UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

GLÁUCIA VIVIANE DE ALMEIDA

Máximo Divisor Comum e Mínimo Múltiplo Comum

Maringá - PR
2015

GLÁUCIA VIVIANE DE ALMEIDA

Máximo Divisor Comum e Mínimo Múltiplo Comum

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, do Departamento de Matemática, da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre.
Área de concentração: Matemática

Orientadora:
Prof[a]. Dr[a]. Claudete Matilde Webler Martins

Maringá - PR
2015

GLÁUCIA VIVIANE DE ALMEIDA

Máximo Divisor Comum e Mínimo Múltiplo Comum

Dissertação apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional - PROFMAT, do Departamento de Matemática, da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre.

Aprovada em 23/02/2015.
Local da defesa: Auditório do DMA, Bloco F67, UEM/Maringá.

BANCA EXAMINADORA

Profª. Drª. Claudete Matilde Webler Martins
(DMA/Universidade Estadual de Maringá)

Profª. Drª. Neuza Teramon
(Dpto de Matemática/Universidade Estadual de Londrina)

Prof. Dr. Rodrigo Martins
(DMA/Universidade Estadual de Maringá)

Maringá - PR
2015

Dedico este trabalho a meu filho, Isaac Bryan de Almeida Ribeiro, que é minha inspiração a prosseguir e o que me faz ir em busca de meus sonhos e objetivos.

Agradecimentos

À Deus que me capacitou e me fortaleceu durante estes anos de estudos, me permitindo chegar até aqui.

À minha família por toda estrutura que me possibilitou dedicar aos estudos.

Aos meus amigos e companheiros de classe, pelo apoio e ajuda.

À Profª. Drª. Claudete Matilde Webler Martins, não só pela constante orientação neste trabalho, mas sobretudo pela sua amizade.

Ao programa de pós-graduação em matemática, Profmat e aos professores pela boa formação que me proporcionaram.

À Capes pelo apoio financeiro.

Resumo

Neste trabalho estudamos os conceitos de Máximo Divisor Comum e Mínimo Múltiplo Comum no conjunto dos números inteiros, no conjunto dos números reais e em anéis.

Palavras chave: Divisores, Múltiplos, Números Comensuráveis, Anéis.

Abstract

We study the concepts of Highest Common Factor and Lowest Common Multiple in the set of integers, the set of real numbers and rings.

Keywords: Factors, Múltiples, Commensurable numbers, Rings.

Sumário

1 Introdução

No ensino básico, os cálculos envolvendo Mínimo Múltiplo Comum (mmc) e Máximo Divisor Comum (mdc) estão relacionados com múltiplos e divisores de um número natural. Entendemos por múltiplo, o produto gerado pela multiplicação entre dois números, e um número é considerado divisível por outro quando o resto da divisão entre eles é igual a zero.

A motivação deste trabalho está na extensão destes conceitos para números inteiros, racionais, reais e até mesmo em outros conjuntos matemáticos, como por exemplo, uma matriz, ou um polinômio, devido ao fato que, em problemas do dia a dia, onde podemos usar estes conceitos para resolução, não encontraremos apenas números naturais envolvidos.

No decorrer deste trabalho encontraremos a noção de comensurabilidade que, historicamente, foi introduzida como uma forma de comparar o tamanho de dois segmentos de reta, pode ser definida da seguinte maneira:

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

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

Embora sendo um conceito geométrico, a comensurabilidade pode ser equivalentemente definida como uma relação entre dois números reais, que apresentaremos no segundo capítulo.

A Matemática está presente no nosso dia-a-dia. O *mmc* e o *mdc* possuem inúmeras aplicações cotidianas. Vejamos alguns exemplos:

Exemplo 1: 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.

Solução: Máquina A: $M(3) = 3, 6, 9, 12, 15, 18, 21, ...,$

Máquina B: $M(4) = 4, 8, 12, 16, 20, 24, 28, ...,$

Máquina C: $M(6) = 6, 12, 18, 24, 36, 42, ...$

Notemos que o Mínimo Múltiplo Comum de $3, 4$ e 6 é 12. Portanto, 12 dias após 2 de dezembro haverá manutenção nas três máquinas, logo será dia 14 de dezembro.

Exemplo 2: Duas colegas de classe tem um livro para ler como trabalho escolar. Ambas já começaram a ler o livro, porém a uma resta $\frac{2}{3}$ do livro para terminar e a outra $\frac{3}{5}$. Elas resolveram estudar juntas e dividiram as páginas restantes em partes iguais, de modo que elas lessem, a cada dia, o máximo possível. Em quantos dias cada uma terminará o trabalho?

Exemplo 3: Temos dois repelentes líquidos de spray automático A e B, eles estão programados para agirem 4 vezes a cada 5 minutos e 6 vezes a cada 7 minutos, respectivamente. Se num dado instante os dois espirram juntos, em quanto tempo isso voltará a ocorrer?

Notemos que, estes problemas envolvem os conceitos em questão, além disso, observe que no primeiro exemplo a resposta do problema é um número inteiro. Já os exemplos 2 e 3, não podem ser resolvidos com o mmc e mdc usual. Isto nos ilustra a necessidade de ampliarmos o conceito estudado no ensino básico.

Vimos, no estudo feito, que no conjunto dos números inteiros, quaisquer dois números a e b tem um único mdc e mmc. Vimos também que isso não acontece num anel qualquer. No entanto, existe uma relação entre os elementos que satisfazem a definição de $mmc(a, b)$ e $mdc(a, b)$ (veja capítulo 4).

Num corpo C, pelo fato de todos os elementos possuírem inverso multiplicativo, teremos $mmc(a, b) = mdc(a, b) = 1$, para quaisquer elementos não nulos $a, b \in C$, sendo 1 o elemento unidade (ou elemento neutro da multiplicação). Desta forma, não faz muito sentido trabalharmos com mmc e mdc num anel que tenha as propriedades de corpo (com as definições dadas no capítulo 3).

Este trabalho está dividido da seguinte forma. No primeiro capítulo colocamos definições, exemplos e propriedades referentes ao conjunto dos números inteiros, ou seja, definimos múltiplos, divisores, mmc e mdc, dentre outros.

No segundo capítulo nos baseamos em [6]. Fizemos uma expansão dos conceitos e propriedades já vistos no primeiro capítulo e que agora serão definidos e provados no conjunto dos números reais comensuráveis. Observamos aqui que, sendo $\mathbb{R}$ um corpo, trabalhamos o conceito de múltiplos e divisores (e consequentemente de mmc e mdc) fazendo uma generalização da definição dada no conjunto dos números inteiros.

No terceiro capítulo, ampliamos os conceitos apresentados anteriormente para anéis de integridade e definimos conceitos novos, como, número redutível e irredutível, elementos associados, divisores próprios e impróprios. Podemos destacar ainda o fato de que, quando existe o mmc e mdc de dois elementos do anel, não é garantida a sua unicidade.

Nas considerações finais, destacamos a importância do trabalho feito e resolvemos os exemplos apresentados nesta introdução. Desta forma, nos sentimos motivados ao estudo do tema e reconhecemos a sua importância na educação básica.

2 Definição e Resultados de mmc e mdc em $\mathbb{Z}$

Neste capítulo apresentaremos algumas definições e resultados sobre o *mmc* e *mdc* de números inteiros. Provaremos a maioria dos resultados apresentados, visto que, no conjunto dos números inteiros existem muitas aplicações do conceito estudado. É importante que este capítulo seja bem compreendido já que ampliaremos o *mmc* e o *mdc* a partir deste. Nos baseamos nos conceitos apresentados em [3] e [4].

Definição 2.1 *Dados dois números inteiros a e b, diremos que b é* ***múltiplo*** *de a quando existe $c \in \mathbb{Z}$ tal que $b = c.a$. Neste caso, dizemos também que a é* ***divisor*** *de b.*

Definição 2.2 *Dizemos que l é um* ***múltiplo comum*** *de a e b, se l é um múltiplo de a e de b. Dizemos que k é* ***divisor comum*** *de a e b, se k é divisor de a e de b.*

Sejam $a, b \in \mathbb{Z}$. Vamos definir o Mínimo Múltiplo Comum e o Máximo Divisor Comum de a e b da seguinte forma:

Definição 2.3 *Dizemos que um inteiro M é o* ***Mínimo Múltiplo Comum*** *de a e b, e escrevemos $M = mmc(a, b)$, se:*
(1) $M > 0$;
(2) M é múltiplo comum de a e b;
(3) Se existir $M' > 0$ tal que M' é um múltiplo comum de a e b então $M \leq M'$.

Definição 2.4 *Dizemos que um inteiro positivo D é o* ***Máximo Divisor Comum*** *de a e b, e escrevemos $D = mdc(a, b)$, se:*
(1) D é divisor comum de a e b;
(2) Se D' é divisor comum de a e b então $D' \leq D$.

Proposição 2.5 *Sejam a, b, d, m quatro inteiros positivos tais que $a.b = m.d$. Mostre que m é um múltiplo comum de a e b se, e somente se, d é um divisor comum de a e b.*

Demonstração: Suponhamos que m é um múltiplo comum de a e b, sendo $a, b, m \in \mathbb{Z}^*$. Pelas Definições 2.1 e 2.2, existem x e y inteiros não nulos tais que:

$$m = xa \tag{1}$$

e

$$m = yb. \tag{2}$$

Além disso, por hipótese, temos que $ab = md$.
Usando (1) e as propriedades associativa e comutativa do produto em $\mathbb{Z}$, segue que:

$$ab = (xa)d = a(xd). \tag{3}$$

Pela lei do cancelamento em $\mathbb{Z}$, obtemos:

$$b = xd, \tag{4}$$

ou seja, d é um divisor de b. Analogamente, usando (2), obtemos:

$$a = yd. \tag{5}$$

Portanto, por (4) e (5), d é um divisor comum de a e b.
Reciprocamente, suponhamos que d é um divisor comum de a e b. Por definição, existem x,$y \in \mathbb{Z}$ tais que

$$dy = a \qquad \text{e} \qquad dx = b. \tag{6}$$

Como $ab = md$, segue que:

$$(dy)(dx) = md. \tag{7}$$

Pela associatividade, comutatividade do produto em $\mathbb{Z}$ e pela lei do cancelamento, temos:

$$(dx)y = m \qquad \text{e} \qquad (dy)x = m. \tag{8}$$

Por (6) e (8), vem que

$$m = by \qquad \text{e} \qquad m = ax, \tag{9}$$

ou seja, existem x,$y \in \mathbb{Z}$ tais que

$$m = yb \qquad \text{e} \qquad m = xa. \tag{10}$$

Portanto m é múltiplo comum de a e b. ■

O próximo teorema é conhecido como o Teorema da Divisão Euclidiana.

Teorema 2.6 *Sejam a e b dois números inteiros com $a \neq 0$. Existem dois únicos números inteiros q e r tais que $b = a.q + r$, com $0 \leq r <\mid a \mid$.*

Demonstração: Veja [1] (pág. 125).

Proposição 2.7 *Todo múltiplo comum de dois inteiros positivos a e b é múltiplo comum de $mmc(a, b)$.*

Demonstração: Seja $m = mmc(a, b)$. Suponha que m' seja um múltiplo comum de a e b. Queremos mostrar que m' é múltiplo de m.
Se $m' = 0$, nada temos a provar (pois 0 é múltiplo de qualquer inteiro, inclusive de m).
Suponhamos que $m' \neq 0$. Por definição

$$m = mmc(a, b) > 0.$$

Pelo Teorema 2.6, podemos escrever

$$m' = m.q + r \qquad \text{com} \qquad 0 \leq r < m. \tag{11}$$

Assim

$$r = m' - mq. \tag{12}$$

Como m' é múltiplo comum de a e b, então existem $x, y \in \mathbb{Z}$ tais que

$$m' = x.a \qquad \text{e} \qquad m' = y.b. \tag{13}$$

Pela Definição 2.3, m é múltiplo comum de a e b. Consequentemente, mq é múltiplo comum de a e b. Logo existem $z, w \in \mathbb{Z}$ tais que

$$mq = z.a \qquad \text{e} \qquad mq = w.b. \tag{14}$$

Assim,

$$r = m' - mq = x.a - z.a = (x - z).a, \qquad \text{onde} \qquad (x - z) \in \mathbb{Z} \tag{15}$$

e

$$r = y.b - w.b = (y - w).b, \qquad \text{onde} \qquad (y - w) \in \mathbb{Z}, \tag{16}$$

ou seja, r é múltiplo comum de a e b. Disto resulta que $r = 0$, pois caso contrário, teríamos um múltiplo comum r de a e b, tal que

$$0 < r < m,$$

contradizendo a definição de mmc, onde m é o mínimo dos múltiplos e, neste caso,

$$r < m.$$

Logo, como $r = 0$, temos: $m' = mq$, ou seja, m' é múltiplo de $m = mmc(a, b)$. ■

Na demontração do próximo Teorema usaremos o seguinte lema, conhecido como o princípio da Boa Ordenação.

