Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Aplicação do Lema de Euclides para Cálculo do Máximo Divisor Comum no Ensino Fundamental

por

Adriane Martins Arruda

Brasília, 2016

Adriane Martins Arruda

Aplicação do Lema de Euclides para Cálculo do Máximo Divisor Comum no Ensino Fundamental

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos para a obtenção do grau de

Mestre

Orientador: Prof. Dr. Helder de Carvalho Matos

Brasília
2016

Ficha catalográfica elaborada automaticamente,
com os dados fornecidos pelo(a) autor(a)

Ma

Martins Arruda, Adriane
Aplicação do Lema de Euclides para Cálculo do Máximo Divisor Comum no Ensino Fundamental / Adriane Martins Arruda; orientador Helder de Carvalho Matos. -- Brasília, 2016.
53 p.

Dissertação (Mestrado - Mestrado Profissional em Matemática) -- Universidade de Brasília, 2016.

1. Lema de Euclides. 2. Algoritmo de Euclides. 3. Divisão nos inteiros. 4. Teorema Fundamental da Aritmética. 5. Equações Diofantinas. I. de Carvalho Matos, Helder, orient. II. Título.

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Aplicação do Lema de Euclides para Cálculo do Máximo Divisor Comum no Ensino Fundamental

por

Adriane Martins Arruda*

Dissertação apresentada ao Departamento de Matemática da Universidade de Brasília, como parte dos requisitos do "Programa" de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, para obtenção do grau de

MESTRE

Brasília, 13 de maio de 2016.

Comissão Examinadora:

Prof. Dr. Helder de Carvalho Matos – MAT/UnB (Orientador)

Prof. Dr. Raimundo de Araújo Bastos Júnior – MAT/UnB (Membro)

Prof. Dr. Eudes Antônio da Costa –UFT (Membro)

* O autor foi bolsista CAPES durante a elaboração desta dissertação

Dedicatória

Dedico este trabalho à minha filha Amanda.

Agradecimentos

Agradeço a Deus, pois sem sua permissão nada disso seria possível.

Ao meu esposo, Welington, por sua compreensão e incentivo, pelas vezes que me levou para a faculdade, por todas as vezes que estudou comigo e por ser um ótimo amigo, companheiro e esposo maravilhoso.

Aos meus pais, Lúcia e Colemar, por me ensinar o valor dos estudos, por me educar e mostrar o caminho para ser uma boa pessoa.

Aos professores da UnB que participaram do curso e contribuíram para uma melhor formação dos alunos.

À SBM que, através do PROFMAT, está promovendo uma melhor capacitação dos professores no ensino da matemática.

Ao meu orientador Dr. Helder de Carvalho Matos, pela colaboração no desenvolvimento desse trabalho e por todo conhecimento transmitido.

Ao professor Dr. Rui Seimetz, coordenador do PROFMAT na UnB, pela dedicação na condução do curso e pelos ensinamentos transmitidos.

Aos colegas de turma.

À direção da escola Centro de Ensino Fundamental 405 do Recanto das Emas por permitir que eu aplicasse o minicurso Máximo Divisor Comum.

Aos alunos da escola Centro de Ensino Fundamental 405 do Recanto das Emas que participaram do minicurso Máximo Divisor Comum.

À CAPES, pelo incentivo financeiro.

À SEDF, por conceder afastamento remunerado para estudos.

Resumo

O objetivo deste é mostrar a aplicação do Lema de Euclides para cálculo do Máximo Divisor Comum no Ensino Fundamental e avaliar a receptividade que os alunos tiveram ao método. Para tanto, estudamos e escrevemos sobre a divisão nos inteiros, divisibilidade e propriedades envolvidas, o Teorema da Divisão Eucliana, o máximo divisor comum, o Lema de Euclides, o Algoritmo de Euclides, o Teorema Fundamental da Aritmética e também sobre as Equações Diofantinas que são uma aplicação interessante do MDC. Aplicamos um minicurso sobre MDC em duas turmas de Ensino Fundamental e apresentamos alguns resultados obtidos.

Palavras-chave: Divisão nos Inteiros, Divisibilidade, Teorema da Divisão Euclidiana, Máximo Divisor Comum, Lema de Euclides, Algoritmo de Euclides, Teorema Fundamental da Aritmética, Equações Diofantinas.

Abstract

The objective of this is to show the application of Euclid's Lemma to calculate the Greatest Common Divisor in Elementary Education and evaluate the receptivity that the students had the method. We studied and wrote about the division in integers, divisibility and properties involved, the theorem euclidian division, the greatest common divisor, Euclid's Lemma, the euclidean algorithm, the Fundamental Theorem of Arithmetic and also on the Diophantine Equations they are an interesting application of the Greatest Common Divisor. We use a short course on Greatest Common Divisor in two elementary school classes and present some results obtained.

Keywords: Division in the Integers, Divisibility, Theorem Euclidean Division, Greatest Common Divisor, Euclid's Lemma, Euclidean Algorithm, Fundamental Theorem of Arithmetic, Diophantine Equations.

Lista de Figuras

Lista de abreviaturas e siglas

CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
MDC	Máximo Divisor Comum
PROFMAT	Mestrado Profissional em Matemática em Rede Nacional
PROUNI	Programa Universidade para Todos
SEDF	Secretaria de Educação do Distrito Federal
SBM	Sociedade Brasileira de Matemática
UnB	Universidade de Brasília
UFT	Universidade Federal do Tocantins

Sumário

Introdução

Após lecionar durante seis anos para turmas de Ensino Fundamental percebe-se a dificuldade dos alunos em calcular o Máximo Divisor Comum (MDC) entre dois números naturais. Analisando alguns livros didáticos, [2], [3] e [8], observa-se que os principais métodos adotados para efetuar o cálculo do MDC são a decomposição em fatores primos e a listagem de divisores. Destes, apenas [3], aborda como método alternativo o Algoritmo de Euclides.

No método em que se decompõem os números em fatores primos para calcular o MDC os alunos encontram dificuldade pois precisam efetuar a divisão corretamente, conhecer os números primos e critérios de divisibilidade e além disso, confundem este método com o utilizado para calcular mínimo múltiplo comum.

O método em que se listam os divisores para encontrar o Máximo Divisor Comum é mais facilmente compreendido pelos alunos porém não é prático para números grandes e se o aluno esquece algum divisor o resultado pode ficar errado.

No Algoritmo de Euclides, para calcular o MDC os alunos precisam apenas efetuar a divisão corretamente. No Lema de Euclides os alunos precisam saber o que é múltiplo e efetuar subtrações corretamente. Desta forma, observa-se que neste método os alunos têm menos chance de errar.

Portanto, a proposta deste trabalho é ensinar para os alunos em um minicurso como se calcula o MDC através destes métodos e analisar a aceitação dos alunos em calcular o MDC pelo Lema de Euclides.

O trabalho tem a seguinte estrutura:

No primeiro capítulo fala-se sobre a divisão nos inteiros, defini-se divisibilidade, lista-se e demonstra-se propriedades da divisão e, enuncia-se e demonstra-se o teorema da divisão euclidiana.

No segundo capítulo, defini-se máximo divisor comum. Enuncia-se e demonstra-se o Lema de Euclides, o Algoritmo de Euclides e o Teorema Fundamental da Aritmética, que são formas de calcular o Máximo Divisor Comum entre dois números naturais.

No terceiro capítulo, aborda-se sobre as Equações Diofantinas, que é uma

aplicação do MDC. Defini-se o que são e mostra-se como encontrar o conjunto de soluções dessas equações.

No último capítulo, comenta-se um minicurso sobre MDC realizado com duas turmas de Ensino Fundamental e averigua-se a viabilidade de ensinar o Lema de Euclides para calcular o MDC nesta etapa de ensino.

Capítulo 1

Divisão nos inteiros

Neste capítulo, foram utilizadas as seguintes referências: [1], [3], [4], [5], [6] e [7].

1.1 Definição de divisibilidade

Definição 1.1 (Divisibilidade) *Dados dois números inteiros a e b, diremos que a divide b, denotando por $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = ca$.*

Se a não dividir b escreve-se $a \nmid b$.

Exemplo 1.1 *Tem-se que:*

(i) $-8 \mid 8$, pois $-1 \in \mathbb{Z}$ tal que $8 = -1 \cdot (-8)$.

(ii) $3 \mid -15$, pois $-5 \in \mathbb{Z}$ tal que $-15 = -5 \cdot 3$.

(iii) $5 \mid 0$, pois $0 \in \mathbb{Z}$ tal que $0 = 0 \cdot 5$.

(iv) $0 \mid 0$, pois existe $c \in \mathbb{Z}$ tal que $0 = c \cdot 0$.

1.2 Propriedades da Divisão

Proposição 1.1 *Seja $a \in \mathbb{Z}$. Então:*

(i) $1 \mid a$;

(ii) $a \mid a$;

(iii) $a \mid 0$;

(iv) $0 \mid a$ *se, e somente se,* $a = 0$.

Demonstração:

(i) $1 \mid a$, pois existe $a \in \mathbb{Z}$ tal que $a = a \cdot 1$;

(ii) $a \mid a$, pois $1 \in \mathbb{Z}$ e $a = 1 \cdot a$;

(iii) $a \mid 0$, pois $0 \in \mathbb{Z}$ e $0 = 0 \cdot a$;

(iv) ($\Rightarrow$) Como $0 \mid a$ existe $c \in \mathbb{Z}$ tal que $a = c \cdot 0$, ou seja, $a = 0$.
($\Leftarrow$) $a = 0 = c \cdot 0$ para algum $c \in \mathbb{Z}$, ou seja, $0 \mid a$.

□

Proposição 1.2 *Sejam a e $b \in \mathbb{Z}$. Então, $a \mid b$ se, e somente se, $|a| \mid |b|$.*

Demonstração:

($\Rightarrow$)Se $a \mid b$, então existe $c \in \mathbb{Z}$ tal que $b = c \cdot a$, assim $|b| = |c \cdot a| = |c| \cdot |a|$. Como $c \in \mathbb{Z}$, temos que $|c| \in \mathbb{Z}$, logo $|a| \mid |b|$.

($\Leftarrow$)Se $|a| \mid |b|$, então existe $c \in \mathbb{Z}$ tal que $|b| = c \cdot |a|$. Como $|b| \geqslant 0$, temos que $c \cdot |a| \geqslant 0$, então $c \cdot |a| = |c \cdot a|$, ou seja, $|b| = |c \cdot a|$, consequentemente $b = \pm c \cdot a$. Como $\pm c \in \mathbb{Z}$, temos que $a \mid b$.

□

Proposição 1.3 *Seja a, b, c e $d \in \mathbb{Z}$. Então:*

(i) Se $a \mid b$ e $b \mid c$, então $a \mid c$;

(ii) Se $a \mid b$ e $c \mid d$, então $ac \mid bd$;

(iii) Caso $c \neq 0$, $a \mid b$ se, e somente se, $ac \mid bc$.

Demonstração:

(i) Se $a \mid b$ e $b \mid c$, então existem k_1, $k_2 \in \mathbb{Z}$ tal que $b = k_1 a$ e $c = k_2 b$, assim $c = k_2(k_1 a) = (k_1 k_2)a$. Como k_1, $k_2 \in \mathbb{Z}$, temos que $k_1 k_2 \in \mathbb{Z}$, então $a \mid c$.

(ii) Se $a \mid b$ e $c \mid d$, então existem k_1, $k_2 \in \mathbb{Z}$ tal que $b = k_1 a$ e $d = k_2 c$, assim $bd = k_1 a k_2 c = k_1 k_2 ac$. Como k_1, $k_2 \in \mathbb{Z}$, temos que $k_1 k_2 \in \mathbb{Z}$, logo $ac \mid bd$.

(iii) ($\Rightarrow$) Imediato.
($\Leftarrow$) Se $ac \mid bc$, então existe $k \in \mathbb{Z}$; $bc = kac$. Como $c \neq 0$, temos que $b = ka$, logo $a \mid b$.

□

Proposição 1.4 *Sejam a, b e $c \in \mathbb{Z}$. Se $a \mid b + c$, então $a \mid b$ se, e somente se, $a \mid c$.*

Demonstração: Se $a \mid b + c$, então existe $k_1 \in \mathbb{Z}$ tal que $b + c = k_1 a$.

($\Rightarrow$)Se $a \mid b$, então existe $k_2 \in \mathbb{Z}$ tal que $b = k_2 a$. Como $b + c = k_1 a$, temos que $k_2 a + c = k_1 a$, assim $c = k_1 a - k_2 a$, ou seja, $c = (k_1 - k_2)a$. Como k_1 e $k_2 \in \mathbb{Z}$, temos que $k_1 - k_2 \in \mathbb{Z}$, logo $a \mid c$.

($\Leftarrow$)Se $a \mid c$, então existe $k_3 \in \mathbb{Z}$ tal que $c = k_3 a$. Como $b + c = k_1 a$, temos que $b + k_3 a = k_1 a$, assim $b = k_1 a - k_3 a$, ou seja, $b = (k_1 - k_3)a$. Como k_1 e $k_3 \in \mathbb{Z}$, temos que $k_1 - k_3 \in \mathbb{Z}$, logo $a \mid b$.

□

Exemplo 1.2 *Encontre todos os números inteiros positivos n para os quais $n + 2 \mid n^4 + 2$.*

Solução:

Se $n+2 \mid n^4+2$, então $n+2 \mid n^4-16+18$. Como $n^4-16 = (n^2+4)(n^2-4) = (n^2+4)(n-2)(n+2)$, temos que $n+2 \mid n^4-16$. Pela proposição 1.4, como $n+2 \mid n^4-16$ e $n+2 \mid n^4-16+18$ tem-se que $n+2 \mid 18$. Logo, $n+2 \in \{1, 2, 3, 6, 9, 18\}$. Como n é inteiro positivo, os valores possíveis para n são $n = 1$, $n = 4$, $n = 7$ ou $n = 16$.

