)}{\mathsf{mmc}(3,7)} = \frac{1}{21}.$

2) $\mathsf{mmcg}\left(\frac{1}{2}, \frac{3}{4}\right) = \frac{\mathsf{mmc}(1,3)}{\mathsf{mdc}(2,4)} = \frac{3}{2}$ e $\mathsf{mdcg}\left(\frac{1}{2}, \frac{3}{4}\right) = \frac{\mathsf{mdc}(1,3)}{\mathsf{mmc}(2,4)} = \frac{1}{4}$

(note que este cálculo explica o valor encontrado pelo GraphEquation (1)).

3) $\mathsf{mmcg}\left(\frac{1}{2}, 1\right) = \frac{\mathsf{mmc}(1,1)}{\mathsf{mdc}(2,1)} = 1$ e $\mathsf{mdcg}\left(\frac{1}{2}, 1\right) = \frac{\mathsf{mdc}(1,1)}{\mathsf{mmc}(2,1)} = \frac{1}{2}.$

4) $\mathsf{mmcg}\left(\frac{2}{3}\pi, \frac{1}{4}\pi\right) = 2\pi$ e $\mathsf{mdcg}\left(\frac{2}{3}\pi, \frac{1}{4}\pi\right) = \frac{2\pi/3}{8} = \frac{1}{12}\pi,$

pois

$$\frac{2\pi/3}{\pi/4} = \frac{8}{3}, \text{ e então } 3 \times \frac{2\pi}{3} = 2\pi = 8 \times \frac{\pi}{4}.$$

5) $\mathsf{mmcg}(16\sqrt{3}, 5\sqrt{3}) = 5 \times 16\sqrt{3} = 80\sqrt{3}.$

Mostramos agora que as identidades (3), (4) e (5) se generalizam também para mmcg e mdcg entre reais comensuráveis:

Corolário 2.9. *Sejam r e s dois reais não nulos comensuráveis. Então:*

i) $rs = \mathsf{mdcg}(r, s) \times \mathsf{mmcg}(r, s)$;

ii) dado qualquer real não nulo c, temos ainda cr e cs comensuráveis e

$$\mathsf{mmcg}(cr, cs) = |c| \times \mathsf{mmcg}(r, s)$$
$$\mathsf{mdcg}(cr, cs) = |c| \times \mathsf{mdcg}(r, s)$$

Prova. Consideraremos aqui apenas o caso c, r e s positivos. Suponhamos que m, n são naturais não nulos tais que

$$\frac{r}{s} = \frac{n}{m} \text{ e } \mathsf{mdc}(n, m) = 1.$$

Daí temos

$$\mathsf{mmcg}(r, s) = mr = ns \quad \text{e} \quad \mathsf{mdcg}(r, s) = \frac{r}{n} = \frac{s}{m},$$

de onde segue que

$$\mathsf{mdcg}(r,s) \times \mathsf{mmcg}(r,s) = \frac{r}{n} \times ns = rs,$$

o que prova *(i)*.

Além disso, como

$$\frac{cr}{cs} = \frac{n}{m},$$

temos

$$\mathsf{mmcg}(cr, cs) = mcr = c \times \mathsf{mmcg}(r,s)$$
$$\mathsf{mdcg}(cr, cs) = \frac{cr}{n} = c \times \mathsf{mdcg}(r,s),$$

o que prova *(ii)*. ■

O Corolário a seguir nos mostra que as propriedades acima nos permitem calcular o mínimo múltiplo comum generalizado entre dois racionais de expansão decimal finita de uma forma mais rápida. Não é difícil se convencer que este resultado também vale quando substituímos a base 10 de numeração por uma base b qualquer.

Corolário 2.10. *Se r e s são dois números racionais que podem ser representados por uma fração decimal, digamos,*

$$r = \frac{u}{10^k} \quad e \quad s = \frac{v}{10^l}$$

e se $t \geq k$ e $t \geq l$ então

$$\mathsf{mmcg}(r,s) = \frac{\mathsf{mmc}(10^t r, 10^t s)}{10^t} \quad e \quad \mathsf{mdcg}(r,s) = \frac{\mathsf{mdc}(10^t r, 10^t s)}{10^t}$$

Prova. Imediata. ■

Exemplo: No Exemplo 2 acima, poderíamos ter calculado o mmcg da seguinte forma:

$$\mathsf{mmcg}\left(\frac{1}{2}, \frac{3}{4}\right) = \mathsf{mmcg}(0.5\ ;\ 0.75) = \frac{\mathsf{mmc}(100 \times 0.5, 100 \times 0.75)}{100}$$
$$= \frac{\mathsf{mmc}(50, 75)}{100} = \frac{150}{100} = \frac{3}{2}$$

3 Divisibilidade em anéis

Rclembramos que um anel é um conjunto munido de duas operações que satisfazem certas propriedades. Para a definição precisa indicamos [3].

