UNIVERSIDADE FEDERAL DO AMAPÁ

PRÓ-REITORIA DE ENSINO DE GRADUAÇÃO

CURSO DE LICENCIATURA EM MATEMÁTICA

Marcio Mauriti Cardoso Graça
Pablo Ricardo Moraes de Souza
Valdinelson Europa Silva

MÍNIMO MÚLTIPLO COMUM E O MÁXIMO DIVISOR COMUM GENERALIZADOS

Macapá - 2012

Marcio Mauriti Cardoso Graça
Pablo Ricardo Moraes de Souza
Valdinelson Europa Silva

Mínimo Múltiplo Comum e o Máximo Divisor Comum Generalizados

Trabalho de Conclusão de Curso apresentado ao corpo docente do Curso de Licenciatura em Matemática - UNIFAP, como requisito parcial para a obtenção da Graduação em Licenciatura em Matemática.

Área de Concentração: **Teoria dos Números**
Orientador: *Ms.* Márcio Aldo Lobato Bahia.

Macapá - 2012

Mínimo Múltiplo Comum e o Máximo Divisor Comum Generalizados

por

GRAÇA, Marcio Mauriti Cardoso
SOUZA, Pablo Ricardo Moraes de
SILVA, Valdinelson Europa

Este Trabalho de Conclusão de Curso, foi julgado e aprovado, pelo Corpo Docente do Curso de Licenciatura em Matemática - UNIFAP, como requisito parcial para a obtenção da Graduação de Licenciatura em Matemática.

Macapá, 12 de Abril de 2012

Prof. *Ms.* Marcio Aldo Lobato Bahia
Coordenador do Curso de Licenciatura em Matemática - UNIFAP

Banca Examinadora

Orientador: Prof. *Ms.* Márcio Aldo Lobato Bahia.
Universidade Federal do Amapá - UNIFAP

Co-orientador: Prof. *Esp.* João Socorro Pinheiro Ferreira.
Universidade Federal do Amapá - UNIFAP

Membro: Prof. *Dr.* Erasmo Senger.
Universidade Federal do Amapá - UNIFAP

Ora, a fé é o firme fundamento das coisas que se esperam e a prova das coisas que não se vêem. Porque por ela os antigos alcançaram bom testemunho. Pela fé entendemos que os mundos foram criados pela palavra de Deus; de modo que o visível não foi feito daquilo que se vê.

(HEBREUS 11:1-3, B. Sagrada.)

Agradecimentos

⋆ Agradeço à Deus, que me permitiu tudo isso, a quem dirijo minha maior gratidão, a quem deu propósito à minha vida. Vem dele tudo o que sou, o que tenho e o que espero, o maior dos mestres;

⋆ Ao Colegiado do Curso de Licenciatura em Matemática e também a Universidade Federal do Amapá;

⋆ Em particular o nosso Professor Orientador *Ms.* Márcio Bahia, pelas orientações, discussões, dedicação, paciência e apoio durante esta longa jornada;

⋆ Às nossas famílias, pelas orações, conselhos, empenho, estímulo, e força para realizar este trabalho e o grande amor dado a mim em todos os momentos de minha vida;

⋆ À cinco grandes amigos: Europa, Gabriel, Mauriti, Pablo e Sandro pelas horas que, juntas, dividimos, tristezas, incertezas e inseguranças... Mas somamos entusiasmo, forças, alegrias, desafios e conquistas;

⋆ À todos os professores, em especial ao Professor Esp. João Ferreira, que foram em parte os responsáveis pela nossa formação acadêmica, pessoal e profissional;

⋆ À todos que contribuíram de alguma forma para que esta etapa de minha vida se concretizasse.

"Devemos ter perseverança para aprender o que nos é ensinado,
e transmitir os ensinamentos com a mesma virtude".

BAHIA, Márcio Aldo Lobato, 2005

Resumo

Neste trabalho estudamos o Artigo intitulado "O Máximo Divisor Comum e Mínimo Múltiplo Comum Generalizados"publicado na edição de nº 40 - junho/2006 da Revista Matemática Universitária - SBM, dos autores Cydara C. Ripoll, Jaime C. Ripoll e Alveri A. Sant'Ana. O artigo trata de uma generalização do conceito de MDC e MMC voltado para os conjuntos números reais, uma vez que o universo de discursão para esses conceitos ensinados no ensino dos níveis fundamental, médio e superior, é no máximo o conjunto dos números inteiros.

Para tanto ficou evidenciado a importância da definição de números comensuráveis, pois é através desta que foi possível a construção desses conceitos para o universo de discursão como sendo o conjunto dos números reais. Foi também apresentado neste trabalho, duas importantes aplicações desses estudo, a primeira usada para o cálculo de período de funções e a segunda usada na construções de engrenagens mecânicas.

Palavras-chave: Números Inteiros, Propriedades, MMC, MDC e Números Comensuráveis.

Abstract

In this paper approached Mathematics University Magazine article issue No. 40 - june, 2006, themed "The Greatest Commom Divisor and Least Commom Multiple Generalized" Authors Cydara C. Ripoll, Jaime C. Ripoll and A. Alveri St. Anne. In the article we found a generalization of the concepts of GCD and LCM focused onthe set real numbers, ie, since the universe discursao for these concepts taught in the teaching of critical levels, medium and higher, and the maximum whole numbers.

For this it was evident the importance of the definition of numbers comensurables, and through this it was possible the construction of these concepts to the universe of discursao as the set of real numbers. It was also presented in this paper, two important applications of these studies, the first used for the calculation of the second period and functions used in the constructions of mechanical gears.

keyword: Integer numbers, Properties, LCM, GCD and Commensurable Numbers.

SUMÁRIO

Introdução

Entre os vários ramos da matemática, a Teoria dos Conjuntos ocupa um lugar de destaque e, juntamente com a lógica, fundamentam toda a matemática conhecida. Desse modo, os vários ramos da matemática podem ser considerados formalmente incluídos na Teoria dos Conjuntos.

Como consequência desta inclusão, questões fundamentais à cerca da natureza da matemática reduzem-se a perguntas a cerca da teoria dos conjuntos. Perguntas como: O que é um conjunto? O que é um número? Motivaram grande parte dos matemáticos e dos filósofos dos fundamentos da matemática durante o século XIX e parte do século XX. A caracterização dos números inteiros, racionais e dos números reais foi um problema central para as investigações de Weierstrass, Dedekind, Kronnecker, Frege, Peano, Russell, Whitehead, Brower e outros.

Capítulo 1

Preliminares

1.1 Noções Primitivas

Para que os conceitos primitivos sejam empregados adequadamente torna-se necessário estabelecer regras que regulamentem sua utilização e estabeleçam suas propriedades.

Teorema e Demonstrações

Axiomas e Proposições

Fonte: Wikipédia

Proposição é uma sentença declarativa, que pode ser verdadeira ou falsa. Geralmente, de simples prova e de importância Matemática menor.

Um axioma é uma sentença ou proposição que não é provada ou demonstrada e é considerada como óbvia ou como um consenso inicial necessário para a construção ou aceitação de uma teoria. Por essa razão, é aceito como verdade e serve como ponto inicial para dedução e inferências de outras verdades (dependentes de teoria).

Na matemática, um axioma é uma hipótese inicial de qual outros enunciados são logicamente derivados. Pode ser uma sentença, uma proposição, um enunciado ou uma regra que permite a construção de um sistema formal. Diferentemente de teoremas, axiomas não podem ser derivados por princípios de dedução e nem são demonstráveis por derivações formais, simplesmente porque eles são hipóteses iniciais. Isto é, não há mais nada a partir do que eles seguem logicamente (em caso contrário eles seriam chamados teoremas). Em muitos contextos, "axioma", "postulado" e "hipótese" são usados como sinônimos.

A palavra "axioma" vem do grego, que significa "considerado válido ou adequado" ou "considerado auto-evidente".

Um Teorema é uma proposição glorificada. Ou seja, é um resultado importante que se destaca. Usualmente deixa-se o termo "teorema" para as afirmações que podem ser provadas de grande "importância matemática". São dados outros nomes para os outros tipos dessas afirmações (proposições):

Lema: é um "pré-teorema". Um teorema que serve para ajudar na prova de outro teorema maior. A distinção entre teoremas e lemas é um tanto quanto arbitrária, uma vez que grandes resultados são usados para provar outros. Por exemplo, o Lema de Gauss e o Lema de Zorn são muito interessantes, e muitos autores os denominam de Lemas, mesmo que não os usem para provar alguma outra coisa.

Corolário: é uma consequência direta de outro teorema ou de uma definição, muitas vezes tendo suas demonstrações omitidas, por serem simples;

Escólio: é uma consequência direta da demonstração (ou parte da demonstração) de um teorema.

Provar teoremas é a principal atividade dos matemáticos.

Teoremas

A generalidade dos resultados matemáticos assumem a seguinte forma: admitindo a validade de uma ou mais premissas, decorre(m) obrigatoriamente uma ou mais conclusões, ou consequências. Um tal enunciado de resultados tem o nome de Teorema. A validade de um teorema tem de ser provada, ou demonstrada. A sucessão finita de argumentos lógicos mostrando que determinada afirmação é necessáriamente verdadeira quando se assumem certas premissas, damos o nome de prova ou demonstração.