Lema 2.8 *Todo subconjunto não vazio formado por números naturais possui um menor elemento.*

Demonstração: Veja [7] (pág. 3).

O pricípio da Boa Ordem é equivalente a: Todo subconjunto não vazio limitado superiormente de $\mathbb{Z}$, possui um máximo.

Observação 2.9 *Seja A um subconjunto não vazio de $\mathbb{Z}$.*

(1) Dizemos que A é limitado inferiormente por um inteiro m se $a \geqslant m$, para cada a em A;

(2) Dizemos que A é limitado superiormente por um inteiro M se $a \leqslant M$, para cada a em A.

Proposição 2.10

(1) Todo subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente tem um menor elemento;

(2) Todo subconjunto não vazio de $\mathbb{Z}$ e limitado superiormente tem um maior elemento.

Demonstração: (1) Seja $R \subset \mathbb{Z}$ um subconjunto qualquer, não vazio, limitado inferiormente. Logo, existe $m \in \mathbb{Z}$ tal que

$$a \geqslant m, \forall a \in R. \tag{17}$$

Caso $R = \{m\}$ então m é o maior e o menor elemento de R, não há o que provar. Se $R \neq \{m\}$, considere o conjunto

$$R' = \{x \in \mathbb{Z}; x = a - m, a \in R\}.$$

Para cada $a \in R$, por (17) temos

$$a - m \geq 0,$$

o que implica que cada $x \in R'$ é um número natural. Assim, R' está contido no conjunto dos números naturais. Como $R \neq \varnothing$, então $R' \neq \varnothing$. Pelo princípio da Boa Ordenação, existe $x_0 \in R'$ tal que, para cada $x \in R'$

$$x \geq x_0.$$

Sendo x_0 um elemento de R', temos que

$$x_0 = a_0 - m,$$

para algum inteiro $a_0 \in R$. Logo, para todo $x \in R'$

$$x \geq a_0 - m.$$

Donde segue que para todo $a \in R$,

$$a - m \geq a_0 - m.$$

Somando m em ambos os lados da desigualdade temos

$$a \geq a_0, \forall a \in R.$$

Portanto, $a_0 \in R$ é o menor elemento deste conjunto.

(2) Seja $S \subset \mathbb{Z}$ um subconjunto qualquer, não vazio e limitado superiormente. Logo, existe $M \in \mathbb{Z}$ tal que

$$a \leq M, \forall a \in S.$$

A equivalência do Princípio da Boa Ordem segue do seguinte fato: S é limitado inferiormente se, e somente se, $-S$ é limitado superiormente, onde

$$-S = \{-x \in \mathbb{Z}; x \in S\}.$$

De fato, considere o conjunto:

$$S' = \{x \in \mathbb{Z}; x = -a, a \in S\}.$$

Para cada $a \in S$, temos

$$a \leq M$$

ou, equivalentemente,

$$-a \geq -M.$$

Logo, para cada $x \in S'$ temos

$$x \geq -M.$$

Pelo item anterior, já provado, S' tem um primeiro elemento, ou seja, existe $y_0 \in S'$ tal que

$$x \geq y_0, \forall x \in S'.$$

Pela caracterização dos elementos de S' temos

$$y_0 = -z_0,$$

para algum $z_0 \in S$. Daí, para cada $a \in S$

$$-a \geq -z_0,$$

ou seja,

$$a \leq z_0.$$

■

Teorema 2.11 *(Relação de Bézout) Dados dois inteiros a e b quaisquer, não ambos nulos, existem dois inteiros m e n tais que $mdc(a, b) = a.n + b.m$.*

Demonstração: Considere o conjunto

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

Seja $S = S' \cap \mathbb{N}$. Temos $S \neq \varnothing$, pois como $a, b \in \mathbb{Z}$, segue que

$$a = a.(1) + b.0 \in S',$$

$$-a = a.(-1) + b.0 \in S'$$

e assim

$$a, -a, b, -b \in S',$$

sendo pelo menos um deles um inteiro positivo.
Assim $S \subset \mathbb{N}$ e $S \neq \varnothing$, segue do Princípio da Boa Ordenação que S tem um menor elemento. Seja d o menor elemento de S,

$$d = am + bn, \tag{18}$$

para algum $m, n \in \mathbb{Z}$. Primeiramente mostraremos que d é divisor comum de a e b. Pelo algoritmo da Divisão de Euclides

$$a = qd + r, 0 \leq r < d.$$

Se $r > 0$ então teríamos

$$r = a - qd = a - q(am + bn) =$$
$$= a(1 - qm) + b(-qn) \in S',$$

contradizendo o fato de d ser o mínimo. Assim $r = 0$ e $a = qd$, ou seja, d é divisor de a
Com argumento similar podemos mostrar que d é divisor de b.
Finalmente, seja $d' > 0$ um divisor comum qualquer de a e b. Pela Definição 2.1, existem $u, v \in \mathbb{Z}$ tais que

$$a = u.d' \qquad \text{e} \qquad b = v.d'. \tag{19}$$

Assim de (18) e (19), temos:

$$d = a.m + b.n = (ud').m + (vd').n =$$

$$= (um).d' + (vn).d' =$$

$$= (um + vn).d',$$

com $(um + vn) \in \mathbb{Z}_+$ (pois $d > 0 \quad$ e $\quad d' > 0$).
Portanto d é um múltiplo de d' (ou d' é divisor de d). Disto segue que $d' \leq d$.
(Caso $d' < 0$ então também vale $d' < 0 < d$).
Mostramos assim que: $d > 0$ (pois $d \in \mathbb{N} \cap \mathbb{S}'$), d é divisor comum de a e b e se d' é outro divisor comum de a e b então

$$d' \leq d.$$

Pela Definição 2.4, segue que

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

Agora o resultado segue de (18). ■

Como consequência da demonstração acima temos o seguinte resultado.

Corolário 2.12 *Dados dois inteiros a e b, não ambos nulos, o menor elemento positivo do conjunto $a\mathbb{Z} + b\mathbb{Z}$ é $mdc(a, b)$.*

A seguinte proposição nos mostra, no item (2), uma importante relação entre o $mmc(a, b)$ e o $mdc(a, b)$, onde a e b são números inteiros.

Proposição 2.13 *Sejam a, b inteiros não nulos quaisquer. Valem as propriedades:*

(1) Sempre existem os números $mmc(a, b)$ e $mdc(a, b)$;

(2) $|a|.|b| = mmc(a, b).mdc(a, b)$;

(3) Para qualquer $c \in \mathbb{Z}$,

$$mdc(ac, bc) = |c|mdc(a, b) \tag{20}$$

e

$$mmc(ac, bc) = |c|mmc(a, b). \tag{21}$$

Demonstração: (1) Seja D o conjunto dos divisores comuns de a e b. Temos $D \neq \varnothing$ pois $1 \in \mathbb{Z}$ é divisor comum de a e b. Mostraremos primeiramente que D é limitado inferiormente e superiormente. Para isso, seja $z \in \mathbb{Z}$, então z é divisor comum de a e b, logo existem $x, y \in D$ tais que

$$a = xz \qquad \text{e} \qquad b = yz. \tag{22}$$

Como $a \neq 0$ e $b \neq 0$, devemos ter

$$|x| \geq 1 \qquad \text{e} \qquad |y| \geq 1.$$

Assim

$$|z| \leq |z||x| = |a|$$

e

$$|z| \leq |y||z| = |b|.$$

Portanto qualquer divisor comum de a e b satisfaz

$$-|a| \leq z \leq |a| \qquad \text{e} \qquad -|b| \leq z \leq |b|. \tag{23}$$

Seja $K = max\{|a|, |b|\}$. Então de (23) temos

$$-K \leq z \leq K.$$

Portanto, $D \subset \mathbb{Z}$ é limitado superiormente e assim segue da Proposição 2.10 que D tem um maior elemento, ou seja, existe $mdc(a, b)$.
Seja M o conjunto dos múltiplos positivos comuns de a e b. Assim, M é limitado inferiormente por 0. $M \neq \varnothing$, pois $|a||b| \in M$. Assim $M \subset \mathbb{N}$, $M \neq \varnothing$ e é limitado inferiormente, segue da Proposição 2.10 que M tem um menor elemento. Portanto existe $mmc(a, b)$.

(2) Como a e b são múltiplos de $d = mdc(a, b) > 0$ então pelas Definições 2.4 e 2.1, existem $x, y \in \mathbb{Z}$ tais que

$$a = x.d \qquad \text{e} \qquad b = y.d. \tag{24}$$

Disto segue que $a.b$ é múltiplo de d. Logo existe $m \in \mathbb{Z}$ tal que

$$a.b = m.d.$$

Pela Proposição 2.5 temos que m é um múltiplo comum de a e b e, consequentemente,pela Proposição 2.7, temos que

$$m = mmc(a, b).c,$$

para algum $c \in \mathbb{Z}$. Assim,

$$a.b = mmc(a, b).c.mdc(a, b). \tag{25}$$

Novamente pela Proposição 2.5, segue que, $c.mdc(a, b)$ é um divisor comum de a e b. Logo, sendo o $mdc(a, b)$ o maior dentre esses divisores segue que:

$$c.mdc(a, b) \leq mdc(a, b).$$

Se $a > 0$ e $b > 0$, ou $a < 0$ e $b < 0$, segue de (25) que $c \geq 1$ (pois $c > 0$ e $c \in \mathbb{Z}$). Daí temos

$$mdc(a, b) \leq c.mdc(a, b).$$

Pelas duas desigualdades acima temos que $c = 1$. Donde segue por (25) que

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

Se a e b tem sinais opostos, suponhamos sem perda de generalidade, que $a > 0$ e $b < 0$. Como $c.mdc(a, b)$ é um divisor comum de a e b, temos que $(-c).mdc(a.b)$ também é um divisor comum de a e b. Assim

$$(-c)mdc(a, b) \leq mdc(a, b).$$

Como $(-c) \geq 0$ e $(-c) \in \mathbb{Z}$, segue que $-c \geq 1$ e desta forma

$$mdc(a, b) \leq (-c).mdc(a, b).$$

Assim $(-c) = 1$, ou seja, se a e b tem sinais opostos então

$$a.b = (-1)mmc(a, b).mdc(a, b).$$

Disto resulta que

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

(3) Para provarmos (20), denotemos por $minA$ o menor elemento de um conjunto de números naturais A. Sabemos pela Proposição 2.12 que

$$mdc(a,b) = min\{x \in a\mathbb{Z} + b\mathbb{Z}, x > 0\}.$$

Portanto,

$$\begin{aligned} mdc(ac,bc) &= min\{x \in ac\mathbb{Z} + bc\mathbb{Z}, x > 0\} = \\ &= |c|.min\{x \in a\mathbb{Z} + b\mathbb{Z}, x > 0\} = \\ &= |c|.mdc(a,b). \end{aligned}$$

Logo,

$$mdc(ac,bc) = |c|.mdc(a,b).$$

Provemos (21). Pela propriedade anterior, temos:

$$mmc(ac,bc).mdc(ac,bc) = (ac).(bc).$$

Como $mdc(a,b) \in \mathbb{N}$, então $mdc(a,b) > 0$ e usando (20), temos

$$mmc(ac,bc) = \frac{ac.bc}{mdc(ac,bc)} = \frac{abc^2}{|c|.mdc(a,b)} = \frac{ab|c|}{mdc(a,b)} = |c|.mmc(a,b).$$

■

Definição 2.14 *Dois inteiros a e b são* ***primos entre si*** *se $mdc(a,b) = 1$.*

Observação 2.15 *Toda fração que possua numerador e denominador primos entre si é chamada de* ***fração irredutível****.*

3 mmc e mdc de Números Reais

Estudaremos, neste capítulo, uma extensão do conceito de múltiplos, divisores, mdc e mmc dos inteiros para os números reais. Faremos isso usando o conceito de números reais comensuráveis. A referência bibliográfica principal deste capítulo é [6].

