



**UNIVERSIDADE DA INTEGRAÇÃO INTERNACIONAL DA LUSOFONIA
AFRO-BRASILEIRA
INSTITUTO DE CIÊNCIAS EXATAS E DA NATUREZA
PROGRAMA DE MESTRADO PROFISSIONAL
EM MATEMÁTICA EM REDE NACIONAL**

ANTONIO CARLOS PEREIRA DE FREITAS

TEOREMA FUNDAMENTAL DA ARITMÉTICA E APLICAÇÕES

REDENÇÃO

2023

ANTONIO CARLOS PEREIRA DE FREITAS

TEOREMA FUNDAMENTAL DA ARITMÉTICA E APLICAÇÕES

Dissertação apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional da Universidade da Integração Internacional da Lusofonia Afro Brasileira, como parte dos requisitos necessários para a obtenção do título de mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. Joserlan Perote da Silva

REDENÇÃO

2023

Universidade da Integração Internacional da Lusofonia Afro-Brasileira
Sistema de Bibliotecas da UNILAB
Catalogação de Publicação na Fonte.

Freitas, Antonio Carlos Pereira de.

F866t

Teorema fundamental da aritmética e aplicações / Antonio Carlos Pereira de Freitas. - Redenção, 2023.
106fl: il.

Dissertação - Curso de , Mestrado Profissional em Matemática em Rede Nacional, Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Redenção, 2023.

Orientador: Prof. Dr. Joserlan Perote da Silva.

1. Aritmética - Estudo e ensino. 2. Aplicações. 3. Irrracionalidade. 4. Criptografia. I. Título

CE/UF/BSCA

CDD 512

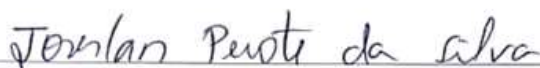
ANTONIO CARLOS PEREIRA DE FREITAS

TEOREMA FUNDAMENTAL DA ARITMÉTICA E APLICAÇÕES

Dissertação apresentada como requisito para obtenção do título de Mestre em Matemática, na Universidade da Integração Internacional da Lusofonia Afro-Brasileira, UNILAB - Campus Auroras.

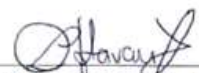
Aprovada em: 24/08/2023.

BANCA EXAMINADORA



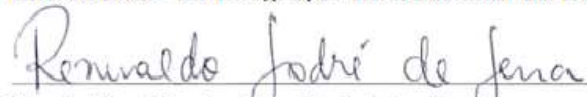
Prof. Dr. Joserlan Perote da Silva (Orientador)

Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)



Prof.ª Dra. Danila Fernandes Tavares

Universidade da Integração Internacional da Lusofonia Afro-Brasileira (UNILAB)



Prof. Dr. Renivaldo Sodré de Sena

Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

Dedico este trabalho a meus pais, especialmente a minha mãe que sempre foi minha maior apoiadora na minha caminhada acadêmica.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, por ter me concedido a realização de mais um sonho.

À CAPES, pelo apoio financeiro com a manutenção da bolsa de auxílio.

Ao Prof. Dr. Joserlan Perote da Silva, por ter aceitado de imediato o convite para a minha orientação e pela paciência que sempre teve diante de minhas dificuldades. Pelas sugestões, por todas as contribuições. Agradeço pela excelente orientação.

Aos professores participantes da banca examinadora Danila Fernandes Tavares e Renivaldo Sodré de Sena pelo aceite ao convite, pela disponibilidade de seu tempo e pelas valiosas contribuições.

Aos professores que lecionaram as disciplinas da grade curricular, Rodrigo Pereira (Matemática Discreta, Números e funções reais), João Francisco (Aritmética, Resolução de Problemas), Danila Fernandes (Geometria, Resolução de problemas), Amanda Angélica (Fundamentos de Calculo), Antonio Alisson (Recursos Computacionais no Ensino de Matemática), Geometria Analítica (Wesley Marinho), Marcelo Dário (Tópicos de Historia da Matemática), Rafael Diógenes (Resolução de Problemas) e mais uma vez Joserlan Perote (Resolução de Problemas). A eles agradeço pelos ensinamentos e pela paciência e entendimento diante de nossas dificuldades.

Aos colegas da turma de mestrado (Ênio, Naiara, Davi, Arthur, Jeferson torres, Jeferson Mascarenha, Fábio, Alneir, Edvan, Ricardo, Joabe, Paulo Cesar, José Cordeiro, Marcos Aurélio, Márcio de Lacerda), que estavam sempre dispostos a ajudar diante das dificuldades que surgiram, formaram uma verdadeira família.

E por fim a minha família, que sempre me apoiou na minha formação acadêmica.

“Deus criou os inteiros; todo o resto é trabalho do homem.” Leopold Kronecker

RESUMO

Neste trabalho, apresentamos o Teorema Fundamental da Aritmética e aplicações. Iniciamos apresentando os conteúdos básicos necessários para a compreensão do Teorema Fundamental da Aritmética e o conhecimento necessário para entender as suas aplicações. No Teorema Fundamental da Aritmética é apresentado um breve contexto histórico do Teorema Fundamental da Aritmética, é enunciado e provado usando o princípio da indução matemática e é apresentado aplicações que são consequências imediatas do teorema como: reformulação do Teorema de Euler, encontrar a forma do divisor de um número natural, a contagem dos divisores de um número natural, a somar e multiplicar os divisores de um número natural, calcular o MMC e o MDC conhecendo a forma fatorada do número natural. Apresentamos também algumas aplicações não imediatas do teorema como: determinar os fatores do fatorial de um número natural, determinar qual o menor inteiro deve-se multiplicar ou dividir a $\sqrt[n]{a}$, com $a \in \mathbb{N}$, para ter como resultado um inteiro positivo, provar a irracionalidade de $\sqrt[n]{p}$, com p primo, e a irracionalidade de $\sqrt[n]{p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}}$ onde, $m_i < n$ para $i = \{1, 2, 3, \dots, r\}$ e p_i para $i = 1, 2, 3, \dots, r$ primos; provar a irracionalidade do $\log 2$, mostrar uma relação entre coeficientes primos distintos de uma equação do 2^{o} grau e raiz dupla, mostrar que alguns polinômios especiais não podem ter raízes inteiras positivas e por fim mostrar como funciona o processo de criptografia RSA e, na última sessão apresentamos as conclusões finais.

Palavras-chave: Teorema Fundamental da Aritmética. Aplicações. Irracionalidade. Criptografia RSA.

ABSTRACT

In this work, we present the Fundamental Theorem of Arithmetic and applications. We begin by presenting the basic contents needed to understand the Fundamental Theorem of Arithmetic and the knowledge needed to understand its applications. In the Fundamental Theorem of Arithmetic a brief historical context of the Fundamental Theorem of Arithmetic is presented, it is stated and proved using the principle of mathematical induction and applications are presented that are immediate consequences of the theorem such as: reformulation of Euler's Theorem, finding the form of the divisor of a natural number, counting the divisors of a natural number, adding and multiplying the divisors of a natural number, calculating the MMC and GDC knowing the factored form of the natural number. We also present some non-immediate applications of the theorem such as: determining the factorial factors of a natural number, determining which is the smallest integer to multiply or divide $\sqrt[n]{a}$, with $a \in \mathbb{N}$, to get a positive integer as result, prove the irrationality of $\sqrt[n]{p}$, with p prime, and the irrationality of $\sqrt[n]{p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}}$ where, $m_i < n$ for $i = \{1, 2, 3, \dots, r\}$ and p_i for $i = 1, 2, 3, \dots, r$ primes; prove the irrationality of $\log 2$, show a relationship between distinct prime coefficients of a 2nd degree equation and double root, show that some special polynomials cannot have positive integer roots and finally show how the RSA cryptography process works and, in the last session we present the final conclusions.

Keywords: Fundamental Theorem of Arithmetic. Applications. Irrationality. RSA encryption.

LISTA DE FIGURAS

Figura 1 – Euclides de Alexandria	69
Figura 2 – Euler	70
Figura 3 – Adrien-Marie Legendre (1752-1833)	71
Figura 4 – Johann Carl Friedrich Gauss	72

LISTA DE TABELAS

Tabela 1 – Diagrama do MDC de a e b	40
Tabela 2 – Elementos organizados em n colunas, com m elementos em cada.	58
Tabela 3 – Primos menores que 150	61
Tabela 4 – Tabela de pré-codificação	93
Tabela 5 – Blocos escolhidos	93

LISTA DE ABREVIATURAS E SIGLAS

MDC	Máximo Divisor Comum
MMC	Mínimo Múltiplo Comum
ENQ	Exame Nacional de Qualificação.
ENA	Exame Nacional de Acesso
RPM	Revista do Professor de Matemática
TFA	Teorema Fundamental da Aritmética
BNCC	Base Nacional Comum Curricular
OBM	Olimpíada Brasileira de Matemática
PCN's	Parâmetros Curriculares Nacionais
ENEM	Exame Nacional do Ensino Médio

SUMÁRIO

1	INTRODUÇÃO	14
2	PRELIMINARES	16
2.1	PRINCÍPIO DA BOA ORDENAÇÃO	16
2.2	PRINCÍPIO DA INDUÇÃO MATEMÁTICA	17
2.3	DIVISIBILIDADE E PROPRIEDADES BÁSICAS	19
2.4	ALGORITMO DA DIVISÃO DE EUCLIDES	24
2.5	SISTEMA DE NUMERAÇÃO DECIMAL	29
2.6	MÁXIMO DIVISOR COMUM	32
2.7	O TEOREMA DE ÉTIENNE BÉZOUT	33
2.8	ALGORITMO DE EUCLIDES PARA O CÁLCULO DO MÁXIMO DIVISOR COMUM	38
2.9	ALGORITMO DE EUCLIDES ESTENDIDO	41
2.10	MÍNIMO MÚLTIPLO COMUM	43
3	RESULTADOS AUXILIARES	45
3.1	EQUAÇÕES DIOFANTINAS LINEARES	45
3.2	ARITMÉTICA MODULAR	49
3.3	NÚMEROS PRIMOS	59
3.4	O TEOREMA DE EULLER E PEQUENO TEOREMA DE FERMAT	65
4	TEOREMA FUNDAMENTAL DA ARITMÉTICA	68
4.1	CONTEXTO HISTÓRICO	68
4.2	TEOREMA FUNDAMENTAL DA ARITMÉTICA	73
4.3	REFORMULAÇÃO DO TEOREMA DE EULLER	75
4.4	OS DIVISORES DE UM NÚMERO NATURAL	76
4.5	QUANTIDADE DE DIVISORES DE UM NÚMERO NATURAL	77
4.6	A SOMA DOS DIVISORES DE UM NÚMERO NATURAL	80
4.7	O PRODUTO DOS DIVISORES DE UM NÚMERO NATURAL	82
4.8	MÁXIMO DIVISOR COMUM E MÍNIMO MÚLTIPLO COMUM DE UM NÚMERO NATURAL	83
5	APLICAÇÕES DO TEOREMA FUNDAMENTAL DA ARITMÉTICA	84
5.1	VERIFICAR SE $\sqrt[n]{a}$ É UM NÚMERO INTEIRO POSITIVO	84
5.2	FATORES DO FATORIAL	85
5.3	A IRRACIONALIDADE DE $\sqrt[n]{p}$ COM $p, n \in \mathbb{N}, n > 1$ E p PRIMO	86
5.4	A IRRACIONALIDADE DE $\sqrt[n]{p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}}$ COM, $m_i < n$ PARA $i = \{1, 2, 3, \dots, r\}$	87
5.5	A IRRACIONALIDADE DO $\log 2$	88

5.6	CONDIÇÃO SOBRE OS TERMOS DO LOGARITMO PARA $\log_a b$ SER IRRACIONAL.	89
5.7	RELAÇÃO ENTRE COEFICIENTES PRIMOS DISTINTOS DE UMA EQUAÇÃO DO 2º GRAU E RAÍZES DUPLAS.	89
5.8	APLICAÇÕES EM POLINÔMIOS ESPECIAIS	90
5.9	CRIPTOGRAFIA	90
6	CONCLUSÃO	102
	REFERÊNCIAS	104

1 INTRODUÇÃO

Na disciplina de aritmética tive contato com o Teorema Fundamental da Aritmética de forma mais profunda, me chamou a atenção as suas aplicações, pois percebi que já usava esse teorema com os meus alunos do ensino fundamental de forma mecânica, com o cálculo de *MMC* e *MDC*, então a partir dali resolvi escrever sobre esse importante teorema da aritmética e suas aplicações.

Os professores que trabalham com a disciplina de matemática, tem como principal objetivo trabalhar os conteúdos de forma a relacioná-los com problemas de nossa vivência diária, pois um dos fatores que levam os alunos a não se interessarem pela disciplina é a forma abstrata de seus conteúdos. Para os alunos a matemática não tem relação com as coisas do dia a dia, o que mostra que estão bastante enganados pois a mesma é de fundamental importância para o desenvolvimento de nosso raciocínio lógico dedutivo, e é responsável pelo desenvolvimento da física, da computação, da química, da biologia. A matemática é responsável pelo desenvolvimento da sociedade, pois é devido a aplicações de seus conteúdos nos mais variados campos do conhecimento que temos as mordomias da vida moderna.

Com o objetivo de trazer o interesse do aluno para a disciplina, com relação ao Teorema Fundamental da Aritmética, o trabalho mostra aplicações práticas do teorema na vida real e aplicações relacionadas a outros conteúdos que podem ajudar em outras demonstrações de problemas relacionados a outros ramos da matemática.

No segundo e no terceiro capítulo encontram-se os conhecimentos básicos necessários para enunciar e provar o Teorema Fundamental da Aritmética além dos conhecimentos necessários para a compreensão de suas aplicações.

No quarto capítulo é apresentado um breve contexto histórico do TFA, quando e onde surgiu, quais os matemáticos que o usaram de forma parcial e quem o demonstrou pela primeira vez de forma completa, mostrando a sua existência e unicidade. Nele é enunciado e provado o Teorema Fundamental da Aritmética, usando o princípio da indução matemática. Também é mostrado no capítulo, aplicações que são consequências imediatas do Teorema Fundamental da Aritmética, como: a forma do divisor de um número natural, a quantidade de divisores de um número natural, a soma e o produto dos divisores de um número natural, o máximo divisor comum e o mínimo múltiplo comum de um número natural.

No quinto capítulo é apresentada uma série de aplicações do TFA, como: verificar em que situações a radiciação em que o radicando é um número natural representa um número natural, calcular os fatores do fatorial, provar a irracionalidade de $\sqrt[n]{p}$, com $p, n \in \mathbb{N}$, $n > 1$ e p primo, e a irracionalidade de $\sqrt[n]{p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}}$ com, $m_i < n$ para $i = \{1, 2, 3, \dots, r\}$, a irracionalidade do $\log 2$, condição sobre os termos do logaritmo para $\log_a b$ ser irracional, relação entre coeficientes primos inteiros e raiz dupla, aplicações em

polinômios especiais e encerramos o capítulo com a aplicação mais prática e importante do TFA na criptografia RSA, um dos métodos mais usados até os dias atuais para criptografar mensagens e que aliado ao uso de computadores é uma ferramenta de fundamental importância para que haja segurança em tarefas que se tornaram básicas em nosso dia a dia, como realizar compras pela internet, realizar transações bancárias, trocar mensagens, fotos e vídeos por aplicativos de conversas como *whatsapp*, *telegram*, *facebook*, *intagram* entre outros.

Precisava organizar em um trabalho as aplicações desse teorema para que outros professores, e mesmo alunos possam ter reunido algumas das aplicações desse teorema, para enriquecer os seus estudos e ter mais uma alternativa para planejar e estudar para as suas aulas.

2 PRELIMINARES

Neste capítulo serão apresentadas as definições, propriedades, axiomas, proposições, lemas, corolários, teoremas e demonstrações de resultados que serão necessários para o desenvolvimento do resultado principal desse trabalho: o Teorema Fundamental da Aritmética e suas aplicações.

Serão apresentados: O princípio da boa ordenação (*PBO*), o princípio da indução finita, conceito e propriedades de divisibilidade, o algoritmo da divisão de Euclides, sistema de numeração, teorema de Bézout, conceitos, propriedades e definição de máximo divisor comum, mínimo múltiplo comum e Lema de Euclides. Esses resultados serão ferramentas importantes para resolver equações diofantina lineares e desenvolver as propriedades básicas de aritmética modular, para conhecer os teoremas de Euler e pequeno teorema de Fermat, que serão apresentados no capítulo seguinte.

O objetivo do capítulo Preliminares e Resultados Auxiliares é fazer com que o leitor tenha todas as ferramentas necessárias para a compreensão de todas as passagens do trabalho apresentado.

2.1 PRINCÍPIO DA BOA ORDENAÇÃO

Começemos com um axioma que servirá como base para boa parte das demonstrações de teoremas e proposições que será essencial para o desenvolvimento dos resultados que envolvem divisibilidade, o princípio da boa ordenação (*PBO*).

Axioma: Princípio da Boa Ordenação (*PBO*): Se $A \subseteq \mathbb{N}$ é um subconjunto não vazio de $\mathbb{N}$, então A possui um menor elemento, ou seja, existe um $n_0 \in A$ tal que $n_0 \leq x$, para todo x de A .

Do axioma podemos demonstrar muitas proposições e corolários básicos, entre elas as apresentadas e demonstradas abaixo. Segundo Hefez (2016), este é o único axioma que faltava para caracterizar os números inteiros. Vejamos algumas proposições que podem ser provadas de forma direta com o princípio da boa ordenação.

Proposição 2.1. *Não existe nenhum número inteiro n tal que $0 < n < 1$.*

Demonstração: Suponha que exista n com a propriedade mencionada. Logo, o conjunto

$$S = \{n \in \mathbb{Z}; 0 < n < 1\}$$

é não vazio e limitado inferiormente por 0, logo, pelo princípio da boa ordenação S possui um elemento mínimo a_0 com $0 < a_0 < 1$.

Multiplicando a desigualdade por $a_0 > 0$ teremos que:

$$0 < a_0^2 < a_0 < 1.$$

Como $a_0^2 \in S$ e é menor que o elemento mínimo a_0 , temos uma contradição. Portanto a suposição inicial é falsa, logo $S = \emptyset$, como queríamos demonstrar. ■

Corolário 2.1. *Dado um número inteiro a qualquer, não existe nenhum número inteiro b , tal que $a < b < a + 1$.*

Demonstração: Suponha que exista b satisfazendo $a < b < a + 1$, subtraindo a de ambos os membros da desigualdade, teremos:

$$a - a < b - a < a + 1 - a \implies 0 < b - a < 1.$$

Um absurdo pela proposição (2.1). ■

2.2 PRINCÍPIO DA INDUÇÃO MATEMÁTICA

Um resultado que será bastante utilizado em muitas das demonstrações e que segundo Hefez (2016) é uma das mais importantes consequências do princípio da boa ordenação é o princípio de indução matemática, que está baseado no quarto axioma de Peano. O apresentaremos como teorema, e também pode ser encontrado em algumas literaturas como o princípio da indução finita (*PIF*). Para um maior aprofundamento, consulte Carvalho e Morgado (2015).

Pode-se apresentar o princípio de indução matemática de duas formas, como enunciadas e demonstradas a seguir:

Teorema 2.1 (princípio de indução matemática). *Seja $A \subseteq \mathbb{N}$, tal que:*

- i) $1 \in A$;*
- ii) Se $k \in A \implies (k + 1) \in A$, então $A = \mathbb{N}$.*

Demonstração: Defina o conjunto $S = \mathbb{N} - A$, queremos mostrar que $A = \mathbb{N}$, ou seja $S = \emptyset$. Vamos supor por absurdo que $S \neq \emptyset$, assim, pelo princípio da boa ordenação S possui um elemento mínimo $n_0 \in S$ com $n_0 \neq 1$, pois $1 \in A$.

Dessa forma o elemento $n_0 - 1 \notin S \implies n_0 - 1 \in A$ e pela segunda parte do princípio de indução, $n_0 - 1 + 1 \in A \implies n_0 \in A$, chegando assim a um absurdo, pois $n_0 \in S$. Como os conjuntos A e S são complementares ($A \cap S = \emptyset$), logo $A = \mathbb{N}$. Como queríamos demonstrar. ■

Teorema 2.2 (princípio de indução matemática 2ª forma). *Seja $A \subseteq \mathbb{N}$, tal que:*

- i) $1 \in A$;*
- ii) Se $1, 2, 3, \dots, k \in A \implies (k + 1) \in A$, então $A = \mathbb{N}$.*

Demonstração: Suponhamos por absurdo que $A \neq \mathbb{N}$, logo o conjunto $X = \mathbb{N} - A$ é um subconjunto não vazio dos naturais, logo pelo princípio da boa ordenação o subconjunto X possui um elemento mínimo que chamaremos de j , com $j > 1$, pois pela condição (1), $1 \in A$. Dessa forma os elementos $1, 2, \dots, j - 1$ pertencem ao conjunto A . Pela condição (2) o elemento $(j - 1) + 1 \in A \implies j \in A$, o que é uma contradição pois $j \in X$. Dessa

forma $A = \mathbb{N}$, como queríamos demonstrar. ■

Para uma melhor compreensão dos resultados apresentados vejamos a solução dos exemplos abaixo.

Exemplo 2.1. Mostrar por indução que:

$$1^1 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Solução: (Caso base) Temos que, para $n = 1$, fica:

$$1^2 = \frac{1 \cdot (1+1) \cdot (2 \cdot 1+1)}{6} = 1.$$

(Hipótese de indução) Suponhamos que vale para algum $n > 1$ com $n \in \mathbb{N}$, ou seja,

$$1^1 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

(Tese) Devemos mostrar que vale para $n+1$, ou seja,

$$1^1 + 2^2 + \dots + n^2 + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}.$$

Temos pela hipótese de indução que:

$$1^1 + 2^2 + \dots + n^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2.$$

Portanto:

$$\begin{aligned} 1^1 + 2^2 + \dots + n^2 + (n+1)^2 &= \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{(n+1)(2n^2 + 7n + 6)}{6} \\ &= \frac{(n+1)(n+2)(2n+3)}{6}. \end{aligned}$$

E isso conclui a nossa prova. Logo a sentença é válida para todo $n \in \mathbb{N}$.