Proposição 1.5 *Sejam a, b e $c \in \mathbb{Z}$. Se $a \mid b$ e $a \mid c$, então para todo x, $y \in \mathbb{Z}$, $a \mid xb + yc$.*

Demonstração:

Se $a \mid b$ e $a \mid c$, então existem k_1 e $k_2 \in \mathbb{Z}$ tal que $b = k_1 a$ e $c = k_2 a$, assim $xb + yc = xk_1 a + yk_2 a$, ou seja, $xb + yc = (xk_1 + yk_2)a$. Como k_1, k_2, x e $y \in \mathbb{Z}$, tem-se que $xk_1 + yk_2 \in \mathbb{Z}$ então $a \mid xb + yc$.

□

Exemplo 1.3 *Mostre que para algum n, $m \mid 35n + 26$, $m \mid 7n + 3$ e $m > 1$, então $m = 11$.*

Solução:

Pela proposição 1.5, como $m \mid 35n + 26$ e $m \mid 7n + 3$, tem-se que

$$m \mid 35n + 26 - 5(7n + 3) \Rightarrow$$
$$\Rightarrow m \mid 35n + 26 - 35n - 15 \Rightarrow$$
$$\Rightarrow m \mid 11 \Rightarrow$$
$$\Rightarrow m = 1 \text{ ou } m = 11.$$

Como $m > 1$, tem-se que $m = 11$.

Proposição 1.6 *Sejam a e $b \in \mathbb{Z}$. Então:*

(i) Se $a \mid b$ e $b \neq 0$, então $|a| \leqslant |b|$;

(ii) $a \mid b$ e $b \mid a$ se, e somente se $|a| = |b|$.

Demonstração:

(i) Se $a \mid b$, então existe $c \in \mathbb{Z}$ tal que $b = ca$, ou seja, $|b| = |ca| = |c| \cdot |a|$. Como $b \neq 0$, temos que $c \neq 0$, logo $|c| \geqslant 1$. Assim, $1 \cdot |a| \leqslant |c| \cdot |a|$ e, portanto, $|a| \leqslant |b|$.

(ii) Temos três casos a considerar:

(a) Caso $a = 0$:
($\Rightarrow$)Como $a \mid b$, temos que $0 \mid b$. Pela proposição 1.1, temos que $b = 0$, então $|a| = |b|$.
($\Leftarrow$) Como $|a| = |b|$, temos que $|b| = 0$, ou seja, $b = 0$. Pela proposição 1.1, temos que $0 \mid b$ e $b \mid 0$, ou seja, $a \mid b$ e $b \mid a$.

(b) Caso $b = 0$: Análogo ao caso $a = 0$.

(c) Caso $a \neq 0$ e $b \neq 0$.
($\Rightarrow$) Pela proposição 1.6, se $a \mid b$ e $b \mid a$, então $|a| \leqslant |b|$ e $|b| \leqslant |a|$, ou seja, $|a| = |b|$.
($\Leftarrow$) Se $|a| = |b|$, então $a = \pm b$ e, portanto, $a \mid b$ e $b \mid a$.

□

Proposição 1.7 *Sejam a e $b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b \mid a^n - b^n$.*

Demonstração:

Faremos a demonstração por indução sobre n.

A proposição é válida para $n = 1$, pois pela proposição 1.1, $a - b \mid a - b$.

Suponhamos que para algum $n \in \mathbb{N}$, $a - b \mid a^n - b^n$. Logo existe $c \in \mathbb{Z}$ tal que $a^n - b^n = c(a - b)$. Então:

$$\begin{aligned} & a^{n+1} - b^{n+1} = \\ & = aa^n - bb^n = \\ & = aa^n - ba^n + ba^n - bb^n = \\ & = (a - b)a^n + b(a^n - b^n) = \\ & = (a - b)a^n + bc(a - b) = \\ & = (a^n + bc)(a - b). \end{aligned}$$

Portanto, $a - b \mid a^{n+1} - b^{n+1}$

□

Exemplo 1.4 *Tem-se que:*

(i) $10 \mid 11^n - 1$, *pois* $10 = 11 - 1 \mid 11^n - 1^n = 11^n - 1$;

(ii) $3 \mid 10^n - 7^n$, *pois* $3 = 10 - 7 \mid 10^n - 7^n$;

(iii) $8 \mid 3^{2n} - 1$, *pois* $8 = 9 - 1 \mid 9^n - 1^n = (3^2)^n - 1 = 3^{2n} - 1$.

Proposição 1.8 *Sejam a e $b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a + b \mid a^{2n+1} + b^{2n+1}$.*

Demonstração:

Faremos a demonstração por indução sobre n.

A proposição é válida para $n = 0$, pois pela proposição 1.1, $a + b \mid a + b$.

Suponhamos que para algum $n \in \mathbb{N} \cup \{0\}$, $a + b \mid a^{2n+1} + b^{2n+1}$. Logo existe $c \in \mathbb{Z}$ tal que $a^{2n+1} + b^{2n+1} = c(a - b)$. Então:

$$\begin{aligned}
&a^{2(n+1)+1} + b^{2(n+1)+1} = \\
&= a^{2n+3} + b^{2n+3} = \\
&= a^2a^{2n+1} + b^2b^{2n+1} = \\
&= a^2a^{2n+1} + a^2b^{2n+1} - a^2b^{2n+1} + b^2b^{2n+1} = \\
&= a^2(a^{2n+1} + b^{2n+1}) - b^{2n+1}(a^2 - b^2) = \\
&= a^2c(a + b) - b^{2n+1}(a - b)(a + b) = \\
&= [a^2c - b^{2n+1}(a - b)](a + b).
\end{aligned}$$

Portanto, $a + b \mid a^{2(n+1)+1} + b^{2(n+1)+1}$.

□

Exemplo 1.5 *Tem-se que:*

(i) $17 \mid 10^{2n+1} + 7^{2n+1}$, *pois* $17 = 10 + 7 \mid 10^{2n+1} + 7^{2n+1}$;

(ii) $19 \mid 3^{2n+1} + 4^{4n+2}$, *pois* $19 = 3 + 16 \mid 3^{2n+1} + 16^{2n+1} = 3^{2n+1} + (4^2)^{2n+1} = 3^{2n+1} + 4^{4n+2}$;

(iii) $14 \mid 3^{4n+2}+5^{2n+1}$, *pois* $14 = 9+5 \mid 9^{2n+1}+5^{2n+1} = (3^2)^{2n+1}+5^{2n+1} = 3^{4n+2}+5^{2n+1}$;

Proposição 1.9 *Sejam* a *e* $b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. *Temos que* $a + b \mid a^{2n} - b^{2n}$.

Demonstração:

Faremos a demonstração por indução sobre n.

A proposição é válida para $n = 1$, pois $a + b \mid a^2 - b^2$, pois $a^2 - b^2 = (a - b)(a + b)$.

Suponhamos que para algum $n \in \mathbb{N}$, $a + b \mid a^{2n} - b^{2n}$. Logo existe $c \in \mathbb{Z}$ tal que $a^{2n} - b^{2n} = c(a + b)$. Então:

$$\begin{aligned}
&a^{2(n+1)} - b^{2(n+1)} = \\
&= a^{2n+2} - b^{2n+2} = \\
&= a^2a^{2n} + b^2b^{2n} = \\
&= a^2a^{2n} - a^2b^{2n} + a^2b^{2n} + b^2b^{2n} = \\
&= a^2(a^{2n} - b^{2n}) + (a^2 - b^2)b^{2n} = \\
&= a^2c(a + b) + b^{2n}(a - b)(a + b) = \\
&= [a^2c + b^{2n}(a - b)](a + b).
\end{aligned}$$

Portanto, $a + b \mid a^{2(n+1)} - b^{2(n+1)}$.

□

Exemplo 1.6 *Tem-se que:*

(i) $16 \mid 13^{2n} - 3^{2n}$, *pois* $16 = 13 + 3 \mid 13^{2n} - 3^{2n}$;

(ii) $13 \mid 9^{2n} - 2^{4n}$, *pois* $13 = 9 + 4 \mid 9^{2n} - 4^{2n} = 9^{2n} - (2^2)^{2n} = 9^{2n} - 2^{4n}$;

(iii) $53 \mid 7^{4n} - 2^{4n}$, *pois* $53 = 49 + 4 \mid 49^{2n} - 4^{2n} = (7^2)^{2n} - (2^2)^{2n} = 7^{4n} - 2^{4n}$.

1.3 Divisão Euclidiana

Teorema 1.1 (Divisão Euclidiana) *Dados dois números inteiros a e b, $b \neq 0$, existe um único par de inteiros q e r tais que $a = bq + r$, com $0 \leqslant r < |b|$. Chamamos q e r de quociente e resto, respectivamente.*

Demonstração:

1. Prova da existência: Como a e $b \in \mathbb{Z}$, temos duas possibilidades:

   (a) $b \mid a$:

   Então existe $q \in \mathbb{Z}$ tal que $a = bq$, ou seja, $a = bq + 0$, com $r = 0$.

   (b) $b \nmid a$:

   Então a não é múltiplo de b e portanto está compreendido entre dois múltiplos consecutivos de b.

   Caso $b > 0$, temos que $bq < a < b(q+1)$, com $q \in \mathbb{Z}$. De $bq < a$, temos que $a = bq + r$ onde $r \in \mathbb{Z}$ e $r > 0$. De $a < b(q+1)$, temos que $bq + r < bq + b$ assim, $r < b$, donde $0 < r < b$ e, portanto $0 < r < |b|$.

   Caso $b < 0$, temos que $-b > 0$. Logo, existem q e $r \in \mathbb{Z}$ tal que $a = -bq + r$ onde $0 < r < |b|$. Assim, $a = b(-q) + r$ onde $0 < r < |b|$, com $-q$ e $r \in \mathbb{Z}$.

2. Prova da unicidade: Suponhamos que existam q_1, q_2, r_1 e $r_2 \in \mathbb{Z}$, onde $a = bq_1 + r_1 = bq_2 + r_2$, com $0 \leqslant r_1 < |b|$ e $0 \leqslant r_2 < |b|$. Temos que

$$\begin{aligned} & 0 < r_2 < r_2 + r_1 \Rightarrow \\ & \Rightarrow -r_1 < r_2 - r_1 < r_2 \Rightarrow \\ & \Rightarrow -|b| < -r_1 < r_2 - r_1 < r_2 < |b| \Rightarrow \\ & \Rightarrow -|b| < r_2 - r_1 < |b| \Rightarrow \\ & \Rightarrow |r_2 - r_1| < |b|. \end{aligned}$$

   Por outro lado,

$$\begin{aligned} & bq_1 + r_1 = bq_2 + r_2 \Rightarrow \\ & \Rightarrow b(q_1 - q_2) = r_2 - r_1 \Rightarrow \\ & \Rightarrow b \mid r_2 - r_1. \end{aligned}$$

Pela proposição 1.6, se $r_2 - r_1 \neq 0$ e $b \mid r_2 - r_1$ então $|b| < |r_2 - r_1|$. O que é um absurdo! Logo,

$$r_2 - r_1 = 0 \Rightarrow$$
$$\Rightarrow b(q_1 - q_2) = 0 \Rightarrow$$
$$\Rightarrow q_1 - q_2 = 0, \text{ pois } b \neq 0 \Rightarrow$$
$$\Rightarrow q_1 = q_2.$$

□

Exemplo 1.7 *O Teorema da Divisão Euclidiana garante que dado $n \in \mathbb{Z}$, o resto da divisão de n por 2 é 0 ou 1, pois $n = 2q + r$, com q e $r \in \mathbb{Z}$ e $0 \leqslant r < 2$. Desta forma, todo número $n \in \mathbb{Z}$ pode ser escrito em uma, e somente uma, das seguintes formas: $2q$ ou $2q + 1$, que nomeamos como par ou ímpar, respectivamente.*

Generalizando, todo número inteiro n pode ser escrito em uma, e somente uma, das sequintes formas:

- $3q$, $3q + 1$ ou $3q + 2$;
- $4q$, $4q + 1$, $4q + 2$ ou $4q + 3$;
- $5q$, $5q + 1$, $5q + 2$, $5q + 3$ ou $5q + 4$;
- $mq + r$, onde $m \in \mathbb{N}$, com $m \geqslant 2$ e q e $r \in \mathbb{Z}$ e $0 \leqslant r < m$.

Exemplo 1.8 *Prove que não existe $n \in \mathbb{N}$ tal que $7 \mid 4n^2 - 3$.*

Solução:

Pelo Teorema da Divisão Euclidiana, temos que existem q e $r \in \mathbb{Z}$ únicos tais que $n = 7q + r$, com $0 < r < 7$. Daí,

$$4n^2 - 3 = 4(7q + r)^2 - 3a =$$
$$= 4(49q^2 + 14qr + r^2) - 3 =$$
$$= 7(28q^2 + 8qr) + 4r^2 - 3.$$

Se $7 \mid 4n^2 - 3$ então $7 \mid 7(28q^2 + 8qr) + 4r^2 - 3$ e pela proposição 1.4, como $7 \mid 7(28q^2 + 8qr)$ temos que $7 \mid 4r^2 - 3$. Como $0 \leqslant r < 7$, temos que para:

- $r = 0$, $7 \mid -3$, o que é absurdo;
- $r = 1$, $7 \mid 1$, o que é absurdo;
- $r = 2$, $7 \mid 13$, o que é absurdo;
- $r = 3$, $7 \mid 33$, o que é absurdo;

- $r = 4$, $7 \mid 61$, o que é absurdo;
- $r = 5$, $7 \mid 97$, o que é absurdo;
- $r = 6$, $7 \mid 141$, o que é absurdo.