Definição 3.1 *Dois números reais r e s são* ***comensuráveis*** *se existem inteiros não nulos m e n tais que $m.r = n.s$.*

Exemplo 3.2 *Dois racionais são sempre comensuráveis. De fato, sejam $r, s \in \mathbb{Q}$. Caso $r = 0$ ou $s = 0$ é trivial. Suponhamos que $r \neq 0$ e $s \neq 0$. Logo, existem $a, b, c, d \in \mathbb{Z}^*$, tais que:*

$$r = \frac{a}{b} \qquad e \qquad s = \frac{c}{d}.$$

Tomemos $m = abc \in \mathbb{Z}^*$ e $n = a^2d \in \mathbb{Z}^*$. Assim,

$$r.m = \frac{a}{b}.abc = a^2c = \frac{a^2cd}{d} = ns.$$

Logo, r e s são comensuráveis.

Exemplo 3.3 *Dois irracionais podem ser comensuráveis. Por exemplo, $\sqrt{2}$ e $2\sqrt{2}$, basta tomarmos $m = 2$ e $n = 1$ e teremos*

$$m\sqrt{2} = n.2\sqrt{2},$$

donde vem que $\sqrt{2}$ e $2\sqrt{2}$ são reais comensuráveis.

Exemplo 3.4 *Dois reais quaisquer nem sempre são comensuráveis. Por exemplo: tomemos o racional $\frac{1}{2}$ e o irracional $\sqrt{2}$. Suponhamos que $\frac{1}{2}$ e $\sqrt{2}$ sejam comensuráveis. Então existem $x, y \in \mathbb{Z}^*$ tais que*

$$x.\frac{1}{2} = y.\sqrt{2},$$

ou seja,

$$\frac{x}{2y} = \sqrt{2}.$$

Do lado esquerdo da igualdade, temos um número racional e do lado direito um irracional, o que é uma contradição. Portanto, $\frac{1}{2}$ e $\sqrt{2}$ não são comensuráveis.

Definição 3.5 *Dizemos que um número real r é um* ***múltiplo inteiro*** *de um real s, ou que, s é um* ***divisor inteiro*** *de r, se existe um inteiro a tal que $r = a.s$.*

Observação 3.6 *Se r é um múltiplo inteiro de um real s, então $-r$ também é múltiplo inteiro de s. Analogamente, $-s$ será um divisor de r.*

Proposição 3.7 *Sejam r e s dois reais não nulos. As seguintes afirmações são equivalentes:*

(1) r e s são comensuráveis;

(2) O quociente $\frac{r}{s}$ é um número racional;

(3) Existe um real $t \neq 0$ que é múltiplo inteiro comum de r e de s;

(4) Existe um real u que é divisor inteiro comum de r e de s.

Demonstração: (1) $\Rightarrow$ (2) Sejam r e s reais comensuráveis não nulos. Então existem $m, n \in \mathbb{Z}^*$ tais que

$$m.r = n.s.$$

Assim, como m, n, r, s são não nulos, podemos escrever:

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

Donde vem que $\frac{r}{s} \in \mathbb{Q}$.

(2) $\Rightarrow$ (3) Suponhamos que $\frac{r}{s} \in \mathbb{Q}$. Então, existem $m, n \in \mathbb{Z}^*$ tais que:

$$\frac{r}{s} = \frac{n}{m}. \tag{26}$$

Quero obter $t \in \mathbb{R}^*$ tal que:

$$t = m.r \quad \text{e} \quad t = n.s \quad \text{onde} \quad m, n \in \mathbb{Z}. \tag{27}$$

Para isso, basta multiplicarmos (26) por sm e obtemos que

$$t := rm = sn,$$

ou seja, existe $t \neq 0$ que é um múltiplo inteiro comum a r e s.

(3) $\Rightarrow$ (4) Seja $t \in \mathbb{R}^*$ um múltiplo inteiro comum de r e s. Então existem $m, n \in \mathbb{Z}$ tais que

$$t = m.r \quad \text{e} \quad t = n.s. \tag{28}$$

Queremos obter $u \in \mathbb{R}$ tal que

$$r = n.u \quad \text{e} \quad s = m.u,$$

onde $m, n \in \mathbb{Z}^*$. De (28) segue que

$$m.r = n.s.$$

Disto vem que

$$r = n.\frac{s}{m} \quad \text{ou} \quad s = m.\frac{r}{n}.$$

Basta tomarmos

$$u = \frac{s}{m} \in \mathbb{R} \qquad \text{ou} \qquad u = \frac{r}{n} \in \mathbb{R}$$

e teremos que u é divisor inteiro de r e s.

(4) $\Rightarrow$ (1) Suponhamos que existe $u \in \mathbb{R}$ que é divisor comum de r e s, ou seja, existem $m, n \in \mathbb{Z}$ tais que

$$r = n.u \quad \text{e} \quad s = m.u. \tag{29}$$

Queremos mostrar que r e s são comensuráveis. De fato, por (29) obtemos

$$\frac{r}{n} = u \qquad \text{e} \qquad \frac{s}{m} = u.$$

Assim,

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

o que implica que

$$r.m = s.n,$$

onde $m, n \in \mathbb{Z}^*$, ou seja, r e s são comensuráveis. ■

Definição 3.8 *Sejam r e s dois reais comensuráveis não nulos. Dizemos que t é o* ***Mínimo Múltiplo Comum Generalizado*** *entre r e s, e escrevemos $t = mmcg(r, s)$ se:*

(1) $t > 0$;

(2) t é um múltiplo inteiro comum de r e s;

(3) Se t' é múltiplo inteiro comum de r e s e $t' > 0$, então $t \leq t'$.

Exemplo 3.9 *Sejam $r, s, t, t' \in \mathbb{R}^*$, onde $r = \frac{3}{2}$, $s = \frac{1}{4}$, $t = \frac{3}{2}$ e $t' = 3$. Vamos verificar os três itens da Definição acima:*
(1) $t = \frac{3}{2} > 0$;
(2) $t = a.r$, com $a = 1 \in \mathbb{Z}$ e $t = b.s$, com $b = 6 \in \mathbb{Z}$;
(3) $t' = c.r$, com $c = 2 \in \mathbb{Z}$ e $t' = d.s$, com $d = 12 \in \mathbb{Z}$, então $t \leq t'$.
Portanto, podemos dizer que $t = mmcg(r, s)$, ou seja, $mmcg(\frac{3}{2}, \frac{1}{4}) = \frac{3}{2}$
Devemos observar que neste exemplo para qualquer t' que for múltiplo inteiro comum a r e s, temos que $t \leq t'$, por isso afirmamos que $t = mmcg(r, s)$.

Definição 3.10 *Dizemos que u é o* ***Máximo Divisor Comum Generalizado*** *entre r e s, onde r e s são reais comensuráveis não nulos, e escrevemos $u = mdcg(r, s)$, se:*

(1) u é um Divisor Inteiro Comum de r e s;

(2) Se u' é Divisor Inteiro Comum de r e s então $u' \leq u$.

Exemplo 3.11 *Sejam $r = 2\sqrt{2}, s = \sqrt{2}, u = \sqrt{2}$ e $u' = \frac{\sqrt{2}}{2}$. Observemos que u e u' são divisores inteiro comum a r e s. Além disso, $u' \leq u$. Portanto u é o máximo divisor comum generalizado entre r e s.*

Teorema 3.12 *Sejam r e s dois reais comensuráveis não nulos. Então*

$$mmcg(r, s) = |v.r| = |u.s|$$

e

$$mdcg(r, s) = \left|\frac{r}{u}\right| = \left|\frac{s}{v}\right|,$$

onde $\frac{u}{v}$ é a forma irredutível do racional $\frac{r}{s}$.

Demonstração: Como r e s são reais comensuráveis não nulos, pela Proposição 3.7, $\frac{r}{s}$ é um racional. Seja $\frac{u}{v}$ a forma irreditível de $\frac{r}{s}$. Provaremos inicialmente que

$$mmcg(r, s) = |v.r| = |u.s|.$$

Consideremos o caso $r > 0$ e $s > 0$. Temos que

$$\frac{r}{s} = \frac{u}{v},$$

isto implica que

$$rv = su = x \in \mathbb{Z}.$$

Logo x é múltiplo inteiro comum a r e s.
Seja $y \in \mathbb{Z}^*$ outro múltiplo inteiro comum a r e s. Por definição, existem $a, b \in \mathbb{Z}^*$ tais que

$$y = br \qquad \text{e} \qquad y = as.$$

Daí,

$$\frac{u}{v} = \frac{r}{s} = \frac{a}{b}.$$

Sendo $\frac{u}{v}$ irredutível, temos $u \leq a$ e $v \leq b$. Como $r > 0$ e $s > 0$, então

$$su \leq sa \qquad \text{e} \qquad rv \leq rb,$$

ou seja, $x \leq y$. Pela Definição 3.8, $mmcg(r, s) = x = |v.r| = |u.s|$.
Nos demais casos ($r > 0$ e $s < 0$, $r < 0$ e $s > 0$ ou $r < 0$ e $s < 0$), considerando a Observação 3.6 e Definição 3.8, também teremos $mmcg(r, s) = |v.r| = |u.s|$.

Vamos provar agora que

$$mdcg(r, s) = \left|\frac{r}{u}\right| = \left|\frac{s}{v}\right|.$$

Suponhamos primeiro que $r > 0$ e $s > 0$. Então, temos

$$\frac{r}{s} = \frac{u}{v}, \tag{30}$$

ou seja,

$$r = u.\frac{s}{v}. \tag{31}$$

Notemos também que

$$s = v\frac{s}{v}. \tag{32}$$

De (31) e (32) segue que $\frac{s}{v}$ é divisor inteiro comum a r e s.
Suponhamos agora que m é divisor inteiro comum a r e s, qualquer. Vamos mostrar que $m \leq \frac{s}{v}$. Como m é divisor inteiro de r e de s, segue da Definição 3.5 que existem $x, y \in \mathbb{Z}^*$ tais que

$$m.x = r \qquad \text{ou} \qquad m = \frac{r}{x}$$

e

$$m.y = s \qquad \text{ou} \qquad m = \frac{s}{y}.$$

Logo

$$\frac{r}{x} = \frac{s}{y} \qquad \text{ou} \qquad r = x.\frac{s}{y}, \tag{33}$$

e também,

$$s = y.\frac{s}{y}. \tag{34}$$

De (33) e (34) temos $\frac{s}{y}$ é divisor comum de r e s. Como $\frac{u}{v}$ é a fração irredutível de $\frac{r}{s}$, então de (33) segue que

$$\frac{r}{s} = \frac{x}{y},$$

isto implica que

$$\frac{x}{y} = \frac{u}{v}$$

e $\frac{u}{v}$ é irredutível, donde vem que

$$v < y,$$

ou seja,

$$\frac{1}{v} > \frac{1}{y}$$

e $s > o$, logo

$$\frac{s}{v} > \frac{s}{y}.$$

Portanto, pela Definição 3.10, $\frac{s}{v}$ é o máximo divisor inteiro comum a r e s, e ainda,

$$\frac{r}{s} = \frac{u}{v} \qquad \text{ou} \qquad \frac{r}{u} = \frac{s}{v}.$$

Assim,

$$mdcg(r,s) = \left|\frac{r}{u}\right| = \left|\frac{s}{v}\right|.$$

Suponhamos agora que $r > 0$ e $s < 0$. Assim,

$$\frac{r}{s} = \frac{a}{b} < 0 \Rightarrow a < 0 \quad \text{e} \quad b > 0 \quad \text{ou} \quad b < 0 \quad \text{e} \quad a > 0.$$

Se $a < 0$, então

$$r.b = s.a > 0$$

e se $b < 0$, então

$$r.b < 0, \quad s.a < 0 \quad \text{e} \quad r.b = s.a > 0.$$

Suponha que $r < 0$ e $s < 0$. Assim

$$\frac{r}{s} = \frac{a}{b} < 0 \Rightarrow a > 0 \quad \text{e} \quad b < 0 \quad \text{ou} \quad a < 0 \quad \text{e} \quad b > 0.$$

Se $a > 0$, então

$$r.b = s.a > 0$$

e se $a < 0$, então

$$r.b = s.a > 0.$$

Portanto, para quaisquer $r, s \in \mathbb{R}$ não nulos temos:

$$mdcg(r,s) = \left|\frac{r}{u}\right| = \left|\frac{s}{v}\right|.$$

■

Corolário 3.13 *Sejam r, s racionais não nulos e sejam $a, b, c, d \in \mathbb{Z}$ tais que $\frac{a}{b}$ e $\frac{c}{d}$ são as representações para r e s, respectivamente, na forma de fração irredutível. Então,*

$$mmcg(r,s) = \frac{mmc(a,c)}{mdc(b,d)} \qquad e \qquad mdcg(r,s) = \frac{mdc(a,c)}{mmc(b,d)}. \tag{35}$$

Demonstração: Temos que $mdc(a,b) = mdc(c,d) = 1$ (veja Observação 2.15) e

$$\frac{r}{s} = \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{a.d}{b.c}.$$

