



**UNIVERSIDADE ESTADUAL DO CEARÁ  
CENTRO DE CIÊNCIAS E TECNOLOGIA  
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL**

**FABRÍCIO LEMOS DO NASCIMENTO**

**MÁXIMO DIVISOR COMUM E MÍNIMO MÚLTIPLO COMUM:  
UMA ABORDAGEM DE SUAS PROPRIEDADES E APLICAÇÕES**

**FORTALEZA - CEARÁ  
2015**

**FABRÍCIO LEMOS DO NASCIMENTO**

**MÁXIMO DIVISOR COMUM E MÍNIMO MÚLTIPLO COMUM:  
UMA ABORDAGEM DE SUAS PROPRIEDADES E APLICAÇÕES**

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como exigência parcial para a obtenção do título de mestre em Matemática.

Orientador: Prof. Dr. José Othon Dantas Lopes.

FORTALEZA - CEARÁ

2015

Dados Internacionais de Catalogação na Publicação

Universidade Estadual do Ceará

Sistema de Bibliotecas

Nascimento, Fabrício Lemos do.

Máximo Divisor comum e mínimo múltiplo comum: uma abordagem em suas propriedades e aplicações [recurso eletrônico] / Fabrício Lemos do Nascimento. - 2015.

1 CD-ROM: il.; 4 ¼ pol.

CD-ROM contendo o arquivo no formato PDF do trabalho acadêmico com 59 folhas, acondicionado em caixa de DVD Slim (19 x 14 cm x 7 mm).

Dissertação (mestrado profissional) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Mestrado Profissional em Matemática em Rede Nacional, Fortaleza, 2015.

Área de concentração: Matemática.

Orientação: Prof. Dr. José Othon Dantas Lopes.

1. Máximo divisor comum. 2. Mínimo múltiplo comum.  
3. Domínio euclidiano. I. Título.

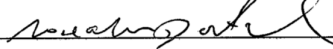
FABRÍCIO LEMOS DO NASCIMENTO

Máximo Divisor Comum e Mínimo Múltiplo Comum:  
Uma Abordagem de suas Propriedades e Aplicações.

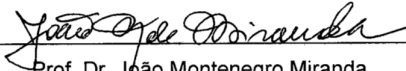
Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como exigência parcial para a obtenção do título de mestre em Matemática, sob a orientação do Prof. Dr. José Othon Dantas Lopes.

Aprovada em: 30/11/2015

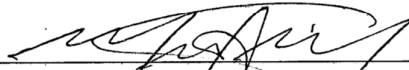
BANCA EXAMINADORA



Prof. Dr. José Othon Dantas Lopes.



Prof. Dr. João Montenegro Miranda.



Prof. Dr. Marcos Ferreira de Melo.

## **AGRADECIMENTOS**

Agradeço primeiramente a Deus, por ser tão presente na minha vida e possibilitar esta grande conquista.

Aos meus pais, que me prestaram apoio incondicional ao longo de todos os meus anos de estudo.

A minha esposa Raquel que sempre trazia palavras de incentivos, principalmente nos momentos de angustias.

A todos os professores que contribuíram com seus conhecimentos e foram de grande importância na minha formação.

Aos meus colegas do PROFMAT, que estiveram juntos comigo, com muito companheirismo, nessa caminhada tão árdua.

Por fim, agradeço ao meu orientador, Prof. Prof. Dr. José Othon Dantas Lopes, que pacientemente com sua orientação acompanhou o progresso do meu trabalho.

“Algo só é impossível até que alguém  
duvide e prove ao contrário.”

(Albert Einstein)

## RESUMO

O Máximo Divisor Comum (MDC) e o Mínimo Múltiplo Comum (MMC) são assuntos da teoria dos números com diversas aplicações que podem nos ajudar a solucionar problemas do nosso cotidiano. O propósito deste trabalho é fazer uma abordagem destes conteúdos partindo de conceitos mais básicos, que são ensinados no ensino fundamental da educação básica, bem como, fundamentações teóricas mais elaboradas vistas no ensino superior. Para isto, é feita uma revisão sobre a divisibilidade e a divisão euclidiana. Em seguida, aborda-se o máximo divisor comum e o mínimo múltiplo comum nos inteiros. Finalmente, conclui-se com o estudo do domínio euclidiano e a existência do máximo divisor comum entre dois elementos. Para ilustrar a relevância de tais conceitos, vários exemplos de aplicações dos mesmos são apresentados neste trabalho.

**Palavras-chave:** Máximo divisor comum. Mínimo múltiplo comum. Domínio euclidiano.

## **ABSTRACT**

The Greatest Common Divisor (GCD) and The Least Common Multiple (LCM) are subjects of number theory with various applications that can help us solve our daily problems. The aim of this work is making an approach about these contents, starting from the most basic concepts that are taught in elementary school of basic education, as well as, theoretical foundations that are seen in higher education. In order to do that, first it is done a review of divisibility and Euclidean division. Then, it addresses the greatest common divisor and least common multiple in whole. Finally, with the study of Euclidean domain and the existence of the greatest common divisor. In order to illustrate the relevance of such concepts, several examples of applications are presented in this work.

**Keywords:** Great common divisor. Least common multiple. Euclidean domain.



## LISTA DE ILUSTRAÇÕES

Figura 1 - Conjuntos com as fatorações de 3000 e 900 .....	26
Figura 2 - Interpretação geométrica do MDC .....	37
Figura 3 - Interpretação geométrica do MDC .....	37
Figura 4 - Conjuntos com as fatorações de 360 e 150 .....	43
Figura 5 - Conjuntos com as fatorações de 250 e 420 .....	43
Figura 6 - Interpretação geométrica do MMC. ....	48
Figura 7 - Interpretação geométrica do MDC e do MMC. ....	49
Figura 8 - Reta de equação $y = \frac{b}{a} x$ .....	49

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO .....</b>	<b>11</b>
<b>2</b>	<b>REVISÃO DE TÓPICOS DA TEORIA DOS NÚMEROS .....</b>	<b>13</b>
2.1	DIVISIBILIDADE NOS INTEIROS .....	13
2.2	DIVISÃO EUCLIDIANA .....	18
<b>3</b>	<b>MÁXIMO DIVISOR COMUM .....</b>	<b>23</b>
3.1	MÁXIMO DIVISOR COMUM NOS INTEIROS .....	23
3.2	APLICAÇÕES ENVOLVENDO O MÍNIMO MÚLTIPLO COMUM .....	33
3.3	UM MÉTODO GEOMÉTRICO PARA OBTER O MÁXIMO DIVISOR COMUM.....	36
<b>3</b>	<b>MÍNIMO MÚLTIPLO COMUM .....</b>	<b>38</b>
4.1	MÍNIMO MÚLTIPLO COMUM NOS INTEIROS .....	38
4.2	APLICAÇÕES ENVOLVENDO O MÍNIMO MÚLTIPLO COMUM .....	44
4.3	MÉTODOS GEOMÉTRICOS PARA OBTER O MÍNIMO MÚLTIPLO COMUM.....	47
<b>5</b>	<b>A EXISTÊNCIA DO MÁXIMO DIVISOR COMUM.....</b>	<b>51</b>
5.1	ANÉIS .....	51
5.2	DOMÍNIO EUCLIDEANO .....	54
<b>6</b>	<b>CONCLUSÃO .....</b>	<b>58</b>
	<b>REFERÊNCIAS .....</b>	<b>59</b>

## 1 INTRODUÇÃO

Existe uma frase no livro *Didática da Matemática* do professor de matemática Roland Charnay que diz: "O aluno deve ser capaz não só de repetir ou refazer, mas também de ressignificar diante de novas situações, adaptando e transferindo seus conhecimentos para resolver desafios". Esse pensamento vem transmitir o que seria ideal para a aprendizagem dos nossos alunos, mas infelizmente a realidade encontrada nas salas de aulas é um pouco diferente, pois, muitas vezes notamos que eles aprendem o processo, mas não conseguem entender o significado que existe por trás dele.

Uma situação que exemplifica claramente este fato é o ensino de Máximo Divisor Comum (MDC) e de Mínimo Múltiplo Comum (MMC) na educação básica, principalmente no ensino fundamental, pois pouco se fala sobre o que eles significam e suas aplicações.

Embora os conceitos de Máximo Divisor Comum e de Mínimo Múltiplo Comum apareçam em vários resultados teóricos e na resolução de problemas, principalmente, para o Conjunto dos Números Naturais no Ensino Fundamental e Médio, e seguidamente, para os Números Inteiros no Ensino Superior, sua aplicação mais comum no ensino básico é no cálculo com frações ordinárias, isto é, ao simplificar frações é que os textos didáticos usam o MDC e para comparar, somar ou subtrair frações, que aparece o MMC.

Os PCNs deixa bem claro sua posição sobre o ensino desses assuntos na educação básica:

" ... Conceitos como os de múltiplo e divisor de um número natural ou o conceito de número primo podem ser abordados neste ciclo como uma ampliação do campo multiplicativo, que já vinha sendo construído nos ciclos anteriores, e não como assunto novo, desvinculado dos demais. Além disso, é importante que tal trabalho não se resuma a apresentação de diferentes técnicas ou de dispositivos práticos que permitem ao aluno encontrar, mecanicamente, o mínimo múltiplo comum e máximo divisor comum sem compreender as situações-problema que esses conceitos permitem resolver." (PCNs, Terceiro e Quarto Ciclos do Ensino Fundamental - Matemática, 2a Parte, Conteúdos propostos para o ensino de Matemática no terceiro ciclo, p. 66).

Talvez, a forma de transmitir esses assuntos, sem dar muito sentido ao que se está fazendo, venha do fato dos professores de matemática não possuírem

um conhecimento mais amplo dos mesmos e assim faltam recursos para que sejam ensinados de outras formas.

Neste sentido, esse trabalho objetiva elaborar um material que venha fazer uma abordagem mais abrangente sobre MDC e MMC e que sirva de apoio aos professores para que possam compreender melhor o conteúdo. Esta pesquisa trata tanto de resultados mais simples, que são demonstrados nos livros didáticos do fundamental quanto das proposições, propriedades e exercícios mais elaborados que são vistos no ensino superior e com isso, mostrar que sua utilidade vai muito além de servir como ferramenta para trabalhar com frações ordinárias.

No segundo capítulo fazemos uma revisão de assuntos importantes da teoria dos números para que possamos ter um melhor entendimento dos conceitos de MDC e de MMC. Discorremos sobre divisibilidade nos números inteiros apresentando suas definições e aplicações, em seguida, tratamos da divisão euclidiana.

Já no terceiro e quarto capítulos, mostramos as principais definições, teoremas e proposições que fundamentam os conceitos de MDC e MMC no conjunto dos Inteiros, onde utilizamos o Algoritmo de Euclides como uma das principais ferramentas para o cálculo do MDC. Também apresentamos alguns exemplos de aplicações desta fundamentação teórica, bem como, os principais métodos utilizados pelos professores do ensino básico para a obtenção do MDC e do MMC nos números naturais. Finalizamos com uma demonstração de métodos geométricos apresentado na Revista do Professor de Matemática para o cálculo do MDC e do MMC.

E por fim, no último capítulo estudamos os domínios e que através dos quais analisamos a condição de existência do MDC para outras classes de números.

## 2 REVISÃO DE TÓPICOS DA TEORIA DOS NÚMEROS.

Nesse capítulo abordamos a divisibilidade e a divisão euclidiana visando maior embasamento para o estudo do máximo divisor comum e do mínimo múltiplo comum.

### 2.1 DIVISIBILIDADE NOS INTEIROS

**Definição 2.1.1** Dados dois números inteiros  $a$  e  $b$ , diremos que  $a$  divide  $b$ , escrevendo  $a \mid b$ , quando existir um número inteiro  $c$  tal que  $b = c \cdot a$ . Neste caso, diremos também que  $a$  é um divisor ou um fator de  $b$  ou, ainda, que  $b$  é um múltiplo de  $a$ . Quando  $a$  não dividir  $b$ , representamos esse fato por  $a \nmid b$ .

**Exemplo 2.1.1:**  $3 \mid 6$ , pois  $6 = 2 \cdot 3$ , temos também  $5 \mid 0$ , pois  $0 = 0 \cdot 5$ , mas  $7 \nmid 10$  pois não existe nenhum número inteiro tal que aconteça a igualdade  $10 = c \cdot 7$ .

**Proposição: 2.1.1** Sejam  $a, b, c \in \mathbb{Z}$ . Tem-se que:

- i)  $1 \mid a$ ,  $a \mid a$  e  $a \mid 0$ .
- ii) Se  $a \mid b$  e  $b \mid c$ , então  $a \mid c$ .

**Demonstração:**

i) As provas decorrem das seguintes igualdades;  $a = a \cdot 1$ ,  $a = 1 \cdot a$  e  $0 = a \cdot 0$ , respectivamente.

ii) Se  $a \mid b$  e  $b \mid c$  implica que existem  $r$  e  $s \in \mathbb{Z}$  tais que  $b = r \cdot a$  e  $c = s \cdot b$ , com isso teremos:  $c = s \cdot b = s \cdot (r \cdot a) = (s \cdot r) \cdot a$ , o que mostra que  $a \mid c$ .

**Proposição 2.1.2.** Se  $a, b, c, d \in \mathbb{Z}$ , então:  $a \mid b$  e  $c \mid d \Rightarrow a \cdot c \mid b \cdot d$ .

**Demonstração:** Se  $a \mid b$  e  $c \mid d$ , então existem  $r, s \in \mathbb{Z}$  tais que, que  $b = r \cdot a$  e  $d = s \cdot c$ . Logo,  $b \cdot d = (r \cdot a) \cdot (s \cdot c) = (r \cdot s) \cdot (a \cdot c)$  o que nos mostra que  $a \cdot c \mid b \cdot d$ .

**Proposição 2.1.3.** Sejam  $a, b, c \in \mathbb{Z}$  e  $c \neq 0$ . Então  $ac \mid bc \Leftrightarrow a \mid b$ .

**Demonstração:**

( $\Rightarrow$ ) Seja  $a \cdot c \mid b \cdot c$  então existe um  $s \in \mathbb{N}$  tal que  $b \cdot c = s \cdot a \cdot c$ , logo  $b \cdot c - s \cdot a \cdot c = 0$  logo  $c(b - s \cdot a) = 0$ .

Como  $c \neq 0$ , temos que  $b - s \cdot a = 0$  então  $b = s \cdot a$  e logo  $a \mid b$ .

( $\Leftarrow$ ) Vamos agora supor que  $a \mid b$  então existe um  $t \in \mathbb{Z}$  tal que  $b = t \cdot a$ . Para  $c \in \mathbb{Z}$  temos que  $b \cdot c = t \cdot a \cdot c$  de onde  $a \cdot c \mid b \cdot c$ .

Portanto,  $a \cdot c \mid b \cdot c \Leftrightarrow a \mid b$ .

**Proposição 2.1.4.** Sejam  $a, b, c \in \mathbb{Z}$ , tais que  $a \mid (b \pm c)$ . Então  $a \mid b \Leftrightarrow a \mid c$ .

**Demonstração:**

Suponhamos que  $a \mid (b + c)$ . Com isso, deve existir  $r \in \mathbb{Z}$  tal que  $b + c = r \cdot a$ .

( $\Rightarrow$ ) Se  $a \mid b$ , temos que existe  $s \in \mathbb{Z}$  tal que  $b = s \cdot a$ . Agrupando as duas igualdades, teremos que  $s \cdot a + c = r \cdot a$ . Isso acarreta  $c = r \cdot a - s \cdot a = (r - s) \cdot a$ . Portanto  $a \mid c$ .

Agora suponha que  $a \mid (b - c)$ , logo existe um inteiro  $n$  tal que  $b - c = n \cdot a$ .

( $\Leftarrow$ ) Se  $a \mid c$  então existirá outro inteiro  $m$  tal que  $c = m \cdot a$ . Ao substituir a segunda igualdade na primeira temos que  $b - m \cdot a = n \cdot a$ , logo  $b = m \cdot a + n \cdot a = (m + n) \cdot a$ .

Portanto  $a \mid b$ .

