MÁXIMO DIVISOR COMUM E MÍNIMO MÚLTIPLO COMUM NO CONTEXTO DA TEORIA DOS NÚMEROS E SUAS APLICAÇÕES EM RESOLUÇÃO DE PROBLEMAS

Andressa Silva **MARTINS**[1]

Prof° MSc. Fabio Crivelli **AVILA**

RESUMO

O presente trabalho aborda um estudo teórico através de pesquisa bibliográfica apresentando uma parte relevante da Teoria dos Números. Foi realizada a pesquisa em livros didáticos de ensino superior, além de publicações na área de Educação Matemática em busca de métodos práticos aplicados aos conteúdos dessas modalidades de ensino formalizando suas definições. A princípio foi ressaltada a história da Teoria dos Números, para que se familiarize com a necessidade de pré-definir conceitos para o desenvolvimento lógico da matemática com o passar do tempo. O principal objetivo que se propõe é enunciar a teoria que justifica os processos práticos de máximo divisor comum e mínimo múltiplo comum, e por fim, foi apresentado suas aplicações nas mais comuns situações problemas propostas em avaliações de concursos ou vestibulares.

PALAVRAS CHAVE

Mínimo Múltiplo Comum; Máximo Divisor Comum; Teoria dos Números; Resolução de Problemas

1. Introdução

Tendo em vista as diversas aplicações de mínimo múltiplo comum (mmc) e de máximo divisor comum (mdc) em situações problemas; as mesmas que causam o surgimento de inúmeras dúvidas ou incertezas em seus praticantes na hora de solucionar alguns exercícios, tanto de vestibular como em concursos (os quais são mais comuns), este trabalho abordará através de conceitos definidos de uma forma logico-dedutiva pela Teoria dos Números, os mesmos conceitos que são ensinados na educação básica como um processo um quanto mecânico, que não são ressaltados, muitas vezes, de onde vieram tais definições ou sua suma importância de compreensão para os processos práticos de uma maneira mais profunda. Dessa forma, este trabalho abordará conceitos fundamentados de divisibilidade, números primos e com enfoque principal no tratamento

[1] Aluna da Pós de Matemática e suas Tecnologias-FIRA- Faculdades Integradas Regionais de Avaré – 18700-092 – Avaré-SP- Brasil – dryka.engmat@hotmail.com

dado ao mmc e mdc através de suas propriedades e processos práticos pela Teoria dos Números.

Inicia-se com um breve resumo da história da Teoria dos Números, mostrando como foi importante a formalização da matemática através de postulados e axiomas por vários autores importantes no decorrer dos séculos, como Giovanni Campano (1260), Gottfried w. Leibniz (1646-1716), Tales de Mileto (séc. VI a.C.), Pitágoras (560-497 a.C), Filolaus (450-365 a.C.), Platão (428-328 a.C.), Euclides (300 a.C.), Hermann G. Grassmann (1809- 1877), Richard Dedekind (1831-1916), todos contribuintes para o desenvolvimento da matemática que conhecemos atualmente.

Antes de falar de máximo divisor comum e mínimo múltiplo comum se faz necessária a apresentação do conceito de divisibilidade e suas propriedades.

Este trabalho mostra como calcular o mmc e mdc antes da forma que conhecemos atualmente no ensino, através de processos práticos simplificados.

Uma abordagem importante é toda a conceituação de números primos, os quais justificam os processos práticos para o cálculo de máximo divisor comum e mínimo múltiplo comum, e no último capítulo são realizadas aplicações de toda teoria apresentada em situações problemas das mais comuns encontradas com frequência em provas de concursos e vestibulares.

1.1. História da Teoria dos Números

Na antiguidade, tanto os egípcios quanto os babilônicos construíram, um grande acervo matemático no qual desenvolveram a Aritmética, Geometria e a Álgebra; porém apesar de suficiente, tinha muitas limitações ao ver cientifico.

Devido a matemática desses povos não passar de coleções de conclusões empíricas a qual os mesmos chegaram ao decorrer dos séculos, não se origina de conceitos teóricos e nem de deduções lógicas; outro ponto que impedia o desenvolvimento da matemática de egípcios e babilônicos era sua falta de abstração, no entanto, na Grécia antiga, por volta do século VI a.C., passaram a adotar a razão como instrumento na busca da verdade, no que relaciona-se com a matemática, esse pensamento deu ênfase ao método dedutivo a partir de axiomas. A primeira fase importante para o desenvolvimento da matemática grega se deu juntamente com as escolas filosóficas resultando assim algumas diretrizes, como a organização lógica e o caráter abstrato.

Tales de Mileto (séc. VI a.C.) foi o primeiro matemático nomeado, e filósofo grego. Não se sabe muito sobre sua vida, porém, acredita-se que ele tenha sido o primeiro a formular algumas das propriedades gerais sobre figuras geométricas, a qual possibilitou a geometria ser vista então como ciência.