Sejam

$$u = \frac{a.d}{mdc(a,c).mdc(b,d)}$$

e

$$v = \frac{b.c}{mdc(a,c).mdc(b.d)}.$$

Temos que $\frac{u}{v}$ é a fração irredutível de $\frac{r}{s}$. Pelo Teorema 3.12 e, como,

$$r.v = s.u,$$

temos:

$$mmcg(r,s) = |v.r| = \left|\frac{r.b.c}{mdc(a,c).mdc(b,d)}\right| = \left|\frac{\frac{a}{b}.b.c}{mdc(a,c).mdc(b,d)}\right| = \left|\frac{a.c}{mdc(a,c).mdc(b,d)}\right|. \tag{36}$$

Pela Proposição 2.13, item 2, temos

$$x.y = mmc(x,y).mdc(x,y),$$

onde $x, y \in \mathbb{Z}$. Assim,

$$\frac{a.c}{mdc(a,c)} = mmc(a,c).$$

Logo,

$$mmcg(r,s) = \left|\frac{mmc(a,c)}{mdc(b,d)}\right|,$$

como $mmc(a,c) > 0$ e $mdc(b,d) > 0$, para convenientes $a, b, c, d \in \mathbb{Z}$ teremos:

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

Analogamente temos pelo Teorema 3.12

$$mdcg(r,s) = \left|\frac{r}{u}\right| = \left|\frac{\frac{a}{b}}{\frac{a.d}{mdc(a,c).mdc(b,d)}}\right| = \left|\frac{a.mdc(a,c).mdc(b,d)}{a.b.d}\right| = \left|\frac{mdc(a,c)}{mmc(b,d)}\right| = \frac{mdc(a,c)}{mmc(b,d)}.$$

■

Observação 3.14 *A hipótese (na forma de fração irredutível) no Corolário 3.13 é extremamente importante, isto é, a fórmula (35) quando aplicada a frações não irredutíveis não proporciona necessariamente o mmcg(r,s) e o mdcg(r,s), como nos mostra o exemplo a seguir. Seja* $r = \frac{6}{8}$ *e* $s = \frac{1}{5}$*, então*

$$\frac{mmc(6,1)}{mdc(8,5)} = 6 \neq 3 = \frac{mmc(3,1)}{mdc(4,5)} = mmcg(r,s)$$

e

$$\frac{mdc(6,1)}{mmc(8,5)} = \frac{1}{40} \neq \frac{1}{20} = \frac{mdc(3,1)}{mmc(4,5)} = mdcg(r,s).$$

Do Teorema 3.12 obtemos os seguintes exemplos:

Exemplo 3.15

$$mmcg(\frac{20}{16}, \frac{1}{5}) = mmcg(\frac{5}{4}, \frac{1}{5}) = \frac{mmc(5,1)}{mdc(4,5)} = \frac{5}{1} = 5$$

e

$$mdcg(\frac{20}{16}, \frac{1}{5}) = mdcg(\frac{5}{4}, \frac{1}{5}) = \frac{mdc(5,1)}{mmc(4,5)} = \frac{1}{20}.$$

Exemplo 3.16

$$mmcg(\frac{3}{5}, \frac{2}{7}) = \frac{mmc(3,2)}{mdc(5,7)} = \frac{6}{1} = 6 \quad e \quad mdcg(\frac{3}{5}, \frac{2}{7}) = \frac{mdc(3,2)}{mmc(5,7)} = \frac{1}{35}.$$

O seguinte Corolário nos garante uma importante relação entre o *mmcg* e o *mdcg* de dois números reais comensuráveis. Esta relação também foi provado no capítulo anterior no conjunto dos números inteiros.

Corolário 3.17 *Sejam* r *e* s *dois reais não nulos comensuráveis. Então:*

(1) $r.s = mdcg(r,s).mmcg(r,s)$*;*

(2) Dado qualquer real não nulo c*, temos ainda* $c.r$ *e* $c.s$ *comensuráveis e*

$$mmcg(cr, cs) = |c|mmcg(r,s) \qquad e \qquad mdcg(cr, cs) = |c|mdcg(r,s).$$

Demonstração: (1) Suponhamos r e s positivos. Sejam $\frac{r}{s} = \frac{u}{v}$, onde $\frac{u}{v}$ é fração irredutível de $\frac{r}{s}$. Pelo Teorema 3.12, temos:

$$mmcg(r,s) = |vr| = |su| \qquad \text{e} \qquad mdcg(r,s) = \left|\frac{r}{u}\right| = \left|\frac{s}{v}\right|.$$

Assim,

$$mmcg(r,s).mdcg(r,s) = |vr|.|\frac{s}{v}| = |\frac{vrs}{v}| = |rs|,$$

como $r > 0$ e $s > 0$ então

$$rs = mmcg(r,s).mdcg(r,s).$$

Suponhamos agora $r < 0$ e $s < 0$, daí

$$rs = |rs|$$

e teremos o desejado. Se $r > 0$ e $s < 0$, então temos

$$u > 0 \quad \text{e} \quad v < 0 \qquad \text{ou} \qquad u < 0 \quad \text{e} \quad v > 0,$$

logo para $u > 0$ e $v < 0$

$$mmcg(r, s) = |vr| = -vr \quad \text{e} \quad mdcg(r, s) = |\frac{s}{v}| = \frac{s}{v},$$

assim

$$mmcg(r, s).mdcg(r, s) = -vr.\frac{s}{v} = -rs > 0,$$

e para, $u < 0$ e $v > 0$

$$mmcg(r, s) = |vr| = vr \quad \text{e} \quad mdcg(r, s) = |\frac{s}{v}| = \frac{-s}{v},$$

assim

$$mmcg(r, s).mdcg(r, s) = vr.\frac{-s}{v} = -rs > 0.$$

Finalmente, se $r < 0$ e $s > 0$, então

$$u > 0 \quad e \quad v < 0 \qquad \text{ou} \qquad u < 0 \quad \text{e} \quad v > 0,$$

logo para $u > 0$ e $v < 0$

$$mmcg(r, s) = |vr| = vr \quad \text{e} \quad mdcg(r, s) = |\frac{s}{v}| = \frac{-s}{v},$$

assim

$$mmcg(r, s).mdcg(r, s) = vr.\frac{-s}{v} = -rs > 0,$$

e para, $u < 0$ e $v > 0$

$$mmcg(r, s) = |vr| = -vr \quad \text{e} \quad mdcg(r, s) = |\frac{s}{v}| = \frac{s}{v},$$

assim

$$mmcg(r, s).mdcg(r, s) = -vr.\frac{s}{v} = -rs > 0.$$

(2) Como $\frac{u}{v}$ é fração irredutível de $\frac{r}{s}$, temos:

$$\frac{r}{s} = \frac{u}{v} \Rightarrow \frac{cr}{cs} = \frac{u}{v} \Rightarrow crv = csu,$$

onde $c \in \mathbb{R}^*$. Pelo Teorema 3.12

$$mmcg(cr, cs) = |crv| = |c|.|rv| = |c|.mmcg(r, s)$$

e

$$mdcg(cr, cs) = |\frac{cr}{u}| = |c|.|\frac{r}{u}| = |c|.mdcg(r, s),$$

como queríamos. ■

Corolário 3.18 *Se r e s são dois números racionais que podem ser representados por uma fração decimal,digamos,*

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

então

$$mmcg(r,s) = \frac{mmc(10^t r, 10^t s)}{10^t}$$

e

$$mdcg(r,s) = \frac{mdc(10^t r, 10^t s)}{10^t}.$$

Demonstração: Como $r = \frac{u}{10^k}$, $s = \frac{v}{10^l}$ e $t \geq k$, $t \geq l$, então

$$10^t r = 10^{t-k}u \qquad \text{e} \qquad 10^t s = 10^{t-l}v$$

com $(t-k) \geq 0$, $(t-l) \geq 0$ consequentemente,$(10^{t-k}u) \in \mathbb{Z}$ e $(10^{t-l}v) \in \mathbb{Z}$ necessário quando usamos o Corolário 3.13. Assim,

$$mmcg(r,s) = mmcg(\frac{10^t}{10^t}r, \frac{10^t}{10^t}s).$$

Pelo Corolário 3.17

$$mmcg(\frac{10^t}{10^t}r, \frac{10^t}{10^t}s) =$$

$$= \frac{1}{10^t} mmcg(10^t r, 10^t s) =$$

$$= \frac{1}{10^t} mmcg(\frac{10^t r}{1}, \frac{10^t s}{1})$$

e, de acordo com com o Corolário 3.13

$$\frac{1}{10^t} mmcg(\frac{10^t r}{1}, \frac{10^t s}{1}) =$$

$$= \frac{1}{10^t} . \frac{mmc(10^t r, 10^t s)}{mdc(1,1)} =$$

$$= \frac{1}{10^t} . \frac{mmc(10^t r, 10^t s)}{1} =$$

$$= \frac{mmc(10^t r, 10^t s)}{10^t}.$$

Logo,

$$mmcg(r,s) = \frac{mmc(10^t r, 10^t s)}{10^t}. \tag{37}$$

Pela Proposição 2.13 (item2) temos que

$$mmc(10^t r, 10^t s) = \frac{10^t r . 10^t s}{mdc(10^t r, 10^t s)}. \tag{38}$$

Pelo Corolário 3.17 temos

$$r.s = mdcg(r,s).mmcg(r,s),$$

donde segue de (37) que

$$rs = \frac{mmc(10^t r, 10^t s)}{10^t}.mdcg(r,s). \tag{39}$$

De (38) e (39) temos

$$rs = \frac{rs10^t}{mdc(10^t r, 10^t s)}.mdcg(r,s).$$

Portanto, $mdcg(r,s) = \dfrac{mdc(10^t r, 10^t s)}{10^t}$. ■

Utilizaremos as propriedades enunciadas neste capítulo para resolvermos os exemplos apresentados na introdução deste trabalho. A resolução dos mesmos será realizada nas considerações finais.

4 mmc e mdc em Anéis de Integridade

A noção de Mínimo Múltiplo Comum e Máximo Divisor Comum introduzida no conjunto dos números inteiros será estendida para um anel de integridade. Neste capítulo, a bibliografia principal utilizada foi [1] e também nos baseamos em [2].

Definição 4.1 *Um* ***Anel*** *é um conjunto não vazio A munido de duas operações internas, uma chamada Soma e denotada por $+$ e a outra chamada Multiplicação e denotada por $*$ satisfazendo as seguintes propriedades:*

(A1) Para quaisquer $a, b \in A$ tem-se $a + b = b + a$;

(A2) Para quaisquer $a, b, c \in A$ tem-se $a + (b + c) = (a + b) + c$;

(A3) Existe $0 \in A$ tal que $a + 0 = 0 + a = a$ para qualquer $a \in A$;

(A4) Para qualquer $a \in A$ existe $-a \in A$ tal que $a + (-a) = (-a) + a = 0$;

(A5) (Associativa) Para quaisquer $a, b, c \in A$ tem-se $a * (b * c) = (a * b) * c$;

(A6) (Distributiva) Para quaisquer $a, b, c \in A$ tem-se $a * (b + c) = (a * b) + (a * c)$ e $(b + c) * a = (b * a) + (c * a)$.

Definição 4.2 *Diz-se que um Anel A é* ***comutativo*** *se, e somente se, quaisquer que sejam $a, b \in A$, tem-se*

$$a * b = b * a,$$

(isto é, vale a propriedade comutativa da multiplicação).

Definição 4.3 *Diz-se que um anel A tem* ***elemento unidade*** *se, e somente se, existe um elemento $1 \in A$ tal que*

$$a * 1 = a = 1 * a,$$

para todo $a \in A$ (existência do elemento unidade da multiplicação).