Exemplo 2.2. Mostrar por indução que:

$$1 + 3 + 5 + \dots + (2n-1) = n^2.$$

Solução: Usando indução, temos que:

(Caso base) Para $n = 1$, teremos que $1 = 1^2 = 1$. Logo é verdade para $n = 1$.

(Hipótese de indução) Suponhamos que vale para algum $n > 1$ com $n \in \mathbb{N}$, ou seja,

$$1 + 3 + \dots + (2n-1) = n^2.$$

(Tese) Devemos mostrar que vale para $n + 1$, ou seja,

$$1 + 3 + \dots + (2n + 1) = (n + 1)^2.$$

Como

$$1 + 3 + \dots + (2n + 1) = 1 + 3 + \dots + (2n - 1) + (2n + 1).$$

Usando a hipótese de indução teremos que:

$$1 + 3 + \dots + (2n + 1) = 1 + 3 + \dots + (2n - 1) + (2n + 1) = n^2 + (2n + 1) = (n + 1)^2.$$

Como queríamos demonstrar. Logo a proposição é válida para todo $n \in \mathbb{N}$.

2.3 DIVISIBILIDADE E PROPRIEDADES BÁSICAS

Agora apresentaremos o conceito de divisibilidade e suas propriedades que foram de suma importância para o desenvolvimento da teoria dos números. Muitas proposições e teoremas fundamentais precisaram das propriedades de divisibilidades para poderem ser demonstrados.

Definição 2.1. (Divisibilidade). Dados dois números inteiros a e b , com $a \neq 0$, diremos que a divide b , escrevendo $a|b$, quando existir um número $c \in \mathbb{Z}$ tal que

$$b = a \cdot c.$$

Ainda podemos dizer:

- a é um divisor ou fator de b
- b é um múltiplo de a
- b é divisível por a

Observe que a notação $a|b$ não representa nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe um número c inteiro tal que $b = a \cdot c$.

A negação dessa sentença é representada por $a \nmid b$, leem-se (a não divide b), significando que não existe nenhum número inteiro c tal que $b = ac$.

Vejamos o exemplo.

Exemplo 2.3.

- $5|20$ pois, $20 = 5 \cdot 4$.
- $3|192$ pois, $192 = 3 \cdot 64$.
- $7|147$ pois, $147 = 7 \cdot 21$.

Por outro lado:

- $6 \nmid 11$ pois não existe um inteiro c , tal que $11 = 6c$. Ou ainda, 11 não é múltiplo de 6.

- $3 \nmid 101$ pois, não existe um inteiro c , tal que $101 = 3 \cdot c$. Ou ainda, 101 não é divisível por 3.

Proposição 2.2. *Sejam $a, b \in \mathbb{Z}^*$ e $c, d \in \mathbb{Z}$. Tem-se que:*

1. $a|0$, $1|a$ e $a|a$;
2. Se $a|1$, então $a = \pm 1$;
3. Se $a|b$ e se $c|d$, então $ac|bd$;
4. Se $a|b$ e se $b|c$, então $a|c$; (transitividade)
5. Se $a|b$ e se $b|a$, então $a = \pm b$;
6. Se $a|b$ com $b \neq 0$, então, $|a| \leq |b|$; (minimalidade)
7. Se $a|b$ e se $a|c$, então $a|(bx \pm cy)$, para todo x e y inteiros.

Demonstração:

1. Pela definição:
 - (a) se $a|0$, existe $q_1 \in \mathbb{Z}$ tal que $0 = a \cdot q_1$, daí $q_1 = 0$, ou seja, $0 = a \cdot 0$;
 - (b) se $1|a$ existe $q_2 \in \mathbb{Z}$ tal que $a = 1q_2$, daí $q_2 = a$, ou seja, $a = 1 \cdot a$;
 - (c) se $a|a$ existe $q_3 \in \mathbb{Z}$ tal que $a = a \cdot q_3$, daí $q_3 = 1$, ou seja, $a = a \cdot 1$.
2. Se $a|1$, então existe um $q \in \mathbb{Z}$ tal que $1 = a \cdot q$ implicando nas seguintes possibilidades: $a = 1$ e $q = 1$ ou $a = -1$ e $q = -1$. Logo $a = \pm 1$.
3. Se $a|b$ e $c|d$, então, pela definição (2.1) existem os inteiros q_1 e q_2 tais que:

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}. \quad (1)$$

$$d = c \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \quad (2)$$

Multiplicando membro a membro (1) e (2), tem-se

$$b \cdot d = (a \cdot c)(q_1 \cdot q_2) \implies a \cdot c | b \cdot d.$$

4. Se $a|b$ e $b|c$, então, pela Tese de divisibilidade existem os inteiros q_1 e q_2 tais que:

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}. \quad (3)$$

$$c = b \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \quad (4)$$

Multiplicando membro a membro (3) e (4), tem-se

$$\begin{aligned} b \cdot c &= (a \cdot b)(q_1 \cdot q_2) \implies c = a(q_1 \cdot q_2) \\ &\implies a|c. \end{aligned}$$

5. Se $a|b$ e se $b|a$, então, pela definição (2.1) existem os inteiros q_1 e q_2 tais que:

$$b = a \cdot q_1, \text{ com } q_1 \in \mathbb{Z}. \quad (5)$$

$$a = b \cdot q_2, \text{ com } q_2 \in \mathbb{Z}. \quad (6)$$

Substituindo (5) em (6),

$$a = a \cdot (q_1 q_2) \implies q_1 \cdot q_2 = 1 \implies q_1 | 1.$$

Pelo item 2 da proposição (2.2) implica que $q_1 = \pm 1$,
então $a = \pm b$.

6. Se $a|b$ com $b \neq 0$, então por definição existe $q \in \mathbb{Z}$ tal que $b = a \cdot q$, aplicando o módulo em ambos os membros e usando propriedades básicas de módulo, temos que;

$$|b| = |a \cdot q| = |a| \cdot |q|. \quad (7)$$

Como $a \neq 0$, por definição e por hipótese temos que $b \neq 0$, então $1 \leq |q|$, daí multiplicando por $|a|$, tem-se

$$|a| \leq |q| |a|. \quad (8)$$

Logo de (7) e (8) obtemos que:

$$|a| \leq |b|.$$

Como queríamos demonstrar.

7. Se $a|b$ e se $a|c$, então por definição existe q_1 e q_2 tais que:

$$b = a \cdot q_1, \quad (9)$$

com $q_1 \in \mathbb{Z}$.

$$c = a \cdot q_2, \quad (10)$$

com $q_2 \in \mathbb{Z}$.

Portanto, quaisquer que sejam os inteiros x e y , multiplicando (9) por x e (10) por y e somando membro a membro, obteremos:

$$bx + cy = aq_1x + aq_2y = a(q_1x + q_2y),$$

então $a|(bx + cy)$, para todo x e y inteiros. A subtração é feita de forma totalmente análoga. Portanto, $a|(bx \pm cy)$, como queríamos demonstrar. ■

A Proposição (2.2) vai ser bastante utilizada em diversas demonstrações apresentadas nesse trabalho, e para ter um melhor entendimento dos resultados estudados neste trabalho, vejamos alguns exemplos com suas respectivas soluções.

Exemplo 2.4. Sejam a , b e c inteiros. Mostre que se $a|b$ e se $a|c$, então $a^2|bc$.

Demonstração: Se $a|b$ e se $a|c$, então por definição existem os inteiros q_1 e q_2 tais que:

$$b = a \cdot q_1 \quad e \quad c = a \cdot q_2 \quad (11)$$

com q_1 e $q_2 \in \mathbb{Z}$.

Multiplicando membro a membro (11), obteremos:

$$bc = aa(q_1q_2).$$

E portanto, $bc = a^2 \cdot (q_1q_2)$. Ou seja, $a^2|bc$. ■

Exemplo 2.5. Se a e b são dois números naturais e $2a + b$ é divisível por 13, mostre que $93a + b$ também é divisível por 13.

Solução: Temos que $93a + b = 91a + (2a + b)$. Como $13|91a$ e por hipótese $13|(2a + b)$, pelo item (7) da Proposição (2.2) temos que:

$$13|91a + (2a + b) \implies 13|93a + b.$$

As proposições apresentadas a seguir são de grande utilidade na demonstração de vários resultados em teoria dos números e todas podem ser demonstradas usando o princípio da indução matemática.

Proposição 2.3. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a + b$ divide $a^{2n+1} + b^{2n+1}$.*

Demonstração: Vamos provar isto por indução sobre n .

(Caso Base) A afirmação é verdade para $n = 1$, pois $a + b$ divide $a^3 - b^3 = (a + b)(a^2 - ab + b^2)$.

(Hipótese de indução) Suponhamos, agora, que $(a + b)|(a^{2n+1} + b^{2n+1})$, para algum $n > 1$ com $n \in \mathbb{N}$.

(Tese) Devemos mostrar que $(a + b)|(a^{2n+3} + b^{2n+3})$. Temos que:

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

Como $(a + b)|(a^2 - b^2) = (a + b)(a - b)$ e, por hipótese, $(a + b)|(a^{2n+1} + b^{2n+1})$, decorre da igualdade acima e da Proposição (2.2) item (7) que $(a + b)|(a^{2n+3} + b^{2n+3})$.

Estabelecendo o resultado para todo $n \in \mathbb{N}$, como queríamos demonstrar. ■

Proposição 2.4. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a + b$ divide $a^{2n} - b^{2n}$.*

Demonstração: Vamos provar isto por indução sobre n .

(Caso Base) A afirmação é verdade para $n = 1$, pois $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$.

(Hipótese de indução) Suponhamos, agora, que $(a + b)|(a^{2n} - b^{2n})$, para algum $n > 1$ com $n \in \mathbb{N}$.

(Tese) Devemos mostrar que $(a - b)|(a^{2n+2} - b^{2n+2})$. Temos que:

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

Como $(a + b)|(a^2 - b^2)$ e, por hipótese, $(a + b)|(a^{2n} - b^{2n})$, decorre da igualdade acima e da Proposição (2.2) item (7) que $(a + b)|(a^{2n+2} - b^{2n+2})$.

Estabelecendo o resultado para todo $n \in \mathbb{N}$, como queríamos demonstrar. ■

Proposição 2.5. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b$ divide $a^n - b^n$.*

Demonstração: Vamos provar isto por indução sobre n .

(Caso Base) A afirmação é verdade para $n = 1$, pois $a - b$ divide $a^1 - b^1 = a - b$.

(Hipótese de indução) Suponhamos, agora, que $(a - b)|(a^n - b^n)$, para algum $n > 1$ com $n \in \mathbb{N}$.

(Tese) Devemos mostrar que $(a - b)|(a^{n+1} - b^{n+1})$. Temos que:

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

Como $(a - b)|(a - b)$ e, por hipótese, $(a - b)|(a^n - b^n)$, decorre da igualdade acima e da Proposição (2.2) item (7) que $(a - b)|(a^{n+1} - b^{n+1})$.

Estabelecendo o resultado para todo $n \in \mathbb{N}$, como queríamos demonstrar. ■

Vejamos a solução de alguns exemplos para uma melhor compreensão dos resultados apresentados.

Exemplo 2.6. Mostre que $8|3^{2n} - 1$ para todo $n \in \mathbb{N}$.

Solução: Note que:

$$3^{2n} - 1 = 9^n - 1 = 9^n - 1^n.$$

Pela Proposição (2.5), temos que

$$9 - 1|9^n - 1^n.$$

Logo,

$$8|3^{2n} - 1.$$

Exemplo 2.7. Mostre que $14|3^{4n+2} + 5^{2n+1}$ para todo $n \in \mathbb{N} \cup \{0\}$

Solução: Note que:

$$3^{4n+2} + 5^{2n+1} = 3^{2(2n+1)} + 5^{2n+1} = 9^{2n+1} + 5^{2n+1}.$$

Pela Proposição (2.3), temos que

$$9 + 5 \mid 9^{2n+1} + 5^{2n+1}.$$

Logo,

$$14 \mid 3^{4n+2} + 5^{2n+1}.$$

Exemplo 2.8. Mostre que $13 \mid 9^{2n} - 4^{2n}$ para todo $n \in \mathbb{N}$.

Solução: Note que:

$$9^{2n} - 4^{4n} = 9^{2n} - 2^{2(2n)} = 9^{2n} - 4^{2n}.$$

Pela Proposição (2.4), temos

$$9 + 5 \mid 9^{2n} - 4^{2n}.$$

Logo,

$$13 \mid 9^{2n} - 4^{2n}.$$

2.4 ALGORITMO DA DIVISÃO DE EUCLIDES

O lema a seguir é usado para demonstrar o próximo teorema (o algoritmo da divisão de Euclides), um resultado que será usado para demonstrar outros teoremas, entre eles o teorema de Bézout, um resultado essencial em teoria dos números utilizado na demonstração de muitos resultados dentro desse ramo da matemática.

Lema 2.1. *Se a e b são dois inteiros positivos, com $b \neq 0$, existem os inteiros q e r que satisfazem as condições:*

$$a = qb + r, \text{ com } 0 \leq r < b.$$

Demonstração: Seja o conjunto

$$S = \{a - (bx)/x \in \mathbb{Z} \text{ com, } a - (bx) \geq 0\}.$$

Note que se $x = -|a|$, temos que $a - b(-|a|) = a + |a| \geq 0$, pois $b \geq 1$. Isso mostra que o conjunto $S \neq \emptyset$. Logo pelo princípio da boa ordenação o conjunto S possui um elemento mínimo. Seja r o mínimo de S , logo $r = a - b \cdot q$ para algum $q \in \mathbb{Z}$, pois todos os elementos de S têm essa forma.

Vamos mostrar que $r < b$.

Suponhamos por absurdo que o contrário acontece, ou seja $r \geq b$. Dessa forma temos que:

$$r - b = a - b \cdot q - b = a - b(q + 1) \geq 0.$$

note que $a - b(q + 1) \geq 0$ é um elemento de S , pois é da forma $a - bx$. Mas

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

Como r é o menor elemento de S e encontramos um valor em S abaixo do mínimo temos um absurdo, pelo princípio da boa ordenação, logo devemos ter $r < b$.

Agora demonstraremos a Unicidade.

Suponhamos que: $a = bq + r$ com $0 \leq r < b$ e $a = bq_1 + r_1$ com $0 \leq r_1 < b$.

Daí teremos que: $b(q - q_1) = r_1 - r \implies b|r_1 - r$

Por outro lado temos que:

$$\begin{aligned} -b < -r \leq 0 \text{ e } 0 \leq r_1 < b &\implies -b < r_1 - r < b \\ &\implies |r_1 - r| < b \end{aligned}$$

Assim de $b|r_1 - r$ e $|r_1 - r| < b$, temos que $r_1 - r = 0$ e como $b \neq 0$ temos que $q - q_1 = 0$. Portanto $r = r_1$ e $q = q_1$. Como queríamos demonstrar. ■

Vejamos o resultado do Lema (2.1) aplicado no exemplo a seguir.

Exemplo 2.9. Sejam os números 201 e 80. quais os valores do par (q, r) que satisfaz o Lema (2.1) ?

Solução: Note que $201 = 2 \cdot 80 + 41$. Logo $q = 2$ e $r = 41$ é o único par de números que satisfaz as duas condições do lema.

O teorema a seguir é uma generalização do Lema (2.1) apresentado acima. Ele é conhecido como Algoritmo da Divisão de Euclides.

Teorema 2.3 (Algoritmo da Divisão de Euclides). *Dados dois inteiros a e b , com $b \neq 0$, então existe um único par (q, r) de inteiros tais que $a = bq + r$ onde $0 \leq r < |b|$. Os números q e r são chamados respectivamente de quociente e resto da divisão. $r = 0$ se, e somente se, b é divisor de a , ou seja, $b|a$.*

Demonstração: Separando em casos:

1° caso: Se $b > 0$.

- Quando $a \geq 0$ o lema anterior garante a existência do par (q, r) ;
- Quando $a < 0$, podemos considerar $|a|$, logo pelo lema anterior existem q_1 e r_1 tal que

$$|a| = bq_1 + r_1,$$

com $0 \leq r_1 < b$.

i) Se $r_1 = 0$ temos que:

$$-|a| = b(-q_1) - 0 = b(-q_1).$$

Logo o par $(-q_1, 0)$ satisfaz as condições do teorema.

ii) Se $r_1 > 0$ temos que:

$$-|a| = b(-q_1) - r_1 = b(-q_1) + b - b - r_1 = b(-q_1 - 1) + (b - r_1).$$

Como $0 < b - r_1 < b$. Então o par $(-q_1 - 1, b - r_1)$, garante as condições do teorema.

2° caso: Se $b < 0$.

Qualquer que seja a podemos determinar q_1 e r_1 tal que: $a = |b|q_1 + r_1$ com $0 \leq r_1 < |b|$.

- Se $b < 0$ e $a > 0$. Como, $b < 0$ então $|b| = -b$. Dessa forma:

$$\begin{aligned} a &= |b|q_1 + r_1 \\ &= -bq_1 + r_1 \\ &= b(-q_1) + r_1. \end{aligned}$$

Logo temos que o par $(-q_1, r_1)$ satisfaz o teorema.

- Se $b < 0$ e $a < 0$, temos que $|b| = -b$ e $|a| = -a$. Dessa forma:

$$\begin{aligned} |a| = -a &= -|b|q_1 - r_1 \\ &= -|b|q_1 - |b| + |b| - r_1 \\ &= |b|(-q_1 - 1) + (|b| - r_1). \end{aligned}$$

Logo temos que o par $(-q_1 - 1, |b| - r_1)$ satisfaz o teorema. E isso conclui a existência.

Provaremos agora a unicidade. Suponha que $a = bq + r$ com $0 \leq r < |b|$ e $a = bq_1 + r_1$ com $0 \leq r_1 < |b|$. sem perda de generalidade suponha que $r_1 \geq r$, Dessa forma,

$$bq + r = bq_1 + r_1 \text{ ou seja, } b(q - q_1) = r_1 - r.$$

Como $|b| > r_1$, temos que $r_1 - r < |b|$. Por outro lado,

$$b(q - q_1) = r_1 - r < |b|.$$

Aplicando módulo em ambos os membros teremos que:

$$|b(q - q_1)| = |r_1 - r| < |b|.$$

Pelas propriedades de módulo fica:

$$0 \leq |b|(q - q_1)| < |b|.$$

Como $b \neq 0$, então $|b| > 0$. Dividindo a inequação por $|b| > 0$ teremos:

$$0 \leq |(q - q_1)| < 1.$$

Uma vez que não existe inteiro no intervalo, temos que $q - q_1 = 0$ implica $q = q_1$. Assim

$$qb + r = q_1b + r_1 \implies r = r_1.$$

Logo esse par (q, r) quando existe é único, como queríamos demonstrar. ■

Agora para uma melhor assimilação das casos apresentados, serão resolvidos exemplos tratando caso a caso.

Exemplo 2.10. Determine o quociente q e o resto r na divisão de $a = 53$ por $b = -13$ que satisfazem às condições do Algoritmo da Divisão.

Solução: Efetuando a divisão usual dos valores absolutos de a e b , obtemos:

$$53 = 13 \cdot 4 + 1 \implies 53 = (-13) \cdot (-4) + 1,$$

onde $0 \leq 1 < |-13|$. Logo, o quociente $q = -4$ e o resto $r = 1$.

Exemplo 2.11. Determine o quociente q e o resto r na divisão de $a = -89$ por $b = 11$ que satisfazem às condições do algoritmo da divisão.

Solução: Efetuando a divisão usual dos valores absolutos de a e b , obtemos:

$$89 = 11 \cdot 8 + 1 \implies -89 = 11(-8) - 1.$$

Como $r = -1 < 0$ não satisfaz à condição $0 \leq r < |11|$, somando e subtraindo o valor de 11 ao segundo membro da igualdade anterior, teremos:

$$-89 = 11(-8) + -11 + 11 - 1 \implies -89 = 11(-9) + 10.$$

Como $0 \leq 10 < 11$, logo o quociente $q = -9$ e o resto $r = 10$, satisfaz as condições do teorema.

Exemplo 2.12. Determine o resto da divisão de $a = -89$ e $b = -11$, que satisfaz a condição do teorema.

Solução: Efetuando a divisão usual, temos que:

$$\begin{aligned} 89 = 11 \cdot 8 + 1 &\implies -89 = -11 \cdot 8 - 1 \\ &= -11 \cdot 8 - 11 + 11 - 1 \\ &= -11(9) + 10. \end{aligned}$$

Logo os valores de q e r que satisfaz as condições do teorema são $q = 9$ e $r = 10$.

Corolário 2.2 (Eudoxius). *Dados a e b inteiros com $b \neq 0$, então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b , isto é, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiro n tal que, para $b > 0$,*

$$nb < a < (n + 1)b,$$

e para $b < 0$

$$nb < a < (n - 1)b.$$

Demonstração: Pelo Algoritmo da Divisão de Euclides, Teorema (2.3), existem únicos q e $r \in \mathbb{Z}$ tais que $a = bq + r$ com $0 \leq r < |b| = b$. Somando bq na desigualdade teremos:

$$bq \leq bq + r < b + bq = b(q + 1),$$

fazendo $n = q$, fica:

$$nb \leq a < b(n + 1),$$

que é o resultado desejado, como queríamos demonstrar. ■

Esse resultado segundo Santos (2000) é erroneamente atribuído a Arquimedes e chamado de "Princípio de Arquimedes".