**Proposição 2.1.5** Sejam  $a, b, c \in \mathbb{Z}$ , tais que  $a \mid b$  e  $a \mid c$ , então  $a \mid (xb + yc)$ , para todo  $x, y \in \mathbb{Z}$ .

**Demonstração:** Se  $a \mid b$  e  $a \mid c$ , então existem  $r$  e  $s \in \mathbb{Z}$ , tais que  $b = r \cdot a$  e  $c = s \cdot a$ , então  $x \cdot b + y \cdot c = x \cdot (r \cdot a) + y \cdot (s \cdot a) = (x \cdot r) \cdot a + (y \cdot s) \cdot a = (x \cdot r + y \cdot s) \cdot a$ , logo  $a \mid (x \cdot b + y \cdot c)$ .

**Exemplo 2.1.2:** Prove que o número  $N = 5^{45362} - 7$  não é divisível por 5.

**Solução:** Suponha que  $N$  é divisível por 5, então temos que  $5^{45362} - 7 = 5q$ . Logo,  $7 = 5^{45362} - 5q$ , ou seja, 7 é divisível por 5, o que é um absurdo. Portanto  $5^{45362} - 7$  não é divisível por 5.

**Proposição 2.1.6:** Sejam  $a$  e  $b$  inteiros não nulos, se  $a \mid b$  e  $b \mid a$ , então  $a = \pm b$ .

**Demonstração:** Como  $a \mid b$  e  $b \mid a$ , existem  $p$  e  $q$  inteiros tais que:

$$b = a \cdot p \text{ e } a = b \cdot q.$$

Assim,  $a = (a \cdot p) \cdot q$ , ou seja,  $a = a \cdot (p \cdot q)$ , isso implica que  $a(pq - 1) = 0$ , então temos que  $p \cdot q = 1$ , ou seja,  $p = q = \pm 1$ . Portanto,  $a = \pm b$ .

**Observação 2.1.2:** O Princípio da Boa Ordem diz que em todo subconjunto  $C$ , não vazio, dos naturais; existe  $c \in C$ , tal que  $c \leq x$ , para todo  $x \in C$ .

**Proposição 2.1.7.** Dados  $a, b \in \mathbb{N}$ , temos que:  $a \mid b$ , então  $a \leq b$ .

**Demonstração:** Se considerarmos que  $a \mid b$ , Então existe  $c \in \mathbb{Z}$  tal que  $b = c \cdot a$ . Como  $a, b > 0$ , então  $c \in \mathbb{N}$ . Como  $1 \leq c$ , segue-se que  $a \leq a \cdot c = b$ .

**Proposição 2.1.8.** Sejam  $a, b \in \mathbb{Z}$  e  $n \in \mathbb{N}$ . Temos que  $a + b$  divide  $a^{2n+1} + b^{2n+1}$ .

**Demonstração:** A prova é feita por indução sobre  $n$ .

Fazendo  $n = 1$  temos que mostrar que  $a + b$  divide  $a^3 + b^3$ .

$$a^3 + b^3 = a^3 + a^2b - a^2b + b^3 =$$

$$a^2(a + b) + b(b^2 - a^2) =$$

$$a^2(a + b) + b(b - a)(a + b) =$$

$$(a + b)(a^2 + b(b - a))$$

O que mostra que  $a + b$  divide  $a^3 + b^3$

Suponhamos que  $(a + b) \mid a^{2n+1} + b^{2n+1}$ , então vamos mostrar que  $(a + b) \mid a^{2(n+1)+1} + b^{2(n+1)+1}$ .

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

Mas sabemos que  $a + b$  divide  $a^2 - b^2 = (a + b)(a - b)$  e, por hipótese de indução temos que,  $(a + b) \mid a^{2n+1} + b^{2n+1}$ , decorre das igualdades acima e da Proposição 1.1.4. que  $(a + b) \mid a^{2(n+1)+1} + b^{2(n+1)+1}$ . Mostrando, assim, o resultado para todo  $n \in \mathbb{N}$ .

**Proposição 2.1.9.** Sejam  $a, b \in \mathbb{Z}$  e  $n \in \mathbb{N}$ . Temos que  $a + b$  divide  $a^{2n} - b^{2n}$ .

**Demonstração:** A prova é feita por indução sobre  $n$ .

Podemos observar que a proposição é válida para  $n = 1$ , pois  $a + b$  divide  $a^2 - b^2 = (a + b)(a - b)$ .

Suponha que  $(a + b) \mid (a^{2^n} - b^{2^n})$ . Vamos mostrar que  $(a + b) \mid (a^{2^{(n+1)}} - b^{2^{(n+1)}})$ . Tomamos  $a^{2^{(n+1)}} - b^{2^{(n+1)}} = a^2 \cdot a^{2^n} - b^2 \cdot a^{2^n} + b^2 \cdot a^{2^n} - b^2 \cdot b^{2^n} = (a^2 - b^2)a^{2^n} + b^2(a^{2^n} - b^{2^n})$ . Mas sabemos que  $(a + b) \mid (a^2 - b^2)$  e, por hipótese de indução temos que,  $(a + b) \mid (a^{2^n} - b^{2^n})$ , decorre das igualdades acima e da Proposição 1.1.4. que  $(a + b) \mid (a^{2^{(n+1)}} + b^{2^{(n+1)}})$ . Mostrando, assim, o resultado para todo  $n \in \mathbb{N}$ .

**Exemplo 2.1.3:** Temos que  $7 \mid 175$ , pois  $175 = 4^{2^2} - 3^{2^2}$  e pela proposição a cima temos que  $7 \mid (4^{2^2} - 3^{2^2})$ .

**Exemplo 2.1.4:** (OBMEP - 2015) Sejam  $a$  e  $b$  dois dígitos diferentes de zero não necessariamente diferentes. O número de dois dígitos  $\overline{ab}$  é chamado de curioso, se ele for um divisor do número  $\overline{ba}$ , que é formado pela troca da ordem dos dígitos de  $\overline{ab}$ . Ache todos os números curiosos. Observação: O traço sobre os números serve para distinguir o produto  $a \cdot b$  do número de dois dígitos  $\overline{ab}$ .

**Solução:** Podemos escrever  $\overline{ab}$  como  $10a + b$ , assim como  $\overline{ba} = 10b + a$ . Se  $10a + b$  é divisor de  $10b + a$ , temos  $10b + a = (10a + b)k$ , onde  $k$  é um inteiro menor ou igual a 9 já que os dois números possuem dois dígitos. Segue que:

$$10b + a = (10a + b)k$$

$$10b + a + 10a + b = (10a + b)(k + 1)$$

$$11(a + b) = (10a + b)(k + 1).$$

Pela última equação, o número  $(10a + b)(k + 1)$  deve ser múltiplo de 11. Como  $k \leq 9$ , temos  $k + 1 \leq 10$  e, conseqüentemente,  $k + 1$  não possui fator 11, implicando que  $10a + b$  deve ser múltiplo de 11. Todos os números de dois dígitos múltiplos de 11 possuem dígitos iguais e isso nos permite concluir que necessariamente  $a = b$ . Quando  $a = b$ ,  $\overline{ab} = \overline{ba}$ . e, certamente, um divide o outro. Portanto, o conjunto dos números curiosos é  $\{11, 22, 33, 44, 55, 66, 77, 88, 99\}$

**Exemplo 2.1.5:** Mostre que  $6 \mid n(n + 1)(2n + 1)$ , para todo  $n \in \mathbb{N}$ .

**Solução:** Primeiramente vamos usar a indução sobre  $n$ .

Verificamos que se  $n = 1$  a afirmação é válida, pois teremos  $(1)(2)(3) = 6$  que é divisível por 6.



Agora vamos mostrar agora que se  $6 \mid n(n + 1)(2n + 1)$ , ou seja,  $n(n + 1)(2n + 1) = 6k$ , para algum  $k$ ,  $n$  que pertença aos naturais então  $6 \mid (n + 1)((n + 1) + 1)(2(n + 1) + 1)$ , isto é existe um  $q$  que também pertença aos naturais tal que  $(n + 1)(n + 1 + 1)(2(n + 1) + 1) = 6q$ .

Desenvolvendo a expressão  $(n + 1)[(n + 1) + 1][2(n + 1) + 1]$  temos que:

$$(n + 1)(n + 2)[(2n + 1) + 2] =$$

$$n(n + 1)(2n + 3) + 2(n + 1)(2n + 3) =$$

$$n(n + 1)(2n + 1) + 2n(n + 1) + 2(n + 1)(2n + 3).$$

Aplicando a hipótese de indução a última expressão é igual a:

$$6k + 2(n + 1)[n + (2n + 3)] =$$

$$6k + 2(n + 1)(3n + 3) =$$

$$6k + 2(n + 1)[3(n + 1)] =$$

$$6k + 6(n + 1)^2 =$$

$$6[k + (n + 1)^2] = 6q \text{ onde } q \in \mathbb{N} \text{ como queríamos provar.}$$

Portanto,  $6 \mid n(n + 1)(2n + 1)$ , para todo  $n \in \mathbb{N}$ .

**Exemplo 2.1.6:** Para quais valores de  $a \in \mathbb{N}$  teremos que  $(a - 2) \mid (a^3 + 4)$ ?

**Solução:** Suponha que  $(a - 2) \mid (a^3 + 4)$  então existe  $q \in \mathbb{N}$  tal que  $a^3 + 4 = (a - 2)q$  isto é:  $a^3 - 8 + 12 = (a - 2)q$ , então  $(a - 2)(a^2 + 2a + 4) + 12 = (a - 2)q$ , com isso,  $(a - 2)q - (a - 2)(a^2 + 2a + 4) = 12$ , logo  $(a - 2)[q - (a^2 + 2a + 4)] = 12$  e isso implica que  $q - (a^2 + 2a + 4) = q \frac{12}{a-2}$ . Como,  $q - (a^2 + 2a + 4) \in \mathbb{N}$ , temos que os possíveis valores para  $a$  serão: 8, 6, 5, 4 e 3.

**Exemplo 2.1.7:** Se  $a \neq b$ , mostre que, para todo  $n \in \mathbb{N}$ ,  $n \geq 2$ ,

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2} \cdot b + \dots + a \cdot b^{n-2} + b^{n-1}:$$

**Solução:** Para essa demonstração vamos usar indução sobre  $n \geq 2$  quando  $b \neq a$ .

$$\text{Para } n = 2 \text{ temos } a^2 - b^2 = (a - b)(a + b) \Rightarrow \frac{a^2 - b^2}{a - b} = \frac{(a + b)(a - b)}{a - b} = a + b, \text{ logo}$$

é válido.

Vamos supor que exista um  $n \in \mathbb{N}$  tal que seja verdade:

$$\frac{a^n - b^n}{a - b} = a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + ab^{n-2} + b^{n-1}. \text{ Devemos mostrar que também é}$$

válido para  $n + 1$ , ou seja, temos que provar que:

$$\frac{a^{n+1} - b^{n+1}}{a - b} = a^n + a^{n-1}b + a^{n-2}b^2 + \dots + ab^{n-2} + b^{n-1} + b^n.$$

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

Mas se  $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + ab^{n-2} + b^{n-1})$ , então  $a^{n+1} - b^{n+1} = a[(a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + ab^{n-2} + b^{n-1})] + b^n(a - b) = a^{n+1} - b^{n+1} = (a - b)[a(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \dots + ab^{n-2} + b^{n-1}) + b^n] =$

$\frac{a^{n+1} - b^{n+1}}{a - b} = a^n + a^{n-1}b + a^{n-2}b^2 + \dots + ab^{n-2} + b^{n-1} + b^n$ . Como queríamos provar.

## 2.2 DIVISÃO EUCLIDIANA

Nessa etapa do capítulo será apresentada a divisão euclidiana, como também, alguns exemplos e aplicações.

**Teorema 2.2.1.** Sejam  $a$  e  $b$  dois números inteiros com  $a \neq 0$ . Existem dois únicos números inteiros  $q$  e  $r$  tais que  $b = a \cdot q + r$ ; com  $0 \leq r < |a|$ . Neste caso, chamaremos:

$b$  - Dividendo;

$a$  - Divisor;

$q$  - Quociente;

$r$  - Resto.

**Demonstração:** Vamos utilizar na demonstração desse teorema o Princípio da boa ordenação que diz: Todo conjunto não vazio  $A$  de inteiros não negativos possui um menor elemento.

Existência: Tome que  $b > a$ . Considere o conjunto  $S = \{b, b - a, b - 2a, \dots, b - n \cdot a\}$ , com  $n$  inteiro e  $b - na \geq 0$ .

O Princípio da boa ordenação diz que esse conjunto tem um menor elemento  $r$ , temos então  $r \geq 0$  e  $r = b - aq$ , ou seja,  $b = aq + r$ , com  $q \in \mathbb{Z}$ . Temos ainda que  $r < a$ , pois se isso não ocorrer teríamos  $r \geq a$ , logo  $r - a \geq 0$  e com isso  $b - aq - a \geq 0$  então  $b - a(q + 1) < r$ , portanto  $r$  não seria o menor elemento de  $S$ .

Unicidade: Vamos supor que existam  $q, q_1, r$  e  $r_1 \in \mathbb{Z}$ , tais que  $b = aq_1 + r_1$  com  $0 \leq r_1 < a$ . Tomando  $b = aq + r$ , e igualando  $b = aq_1 + r_1$ , teremos:  
 $aq + r = aq_1 + r_1$  logo  $aq - aq_1 = r_1 - r$  e com isso  $a \cdot (q - q_1) = r_1 - r$ , e portanto,  $a$  divide  $r_1 - r$ . Mas se  $r_1 < a$  e  $r < a$ , temos  $|r_1 - r| < a$  e como  $a$  divide  $r_1 - r$ , teremos  $r_1 - r = 0$ , logo,  $r_1 = r$ . Desta forma,  $aq = aq_1$ , como, por hipótese  $a \neq 0$ , temos  $q = q_1$ .

**Exemplo 2.2.1:** Encontre o quociente e o resto da divisão de 32 por 5.

$$r_1 = 32 - 1 \cdot 5 = 27$$

$$r_2 = 32 - 2 \cdot 5 = 22$$

$$r_3 = 32 - 3 \cdot 5 = 17$$

$$r_4 = 32 - 4 \cdot 5 = 12.$$

$$r_5 = 32 - 5 \cdot 5 = 7$$

$$r_6 = 32 - 6 \cdot 5 = 2.$$

Portanto  $q = 6$  e  $r = 2$ , escrevendo assim  $32 = 6 \cdot 5 + 2$ .

**Exemplo: 2.2.2** Vamos achar os múltiplos de 7 que se encontram entre 1 e 144.

**Solução:** Pelo algoritmo da divisão temos que:

$$144 = 7 \cdot 20 + 4;$$

Ou seja, o maior múltiplo de 7 que cabe em 144 é  $7 \cdot 20$ , onde 20 é o quociente da divisão de 144 por 7. Portanto, os múltiplos de 7 entre 1 e 144 são:  $7 \cdot 1, 7 \cdot 2, 7 \cdot 3, \dots, 7 \cdot 20$  e, conseqüentemente, são em número de 20.

**Exemplo 2.2.3:** (OBMEP - 2015) Um grilo pode dar pulos de duas distâncias: 9 e 8 metros. Ele disputa uma corrida de 100 metros que vai até a beira de um penhasco. Quantos pulos o grilo deve dar para chegar ao fim da corrida, mas sem passar do ponto final e cair do penhasco?

**Solução:** Sejam  $x$  o número de pulos de 9m e  $y$  o número de pulos de 8m. Queremos determinar  $x + y$ , sabendo que:  $100 = 9x + 8y = 8(x + y) + x$ . Como 100 deixa resto 4 na divisão por 8, o mesmo deve ocorrer com o número  $8(x + y) + x$ . Ou seja,  $x$  deve deixar resto 4 na divisão por 8 pois  $8(x + y)$  já é múltiplo de 8. Se  $x > 4$ , saberemos que  $x$  é pelo menos  $8 \cdot 1 + 4 = 12$  que é o próximo número que deixa resto 4 por 8 depois de 4. Se o grilo der 12 pulos de 9m, ele chegará a  $9 \cdot 12 = 108$  m

e cairá do penhasco. Logo,  $x = 4$  e após sua substituição na equação acima, podemos concluir que  $y = (100 - 9 \cdot 4)/8 = 8$ .