1.2 Uma Fundamentação Axiomática

Os números inteiros formam um conjunto, que notaremos por $\mathbb{Z}$, no qual estão definidas duas operações, que chamaremos de adição e multiplicação e denotaremos por $+$ e $\cdot$. Em $\mathbb{Z}$ também está definida uma relação que permite comparar os seus elementos, a relação "menor ou igual" , que indicaremos por $\leq$.

Como não desejamos ser excessivamente formais, não definiremos aqui os conceitos de operação e relação; limitar-nos-emos a usálos no seu sentido intuitivo.

Os axiomas que passaremos a detalhar descreverão algumas das propriedades básicas das operações e da relação "menor ou igual" , que tomaremos como base para desenvolver a teoria. Qualquer outra propriedade, mesmo que intuitivamente óbvia, poderá ser demonstrada a partir dessas.

Observamos que em qualquer apresentação axiomática o começo tende a ser cansativo, precisamente por ser necessário demonstrar alguns fatos que são bem conhecidos. Tentamos poupar o leitor, na medida do possível, desse inevitável aborrecimento. Assim, nosso sistema de axiomas é superabundante, isto é, admitimos mais propriedades do que as estritamente necessárias, esperando tornar mais fluente a exposição.

O primeiro grupo de axiomas decreverá algumas propriedades da soma que certamente são familiares ao leitor.

A.1 Propriedade Associativa: Para toda terna $a,\ b,\ c$ de inteiros tem-se que

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

A.2 Propriedade do Neutro: Existe um único elemento, denominado neutro aditivo ou zero, que indicaremos por 0, tal que

$$a + 0 = a, \text{ para todo a} \in \mathbb{Z} \ .$$

A.3 Existência do Oposto: Para cada inteiro a existe um único elemento que chamaremos oposto de a e indicaremos por -a, tal que

$$a + (-a) = 0 \ .$$

A.4 Propriedade Comutativa: Para todo par $a,\ b$ de inteiros tem-se que

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

O próximo grupo de axiomas explicita algumas das propriedades da multiplicação.

M.5 Propriedade Associativa: Para toda terna $a,\ b,\ c$ de inteiros tem-se que

$$a(bc) = (ab)c\ .$$

M.6 Propriedade do Neutro: Existe um único elemento, diferente zero, denominado *neutro multiplicativo*, que indicaremos por 1, tal que

$$1 \cdot a = a, \text{ para todo } a \in \mathbb{Z}\ .$$

M.7 Propriedade Cancelativa: Para toda terna $a,\ b,\ c$ de inteiros, com $a \neq 0$, tem-se que,

$$\text{Se } ab = ac\ \text{, então, } b = c\ .$$

M.8 Propriedade Comutativa: Para todo par $a,\ b$ de inteiros tem-se que

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

Comparando o grupo de axiomas dados para a adição e a multiplicação, percebe-se uma grande semelhança entre ambos. A única diferença notável surge entre axiomas $A.3$ e $M.7$. Um análogo a A.3 para multiplicação afirmaria que para todo a $\in \mathbb{Z}$ existe um elemento, digamos, $a' \in \mathbb{Z}$, tal que $a \cdot a' = 1$. Sabemos, porém, que isso não acontece: quando $a = 2$, por exemplo, não existe nenhum inteiro a' tal que 2a'= 1.

Poderiamos nos perguntar ainda por que não colocar, entre os axiomas da adição, um análogo à propriedade cancelativa $M.7$. Não o fizemos apenas porque é muito fácil *demonstrar* esse resultado a partir dos axiomas.

Os resultados que agora se seguem foram retirados da ref. [12] como demonstrações seram omitidas por acharmos que da forma como foram feitas na referida referencia está numa linguagem de fácil entendimento para o leitor a nível de graduação.

Alguma demonstração serão feitas por se tratarem de argumentos e técnicas que serão repetidas em demonstrações de proposições.

Proposição 1.2.0.1 (Propriedade Cancelativa da Adição)**.** *Para toda terna a, b, c de inteiros tem-se que,*

$$\text{se } a + b = a + c, \text{ então } b = c\ .$$

Demonstração: Ver ref. [12] de outros capítulos.

Proposição 1.2.0.2. *Para todo inteiro a, tem-se que $a \cdot 0 = 0$.*

Demonstração: Ver na ref [12].

Proposição 1.2.0.3 (Regra dos Sinais)**.** *Sejam a e b inteiros. Então vale:*

(i) $-(-a) = a$

(ii) $(-a)(b) = -(ab) = a(-b)$

(iii) $(-a)(-b) = (ab)$.

Demonstração: Ver ref. [12].

Enunciaremos a seguir os axiomas referentes à relação "menor ou igual".

A.10 Propriedade Reflexiva: Para todo inteiro a tem-se que $a \leq a$.

A.11 Propriedade Anti-simétrica: Dados dois inteiros a e b, se $a \leq b$ e $b \leq a$, então $a = b$.

A.12 Propriedade Transitiva: Para toda terna a, b, c de inteiros tem-se que, se $a \leq b$ e $b \leq c$, então $a \leq c$.

Por causa dos axiomas $A.10$, $A.11$ e $A.12$ diz-se que a relação $\leq$ é *uma relação de ordem.*

Usaremos o símbolo $a < b$ para indicar que $a \leq b$, mas $a \neq b$; nesse caso, diremos que a é menor que b. No que segue, empregaremos os termos "positivo" e "negativo" no seu sentido usual, isto é, para indicar que um certo número é maior ou menor que zero, repectivamente. Quando conveniente, usaremos também os símbolos $b \geq a$ ou $b > a$ para indicar que $a \leq b$ ou $a < b$.

A.13 Tricotomia: Dados dois inteiros quaisquer a e b tem-se que ou $a < b$ ou $a = b$ ou $b < a$.

Devemos ainda introduzir alguns axiomas que vinculem a relação de ordem com as operações:

A.14 Para toda terna de a, b, c de inteiros, se $a \leq b$, então $a + c \leq b + c$.

A.15 Para toda terna a, b, c de inteiros, se $a \leq b$ e $0 \leq c$, então $ac \leq bc$.

Note que, no nosso sistema de axiomas, admite-se que $1 \neq 0$, porém, não sabemos ainda se $0 < 1$ ou $1 < 0$. Felizmente, já estamos em condições de elucidar essa dúvida tão pouco razoável.

Proposição 1.2.0.4. *Seja a um inteiro. Então:*

(i) Se $a \leq o$, então $-a \geq 0$.

(ii) Se $a \geq 0$, então $-a \leq 0$.

(iii) $a^2 \geq 0$ (isto é, terminologia usual, todo quadrado é não negativo).

(iv) $1 > 0$.

Demonstração: Ver ref. [3].

Definição 1.2.1. *Seja* A *um subconjunto de $\mathbb{Z}$. Diz-se que* A *é limitado inferiormente se existe algum inteiro* K *tal que, para todo $a \in$ A, tem-se que $K \leq a$.*

Um elemento $a_0 \in A$ diz-se que A é mínimo de A se, para todo $a \in A$, tem-se $a_0 \leq a$ (verifique que, se existe um elemento mínimo de A, ele é único).

De forma análoga define-se conjunto *limitado superiormente* e *elemento máximo* de um conjunto.

Usaremos os símbolos *min A* e *max A* para indicar o mínimo e o máximo de um conjunto A, quando existirem.

A.16 Princípio da Boa Ordem: Todo conjunto não-vazio de inteiros não-negativos contém um elemento mínimo.

Note que, como consequencia dos axiomas $A.14$ e $A.15$, podemos provar que $0 < 1$. Porém, ainda não conseguimos demonstrar o fato óbvio de que não existem inteiros entre 0 e 1. Esse é o conteúdo da próxima proposição.

Proposição 1.2.0.5. *Seja a um inteiro tal que $0 \leq a \leq 1$. Então, $a = 0$ ou $a = 1$.*

Demonstração: Ver ref. [12].

Proposição 1.2.0.6 (Propriedade Arquimediana)**.** *Sejam a e b inteiros positivos. Então, existe um inteiro positivo n tal que $na > b$.*

Demonstração: Ver ref. [12].

Note que, trivialmente, se um conjunto A tem um mínimo, então A é limitado inferiormente. A recíproca também é verdadeira, como demonstraremos a seguir.

Proposição 1.2.0.7. *Todo conjunto não-vázio de inteiros limitados inferiormente tem mínimo.*

Demonstração: Seja A um tal conjunto e seja $k \in \mathbb{Z}$ tal que, para todo a $\in A$, tem-se que $k \leq a$. Consideramos então o conjunto.

$$S = \{a - k | a \in A\}.$$

Obviamente, $S \neq \phi$, já que A é não-vázio. E, como $k \leq a$, para todo $a \in A$, os elementos de S são não-negativos. Do Princípio da Boa Ordem, existe $m = min\ S$, que será da forma $m = a_0 - k$, para algum $a_0 \in A$. Mostraremos que o elemento a_0 assim determinado é o mínimo de A.

Como a_0 é um elemento de A, só resta verificar que, para todo $a \in A$, tem-se que $a_0 \leq a$. Suponhamos que isso não aconteça; existiria, então, $a_1 \in A$ tal que $a_1 < a_0$. Somando $-k$ a ambos os membros, $a_1 - k < a_0 - k = m$. Teríamos exibido, assim, um elemento de S menor que $m = min\ S$, uma contradição.

