UNICAMP

UNIVERSIDADE ESTADUAL DE
CAMPINAS

Instituto de Matemática, Estatística e
Computação Científica

JULIANA DE OLIVEIRA FIORELLI

Máximo Divisor Comum e Mínimo Múltiplo Comum Generalizados Aplicados no Ensino Básico.

Campinas

2017

Juliana de Oliveira Fiorelli

Máximo Divisor Comum e Mínimo Múltiplo Comum Generalizados Aplicados no Ensino Básico.

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestra.

Orientador: Sergio Antonio Tozoni

Este exemplar corresponde à versão final da Dissertação defendida pela aluna Juliana de Oliveira Fiorelli e orientada pelo Prof. Dr. Sergio Antonio Tozoni.

Campinas

2017

Agência(s) de fomento e nº(s) de processo(s): CAPES

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

F512m

Fiorelli, Juliana de Oliveira, 1980-
Máximo divisor comum e mínimo múltiplo comum generalizados aplicados no ensino básico / Juliana de Oliveira Fiorelli. – Campinas, SP : [s.n.], 2017.

Orientador: Sergio Antonio Tozoni.
Dissertação (mestrado profissional) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Mínimo múltiplo comum. 2. Máximo divisor comum. 3. Números racionais. 4. Números irracionais. I. Tozoni, Sergio Antonio,1953-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Greatest common divisor and least common multiple applied in basic education
Palavras-chave em inglês:
Least common multiple
Greatest common divisor
Rational numbers
Irrational numbers
Área de concentração: Matemática em Rede Nacional
Titulação: Mestra
Banca examinadora:
Sergio Antonio Tozoni [Orientador]
Benjamin Bordin
Mariana Matulovic da Silva Rodrigueiro
Data de defesa: 07-07-2017
Programa de Pós-Graduação: Matemática em Rede Nacional

Dissertação de Mestrado profissional defendida em 07 de julho de 2017 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SERGIO ANTONIO TOZONI

Prof(a). Dr(a). BENJAMIN BORDIN

Prof(a). Dr(a). MARIANA MATULOVIC DA SILVA RODRIGUEIRO

As respectivas assinaturas dos membros encontram-se na Ata de defesa

Dedico ao meu amado pai, Paulo Miguel Fiorelli, que há muito não está conosco, mas que Sempre me deu motivação para seguir em frente.

Agradecimentos

Primeiramente à Deus, pois sem a Sua presença esta dissertação não existiria. É Dele que provem todo o conhecimento.

Aos meus pais, por me darem a vida e sempre estarem ao meu lado, de alguma maneira, na minha caminhada.

Aos meus irmãos, familiares e amigos, que entenderam meu afastamento, nervosismos e preocupações.

À minha saudosa avó Leonor, meu exemplo de vida e de luta, minha maior incentivadora na escolha da minha profissão e em seguir a carreira acadêmica, que, infelizmente, não verá a conclusão dessa etapa da minha vida.

Ao meu orientador Sergio Antonio Tozoni, pela orientação inigualável e eficiente, pelas sugestões que contribuíram imensamente nessa pesquisa desafiadora.

À todos meus professores, do ensino básico ao mestrado, responsáveis pela aquisição do meu conhecimento.

À CAPES, pelo auxílio financeiro. Pois sem esse auxílio esse sonho não seria realizado.

Aos colegas do PROFMAT, que se tornaram amigos, pelas poucas horas de descontração e gargalhadas e pelas muitas horas de estudos coletivos.

Aos funcionários da Unicamp, que sempre fizeram seu serviço da melhor maneira.

Às minhas diretoras, Meiris e Daniela, e a coordenadora, na época do mestrado e realização do projeto, Hellen, da E.E. Professora Maria Neiva Abdelmassih Justo, que sempre me auxiliaram nas dificuldades docentes e por autorizarem a realização do projeto.

À minha querida amiga e companheira de disciplina, Renata, pelo compartilhamento de saberes e pela compreensão e auxílio.

À todos os meus colegas de profissão que sabem o quão difícil, mas gratificante, é nossa carreira, pela ajuda em diversos momentos.

À minha ex aluna Maria Angélica, que superou a mestre, pelos muitos auxílios.

Ao meu cunhado, Marcelo, que, com sua generosidade, compartilhou comigo seus conhecimentos acadêmicos. Estou imensamente grata.

À minha tão amada amiga, Mari, que sempre fora meu exemplo em tudo, desde a época da faculdade. Sem seu apoio e motivação não teria nem começado o mestrado.

Não há palavras para descrever como sou eternamente grata.

Resumo

Este trabalho teve por objetivo utilizar-se da estrutura curricular da disciplina de matemática no estado de São Paulo e dos conceitos de mínimo múltiplo comum (MMC) e de máximo divisor comum (MDC), a fim de expor o déficit no ensino de tal conteúdo para alunos de Ensino Fundamental 2 e Ensino Médio. Tal problema fica evidente ao exigir do aluno a habilidade de generalização das propriedades destas operações durante a aprendizagem de outros conteúdos, como em funções e equações trigonométricas. Por fim, o trabalho argumenta sobre a necessidade de sempre retomar os conceitos de MMC e MDC a medida que um novo conjunto numérico é introduzido ao aluno.

Palavras-chave: Mínimo Múltiplo Comum. Máximo Divisor Comum. Conjuntos Numéricos. Grandezas Comensuráveis. Mínimo Múltiplo Comum Generalizado. Máximo Divisor Comum Generalizado.

Abstract

This work had as objective to use the curriculum of the discipline of mathematics in the state of São Paulo and the concepts of least common multiple (LCM) and greatest common divisor (GCD), in order to expose the deficit in teaching such content to students in Elementary and High School. Such a problem is evident when we require from the student the ability of generalization of the properties of these operations during the learning of other content, such as functions and trigonometric equations. Finally, the work argues the need to always recollect the contents of LCM and GCD whenever a new numeric set is introduced to the student.

Keywords: Least Common Multiple. Greatest Common Divisor. Numerical Sets. Commensurable Quantities. Generalized Least Common Multiple. Generalized Greatest Common Divisor.

Sumário

INTRODUÇÃO 11

1 A MATEMÁTICA E SUAS CRISES! 13
1.1 As Crises 13

2 O MÁXIMO DIVISOR COMUM E O MÍNIMO MÚLTIPLO COMUM. 24
2.1 Os Conceitos de mmc e mdc no Conjunto dos Números Naturais. . 24
2.2 Os Conceitos de mmc e mdc no Conjunto dos Números Inteiros. . . 42
2.3 Números Reais Comensuráveis 51

3 APLICAÇÃO DO PROJETO: MMC E MDC: GOSTOSURA OU TORTURA? 57
3.1 Matemática para o Ensino Fundamental II e para o Ensino Médio . 57
3.2 O Motivo da Escolha dos Temas para o Projeto 59
3.3 Desenvolvimento do Projeto 60
3.4 Oitavo ano do Ensino Fundamental. 60
3.5 Terceiro Ano do Ensino Médio. 66
3.6 Fotos do Projeto 69

4 CONCLUSÃO 71

REFERÊNCIAS 72

Introdução

Para os Pitagóricos tudo podia ser representado por números comensuráveis, os quais caracterizam-se por serem subdivididos por uma mesma unidade de medida. Mas essa certeza não durou para sempre.

Tudo estava perfeito até que descobriram que o lado do quadrado e sua diagonal não eram comensuráveis, emergindo assim um descontentamento na comunidade matemática da época, que se configurou como a primeira grande crise da matemática. Os Pitagóricos perceberam a necessidade da existência de outro tipo de número, os incomensuráveis.

Anos mais tarde, outra grande crise da matemática- a crise dos fundamentos - modificou a maneira como o conhecimento matemático era transmitido. Através da questão da impossibilidade do movimento oriundo do Paradoxo de Zenão e o método de provas por exaustão de Eudoxo - ambos possuíam como base teórica a idéia de conjuntos infinitos - começou uma discussão em torno da possibilidade de termos diferentes tipos ou categorias de infinitos, ou seja, de possuirmos conjuntos do tipo transfinitos, tal como elaborado por Cantor.

Mas se existe ao menos mais que um conjunto infinito, então podemos ter o conjunto de todos os conjuntos? Se sim, então, como ficaria o conjunto das partes deste conjunto de todos os conjuntos em termos de cardinalidade? Essas indagações desencadearam o surgimento de paradoxos que prejudicavam a nascente teoria de conjuntos de Cantor, a qual naquele momento fundamentava a matemática.

Hilbert, em um congresso em Vianna, conclama a comunidade matemática a deixar de lado a teoria dos conjuntos infinitos e fundamentar a matemática em caminhos e definições de base finita visto que na Natureza nada é infinito. Segue, a partir dos trabalhos de Hilbert, uma primeira compartimentação dos conteúdos matemáticos em razão desta busca por uma base finita para a formalização da matemática.

Mas é Descartes que trouxe a maior influência para o ensino hoje, com seu Método de fragmentar um problema em outras partes menores com o intuito de encontrar uma solução para o mesmo. A transmissão do conhecimento, não só em matemática, é todo fragmentado, o que muitas vezes atrapalha na interiorização dos conceitos pelos alunos.

É por tudo isso que o objetivo deste trabalho é apresentar a importância de retomar os conceitos de mínimo múltiplo comum (MMC) e de máximo divisor comum (MDC) à medida que outros conjuntos numéricos, além dos naturais, são introduzidos aos alunos, de uma forma mais lúdica, pensando na inter e transdisciplinariedade, visto que estes não generalizam as propriedades das operações como esperado pela maior parte dos professores.

No caso da interação de alunos de ensino fundamental e médio com o conteúdo matemático, especialmente MMC e MDC, é observável que o nível de desenvolvimento atual, contempla somente o âmbito dos números naturais, e os demais conjuntos numéricos se encontram na gama de possibilidades, sendo necessário a intervenção do docente para o sucesso da aprendizagem.

A referência principal deste trabalho foi o artigo de C.C. Ripoll, J. B. Ripoll e A. A. Sant'Ana [12], "O Mínimo Múltiplo Comum e Máximo Divisor Comum Generalizados", pelo lado didático dos conceitos abordados no trabalho, e pela forma como os quais são tratados progressivamente durante o ensino da matemática.

Passando a uma descrição do conteúdo oferecido por capítulo, tem-se:

No Capítulo 1, busca-se explicitar que o modo de ensino da matemática, que busca um formalismo finito e claro desta, se desenvolveu junto à teoria dos conjuntos de Cantor e a crise dos fundamentos gerada por esta.

Já o Capítulo 2, inicia-se com conceitos, propriedades e teorias acerca do mínimo múltiplo comum e do máximo divisor comum, porém tratando-os com maior rigor do que livros didáticos de nível Fundamental e Médio. Em seguida, generaliza-se as acepções desses para além dos números naturais, retomando ao tema do projeto.

Por fim, o último capítulo, Capítulo 3, expõe a grade curricular do ensino da matemática no estado de São Paulo buscando subsidiar a prática do conteúdo abordado no projeto com os alunos do 8º ano do ensino fundamental e do 3º ano do ensino médio, para então ser apresentado o projeto.

1 A Matemática e Suas Crises!

"Definição: dizem-se grandezas comensuráveis as que se medem pela mesma medida, e incomensuráveis aquelas das quais não é possível nada tornar-se medida comum."
(Euclides, Livro X dos Elementos)

Neste primeiro capítulo expomos acerca das principais crises que acometeram as bases fundamentacionais da matemática. A ideia é evidenciar o desenvolvimento ocorrido em matemática em razão destas crises para evidenciarmos que o ensino institucionalizado de modo compartimentado e disciplinar decorre, principalmente, da busca de um formalismo finito e claro da matemática frente aos problemas enfrentados com o advento das coleções infinitas de Cantor.

1.1 As Crises

Podemos dizer que a matemática passou por duas grandes crises em sua história: a conhecida *crise dos incomensuráveis*, emergida do surgimento dos números ditos incomensuráveis e a *crise dos fundamentos*, gerada a partir do desenvolvimento da teoria dos conjuntos de Cantor, com seus conceitos de números transfinitos.

Qualquer pessoa que queira estudar sobre a descoberta dos incomensuráveis na Grécia Antiga encontrará em livros de história da matemática e/ou de matemática duas visões contraditórias sobre o assunto. A primeira delas, a mais difundida, afirma que tal descoberta surgiu após uma crise no pensamento pitagórico. Nessa versão, a existência da incomensurabilidade entra em contradição com o princípio pitagórico de que tudo poderia ser explicado ou representado por meio de números ([8], 2010).

A segunda versão da descoberta dos incomensuráveis até hoje está restrita quase que somente aos meios especializados da história antiga ou da história da matemática. Segundo essa versão, ao estudar as fontes mais confiáveis para o assunto percebe-se que estas não trazem nenhuma evidência de uma possível crise e que o erro disto estaria nos estudiosos que fizeram uma leitura pouco rigorosa de fontes menos confiáveis.

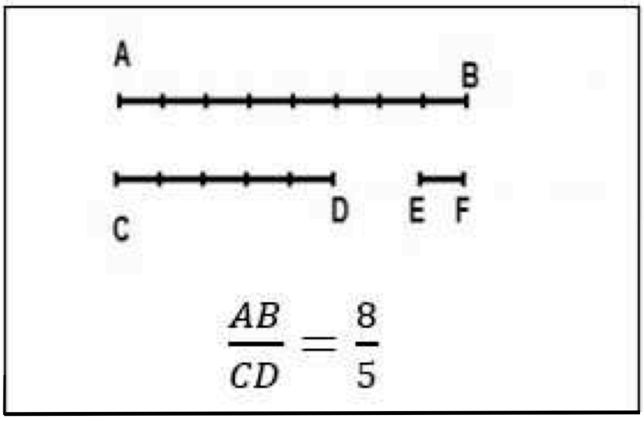
Para os Pitagóricos a essência de todas as coisas, seja na geometria ou nos assuntos práticos e teóricos do ser humano, é explicável apenas em termos dos números inteiros ou de suas razões. Quando as razões são expressas por números inteiros, as denominamos por **razões comensuráveis**. Caso contrário, elas são ditas **incomensuráveis**. Os números, associados ao processo de contagem, pareciam tão fundamentais a Pitágoras e a seus discípulos que eles chegaram a declarar que: "Tudo é número" ([1], 1974).

> Tinha sido uma crença fundamental do pitagorismo que a essência de todas as coisas, e, geometria, tanto nos negócios práticos e teóricos em geral, é explicável em termos dos *arithmos*, ou propriedades intrínsecas dos números inteiros ou das razões entre eles. Os diálogos de Platão mostram, contudo, que a matemática grega foi abalada por uma revelação que virtualmente demoliu a base da fé dos pitagóricos nos números inteiros. Foi descoberto que, na própria geometria, os números inteiros e as razões entre eles são inadequados mesmo para expressar simples propriedades fundamentais ([2], 1974, p. 79).

Ao explorar alguns fatos notáveis e inesperados, que estão ligados à primeira grande crise do desenvolvimento da matemática, verifica-se a existência de uma questão com que lidavam os matemáticos gregos daquela época, que consistia em comparar grandezas da mesma espécie, como dois segmentos de reta, duas áreas ou dois volumes.

Tal como exposto em ([2], 2011), um exemplo dessa questão é, no caso de dois segmentos retilíneos AB e CD, dizer que a razão AB/CD é o número racional m/n. Para os gregos isto significava (e atualmente a mesma acepção se configura) que existia um terceiro segmento EF tal que AB fosse m vezes EF e CD, n vezes esse mesmo segmento EF. Esse exemplo pode ser observado na Figura 1 ilustrada abaixo, para $m = 8$ e $n = 5$.

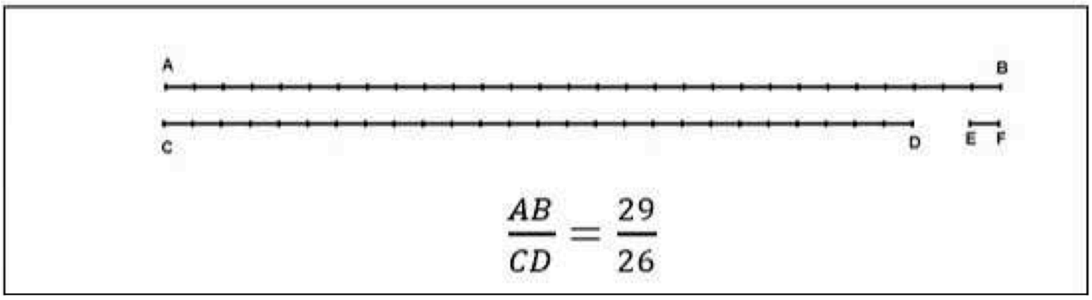
Figura 1 – Segmentos na razão 8/5.



Fonte: Elaborada pela autora.

Durante boa parte do século V a.C., aproximadamente o período em que Pitágoras viveu, tinham-se a certeza que os números racionais eram suficientes para comparar segmentos de reta. Isto consistia em dizer que, dados dois segmentos AB e CD seria sempre possível encontrar um terceiro segmento EF, por menor que fosse necessário, contido um número inteiro de vezes em AB e outro número inteiro de vezes em CD, ou

Figura 2 – Segmentos na razão 29/26

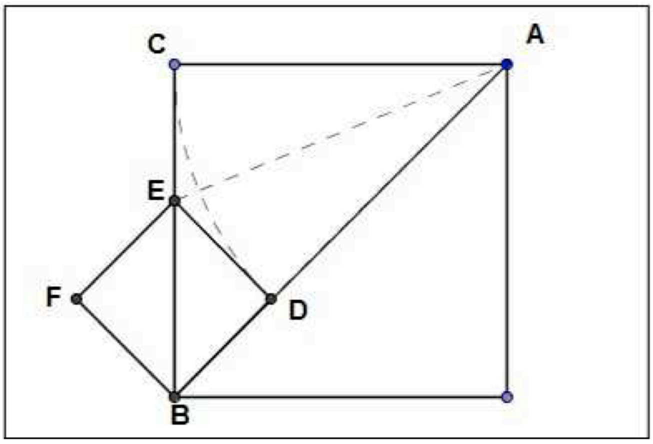


Fonte: Elaborada pela autora.

seja, EF é um submúltiplo comum de AB e CD. Um exemplo da situação está na Figura 2.

As grandezas incomensuráveis, conforme já exposto, foram descobertas pelos próprios pitagóricos por meio do argumento geométrico que demonstra que o lado e a diagonal de um quadrado são segmentos incomensuráveis.

Figura 3 – Segmentos incomensuráveis



Fonte: Elaborada pela autora.

A Figura 3 representa um quadrado com diagonal $d = AB$ e lado $l = AC$. Se d e l são segmentos comensuráveis, então existe um terceiro segmento que é submúltiplo comum de d e l. Diante deste contexto, foi traçado o arco CD com centro em A, partindo de C até interseccionar o segmento AB no ponto D. É certo que $AD = AC$. Então, nos triângulos retângulos ACE e ADE, os catetos AC e AD são congruentes e a hipotenusa AE é comum. Logo são também congruentes os catetos CE e DE. Por sua vez o segmento BD também é congruente aos segmentos CE e DE, pois ao observar o triângulo retângulo EBD percebe-se que é isósceles.