Portanto, o grilo deve dar  $4 + 8 = 12$  pulos.

**Exemplo 2.2.4:** (OBMEP - 2015) Os números que são inteiros positivos elevados ao quadrado são chamados quadrados perfeitos, por exemplo, 16 é um quadrado perfeito, pois é igual a  $4^2$ . Um fato curioso é que números que são quadrados perfeitos deixam apenas restos 0 ou 1 na divisão por 4. Com isso podemos provar, por exemplo, que 2014 não é um quadrado perfeito, pois 2014 deixa resto 2 na divisão por 4.

a) Sabendo que todo número inteiro ímpar é da forma  $2k + 1$ , mostre que os quadrados perfeitos ímpares deixam resto 1 na divisão por 8.

**Solução:** Ao desenvolver o produto notável relativo ao quadrado de um número ímpar temos:

$$(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1.$$

Como pelo menos um dentre  $k$  e  $k + 1$  é par, segue que  $k(k + 1)$  é par e que  $4k(k + 1)$  é múltiplo de  $4 \cdot 2 = 8$ . Consequentemente,  $4k(k + 1) + 1$  deixa resto 1 na divisão por 8.

**Exemplo 2.2.5:** Seja  $a$  um inteiro. Provar que um dos inteiros  $a$ ,  $a + 2$ ,  $a + 4$  é múltiplo de 3.

**Solução:** Aplicando o algoritmo da divisão por 3 temos que  $a = 3q + r$ , sendo  $0 \leq r < 3$ . Se  $r = 0$  temos  $a = 3q$ . Logo  $a$  é múltiplo de 3.

Se  $r = 1$  temos  $a = 3q + 1$ , somando 2 membro a membro temos  $a + 2 = 3q + 1 + 2$ , ou seja  $a + 2 = 3q + 3 = 3(q + 1)$ . Logo  $a + 2$  é múltiplo de 3.

Se  $r = 2$  temos  $a = 3q + 2$ , somando 4 membro a membro temos  $a + 4 = 3q + 2 + 4$ , ou seja  $a + 4 = 3q + 6 = 3(q + 2)$ . Logo,  $a + 4$  é múltiplo de 3.

Portanto se  $a$  é um inteiro então um dos inteiros  $a$ ,  $a + 2$  ou  $a + 4$  é múltiplo de 3.

**Exemplo 2.2.6:** O dobro de um número dividido por 5 deixa resto 1. Qual é o resto da divisão desse número por 5?

**Solução:** Sabemos que o número inteiro  $n$  procurado satisfaz  $2n = 5m + 1$ , para algum inteiro  $m$ . Então o produto  $5m = 2n - 1$  de 5 por  $m$  é ímpar, o que implica que  $m$  é ímpar. Assim,  $m = 2k + 1$ , para algum inteiro  $k$  e, portanto,  
 $2n = 5m + 1 = 5(2k + 1) + 1 = 10k + 6 = 2(5k + 3)$ , ou seja,  $n = 5k + 3$  deixa resto 3 na divisão por 5.

**Exemplo 2.2.7:** se  $n$  é ímpar, então  $n^2 - 1$  é divisível por 8.

**Solução:** Se  $n$  é ímpar, então  $n$  é da forma  $2k + 1$ ;  $k \in \mathbb{N}$ . Logo  $n^2 - 1 = (2k + 1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k(k + 1)$ , mas como o produto de dois números naturais consecutivos sempre é par, temos  $k(k + 1)$  será par, com isso,  $n^2 - 1 = 8q$ , onde  $q \in \mathbb{N}$ . Portanto,  $n^2 - 1$  é divisível por 8.

**Exemplo 2.2.8:** Demonstre que o quadrado de um inteiro é da forma  $8n$  ou  $8n+1$  ou  $8n + 4$ .

**Solução:** Seja  $m$  um número inteiro. Podemos escrever  $m = 4k$ ,  $m = 4k + 1$ ,  $m = 4k + 2$  ou  $m = 4k + 3$ .

Se  $m = 4k$  então  $m^2 = 16k^2 = 8(2k^2) = 8n$ .

Se  $m = 4k + 1$  então  $m^2 = (4k + 1)^2 = 16k^2 + 8k + 1 = 8(2k^2 + k) + 1 = 8n + 1$ .

Se  $m = 4k + 2$  então  $m^2 = (4k + 2)^2 = 16k^2 + 16k + 4 = 8(2k^2 + 2k) + 4 = 8n + 4$ .

Se  $m = 4k + 3$  então  $m^2 = (4k + 3)^2 = 16k^2 + 24k + 9 = 16k^2 + 24k + 8 + 1 = 8(2k^2 + 3k + 1) + 1 = 8n + 1$ .

**Exemplo 2.2.9:** (OBMEP - 2015): Sejam  $p$ ,  $q$  e  $r$  três números primos maiores que 3. Sabe-se que o número  $p + q + r$  também é primo. Mostre que  $p + q$ ,  $p + r$  ou  $q + r$  é um múltiplo de 6.

**Solução:** Primeiramente vejamos que, se um número  $n$  é maior que 3 e deixa resto 0, 2, 3 ou 4 na divisão por 6, então esse número não pode ser primo. Para isso, basta mostrar que o número pode ser escrito como o produto de dois números maiores que 1:

$$n = 6m + 0 = 2 \cdot 3 \cdot m;$$

$$n = 6m + 2 = 2 \cdot (3m + 1);$$

$$n = 6m + 3 = 3 \cdot (2m + 1);$$

$$n = 6m + 4 = 2 \cdot (3m + 2).$$

Logo, números primos maiores que 3 deixam resto 1 ou 5 na divisão por 6. Apliquemos isso aos números do enunciado. Como  $p + q + r$  também é primo, podemos concluir que os três não podem deixar todos os restos iguais a 1 ou todos restos iguais a 5, pois isso faria com que  $p + q + r$  fosse um múltiplo de 3 maior que 3 e naturalmente não poderia ser primo. Então, dentre os números  $p$ ,  $q$  e  $r$ , pelo menos um deixa resto 1 e pelo menos outro deixa resto 5 na divisão por 6. Somando-os, chegamos a um número múltiplo de 6.

**Exemplo 2.2.10:** Dados três inteiros,  $x$ ,  $y$ ,  $z$ , tais que  $x^2 + y^2 = z^2$ , mostre que  $x$  e  $y$  não são ambos ímpares e que  $xy$  é múltiplo de 6.

**Solução:** Suponha por absurdo  $x$  e  $y$  ímpares. Sendo  $x = 2m + 1$  e  $y = 2n + 1$  com  $m, n \in \mathbb{Z}$ . Como  $x^2 + y^2 = z^2$  logo  $4m^2 + 4m + 1 + 4n^2 + 4n + 1 = z^2$ , com isso  $4(m^2 + m + n^2 + n) + 2 = z^2$ , então  $4p + 2 = z^2$ , mostrando que  $z^2$  é par. Portanto  $z$  é par também. Fazendo  $z^2 = 4q^2$ . Com isso,  $4p + 2 = 4q^2$ , dividindo por 2 ambos os membros temos que  $2p + 1 = 2q^2$  o que é um absurdo.

Agora vamos mostrar que  $xy$  é um múltiplo de 3.

Também a prova será por absurdo. Suponha que  $x$  e  $y$  não são múltiplos de 3, logo  $x = 3q_1 + r_1$  e  $y = 3q_2 + r_2$  e com  $\{r_1, r_2\} \subset \{1, 2\}$ . Temos que :

$x^2 + y^2 = (3q_1 + r_1)^2 + (3q_2 + r_2)^2 = 9q_1^2 + 6q_1r_1 + r_1^2 + 9q_2^2 + 6q_2r_2 + r_2^2 = 3q_3 + 2 \neq z^2$ , pois temos que:

$$\text{Se } z = 3k \rightarrow z^2 = 3w_1$$

$$\text{Se } z = 3k + 1 \rightarrow z^2 = 3w_2 + 1$$

$$\text{Se } z = 3k + 2 \rightarrow z^2 = 3w_3 + 1$$

Logo um absurdo e Como  $x$  e  $y$  não são ímpares e  $xy$  é múltiplo de 3 então  $xy$  é múltiplo de 6.

**Observação 2.2.1:** Podemos usar os inteiros  $-8$ ,  $15$  e  $17$  para tratar do exemplo acima. Fazendo  $x = -8$ ,  $y = 15$  e  $z = 17$  podemos observar que  $(-8)^2 + (15)^2 = (17)^2$  e que  $-8$  e  $15$  não são ambos ímpares e também que o produto  $(-8)(15) = -120$  é um múltiplo de 6

### 3 MÁXIMO DIVISOR COMUM

No capítulo 2 foi abordado o conceito de divisor de um número inteiro dado, ou seja,  $a$  é divisor de  $b$  se existe  $q$  tal que  $b = a \cdot q$ . Agora vamos analisar os divisores comuns de dois inteiros dados, em particular, o maior destes divisores comum, é chamado de máximo divisor comum (MDC). Após apresentar a definição do MDC vamos analisar suas propriedades, bem como, trabalhar com métodos práticos que auxiliem na obtenção do MDC nos números inteiros e em seguida resolver situações problemas que envolvam o assunto. Por fim, apresentaremos os principais métodos ensinados pelos professores para o cálculo do MDC de números naturais no ensino básico.

#### 3.1.1 MÁXIMO DIVISOR COMUM NOS INTEIROS

Sabemos que se  $b$  é divisível por um inteiro  $a$ , então  $a$  divide  $b$ , Com isso podemos determinar o conjunto dos divisores inteiros de um número inteiro  $b$ , representado por  $D(b)$ .

##### Exemplo 3.1.1:

$$D(12) = \{ \pm 1, \pm 2, \pm 3, \pm 4, \pm 6 \text{ e } \pm 12 \}$$

$$D(18) = \{ \pm 1, \pm 2, \pm 3, \pm 6, \pm 9 \text{ e } \pm 18 \}$$

$$D(25) = \{ \pm 1, \pm 5 \text{ e } \pm 25 \}$$

Observando os conjuntos  $D(12)$  e  $D(18)$ , Notamos que existem números comuns entre os mesmos. Se denominarmos o conjunto  $D(12,18)$ , como sendo o conjunto dos divisores comuns de 12 e 18, temos que:  $D(12,18) = \{ \pm 1, \pm 2, \pm 3, \pm 6 \}$ .

Em Hefez (2005) encontraremos a seguinte definição de máximo divisor comum.

**Definição 3.1.1:** Diremos que um número natural  $d$  é um máximo divisor comum (MDC) de  $a$  e  $b$ , não simultaneamente nulos, se possuir as seguintes propriedades:

- i)  $d > 0$
- ii)  $d$  é um divisor comum de  $a$  e de  $b$ , e

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

**Exemplo 3.1.2:** Se os divisores comuns positivos dos inteiros 12 e 18 são tais que,  $D(12,18) = \{\pm 1, \pm 2, \pm 3, \pm 6\}$ . Logo o MDC dos números 12 e 18 será 6.

De fato, se  $d$  é um mdc de  $a$  e  $b$ , e  $c$  é um divisor comum desses números, então  $c \leq d$ . Isto mostra que o máximo divisor comum de dois números é o maior dentre todos os divisores comuns desses dois números.

Em particular, se  $d$  e  $d_0$  são máximos divisores comuns de um mesmo par de números, então  $d \leq d_0$  e  $d_0 \leq d$ , e, conseqüentemente,  $d = d_0$ , ou seja, o mdc de dois números é único.

Vamos representar o MDC de dois números inteiros  $a$  e  $b$  por  $(a, b)$  e como o MDC de  $a$  e  $b$  não está sujeito a ordem em que são tomados, temos que  $(a, b) = (b, a)$ .

**Observação 3.1.1:** Se  $a$  e  $b$  são números inteiros não ambos nulos, se existir o MDC de  $a$  e  $b$ , então:  $(a, b) = (-a, b) = (a, -b) = (-a, -b)$ . Com isso, quando o MDC de dois números for calculado, podemos supô-los não negativos. Como mostra a proposição seguinte:

**Proposição 3.1.1:** Se  $a$  e  $b$  forem inteiros não nulos então:

- i)  $(a, b) = (|a|, |b|)$ ;
- ii)  $(a, b) \leq \min\{|a|, |b|\}$ .

**Demonstração:** A prova de i) é fácil ver, pois os divisores comuns de  $a$  e  $b$  são os mesmos divisores comuns de  $|a|$  e  $|b|$ . Temos ainda, se  $d = (a, b)$ , então  $d$  é positivo e, como divide  $|a|$  e também divide  $|b|$ , com certeza vamos ter  $d \leq |a|$  e  $d \leq |b|$ , terminando a prova de ii).

**Observações 3.1.2:**

- i)  $(a, 1) = 1$ .
- ii)  $(a, 0) = |a|$ , com  $a \neq 0$ .
- iii) Se  $a$  é divisor de  $b$ , então  $(a, b) = a$ .
- iv) Se  $(a, b) = 1$ , então  $a$  e  $b$  são denominados primos entre si ou coprimos.

a)  $(23, 1) = 1$



b)  $(5,0) = 5$

c)  $(8,16) = 8$ , pois é divisor de 16.

d)  $(-5, 15) = (5, -15) = (-5, -15) = (5,15) = 5$ .

Outra maneira de calcular o MDC, a qual é ensinada no ensino fundamental do ensino básico, de dois ou mais números naturais é fazendo a decomposição desses números em fatores primos. O processo é o seguinte:

- 1) Será feita a decomposição desses números em fatores primos;
- 2) O MDC será o produto dos fatores primos comuns.

**Exemplo 3.1.3:** Vamos calcular o MDC entre 36 e 54:

**Solução:**  $36 = 2 \times 2 \times 3 \times 3$  e  $54 = 2 \times 3 \times 3 \times 3$ . Então o MDC será o produto dos fatores primos comuns:  $(36, 54) = 2 \times 3 \times 3 = 18$ .

**Observação 3.1.3:** O Teorema Fundamental da Aritmética nos diz que Todo número natural  $n$  maior que 1 pode ser escrito como um produto:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_m^{\alpha_m}$$

onde  $m \geq 1$  é um número natural,  $\alpha_i \in \mathbb{N}$  e  $p_i$  é primo para todo  $1 \leq i \leq m$ .

**Observação 3.1.4:** O MDC de dois números quando decomposto em fatores primos, é o produto dos fatores comuns a eles cada um elevado ao menor expoente.

Escrevendo a fatoração de 36 e 54 na forma de potência temos:  $36 = 2^2 \times 3^2$  e  $54 = 2 \times 3^3$ . Portanto  $(36, 54) = 2 \times 3^2 = 18$ .

**Exemplo 3.1.4:** (OBMEP - 2007) O produto de dois números de dois algarismos cada é 1728. Se o máximo divisor comum (MDC) deles é 12, quais são esses números?

**Solução:** Como 12 é o MDC dos dois números e cada um tem dois algarismos, os únicos candidatos são os múltiplos de 12 menores do que 100, ou seja, 12, 24, 36, 48, 60, 72, 84 e 96.

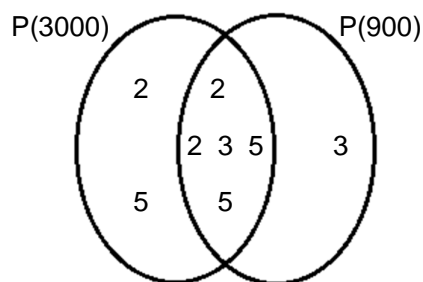
Como  $1728 = 12 \times 12 \times 12 = 2^6 \times 3^3$ , os múltiplos 60 (com fator 5) e 84 (com fator 7) não são divisores de 1728. Também  $1728 \div 12 = 144$  e  $1728 \div 96 = 18$ , de modo que a lista reduz para 24, 36, 48 e 72, com  $24 \times 72 = 36 \times 48 = 1728$ . Como o

MDC de 24 e 72 é 24, temos uma única solução, a saber, 36 e 48, cujo produto é 1728 e o MDC é 12.