Vejamos a solução do exemplo:

Exemplo 2.13. Para $a = 17$ e $b = 4$, devemos tomar $n = 4$, pois,

$$4 \cdot 4 < 17 < 5 \cdot 4 \implies 16 < 17 < 20.$$

Para $a = -17$ e $b = 4$, escolhemos $n = -5$, pois

$$(-5) \cdot 4 < -17 < (-4) \cdot 4 \implies -20 < -17 < -16.$$

Conhecer as características do nosso sistema de numeração e os critérios de divisibilidade é uma ferramenta bastante útil para decidirmos de forma rápida sem muitos cálculos se dois números são divisíveis. Na próxima sessão apresentaremos alguns conceitos básicos do nosso sistema de numeração decimal, bem como os critérios básicos de divisibilidade.

2.5 SISTEMA DE NUMERAÇÃO DECIMAL

No sistema de numeração decimal, também conhecido como sistema numérico na base 10, todo número pode ser representado pelos símbolos da sequência $\{0, 1, 2, 3, \dots, 9\}$.

Por serem dez os algarismos, o sistema é chamado, sistema de numeração decimal.

Por exemplo, o número 345 escreve-se na base decimal da seguinte forma

$$345 = 300 + 40 + 5 = 3 \cdot 10^2 + 4 \cdot 10 + 5.$$

Assim como 2768 se escreve da forma:

$$2768 = 2000 + 700 + 60 + 8 = 2 \cdot 10^3 + 7 \cdot 10^2 + 6 \cdot 10 + 8.$$

De modo geral, denotamos por

$$a = r_n r_{n-1} \cdots r_1 r_0,$$

o número inteiro positivo formado pelos algarismos $r_n, r_{n-1}, \dots, r_1$ e r_0 , nessa ordem.

Portanto a se escreve na base decimal da seguinte forma:

$$a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \dots + r_1 \cdot 10^1 + r_0.$$

A notação acima também é chamada de expansão decimal do número na base decimal, onde $0 \leq r_k \leq 9$, para $k \in \mathbb{N}$ sendo que o primeiro termo para $k = n$ devemos ter $r_n \neq 0$.

Observação 2.1. De uma forma mais geral, dados os números inteiros a e b com $a > 0$ e $b > 1$ existem números inteiros $n \geq 0$ e $0 \leq r_0, r_1, r_2, \dots, r_n < b$ com $r_n \neq 0$ univocamente determinados, tais que

$$a = r_0 + r_1 b + r_2 b^2 + \dots + r_n b^n.$$

Ou seja podemos escrever um número em qualquer base e essa representação será única pelo Algoritmo da Divisão de Euclides. Para consultar uma demonstração desse fato, consulte Hefez (2016).

Daremos, a seguir, os critérios de divisibilidade por 2, 3, 4, 5, 6, 7, 8, 9 e 10 para números representados na base do sistema de numeração decimal.

Proposição 2.6 (Divisibilidade por 2). *Um número é divisível por 2, se e somente se, o algarismo das unidades é par (0, 2, 4, 6, 8).*

Demonstração: Temos que todo número pode ser escrito na forma

$$a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \dots + r_1 \cdot 10^1 + r_0 = 10(r_n \cdot 10^{n-1} + r_{n-1} \cdot 10^{n-2} + \dots + r_1) + r_0.$$

($\Rightarrow$) Se,

$$\begin{aligned}
2 \mid a &\implies 2 \mid r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \dots + r_1 \cdot 10^1 + r_0 \\
&\implies 2 \mid 10(r_n \cdot 10^{n-1} + r_{n-1} \cdot 10^{n-2} + \dots + r_1) + r_0.
\end{aligned}$$

Como $2 \mid 10 \implies 2 \mid 10(r_n \cdot 10^{n-1} + r_{n-1} \cdot 10^{n-2} + \dots + r_1)$ e por hipótese $2 \mid a$, pela Proposição (2.2) item (7) então, $2 \mid r_0$. Portanto, $r_0 = (0, 2, 4, 6, 8)$

($\Leftarrow$) Se r_0 par, então $2 \mid r_0$, como $2 \mid 10(r_n \cdot 10^{n-1} + r_{n-1} \cdot 10^{n-2} + \dots + r_1)$ então pela Proposição (2.2) item (7) temos que 2 divide a soma, ou seja, $2 \mid 10(r_n \cdot 10^{n-1} + r_{n-1} \cdot 10^{n-2} + \dots + r_1) + r_0$ portanto, $2 \mid a$, como queríamos demonstrar. ■

Observação 2.2. A divisibilidade por 5 e 10 é demonstrada de forma análoga.

Proposição 2.7 (Divisibilidade por 3). *Um número será divisível por 3, se e somente se, a soma dos algarismos é um múltiplo de 3.*

Demonstração: Pela Proposição (2.5) temos que $(a - b) \mid (a^n - b^n)$ fazendo $a = 10$ e $b = 1$ teremos que:

$$(10 - 1) \mid (10^n - 1) \implies 9 \mid (10^n - 1) \quad (12)$$

$$\implies (10^n - 1) = 9k, \quad (13)$$

com $k \in \mathbb{Z}$.

Sendo

$$a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \dots + r_1 \cdot 10^1 + r_0,$$

a expansão decimal do número, temos que:

$$\begin{aligned}
3 \mid a &\Rightarrow 3 \mid r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \dots + r_1 \cdot 10^1 + r_0 \\
&\Rightarrow 3 \mid r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \dots + r_1 \cdot 10^1 + r_0 + (r_n + \dots + r_1) - (r_n + \dots + r_1) \\
&\Rightarrow 3 \mid r_n \cdot (10^n - 1) + r_{n-1} \cdot (10^{n-1} - 1) + \dots + r_1 \cdot (10^1 - 1) + r_n + \dots + r_1 + r_0.
\end{aligned}$$

Pelo resultado apresentado em (13), podemos escrever da forma:

$$3 \mid 9k_n + \dots + 9k_1 + r_n + \dots + r_1 + r_0 \Rightarrow 3 \mid 9q + r_n + \dots + r_1 + r_0,$$

onde $q \in \mathbb{Z}$ sendo $q = (k_1 + k_2 + \dots + k_n)$.

Como por hipótese $3 \mid a$ e mostramos que $3 \mid 9q$ temos pelo item (7) da Proposição (2.2), que $3 \mid r_n + \dots + r_1 + r_0$.

Reciprocamente, admitindo que $3 \mid r_n + \dots + r_1 + r_0$ e como $3 \mid r_n \cdot (10^n - 1) + r_{n-1} \cdot (10^{n-1} - 1) + \dots + r_1 \cdot (10^1 - 1)$ então pelo item (7) da Proposição (2.2), 3 divide a soma, logo:

$$3 \mid a \implies 3 \mid r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \dots + r_1 \cdot 10^1 + r_0,$$

como queríamos demonstrar. ■

Observação 2.3. De forma completamente análoga mostra-se que $9|a$

Proposição 2.8. *Um número será divisível por 4 se, e somente se, o número formado por seus dois últimos algarismos é divisível por 4.*

Demonstração: sendo $a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \dots + r_1 \cdot 10^1 + r_0$, podemos reescrevê-lo como segue, $a = 100 \cdot (r_n \cdot 10^{n-2} + \dots r_{n-1} \cdot 10^{n-3}) + r_1 r_0$ com por hipótese $4|a$ e $4|100 \cdot (r_n \cdot 10^{n-2} + \dots r_{n-1} \cdot 10^{n-3})$, temos pelo item (7) da Proposição (2.2) que $4|r_1 r_0$.

A reciprocidade se demonstra de forma análoga. ■

Observação 2.4. A divisibilidade por 8 se demonstra usando o mesmo raciocínio.

Proposição 2.9. *Um número será divisível por 6, se e somente se, for múltiplo de 2 e de 3 simultaneamente.*

Demonstração: Por ser divisível por 2, o algarismo da unidade deve ser par e para ser divisível por 3, a soma de seus algarismos deve ser um múltiplo de 3. Portanto combinando os resultados de divisibilidade por 2 e por 3 chegamos ao resultado desejado. ■

Proposição 2.10. *Um número será divisível por 7, se a diferença entre o número formado pelo número inicial dado, retirado o algarismo das unidades e o dobro do algarismo das unidades é divisível por 7.*

Demonstração: Sendo

$$a = r_n \cdot 10^n + r_{n-1} \cdot 10^{n-1} + \dots + r_1 \cdot 10^1 + r_0 = 10 \cdot (r_n \cdot 10^{n-1} + r_{n-1} \cdot 10^{n-2} + \dots + r_1) + r_0 = 10k + r_0,$$

com $k \in \mathbb{Z}$.

Se $7|a \Rightarrow 7|10k + r_0 \Rightarrow 10k + r_0 = 7m \Rightarrow r_0 = 7m - 10k$, e portanto temos que:

$$k - 2r_0 = k - 2(7m - 10k) = k - 14m + 20k = 14m + 21k = 7(2m + 3k).$$

Logo, $7|k - 2r_0$.

Reciprocamente, se $k - 2r_0$ é múltiplo de 7 então existe $n \in \mathbb{Z}$ tal que $k - 2r_0 = 7n$ e, portanto,

$$10k + r_0 = 10(7n + 2r_0) + r_0 = 70n + 21r_0 = 7(10n + 3r_0).$$

Isso mostra que $7|10k + r_0$. O que conclui a demonstração. ■

O exemplo a seguir ajudará a fixar melhor os critérios de divisibilidade apresentados acima.

Exemplo 2.14. . Determine TODOS os valores possíveis para os algarismos x e y de modo que o número $3x90586y$, representado na base 10, seja divisível por 60.

Solução: Note que,

$60 = 2^2 \cdot 3 \cdot 5$. Portanto, $3x90586y$ é divisível por $2^2 \cdot 3 \cdot 5 = 60$, se é divisível simultaneamente por 4, 3 e 5.

- $3x90586y$ é divisível por 5 se, e somente se, $y = 0$ ou $y = 5$.
- $3x90586y$ é divisível por 4 se, e somente se, $6y$ é divisível por 4. Pelo item anterior, $y = 0$, pois 65 não é divisível por 4.
- $3x905860$ é divisível por 3 se, e somente se,

$$3 + x + 9 + 0 + 5 + 8 + 6 + 0 = 31 + x$$

é divisível por 3. Assim, os possíveis valores para x são 2, 5 e 8.

Logo, 32905860, 35905860 e 38905860 são os números procurados.

2.6 MÁXIMO DIVISOR COMUM

Agora apresentaremos as definições e propriedades básicas relacionadas ao máximo divisor comum (*MDC*) que serão de grande importância no desenvolvimento de ferramentas essenciais a resultados que desenvolveram a teoria dos números. Vamos conhecer ferramentas que são úteis para encontrar os valores do *MDC* de dois ou mais números inteiros. Além de conhecer os divisores naturais de um número é muito útil calcular o maior divisor de dois números. Vejamos a seguir a definição:

Definição 2.2. (Máximo Divisor Comum). Sejam a e b inteiros diferentes de zero. O máximo divisor comum, entre a e b é o número d que satisfaz as seguintes condições:

1. d é um divisor comum de a e b , isto é, $d|a$ e $d|b$;
2. d é o maior inteiro positivo com a propriedade (1), isto é, se $c|a$ e se $c|b$, então, $c|d$.

Neste caso, denotamos o máximo divisor comum entre a e b por d . E representaremos por $(a, b) = d$ ou $(b, a) = d$.

Usando a definição apresentada, vejamos a solução do exemplo:

Exemplo 2.15. Os divisores dos números 6, 14 e 15 são:

$$D(6) = \{1, 2, 3, 6\}$$

$$D(14) = \{1, 2, 7, 14\}$$

$$D(15) = \{1, 3, 5, 15\}$$

Assim o *MDC* de 6 e 14 é 2, e representamos por $(6, 14) = 2$.

E o *MDC* de 14 e 15 é 1 e representamos por $(14, 15) = 1$.

Observação 2.5. Quando o *MDC* entre 2 números for igual a 1 diremos que esses números são coprimos ou primos entre si, ou seja $(a, b) = 1$. Portanto, 14 e 15 são números primos entre si.

Propriedades dos divisores comuns de dois números inteiros a e b . Para estes números é imediato e valem as seguintes afirmações:

1. $(a, 1) = 1$;
2. se $a \neq 0$, então, $(a, 0) = |a|$;

3. se $a \neq 0$, então, $(a, a) = |a|$;
4. se $a|b$, então, $(a, b) = |a|$.

Em particular, é imediato verificar que:

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

Observação 2.6. O máximo divisor comum de $(0, 0)$ não existe. Para mais detalhes veja Bertone (2014).

2.7 O TEOREMA DE ÉTIENNE BÉZOUT

O próximo Teorema é uma ferramenta que será bastante utilizada na demonstração de vários outros teoremas neste trabalho. O resultado foi provado pela primeira vez por Claude–Gaspard Bachet de Méziriac (1581 – 1638) e mais tarde generalizado para polinômios por Étienne Bézout (1730 – 1783). Frequentemente, na literatura se enuncia este resultado como Teorema de Bézout.

Segundo Hefez(2016) o teorema nos dá uma outra demonstração da existência do máximo divisor comum (MDC) de dois números a e b e da existência de inteiros m e n tais que, $ma + bn = (a, b)$. Vejamos o que diz o teorema:

Teorema 2.4 (Teorema de Bézout). *Seja d o máximo divisor comum entre a e b , então existem inteiros m e n tais que $(a, b) = am + bn$ isto é, (a, b) é uma combinação linear de a e b .*

Demonstração: Seja S o conjunto de todas as combinações lineares $ma + nb$ onde m e n são inteiros, isto é:

$$S = \{ma + nb; m, n \in \mathbb{Z}\}.$$

Este conjunto contém, claramente, números negativos, positivos e também o zero. Vamos considerar o subconjunto de S .

$$S' = S \cap \mathbb{N}.$$

S' não é vazio ($S \neq \emptyset$), logo pelo Princípio da Boa Ordenação, S' possui um elemento mínimo c tal que $c = m_0a + n_0b$, onde m_0 e $n_0 \in \mathbb{Z}$.

Vamos provar que $c|a$ e que $c|b$. Como as demonstrações são análogas, mostraremos apenas que $c|a$. A demonstração se dará por contradição.

Suponhamos por contradição que $c \nmid a$. Pelo Teorema Algoritmo da Divisão de Euclides, existem q e r tais que

$$a = qc + r,$$

com $0 < r < c$. Colocando r em destaque, teremos:

$$\begin{aligned} r &= a - qc \\ &= a - q(m_0a + n_0b) \\ &= (1 - qm_0)a + (-qn_0)b. \end{aligned}$$

Isto é, o resto r é uma combinação linear de a e b . Isto mostra que $r \in S'$, pois $(1 - qm_0)$ e $(-qn_0)$ são inteiros, o que é uma contradição, visto que $0 < r < c$ e c é o menor elemento positivo de S' .

Logo $c|a$, e de forma análoga se prova que $c|b$. Como d é um divisor comum de a e b , existem inteiros k_1 e k_2 tais que $a = k_1d$ e $b = k_2d$ e, portanto,

$$\begin{aligned} c &= m_0a + n_0b \\ &= m_0k_1d + n_0k_2d \\ &= d(m_0k_1 + n_0k_2), \end{aligned}$$

ou seja, $d|c$ e pelas propriedades de divisibilidade $d \leq c$ (visto que c e d são números positivos). como $d = (a, b)$, segue que $d \geq c$. logo devemos ter:

$$d = c = m_0a + n_0b,$$

como queríamos demonstrar. ■

Para uma melhor compreensão do Teorema (2.4) (Teorema de Bézout) apresentado, vejamos o exemplo:

Exemplo 2.16. Sejam os inteiros $a = 7$ e $b = 8$. Temos $(7, 8) = 1 \implies 7x + 8y = 1$. Tomando $x_0 = -1$ e $y_0 = 1$ tem-se que $7(-1) + 8(1) = 1$.

Note que os coeficientes $x_0 = -1$ e $y_0 = 1$ não são únicos, pois se k é um inteiro qualquer, então todos os pares de inteiros (x, y) que satisfazem a expressão, pode ser obtido por:

$$x = x_0 + bk = -1 + 8k$$

e

$$y = y_0 - ak = 1 - 7k,$$

onde $k \in \mathbb{Z}$. O resultado será demonstrado mais a frente como um corolário.

Como consequência imediata do Teorema de Bézout, temos os Corolários (2.3) e (2.4) apresentados a seguir.

Corolário 2.3. Para quaisquer que sejam $a, b \in \mathbb{Z}$, não ambos nulos, e $n \in \mathbb{N}$, tem-se que

$$(na, nb) = n(a, b).$$

Demonstração: Pelo Teorema de Bézout,

$$naX + nbY = (na, nb),$$

ou seja, (na, nb) é o menor valor positivo de $naX + nbY = n(aX) + n(bY)$ com $X, Y \in \mathbb{Z}$ logo, temos que

$$(na, nb) = naX + nbY = n(aX) + n(bY) = n(aX + bY). \quad (14)$$

Como $(a, b) = aX + bY$ representa o menor inteiro positivo, substituindo em (14) temos o desejado, ou seja $(na, nb) = n(a, b)$, como queríamos demonstrar. ■

Corolário 2.4. *Dados $a, b \in \mathbb{Z}$, não ambos nulos, tem-se que*

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)} \right) = 1.$$

Demonstração: Seja $d = (a, b)$ logo pelo Teorema de Bézout, existem inteiros x e y tais que:

$$ax + by = (a, b) = d.$$

Dividindo ambos os membros por (a, b) , encontramos,

$$\frac{ax}{(a, b)} + \frac{by}{(a, b)} = 1,$$

que após uma reordenação de forma conveniente, fica:

$$\left(\frac{a}{(a, b)} \right) \cdot x + \left(\frac{b}{(a, b)} \right) \cdot y = 1.$$

Portanto, ainda pelo Teorema de Bézout,

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)} \right) = 1,$$

como queríamos demonstrar. ■

Vejamos a solução do exemplo:

Exemplo 2.17. Mostre que se $a, b, x, y \in \mathbb{Z}$, com $ax + by = (a, b)$ então $(x, y) = 1$.

Solução: Note que:

$$ax + by = (a, b) \implies \frac{a}{(a, b)}x + \frac{b}{(a, b)}y = 1$$

Logo, pelo Teorema de Bézout temos que $(x, y) = 1$.

Corolário 2.5. *Se $(a, b) = 1$ e $(a, c) = 1$ se e somente se, $(a, bc) = 1$*

Demonstração: Pelo Teorema de Bézout existem x, y, z e t inteiros tal que:

$$ax + by = 1 \quad (15)$$

$$az + ct = 1 \quad (16)$$

Portanto

$$1 = ax + by(az + ct) = a(x + byz) + bc(yt).$$

Portanto $(a, bc) = 1$.

Reciprocamente, como $(a, bc) = 1$ então pelo Teorema de Bézout, existem inteiros x e y tal que,

$$ax + bcy = 1,$$

que pode ser escrito como:

$$ax + b(cy) = 1 \implies (a, b) = 1 \quad (17)$$

$$ax + c(by) = 1 \implies (a, c) = 1. \quad (18)$$

Como queríamos demonstrar. ■

Os leitores mais curiosos podem consultar Santos(2000) para mais detalhes.

O Teorema (2.5) apresentado a seguir será de grande utilidade na demonstração de propriedades relacionadas aos números primos, cuja a definição e propriedades serão apresentadas na próxima sessão. O resultado do Teorema (2.5) junto com o Teorema de Bézout será útil na demonstração de vários resultados que serão apresentados neste trabalho.

Teorema 2.5 (Lema de Gauss). *Sejam a, b e $c \neq 0 \in \mathbb{Z}$. Se $a|bc$ e $(a, b) = 1$, então $a|c$.*

Demonstração: Se $a|bc$ então existe $d \in \mathbb{Z}$ tal que $bc = ad$. Se $(a, b) = 1$ pelo Teorema de Bézout, temos que existem inteiro x, y tal que:

$$ax + by = 1. \quad (19)$$

Multiplicando por c a igualdade (19), fica:

$$c = xac + byc. \quad (20)$$

substituindo bc por ad em (20) teremos:

$$c = xac + ady = a(xc + dy).$$

O que mostra que $a|c$, como queríamos demonstrar. ■

Vejamos um exemplo para uma melhor compreensão do Teorema (2.5) apre-

sentado acima:

Exemplo 2.18. Veja que $15 \mid 600$.

Como $600 = 2 \cdot 300$ e $(15, 2) = 1$, temos que $15 \mid 2 \cdot 300$ e, portanto pelo Teorema (2.5) $15 \mid 300$.

Corolário 2.6. *Dados a, b e $c \in \mathbb{Z}$ com b e c não ambos nulos, temos que:*

$$b \mid a \text{ e } c \mid a \Leftrightarrow \frac{bc}{(b, c)} \mid a.$$

Demonstração: ($\Rightarrow$) Note que $a = b \cdot n = c \cdot m$ para alguns $n, m \in \mathbb{Z}$ logo:

$$n \frac{b}{(b, c)} = m \frac{c}{(b, c)}.$$

Pelo Corolário (2.4), $(\frac{b}{(b, c)}, \frac{c}{(b, c)}) = 1$, e o Lema de Gauss, conclui-se que: $\frac{b}{(b, c)} \mid m \Rightarrow \frac{cb}{(b, c)} \mid mc = a \Rightarrow \frac{cb}{(b, c)} \mid a$.

($\Leftarrow$) note que $\frac{bc}{(b, c)} \mid a$ implica que $a = \frac{bc}{(b, c)} \cdot k$ com $k \in \mathbb{Z}$. Daí conclui-se de forma direta que:

$$a = c \left(\frac{b}{(b, c)} \cdot k \right) \Rightarrow c \mid a$$

e que:

$$a = b \left(\frac{c}{(b, c)} \cdot k \right) \Rightarrow b \mid a,$$

o que conclui a demonstração. ■

O conceito de *MDC* pode ser generalizado para n elementos pela proposição a seguir.