Por tudo isso têm-se, então que,

$$d = AB = AD + BD = l + BD,$$

$$l = BC = BE + EC = BE + BD.$$

Ou seja,

$$d = l + BD \quad (1.1)$$

$$l = BE + BD. \quad (1.2)$$

O segmento que é submúltiplo comum de d e l, é também, por (1.1), submúltiplo de BD e, em (1.2), de BE. Portanto se houver um segmento que seja submúltiplo comum de $d = AB$ e $l = AC$, então o mesmo segmento será submúltiplo comum de BE e BD, segmentos esses que são a diagonal e o lado do quadrado $BDEF$.

Prosseguindo na mesma construção geométrica que permitiu passar do quadrado original ao quadrado $BDEF$, chegamos a um quadrado menor ainda; e assim por diante, indefinidamente; e esses quadrados vão se tornando arbitrariamente pequenos, pois as dimensões de cada quadrado diminuem em mais da metade quando passa-se de um deles a seu sucessor. Com esse procedimento conclui-se que o segmento deverá ser submúltiplo comum do lado e da diagonal de um quadrado tão pequeno quanto se queira.

Evidentemente, isso é um absurdo! O que rejeita a suposição inicial de que o lado AC e a diagonal AB do quadrado inicial são comensuráveis. Conclui-se, portanto, que o *lado* e a *diagonal* de qualquer quadrado são grandezas incomensuráveis.

Uma das consequências do aparecimento dos números incomensuráveis é a existência de pontos na reta sem abscissas racionais. Ao desenhar um quadrado de lado OU, medindo uma unidade, sobre a reta r, e com o auxílio de um compasso, ao transpormos a medida da diagonal AO para reta, formamos o segmento OP, como monstrado na figura 4 (Figura 4). Pode-se perceber que tomando $OP = AO$, em que AO é a diagonal de um quadrado de lado unitário OU, e como OP e OU são incomensuráveis, não é possível expressar a razão OP/OU como um número racional.

Que número seria a abscissa de P? Pelo teorema de Pitágoras temos que

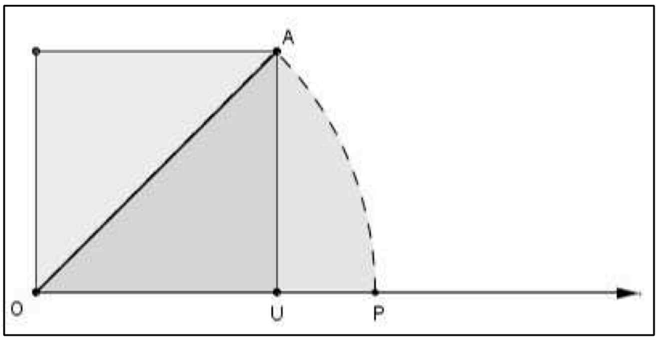
$$OA^2 = OU^2 + AU^2.$$

Da Figura 4 sabe-se que $AO = OP$ e que $OU = AU = 1$, obtendo assim:

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

Ou seja,

Figura 4 – Construindo $\sqrt{2}$



Fonte: Elaborada pela autora.

$$OP = \sqrt{2}.$$

Portanto, essa é a abscissa de P ao ser tomado OU como unidade de comprimento.

Pontos de uma reta que não possuem abscissas racionais, têm por abscissas números irracionais, e $\sqrt{2}$ é um desses números, como mostrado na Figura 4.

Por meio de argumentos estritamentes numéricos, demonstraremos que $\sqrt{2}$ é um número irracional. Para isso supõe-se que existe uma fração irredutível m/n, tal que $\sqrt{2} = m/n$. Então:

$$2 = m^2/n^2$$

e

$$m^2 = 2n^2. \tag{1.3}$$

De (1.3), segue-se que m^2 é um número par, e em consequência m também é par. Utilizando $m = 2r$ e substituindo em (1.3), tem-se que:

$$4r^2 = 2n^2,$$

ou ainda,

$$n^2 = 2r^2. \tag{1.4}$$

Em (1.4), percebe-se que n^2 é também par, por definição n é par.

Têm-se que m e n não podem ser números pares ao mesmo tempo, pois no início da demonstração, instituiu-se que m/n é uma fração irredutível. Temos, portanto, um absurdo e a rejeição da suposição inicial de que $\sqrt{2}$ é um número racional da forma m/n.

A demonstração acima está baseada em um argumento que, segundo Aristóteles, teria sido usado na descoberta de grandezas incomensuráveis. Este argumento tem um alto grau de abstração, o que fez com que muitos historiadores da Ciência acreditassem que a descoberta dos incomensuráveis tenha ocorrido com um raciocínio mais concreto, como o argumento geométrico utilizado na Figura 3.

Demonstrações como as que foram apresentadas acima, da incomensurabilidade do lado e da diagonal do quadrado, ou da irracionalidade de $\sqrt{2}$, foram as primeiras demonstrações por redução ao absurdo que se fizeram na Antiguidade.

Há grandes evidências históricas que apontam para o argumento de que não houve, de fato, uma crise gerada pela "descoberta" dos números incomensuráveis, tal como evidenciado em ([8], 2010). Neste artigo os autores expõem alguns pontos em defesa da existência da crise, como por exemplo, a lenda propagada pelos seguidores pitagóricos de que Hipaso, também um pitagórico, fora lançado ao mar em decorrência dele ter revelado a estranhos de que não era possível a redução de todos os fenômenos do universo aos números inteiros e suas razões.

Mas, segundo os autores, há um número considerável de pesquisadores que discordam que a descoberta da incomensurabilidade tenha causado uma crise no pensamento pitagórico, tais como Ivor Grattan-Guinness em ([9], 1997), o qual argumenta que a descoberta do $\sqrt{2}$, que provocou a crise, não fora mencionada pelos comentadores da época, como por exemplo, Aristóteles, Burkert em ([3], 1972), dentre outros. Assim, de acordo com ([9], 1997, p. 47–48), "...longe de experimentar uma crise de fundamentos, os gregos antigos podem ter gozado uma época de grandes jornadas matemáticas."

Já Burkert expõe que há evidências que sugerem fortemente que o relato de Eudemo (um dos possíveis discípulos de Pitágoras) a respeito da descoberta dos números irracionais, não faz originalmente qualquer referência à Pitágoras. Para maiores detalhes a respeito da argumentação dos referidos autores, consultar as obras supracitadas.

De fato, é difícil separar a história da lenda no que diz respeito às obras dos pitagóricos. Mas, em concordância com Boyer em ([1], 1974, p.36), o fato de que Pitágoras "[...]foi uma das figuras mais influentes da história é difícil negar, pois seus seguidores, seja iludidos, seja inspirados, espalharam suas crenças por quase todo o mundo grego".

Também é concebido que os Pitagóricos assumiam que o espaço e o tempo poderiam ser pensados como constituídos de pontos e instantes. Nas palavras de Boyer, ([1], 1974, p. 55),"Os elementos terminais, que constituíram uma pluralidade, de um lado eram supostos como possuindo as características de unidades geométricas, o ponto, e de outro como possuindo certas características de unidades numéricas".

O paradoxo de Zenão foi aparentemente dirigido contra os Pitagóricos, isto é, contra esta acepção de espaço e tempo como consistindo de pontos e instantes, sendo que o mesmo pode ser descrito como: Aquiles e uma tartaruga movem-se na mesma direção, ao longo de uma linha reta. Aquiles é mais veloz que a tartaruga, mas para alcançar a tartaruga, ele tem que passar primeiro pelo ponto P, do qual a tartaruga partiu. Quando Aquiles chega no ponto P, a tartaruga já está no ponto P_1. Aquiles não pode alcançar a tartaruga sem passar pelo ponto P_1, mas a tartaruga avançou para um novo ponto P_2. Quando Aquiles estiver em P_2, a tartaruga estará em P_3 e assim por diante. Por isso, Aquiles nunca poderá alcançar a tartaruga.

O interessante é que os argumentos de Zenão indicavam que um segmento finito poderia ser dividido em um número infinito de pequenos segmentos, cada um deles com um comprimento finito. A resolução usual do paradoxo de Zenão se faz por meio do cálculo em termos de limites. Mas esta resolução depende de "suposições disfarçadas sobre a natureza do infinito e é exatamente o infinito que é problema aqui" ([4], 2009, p. 26).

Após a crise dos incomensuráveis, e a influência do Paradoxo de Zenão no desenvolvimento da matemática, os matemáticos gregos desenvolveram o método que denominamos atualmente de método de exaustão, que permitiu um tratamento rigoroso dos cálculos de áreas e volumes. A ideia norteadora era de se "exaurir" a área entre o círculo e um polígono regular nele inscrito, aumentando o número de lados desse último. Deste modo, era possível efetuar, de forma finita e precisa, cálculos de comprimentos, áreas e volumes de figuras geométricas.

Com o "método de exaustão", Eudoxo exibia uma resposta ao Paradoxo de Zenão, pois se "evitava as dificuldades dos infinitesimais renunciando simplesmente a eles, pela redução dos problemas que conduzem a infinitesimais a problemas que envolvem apenas o uso da lógica formal" ([14], 2000).

De acordo com ([7], 2012):

> "O termo infinitésimus, cunhado no latim utilizado nos séculos XVI e XVII, é formado a partir do radical infinit e do sufixo esimus. Além do uso em ordinais, este sufixo corresponde aproximadamente ao substantivo português avo, utilizado em números fracionários, como por exemplo, em 1/12 ("um doze avos"). Portanto, originalmente infinitésimo significava $1/\infty$ ou "a unidade dividida pelo infinito", uma quantidade infinitamente pequena. Em linhas gerais, um infinitésimo é considerado uma magnitude não-nula menor do que qualquer outra magnitude não- nula da mesma classe.".

Nas obras "Sobre Conóides e Esferóides", "Quadratura da Parábola" e "O Método", Arquimedes utiliza o método de exaustão trabalhando com os infinitésimos sem magnitude, pois os mesmos não são obtidos pela divisão de entes geométricos.

Já no século XVII, Johannes Kepler utiliza transformações geométricas e métodos infinitesimais no cálculo do volume de inúmeros sólidos de revolução enquanto que Galileu Galilei e seu discípulo Torricelli aplicam, com relativo rigor e sucesso, o método infinitesimal à física e à matemática. A evolução do cálculo diferencial e integral, tendo como precursores, René Descartes, Pierre de Fermat e John Wallis, deu-se principalmente pelos trabalhos do sr. Isaac Newton e Gottfried Leibniz ([7], 2012).

Ainda de acordo com os autores acima, dentre as primeiras contribuições do sr. Isaac Newton à matemática, em 1665, está o desenvolvimento da expressividade de funções em termos de séries infinitas. Além disso, Newton introduz, por meio das entidades que define, dois tipos de problemas: o de encontrar a fluxão associada a fluentes dados, a partir de relações conhecidas entre os mesmos, o que corresponde ao processo de diferenciação do cálculo usual; e o de determinar a relação entre as fluxões de dois fluentes, dada a equação que traduz a relação existente entre tais fluentes, processo inverso ao primeiro e que corresponde ao processo de integração do cálculo usual.

Independentemente de Newton, em 1684, Gottfried Wilhelm Leibniz introduz e sistematiza seu cálculo diferencial, com uma notação completamente intuitiva e bem mais simples do que a utilizada por Newton. Ocorre que Leibniz possuía uma forte concepção a respeito da importância do uso de boas e claras notações para expressar o pensamento e suas contribuições para o cálculo foram realmente eficazes.

De Newton e Leibniz até Laplace (1749), quase toda produtividade da matemática centrou-se em torno do cálculo diferencial integral e suas aplicações na mecânica. Apesar de Leibniz ter se preocupado com o uso de formalismos em suas demonstrações e ter almejado a construção de uma linguagem universal (a *characteristic universalis*) para tratar do racicínio exato e preciso exigido na matemática, os desenvolvimentos em matemática tornaram-se tão voltados à aplicabilidade e técnicas de computação em máquinas (em decorrência da Revolução industrial ocorrida na Inglaterra), que o rigor necessário ao tratamento dessas informações foram deixadas em segundo plano ([7], 2012).

Na tentativa de se formalizar as demonstrações matemáticas e em ciências, que utilizavam a linguagem natural como ferramenta de prova, Gotlob Frege, em "Begriffsschrift", desenvolve uma linguagem formal pautada em símbolos e axiomas formais, mas fundamentada em uma teoria análoga à da linguagem natural, para ser trabalhada em contextos científicos.

Tendo em mãos uma linguagem formal apta para ser usada em contextos matemáticos e científicos e uma teoria que trata dos infinitesimais (cálculo diferencial e integral), a questão da enumerabilidade dos números é atacada por George Cantor.

É quase impossível resumir em poucas palavras a obra de Cantor relativa à teoria dos conjuntos. Na última parte do século XIX, o matemático alemão propôs, dentre outras coisas importantes, uma teoria de conjuntos na qual introduzia coleções infinitas em matemática.

Se considerarmos, por exemplo, o conjunto $\{a, b, c\}$ formado pelas letras a, b e c, vemos que esse conjunto possui três elementos. De modo geral, um conjunto que possuir um número natural, n, de elementos, denomina-se finito. Em particular, existe um conjunto, que se denota por $\varnothing$ que não tem elementos, ou, o que dá no mesmo, que possui 0 (zero) elementos.

Mas, em matemática, existem conjuntos que não são finitos, os ditos infinitos. Um exemplo de conjunto infinito é o conjunto de todos os pontos de uma reta da geometria elementar.

Na última metade do século XIX, Cantor propõe uma teoria dos conjuntos que trabalha com coleções infinitas, de modo que os inteiros foram definidos como classes de equivalêcia de pares ordenados de números naturais[1]; os racionais como classes de equivalências de pares ordenados de inteiros e os números reais como coleções infinitas de racionais. Desde então, as coleções infinitas tem sido intensamente utilizadas na matemática moderna. Mas qual seria o tamanho do infinito, isto é, qual a sua cardinalidade?

Dea acordo com ([4], 2009), Cantor demonstrou que existe pelo menos dois tipos de infinito: um infinito que é o mesmo para os conjuntos dos números naturais ($\mathbb{N}$), dos números inteiros ($\mathbb{Z}$) e dos números racionais ($\mathbb{Q}$) e outro que corresponde ao conjunto dos números reais ($\mathbb{R}$). A genialidade de Cantor evidencia-se na concepção de que, dois conjuntos tem o mesmo número de elementos se existir uma função bijetora de um no outro, sejam estes conjuntos finitos ou infinitos.

Partindo desta acepção, de acordo com os autores supracitados, Cantor demonstra que tanto os números inteiros quanto os racionais podem ser colocados em correpondência biunívoca com os Naturais. Quando isto ocorre dizemos que o conjunto é *enumerável*. O mesmo não acontece com os reais, ou seja, não há uma correspondência "um para um" dos Naturais nos Reais. Portanto, o conjunto dos números reais é dito *não-enumerável*.

Além disso, Cantor atesta que há muitos níveis de infinito (na realidade uma infinidade de infinitos). Tal concepção é descrita por meio da demonstração de que a cardinalidade do conjunto das partes de qualquer conjunto é maior do que a cardinalidade do próprio conjunto. Mas o que acontece se consideramos U o conjunto de *todos* os conjuntos?

Se o conjunto das partes é maior em termos de cardinalidade do que o conjunto U, como podemos considerar U como o conjunto de todos os conjuntos? Eis aqui o que ficou conhecido como o problema da *antinomia de Cantor* e que foi elucidado pelo *Paradoxo de Russell*

A introdução de métodos algébricos abstratos em diferentes sistemas matemáticos ajudou a unificar desenvolvimentos em análise, teoria dos números, teoria das equações,

[1] Alguns dos conceitos citados aqui serão vistos no capítulo 2

geometria, etc. O final do século XIX foi marcado, principalmente, pela introdução de uma nova linguagem teórica fundamentada na nascente teoria dos conjuntos e pelo surgimento de métodos infinitos de prova, cujo objetivo era suprimir ou minimizar conteúdos computacionais tão comumente usados nas argumentações matemáticas desta época.

No entanto, essas mudanças deram origem a uma forte preocupação a respeito da possibilidade de tais métodos serem apropriados e significativos para a matemática. A descoberta dos *paradoxos* decorrentes do uso excessivamente ingênuo dessa nova linguagem bem como da nascente teoria dos conjuntos, conduziram a preocupações ainda mais importantes, como a verificabilidade da consistência desses métodos.

Tudo isto desencadeou uma crise nos fundamentos da matemática e uma busca incessante para uma base matemática mais segura e certa foi iniciada. As ameaças definicionais colocadas pela descoberta dos paradoxos originaram acaloradas batalhas ideológicas entre os pesquisadores de várias escolas do pensamento deste período.

De acordo com [4], 2009, p.75), "A estranheza dos resultados acerca dos infinitos distintos e a confusão conceitual engedrada pelo paradoxo de Russell levaram muitos matemáticos do começo do século XX a questionar a legitimidade do uso de coleções infinitas em matemática".

Em palestras apresentadas em 1922, David Hilbert lançou sua *"Teoria da Prova"*, *Beweistheorie*, cujo objetivo era justificar a utilização de métodos modernos em provas e acabar, de uma vez por todas, com a crise dos fundamentos da matemática. Assim, segundo Hilbert, teríamos que representar o sistema matemático, que é infinito, por meio de sistemas formais, pelo fato deles estabelecerem uma linguagem formal fixa e regras de inferências precisas. Logo, as provas desses sistemas seriam finitas e consistentes.

Sendo assim, para Hilbert era necessário uma formalização de toda a matemática de um modo axiomático no qual deveria ser demonstrado, por métodos finitos, que esta axiomatização era de fato consistente. Diante disso, o caráter epistemológico do raciocínio finito produziria a justificação matemática tão almejada naquele momento de crise. Como se sabe, os famosos teoremas de incompletude de Kurt Gödel representaram um enorme obstáculo a esse projeto.

Desde os problemas com o desenvolvimento da teoria dos conjuntos, em virtude do paradoxo de Russel, da busca por um formalismo extremo onde o infinito ficaria guardado no plano ideal, e por fim os teoremas de Gödel, teorema da incompletude e da inconsistência da matemática, e o desenvolvimento da Inteligência Artificial e da computação, a matemática, e consequentemente, o ensino em matemática, tem passado por transformações marcantes durante estas últimas décadas.

A teoria de conjuntos de Cantor e o formalismo Hilbertiano influenciaram fortemente todas as áreas de desenvolvimento e aplicabilidade da matemática, incluindo a educação. No começo dos anos 80, era comum as crianças serem alfabetizadas em matemática por meio da noção de conjuntos e das operações entre os diferentes conjuntos; a matemática deixou de ser uma ferramenta para a busca de explicações para questões que intrigam e encantam o ser humano, para ser algo abstrato e, na maioria das vezes, desconectada com a realidade das pessoas, principalmente, dos alunos.