Através de um livro escrito por um discípulo da escola pitagórica fundada por Pitágoras (560-497 a.C) o qual continha a revelação de parte do conhecimento de sua escola. Com o acesso de Platão (428-328 a.C.) a está obra, a matemática pitagórica entrou em Atenas, o que nos leva a crer que a atitude de tentar explicar o universo racionalmente começou com os gregos; mais tarde muitos conceitos da matemática pitagórica foram reunidos nos *Elementos,* de Euclides (300 a.C.), uma obra de treze livros que continham várias definições e descobertas tanto na Geometria quanto da Aritmética.

Em relação aos números, a primeira tentativa no sentido de um tratamento lógico-dedutivo foi de Giovanni Campano (viveu por volta de 1260), do qual fundamentou os números naturais em 4 postulados e afirmava que um número natural não pode diminuir indefinidamente. Gottfried w. Leibniz (1646-1716) afirmou a partir do conceito de número que devem ser objeto de demonstração, verdades tão evidentes como 2+2=4, assim como a comutativa da adição e da multiplicação, porém Leibniz não se prolongou no assunto. Enquanto a Geometria, nos elementos de Euclides já tinha um tratamento lógico-dedutivo, com postulados e axiomas, definições e teoremas, na Teoria dos Números demoraram muito para se ter este mesmo tipo de tratamento. A partir do século XIX a matemática não poderia mais se apoiar em intuições, assim sendo implementado a ampla investigação de seus alicerces se baseando em fundamentações lógicas. Ao se referir aos números, Hermann G. Grassmann (1809- 1877), que definiu adição e multiplicação de números inteiros, e demonstrou suas propriedades fundamentais pelo princípio de indução através da função sucessor $x \longrightarrow x+1$; o primeiro sistema completo de axiomas para a aritmética foi apresentado por Richard Dedekind (1831-1916) em 1888.

2. Divisibilidade em In

Neste capítulo serão elucidadas as definições e propriedades que justificam os processos dos cálculos de máximo divisor comum e mínimo múltiplo comum, revisando toda fundamentação destes conteúdos.

2.1. Divisibilidade

Definição: Para dizer que um número natural a divide um número natural b, deve-se verificar se $b = ac$, para algum $c \in \mathbb{N}$. Assim pode-se dizer também que a é divisor de b e que b é múltiplo de a, ou ainda que b é divisível por a. Indica-se por $a|b$ o fato de que a divide b, e $a \nmid b$ se a não divide b.

Exemplo: $2|18$ pois $\exists\ c = 9 \in \mathbb{N}\ /\ 18 = 2.9$

$18 \nmid 2$ pois $\nexists\ c \in \mathbb{N}\ /\ 2 = 18c$

O elemento $c \in \mathbb{N}$, tal que $b = ac$, onde $a \neq 0$, é indicado por $c = \frac{b}{a}$, e c é chamado quociente de b por a. Por exemplo $2|6$ pois, $6 = 2.3$, $5|10$ pois $10=5.2$, $1|a$ ($\forall\ a \in \mathbb{N}$) pois $a = 1a$ e $0|0$ uma vez que $0 = 0a$ ($\forall\ a \in \mathbb{N}$). Mas, se $b \neq 0$, então $0 \nmid b$ pois $0c = 0 \neq b$, ($\forall\ c \in \mathbb{N}$).

Observação importante:

Não se deve confundir o símbolo | (divide) com fração, que por sua vez pode ser representado com / (barra inclinada) ou — (traço de fração). Por exemplo: $2|6$ não deve ser confundido com $\frac{2}{6}$ ou $\frac{6}{2}$, pois enquanto estes dois últimos símbolos indicam numerais, $2|6$ expressa uma relação particular entre 2 e 6 que equivale a $6 = 2.3$.Assim $0|0$ é uma notação verdadeira, enquanto $\frac{0}{0}$ é uma expressão indeterminada.

2.2. Propriedades da divisibilidade em N:

P1 - $a|a$, $\forall\ a \in \mathbb{N}$, pois $a = 1.a$ (reflexiva)

P2 - $a|b$ e $b|a \Longrightarrow a = b$ (anti-simétrica)

P3 - $a|b$ e $b|c \Longrightarrow a|c$ (transitiva)

P4 - Se $a|b$ e $a|c$, então $a|\ (bx + cy)$, $\forall\ x,y \in \mathbb{N}$.

P5 - Se $c|a$, $c|b$ e $a \leq b$, então $c|(b-a)$

P6 - Seja $a = b + c$ e suponhamos $d|b$, então : $d|a \Longleftrightarrow d|c$

P7 - Se $a|b$ e $b \neq 0$, então $a \leq b$

3. Máximo Divisor Comum

De uma forma geral pode-se entender máximo divisor comum entre dois ou mais números como sendo o maior fator entre eles, ou seja, o maior número inteiro que divide os dois ou mais números.

Definição: Sejam $a, b \in \mathbb{N}$. Um número $d \in \mathbb{N}$ se diz *máximo divisor comum* de a e b se:

i) $d|a$ e $d|b$

ii) c é número natural tal que $c|a$ e $c|b$, então $c|d$

Exemplo: Sejam **a** = 6 e **b** = 8. Indicando por Dx o conjunto dos divisores de $x \in \mathbb{N}$, então $D_6 = \{1,2,3,6\}$ e $D_8 = \{1,2,4,8\}$ do que segue: $D_6 \cap D_8 = \{1,2\}$.