Portanto, não existe $n \in \mathbb{N}$ tal que $7 \mid 4n^2 - 3$.

Exemplo 1.9 *Mostre que se $n \in \mathbb{N}$ é ímpar, então $8 \mid n^2 - 1$.*

Solução:

Pelo Teorema da Divisão Euclidiana, n pode ser escrito de uma, e somente uma das seguintes formas: $4q$, $4q+1$, $4q+2$ ou $4q+3$. Como n é ímpar, temos que n assume somente as formas $4q+1$ ou $4q+3$. Para:

- $n = 4q+1$, $n^2 - 1 = (4q+1)^2 - 1 = 16q^2 + 8q + 1 - 1 = 16q^2 + 8q = 8(q^2 + q)$ e portanto, $8 \mid n^2 - 1$;
- $n = 4q+3$, $n^2 - 1 = (4q+3)^2 - 1 = 16q^2 + 24q + 9 - 1 = 16q^2 + 24q + 8 = 8(q^2 + 3q + 1)$ e portanto, $8 \mid n^2 - 1$.

Capítulo 2

Máximo Divisor Comum

Neste capítulo, foram utilizadas as seguintes referências: [1], [3], [4], [5], [6] e [7].

2.1 Definição

Definição 2.1 (Máximo Divisor Comum) *Sejam $d \in \mathbb{Z}$, $d > 0$, d é máximo divisor comum de dois inteiros a e b, denotado por $mdc(a, b) = d$ se possuir as seguintes propriedades:*

(i) $d \mid a$ *e* $d \mid b$*;*

(ii) Se $c \mid a$ *e* $c \mid b$*, então* $c \mid d$*.*

Exemplo 2.1 *Seja a e $b \in \mathbb{N}$. Tem-se que:*

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

(ii) $mdc(0, a) = a$.

(iii) $mdc(a, a) = a$.

(iv) $mdc(a, b) = mdc(-a, b) = mdc(a, -b) = (-a, -b)$.

Teorema 2.1 *Sejam a, b, q e $r \in \mathbb{Z}$, onde $a = bq + r$, então:*

$$mdc(a, b) = mdc(b, r)$$

Demonstração:

Seja $d = mdc(a, b)$. Então:

Pela proposição 1.5, como $d \mid a$ e $d \mid b$ e $q \in \mathbb{Z}$ temos que $d \mid a - bq = r$.

Suponhamos que $c \mid b$ e $c \mid r = a - bq$, então pela proposição 1.5, $c \mid bq + a - bq = a$, logo $c \mid d$.

□

2.2 Lema de Euclides

Lema 2.1 (Lema de Euclides) *Sejam a, b e $n \in \mathbb{Z}$, então:*

$$mdc(a, b) = mdc(a, b - na)$$

Demonstração:

Seja $b - na = d$. Então $b = an + d$. Portanto, pelo Teorema 2.1, como a, b, n e $d \in \mathbb{Z}$, $mdc(a, b) = mdc(a, d) = mdc(a, b - na)$.

□

Exemplo 2.2 *Utilizando o Lema de Euclides, calcule $mdc(468, 326)$.*

Solução:

$$\begin{aligned}
&mdc(468, 326) = \\
&= mdc(468 - 326, 326) = \\
&= mdc(142, 326) = \\
&= mdc(142, 326 - 2 \cdot 142) = \\
&= mdc(142, 42) = \\
&= mdc(142 - 3 \cdot 42, 42) = \\
&= mdc(16, 42) = \\
&= mdc(16, 42 - 2 \cdot 16) = \\
&= mdc(16, 10) = \\
&= mdc(16 - 10, 10) = \\
&= mdc(6, 10) = \\
&= mdc(6, 10 - 6) = \\
&= mdc(6, 4) = \\
&= mdc(6 - 4, 4) = \\
&= mdc(2, 4) = \\
&= mdc(2, 4 - 2 \cdot 2) = \\
&= mdc(2, 0) = 2.
\end{aligned}$$

Exemplo 2.3 *Seja $n \in \mathbb{Z}$. Mostre que:*

(a) $mdc(n, 2n + 1) = 1$

(b) $mdc(n + 1, n^2 + n + 1) = 1$

(c) $mdc(2n + 1, 9n + 4) = 1$

(d) $mdc(n! + 1, (n + 1)! + 1) = 1$

Solução:

(a) Pelo Lema de Euclides, temos que

$$\begin{aligned} & mdc(n, 2n+1) = \\ & = mdc(n, 2n+1-2n) = \\ & = mdc(n, 1) = 1. \end{aligned}$$

(b) Pelo Lema de Euclides, temos que

$$\begin{aligned} & mdc(n+1, n^2+n+1) = \\ & = mdc(n+1, n^2+n+1-(n+1)^2) = \\ & = mdc(n+1, n^2+n+1-n^2-2n-1) = \\ & = mdc(n+1, -n) = \\ & = mdc(n+1, -n+n+1) = \\ & = (n+1, 1) = 1. \end{aligned}$$

(c) Pelo Lema de Euclides, temos que

$$\begin{aligned} & mdc(2n+1, 9n+4) = \\ & = (2n+1, 9n+4-4(2n+1)) = \\ & = (2n+1, 9n+4-8n-4) = \\ & = (2n+1, n) = (2n+1-2n, n) = \\ & = (1, n) = 1. \end{aligned}$$

(d) Pelo Lema de Euclides, temos que

$$\begin{aligned} & mdc(n!+1, (n+1)!+1) = \\ & = mdc(n!+1, (n+1)!+1-(n+1)(n!+1)) = \\ & = mdc(n!+1, (n+1)!+1-(n+1)!-n-1) = \\ & = mdc(n!+1, -n) = \\ & = mdc(n!+1-(n-1)!(-n), -n) = \\ & = mdc(1, -n) = 1 \end{aligned}$$

2.3 Algoritmo de Euclides

Teorema 2.2 (Algoritmo de Euclides) *Sejam a, b e $r_j \in \mathbb{Z}$, $j = \{1, 2, ..., n, n+1\}$. Efetuando o algoritmo da Divisão Euclidiana sucessivamente de a por b, b por r_1, r_1 por r_2, ...,r_{n-1} por r_n, até que $r_{n+1} = 0$, como abaixo, tem-se que $mdc(a, b) = r_n$.*

$$a = bq_1 + r_1,\ 0 \leqslant r_1 < |b|$$
$$b = r_1 q_2 + r_2,\ 0 \leqslant r_2 < r_1$$

$$
\begin{aligned}
r_1 &= r_2q_3 + r_3,\ 0 \leqslant r_3 < r_2 \\
r_2 &= r_3q_4 + r_4,\ 0 \leqslant r_4 < r_3 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n,\ 0 \leqslant r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1},\ r_{n+1} = 0.
\end{aligned}
$$

Demonstração:

Como $|b| > r_1 > r_2 > r_3 > ...$, temos pelo Princípio da Boa Ordenação que teremos um número finito de divisões e consequentemente algum $r_{n+1} = 0$.

Pelo Teorema 2.1, temos que

$mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = ... = mdc(r_{n-1}, r_n) = mdc(r_n, 0) =$
$= r_n$.

□

Exemplo 2.4 *Utilizando o Algoritmo de Euclides calcule* $mdc(702, 690)$.

Solução:

Temos que

$$
\begin{aligned}
702 &= 690 \cdot 1 + 12 \\
690 &= 12 \cdot 57 + 6 \\
12 &= 6 \cdot 2
\end{aligned}
$$

Logo, $mdc(702, 690) = 6$.

Teorema 2.3 *Sejam* a *e* $b \in \mathbb{Z}$. *Então existem inteiros* x *e* y *tais que* $ax + by = mdc(a, b)$. *Além disso,* $ax + by$ *é o menor inteiro positivo pertencente ao conjunto* $A = \{am + bn; m, n \in \mathbb{Z}\}$.

Demonstração:

Considere o conjunto de todas as combinações lineares $A = \{am+bn; m, n \in \mathbb{Z}\}$. Temos que $A \cup \mathbb{N}$ é não-vazio, pois $a^2 + b^2 = a \cdot a + b \cdot b \in A \cup \mathbb{N}$. Seja $d = ax + by$ o menor inteiro positivo pertencente ao conjunto A. Vamos provar que $d = mdc(a, b)$.

Provaremos que $d \mid a$ por contradição. Suponha, por contradição, que $d \nmid a$. Pelo algoritmo da Divisão Euclidiana exitem únicos q e $r \in \mathbb{Z}$ tais que $a = dq + r$, com $0 < r < d$. Temos que

$$
\begin{aligned}
r &= a - dq = \\
&= a - (ax + by)q = \\
&= a - axq - byq = \\
&= a(1 - xq) + b(-yq).
\end{aligned}
$$

Portanto $r \in A \cup \mathbb{N}$ e como $r < d$, temos que r é o menor inteiro positivo pertencente ao conjunto A, o que é uma contradição. Logo, $d \mid a$.

Analogamente, temos que $d \mid b$.

Suponhamos que $c \mid a$ e $c \mid b$. Então, existem q_1 e $q_2 \in \mathbb{Z}$ tais que $a = cq_1$ e $b = cq_2$. Então

$$\begin{aligned} d &= ax + by = \\ &= cq_1x + cq_2y = \\ &= c(q_1x + q_2y). \end{aligned}$$

Portanto, $c \mid d$.

□

Corolário 2.1 *Sejam a e $b \in \mathbb{Z}$ e $c \in \mathbb{N}$. Então $mdc(ca, cb) = c \cdot mdc(a, b)$.*

Demonstração:

Pelo Teorema 2.3, temos que $mdc(ca, cb) = cax + cby$, com x e $y \in \mathbb{Z}$, onde $cax+cby = c(ax+by)$ é o menor inteiro positivo do conjunto $A = \{cam+cbn; m, n \in \mathbb{Z}\}$. Logo $ax + by$ é o menor inteiro positivo do conjunto $B = \{am + bn; m, n \in \mathbb{Z}\}$ e, portanto, $mdc(a, b) = ax + by$. Assim, $mdc(ca, cb) = cax + cby = c(ax + by) = c \cdot mdc(a, b)$.

□

Corolário 2.2 *Sejam a e $b \in \mathbb{Z}$. Se $mdc(a, b) = d$, então $mdc(\frac{a}{d}, \frac{b}{d}) = 1$.*

Demonstração:

Pelo corolário 2.1, temos que

$$\begin{aligned} d \cdot mdc(\tfrac{a}{d}, \tfrac{b}{d}) &= \\ &= mdc(d\tfrac{a}{d}, d\tfrac{b}{d}) = \\ &= mdc(a, b) = d. \end{aligned}$$

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

□

Definição 2.2 *Sejam a e $b \in \mathbb{Z}$, dizemos que a e b são primos entre si quando $mdc(a, b) = 1$.*

Exemplo 2.5 *Temos que 20 e 49 são primos entre si pois, pelo Lema de Euclides:*

$$\begin{aligned} &mdc(20, 49) = \\ &= mdc(20, 49 - 2 \cdot 20) = \\ &= mdc(20, 9) = \\ &= mdc(20 - 2 \cdot 9, 9) = \\ &= mdc(2, 9) = \\ &= mdc(2, 9 - 4 \cdot 2) = \\ &= mdc(2, 1) = 1. \end{aligned}$$

Proposição 2.1 *Sejam a, b e $c \in \mathbb{Z}$. Se $a \mid bc$ e $mdc(a, b) = 1$, então $a \mid c$.*

Demonstração:

De $a \mid bc$, temos que existe $q \in \mathbb{Z}$ tal que $bc = aq$. De $mdc(a, b) = 1$ temos que existem x e $y \in \mathbb{Z}$ tal que $ax + by = 1$. Logo,

$$\begin{aligned} & ax + by = 1 \Rightarrow \\ & \Rightarrow cax + cby = c \Rightarrow \\ & \Rightarrow cax + aqy = c \Rightarrow \\ & \Rightarrow a(cx + qy) = c \Rightarrow \\ & \Rightarrow a \mid c. \end{aligned}$$

□

Corolário 2.3 *Sejam a, b e $c \in \mathbb{Z}$. Então $b \mid a$ e $c \mid a$ se, e somente se, $\frac{bc}{mdc(b,c)} \mid a$.*

Demonstração:

($\Rightarrow$)Se $b \mid a$ e $c \mid a$, então existem q_1 e $q_2 \in \mathbb{Z}$ tais que $a = bq_1$ e $a = cq_2$, assim $bq_1 = cq_2$ donde $\frac{b}{mdc(b,c)}q_1 = \frac{c}{mdc(b,c)}q_2$ e, portanto, $\frac{b}{mdc(b,c)} \mid \frac{c}{mdc(b,c)}q_2$.

Como, $mdc(\frac{b}{mdc(b,c)}, \frac{c}{mdc(b,c)}) = 1$ (corolário 2.2), temos pela Proposição 2.1 que $\frac{b}{mdc(b,c)} \mid q_2$. Portanto, $\frac{bc}{mdc(b,c)} \mid cq_2 = a$.

($\Leftarrow$)Temos, como consequência imediata da definição de Divisibilidade que se $\frac{bc}{mdc(b,c)} \mid a$, então $b \mid a$ e $c \mid a$.

□

Como consequência imediata do Corolário 2.3, temos que se $b \mid a$, $c \mid a$ e $mdc(b, c) = 1$, então $bc \mid a$.