**Exemplo 3.1.5:** calcular o M.D.C. entre 3000 e 900:

**Solução:** Temos que  $3000 = 2^3 \times 3 \times 5^3$  e  $900 = 2^2 \times 3^2 \times 5^2$ . Logo  $(3000, 900) = 2^2 \times 3 \times 5^2 = 300$ .

Utilizaremos os conceitos de conjuntos para calcular o MDC entre 3000 e 900. Para isso chamaremos de  $P(3000)$  e  $P(900)$ , respectivamente, os conjuntos dos fatores primos de 3000 e 900. Sendo assim, o MDC desses dois números será dado pelo produto dos elementos da interseção desses dois conjuntos.



**Figura 1:** Conjuntos com as fatorações de 3000 e 900. Fonte : Autor.

Logo o MDC de 3000 e 900 será dado por:  
 $(3000, 900) = P(3000) \cap P(900) = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 300$ .

O método acima nem sempre é o melhor de ser aplicado, pois, a fatoração pode ser bem trabalhosa quando forem dados números grandes. Existem outros métodos práticos que permitem obter o máximo divisor comum de dois inteiros, sem passar pela fatoração em primos, e um deles é conhecido como algoritmo de Euclides.

O lema abaixo auxiliará no entendimento do Algoritmo de Euclides e ele é mais conhecido como Lema de Euclides.

**Lema de Euclides 3.1.1:** Dados  $a, b, n \in \mathbb{N}$  com  $a < na < b$ . Vale a seguinte igualdade:  $(a, b) = (a, b - na)$ .

**Demonstração:** Seja  $(a, b - na) = d$ , logo  $d \mid (b - na)$ , mas também  $d \mid a$  (hipótese), com isso  $d \mid (b - na) + na$ , portanto  $d \mid b$ , assim  $d$  é um divisor comum de  $a$  e  $b$ , agora resta saber se  $d$  é máximo dos divisores comuns. Sendo  $c \in \mathbb{N}$  um divisor comum de  $a$  e  $b$ , nesse caso  $c \mid a$  e  $c \mid b$ , logo  $c \mid (b - na)$ , e então  $c \mid d$ . Portanto  $(a, b) = d$ .

A constatação da existência do MDC dada foi dada por Euclides no livro (Os Elementos, Livro VII). O algoritmo de Euclides é um método bem prático para obter o máximo divisor comum entre dois números inteiros, já que o MDC é o maior inteiro que divide os dois valores sem deixar resto. O algoritmo inicialmente foi descrito apenas para números naturais e comprimentos geométricos, mas em seguida foi estendido para outras classes de números. Em Hefez (2005) encontraremos a demonstração desse método.

**Teorema 3.1.1** Dados  $a, b \in \mathbb{N}$ , podemos supor  $a \leq b$ . Se  $a = 1$  ou  $a = b$ , ou ainda  $a \mid b$ , já vimos que  $(a, b) = a$ . Suponhamos, então, que  $1 < a < b$  e que  $a \nmid b$ . Logo, pela divisão euclidiana, podemos escrever:

$$b = aq_1 + r_1, \text{ com } 0 < r_1 < a:$$

Temos duas possibilidades:

a) Se  $r_1 \mid a$ , e, nesse caso, pela observação 2.1.2 iii) e pelo Lema de Euclides, temos que:  $r_1 = (a, r_1) = (a, b - q_1a) = (a, b)$ , e termina o algoritmo, senão temos:

b)  $r_1 \nmid a$ , e, em tal caso, podemos efetuar a divisão de  $a$  por  $r_1$ , obtendo  $a = r_1q_2 + r_2$ , com  $0 < r_2 < r_1$ : Novamente, temos duas possibilidades:

a')  $r_2 \mid r_1$ , e, em tal caso, novamente, pela observação 2.1.2 iii) e pelo Lema de Euclides, temos que:

$r_2 = (r_1, r_2) = (r_1, a - q_2r_1) = (r_1, a) = (b - q_1a, a) = (b, a) = (a, b)$ , e paramos, pois termina o algoritmo, senão temos

b')  $r_2 \nmid r_1$ , e, nesse caso, podemos efetuar a divisão de  $r_1$  por  $r_2$ , obtendo  $r_1 = r_2q_3 + r_3$ ; com  $0 < r_3 < r_2$ :

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais  $a > r_1 > r_2 > \dots$  que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordenação. Logo, para algum  $n$ , temos que  $r_n \mid r_{n-1}$  o que implica que  $(a, b) = r_n$ .

Vejamos um exemplo que ilustra melhor o teorema acima.

**Exemplo 3.1.6:** Qual é máximo divisor comum de 2248 e 1042?

**Solução:** Primeiramente vamos usar a divisão euclidiana e vamos notar que  $(2248, 1042)$  é igual ao  $(1042, r)$ , como foi visto anteriormente, e que  $r$  é o resto da divisão de 2248 por 1042, e assim, repetindo sucessivamente a divisão euclidiana teremos:

$$2248 = 1042 \cdot 2 + 164$$

$$1042 = 164 \cdot 6 + 58$$

$$164 = 58 \cdot 2 + 48$$

$$58 = 48 \cdot 1 + 10$$

$$48 = 10 \cdot 4 + 8$$

$$10 = 8 \cdot 1 + 2$$

$$8 = 2 \cdot 4 + 0.$$

Ou seja, do algoritmo de Euclides temos:  $(2248, 1042) = (1042, 164) = (164, 58) = (58, 48) = (48, 10)$ , e por fim é igual ao  $(10, 8) = 2$ , ou seja,  $(2248, 1042) = 2$ .

Então é notório que o Algoritmo de Euclides propicia uma maneira prática de fazer o MDC de dois números como a soma de dois múltiplos dos números em questão.

Podemos apresentar o algoritmo à cima usando o seguinte dispositivo prático:

<b>Quociente</b>		<b>2</b>	<b>6</b>	<b>2</b>	<b>1</b>	<b>4</b>	<b>1</b>	<b>4</b>
	<b>2248</b>	<b>1042</b>	<b>164</b>	<b>58</b>	<b>48</b>	<b>10</b>	<b>8</b>	<b>2</b>
<b>Resto</b>	<b>164</b>	<b>58</b>	<b>48</b>	<b>10</b>	<b>8</b>	<b>2</b>	<b>0</b>	

Vamos escrever o Algoritmo de Euclides de trás para frente, pois será apresentada uma informação complementar de grande importância:

Das igualdades acima podemos escrever:

$$\begin{aligned}
 2 &= 10 - 8 \cdot 1 \\
 8 &= 48 - 10 \cdot 4 \\
 10 &= 58 - 48 \cdot 1 \\
 48 &= 164 - 58 \cdot 2 \\
 58 &= 1042 - 164 \cdot 6 \\
 164 &= 2248 - 1042 \cdot 2
 \end{aligned}$$

Com isso temos,

$$\begin{aligned}
 2 &= 10 - 8 \cdot 1 \\
 &= 10 - (48 - 10 \cdot 4) \cdot 1 \\
 &= 10 - 48 \cdot 1 + 10 \cdot 4 \\
 &= 10 \cdot 5 - 48 \cdot 1 \\
 &= (58 - 48 \cdot 1) \cdot 5 - 48 \cdot 1 \\
 &= 58 \cdot 5 - 48 \cdot 5 - 48 \cdot 1 \\
 &= 58 \cdot 5 - 48 \cdot 6 \\
 &= 58 \cdot 5 - (164 - 58 \cdot 2) \cdot 6 \\
 &= 58 \cdot 5 - 164 \cdot 6 + 58 \cdot 12 \\
 &= 58 \cdot 17 - 164 \cdot 6 \\
 &= (1042 - 164 \cdot 6) \cdot 17 - 164 \cdot 6 \\
 &= 1042 \cdot 17 - 164 \cdot 102 - 164 \cdot 6 \\
 &= 1042 \cdot 17 - 164 \cdot 108 \\
 &= 1042 \cdot 17 - (2248 - 1042 \cdot 2) \cdot 108 \\
 &= 1042 \cdot 17 - 2248 \cdot 108 + 1042 \cdot 216 \\
 &= 1042 \cdot 233 - 2248 \cdot 108
 \end{aligned}$$

Sendo assim, podemos escrever:

$$2 = (2248, 1042) = (1042, 2248) = 1042 \cdot 233 - 2248 \cdot 108 = 1042 \cdot 233 + 2248 \cdot (-108).$$

Esse processo nos traz a um resultado muito importante na matemática que infelizmente algumas explicações no ensino fundamental omitem um fato interessante a respeito do máximo divisor comum de dois inteiros: O de que podemos expressá-lo como uma combinação linear desses dois números, ou seja: se  $d$  for o MDC de  $a$  e  $b$ , então é possível encontrar inteiros  $x$  e  $y$  tais que  $d = x \cdot a + y \cdot b$ .

**Teorema 3.1.2 (Relação de Bézout).** Seja  $d$  o máximo divisor comum de  $a$  e  $b$ . Então existem  $x_1$  e  $y_1$  inteiros, tais que  $d = x_1a + y_1b$ .

**Demonstração.** Seja  $A$  o conjunto de todas as combinações lineares  $xa + yb$ , com  $x$  e  $y$  inteiros. Obviamente,  $A$  contém números negativos, positivos e também o zero. Vamos escolher  $x_1$  e  $y_1$  tais que  $c = x_1a + y_1b$  seja o menor inteiro positivo pertencente ao conjunto  $A$ .

Primeiramente, será provado que  $c \mid a$  e  $c \mid b$ . Supondo que  $c \nmid a$ , logo, pelo Teorema 2.2.1, existem  $q$  e  $r$  tais que  $a = q \cdot c + r$  com  $0 \leq r < c$ . Portanto,

$$r = a - q \cdot c = a - q(x_1a + y_1b) = (1 - qx_1)a + (-qy_1)b.$$

Isto mostra que  $r \in A$ , o que é uma contradição, uma vez que  $0 \leq r < c$  e, por hipótese,  $c$  é o menor elemento positivo de  $A$ . Logo  $c \mid a$  e de forma análoga se prova que  $c \mid b$ . Daí,  $c \mid d$  pois  $d = (a, b)$ , portanto  $c \leq d$ .

Como  $d$  é o máximo divisor comum de  $a$  e  $b$ , então, existem inteiros  $q_1$  e  $q_2$  tais que  $a = q_1 \cdot d$  e  $b = q_2 \cdot d$  e, portanto,

$$c = x_1 \cdot a + y_1 \cdot b = x_1 \cdot q_1 \cdot d + y_1 \cdot q_2 \cdot d = d \cdot (x_1 \cdot q_1 + y_1 \cdot q_2) \text{ o que implica } d \mid c.$$

Logo  $d \leq c$ , e como  $c \leq d$ , segue que  $c = d = x_1a + y_1b$ .

**Proposição 2.1.2:** Sejam  $a, b \in \mathbb{Z}$ . Temos  $(a, b) = 1$  se, e somente se, existem inteiros  $x$  e  $y$  tais que  $1 = ax + by$ .

**Demonstração:** Pelo Teorema, está claro que se  $(a, b) = 1$  então existem inteiros  $x$  e  $y$  tais que  $1 = ax + by$ . Por outro lado, se existem tais inteiros e  $d = (a, b)$  então  $d \mid a$  e  $d \mid b$ , mas, assim,  $d \mid (ax + by)$ , ou seja,  $d \mid 1$ . Deste modo,  $d = 1$  o que termina a demonstração.

**Exemplo 3.1.7:** Provar que a fração  $\frac{2n+8}{4n+15}$  é irredutível para todo número natural  $n$ .

**Solução:** Usando o algoritmo de Euclides temos que:

$$4n + 15 = (2n + 8) \cdot 1 + 2n + 7;$$

$$2n + 8 = (2n + 7) \cdot 1 + 1;$$

$$2n + 7 = (2n + 7) \cdot 1.$$

Então o  $(4n + 15, 2n + 8) = 1$  e, portanto  $4n + 15$  e  $2n + 8$  são primos entre si para qualquer valor de  $n$ .

**Exemplo 3.1.8:** Seja  $n \in \mathbb{N}$ . Mostre que:  $(2n + 1, 9n + 4) = 1$

**Solução:** Observe que  $9n + 4 > 2n + 1$ , pelo algoritmo de Euclides segue que  $9n + 4 = 4 \times (2n + 1) + (n + 0)$  então  $2n + 1 = 2 \times n + 1$ , logo  $1 = 1 \times (2n + 1) + (-2) \times n$ , com isso,  $1 = 1 \times (2n + 1) + (-2)[9n + 4 - 4 \times (2n + 1)]$ , isto é,  $1 = (-2) \times (9n + 4) + 9 \times (2n + 1)$ . Então o  $(2n + 1, 9n + 4) = 1$  são primos entre si.

### Propriedades do Máximo Divisor Comum.

**Proposição 3.1.3.** Dados  $a$  e  $b$  números inteiros e  $n$  um inteiro positivo, tem-se que  $(na, nb) = n(a, b)$ .

**Demonstração:** Seja  $d = (a, b)$ , pelo teorema 2.1.1 existem  $x$  e  $y$  inteiros de modo que  $d = xa + yb$ . Como  $d \mid a$  e  $d \mid b$ , segue da proposição 1.1.3 que:

$nd \mid na$  e  $nd \mid nb$ , com  $n$  inteiro, portanto  $nd \mid (na, nb)$

Agora como  $(na, nb) \mid na$  e  $(na, nb) \mid nb$ , temos que:

$$(na, nb) \mid xna + ynb = n(xa + yb) = nd.$$

Logo, como  $nd \mid (na, nb)$ ,  $(na, nb) \mid nd$  e  $(na, nb) > 0$ , segue da proposição 1.1.6 que  $(na, nb) = nd$ , ou seja,  $(na, nb) \mid n(a, b)$ .

**Proposição 3.1.4.** Se  $c > 0$  e  $a$  e  $b$  são divisíveis por  $c$ , então  $\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)$ .

**Demonstração:** Como  $a$  e  $b$  são divisíveis por  $c$ , segue que  $\frac{a}{c}$  e  $\frac{b}{c}$  são números inteiros. Substituindo  $a$  por  $\frac{a}{c}$  e  $b$  por  $\frac{b}{c}$  e tomando  $k = c$  na Proposição 2.1.3 chega-se ao resultado desejado.

**Proposição 2.1.5:** Sejam  $a, b, c, d \in \mathbb{Z}$ . Valem as seguintes propriedades do máximo divisor comum:

i) se  $(a, b) = d$  então  $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ ;

ii) se  $a \mid b \cdot c$  e  $(a, b) = 1$  então  $a \mid c$ .

**Demonstração:** Para a demonstração de (i), usamos o Teorema e escrevemos  $d = a \cdot x + b \cdot y$ . Então, como  $d \mid a$  e  $d \mid b$  temos que os números  $\frac{a}{d}$  e  $\frac{b}{d}$  são naturais e, além disso,  $1 = \frac{a}{d}x + \frac{b}{d}y$ . Assim, pela proposição anterior, concluímos que  $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ . Agora para a prova (de ii) temos que se  $a \mid b \cdot c$  e  $(a, b) = 1$  então existem inteiros  $q, x$  e  $y$  tais que:

$$a \cdot q = b \cdot c \text{ e } 1 = a \cdot x + b \cdot y. (*)$$

Para garantir que  $a \mid c$ , devemos mostrar que existe  $s \in \mathbb{Z}$  tal que  $c = a \cdot s$ . Para chegar nesta afirmação, vamos multiplicar a segunda equação em (\*) por  $c$ :

$$c = a \cdot x \cdot c + \underbrace{b \cdot c}_{aq} \cdot y, \text{ ou seja, } c = a \cdot \underbrace{(x \cdot c + q \cdot y)}_s, \text{ com } s \in \mathbb{Z}, \text{ o que prova a proposição.}$$

**Proposição 3.1.6:** Se  $a, b, c, d \in \mathbb{Z}$  então vale o seguinte:

i) se  $a \mid c, b \mid c$  e  $(a, b) = d$  então  $\frac{a \cdot b}{d} \mid c$ ;

ii) se  $a \mid c, b \mid c$  e  $a$  e  $b$  são primos entre si então  $a \cdot b \mid c$ .