Proposição 2.11. *Dados números inteiros $a_1, a_2, \dots, a_n$ não todos nulos, existe o seu *MDC* e*

$$(a_1, a_2, \dots, a_n) = (a_1, a_2, \dots, (a_{n-1}, a_n)).$$

Demonstração:

A demonstração será feita por indução matemática.

(Caso base) Para $n = 2$ nada temos a mostrar.

(Hipótese de indução) Suponha que o resultado vale para algum $n > 2$ com $n \in \mathbb{N}$, ou seja existe o *MDC* dos números:

$$a_1, a_2, \dots, a_n.$$

(Tese) Devemos mostrar que vale para $(n + 1)$, ou seja, devemos mostrar que existe o *MDC* de:

$$a_1, a_2, \dots, a_n, a_{n+1}.$$

Seja d o MDC de $a_1, a_2, \dots, (a_n, a_{n+1})$.

Usando a hipótese, esse número existe. Logo $d|a_1, d|a_2, \dots, d|(a_n, a_{n+1})$.

Como, $d|(a_n, a_{n+1})$, implica que $d|a_n$ e $d|a_{n+1}$.

Por outro lado, seja c um divisor comum de $a_1, a_2, \dots, a_n, a_{n+1}$; logo c é um divisor comum de $a_1, a_2, \dots, (a_n, a_{n+1})$.

Portanto pelas propriedades de MDC , $c|d$, o que conclui a demonstração. ■

Vejamos a solução do exemplo abaixo, para uma melhor assimilação da proposição apresentada.

Exemplo 2.19. Calcule $(10, 11, 15)$

Solução: Pela proposição apresentada, temos que:

$$(10, 11, 15) = (10, (11, 15)).$$

Como $(11, 15)=1$, temos que:

$$(10, 11, 15) = (10, (11, 15)) = (10, 1) = 1.$$

2.8 ALGORITMO DE EUCLIDES PARA O CÁLCULO DO MÁXIMO DIVISOR COMUM

Apesar de conhecermos propriedades teóricas do máximo divisor comum entre dois inteiros, encontrá-lo de fato pode ser uma tarefa complicada sem o auxílio das ferramentas corretas.

Lembrando o seu significado, o leitor talvez pudesse pensar que devemos calcular todos os divisores de a , todos os divisores de b e descobrir qual é o maior elemento comum aos dois conjuntos. De fato, isso seria muito trabalhoso, caso os valores de a e b sejam números grandes.

Uma outra ferramenta desenvolvida por Euclides que pode ser encontrada em sua obra, Os Elementos, para encontrar o MDC de dois números sem que tenhamos de encontrar os divisores de cada um deles e verificar qual o maior deles, é o importante método, denominado Algoritmo de Euclides. O próximo Lema nos apresenta um resultado elementar, mas de fundamental importância na demonstração do Algoritmo de Euclides.

Lema 2.2. *Sejam $a, b, n \in \mathbb{Z}$. Se existe o número $(a, b - an)$ então (a, b) existe e*

$$(a, b - an) = (a, b).$$

Demonstração: Seja $d = (a, b - na)$, temos que $d|a$ e $d|(b - na)$. Se $d|a$ segue pelas propriedades de divisibilidade que $d|a \cdot n$. Logo pela Proposição (2.2) item (7), d divide a soma, ou seja,

$$d|a \cdot n + (b - a \cdot n) \implies d|b.$$

Portanto, d é um divisor comum de a e b .

Suponha agora que c seja um divisor comum de a e b . Logo, c é um divisor comum de a e $b - na$ e, conseqüentemente, $c|d$. Isso prova que $d = (a, b)$, como queríamos demonstrar. ■

Vejamos o exemplo:

Exemplo 2.20. Qual o máximo divisor dos números 200 e 24?

Solução: Pelo Lema (2.2), temos que:

$$(24, 200) = (24, 200 - 24 \cdot 8) = (24, 8) = (8, 24 - 8 \cdot 3) = (8, 0) = 8.$$

Euclides deu uma prova construtiva da existência do máximo divisor comum, usando o Lema (2.2) apresentado acima. Esta construção está no seu livro Os Elementos, livro VII, proposição II. Hefez (2016) diz que o método chamado de Algoritmo de Euclides, é um primor do ponto de vista computacional e pouco conseguiu-se aperfeiçoar em mais de dois milênios. Este algoritmo tem a seguinte estrutura:

Dados $a, b \in \mathbb{Z}$ podemos supor $b \leq a$. Se $b = 1$ ou $a = b$, ou ainda $b|a$, já vimos que $(a, b) = b$. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela divisão euclidiana, podemos escrever: $a = bq_1 + r_1$, com $r_1 < b$. Temos duas possibilidades:

- $r_1|b$.

Em tal caso $r_1 = (b, r_1)$ e, pelo Lema (2.2), temos que:

$$r_1 = (b, r_1) = (b, a - q_1b) = (b, a) = (a, b)$$

e o algoritmo termina.

- $r_1 \nmid b$.

Em tal caso, podemos efetuar a divisão de b por r_1 obtendo $b = r_1q_2 + r_2$, com $0 < r_2 < r_1$.

Novamente, temos duas possibilidades:

- $r_2|r_1$. Nesse caso $r_2 = (r_1, r_2)$ e novamente, pelo Lema (2.2):

$$r_2 = (r_1, r_2) = (r_1, b - q_2r_1) = (r_1, b) = (a - q_1b, b) = (a, b)$$

e paramos, pois, termina o algoritmo.

- $r_2 \nmid r_1$. Nesse caso, podemos efetuar a divisão de r_1 por r_2 obtendo $r_1 = r_2q_3 + r_3$, com $0 < r_3 < r_2$.

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais $a > r_1 > r_2 > \dots$ que não possui menor elemento, o que não é possível pela Princípio da Boa Ordem.

Logo, para algum n , temos que $r_n|r_{n-1}$, o que implica que $(a, b) = r_n$.

O algoritmo demonstrado a cima é praticado no processo de divisões sucessivas

conhecido como jogo da velha. o mesmo pode ser sintetizado e mostrado na pratica como mostrado a seguir.

Iniciando a divisão de a por b teremos um quociente q_1 e um resto r_1 . Colocando as variáveis envolvidas no diagrama abaixo, fica:

	q_1	
a	b	
r_1		

Agora realizando a divisão de b por r_1 encontramos o quociente q_2 e o resto r_2 e colocando no diagrama fica:

	q_1	q_2
a	b	r_1
r_1	r_2	

Prosseguindo o processo até encontrar resto 0, o diagrama ficará da seguinte forma:

Tabela 1 – Diagrama do MDC de a e b .

	q_1	q_2	q_3	$\dots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\dots$	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	$\dots$		r_n	

Fonte: Elaborada pelo autor.

Vejamos a solução do exemplo:

Exemplo 2.21. Calcule o *MDC* de 58 e 14 (58, 14), usando o método descrito acima, popularmente conhecido por "jogo da velha".

Solução: Fazendo o processo de divisões sucessivas, como apresentado acima, e representando no diagrama, teremos:

	4	7
58	14	$2=(58,14)$
2	0	

Como o último resto não nulo é o 2, esse é o máximo divisor comum dos números 58 e 14. ou seja $(58, 14) = 2$.

Exemplo 2.22. Encontre o $(963, 657)$ pelo algoritmo de Euclides, e a sua expressão como combinação linear de 963 e 657.

Solução: Para encontrar a combinação linear, é mais útil escrever os resultados obtidos

utilizando o método descrito acima da seguinte forma:

$$963 = 657 \cdot 1 + 306 \quad (21)$$

$$657 = 306 \cdot 2 + 45 \quad (22)$$

$$306 = 45 \cdot 6 + 36 \quad (23)$$

$$45 = 36 \cdot 1 + 9 \quad (24)$$

$$36 = 9 \cdot 4 + 0. \quad (25)$$

Como o último resto não nulo obtido foi o 9, temos que: $(963, 657) = 9$. Note que por tentativa o par $x = 642$ e $y = -941$ satisfaz a expressão $963x + 657y = 9$ pois:

$$963 \cdot 642 + 657 \cdot (-941) = 618246 - 618237 = 9$$

Observação 2.7. Para encontrar os inteiros m e n que satisfaçam a combinação linear $am + bn = (a, b)$, temos dois caminhos, por tentativas ou pelo processo conhecido como algoritmo de Euclides estendido.

2.9 ALGORITMO DE EUCLIDES ESTENDIDO

O processo conhecido por algoritmo de Euclides estendido é uma ferramenta indispensável para encontrar os valores m e n da combinação linear $m \cdot a + n \cdot b = (a, b)$. Segundo Hefez (2016), quando utilizarmos o algoritmo de Euclides para expressar (a, b) na forma $m \cdot a + n \cdot b$ com m e $n \in \mathbb{Z}$, referir-nos-emos a ele como Algoritmo de Euclides estendido. Portanto para encontrarmos os inteiros m e n que satisfaçam a combinação linear $m \cdot a + n \cdot b = (a, b)$, devemos usar o algoritmo de Euclides de trás para frente. A partir do último resto não nulo que é o *MDC*, montamos a nossa primeira expressão, a partir daí vamos substituindo os restos imediatamente anteriores, chegando ao final do processo teremos a expressão $m \cdot a + n \cdot b = (a, b)$, ou seja, uma combinação do máximo divisor comum dos inteiros a e b .

Vejam os a solução do exemplo anterior, usando o processo do algoritmo de Euclides estendido.

Exemplo 2.23. Encontre os inteiros m e n tais que $936 \cdot m + 657 \cdot n = 9 = (936, 657)$

Solução: Para encontrar a combinação linear, é mais útil escrever os resultados obtidos

utilizando o método do algoritmo de Euclides da seguinte forma:

$$963 = 657 \cdot 1 + 306 \quad (26)$$

$$657 = 306 \cdot 2 + 45 \quad (27)$$

$$306 = 45 \cdot 6 + 36 \quad (28)$$

$$45 = 36 \cdot 1 + 9 \quad (29)$$

$$36 = 9 \cdot 4 + 0. \quad (30)$$

Como o último resto não nulo obtido foi o 9, temos que: $(963, 657) = 9$. A expressão linear se obtêm substituindo:

$$36 = 306 - 45 \cdot 6,$$

em (29), obtendo

$$9 = 45 - (306 - 45 \cdot 6) = 45 \cdot 7 - 306. \quad (31)$$

Agora devemos substituir o resto anterior a 36, que é 45, por:

$$45 = 657 - 306 \cdot 2,$$

em (31), obtendo:

$$9 = (657 - 306 \cdot 2) \cdot 7 - 306 = 657 \cdot 7 - 306 \cdot 15 \quad (32)$$

Agora devemos substituir o resto anterior a 45, que é 306 por:

$$306 = 963 - 657,$$

em (32), obtendo:

$$9 = 657 \cdot 7 - 306 \cdot 15 = 657 \cdot 7 - 15 \cdot (963 - 657) = 22 \cdot 657 - 15 \cdot 963.$$

Ou seja:

$$(963, 657) = 9 = 963(-15) + 657(22),$$

onde $x = -15$ e $y = 22$.

O processo apresentado também será bastante útil para calcular o inverso multiplicativo de um número; resultado que será aplicado como uma das etapas para o processo de codificação de uma mensagem, pelo processo de criptografia RSA.

Para mais detalhes veja Alencar Filho (1981), Nascimento (2013) e Coutinho (2005).

2.10 MÍNIMO MÚLTIPLO COMUM

Agora apresentaremos a definição de mínimo múltiplo comum (MMC), suas propriedades básicas e uma proposição que mostra que MMC e MDC são dependentes um do outro, são uma espécie de operação inversa, ou seja, se tivermos um deles, podemos encontrar o outro.

Definição 2.3. (Mínimo Múltiplo Comum). Sejam a e b inteiros diferentes de zero. O mínimo múltiplo comum, resumidamente MMC , entre a e b é o inteiro positivo m que satisfaz as seguintes condições:

1. m é um múltiplo comum de a e b , isto é, $a|m$ e $b|m$;
2. se c é um múltiplo comum de a e b , então $m|c$.

Se c é um múltiplo comum de a e b , então, da condição (2) da definição acima, temos que $m|c$, e, portanto, $m \leq c$, o que nos diz que o mínimo múltiplo comum, se existe, é único e é o menor dos múltiplos comuns de a e b .

O mínimo múltiplo comum de a e b , se existe, será denotado por $[a, b]$. Caso exista $[a, b]$ é fácil mostrar que

$$[-a, b] = [a, -b] = [-a, -b] = [a, b].$$

Portanto, para efeito do cálculo do MMC de dois números, podemos sempre os supor não negativos, como fizemos com o MDC .

É também fácil verificar que $[a, b] = 0$ se, e somente se, $a = 0$ ou $b = 0$. De fato, se $[a, b] = 0$, então 0 divide $a \cdot b$, que é múltiplo de a e de b , logo $a \cdot b = 0$ e, portanto, $a = 0$ ou $b = 0$.

Reciprocamente, se $a = 0$ ou $b = 0$ então 0 é o único múltiplo comum de a e b , logo $[a, b] = 0$.

Proposição 2.12. *Dados dois números inteiros a e b , temos que $[a, b]$ existe e*

$$(a, b)[a, b] = ab.$$

Demonstração: Ponhamos $m = \frac{ab}{(a, b)}$. Como

$$m = a \frac{b}{(a, b)} = b \frac{a}{(a, b)},$$

temos que $a|m$ e $b|m$.

Seja c um múltiplo comum de a e b ; logo, $c = na = n'b$. Segue daí que:

$$c = n \frac{a}{(a, b)} = n' \frac{b}{(a, b)}.$$

Como, $\frac{a}{(a, b)}$ e $\frac{b}{(a, b)}$ são primos entre si, segue-se, que $\frac{a}{(a, b)}$ divide n' e,

portanto, $m = \frac{b}{(a,b)}$ divide $n'b$ que é igual a c , como queríamos demonstrar. ■

Vejam os uma aplicação do resultado apresentado na proposição acima na resolução de um problema, para uma melhor fixação do resultado.

Exemplo 2.24. Sabendo que o produto entre dois números inteiros positivos é igual 30000 e o máximo divisor comum entre eles é 50. Qual o mínimo múltiplo comum desses dois números?

Solução: Pela Proposição (2.12) temos que: $(a,b) \cdot [a,b] = a \cdot b$. Pelos dados do problema, temos que $(a,b) = 50$ e $a \cdot b = 30000$, substituindo os valores na expressão temos que $[a,b] = 30000/50 = 600$. Logo o mínimo múltiplo comum dos números é igual a 600.

O próximo resultado é uma ferramenta que auxilia bastante no cálculo do mínimo múltiplo comum, mostrando o porquê de algumas vezes para encontrar o *MMC*, basta-nos multiplicar os números inteiros positivos envolvidos.

Corolário 2.7. Se a e b são números inteiros primos entre si, então $[a,b] = ab$.

Demonstração: Como a e b são primos, segue-se que $(a,b) = 1$, usando a Proposição (2.12), temos:

$$(a,b) \cdot [a,b] = a \cdot b \implies 1 \cdot [a,b] = ab \implies [a,b] = a \cdot b.$$

Como queríamos demonstrar. ■

Da forma como podemos calcular o *MDC* de vários números, podemos estender também a noção de *MMC* para vários números, como faremos a seguir.

Diremos que um número natural m é o *MMC* dos inteiros não nulos $a_1, a_2, \dots, a_n$, se m é um múltiplo comum de $a_1, a_2, \dots, a_n$, e, se para todo múltiplo comum m_0 desses números, tem-se que $m|m_0$.

Verificamos que o *MMC*, se existe, é único, sendo denotado por $[a_1, a_2, \dots, a_n]$. Além disso, o *MMC* de vários inteiros não nulos é o menor múltiplo comum positivo desses inteiros. O resultado segue da proposição a seguir.

Proposição 2.13. Sejam $a_1, a_2, \dots, a_n$ números naturais. Então existe o número $[a_1, a_2, \dots, a_n]$ e

$$[a_1, \dots, a_{n-2}, a_{n-1}, a_n] = [a_1, \dots, a_{n-2}, [a_{n-1}, a_n]].$$

Demonstração: A demonstração é feita por indução, análoga a forma como fizemos para o *MDC*.

Os resultados apresentados no próximo tópico serão bastante úteis para a compreensão do uso da criptografia RSA, uma das aplicações do Teorema Fundamental da Aritmética. ■

3 RESULTADOS AUXILIARES

Neste capítulo serão apresentados e demonstrados resultados que serão muito utilizados nas demonstrações das aplicações do Teorema Fundamental da Aritmética. Esses resultados terão como base em suas demonstrações os resultados apresentados no capítulo anterior.

Neste capítulo conheceremos uma equação Diofantina linear e como encontrar as suas soluções, quando esta apresentar soluções; conheceremos o conceito de congruência, suas propriedades básicas e os teoremas de Euler e de Fermat, ferramentas estas que serão de suma importância para a compreensão da criptografia RSA que junto ao Teorema Fundamental da Aritmética nos mostra uma aplicação prática desse importante teorema da aritmética em situações práticas do nosso cotidiano. Também apresentaremos o conceito de números primos e suas principais propriedades, como também várias conjecturas e resultados importantes sobre os primos e por fim demonstraremos alguns resultados apresentados por matemáticos famosos que demonstram a sua infinitude.

3.1 EQUAÇÕES DIOFANTINAS LINEARES

Definição 3.1. Equação Diofantina é qualquer equação com uma ou mais incógnitas que assumirem apenas valores inteiros.

Nesse trabalho vamos ver as equações diofantinas lineares mais simples, são as com duas variáveis x e y . São as equações que se apresentam da seguinte forma:

$$ax + by = c,$$

onde a , b e c são inteiros dados.

O termo diofantina se refere ao matemático Diofanto de Alexandria, que viveu no século III; ele foi o primeiro a estudar tais tipos de equações.

Todo par de inteiros x_0 e y_0 é solução da equação, se satisfaz a equação, ou seja:

$$ax_0 + by_0 = c.$$

Exemplo 3.1. Determine a solução da equação diofantina linear com duas variáveis, $2x + 5y = 19$.

Solução: Note que os pares $(2, 3)$, $(7, 1)$ e $(12, -1)$ são soluções da equação, pois:

$$\begin{aligned} 2 \cdot 2 + 5 \cdot 3 &= 19 \\ 2 \cdot 7 + 5 \cdot 1 &= 19 \\ 2 \cdot 12 + 5 \cdot (-1) &= 19. \end{aligned}$$

Observação 3.1. Existem equações diofantinas que não possuem soluções inteiras.

Exemplo 3.2. A equação diofantina linear com duas variáveis $4x + 6y = 11$ não possui solução. Pois quaisquer valores inteiros atribuído as variáveis x e y , teremos sempre um resultado par, pelas propriedades de paridade dos números inteiros.

Teorema 3.1. *A equação diofantina linear $ax + by = c$ tem solução se, e somente se, $(a, b) | c$.*

Demonstração: Suponha que a equação $ax + by = c$ tem solução, isto é, existe o par de inteiro x_0 e y_0 , tal que $ax_0 + by_0 = c$. Seja $d = (a, b)$, logo pela conceito de divisibilidade existem os inteiros r e s tal que $a = dr$ e $b = ds$. Assim teremos que:

$$\begin{aligned} c &= ax_0 + by_0 \\ &= drx_0 + dsy_0 \\ &= d(rx_0 + sy_0). \end{aligned}$$

Logo $d = (a, b) | c$.

Suponha que $d = (a, b) | c$, ou seja $c = qd$ com $q \in \mathbb{Z}$.

Por ser d o *MDC* de a e b , temos que existem os inteiros x_0 e y_0 tal que $ax_0 + by_0 = d$, pelo Teorema de Bézout. O que implica que:

$$c = dq = (ax_0 + by_0)q = a(x_0q) + b(y_0q).$$

Isto é, o par de inteiros:

$$x = qx_0 = (c/d)x_0 \text{ e } y = qy_0 = (c/d)y_0,$$

é solução da equação diofantina linear $ax + by = c$, como queríamos demonstrar. ■

Teorema 3.2. *Sendo $d = (a, b)$ e se $d | c$ na equação diofantina $ax + by = c$ e, se o par x_0 e y_0 é solução particular da equação, então todas as outras soluções são da forma $x = x_0 + (b/d)t$ e $y = y_0 + (a/d)t$ onde $t \in \mathbb{Z}$.*

Demonstração: Suponha que o par de inteiros x_0 e y_0 é solução particular da equação $ax + by = c$ e seja x_1 e y_1 uma outra solução da equação. Então temos que:

$$ax_0 + by_0 = c = ax_1 + by_1,$$

e portanto

$$ax_0 + by_0 = ax_1 + by_1.$$

Como $(a, b) = d$ existem inteiros r e s tais que $a = dr$ e $b = ds$, com r e s primos entre si. Substituindo esses valores na igualdade anterior, e fazendo os devidos cancelamentos, fica:

$$\begin{aligned} drx_0 + dsy_0 &= drx_1 + dsy_1 \implies rx_0 + sy_0 = rx_1 + sy_1 \\ &\implies r(x_0 - x_1) = s(y_1 - y_0). \end{aligned}$$

Como $r|s(y_1 - y_0)$ e como r e s são primos entre si, então $r|(y_1 - y_0)$. Ou seja

$$(y_1 - y_0) = rq,$$

com $q \in \mathbb{Z}$.

E de forma análoga:

$$(x_0 - x_1) = sq,$$

com $q \in \mathbb{Z}$.