O interessante é que, o Mundo torna-se cada vez mais dependente da matemática em virtude dos desenvolvimentos em sistemas informacionais e computacionais, cada vez mais as pessoas usam e se interessam por tecnologias que abusam de conteúdos matemáticos em seu desenvolvimento, mas no entanto, os conteúdos matemáticos lecionados nas escolas, principalmente nas públicas, estão cada vez mais abstratos e desinteressantes.

Apensar de parecer retórico, é importante enfatizarmos as consequências da influência Hilbertiana e Cantoriana nas grades curriculares das universidades que formam professores de matemática. Quando as estruturas algébricas são definidas e expostas aos então discentes, com todo o seu formalismo, é comum encontrar entre os formandos em matemática, dúvidas a respeito da diferença significativa entre os mmc e mdc ditos usuais dos mmcg e mdcg (máximos e mínimos generalizados). Tal confusão quase sempre é repassada aos futuros alunos desses professores (isto quando eles abordam os mínimos e máximos generalizados)

Diante deste contexto, o objetivo deste projeto é analisar os conceitos de mínimo múltiplo comum e máximo divisor comum de um modo lúdico, bem como auxiliar em uma compreensão significativa da concepção de *menor divisor comum generalizado* e *maior múltiplo comum generalizado*, tendo como ponto inicial a noção da comensurabilidade dos números racionais e seguindo com as definições de grupo, anéis e corpos.

2 O Máximo Divisor Comum e o Mínimo Múltiplo Comum.

"Os encantos dessa sublime ciência se revelam apenas àqueles que tem coragem de irem a fundo nela."
(Carl Friedrich Gauss)

Nesta seção exporemos, sucintamente e nos moldes de ([11], 2009), os conceitos, propriedades e teorias essenciais para um entendimento claro acerca das noções de máximo divisor comum e mínimo múltiplo comum. Iniciaremos nosso plano de análise elencando as teorias e definições alicerçados no conjunto dos números naturais, para então expandirmos para as acepções de mmc e mdc generalizados, temas estes de nosso projeto.

2.1 Os Conceitos de mmc e mdc no Conjunto dos Números Naturais.

As noções acerca dos conceitos de mmc (menor múltiplo comum) e mdc (máximo divisor comum) parecem ser tão naturais para a maioria dos professores de matemática que os mesmos se esquecem o quanto estes temas tornam-se abstratos quando são ministrados de modo não muito didático e nem significativo e lúdico para o corpo discente. Para adentrarmos nas concepções inerentes aos conjuntos construídos a partir de uma propriedade ou característica (em que ser um *mínimo múltiplo* ou *máximo divisor comum* é uma propriedade que caracteriza um conjunto), é importante que salientemos a noção de conjunto. O que são conjuntos?

Em concordância com ([10], 1999, p. 01), um conjunto é caracterizado como qualquer coleção, grupo ou conglomerado cujos objetos constituintes possuem uma propriedade em comum (ou ausência dela). Estes objetos são denominados *elementos ou membros* de um conjunto e dizemos que eles pertencem ao conjunto.

Nesta seção trataremos de conjuntos formados por elementos matemáticos, tais como, números, pontos, funções, etc. Uma das propriedades mais importantes da teoria dos conjuntos é a de "ser elemento ou membro" de um determinado conjunto. Por exemplo, dizer que "x é um elemento de um conjunto X", significa que x tem a propriedade ou característica que caracteriza o conjunto X. Denotamos esta propriedade por "$x \in X$". Por convenção, os conjuntos são representados por letras maiúsculas do alfabeto (também denominado por variáveis), tais como A, B, X, Y, etc. Os elementos são denotados por letras minúsculas. O símbolo “=” é utilizado para representar que duas variáveis, por exemplo X e Y, denotam o mesmo conjunto.

Uma outra propriedade tida como fundamental sobre conjuntos é a de *subconjunto*. Um conjunto X é subconjunto de um conjunto Y se todo elemento de X é, também, elemento de Y. Quando isto ocorre, representamos por “$X \subseteq Y$”. A igualdade no símbolo refere-se ao fato dos elementos de X além de pertencerem ao conjunto Y, são os próprios constituintes de Y.

A propriedade $\subseteq$ é chamada de *inclusão*, para a qual podemos afirmar que: dados quaisquer conjuntos X, Y e Z, temos que:

1. $X \subseteq X$;
2. se $X \subseteq Y$ e $Y \subseteq X$ então $X = Y$;
3. se $X \subseteq Y$ e $Y \subseteq Z$, então $X \subseteq Z$.

A partir da concepção de conjuntos e da elucidação de algumas de suas propriedades tidas como fundamentais, podemos operar com conjuntos. Assim, temos:

Definição 2.1. A **intersecção** de X e Y é o conjunto de todos os elementos x que pertecem tanto ao conjunto X quanto ao conjunto Y.

Notação: $X \cap Y$.

Definição 2.2. A **união** de X e Y é o conjunto de todos os elementos x que pertecem ao conjunto X ou ao conjunto Y.

Notação: $X \cup Y$.

Definição 2.3. A **diferença** de X e Y é o conjunto de todos os $x \in X$ que não pertencem a Y.

Notação: $X \backslash Y$.

Definição 2.4. A **diferença simétrica** de X e Y é definida por:

$$X \Delta Y = (X \backslash Y) \cup (Y \backslash X).$$

Notação: $X \Delta Y$.

Eis algumas propriedades das operações supracitadas.

- Comutatividade:

$$X \cup Y = Y \cup X,$$
$$X \cap Y = Y \cap X.$$

- Associatividade:

$$X \cup (Y \cup Z) = (X \cup Y) \cup Z,$$
$$X \cap (Y \cap Z) = (X \cap Y) \cap Z.$$

- Distributividade:

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z),$$
$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z).$$

- Leis de De Morgan:

$$Z - (X \cap Y) = (Z - X) \cup (Z - Y),$$
$$Z - (X \cup Y) = (Z - X) \cap (Z - Y).$$

- Outras Propriedades:

$$\begin{aligned} X \cap (Y - Z) &= (X \cap Y) - Z, \\ X - Y &= \varnothing \Leftrightarrow X \subseteq Y, \\ X \Delta X &= \varnothing, \\ X \Delta Y &= Y \Delta X, \\ (X \Delta Y) \Delta Z &= X \Delta (Y \Delta Z). \end{aligned}$$

O conjunto dos números naturais e o conjunto dos números inteiros serão definidos a partir da noção de sucessor de um conjunto. Sendo assim, para caracterizá-los precisamos da concepção de relação. Tal como exposto em ([10], 1999), se x e y são objetos (que podem ser conjuntos, ou elementos de um conjunto), então o **par não-ordenado**, $\{x, y\}$ é o conjunto cujos elementos são exatamente x e y. A ordem em que x e y são colocados no conjunto é desconsiderada. Portanto, neste caso:

$$\{x, y\} = \{y, x\}.$$

Se $x = y$, note que o par não-ordenado $\{x, x\}$ nada mais é que o conjunto com um elemento $\{x\}$.

Definimos o **par ordenado** (x, y) como sendo o conjunto $\{\{x\}, \{x, y\}\}$, isto é, $(x, y) = \{\{x\}, \{x, y\}\}$. Note que desta maneira x é a primeira coordenada do par e y é a segunda coordenada do par. Assim, se $x \neq y$, temos:

$$(x, y) \neq (y, x).$$

Denominamos por **relação** uma correspondência existente entre elementos de um mesmo conjunto ou entre conjuntos distintos. Quando esta correspondência ocorre entre dois elementos, dizemos que a relação é binária; entre três elementos, a relação é dita ternária, e assim por diante.

Definição 2.5. Um conjunto R é uma **relação binária** em X se todos os elementos de R são pares ordenados de elementos de X, isto é, se para todo $z \in R$, existem x e y em X tais que:

$$z = (x, y).$$

É comum utilizarmos a notação xRy ao invés de $(x, y) \in R$.

Consideremos uma relação binária R definida sobre um conjunto X. Dizemos que:

1. R é **reflexiva** em X se para todo $x \in X, xRx$;
2. R é dita **simétrica** em X se para todo $x, y \in X, xRy \Rightarrow yRx$;
3. R é chamada de **transitiva** em X se para todo $x, y, z \in X, xRy$ e $yRz \Rightarrow xRz$;
4. R é dita **anti-simétrica** em X se para todo $x, y \in X, xRy$ e yRx somente ocorre se $x = y$.

Definição 2.6. Quando uma relação R em X é, ao mesmo tempo, reflexiva, simétrica e transitiva, a classificamos como uma **relação de equivalência**.

Consideremos, por exemplo, R uma relação definida em um conjunto X dada por:

$$xRy \Leftrightarrow x - y \text{ é divisível por } 2, \ \forall x, y \in X.$$

Isso significa que dois números são equivalentes se a diferença entre eles é par. Sendo assim, categorizamos uma classe de elementos de R que satisfaz a propriedade de ser par. Concomitantemente, temos uma outra classe definida que contempla as diferenças ímpares. Assim, temos:

Definição 2.7. Seja R uma relação de equivalência em X e $a \in X$. A **classe de equivalência módulo R de a** é o conjunto

$$[a]_R = \{y \in X : yRa\}.$$

Uma relação importante na caracterização do conjunto dos números naturais é a de ordem.

Definição 2.8. Quando uma relação R em X é, ao mesmo tempo, reflexiva, anti-simétrica e transitiva, a classificamos como uma **relação de ordem em X**.

Se R é uma relação de ordem, o par (X, R) é denominado **conjunto ordenado**. Deste modo, xRy, pode ser lido como "x é menor ou igual a y" ou "y é maior ou igual a x".

Em termos de notação temos que: xRy se $x \leqslant y$ ou $y \geqslant x$. Nossa intenção é de caracterizar o conjunto dos números naturais em termos da Teoria de Conjuntos, seguindo o formalismo de ([10], 1999). Iniciaremos por caracterizar um número natural como um conjunto. É importante destacar que, na Teoria de Conjuntos, temos o seguinte ([10], 1999, p. 07):

O conjunto que não possui elementos será chamado de conjunto vazio e denotado por $\varnothing$ e o conjunto dos números naturais $\{0, 1, 2, ...\}$ será denotado por $\mathbb{N}$, isto é,

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

Ademais, temos o:

Princípio da Indução Finita ([10], 1999, p. 42)**.** *Seja $P(n)$ uma propriedade do número natural n que satisfaz*

(i) $P(0)$ é válida.

(ii) Para todo $n \in \mathbb{N}$, $P(n)$ implica $P(n+1)$.

Então, a propriedade $P(n)$ é válida para todo $n \in \mathbb{N}$.

Se $n \in \mathbb{N}$, dizemos que $n + 1$ é o sucessor de n. Consideramos $\mathbb{N}$ com a ordem:

$$0 < 1 < 2 < 3 < \cdots < n < n + 1 < \cdots$$

Em termos de intervalos numéricos em $\mathbb{N}$, dados $a, b \in \mathbb{N}$, temos:

$$\begin{aligned}
[a,b] &:= \{x \in \mathbb{N} \colon a \leqslant x \leqslant b\},\\
(a,b) &:= \{x \in \mathbb{N} \colon a < x < b\},\\
(a,b] &:= \{x \in \mathbb{N} \colon a < x \leqslant b\},\\
[a,b) &:= \{x \in \mathbb{N} \colon a \leqslant x < b\}.
\end{aligned}$$

Os dois primeiros conjuntos são denominados, respectivamente, de intervalo fechado e intervalo aberto. Já os outros dois são denominados de intervalos semiabertos ou semifechados, indiferentemente.

Teorema 2.9. *Dado um subconjunto $A \subseteq \mathbb{N}$ não vazio, existe um elemento a de A tal que $a \leqslant b$, para todo elemento b de A.*

Demonstração: Temos $\varnothing \neq A \subseteq \mathbb{N}$. Suponha, por absurdo, que não exista um elemento $a \in A$ com $a \leqslant b$ para todo $b \in A$. Mostraremos que A deve ser necessariamente o conjunto vazio. Tal contradição finalizará a demonstração deste teorema.

Agora, nossa suposição implica que $0 \notin A$. Dado outro $n \in \mathbb{N}$, se $k \notin A$ para todo $k < n$, então $n \notin A$, caso contrário, $n \leqslant b$ para todo $b \in A$, o que estamos supondo que não acontece. Por conseguinte, $n + 1 \notin A$, pois $k \notin A$ para todo $k < n + 1$. Pelo Princípio da Indução Finita, segue que $n \notin A$ para todo $n \in \mathbb{N}$, donde $A = \varnothing$, como queríamos. ∎

A propriedade descrita no teorema anterior é chamada de Princípio da Boa Ordenação. Dizemos, portanto, que $\mathbb{N}$ é um conjunto *bem ordenado*. Após a caracterização do conjunto $\mathbb{N}$, vamos operar com os constituintes deste conjunto. Para tal, nós admitiremos que $\mathbb{N}$ é um subconjunto da reta real $\mathbb{R}$.

Definição 2.10. Sejam dados dois elementos a e b de $\mathbb{N}$. A **adição** de a por b é o deslocamento do número a, b unidades para a direita na reta numérica. Essa operação é denotada por $a + b$ e chamada de soma de a por b.

As propriedades da adição são dadas por:

i) Comutatividade.

Para quaisquer dois números naturais a e b, vale a relação:

$$a + b = b + a.$$

ii) Elemento Neutro.

Para qualquer $a \in \mathbb{N}$, existe um elemento, chamado de zero (0) tal que $0 < a$, para o qual vale a propriedade:

$$0 + a = a = a + 0.$$

iii) Associatividade.

Para quaisquer $a, b, c \in \mathbb{N}$, temos:

$$(a + b) + c = a + (b + c).$$

iv) Adição e Ordem.

Existe uma relação de compatibilidade entre a ordem e a adição nos números naturais, que diz o seguinte: dados $a, b, c \in \mathbb{N}$:

$$a < b \Rightarrow a + c < b + c.$$

A recíproca dessa propriedade também é válida, isto é:

$$a + c < b + c \Rightarrow a < b.$$

Definição 2.11. Sejam dados $a, b \in \mathbb{N}$, sendo que $a \leqslant b$. Definimos a **subtração** de b por a, como o deslocamento de b, a unidades para a esquerda na reta numérica. Essa operação é denotada por $b - a$ e chamada de diferença entre b e a.

As propriedades da subtração são dadas por:

i) Propriedade fundamental.

Dados $a, b \in \mathbb{N}$, diretamente da definição temos:

$$a + (b - a) = b.$$

ii) Da propriedade acima temos:

Dados $a, b, c \in \mathbb{N}$ tais que $a + c = b$, então $c = b - a$.

iii) Para todo número natural a, temos: $a - a = 0$.

iv) Para qualquer número natural b vale a propriedade: $b - 0 = b$.

Diz-se que a operação subtração é a operação inversa da adição, pois ao deslocarmos a, b unidades para a direita, temos $a+b$, e se deslocarmos $(a+b)$, b unidades para a esquerda, voltamos para a:

$$(a+b)-b=a.$$

Por outro lado, sendo $a \leqslant b$, se deslocamos b, a unidades para a esquerda temos $(b-a)$, por sua vez se deslocarmos $(b-a)$, a unidades para a direita, voltamos para b:

$$(b-a)+a=b.$$

A relação $(b-a)$, para $b>a$, ajuda a encontrar a quantidade de elementos que existe no intervalo $[a,b]$, pois, se $a<b$, o intervalo $[a,b]$ possui $(b-a)+1$ elementos.

Definição 2.12. Dados $a,b \in \mathbb{N}$, a **multiplicação** de a por b é o deslocamento de a unidades para a direita, repetindo-se b vezes esse procedimento. Essa operação será denotada por $a \cdot b$ e é chamada de multiplicação de a por b.

A multiplicação nada mais é do que a soma de parcelas iguais, isto é:

$$a \cdot b = a + \cdots + a$$

(a soma de b fatores iguais a a).

Em termos de propriedades, temos que:

i) Comutatividade.

Para quaisquer dois números naturais a e b, vale a seguinte relação:

$$a \cdot b = b \cdot a.$$

ii) Elemento Neutro.

Para qualquer $a \in \mathbb{N}$, existe um elemento, chamado de *elemento neutro* tal que:

$$e \cdot a = a = a \cdot e.$$

Em se tratando da operação de multiplicação, o único número natural que torna a relação válida é o número 1, isto é:

$$1 \cdot a = a = a \cdot 1.$$

iii) Associatividade.

Para quaisquer $a, b, c \in \mathbb{N}$, tem-se:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

iv) Distributividade da multiplicação em relação à adição.

Dados $a, b, c \in \mathbb{N}$, tem-se:

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

v) Analogamente verifica-se a distributividade da multiplicação em relação à subtração.

Dados $a, b, c \in \mathbb{N}$ tem-se:

$$a \cdot (b - c) = (a \cdot b) - (a \cdot c).$$

vi) Multiplicação e Ordem.

Assim como o conceito de multiplicação está diretamente ligado ao da adição, a relação entre a adição e a ordem refletirá diretamente em termos de multiplicação e ordem. Então:

$$a < b, c > 0 \Rightarrow (a \cdot c) < (b \cdot c).$$

Dentro da operação de multiplicação é importante ressaltar o conceito de múltiplos de um número. Dado um número $a \in \mathbb{N}$, os múltiplos de a são determinados por meio da multiplicação dos elementos do conjunto $\mathbb{N}$ por a. Logo:

$$\begin{gathered} 0 \cdot a = 0, \\ 1 \cdot a = 1a, \\ 2 \cdot a = a + a = 2a, \\ 3 \cdot a = a + a + a = 3a, \\ 4 \cdot a = a + a + a + a = 4a. \\ \vdots \end{gathered}$$

Outra forma de representar os múltiplos é dada por:

$$M(a) = \{0, 1a, 2a, 3a, 4a, ...\}.$$

O conjunto dos múltiplos de um número natural é sempre um subconjunto de $\mathbb{N}$ e, pelo Axioma da Infinitude, é infinito.

Do conceito de múltiplos de um número, obtém-se o conceito de múltiplo comum entre dois números naturais a e b, que por definição é um número natural m que é múltiplo tanto de a quanto de b. Por exemplo, $a \cdot b$ é um múltiplo comum de a e b. Dentre os múltiplos comuns de um número, temos:

Definição 2.13. Sejam $a, b \in \mathbb{N}$. Dizemos que $m \in \mathbb{N}$ é o **menor múltiplo comum** de a e b, e escrevemos $m = \operatorname{mmc}(a, b)$ se:

(i) $m \neq 0$ e m é um múltiplo comum de a e b;

(ii) m é o menor dos múltiplos comuns não-nulos, no sentido que se $m' \in \mathbb{N}\backslash\{0\}$ é um múltiplo de a e de b, então $m' \geqslant m$.