Definição 3.1. *Seja A um anel. Dados $a, b \in A$, dizemos que a é **múltiplo** de b, ou que b é um **divisor** de a, se $a = tb$ para algum $t \in A$.*

Exemplos:

1) Se $A = \mathbb{Z}$, então a definição acima coincide com a Definição 1.1.

2) Se A é o anel de polinômios com coeficientes reais, então o polinômio $3X^3 + 4X^2 + 3X + 4$ é múltiplo de $X^2 + 1$, pois

$$3X^3 + 4X^2 + 3X + 4 = (X^2 + 1)(3X + 4).$$

3) Se A é o anel dos inteiros de Gauss

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\},$$

então $(1 + 2i)$ é divisor de 5, pois $(1 + 2i)(1 - 2i) = 5$.

Note que, no caso em que o anel A é até um corpo (ou seja, todo elemento não nulo de A tem inverso multiplicativo), como $\mathbb{Q}$ ou $\mathbb{R}$ por exemplo, todo elemento não nulo a de A é divisor de 1, pois

$$1 = a(a^{-1}),$$

e portanto 1 é múltiplo comum a quaisquer dois elementos não nulos de A. Mais até: num corpo, quaisquer elementos não nulos a, b, c satisfazem a propriedade de que qualquer um deles é um múltiplo comum e também um divisor comum dos demais. Por exemplo,

$$b(b^{-1}c) = c = a(a^{-1}c)$$

e

$$b = c(c^{-1}b) \quad \text{e} \quad a = c(c^{-1}a).$$

Portanto, não faz sentido falar em mmc e mdc em corpos, se pensamos em múltiplos e divisores como dados pela Definição 3.1, ficando assim justificada a segunda afirmação feita na introdução deste trabalho.

4 Voltando à motivação deste trabalho

As justificativas para as duas afirmações mencionadas na Introdução foram explicadas por duas generalizações diferentes da idéia de múltiplo e de divisor de inteiros (compare as Definições 1.1, 2.3 e 3.1). Tais generalizações dependeram da maneira como encaramos o produto na igualdade (2):

- por um lado, concentrando-nos na soma de inteiros, $v = tu$ significa, supondo $t > 0$, que

$$v = \underbrace{u + ... + u}_{t \text{ vezes}}$$

(para $t < 0$ encaramos tu como a soma de $-t$ parcelas iguais a $-u$);

- por outro lado, concentrando-nos no produto de inteiros, $v = tu$ significa que v é o produto de dois elementos do anel $\mathbb{Z}$.

A primeira maneira de encarar a igualdade (2) nos permite considerar a idéia de múltiplo inteiro em qualquer conjunto que possua a estrutura de $\mathbb{Z}-$módulo (ou seja, em qualquer grupo). Já a segunda maneira nos permite considerar a idéia de múltiplo e divisor em qualquer conjunto que possua a estrutura de anel.

Assim, as duas afirmações do início deste trabalho, que foram apresentadas aos alunos em contextos distintos, estão corretas. No entanto, a simples nomenclatura "lcm" (mínimo múltiplo comum) utilizada pelo GraphEquation em lugar de "glcm - Mínimo Múltiplo Comum Generalizado" é que causou, ao nosso ver, a maior confusão por parte dos alunos, pois não proporcionou a reflexão sobre o assunto. O termo "generalizado", se utilizado, teria instigado o aluno a refletir: "Por que 'generalizado'? Como o conceito tradicional de mmc entre inteiros está sendo generalizado?".