Observa-se que: **i)** 2|6, 2|8 e **ii)** 1|6 e 1|8, porém 1|2. Logo, 2 é o máximo divisor comum de 6 e 8.

Teorema : O máximo divisor de dois números a e b é único.

Demonstração: Suponhamos que existam dois *máximos divisores comuns*, sejam eles, d e d'. Logo d é divisor de a e de b, assim $d|d'$ pois d' é o *máximo divisor comum* de a e b e analogamente, d' é divisor de a e de b, assim $d'|d$ pois d é o *máximo divisor comum* de a e b. De $d|d'$ e $d'|d$ conclui-se que $d = d'$.

Proposição 1: Se $a|b$, então mdc $(a,b) = a$.

Demonstração: De fato, $a|a$ e $a|b$ (hipótese). E se $c|a$ e $c|b$, é obvio que $c|a$.

Proposição 2: Se $a = bq+r$ e $d =$ mdc (a,b), então $d =$ mdc(b,r). E se $d =$ mdc (b,r), então $d=$ mdc (a,b).

Demonstração: Como $d =$ mdc (a,b), então $d|a$ e $d|b$. Desta última relação resulta que $d|br$. Logo, $d|(a-bq)$, ou seja, $d|r$. Por outro lado, se $c|b$ e $c|r$, então $c|(bq+r)$ devido a 4ª propriedade de múltiplos e divisores; como $bq+r= a$, então $c|a$ e $c|b$, o que implica $c|d$, já que $d =$ mdc(a,b).

A segunda afirmação se prova de maneira análoga.

Retoma-se agora a questão de existência de *máximo divisor comum*. Para provar a existência aplicaremos, sucessivamente, a partir de a e b, o algoritmo da divisão da seguinte maneira:

$$a = b.q_1 + r_1 \ (r_1 < b)$$

$$b = r_1.q_2 + r_2 \ (r_2 < r_1)$$

$$r_1 = r_2.q_3 + r_3 \ (r_3 < r_2)$$

$$\vdots$$

É claro que, se acontecer de r_1 ser nulo, então a proposição 1 nos garante que b=mdc (a,b) e o processo termina na primeira etapa. Mas, de qualquer maneira, na sequência b> $r_1 > r_2 > r_3 >$ ... para algum índice n deverá ocorrer $r_{n+1}=0$. De fato, se todos os r_i forem não nulos, então $\{b, r_1, r_2, ...\}$ não teria mínimo, o que não é possível. Assim, para algum n:

$$R_{n-2} = r_{n-1} \,.\, q_n + r_n$$

$$R_{n-1} = r_n \,.\, q_{n+1}$$

Como consequência das proposições anteriores, obtém-se então o seguinte:

R_n = mdc (r_{n-1}, r_n)= mdc(r_{n-2}, r_{n-1}) = ... = mdc (b, r_1) = mdc (a, b), ou seja, r_n= mdc (a, b)

Essa demonstração obviamente é construtiva e o dispositivo prático que se costuma empregar para aplicá-la é conhecido como processo das divisões sucessivas.

Exemplo: mdc (36,10)

36= 10 . 3 + ***6*** → mdc (10, 6)

10= 6 . 1 + ***4*** → mdc (6,4)

6= 4 . 1 + ***2*** → mdc (4,2) → logo pelo lema 1 , mdc(4,2) =2

4= 2 .2 + ***0***

Dessa forma mdc(36,10)=mdc(10,6)=mdc(6,4)=mdc(4,2)=2

3.1. Máximo divisor comum pelo Método Da Chave (Processo Das Divisões Sucessivas)

Para realizar esse método pega-se o maior dos dois números e divide-se pelo menor. Com a primeira divisão feita, obtém-se um quociente e um resto, para a segunda operação o divisor torna-se dividendo e o resto passa a ser o divisor, a operação se repete dessa forma até obter-se o resto igual a zero.

Quando se chega no resto igual a zero, determina-se como máximo divisor comum entre os números o que foi divisor na última passagem.

Para calcular o máximo divisor comum entre os números 52 e 24 pelo método das divisões sucessivas observa-se que:

$52= 24 . 2 + 4$

$24 = 4.6$

Assim,

	2	6
52	24	4
	4	0

Logo, mdc (52,24) = 4

Definição: Dois números naturais *a* e *b* se dizem primos entre si se mdc (a,b)=1.

Proposicão 3: Dois números consecutivos *a* e *a+1* são sempre primos entre si. De fato, é claro que $1|a$ e $1|(a+1)$. Agora se $c|a$ e $c|(a+1)$, então $c\,|[(a+1)-a]$, ou seja, $c|1$, logo mdc (a,a+1)=1

Proposição 4: se d = mdc (a,b), então mdc (s.a,s.b)= $s.d$, para todos $s \in \mathbb{N}$.