Definição 2.14. Dados dois números naturais a e n, tais que $a \neq 0$ e n um número qualquer, define-se a **potenciação** do seguinte modo:

$a^n = 1$, se $n = 0$,

$a^n =$ a, se $n = 1$,

$a^n = a \cdot a \cdot a \cdots a$ (n fatores a), se $n > 1$.

Observação 2.15. Define-se $0^n = 0$, para todo n diferente de zero.

Segue algumas propriedades da potenciação:

i) $1^n = 1$,

ii) $a^n \cdot a^m = a^{(n+m)}$,

iii) $(a^n)^m = a^{n \cdot m}$,

iv) $a^n \cdot b^n = (a \cdot b)^n$.

Analisaremos agora a noção de múltiplo analisado sob um outro aspecto.

Definição 2.16. Diz-se que um número natural d é **divisor** de um outro natural a, se a for múltiplo de d, ou seja:

$$a = d \cdot b, \text{ sendo } b \text{ um número também natural.}$$

Quando um número natural a é múltiplo de outro natural d, diz-se que a **é divisível por** d, ou ainda que d **divide** a, esta última relação representada por $d \mid a$. Se d não dividir a, representamos por $d \nmid a$.

O conjunto de todos os divisores de um número natural a é um conjunto finito e definido por:

$$D(a) = \{d \in \mathbb{N} \colon d \mid a\}.$$

Da definição acima decorrem as seguintes proposições:

Proposição 2.17. *Se $a, b, c \in \mathbb{N}$, $a \mid b$ e $b \mid c$ então $a \mid c$.*

Demonstração: Como $a \mid b$ e $b \mid c$, existem $n_1, n_2 \in \mathbb{N}$ com $b = n_1 \cdot a$ e $c = n_2 \cdot b$. Substituindo o valor de b na equação $c = n_2 \cdot b$ tem-se $c = n_2 \cdot n_1 \cdot a$ o que implica $a \mid c$. ■

Exemplo 2.18. Como $4 \mid 12$ e $12 \mid 60$, então $4 \mid 60$.

Proposição 2.19. *Dados $a, b, c, m, n \in \mathbb{N}$, $c \mid a$ e $c \mid b$, então $c \mid (m \cdot a + n \cdot b)$.*

Demonstração: Se $c \mid a$ e $c \mid b$ então $a = n_1 \cdot c$ e $b = n_2 \cdot c$. Multiplicando-se as duas equações por m e n, respectivamente, tem-se $m \cdot a = m \cdot n_1 \cdot c$ e $n \cdot b = n \cdot n_2 \cdot c$. Somando-se membro a membro obtém-se $m \cdot a + n \cdot b = m \cdot n_1 \cdot c + n \cdot n_2 \cdot c$, o que equivale a $m \cdot a + n \cdot b = (m \cdot n_1 + n \cdot n_2)c$. Isto significa que $c \mid (m \cdot a + n \cdot b)$. ■

Exemplo 2.20. Como $5 \mid 30$ e $5 \mid 45$, então $5 \mid (2 \times 30 + 3 \times 45)$.

Proposição 2.21. *Propriedades da divisão:*

1. $n \mid n$,
2. $d \mid n \Rightarrow a \cdot d \mid a \cdot n$,
3. $d \mid n \Rightarrow a \cdot d \mid n \cdot a$,
4. $a \cdot d \mid a \cdot n$ e $a \neq 0 \Rightarrow d \mid n$,
5. $1 \mid n$,
6. $n \mid 0$,
7. $d \mid n$ e $n \neq 0 \Rightarrow d \leqslant n$,
8. $d \mid n$ e $n \mid d \Rightarrow d = n$,
9. $d \mid n$ e $d \neq 0 \Rightarrow (n/d) \mid n$.

Demonstração: Temos que $n \mid n$ pois $n = n \cdot 1$, provando o item 1. Se $d \mid n$ existe $q \in \mathbb{N}$ tal que $n = d \cdot q$, donde $a \cdot n = a \cdot d \cdot q$, o que prova o item 2. O item 3 é análogo ao item 2, tendo em vista a propriedade comutativa da multiplicação. Para o item 4, se $a \cdot d \mid a \cdot n$, novamente existe $q \in \mathbb{N}$ tal que $a \cdot n = (a \cdot d) \cdot q$. Como $a \neq 0$ podemos dividir ambos os lados da igualdade por a obtendo $n = d \cdot q$, donde $d \mid n$. O item 5 segue do fato que $n = 1 \cdot n$ e o item 6 pois $0 = n \cdot 0$.

Para o item 7, como $d \mid n$, sabemos que existe $q \in \mathbb{N}$ satisfazendo $n = d \cdot q$. Por outro lado, $n \neq 0$ implica que $q \geqslant 1$. Logo, $n = d \cdot q \geqslant d \cdot 1 = d$, como queríamos.

Já para o item 8, primeiro note que se $n = 0$ e $n \mid d$, então d também é igual a 0. Portanto, podemos assumir que $n \neq 0$. Por um lado, $d \mid n$ implica que existe $q \in \mathbb{N}$ tal que $n = d \cdot q$. Note que como $n \neq 0$, obtemos, de passagem, que $d \neq 0$ também. Por outro lado, $n \mid d$ implica que existe $r \in \mathbb{N}$ tal que $d = n \cdot r$. Logo, obtemos que $d = d \cdot q \cdot r$. Visto que $d \neq 0$, podemos dividir ambos os lados da equação por d, donde obtemos $1 = q \cdot r$, o que implica $q = r = 1$, isto é, $n = d$. Finalmente, supondo que $d \mid n$, temos que $n = d \cdot q$. Isto implica que $q \mid n$. Mas $q = (n/d)$, se $d \neq 0$, donde segue o resultado. ■

Teorema 2.22. *(Teorema de Eudóxio) Dados a e b naturais com $b \neq 0$ então a é um múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, correspondendo a cada par de números naturais a e $b \neq 0$ existe um número natural q tal que*

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

Demonstração: Utilizando a noção geométrica que $\mathbb{N} \subseteq [0, \infty) \subseteq \mathbb{R}$, como $b \neq 0$, note que

$$[0, \infty) = \bigcup_{q \in \mathbb{N}} [q \cdot b, (q+1) \cdot b)$$

e portanto, existe $q \in \mathbb{N}$ tal que $q \cdot b \leqslant a < (q+1) \cdot b$, como queríamos demonstrar. ■

Teorema 2.23. *Dados dois naturais a e b, $b > 0$, existe um único par de naturais q e r tais que:*

$$a = q \cdot b + r,$$

com $0 \leqslant r < b$ ($r = 0 \Leftrightarrow b \mid a$). O número q é chamado de quociente e r de resto da divisão de a por b.

Demonstração: Suponha primeiro que existe um par $(q, r) \in \mathbb{N} \times \mathbb{N}$, tal que $0 \leqslant r < b$ e que satisfaça a igualdade $a = q \cdot b + r$. Partindo do suposto de que pode haver outro par de números q' e r' que torna a condição anteriormente descrita verdadeira, a pode ser escrito como: $a = q' \cdot b + r'$. Sendo q e q' números naturais e $q \neq q'$, assuma que $q < q'$. Logo é possível supor que $q + 1 \leqslant q'$. Assim:

$$0 \leqslant r' = a - q' \cdot b \leqslant a - (q+1) \cdot b = a - q \cdot b - b = r - b < 0,$$

o que é contraditório. Similarmente, se $q' < q$, trocando r' por r e q' por q acima também obtemos uma contradição. Sendo assim $q' = q$, donde $q' \cdot b + r' = a = q \cdot b + r$ e $r = r'$. Isso prova a unicidade de um par (q, r) como no enunciado.

Utilizando o Teorema de Eudóxio, existe $q \in \mathbb{N}$ tal que $q \cdot b \leqslant a < (q+1) \cdot b$. Isto implica que $0 \leqslant (a - b \cdot q) < b$. Ponha $r = a - q \cdot b$. Isto termina a demonstração deste teorema. ∎

Vimos que, dados $a, b \in \mathbb{N}$, então $a \cdot b$ é um múltiplo comum de a e b. Como uma aplicação do teorema anterior e com o conceito de divisor propriamente definido, podemos demonstrar que:

Lema 2.24. *Dados $a, b \in \mathbb{N}$, temos que* $\mathrm{mmc}(a, b)$ *divide $a \cdot b$.*

Demonstração: Podemos demonstrar algo ainda mais forte: se $m := \mathrm{mmc}(a, b)$ e M é qualquer múltiplo comum de a e b (em particular se $M = a \cdot b$), então m divide M. De fato, como $m \leqslant M$, apliquemos o teorema anterior para obtermos $q, r \in \mathbb{N}$ com $0 \leqslant r < m$ tais que

$$M = m \cdot q + r.$$

Já que M e m são ambos múltiplos de a, segue que $r = M - m \cdot q \in \mathbb{N}$ também o é. Com o mesmo argumento temos que r é um múltiplo de b. Segue que r é um múltiplo comum de a e b. Mas, como $0 \leqslant r < m$, e $m = \mathrm{mmc}(a, b)$, segue que $r = 0$, isto é, m divide M. ∎

Definição 2.25. Dados dois números naturais a e b, dizemos que $d \in \mathbb{N}$ é o **máximo divisor comum** entre a e b, e escrevemos $d = \mathrm{mdc}(a, b)$, se:

(i) d é um divisor comum de a e b, isto é, d é divisor tanto de a quanto de b;

(ii) d é o maior dos divisores comuns, no sentido de que se d' é um divisor de a e b então $d' \leqslant d$.

Observação 2.26. $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, a)$.

Teorema 2.27. *Se d é o máximo divisor comum de a e b, então existem $n, m \in \mathbb{N}$ tais que $d = n \cdot a + m \cdot b$.*

Demonstração: É um caso particular do Teorema 2.59, demonstrado abaixo (veja Observação 2.60). ∎

Existem algumas regras para saber se um número é divisível por $2, 3, 4, 5, 6, 7, 8, 9, 10$ e 11, por exemplo, que auxilia na determinação de todos os divisores de um número. Estas regras explicitam os *Critérios de Divisibilidade* de um determinado número.

- Divisibilidade por 2.

  Proposição 2.28. *Todo número natural terminado em* $0, 2, 4, 6$ *ou* 8*, é divisível por* 2.

Demonstração: Na base decimal, escrevamos $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$. Devemos demonstrar que se a_0 é par, então a é par. Suponha, então, $a_0 = 2 \cdot b_0$. Temos

$$a = 10(a_n \cdot 10^{n-1} + \cdots + a_1) + 2 \cdot b_0,$$

donde $a = 2 \cdot (5(a_n \cdot 10^{n-1} + \cdots + a_1) + b_0)$, isto é, a é divisível por 2. ∎

- Divisibilidade por 3.

Proposição 2.29. *Se a soma dos algarismos de um número tem como resultado um múltiplo de* 3*, então ele é divisível por* 3*.*

Demonstração: Novamente, escrevamos $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$. Devemos demonstrar que se $a_0 + a_1 + \cdots + a_n$ é divisível por 3, então a é divisível por 3. Suponha, então, $a_0 + a_1 + \cdots + a_n = 3 \cdot k$. Temos então

$$a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + (3 \cdot k - a_1 - \cdots - a_n),$$

donde concluímos que

$$a = a_n \cdot (10^n - 1) + \cdots + a_1 \cdot (10 - 1) + 3 \cdot k.$$

Agora, afirmamos que $(10^n - 1)$ é divisível por 9 para todo $n \in \mathbb{N} \backslash \{0\}$. Podemos demonstrar isso usando o Princípio da Indução Finita. Como $10 - 1 = 9$, tal afirmação é válida para $n = 1$. Assumindo que

$$10^n - 1 = 9 \cdot u$$

para algum $u \in \mathbb{N}$, temos que

$$10^{n+1} - 1 = 10^{n+1} + 9 - 10 = 10(10^n - 1) + 9,$$

donde conclui-se que $10^{n+1} - 1 = 9(10 \cdot u + 1)$ é divisível por 9, demonstrando a afirmação. Agora, se $b = 9 \cdot c$, então $b = 3 \cdot (3 \cdot c)$, logo ser divisível por 9 implica ser divisível por 3. Segue, então, que

$$a = a_n \cdot (10^n - 1) + \cdots + a_1 \cdot (10 - 1) + 3 \cdot k$$

é divisível por 3, pois todos os termos dessa soma são divisíveis por 3. ∎

- Divisibilidade por 4.

Proposição 2.30. *Todo número cujos dois últimos algarismos formarem, na mesma ordem, um número múltiplo de* 4*, é divisível por* 4*.*

Demonstração: Primeiro, note que 10^n é divisível por 4, para todo $n \geqslant 2$. De fato, se $n \geqslant 2$, existe $m \in \mathbb{N}$ tal que $n = 2 + m$, e então,

$$10^n = 10^2 \cdot 10^m = 4 \cdot (25 \cdot 10^m),$$

donde segue que 4 divide 10^n. Dito isso, se $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$ e 4 divide $(a_1 \cdot 10 + a_0)$, pela afirmação acima segue que 4 divide todos os números naturais

$$a_n \cdot 10^n, \ldots, a_2 \cdot 10^2, (a_1 \cdot 10 + a_0),$$

donde conclui-se que que 4 divide a. ■

- Divisibilidade por 5.

Proposição 2.31. *Todo número que tenha* 0 *ou* 5 *como algarismo da unidade é um número divisível por* 5.

Demonstração: Escrevamos $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$. Se $a_0 = 0$, temos $a = 5 \cdot (2(a_n \cdot 10^{n-1} + \cdots + a_1))$. Se $a_0 = 5$, temos $a = 5 \cdot (2(a_n \cdot 10^{n-1} + \cdots + a_1) + 1)$. Em ambos os casos, a é divisível por 5. ■

- Divisibilidade por 6.

Proposição 2.32. *Se um número é terminado em* $0, 2, 4, 6$ *ou* 8 *e a soma de seus algarismos é divisível por* 3, *então ele é divisível por* 6.

Demonstração: Dos critérios já enunciados, devemos demonstrar que se a um número divisível ao mesmo tempo por 2 e por 3, então ele é divisível por 6. Aplicando o Teorema 2.23, escrevemos $a = 6q + r$, com $0 \leqslant r < 6$. Por outro lado, como 2 divide a, temos $a = 2b$ e então

$$r = 2b - 6q = 2(b - 3q),$$

donde r é divisível por 2. Analogamente, demonstramos que r é divisível por 3. Mas, é fácil verificar que o único número natural r no intervalo $[0, 6)$ que é, ao mesmo tempo, múltiplo de 2 e de 3 é o zero, donde segue o resultado. ■

- Divisibilidade por 7.

Proposição 2.33. *Um número é divisível por* 7 *se e somente se o dobro do último algarismo, subtraído do número sem o último algarismo, for um número múltiplo de* 7.

Demonstração: Escreva $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$, com $0 \leqslant a_i < 10$. Devemos demonstrar que $7 \mid a$ se, e somente se

$$7 \mid [(a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) - 2a_0]. \tag{2.1}$$

Por um lado, se $7 \mid a$, então existe q tal que $a = 7q$ e portanto

$$-2a_0 = 2(a_n \cdot 10^n + \cdots + a_1 \cdot 10) - 2 \cdot 7q. \tag{2.2}$$

Usando (2.2), temos

$$\begin{aligned}(a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) - 2a_0 &= 21(a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) - 14q \\ &= 7(3(a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) - 2q),\end{aligned}$$

donde concluímos que $7 \mid [(a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) - 2a_0]$. Reciprocamente, assumindo (2.1), escreva $(a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) - 2a_0 = 7q$. Multiplicando ambos os lados por 10 obtemos que

$$\begin{aligned}70q &= (a_n \cdot 10^n + \cdots + a_1 \cdot 10) - 20a_0 \\ &= (a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0) - 21a_0 \\ &= a - 21a_0,\end{aligned}$$

donde concluímos que $a = 7(10q + 3a_0)$, isto é, $7 \mid a$. ■

- Divisibilidade por 8.

Proposição 2.34. *Todo número cujos* 3 *últimos algarismos formarem, na mesma ordem, um número múltiplo de* 8*, é um número divisível por* 8*.*

Demonstração: A prova é similar ao critério de divisibilidade por 4. Note 10^n é divisível por 8, para todo $n \geqslant 3$. De fato, se $n \geqslant 3$, existe $m \in \mathbb{N}$ tal que $n = 3 + m$, e então,

$$10^n = 10^3 \cdot 10^m = 8 \cdot (125 \cdot 10^m),$$

donde segue que 8 divide 10^n. Dito isso, se $a = a_n \cdot 10^n + \cdots + a_2 \cdot 100 + a_1 \cdot 10 + a_0$ e 8 divide $(a_2 \cdot 100 + a_1 \cdot 10 + a_0)$, pela afirmação acima segue que 8 divide todos os fatores

$$a_n \cdot 10^n, \ldots, a_3 \cdot 10^3, (a_2 \cdot 100 + a_1 \cdot 10 + a_0),$$

donde conclui-se que 8 divide a. ■

- Divisibilidade por 9.

Proposição 2.35. *Um número é divisível por* 9*, se a soma dos seus algarismos ter como resultado um número múltiplo de* 9*.*

Demonstração: Esta prova é análoga ao Critério de divisibilidade por 3. ■

- Divisibilidade por 10.

Proposição 2.36. *Todo número que tenha* 0 *como algarismo da unidade é um número divisível por* 10*.*

Demonstração: Se $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$ e $a_0 = 0$, temos $a = 10 \cdot (a_n \cdot 10^{n-1} + \cdots + a_1)$, donde segue o resultado. ■

- Divisibilidade por 11.

Proposição 2.37. *Um número é divisível por* 11 *se e somente se a soma dos algarismos de ordem par (Dezena, Unidade de Milhar, etc.) menos a soma dos algarismos de ordem ímpar (Unidade, Centena, etc.) for um número múltiplo de* 11*.*

Demonstração: Primeiro, demonstraremos o seguinte resultado auxiliar: para todo natural $n \geqslant 1$, 10^n é da forma $11q + (-1)^n$. De fato, a prova será por indução. Para $n = 1$ isto é claro, com $q = 1$. Supondo válido para $n = k > 1$, devemos demonstrar para $n = k + 1$. Mas:

$$\begin{aligned} 10^{k+1} &= 10^k \cdot 10 \\ &= (11q + (-1)^k) \cdot 10 \\ &= 11q \cdot 10 + (-1)^k \cdot (11 - 1) \\ &= 11(10q + (-1)^k) + (-1)^{k+1} \\ &= 11q' + (-1)^{k+1}, \end{aligned}$$

como queríamos. Agora, escreva $a = a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0$, com $0 \leqslant a_i < 10$. Pelo resultado auxiliar que acabamos de demonstrar segue que podemos escrever

$$\begin{aligned} a &= a_n \cdot (11q_n + (-1)^n) + \cdots + a_1 \cdot (11q_1 + (-1)) + a_0 \\ &= 11(a_n \cdot q_n + \cdots + a_1 \cdot q_1) + (a_0 - a_1 + \cdots + (-1)^n a_n). \end{aligned}$$

Ponha $q := a_n \cdot q_n + \cdots + a_1 \cdot q_1$ e $r := a_0 - a_1 + \cdots + (-1)^n a_n$. Segue que $a = 11q + r$ e portanto a é divisível por 11 se, e somente se, $11|r$, provando a proposição. ■

Nem sempre descrever o conjunto de todos os divisores de cada número e depois comparar os conjuntos (por meio da análise de sua intersecção), é algo eficiente. Por exemplo, ao comparar dois números muito extensos, a utilização desse método fica praticamente inviável pois sua resolução demandaria uma boa quantidade de horas.