Portanto teremos as fórmulas:

$$x_1 = x_0 - sq = x_0 - (b/d)q$$

e

$$y_1 = y_0 + rq = y_0 + (a/d)q,$$

com $q \in \mathbb{Z}$. Como queríamos demonstrar. ■

Estes valores de x_1 e y_1 , satisfazem realmente a equação $ax + by = c$ pois substituindo na equação, teremos:

$$\begin{aligned} ax_1 + by_1 &= a(x_0 - (b/d)q) + b(y_0 + (a/d)q) \\ &= ax_0 + by_0 + (ab/d - ab/d)q \\ &= c + 0q \\ &= c \end{aligned}$$

Com isso vemos que existem infinitas soluções para uma equação diofantina linear, uma para cada $t \in \mathbb{Z}$

Corolário 3.1. *Se $(a, b) = 1$ e x_0 e y_0 é uma solução particular de $ax + by = c$ então todas as outras soluções dessa equação são da forma:*

$$x = x_0 + bt$$

e

$$y = y_0 - at,$$

com $t \in \mathbb{Z}$

Demonstração: Basta fazer $d = 1$ no Teorema (3.2) e teremos o resultado desejado. ■

Observação 3.2. Uma solução particular de uma equação diofantina linear se obtém por tentativa ou pelo algoritmo de Euclides estendido e em ambos os casos a solução geral se obtém aplicando o Teorema (3.2).

Vejamos algumas aplicações dos resultados apresentados nos exemplos a seguir.

Exemplo 3.3. Determine todas as soluções da equação diofantina linear $15x - 3y = 6$.

Solução: Como $(15, 3) = 3$ e como $3|6$ a equação possui solução.

Note que $x = 2$ e $y = 8$ é uma solução particular da equação, pois:

$$15 \cdot 2 - 3 \cdot 8 = 30 - 24 = 6.$$

Logo pelo Teorema (3.2) as soluções são:

$$x = 2 + t$$

e

$$y = 8 + 5t,$$

com $t \in \mathbb{Z}$.

Exemplo 3.4. Determine todas as soluções inteiras da equação diofantina linear

$$18x + 5y = 48.$$

Solução: Usando o algoritmo de Euclides temos que:

$$18 = 5 \cdot 3 + 3 \tag{33}$$

$$5 = 3 \cdot 1 + 2 \tag{34}$$

$$3 = 2 \cdot 1 + 1 \tag{35}$$

$$2 = 2 \cdot 1 + 0. \tag{36}$$

Para achar a combinação linear de 18 e 5, basta substituir a expressão:

$$2 = 5 - 3$$

em (35) e encontramos:

$$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot 3 - 5, \quad (37)$$

Agora substituindo

$$3 = 18 - 5 \cdot 3,$$

em (37) e teremos:

$$1 = 2(18 - 5 \cdot 3) - 5 = 2 \cdot 18 + 5 \cdot (-7). \quad (38)$$

Ou seja:

$$1 = 18 \cdot 2 + 5 \cdot (-7).$$

Multiplicando o resultado por 48, fica conforme o desejado:

$$48 = 18 \cdot 96 + 5 \cdot (-336).$$

Portanto o par de inteiros $x_o = 96$ e $y_o = -336$ é uma solução particular da equação. Aplicando o Corolário (3.1) teremos como solução geral:

$$x = 96 + 5t$$

e

$$y = -336 - 18t.$$

Com $t \in \mathbb{Z}$.

Para maiores detalhes, consulte Alencar Filho (1981).

3.2 ARITMÉTICA MODULAR

Para iniciar o tópico que trata sobre aritmética modular, comecemos com a seguinte pergunta, "em que situação $8+5=1$?". Se essa pergunta for feita a um de nossos alunos, provavelmente vão pensar que estamos ficando loucos. Mas se colocarmos a mesma operação dentro de contexto da seguinte situação problema: João iniciou uma prova pra concurso que teve início as 8 horas da manhã e sabendo que a mesma tem 5 horas de duração. Que horário João terminará a prova? Certamente eles concordarão com a operação. Segundo Coutinho (2005) Isso não é privilegio das horas; qualquer fenômeno cíclico vai produzir uma aritmética peculiar.

E a aritmética relacionada com esse tipo de fenômeno é conhecida como aritmética modular. Os resultados apresentados relacionados a aritmética modular será de suma importância para a compreensão da aplicação do Teorema Fundamental da Aritmética junto a criptografia RSA.

Definição 3.2. Seja $m \in \mathbb{N}$, diremos que dois números inteiros a e b são congruentes módulo m se os restos de suas divisões euclidianas por m são iguais, quando isso ocorrer representaremos: por

$$a \equiv b \pmod{m}.$$

Exemplo 3.5. $23 \equiv 11 \pmod{3}$ pois os restos das divisões de 23 por 3 e 11 por 3 são iguais a 2.

Quando os restos forem diferentes diremos que os números são incongruentes e representaremos por:

$$a \not\equiv b \pmod{m}.$$

Observação 3.3. Como o resto da divisão de qualquer número inteiro por 1 é sempre 0, teremos que $a \equiv b \pmod{1}$, o que torna desinteressante a matemática modular dos restos. Assim consideraremos sempre $m > 1$

Proposição 3.1. *Seja a, b e $m \in \mathbb{Z}$, com $m > 1$. tem-se que $a \equiv b \pmod{m}$ se, e somente se $m \mid b - a$.*

Demonstração: As divisões euclidianas de a e b por m são respectivamente:

$$a = mq_1 + r_1$$

e

$$b = mq_2 + r_2.$$

Logo

$$b - a = m(q_1 - q_2) + (r_1 - r_2).$$

Portanto, $a \equiv b \pmod{m}$ se, e somente se, $r_1 = r_2$, o que em vista da igualdade acima, é equivalente a dizer que $m \mid b - a$, já que $|r_1 - r_2| < m$. ■

Da definição temos que a congruência módulo um inteiro fixo m é uma relação de equivalência, vejamos a proposição abaixo.

Proposição 3.2. *Se a, b, c e m são números inteiros, com $m > 0$, as sentenças a seguir são verdadeiras:*

1. $a \equiv a \pmod{m}$;
2. Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$;
3. Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração: Dado que $m \mid 0$, então $m \mid a - a$, portanto $a \equiv a \pmod{m}$.

Se $a \equiv b \pmod{m}$, então $a - b = tm$ para t inteiro. Portanto:

$$b - a = -tm \Rightarrow b \equiv a \pmod{m},$$

Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então existem k_1 e k_2 inteiros tais que $a = k_1m + b$ e $b = k_2 \cdot m + c$, o que implica que:

$$a - b = k_1m;$$

e

$$b - c = k_2m.$$

Ao somarmos membro a membro as duas ultimas equações, temos:

$$(a - b) + (b - c) = k_1m + k_2m,$$

ou seja,

$$a - c = (k_1 + k_2)m,$$

o que implica que

$$a = (k_1 + k_2)m + c,$$

onde $(k_1 + k_2)m \in \mathbb{Z}$. Portanto, usando a linguagem de congruência, temos que,

$$a \equiv c \pmod{m}.$$

O que conclui nossa demonstração. ■

Proposição 3.3. *Sejam a, b, c e m números inteiros tais que $a \equiv b \pmod{m}$, então:*

1. $a + c \equiv b + c \pmod{m}$;
2. $a \cdot c \equiv b \cdot c \pmod{m}$.

Demonstração:

1. Como $a \equiv b \pmod{m}$, então $m|a - b$. Logo,

$$m|a - b + c - c,$$

reordenando os termos de forma conveniente, temos que

$$m|(a + c) - (b + c).$$

Portanto $a + c \equiv b + c \pmod{m}$.

2. Como:

$$a \equiv b \pmod{m},$$

temos que $m|a - b$, logo existe $q \in \mathbb{Z}$ tal que $a - b = m \cdot q$ e pelas propriedades de divisibilidade, temos que:

$$(a - b) \cdot c|m \cdot q \cdot c.$$

Portanto

$$a \cdot c - b \cdot c | m \cdot (qc),$$

onde $q \cdot c \in \mathbb{Z}$. Assim,

$$ac \equiv bc \pmod{m}.$$

O que conclui a demonstração. ■

Vejamos uma aplicação para uma melhor fixação da proposição apresentada

Exemplo 3.6. Como $23 \equiv 3 \pmod{5}$, então $23 + 1 \equiv 3 + 1 \pmod{5} \implies 24 \equiv 4 \pmod{5}$ e $23 \equiv 3 \pmod{5}$, então $23 \cdot 2 \equiv 3 \cdot 2 \pmod{5} \implies 46 \equiv 6 \pmod{5}$.

Proposição 3.4. *Se a, b, c, d e m são números inteiros, com $m > 1$, temos que:*

1. *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:*

$$a + c \equiv b + d \pmod{m};$$

2. *Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então:*

$$ac \equiv bd \pmod{m}.$$

Demonstração:

Temos que $m|a - b$ e $m|c - d$ assim:

$$a - b = mq_1 \tag{39}$$

e

$$c - d = mq_2, \tag{40}$$

com q_1 e $q_2 \in \mathbb{Z}$. Somando as igualdades (39) e (40) e ordenando os termos de forma conveniente teremos:

$$(a - b) + (c - d) | mq_1 + mq_2 \implies (a + c) - (b + d) | m(q_1 + q_2),$$

onde $(q_1 + q_2) \in \mathbb{Z}$. Daí $m|(a + c) - (b + d)$, portanto, $(a + c) \equiv (b + d) \pmod{m}$.

De $a \equiv b \pmod{m}$ temos que:

$$a = b + mk_1.$$

De $b \equiv c \pmod{m}$ temos que

$$b = c + mk_2.$$

Multiplicando membro a membro os resultados obtidos teremos:

$$ab = bc + bmk_2 + cmk_1 + m^2k_1k_2,$$

colocando m em evidência teremos:

$$ab = cd + m(k_1 + k_2 + mk_1k_2),$$

onde $(k_1 + k_2 + mkk_1) \in \mathbb{Z}$. Assim

$$ab \equiv cd \pmod{m},$$

o que conclui a demonstração. ■

Vejamos uma aplicação do resultado apresentado:

Exemplo 3.7. Se $10 \equiv 3 \pmod{7}$ e $9 \equiv 2 \pmod{7}$ pela propriedade anterior, teremos que:

$$10 + 9 \equiv 3 + 2 \pmod{7} \implies 19 \equiv 5 \pmod{7}$$

e

$$10 \cdot 9 \equiv 3 \cdot 2 \pmod{7} \implies 90 \equiv 6 \pmod{7}.$$

Corolário 3.2. Para todo a e $b \in \mathbb{Z}$ e $n \in \mathbb{N}$, então temos que:

$$a \equiv b \pmod{m} \implies a^n \equiv b^n \pmod{m}.$$

Demonstração: Utilizando o 1º princípio de indução finita sobre n .

(Caso base) Para $n = 1$, temos que a afirmação é verdadeira pois $a^1 = a$ e $b^1 = b$

(Hipótese de indução) Supondo verdade que se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$, para algum $n > 1$ com $n \in \mathbb{N}$,

(Tese) Devemos mostrar que a afirmação é válida para $n + 1$. Ou seja,

$$a^{n+1} \equiv b^{n+1}.$$

Como $a \equiv b \pmod{m}$ e $a^n \equiv b^n \pmod{m}$, então pela Proposição 2.9 item 2, temos que:

$$aa^n \equiv bb^n \pmod{m} \implies a^{n+1} \equiv b^{n+1} \pmod{m}.$$

Demonstrando assim a afirmação para $(n+1)$. Logo a afirmação é válida para todo $n \in \mathbb{N}$. Concluindo aqui nossa demonstração por indução finita. ■

Vejamos a aplicação do corolário apresentado no exemplo a seguir.

Exemplo 3.8. Se $12 \equiv 2 \pmod{5}$, temos que $12^4 \equiv 2^4 \equiv 1 \pmod{5}$.

A próxima proposição, mostra que é válida a lei do cancelamento, quando se trata de uma soma em uma congruência, ou seja caso tenhamos uma congruência e se em cada termo dessa congruência tenhamos uma soma com elementos repetidos em ambos os membros, podemos fazer o cancelamento dos termos repetidos um a um.

Proposição 3.5. *Sejam a, b, c e m números inteiros, com $m > 1$. Temos que:*

$$a + c \equiv b + c \pmod{m} \Leftrightarrow a \equiv b \pmod{m}.$$

Demonstração:

($\Rightarrow$) como $a \equiv b \pmod{m}$ e $c \equiv c \pmod{m}$ pela Proposição (3.4) item (1) temos que

$$(a + c) \equiv (b + c) \pmod{m}$$

($\Leftarrow$) Se $a + c \equiv b + c \pmod{m}$, então $m | b + c - (a + c)$, o que implica que $m | b - a$, ou seja, $a \equiv b \pmod{m}$. ■

Veja a aplicação da proposição no exemplo a seguir.

Exemplo 3.9. Mostre que se $39 \equiv 5 \pmod{17}$ então $35 \equiv 1 \pmod{17}$.

$$39 \equiv 5 \pmod{17} \Leftrightarrow 35 + 4 \equiv 1 + 4 \pmod{17} \Leftrightarrow 35 \equiv 1 \pmod{17}.$$

A Proposição (3.5) mostra que vale a relação do cancelamento em relação a adição, no entanto nem sempre vale no cancelamento quando tratamos de um produto de congruências.

Observação 3.4. Note que $5 \cdot 8 \equiv 10 \cdot 8 \pmod{10}$. Note que se aplicarmos o cancelamento temos que, $5 \equiv 10 \pmod{10}$ o que é falso, pois 5 e 10 deixa restos diferentes na divisão por 10. Logo $5 \not\equiv 10 \pmod{10}$

A proposição a seguir nos mostrará em que condições vale a lei do cancelamento para a multiplicação.

Proposição 3.6. *Dados a, b, c e m números naturais, com $c \neq 0$ e $m > 1$, temos que*

$$ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{(c, m)}}.$$

Demonstração: Como $\frac{m}{(c, m)}$ e $\frac{c}{(c, m)}$ são primos entre si, pelo Corolário (2.4) temos que:

$$ac \equiv bc \pmod{m} \Leftrightarrow m | (b-a)c \Leftrightarrow \frac{m}{c, m} | (b-a) \frac{c}{(c, m)} \Leftrightarrow \frac{m}{(c, m)} | b-a \Leftrightarrow a \equiv b \pmod{\frac{m}{(c, m)}}.$$

Como queríamos demonstrar. ■

Vejamos a solução de um exemplo, para uma melhor fixação da proposição apresentada.

Exemplo 3.10. $5 \cdot 8 \equiv 10 \cdot 8 \pmod{10}$, pelo teorema $5 \equiv 10 \pmod{\frac{10}{(8, 10)}}$. Como $(8, 10) = 2$

então:

$$5 \equiv 10 \pmod{\frac{10}{2}} \Rightarrow 5 \equiv 10 \pmod{5}.$$

Corolário 3.3. *Dados a, b, c e m números naturais, com $m > 1$ e $(c, m) = 1$, tem-se que $ac \equiv bc \pmod{m} \Leftrightarrow a \equiv b \pmod{m}$.*

Demonstração: O resultado segue imediatamente da Proposição (3.6), pois quando $(c, m) = 1$, teremos que $\pmod{\frac{m}{(c, m)}} = \pmod{m}$ e o resultado segue. Como queríamos demonstrar. ■

Vejam os uma aplicação do resultado apresentado no Corolário (3.3) para uma melhor compreensão do resultado apresentado.

Exemplo 3.11. Se $3 \cdot 5 \equiv 7 \cdot 5 \pmod{2}$ como $(5, 2) = 1$ pelo Corolário (3.3) teremos que $3 \equiv 7 \pmod{2}$.

Observação 3.5. Assim, dada a congruência $ac \equiv bc \pmod{m}$, só se aplica a lei do cancelamento de forma direta se, e somente se, $(c, m) = 1$.

Proposição 3.7. *Sejam $a, k, m \in \mathbb{Z}$ e $(k, m) = 1$. Se $a_1, a_2, \dots, a_m$ é um sistema completo de resíduos módulo m , então*

$$a + ka_1, a + ka_2, \dots, a + ka_m,$$

também é um sistema completo de resíduos módulo m .

Demonstração: Como do Corolário (3.3) para $i, j = 0, \dots, (m - 1)$, temos que:

$$\begin{aligned} a + ka_i \equiv a + ka_j \pmod{m} &\Leftrightarrow ka_i \equiv ka_j \pmod{m} \\ &\Leftrightarrow a_i \equiv a_j \pmod{m} \\ &\Leftrightarrow i = j. \end{aligned}$$

O que mostra que $a + ka_1, \dots, a + ka_m$ são, dois a dois, não congruentes módulo m e, portanto formam um sistema completo de resíduos módulo m . Encerrando assim a demonstração. ■

Vejam os exemplo para uma melhor compreensão do resultado apresentado.

Exemplo 3.12. Note que o conjunto $\{0, 1, 2, 3, 4, 5\}$ é um sistema completo de resíduos módulo 6 e como $(5, 6) = 1$ a sequência:

$$2 + 5 \cdot 0; 2 + 5 \cdot 1; 2 + 5 \cdot 2; 2 + 5 \cdot 3; 2 + 5 \cdot 4; 2 + 5 \cdot 5 = 2; 7; 12; 17; 22; 27,$$

forma também um sistema reduzido de resíduos módulo 6 pela proposição anterior.

A próxima proposição será importante na demonstração do uso da criptografia RSA, no processo de codificação e decodificação.

Proposição 3.8. *Sejam, $a, b \in \mathbb{Z}$ e $n, m, m_1, \dots, m_r$ inteiros maiores do que 1. Temos que:*

1. *Se $a \equiv b \pmod{m}$ e $n|m$, então $a \equiv b \pmod{n}$;*
2. *Se $a \equiv b \pmod{m_i}$, para todo $i = 1, 2, \dots, r \Leftrightarrow a \equiv b \pmod{[m_1 \cdot \dots \cdot m_r]}$.*
3. *Se $a \equiv b \pmod{m}$ então $(a, m) = (b, m)$*

Demonstração:

1. Como $a \equiv b \pmod{m}$, temos que $m|a - b$. Além disso, como $n|m$, temos que $n|a - b$ por transitividade. Logo, $a \equiv b \pmod{n}$.
2. ($\Rightarrow$) Se $a \equiv b \pmod{m_i}$, $i = 1, \dots, r$, então $m_i|a - b$, para todo i . Sendo $a - b$ um múltiplo de cada m_i , temos que $[m_1, \dots, m_r]|a - b$. Logo, $a \equiv b \pmod{[m_1, \dots, m_r]}$. ($\Leftarrow$) se $a \equiv b \pmod{[m_1, \dots, m_r]}$, então $[m_1, \dots, m_r]|a - b$. Além disso, $m_i|[m_1, \dots, m_r]$, portanto, $m_i|a - b$. Logo, $a \equiv b \pmod{m_i}$.
3. Se $a \equiv b \pmod{m} \Rightarrow m|b - a$ e, portanto, $b = a + mt$ com $t \in \mathbb{Z}$ assim pelo Lema de Euclides temos:

$$(b, m) = (m, b) = (m, a + mt) = (m, a) = (m, a).$$

Concluindo assim a demonstração. ■

Proposição 3.9. *Sejam a e m números inteiros, com $m > 1$. Existe x_0 inteiro com $ax_0 \equiv 1 \pmod{m}$ se, e somente se, $(a, m) = 1$. Além disso, x é uma solução da congruência se, e somente se, $x \equiv x_0 \pmod{m}$.*

Demonstração: A congruência tem solução se, e somente se, $m|ax_0 - 1$, o que equivale a equação Diofantina $aX - mY = 1$ que só possui solução se $(a, m) = 1$ pelo Teorema de Bézout. Por outro lado, se x_0 e x são soluções da congruência

$$aX \equiv 1 \pmod{m} \implies ax \equiv ax_0 \pmod{m}.$$

Como $(a, m) = 1$, pelo Corolário (3.3), podemos fazer o cancelamento de a , assim $x \equiv x_0 \pmod{m}$ o que mostra que x também é solução da mesma congruência, pois

$$ax \equiv ax_0 \equiv 1 \pmod{m}.$$

O que conclui a demonstração. ■

O resultado apresentado será muito utilizado em aritmética modular para o desenvolvimento de várias outras demonstrações importantes.

Para uma melhor compreensão do resultado, vejamos o exemplo abaixo:

Exemplo 3.13. A congruência $8x \equiv 1 \pmod{2}$ não possui solução já que $(8, 2) = 2$, e como $2 \nmid 1$ pela definição de divisibilidade. Dessa forma a equação Diofantina $8x - 2y = 1$ não possui solução inteira.

Definição 3.3. Dizemos que a é invertível módulo m quando $(a, m) = 1$. E o seu inverso, chamado de inverso multiplicativo de a módulo m , é o número b tal que $ab \equiv 1 \pmod{m}$.

Exemplo 3.14. Como $4 \cdot 2 \equiv 1 \pmod{7}$, temos que 2 é o inverso multiplicativo de 4 módulo 7.

Note que nem todo inteiro tem um inverso módulo m . Veja o exemplo a seguir:

Exemplo 3.15. O número 2 não tem inverso módulo 4, porque a congruência linear $2x \equiv 1 \pmod{4}$ não tem solução. Pois como a congruência é equivalente a equação diofantina $2x - 4y = 1$ e pela proposição 3.9, a equação só possui solução se, e somente se, $(2, 4) = 2$ divide 1, o que não ocorre pelas propriedades de divisibilidade.

Definição 3.4. Um sistema completo de resíduos módulo m é todo conjunto de inteiros tais que os restos pela divisão por m deixam como restos os elementos do conjunto $(0, 1, 2, \dots, m-1)$.

Vejamos o exemplo pra melhor compreensão da definição.

Exemplo 3.16. Os conjuntos $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$ e $B = \{24, 73, 10, 43, 84, 103, 46, 87\}$ são sistemas completos de resíduos módulo 8 pois são congruos a $\{0, 1, 2, 3, 4, 5, 6, 7\}$ na divisão por 8.