Demonstração: Multiplica-se por s cada uma das igualdades obtidas pelo algoritmo da divisão no processo das divisões sucessivas que leva a *d*, a partir de *a* e *b*:

$$\mathbf{s.a= (s.b) .q_1 + s.r_1}$$

$$\mathbf{s.b= (s.r_1) . q_2 + s.r_2}$$

$$\vdots$$

$$\mathbf{s.r_{n-2} = (s.r_{n-1}). q_n + s.r_n}$$

$$\mathbf{s.r_{n-1} = (s. r_n). q_{n+1}}$$

As proposições 1 e 2 nos garantem então:

$s.d = s. r_n=$ mdc $(s.r_{n-1},.s.r_n)= \ldots =$ mdc $(s.b,s.r_1)=$ mdc (a.s,s.b).

Exemplo: mdc(18,12)=6

mdc (18000,12000) = mdc(1000.18,1000.12)=1000.6, logo mdc (18000,12000)=6000

Corolário 1: Se $a, b \in \mathbb{N}^*$ e d = mdc (a,b),então mdc $(\frac{a}{d},\frac{b}{d})$=1. Ou seja: $\frac{a}{d}$ e $\frac{b}{d}$,são primos entre si:

Demonstração: Como d= mdc (a,b) = mdc (d $\frac{a}{d}$,d $\frac{b}{d}$) = d . mdc $(\frac{a}{d}, \frac{b}{d})$ e $d \neq 0$, então:

mdc $(\frac{a}{d}, \frac{b}{d})$=1

Corolário 2: Se a | bc e mdc (a,b) = 1, então a | c.

Demonstração: Da hipótese mdc (a,b) = 1 decorre, levando em conta a proposição 4, que mdc (ac,bc) = c, como a | bc por hipótese e obviamente a | ac, então a | mdc (ac,bc). Ou seja, a | c.

Corolário 3: Se a e b são divisores de $c \neq 0$ e mdc (a,b) = 1, então ab | c.

Demonstração: De mdc (a,b) = 1 decorre, em virtude da proposição 4, que mdc (ac,bc) = c. Mas ab | ac, pois b | c e ab | bc já que a | c. Logo, ab divide mdc (ac,bc), isto é, ab | c.

Exemplo: Para que um número seja divisível por 6 é necessário e suficiente que seja divisível por 2 e por 3 já que mdc (2,3) = 1.

A definição de máximo divisor comum pode ser entendida de maneira óbvia para três ou mais números. Para o cálculo do máximo divisor comum de três números, por exemplo, pode-se lançar mão do seguinte resultado:

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

4. Mínimo Múltiplo Comum

Diz-se que um número é mínimo múltiplo comum de um conjunto de múltiplos de dois ou mais números quando ele é o menor dos múltiplos comuns.

Definição: Um número m se diz mínimo múltiplo comum de a, $b \in \mathbb{N}$ se:

i) a | m e b | m (m é múltiplo de a e de b);

ii) a | m´ e b | m´ $\Longrightarrow$ m | m´ (todo múltiplo de a e b é também múltiplo de m).

Se m e m_1 satisfazem essa definição, então m | m_1 (pois m_1 é múltiplo de a e b) e m_1 | m (já que m é múltiplo de a e b e m_1 é mínimo múltiplo comum de a e b). Logo, $m = m_1$, ou seja, dois números a e b não podem ter mais que um mínimo múltiplo comum. Se m é mínimo múltiplo comum de a e b, usando a notação m = mmc (a,b). Da definição decorre diretamente que mmc (a,b) = mmc (b,a).

Quanto à existência de mínimo múltiplo comum, considera-se inicialmente o caso $a = 0$ e b qualquer. Observa-se assim que mmc (0,b) = 0, pois **i)** $0 \mid 0$ e $b \mid 0$ e **ii)** $0 \mid m'$ e $b \mid m'$, obviamente $0 \mid m'$.Para os demais casos a garantia de existência é dada pela proposição abaixo, que traz o primeiro método conhecido para se encontrar o mínimo múltiplo comum.

Proposição 1: Para quaisquer $a,b \in \mathbb{N}^*$, se $d = \text{mdc}\ (a,b)$, então $m = \frac{ab}{d}$ é o mínimo múltiplo comum de a e b.

Demonstração: Notando primeiro que como $d \mid (ab)$ (pois $d \mid a$ e $d \mid b$), então $m \in \mathbb{N}$. **i)** Como, evidentemente, $a\frac{b}{d} = \frac{ab}{d} = m$, então $a|m$. Analogamente se mostra que $b \mid m$ e **ii)** Seja m' um múltiplo de a e de b e supondo $m' = ar$ e $m' = bs$. Então $ar = bs$ e portanto: $\frac{a}{d}r = \frac{b}{d}s$, daí segue que $\frac{a}{d}$ divide $\frac{b}{d}s$ e, como mdc $(\frac{a}{d},\frac{b}{d})= 1$ então $\frac{a}{d}|s$. Assim $s= \frac{a}{d}t$ para algum $t \in \mathbb{N}$ e como $m' = bs$, obtém-se $m' = b\frac{a}{d}t = \frac{ab}{d}t = mt$,ou seja, $m \mid m'$.

Assim, tem-se o primeiro método conhecido para encontrar o mínimo múltiplo comum.