■

Capítulo 2

Divisibilidade

2.1 Algoritmo da Divisão

Uma equação do tipo $bx = a$ pode não ter solução no conjunto dos números inteiros; isso dependerá dos coeficintes a e b da equação. Quando tal solução existe, diz-se a é divisível por b. Mais precisamente:

Definição 2.1.1. *Sejam a e b números inteiros. Diz-se que b* divide *a (ou que b é **divisor** de a ou, ainda, que a é um **múltiplo** de b) se existe um inteiro c tal que $bc = a$.*

Usaremos a notação $b|a$ para indicar que b divide a. A negação dessa afirmação será por $b \nmid a$.

Convém observar que, se $b \neq 0$, o inteiro c nas condições da definição é único. De fato, se existisse outro c' tal que $bc' = a$, teríamos que $bc = bc'$ e, cancelando, vem que $c = c'$. O inteiro assim definido chama-se *quociente* de a por b e é indicado por

$$c = a/b = \frac{a}{b}.$$

Por outro lado, note que $0|a$ se e somente se $a = 0$. Nesse caso, o quociente não é único pois $0 \cdot c = 0$, para todo inteiro c. Por causa disso, costuma-se excluir o caso em que o divisor é nulo, e nós vamos aderir a essa conveção: em tudo o que segue, mesmo que não seja explicitado dito, estaremos admitindo que todos os divisores considerados são diferentes de zero.

Proposição 2.1.0.8. *Se b/a e $a \neq 0$, então $|b| \leq |a|$.*

Demonstração: Se $a|b$, existe $c \in \mathbb{Z}$ tal que $bc = a$. Tomando módulos em ambos os membros, tem-se que $|b||c| = |a|$.

Como $|c|$ é um interio positivo, temos que $1 \leq |c|$ e, multiplicando ambos os membros dessa desigualdade por $|b|$, temos que $|b| \leq |b||c| = |a|$.

■

Corolário 2.1.1. *:*

(i) Os únicos divisores de 1 são 1 e -1.

(ii) Se a/b e b/a, então $a = \pm b$.

Demonstração:

(i) Se b é um divisor de 1, temos, pela proposição anterior, que $|b| \leq 1$. Sabemos que não existe inteiros entre 0 e 1; como $b \neq 0$, temos que $0 < |b|$. Logo, $|b| = 1$ e, portanto, $b = +1$ ou $b = -1$.

(ii) Se $a|b$ e $b|a$, existe inteiros c e d tais que $ac = b$ e $bd = a$. Substituindo na segunda igualdade na segunda igualdade o valor de b dado pela primeira, temos

$$acd = a$$

e, como $a \neq 0$, podemos cancelar, daí

$$cd = 1.$$

Logo, d é um divisor de 1; pela parte anterior, $d = \pm 1$. Consequentemente,

$$a = \pm b.$$

■

Na proposição seguinte, reunimos algumas das propriedades elementares da divisibilidade.

Proposição 2.1.0.9. *Quaisquer que seja os números inteiros a, b, c, d (lembrando que propriedade assumimos os divisores diferentes de zero), valem:*

(i) a/a.

(ii) Se a/b e b/c, então a/c.

(iii) Se a/b e c/d, então ac/bd.

(iv) Se a/b e a/c, então $a/(a+b)$.

(v) Se a/b e a/c, então para todo $m \in \mathbb{Z}$, tem-se que a/mb.

(vi) Se a/b e a/c, então, para todos $m, n \in \mathbb{Z}$, tem-se que $a/(mb+nc)$.

Demonstração: Deixamos a cargo do leitor a demonstração (ou em todo caso procurar na ref. [12]).

Note que a relação "$|$" tem algumas propriedades semelhantes àquelas da relação $\leq$. Com efeito, compare (i) e (ii) da proposição anterior com as dadas pelos axiomas $A.10$ e $A.12$. Por outro lado, existem também algumas diferenças; por exemplo, compare a prte (ii) do corolário 2.1.1 com axioma $A.11$. Ainda, conforme o axioma $A.13$, dois inteiros a e b são sempre comparáveis, na relação $\leq$, isto é, $a \leq b$ ou $b \leq a$. Isso não é necessariamente verdadeiro para relação "$|$"; de fato, por exemplo, que $3 \nmid 4$ e também que $4 \nmid 3$.

Lema 2.1.1. *Sejam a e b inteiros, tais que $a \geq 0$ e $b > 0$. Então, existem q e r, tais que $a = bq + r$ e $0 \leq r < b$.*

Demonstração: Ver ref. [7]

Teorema 2.1.1. *(Algoritmo da Divisão) Sejam a e b inteiros, com $b \neq 0$. Então, existem inteiros q e r, únicos, tais que $a = bq + r$ e $0 \leq r < |b|$.*

Demonstração:

Mostraremos inicialmente que poderemos determinar q e r quando $b > 0$ e a é qualquer.

O caso $a \geq 0$ está dado pelo lema anterior.

Se $a < 0$ podemos, ainda pelo lema anterior, determinar q' e r' tais que

$$|a| = bq' + r' \text{ e } 0 \leq r' < b.$$

Se $r' = 0$, temos $-|a| = a = b(-q') + 0$, e o par $q = q'$, $r = 0$ verifica as condições do teorema.

Se $r' > 0$, temos

$$a = -|a| = b(-q') - r' = b(-q') - b + b - r' = b(-q' - 1) + (b - r').$$

Obviamente, $0 < b - r' < b$*; logo, os inteiros* $q = q' - 1$ *e* $r = b - r'$ *verificam as condições do enunciado.*

Agora provaremos que resultado também vale quando $b < 0$*. Qualquer que seja* a*, pela parte anterior, podemos determinar* q' *e* r' *tais que*

$$a = |b|q' + r' \text{ e } 0 \leq r' < |b|.$$

Quando $b < 0$*, temos que* $|b| = -b$*, logo,*

$a = |b|q' + r' = (-b)q' + r' = b(-q') + r'$*, e os inteiros* $q = q'$ *e* $r = r'$ *estão nas condições do enunciado.*

Finalmente, provaremos que, se (q, r) *e* (q', r') *são dois pares de inteiros verificando as condições do enunciado, então* $q = q'$ *e* $r = r'$*.*

De fato, temos que: 2.1.2 $qb + r = a = q'b + r'$*.*

Podemos supor, por exemplo, que $r' \geq r$*. Da igualdade acima, temos* $(q - q')b = r' - r$*.*

Como $|b| > r'$*, também temos* $r' - r < |b|$*. Substituindo,* $(q - q')b < |b|$ *e , tomando módulos,*

$$0 \leq |q - q'||b| < |b|.$$

Como $|b| > 0$*, podemos cancelar e obtemos* $0 \leq |q - q'| < 1$*. Da proposição* 1.2.0.5*, vem que* $|q - q'| = 0$*, isto é,* $q = q'$*. Na igualdade* 2.1.7*, temos agora* $qb + r = qb + r'$*. Cancelando, segue* $r = r'$*.*

■

Definição 2.1.2. *Os números* q *e* r *determinados no teorema anterior chamam-se, respectivamente,* ***quociente*** *e* ***resto*** *da divisão de* a *por* b*.*

2.2 Ideais e Máximo Divisor Comum

Definição 2.2.1. *Um conjunto não-vazio J de números inteiros diz-se um ideal de $\mathbb{Z}$ se*

(i) $\alpha, \beta \in J \Rightarrow \alpha + \beta \in J$.

(ii) $\alpha \in J, a \in \mathbb{Z} \Rightarrow \alpha a \in J$.

É fácil dar exemplos triviais de ideais: o próprio conjunto $\mathbb{Z}$ de todos os números inteiros certamente é um ideal de $\mathbb{Z}$, e o conjunto $\{0\}$ também o é.

Um exemplo mais interessante é o conjunto dos números pares; de fato, a soma de números pares é par e o produto dos números par por qualquer número também é par. Porém, é fácil ver que o conjunto I dos números ímpares não é ideal; de fato, a soma de dois elementos de I não pertence a I.

O conjunto dos números pares nada mais é do que o conjunto dos múltiplos de 2. Podemos obter novos exemplos com uma construção análoga.

Dado um inteiro m, indicaremos por $m\mathbb{Z}$ o conjunto:

$$m\mathbb{Z} = \{mx | x \in \mathbb{Z}\},$$

isto é, o conjunto de todos os múltiplos de m.

Mostraremos que $m\mathbb{Z}$ é um ideal. Com efeito, dados $\alpha, \beta \in m\mathbb{Z}$, existem $x, y \in \mathbb{Z}$, tais que $\alpha = mx$ e $\beta = my$. Então, temos que $\alpha + \beta = m(x + y) \in m\mathbb{Z}$. Por outro lado, $a \in \mathbb{Z}$, temos que $\alpha a = m(xa) \in m\mathbb{Z}$.

Teorema 2.2.1. *Seja J um ideal de $\mathbb{Z}$. Então, $J = \{0\}$ ou existe um inteiro positivo m tal que $J = m\mathbb{Z}$.*

Demonstração:

Seja J um ideal de $\mathbb{Z}$.