**Demonstração:** É suficiente fazer a prova do item (i), pois o item (ii) é um resultado imediato do mesmo.

Se  $a \mid c$  então existe um  $q \in \mathbb{Z}$  tal que  $c = a \cdot q$ .

E também se  $b \mid c$  então existe um  $k \in \mathbb{Z}$  tal que  $c = b \cdot k$

E ainda se  $(a, b) = d$  então existem  $x, y \in \mathbb{Z}$  tais que  $d = a \cdot x + b \cdot y$ . Com isso, ao multiplicar a última equação por  $c$ , obtemos:

$$d \cdot c = a \cdot x \cdot \underbrace{c}_{bk} + b \cdot y \cdot \underbrace{c}_{aq}, \text{ ou seja,}$$

$$d \cdot c = a \cdot b \cdot \underbrace{(x \cdot k + y \cdot q)}_m, \text{ com } m \in \mathbb{Z}. \text{ Mas como } \frac{a \cdot b}{d} \text{ pertence aos inteiros, logo,}$$

$$c = \frac{a \cdot b}{d} m, \text{ isto é, } \frac{a \cdot b}{d} \mid c.$$

### 3.2 APLICAÇÕES ENVOLVENDO O MÁXIMO DIVISOR COMUM



Nesta seção do capítulo serão resolvidos alguns problemas envolvendo os conceitos sobre o MDC.

**Problema 3.2.1:** (OBMEP - 2013) Um prédio tem três escadas diferentes, todas começando na base do prédio e terminando no topo. Uma escada tem 104 degraus, outra tem 117 degraus, e a outra tem 156 degraus. Sempre que os degraus das três escadas estão na mesma altura, há um andar. Quantos andares tem o prédio?

**Solução:** Chamaremos de X, Y e Z as três escadas, que têm 104, 117 e 156 degraus, respectivamente. Seja x o número de degraus da escada X entre cada dois andares, y o número de degraus da escada Y entre cada dois andares, e z o número de degraus da escada Z entre cada dois andares. Dividindo o número total de degraus de uma escada pelo número de degraus que esta escada tem entre cada dois andares, obtém-se o número de andares. Logo,

$$\frac{104}{x} = \frac{117}{y} = \frac{156}{z} = d$$

Onde d é o número de andares do prédio. Ou seja, d é um divisor comum de 104, 117 e 156. Além disso, d deve ser o maior possível, pois x, y e z são os menores possíveis. Portanto, d é o MDC de 104, 117 e 156. Calculando o MDC de 104, 117 e 156 pelo método da decomposição de fatores primos têm que:

$$104 = 2^3 \cdot 13$$

$$117 = 3^2 \cdot 13$$

$$156 = 2^2 \cdot 3 \cdot 13$$

Com isso, obtemos o número 13 como o MDC. Logo, o número de andares deste prédio é 13.

**Problema 3.2.2** O piso da sala de uma casa com o formato retangular, medindo 4,5 m × 3,6 m será revestido com cerâmicas quadradas, de mesma dimensão, inteiras, de forma que não fique espaço vazio entre cerâmicas vizinhas. As cerâmicas serão selecionadas de modo que tenham a maior dimensão possível. Nesse caso a dimensão do lado da cerâmica será?

**Solução:** Primeiramente, vamos converter essas dimensões da sala para centímetros: 4,5 m = 450 cm e 3,6 m = 360 cm

Para escolher a dimensão adequada do cerâmica que irá revestir o piso retangular devemos fazer o MDC de 450 e 360. O método que vamos escolher para resolver este problema será o Algoritmo de Euclides.

<b>Quociente</b>		<b>1</b>	<b>4</b>
	<b>450</b>	<b>360</b>	<b>90</b>
<b>Resto</b>	<b>90</b>	<b>0</b>	

A cerâmica quadrada que irá revestir a sala retangular terá 90 cm x 90 cm de dimensões.

**Problema 3.2.3 (Olimpíada Inglesa)** Se  $x$  e  $y$  são inteiros tais que  $2xy$  divide  $x^2 + y^2 - x$ , prove que  $x$  é um quadrado perfeito.

**Solução:** Seja  $d = (x, y)$ , isso implica que  $x = d \cdot a$  e  $y = d \cdot b$ , com  $a$  e  $b$  sendo coprimos. Do enunciado, temos:

$$2a \cdot b \cdot d^2 \mid d^2 \cdot a^2 + d^2 \cdot b^2 - d \cdot a \Rightarrow d^2 \mid d^2 \cdot a^2 + d^2 \cdot b^2 - d \cdot a \Rightarrow d^2 \mid -d \cdot a \Rightarrow d \mid a.$$

Logo,  $a = d \cdot c$ , para algum  $c$ . Como  $x \mid y^2$  obtemos que  $d^2 \cdot c \mid d^2 \cdot b^2$ , ou seja,  $c \mid b^2$  e  $(c, b^2) = c$ . Usando que  $(a, b) = 1$  e que todo divisor comum de  $b$  e  $c$  também é um divisor comum de  $a$  e  $b$ , podemos concluir que  $(c, b) = 1$  então  $(c, b^2) = 1$ . Portanto,  $c = 1$  e  $x = d^2 \cdot c = d^2$ .

**Problema 3.2.4:** Mostre que  $a \mid b \cdot c$  se, e somente se,  $\frac{a}{(a,b)} \mid c$ .

**Solução:**

( $\Rightarrow$ ) Vamos supor que  $a \mid b \cdot c$ , com isso,  $bc = ka$ . Para todo  $a, b \in \mathbb{N}$  temos que

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1, \text{ então } \frac{ax}{(a,b)} + \frac{by}{(a,b)} = 1, \text{ para todo } x, y \text{ pertencentes aos inteiros.}$$

Mas fazendo,  $\frac{acx}{(a,b)} + \frac{bcy}{(a,b)} = c$ , isso implica que  $\frac{axc}{(a,b)} + \frac{kay}{(a,b)} = c$ , com isso,

$$\frac{a}{(a,b)}(xc + ky) = c, \text{ portanto se } a \mid b \cdot c \text{ então } \frac{a}{(a,b)} \mid c.$$

( $\Leftrightarrow$ ) Agora suponha que  $\frac{a}{(a,b)} \mid c$ , então  $c = r \frac{a}{(a,b)}$ , com isso  $cb = r \frac{ab}{(a,b)} = \left[ \frac{rb}{(a,b)} \right] a$ .

Portanto, se  $\frac{a}{(a,b)} \mid c$  então  $a \mid b \cdot c$ .

**Problema 3.2.5 (ENEM 2015)** Um arquiteto está reformulando uma casa. De modo a contribuir com o meio ambiente, decide reaproveitar tábuas de madeira retiradas da casa. Ele dispõe de 40 tábuas de 540 cm, 30 de 810 cm e 10 de 1080 cm, todas de mesma largura e espessura. Ele pediu a um carpinteiro que cortasse as tábuas em pedaços de mesmo comprimento, sem deixar sobras, e de modo que as novas peças ficassem com o maior tamanho possível, mas de comprimento menor que 2 m.

Atendendo ao pedido do arquiteto, o carpinteiro deverá produzir:

- a) 105 peças.
- b) 120 peças.
- c) 210 peças.
- d) 243 peças.
- e) 420 peças.

**Solução:** Decompondo em fatores primos os números 540, 810 e 1080 teremos:

$$540 = 2^2 \cdot 3^3 \cdot 5^1,$$

$$810 = 2^1 \cdot 3^4 \cdot 5^1$$

$$1080 = 2^3 \cdot 3^3 \cdot 5^1$$

Portanto o MDC desses três números será  $2^1 \cdot 3^3 \cdot 5^1 = 270$ .

O comprimento de cada peça deve ser um divisor de 270 e como deve ser o maior possível e menor que 200 cm (2m), que será 135 cm.

A quantidade de peças obtidas pelo carpinteiro foi:

$$(40 \times 540 + 30 \times 810 + 10 \times 1080) / 135 = 420 \text{ peças.}$$

**Problema 3.2.6 (ENEM 2015):** O gerente de um cinema fornece anualmente ingressos gratuitos para escolas. Este ano serão distribuídos 400 ingressos para uma sessão vespertina e 320 ingressos para uma sessão noturna de um mesmo filme. Várias escolas podem ser escolhidas para receberem ingressos. Há alguns critérios para a distribuição dos ingressos:

- 1) cada escola deverá receber ingressos para uma única sessão;
- 2) todas as escolas contempladas deverão receber o mesmo número de ingressos;
- 3) não haverá sobra de ingressos (ou seja, todos os ingressos serão distribuídos).

O número mínimo de escolas que podem ser escolhidas para obter ingressos, segundo os critérios estabelecidos, é

- a) 2.
- b) 4.
- c) 9.
- d) 40.
- e) 80.

**Solução:** Usando o Algoritmo de Euclides vamos encontrar o mdc de 400 e 320:

	1	4
400	320	80
40	0	

Com isso, cada escola terá 80 ingressos, logo  $720/80 = 9$  será o número mínimo de escolas que podem ser escolhidas.

### 3.3 UM MÉTODO GEOMÉTRICO PARA OBTER O MÁXIMO DIVISOR COMUM.

Na revista professor de matemática (RPM), edição 29, existe um artigo interessante, do professor Zelci Clasen de Oliveira, que fala de um método geométrico para obtenção do MDC. O método consiste basicamente assim:

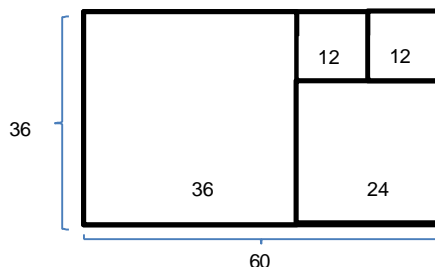
Dados dois números naturais  $a$  e  $b$ , construímos um retângulo com essas dimensões. Cobrindo esse retângulo com os maiores quadrados possíveis, o lado do menor quadrado será o MDC entre  $a$  e  $b$ .

Esse método utiliza o princípio das divisões sucessivas, visto através de uma imagem geométrica.

**Exemplo 3.2.1:** Calcular o mdc entre 60 e 36:

**Solução:** Observe, na figura abaixo, o retângulo de dimensões 60 e 36. Vamos cobrir esse retângulo com os maiores quadrados possíveis. Temos um quadrado de

lado 36, um quadrado de lado 24 e dois quadrados de lado 12. Isso quer dizer que o MDC entre 60 e 36 é 12.

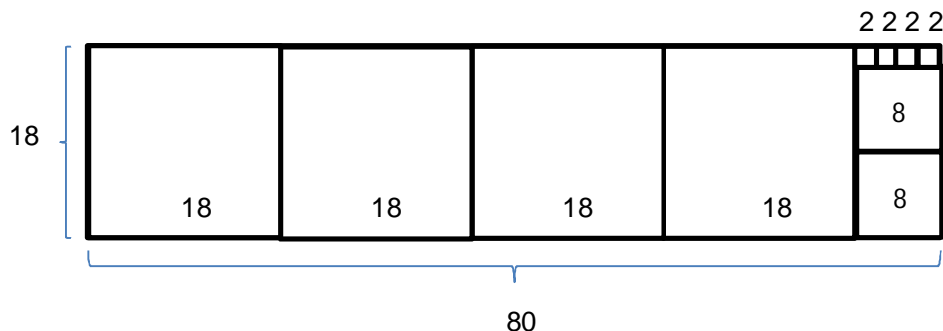


**Figura 2:** Interpretação geométrica do MDC. Fonte : Autor.

**Exemplo 3.2.2:** Um engenheiro deseja construir uma casa num terreno retangular de dimensões de 18 m de frente e 80 metros de profundidade. Mas antes deseja cercar o terreno com estacas. Se tiver uma estaca em cada canto do terreno e utilizar a mesma distância entre duas estacas seguidas, qual o número mínimo de estacas utilizadas?

**Solução:** O problema envolve o conceito de MDC. Se for o utilizado o Método geométrico ele pode ser resolvido da seguinte forma.

Observe, na figura abaixo, o retângulo de dimensões 80 por 18. Em seguida vamos dividir esse retângulo com os maiores quadrados possíveis. Serão quatro quadrados de lado 18, dois quadrados de lado 8 e 4 quadrados de lado 2. Portanto o MDC entre 80 e 18 será 2.



**Figura 3:** Interpretação geométrica do MDC. Fonte : Autor.

Na profundidade de 80 m teremos:  $80: 2 = 40$  estacas, somadas com as 40 do lado paralelo teremos 80 estacas.

Na frente de 18 m vamos ter:  $18: 2 = 9$  estacas, somadas com as nove do lado paralelo teremos 18 estacas. Portanto ao todo serão  $80 + 18 = 98$  estacas.

## 4 MÍNIMO MÚLTIPLO COMUM

Como foi realizado no capítulo anterior com o máximo divisor comum, também utilizaremos a mesma metodologia com mínimo múltiplo comum nesta seção. Primeiramente será apresentada sua definição, em seguida, suas propriedades, aplicações e principais métodos ensinados no ensino fundamental. E por fim também ilustraremos um método geométrico que foi demonstrado na revista do professor de matemática.

### 4.1 MÍNIMO MÚLTIPLO COMUM NOS INTEIROS

Seja  $n$  um número inteiro, tal que  $n \neq 0$ . Se multiplicarmos  $n$  pelo conjunto dos números inteiros,  $Z = \{\dots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, \dots\}$ , obteremos o conjunto  $M(n)$ , denominado o conjunto dos múltiplos de  $n$ .

#### **Exemplo 4.1.1:**

$$a) M(6) = \{\dots, -24, -18, -12, -6, 0, 6, 12, 18, 24, \dots\}$$

$$b) M(-8) = \{\dots, -32, -24, -16, -8, 0, 8, 16, 24, 32, \dots\}$$

$$c) M(10) = \{\dots, -30, -20, -10, 0, 10, 20, 30, \dots\}$$

**Observação 4.1.1:** notamos que, o inteiro zero é múltiplo de todo número inteiro, e que  $M(n) = M(-n)$ .

Ao comparar os conjuntos  $M(6)$  e  $M(-8)$ , observamos que nesses conjuntos constam alguns números comuns. Se denominarmos o conjunto  $M(6, -8)$ , como sendo o conjunto dos múltiplos comuns dos inteiros 6 e de -8, temos que:  $M(6, -8) = \{\dots, \pm 24, \pm 48, \pm 72, \dots\}$ .

**Definição 4.1.1:** Considere  $a$  e  $b$  inteiros não nulos. O mínimo múltiplo comum de  $a$  e  $b$  é o menor dentre os múltiplos positivos comuns de  $a$  e  $b$ .

**Definição 3.1.2:** Outra maneira de definir o mínimo múltiplo comum de dois números é se ele possuir as seguintes propriedades:

- (i)  $m > 0$
- (ii) é um múltiplo comum de  $a$  e  $b$ ;
- (iii) se  $c$  é um múltiplo comum de  $a$  e  $b$ , então  $m \mid c$ .

Suponha que  $m$  e  $m'$  são dois mínimos múltiplos comuns de  $a$  e  $b$ , então, temos de (ii) que  $m \mid m'$  e  $m' \mid m$ . Mas se  $m$  e  $m'$  são números naturais, temos que  $m = m'$ , o que prova que o mínimo múltiplo comum, se existir, ele será único. Agora, se  $m$  é o MMC de  $a$  e  $b$  e  $k$  é um múltiplo comum de  $a$  e  $b$ , então  $m \mid k$ . Logo, se  $k$  é positivo, temos que  $m \leq k$ , afirmando que  $m$  é o menor dos múltiplos comuns positivos de  $a$  e  $b$ .

**Observação 4.1.2:** Vamos representar o MMC de dois números inteiros  $a$  e  $b$ , não nulos, por  $[a, b]$ . Temos ainda que  $[-a, b] = [a, -b] = [-a, -b] = [a, b]$ .