Exemplo 1. Para encontrar o mínimo múltiplo comum dos números 60 e 72, encontra-se inicialmente o máximo divisor comum entre eles

	5	
72	**60**	12
12	0	

Assim, $\text{mmc}(60,72) = \frac{60.72}{mdc(60,72)} = \frac{60.72}{12} = 360$

Exemplo 2. Calcule x sabendo que mdc(a,b)=12, mmc(a,b)= 32x+272 e ab=78x+10302

Segundo o teorema: mmc(a,b) . mdc$(a,b) = a.b$

(32x+272).12=78x+10302

306x=7038

x=23

Corolário: Se a e b são primos entre si, então mmc $(a,b) = ab$.

Demonstração: De fato, como d = mdc $(a,b) = 1$, então mmc $(a,b) = \frac{ab}{1} = ab$.

Proposição 2: Se m= mmc (a,b),então mmc $(sa,sb)=sm$, para qualquer $s \in \mathbb{N}$.

Demonstração: Quando a=0 ou b=0, então m=0 e as=0 ou sb=0; dai mmc $(as,sb)=0=sm$. Se s=0, ficamos com mmc (0,0)=0, que também é verdadeira. Suponhamos por fim a,b e s não nulos; levando em conta as duas proposições anteriores:

$$\text{mmc}(as,sb)= \frac{sa.sb}{mdc(sa,sb)} = \frac{s^2.ab}{s.mdc(a,b)} = s\frac{a.b}{mdc(a,b)} = s.\text{mmc}(a,b).$$

Exemplo: Sabendo que mmc (6,8) = 24 então

mmc(60 000,80 000) = 10 000. mmc (6,8) = 10 000 , 24 = 240 000

5. Números Primos

Definição: Diz-se número primo todo número que possui dois divisores naturais, 1 e ele mesmo. Um $p \in \mathbb{N}$ se diz primo se:

i) $p \neq 0$ e $p \neq 1$

ii) Os únicos divisores naturais de p são 1 e p.

Um número $a \in \mathbb{N}, a \neq 0$ e $a \neq 1$, é chamado composto se a não é primo, assim a pode ser fatorado num produto $a = bc$, onde $b \neq 1$ e $c \neq 1$.Observa-se então que 0 e 1 não são primos nem compostos.

Exemplo: O número 2 é o único primo par pois, se $a > 2$ é par, então $a = 2q$ onde $q > 1$ e portanto 1, 2 e q são divisores de a, distintos entre si. Pode-se notar então que nenhum número par maior que 2 é primo.

Proposição1: Se p é primo e p|ab, então p|a ou p|b.

Proposição 2: Seja $a \in \mathbb{N}$, $a \neq 0$ e $a \neq 1$. Então o mínimo de S={ $x \in \mathbb{N}$: x>1 e x|a} é um número primo.

5.1. Teorema Fundamental de Aritmética

Para todo número natural $a > 1$ existem números primos $p_1, p_2 \dots , p_r$ $(r \geq 1)$, de maneira que $a = p_1 . p_2 \dots .p_r$. Além disso, se também $a = q_1 . q_2 \dots q_r$ $(s \geq 1)$, onde os q_i são igualmente primos, então $r = s$ e cada p_i é igual a algum dos q_i.

Demonstração: Usa-se o segundo princípio da indução. Se $a = 2$, como 2 é primo, a afirmação de existência é trivialmente verdadeira. Suponhamos $a > 2$ e o teorema válido, em sua primeira afirmação, para todo b, $2 \leq b < a$. A proposição anterior nos garante que a admite um divisor primo p_1: $a = p_1 . a_1$ $(a_1 \in \mathbb{N}^*)$. Se $a_1 = 1$ ou a_1 é primo, a demonstração se encerra. Caso contrário, visto que então $2 \leq a_1 < a$, a hipótese de indução nos assegura que há $r - 1$ primos $p_2, \dots , p_r$ $(r - 1 \geq 1)$ de modo que $a_1 = p_2 . p_3 \dots p_r$. Se $p_1 . p_2 \dots p_r = q_1 . q_2 \dots q_s$, conforme o enunciado, então p_1 divide o segundo membro e portanto divide um de seus fatores, como q_1 . Sendo apenas 1 e q_1 os divisores de q_1 e sendo $p_1 \neq 1$, então $p_1 = q_1$. Cancelando p_1 com q_1, na igualdade inicial, obtemos $p_2 . p_3 \dots p_r = q_2 . q_3 \dots q_s$. Repetindo essa argumentação o quanto for necessário, chegando à unicidade conforme enunciado. Baseado nos resultados tem-se o processo prático elementar usado para decompor um

número em fatores primos.

Exemplo:

84	2
42	2
21	3
7	7
1	

$84 = 2.2.3.7 = 2^2.3.7$

5.2. O crivo de Erastóstenes

O crivo de Erastóstenes é um critério utilizado para determinar se um número é primo ou não, neste processo é possível encontrar todos os primos de 1 até certo $n \in \mathbb{N}^*$.

O processo para ser aplicado, parte de um quadro formado pelos números naturais de 1 a n do qual se vão eliminando, por etapas, os elementos que não são primos.

Proposição: Se $n > 1$ é um número composto, então há um primo p tal que: $p|n$ e $p^2 \leq n$ (ou seja, $p \leq \sqrt{n}$).