Exemplo 2.6 *Mostre que para todo $n \in \mathbb{N}$, $24 \mid n(n^2 - 1)(3n + 2)$.*

Solução:

(a) $3 \mid n(n^2 - 1)(3n + 2)$:

Pelo Teorema da Divisão Euclidiana, temos que existem q e $r \in \mathbb{Z}$ únicos tais que $n = 3q + r$, com $0 < r < 3$. Então,

$$\begin{aligned} & n(n^2 - 1)(3n + 2) = \\ & = (3q + r)[(3q + r)^2 - 1][3(3q + r) + 2] = \\ & = (3q + r)(9q^2 + 6qr + r^2 - 1)(9q + 3r + 2). \end{aligned}$$

Logo, se:

- $r = 0$, então $n(n^2 - 1)(3n + 2) = 3q(9q^2 - 1)(9q + 2)$.
  Ou seja, $3 \mid n(n^2 - 1)(3n + 2)$.
- $r = 1$, então $n(n^2 - 1)(3n + 2) = (3q + 1)(9q^2 + 6q)(9q + 5) =$
  $= 3(3q + 1)(3q^2 + 2q)(9q + 5)$.
  Ou seja, $3 \mid n(n^2 - 1)(3n + 2)$.

- $r = 2$, então $n(n^2-1)(3n+2) = (3q+2)(9q^2+12q+3)(9q+8) =$
  $= 3(3q+2)(3q^2+4q+1)(9q+8)$.
  Ou seja, $3 \mid n(n^2-1)(3n+2)$.

(b) $8 \mid n(n^2-1)(3n+2)$:

Pelo Teorema da Divisão Euclidiana, temos que existem q e $r \in \mathbb{Z}$ únicos tais que $n = 4q + r$, com $0 < r < 4$. Então,

$$n(n^2-1)(3n+2) =$$
$$= (4q+r)[(4q+r)^2-1][3(4q+r)+2] =$$
$$= (4q+r)(16q^2+8qr+r^2-1)(12q+3r+2).$$

Logo, se:

- $r = 0$, então $n(n^2-1)(3n+2) = 4q(16q^2-1)(12q+2) =$
  $= 8q(16q^2-1)(6q+1)$.
  Ou seja, $8 \mid n(n^2-1)(3n+2)$.
- $r = 1$, então $n(n^2-1)(3n+2) = (4q+1)(16q^2+8q)(12q+5) =$
  $= 8(4q+1)(2q^2+1)(12q+5)$.
  Ou seja, $8 \mid n(n^2-1)(3n+2)$.
- $r = 2$, então $n(n^2-1)(3n+2) = (4q+2)(16q^2+16q+3)(12q+8) =$
  $= 8(2q+1)(16q^2+16q+3)(3q+2)$.
  Ou seja, $8 \mid n(n^2-1)(3n+2)$.
- $r = 3$, então $n(n^2-1)(3n+2) = (4q+3)(16q^2+24q+8)(12q+11) =$
  $= 8(4q+3)(2q^2+2q+1)(12q+11)$.
  Ou seja, $8 \mid n(n^2-1)(3n+2)$.

Como $3 \mid n(n^2-1)(3n+2)$, $8 \mid n(n^2-1)(3n+2)$ e $mdc(3,8) = 1$ temos, pelo Corolário 2.3, que $24 \mid n(n^2-1)(3n+2)$.

Definição 2.3 *Sejam $p \in \mathbb{N}$, com $p \neq 1$. Se p tem apenas dois divisores: 1 e p, então p é dito primo.*

Se um número $a \neq 1 \in \mathbb{N}$ não é primo, então a é composto. Logo, se n é composto existe $b \in \mathbb{N}$ tal que $b \mid a$, sendo que $b \neq 1$ e $b \neq a$. E, portanto, existe $c \in \mathbb{N}$ tal que $a = bc$, sendo que $1 < b < a$ e $1 < c < a$.

Exemplo 2.7 *Os números primos menores que 100 são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97.*

Corolário 2.4 *Sejam a, $b \in \mathbb{Z}$ e p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração:

Se $p \mid a$, não há o que demonstrar. Se $p \nmid a$, temos que $mdc(a, p) = 1$. Pela proposição 2.1, como $p \mid ab$ e $mdc(a, p) = 1$, temos que $a \mid b$.

□

2.4 Teorema Fundamental da Aritmética

Teorema 2.4 (Teorema Fundamental da Aritmética) *Todo número natural maior do que 1 é primo ou se escreve de modo único (a menos de ordem dos fatores) como um produto de números primos.*

Demonstração:

Faremos a demonstração por indução sobre n.

Como 2 é primo, temos que o teorema é verdadeiro para $n = 2$.

Suponhamos que o teorema seja válido para $2, 3, \cdots, n-1$, vamos provar que vale para n. Caso n seja primo não há o que demonstrar. Suponhamos que n seja composto, então existem a e $b \in \mathbb{N}$ tais que $n = ab$, com $1 < a < n$ e $1 < b < n$. Logo, por hipótese de indução, $a = p_1 p_2 \cdots p_r$ e $b = q_1 q_2 \cdots q_s$, com p_i e q_j primos. Portanto, $n = ab = p_1 p_2 \cdots p_r q_1 q_2 \cdots q_s$.

Vamos mostrar a unicidade da escrita. Suponhamos que $n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, sendo p_i e q_j números primos, então $p_1 \mid q_1 q_2 \cdots q_s$ assim, $p_1 \mid q_1$ ou $p_1 \mid q_2$ ou $\cdots$ ou $p_1 \mid q_s$ (pelo corolário 2.4) e, portanto, $p_1 = q_1$ ou $p_1 = q_2$ ou $\cdots$ ou $p_1 = q_s$.

Suponhamos que $p_1 = q_1$. Então $p_2 \cdots p_r = q_2 \cdots q_s < n$ e por hipótese de indução temos que $p_2 \cdots p_r = q_2 \cdots q_s$ pode ser escrito de forma única como um produto de fatores primos, então necessariamente $r = s$ e $p_i = q_j$ aos pares.

□

Proposição 2.2 *Sejam a e $b \in \mathbb{N}$. Se $a = p_1^{n_1} \cdots p_t^{n_t}$ e $b = p_1^{m_1} \cdots p_t^{m_t}$ sendo n_i e $m_i \in \mathbb{N} \cup \{0\}$ e p_i primo, com $n_i \leqslant m_i$ e $1 \leqslant i \leqslant t$, então $a \mid b$.*

Demonstração:

Como $n_i \leqslant m_i$, temos que: $n_i = m_i$ ou $n_i < m_i$.

- $n_i = m_i \Rightarrow p_i^{n_i} = p_i^{m_i} \Rightarrow p_i^{n_i} \mid p_i^{m_i}$;
- $n_i < m_i \Rightarrow m_i = n_i + r \Rightarrow p_i^{m_i} = p_i^{n_i + r} \Rightarrow p_i^{m_i} = p_i^{n_i} p^r \Rightarrow p_i^{n_i} \mid p_i^{m_i}$.

Como $p_i^{n_i} \mid p_i^{m_i}$, temos que $p_1^{n_1} \mid p_1^{m_1}$, $\cdots$, $p_t^{n_t} \mid p_t^{m_t}$. Logo, pela proposição 1.1, temos que $p_1^{n_1} \cdots p_t^{n_t} \mid p_1^{m_1} \cdots p_t^{m_t}$ e, portanto, $a \mid b$.

□

Proposição 2.3 *Sejam a e $b \in \mathbb{N}$. Se $a \mid b$ e $b = p_1^{m_1} \cdots p_t^{m_t}$ sendo $m_i \in \mathbb{N} \cup \{0\}$ e p_i primo, com $1 \leqslant i \leqslant t$, então $a = p_1^{n_1} \cdots p_t^{n_t}$, com $n_i \leqslant m_i$, sendo $n_i \in \mathbb{N} \cup \{0\}$.*

Demonstração:

Seja p^n, com p primo e $n \in \mathbb{N}$, um fator na decomposição de a, logo $p^n \mid a$. Como $a \mid b$ temos que $p^n \mid b = p_1^{m_1} \cdots p_t^{m_t}$, logo

$$\begin{aligned}
&p^n \mid p_i^{m_i} \Rightarrow \\
&\Rightarrow p_i^{m_i} = p^n q, \text{ com } q \in \mathbb{N} \Rightarrow \\
&\Rightarrow p = p_i \text{ e } q = p_i^r, \text{ com } r \in \mathbb{N}, \text{ pois } p_i \text{ é primo} \Rightarrow \\
&\Rightarrow p_i^{m_i} = p_i^n p_i^r \Rightarrow \\
&\Rightarrow p_i^{m_i} = p_i^{n+r} \Rightarrow \\
&\Rightarrow m_i = n + r \Rightarrow \\
&\Rightarrow n \leqslant m_i.
\end{aligned}$$

Logo $a = p_1^{n_1} \cdots p_t^{n_t}$, com $n_i \leqslant m_i$.

□

Teorema 2.5 *Sejam a e $b \in \mathbb{N}$. Se $a = p_1^{n_1} \cdots p_t^{n_t}$ e $b = p_1^{m_1} \cdots p_t^{m_t}$ com n_i e $m_i \in \mathbb{N} \cup \{0\}$ e p_i primo, com $1 \leqslant i \leqslant t$, então $mdc(a, b) = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, em que $\alpha_i = min\{n_i, m_i\}$.*

Demonstração:

(a) Seja $d = p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, onde $\alpha_i = min\{n_i, m_i\}$. Como $\alpha_i = min\{n_i, m_i\}$, temos que: $\alpha_i \leqslant n_i$. Pela proposição 2.2 temos que $d \mid a$ e $d \mid b$.

(b) Seja $c \in \mathbb{N}$ tal que $c \mid a$ e $c \mid b$. Logo, pela proposição 2.3 temos que $c = p_1^{\beta_1} \cdots p_t^{\beta_t}$, com $\beta_i \leqslant n_i$ e $\beta_i \leqslant m_i$. Como $\alpha_i = min\{n_i, m_i\}$, temos que $\beta_i \leqslant \alpha_i$. Logo, pela proposição 2.2, $c \mid d$.

□

Exemplo 2.8 *Calcule o $mdc(360, 378)$ utilizando o teorema 2.5.*

Solução:

$$\begin{aligned}
&360 = 2^3 \cdot 3^2 \cdot 5^1 \text{ e } 378 = 2^1 \cdot 3^3 \cdot 7^1 \Rightarrow \\
&\Rightarrow 360 = 2^3 \cdot 3^2 \cdot 5^1 \cdot 7^0 \text{ e } 378 = 2^1 \cdot 3^3 \cdot 5^0 \cdot 7^1 \Rightarrow \\
&\Rightarrow mdc(360, 378) = 2^{min\{1,3\}} \cdot 3^{min\{2,3\}} \cdot 5^{min\{0,1\}} \cdot 7^{min\{0,1\}} \Rightarrow \\
&\Rightarrow mdc(360, 378) = 2^1 \cdot 3^2 \cdot 5^0 \cdot 7^0 \Rightarrow \\
&\Rightarrow mdc(360, 378) = 18.
\end{aligned}$$

Capítulo 3

Uma aplicação do MDC: Equações Diofantinas

Neste capítulo, foram utilizadas as seguintes referências: [1], [3], [4], [5], [6] e [7].

3.1 Equações Diofantinas

Definição 3.1 (Equações Diofantinas) *Dados a, b e $c \in \mathbb{Z}$, com $ab \neq 0$, chamamos de Equações Diofantinas as equações do tipo*

$$ax + by = c$$

em que x e y são incógnitas inteiras.

Proposição 3.1 *Sejam a, b e $c \in \mathbb{Z}$, com $ab \neq 0$. A equação $ax + by = c$ admite soluções se, e somente se, $mdc(a, b) \mid c$.*

Demonstração:

($\Rightarrow$) Se a equação possui solução, então existem x e $y \in \mathbb{Z}$ tais que $ax + by = c$. Temos que $mdc(a, b) \mid a$ e $mdc(a, b) \mid b$ e pela proposição 1.5, temos que $mdc(a, b) \mid ax + by$ e, portanto, $mdc(a, b) \mid c$.

($\Leftarrow$) Temos, pelo teorema 2.3, existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = mdc(a, b)$. Como $mdc(a, b) \mid c$ temos que existe $q \in \mathbb{Z}$ tal que $mdc(a, b)q = c$. Daí, $(ax_0 + by_0)q = c$, ou seja, $a(x_0q) + b(y_0q) = c$. Como x_0q e $y_0q \in \mathbb{Z}$ temos que a equação $ax + by = c$ possui solução. □

Exemplo 3.1 *Verifique se possuem soluções as equações:*

(a) $15x + 25y = 12$

(b) $12x + 16y = 8$

Solução:

(a) Como $mdc(15, 25) = 5$ e $5 \nmid 12$, temos que a equação $15x + 25y = 12$ não possui solução.

(b) Como $mdc(12, 16) = 4$ e $4 \mid 8$, temos que a equação $12x + 16y = 8$ possui solução.

Exemplo 3.2 *Para quais valores de c a equação $102x + 54y = c$ tem solução?*

Solução:

Pela proposição 3.1, para que a equação tenha solução precisamos que $mdc(102, 54) \mid c$. Utilizando o Lema de Euclides, temos que:

$$\begin{aligned} & mdc(102, 54) = \\ & = mdc(48, 54) = \\ & = mdc(48, 6) = \\ & = mdc(0, 6) = 6 \end{aligned}$$

Portanto, a equação tem solução se $6 \mid c$, ou seja, se $c = 6k$, com $k \in \mathbb{Z}$.