Definição 3.5. Um sistema reduzido de resíduos módulo m é o conjunto de inteiros $\{r_1, r_2, \dots, r_s\}$ tais que:

- $(r_i, m) = 1$ para todo $i = 1, 2, \dots, s$
- $r_i \not\equiv r_j \pmod{m}$ para todo $i \neq j$.
- Para cada $a \in \mathbb{Z}$ tal que $(a, m) = 1$ existe i tal que $a \equiv r_i \pmod{m}$.

Vejamos o exemplo a seguir.

Exemplo 3.17. O conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8. O subconjunto de A formado pelos elementos $\{1, 3, 5, 7\}$ forma o sistema reduzido de resíduos módulo 8, pois $(1, 8) = (3, 8) = (5, 8) = (7, 8) = 1$.

Definição 3.6. A função de Euler denotada por $\varphi(n)$, onde $\varphi(n)$ é o número de inteiros q tais que $q < n$ e $(q, n) = 1$.

Exemplo 3.18. $\varphi(11) = 10$. Pois o conjunto formado pelos elementos $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, temos que: $(1, 11) = (2, 11) = (3, 11) = \dots = (10, 11) = 1$.

Exemplo 3.19. $\varphi(12) = 4$. Pois o conjunto formado pelos elementos $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, temos que, somente os elementos $\{1, 5, 7, 11\}$ são primos com o número 12.

Observação 3.6. se p é primo $\varphi(p) = p - 1$.

Proposição 3.10. Sejam m e n números naturais tais que $(m, n) = 1$. Então $\varphi(mn) = \varphi(m)\varphi(n)$.

Demonstração: Sejam dois inteiros positivos m e n tais que $(m, n) = 1$. Note que a

proposição é verdadeira se m ou n é igual a 1, pois temos que:

$$\begin{aligned}(1 \cdot m) &= \varphi(m) = 1 \cdot \varphi(m) = \varphi(1) \cdot \varphi(m) \\ (1 \cdot n) &= \varphi(n) = 1 \cdot \varphi(n) = \varphi(1) \cdot \varphi(n).\end{aligned}$$

Suponhamos pois $m > 1$ e $n > 1$. Nesse caso vamos considerar os inteiros $1, 2, 3, \dots, mn$, onde $(m, n) = 1$, dispostos em n colunas com m elementos em cada uma delas, como representado na Tabela (2) abaixo:

Tabela 2 – Elementos organizados em n colunas, com m elementos em cada.

1	2	$\dots$	r	$\dots$	n
$1+n$	$2+n$	$\dots$	$r+n$	$\dots$	$2n$
$1+2n$	$2+2n$	$\dots$	$r+2n$	$\dots$	$3n$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$1+(m-1)n$	$2+(m-1)n$	$\dots$	$r+(m-1)n$	$\dots$	mn

Fonte: Elaborada pelo autor.

Seja t um elemento da tabela, devemos ter que $(t, m \cdot n) = 1$, o que só ocorre se, e somente se, $(t, m) = 1$ e $((t, n) = 1)$, pelo Corolário (2.5) apresentado. Dessa forma para calcular $\varphi(mn)$, devemos encontrar na tabela os elementos da tabela que são primos com m e n .

Note que na primeira linha temos um sistema completo de resíduos módulo n , e sabemos pelo lema de Euclides que $(q \cdot r + n, r) = (n, r)$.

Daí concluímos desses dois resultados que, se um elemento da primeira linha é primo com n , então toda a coluna em que ele se encontra também é primo com n , logo os elementos primos com n , estão nas $\varphi(n)$ colunas.

Vejamos agora quais dos elementos dessas $\varphi(n)$ colunas são primos com m .

Veja que em cada uma das $\varphi(n)$ colunas, existem m elementos que formam um sistema completo de resíduos modulo m , pela Proposição (3.7), como podemos observar na sequência abaixo:

$$r, r + n, r + 2n, \dots, r + (m - 1)n.$$

Portanto existem $\varphi(m)$ elementos de cada coluna $\varphi(n)$ que são primos com m , assim os inteiros da tabela que são primos com n e m , isto é que são primos com $n \cdot m$ é igual a $\varphi(n) \cdot \varphi(m)$. Portanto $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$, como queríamos demonstrar. ■

Vejamos o exemplo abaixo para uma melhor compreensão do resultado apresentado.

Exemplo 3.20. Qual o valor de $\varphi(5 \cdot 8)$?

Solução: Note que $(5, 8) = 1$. Logo pela Proposição (3.10), temos que:

$$\varphi(5 \cdot 8) = \varphi(5) \cdot \varphi(8) = 4 \cdot 4 = 16.$$

Portanto $\varphi(5 \cdot 8)$ é igual a 16.

Proposição 3.11. *Seja $r_1, \dots, r_{\varphi(m)}$ um sistema reduzido de resíduos $\pmod m$ e seja $a \in \mathbb{Z}$ tal que $(a, m) = 1$. Então $a \cdot r_1, \dots, a \cdot r_{\varphi(m)}$ é um sistema de resíduos $\pmod m$.*

Demonstração: Seja $a_1, \dots, r_m$ um sistema completo de resíduos $\pmod m$ do qual foi tirado o sistema reduzido de resíduos $r_1, \dots, r_{\varphi(m)}$. Do fato de $(a, m) = 1$, tem-se que $(a_i, m) = 1$ se, e somente se, $(a \cdot a_i, m) = 1$. O que conclui a demonstração. ■

3.3 NÚMEROS PRIMOS

A compreensão dos resultados apresentados sobre números primos é de fundamental importância para a compreensão do Teorema Fundamental da Aritmética, pois sua demonstração, tanto existência, quanto unicidade tomará como base propriedade dos números primos.

Definição 3.7. (Número Primo). Um número maior do que 1 que só possui como divisores 1 e ele próprio é chamado de número primo.

Dados dois números primos p e q e, um número inteiro a qualquer, decorrem da definição acima os seguintes fatos:

1° Se $p|q$, então $p = q$.

Demonstração:

De fato, como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$. ■

2° Se $p \nmid a$, então $(p, a) = 1$.

Demonstração:

De fato, se $(p, a) = d$, temos que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois p não divide a e, conseqüentemente, $d = 1$. ■

Um número maior do que 1 e que não é primo será chamado número composto. Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $1 < n_1 < n$. Logo, existirá um número natural n_2 tal que $n = n_1 n_2$, com $1 < n_1 < n$ e, $1 < n_2 < n$.

Exemplo 3.21. Os números 2, 3, 5, 7, 11, 13 e 59 são números primos, enquanto que 4, 6, 8, 9, 10, 12 e 15 são compostos.

Observação 3.7. O número 1 não é primo e nem composto e todo número primo é ímpar, exceto o primo 2.

A proposição a seguir, mostra uma propriedade muito importante dos números primos, segundo Coutinho (2005) já conhecida pelos Gregos antigos e aparece como

proposição 30 do livro VII dos Elementos de Euclides.

Proposição 3.12 (Lema de Euclides). *Sejam $a, b, p \in \mathbb{Z}$ com p primo. Se $p|ab$, então: $p|a$ ou $p|b$.*

Demonstração: Se $p|a$, nada há o que demonstrar, pois o resultado segue.

Suponhamos então que p não divide a , logo são ditos primos entre si, ou seja, $(a, p) = 1$. Logo se tem que $p|b$, pelo Lema de Gauss, o que conclui a demonstração. ■

Vejamos o exemplo para uma melhor compreensão do resultado.

Exemplo 3.22. Note que $7|140 \cdot 92$. Logo pelo Lema de Euclides, $7|140$ ou $7|92$, como $7 \nmid 92$ pelos critérios de divisibilidade por 7, então $7|140$.

O próximo resultado mostra uma aplicação direta do Lema de Euclides e que será usado na demonstração do teorema principal desse trabalho.

Corolário 3.4. *Se $p, p_1, \dots, p_n$ são números primos e, se $p|p_1 \cdot \dots \cdot p_n$, então $p = p_i$, para algum $i = 1, \dots, n$.*

Demonstração: Aplicando o Princípio de Indução Finita sobre n .

- (caso base) Para $n = 1$, temos que se $p|p_1$, temos que $p = p_1$.
- (hipótese de indução) Supondo que se $p|p_1 \cdot \dots \cdot p_n$ então $p = p_k$ para algum $k = 1, 2, \dots, n$.
- (tese) Devemos mostrar que se $p|p_1 \cdot \dots \cdot p_n \cdot p_{n+1}$ então $p = p_k$ para algum $k = 1, \dots, n, n+1$.

Sendo $q = p_1 \cdot \dots \cdot p_n$, temos que pela hipótese de indução $p|q$ e $p = p_k$.

Se $p|p_1 \cdot \dots \cdot p_n \cdot p_{n+1}$ então $p|q \cdot p_{n+1}$, e pela Proposição (3.12), $p|q$ ou $p|p_{n+1}$.

Como por hipótese, sabemos que se $p|q$, então $p = p_i$ para algum $i = 1, \dots, n$.

Se $p|p_{n+1}$, então $p = p_{n+1}$, logo $p = p_j$ para algum $j = 1, 2, \dots, n, (n+1)$.

Logo a proposição é válida para todo $n \in \mathbb{N}$, como queríamos demonstrar. ■

Corolário 3.5. *Se $p_1 \cdot p_2 \cdot \dots \cdot p_n | a^r$ então, $p_1 \cdot p_2 \cdot \dots \cdot p_n | a$, onde $p_1, p_2, \dots, p_n$ são números primos e n e $r \in \mathbb{Z}$.*

Demonstração: Faremos a demonstração por contra positiva.

Se $p_1 \cdot p_2 \cdot \dots \cdot p_n \nmid a$, então a não é nenhum dos primos $p_1, p_2, \dots, p_n$. Seja p_i com $1 \leq i \leq n$ um desses primos então, p_i não é fator de a^r e, dessa forma não existe p_i com $1 \leq i \leq n$ que divida a^r , o que implica que $p_1 \cdot p_2 \cdot \dots \cdot p_n \nmid a^r$, como queríamos demonstrar. ■

Sabendo que existem infinitos números primos, podemos nos perguntar como obter uma lista contendo os números primos até uma dada ordem. Um dos mais antigos métodos para elaborar tabelas de números primos é devido ao matemático grego Eratóstenes, que viveu por volta de 230 anos antes de Cristo. O método, chamado de Crivo de Eratóstenes, permite determinar todos os números primos até a ordem que se desejar, mas não é muito eficiente para ordens muito elevadas.

Como exemplo, vamos utilizar o crivo de Eratóstenes que segundo Coutinho (2005) é o mais antigo dos métodos para achar primos, e não envolve nenhuma fórmula

explícita.

No dicionário uma das definições da palavra crivo é peneira, logo o crivo de Eratóstenes é uma espécie de peneira para separar os números primos dos números compostos. Para mostrar como funciona esse crivo, vamos encontrar os números primos menores que 150.

O crivo funciona da seguinte forma: Primeiramente, escrevemos todos os números naturais de 2 a 150. Em seguida riscaremos todos os números compostos de acordo com o que segue:

- Primeiro riscamos todos os múltiplos de 2 maiores que 2, que é o primeiro número primo.
- O segundo número primo é o menor número maior que 2 que não foi riscado, isto é, o 3.
- Agora riscamos todos os múltiplos de 3 maiores que 3 (note que alguns já foram riscados). O menor número maior que 3 que ainda não foi riscado, o 5, é o terceiro número primo.
- Riscamos todos os múltiplos de 5 maiores que 5 (os que ainda não foram riscados).
- Riscaremos os múltiplos do 4º número primo (com exceção dele mesmo) que é o menor número maior que 5, que não foi riscado, no caso, o (7).
- Por fim riscamos os múltiplos do próximo número primo depois do 7, no caso o (11).

Após o processo estaremos só com os números primos menores que 150, destacados com (●) conforme tabela abaixo:

Tabela 3 – Primos menores que 150

●2	●3	4	●5	6	●7	8	9	10	●11
12	●13	14	15	16	●17	18	●19	20	21
22	●23	24	25	26	27	28	●29	30	●31
32	33	34	35	36	●37	38	39	40	●41
42	●43	44	45	46	●47	48	49	50	51
52	●53	54	55	56	57	58	●59	60	●61
62	63	64	65	66	●67	68	69	70	●71
72	●73	74	75	76	77	78	●79	80	81
82	●83	84	85	86	87	88	●89	90	91
92	93	94	95	96	●97	98	99	100	●101
102	●103	104	105	106	●107	108	●109	110	111
112	●113	114	115	116	117	118	119	120	121
122	123	124	125	126	●127	128	129	130	●131
132	133	134	135	136	●137	138	●139	140	141
142	143	144	145	146	147	148	●149	150	

Fonte: Elaborada pelo autor.

O Teorema a seguir, devido ao próprio Eratóstenes, nos mostra que para encontrar os primos menores que 150 não precisamos repetir além do número 11, o procedimento descrito acima.

Teorema 3.3. *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.*

Demonstração: Se n é composto então n possui necessariamente um par de inteiros n_1 e n_2 tal que $n = n_1 \cdot n_2$. suponhamos sem perda de generalidade

$$n_1 \leq n_2 \implies n_1 \cdot n_1 \leq n_2 \cdot n_1 \implies n_1^2 \leq n.$$

Pelo Teorema Fundamental da Aritmética, temos que n_1 é primo ou composto, assim temos dois casos a considerar:

- Se n_1 é primo não há mais nada a demonstrar
- Se n_1 é composto $n_1 = p \cdot k$, com $k \in \mathbb{N}$, e p primo. Como o $\max(p, k) < n_1 \leq n_1^2 \leq n$.
O que conclui a demonstração. ■

Vejamos como funciona o teorema apresentado através dos exemplos a seguir.

Exemplo 3.23. Usando o Teorema (3.3), mostre que o número 197 é primo.

Solução: Como $\sqrt{197} \cong 14,03$, devemos verificar se alguns dos primos menores que 14 (2, 3, 5, 7, 11, 13) divide 197. como nenhum dos primos divide 197, então 197 é primo.

Exemplo 3.24. Verifique se o número 259 é primo ou não.

Solução: Note que $\sqrt{259} \cong 16,09$. Agora pelo teorema acima devemos verificar se alguns dos primos menores que 14 (2, 3, 5, 7, 11, 13) divide 259. Como $7|259$, temos que o número 259 é composto.

Note que tanto o crivo de Eratóstenes quanto o teorema apresentado acima nos fornece um teste de primalidade, e são bem eficientes, só que se torna muito trabalhoso a medida em que se aumenta a cardinalidade do conjunto.

Uma questão que se coloca é a forma como os números primos estão distribuídos dentro do conjunto dos números naturais: a medida que consideramos intervalos cada vez maiores de números naturais a densidade dos primos, aumenta ou diminui? o qual estão próximos ou afastados dois números primos? pela tabela apresentada acima vemos que há pares de números primos com duas unidades de diferença, exemplo (3, 5), (5, 7), (11, 13), pares primos com essa propriedade, são definidos como números primos gêmeos. Em contraste com esses primos, existem pares de números primos consecutivos arbitrariamente afastados, ou seja, é possível obter uma sequência de números compostos tão grande quanto se queira e garantir que naquele intervalo não existe nenhum primo, como apresentado no Teorema (3.4) a seguir.

Teorema 3.4. *Dado um número inteiro $n > 1$, é possível determinar n inteiros consecutivos tais que nenhum deles seja primo.*

Demonstração: De fato, dado $n \in \mathbb{N}$, a sequência $(n+1)!+2, (n+1)!+3, (n+1)!+4, \dots,$

$(n+1)! + n + 1$ é uma sequência de números naturais formada por n números compostos, pois o primeiro é múltiplo de 2 e não é igual a 2, o segundo é múltiplo de 3 e não é igual a 3 e assim segue até o último número da sequência que é múltiplo de $(n+1)! + n + 1$ e não é igual a $(n+1)! + n + 1$. ■

Foi o matemático Adrien-Marie Legendre (1752-1833) quem primeiro conjecturou uma certa ordem na distribuição dos números primos, quando observando tabela de números primos viu que $\pi(x)$ podia ser aproximado pela função $\frac{x}{\ln(x)}$, e que essa aproximação seria tanto melhor, quanto maior fosse o natural x . O matemático Carl Friedrich Gauss (1777-1855) também chegou a conjecturar algo semelhante ao que Legendre conjecturou. As ideias de Legendre e Gauss, só foram realmente demonstradas cerca de 100 anos mais tarde. Foi no ano de 1896 que foi demonstrada pela primeira vez, e foram duas demonstrações independentes, uma pelo matemático francês Jacques Hadamard (1865-1963) e outra pelo belga Charles de la Vallée Poussin (1866-1962). Essas demonstrações se baseavam nas ideias de um outro grande matemático do século, Bernhard Riemann (1826-1866). O resultado demonstrado é o famoso teorema dos números primos, que afirma que:

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1.$$

O que torna os números primos interessantes é que sabendo a posição de um número primo não existe um padrão para se chegar ao próximo. É essa distribuição "irregular" dos primos que fez e faz com que muitos matemáticos famosos conjecturassem fórmulas polinomiais para determinar somente números primos dentro do conjunto dos naturais, mas nenhuma das conjecturas criadas consegue cobrir uma infinidade de primos, só funcionam para alguns elementos na sequência do conjunto dos números naturais. Como exemplos bem conhecidos temos as fórmulas(conjecturas):

- Leonhard Euler $n^2 + n + 41$ (só funciona para valores de 0 a 39)
- Mersenne (Só funciona para alguns primos) $M_p = 2^p - 1$.
- Fermat $F_n = 2^{2^n} + 1$ (só funciona para n de 1 a 4)

Observação 3.8. Os maiores primos conhecidos atualmente são os primos da forma $M_p = 2^p - 1$. O maior conhecido até o momento é o 51º número primo de Mersenne, que é o número: $2^{82589933} - 1$. Para se ter uma ideia, esse número é formado por 24862048 dígitos, cerca de 1,5 milhão de que o último número primo descoberto em 2017, o 50º primo de Mersenne: $(2^{77232917} - 1)$.

A distribuição dos números primos ainda envolve muitos mistérios e a esse fato ainda existem muitos problemas em aberto. vejamos alguns:

1. Existem infinitos pares de primos gêmeos?
2. Sempre existe um número primo entre dois números quadrados consecutivos?
3. A sequência de Fibonacci contém infinitos números primos?
4. A famosa conjectura que Goldbach formulou a Euler: todo número inteiro par

maior que ou igual a 4 é a soma de dois números primos?

5. Existem infinitos primos da forma $k^2 + 1$.
6. Primos de Sophie Germain: Um número primo p é um primo de Sophie Germain se $2p + 1$ também é primo. Existem infinitos primos de Sophie Germain? Segundo Hefez (2016) o mais importante problema em aberto em teoria dos números é a hipótese de Riemann. Essa conjectura afirma que a distribuição dos números primos não é aleatória e que segue um padrão descrito por uma equação chamada função zeta de Riemann.

Os próximos resultados mostram algumas demonstrações que atestam a infinitude dos números primos. Existe uma grande quantidade de demonstrações por muitos matemáticos famosos. Apresentaremos a mais famosa, a dada por Euclides de Alexandria em seu livro Os elementos, uma demonstração usando os números de Fermat e por último uma demonstração atribuída ao matemático Francês Charles Hermite (1822-1901), uma demonstração bem simples e direta sobre a infinitude dos números primos.

Teorema 3.5 (Teorema de Euclides). *A quantidade de números primos é infinita.*

Demonstração: Faremos a prova por redução ao absurdo.

Suponha que existe uma quantidade finita de números primos e denotemos estes por $p_1, p_2, p_3, \dots, p_n$. Consideremos o número

$$N = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1.$$

Se chamamos de p o seu menor divisor primo, obviamente p não coincide com nenhum dos números p_i , $1 \leq i \leq n$, pois caso contrário, como ele divide N , teria que dividir 1, pela Proposição (2.2) item (7), o que não pode acontecer, pois todo $p \geq 2$. Logo, temos uma contradição à hipótese de termos uma quantidade finita de primos. ■

Embora os números de Fermat não seja uma boa fonte de números primos pode-se mostrar que existem infinitos números primos através deles pela proposição a seguir

Proposição 3.13. *Se $m \neq n$ então $(f_n, f_m) = 1$.*

Demonstração: Suponhamos sem perda de generalidade que $n > m$, então $n = m + x$, $x \in \mathbb{N}$ como:

$$2^{2^{n+1}} - 1 = (2^{2^n} + 1)((2^{2^n} - 1)),$$

temos,

$$\begin{aligned} (2^{2^{m+x}} - 1) &= ((2^{2^{m+x-1}} + 1)((2^{2^{m+x-1}} - 1))) \\ &= ((2^{2^{m+x-1}} + 1)((2^{2^{m+x-2}} + 1)((2^{2^{m+x-2}} - 1)))) \\ &= ((2^{2^{m+x-1}} + 1)((2^{2^{m+x-2}} + 1)((2^{2^{m+x-3}} + 1)) \dots (2^{2^n} + 1)((2^{2^n} - 1)).) \end{aligned}$$

Logo,

$$2^{2^n} + 1 \mid 2^{2^m} - 1.$$

Ou seja, existe $k \in \mathbb{Z}$

$$2^{2^m} - 1 = (2^{2^n} + 1)k.$$

E então

$$(2^{2^m} + 1) - (2^{2^n} + 1)k = 0.$$

Adicionando 2 em ambos os membros, teremos:

$$(2^{2^m} - 1) + 2 - (2^{2^n} + 1)k = 0 + 2.$$

Portanto,

$$(2^{2^m} + 1) - (2^{2^n} + 1)k = 2.$$

Seja $d = (f_n, f_m)$, como $d \mid f_n$ e $d \mid f_m$ pelas propriedades de divisibilidade, $d \mid f_n - k \cdot f_m = 2$, portanto $d \mid 2$. Assim $d = 1$ ou $d = 2$. Como todos os números de Fermat são ímpares, devemos ter $d = 1$. Como temos infinitos números de Fermat e dois a dois são primos entre si então podemos concluir que os números primos são infinitos. ■

Teorema 3.6. *Dado $n \in \mathbb{N}$ com $n > 3$, sempre existe um primo p maior que n .*

Demonstração: Seja o número $n! - 1 > 1$, temos que esse número é primo ou composto.