**Proposição 4.1.1** Dados  $a$  e  $b$  inteiros positivos. Então se  $a$  é múltiplo de  $b$ , teremos que  $[a, b] = a$ .

**Demonstração:** Sabemos que os múltiplos comuns de  $a$  e  $b$  são múltiplos de  $a$ . Mas também, se um número é múltiplo de  $a$  igualmente será múltiplo de  $b$ , ou seja, um múltiplo comum de  $a$  e  $b$ . Com isso, o conjunto dos múltiplos comuns de  $a$  e  $b$  terão os mesmos elementos do conjunto dos múltiplos de  $b$ . Mas, Como o menor múltiplo positivo de  $a$  é ele mesmo, tem-se que  $[a, b] = a$ .

**Exemplo 4.1.2:**  $[5, 10] = 10$ .

**Proposição 4.1.2:** Dados dois números inteiros  $a$  e  $b$ , ambos não nulos, temos que  $[a, b]$  existe e  $[a, b](a, b) = |a \cdot b|$ :

**Demonstração:** Vamos dizer que  $a, b \in \mathbb{N}$ , e que  $k = \frac{ab}{(a,b)}$ , logo temos que,

$k = a \frac{b}{(a,b)} = b \frac{a}{(a,b)}$ , logo  $a \mid k$  e  $b \mid k$ . Agora, dado um  $c$  que seja múltiplo comum de  $a$

e  $b$ , então temos que  $c = na = n'b$ . Com isso,  $n \frac{a}{(a,b)} = n' \frac{b}{(a,b)}$ , mas sabemos do

capítulo anterior que,  $\frac{a}{(a,b)}$  e  $\frac{b}{(a,b)}$  são primos entre si, portanto  $\frac{a}{(a,b)}$  divide  $n'$  e que

$k = \frac{a}{(a,b)}b$  divide  $n'b$  que é igual a  $c$ .

Baseado na proposição acima, podemos através Algoritmo de Euclides calcular o mínimo múltiplo comum de dois inteiros, para isso, devemos dividir o módulo do produto dos dois números pelo seu MDC.

**Exemplo 4.1.3:** O máximo divisor de dois números é igual a 12 e o mínimo múltiplo comum deles é igual a 72. Se um deles é igual a 24, qual o outro?

**Solução:** Chamando de  $x$  o número a ser encontrado e pela a proposição a cima temos que:  $(x, 24)[x, 24] = x \cdot 24$  logo,  $12 \cdot 72 = 24 \cdot x$ , então  $864 = 24 \cdot x$ , portanto  $x = 36$ .

**Exemplo 4.1.4:** O produto de dois naturais  $a$  e  $b$  é igual a 100. Sabendo que  $[a, b] < 50$ , determine os possíveis valores de  $a$  e  $b$ .

**Solução:** Pelo teorema acima, temos  $ab = (a, b)[a, b]$  e como  $100 = 2^2 \cdot 5^2$ , então:  $100 = 2^2 \cdot 5^2 = (a, b)[a, b] < 2 \cdot 5^2 \cdot (a, b)$ . Então  $(a, b) > 2$ . Assim,  $a$  e  $b$  têm fator comum maior que 2 e como  $ab = 2^2 \cdot 5^2$ , as possibilidades são:  $a = 2 \cdot 5$  e  $b = 2 \cdot 5$  ou  $a = 5$  e  $b = 2^2 \cdot 5$ .

**Exemplo 4.1.5:** Se  $m$  é um múltiplo comum não nulo de  $a$  e  $b$ , mostre que:

$$m = [a, b] \Leftrightarrow \left(\frac{m}{a}, \frac{m}{b}\right) = 1$$

**Solução:**

( $\Rightarrow$ ) Seja  $m$  um múltiplo comum de  $a$  e  $b$ , logo  $a \mid m$  e  $b \mid m$ , e com isso,  $m = x \cdot a$  e  $m = y \cdot b$ .

Se  $m = [a, b]$ , então pela definição a cima temos que  $[a, b] \cdot (a, b) = ab$  de onde  $(m \cdot a, m \cdot b) = a \cdot b$  daí, se dividirmos  $a \cdot b$  por ambos membros da igualdade teremos que:

$$\frac{1}{a \cdot b}(m \cdot a, m \cdot b) = 1 \Rightarrow \left(\frac{m}{a}, \frac{m}{b}\right) = 1. \text{ Portanto, se } m = [a, b] \Rightarrow \left(\frac{m}{a}, \frac{m}{b}\right) = 1.$$



( $\Leftarrow$ ) Agora, digamos que  $\left(\frac{m}{a}, \frac{m}{b}\right) = 1$ , e se  $m$  é múltiplo de  $a$  e  $b$ , temos que  $m = x \cdot a$  e  $m = y \cdot b$ , logo  $(x, y) = 1$ . Com isso,  $(m \cdot x, m \cdot y) = m$ , sendo  $m \cdot x$  e  $m \cdot y$  múltiplos de  $a$  e  $b$ , e como  $m \mid m \cdot x$  e  $m \mid m \cdot y$ , e  $m$  é o menor dos múltiplos de  $a$  e  $b$ , segue que  $m = [a, b]$ . Portanto,  $\left(\frac{m}{a}, \frac{m}{b}\right) = 1 \Rightarrow m = [a, b]$ .

**Proposição 4.1.3:** Sejam  $a, b$  inteiros não nulos e  $n$  natural, mostre  $[na, nb] = n[a, b]$ .

Demonstração: Pela proposição 3.1.2 segue que  $[na, nb](na, nb) = na \cdot nb$ , agora usando a proposição 2.1.3 do capítulo anterior temos que  $na \cdot nb = n[na, nb](a, b)$ , isso implica que  $n \cdot \frac{ab}{(a, b)} = [na, nb]$ , logo  $n[a, b] = [na, nb]$  como queríamos provar.

O conceito de MMC entre dois números inteiros pode ser estendido a mais de dois números. Podemos encontrar a proposição que fala disso em Hefez.

**Definição 4.1.3** Diremos que o número natural  $m$  é um mmc dos inteiros não nulos  $a_1, \dots, a_n$ , se  $m$  é um múltiplo comum de  $a_1, \dots, a_n$ , e, se para todo múltiplo comum  $m'$  desses números, tem-se que  $m \mid m'$ . É fácil ver que o mmc, se existe, é único, sendo denotado por  $[a_1, \dots, a_n]$ .

**Proposição 4.1.4:** Sejam  $a_1, \dots, a_n$  números inteiros não nulos. Então existe o número  $[a_1, \dots, a_n]$  e  $[a_1, \dots, a_{n-1}, a_n] = [a_1, \dots, [a_{n-1}, a_n]]$ .

**Demonstração:** Teremos que provar que, se existe  $[a_1, \dots, [a_{n-1}, a_n]]$ , então acontecerá a igualdade acima.

A existência do MMC segue facilmente disso, por indução.

Seja  $m = [a_1, \dots, [a_{n-1}, a_n]]$ . Logo,  $a_1, \dots, a_{n-2}$  e  $[a_{n-1}, a_n]$  dividem  $m$ .

Como  $a_{n-1} \mid [a_{n-1}, a_n]$  e  $a_n \mid [a_{n-1}, a_n]$ , segue que  $m$  é um múltiplo comum de  $a_1, \dots, a_n$ . Por outro lado, suponha que  $m'$  seja um múltiplo comum de  $a_1, \dots, a_n$ . Logo,  $a_1 \mid m', \dots, a_{n-2} \mid m'$  e  $[a_{n-1}, a_n] \mid m'$ ; daí concluímos que  $m'$  é múltiplo de  $m = [a_1, \dots, [a_{n-1}, a_n]]$ .

**Exemplo 4.1.6:** Em uma casa há quatro lâmpadas, a primeira acende a cada 27 horas, a segunda acende a cada 45 horas, a terceira acende a cada 60 horas e a

quarta só acende quando as outras três estão acesas ao mesmo tempo. De quantas em quantas horas a quarta lâmpada vai acender?

**Solução:** Para resolver o problema vamos calcular o MMC entre 27, 45 e 60.

$$[27, 45, 60] = [27, [45, 60]] = [27, 180] = 540.$$

Nessa parte do capítulo vamos mostrar como é trabalhado o ensino do MMC de dois ou mais números naturais nos primeiros anos do ensino fundamental.

O MMC de dois ou mais números naturais é dado pelo produto de seus fatores primos positivos, comuns e não comuns, elevados aos seus maiores expoentes.

**Exemplo 4.1.7:** Calcule:

a)  $[360, 150]$ .

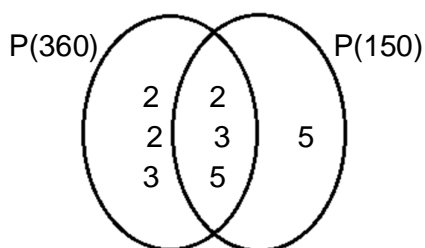
**Solução:** Escrevendo os números 360 e 150 na forma fatorada temos:

$$360 = 2^3 \cdot 3^2 \cdot 5 \text{ e } 150 = 2 \cdot 3 \cdot 5^2.$$

$$\text{Assim, } [360, 150] = 2^3 \cdot 3^2 \cdot 5^2 = 1800.$$

Do mesmo modo que fizemos com o MDC, vamos utilizar as ideias sobre conjuntos para encontrar o MMC do exemplo à cima.

Chamando  $P(360)$  e  $P(150)$ , respectivamente, os conjuntos dos fatores primos de 360 e 150, então:



**Figura 4:** Conjuntos com as fatorações de 360 e 150. Fonte : Autor.

Logo o MMC de 360 e 150 será dado pelo produto da união dos elementos  $P(360)$  e  $P(150)$ , ou seja:

$$(360, 150) = P(360) \cup P(150) = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 = 1800.$$

b)  $[250, 420]$ .

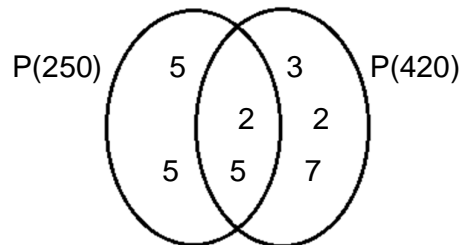
Colocando os elementos em fatores primos temos:

$$250 = 2 \cdot 5^3$$

$$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$$

$$\text{Assim, } [250, 420] = 2^2 \cdot 3 \cdot 5^3 \cdot 7 = 10500.$$

Fazendo pelo diagrama:



**Figura 5:** Conjuntos com as fatorações de 250 e 420. Fonte: Autor.

$$\text{Então: } [250, 420] = P(250) \cup P(420) = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 5 \cdot 7 = 10500.$$

Nesta parte do capítulo falaremos de um dos métodos mais aplicados para o cálculo do MMC, de dois ou mais números naturais, conhecido como decomposição simultânea em fatores primos. Nesse método os números dados são divididos simultaneamente por um número primo comuns. Se o resultado for uma divisão exata, será usado na sequência do cálculo o quociente dessa divisão. Mas, se o resultado dessa divisão não for possível de forma exata para todos os valores, repetimos o número que não foi dividido. Este processo segue até aparecer o número 1 em todas as sequências de divisões. Daí, resultando que o MMC será o produto dos fatores primos utilizados nessa fatoração.

**Exemplo 4.1.8:** Três satélites artificiais giram em torno da Terra em órbitas constantes. O tempo de rotação do primeiro é de 42 minutos, do segundo é de 72 minutos e do terceiro é de 126 minutos. Em dado momento eles se alinham em um mesmo meridiano, embora em latitudes diferentes. Eles voltarão em seguida a passar simultaneamente pelo mesmo meridiano depois de:

**Solução:** Para encontrar o tempo em que os satélites irão se alinhar novamente no mesmo meridiano temos que encontrar o MMC do tempo de rotações dos três satélites, logo:

42, 72, 126	2
21, 36, 63	2
21, 18, 63	2
21, 9, 63	3
7, 3, 21	3
7, 1, 7	7
1, 1, 1	

$[42, 72, 126] = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 = 504$ . Ou seja, os três satélites irão se alinhar novamente a 504 minutos do último alinhamento que equivale a 8 horas e 24 minutos.

#### 4.2 APLICAÇÕES ENVOLVENDO O MÍNIMO MÚLTIPLO COMUM

Nesta seção do capítulo vamos apresentar algumas aplicações envolvendo os conceitos sobre o MMC.

**Problema 4.2.1:** (PROFMAT - 2011) O máximo divisor comum entre dois números naturais é 16 e o mínimo múltiplo comum desses números é 576. É correto afirmar que:

- (a) Os dois números são maiores que 50.
- (b) O produto dos dois números é maior que 8000.
- (c) Os dois números são múltiplos de 32.
- (d) Os dois números são divisores de 96.
- (e) Um dos números é múltiplo do outro.

**Solução:** Usando a Proposição 3.1.2 temos que o produto de dois números é igual ao produto do seu MDC pelo seu MMC, logo  $16 \times 576 = 9216 > 8\ 000$ . Portanto a opção (B) é a verdadeira. O par (16, 576) é contraexemplo para (A), (C) e (D), e o par (64, 144) é contraexemplo para (E).

**Problema 3.2.2** (OBMEP - 2015) Em uma lousa são escritos os 2014 inteiros positivos de 1 até 2014. A operação permitida é escolher dois números  $a$  e  $b$ , apagá-los e escrever em seus lugares os números  $\text{mdc}(a, b)$  (Máximo Divisor Comum) e  $\text{mmc}(a, b)$  (Mínimo Múltiplo Comum). Essa operação pode ser feita com quaisquer dois números que estão na lousa, incluindo os números que resultaram de operações anteriores. Determine qual a maior quantidade de números 1 que podemos deixar na lousa.

**Solução:** A maior quantidade de números 1 que podemos deixar é 1007. Primeiro vamos mostrar como obtê-los. Para isso, basta tomar os pares de números consecutivos,  $(1, 2)$ ,  $(3, 4)$ ,  $(5, 6)$ , ...,  $(2013, 2014)$  e realizar a operação em cada par. Sabendo que números consecutivos não têm fator comum, cada um dos máximos divisores comuns será 1. Não é possível obter mais do que isso, pois a quantidade de números pares não se altera no decorrer das operações. Isso ocorre, pois, se operarmos com dois números pares, teremos como resultado dois números pares, se operarmos com dois números ímpares teremos como resultado dois números ímpares e se operarmos com um número par e um número ímpar obteremos também um número par e um número ímpar. Começamos com 1007 números pares e sempre teremos 1007 números pares.

**Problema 4.2.3** Mostre que  $(a, b) = [a, b]$ , se e somente se  $a = b$ .

**Solução:**

$(\Rightarrow)$  Suponha que  $(a, b) = [a, b]$ , então pela Proposição 3.1.2 temos que:

$[a, b](a, b) = ab$ , isso implica que  $[a, b]^2 = ab$ . Chamando  $m = [a, b]$  tal que  $m = xa$  e  $m = yb$  daí,

$$m^2 = (xa)^2 = ab \rightarrow x^2a = b \text{ ou}$$

$$m^2 = (yb)^2 = ab \rightarrow y^2b = a.$$

Substituindo um no outro temos que:

$$y^2(x^2a) = a \rightarrow (yx)^2 = 1 \rightarrow x = y = 1, \text{ logo } a = b.$$

$(\Leftarrow)$  Seja  $a = b$  então,  $[a, b] = [a, a] = a$  e  $(a, b) = (a, a) = a$ , Portanto  $[a, b] = (a, b)$ .

**Problema 4.2.4** (OBMEP - 2009) Uma doceira foi ao mercado comprar ovos para fazer 43 bolos, todos com a mesma receita, que requer menos do que nove ovos. O

vendedor repara que se tentar embrulhar os ovos que a doceira comprou em grupos de dois, ou de três, quatro, cinco, ou seis ovos, sempre sobra um ovo. Quantos ovos ela usa em cada bolo? Qual é o menor número de ovos que a doceira vai gastar para fazer os 43 bolos?