Proposição 3.2 *Sejam a, b e $c \in \mathbb{Z}$, com $ab \neq 0$ e $d = mdc(a, b)$. Se x_0 e y_0 é uma solução particular da equação $ax + by = c$, então todas as outras soluções da equação são dadas por:*

$$x = x_0 + \frac{b}{d}t \text{ e } y = y_0 - \frac{a}{d}t, \text{ com } t \in \mathbb{Z}.$$

Demonstração:

Sejam x e y uma solução da equação $ax + by = c$. Então,

$$\begin{aligned} & ax + by = ax_0 + by_0 \Rightarrow \\ & \Rightarrow ax - ax_0 = by_0 - by \Rightarrow \\ & \Rightarrow a(x - x_0) = b(y_0 - y) \Rightarrow \\ & \Rightarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y) \Rightarrow \\ & \Rightarrow \frac{b}{d} \mid \frac{a}{d}(x - x_0). \end{aligned}$$

Pelo corolário 2.2, $(\frac{b}{d}, \frac{a}{d}) = 1$. Logo, pela proposição 2.1, temos que $\frac{b}{d} \mid x - x_0$, ou seja, existe $t \in \mathbb{Z}$ tal que $x - x_0 = \frac{b}{d}t$. Portanto, $x = x_0 + \frac{b}{d}t$.

De $x - x_0 = \frac{b}{d}t$ e $a(x - x_0) = b(y_0 - y)$, temos que $a\frac{b}{d}t = b(y_0 - y)$. Assim, $\frac{a}{d}t = y_0 - y$ e, portanto, $y = y_0 - \frac{a}{d}t$.

Isso mostra que as solução são do tipo exibido, por outro lado, temos que x e y, são soluções da equação, pois

$$ax + by = a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d})t = ax_0 + by_0 + \frac{ab}{d}t - \frac{ab}{d}t = c$$

□

Exemplo 3.3 *Resolva a equação $36x + 16y = 20$.*

Solução:

Primeiramente iremos calcular o $mdc(36, 16)$ pelo Algoritmo de Euclides.

$$36 = 16 \cdot 2 + 4$$
$$16 = 4 \cdot 4$$

Logo, $mdc(36, 16) = 4$ e como $4 \mid 20$ temos que a equação $36x + 16y = 20$ possui solução. Como $36 - 16 \cdot 2 = 4$ temos que

$$36 \cdot (1) + 16 \cdot (-2) = 4 \Rightarrow$$
$$\Rightarrow 36 \cdot (1 \cdot 5) + 16 \cdot (-2 \cdot 5) = 4 \cdot 5 \Rightarrow$$
$$\Rightarrow 36 \cdot (5) + 16 \cdot (-10) = 20.$$

Logo $x_0 = 5$, $y_0 = -10$ é uma solução particular da equação e portanto, pela proposição 3.2 o conjunto de soluções da equação é dado por:

$$x = 5 + \tfrac{16}{4}t \text{ e } y = -10 - \tfrac{36}{4}t, \text{ com } t \in \mathbb{Z},$$

ou seja,

$$x = 5 + 4t \text{ e } y = -10 - 9t, \text{ com } t \in \mathbb{Z}.$$

Corolário 3.1 *Sejam a, b e $c \in \mathbb{Z}$, com $ab \neq 0$ e $mdc(a, b) = 1$. Se x_0 e y_0 é uma solução particular da equação $ax + by = c$, então todas as outras soluções da equação são dadas por:*

$$x = x_0 + bt \text{ e } y = y_0 - at, \text{ com } t \in \mathbb{Z}.$$

Demonstração:

Pela proposição 3.2, temos que:

$x = x_0 + \frac{b}{1}t$ e $y = y_0 - \frac{a}{1}t$, com $t \in \mathbb{Z}$ e, portanto, $x = x_0 + bt$ e $y = y_0 - at$, com $t \in \mathbb{Z}$.

□

Exemplo 3.4 *Resolva a equação $18x + 5y = 4$.*

Solução:

Primeiramente iremos calcular o $mdc(18, 5)$ pelo Algoritmo de Euclides.

$$18 = 5 \cdot 3 + 3$$
$$5 = 3 \cdot 1 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2$$

Logo, $mdc(18, 5) = 1$ e como $1 \mid 4$ temos que a equação $18x + 5y = 4$ possui solução. Como $1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5 = 2 \cdot (18 - 3 \cdot 5) - 5 = 2 \cdot 18 - 7 \cdot 5$, temos que

$$18 \cdot (2) + 5 \cdot (-7) = 1 \Rightarrow$$
$$\Rightarrow 18 \cdot (2 \cdot 4) + 5 \cdot (-7 \cdot 4) = 1 \cdot 4 \Rightarrow$$
$$\Rightarrow 18 \cdot (8) + 5 \cdot (-28) = 4.$$

Logo $x_0 = 8$, $y_0 = -28$ é uma solução particular da equação e portanto, pelo corolário 3.1, o conjunto de soluções da equação é dado por:

$$x = 8 + 5t \text{ e } y = -28 - 18t, \text{ com } t \in \mathbb{Z}.$$

Exemplo 3.5 *Determine o menor inteiro positivo que, quando dividido por 50, deixa resto 13 e, quando dividido por 56, deixa resto 21.*

Solução:

Seja n este número. Temos que $n = 50x + 13$ e $n = 56y + 21$. Portanto,

$$50x + 13 = 56y + 21 \Rightarrow$$
$$\Rightarrow 50x - 56y = 8$$
$$\Rightarrow 25x - 28y = 4.$$

Primeiramente iremos calcular o $mdc(25, 28)$ pelo Algoritmo de Euclides.

$$28 = 25 \cdot 1 + 3$$
$$25 = 3 \cdot 8 + 1$$
$$3 = 1 \cdot 3$$

Logo, $mdc(25, 28) = 1$ e como $1 \mid 4$ temos que a equação $25x - 28y = 4$ possui solução. Como $1 = 25 - 8 \cdot 3 = 25 - 8(28 - 25) = 25 \cdot 9 - 28 \cdot 8$, temos que

$$25 \cdot (9) - 28 \cdot (8) = 1 \Rightarrow$$
$$\Rightarrow 25 \cdot (9 \cdot 4) - 28 \cdot (8 \cdot 4) = 1 \cdot 4 \Rightarrow$$
$$\Rightarrow 25 \cdot (36) - 28 \cdot (32) = 4.$$

Logo $x_0 = 36$, $y_0 = 32$ é uma solução particular da equação e portanto, pelo corolário 3.1 o conjunto de soluções da equação é dado por:

$$x = 36 - 28t \text{ e } y = 32 - 25t, \text{ com } t \in \mathbb{Z}.$$

Como $n = 50x + 13$, temos que:

$$n = 50(36 - 28t) + 13 \Rightarrow$$
$$\Rightarrow n = 1800 - 1400t + 13 \Rightarrow$$
$$\Rightarrow n = 1813 - 1400t.$$

Mas, como queremos o menor inteiro positivo, temos que

$$n > 0 \Rightarrow 1813 - 1400t > 0 \Rightarrow$$
$$\Rightarrow 1400t < 1813 \Rightarrow$$
$$\Rightarrow t < \tfrac{1813}{1400} \Rightarrow$$
$$\Rightarrow t \leqslant 1.$$

Para $t = 1$, temos que $n = 1813 - 1400 \cdot 1$ e, portanto $n = 413$.

Para $t = 0$, temos que $n = 1813 - 1400 \cdot 0$ e, portanto $n = 1813$.

Para $t = -1$, temos que $n = 1813 - 1400 \cdot (-1)$ e, portanto $n = 3213$.

Para $t = -2$, temos que $n = 1813 - 1400 \cdot (-2)$ e, portanto $n = 4613$.

Logo, $n \in \{413, 1813, 3213, 4613 \cdots\}$ e portanto, o número procurado é 413.

Exemplo 3.6 *Determine duas frações positivas que tenham* 19 *e* 31 *como denominadores e cuja soma seja igual a* $\frac{305}{589}$.

Solução:

Sejam $\frac{x}{19}$ e $\frac{y}{31}$ estas frações. Logo, $31x + 19y = 305$.

Primeiramente iremos calcular o $mdc(31, 19)$ pelo Algoritmo de Euclides.

$$31 = 19 \cdot 1 + 12$$
$$19 = 12 \cdot 1 + 7$$
$$12 = 7 \cdot 1 + 5$$
$$7 = 5 \cdot 1 + 2$$
$$5 = 2 \cdot 2 + 1$$
$$2 = 1 \cdot 2$$

Logo, $mdc(31, 19) = 1$ e como $1 \mid 301$ temos que a equação $31x + 19y = 305$ possui solução. Como $1 = 5 - 2 \cdot 2 = 5 - 2(7 - 5) = 3 \cdot 5 - 2 \cdot 7 = 3(12 - 7) - 2 \cdot 7 = 3 \cdot 12 - 5 \cdot 7 = 3 \cdot 12 - 5(19 - 12) = 8 \cdot 12 - 5 \cdot 19 = 8(31 - 19) - 5 \cdot 19 = 8 \cdot 31 - 13 \cdot 19$, temos que

$$31 \cdot (8) + 19 \cdot (-13) = 1 \Rightarrow$$
$$\Rightarrow 31(8 \cdot 305) + 19(-13 \cdot 305) = 305 \Rightarrow$$
$$\Rightarrow 31(2440) + 19(-3965) = 305.$$

Logo $x_0 = 2440$, $y_0 = -3965$ é uma solução particular da equação e portanto, pelo corolário 3.1 o conjunto de soluções da equação é dado por

$$x = 2440 - 19t \text{ e } y = -3965 + 31t, \text{ com } t \in \mathbb{Z}.$$

Como procuramos duas frações positivas, temos que

$$x > 0 \Rightarrow$$
$$\Rightarrow 2440 - 19t > 0 \Rightarrow$$
$$\Rightarrow 19t < 2440 \Rightarrow$$
$$\Rightarrow t < \tfrac{2440}{19} \Rightarrow$$
$$\Rightarrow t \leqslant 128$$

e

$$y > 0 \Rightarrow$$
$$\Rightarrow -3965 + 31t > 0 \Rightarrow$$
$$\Rightarrow 31t > 3965 \Rightarrow$$
$$\Rightarrow t > \tfrac{3965}{31} \Rightarrow$$
$$\Rightarrow t \geqslant 128.$$

Portanto, $t = 128$, ou seja, $x = 8$ e $y = 3$ e consequentemente as frações são $\frac{8}{19}$ e $\frac{3}{31}$.

Exemplo 3.7 *Cinco piratas atacaram o navio de um rico navegante e roubaram seu baú com moedas de ouro. Quando se afastaram do navio com o baú, caiu a noite e eles concordaram em dividir as moedas apenas na manhã seguinte.*

Durante a noite, um dos piratas decidiu pegar parte do ouro para si. Ele foi sorrateiramente até o baú e dividiu as moedas em 5 pilhas iguais, restando uma

moeda. Depois, colocou a moeda que restou na sua pilha e escondeu esta pilha consigo, devolvendo as outras 4 pilhas ao baú.

Um por um, os outros piratas fizeram o mesmo: eles iam sorrateiramente até o baú, dividiam as moedas em 5 pilhas, restando sempre uma moeda; colocavam a moeda que restava em suas próprias pilhas, escondiam-nas e devolviam as 4 pilhas restantes ao baú.

Qual é o menor número de moedas que poderia existir originalmente no baú?

Solução:

Seja n a quantidade de moedas da pilha original.

O primeiro pirata dividiu n moedas em 5 pilhas iguais, restando uma moeda, logo

$$n = 5n_1 + 1, n_1 \in \mathbb{N}$$

Em seguida, o primeiro pirata escondeu uma pilha mais uma moeda para si, ou seja, $n_1 + 1$ moedas, deixando $4n_1$ moedas no baú.

Como o primeiro, o segundo pirata dividiu $4n_1$ moedas em 5 pilhas iguais, restando uma moeda, logo

$$4n_1 = 5n_2 + 1, n_2 \in \mathbb{N}$$

Da mesma forma que o primeiro, ele escondeu uma pilha mais uma moeda para si, ou seja, $n_2 + 1$ moedas, deixando $4n_2$ moedas no baú.

O terceiro pirata dividiu $4n_2$ moedas em 5 pilhas iguais, restando uma moeda, logo

$$4n_2 = 5n_3 + 1, n_3 \in \mathbb{N}$$

Ele escondeu uma pilha mais uma moeda para si, ou seja, $n_3 + 1$ moedas, deixando $4n_3$ moedas no baú.

O quarto pirata dividiu $4n_3$ moedas em 5 pilhas iguais, restando uma moeda, logo

$$4n_3 = 5n_4 + 1, n_4 \in \mathbb{N}$$

Ele escondeu uma pilha mais uma moeda para si, ou seja, $n_4 + 1$ moedas, deixando $4n_4$ moedas no baú.

O quinto pirata dividiu $4n_4$ moedas em 5 pilhas iguais, restando uma moeda, logo

$$4n_4 = 5n_5 + 1, n_5 \in \mathbb{N}$$

Ele escondeu uma pilha mais uma moeda para si, ou seja, $n_5 + 1$ moedas, deixando $4n_5$ moedas no baú.