- Se $n! - 1$ for primo, certamente é maior que n .
- Se $n! - 1$ for composto existe $p \mid n! - 1$. Suponhamos que $p \leq n$, então $p \mid n!$, como $p \mid n! - 1$ e $p \mid n!$ então $p \mid 1$ que é sua diferença, logo $p = 1$, o que é um absurdo. Portanto só pode ser $p > n$, como queríamos demonstrar. ■

3.4 O TEOREMA DE EULLER E PEQUENO TEOREMA DE FERMAT

O próximo teorema e a sua consequência imediata o Pequeno Teorema de Fermat e o Teorema Fundamental da Aritmética são ferramentas fundamentais para o desenvolvimento da aplicação prática da teoria dos números no ramo da Criptografia RSA.

Teorema 3.7 (Teorema de Euler). *Sejam $m, a \in \mathbb{Z}$ e $(a, m) = 1$. Então:*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Demonstração: Seja $r_1, \dots, r_{\varphi(m)}$ um sistema reduzido de resíduos $\pmod{m}$. Pela Proposição (3.11), temos que $a \cdot r_1 \cdot \dots \cdot a \cdot r_{\varphi(m)}$ forma um sistema de resíduos $\pmod{m}$ e, portanto,

$$a \cdot r_1 \cdot \dots \cdot a \cdot r_{\varphi(m)} \equiv r_1 \cdot \dots \cdot r_{\varphi(m)} \pmod{m}.$$

Dessa forma,

$$a^{\varphi(m)} \cdot r_1 \cdot \dots \cdot r_{\varphi(m)} \equiv r_1 \cdot \dots \cdot r_{\varphi(m)} \pmod{m}.$$

Como $(r_1 \cdot \dots \cdot r_{\varphi(m)}, m) = 1$ podemos realizar o corte, pelo Corolário (3.3), assim:

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

■

Segundo Lemos (2001), o próximo resultado que foi provado por Fermat, é uma consequência de um resultado bem mais geral obtido por Euler. Aqui apresentaremos como corolário pois é uma aplicação direta do Teorema de Euler apresentado acima.

Corolário 3.6 (Pequeno Teorema de Fermat). *Sejam $a \in \mathbb{Z}$ e p um número primo tais que $(a, p) = 1$. tem-se que:*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demonstração: Como $\varphi(p) = p - 1$ substituindo na função de Euler teremos o resultado desejado. ■

Para outra demonstração consulte Hefez (2016).

Vejamos a solução dos exemplos apresentados a seguir para uma melhor compreensão dos resultados apresentados.

Exemplo 3.25. Qual o resto da divisão de 2023^{58} por 59?

Solução: Note que $(2023, 59) = 1$ e 59 é primo. Logo pelo pequeno Teorema de Fermat temos que:

$$2023^{58} \equiv 1 \pmod{59}.$$

Logo o resto da divisão é 1.

Exemplo 3.26. Vamos achar o resto da divisão de 237^{28} por 13.

Solução: Note que $237 \equiv 3 \pmod{13}$, pois 3 é o resto da divisão de 237 por 13.

Como $(237, 13) = 1$. Pelo Pequeno Teorema de Fermat, que

$$237^{12} \equiv 1 \pmod{13}.$$

Logo pelas propriedades de congruência, teremos que:

$$237^{24} \equiv (237^{12})^2 \equiv 1 \pmod{13}. \quad (41)$$

De forma análoga

$$237^4 \equiv 3^4 \equiv 81 \equiv 3 \pmod{13}. \quad (42)$$

Multiplicando membro a membro as congruências (41) e (42), teremos que:

$$237^{28} \equiv 3 \pmod{13}.$$

Portanto, o resto da divisão de 237^{28} por 13 é 3.

4 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Neste capítulo iremos apresentar o resultado principal desse trabalho. O Teorema Fundamental da Aritmética, também conhecidos em algumas literaturas como teorema da fatoração única. O resultado desse teorema será apresentado em duas partes, existência e unicidade.

Descobrir as menores partes que constituem uma substância, os seus átomos é essencial para que possamos desvendar as suas principais propriedades. Na matemática com os números inteiros ocorre algo semelhante, no caso os números primos são os átomos, e cada número inteiro pode ser escrito como um produto de números primos. Segundo Coutinho(2005) "O conhecimento dessa decomposição nos levará a descobrir várias propriedades interessantes sobre os números inteiros."

Essa importante propriedade dos números inteiros começou a ser desvendada na Grécia antiga por Euclides que em sua principal obra Os Elementos, escreveu proposições que juntas equivalem ao Teorema Fundamental da Aritmética. a partir daí o resultado foi sendo usado por vários outros matemáticos, e como Euclides não tiveram a preocupação de demonstrá-lo em sua totalidade, talvez por estarem preocupados em demonstrar outros resultados. Foi somente no ano de 1801 que essa importante propriedade dos números inteiros foi formalmente demonstrada em sua totalidade: existência e unicidade, na obra *Disquisitiones arithmeticae* do matemático C.F. Gauss.

4.1 CONTEXTO HISTÓRICO

O estudo das propriedades dos números inteiros é atestado desde as civilizações mais antigas, no entanto é na Grécia antiga nos escritos do matemático Euclides de Alexandria (por volta de 325 a.C.-265 a.C.) (Figura 1), onde primeiro identificamos a teoria dos números como a conhecemos hoje, na sua mais famosa obra Os Elementos de Euclides.

O Teorema Fundamental da Aritmética já era utilizado nessa época, como podemos ver nas proposições 30, 31 e 32 do livro VII e 14 do livro IX, sobre isso Hefez (2016) afirma, "Esse resultado, porém, não explicitamente enunciado em sua totalidade, está essencialmente contido nos Elementos de Euclides. pois ele é consequência quase que imediata de proposições que lá se encontram."

Figura 1 – Euclides de Alexandria



Fonte: Vicentin e Aguiar (2020) .

Vejamos o que dizia cada proposição:

Proposição-30. Caso dois números sendo multiplicados entre si, façam algum e algum número primo meça o produzido deles, medirá também um dos do princípio.

Proposição-31. Todo número composto é medido por algum número primo.

Proposição-32. todo número ou é primo ou é medido por algum número primo.

Proposição-14. Caso um número seja o menor medido por primos, será medido por nenhum outro primo além dos que medem no princípio.

A combinação dos resultados das proposições dá uma ideia do que conhecemos hoje como, o Teorema Fundamental da Aritmética.

Para mais detalhes veja: Bicudo (2009).

Ao longo da História muitos outros matemáticos apresentaram resultados em que se usava o Teorema Fundamental da Aritmética, mas não tiveram a preocupação de demonstrá-lo em sua totalidade. Isso se confirma em Coutinho (2005), quando afirma:

O primeiro a enunciá-lo na forma com o conhecemos hoje foi C.F. Gauss na §16 de seu famoso livro *Disquisitiones arithmeticae*. Isto não significa que o fato expresso no teorema não houvesse sido usado implicitamente por outros matemáticos desde a Grécia antiga.

Podemos citar entre os mais famosos: Leonard Paul Euler (1707-1783) e Adrien-Marie Legendre (1752-1833).

Segundo Coutinho (2005) "Euler foi sem dúvidas um dos maiores e mais férteis matemáticos de todos os tempos. Na matemática deu sua contribuição em muitas áreas". O matemático Leonard Paul Euler (1707-1783) (Figura 2) que em seu livro *Elements of Álgebra* (1765) estabelece uma parte do Teorema Fundamental da Aritmética sem prová-lo propriamente e também apresentou uma afirmação para a parte da unicidade.

Na parte I, na sessão I do Capítulo IV e parágrafo 41, Euler afirmou a existência da fatoração em primos e forneceu uma prova parcial. Como podemos ver no escrito do parágrafo 41.

Vejamos o que diz o parágrafo 41:

Todos os números compostos pode ser representado por fatores, resultando a partir dos números primos mencionados; ou seja, todos os seus fatores são números primos. Para se encontrar um fator que não é número primo, pode sempre ser decomposto e representado por dois ou mais números primos. Quando temos representado por exemplo o número 30 por 5×6 é evidente que 6 não ser um número primo, mas sendo reproduzido por 2×3 , poderíamos ter representado 30 por $5 \times 2 \times 3$ ou $2 \times 3 \times 5$; quer dizer, por todos os fatores que são todos os números primos.

Euler também não demonstrou a unicidade da fatoração em números primos, porém ele deu uma declaração relacionada, sem provas, que pode ser equiparada a unicidade, no Parágrafo 65, do Capítulo VI, da Seção 1 da Parte 1.

Veja o que diz o parágrafo 65:

Quando, portanto, conseguimos representar qualquer número, por seus fatores simples, fica mais fácil exibir todos os números pelos quais ele é divisível. Para isso temos, em primeiro lugar, que tomar os fatores simples um a um, e, em seguida, multiplicá-los entre si dois a dois, três a três, quatro a quatro, etc. Até que chegamos ao número proposto.

Figura 2 – Euler



Fonte: Euler (2004).

O leitor interessado em mais detalhes pode consultar Euler (2012).

Adrien-Marie Legendre (1752-1833) (Figura 3) foi um matemático Francês que contribuiu em várias áreas da matemática, em teoria dos números, se destaca o seu livro

Théorie des Nombres publicado em 1830. É nesse livro que ao se referir aos números compostos, escreveu que, "qualquer número não primo N , pode ser representado por um produto de vários números primos α, β, γ , etc. Cada elevado a alguma potência, de modo que sempre se pode supor $N = \alpha^m \cdot \beta^n \cdot \gamma^p \cdot etc.$ " (LEGENDRE, 1808). Em seguida, sua prova segue-se imediatamente dando continuidade a mesma proposição VIII como:

O método a seguir, a fim de executar essa decomposição, consiste em tentar dividir N por cada um dos números primos 2, 3, 5, 7, 11, etc., começando com o menor. Quando a divisão é bem sucedida com um destes números α , repete-se quantas vezes quanto for possível, por exemplo, m vezes, e chamando o último quociente P , temos $N = \alpha^m \cdot P$. O número P não pode ser dividido por α , e é inútil tentar dividir P por um número primo menor do que α , se P for divisível por θ , onde θ é inferior a α , é claro que N também seria divisível por θ , o que contraria a hipótese. Devemos, portanto, tentar dividir P por números primos maiores que α ; assim obtemos em sucessão $P = \beta^n \cdot Q$; $Q = \gamma^p \cdot R$, etc., que irá dar origem a $N = \alpha^m \beta^n \gamma^p \cdot etc.$

Pelo método apresentado por Legendre, qualquer número dado tem a mesma decomposição em fatores primos. O resultado apresentado por Adrien-Marie Legendre poderia ser considerado o Teorema Fundamental da Aritmética, pois o enunciado mostra a existência, porém nessa proposição não se fala nada sobre a unicidade do Teorema Fundamental da Aritmética.

Quanto a unicidade, uma declaração relacionada com a mesma foi dada no mesmo livro "Um número N pode ser expresso na forma $\alpha^m \cdot \beta^n \cdot \gamma^p \cdot etc.$, cada um divisor de N será também de forma $\alpha^u \cdot \beta^v \cdot \gamma^q \cdot etc.$, onde os expoentes u, v, q , etc., não ser maior que m, n, p , etc." (LEGENDRE, 1808). Nessa passagem, o que o matemático Adrien Marie Legendre estava querendo, era encontrar todos os divisores de um número, e, também a soma desses mesmos divisores. A partir dessa afirmação, se poderia facilmente provar a unicidade.

Figura 3 – Adrien-Marie Legendre (1752-1833)



Fonte: Eves (2004).

Para mais detalhes consulte Legendre (1808).

O Teorema Fundamental da Aritmética, foi provado em sua totalidade, somente no ano de 1801, quando o famoso matemático Johann Carl Gauss (1777-1855) (Figura 4) enunciou e provou as duas partes do teorema (existência e unicidade) da fatoração em primos para os números inteiros positivos no artigo 16 da sessão II, em seu livro, *Disquisitiones Arithmeticae*. Segundo Coutinho(2005):

Aos 17 anos Gauss decide incursionar na Aritmética, com o projeto de esclarecer, completar e desenvolver o que seus predecessores haviam realizado. Em 1798, aos 21 anos, Gauss produz uma das obras primas de toda a matemática o livro *Disquisitiones Arithmeticae* que seria publicado somente em 1801.

No artigo 16 o teorema está enunciado da seguinte maneira, "Qualquer número composto pode ser resolvido em fatores primos de uma única maneira". (GAUSS,1995). Exatamente da forma como o conhecemos hoje.

Figura 4 – Johann Call Friedrich Gauss



Fonte: Wittmann (2020).

Segundo Coutinho (2005), "Euler popularizou a teoria dos números como Fermat não o havia conseguido. Mas o desenvolvimento sistemático da teoria só teria início com a *Disquisitiones arithmeticae* do alemão C F Gauss".

A notação desenvolvida e utilizada por Gauss em seu livro *Disquisitiones arithmeticae* é a mesma que utilizamos até os dias de hoje. Segundo Boyer (2019)

uma das contribuições de *Disquisitiones*, foi uma prova rigorosa do teorema, conhecido desde os dias de Euclides, que diz que todo inteiro positivo pode ser representado de uma e uma só maneira (exceto pela ordem dos fatores) como produto de primos.

A demonstração apresentada por C.F. Gauss(1995) em seu livro *Disquisitiones Arithmeticae* diz:

Demonstração: Está claro a partir de considerações elementares que qualquer número composto pode ser resolvido em fatores primos, mas muitas vezes é erroneamente dado como certo que isso não pode ser feito em várias maneiras diferentes. Suponhamos que um número composto $A = a^\alpha \cdot b^\beta \cdot c^\gamma$, etc., com a, b, c , etc. números primos desiguais, podem ser resolvido de outra maneira em fatores primos. Primeiro é claro que neste segundo sistema de fatores não pode aparecer nenhum outro primos exceto a, b, c , etc., já que nenhum outro primo pode dividir A que é composto por esses primos. Da mesma forma, neste segundo sistema de fatores nenhum dos números primos a, b, c , etc pode estar faltando, caso contrário, não dividiria A (artigo anterior). E assim estas duas resoluções em fatores podem diferir apenas no fato de que em um deles algum número primo aparece com mais frequência do que no outro. Deixa o primo p , que aparece em uma resolução m vezes e na outras n vezes, e seja $m > n$. Agora remova de cada sistema o fator p , n vezes. Como resultado, p permanecerá em um sistema $m - n$ vezes e estará completamente ausente do outro. Isto é, temos duas resoluções em fatores do número A/p^n . Uma delas não contém o fator p , o outro contém $m - n$ vezes, contradizendo o que acabamos de mostrar.

Pela demonstração dada por F.C. Gauss ele não comentou nada sobre a existência, foi aceita a partir de considerações elementares. Gauss se esforçou em demonstrar a unicidade a partir do artigo anterior, conhecido como o Lema de Euclides.

Para mais detalhes consulte Gauss (1995).

4.2 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Depois desse breve contexto histórico, agora enunciaremos e demonstraremos o Teorema Fundamental da Aritmética.

Teorema 4.1 (Teorema Fundamental da Aritmética). *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Veja que o teorema nos diz duas coisas, primeiro que a fatoraçoão existe e segundo que essa fatoraçoão é única. Portanto devemos provar dois fatos: existência e unicidade.

Vejamos a demonstração a seguir.

Demonstração: Usaremos a segunda forma do Princípio de Indução.

Se $n = 2$, o resultado é obviamente verificado.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n .

Se o número n é primo, nada temos a demonstrar.

Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 \cdot n_2$, com $1 < n_1 < n$ e, $1 < n_2 < n$.

Pela hipótese de indução, temos que existem números primos $p_1, p_2, \dots, p_r$ e $q_1, q_2, \dots, q_s$

tais que $n_1 = p_1 \cdot p_2 \cdot \dots \cdot p_r$ e $n_2 = q_1 \cdot q_2 \cdot \dots \cdot q_s$. Portanto,

$$n = n_1 \cdot n_2 = p_1 \cdot p_2 \cdot \dots \cdot p_r \cdot q_1 \cdot q_2 \cdot \dots \cdot q_s.$$

Como queríamos demonstrar.

Vamos, agora, provar a unicidade da escrita.

Suponha que $n = p_1 \cdot p_2 \cdot \dots \cdot p_r$ e $n = q_1 \cdot q_2 \cdot \dots \cdot q_s$, ou seja,

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_s$$

onde os p_i e os q_j são números primos. Daí,

$$p_1 | q_1 \cdot q_2 \cdot \dots \cdot q_s,$$

e, pelo Corolário (3.4), temos que $p_1 = q_j$ para algum j do conjunto $\{1, 2, \dots, s\}$ que, após reordenamento de $q_1, \dots, q_s$, podemos supor que seja q_1 . Assim $p_1 = q_1$. Fazendo o cancelamento teremos que:

$$p_2 \cdot \dots \cdot p_r = q_2 \cdot \dots \cdot q_s.$$

Pelo mesmo processo temos que $p_2 = q_2$, assim

$$p_3 \cdot p_4 \cdot \dots \cdot p_r = q_3 \cdot q_4 \cdot \dots \cdot q_s.$$

Continuando o processo e supondo sem perda de generalidade que $r < s$ chegaremos que:

$$1 = q_{r+1} \cdot q_{r+2} \cdot \dots \cdot q_s.$$

O que é impossível pois todos os números da direita da igualdade são números primos e logo por definição maiores que ou igual a 2.

De forma análoga e supondo $s < r$, chegaremos que:

$$1 = p_{s+1} \cdot p_{s+2} \cdot \dots \cdot p_r.$$

O que também é impossível.

Logo só podemos ter $r = s$ e $p_i = q_i$ para cada $i = 1, 2, \dots, r$. O que conclui a demonstração. ■

Sendo $n = p_1 \cdot p_2 \cdot \dots \cdot p_r$ note que da forma como estão definidos os primos p_k com $1 \leq k \leq r$ podem ser distintos ou não. Dessa forma podemos reordenar os primos iguais na forma de potência e reescrever n da seguinte forma,

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdot \dots \cdot p_s^{n_s},$$

onde os números primos $p_1, p_2, p_3, \dots, p_s$ são distintos dois a dois, e $n_1, n_2, n_3, \dots, n_s \in \mathbb{N}$, com $s > 1$.

Observamos que escrito nessa forma, n está decomposto como produto de potências cujas bases são números primos distintos dois a dois. Esta forma de representar o número natural $n > 1$, como sendo:

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdot \dots \cdot p_s^{n_s}.$$

Essa maneira de representação dos números é denominada forma canônica, e essa representação será bastante utilizada para demonstrar as aplicações deste teorema, já que a fatoração de um número natural em primos revela a sua estrutura multiplicativa.

Para os leitores mais curiosos que pretendem ver outras demonstrações, consulte Coutinho (2005) e Hefez (2016).

O próximo capítulo apresentará uma série de resultados e aplicações em que se utiliza o Teorema Fundamental da Aritmética como ferramenta indispensável na obtenção dos resultados.

Agora, apresentaremos algumas das aplicações que são consequências imediatas desse importante teorema da teoria dos números:

- Reformulação do Teorema de Euler
- Divisores de um número natural.
- Quantidade de divisores de um número natural.
- Soma dos divisores de um número natural.
- produto dos divisores de um número natural.
- MMC e MDC de um número natural.

4.3 REFORMULAÇÃO DO TEOREMA DE EULER

O próximo resultado que será apresentado como uma proposição é uma formulação do Teorema de Euler. Segundo Coutinho (2005) esse resultado é fundamental para o sistema criptográfico RSA.

Proposição 4.1. *Seja m um inteiro livre de quadrados, então para todo $a \in \mathbb{Z}$ e todo $k \in \mathbb{Z}$ tem-se que:*

$$a^{k\varphi(m)+1} \equiv a \pmod{m}.$$

Demonstração: Como m é livre de quadrados, sua forma decomposta em fatores primos é:

$$m = p_1 \cdot p_2 \cdot \dots \cdot p_r,$$

onde, $p_1, p_2, \dots, p_r$ são primos distintos. Como,

$$\varphi(m) = \varphi(p_1) \cdot \varphi(p_2) \cdot \dots \cdot \varphi(p_r) = (p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_r - 1).$$

Fazendo, $k_i = k(p_1 - 1) \cdot (p_2 - 1) \cdot \dots \cdot (p_{i-1} - 1) \cdot (p_{i+1} - 1) \cdot \dots \cdot (p_r - 1)$. Temos que:

$$a^{k\varphi(m)+1} = a^{k_i(p_i-1)+1} \equiv a \pmod{p_i}.$$

Como pela Proposição (3.8) item 2, temos que, $[p_1, \dots, p_r] = p_1 \cdot \dots \cdot p_r = m$. Logo:

$$a^{k\varphi(m)+1} \equiv a \pmod{[p_1, \dots, p_r]} \implies a^{k\varphi(m)+1} \equiv a \pmod{m}.$$

Como queríamos demonstrar. ■

4.4 OS DIVISORES DE UM NÚMERO NATURAL

Teorema 4.2. *Seja $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$ a decomposição canônica do inteiro positivo $n > 1$, então os divisores positivos de n são precisamente os inteiros d da forma:*

$$d = p_1^{h_1} \cdot p_2^{h_2} \cdot p_3^{h_3} \cdot \dots \cdot p_r^{h_r},$$

onde $0 \leq h_i \leq k_i (i = 1, 2, \dots, r)$.