Definição 4.4 *Dado um conjunto $A \neq 0$ sobre o qual estão definidas as operações de adição e de multiplicação como na Definição 4.1. Dizemos que A é um* ***Anel comutativo com unidade*** *se para quaisquer elementos $a, b, c \in A$ são satisfeitas as seguintes condições:*

(A1) $a + (b + c) = (a + b) + c$;

(A2) $a + b = b + a$;

(A3) $a + 0 = 0 + a = a$;

(A4) $a + (-a) = (-a) + a = 0$;

(M1) $(a * b) * c = a * (b * c)$;

(M2) $a * b = b * a$;

(M3) $a * 1 = 1 * a = a$;

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

Definição 4.5 *Quaisquer que sejam a e b em A, existe um único elemento $x \in A$ tal que*

$$b + x = a.$$

Este elemento é denominado ***Diferença*** *entre a e b e é indicado por $a - b$, logo,*

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

A operação $-$ é denominada ***Subtração****.*

Teorema 4.6 *(Propriedade Distributiva da Multiplicação em relação à Subtração) Quaisquer que sejam os elementos a, b e c de um anel comutativo A, tem-se*

$$a * (b - c) = (a * b) - (a * c).$$

Demonstração: Temos, conforme Definição 4.5 e Definição 4.4, que

$$a * b = a * [c + (b - c)] = a * c + a * (b - c),$$

Portanto,

$$a * (b - c) = (a * b) - (a * c).$$

■

Definição 4.7 *Um elemento a de um anel com elemento unidade 1 é inversível se, e somente se, a é* ***inversível*** *para a multiplicação definida sobre A.*

Observação 4.8 *Se a é inversível então existe um único elemento a^{-1} (denominado inverso de a) tal que*

$$a * a^{-1} = 1 = a^{-1} * a$$

Indicaremos por $U(A)$ **o conjunto dos elementos inversíveis do anel** A.
Vamos mostrar que $u^{-1} \in A$ é único. Para cada $u \in U(A)$, temos $u^{-1} \in A$, pois

$$u * u^{-1} = 1.$$

Suponhamos que exista $x \in A$ tal que

$$u * x = 1,$$

assim

$$u * u^{-1} = u * x$$
$$(u^{-1} * u) * u^{-1} = (u^{-1} * u) * x$$
$$1 * u^{-1} = 1 * x$$
$$u^{-1} = x,$$

logo u^{-1} é único.

Observação 4.9 *Se um produto de elementos de um anel A tem pelo menos um fator igual a zero, então este produto é igual a zero, pois*

$$a * 0 = 0 = 0 * a,$$

para todo elemento $a \in A$. É importante observar que, em geral, não é verdadeira a recíproca desta propriedade, isto é, um produto de elementos de A pode ser nulo com todos os fatores diferentes de zero, o exemplo abaixo ilustra esta afirmação.

Exemplo 4.10 *Consideremos o conjunto A de todas as funções reais e contínuas definidas sobre o conjunto dos números reais. Se f e g são dois elementos quaisquer de A definiremos $f + g$ e $f * g$ por*

$$(f + g)(x) = f(x) + g(x) \qquad e \qquad (f * g)(x) = f(x) * g(x),$$

para todo $x \in \mathbb{R}$. As funções $f + g$ e $f * g$ pertencem a A, pois a soma e o produto de duas funções contínuas são funções contínuas e ficam assim definidas operações de adição e de multiplicação sobre o conjunto A.
É facil verificar que estão satisfeitas as condições $A1 - A4, M1 - M3$ e D. Portanto estas operações definem uma estrutura de anel comutativo com elemento unidade sobre o conjunto A.
Notemos que o elemento zero de A é a função constante igual a zero e o elemento unidade de A é a função constante igual a 1. Sejam f e g as funções definidas por

$$f(x) = \begin{cases} x, & se \quad x \geq 0 \\ 0, & se \quad x < 0 \end{cases}$$

e

$$g(x) = \begin{cases} 0, & se \quad x \geq 0 \\ -x, & se \quad x < 0 \end{cases}$$

É imediato que $f \neq 0$, $g \neq 0$ e, além disso, f e g são contínuas. Por outro lado, temos $f * g = 0$, pois, para todo $x \in \mathbb{R}$ pelo menos um dos números reais $f(x)$ ou $g(x)$ é nulo.

Definição 4.11 *Diz-se que um elemento a, de um anel comutativo não nulo A, é um* ***divisor do zero*** *se, e somente se, existe $b \in A$, $b \neq 0$, tal que $a * b = 0$. Se a é divisor do zero, diremos que a é um* ***divisor próprio do zero****.*

Definição 4.12 *Um anel A é chamado de Domínio de Integridade, se A* ***não possui divisor de zero****, isto é, se $a \neq 0$ e $b \neq 0$, então $a * b \neq 0$, ou equivalentemente $a * b = 0$, então $a = 0$ ou $b = 0$.*

Corolário 4.13 *(Lei Restrita do Cancelamento da Multiplicação) Quaisquer que sejam os elementos a, b e c, de um anel comutativo e não nulo A, se $a * b = a * c$ e se a não é divisor do zero, então $b = c$.*

Demonstração: De

$$a * b = a * c,$$

segue que

$$(a * b) + (-(a * c)) = (a * c) + (-(a * c)) = 0,$$

donde vem que

$$(a * b) - (a * c) = 0,$$

logo pela Propriedade distributiva da multiplicação em relação à subtração

$$a * (b - c) = 0$$

Como a não é divisor de zero, então

$$b - c = 0.$$

Portanto $b = c$. ■

Definição 4.14 *Chama-se* ***Anel de Integridade*** *a todo anel comutativo com elemento unidade $1 \neq 0$, que não possui divisores próprios do zero.*

Exemplo 4.15 *O conjunto $\mathbb{Z}$ dos inteiros com as operações de adição e multiplicação usuais é um exemplo de anel de integridade. Analogamente os conjuntos $\mathbb{Q}$ dos racionais e $\mathbb{R}$ dos reais também são anéis de integridade.*

Apresentaremos agora a definição de anel fatorial, analisaremos suas propriedades gerais, daremos as noções de divisor próprio, impróprio, elemento redutível e irredutível num anel de integridade qualquer.

Definição 4.16 *Sejam a e b dois elementos de um anel comutativo A com elemento unidade; diz-se que a é um* ***divisor*** *de b se, e somente se, existe c em A tal que $b = a * c$.*

Usaremos a notação a/b para indicar que a é divisor de b, ou que a divide b.

Observação 4.17 *Notemos que $a/0$ para todo $a \in A$ e que $0/a$ se, e somente se, $a = 0$.*

Exemplo 4.18 *Temos $u/1$ se, e somente se, u é um elemento inversível do anel A. Portanto, o conjunto $U(A)$ dos elementos inversíveis de A pode ser definido por*

$$U(A) = \{u \in A; u/1\}.$$

Teorema 4.19 *Quaisquer que sejam os elementos $a, b, c \in A$, onde A é um anel comutativo com unidade, tem-se:*

(1) Propriedade Simétrica: a/a;

(2) Propriedade Transitiva: Se a/b e b/c, então a/c;

(3) Se a/b e se a/c, então $a/(b \pm c)$;

(4) Se a/b então $(a * c)/(b * c)$.

Demonstração: (1) Temos que

$$a = a * 1,$$

logo a é divisor de a, ou seja, a/a.
(2) Como

$$a/b \qquad \text{e} \qquad b/c,$$

então existem $x, y \in A$ tais que

$$a * x = b \qquad \text{e} \qquad b * y = c.$$

Donde vem que

$$c = (a * x) * y,$$

por (M1) e (M2) da Definição 4.4 temos

$$c = (x * y) * a.$$

Portanto a/c.
(3) Como a/b e a/c, então existem $x, y \in A$ tais que

$$a * x = b \qquad \text{e} \qquad a * y = c.$$

Assim $b \pm c = a * x \pm a * y$, daí pelo item (D) da Definição 4.4 temos:

$$b \pm c = a * (x \pm y).$$

Donde segue que

$$a/(b \pm c).$$

(4) Temos que a/b, assim existe $x \in A$ tal que

$$a * x = b.$$

Multiplicando ambos os lados da igualdade por $c \in A$, obtemos

$$c * (a * x) = c * b.$$

Utilizando a Definição 4.4, itens (M1) e (M2), vem que

$$(a * c) * x = b * c.$$

Portanto

$$a * c/b * c.$$

■

Corolário 4.20 *Quaisquer que sejam os elementos a, b e c de um anel de integridade A, com $c \neq 0$, temos a/b se, e somente se, $(a * c)/(b * c)$.*

Demonstração: Suponhamos, inicialmente, que a/b, logo pelo item (d) do Teorema anterior temos

$$a * c/b * c.$$

Reciprocamente, como A é anel de integridade, então todos os seus elementos não são divisores próprio do zero, logo pelo Corolário 4.13 segue o desejado. ■

Teorema 4.21 *Se a e b são dois elementos quaisquer de um anel de integridade A, temos a/b e b/a se, e somente se, existe u em $U(A)$ tal que $b = a * u$.*

Demonstração: Sejam a, b elementos do anel A tais que

$$a/b \qquad \text{e} \qquad b/a. \tag{40}$$

Se $a = 0$, então de (40) segue que

$$0/b \qquad \text{e} \qquad b/0$$

e pela Observação 4.17 temos $b = 0$, logo $b = a * u$ para qualquer $u \in A$.
Desta forma, vamos supor que $a \neq 0$. Se a/b e b/a, então por definição existem $u, v \in A$ tais que

$$a * u = b, \tag{41}$$

$$b * v = a. \tag{42}$$

Logo, substituindo (41) em (42) temos

$$(a * u) * v = a,$$

ou seja,

$$a * u/a,$$

ou ainda,

$$a * u/a * 1.$$

Assim pelo Corolário 4.20

$$u/1,$$

donde segue que

$$u \in U(A).$$

Reciprocamente, suponha que exista $u \in U(A)$ tal que

$$b = a * u, \tag{43}$$

logo a/b. Por outro lado, temos que $u^{-1} \in U(A)$ tal que

$$u^{-1} * u = 1.$$

Assim de (43) multiplicando ambos os lados da igualdade por u^{-1} e usando as propriedades comutativa, associativa e do elemento inversível de A obtemos

$$b * u^{-1} = a.$$

Portanto

$$b/a.$$

■

Definição 4.22 *Sejam a e b dois elementos quaisquer de um anel de integridade A. Diz-se que a é **associado** a b se, e somente se, a/b e b/a.*

Usaremos a notação $a \sim b$ para indicar que a é associado a b.

Observação 4.23 *De acordo com o Teorema 4.21, temos $a \sim b$ se, e somente se, existe $u \in U(A)$ tal que $b = a * u$.*

Definição 4.24 *Seja A um anel de integridade, para todo elemento não nulo $a \in A$ chamaremos de* ***divisores de*** *a, denotado por $D(a)$ o seguinte conjunto:*

$$D(a) = \{x \in A; x/a\}.$$

Proposição 4.25 *De acordo com a definição acima, temos que $D(a) = D(b)$, com $a, b \in A^*$, se, e somente se, $a \sim b$.*

Demonstração: Suponhamos inicialmente que $D(a) = D(b)$, pelo Teorema 4.19(a) temos que a/a logo, $a \in D(a)$, assim por hipótese $a \in D(b)$, donde vem que

$$a/b.$$

Analogamente, temos que b/b, logo $b \in D(b)$, ou seja, $b \in D(a)$, donde segue que

$$b/a.$$

Portanto

$$a \sim b.$$

Reciprocamente, suponhamos que $a \sim b$, assim por definição a/b e b/a, ou seja,

$$a \in D(b); \tag{44}$$

$$b \in D(a). \tag{45}$$

Seja $x \in D(b)$ um elemento qualquer, temos x/b e por (45) vem que b/a, logo pelo Teorema 4.19(b)

$$x/a,$$

ou seja,

$$x \in D(a).$$

Portanto, $D(b) \subset D(a)$. De forma análoga, por (44) segue que $D(a) \subset D(b)$. Portanto

$$D(a) = D(b).$$

■

Definição 4.26 *Definimos o* ***conjunto*** *$a * U(A)$ por: $a * U(A) = \{a * u, \quad com \quad u \in U(A)\}$*

Observação 4.27 *Sejam $a \in A$ e $u \in U(A)$, temos que u/a e $(a * u)/a$, pois*

$$a = u * (u^{-1} * a) = (a * u) * u^{-1}.$$

Disto segue que

$$U(A) \cup aU(A) \subset D(a),$$

para todo $a \in A^*$.

Definição 4.28 *Os elementos do conjunto $U(A) \cup aU(A)$ passam a ser denominados* ***Divisores Impróprios*** *de a e qualquer outro divisor de a (caso exista) é chamado* ***Divisor Próprio*** *de a e denotaremos por $P(a)$ o conjunto de todos os elementos que são divisores próprios de a.*

Proposição 4.29 *Seja $b \in A$, onde A é um anel de integridade. Temos que b é um divisor próprio de a se, e somente se, b/a e b não é inversível e nem associado ao elemento a.*

Demonstração: Suponhamos que $b \in P(a)$, logo por definição b/a e b não é inversível. Suponhamos por absurdo que a/b. Como, por hipótese, b/a temos

$$a \sim b$$

assim pelo Teorema 4.21 existe $u \in U(A)$ tal que

$$b = a * u.$$

Como $a * u \in aU(A)$, então $b \in aU(A)$, logo b não seria divisor próprio de a, absurdo. Portanto a e b não são associados.
Por outro lado, suponhamos que b/a, $b \notin U(A)$, $a \nmid b$ e suponhamos, por absurdo, que

$$b \notin P(a).$$

Logo temos que b é divisor impróprio de a, ou seja, $b \in U(A) \cup aU(A)$, assim $b \in aU(A)$, disto segue que existe $u \in U(A)$ tal que

$$b = a * u.$$

Portanto, pelo Teorema 4.21

$$a \sim b.$$

O que é uma contradição. ■

Definição 4.30 *Seja A um anel de integridade, diz-se que um elemento $a \in A$ é* ***irredutível*** *se, e somente se, as seguintes condições são verificadas:*

(1) $a \notin U(A) \cup \{0\}$;

(2) $P(a) = \varnothing$, isto é, os únicos divisores de a são os divisores impróprios.