Se $J \neq \{0\}$, existe pelos menos um inteiro $a \neq 0$ tal que $a \in J$. Da condição (ii) da definição de ideal vem que $-a \in J$. Como a e $(-a)$ pertencem a J, podemos afirmar que J contém inteiros positivos. Assim, o conjunto $J^+ = \{\alpha \in J / \alpha > 0\}$ é não-vazio. Pelo Princípio da Boa Ordem, existem $m = mim J^+$.

Provaremos que J é, precisamente, o conjunto dos múltiplos de m, isto é, $J = m\mathbb{Z}$.

De fato, como $m \in J$, a condição (ii) da definição de ideal mostra que, para todo $x \in \mathbb{Z}$, tem-se que $mx \in J$, logo, $m\mathbb{Z} \subset J$. Para provar a inclusão contrária, consideramos um elemento qualquer $\alpha \in J$ e por m podemos determinar q e r tais que $\alpha = mq + r$, em que $0 \leq r < m$. Se $r \neq 0$, como $r = \alpha - mq$ e tanto α quanto mq pertencem a J, teríamos que $r \in J^+$. Mas, $r < m = mimJ^+$, uma contradição. Assim, $r = 0$, logo $\alpha = mq$ é um múltiplo de m.

■

Definição 2.2.2. *Chama-se máximo divisor comum de a e b o maior de seus divisores comuns, isto é,*

$$mdc\,(a,b) = maxD\,(a,b).$$

Teorema 2.2.2. *de Bézout Sejam a, b inteiros e $d = mdc\,(a,b)$. Então, existem inteiros r e s tais que $d = ra + sb$.*

Demonstração: Ver ref. [12].

Teorema 2.2.3. *Sejam a, b inteiros. Um inteiro positivo d é o máximo divisor comum de a e b se somente se verifica*

(i) d/a e d/b.

(ii) Se d'/a e d'/b, então d'/d.

Demonstração:

Seja $d = mdc\,(a,b)$. Então, obviamente d verifica (i), e, na demonstração do Teorema de Bézout, provamos também que a condição (ii) se verifica.

Reciprocamente, se um inteiro positivo d verifica (i), então $d \in D\,(a,b)$. A condição (ii) afirma que, se $d' \in D\,(a,b)$, então d'/d; logo, $d' \leq d$, donde segue que d é o maior dos divisores comuns. Portanto, $d = mdc\,(a,b)$.

■

A caracterização do máximo divisor comum dada pelo teorema anterior apresenta algumas vantagens. Entre outras, é mais fácil de ser usada e simplificará algumas das demonstrações que seguem.

Proposição 2.2.0.10. *Sejam a, b inteiros, $d = mdc(a, b)$ e c um inteiro não nulo. Então:*

(i) $mdc(ac, bc) = d|c|$.

(ii) Se c/a e a/b, então $mdc(a/c, b/c) = d/|c|$.

Demonstração:

Para (i), monstraremos que $d|c|$ verifica as condições (i) e (ii) do teorema 2.2.3 em relação aos inteiros ab e bc.

De fato, como $d = mdc(a, b)$, temos em particular que d/a, logo, $(d|c|) / (ac)$. Da mesma forma, $(d|c|) / (bc)$. Ainda, do Teorema de Bézout, temos que existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$. Logo,

$$d|c| = r(a|c|) + s(b|c|).$$

Agora, se d' é um inteiro tal que d'/ac e d'/bc, da relação acima vem imediatamente que $d'/(d|c|)$.

Para provar (ii), poderíamos usar um raciocínio análogo, mas daremos uma demonstração mais breve, usando o resultado anterior. Seja $x = mdc(a/c, b/c)$. De (i) temos que

$mdc(a, b) = mdc\left(\frac{a}{c} \cdot c, \frac{b}{c} \cdot c\right) = mdc\left(\frac{a}{c}, \frac{b}{c}\right) \cdot |c|$, isto é, $d = x|c|$, donde $x = d/|c|$.

■

O próximo resultado, embora de demonstração simples, será de uso frequente na teoria.

Teorema 2.2.4 (Teorema de Euclides)**.** *Sejam a, b, c inteiros que a/bc. Se $mdc(a, b) = 1$, então a/c.*

Demonstração: Se $mdc(a, b) = 1$, da proposição anterior temos que $mdc(ac, bc) = |c|$. Agora, obviamente $a|ac$ e, da hipótese, $a|bc$. Consequetemente, usando (ii) do teorema (i) temos que $|a||c|$, logo $a|c$.

■

Definição 2.2.3. *Dois inteiros a e b dizem-se relativamente primos $mdc(a, b) = 1$.*

Podemos então enunciar o Teorema de Euclides da seguinte forma: se um número divide um produto de dois fatores e é relativamente primo com um deles, então divide o outro.

Proposição 2.2.0.11. *Sejam a e b inteiros relativamente primos, e seja c um outro inteiro tal que a/c e b/c. Então, ab/c.*

Demonstração: Ver ref. [12].

2.3 O Algoritimo de Euclides

O leitor certamente conhece, do curso secundário, o método para determinar o *mdc* de dois números usando a decomposição deles em fatores primos. Porém, quando se trata de números muito grandes, pode não ser fácil encontrar essa decomposição. O método que damos a seguir é baseado apenas em divisões sucessivas e aparece no livro sétimo dos *Elementos de Euclides*; porém, há evidências históricas de que o método seja anteior a essa obra.

Lema 2.3.1. *Sejam a, b inteiros, $b \neq 0$, e sejam q, r o quociente e o resto da divisão de a por b, respectivamente. Então, $D(a,b) = D(b,r)$; temos também que mdc (a,b) = mdc (b,r).*

Demonstração: Ver ref. [3].

Naturalmente, pode-se repetir esse processo. Fazendo divisões sucessivas, teremos:

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leq r_1 < |b|. \\ b &= r_1q_2 + r_2, & 0 \leq r_2 < r_1. \\ r_1 &= r_2q_3 + r, & 0 \leq r_3 < r_2. \\ \cdots\cdots\cdots & & \cdots\cdots\cdots \\ r_{n-2} &= r_{n-1}q + r_n, & 0 \leq r_n < r_{n-1}. \\ r_{n-1} &= r_nq_{n+1}. \end{aligned}$$

Como o resto diminui a cada passo, o processo não pode continuar indefinidamente, e alguma das divisões de ser exata. Suponhamos então que r_{n+1} seja o primeiro resto nulo, como está indicado antes. Do lema, temos que

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = \cdots\cdots = mdc(r_{n-1},r_n)$$

Finalmente, como $\dfrac{r_n}{r_{n-1}}$ é fácil ver que $mdc(r_{n-1},r_n) = r_n$, logo, $mdc(a,b) = r_n$. Demonstramos assim que, nesse processo, o resto máximo divisor comum de a e b é o último resto diferente de zero.

2.4 Mínimo Múltiplo Comum

Sejam a e b inteiros não-nulos. Um inteiro c diz-se *múltiplo comum de a e b se $a|c$ e $b|c$.* Indicaremos por $M(a,b)$ o conjunto de todos os múltiplos comuns de a e b e por $M^+(a,b)$ o conjunto de todos os múltiplos comuns positivos de a e b.

Certamente $M^+(a,b) \neq \Phi$, pois $|a||b| \in M^+(a,b)$; logo, pelo Princípio da Boa Ordem, esse conjunto contém um elemento mínimo.

Definição 2.4.1. *Chama-se* mínimo múltiplo comum *de a e b o menor dos seus múltiplos positivos comuns, isto é,*

$$mmc(a,b) = minM^+(a,b)$$

Lema 2.4.1. *Sejam a e b inteiros. Então, o $mmc(a,b)$ divide todo outro múltiplo comum de a e b.*

Demonstração: Usaremos novamente a noção de ideal.

Mostraremos inicialmente que $M(a,b)$ é um ideal. De fato, sejam $\alpha, \beta \in M(a,b)$. Temos que a/α e a/β; logo, $a/(\alpha+\beta)$. Da mesma forma, $b/(\alpha+\beta)$. A outra contradição da definição 2.2.1 segue facilmente.

Do teorema 2.2.1, sabemos que $M(a,b)$ deve ser da forma $m\mathbb{Z}$, em que m é precisamente o elemento mínimo de $M^+(a,b)$, isto é, $m = mmc(a,b)$.

Assim, se $m' \in M(a,b) = m\mathbb{Z}$, então m/m', como queríamos demonstrar.

■

Podemos agora dar uma outra caracterização do *mmc* de dois inteiros.

Teorema 2.4.1. *Sejam a e $b \in \mathbb{Z}$ e m um inteiro positivo. Então, $m = mmc(a,b)$ se e somente se m verifica:*

(i) a/m, b/m.

(ii) Se a/m' e b/m', então m/m'.

Demonstração: Do lema 2.4.1 vem que o $mmc(a,b)$ verifica as condições (i) e (ii) do enunciado.

Reciprocamente, se m verifica as condições, de (i) temos que $m \in M^+(a,b)$, e (ii) mostra que $m = minM^+(a,b)$, já que $m \leq |m'|$. Logo, $m = mmc(a,b)$.

■

Teorema 2.4.2. *Sejam a e $b \in \mathbb{Z}$, $d = mdc(a,b)$ e $m = mmc(a,b)$. Então, $md = |ab|$.*

Demonstração: Ver ref. [12].