Antes de passarmos às aplicações, um último comentário sobre a utilização da nomenclatura "mínimo múltiplo comum": é comum nos

depararmos no Ensino Médio com cálculos do tipo

$$\frac{3}{2\sqrt{2}} + \frac{5}{4\sqrt{3}} = \frac{6\sqrt{3}+5\sqrt{2}}{4\sqrt{6}} \tag{10}$$

e, impensadamente, chamarmos o denominador $4\sqrt{6}$de mmc entre $2\sqrt{2}$ e $4\sqrt{3}$. Esta nomenclatura não está adequada, mesmo segundo a definição que demos aqui de mínimo múltiplo comum generalizado, pois $2\sqrt{2}$ e $4\sqrt{3}$ não são reais comensuráveis. No entanto, salientamos que o cálculo é válido. De fato, num corpo podemos também utilizar a notação de fração, com o seguinte significado: dados r, s elementos de um corpo K, com $s \neq 0$, denotamos por r/s o elemento rs^{-1}. Desta maneira, utilizando as propriedades das operações $+$ e $\times$ definidas em K, temos ainda válida em K a regra de somar frações: dados $r, s, u, v \in K$ com $s \neq 0 \neq v$, temos

$$\frac{r}{s} + \frac{u}{v} = rs^{-1} + uv^{-1} = s^{-1}v^{-1}(rv+su) = (sv)^{-1}(rv+su) = \frac{rv+su}{sv}. \tag{11}$$

Ainda, dado $a \in K$, $a \neq 0$, tal que $s = as'$ e $v = av'$, temos

$$\frac{r}{s} = \frac{1}{a}\frac{r}{s'} \quad \text{e} \quad \frac{u}{v} = \frac{1}{a}\frac{u}{v'};$$

daí, poderíamos também operar em K da seguinte maneira:

$$\frac{r}{s} + \frac{u}{v} = \frac{1}{a}\frac{r}{s'} + \frac{1}{a}\frac{u}{v'} = \frac{1}{a}\left(\frac{r}{s'} + \frac{u}{v'}\right) = \frac{1}{a}\frac{rv'+us'}{s'v'}.$$

Ora, no caso em que $s = m\sqrt{p}$ e $v = n\sqrt{q}$, com m, n inteiros e $\sqrt{p}$, $\sqrt{q}$ não comensuráveis, podemos escrever

$$s = \mathsf{mdc}(m,n)m'\sqrt{p} \quad \text{e} \quad v = \mathsf{mdc}(m,n)n'\sqrt{q},$$

onde $m' = \dfrac{m}{\mathsf{mdc}(m,n)}$ e $n' = \dfrac{n}{\mathsf{mdc}(m,n)}$. Portanto, temos

$$\frac{r}{m\sqrt{p}} + \frac{u}{n\sqrt{q}} = \frac{1}{\mathsf{mdc}(m,n)}\left(\frac{r}{m'\sqrt{p}} + \frac{s}{n'\sqrt{q}}\right) \overset{(11)}{=} \frac{1}{\mathsf{mdc}(m,n)}\left(\frac{rn'+sm'}{m'n'\sqrt{pq}}\right).$$

Mas, por (3),

$$\frac{1}{\mathsf{mdc}(m,n)}\frac{1}{m'n'} = \frac{1}{\mathsf{mdc}(m,n)}\frac{[\mathsf{mdc}(m,n)]^2}{mn} = \frac{\mathsf{mdc}(m,n)}{mn} = \mathsf{mmc}(m,n)$$

e, conseqüentemente,

$$\frac{r}{m\sqrt{p}} + \frac{s}{n\sqrt{q}} = \frac{1}{\mathsf{mdc}(m,n)}\left(\frac{rn'+sm'}{m'n'\sqrt{pq}}\right) = \frac{rn'+sm'}{\mathsf{mmc}(m,n)\sqrt{pq}}$$

que nada mais é do que a fórmula aplicada em (10).

5 Aplicações:

Apresentamos a seguir duas aplicações dos conceitos de mínimo múltiplo comum e máximo divisor comum generalizados:

I) Para o mmcg:

Definição 5.1. *Uma função $f : \mathbb{R} \to \mathbb{R}$ é dita* ***periódica*** *quando existe um número real $p \neq 0$ tal que*

$$f(x+p) = f(x), \text{ para todo } x \in \mathbb{R}. \tag{12}$$

Dizemos que p é um ***período*** *de f, ou também que f é uma* ***função periódica de período*** *p.*

Note que se f é uma função periódica de período p, então kp também é um período para f, para todo $k \in \mathbb{Z}\backslash\{0\}$. Podemos então provar:

Teorema 5.2. *Sejam $f : \mathbb{R} \to \mathbb{R}$ e $g : \mathbb{R} \to \mathbb{R}$ funções periódicas de períodos p_f e p_g respectivamente. Se p_f e p_g são números* ***comensuráveis*** *então as funções: $f+g$ e $f.g$ são periódicas de período* $\mathsf{mmcg}(p_f, p_g)$.