Demonstração: Por hipótese, n pode ser decomposto da seguinte maneira: $n = ab$ $(2 \leq a \leq b < n)$; Logo, $n = ab \geq a^2$. Seja p um divisor primo de a. Então $p^2 \mid a^2$ e portanto $p^2 \leq a^2$.Donde $p^2 \leq n$, o que pode ser traduzido por $p \leq \sqrt{n}$.

Consequência: Se um número $n > 1$ não é divisível por nenhum dos primos $p \leq \sqrt{n}$, então n é primo. De fato, se fosse composto, admitiria um divisor primo menor ou igual a $\sqrt{n}$.

Exemplo: O número 271 é primo, pois observa-se que $\sqrt{271} < 17$.

Os números primos que não superam 17 são: 2, 3, 5, 7, 11 e 13. Mas nenhum deles é divisor de 271.

Para o procedimento do crivo de Erastóstenes faz-se inicialmente uma tabela com os números de 2 a n e no quadro obtido devem ser cancelados todos os múltiplos de 2, exceto o 2, todos os múltiplos de 3, exceto o 3, todos os de 5, exceto o 5, e assim por diante, e é dessa forma que não sobrarão outros números senão os primos.

Mas é importante saber, nesse processo, em que o primo p parar, por serem desnecessárias as etapas seguintes. A resposta é : $2 \leq p \leq \sqrt{n}$.

De fato, seja um número natural, $2 < a \leq n$. Se a é composto, então existe um primo p tal que $p \mid a$ e $p \leq \sqrt{a}$. Concluí-se que $p \leq \sqrt{n}$.

Logo, o número a será efetivamente cancelado quando se aplica o processo dos primos $p \leq \sqrt{n}$.

Exemplo do crivo de Erastóstenes dos números primos ≤ 50, e nota-se que os números que sobram são primos.

	2	**3**	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	**29**	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	**37**	~~38~~	~~39~~	~~40~~
41	~~42~~	**43**	~~44~~	~~45~~	~~46~~	**47**	~~48~~	~~49~~	~~50~~

5.3. Número de divisores de um número natural, usando a decomposição em fatores primos

Para todo $a \in \mathbb{N}^*$, indica-se por $\tau(a)$ o número de divisores de a. Por exemplo: $\tau(1)= 1$, $\tau(2) = 2$, $\tau(3)=2$, $\tau(4)=3$ (os divisores de 4 são: 1,2 e 4). Se p é primo, então $\tau(p)=2$. Nota-se que τ é uma função numérica definida em $\mathbb{N}^*$.

Determinando uma fórmula para $\tau(a)$, sempre que $a > 1$. Supondo $a= p_1^{\alpha 1}. p_2^{\alpha 2}. \dots . p_s^{\alpha s}$ ($\alpha_1, \dots, \alpha_s \geq 1$), levando em conta que $b|a \Leftrightarrow b= p_1^{\beta 1}.p_2^{\beta 2}. \dots . p_s^{\beta s}$($0 \leq \beta_i \leq \alpha_i$; $i= 1,2, \dots , s$), a questão pode ser encerrada sob o ponto de vista da combinatória: como cada β_i pode assumir, independente, os α_i +1 valores 0,1,2,..., α_i, então: $\tau(a) = (\alpha_1 +1). (\alpha_2 +1)...(\alpha_s +1)$.

O número de divisores de $72=2^3. 3^2$ é dado por $\tau(72)= (3+1).(2+1)=4.3=12$

Na resolução o primeiro passo é fazer a fatoração do número em fatores primos, para depois somar 1 a cada expoente e multiplicar essas somas, resultando na quantidade de divisores do número.

5.4. Máximo divisor comum

O teorema seguir irá justificar os processos práticos amplamente divulgados para encontrar o máximo divisor comum entre dois números naturais.

Teorema (mdc)

Considerando a decomposição de um número em fatores primos, incluindo aqueles cujo expoente é nulo, pode-se provar que para quaisquer números não nulos a e b, se $a=p_1^{\alpha 1}. p_2^{\alpha 2}. \dots . p_s^{\alpha s}$ e $b= p_1^{\beta 1}.p_2^{\beta 2}. \dots . p_s^{\beta s}$ e se $\gamma_i = \min \{ \alpha_i, \beta_i\}$, então $d= p_1^{\gamma 1}. p_2^{\gamma 2}. \dots . p_s^{\gamma s}$ é o *máximo divisor comum* de a e b.

Demonstração: Sabe-se que d|a e d|b. Agora, se $c \in \mathbb{N}$ é um divisor de a e b, então $c=p_1^{\delta 1}.p_2^{\delta 2}. \dots . p_s^{\delta s}$, onde $0 \leq \delta_i \leq \alpha_i$ e $0 \leq \delta_i \leq \beta_i$, (i=1,2,...,s). Mas então, para cada um desses índices, i: $0 \leq \delta_i \leq \min \{ \alpha_i, \beta_i\} = \gamma_i$.

Pois $\min \{ \alpha_i, \beta_i\}= \alpha_i$, ou $\min \{ \alpha_i, \beta_i\}= \beta_i$. Donde c|d. Portanto d é o *máximo divisor comum* de a e b.