Euclides, no século III a.C., descreveu um algoritmo para facilitar o encontro do mdc entre dois números naturais.

O **Algoritmo ou Lema de Euclides**, como é conhecido o método por ele desenvolvido, consiste em: dados dois números naturais a e b, os divisores comuns desses dois são os mesmos divisores comuns de a e $(b - a \cdot c)$, sendo c um número natural fixo.

Se considerarmos o maior entre os divisores comuns do algoritmo acima, obtemos a fórmula:

$$\operatorname{mdc}(a, b) = \operatorname{mdc}(a, (b - a \cdot c)).$$

Exemplo 2.38. Calcular o $\operatorname{mdc}(a, b)$, para $a = 49$ e $b = 210$. Para isso é necessário encontrar um múltiplo de 49, mais próximo de 210. Observando o conjunto dos múltiplos de 49, $M(49) = \{0, 49, 98, 147, 196, 245, \ldots\}$, percebemos que,

$$210 = (4 \cdot 49) + 14.$$

Agora utilizando o Algoritmo de Euclides para encontrar o $\operatorname{mdc}(49, 210)$:

$$\operatorname{mdc}(49, 210) = \operatorname{mdc}(49, 210 - 4 \cdot 49) = \operatorname{mdc}(49, 14).$$

Aplicando o mesmo processo ao par $a_1 = 49$ e $b_1 = 14$ e assim sucessivamente, tem-se:

$$\operatorname{mdc}(49, 14) = \operatorname{mdc}(49 - 3 \cdot 14, 14) = \operatorname{mdc}(7, 14),$$

$$\operatorname{mdc}(7, 14) = \operatorname{mdc}(7, 14 - 2 \cdot 7) = \operatorname{mdc}(7, 0) = 7.$$

Logo, $\operatorname{mdc}(49, 210) = 7$.

Observação 2.39. Esse algoritmo também pode ser estendido para números inteiros.

Os conceitos de mmc e mdc se relacionam da seguinte maneira:

Lema 2.40. *Dados $a, b \in \mathbb{N}$, então $a \cdot b = \operatorname{mmc}(a, b) \cdot \operatorname{mdc}(a, b)$.*

Demonstração: Note que $m := (a \cdot b)/\operatorname{mdc}(a, b) = a \cdot (b/\operatorname{mdc}(a, b)) = (a/\operatorname{mdc}(a, b)) \cdot b \in \mathbb{N}$ é um múltiplo comum de a e b, donde $\operatorname{mmc}(a, b) \leqslant m$, isto é

$$\operatorname{mmc}(a, b) \cdot \operatorname{mdc}(a, b) \leqslant a \cdot b.$$

Por outro lado, seja $d := (a \cdot b)/\operatorname{mmc}(a,b)$. Pelo Lema 2.24, segue que $d \in \mathbb{N}$. Mais ainda, temos

$$a = d \cdot \left(\frac{\operatorname{mmc}(a,b)}{b}\right) \quad \text{e} \quad b = d \cdot \left(\frac{\operatorname{mmc}(a,b)}{a}\right),$$

portanto d é um divisor comum de a e b, donde segue que $d \leqslant \operatorname{mdc}(a,b)$, isto é

$$a \cdot b \leqslant \operatorname{mdc}(a,b) \cdot \operatorname{mmc}(a,b).$$

Concluímos que $a \cdot b = \operatorname{mdc}(a,b) \cdot \operatorname{mmc}(a,b)$, como queríamos demonstrar. ■

2.2 Os Conceitos de mmc e mdc no Conjunto dos Números Inteiros.

O conjunto dos números inteiros surgiram da necessidade de se operar $(b - a)$ quando $b < a$. Diante deste contexto, os matemáticos ampliaram o conjunto dos naturais a fim de se preservar a validade de $(b - a)$, independentemente da posição dos elementos a e b. O conjunto dos números inteiros ($\mathbb{Z}$) é constituído por números ditos positivos, negativos e 0.

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

Os números negativos, são os números colocados à esquerda do zero e os positivos são os que estão à direita do zero, sendo este número considerado como neutro, nem negativo, nem positivo.

Como o zero é neutro, os pares de números que estão a uma mesma distância deste, sendo um a esquerda e um a direita, são denominados **números simétricos**, ou mais especificamente, **números opostos**.

Exemplo 2.41. (-1) e $(+1)$, (-5) e $(+5)$, (-20) e $(+20)$, são pares de números opostos.

O oposto de um número a, será representado por $-a$, sendo a negativo ou positivo. Dessa representação, podemos concluir que: $-(-a) = a$ (o oposto do oposto de um número é o próprio número). Ademais, dado um número inteiro não-nulo a, denotamos por $|a|$, dito **valor absoluto de** a, ao elemento positivo dentre o par de números opostos $\{a, -a\}$. Definimos $|0| = 0$.

Em $\mathbb{Z}$ as operações são definidas do seguinte modo:

Definição 2.42. Para quaisquer dois números inteiros a e b, a **adição de** a **por** b, $a + b$ é definida como sendo o deslocamento de a, b unidades para a direita se $b \geqslant 0$ ou b unidades para a esquerda se $b < 0$.

Todas as propriedades da adição no conjunto dos números naturais, também são válidas para este conjunto, não havendo necessidade de elencá-las novamente.

Definição 2.43. Para quaisquer dois números inteiros a e b, a **subtração de** a **por** b, $b - a$ é definida como sendo o deslocamento de b, a unidades para a esquerda se $a > 0$, ou a unidades para a direita se $a < 0$.

Portanto concluímos que a subtração é a operação inversa da adição.

$$b - a = b + (-a).$$

Definição 2.44. Sejam a e b números inteiros. Se ambos forem positivos, a **multiplicação de** a **por** b, $a \cdot b$ é definida como o deslocamento de a unidades para a direita, repetindo-se b vezes esse procedimento. Por outro lado, utilizando

$$(-a) \cdot b = a \cdot (-b) = -(a \cdot b),$$

$$(-a) \cdot (-b) = -((-a) \cdot b) = -(-(a \cdot b)) = a \cdot b.$$

definimos $a \cdot b$ para quaisquer $a, b \in \mathbb{Z}$.

Todas as propriedades da multiplicação no conjunto dos números naturais continuam sendo válidas também no conjunto dos números inteiros.

A multiplicação é compatível com a ordem, somente para: dados a, b e c números inteiros e $c > 0$, temos: se $a < b$, então $a \cdot c < b \cdot c$.

O conjunto dos **múltiplos** de um número inteiro qualquer a é definido por:

$$M(a) = \{a \cdot b \colon b \in \mathbb{Z}\}.$$

Proposição 2.45. *Sejam $a, m, m' \in \mathbb{Z}$. Então:*

i) 0 é múltiplo de a.

ii) Se m é múltiplo de a, então $-m$ é múltiplo também de a.

iii) Um múltiplo de um múltiplo de a é também um múltiplo de a.

iv) Se m e m' são múltiplos de a, então $m + m'$ e $m - m'$ também são múltiplos de a.

v) Se m e m' são múltiplos de a, então $f \cdot m + g \cdot m'$ também é múltiplo de a, para quaisquer $f, g \in \mathbb{Z}$.

vi) Se $m + m'$ e $m - m'$ são múltiplos de a, então não necessariamente temos que m e m' também são múltiplos de a.

Demonstração:

i) Para ser múltiplo, deve haver um número $c \in \mathbb{Z}$ tal que $0 = c \cdot a$. Como $0 = 0 \cdot a$, segue que 0 é múltiplo de a.

ii) Sendo m um múltiplo de a, existe $c \in \mathbb{Z}$ tal que $m = c \cdot a$. Como $-m = (-1) \cdot m = (-1) \cdot c \cdot a = (-c) \cdot a$, segue que $-m$ também é múltiplo de a.

iii) Seja k um múltiplo de a e l um múltiplo de k. Logo, existem $c, d \in \mathbb{Z}$ tais que $k = c \cdot a$ e $l = d \cdot k$, donde concluímos que $l = d \cdot c \cdot a = (c \cdot d) \cdot a$, isto é, l é um múltiplo de a.

iv) Sendo múltiplos de a , m e m' podem ser escritos como $m = c \cdot a$ e $m' = c' \cdot a$, com $c, c' \in \mathbb{Z}$. Logo $m + m' = c \cdot a + c' \cdot a = (c + c') \cdot a$ e $m - m' = (c - c') \cdot a$. Portanto, ambos são múltiplos de a.

v) Analogamente ao item anterior, $m = c \cdot a$ e $m' = c' \cdot a$, com $c, c' \in \mathbb{Z}$. Logo, quaisquer que sejam $f, g \in \mathbb{Z}$, temos

$$f \cdot m + g \cdot m' = f \cdot c \cdot a + g \cdot c' \cdot a = (f \cdot c + g \cdot c') \cdot a,$$

donde segue o resultado.

vi) De fato, ponha $m = 5, m' = 1$ e $a = 2$. Temos:

$$m + m' = 5 + 1 = 6 = 3 \cdot 2$$

$$m - m' = 5 - 1 = 4 = 2 \cdot 2.$$

Mas, nem $m = 5$, nem $m' = 1$, são múltiplos de 2.

Isso encerra a demonstração. ■

Os múltiplos comuns de a e b, são todos os elementos que pertencem a $M(a)$ e $M(b)$ ao mesmo tempo.

Proposição 2.46. *Sejam $a, b, m, m' \in \mathbb{Z}$. Então:*

i) 0 é múltiplo comum de a e b.

ii) Se m é múltiplo comum de a e b, então $-m$ também é múltiplo comum de a e b.

iii) Um múltiplo de um múltiplo comum de a e b é também um múltiplo comum de a e b.

iv) Se m e m' são múltiplos comuns de a e b, então $m + m'$ e $m - m'$ também são múltiplos comuns de a e b.

v) Se m e m' são múltiplos comuns de a e b, então $f \cdot m + g \cdot m'$ também é múltiplo comum de a e b, para quaisquer $f, g \in \mathbb{Z}$.

vi) Se $m+m'$ e $m-m'$ são múltiplos comuns de a e b, então não necessariamente temos que m e m' também são múltiplos comuns de a e b.

Demonstração: Segue direto da proposição anterior. ∎

Será descrita agora como ficam caracterizadas as definições de mmc, divisores e mdc em $\mathbb{Z}$.

Definição 2.47. Sejam $a, b \in \mathbb{Z}$. Dizemos que $m \in \mathbb{N}$ é o **menor múltiplo comum** de a e b, e escrevemos $m = \text{mmc}(a, b)$ se:

(i) $m \neq 0$ e m é um múltiplo comum de a e b;

(ii) m é o menor dos múltiplos comuns, no sentido que se $m' \in \mathbb{N}$, $m' \neq 0$, é um múltiplo de a e de b, então $m' \geqslant m$.

Definição 2.48. Diz-se que um número inteiro d é **divisor** de um outro número inteiro a, se a for múltiplo de d, ou seja, $a = d \cdot b$, sendo b um número também inteiro. Quando um número inteiro a é múltiplo de outro inteiro d, diz-se que a **é divisível por** d, ou ainda que d **divide** a, esta última relação representada por $d \mid a$. Se d não dividir a, representa-se por $d \nmid a$.

O conjunto de todos os divisores de um número inteiro a é um conjunto finito denotado por

$$D(a) = \{d \in \mathbb{Z} \colon d \mid a\}.$$

Da definição acima decorrem as seguintes proposições:

Proposição 2.49. *Se $a, b, c \in \mathbb{Z}$, $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração: Como $a \mid b$ e $b \mid c$, existem inteiros n_1 e n_2 com $b = n_1 \cdot a$ e $c = n_2 \cdot b$. Substituindo o valor de b na equação $c = n_2 \cdot b$ tem-se $c = n_2 \cdot n_1 \cdot a$ o que implica $a \mid c$. ∎

Exemplo 2.50. Como $4 \mid 12$ e $12 \mid 60$, então $4 \mid 60$.

Proposição 2.51. *Se $a, b, c, m, n \in \mathbb{Z}$, $c \mid a$ e $c \mid b$, então $c \mid (m \cdot a + n \cdot b)$.*

Demonstração: Se $c \mid a$ e $c \mid b$ então $a = n_1 \cdot c$ e $b = n_2 \cdot c$. Multiplicando as duas equações por m e n, respectivamente, tem-se $m \cdot a = m \cdot n_1 \cdot c$ e $n \cdot b = n \cdot n_2 \cdot c$. Somando membro a membro obtém-se $m \cdot a + n \cdot b = m \cdot n_1 \cdot c + n \cdot n_2 \cdot c$, o que equivale a $m \cdot a + n \cdot b = (m \cdot n_1 + n \cdot n_2) \cdot c$, que significa que $c \mid (m \cdot a + n \cdot b)$. ∎

Proposição 2.52. *Sejam $n, d, a \in \mathbb{Z}$. Então:*

1. $n \mid n$,
2. $d \mid n$ *então* $a \cdot d \mid a \cdot n$,
3. $a \cdot d \mid a \cdot n$ *e* $a \neq 0$ *então* $d \mid n$,
4. $1 \mid n$,
5. $n \mid 0$, *pois zero é múltiplo de todos os números*,
6. $d \mid n$ *e* $n \neq 0$ *então* $|d| \leqslant |n|$,
7. $d \mid n$ *e* $n \mid d$ *então* $|d| = |n|$,
8. $d \mid n$ *e* $d \neq 0$ *então* $(n/d) \mid n$,
9. $d \mid a$ *então* $d \mid -a$, $-d \mid a$ *e* $d \mid -a$.

Demonstração: A demonstração desta proposição será omitida pois ela é similar à demonstração da Proposição 2.21. ∎

Definição 2.53. Sejam $a, b, d \in \mathbb{Z}$. O número d é dito um **divisor comum** de a e b se $d \mid a$ e $d \mid b$.

O conjunto de todos os divisores comuns dos números inteiros a e b é um conjunto finito.

Proposição 2.54. *Sejam $a, b, d \in \mathbb{Z}$. Então:*

i) *Se* $d \mid a$ *e* $d \mid b$, *então* $d \mid (b + a)$ *e* $d \mid (b - a)$.

ii) *Se* $d \mid (b + a)$ *ou* $d \mid (b - a)$ *e* $d \mid a$, *então* $d \mid b$.

Demonstração:

i) Sendo a divisível por d, $a = c \cdot d$, com $c \in \mathbb{Z}$. Analogamente $b = c' \cdot d$ com $c' \in \mathbb{Z}$. Logo, $b + a = c' \cdot d + c \cdot d = (c' + c) \cdot d$ e $b - a = (c' - c) \cdot d$. Portanto, existe um número pertencente aos inteiros tal que este multiplicado por d seja $b + a$ assim como existe um número pertencente aos inteiros tal que multiplicado por d seja $b - a$.

ii) Supondo que b não seja divisível por d, então podemos escrever $b = q \cdot d + r$ com $0 < r < d$. Sendo a divisível por d, podemos escrever $a = q' \cdot d$ com $q' \in \mathbb{Z}$. Assim temos que:
$$b + a = q \cdot d + r + q' \cdot d = (q' + q) \cdot d + r,$$
$$b - a = q \cdot d + r - q' \cdot d = (q' - q) \cdot d + r.$$
Sendo $b + a$ ou $b - a$ divisível por d, conclui-se que $r = 0$ ou $r = d$, e ambos os casos são absurdos, logo a suposição de que b não é divisível por d é absurda. Portanto b é divisível por d.

Isso encerra a demonstração. ∎

Definição 2.55. Sejam $a, b \in \mathbb{Z}$. Dizemos que $d \in \mathbb{N}$ é o **máximo divisor comum** entre a e b e escrevemos $d = \mathrm{mdc}(a, b)$ se

(i) d é um divisor comum de a e b;

(ii) d é o maior dos divisores comuns, no sentido que se $d' \in \mathbb{N}$ é um divisor de a e de b, então $d' \leqslant d$.

Observação 2.56. $\mathrm{mdc}(a, b) = \mathrm{mdc}(b, a)$.

Proposição 2.57. *Sejam $a, b \in \mathbb{Z}$. Então:*

i) Não existe $\mathrm{mdc}(0, 0)$.

ii) $\mathrm{mdc}(0, b) = b$, *se* $b > 0$ *e* $\mathrm{mdc}(0, b) = -b$, *se* $b < 0$.

iii) Se a e b, são números inteiros e não nulos, então:
$$\mathrm{mdc}(a, b) = \mathrm{mdc}(-a, b) = \mathrm{mdc}(a, -b) = \mathrm{mdc}(-a, -b).$$

Demonstração:

i) De fato, suponha que exista $d \in \mathbb{N}$ satisfazendo as propriedades (i) e (ii) da Definição 2.55. No entanto, $d' = d + 1 > d$ e satisfaz $d' \mid 0$, contradizendo o item (ii) da definição. Logo, tal d não existe.

ii) Suponha $b > 0$. Claramente b divide b e b divide 0. Se $d \in \mathbb{N}$ e divide b, então $d \leqslant b$ e como qualquer número natural divide 0, segue que $b = \mathrm{mdc}(0, b)$. Se $b < 0$, então $-b \in \mathbb{N}$, divide b e divide 0. Se $d \in \mathbb{N}$ divide b, então d também divide $-b$, logo $d \leqslant -b$, donde concluímos o resultado.

iii) Observe que se $c \in \mathbb{Z}$, temos que se $d' \in \mathbb{N}$ divide c, então $d' \mid (-c)$. Dito isso, segue que se $d \in \mathbb{N}$ é um divisor comum de a e b, então d divide tanto $u \cdot a$ quanto $v \cdot b$, quaisquer que sejam $u, v \in \{-1, 1\}$. Essa observação implica o resultado.