**Solução:** Como os 43 bolos tem a mesma receita, o número de ovos que a doceira precisa é um múltiplo de 43. Por outro lado, esse numero também é um múltiplo de 2, 3, 4, 5 e 6 acrescido de 1. O MMC de 2, 3, 4, 5 e 6 é 60, mas  $60 + 1 = 61$  não é múltiplo de 43. Precisamos, então, encontrar um numero com essas duas propriedades:

- é múltiplo de 43;
- acrescido de 1 é múltiplo de 2, 3, 4, 5 e 6.

Lembre também que como a receita gasta menos de 9 ovos, o número que estamos procurando é menor do que  $43 \times 9 = 387$ . Temos:

$$60 \times 2 + 1 = 121 \text{ não é múltiplo de } 43$$

$$60 \times 3 + 1 = 181 \text{ não é múltiplo de } 43$$

$$60 \times 4 + 1 = 241 \text{ não é múltiplo de } 43$$

$$60 \times 5 + 1 = 301 \text{ é múltiplo de } 43$$

$$60 \times 6 + 1 = 361 \text{ não é múltiplo de } 43$$

Podemos parar por aqui porque os próximos números serão maiores do que 387. Logo, a doceira comprou 301 ovos

**Problema 4.2.5** Sejam  $a$ ,  $b$  e  $c$  três números naturais não nulos. Mostre que:

$$abc = [a, b, c](ab, ac, bc):$$

**Solução:** Chamando de  $d$  o MDC de  $a$  e  $b$ , como  $(ab, ac, bc) = (ab, (ac, bc))$ , então:

$$(ab, ac, bc) = (ab, (ac, bc)) = (ab, c(a, b)) = (ab, cd):, \text{ isto implica que :}$$

$$(ab, ac, bc) = (ab, cd) = \frac{abcd}{[ab,cd]}.$$

Por outro lado,  $[a, b, c] = [[a, b], c] = \left[\frac{ab}{d}, c\right] = [am, c]$ , onde  $b = md$ .

$$(ab, ac, bc) = \frac{abcd}{[ab,cd]} = \frac{abcd}{[amd,cd]} = \frac{abcd}{d[am,c]} = \frac{abc}{[am,c]} = \frac{abc}{[a,b,c]} . \text{ Portanto,}$$

$abc = [a, b, c](ab, ac, bc)$  como queríamos provar.

Observação:  $am = [a,b]$ , pois  $(a,b)[a,b] = ab \Rightarrow d[a,b] = amd \Rightarrow am = [a,b]$

### 4.3 MÉTODOS GEOMÉTRICOS PARA O CÁLCULO DO MÍNIMO MÚLTIPLO COMUM.

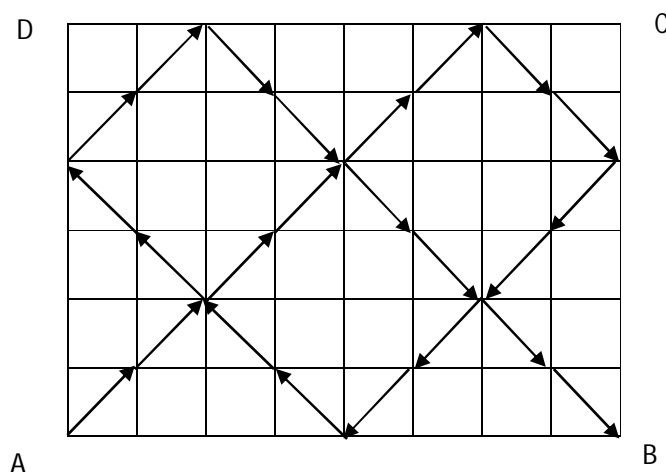
No capítulo anterior foi apresentado um método geométrico para o cálculo do Máximo divisor comum. Esse método usa o conceito das divisões sucessivas de dois números naturais adaptada a geometria.

A mesma revista, na edição 32 também traz um artigo, escrito pelos professores Mário Lúcio Cardoso e Otânio Alves Gonçalves, que fala de um modelo geométrico para o cálculo do MMC. Esse método pode ser descrito como:

- 1) Tomemos um retângulo ABCD de lados  $m$  e  $n$ . O retângulo deverá estar subdividido em quadrados unitários.
- 2) Partindo de um dos vértices do retângulo, traçamos as diagonais dos quadrados unitários observando a seguinte ordem:
  - a) traçamos a diagonal do quadrado que tem o vértice coincidente com o vértice escolhido do retângulo.
  - b) traçamos, a partir do vértice no qual paramos, as diagonais dos quadrados que têm um ângulo oposto pelo vértice com o quadrado anterior ou, na ausência desse quadrado, traçamos a diagonal do quadrado ao lado e a partir do vértice onde paramos.
  - c) As diagonais dos quadrados unitários devem ser traçadas até que se chegue a um dos outros vértices do retângulo ABCD.
  - d) Contamos quantos quadrados tiveram suas diagonais traçadas. O número encontrado é o MMC de  $m$  e  $n$ .

**Exemplo 4.3.1:** Dois navios fazem viagens entre dois portos. O primeiro a cada 6 dias, o segundo a cada 8 dias. Se esses navios partirem juntos, depois de quantos dias voltarão a sair juntos, novamente?

Primeiramente, vamos construir um retângulo dividido em quadrados unitários, com dimensões 8 por 6. Depois iremos escolher um vértice desse retângulo para iniciar as ligações das diagonais.



**Figura 6:** Interpretação geométrica do MMC. Fonte : Autor.

Portanto, ao chegar ao outro vértice do retângulo foram contabilizados 24 diagonais nos quadrados unitários. Isso significa que o MMC entre 8 e 6 será 24.

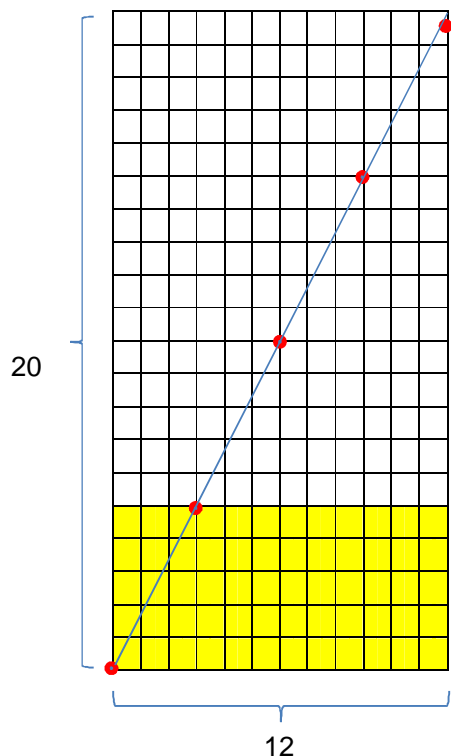
Apesar desse método ser interessante para nossos alunos, ele não seria muito prático para o cálculo do MMC envolvendo números de valores alto, pois seria um pouco trabalhoso construir o retângulo subdividido em quadrados unitários para em seguida traçar suas diagonais.

No encerramento desse capítulo vamos destacar um novo método muito interessante que possibilita mostrar o mesmo tempo o MDC e o MMC de dois números naturais. Esse procedimento também foi demonstrado pelo professor Marcelo Polezzi na revista professor de matemática edição 51. Para realizar tal feito devemos seguir as etapas:

1. Faça um retângulo de dimensões inteiras  $a$  e  $b$ , dividido em quadradinhos unitários.
2. Escolha um vértice do retângulo e trace sua diagonal. Marque pontos na interseção dessa diagonal com os vértices dos quadradinhos unitários.
3. Contabilize em quantos segmentos esses pontos dividem a diagonal: É esse número  $d$  é o MDC de  $a$  e  $b$ .
4. Agora faça linhas verticais (horizontais) passando por cada um dos pontos que você marcou, unindo dois lados opostos do retângulo. Conte o número de quadradinhos unitários existentes em qualquer um dos  $d$  retângulos determinados por essas linhas verticais (horizontais): Esse número  $m$  é o MMC de  $a$  e  $b$ .



**Exemplo 4.3.2:** A figura a seguir ilustra o procedimento para  $a = 12$  e  $b = 20$ .



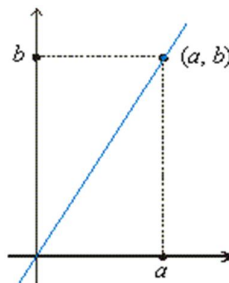
**Figura 7:** Interpretação geométrica do MDC e do MMC. Fonte: Autor.

A diagonal está dividida em quatro partes iguais, logo,  $(12, 20) = 4$ .

O número de quadradinhos existentes em qualquer um dos três retângulos é  $5 \times 12 = 60$ , Portanto  $[12, 60] = 60$ .

### Justificativa do método

Chamando o MDC entre  $a$  e  $b$  de  $d$  e supondo que existam  $p$  e  $q$  números inteiros tais que  $a = d \cdot p$  e  $b = d \cdot q$ , onde  $p$  e  $q$  são coprimos. Fazemos um sistema de coordenadas ortogonais com a origem em um dos vértices do retângulo.



**Figura 8:** Reta de equação  $y = \frac{b}{a} x$ .

Se observarmos a reta de equação  $y = \frac{b}{a}x$  é a diagonal desse retângulo. Notemos que  $\frac{b}{a} = \frac{q}{p}$ , com isso,  $(0,0)$ ;  $(p, q)$ ;  $(2p, 2q)$ ; ...;  $(d \cdot p, d \cdot q)$  pertencem a reta da diagonal. Logo existem  $d + 1$  coordenadas inteiras, com a mesma distância entre elas.

Para provar que são apenas essas as coordenadas inteiras que pertence a essa diagonal, vamos supor que  $(r, s)$  está contido nessa diagonal e possui coordenadas inteiras, logo  $s = \frac{b}{a}r = \frac{q}{p}r$ . Então  $s \cdot p = q \cdot r$  e, como  $(p, q) = 1$ , tem-se que  $s = t \cdot q$  e  $r = t \cdot p$ , com  $0 \leq t \leq d$ . Logo, a diagonal fica dividida em  $d$  pedaços iguais.

Se as  $d + 1$  coordenadas são igualmente espaçadas, os  $d$  retângulos obtidos na condição 4 têm a mesma área  $m$ . Com isso,  $m \cdot d = a \cdot b$ , o que prova que  $m = [a, b]$  e  $m$  é também o número de quadradinhos contido nos retângulos.

## 5 A EXISTÊNCIA DO MÁXIMO DIVISOR COMUM

Vimos que o MDC existe nos inteiros. Nesta última etapa do trabalho abordaremos sobre o domínio Euclideano, ilustrando alguns exemplos, bem como os seus principais resultados para enfim chegar ao objetivo principal que é demonstrar a existência do máximo divisor comum entre dois elementos em outros conjuntos numéricos.

Sabemos que nem sempre dois números possuem o MDC. Por exemplo, temos os pares de elementos  $4$  e  $2 + 2\sqrt{3}i$ . Podemos observar que ambos são divididos por  $2$  e  $1 + \sqrt{3}i$ , mas os mesmos não são múltiplos um do outro, portanto  $4$  e  $2 + 2\sqrt{3}i$  não podem ter MDC. Com isso, para tratar da existência do MDC entre dois elementos temos que conhecer outras classes de números, mas especificamente os domínios euclidianos.

Antes de falarmos dos domínios euclidianos apresentaremos algumas definições que serão bastante úteis para que possamos entender melhor a estrutura desses domínios.

### 5.1 ANÉIS

**Definição 5.1.1:** Um anel  $(A, +, \cdot)$  é um conjunto provido de uma operação chamada de adição e expressada por  $+$  e outra operação chamada de multiplicação e denotada por  $\cdot$  e que atendam os seguintes requisitos:

- A1. Para todo  $x, y, z \in A$ ,  $(x + y) + z = x + (y + z)$  (associatividade da adição);
- A2. Existe  $0 \in A$  tal que para todo  $x \in A$ ,  $x + 0 = x$  e  $0 + x = x$  (existência do elemento neutro referente a adição);
- A3. Para todo  $x \in A$  existe um único  $y \in A$ , expressado por  $y = -x$ , tal que  $x + y = 0$  e  $y + x = 0$  (existência do inverso aditivo);
- A4. Para todo  $x, y \in A$ ,  $x + y = y + x$  (A adição é comutativa);
- A5. Para todo  $x, y, z \in A$ ,  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$  (A multiplicação é associativa);

A6. Para todo  $x, y, z \in A$ ,  $x \cdot (y + z) = x \cdot y + x \cdot z$  (A adição é distributiva relativamente à multiplicação).

A7. Dizemos que um anel  $(A, +, \cdot)$  é um anel com unidade se satisfizer a seguinte propriedade: Existe  $1 \in A - \{0\}$ , tal que  $x \cdot 1 = 1 \cdot x = x$ , qualquer que seja  $x \in A$ .

A8. Dizemos que um anel  $(A, +, \cdot)$  é comutativo se satisfizer a seguinte propriedade: Para todo  $x, y \in A$ ,  $x \cdot y = y \cdot x$ .

**Definição 5.1.2:** Dado um anel comutativo  $A$ , ele será dito um domínio de integridade desde que possua a propriedade:

Para todo  $a, b \in A$ , se  $a \cdot b = 0$ , então  $a = 0$  ou  $b = 0$ , ou seja,  $A$  é um domínio de integridade se, e somente se, para todo  $a, b \in A \setminus \{0\}$ ; tem - se que  $a \cdot b \neq 0$ .

**Exemplo 5.1.1:** Os conjuntos dos números inteiros, racionais, reais e os dos números complexos são exemplos de domínios de integridade.

**Definição 5.1.3:** Seja  $A$  um anel comutativo. Um elemento  $a \in A$  invertível com relação ao produto é denominado uma unidade.

**Exemplo 4.1.2:** Os números 1 e -1 são as unidades nos conjuntos dos inteiros.

**Definição 5.1.4:** Seja  $B$  um subconjunto não vazio de um anel  $A$  será dito um subanel de  $A$  se, com as operações de  $A$ , continuar ainda sendo um anel.

**Exemplo 5.1.3:**  $n\mathbb{Z}$  é um subanel de  $\mathbb{Z}$ . Mais geralmente,  $n\mathbb{Z} \subseteq \mathbb{Z}$  são subanéis, para todo  $n \geq 0$ . De fato, para todo  $a, b \in n\mathbb{Z} \Rightarrow a = nk_1, b = nk_2$ , com  $k_1, k_2 \in \mathbb{Z}$ . Assim,  $a - b = n(k_1 - k_2) \in n\mathbb{Z}$  e  $a \cdot b = n(k_1 k_2 n) \in n\mathbb{Z}$ .

**Definição 5.1.5:** Um subconjunto não vazio  $B$  de um anel  $A$  é um subanel de  $A$  se, e somente se, as seguintes condições são atendidas:

- (i)  $0 \in B$ ;
- (ii)  $1 \in B$ ;
- (iii) se  $a, b \in B$ , então  $a + b \in B$ ;
- (iv) se  $a, b \in B$ , então  $a \cdot b \in B$ ;
- (v) se  $a \in B$ , então  $-a \in B$ .

**Observação 5.1.1:** todo subanel  $A$  dos números complexos necessariamente contém os inteiros, pois possui 0 e 1 e é fechado para as operações de adição e de subtração. Logo,  $\mathbb{Z}$  é um subanel de  $A$ . Além do mais, todo subanel dos números complexos é um domínio de integridade, já que o conjunto dos complexos é um domínio de integridade.

**Definição 5.1.6:** um anel  $(K, +, \cdot)$  será chamado de corpo se ele possuir a seguinte condição: Todo elemento diferente de zero de  $K$  possui um elemento inverso com respeito à multiplicação, isto é, Para todo  $x \in K \setminus \{0\}$ , existe  $y \in K$  tal que  $x \cdot y = 1$ .

**Exemplo 5.1.4.** Com as operações usuais, o anel dos inteiros  $\mathbb{Z}$  é um domínio que não é corpo. Já os conjuntos  $\mathbb{R}$ ,  $\mathbb{Q}$ ,  $\mathbb{C}$  são corpos.