Definição 4.31 *Seja A um anel de integridade, diz-se que um elemento $a \in A$ é* ***redutível*** *se, e somente se, as seguintes condições são verificadas:*

(1) $a \notin U(A) \cup \{0\}$;

(2) $P(a) \neq \varnothing$, isto é, a admite pelo menos um divisor próprio.

Definição 4.32 *Diz-se que um anel comutativo K, com elemento unidade $1 \neq 0$, é um* ***corpo*** *se, e somente se, todo elemento não nulo de K é inversível para a multiplicação.*

Exemplo 4.33 *No caso de um corpo K temos $U(K) = K - \{0\}$, portanto, não existem em K elementos irredutíveis ou redutíveis. De fato, por definição, para que um elemento seja irredutível ou redutível, primeiramente ele deve ser não inversível, mas num corpo todos os elementos são inversíveis.*

Exemplo 4.34 *No anel $\mathbb{Z}$ dos números inteiros temos $U(\mathbb{Z}) = \{-1, 1\}$, logo, para todo inteiro não nulo a, temos:*

$$U(\mathbb{Z}) \cup aU(\mathbb{Z}) = \{-1, 1, -a, a\}.$$

Definição 4.35 *Diz-se que um número inteiro p é **primo** se, e somente se, p satisfaz as seguintes condições:*

(1) $p \neq 0$ e $p \neq \pm 1$;

(2) Os únicos divisores de p são -1,1,p e -p.

Definição 4.36 *Diz-se que um número inteiro a é **composto** se, e somente se, a satisfaz as seguintes condições:*

(1) $a \neq 0$ e $a \neq \pm 1$;

(2) a admite pelo menos um divisor próprio.

Segue imediatamente das definições de número primo e de composto a seguinte Proposição.

Proposição 4.37 *Um número inteiro p, com $p \neq 0$ e $p \neq \pm 1$, é irredutível se, e somente se, os únicos divisores de p são ± 1 e $\pm p$; portanto, p é irredutível se, e somente se, p é primo. Analogamente, um inteiro a é redutível se, e somente se, a é composto.*

Definição 4.38 *Diz-se que um anel de integridade A é um **Anel Fatorial** se, e somente se, são válidas as seguintes condições:*

(AF1) para todo elemento não nulo e não inversível a existem elementos irredutíveis $p_1, p_2, ..., p_s$ em A tais que

$$a = p_1 * p_2 * ... * p_s; \tag{46}$$

(AF2) quaisquer que sejam as famílias $(p_i)_{1 \leq i \leq s}$ e $(q_j)_{1 \leq j \leq t}$, de elementos irredutíveis de A, se

$$p_1 * p_2 * ... * p_s = q_1 * q_2 * ... * q_t,$$

então $s = t$ e existe uma permutação σ de $\{1, 2, ..., s\}$ tal que

$$p_i \sim q_{\sigma(i)}$$

para $i = 1, 2, ..., s$.

Observação 4.39 *Quando $s > 1$ esta decomposição não é única, podemos obter outras decomposições de a, por exemplo:*

(1) se $u_1, u_2, ..., u_s$ são elementos inversíveis de A tais que $u_1 * u_2 * ... * u_s = 1$ e se $p'_i = u_i * p_i$, então $a = p'_1 * p'_2 * ... * p'_s$, onde cada p'_i é irredutível;

(2) mudança da ordem dos fatores irredutíveis em (46).

No que segue consideraremos estas decomposições como idênticas e teremos assim a noção de unicidade da decomposição de a a menos da ordem dos fatores irredutíveis e a menos de elementos inversíveis.

Exemplo 4.40 *O anel $\mathbb{Z}$ dos números inteiros é um anel fatorial. Podemos citar outros exemplos de anéis fatoriais: anel de polinômios com coeficientes num corpo, anéis euclidianos e anéis de polinômios com coeficientes num anel fatorial. Veja em [1].*

Definição 4.41 *Seja A um anel de integridade. Diz-se que um elemento $p \in A$ é* ***primo*** *em A se, e somente se, são válidas as seguintes condições:*

(1) $p \notin U(A) \cup \{0\}$;

(2) quaisquer que sejam a e b em A, se $p/(a * b)$, então p/a ou p/b.

Lema 4.42 *Todo elemento primo é irredutível.*

Demonstração: Se p é primo, então por definição, $p \notin U(A) \cup \{0\}$, logo, está satisfeito o item (1) da Definição 4.30. Basta verificarmos que $P(p) = \varnothing$.
Seja a um divisor de p. Então

$$p = a * b,$$

para algum $b \in A$. Logo, $p/(a * b)$ e como p é primo tem-se

$$p/a \qquad \text{ou} \qquad p/b.$$

Se p/a, então $(a * b)/a$, donde segue pelo Corolário 4.20 que $b/1$. Portanto $b \in U(A)$. Disto temos que

$$b^{-1} * p = a,$$

ou seja, $a \in pU(A)$.
Se p/b, então novamente pelo Corolário 4.20 temos

$$a \in U(A).$$

Como a era um divisor qualquer e provamos que $a \in U(A) \cup pU(A)$, então os únicos divisores de p são os impróprios. Logo $P(p) = \varnothing$. ■

Teorema 4.43 *Um anel de integridade A é um anel fatorial se, e somente se, A satisfaz a condição (AF1) e a seguinte condição:*

(AF3) para todo $p \in A$, se p é irredutível, então p é primo.

Demonstração: Suponhamos que A seja um anel fatorial, logo, por definição, A satisfaz a condição (AF1). Seja p um elemento irredutível em A, logo $p \notin U(A) \cup \{0\}$ e $P(p) = \varnothing$, isto é, os únicos divisores de p são os impróprios. Assim, basta mostrar que para quaisquer $a, b \in A$ se $p/(a * b)$, então p/a ou p/b.
Sejam $a, b \in A - (U(A) \cup \{0\})$ tais que

$$p/(a * b), \tag{47}$$

de acordo com (AF1) existem elementos irredutíveis $p_1, p_2, ..., p_s, q_1, q_2, ..., q_t$ tais que $a = p_1 * p_2 * ... * p_s$ e $b = q_1 * q_2 * ... * q_t$. Como $p/(a * b)$ resulta que existe $c \in A$ tal que

$$p * c = a * b \tag{48}$$

ou

$$p * c = p_1 * p_2 * ... * p_s * q_1 * q_2 * ... * q_t. \tag{49}$$

Podemos dizer que $c \neq 0$, pois a, b e p são não nulos. Além disso podemos considerar que c é irredutível (pela Observação 4.39). Assim, em virtude da condição (AF2), p é associado a um dos fatores irredutíveis do segundo membro de (49), isto é, existe um índice i ou um índice j, com $1 \leq i \leq s$ e $1 \leq j \leq t$, tal que $p \sim p_i$ ou $p \sim q_j$, de onde vem que,

$$p/p_i \qquad \text{ou} \qquad p/q_j,$$

logo,

$$p/a \qquad \text{ou} \qquad p/b.$$

Portanto, p é primo, donde vem que A satisfaz a condição (AF3).

Reciprocamente, suponhamos que o anel de integridade A satisfaça as condições (AF1) e (AF3), precisamos mostrar que (AF2) também está satisfeita.
Sejam duas famílias $(p_i)_{1\leq i\leq s}$ e $(q_j)_{1\leq j\leq t}$ de elementos irredutíveis de A e suponhamos que

$$p_1 * p_2 * ... * p_s = q_1 * q_2 * ... * q_t, \tag{50}$$

precisamos mostrar que $s = t$ e que $p_i \sim q_i$ para $i = 1, 2, ..., s$. Faremos indução finita sobre o número natural s.
Para $s = 1$, temos

$$p_1 = q_1 * q_2 * ... * q_t,$$

como p_1 é irredutível resulta $t = 1$, ou seja, $p_1 = q_1$.

Vamos supor agora que a condição (50) seja válida para $(s-1)$, assim, quaisquer que sejam as famílias $(p_i)_{1\leq i\leq s-1}$ e $(q_j)_{1\leq j\leq t-1}$, de elementos irredutíveis de A, se

$$p_1 * p_2 * ... * p_{s-1} = q_1 * q_2 * ... * q_{t-1},$$

então $s - 1 = t - 1$ e existe uma permutação σ tal que

$$p_i \sim q_{\sigma(i)}$$

para $i = 1, 2, ..., s$. De (50) vem que

$$p_1/(q_1 * q_2 * ... * q_t),$$

como p_1 é primo resulta que existe um índice i, com $1 \leq i \leq t$, tal que p_1/q_i.
Suponhamos que $i = 1$, logo p_1/q_1 e daqui concluimos que

$$p_1' = u * p_1,$$

onde $u \in U(A)$. Pondo-se $p_2' = u * p_2$ e cancelando o fator q_1 em (50), temos

$$p_2' * p_3 * ... * p_s = q_2 * q_3 * ... * q_t,$$

onde os fatores $p_2', p_3, ..., p_s, q_2, q_3, ..., q_t$ são irredutíveis, logo, em virtude da hipótese de indução, temos $s - 1 = t - 1$ e, com uma notação conveniente,

$$p_2' \sim q_2, ..., p \sim q_s;$$

portanto, $s = t$ e $p_i \sim q_i$ para $i = 1, 2, ..., s$. ■

Faremos agora uma extensão da noção de máximo divisor comum para um anel de integridade.

Definição 4.44 *Sejam a e b dois elementos quaisquer de um anel de integridade A. Diz-se que um elemento d, de A, é um* ***máximo divisor comum*** *de a e b, denotado por mdc(a,b) se, e somente se, são válidas as seguintes condições:*

(D1) *d/a e d/b;*

(D2) *para todo $d' \in A$, se d'/a e se d'/b, então d'/d.*

O máximo divisor comum de dois elementos de A, caso exista, não é, em geral, determinado de modo único, como veremos a seguir:

Proposição 4.45 *Se d=mdc(a,b), então um elemento $d_1 \in A$ também é um mdc(a,b) se, e somente se, $d_1 \sim d$.*

Demonstração: Suponhamos, inicialmente, que d é um mdc de a e b.
Se $d_1 \in A$ é um mdc de a e b também, então d_1/a e d_1/b, logo por (D2)

$$d_1/d.$$

De modo análogo, temos que

$$d/d_1.$$

Portanto $d \sim d_1$.
Reciprocamente, suponhamos que d=mdc(a,b) e $d \sim d_1$, onde d_1 é um elemento qualquer de A. Assim

$$d/a \qquad \text{e} \qquad d/b$$

e

$$d/d_1 \qquad \text{e} \qquad d_1/d.$$

Por transitividade resulta que

$$d_1/a \qquad \text{e} \qquad d_1/b.$$

Além disso, se $d_2 \in A$ com d_2/a e d_2/b, então como $d = mdc(a,b)$, segue que d_2/d. Assim, novamente por (D_2), d/d_1, por transitividade implica que

$$d_2/d_1.$$

Portanto, pela definição acima, $d_1 = mdc(a,b)$. ■

Definição 4.46 *Uma relação de equivalência é uma relação entre elementos de um dado conjunto, que satisfaz as propriedades de reflexiva, simétrica e transitiva.*

Observação 4.47 *Segue do Corolário anterior que, em geral, o mdc não é único. No entanto, como a relação $\sim$ é de equivalência, segue que se $mdc(a,b) = d$, então $mdc(a,b) = d_1$ para todo $d_1 \in A$, onde $d_1 \sim d$ (d_1 e d estão na mesma classe de equivalência).*

Observação 4.48 *Se $a = b = 0$ teremos $d/0$ para todo $d \in A$ e também $0/a$ se, e somente se, $a = 0$. Logo se mdc(a,b)=0, então $a = b = 0$.*

Observação 4.49 *Se um dos elementos a ou b é inversível, então existe um mdc(a,b) e temos $d \sim 1$, ou seja, $d \in U(A)$.*

De fato, se $a \in U(A)$ ou $b \in U(A)$, então existem $x, y \in U(A)$ tais que

$$a * x = 1 \qquad \text{ou} \qquad b * y = 1, \tag{51}$$

ou ainda,

$$a = 1 * x^{-1} \qquad \text{ou} \qquad b = 1 * y^{-1}, \tag{52}$$

assim, de (52) segue que

$$1/a \qquad \text{ou} \qquad 1/b. \tag{53}$$

Seja $d \in A$ tal que

$$d/a \qquad \text{e} \qquad d/b, \tag{54}$$

como de (51) temos

$$a/1 \qquad \text{ou} \qquad b/1, \tag{55}$$

por transitividade em (54) e (55) vem que

$$d/1. \tag{56}$$

Logo, pela Definição 4.44 e por (53), (54) e (56) d é um mdc(a,b).
Como $1/c$ para todo $c \in A$, então

$$1/d. \tag{57}$$

Donde vem por (56) e (57) que

$$d \sim 1.$$

■

Veremos a seguir que nem sempre existe um mdc de dois elementos quaisquer de um anel de integridade arbitrário. Destacaremos, então, os anéis de integridade que admitem mdc.