Desta forma, temos que

$$n = 5n_1 + 1 =$$

$$
\begin{aligned}
&= 5(\tfrac{5n_2+1}{4}) + 1 = \\
&= \tfrac{25n_2}{4} + \tfrac{5}{4} + \tfrac{1\cdot 4}{4} = \\
&= \tfrac{25}{4}n_2 + \tfrac{9}{4} = \\
&= \tfrac{25}{4}(\tfrac{5n_3+1}{4}) + \tfrac{9}{4} = \\
&= \tfrac{125}{16}n_3 + \tfrac{25}{16} + \tfrac{9\cdot 4}{4\cdot 4} = \\
&= \tfrac{125}{16}n_3 + \tfrac{61}{16} = \\
&= \tfrac{125}{16}(\tfrac{5n_4+1}{4}) + \tfrac{61}{16} = \\
&= \tfrac{625}{64}n_4 + \tfrac{125}{64} + \tfrac{61\cdot 4}{16\cdot 4} = \\
&= \tfrac{625}{64}(n_4) + \tfrac{369}{64} = \\
&= \tfrac{625}{64}(\tfrac{5n_5+1}{4}) + \tfrac{369}{64} = \\
&= \tfrac{3125}{256}n_5 + \tfrac{625}{256} + \tfrac{369\cdot 4}{64\cdot 4} = \\
&= \tfrac{3125}{256}n_5 + \tfrac{2101}{256}.
\end{aligned}
$$

Ou seja, $n = \frac{3125}{256}n_5 + \frac{2101}{256}$ donde obtemos que $3125n_5 + 2101 = 256n$, equivalentemente $256n - 3125n_5 = 2101$.

Primeiramente, iremos calcular o $mdc(3125, 256)$ pelo Algoritmo de Euclides.

$$
\begin{aligned}
3125 &= 256 \cdot 12 + 53 \\
256 &= 53 \cdot 4 + 44 \\
53 &= 44 \cdot 1 + 9 \\
44 &= 9 \cdot 4 + 8 \\
9 &= 8 \cdot 1 + 1 \\
8 &= 1 \cdot 8
\end{aligned}
$$

Logo, $mdc(3125, 256) = 1$ e como $1 \mid 2101$ temos que a equação $256n - 3125n_5 = 2101$ possui solução.

Como $1 = 9-8 = 9-(44-4\cdot 9) = 5\cdot 9-44 = 5(53-44)-44 = 5\cdot 53-6\cdot 44 = 5 \cdot 53 - 6(256 - 4 \cdot 53) = 29 \cdot 53 - 6 \cdot 256 = 29 \cdot 3125 - 354 \cdot 256$, temos que

$$
\begin{aligned}
&256 \cdot (-354) - 3125 \cdot (-29) = 1 \Rightarrow \\
&\Rightarrow 256(-354 \cdot 2101) - 3125(-29 \cdot 2101) = 1 \cdot 2101 \Rightarrow \\
&\Rightarrow 256(-743754) - 3125(-60929) = 2101.
\end{aligned}
$$

Logo $n = -743754$, $n_5 = -60929$ é uma solução particular da equação e portanto, pelo corolário 3.1 o conjunto de soluções da equação é dado por:

$$n = -743754t - 3125t \text{ e } n_5 = -60929 - 256t, \text{ com } t \in \mathbb{Z}.$$

Como n é o menor número de moedas que pode existir originalmente no baú, temos que $n > 0$ e portanto

$$
\begin{aligned}
&-743754 - 3125t > 0 \Rightarrow \\
&\Rightarrow 3125t < -743754 \Rightarrow \\
&\Rightarrow t < \tfrac{-743754}{3125} \Rightarrow
\end{aligned}
$$

$\Rightarrow t \leqslant -239$.

Para $t = -239$, temos que $n = 3121$.

Para $t = -240$, temos que $n = 6246$.

Para $t = -241$, temos que $n = 9371$.

Para $t = -242$, temos que $n = 12496$.

Logo, $n \in \{3121, 6246, 9371, 12496 \cdots\}$ e, portanto, $n = 3121$.

Desta forma, verificamos que:

O primeiro pirata dividiu as 3121 moedas em 5 pilhas iguais de 624 restando uma moeda. Depois, colocou a moeda que restou na sua pilha e escondeu para si 625 moedas deixando apenas $624 \cdot 4 = 2496$ moedas no baú.

O segundo pirata dividiu as 2496 moedas em 5 pilhas iguais de 499 restando uma moeda. Depois, colocou a moeda que restou na sua pilha e escondeu para si 500 moedas deixando apenas $499 \cdot 4 = 1996$ moedas no baú.

O terceiro pirata dividiu as 1996 moedas em 5 pilhas iguais de 399 restando uma moeda. Depois, colocou a moeda que restou na sua pilha e escondeu para si 400 moedas deixando apenas $399 \cdot 4 = 1596$ moedas no baú.

O quarto pirata dividiu as 1596 moedas em 5 pilhas iguais de 319 restando uma moeda. Depois, colocou a moeda que restou na sua pilha e escondeu para si 320 moedas deixando apenas $319 \cdot 4 = 1276$ moedas no baú.

O quinto pirata dividiu as 1276 moedas em 5 pilhas iguais de 255 restando uma moeda. Depois, colocou a moeda que restou na sua pilha e escondeu para si 256 moedas deixando apenas $255 \cdot 4 = 1020$ moedas no baú.

Capítulo 4

Aplicação em sala de aula e avaliação dos resultados

4.1 Minicurso Máximo Divisor Comum no 9º ano do Ensino Fundamental

Descreveremos agora uma aplicação em sala de aula de um minicurso sobre Máximo Divisor Comum. O objetivo deste minicurso, de cunho extracurricular, é averiguar a viabilidade da proposta em inserir o Lema de Euclides para o cálculo do MDC no Ensino Fundamental.

Para a aplicação do referido minicurso, foi pedida autorização da direção da escola Centro de Ensino Fundamental 405 do Recanto das Emas situada no Distrito Federal. Segundo dados da direção, a instituição de ensino funciona nos três turnos e atende alunos de baixa renda da zona urbana.

Após a autorização da direção, foi feito um convite informal aos alunos do 9º ano do Ensino Fundamental a participar do minicurso "Máximo Divisor Comum". Os alunos convidados já participavam espontaneamente de um grupo de estudos de matemática no contraturno. Dos 20 alunos convidados, 10 manifestaram vontade de participar do minicurso cuja duração seria de 6 horas/aula divididas em três encontros presenciais com 2 horas/aula.

Apesar de 10 alunos manifestarem a vontade de participar do minicurso, no dia do primeiro encontro compareceram apenas 3 alunos. Por respeitar o interesse dos alunos em participar do minicurso voluntariamente e sem o retorno de notas, o minicurso ocorreu normalmente com apenas 3 alunos apesar de meu orientador me informar que a quantidade de alunos seria inviável para avaliar a proposta.

Segue abaixo o plano do minicurso ministrado no 9º ano e também as avaliações aplicadas e os resultados obtidos em cada uma delas.

4.2 Plano de minicurso 9º ano

Conteúdo:

- Máximo Divisor Comum.

Objetivos gerais:

- Calcular Máximo Divisor Comum;
- Resolver situações-problema que envolvam o cálculo do Máximo Divisor Comum.

Objetivos específicos:

- Compreender o que é divisor de um número natural;
- Listar os divisores positivos de um número natural;
- Calcular o Máximo Divisor Comum através da listagem dos divisores;
- Calcular o Máximo Divisor Comum através da decomposição em fatores primos;
- Calcular o Máximo Divisor Comum através do Lema de Euclides;
- Calcular o Máximo Divisor Comum através do Algoritmo de Euclides;
- Resolver situações-problema que necessitem do cálculo do Máximo Divisor Comum.

Desenvolvimento:

Aula 1 (2 h):

- Aplicar a avaliação diagnóstica;
- Mostrar o que é divisor de um número natural;
- Exibir a listagem de divisores positivos de um número natural;
- Calcular o Máximo Divisor Comum através da listagem dos divisores;
- Calcular o Máximo Divisor Comum através da decomposição em fatores primos;
- Mostrar aplicações do Máximo Divisor Comum em situações-problema.

Aula 2 (2 h):

- Calcular o Máximo Divisor Comum através do Lema de Euclides;
- Calcular o Máximo Divisor Comum através do Algoritmo de Euclides.

- Mostrar aplicações do Máximo Divisor Comum em situações-problema.

Aula 3 (2 h):

- Revisar os assuntos estudados nas aulas anteriores;
- Aplicar a avaliação final.

Metodologia:

- Aulas expositivas dialogadas.

4.3 Avaliação diagnóstica 9º ano e resultados

1. Responda:
   (a) 5 é divisor de 15? Por quê?
   (b) 5 é divisor de 18? Por quê?
   (c) Você sabe o que é Máximo Divisor Comum? Se sim, explique.
2. Calcule:
   (a) $mdc(24, 30)$
   (b) $mdc(12, 40)$
   (c) $mdc(84, 150)$
   (d) $mdc(52, 91)$
3. Marque as frações irredutíveis. Justifique sua resposta.
   (a) ( ) $\frac{40}{48}$
   (b) ( ) $\frac{261}{319}$
4. Simplifique as frações até que se tornem irredutíveis:
   (a) $\frac{57}{190}$
   (b) $\frac{102}{136}$
   (c) $\frac{240}{600}$
   (d) $\frac{256}{392}$
5. Em uma escola havia duas turmas de 9º ano, a turma A com 28 alunos e a turma B com 36. Para a realização de uma gincana, cada turma foi dividida em grupos com o mesmo número de alunos, de forma que em cada grupo tivesse o maior número possível de alunos.

(a) Quantos alunos compõem cada grupo?

(b) Quantos grupos foram formados na turma A? E na turma B?

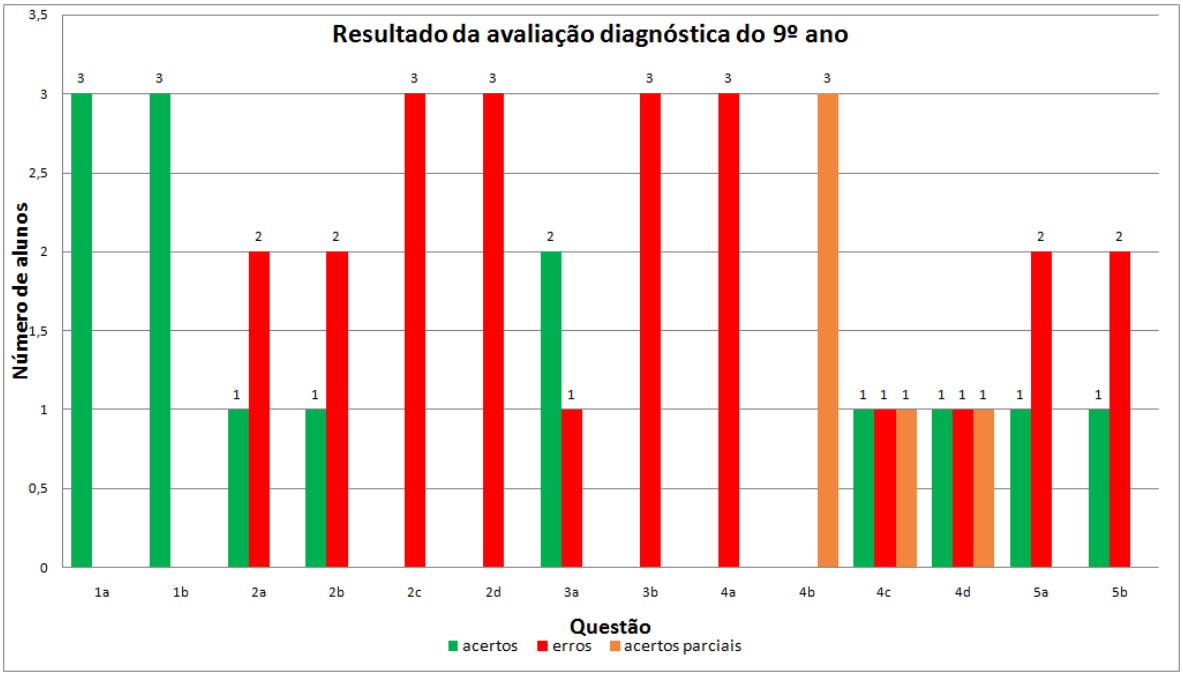

Figura 4.1: Resultado da Avaliação Diagnóstica do 9º ano

Todos os alunos responderam não saber o que é Máximo Divisor Comum apesar de o gráfico da figura 4.1 indicar que 100% dos alunos sabem o que é divisor. Como um dos alunos conseguiu calcular corretamente o $mdc(24, 30)$ e o $mdc(12, 40)$ verificamos que ele sabia do que se tratava apesar de não conseguir formular uma definição adequada.

Apenas um aluno calculou o $mdc(24, 30)$ e o $mdc(12, 40)$, que são cálculos relativamente simples. Este mesmo aluno respondeu que $mdc(84, 150) = 2$ e $mdc(52, 91) = 1$, ou seja, colocou um divisor como resposta porém não conseguiu encontrar o máximo. Isso nos mostra que lhe faltava técnicas que lhe facilitassem esses cálculos.

Os resultados obtidos na questão 3 mostram que a maioria dos alunos sabem o que é uma fração irredutível. A maioria respondeu que a fração $\frac{40}{48}$ não é irredutível pois pode ser simplificada, o que é correto, porém nenhum dos alunos respondeu que esta fração não é irredutível porque o $mdc(40, 48) = 8$, que seria a resposta mais formal. Todos alunos responderam que a fração $\frac{261}{319}$ é irredutível e justificaram dizendo que esta fração não poderia ser simplificada, o que está incorreto pois o $mdc(261, 319) = 29$ e, portanto, esta fração também não é irredutível. Observamos que, os alunos tiveram dificuldade de identificar o 29 como divisor de 261 e 319, provavelmente porque este número é primo.

Na questão 4, nenhum aluno conseguiu simplificar a fração $\frac{57}{190}$, provavelmente porque o $mdc(57, 190) = 19$. Todos simplificaram parcialmente a fração $\frac{102}{136}$ por 2, não identificando 17 como um divisor comum de 102 e 136. Notamos que 19 e 17 são números primos.