O teorema acima dá então um método de cálculo para o $mmc(a, b)$. Dados $a, b \in \mathbb{Z}$, podemos calcular o $mdc(a, b)$ pelo Algorítmo de Euclides e depois obter

$$mmc(a, b) = \frac{|ab|}{mdc(a, b)}$$

2.5 O Teorema Fundamental da Aritmética

Nesta seção mostraremos que todo inteiro diferente de 0, 1 e -1 pode-se expressar como produto de números primos, de forma única, a menos da ordem dos fatores. Esse resultado, conhecido como o Teorema Fundamental da Aritmétrica, já aparece do livro IX dos Elementos de Euclides e destaca a importância na Teoria dos Números: eles desempenham um papel análogo ao dos átamos na estrutura da matéria. Todos os outros números podem ser obtidos através de produtos dos números primos.

Começaremos lembrando sua definição.

Definição 2.5.1. *Um inteiro p diz-se primo se tem exatamenta dois divisores positivos, 1 e $|p|$.*

Note que a definição exclui propositadamente o 0, que tem infinitos divisores positivos, e os inteiros 1 e -1 que têm um divisor positivos.

Um número diferente de 0, 1 e -1 que não é primo diz-se composto. Note que, da definição, vem imediatamente que, se se um inteiro não-nulo a é composto, ele admite um divisor b tal que $|b|$ seja diferente de 1 e de $|a|$, isto é, um divisor b tal que $1 < |b| < |a|$. Um divisor nessas condições diz-se um *divisor próprio* de a.

Começaremos provando uma propriedade muito importante dos números primos.

Proposição 2.5.0.12. *Seja p um número primo, e sejam a e b inteiros.*

(i) Se $p \dagger a$, então $mdc(p, a) = 1$.

(ii) Se p/ab, então p/a ou p/b.

Demonstração:

(i) Se $p \dagger a$, o divisor comum positivo de a e p é 1, donde segue imediatamente a tese.

(ii) Suponhamos que p/ab. Se p/a, a tese está verificada. Em caso contrário, da parte anterior temos que $mdc(p, a) = 1$, e, do Teorema de Euclides 2.2.4, vem que p/b.

■

Corolário 2.5.1. *Se um número primo p divide um produto $a_1a_2...a_n$, então p/a_k, para algum $k, 1 \leq k \leq n$.*

Demonstração:

Segue imediatamente da proposição, usando indução.

■

Notamos ainda a parte (ii) da proposição 2.5.0.12 pode ser usada para caracterizar a noção de números primos.

Teorema 2.5.1. *Seja p um inteiro diferente de $0, 1$ e -1. Então, p é um primo se e somente se, toda vez que p divide um produto de dois números, p divide pelo menos um dos fatores.*

Demonstração: Ver ref. [12].

A seguir daremos o primeiro passo na direção do resultado mais importante desta seção.

Lema 2.5.1. *Todo inteiro $a > 1$ pode ser escrito como produto de números primos.*

Demonstração: Ver ref. [12].

Teorema 2.5.2. *Seja $a > 1$ um inteiro. Então, existem prios positivos $p_1 \leq p_2 \leq ... \leq p_t$ tais que $a = p_1p_2...p_t$, e essa decomposição é única.*

Demonstração: No lema anterior, provamos a existência da decomposição. Resta apenas provar sua unicidade.

Dado um inteiro a, ele pode admitir, em príncipio, mais de uma decomposição

em produto de primos. Chamaremos comprimento de uma decomposição ao número de fatores que nela comparecem.

Faremos demonstração por indução no comprimento de uma cecomposição de a.

Suponhamos que a admita uma decomposição do tipo $a = p_1$, onde p_1 é primo, e que vale

$$a = p_1 = q_1 q_2 ... q_s,$$

em que $q_1 \leq q_2 \leq ... \leq q_s$ são primos positivos. Como q_1 divide $q_1 q_2 ... q_s$, q_1 deve dividir p_1, que é primo. Então, devemos ter $p_1 = q_1$. Cancelando, vem $1 = q_2 ... q_s$. Se $a > 1$, teríamos que o primo q_2 seria inversível, uma contradição. Assim, $s = 1$ e, como já provamos que $p_1 = q_1$, o primeiro passo de indução está verificado.

Suponhamos agora o resultado verdadeiro para todo inteiro que admita uma decomposição de comprimento $k \geq 1$, e seja a um inteiro com uma decomposição de comprimento $k + 1$. Se a admite outra decomposição, temos

2.5.3 $a = p_1 ... p_{k+1} = q_1 ... q_s$, em que $q_1 \leq q_2 \leq ... \leq q_s$ são primos positivos.

Como na primeira parte, $q_1 | p_1 \ldots p_{k+1}$ e, pelo colorário 2.5.1, temos que $q_1 | p_i$, para algum i. Como p_i é primo, devemos ter novamente que $q_1 = p_i$. Em particular, $q_1 \geq p_1$.

De forma análoga, pode-se obter que $p_1 = p_j$, para algum j. Logo, $p_1 \geq q_1$. De ambas as desigualdes, vem que $p_1 = q_1$. Finalmente, camcelando em 2.6.7, temos que

$$p_2 ... p_{k+1} = q_2 ... q_s.$$

Agora, o primeiro membro da igualdade tem uma decomposição de comprimento k, logo, da hipótese de indução, admite uma única decomposição. Assim, temos $k = s - 1$, donde $k + 1 = s$ e $p_i = q_i$, para $i = 2, ..., k + 1$. Como já provamos que $p_1 = q_1$, ambas as expreções de a coincidem.

■

2.6 Números reais Comensuráveis

O conceito de comensurabilidade, historicamente, foi introduzida e utilizada como uma forma de comparar o tamanho de dois segmentos de reta.

Para os Pitagóricos, todas as grandezas (comprimento, área, volume...) podiam ser

associadas a um numero inteiro ou uma razão entre dois números inteiros. Admitiam que os números racionais fossem suficientes para comparar, por exemplo, segmentos quaisquer de reta. Dados dois segmentos, supunham que sempre existia um segmento que cabia um numero inteiro de vezes num deles e um números de inteiros de vezes no outro. Neste caso, os segmentos eram comensuráveis.

Definição 2.6.1. *Dizemos que um segmento de reta $\overline{AB}$ é dito comensurável com a unidade dada pelo segmento $\overline{CD}$ quando existi uma subunidade que cabe um numero inteiro de vezes em $\overline{AB}$ e em $\overline{CD}$. Dizemos que $\overline{AB} = m.v$, $\overline{CD} = n.v$, onde m e n são números inteiros positivos e que a razão entre estas medidas e o numero $\frac{n}{m}$.*

Definição 2.6.2. *Dizemos que dois segmentos de reta dizem-se comensuráveis se são múltiplos de um segmento comum. Em outros termos, sejam $\overline{AB}$ e $\overline{CD}$ dois segmentos. Se existir um segmento $\overline{EF}$ e se existirem inteiros positivos m e n tais que $\overline{AB} = mEF$ e $\overline{CD} = nEF$, então $\overline{AB}$ e $\overline{CD}$ são múltiplos do segmento comum $\overline{EF}$, e assim se dizem comensuráveis.*

Vamos analizar uma caracteristica que ocorre em seguimentos (grandezas) com medidas racionais.

Exemplo 2.6.1. *Dado dois seguimentos de reta $\overline{AB}$ e $\overline{CD}$ medindo três unidades $(3u)$ e cinco unidades $(5u)$ respectivamente, dai existe um terceiro seguimento medindo a unidade, tal que mensure de forma justaposta $\overline{AB}$ e $\overline{CD}$. Observe ainda que*

$$\frac{\overline{AB}}{\overline{CD}} = \frac{3u}{5u} = \frac{3}{5}$$

Exemplo 2.6.2. *Dado dois seguimentos de reta $\overline{AB}$ e $\overline{CD}$ medindo $\frac{3}{2}u$ e $4u$ respectivamente, dai existe um terceiro seguimento de medida $\frac{1}{2}u$, tal que cabe 3 vesez de forma justa posta no seguimento $\overline{AB}$ e 8 vezes de forma justaposta no seguimento $\overline{CD}$. Observe que*

$$\frac{\overline{AB}}{\overline{CD}} = \frac{\frac{3}{2}}{4} = \frac{3}{8}$$

Tomando os exemplos acima, observamos que quando uma terceira grandeza que mensure A e B de forma justaposta dizemos que essas grandesas A e B são comensuráveis.