Definição 4.50 *Diz-se que um anel de integridade A é um* ***anel com máximo divisor comum*** *se, e somente se, dois elementos quaisquer de A admitem um mdc em A.*

Exemplo 4.51 *Em virtude da Proposição 2.13, o anel $\mathbb{Z}$ dos números inteiros é um anel com máximo divisor comum.*

Lema 4.52 *Todo anel fatorial A é um anel com mdc.*

Demonstração: Sejam a e b dois elementos quaisquer de A tais que

$$a \notin U(A) \cup \{0\} \qquad \text{e} \qquad b \notin U(A) \cup \{0\},$$

(pelas Observações 4.48 e 4.49, nos demais casos o mdc existe). Portanto pela Definição 4.38 item AF1, existem elementos irredutíveis $q_1, q_2, ..., q_s$ e $q'_1, q'_2, ..., q'_t$ (não necessariamente distintos) tais que

$$a = q_1 * q_2 * ... * q_s \qquad \text{e} \qquad b = q'_1 * q'_2 * ... * q'_t.$$

Consideremos, então, o conjunto

$$\{\overline{q}_1, \overline{q}_2, ..., \overline{q}_s, \overline{q'}_1, \overline{q'}_2, ..., \overline{q'}_t\},$$

onde $\overline{q}_i = q_i * U(A)$, com $i = 1, 2, ..., s$ e $\overline{q'}_j = q'_j * U(A)$, com $j = 1, 2, ..., t$. Indiquemos por r o número de elementos deste conjunto e ponhamos

$$\{\overline{q}_1, \overline{q}_2, ..., \overline{q}_s, \overline{q'}_1, \overline{q'}_2, ..., \overline{q'}_t\} = \{\overline{p}_1, \overline{p}_2, ..., \overline{p_r}\}$$

(note que $r \leq s + t$).
Cada elemento p_i é irredutível (pois q_i e q'_i são irredutíveis) e se $i \neq j$ para $1 \leq i, j \leq r$, então p_i não é associado a p_j.
Além disso, cada elemento q_i $(1 \leq i \leq s)$ ou q'_j $(1 \leq j \leq t)$ é associado a um, e somente um, fator irredutível p_k $(1 \leq k \leq r)$. Portanto, os elementos a e b podem ser representados sob a forma

$$a = u * p_1^{\alpha_1} * p_2^{\alpha_2} * ... * p_r^{\alpha_r} \qquad \text{e} \qquad b = v * p_1^{\beta_1} * p_2^{\beta_2} * ... * p_r^{\beta_r}, \tag{58}$$

onde cada elemento α_i ou β_i é um número natural e u e v são elementos inversíveis de A.
Observamos que sob estas notações, temos a/b se, e somente se, $\alpha_i \leq \beta_i$ para $i = 1, 2, ..., r$.
Seja $\delta_i = min\{\alpha_i, \beta_i\}$, $i = 1, 2, ..., r$ e consideremos o elemento

$$d = p_1^{\delta_1} * p_2^{\delta_2} * ... * p_r^{\delta_r}.$$

Afirmamos que d é um mdc de a e b. De fato, vamos mostrar que d satisfaz as condições (D1) e (D2) da Definição 4.44.
(D1) Como $\delta_i \leq \alpha_i$ e $\delta_i \leq \beta_i$ para $i = 1, 2, ..., r$, segue que

$$d/a \qquad \text{e} \qquad d/b.$$

(D2) Sejam $d' \in A$ um divisor comum de a e b. Temos duas possibilidades, $d' \in U(A)$ ou $d' \notin U(A)$.
Se $d' \in U(A)$, então

$$d = d * (d')^{-1} * d',$$

ou seja,

$$d'/d.$$

Se $d' \notin U(A)$ então existem elementos irredutíveis $q"_1, q"_2, ..., q"_n$ tais que

$$d' = q"_1 * q"_2 * ... * q"_n.$$

Como d'/a e d'/b resulta que cada fator $q"_i$ é associado a um, e somente um, fator irredutível p_k $(1 \leq k \leq r)$ (segue da Observação 4.39).
Logo, d' pode ser representado sob a forma

$$d' = w * p_1^{r_1} * p_2^{r_2} * ... * p_r^{r_r},$$

onde w é inversível e cada r_k é um número natural.
De d'/a e d'/b resulta

$$r_k \leq \alpha_k \qquad \text{e} \qquad r_k \leq \beta_k.$$

Logo $r_k \leq min\{\alpha_k, \beta_k\} = \delta_k$ para $k = 1, 2, ..., r$ e então

$$d'/d.$$

■

Definição 4.53 *Sejam a e b dois elementos de um anel de integridade A e suponhamos que exista $d \in A$, tal que $d = mdc(a, b)$. Dizemos que a e b são* ***primos entre si*** *se, e somente se, $d \sim 1$.*

Lema 4.54 *Sejam a e p dois elementos de um anel A com mdc. Se p é irredutível e se $p \nmid a$, então, a e p são primos entre si.*

Demonstração: Seja $d = mdc(a, p)$, sendo $a, p \in A$ com p irredutível e $p \nmid a$.
Segue da definição de mdc que d/p. Como p é irredutível, os únicos divisores de p são os impróprios, ou seja,

$$d \in U(A) \cup p * U(A).$$

Suponhamos que $d \in p * U(A)$, então

$$d = p * u,$$

para algum $u \in U(A)$. Por outro lado, d/a e assim existe $k \in A$ tal que

$$a = k * d = k * (u * p) = (k * u) * p$$

e teríamos p/a, o que contradiz a hipótese.
Portanto $d \notin p * U(A)$. Daí $d \in U(A)$ e, consequentemente $d \sim 1$ (pois $1 = d * d^{-1}$ e $d = 1 * d$).
Segue da Definição 4.53 que a e p são primos entre si. ■

Teorema 4.55 *Sejam a e b dois elementos quaisquer de um anel A com mdc e seja d um mdc de a e b. Nestas condições, para todo $c \in A$, $mdc(a * c, b * c) = d * c$.*

Demonstração: Por observação já feita anteriormente, podemos, evidentemente, supor que $a, b, c \neq 0$. Como A é um anel com mdc, então existe $e \in A$ tal que

$$e = mdc(a * c, b * c), \tag{59}$$

precisamos demonstrar que $e \sim (d * c)$.
Temos que d/a e d/b, logo pelo Corolário 4.20

$$(d * c)/(a * c) \qquad \text{e} \qquad (d * c)/(b * c).$$

Portanto, em virtude da condição (D2) da Definição 4.44 teremos

$$(d * c)/e. \tag{60}$$

Logo, existe $u \in A$ tal que

$$e = u * (d * c).$$

Por (59) temos que $e/(a * c)$ e $e/(b * c)$, logo

$$u * (d * c)/(a * c) \qquad \text{e} \qquad u * (d * c)/(b * c).$$

Usando as propriedades associativa, comutativa e a lei do cancelamento, obtemos

$$(u * d)/a \qquad \text{e} \qquad (u * d)/b.$$

Novamente, pela condição (D2) da Definição 4.44

$$(u * d)/d,$$

ou seja,

$$(u * d) * c/d * c,$$

ou ainda,

$$e/(d * c). \tag{61}$$

Finalmente, por (60) e (61) temos

$$e \sim (d * c).$$

■

Teorema 4.56 *Sejam $a, b, c \in A$, onde A é um anel com mdc. Se $a/(b * c)$ e se a é primo com b, então a/c.*

Demonstração: Seja $d = mdc(a, b)$, pela Definição 4.53 temos que $d \sim 1$, donde vem, pela Proposição 4.45, que

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

Em virtude do Teorema 4.55 segue que

$$mdc(a * c, b * c) = c. \tag{62}$$

Sabemos que, qualquer que seja $a, c \in A$, temos

$$a/(a * c). \tag{63}$$

E, por hipótese,

$$a/(b * c). \tag{64}$$

Portanto, conforme a condição (D2) da Definição 4.44, por (62), (63) e (64) vem que

$$a/c.$$

■

Teorema 4.57 *Um anel de integridade A é um anel fatorial se, e somente se, A satisfaz as condições:*

(1) para todo elemento não nulo e não inversível a existem elementos irredutíveis $p_1, p_2, ..., p_s$ em A tais que

$$a = p_1 p_2 ... p_s;$$

(2) dois elementos quaisquer de A admitem um mdc em A.

Demonstração: Suponhamos que o anel de integridade A seja uma anel fatorial, então a condição (1) está satisfeita pela Definição 4.38 e a condição (2) está satisfeita pelo Lema 4.52.
Reciprocamente suponhamos que o anel de integridade A satisfaça as condições (1) e (2). Mostraremos então que, para todo $p \in A$, se p é irredutível, então p é primo e disto resultará, em virtude do Teorema 4.43, que A é um anel fatorial.

Seja p um elemento irredutível em A, queremos mostrar que se $p/(a*b)$ então p/a ou p/b. Suponhamos que

$$p/(a*b) \qquad \text{e} \qquad p \nmid a$$

com $a, b \in A$, conforme o Lema 4.54, a e p são primos entre si, logo, o Teorema 4.56 nos garante que p/b. Portanto, pela Definição 4.41, p é primo. ■

A noção de mínimo múltiplo comum introduzida no conjunto dos números inteiros e explorada nos números reais comensuráveis será estendida para um anel de integridade qualquer do seguinte modo:

Definição 4.58 *Sejam a e b dois elementos quaisquer de um anel de integridade A. Diz-se que um elemento $m \in A$ é um* ***mínimo múltiplo comum*** *de a e b, mmc(a,b) se, e somente se, são válidas as seguintes condições:*

(M1) *a/m e b/m;*

(M2) *para todo $m' \in A$, se a/m' e se b/m', então m/m'.*

O mmc (caso exista) de dois elementos de um anel de integridade A não é, em geral, determinado de modo único, como veremos a seguir.

Proposição 4.59 *Seja A é um anel de integridade, se m é um mmc(a,b), então $m_1 \in A$ também é um mmc(a,b) se, e somente se, $m_1 \sim m$.*

Demonstração: Temos que $m = mmc(a, b)$, então

$$a/m \qquad \text{e} \qquad b/m$$

Suponhamos que existe $m_1 \in A$ tal que $m_1 = mmc(a, b)$, então

$$a/m_1 \qquad \text{e} \qquad b/m_1.$$

Logo, pela condição (M2) da Definição 4.58 vem que

$$m/m_1 \qquad \text{e} \qquad m_1/m,$$

ou seja,

$$m_1 \sim m.$$

Reciprocamente, suponhamos que $m = mmc(a, b)$. Disto vem que

$$a/m \qquad \text{e} \qquad b/m. \tag{65}$$

Seja $m_1 \in A$ tal que $m \sim m_1$, ou seja,

$$m/m_1 \qquad \text{e} \qquad m_1/m. \tag{66}$$

De (65) e (66) e da propriedade transitiva segue que

$$a/m_1 \qquad \text{e} \qquad b/m_1$$

Seja $m' \in A$ tal que

$$a/m' \qquad \text{e} \qquad b/m'.$$

Como $m = mmc(a, b)$ segue por (M2) que

$$m/m'.$$

Usando a propriedade transitiva e (66) obtemos

$$m_1/m \qquad \text{e} \qquad m/m',$$

donde vem m_1/m'. Portanto

$$m_1 = mmc(a, b).$$

■

Observação 4.60 *Se $a = 0$ ou $b = 0$, então $m = 0$ é o único mmc de a e b. Reciprocamente, se o mmc de a e b é nulo, então $a = 0$ ou $b = 0$, em virtude da condição (M1) da Definição 4.58.*

Veremos agora, que nem sempre existe um mmc de dois elementos de um anel de integridade arbitrário.