Apenas um aluno respondeu corretamente a questão 5. Isto demonstra que além de ter dificuldade com o conteúdo "Máximo Divisor Comum"os alunos também têm dificuldade na interpretação de problemas.

Observamos que na avaliação diagnóstica os alunos obtiveram 39,3% de aproveitamento. Porém, se desconsiderarmos a questão 1, para compararmos com a avaliação final, observamos um aproveitamento de apenas 29,2%.

4.4 Avaliação final 9º ano

1. Calcule:

   (a) $mdc(36, 60)$

   (b) $mdc(20, 32)$

   (c) $mdc(153, 221)$

   (d) $mdc(168, 224)$

2. Marque as frações irredutíveis. Justifique sua resposta.

   (a) ( ) $\frac{15}{29}$

   (b) ( ) $\frac{296}{629}$

3. Simplifique as frações até que se tornem irredutíveis:

   (a) $\frac{78}{260}$

   (b) $\frac{152}{266}$

   (c) $\frac{210}{700}$

   (d) $\frac{408}{456}$

4. Laura tem 28m de fita verde e 20m de fita amarela para decorar pacotes de presente. Ela quer cortar essas fitas de modo que os pedaços tenham o mesmo tamanho, que sejam o maior possível e que não haja sobras de fita.

   (a) Quantos metros deve ter cada pedaço de fita?

   (b) Quantos pedaços de fita verde foram cortados? E de fita vermelha?

5. Por qual método estudado você achou mais fácil o cálculo do máximo divisor comum?

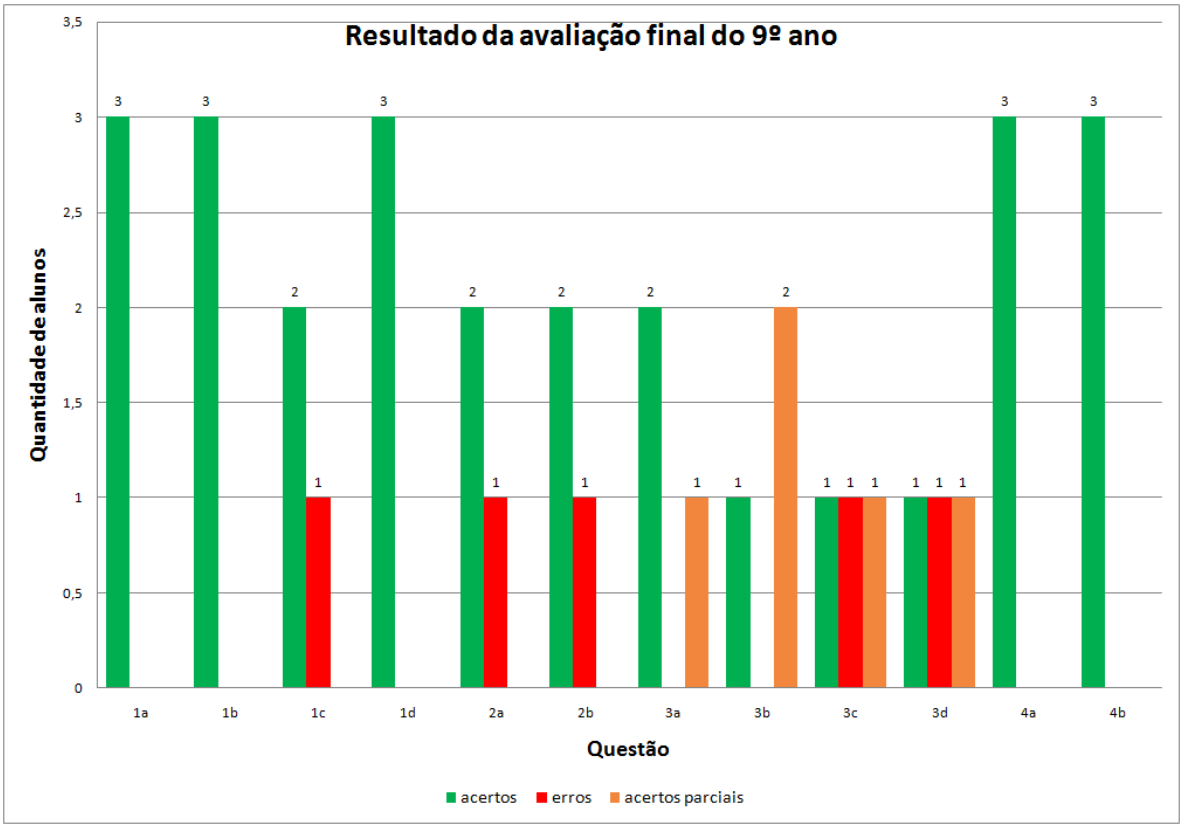

Figura 4.2: Resultado da avaliação final do 9º ano

Observando os dados da Figura 4.2 vemos que os alunos tiveram um aproveitamento de 79,2%, ou seja, comparando-se com a avaliação diagnóstica houve uma melhoria de 50% na compreensão do conteúdo.

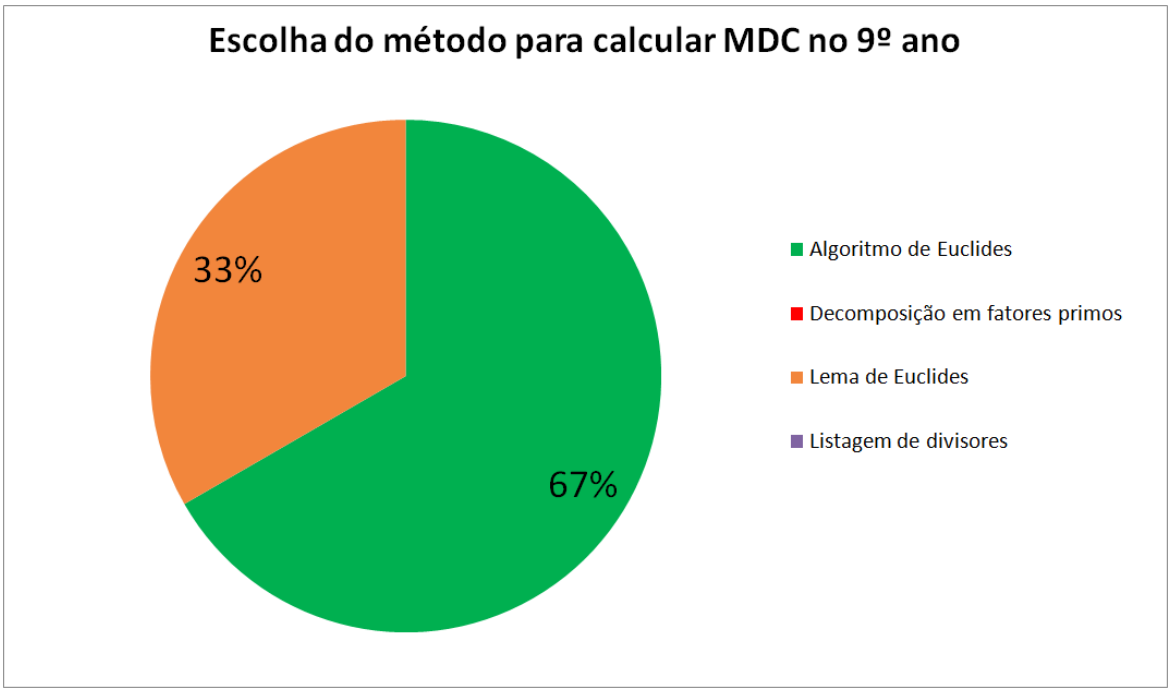

Figura 4.3: Escolha do método para calcular MDC no 9º ano

O gráfico da figura 4.3 mostra que 33% dos alunos acharam o cálculo do MDC pelo Lema de Euclides mais fácil que os outros métodos e 67% preferiram o Algoritmo de Euclides. Mesmo que apenas 3 alunos tenham sido analisados nesta amostra vemos que eles acharam estes métodos mais fáceis que os métodos que geralmente são adotados pelos livros didáticos e professores.

4.5 Minicurso Máximo Divisor Comum no 7º ano do Ensino Fundamental

Após relatar a direção da escola Centro de Ensino Fundamental 405 do Recanto das Emas sobre a dificuldade em avaliar o minicurso ocorrido no 9º ano por causa da pouca quantidade de alunos, eles me informaram que havia uma turma de 7º ano com 34 alunos disponível durante uma semana (6 aulas de 45 minutos) por conta do afastamento da professora regente da turma. Então, aplicamos o mesmo minicurso ofertado ao 9º ano com algumas adequações para a série destes alunos e para o tempo disponível. Porém, neste caso, a participação dos alunos não foi opcional já que eles estavam em horário de aula.

Foram consideradas as avaliações de 30 alunos pois, 4 alunos faltaram algumas aulas do minicurso.

Segue abaixo o plano do minicurso ministrado no 7º ano e também as ava-

liações aplicadas e os resultados obtidos em cada uma delas.

4.6 Plano de minicurso 7º ano

Conteúdo:

- Máximo Divisor Comum.

Objetivos gerais:

- Calcular Máximo Divisor Comum;
- Resolver situações-problema que envolvam o cálculo do Máximo Divisor Comum.

Objetivos específicos:

- Compreender o que é divisor de um número natural;
- Listar os divisores positivos de um número natural;
- Calcular o Máximo Divisor Comum através da listagem dos divisores;
- Calcular o Máximo Divisor Comum através da decomposição em fatores primos;
- Calcular o Máximo Divisor Comum através do Lema de Euclides;
- Calcular o Máximo Divisor Comum através do Algoritmo de Euclides;
- Resolver situações-problema que necessitem do cálculo do Máximo Divisor Comum.

Desenvolvimento:

Aula 1 (45 min):

- Aplicar a avaliação diagnóstica.

Aula 2 (1 h 30 min):

- Mostrar o que é divisor de um número natural;
- Exibir a listagem de divisores positivos de um número natural;
- Calcular o Máximo Divisor Comum através da listagem dos divisores;
- Calcular o Máximo Divisor Comum através da decomposição em fatores primos;
- Mostrar aplicações do Máximo Divisor Comum em situações-problema.

Aula 3 (45 min):

- Calcular o Máximo Divisor Comum através do Lema de Euclides;
- Mostrar aplicações do Máximo Divisor Comum em situações-problema.

Aula 4 (45 min):

- Calcular o Máximo Divisor Comum através do Algoritmo de Euclides.
- Mostrar aplicações do Máximo Divisor Comum em situações-problema.

Aula 5 (45 min):

- Aplicar a avaliação final.

Metodologia:

- Aulas expositivas dialogadas.

4.7 Avaliação Diagnóstica 7º ano

1. Responda:
   (a) 5 é divisor de 15? Por quê?
   (b) 5 é divisor de 18? Por quê?
   (c) Você sabe o que é máximo divisor comum? Se sim, explique.
2. Calcule:
   (a) $mdc(30, 48)$
   (b) $mdc(52, 91)$
3. Simplifique as frações até que se tornem irredutíveis:
   (a) $\frac{51}{68}$
   (b) $\frac{210}{336}$
4. Em uma escola havia duas turmas de 7º ano, a turma A com 28 alunos e a turma B com 36. Para a realização de uma gincana, cada turma foi dividida em grupos com o mesmo número de alunos, de forma que em cada grupo tivesse o maior número possível de alunos.
   (a) Quantos alunos compõem cada grupo?

(b) Quantos grupos foram formados na turma A? E na turma B?

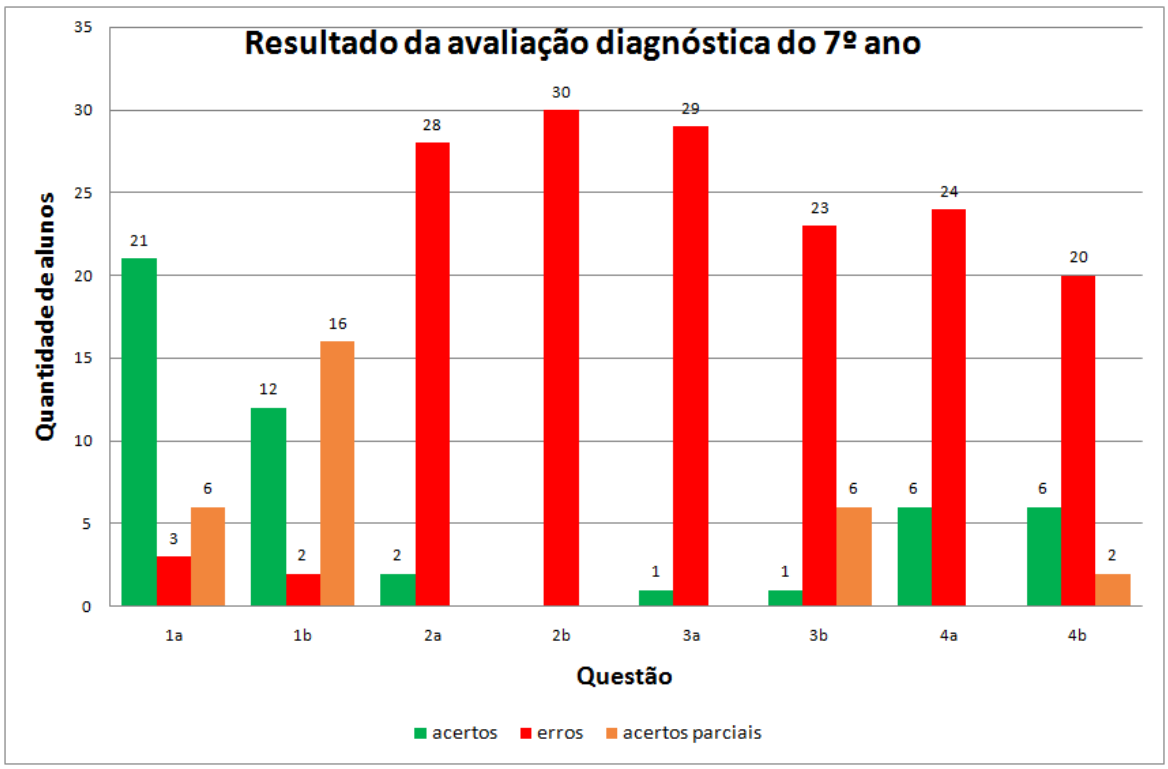

Figura 4.4: Resultado da Avaliação Diagnóstica do 7º ano

Observamos que na avaliação diagnóstica os alunos obtiveram 26,7% de aproveitamento. Porém, se desconsiderarmos a questão 1, para compararmos com a avaliação final, observamos um aproveitamento de apenas 11,1%.