■

Proposição 2.58. *Sejam* $a, b, n \in \mathbb{Z}$*, com* $n \neq 0$*. Então* $\operatorname{mdc}(n \cdot a, n \cdot b) = |n| \operatorname{mdc}(a, b)$ *e* $\operatorname{mmc}(n \cdot a, n \cdot b) = |n| \operatorname{mmc}(a, b)$*.*

Demonstração: Podemos assumir que a, b, n são números naturais. Escreva $d = \operatorname{mdc}(a, b)$ e $m = \operatorname{mmc}(a, b)$. Note que $m' = n \cdot m$ é um múltiplo comum de $n \cdot a$ e $n \cdot b$. Dado um outro múltiplo comum u, existem $x, y \in \mathbb{N}$ tais que $x \cdot n \cdot a = u = y \cdot n \cdot b$, donde u/n é um múltiplo comum de a e b, e, portanto, $u/n \geqslant m$, donde $u \geqslant m'$ e concluímos que $m' = \operatorname{mmc}(n \cdot a, n \cdot b)$. Logo, usando o Lema 2.40, temos que

$$\operatorname{mdc}(n \cdot a, n \cdot b) = \frac{(n \cdot a) \cdot (n \cdot b)}{\operatorname{mmc}(n \cdot a, n \cdot b)} = \frac{n \cdot n \cdot d \cdot m}{n \cdot m} = n \cdot d,$$

concluindo a demonstração. ■

O Algoritmo de Euclides, definido no conjunto dos números naturais e que pode ser estendido aos números inteiros, conduz ao seguinte teorema (ver Teorema 2.27):

Teorema 2.59 (Relação de Bézout)**.** *Dados inteiros* a *e* b*, quaisquer, mas não ambos nulos, existem* $n, m \in \mathbb{Z}$*, tais que:*

$$\operatorname{mdc}(a, b) = a \cdot n + b \cdot m.$$

Demonstração: Considere o conjunto não vazio $C = \{a \cdot m + b \cdot n \ : \ m, n \in \mathbb{Z}\} \cap \mathbb{N}$. Como $\mathbb{N}$ é um conjunto bem ordenado (Teorema 2.9), existe $c = a \cdot m_0 + b \cdot n_0 \in C$ tal que $c \leqslant c'$, para qualquer $c' \in C$.

Se $d = \operatorname{mdc}(a, b)$ sabe-se que $d \mid a$ e $d \mid b$, e, portanto, $d \mid c$. Por outro lado, apliquemos o algoritmo da divisão (Teorema 2.23) para obter $a = c \cdot q + r$, com $0 \leqslant r < c$. Como $r = a - c \cdot q = a \cdot (1 - m_0 \cdot q) + b \cdot (-n_0 \cdot q) \in C$, segue que $r = 0$, pelo fato de c ser um elemento minimal de C. Logo, $c \mid a$. Analogamente, $c \mid b$, donde concluímos que $c \mid d$, pois $d = \operatorname{mdc}(a, b)$. Logo, $c = d$. ■

Observação 2.60. Dados $a, b \in \mathbb{Z}$, sejam $m_0, n_0 \in \mathbb{Z}$ tais que $d = a \cdot m_0 + b \cdot n_0$. Para qualquer solução não trivial da equação $a \cdot x + b \cdot y = 0$ tem-se, então, que para qualquer $u \in \mathbb{Z}$

$$d = d + 0 = d + u \cdot 0 = a \cdot (m_0 + u \cdot x) + b \cdot (n_0 + u \cdot y).$$

Logo, existem infinitas soluções para a equação $\operatorname{mdc}(a, b) = a \cdot m + b \cdot n$. Em particular, podemos escolher $m, n \in \mathbb{N}$.

Esse teorema gera a seguinte propriedade: se d é um divisor comum de dois números inteiros a e b, não simultaneamente nulos, então d divide $\text{mdc}(a, b)$.

Uma maneira bastante comum de calcular o mmc e o mdc de dois números é por meio da decomposição dos números em primos. Para entender esse método é necessário conhecer o conceito de números primos e que, todo número natural maior ou igual a 2, ou é primo ou é formado pela multiplicação de números primos.

Definição 2.61. Um número inteiro positivo é chamado de **número primo**, se ele tiver somente dois elementos no conjunto de seus divisores positivos, o número 1 e o próprio número.

Definição 2.62. Se um número tiver três ou mais elementos em seu conjunto de divisores naturais, esse número será chamado de **número composto**.

Proposição 2.63. *Todo número natural $a > 1$, ou é primo, ou se escreve como produto de primos.*

Demonstração: demonstraremos por indução. Seja $P(n)$ a propriedade n é primo ou n se escreve como um produto de números primos. Como 2 é primo, $P(2)$ é válida. Assuma que $P(m)$ é válida para todo $2 \leqslant m < n$. Devemos mostrar que $P(n)$ é válida. Se n for um número primo, nada temos a mostrar. Se n não for um número primo, existe, por definição, $d \in \mathbb{N}$ um divisor de n distinto de 1 e n. Como d e n/d são menores que n, $P(d)$ e $P(n/d)$ são válidas, e como

$$n = d \cdot (n/d),$$

segue que n se escreve como um produto de números primos. ∎

Observação 2.64. O conjunto dos números primos é um conjunto infinito e também subconjunto dos números naturais. Para encontrar os primeiros números desse conjunto, a melhor maneira é utilizando o Crivo de Eratóstenes, criado pelo matemático que dá nome ao crivo. Esse método consiste em peneirar os números naturais maiores que 2 e menores que n, também natural, eliminando os números que não são primos, ou seja, eliminando os múltiplos desses primos.

Exemplo 2.65. Consideremos um crivo a ser construído para $n = 100$.

$$\begin{array}{cccccccccc}
 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\
21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \\
31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 & 40 \\
\vdots & & & & & & & & & \\
91 & 92 & 93 & 94 & 95 & 96 & 97 & 98 & 99 & 100
\end{array}$$

O número 2 é o primeiro número primo, a partir dele elimina-se todos os seus múltiplos, ou seja, os números pares. Circulando o número 2.

Depois do 2, o próximo número ainda não eliminado é o 3, portanto ele é primo. Circula-se o 3 e elimina-se os números ímpares múltiplos de 3, pois os pares já foram eliminados.

Depois do 3, o próximo número ainda não eliminado é o 5, portanto ele é primo. Circula-se o 5 e elimina-se os números ímpares múltiplos de 5, ou seja os terminados em 5.

Seguindo essa regra serão encontrados os próximos números primos. Esse procedimento termina assim que chegarmos em um número primo p, para o qual $p^2 \geqslant n$.

1	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Figura 5 – Crivo de Eratóstenes

Portanto, ao fim da construção do Crivo de Eratóstenes, foram encontrados os números primos maiores que 2 e menores que 100:

$$P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97\}.$$

Observação 2.66. Uma vez definido o conceito de números primos e compostos, volta-se para o método que possibilita calcular o mdc de dois ou mais números mais facilmente. Primeiro verifica-se se os números em questão são primos ou compostos. Caso sejam todos primos, nada há para ser feito e o mdc entre eles será igual a 1.

Se um ou mais números forem compostos, deve-se fazer a decomposição em fatores primos, encontrando todos os fatores comuns entre todos os números. O mdc entre os números será igual ao produto desses fatores comuns.

Definição 2.67. Dois números inteiros a e b, serão chamados de **primos entre si**, se não houverem fatores primos comuns, isto é, se

$$\text{mdc}(a, b) = 1.$$

Exemplo 2.68. Para calcularmos o $\text{mdc}(a, b)$, para $a = 245$ e $b = 210$, decompomos os números a e b, assim: $a = 5 \cdot 7^2$ e $b = 2 \cdot 3 \cdot 5 \cdot 7$. Os fatores comuns entre a e b são o 5 e o

7, portanto

$$\text{mdc}(245, 210) = 5 \cdot 7 = 35.$$

Observação 2.69. O método usado no exemplo anterior também pode ser usado para calcular o mmc entre números inteiros.

A utilização da composição em fatores primos para o cálculo do mmc é realizado do seguinte modo: primeiro verificando se os números em questão são primos ou compostos. Caso forem todos primos, nada há para ser feito e o mmc entre eles será igual ao produto dos números.

Assim, o mmc de dois números primos p_1 e p_2 é o produto entre eles.

Se um ou mais números forem compostos, deve-se decompô-los em fatores primos a fim de encontrar os que são comuns. O mmc entre os números será o produto entre os fatores primos comuns e não comuns.

Exemplo 2.70. Para calcularmos o mmc(a, b), para $a = 245$ e $b = 210$, decompomos os números a e b, assim: $a = 5 \cdot 7^2$ e $b = 2 \cdot 3 \cdot 5 \cdot 7$. Os fatores comuns entre a e b são o 5 e o 7, portanto os não comuns são o 2, o 3 e o 7. Calculando o mmc temos:

$$\text{mmc}(245, 210) = 5 \cdot 7 \cdot 2 \cdot 3 \cdot 7 = 7350.$$

Normalmente o mmc e o mdc são ensinados para serem trabalhados, principalmente com números inteiros, mas eles podem também ser calculados para números não inteiros, números comensuráveis. Estudaremos em seguida o *mínimo múltiplo comum generalizado* (mmcg) e *máximo divisor comum generalizado* (mdcg), mas para isso é necessário o conceito de números reais comensuráveis.

2.3 Números Reais Comensuráveis

O conceito de comensurabilidade é um conceito muito antigo, visto como a relação existente entre dois segmentos de reta por meio da análise de seus tamanhos.

Definição 2.71. Diz-se 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.

Durante muito tempo, na Grécia Antiga, essa definição era uma verdade absoluta para todos os números. Mas, foi por volta de 450 a.C. a 400 a.C. que, descobriram que a relação entre a medida do lado de um quadrado com a medida da diagonal do mesmo (conforme já exposto), não eram medidas comensuráveis.

Foram muitos anos de discussões para resolver esse problema, o que levou a formulação precisa do problema da comensurabilidade em termos de medida de segmentos, culminando com a criação dos números reais absolutos.

Apesar de ter surgido por definições geométricas, o conceito de comensurabilidade é igualmente interpretado para quaisquer dois números reais.

Definição 2.72. Dois números reais r e s são **comensuráveis** se existem números inteiros não nulos m e n tais que

$$m \cdot r = n \cdot s.$$

Por essa definição chega-se à conclusão que:

1. Dois números racionais são sempre comensuráveis;
2. Dois irracionais podem ser comensuráveis;
3. Dois números reais quaisquer nem sempre serão comensuráveis. Tem-se o caso de um racional com um irracional, são sempre incomensuráveis. A maioria dos pares de números irracionais são incomensuráveis, basta pegar como exemplo $\sqrt{2}$ e $\sqrt{3}$.

Exemplo 2.73. Vamos mostrar que $\sqrt{2}$ e $\sqrt{3}$ não são comensuráveis. Suponhamos que existam dois números inteiros m e n tais que

$$m \cdot \sqrt{2} = n \cdot \sqrt{3}.$$

Elevando ambos os lados da igualdade ao quadrado obtemos $2m^2 = 3n^2$. Considerando a fatoração de um número em fatores primos, chega-se em um absurdo. De fato, mesmo que tanto m quanto n, tenham o número 2 em sua fatoração, teria então uma quantidade ímpar de fatores primos iguais a 2 para o primeiro membro da igualdade $(2m^2)$, enquanto que tería um número par de fatores primos iguais a 2 no segundo membro da igualdade $(3n^2)$.

Esse conceito de comensurabilidade nos números reais, gera uma extensão para a definição de múltiplo e divisor de um número.

Definição 2.74. Diz-se que um número real r é um **múltiplo inteiro** de um número real s, ou que s é um **divisor inteiro** de r, se existe $a \in \mathbb{Z}$ tal que $r = a \cdot s$.

Das definições anteriores decorre a seguinte proposição:

Proposição 2.75. *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.

Demonstração: $(a) \Rightarrow (b)$: Se r e s são comensuráveis então existem $m, n \in \mathbb{Z}$, não nulos, tais que $m \cdot r = n \cdot s$. Consequentemente $r/s = n/m \in \mathbb{Q}$.
$(b) \Rightarrow (c)$: Suponhamos que $r/s \in \mathbb{Q}$. Se $r/s = n/m$, então multiplicando ambos os membros dessa igualdade por $s \cdot m$ obtemos $t = m \cdot r = n \cdot s$ e portanto t é um múltiplo inteiro comum de r e s.
$(c) \Rightarrow (d)$: Seja $t \in \mathbb{R}$ um múltiplo inteiro comum de r e s. Se $t = m \cdot r = n \cdot s$, com m e n números inteiros não nulos, então o número

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

é um divisor inteiro e comum de r e s.
$(d) \Rightarrow (a)$: Seja u um divisor inteiro comum de r e s. Se $r = u \cdot m$ e $s = u \cdot m$, para m e n números inteiros e não nulos, então $m \cdot r = n \cdot s$. ∎

Da proposição anterior concluí-se as seguintes definições.

Definição 2.76. Sejam r e s dois números reais comensuráveis não nulos. Dizemos que t é o **mínimo múltiplo comum generalizado** entre r e s, e escrevemos $t = \mathrm{mmcg}(r, s)$, 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 $t \leqslant t'$.

Definição 2.77. Sejam r e s dois números reais comensuráveis não nulos. Dizemos que u é o **máximo divisor comum generalizado** entre r e s , e denotamos $u = \mathrm{mdcg}(r, s)$, se:

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

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

Será encontrado, agora, uma fórmula para calcular o mmcg e o mdcg para quaisquer dois números comensuráveis.

Teorema 2.78. *Sejam r e s dois reais comensuráveis não nulos. Então*

$$\mathrm{mmcg}(r, s) = |v \cdot r| = |u \cdot s|$$

$$\mathrm{mdcg}(r, s) = |r/u| = |s/v|$$

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

Demonstração: Analisando o teorema, primeiramente, para r e s positivos. Se $a, b, c, d \in \mathbb{Z}$ são tais que $a \cdot r = b \cdot s$ e $c \cdot r = d \cdot s$, então $b/a = d/c$, e estas frações são frações equivalentes de r/s.

Portanto, os menores números naturais a e b que satisfazem a igualdade $a \cdot r = b \cdot s$, são encontrados quando analisamos o numerador e o denominador da fração irredutível que representa o número racional r/s.

A partir daí, pela definição de mmcg e de mdcg, se u/v é a fração irredutível de r/s, então

$$\operatorname{mmcg}(r, s) = v \cdot s = u \cdot s \quad \text{e} \quad \operatorname{mdcg}(r, s) = r/u = s/v,$$

o que demonstra o teorema para r e s positivos. Caso r (ou s) sejam negativos, consideramos $(-r) > 0$ (ou $(-s) > 0$) e aplicamos a demonstração acima. Isso termina a demonstração do teorema. ∎

Se r e s forem números racionais, as fórmulas dadas no teorema serão reescritas da seguinte forma.

Corolário 2.79. *Sejam r e s dois números racionais não nulos e sejam $a, b, c, d \in \mathbb{Z}$ números inteiros tais que $r = a/b$ e $s = c/d$, sendo que a/b e c/d são frações irredutíveis. Então,*

$$\operatorname{mmcg}(r, s) = \operatorname{mmc}(a, c)/\operatorname{mdc}(b, d)$$

e

$$\operatorname{mdcg}(r, s) = \operatorname{mdc}(a, c)/\operatorname{mmc}(b, d).$$

Observação 2.80. No corolário precedente, é imprescindível, que as frações a/b e c/d sejam frações irredutíveis, pois caso contrário as fórmulas encontradas não irão calcular o mmcg e mdcg realmente de r e s.

Demonstração do Corolário 2.79: Demonstraremos o resultado apenas para números reais positivos. Como a/b e c/d são frações irredutíveis, então $\operatorname{mdc}(a, b) = 1 = \operatorname{mdc}(c, d)$. Portanto, temos

$$\frac{r}{s} = \frac{a/b}{c/d} = \frac{a \cdot d}{b \cdot c} = \frac{a' \cdot d'}{b' \cdot c'}$$

onde

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

Como a fração $a' \cdot d'/b' \cdot c'$ é uma fração irredutível, então, pelo Teorema 2.78

$$\operatorname{mmcg}(r,s) = r \cdot b' \cdot c' = \frac{a}{b} \cdot \frac{b}{\operatorname{mdc}(b,d)} \cdot \frac{c}{\operatorname{mdc}(a,c)} = \frac{a \cdot c}{\operatorname{mdc}(b,d) \cdot \operatorname{mdc}(a,c)}.$$

Pelo Lema 2.40, sabemos que $a \cdot c = \operatorname{mmc}(a,c) \cdot \operatorname{mdc}(a,c)$. Assim,

$$\frac{a \cdot c}{\operatorname{mdc}(b,d) \cdot \operatorname{mdc}(a,c)} = \frac{\operatorname{mmc}(a,c) \cdot \operatorname{mdc}(a,c)}{\operatorname{mdc}(b,d) \cdot \operatorname{mdc}(a,c)} = \frac{\operatorname{mmc}(a,c)}{\operatorname{mdc}(b,d)}.$$

Portanto, $\operatorname{mmcg}(r,s) = \operatorname{mmc}(a,c)/\operatorname{mdc}(b,d)$. Do mesmo modo,

$$\begin{aligned} \operatorname{mdcg}(r,s) &= \frac{r}{a' \cdot d'} = \frac{a}{b} \cdot \frac{\operatorname{mdc}(a,c)}{a} \cdot \frac{\operatorname{mdc}(b,d)}{d} \\ &= \frac{\operatorname{mdc}(a,c) \cdot \operatorname{mdc}(b,d)}{b \cdot d}. \end{aligned}$$

Novamente utilizando o Lema 2.40, sabemos que $b \cdot d = \operatorname{mmc}(b,d) \cdot \operatorname{mdc}(b,d)$. Continuando a demonstração tem-se:

$$\frac{\operatorname{mdc}(a,c) \cdot \operatorname{mdc}(b,d)}{b \cdot d} = \frac{\operatorname{mdc}(a,c) \cdot \operatorname{mdc}(b,d)}{\operatorname{mmc}(b,d) \cdot \operatorname{mdc}(b,d)} = \frac{\operatorname{mdc}(a,c)}{\operatorname{mmc}(b,d)}.$$

Portanto, $\operatorname{mdcg}(r,s) = \operatorname{mdc}(a,c)/\operatorname{mmc}(b,d)$. ■

Seguem algumas das propriedades de mmcg e mdcg.

Proposição 2.81. *Sejam r e s dois números reais comensuráveis e não nulos. Então:*

(i) $|r \cdot s| = \operatorname{mdcg}(r,s) \cdot \operatorname{mmcg}(r,s)$.

(ii) Para qualquer número real não nulo f, temos que $f \cdot r$ e $f \cdot s$ são comensuráveis e

$$\operatorname{mmcg}(f \cdot r, f \cdot s) = |f| \cdot \operatorname{mmcg}(r,s) \quad e \quad \operatorname{mdcg}(f \cdot r, f \cdot s) = |f| \cdot \operatorname{mdcg}(r,s).$$

Demonstração:

(i) Seja u/v a forma irredutível do número racional r/s. Do Teorema 2.78, segue que

$$\operatorname{mmcg}(r,s) \cdot \operatorname{mdcg}(r,s) = |v \cdot r| \cdot |s/v| = |r \cdot s|,$$

como queríamos.