Afirmção 2.6.1. *A razão entre duas grandesas comensuráveis é um numero racional.*

Prova 2.6.1. *Considere as grandezas A e B de medidas* r *e* s *reais. Agora considere uma terceira grandeza de medida* p *tal que $r = mp$ e $s = np$, com $m, n \in \mathbb{Z}$, ou seja, as grandezas A e B são comensuráveis. Logo*

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

Capítulo 3

Mínimo Múltiplo Comum e Máximo Divisor Comum Generalizados

Definição 3.0.3. *Quando não existe uma terceira grandeza que mensure de forma justaposta A e B, então dizemos que A e B são incomensuráveis.*

Exemplo 3.0.3. *Um fato interessante é mostrar que a diagonal de um quadrado de lado medindo* 1 *(unidade) não é comensurável com o lado desse quadrado, de fato,*

Suponha que fosse comensurável, ou seja, exeiste $\frac{m}{n} \in \mathbb{Q}$, *tal que* $mdc(m,n) = 1$, *com* $\left(d = \frac{m}{n}\right)$

$$\left(\frac{m}{n}\right)^2 = 1^2 + 1^2, \text{ logo } \left(\frac{m}{n}\right)^2 \text{ é par.}$$

se, e só se, m *é par. Logo* $m = 2p$ *assim,* $4p^2 = 2n^2$ *se, e só se,* $2p^2 = m^2$ *se, e só se,* n^2 *é par se, e só se,* n *é par. Daí a contradição pois, se* n *é par e* m *é par então* $mdcm, n \neq 1$. *Portanto, não existe* $\frac{m}{n} \in \mathbb{Q}$ *com* $mdc(m,n) = 1$, *tal que*

$$\frac{m}{n} = d$$

Observe que a definição acima dada para duas grandesas comensuraveis é equivalente a.

Definição 3.0.4. *Dois números reais* r *e* s *são* ***comensuráveis*** *se existirem inteiros não nulos* m, n *tais que*

$$mr = ns.$$

Exemplo 3.0.4. $r = 1;\ s = 2$

$$m \cdot 1 = n \cdot 2$$

basta tomar $m = 2$ *e* $n = 1$*, segue que* r *e* s *são comensuráveis.*

Exemplo 3.0.5. $\sqrt{2}$ *e* $\sqrt{3}$ *não são comensuráveis.*

De fato, suponha que $\sqrt{2}$ *e* $\sqrt{3}$ *sejam comensuráveis, ou seja, existem* m, $n \in \mathbb{Z}$ *tais que*

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

Assim, elevando ao quadrado a expressão acima, teremos

$$(*) \quad 2m^2 = 3n^2.$$

Note que pela igualdade $3n^2$ *é par. Daí* n^2 *é par, pois caso contrário como* 3 *é ímpar e* n^2 *sendo ímpar teríamos* $3n^2$ *ímpar, contradição, o que implica* n *par. Pelo teorema fundamental da aritmética temos* $n = 2^{\alpha}p_1^{\alpha_1}... \ p_r^{\alpha_r}$ *sendo* $2 < p_1 < p_2 < ... < p_r$ *primos,* $0 < \alpha_1; ... \ ; \alpha_r$ *naturais e* α *o número de vezes que o* 2 *aparece na decomposição de* n*. Conseqüentemente a decomposição de* $3n^2$ *será :*

$$3n^2 = 3(\cdot 2^{\alpha}p_1^{\alpha_1}... \ p_r^{\alpha_r})^2 = 3 \cdot 2^{2\alpha}p_1^{2\alpha_1}... \ p_r^{2\alpha_r}$$

logo, o inteiro 2α *representa o número de vezes que o* 2 *aparece na decomposição do inteiro par* $3n^2$*. Absurdo, pois no* 1^o *membro da igualdade* $(*)$ *o* 2 *aparece um número ímpar de vezes, já que existem primos* $2 \leq q_1 < q_2 < ... < q_r$ *tais que:*

$$2m^2 = 2(2^{\beta}q_1^{\beta_1}... \ q_r^{\beta_r})^2 = 2 \cdot 2^{2\beta}q_1^{2\beta_1}... \ q_r^{2\beta_r} = 2^{2\beta+1}q_1^{2\beta_1}... \ q_r^{2\beta_r}; 0 \leq \beta \in \mathbb{Z}$$

se m^2 *for par, e*

$$2m^2 = 2(q_1^{\beta_1}... \ q_r^{\beta_r})^2$$

se m^2 *for ímpar.*

Portanto concluímos que $\sqrt{2}$ *e* $\sqrt{3}$ *não são comensuráveis.Ou ainda, para mostrarmos que duas grandesas cujas medidas são* $\sqrt{2}$ *e* $\sqrt{3}$ *não são comensuráveis basta verificar que* $\frac{\sqrt{3}}{\sqrt{2}} = \frac{m}{n} \in \mathbb{Q}$*, com* $mdc(m, n) = 1$*. Segue-se que:* $\frac{3}{2} = \frac{m^2}{n^2}$ *se, só se* $3n^2 = 2m^2$*, implica que* $3n^2$ *é par, ou seja,* n^2 *deve ser par. Daí* n *é par. Então* n *é da forma* $n = 2k$*, daí tem-se que* $3 \cdot (2k)^2 = 3 \cdot (4k^2) = 12k^2 = 2m^2$ *se, só se* $m^2 = 2 \cdot (3k^2)$*, isto implica que* m^2 *é par, ou seja,* m *é par. Donde resulta que* $mdc(m, n)$ *não será* 1*. Portanto não existem* $m, n \in \mathbb{Z}$ *tais que* $\frac{\sqrt{3}}{\sqrt{2}} = \frac{m}{n}$*, com* $mdc(m, n) = 1$*.*

Afirmção 3.0.2. *Dadas duas grandesas quaisquer A e B, cujas medidas $r \in \mathbb{R}$ e $s \in \mathbb{R}^*$. Então se $\frac{r}{s} \in \mathbb{Q}$, A e B são comensuráveis.*

Prova 3.0.2

Considere A e B duas grandesas tais que suas medidas são:$A = r$ e $B = s$, com $\frac{r}{s} \in \mathbb{Q}$. Daí, existem m, n e p tais que

$$r = mp \quad e \quad s = np.$$

Logo,

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

Mais isto significa que A e B são comensuráveis.

Comentário 3.0.1. *Para sabermos se duas grandesas são comensuráveis ou não, basta verificar se a razão entre elas é um número racional.*

Afirmção 3.0.3. *Considere as grandesas A e B comensuráveis tais que as medidas de A e B respectivamente r e s são racionais. Digamos $r = \frac{a}{b}$ e $s = \frac{c}{d}$. Então o segmento de medida $\frac{1}{bd} = \frac{1}{mmc(b,d)}$ mensura r e s de forma justaposta.*

Prova 3.0.3

Basta observar que $ad \in \mathbb{Z}$ e $ad \cdot \frac{1}{bd} = \frac{a}{b}$. Da mesma maneira tem-se que $cb \in \mathbb{Z}$ e $cb \cdot \frac{1}{bd} = \frac{c}{d}$. Em outras palavras estamos exibindo uma técnica usando o recurso do menor múltiplo comum para encontrar a medida do terciro segmento que mensure as grandesas A e B comensuráveis de medidas racionais.

Definição 3.0.5. *Considere r e $s \in \mathbb{R}$. Dizemos que r é múltiplo inteiro de s, ou que s é divisor inteiro de r, se $\exists\ a \in \mathbb{Z}$ tal que*

$$r = as.$$

Comentário:
$\frac{\sqrt{3}}{2}$ é múltiplo inteiro de $\frac{\sqrt{3}}{6}$ ou $\frac{\sqrt{3}}{6}$ é divisor inteiro de $\frac{\sqrt{3}}{2}$, pois $\exists\ 3 \in \mathbb{Z}$ tal que $\frac{\sqrt{3}}{2} = 3 \cdot \frac{\sqrt{3}}{6}$.

Proposição 3.0.0.13. *Considere r e s dois números reais não nulos. $\boldsymbol{s}$ é divisor inteiro de u se, e somente se, $-s$ é divisor inteiro de u.*

Prova 3.0.0.13

"⇒": Por hipótese **s** é divisor inteiro de u, ou seja, existe um inteiro n tal que $u = ns$. Daí $u = (-n)(-s)$ e portanto $-s$ é divisor inteiro de u.

"⇐": Por hipótese **-s** é divisor inteiro de u, ou seja, existe um inteiro m tal que $u = m(-s)$. Daí $u = (-m)(-(-s)) = (-m)s$ e portanto s é divisor inteiro de u.

Proposição 3.0.0.14. *Considere* $\boldsymbol{r}$ *e* $\boldsymbol{s}$ *dois números reais não nulos. As seguintes afirmações são equivalentes:*

a) r e s são comensuráveis;

b) o quociente $\frac{r}{s}$ é um número racional;

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

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

Prova 3.0.0.14

$(a) \Rightarrow (b)$: Por hipotese r e s são comensuráveis, isto é, existem inteiros não nulos m e n tais que $mr = ns$. Logo, $\frac{r}{s} = \frac{n}{m} \in \mathbb{Q}$.

$(b) \Rightarrow (c)$: Por hipotese existem inteiros não nulos m e n tais que $\frac{r}{s} = \frac{n}{m}$. Devemos mostrar que $\exists t \in \mathbb{R}$ tal que, t é multiplo inteiro comum de r e s. De fato; Basta tomar $t = mr = ns$, ou seja, t é multiplo inteiro comum de r e s.

$(c) \Rightarrow (d)$: Se t é múltiplo inteiro comum de r e s temos: $t = mr = ns$, com $m, n \in \mathbb{Z}^*$. Assim obtemos

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

tomando $u = \frac{r}{n} = \frac{s}{m}$, com $u \in \mathbb{R}$, segue que $un = r$ e $um = s$, conseqüentemente u é um divisor inteiro comum de r e de s.