Para $a= 48$ e $b=50$

$$\begin{array}{r|l} 48 & 2 \\ 24 & 2 \\ 12 & 2 \\ 6 & 2 \\ 3 & 3 \\ 1 & \end{array} \qquad\qquad \begin{array}{r|l} 50 & 2 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}$$

$48=2^4.3$ $\qquad\qquad$ $50=2.\,5^2$

Colocando também os fatores primos de expoentes nulos, tem-se:

$$48=2^4.3.5^0 \quad \text{e} \quad 50=2.3^0.5^2$$

Então o $\text{mdc}(48,50)=2.3^0.5^0 = 2$

A regra elementar segundo a qual o máximo divisor comum de dois números naturais não nulos é o produto dos fatores primos comuns, cada um com a menor expoente.

5.4.1. Método prático para o cálculo do máximo divisor comum

Um método prático utilizado no ensino de mdc, é quando se fatora os números separadamente em número primos, torna-se seus fatores comuns de menor expoente, multiplica-se esses valores obtendo assim o *Máximo Divisor Comum.*

Para calcular *mdc* (88, 144, 256), fatora-se cada número separadamente

$$\begin{array}{r|l} 88 & 2 \\ 44 & 2 \\ 22 & 2 \\ 11 & 11 \\ 1 & \end{array} \qquad \begin{array}{r|l} 144 & 2 \\ 72 & 2 \\ 36 & 2 \\ 18 & 2 \\ 9 & 3 \\ 3 & 3 \\ 1 & \end{array} \qquad \begin{array}{r|l} 256 & 2 \\ 128 & 2 \\ 64 & 2 \\ 32 & 2 \\ 16 & 2 \\ 8 & 2 \\ 4 & 2 \\ 2 & 2 \\ 1 & \end{array}$$

$88= 2^3.11$ $\qquad$ $144=2^4.3^2$ $\qquad$ $256=2^8$

Assim, o *mdc* (88, 144, 256) = $2^3.3^0.11^0 = 8$.

Outra maneira é fatorar todos os números de uma só vez, fazendo a divisão somente até todos os números serem divididos pelo mesmo fator primo.

Usando os mesmos números como exemplo, tem-se *mdc* (88, 144, 256) = 2.2.2 = 8

88,144,256	2
44,72,128	2
22,36,64	2
11,18,32	

5.5. Mínimo Múltiplo Comum

O teorema a seguir justifica os processos práticos que determinam o mínimo múltiplo comum entre dois números naturais.

Teorema (mmc)

Se a e b são naturais não nulos que se fatoram, como $a=p_1^{\alpha 1}.\, p_2^{\alpha 2}. \ldots .\, p_s^{\alpha s}$ e $b=p_1^{\beta 1}.\, p_2^{\beta 2}. \ldots .\, p_s^{\beta s}$ e se $\rho_i = \max\{\alpha_i, \beta_i\}$ $(1 \leq i \leq s)$, então $m= p_1^{\rho 1}.\, p_2^{\rho 2}. \ldots .\, p_s^{\rho s}$, é *mínimo múltiplo comum* de a e b.

Demonstração: Percebe-se facilmente que m é múltiplo de a e b, além disso, se $m' = p_1^{\delta 1}.\, p_2^{\delta 2}. \ldots .\, p_s^{\delta s}$, é múltiplo de a e de b, então $\delta_i \geq \alpha_i \geq 0$ e $\delta_i \geq \beta_i \geq 0$, $(i=1,2,\ldots,s)$, logo $\delta_i = \max\{\alpha_i, \beta_i\} = \rho_i$ $(1 \leq i \leq s)$ e então $m \mid m'$.Portanto m é o *mínimo múltiplo comum* de a e b.

Para os números 48 e 50 tem-se: $48 = 2^4.3.5^0$ e $50 = 2.3^0.5^2$, então *mmc* (48,50) = $2^4.3.5^2 = 1200$.

Da mesma forma, a regra elementar segundo a qual o mínimo múltiplo comum de dois números naturais não nulos é o produto dos fatores primos comuns, cada um com o maior expoente.

5.5.1. Método prático para o cálculo do mínimo múltiplo comum

Uma maneira prática para encontrar o mínimo múltiplo comum dos números é decompondo-os em fatores primos de forma conjunta e multiplicando esses fatores.

Para calcular o mínimo múltiplo comum dos números 12, 30 e 42

12,30,42	2
6,15,21	2
3,15,21	3
1,5,7	5
1,1,7	7
1,1,1	

Assim *mmc* (12, 30, 42) = $2^2.3.5.7 = 420$

6. Aplicações na Resolução de Problemas

Neste capítulo serão resolvidas algumas situações problema das mais comuns encontradas em questões de concursos e vestibulares, usando as definições e propriedades abordadas nos capítulos anteriores referente a máximo divisor comum e mínimo múltiplo comum.