No item (c) da questão 1, 11 alunos responderam saber o que é Máximo Divisor Comum, porém nenhum aluno conseguiu formular uma definição adequada, o que mostra que os alunos não têm conhecimento sobre o conteúdo apesar de afirmar o contrário. Pelos itens (b) e (c) da mesma questão, observamos que a maioria dos alunos sabe o que é divisor porém, pelo baixo aproveitamento nas questões posteriores vemos que eles apenas sabem verificar se um número é divisor de outro e não sabem encontrar todos os divisores positivos de um número.

Apenas 2 alunos calcularam corretamente o $mdc(30, 48)$, apesar de ser um cálculo relativamente fácil que não necessite de técnicas elaboradas. Nenhum aluno soube calcular o $mdc(52, 91)$ que é 13.

Apenas 1 aluno conseguiu simplificar corretamente as duas frações da questão 3 e 6 alunos conseguiram simplificar a fração do item (b) desta mesma questão, apesar de não deixá-la irredutível. Observamos que os alunos que simplificaram parcialmente o item (b) da questão 3 encontraram as frações $\frac{105}{168}$, $\frac{70}{112}$ ou $\frac{35}{56}$, ou seja simplificaram

por 2, 3 ou por 6 respectivamente. Portanto, nenhum destes alunos simplificou esta fração por 7, o que mostra que os alunos têm dificuldade na compreensão da tabuada de multiplicação do 7, ou porque os critérios de divisibilidade por 7 sejam mais complexos e por isso os alunos não identificam facilmente se 7 é um divisor possível. De qualquer forma, observamos que a maioria dos alunos só encontraram divisores cujos critérios de divisibilidade são muito fáceis.

6 alunos responderam corretamente a questão 4, o que mostra que ao lidar com objetos palpáveis e cotidianos os alunos têm uma compreensão melhor do problema, apesar de representarem apenas 20% da turma. 2 alunos acertaram parcialmente o item (b) da questão 4 e erraram o restante da questão. Por acreditarmos que o acertar o item (b) depende de acertar o item (a), este acerto parcial parece ter sido ao acaso.

Portanto, pelo baixo desempenho na avaliação concluímos que os alunos têm dificuldade em calcular o MDC por métodos tradicionais e que por esses métodos é mais complicado calcular o MDC quando o MDC tem fatores primos diferentes de 2, 3 e 5.

4.8 Avaliação final 7º ano

1. Calcule:
   (a) $mdc(36, 60)$
   (b) $mdc(69, 115)$
2. Simplifique as frações até que se tornem irredutíveis:
   (a) $\frac{76}{133}$
   (b) $\frac{84}{112}$
3. Laura tem 28m de fita verde e 20m de fita amarela para decorar pacotes de presente. Ela quer cortar essas fitas de modo que os pedaços tenham o mesmo tamanho, que sejam o maior possível e que não haja sobras de fita.
   (a) Quantos metros deve ter cada pedaço de fita?
   (b) Quantos pedaços de fita verde foram cortados? E de fita vermelha?
4. Por qual método estudado você achou mais fácil o cálculo do máximo divisor comum?

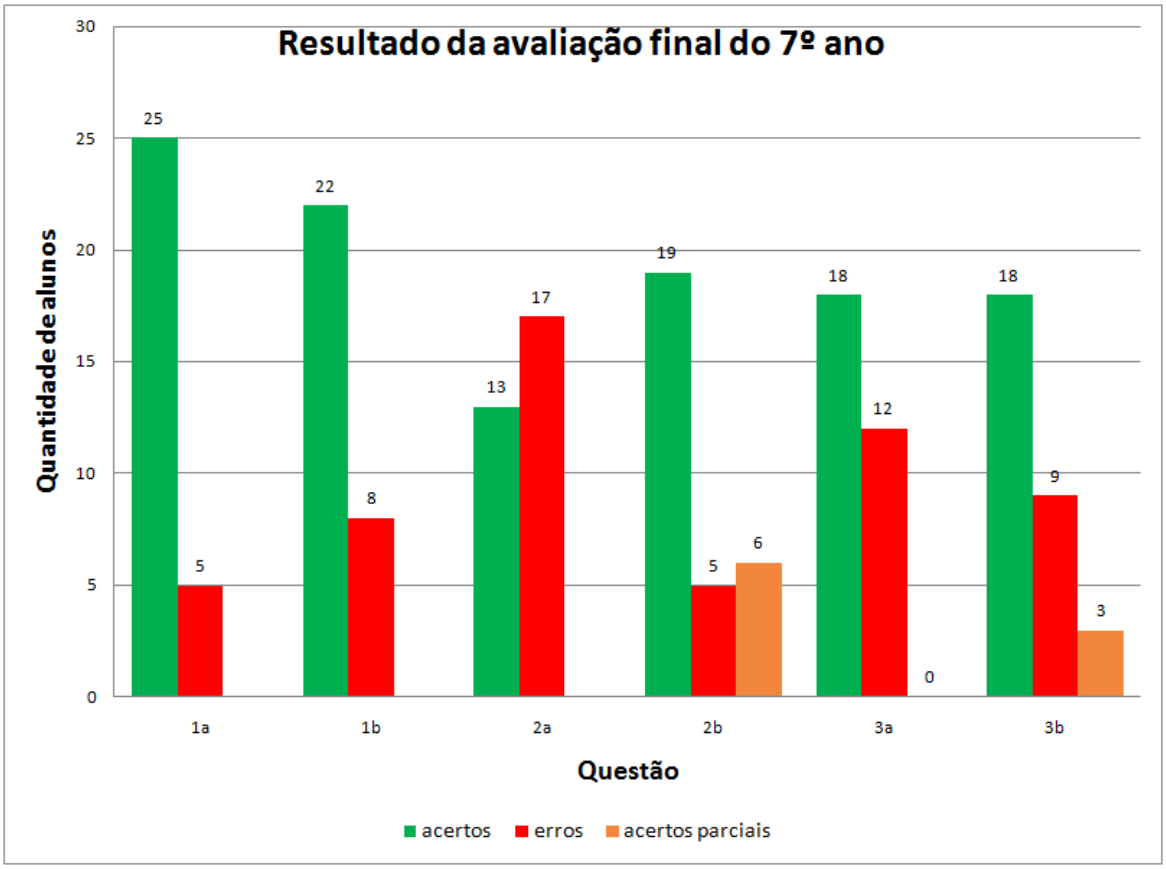

Figura 4.5: Resultado da avaliação final do 7º ano

Observando os dados da Figura 4.5 vemos que os alunos tiveram um aproveitamento de 66,4%, ou seja, comparando-se com a avaliação diagnóstica houve uma melhoria de 55,3% na compreensão do conteúdo.

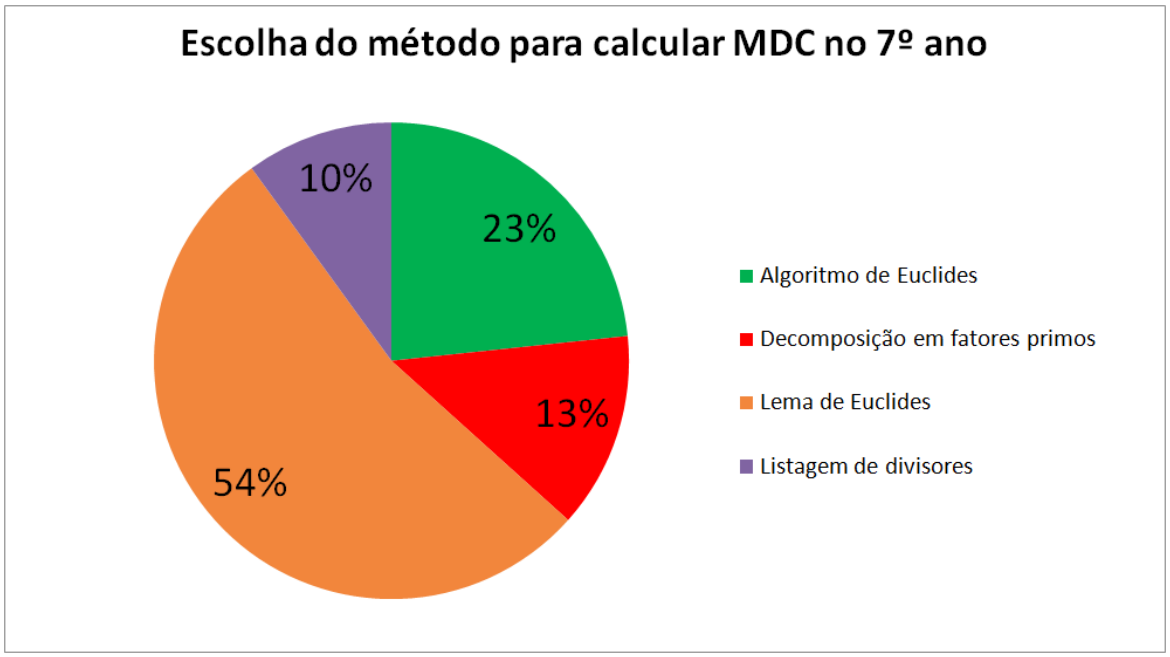

Figura 4.6: Escolha do método para calcular MDC no 7º ano

O gráfico da figura 4.6 mostra que 54% dos alunos acharam o cálculo do MDC pelo Lema de Euclides mais fácil que os outros métodos. Além disso, observamos que 23% consideram o Algoritmo de Euclides o método mais fácil, ou seja, 77% da turma escolheu métodos que geralmente não são adotados nos livros didáticos ou pelos professores.

Portanto, os resultados obtidos demonstram que, mesmo que a amostra de alunos seja baixa para dados estatísticos, ensinar o cálculo do MDC pelo Lema de Euclides é viável no Ensino Fundamental.

Considerações finais

Acreditamos que o tempo dedicado a escrita desta dissertação tenha contribuído de forma significativa e relevante para nossa prática docente, principalmente para trabalhar com o ensino da Aritmética tanto no Ensino Fundamental como no Ensino Médio.

Os resultados obtidos na avaliação diagnóstica aplicada no minicurso Máximo Divisor Comum mostram que os alunos não conseguiam calcular MDC entre dois números naturais, simplificar frações por números primos maiores que 5 e resolver problemas envolvendo o cálculo do MDC. Também ficou evidente que os métodos para o cálculo do MDC abordados pela maioria dos livros didáticos e professores não facilitaram o processo da compreensão do conteúdo já que os alunos têm extrema dificuldade na divisão e na decomposição em fatores primos.

Durante a aplicação do minicurso averiguamos que a aceitação ao Lema de Euclides e ao Algoritmo de Euclides como métodos para calcular o MDC foi muito grande, os alunos chegaram a questionar o motivo desses métodos não serem ensinados anteriormente. O aproveitamento obtido na avaliação final nos mostra que a compreensão do conteúdo melhorou consideravelmente. Ao questionarmos qual o método mais fácil para o cálculo do MDC na turma de 7º ano do Ensino Fundamental que participou do minicurso, 54% dos alunos escolheram o Lema de Euclides e 23% escolheram o Algoritmo de Euclides, ou seja, 77% dos alunos escolheram métodos que geralmente não são ensinados em sala de aula.

Portanto, acreditamos que o Lema de Euclides deveria ser ensinado no Ensino Fundamental como método para cálculo do Máximo Divisor Comum.

Referências Bibliográficas

[1] Alencar Filho, Edgar de, *Teoria elementar dos números*, Rio de Janeiro: Sociedade Brasileira de Matemática, 2ª ed. (2005).

[2] Dante, Luiz Roberto, *Projeto Teláris: Matemática / Luiz Roberto Dante*, São Paulo: Ática, 1ª ed. (2012).

[3] Giovanni, José Ruy, *Aprendendo matemática / José Ruy Giovanni, Eduardo Parente*, São Paulo: FTD, ed. renovada. (2007).

[4] Gonçalves, Adilson, *Introdução à álgebra*, Rio de Janeiro: Instituto de Matemática Pura e Aplicada (1979).

[5] Hefez, Abramo, *Elementos de Aritmética*, São Paulo: Nobel, 2ª ed. (1985).

[6] Salahoddin Shokranian, Marcus Soares, Hemar Godinho, *Teoria de números*, Brasília: Universidade de Brasília, 2ª ed. (1999).

[7] Santos, José Plínio de Oliveira, *Introdução à Teoria de Números*, Rio de Janeiro, Instituto de Matemática Pura e Aplicada, CNPq (1998).

[8] Souza, Joamir Roberto de, *Vontade de saber matemática, 6º ano / Joamir Roberto de Souza, Patricia Rosana Moreno Pataro*, São Paulo: FTD, 2ª ed. (2012).