$(d) \Rightarrow (a)$: Considere u divisor inteiro de r e s , ou seja, existem $m, n \in \mathbb{Z}^*$ tais que $r = un$ e $s = um$. Daí $\frac{r}{s} = \frac{un}{um} = \frac{n}{m} \in \mathbb{Q}$. Logo, $mr = ns$.

Definição 3.0.6. *Sejam* r *e* $s \in \mathbb{R}^*$ *comensuráveis. Dizemos que* t *é o mínimo múltiplo comum generalizado entre* r *e* s*, e escrevemos*

$$t = mmcg(r, s),$$

se:

a) $t > 0$,

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

c) Se t' é múltiplo inteiro comum de r e s e $t' > o$, então $t \leq t'$.
Dizemos que u é o máximo divisor comum generalizado entre r e s, e escrevemos $\beta = mdcg(r, s)$,

se:

a) β é o divisor inteiro comum de r e s

b) Se β' é divisor inteiro comum de r e de s então $\beta' \leq \beta$.

Teorema 3.0.1. *Sejam r e $s \in \mathbb{R}^*$ comensuráveis. Então*
$mmcg(r, s) = |vr| = |us|$ *e* $mdcg(r, s) = \left|\frac{r}{u}\right| = \left|\frac{s}{v}\right|$, *em que* $\frac{u}{v}$ *é a forma irredutível do racional* $\frac{r}{s}$.

Prova 3.0.1

Por hipótese r e s são comensuráveis, isto é, existe u e v inteiros tais que $vr = us$ e $\frac{u}{v}$ irredutível.

Afirmção 3.0.4. *$mmcg(r, s) = |vr| = |us|$, de fato. Note que:*

i) $|vr| = |us| > 0$.

ii) De $vr = us$ segue que vr é múltiplo inteiro de s e us é múltiplo inteiro de r. Logo $|vr| = |us|$ é múltiplo inteiro comum de r e s.

iii) Considere $t' > 0 \in \mathbb{R}$ um múltiplo inteiro comum de r e s, isto é, existem inteiros m, n tais que

$$t' = mr = ns \quad (*).$$

Devemos mostrar que $|vr| \leq t'$, de fato. Note que:

$$\left|\frac{r}{s}\right| = \left|\frac{u}{v}\right| \text{ e de } (*) \text{ temos: } \left|\frac{r}{s}\right| = \left|\frac{n}{m}\right|$$

daí,

$\left|\frac{u}{v}\right| = \left|\frac{n}{m}\right|$ são equivalentes e como $\frac{u}{v}$ é irredutível, segue que $u \leq n$ e $v \leq m$. Daí temos: $u \leq n$ implica $|su| \leq |sn|$ e $|vr| \leq |mr| = |t'| = t'$. Portanto $mmcg(r, s) = |vr| = |us|$.

Afirmção 3.0.5. *$mdcg(r, s) = \left|\frac{r}{u}\right| = \left|\frac{s}{v}\right|$, de fato.*

i) De $vr = us$ segue que $\frac{r}{u}$ é divisor inteiro de s e $\frac{s}{v}$ é divisor inteiro de r. Logo $\left|\frac{r}{u}\right| = \left|\frac{s}{v}\right|$ é divisor inteiro comum de r e s.

ii) considere $\beta' \in \mathbb{R}$ um divisor inteiro comum de r e s, isto é, existem inteiros m, n tais que

$$\beta' = \frac{r}{n} = \frac{s}{m}$$

Devemos mostrar que $\beta' \leq \left|\frac{r}{u}\right|$, de fato.

Note que:

$$\left|\frac{u}{v}\right| = \left|\frac{n}{m}\right|$$

são equivalentes e como $\frac{u}{v}$ é irredutível, segue que $u \leq n$ e $v \leq m$. Daí temos: $u \leq n$ implica $|u| \leq |n|$ consequentemente, $\beta' = \left|\frac{r}{n}\right| \leq \left|\frac{r}{u}\right|$

Portanto

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

Aplicação: $mmcg\left(\frac{3}{5}, \frac{7}{2}\right)$ e $mdcg\left(\frac{3}{5}, \frac{7}{2}\right)$. Note que: $\frac{3/5}{7/2} = \frac{6}{35} = \frac{u}{v}$

daí

$$mmcg\left(\frac{3}{5}, \frac{7}{2}\right): vr = 35 \cdot \frac{3}{5} = 21$$

$$mdcg\left(\frac{3}{5}, \frac{7}{2}\right): \frac{r}{u} = \frac{\frac{3}{5}}{6} = \frac{3}{5} \cdot \frac{1}{6} = \frac{1}{10}.$$

Proposição 3.0.0.15. *Sejam r e s racionais não nulos e a, b, c, d inteiros tais que $r = \frac{a}{b}$ e $s = \frac{c}{d}$, respectivamente, na forma de fração irredutível. Então $mmcg(r,s) = \frac{mmc(a,c)}{mdc(b,d)}$ e $mdcg(r,s) = \frac{mdc(a,c)}{mmc(b,d)}$.*

Prova 3.0.0.15:

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

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

$$s = \frac{c}{d} \longrightarrow mdc(c,d) = 1$$

Note que:

$$mdc(a'd', b'c') = mdc\left(\frac{ad}{mdc(a,c)\cdot mdc(b,d)}, \frac{bc}{mdc(a,c)\cdot mdc(b,d)}\right)$$

Afirmação:

$mdc(ad,bc) = mdc(a,c)\cdot mdc(b,d)$, de fato:

$i)$ $mdc(a,c)\cdot mdc(b,d) > 0$

$ii)$ Note que:

1. $\frac{mdc(a,c)}{a}$ e $\frac{mdc(b,d)}{d}$

   logo,

   $$\frac{mdc(a,c)\cdot mdc(b,d)}{a\cdot d}$$

2. $\frac{mdc(a,c)}{c}$ e $\frac{mdc(b,d)}{b}$

   logo,

   $$\frac{mdc(a,c)\cdot mdc(b,d)}{b\cdot c}$$

3. Considere $d' > 0$ um inteiro tal que $\frac{d'}{ad}$ e $\frac{d'}{bc}$. Daí, $k_1 d' = a\cdot d$ e $k_2 d' = b\cdot c$, devemos mostrar que $mdc(a,c)\cdot mdc(b,d) \geq d'$.

   Se p é primo tal que $\frac{p}{a\cdot b}$ então $\frac{p}{a}$ ou $\frac{p}{b}$.
   Resultados: $c, a, b \in \mathbb{Z}$.

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

$$\text{se } \frac{c}{a} \text{ e } \frac{c}{b} \text{ então } mdc\left(\frac{a}{c},\frac{b}{c}\right) = \frac{d}{|c|}$$

$$\Longrightarrow p \neq 1 \text{ tal que } \frac{p}{a'\cdot d'} \quad \text{e} \quad \frac{p}{b'\cdot c'} \text{ daí,}$$

$$\frac{p}{a'} \quad \text{ou} \quad \frac{p}{d'} \quad \text{e} \quad \frac{p}{b'} \quad \text{ou} \quad \frac{p}{c'}$$

1. $\frac{p}{a'}$ e $\frac{p}{b'}$, daí $\frac{p}{a}$ e $\frac{p}{b}$ pois $mdc(a,b) = 1$.
2. $\frac{p}{a'}$ e $\frac{p}{c'}$, pois $mdc(a',c') = mdc\left(\frac{a}{mdc(a,c)},\frac{c}{mdc(a,c)}\right) = \frac{mdc(a,c)}{mdc(a,c)} = 1$.
3. $\frac{p}{d'}$ e $\frac{p}{b'}$, pois $mdc(b',d') = mdc\left(\frac{b}{mdc(b,d)},\frac{d}{mdc(b,d)}\right) = \frac{mdc(b,d)}{mdc(b,d)} = 1$.
4. $\frac{p}{d'}$ e $\frac{p}{c'}$, daí $\frac{p}{d}$ e $\frac{p}{c}$ pois $mdc(c,d) = 1$.

$$\text{Não existe } \frac{p}{a'\cdot d'} \quad \text{e} \quad \frac{p}{b'\cdot c'}$$

$$\text{Portanto, } mdc(a'd',b'c') = 1$$

■

Aplicação: $mmcg\left(\frac{1}{2},\frac{3}{4}\right) = \frac{mmc(1,3)}{mdc(2,4)} = \frac{3}{2}$

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

Aplicação: $mmcg\left(\frac{10}{6},\frac{1}{7}\right)$ e $mdcg\left(\frac{10}{6},\frac{1}{7}\right)$.