6.1. Número de participantes de uma equipe

Uma empresa de logística é composta de três áreas: administrativa, operacional e vendedores. A área administrativa é composta de 30 funcionários, a operacional de 48 e a de vendedores com 36 pessoas. Ao final do ano, a empresa realiza uma integração entre as três áreas, de modo que todos os funcionários participem ativamente. As equipes devem conter o mesmo número de funcionários e com o maior número possível de funcionários. Determine quantos funcionários devem participar de cada equipe e o número possível de equipes.

Calcula-se o mdc entre os números 48, 36 e 30

48	2	36	2	30	2
24	2	18	2	15	3
12	2	9	3	5	5
6	2	3	3	1	
3	3	1			
1					

A decomposição em fatores primos: $48 = 2^4.3$; $36 = 2^2.3^2$; $30 = 2.3.5$.

Logo, mdc (30, 36, 48) = 2.3 = 6 equipes

Assim cada equipe contará com $48 \div 6 = 8$ funcionários da área operacional, $30 \div 6 = 5$ da administrativa e $36 \div 6 = 6$ vendedores, ou seja, cada equipe terá $8+5+6 = 19$ funcionários .Observe que formar as equipes com o maior número possível equivale a encontrar o menor número de equipes.

6.2. mdc através de mmc e o produto dos números

Se o mmc entre dois números naturais é 2.450 e o produto entre eles é 306.250, então o mdc entre os dois números naturais é?

Sendo o mmc (a,b) = 2450 e a.b = 306250, e segundo a proposição 1 de mínimo múltiplo comum nos capítulos anteriores temos:

mmc(a,b) . mdc$(a,b) = a.b$

$\frac{306250}{2450}$= mdc (a,b)

Então mdc(a,b)= 125

6.3. Horário de medicamentos

Um médico, ao prescrever uma receita, determina que três medicamentos sejam ingeridos pelo paciente de acordo com a seguinte escala de horários: remédio A, de 2 em 2 horas, remédio B, de 3 em 3 horas e remédio C, de 6 em 6 horas. Caso o paciente utilize os três remédios às 8 horas da manhã, qual será o próximo horário de ingestão dos mesmos?

Calcular o mmc dos números 2, 3 e 6.

$$\begin{array}{ccc|c} 2 & 3 & 6 & 2 \\ 1 & 3 & 3 & 3 \\ 1 & 1 & 1 & \end{array}$$

$$\text{mmc}(2, 3, 6) = 2 . 3 = 6$$

De 6 em 6 horas os três remédios serão ingeridos juntos. Portanto, o próximo horário será às 14 horas.

6.4. Manutenção de máquinas

Numa linha de produção, certo tipo de manutenção é feita na máquina A a cada 3 dias, na máquina B, a cada 4 dias, e na máquina C, a cada 6 dias. Se no dia 2 de dezembro foi feita a manutenção nas três máquinas, após quantos dias as máquinas receberão manutenção no mesmo dia.

Temos que determinar o mmc entre os números 3, 4 e 6.

3	4	6	2
3	2	3	2
3	1	3	3
1	1	1	

mmc (3, 4, 6) = 2 . 2 . 3 = 12

Concluímos que após 12 dias, a manutenção será feita nas três máquinas. Portanto, dia 14 de dezembro.

7. Conclusão

Conclui-se que neste trabalho foi falado sobre a importância de vários temas relevantes na área de matemática, como a Teoria dos Números. Abordando primeiramente sua história a fim de esclarecer toda origem de tais estudos e sua importância para a evolução da matemática que temos hoje, logo depois foi abordada a definição de divisibilidade usada como importante ferramenta para que se pudesse definir e construir formalmente conceitos como o de números primos, máximo divisor comum e mínimo múltiplo comum. Em muitos estudos sobre esses assuntos são apresentados apenas os processos práticos, pois funcionam, em muitos casos realmente não é necessário saber a justificativa desses processos serem tão eficientes ou como chegaram a eles. Este trabalho buscou apresentar as justificativas, mostradas através dos corolários e teoremas enunciados dos capítulos anteriores.

Para justificar os processos práticos para o cálculo de mdc e mmc fez-se o uso dos números primos, e por fim foram resolvidas algumas situações problemas, utilizando os conceitos estudados e mostrando sua aplicação.

8. Referencias Bibliográficas

DOMINGUES, Hygino H. **Fundamentos da Aritmética**. São Paulo: Atual. 1991 . 297.

BOYER, Carl B. **História da matemática.** Tradução de Elza F. GOMIDE.2.ed. São Paulo: Edgard Blucher, 1999. 496p.

BLOGGER QUESTÕES DE CONCURSOS, VESTIBULARES E NOTÍCIAS DE CONCURSOS EM ABERTO. **mmc e mdc questões vestibular.** Disponivel em: <http://tudodeconcursosevestibulares.blogspot.com/2012/12/mmc-e-mdc-questoes-vestibular.html> acesso em: 18 mai.2019

BLOGGER MATEMATICA GENIAL. **mmc e mdc - Como saber quando utilizar: mínimo múltiplo comum (mmc) e máximo divisor comum (mdc)** <https://www.matematicagenial.com/2017/05/como-saber-quando-utilizar-minimo-multiplo-comum-mmc-maximo-divisor-comum-mdc.html> acesso em: 18 mai. 2019