**Definição 5.1.7:** Um subconjunto  $K$  de um corpo  $M$  que, com as operações de adição e de multiplicação de  $M$ , é ainda um corpo, será chamado de subcorpo de  $M$ .

**Definição 5.1.8:** Um elemento  $a \in A$  é dito irredutível se para toda fatoração  $a = b \cdot c$  temos  $b$  unidade ou  $c$  unidade.

**Definição 5.1.9:** Um função  $N : A \rightarrow \mathbb{N}$  é dita norma de  $A$  se satisfaz as seguintes condições:

- (i)  $N(ab) = N(a)N(b)$  para todo  $a, b \in R$ ;
- (ii)  $N(a) = 1$  se, e somente se,  $a$  é unidade em  $A$ .

**Definição 5.1.10:** Seja  $(A, +, \cdot)$  um anel e seja  $I$  um subconjunto não vazio de  $A$ . Dizemos que  $I$  é um ideal de  $A$  se:

- $x + y \in I$ , para todo  $x, y \in I$
- $a \cdot x \in I$ , para todo  $a \in A$ .

**Exemplo 5.1.5:**  $\{0\}$  e  $R$  são os ideais triviais de  $R$ .

**Exemplo 5.1.6:** seja  $n \geq 0$  um inteiro. O subconjunto de  $n\mathbb{Z} = \{zn \mid z \in \mathbb{Z}\}$  é um ideal do anel dos inteiros. Mais geralmente, seja  $(A, +, \cdot)$  um anel e sejam  $a_1, a_2, \dots, a_t$  elementos do anel  $A$ . Então, o subconjunto:

$Aa_1 + Aa_2 + \dots + Aa_t = \{a_1x_1 + a_2x_2 + \dots + a_t x_t \mid x_1, x_2, \dots, x_t \in A\}$  é um ideal de  $(A, +, \cdot)$  que será denotado por  $(a_1, a_2, \dots, a_t)$ .

**Definição 5.1.11:** Um domínio de integridade  $A$  que contenha um elemento identidade é um anel principal se todo ideal  $I$  em  $A$  é da forma  $I = \langle a \rangle$ , para algum  $a \in A$ , ou seja, um ideal é principal quando ele é gerado por um único elemento pertencente a  $A$ .

**Definição 5.1.12:** Um domínio  $A$  é chamado de domínio principal se todo ideal de  $A$  for principal.

**Exemplo 5.1.8:** O anel  $\mathbb{Z}$  é um exemplo de domínio principal, pois todos os seus ideais são principais.

## 5.2 DOMÍNIO EUCLIDEANO

Basicamente o algoritmo de Euclides fala que no conjunto dos inteiros é possível fazer a divisão de um elemento  $a$  por um elemento  $b$  gerando “um resto pequeno”, ou melhor, dizendo, um resto onde seu valor absoluto será menor que o valor absoluto de  $b$ . Vamos tentar generalizar esse conceito. Mas, para que isso ocorra devemos ter um conjunto munido de duas operações (adição e multiplicação) e um modo que possamos determinar que um elemento seja menor que o outro. Esse será o conceito de um domínio Euclideano, ou seja, é a generalização do algoritmo de divisão dos inteiros para anéis (domínios de integridade) em geral.

**Definição 5.2.1:** Um domínio euclideano  $\langle D, +, \cdot, v \rangle$  é um domínio de integridade  $\langle D, +, \cdot \rangle$  e uma função  $v$  dos elementos não nulos de  $D$  dos inteiros não negativos tais que:

1. Para todos os pares  $a, b$  de elementos de  $D$  para os quais  $b \neq 0$  existem  $q$  e  $r$  em  $D$  tais que:

$$a = bq + r \text{ e } 0 = r \text{ ou } v(r) \leq v(b).$$

2. Para todos os pares  $a, b$  de elementos de  $D$  para os quais  $a \neq 0$  e  $b \neq 0$

$$v(a) \leq v(ab).$$

**Teorema 5.2.1:** O conjunto  $G$ , denominado de Inteiros gaussianos, onde todos os números complexos da forma  $a + bi$ , tal que  $a$  e  $b$  são números inteiros e tem como norma  $N(\alpha) = \alpha\bar{\alpha}$  será um domínio euclidiano, onde  $\alpha = a + bi$ .

**Demonstração:** Teremos que  $N(\alpha) = 0$  se, e somente se  $\alpha = 0$ . Com isso,  $N(\alpha) \geq 1$ , para todo  $\alpha \neq 0$ . Sabemos da definição 4.1.9 que  $N(\alpha\beta) = N(\alpha)N(\beta)$ , logo  $N(\alpha\beta) \geq N(\alpha)$ .

Se  $\alpha$  e  $\beta \neq 0$ . Então temos que achar  $\rho$  e  $\sigma$  tais que  $\alpha = \beta \cdot \sigma + \rho$ , onde  $\rho = 0$  ou  $N(\rho) < N(\beta)$ . Como  $\beta \neq 0$  segue que  $\rho = \alpha - \beta \cdot \sigma = \beta\left(\frac{\alpha}{\beta} - \sigma\right)$ , e sabemos dos números complexos que  $N(\rho) = \rho\bar{\rho} = |\rho|^2$ , daí  $|\rho|^2 = |\beta|^2 \left|\frac{\alpha}{\beta} - \sigma\right|^2$ . Logo  $N(\rho) < N(\beta)$ . Se  $\left|\frac{\alpha}{\beta} - \sigma\right|^2 < 1$ . Agora temos que escolher  $\sigma \in G$  tal que  $\left|\frac{\alpha}{\beta} - \sigma\right|^2 < 1$ .

Seja  $\alpha = a + bi$  e  $\beta = c + di$  e  $\frac{\alpha}{\beta} = x + yi$  onde  $x$  e  $y$  são números reais. Tomaremos os inteiros  $\theta$  e  $\delta$  tais que  $|x - \theta| < \frac{1}{2}$  e  $|y - \delta| < \frac{1}{2}$  e seja  $\sigma = \theta + \delta i$ , então;  $\sigma \in G$  e  $\left|\frac{\alpha}{\beta} - \sigma\right|^2 = |x + yi - (\theta + \delta i)|^2 = |(x - \theta) + (y - \delta)i|^2 = (x - \theta)^2 + (y - \delta)^2 < \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1$ .

Assim encontrando o  $\sigma$  desejado e fazendo  $\rho = \alpha - \beta\sigma$  teremos provado o teorema.

**Exemplo 5.2.1:** Se  $k$  for um corpo. Então, o anel de polinômios  $K[x]$  é um domínio Euclidiano.

De fato, Chamamos  $\varphi(p(x)) = \text{grau}(p(x))$ . O segundo requisito do domínio Euclidiano é imediato. Vamos nos atentar na primeira condição. Se  $f(x) = 0$  ou  $\text{grau } f(x) < \text{grau } g(x)$ , então nada a fazer. Suponha que  $f(x), g(x) \in K[x]$ , e  $\text{grau } f(x) \geq \text{grau } g(x)$ , faça  $f(x) = a_n x^n + \dots + a_0$  e  $g(x) = b_m x^m + \dots + b_0$ . Note que  $f_1(x) = f(x) - \frac{a_n}{b_m} x^{n-m} g(x)$  é tal que  $\text{grau } f_1(x) < \text{grau } f(x)$  e  $f(x) = \frac{a_n}{b_m} x^{n-m} g(x) + f_1(x)$ . Se  $f_1(x) = 0$  ou  $\text{grau } f_1(x) < \text{grau } g(x)$ , então nada mais a fazer. Caso o contrário, refaça o processo para  $f_1(x)$  e ache  $f_2(x)$ , que atenda  $f_1(x) = p(x) \cdot g(x) + f_2(x)$  com  $\text{grau } f_2(x) < \text{grau } f_1(x)$ . Se  $f_2(x) = 0$  ou  $\text{grau } f_2(x) < \text{grau } g(x)$ , então acabou. Se não, repita as etapas até achar um  $f_k(x)$  apropriado. Portanto  $K[x]$  é um domínio Euclidiano.

Veremos algumas definições envolvendo o algoritmo euclidiano em um domínio euclidiano  $\langle D, +, \cdot, v \rangle$ .

**Lema 5.2.1:** Se  $a \in D$ ,  $a \neq 0$ , então  $v(a) \geq v(1)$ .

**Demonstração:** Se  $1 \cdot a = a$  resulta que  $v(1) \leq v(a)$ .

**Lema 5.2.2:** Se  $0 \neq a \in D$ , então  $v(a) = v(1)$  se, e somente se,  $a$  é unidade.

**Demonstração:** Se  $a$  for unidade, logo existe um elemento  $c \in D$ , tal que  $1 = a \cdot c$ . Com isso,  $v(a) \leq v(a \cdot c) = v(1) \leq v(a)$ , portanto  $v(a) = v(1)$ . Do mesmo modo, se  $v(a) = v(1)$ , e se fazendo  $1 = a \cdot q + r$  onde  $0 = r$  ou  $v(r) < v(a) = v(1)$ . Onde essa última desigualdade não pode ocorrer, logo  $0 = r$  e  $a \mid 1$ . Portanto  $a$  será uma unidade.

**Teorema 5.2.2.** Considere  $D$  um domínio euclidiano. Então  $D$  será um domínio de ideais principais.

**Demonstração:** Considere  $I$  um ideal de  $D$  e  $\varphi$  a função que atende as determinações de um domínio euclidiano. O subconjunto dos inteiros não negativos  $\{\varphi(x) : x \in I\}$  admite um menor elemento. Considere  $x \in I$  tal que  $\varphi(x)$  é o mínimo do conjunto, ou seja, se  $y \in I$ , então  $\varphi(x) \leq \varphi(y)$ . Note que o ideal gerado por  $x$ ,  $\langle x \rangle$ , está contido em  $I$ . Seja agora  $z \in I$ . Então, existem  $q, r \in I$  tais que  $z = xq + r$ , com  $r = 0$  ou  $\varphi(r) < \varphi(x)$ . Note que, como  $z, q \in I$ , temos  $r \in I$ . Logo,  $r$  não pode satisfazer  $\varphi(r) < \varphi(x)$ , e então, temos  $r = 0$ . Segue que  $z = qx$ , e então,  $z \in \langle x \rangle$ . Daí  $\langle x \rangle = I$ , ou seja,  $I$  é um ideal principal. Como  $I$  é arbitrário, segue que  $D$  é um domínio de ideais principais.

**Lema 5.2.3:** Sejam  $a$  e  $b \neq 0$  Pertencentes a um domínio de integridade  $\langle D, +, \cdot, v \rangle$ . Seja  $b = aq + r$ . Se  $b$  e  $r$  possuem um máximo divisor comum  $d$ , então  $d$  é o máximo divisor comum de  $a$  e  $b$ .

**Demonstração:** Se  $a = bq + r$  é claro que cada divisor de  $b$  e  $r$  é um divisor de  $a$ , em particular  $d$  deve dividir  $a$ . Logo  $d$  é um divisor comum de  $a$  e  $b$ . Por outro lado  $r = a - bq$  e assim qualquer divisor comum,  $c$ , de  $a$  e  $b$  divide  $r$  e então é um divisor comum de  $b$  e  $r$ . Logo  $c$  dividir um maior divisor comum de  $b$  e  $r$ , em particular  $c \mid d$ . Portanto,  $d$  é o maior divisor comum de  $a$  e  $b$ .

Agora veremos uns dos principais teoremas a respeito do máximo divisor comum. Sua demonstração podemos encontrar em DEAN (1974).



**Teorema 5.2.3:** (Existência do M D C) Seja  $\langle D, +, \cdot, v \rangle$ . Um domínio euclideano. Se  $a, b \in D$  e um deles é não nulo, então  $a$  e  $b$  tem um maior divisor comum  $e$ , além disso, existem elementos  $x, y \in D$  tais que se  $d = \text{MDC}(a, b)$  então:

$$d = a \cdot x + b \cdot y.$$

**Demonstração:** Se  $b \mid a$  ou  $a \mid b$ , então o teorema torna – se trivial. Se por exemplo,  $b \mid a$ , então  $\text{MDC}(a, b) = b = a \cdot 0 + b \cdot 1$ . Logo o teorema vale em particular, quando um dos  $a$  e  $b$  é uma unidade ou quando eles, mas não ambos, é zero. Assumimos agora que  $b \neq 0$  e procedemos por indução sobre  $m$ , o mínimo de  $v(a)$  e  $v(b)$ . A indução começa no valor mínimo de  $m$ , precisamente  $v(1)$  que ocorre quando  $a$  ou  $b$  é uma unidade e sabemos então que o teorema é válido. Nossa hipótese de indução supõe o teorema válido para quaisquer dois elementos  $c, d$  quando  $c$  ou  $d$  é zero ou o mínimo de  $v(c)$  e  $v(d)$  é menor do que  $m$ . Suponhamos que agora  $a = 0$  ou  $m = v(b) < v(a)$ . Temos  $a = bq + r$  com  $0 = r$  ou  $v(r) < v(b)$ . Se  $r = 0$  então  $b \mid a$ , e o teorema vale. Se  $v(r) < v(b) = m$ , então por indução existe  $\text{MDC}(b, r)$ , e para algum  $w, z \in D$  temos que  $\text{MDC}(b, r) = bw + rz$ . Pelo lema 4.2.3 sabemos que cada  $\text{MDC}(b, r)$  é um  $\text{MDC}(a, b)$  e assim temos  $\text{MDC}(a, b) = \text{MDC}(b, r) = bw + rz = bw + (a - bq)z = az + b(w - qz)$ .

## 6 CONCLUSÃO

Nesta pesquisa apresentamos de forma mais abrangente os conceitos envolvendo o máximo divisor comum e o mínimo múltiplo comum tendo como destaque o capítulo 4 que fala da condição de existência do MDC entre dois elementos.

Um dos principais objetivos desse trabalho é que ele possa trazer uma contribuição tanto para professores de matemática quanto para estudantes do ensino básico, pois nele é possível encontrar assuntos mais elaborados visto no mestrado do PROFMAT, como também, diversas aplicações envolvendo as definições de MDC e de MMC nas olimpíadas de matemática, em especial a OBMEP.

No decorrer do trabalho, também podemos destacar nos capítulos 02 e 03 as formas geométricas para obter o MDC e o MMC. Seria uma abordagem bem interessante e lúdica para os professores acrescentarem esses métodos em suas aulas, até por que os livros didáticos não costumam trabalhar essas metodologias em seus materiais.

Por fim, espero que esses assuntos da matemática tão ricos em aplicações e que podem ser empregados no nosso cotidiano possam ser ensinados nas escolas de modo diferente. Que eles deixem de ser vistos, no ensino fundamental da educação básica, como meros instrumentos para serem trabalhados com frações e possam ser olhados como instrumentos para a resolução de diversas aplicações.

## REFERÊNCIAS

CARDOSO, M. L . GONÇALVES, O. A. ***Uma interpretação geométrica do MMC.*** Rio de Janeiro: RPM v. 32, p. 27 – 28.

DEAN, Richard A. ***Elementos de álgebra abstrata***, tradução de Carlos Alberto A. de Carvalho. Rio de Janeiro: Livros Técnicos e Científicos, 1974.

GARCIA, A. e LEQUAIN, I. ***Elementos de Álgebra.*** Rio de Janeiro: Projeto Euclides, IMPA, 2001.

GONÇALVES, Adilson, ***Introdução à Álgebra.*** Rio de Janeiro: Projeto Euclides, IMPA, 1999.

HEFEZ, Abramo. ***Elementos de aritmética.*** Rio de Janeiro: SBM, 2005.

POLEZZI, M. ***Como obter o MDC e o MMC sem fazer contas.*** Rio de Janeiro: RPM v. 51, p. 29 – 31, 2003.

OLIVEIRA, Krerley Irraciel Martins. ***Iniciação à Matemática: Um curso com problemas e soluções.*** Rio de Janeiro: SBM, 2010.

OLIVEIRA, Z.C. ***Uma interpretação geométrica do MDC.*** RPM v. 29, p. 24 - 26.

<http://www.obmep.org.br/banco.htm>

<http://portal.mec.gov.br/seb/arquivos/pdf/matematica.pdf>