Observação 3.0.1. *Note que:* $\frac{mmc(10,1)}{mdc(6,7)} = 10 \neq 5 = \frac{mmc(5,1)}{mdc(3,7)} = mmcg(r,s)$ *e* $\frac{mdc(10,1)}{mmc(6,7)} = \frac{1}{42} \neq \frac{1}{21} = \frac{mdc(5,1)}{mmc(3,7)} = mdcg(r,s)$ *pois, a fórmula dada quando aplicada a frações não irredutíveis não proporciona necessariamente o* $mmcg(r,s)$ *e o* $mdcg(r,s)$. *Como nos mostra o exemplo. Daí*

$$mmcg\left(\frac{10}{6},\frac{1}{7}\right)= mmcg\left(\frac{5}{3},\frac{1}{7}\right) = \frac{mmc(5,1)}{mdc(3,7)}= 5$$

e

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

Observação 3.0.2. *mmcg* $\left(\frac{2}{3}\pi,\frac{1}{4}\pi\right) = 2\pi$ *e mdcg* $\left(\frac{2}{3}\pi,\frac{1}{4}\pi\right) = \frac{2\pi/3}{8} = \frac{1}{12}\pi$,

pois

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

Observação 3.0.3. *Se a e b são inteiros não nulos, então valem:*

1. $mmcg(a,b) = mmc(a,b)$
2. $mdcg(a,b) = mdc(a,b)$

Prova 3.0.3:

1. note que $a = \frac{a}{1}$ e $b = \frac{b}{1}$ são as frações irredutíveis dos inteiros a e b, respectivamente. Daí utilisando o corolário acima segue que:

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

2. note que $a = \frac{a}{1}$ e $b = \frac{b}{1}$ são as frações irredutiveis dos inteiros a e b, respectivamente. Daí utilisando o corolário acima segue que:

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

Corolário 3.0.1. *Sejam r e* $s \neq 0$*, comensuráveis. Então:*

(i) $|rs| = mdcg(r,s)\cdot mmcg(r,s)$;

(ii) $\forall c \neq 0$, temos ainda cr e cs comensuráveis

$mmcg(cr,cs) = |c|\cdot mmcg(r,s)$ $mdcg(cr,cs) = |c|\cdot mdcg(r,s)$

Demonstração: Considere:

(i) $rs = mdcg(r,s)\cdot mmcg(r,s)$ note que existem inteiros $m, n \in \mathbb{N}^*$ com $mdc(m,n) = 1$ tais que $\frac{r}{s} = \frac{n}{m}$ daí usando o **teorema** 2.6, segue que: $mmcg(r,s) = mr = us$

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

(ii) Note que $\frac{cr}{cs} = \frac{n}{m}$ logo cr e cs são comensuráveis, daí temos:

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

■

Corolário 3.0.2. *Se r e s são dois números racionais que podem ser representados por uma fração decimal, digamos, $r = \frac{u}{10^k}$ e $s = \frac{u}{10^l}$. Considere t um inteiro tal que $t \geq k$ e $t \geq l$ daí, $mmcg(10^t r, 10^t s) = 10^t mmcg(r,s)$. Como $10^t r$ e $10^t s$ são inteiros, dai pela observação 2.2 $mmcg(10^t r, 10^t s) = mmc(10^t r, 10^t s)$, logo; $mmc(10^t r, 10^t s) = 10^t mmcg(r,s)$ $mmcg(r,s) = \frac{mmc(10^t r, 10^t s)}{10^t}$.*

3.1 Aplicações de Mínimo Múltiplo Comum e Máximo Divisor Comum

3.1.1 Aplicação na Matemática

I) Para o MMC:

Definição 3.1.1. *Uma função $f : \mathbb{R} \to \mathbb{R}$ é dita **periódica** quando existe um número real $p \neq 0$ tal que*

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

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

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

Teorema 3.1.1. *Sejam $f : \mathbb{R} \to \mathbb{R}$ e $g : \mathbb{R} \to \mathbb{R}$ funções periódicas de períodos p_f e p_g respectivamente. Se p_f e p_g são números* ***comensuráveis*** *então as funções $f+g$ e $f \cdot g$ são periódicas de período $mmcg(p_f, p_g)$.*

Prova 3.1.1. *Faremos aqui apenas a demonstração para o caso $f + g$. Sendo p_f e p_g por hipótese comensuráveis, está bem definido $M = mmcg(p_f, p_g)$. Existem então $m, n \in \mathbb{Z}\backslash\{0\}$ tais que*

$$mp_f = np_g = M.$$

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

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

o que prova que $f + g$ é periódica de período $mmcg(p_f, p_g)$.

Exemplo 3.1.1. *São funções periódicas de períodos fundamentais $p_f = \dfrac{2\pi}{3}$ e $p_g = \dfrac{2\pi}{7}$, respectivamente. Como p_f e p_g são comensuráveis, temos que a função h dada por*

$$h(x) = sen3x + cos7x$$

é periódica, admitindo 2π para período, pois

$$mmcg\left(\frac{2\pi}{3}, \frac{2\pi}{7}\right) = 3 \cdot \frac{2\pi}{3} = 2\pi,$$

já que

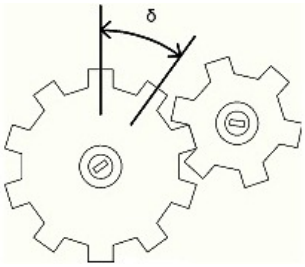
$$\frac{2\pi/3}{2\pi/7} = \frac{7}{3}.$$

3.1.2 Aplicação na Física

I) Para o MDC:

Geometricamente, se dois seguimentos AB e CD têm medidas comensuráveis r e s, respectivamente, então o mdcg(r, s) é a medida do maior segmento OU que, quando escolhido para nova unidade de medida para medir segmentos de reta, proporciona medidas inteiras para AB e CD.

Podemos aplicar esta idéia ao ajuste de engrenagens: Suponhamos que queiramos ajustar duas rodas num sistema de engrenagens, frezando dentes nas mesmas, todos de mesmo tamanho. Ora, cada roda deve ter um número inteiro de dentes e, obviamente, o desgaste sobre as rodas será mínimo quando os comprimentos das circunferências forem comensuráveis: de fato, denotando por δ o dobro do comprimento do dente, e denotando por r_1 e r_2 os raios das rodas, temos que existem m, n naturais tais que $2\pi r_1 = m\delta$ e $2\pi r_2 = n\delta$ se e só se



$$\frac{2\pi r_1}{2\pi r_2} = \frac{m\delta}{n\delta},$$

ou ainda, se e só se r_1 e r_2 forem comensuráveis:

$$nr_1 = mr_2.$$

Portanto, o maior valor de δ é precisamente

$$mdcg(2\pi r_1, 2\pi r_2) = 2\pi \cdot mdcg(r_1, r_2),$$

e se, na prática, este comprimento se revelar inviável (por ser, por exemplo, muito "curvo"um arco de comprimento δ), então, para minimizar o desgaste, teremos que tomar comprimentos iguais a $\dfrac{\delta}{k}$ com k natural.

Salientamos que, no coso de raios incomensuráveis, teremos inevitavelmente um desgaste sobre as rodas dentadas, mas este é tornado mínimo quando utilizamos a teoria das frações contínuas para calcular o valor de δ.

Considerações Finais

Vale observar que uma descoberta em matemática nem sempre diz respeito a um novo objeto, pode ser uma nova maneira de olhar para algo já conhecido por todos. Realmente, o mérito do artigo objeto da discussão deste trabalho, deve-se mais à generalização dos conceitos de MDC e MMC, uma vez que o universo de discussão aqui utilizado foi o conjunto dos números reais e não o conjunto dos números inteiros. Outro fato importante é o contato que tivemos com um artigo científico na área de matemática o qual enrriqueceu nossa formação acadêmica, sobretudo nos aspéctos de conteúdo e na elaboração de trabalhos científicos em nossa grande área de conhecimento.

BIBLIOGRAFIA

[1] ALENCAR FILHO, Edgard de. *Elementos de Ávila Abstrata/Edgard de Alencar Filho*. São Paulo: Nobel. 1978.

[2] ÁVILA, Geraldo. *Análise Matemática para Licenciatura*. 3ª ed., revisada e ampliada. Edgard Blucher, São Paulo, 2006.

[3] DOMINGUES, Hygino H. *Álgebra Moderna: volume único/Hygino H. Domingues, Gelson Iezzi*. 4ª ed. reform., São Paulo: Atual, 2003.

[4] EVARISTO,J.; PERDIGÃO,E. *Introdução à Algebra Abstrata*. 2ª ed., Maceió: Formato Digital, 2010.

[5] FERREIRA, Jamil. *A Construção dos Números*.1ª ed., Rio de Janeiro: SBM (Coleção Textos Univesitários), 2010.

[6] GARCIA, A.; Lequain, Y. *Elementos de Álgebra, Projeto Euclides*, 2002.

[7] HEFEZ, A. *Curso de Álgebra*. Vol. I, Série Matemática Universitária da Sociedade de Matemática, 1993.

[8] Jornal do Professor de Matemática.*Laboratório do Ensino da Matemática*. Maio, 2006. Disponível em http://www.ime.unicamp.br/lem (20/11/2010).

[9] LIMA, E.L. *Análise Real*. vol.1. 9ª ed., Coleção Matemática Universitária, IMPA, Rio de Janeiro, 2007.

[10] LIMA, E.L. e outros. *A Matemática do Ensino Médio*. vol.1. 9ª ed., Rio de Janeiro: SBM (Coleção do Professor de Matemática,2006.

[11] MAIER, R.R., *Álgebra I. (Álgebra Abstrata). Textos de Aula*. 1995.

[12] MILIES,C.P.; COELHO,S.P. *Números - Uma Introdução à Matemática*. 3ª ed., São Paulo: Edusp - Editora da Universidade de São Paulo, 2001.

[13] RIPOLL, Cydara C.; e Outros. *Artigo da Revista Matemática Universitária nº 40*. 2006.