Prova. Faremos aqui apenas a demonstração para o caso $f+g$. Sendo p_f e p_g por hipótese comensuráveis, está bem definido $M = \mathsf{mmcg}(p_f, p_g)$. Existem então $m, n \in \mathbb{Z}\backslash\{0\}$ tais que

$$mp_f = np_g = M. \tag{13}$$

Obviamente, como m, n, p_f, p_g são todos não nulos, temos que M é também não nulo. Agora, dado $x \in \mathbb{R}$, temos:

$$\begin{aligned}(f+g)(x+M) &= f(x+M) + g(x+M) \\ &= f(x+np_f) + g(x+mp_g) \\ &= f(x) + g(x) = (f+g)(x),\end{aligned}$$

o que prova que $f+g$ é periódica de período $\text{mmcg}(p_f, p_g)$. ■

Exemplo 5.3. *$f(x) = \text{sen}3x$ e $g(x) = \cos 7x$ são funções periódicas de períodos fundamentais $p_f = \frac{2\pi}{3}$ e $p_g = \frac{2\pi}{7}$, respectivamente. Como p_f e p_g são comensuráveis, temos que a função h dada por*

$$h(x) = \text{sen}3x + \cos 7x$$

é periódica, admitindo 2π para período, pois

$$\text{mmcg}\left(\frac{2\pi}{3}, \frac{2\pi}{7}\right) = 3 \times \frac{2\pi}{3} = 2\pi,$$

já que

$$\frac{2\pi/3}{2\pi/7} = \frac{7}{3}.$$

II) Para o mdc:

Geometricamente, se dois segmentos AB e CD têm medidas comensuráveis r e s, respectivamente, então o $\text{mdcg}(r, s)$ é a medida do maior segmento OU que, quando escolhido para nova unidade de medida para medir segmentos de reta, proporciona medidas inteiras para AB e CD.

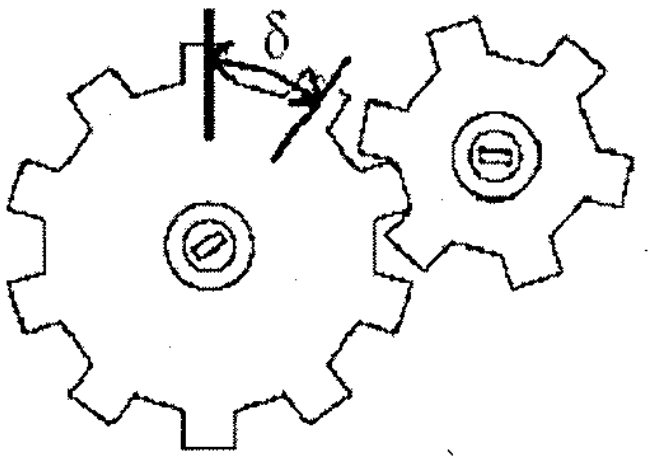
Podemos aplicar esta idéia ao ajuste de engrenagens: suponhamos que queiramos ajustar duas rodas num sistema de engrenagens, frezando dentes nas mesmas, todos de mesmo tamanho. Ora, cada roda deve ter um número inteiro de dentes e, obviamente, o desgaste sobre as rodas será mínimo quando os comprimentos das circunferências forem comensuráveis: de fato, denotando por δ o dobro do comprimento do dente (para levarmos em conta o espaço entre dentes - veja figura),

e denotando por r_1 e r_2 os raios das rodas, temos que existem m, n naturais tais que $2\pi r_1 = m\delta$ e $2\pi r_2 = n\delta$ se e só se

$$\frac{2\pi r_1}{2\pi r_2} = \frac{m\delta}{n\delta},$$

ou ainda, se e só se r_1 e r_2 forem comensuráveis:

$$nr_1 = mr_2.$$



Portanto, o maior valor de δ é precisamente

$$\mathsf{mdcg}(2\pi r_1, 2\pi r_2) \overset{\text{Cor.2.9}}{=} 2\pi \times \mathsf{mdcg}(r_1, r_2),$$

e se, na prática, este comprimento se revelar inviável (por ser, por exemplo, muito "curvo" um arco de comprimento δ), então, para minimizar o desgaste, teremos que tomar comprimentos iguais a δ/k com k natural.