(ii) A demonstração é similar à da Proposição 2.58. Mostremos que $\operatorname{mmcg}(f \cdot r, f \cdot s) = |f| \cdot \operatorname{mmcg}(r,s)$. Seja $m = \operatorname{mmcg}(r,s)$ e defina $m' = |f| \cdot m$. Note que $m' > 0$. Ademais, $m'/(f \cdot r) = (|f|/f) \cdot (m/r)$ é um número inteiro, pois m/r o é e $|f|/f \in \{-1, 1\}$. Concluímos que m' é múltiplo inteiro de $f \cdot r$, e analogamente de $f \cdot s$. Por fim, supondo que $t' > 0$ é outro múltiplo inteiro comum de $f \cdot r$ e $f \cdot s$, temos que $t'/|f|$ é um múltiplo inteiro tanto de r quanto de s. Segue da definição de mmcg(r, s) que $m \leqslant t'/|f|$, donde concluimos que $t' \geqslant m \cdot |f| = m'$. Isto é, $m' = \text{mmcg}(f \cdot r, f \cdot s)$. Por fim, utilizando o item anterior, obtemos

$$\text{mdcg}(f \cdot r, f \cdot s) = \frac{|f \cdot r| \cdot |f \cdot s|}{\text{mmcg}(f \cdot r, f \cdot s)} = \frac{|f|^2 \cdot |r \cdot s|}{|f| \cdot \text{mmcg}(r, s)} = |f| \cdot \text{mdcg}(r, s).$$

Isso conclui a demonstração. ■

Vejamos agora alguns exemplos.

Exemplo 2.82. Calcule o *mmcg* e *mdcg* para os valores comensuráveis $(2; 4)$.

- mmcg(2,4)

  Como $\frac{1}{2}$ é a forma irredutível de $\frac{2}{4}$, então:

$$mmcg(2, 4) = |1.4| = 4 = |2.2|$$

- mdcg(2,4)

  Como $\frac{1}{2}$ é a forma irredutível de $\frac{2}{4}$, então:

$$mdcg(2, 4) = |\frac{2}{1}| = 2 = |\frac{4}{2}|$$

Exemplo 2.83. Calcule o *mmcg* e *mdcg* para os valores incomensuráveis $(\frac{1}{3}; \frac{1}{5})$.

- $mmcg(\frac{1}{3}; \frac{1}{5})$

  Dados que: $a = 1, b = 3, c = 1, d = 5$ e $mmc(1, 1) = 1$ e $mdc(3, 5) = 1$, temos:

$$mmcg(\frac{1}{3}; \frac{1}{5}) = mmc(a, c)/mdc(b, d) = \frac{1}{1} = 1$$

- $mdcg(\frac{1}{3}; \frac{1}{5})$

  Dados que: $a = 1, b = 3, c = 1, d = 5$ e $mdc(1, 1) = 1$ e $mmc(3, 5) = 15$, temos:

$$mmcg(\frac{1}{3}; \frac{1}{5}) = mdc(a, c)/mmc(b, d) = \frac{1}{15}$$

Veremos, no próximo capítulo, como aplicamos as noções expostas aqui em sala de aula por meio de uma pedagogia ainda tradicional mas com aspectos lúdicos.

3 Aplicação do Projeto: mmc e mdc: Gostosura ou tortura?

"A matemática, vista corretamente, possui não apenas verdade, mas também suprema beleza - uma beleza fria e austera, como a da escultura."
(Bertrand Russell)

Neste capítulo expomos a estrutura curricular da disciplina de matemática no estado de São Paulo a fim de subsidiar os conteúdos e práticas que foram utilizadas na aplicação do projeto ao corpo discente do 8º ano do Ensino Fundamental e 3º ano do Ensino Médio. Em seguida, o próprio projeto é então apresentado.

3.1 Matemática para o Ensino Fundamental II e para o Ensino Médio

Na obra ([13], 2011) da Secretaria da Educação do Estado de São Paulo (SEESP), a matemática é evidenciada como um sistema primário de expressão, igualmente entendida como uma das línguas maternas, tal como a linguagem natural- o português-, com a qual interage continuamente. Dentre o rol de competências e habilidades que compõem o currículo básico dos ensinos fundamental e médio da educação paulista, a competência leitora e escritora são almejadas tanto em termos da linguagem natural quanto da artificial. Assim, a matemática também deve interagir com todas as formas de expressão, incluindo aqui as associadas às tecnologias e computação.

O foco principal, não só na matemática mas também de todas as disciplinas do currículo escolar, é a transformação da informação em conhecimento significativo. As informações estão cada vez mais numerosas e de fácil aquisição, mas estão disponíveis de forma desorganizada. Cabe ao professor um papel muito importante neste contexto, que seria o de auxiliar a transformação da informação exposta de modo desorganizado e descontextualizado em conhecimento significativo.

O Currículo da SEESP evidenciou que "um currículo tem a função de mapear os temas/conteúdos considerados relevantes, tendo em vista o tratamento da informação e a construção do conhecimento. As disciplinas têm um programa que estabelece os temas a serem estudados e que constituirão os meios para o desenvolvimento das competências pessoais" ([13], 2011, p. 36).

Para que a construção do conhecimento ocorra entre os discentes é essencial que identifiquemos em cada conteúdo a ser ministrado em sala de aula as ideias fundamentais que permeiam aquele assunto, para que possamos aplicá-las em outros contextos e disciplinas. Sabe-se que a lista de conteúdos disciplinares a serem estudados pelos alunos é bem extensa e fragmentada fazendo com que, muitas vezes, o conhecimento não ocorra de modo significativo. Por esta razão é importante a organização e sistematização destes conhecimentos ou ideias tidos como fundamentais.

Conjecturamos que o reconhecimento e a caracterização dessas ideias fundamentais constituem o verdadeiro "antídoto" para o excesso de fragmentação dos conteúdos disciplinares na forma como são apresentados, no sentido que por serem fundamentais podem ser tratados em um âmbito inter e trasndisciplinar. Foi pensando em tudo isso que, o Currículo da Secretaria da Educação, ([13], 2011), organizou os conteúdos matemáticos em três grandes blocos temáticos: Números, Geometria e Relações.

No bloco temático *Números* estão envolvidas as noções de contagem, medida e representação simbólica de grandezas efetivamente existentes ou imaginadas. Inclui-se aqui também as representações algébricas. Por, outro lado, no bloco *Geometria*, os conteúdos aqui envolvidos dizem respeito diretamente à percepção de formas e de relações entre elementos de figuras planas e espaciais; à construção e representação de formas geométricas, existentes ou imaginadas, e à elaboração de concepção de espaço servindo de suporte para a compreensão do mundo físico. Já no de *Relações* estão fundamentados a noção de medida; a ideia de aproximação; as relações métricas em geral e as relações de interdependência, como a proporção e função.

Apesar de estarem separados em três grandes blocos temáticos, os conteúdos interagem -se o tempo todo, impossibilitando assim a abordagem de um dos blocos sem a participação dos outros. É por causa da existência de tantas temáticas comuns aos blocos que o Currículo, ([13], 2011), articula diversos conteúdos, favorecendo uma aproximação entre variados assuntos evidenciando, assim, uma interdisciplinaridade interna da própria matemática.

Em termos das ideias fundamentais que compõem cada bloco, temos que: no Ensino Fundamental, o bloco *Número* tem como foco principal o enriquecimento da linguagem numérica, iniciando seus trabalhos com situações e problemas envolvendo elementos de contagem e a medida. Essas situações podem estar apoiadas na história, como por exemplo, a ampliação do conjunto dos números naturais e no conjunto dos números inteiros em razão da necessidade da utilização de números não naturais, os chamados números negativos, em ações comerciais do século XV. É incluída também nesse bloco, o estudo das representações dos números na forma algébrica e suas operações correspondentes.

No ensino fundamental, os números racionais surgem de relações entre inteiros, também chamada de razão entre inteiros e a motivação básica para o aprendizado dos irracionais encontra-se nas situações que envolvem grandezas incomensuráveis, como a relação entre as medidas do lado de um quadrado e sua diagonal. Espera-se dos alunos que, ao final do ensino fundamental, eles estejam aptos para a operalização de situações-problemas no campo real, para que ao integrarem-se no ensino médio, esse conhecimento seja o início de um aprofundamento e sistematização de novas relações emergidas das inter-relações ocorridas entre os conteúdos do ensino anterior.

Segundo ([13], 2011, p. 44), "não se pode pretender que exista apenas uma forma adequada de tratamento dos diversos conteúdos disciplinares, o que constituiria uma mistura de ingenuidade e arrogância", pois a implementação desse currículo na rede estadual de ensino, que é abrangente e multifacetada, deve levar em conta a grande diversidade de contextos existentes e um número expressivo de situações educacionais bem sucedidas a serem partilhadas e consolidadas.

Uma experiência que deu certo é a utilização de narrativas, históricas e de estórias, na introdução de novos conteúdos, com o objetivo de auxiliar na aprendizagem do aluno, em termo de construção dos significados. Esse tipo de abordagem é muito comum nas atividades existentes em um material de apoio elaborado pelo Governo do Estado de São Paulo denominado *caderno do aluno*. Nestes cadernos, entendidos informalmente como uma apostila auxiliar para os discentes e docentes, estão elaboradas atividades e situações-problemas que tratam os conteúdos curriculares de modo inter e transdisciplinar. É através do relato histórico dos conteúdos matemáticos que busca-se uma compreensão mais nítida e significativa dos conceitos fundamentais.

Tendo em vista todo o panorama conceitual e didático exposto detalhadamente em ([13], 2011), propomos a implantação do projeto intitulado "MMC e MDC: Gostosura ou Tortura".

3.2 O Motivo da Escolha dos Temas para o Projeto

Conforme a seção anterior, percebe-se que o Currículo, ([13], 2011), está muito preocupado com a qualidade de ensino da matemática. No entanto, analisando mais profundamente a grade curricular dessa disciplina para o ensino fundamental, ciclo II, e para o ensino médio, e também os cadernos do aluno e do professor de todas as séries, verificou-se que alguns conceitos, como por exemplos mínimo múltiplo comum e máximo divisor comum, que deveriam ser discutidos e trabalhados dentro de muitos outros contextos, são praticamente restritos a um único período letivo.

As concepções de mmc e mdc são tratadas somente dentro do conjunto de números naturais, no volume 1 do caderno do aluno do 6º ano, antiga 5º série. O que impressiona é que em nenhum outro caderno trás atividades que trabalham com esse conteúdo. Tal fato também é observado em livros didáticos para o ensino fundamental e médio, pois analisando coleções inteiras para os referidos assuntos, tais como ([5], 2011) e [6], observa-se tal ausência conceitual.

Diante deste contexto, elaboramos um projeto intitulado “MMC e MDC: Gostosura ou Tortura” para ser aplicado aos alunos do 8º ano do Ensino Fundamental e para o 3º ano do Ensino Médio, sendo que para este ciclo a atenção centrou-se nos conceitos de mmc e mdc generalizados.

3.3 Desenvolvimento do Projeto

O projeto foi desenvolvido no primeiro semestre de 2015, na Escola Estadual Professora Maria Neiva Abdelmasshi Justo, localizada no município de Valinhos, no estado de São Paulo. Foram selecionadas cinco salas, três das quais eram do Ensino Fundamental, especificamente turmas do 8º ano, e duas do Ensino Médio, exclusivamente turmas do 3º ano. O relato de todo o desenvolvimento do projeto está, logo abaixo, separado para as respectivas séries.

O motivo da escolha de tais classes deveu-se ao fato de ainda possuírem grande dificuldade de compreensão de conteúdos e habilidades relacionadas aos múltiplos e divisores de um número. Nas turmas de oitavo ano do Ensino Fundamental foi desenvolvido este projeto visando minimizar a dificuldade em compreender mínimo múltiplo comum (mmc) e máximo divisor comum (mdc), cujo objetivo era tornar a aprendizagem mais significativa aos alunos, conscientizando-os nas diferenças concretas entre mmc e mdc em situações do cotidiano.

Com as turmas do terceiro ano do Ensino Médio, além de tornar a aprendizagem mais significativa aos alunos conscientizando os mesmos nas diferenças concretas entre mmc e mdc em situações do cotidiano, o objetivo maior era avançar na aprendizagem expandindo o conhecimento para mmc e mdc generalizados.

3.4 Oitavo ano do Ensino Fundamental.

Em um primeiro momento, conversou-se com as três salas de 8º ano acerca do fato de que durante o período de quatro semanas eles estariam participando da aplicação de um projeto de mestrado e que os mesmos seriam avaliados em dois momentos, no início e no final do projeto.

Resumidamente temos que:

- Primeira semana: de 02 a 06 de fevereiro de 2015.

  i) 1ª e 2ª aulas.

Sem nenhuma explicação do conteúdo, foi aplicada a avaliação diagnóstica com questões de mmc e mdc de números inteiros positivos, questões estas em forma de problemas retiradas de livros didáticos de matemática para o 6º ano e também de provas externas, como da Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP) ou do SARESP (Sistema de Avaliação de Rendimento Escolar do Estado de São Paulo).

Logo após o término da avaliação diagnóstica, foi revisado muito rapidamente o conceito de mmc e mdc de números inteiros pois os alunos, em sua maioria, não conseguiram realizar a avaliação como era esperado, e ficaram curiosos em como poderiam ter resolvido as questões propostas. Exatamente no final da aula, o pesquisador pediu que os alunos trouxessem para as próximas aulas uma caixa de fósforo.

ii) 3ª e 4ª aulas.

Os alunos trouxeram caixas com palitos de fósforo para trabalharem a atividade lúdica de construção de triângulos retângulos, a qual consistia em utilizar o palito como unidade de medida, por terem todos o mesmo tamanho. Nessa atividade foram utilizados palitos para construir os lados. Se a medida de um lado do triângulo era, por exemplo, 3 seriam necessários 3 palitos colocados um em sequência do outro.

O objetivo dessa atividade era que os alunos compreendessem algumas características do triângulo retângulo, como, por exemplo, que a hipotenusa é sempre o maior entre os 3 lados do triângulo. Para isso, antes da atividade em si, foi introduzida aos alunos a definição de triângulo retângulo. As características principais e nomes dos lados do triângulo em questão também foram estudados.

Após essa curta explicação, com o objetivo de encontrar a medida da hipotenusa, foram colocados na lousa a medida dos catetos. As medidas escolhidas para os catetos-pelo pesquisador - eram as dos Triângulos Pitagóricos. Os alunos, divididos em grupos com quatro ou com três integrantes, deveriam construir os catetos utilizando os palitos e ao final, deveriam construir o terceiro lado do triângulo, também com palitos, unindo as extremidades dos catetos.

É claro, que os alunos tiveram que encontrar maneiras de modo a manter um ângulo reto entre os catetos, para assim dar a veracidade à medida da hipotenusa encontrada (ver Figuras 6 e 7 na seção 3.6).

Após terminarem essa atividade, o pesquisador pediu que os alunos escolhessem valores arbitrários para os catetos e tentassem encontrar a hipotenusa. A maioria dos alunos não conseguia encontrar uma quantidade inteira de palitos para a medida da hipotenusa.

Alguns alunos perceberam que se escolhessem medidas que fossem múltiplas as medidas propostas pelo pesquisador, conseguiriam encontrar uma quantidade inteira de palitos para a medida da hipotenusa, uma vez que o próprio pesquisador havia feito isso, mas sem explicitar o fato.

iii) 5ªaula.

Para a quinta aula dessa semana, o pesquisador propôs alguns questionamentos tais como: que conclusões os alunos poderiam fazer sobre a hipotenusa. Aprofundando mais um pouco o pesquisador pediu que todos olhassem para as medidas encontradas e tentassem descobrir uma relação entre os lados do triângulo retângulo e sugeriu que eles utilizassem as operações para isso.

O primeiro questionamento foi respondido unanimemente, isto é, que a hipotenusa era sempre o maior lado. Já para o segundo foi necessário uma discussão maior com as salas, utilizando cálculos com tentativas e erros até que se chegasse a conclusão que o "quadrado da hipotenusa era igual a soma dos quadrados dos catetos".

Durante essas atividades lúdicas foram trabalhadas as habilidades de reconhecimento de um triângulo retângulo, bem como a relação entre os lados; de compreensão do Teorema de Pitágoras e de identificação de triângulos semelhantes.

iv) 6ª aula

Foi iniciada uma outra atividade lúdica com alunos, na qual os mesmos foram desafiados a tentar montar triângulos retângulos com as medidas dos catetos iguais entre si. Eles deveriam utilizar uma única unidade de medida, ou seja, os catetos deveriam medir uma unidade. Essa unidade de medida foi escolhida pelos alunos, começando com medidas maiores, como palitos de churrasco, e chegando a medidas menores como palitos de fósforo. Cada grupo de alunos deveria pegar os materiais escolhidos e tentar encontrar uma quantidade inteira para a hipotenusa.

O objetivo desta segunda atividade lúdica foi despertar nos alunos a possibilidade de haver ou não uma medida de hipotenusa nesses triângulos retângulos com uma unidade ou unidades inteiras. A atividade foi iniciada pelos alunos por levantamento de estimativas e hipóteses. A grande maioria dos deles concordou que para unidades grandes a hipotenusa não iria medir uma unidade inteira e muito menos duas unidades inteiras. Mas alguns achavam que poderia ser possível que unidades menores dessem certo, como, por exemplo, palitos de fósforo, de dente, clipes de papel (ver Figuras 8, 9 e 10 na seção 3.6).

Ao final da aula, os alunos perceberam que com nenhum dos materiais foi possível encontrar uma quantidade inteira para a medida da hipotenusa, e ao associarem com a atividade anterior, que eles deveriam escolher ao acaso medidas para os catetos- quando alguns não conseguiram encontrar quantidades inteiras para a hipotenusa- eles começaram a questionar o porquê isso ocorria, e se com algum material iria dar certo. A habilidade trabalhada nessa atividade foi a de compreender os números não inteiros como uma medida.

- Segunda semana: de 09 a 13 de fevereiro de 2015.

  i) 1ª e 2ª aulas.

  Nestas aulas o pesquisador aproveitou os questionamentos que encerraram a primeira semana para trabalhar com os alunos um pouco de história, situando-os no que ocorria na antiguidade, na época de Pitágoras. Durante essas aulas foi ensinado o conceito de números comensuráveis e chegando ao conceito de números incomensuráveis, através da relação entre a medida do lado de um quadrado e a medida da sua diagonal, o que levou ao Teorema de Pitágoras.

  Com o Teorema de Pitágoras, foi proposto aos alunos que verificassem a veracidade dos valores encontrados para a hipotenusa. Na atividade com os palitos de fósforo, conseguiram verificar que os valores, quando encontrados, eram realmente os valores da hipotenusa. Nessas duas aulas a habilidade trabalhada foi a de utilizar o Teorema de Pitágoras.

  ii) 3ª e 4ª aulas.