Exemplo 4.61 *Dado $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}; a, b \in \mathbb{Z}\}$ um anel de integridade.*
Temos que $9 \in \mathbb{Z}[\sqrt{-5}]$. Observe que:
$9 = 3 * 3$, *com* $3 \in \mathbb{Z}[\sqrt{-5}]$ *e*
$9 = (2 + \sqrt{-5}) * (2 - \sqrt{-5})$, *com* $(2 + \sqrt{-5}), (2 - \sqrt{-5}) \in \mathbb{Z}[\sqrt{-5}]$.
Como existe um elemento em $\mathbb{Z}[\sqrt{-5}]$ que não satisfaz a condição (2) da Definição 4.38 (e Observação 4.39), de acordo com o Teorema 4.67 que veremos adiante este anel não possui mmc. Pois caso o mmc existisse, de acordo com o Teorema já citado, então o anel deveria ser fatorial.

Destacaremos, então os anéis de integridade que admitem mmc.

Definição 4.62 *Diz-se que um anel de integridade A é um* ***anel com mínimo múltiplo comum*** *se, e somente se, dois elementos quaisquer de A admitem um mmc em A.*

Teorema 4.63 *Sejam $a, b \in A$, onde A é um anel com mmc e seja m um mmc de a e b (m=mmc(a,b)). Nestas condições, para todo $c \in A$, mc é um mmc de $a * c$ e $b * c$.*

Demonstração: Podemos supor, pela Observação 4.60 que a, b e c não sejam nulos. Como A é um anel com mmc, então existe $x \in A$ tal que

$$x = mmc(a * c, b * c). \tag{67}$$

Basta mostrar, pela Proposição 4.59, que $x \sim (m * c)$.
Como $m = mmc(a, b)$, então a/m e b/m e pelo Corolário 4.20 temos que

$$(a * c)/(m * c) \qquad \text{e} \qquad (b * c)/(m * c). \tag{68}$$

Portanto, em virtude da condição (M2) da Definição 4.58, de (67) e (68) segue que

$$x/(m * c).$$

Por outro lado, de (67) temos

$$(a * c)/x,$$

ou seja, existe $u \in A$ tal que

$$x = u * (a * c).$$

Usando a propriedade associativa temos que

$$x = y * c,$$

com $y = (u * a) \in A$. Disto resulta que

$$c/x$$

e por (67) temos

$$(a * c)/x \qquad \text{e} \qquad (b * c)/x.$$

De onde vem que

$$(a * c)/(y * c) \qquad \text{e} \qquad (b * c)/(y * c).$$

Pela Lei do Cancelamento, Corolário 4.13, resulta

$$a/y \qquad \text{e} \qquad b/y.$$

Em virtude da condição (M2) da Definição 4.58, temos

$$m/y.$$

Logo, novamente pelo Corolário 4.13,

$$(m * c)/(y * c),$$

ou seja,

$$(m * c)/x.$$

Portanto

$$x \sim (m * c).$$

■

Teorema 4.64 *Um anel de integridade A é um anel com mdc se, e somente se, A é um anel com mmc.*

Demonstração: Suponhamos que A seja um anel com mdc e sejam a e b dois elementos, não nulos, de A. Seja $d = mdc(a, b)$. Temos que
(D1) d/a e d/b;
(D2) Se $d' \in A$, d'/a e d'/b, então d'/d.
Assim, existem $x, y \in A$ tais que

$$a = d * x \qquad \text{e} \qquad b = d * y,$$

donde vem que

$$a * b = (d * x) * (d * y). \tag{69}$$

Usando as propriedades associativa e comutativa dos anéis, obtemos

$$a * b = d * m, \qquad \text{com} \qquad m = d * x * y.$$

Vamos verificar as condições (M1) e (M2) da Definição 4.58 para os elementos a, b e m:
(M1) Temos, por (69), que d/a e d/b, logo pelo Corolário 4.20

$$d * b/a * b \qquad \text{e} \qquad a * d/a * b,$$

ou seja,

$$d * b/d * m \qquad \text{e} \qquad a * d/d * m,$$

de onde vem, pelo Corolário 4.20 que

$$b/m \qquad \text{e} \qquad a/m.$$

(M2) Para todo $m' \in A$, se a/m' e se b/m' temos

$$a * b/m' * b \qquad \text{e} \qquad a * b/a * m'. \tag{70}$$

Como $d = mdc(a, b)$, pelo Teorema 4.55 temos

$$m' * d = mdc(m' * a, m' * b). \tag{71}$$

Por (70), (71) e da definição de mdc, segue que

$$a * b/m' * d,$$

ou seja,

$$d * m/m' * d,$$

e pela Lei do Cancelamento, Corolário 4.13,

$$m/m'.$$

Portanto,

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

Reciprocamente, suponhamos que A seja um anel com mmc e sejam a e b dois elementos, não nulos, de A. Seja $m = mmc(a, b)$, temos que
(M1) a/m e b/m;
(M2) Se $m' \in A$, a/m' e b/m', então m/m'.
Como $a/a * b$ e $b/a * b$ segue de (M2) que existe $d \in A$ tal que

$$m * d = a * b. \tag{72}$$

De (M1) e Corolário 4.20 vem que

$$(a * b)/(m * b) \qquad \text{e} \qquad (a * b)/(m * a). \tag{73}$$

Vamos verificar as condições (D1) e (D2) para os elementos a, b e d:
(D1) Substituindo (72) em (73) obtemos

$$(m * d)/(m * b) \qquad \text{e} \qquad (m * d)/(m * a).$$

Pela Lei do cancelamento, Corolário 4.13,

$$d/b \qquad \text{e} \qquad d/a.$$

(D2) Seja d' um elemento qualquer de A, tal que

$$d'/a \qquad \text{e} \qquad d'/b,$$

temos

$$(d' * b)/(a * b) \qquad \text{e} \qquad (d' * a)/(a * b)$$

e segue da Definição 4.58 (M2) que

$$mmc(a * d', b * d')/(a * b).$$

Segue, pelo Teorema 4.63, que

$$d' * mmc(a, b)/a * b,$$

ou ainda,

$$(d' * m)/(a * b).$$

De (72) vem que

$$(d' * m)/(m * d).$$

Novamente, pela Lei do Cancelamento,

$$d'/d.$$

Portanto,

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

■

Resultam, imediatamente, do Teorema acima os seguintes Corolários.

Corolário 4.65 *Sejam $a, b \in A$, onde A é um anel com mdc. Se $d, m \in A$ são o mdc e o mmc de a e b, respectivamente, então $d * m \sim a * b$.*

Demonstração: Sejam $a, b \in A$, onde A é um anel com mdc, $m = mmc(a, b)$ e $d = mdc(a, b)$. De (72) temos que

$$(d * m)/(a * b) \qquad \text{e} \qquad (a * b)/(d * m)$$

Logo,

$$d * m \sim a * b.$$

■

Corolário 4.66 *Sejam a e b dois elementos de um anel com mdc. Se a e b são primos entre si, então $(a * b)$ é um mmc de a e b.*

Demonstração: Como a e b são primos entre si, temos que

$$d = mdc(a, b) = 1.$$

Pelo Corolário 4.65

$$1 * m \sim a * b,$$

ou seja,

$$m \sim a * b.$$

Portanto, pela Proposição 4.59

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

■

Conforme os Teoremas 4.57 e 4.64 temos a seguinte caracterização de um anel fatorial.

Teorema 4.67 *Um anel de integridade A é um anel fatorial se, e somente se, satisfaz as seguintes condições:*
(1) para todo elemento não nulo e não inversível a existem elementos irredutíveis $p_1, p_2, ..., p_s$ em A tais que

$$a = p_1 p_2 ... p_s;$$

(2) dois elementos quaisquer de A admitem um mmc em A.

5 Considerações Finais

Os Parâmetros Curriculares Nacionais (PCN) do Ensino Fundamental tem, entre seus objetivos específicos, o objetivo de levar o aluno a utilizar as diferentes linguagens - verbal, musical, matemática, gráfica, plástica e corporal - como meio para produzir, expressar e comunicar suas idéias e também questionar a realidade formulando-se problemas e tratando de resolvê-los, utilizando para isso o pensamento lógico, a criatividade, a intuição, a capacidade de análise crítica, selecionando procedimentos e verificando sua adequação.[veja [5]]

É importante que o desenvolvimento dos conteúdos de múltiplos, divisores e primos não se resuma à apresentação de técnicas e dispositivos práticos que permitam encontrar, mecanicamente, o Mínimo Múltiplo Comum (mmc) e o Máximo Divisor Comum (mdc) sem compreender as situações problema que esses conceitos permitem resolver.

Acreditamos que é possível estender os conceitos de mmc e mdc para números inteiros e reais comensuráveis, visto que, no ensino básico são apresentados ao aluno do 6° ano apenas os cálculos envolvendo números naturais. Considerando as várias aplicações do conceito e a cobrança do mesmo nas provas da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas) e em concursos, vemos então a necessidade de ampliar a aprendizagem deste conteúdo.

Finalizamos apresentando as soluções dos exemplos 2 e 3 colocados na introdução deste trabalho. Visto que agora temos as ferramentas necessárias para a resolução dos problemas de mmcg e mdcg.

Exemplo 2: Duas colegas de classe tem um livro para ler como trabalho escolar. Ambas já começaram a ler o livro, porém a uma resta $\frac{2}{3}$ do livro para terminar e a outra $\frac{3}{5}$. Elas resolveram estudar juntas e dividiram as páginas restantes em partes iguais, de modo que elas lessem, a cada dia, o máximo possível. Em quantos dias cada uma terminará o trabalho?
Solução: Verificaremos, inicialmente, a fração do livro que deverá ser estudada todos os dias, será o máximo de divisões comum nas páginas faltantes. Assim, pelo Corolário 3.13

$$mdcg(\frac{2}{3}, \frac{3}{5}) = \frac{mdc(2,3)}{mmc(3,5)} = \frac{1}{15}.$$

Logo, cada uma estudará $\frac{1}{15}$ do restante de seu livro por dia. Agora, faremos uma divisão para verificar em quantos dias terminarão o trabalho.

$$\frac{2}{3} : \frac{1}{15} = \frac{30}{3} = 10;$$

$$\frac{3}{5} : \frac{1}{15} = \frac{45}{5} = 9.$$

Portanto, uma terminará a leitura em 10 dias e a outra em 9 dias.

Exemplo 3: Temos dois repelentes líquidos de spray automático A e B, eles estão programados para agirem 4 vezes a cada 5 minutos e 6 vezes a cada 7 minutos, respectivamente. Se num dado instante os dois espirram juntos, em quanto tempo isso voltará a ocorrer?
Solução: Calculemos a frequência de funcionamento de cada repelente:
Repelente A: $\frac{4}{5}$ e Repelente B: $\frac{6}{7}$.

Para sabermos qual o próximo instante em que eles acionarão o jato juntos, basta obtermos o menor múltiplo comum dos racionais $\frac{4}{5}$ e $\frac{6}{7}$. Assim, resulta do Corolário 3.13 que

$$mmcg(\frac{4}{5}, \frac{6}{7}) = \frac{mmc(4,6)}{mdc(5,7)} = \frac{24}{1} = 24.$$

Portanto, a próxima vez em que os repelentes espirrarão juntos será após 24 minutos.

Diante do exposto, percebemos a necessidade de generalização do conceito estudado e destacamos a importância do desenvolvimento deste trabalho.

Referências

[1] Monteiro, L.H. Jacy., *Elementos de Álgebra*. Coleção Elementos de Matemática, Ao Livro Tecnico, 1969, página 125.

[2] Barros, Carlos J.B., Santana, Alexandre J., *Estruturas Algébricas com enfase em elementos da teoria de Lie*. Maringá: EDUEM, 2011.

[3] Hefez, A. *Iniciação à Aritmética*. Sociedade Brasileira de Matemática. 2009

[4] Oliveira, Krerley I.M.; Corcho, Adán J.F., *Iniciação à Matemática*. Rio de Janeiro: SBM, 2010.

[5] http://portal.mec.gov.br/seb/arquivos/pdf/matematica.pdf 04/02/2015

[6] RIPOLL, Cydara C.; RIPOLL, Jaime B.; SANT'ANA, Alveri A.; *O Mínimo Múltiplo Comum e o Máximo Divisor Comum Generalizados*. Matemática Universitária, Sociedade Brasileira de Matemática, Porto Alegre - RS, n° 40, pp. 59-74, junho/2006.

[7] Lima, E.L.; *Análise Real volume 1: Funções de Uma Variável*. 9.ed. Rio de Janeiro: IMPA, 2007.