Salientamos que, no caso de raios incomensuráveis, teremos inevitavelmente um desgaste sobre as rodas dentadas, mas este é tornado mínimo quando utilizamos a teoria das frações contínuas para calcular o valor de δ (veja [1] e [4]).

Referências Bibliográficas

[1] Beskin, N., *Frações Contínuas,* Coleção Iniciação à Matemática, Ed. MIR, 1980.

[2] Coelho, S.P. - Millies, C.P., *Números: Uma introdução à Matemática,* EDUSP, 3ª edição, 2003.

[3] Gonçalves, A., *Introdução à Álgebra,* Projeto Euclides, IMPA, 3ª edição, 1995.

[4] Lequain, Y., *Aproximação de um número real por números racionais,* 19º Colóquio Brasileiro de Matemática, IMPA, 1994.

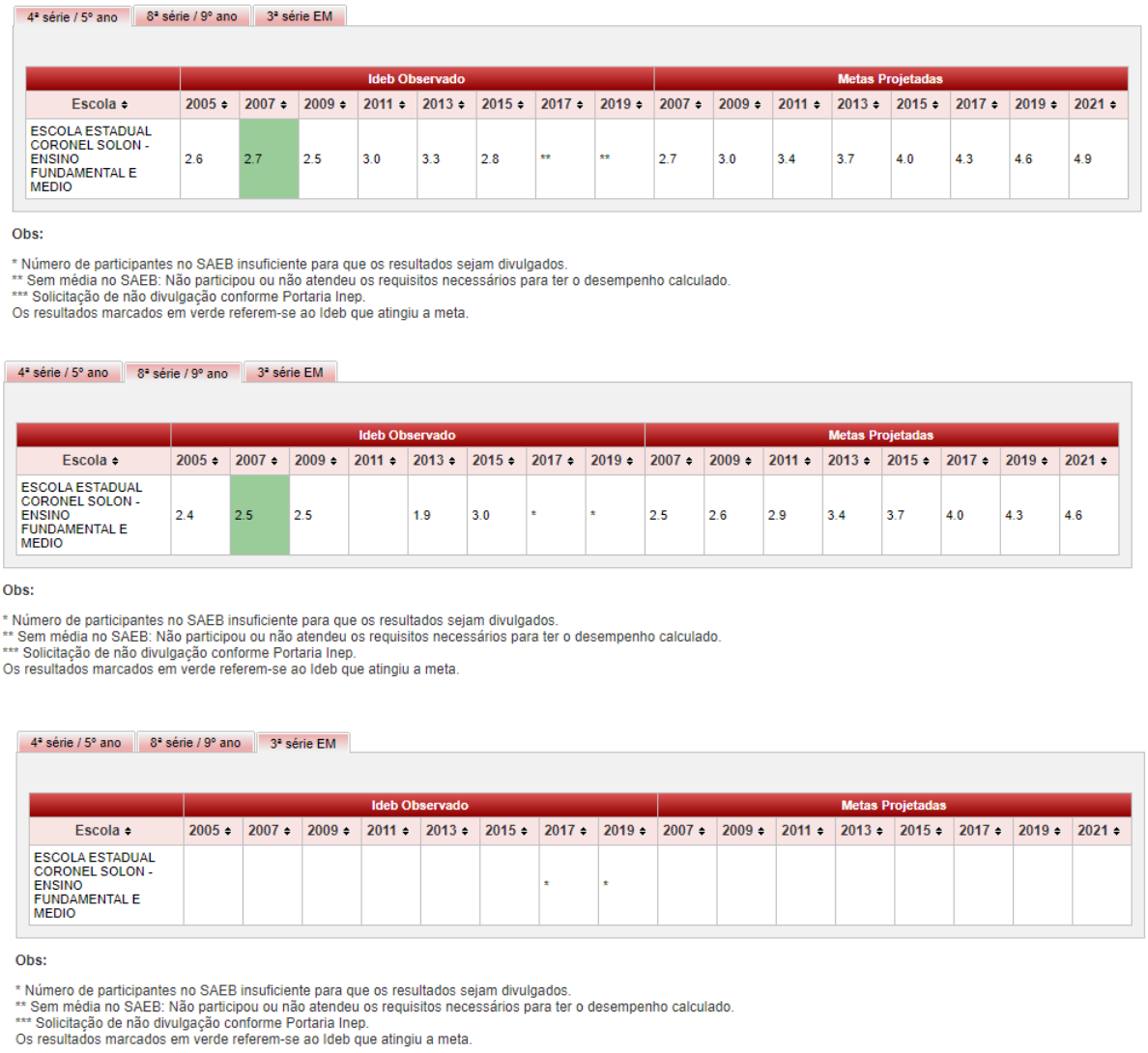
[5] http://www.euler.mat.ufrgs.br/~portosil/ol-peri.html