  O pesquisador iniciou as aulas utilizando divisões e subdivisões do inteiro, utilizou como exemplo duas irmãs que fizeram cada uma um bolo para vender. Mas dividiram o bolo de maneiras diferentes, uma em oito pedaços e a outra em doze pedaços. Como resolveram unir as vendas, tiveram que redividir os bolos para terem pedaços com mesmo tamanho. Dessa maneira os estudantes foram instigados a encontrar um múltiplo comum às duas quantidades de pedaços de cada bolo. Depois de várias tentativas, descobriram que a melhor maneira era dividir cada bolo em vinte e quatro pedaços, para que não ficassem pedaços muito pequenos.

Após a descoberta, foi relembrado o conceito de múltiplos e múltiplos comuns, utilizando o conceito de conjunto e de intersecção de conjuntos, encontrando assim o menor de todos os elementos da intersecção, diferente do elemento nulo. Ao final dessas duas aulas, o pesquisador apresentou dois problemas do livro didático de sexto ano do ensino fundamental, para que resolvessem utilizando o método apresentado.

iii) 5ª e 6ª aulas.

Durante este período, o pesquisador introduziu uma outra maneira para se encontrar o mmc de números inteiros. Que utiliza a decomposição de números compostos em fatores primos. O mmc é encontrado através da união dos fatores primos de cada número, sem repetir os fatores comuns. Depois da explicação, o pesquisador pediu que os alunos sentassem em duplas e resolvessem outros três problemas, também selecionados do livro didático do sexto ano do ensino fundamental, pelos dois métodos expostos.

Nessas quatro últimas aulas foram trabalhadas as habilidades de interpretar problemas e de calcular o menor múltiplo comum.

- Terceira semana: de 23 a 27 de fevereiro de 2015.

  i) 1ª e 2ª aulas.

  O pesquisador deu prosseguimento ao conceito de mmc de números inteiros. Colocou os alunos em grupo de três ou quatro integrantes e promoveu uma disputa entre os grupos. O grupo que terminasse o resolução de um problema primeiro ganhava um ponto, no final ganhou o grupo com mais pontos. Nessas aulas foram propostos problemas que envolvessem o conceito de mmc retirados de provas anteriores da OBMEP ou SARESP, problemas esses mais complexos, mas ainda sim contextualizados.

  ii) 3ª e 4ª aulas.

  Nestas aulas o pesquisador introduziu o conceito de divisores de um número, utilizando um objeto que estava na moda na época, o "Bastão de Selfie". Utilizando a relação de quanto menor a distância necessária para se tirar uma foto, menor deveria ser o tamanho do bastão. Para introduzir o conceito de divisores comuns o pesquisador comentou que tinha 1200 balas de um certo tipo, e 1344 balas de um outro. Disse também que queria distribuir essa quantidade para os alunos, mas com uma condição, cada aluno deveria receber quantidades iguais de cada bala.

Depois das discussões geradas com a problematização, o pesquisador relembrou o conceito de divisores e de divisores comuns de números inteiros, utilizando o conceito de conjuntos e de intersecção entre conjuntos, encontrando assim o maior elemento entre todos os do conjunto intersecção. Para terminar essas duas aulas, o pesquisador propôs aos alunos que resolvessem dois problemas envolvendo mdc de números inteiros, retirados do livro didático do sexto ano do ensino fundamental.

iii) 5ª e 6ª aulas.

Nas últimas duas aulas da terceira semana do projeto, ao dar prosseguimento ao conceito de mdc para números inteiros, o pesquisador expôs um outro método para encontrar o mdc. Esse método consiste em decompor cada número composto em fatores primos, encontrando a intersecção desses fatores.

Após a explicação do método de decomposição em fatores primos. O pesquisador dividiu a sala em grupos de no máximo quatro alunos para que resolvessem outros quatros problemas, retirados, também, do livro didático do sexto ano, pelos dois métodos que foram expostos.

- Quarta semana: de 02 e 06 de março de 2015.

  i) 1ª e 2ª aulas.

  Nas duas primeiras aulas da quarta semana do projeto, o pesquisador deu prosseguimento ao conceito de mdc de números inteiros. Colocou os alunos em grupo de três ou quatro integrantes e promoveu novamente disputa entre os grupos. Nessas aulas foram propostos problemas que envolvessem o conceito de mdc que foram retirados de provas anteriores da OBMEP ou SARESP, problemas esses mais complexos, mas ainda sim contextualizados.

  ii) 3ª e 4ª aulas.

  Ao terminar toda a construção do conhecimento do aluno sobre mmc e mdc de números inteiros, com a resolução de questões problemas da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas), passou-se para um conceito mais aprofundado, o conceito de mínimo múltiplo comum generalizado (mmcg) e máximo divisor comum generalizado (mdcg), para que os alunos percebessem que o cálculo de mmc e mdc entre dois ou mais números não se restringia a números inteiros.

Os alunos perceberam que foi possível calcular o mmc e o mdc para quaisquer dois números racionais, uma vez que os elementos desse conjunto eram sempre números comensuráveis.Para sistematizar esses novos conceitos, o pesquisador trabalhou com os alunos alguns exercícios que envolvessem o cálculo do mmcg e do mdcg.

iii) 5ª e 6ª aulas.

Finalizando o projeto no oitavo ano do ensino médio, o pesquisador aplicou uma segunda avaliação, que tinha o intuito de verificar se o projeto foi ou não eficaz.

Mesmo não tendo uma resposta tão positiva como se esperava, o conceito de números incomensuráveis foi importante, para, mais tarde, introduzir o conjunto dos números irracionais e assim o conjunto dos números reais.

Ao observar os resultados da segunda avaliação diagnóstica e compará-los com os resultados da primeira percebeu-se que não houve melhora na maioria dos casos. Os alunos ainda não compreendiam os conceitos de múltiplos, divisores, mmc e mdc para números inteiros. Analisou-se, também, que muitos discentes ainda não têm interiorizado o algoritmo da divisão.

Muitas questões foram levantadas após essa observação, tais como: Quais foram os erros do projeto? Será que o projeto está muito além da capacidade intelectual dos alunos? Os alunos possuíam os pré-requisitos necessários para a verdadeira compreensão desses conceitos?

3.5 Terceiro Ano do Ensino Médio.

O conceito de números comensuráveis e incomensuráveis estão inseridos no contexto de conjuntos numéricos, que por sua vez compõem a estrutura algébrica de conjuntos em termos de Anel e Corpo, os quais serão temas das atividades propostas para esta turma de discentes, além daquelas destinadas às temáticas de mdc e mmc generalizados.

Resumidamente o projeto será relatado abaixo:

- Primeira semana: de 02 a 06 de fevereiro de 2015.

  i) 1ª e 2ª aulas.

  O projeto, para o 3º ano do ensino médio foi iniciado com uma aula expositiva sobre as estruturas algébricas de Anel e Corpo de uma maneira nada lúdica, deixando os alunos, ao final das aulas, um pouco intrigados.

ii) 3ª e 4ª aulas.

Realização de uma avaliação diagnóstica sobre o tema das primeiras duas aulas, para verificar o que os alunos haviam compreendido. Observou-se que durante a realização dessa avaliação, muitos dos alunos se recusaram a resolvê-la, pois os mesmos não prestaram atenção durante explicação do conteúdo pelo pesquisador. Questionaram o motivo de ter que fazer essa avaliação e se iria prejudicar sua nota se não o fizesse.

Além desse transtorno, como era de se esperar, a maioria dos alunos não conseguiu resolver completamente a avaliação diagnóstica.

- Segunda semana: de 09 a 13 de fevereiro de 2015.

  i) 1ª e 2ª aulas.

  Com o intuito de fazer os alunos compreenderem o real significado de mmc e mdc, foram trabalhados, através de situações problemas do cotidiano, os conceitos de múltiplos, múltiplos comuns e mínimo múltiplo comum (mmc) de números inteiros, divisores, divisores comuns e máximo divisor comum (mdc) de números inteiros. Introduzindo também métodos mais práticos para o cálculo do mmc e do mdc, deixando a critério dos alunos o método mais prático para cada um deles.

  O pesquisador iníciou a aula utilizando um objeto que estava na moda na época do projeto, o "Bastão de Selfie", esse objeto serviu para introduzir o conceito de múltiplos e divisores. Durante a aula teórica pôde-se perceber que a maturidade desses alunos, ajudou-os a compreender muitos conceitos que eles não entendiam na época em que foi ensinado os conceitos de mmc e mdc para números inteiros. Eles próprios perceberam e comentaram o fato.

  ii) 3ª e 4ª aulas.

  Foram trabalhados com os alunos exercícios de mmc e mdc de números inteiros, exercícios estes em forma de problemas, retirados de avaliações externas como a OBMEP e o SARESP. Para essa atividade os alunos estavam sentados em duplas ou trios.

- Terceria semana: de 23 e 27 de fevereiro de 2015.

  i) 1ª e 2ª aulas.

  Neste período o projeto continuou com aula expositava para introduzir o conceito de menor múltiplo comum generalizado e maior divisor comum generalizado, conceitos trabalhados nas aulas seguintes. O pesquisador deu alguns exemplos da importância desses conceitos em várias áreas do conhecimento, na matemática, na física, na astronomia, entre outras. Mostrou também exemplos de profissionais que utilizam o conceito de mmc e mdc para realizar seus trabalhos. Como exemplos, o engenheiro civil quando necessita calcular a viga de uma construção; o arquiteto que utiliza tais conceitos para calcular o madeiramento necessário em uma construção.

Ao final dessas aulas o pesquisador deu um desafio, pediu para que os alunos encontrassem um múltiplo comum, dando preferência ao menor, e um divisor comum, dando preferência para o maior, de dois números racionais. Os alunos tiveram um pouco de trabalho para encontrar o mmc e o mdc desses números. Alguns tentaram encontrar utilizando o método da decomposição de fatores primos, até perceberem que não conseguiriam decompor números não inteiros.

ii) 3ª e 4ª aulas.

O pesquisador aproveitou a dificuldade que os alunos tiveram em encontrar o mmc e mdc de dois números não inteiros para introduzir um conceito novo, o de menor múltiplo comum generalizado (mmcg) e maior divisor comum generalizado (mdcg). Aproveitou-se aqui para explicar o conceito de números comensuráveis e incomensuráveis.

Após explicação os alunos ficaram encantados em saber que existia um método para encontrar o mmcg e mdcg para números comensuráveis não inteiros.

- Quarta semana: de 02 a 06 de março de 2015.

  i) 1ª e 2ª aulas.

  O pesquisador trabalhou com as duas salas de terceiro ano do ensino médio, exercícios que envolveram o cálculo de mmcg e mdcg. Os alunos tiveram a opção de sentarem em duplas, grupos, ou, se preferissem, sozinhos. Pois os mesmos foram acostumados durante todo o ensino médio a resolver exercícios dessa maneira.

  i) 3ª e 4ª aulas.

  Para finalizar o projeto, nas duas últimas aulas da quarta semana, o pesquisador aplicou a avaliação, tal como foi acordado com os estudantes. A segunda avaliação diagnóstica teve o intuito de verificar se os alunos compreenderam os conceitos trabalhados durante o projeto.

Diferentemente, do 8º ano do ensino fundamental, o 3º ano do ensino médio, mostrou um pouco de relutância em participar do projeto de mestrado. Com o passar das aulas alguns alunos, que não estavam participando, passaram a participar. Mas, apesar do aumento de alunos resolvendo a segunda avaliação diagnóstica em relação ao número de alunos que resolveram a primeira avaliação, havia ainda um número considerável de alunos que se mostraram totalmente desinteressados.

Ao observar os resultados obtidos na segunda avaliação diagnóstica, observando somente as avaliações resolvidas, percebesse que muitos alunos alcançaram um bom resultado. Mas em alguns ainda persistia dificuldades em conhecimentos básicos, como números primos, relação de um número com seus fatores. Dificuldades estas que já não deveriam existir para alunos do ensino médio.

3.6 Fotos do Projeto

Figura 6 – Medindo a hipotenusa.

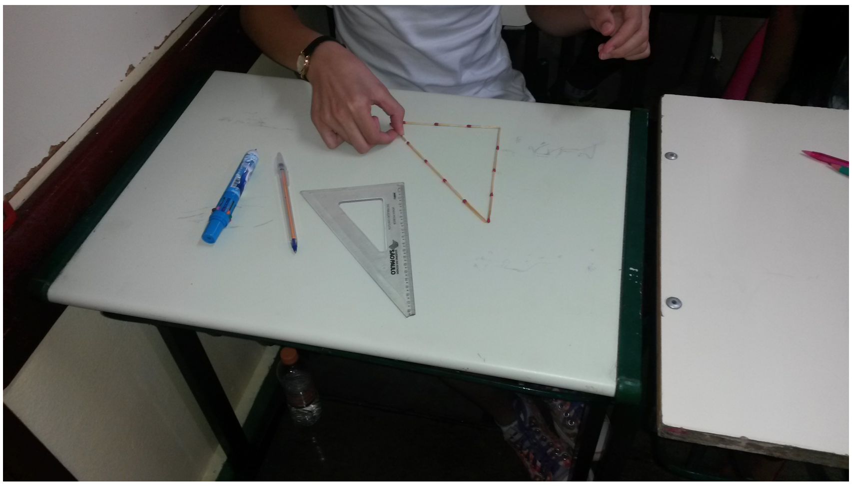


Figura 7 – Medindo a hipotenusa.

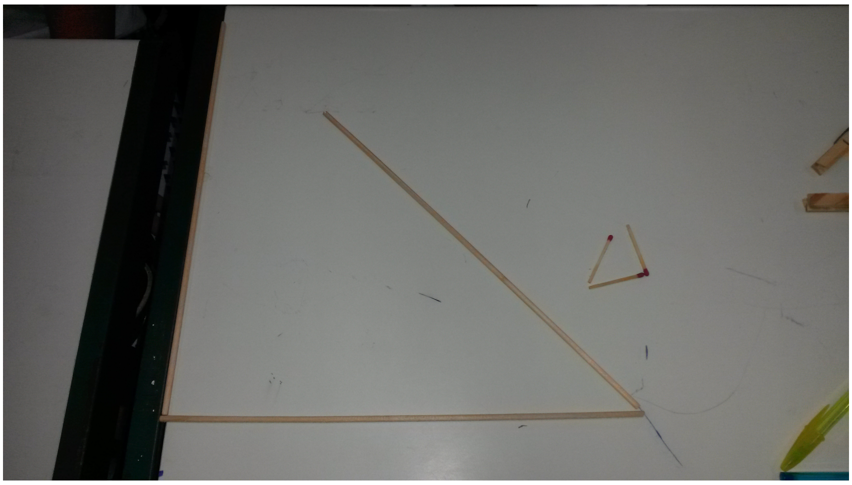


Figura 8 – Descobrindo a existência de medidas incomensuráveis.

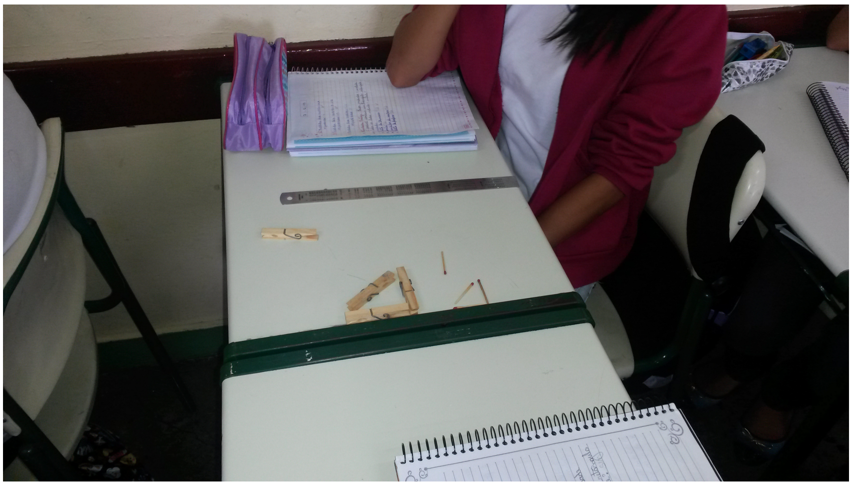


Figura 9 – Descobrindo a existência de medidas incomensuráveis.

Figura 10 – Descobrindo a existência de medidas incomensuráveis.

4 Conclusão

Quando o projeto foi planejado o objetivo central era mostrar que com um ensino interdisciplinar o aprendizado se torna mais significativo. No entanto, verificou-se que um trabalho desse nível não poderia obter resultados significativos em um período tão curto.

Para provar que o conhecimento para ser adquirido plenamente através da relação entre as disciplinas escolares e utilizando, também, os conceitos já adquiridos pelo aluno, o que torna-o muito mais significativo, é necessário um tempo muito maior do que as quatro semanas dedicadas a realização do projeto.

Esse trabalho, então, fica como incentivo aos meus colegas de profissão para que, juntos iniciemos uma reestruturação na maneira como, hoje, transmitimos o conhecimento, desfragmentando os conteúdos, relacionando todas as áreas do conhecimento, com o objetivo de que nossos alunos interiorizem o aprendizado de uma forma bem mais significativa.

Referências

[1] C. B. Boyer. *História da Matemática*. Editora da Universidade de São Paulo, 1974.

[2] C. B. Boyer and U. C. Merzbach. *A history of mathematics*. John Wiley and Sons, 2011.

[3] W. Burkert. *Lore and science in ancient pythagoreanism*. Harvard University Press, 1972.

[4] W. A. Carnielli and R. L. Epstein. *Computabilidade, funções computáveis, lógica e os fundamentos da matemática*. Editora Unesp, 2009.

[5] L. R Dante. *Matemática: contexto e aplicações*. Ática, 2011.

[6] O. Dolce, G. Iezzi, and D. Degenszajn. *Matemática*. Atual, 2015.

[7] I. M. L. D'Ottaviano and F. M. Bertato. George berkeley e os fundamentos do cálculo diferencial e integral. pages 1–29, 2012.

[8] C. H. B. Goncalves and C. Possani. Revisitando a descoberta dos incomensuráveis na grécia antiga. *Revista Matemática Universitária*, pages 16–24, 2010.

[9] I. Grattan-Guinness. The fontana history of the mathematical sciences. *The rainbow of mathematics*, 1997.

[10] K. Hrbacek and T. Jech. *Introduction to Set Theory, Third Edition, Revised and Expanded*. Chapman & Hall/CRC Pure and Applied Mathematics. Taylor & Francis, 1999.

[11] S. Jurkiewicz. *Divisibilidade e Números Inteiros*. OBMEP, 2009.

[12] C. C. Ripoll, J. B. Ripoll, and A. A. Sant'Ana. O mínimo múltiplo comum e máximo divisor comum generalizados. *Revista Matemática Universitária*, pages 59–74, 2006.

[13] S.E São Paulo. *Currículo do Estado de São Paulo: Linguagens, códigos e suas tecnologias*. SE, 2011.

[14] J. Struik. *História Concisa das Matemáticas*. Ciência Aberta, Gradiva, 2000.