[6] http://www.edumatec.mat.ufrgs.br/softwares ou
http://www.peda.com/grafeq

Cydara Cavedon Ripoll, Jaime Bruck Ripoll, Alveri Alves Sant'Ana
Instituto de Matemática
Universidade Federal do Rio Grande do Sul
Avenida Bento Gonçalves 9500
91 509 - 900 Porto Alegre - RS
Brasil
cydara@mat.ufrgs.br, ripoll@mat.ufrgs.br, alveri@mat.ufrgs.br

ANEXO B – DESEMPENHO NO IDEB DA ESCOLA ESTADUAL CORONEL SOLON

Resultado das notas da Escola Estadual Coronel Solon no IDEB/INEP.



4ª série / 5º ano | 8ª série / 9º ano | 3ª série EM

	Ideb Observado								Metas Projetadas							
Escola	2005	2007	2009	2011	2013	2015	2017	2019	2007	2009	2011	2013	2015	2017	2019	2021
ESCOLA ESTADUAL CORONEL SOLON - ENSINO FUNDAMENTAL E MEDIO	2.6	2.7	2.5	3.0	3.3	2.8	**	**	2.7	3.0	3.4	3.7	4.0	4.3	4.6	4.9

Obs:

* Número de participantes no SAEB insuficiente para que os resultados sejam divulgados.
** Sem média no SAEB: Não participou ou não atendeu os requisitos necessários para ter o desempenho calculado.
*** Solicitação de não divulgação conforme Portaria Inep.
Os resultados marcados em verde referem-se ao Ideb que atingiu a meta.

4ª série / 5º ano | 8ª série / 9º ano | 3ª série EM

	Ideb Observado								Metas Projetadas							
Escola	2005	2007	2009	2011	2013	2015	2017	2019	2007	2009	2011	2013	2015	2017	2019	2021
ESCOLA ESTADUAL CORONEL SOLON - ENSINO FUNDAMENTAL E MEDIO	2.4	2.5	2.5		1.9	3.0	*	*	2.5	2.6	2.9	3.4	3.7	4.0	4.3	4.6

Obs:

* Número de participantes no SAEB insuficiente para que os resultados sejam divulgados.
** Sem média no SAEB: Não participou ou não atendeu os requisitos necessários para ter o desempenho calculado.
*** Solicitação de não divulgação conforme Portaria Inep.
Os resultados marcados em verde referem-se ao Ideb que atingiu a meta.

4ª série / 5º ano | 8ª série / 9º ano | 3ª série EM

	Ideb Observado								Metas Projetadas							
Escola	2005	2007	2009	2011	2013	2015	2017	2019	2007	2009	2011	2013	2015	2017	2019	2021
ESCOLA ESTADUAL CORONEL SOLON - ENSINO FUNDAMENTAL E MEDIO							*	*								

Obs:

* Número de participantes no SAEB insuficiente para que os resultados sejam divulgados.
** Sem média no SAEB: Não participou ou não atendeu os requisitos necessários para ter o desempenho calculado.
*** Solicitação de não divulgação conforme Portaria Inep.
Os resultados marcados em verde referem-se ao Ideb que atingiu a meta.

Figura 14 – Notas de desempenho da Escola Estadual Coronel Solon no IDEB. Fonte: <http://ideb.inep.gov.br/resultado/>