Demonstração: Obviamente, os divisores triviais são $d = 1$ e $d = n$ que se obtém quando, respectivamente, temos: $h_1 = h_2 = \dots = h_r = 0$ e $h_1 = k_1, h_2 = k_2, \dots, h_r = k_r$.

Suponhamos, pois, que d é um divisor não trivial de n positivo, e seja p^{h_i} a potência de um primo p que figure na decomposição de d em fatores primos. Como $p^{h_i} | n$, segue pelo Corolário (3.4) e o item 6 da Proposição (2.2), que p^{h_i} divide algum $p_i^{k_i}$ por ser primo com as demais potências de fatores primos de n , e, conseqüentemente, $p = p_i$ e $0 \leq h_i \leq k_i$. Como queríamos demonstrar. ■

Conhecendo a decomposição canônica de um número inteiro positivo se torna bem prático a visualização da forma de seus divisores, e com isso é bem mais fácil encontrar os divisores de determinado número. Enquanto que se não conhece a sua decomposição canônica se torna bem mais complicado encontrar os divisores de um número grande, pois teríamos que realizar uma grande sequência de operações.

Vejamos o exemplo a seguir para um melhor entendimento do resultado apresentado.

Exemplo 4.1. Dados os números $a = 3^9 \cdot 10^9 \cdot 7^{50}$ e $b = 1536$. Mostre que $b|a$.

Solução: Note que a decomposição de b em fatores primos é:

$$b = 2^9 \cdot 3,$$

e fatorando a em fatores primos teremos:

$$a = 2^9 \cdot 3^9 \cdot 5^9 \cdot 7^{50}.$$

Pelo Teorema (4.2), após decompostos os números em fatores primos, $b|a$ se:

- Todos os fatores primos de b estiverem na decomposição de a e;
- Os expoentes desses fatores primos comuns de b , forem menores ou iguais aos expoentes dos fatores comuns que estão em a .

Como todos os fatores primos de b (2 e 3) estão em a e os expoentes desses fatores são menores ou iguais aos expoentes dos fatores comuns que estão em b , temos que $b|a$.

Portanto $1536|3^9 \cdot 10^9 \cdot 7^{50}$.

Agora iremos apresentar um resultado que conta o número de divisores de inteiro positivo, graças ao Teorema Fundamental da Aritmética. As aplicações desse resultado já são apresentadas aos alunos desde o ensino fundamental II e segue até o ensino superior, além de ser cobrado em avaliações e exames de nível nacional como: Exame Nacional do ensino Médio (ENEM), Exame Nacional de Qualificação (ENQ), Exame Nacional de Acesso (ENA-PROFMAT), Olimpíada Brasileira de Matemática (OBM), entre outros, como podemos ver através dos exemplos apresentados.

4.5 QUANTIDADE DE DIVISORES DE UM NÚMERO NATURAL.

Teorema 4.3. *Se $n = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdot \dots \cdot p_r^{k_r}$, é a decomposição canônica do inteiro positivo $n > 1$, então:*

$$d(n) = (k_1 + 1) \cdot (k_2 + 1) \cdot \dots \cdot (k_r + 1),$$

onde: $d(n)$ representa a quantidade de divisores do número n .

Demonstração: Pelo Teorema (4.2), os divisores positivos de n são precisamente os inteiros d da forma:

$$d = p_1^{h_1} \cdot p_2^{h_2} \cdot p_3^{h_3} \cdot \dots \cdot p_r^{h_r},$$

onde: $0 \leq h_1 \leq k_1, 0 \leq h_2 \leq k_2, \dots, 0 \leq h_r \leq k_r$. Temos $k_1 + 1$ maneiras de escolher o expoente h_1 , $k_2 + 1$ maneiras de escolher o expoente h_2 , $\dots$, $k_r + 1$ maneiras de escolher o expoente h_r e, portanto, o número total de maneiras de escolher os expoentes $h_1, h_2, \dots, h_r$ é, pelo princípio fundamental da contagem:

$$(k_1 + 1) \cdot (k_2 + 1) \cdot \dots \cdot (k_r + 1).$$

Assim sendo, o número $d(n)$ de divisores positivos do inteiro $n > 1$ é dado pela fórmula:

$$d(n) = (k_1 + 1) \cdot (k_2 + 1) \cdot \dots \cdot (k_r + 1).$$

Como queríamos demonstrar. ■

Vejamos uma aplicação do resultado apresentado no Exame Nacional de Acesso (ENA).

Exemplo 4.2. (PROFMAT 2012-EXAME NACIONAL DE ACESSO). O número total

de divisores positivos de $10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ é igual a:

- (a) 15
- (b) 270
- (c) 320
- (d) 1024
- (e) $10!$

Solução: Pelo Teorema Fundamental da Aritmética, observe que $10!$ pode ser escrito como:

$$\begin{aligned} 10! &= 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &= (2 \cdot 5) \cdot (3 \cdot 3) \cdot (2 \cdot 2 \cdot 2) \cdot 7 \cdot (2 \cdot 3) \cdot 5 \cdot (2 \cdot 2) \cdot 3 \cdot 2 \cdot 1 \\ &= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7. \end{aligned}$$

Logo, pelo Teorema (4.3), cada divisor de $10!$ será da forma $2^m \cdot 3^n \cdot 5^p \cdot 7^q$ onde, m, n, p, q são números naturais tais que $0 \leq m \leq 8$; $0 \leq n \leq 4$; $0 \leq p \leq 2$; $0 \leq q \leq 1$. Portanto, pelo princípio multiplicativo temos que a quantidade de divisores de $10!$ é $(8+1) \cdot (4+1) \cdot (2+1) \cdot (1+1) = 9 \cdot 5 \cdot 3 \cdot 2 = 270$.

Portanto o item correto é o item (B).

Exemplo 4.3. (OBM 2012 – 1ª FASE – NÍVEL 2). Qual é o menor número ímpar que possui exatamente 10 divisores positivos incluindo o 1 e o próprio número?

- (a) 1875
- (b) 405
- (c) 390
- (d) 330
- (e) 105

Solução: Pelo Teorema Fundamental da Aritmética, os números que possuem exatamente 10 divisores positivos podem assumir apenas uma das possíveis formas: p^4q ou p^9 onde p e q representam primos distintos. O menor número ímpar da primeira forma é $3^4 \cdot 5 = 405$, enquanto o segundo número é 3^9 , que é bem maior do que 405.

Logo, a resposta correta está no item (B).

Exemplo 4.4. (ENQ 2017/1)

1. Prove que um número inteiro positivo n possui uma quantidade ímpar de divisores se, e somente se, é um quadrado perfeito.
2. Sejam a e b números inteiros positivos com $(a, b) = 1$. Prove que, se ab é um quadrado perfeito, então a e b são quadrados perfeitos.

Solução:

1. Pelo Teorema Fundamental da Aritmética

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r},$$

onde $p_1 < p_2 < \dots < p_r$, são números primos e $\alpha_1, \alpha_2, \dots, \alpha_r$, são números inteiros positivos. A quantidade de divisores de n é dada por

$$d(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_r + 1).$$

- ($\Rightarrow$) Se n tem número ímpar de divisores, então todos os fatores de $d(n)$ são números ímpares, ou seja, $\alpha_1, \alpha_2, \dots, \alpha_r$ são números pares. Portanto,

$$n = (p_1^{\frac{\alpha_1}{2}} \cdot p_2^{\frac{\alpha_2}{2}} \cdot \dots \cdot p_r^{\frac{\alpha_r}{2}})^2.$$

Que é um quadrado perfeito.

- ($\Leftarrow$) Reciprocamente, se n é um quadrado perfeito, então $n = c^2$, para algum $c \in \mathbb{Z}$. Isto implica que todos os α_i são números pares e então $d(n)$ é ímpar, por ser o produto de ímpares.
2. Sejam $a = a_1^{\beta_1} \cdot a_2^{\beta_2} \cdot \dots \cdot a_k^{\beta_k}$ e $b = b_1^{\lambda_1} \cdot b_2^{\lambda_2} \cdot \dots \cdot b_t^{\lambda_t}$, a decomposição destes números em fatores primos distintos, pois como $(a, b) = 1$, eles não têm fator primo em comum. Ao efetuar o produto de a e b obtemos,

$$ab = a_1^{\beta_1} \cdot a_2^{\beta_2} \cdot \dots \cdot a_k^{\beta_k} \cdot b_1^{\lambda_1} \cdot b_2^{\lambda_2} \cdot \dots \cdot b_t^{\lambda_t},$$

$$d(ab) = (\beta_1 + 1)(\beta_2 + 1) \dots (\beta_k + 1)(\lambda_1 + 1)(\lambda_2 + 1) \dots (\lambda_t + 1).$$

Que é a decomposição de ab em fatores primos.

Como ab é um quadrado perfeito, pelo item a), a quantidade de divisores de ab é ímpar, isto é,

$$d(ab) = (\beta_1 + 1)(\beta_2 + 1) \dots (\beta_k + 1)(\lambda_1 + 1)(\lambda_2 + 1) \dots (\lambda_t + 1)$$

é ímpar.

E pelo item a): $d(a)$ é ímpar e $d(b)$ é ímpar, ou seja, a e b são quadrados perfeitos.

Exemplo 4.5. Encontre o número de divisores positivo do número

$$A = (3244)^5 + 5(3244)^4 + 10(3244)^3 + 10(3244)^2 + 5(3244) + 1.$$

Solução: Lembrando que $(x + 1)^5 = x^5 + 5x^4 + 10x^3 + 10x^2 + 5x + 1$, a expressão acima pode ser reescrita como:

$$A = (3244 + 1)^5 = 3245^5.$$

Como $3245 = 5 \cdot 11 \cdot 59$ e essa fatoração é única pelo Teorema Fundamental da Aritmética

e, portanto, pelo teorema apresentado teremos:

$$A = 3245^5 = (5 \cdot 11 \cdot 59)^5 = 5^5 \cdot 11^5 \cdot 59^5.$$

Portanto a quantidade de divisores positivos de A é:

$$(5 + 1) \cdot (11 + 1) \cdot (59 + 1) = 6 \cdot 12 \cdot 60 = 4320.$$

Exemplo 4.6. (ENEM 2014). Durante a Segunda Guerra Mundial, para decifram as mensagens secretas, foi utilizada a técnica de decomposição em fatores primos. Um número N é dado pela expressão $2^x \cdot 5^y \cdot 7^z$, na qual x , y e z são números inteiros não negativos. Sabe-se que N é múltiplo de 10 e é múltiplo de 7. O número de divisores de N , diferentes de N , é:

- A) $x \cdot y \cdot z$
- B) $(x + 1) \cdot (y + 1)$
- C) $x \cdot y \cdot z - 1$
- D) $(x + 1) \cdot (y - 1) \cdot z$
- E) $(x + 1) \cdot (y + 1) \cdot (z + 1) - 1$

Solução: Temos que o número $N = 2^x \cdot 5^y \cdot 7^z$. O fato de N ser múltiplo de 10, significa que na decomposição de N irá aparecer pelo menos um fator 2 e pelo menos um fator 5, ou seja, tanto o expoente x como o expoente y são diferentes de 0. Do mesmo modo que o fato de N ser múltiplo de 7 significa que na fatoração de N haverá algum fator 7, ou seja, o expoente z será diferente de 0. Para obtermos o número de divisores de um número N a partir de sua decomposição em fatores primos, devemos obter todas as combinações possíveis para seus expoentes incluindo o zero. Assim, em nosso caso, as possibilidades para o expoente do fator 2 são iguais a x mais o zero, isto é, $x + 1$. De modo análogo, as possibilidades para os expoentes y e z , respectivamente são $y + 1$ e $z + 1$. Assim, temos que o número de divisores de N é $(x + 1)(y + 1)(z + 1)$, incluindo o próprio N . Como queremos os divisores diferentes de N , teremos: $(x + 1) \cdot (y + 1) \cdot (z + 1) - 1$.

4.6 A SOMA DOS DIVISORES DE UM NÚMERO NATURAL.

Através do Teorema Fundamental da Aritmética e com conhecimentos básicos de progressão geométrica é possível encontrar uma expressão para se determinar a soma dos divisores de um número positivo como veremos a seguir através do teorema apresentado abaixo.

Teorema 4.4. Se $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_r^{k_r}$ é a decomposição canônica do inteiro positivo $n > 1$, então a soma dos divisores de n , denotado por $S(n)$, é dada pela expressão:

$$s(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

Demonstração: considere o produto

$$(1 + p_1 + p_1^2 + \dots + p_1^r) \cdot (1 + p_2 + p_2^2 + \dots + p_2^r) \cdot \dots \cdot (1 + p_r + p_r^2 + \dots + p_r^r).$$

Pelo Teorema (4.2) cada termo do produto é um divisor positivo de n .

Assim $s(n)$ é a soma de todos os termos do desenvolvimento, mas cada termo do produto apresentado acima é uma progressão geométrica, de primeiro termo igual a 1 ($a_1 = 1$) e razão p ($r = p$). Logo aplicando a fórmula da soma do termo da progressão geométrica em cada termo do produto

$$(1 + p_1 + p_1^2 + \dots + p_1^r) \cdot (1 + p_2 + p_2^2 + \dots + p_2^r) \cdot \dots \cdot (1 + p_r + p_r^2 + \dots + p_r^r)$$

teremos:

$$s(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \dots \cdot \frac{p_r^{k_r+1} - 1}{p_r - 1}.$$

Como queríamos demonstrar. ■

Vejamos a solução dos exemplos a seguir para uma melhor assimilação do resultado apresentado.

Exemplo 4.7. Determine a soma dos divisores do número $a = 2^9 \cdot 3^6 \cdot 5^5$.

Solução: Pelo Teorema (4.4), a soma dos divisores do número a é:

$$s(2^9 \cdot 3^6 \cdot 5^5) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \frac{p_3^{k_3+1} - 1}{p_3 - 1}$$

substituindo as variáveis, teremos:

$$\begin{aligned} s(2^9 \cdot 3^6 \cdot 5^5) &= \frac{2^{9+1} - 1}{2 - 1} \cdot \frac{3^{6+1} - 1}{3 - 1} \cdot \frac{5^{4+1} - 1}{5 - 1} \\ &= (2^{10} - 1) \cdot \frac{(3^7 - 1)}{2} \cdot \frac{(5^5 - 1)}{4} \\ &= \frac{(2^{10} - 1) \cdot (3^7 - 1) \cdot (5^5 - 1)}{8}. \end{aligned}$$

Exemplo 4.8. A soma dos divisores positivos do número inteiro 180 é:

Solução: Note que a decomposição canônica de 180 é

$$180 = 2^2 \cdot 3^2 \cdot 5.$$

Logo pelo Teorema (4.4), temos que:

$$\begin{aligned}
 s(180) &= s(2^2 \cdot 3^2 \cdot 5) \\
 &= \frac{2^{2+1} - 1}{2 - 1} \cdot \frac{3^{2+1} - 1}{3 - 1} \cdot \frac{5^{1+1} - 1}{5 - 1} \\
 &= \frac{7}{1} \cdot \frac{26}{2} \cdot \frac{24}{4} \\
 &= \frac{4368}{8} \\
 &= 546.
 \end{aligned}$$

Logo a soma pedida é 546.

4.7 O PRODUTO DOS DIVISORES DE UM NÚMERO NATURAL

Uma outra aplicação do Teorema Fundamental da Aritmética é para o cálculo de um resultado pouco usado, o cálculo do produto dos divisores de um número inteiro positivo. Como veremos através do próximo teorema.

Teorema 4.5. *O produto dos divisores positivos de um inteiro positivo $n > 1$ é igual a*

$$n^{\frac{d(n)}{2}}$$

onde $d(n)$ representa a quantidade de divisores no número n .

Demonstração: Sejam $d_1, d_2, \dots, d_{d(n)}$ todos os divisores positivos de n , de modo que existem os inteiros $q_1, q_2, \dots, q_{d(n)}$ tais que $n = d_1 \cdot q_1$, $n = d_2 \cdot q_2$, $\dots$, $n = d_{d(n)} \cdot q_{d(n)}$. Como

$$d_1 \cdot d_2 \cdot \dots \cdot d_{d(n)} = q_1 \cdot q_2 \cdot \dots \cdot q_{d(n)},$$

porque cada um dos inteiros $q_1, q_2, \dots, q_{d(n)}$ também é divisor de n , temos:

$$n^{d(n)} = (d_1 \cdot d_2 \cdot \dots \cdot d_{d(n)})^2 \implies (d_1 \cdot d_2 \cdot \dots \cdot d_{d(n)}) = n^{\frac{d(n)}{2}}.$$

Como queríamos demonstrar. ■

Vejamos o resultado aplicado ao exemplo abaixo.

Exemplo 4.9. Determine o produto dos divisores positivos de 30.

Solução: Como a forma fatorada canônica de $30 = 2 \cdot 3 \cdot 5$. Pelo Teorema (4.2),

$$d(n) = (1 + 1) \cdot (1 + 1) \cdot (1 + 1) = 2 \cdot 2 \cdot 2 = 8.$$

Portanto usando o Teorema (4.5) apresentado teremos que:

$$n^{\frac{d(n)}{2}} = 30^{\frac{8}{2}} = 30^4 = 810000.$$

Uma das aplicações mais usuais do TFA é para o cálculo de MMC e MDC, um assunto já abordado nos nossos livros didáticos desde o ensino fundamental. Com o auxílio do Teorema Fundamental da Aritmética, o cálculo de máximo divisor comum e do mínimo múltiplo comum pode ser realizado de forma bem ágil sem muitos cálculos. Note que nas preliminares foram apresentadas ferramentas bastante úteis para se calcular o MDC e o MMC, só que com as mesmas é necessário realizar bastante cálculo a medida que os números envolvidos crescem, o que não ocorre com os números envolvidos estando em sua decomposição canônica.

4.8 MÁXIMO DIVISOR COMUM E MÍNIMO MÚLTIPLO COMUM DE UM NÚMERO NATURAL.

Teorema 4.6. *Sejam $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_n^{\alpha_n}$ e $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \dots \cdot p_n^{\beta_n}$. Pondo*

$$\gamma_i = \max\{\alpha_i, \beta_i\} \text{ e } \delta_i = \min\{\alpha_i, \beta_i\}, i = 1, 2, \dots, n.$$

tem-se que

$$(a, b) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \dots \cdot p_n^{\gamma_n} :$$

e

$$[a, b] = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_n^{\delta_n}.$$

Demonstração:

- (MDC) pelo Teorema(4.2) temos que: $p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \dots \cdot p_n^{\gamma_n}$ é um divisor comum de a e b . Seja c um divisor comum de a e b ; logo $c = p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot \dots \cdot p_n^{\varepsilon_n}$ onde $\varepsilon_i \leq \min\{\alpha_i, \beta_i\}$ e, portanto, pela condição ii) do MDC, $c | p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot \dots \cdot p_n^{\gamma_n}$.
- (MMC) É claro que $p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_n^{\delta_n}$ é um múltiplo de a e b , seja d um múltiplo comum de a e b , logo $d = p_1^{\theta_1} \cdot p_2^{\theta_2} \cdot \dots \cdot p_n^{\theta_n}$, onde $\theta_i \geq \max\{\alpha_i, \beta_i\}$ e, portanto, pela condição ii) do MMC $p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot \dots \cdot p_n^{\delta_n} | d$. ■

Para uma melhor fixação do resultado, vejamos o próximo exemplo.

Exemplo 4.10. Determinar o MMC e o MDC dos números 40, 95 e 132.

Solução: Como, $40 = 2^3 \cdot 5$ e $95 = 5 \cdot 19$ e $132 = 2^2 \cdot 3 \cdot 11$. Pelo Teorema (4.6), o MDC é:

$$(40, 95, 132) = 2^0 \cdot 3^0 \cdot 5^0 \cdot 11^0 \cdot 19^0 = 1$$

e o MMC é :

$$\begin{aligned} [40, 95, 132] &= 2^3 \cdot 3^1 \cdot 5^1 \cdot 11^1 \\ &= 8 \cdot 3 \cdot 5 \cdot 11 \\ &= 1420. \end{aligned}$$

5 APLICAÇÕES DO TEOREMA FUNDAMENTAL DA ARITMÉTICA

Neste capítulo apresentaremos algumas das aplicações desse importante teorema da teoria dos números, os casos encontrados para a sua aplicação foram:

- Verificar se $\sqrt[n]{a}$ é um número inteiro positivo.
- Verificar qual o menor natural que deve ser multiplicado a $\sqrt[n]{a}$ para se obter um número inteiro positivo.
- Fatores do fatorial.
- A irracionalidade da $\sqrt[n]{p}$
- A irracionalidade da $\sqrt[n]{p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}}$ onde, $m_i < n$ para $i = \{1, 2, 3, \dots, r\}$
- A irracionalidade do $\log 2$
- Relação entre coeficientes primos distintos de uma equação do 2º grau e raiz dupla.
- Verificar se alguns polinômios especiais admitem soluções inteiras.
- Critpografia RSA

5.1 VERIFICAR SE $\sqrt[n]{a}$ É UM NÚMERO INTEIRO POSITIVO.

Uma outra aplicação do TFA é para verificar se $\sqrt[n]{a}$ é um número inteiro positivo. Utilizando o Teorema Fundamental da Aritmética e as propriedades básicas da potenciação podemos chegar de forma clara se $\sqrt[n]{a}$ é ou não um número inteiro, como veremos no próximo teorema apresentado.

Teorema 5.1. *Se $\sqrt[n]{a}$ é um número inteiro positivo, então a decomposição de a em fatores primos, os expoentes de todos os primos da decomposição são da forma $n \cdot k$ com $k \in \mathbb{Z}$*

Demonstração: Pelo Teorema Fundamental da Aritmética $a = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}$ temos que:

$$\sqrt[n]{a} = \sqrt[n]{p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}}.$$

Como por hipótese $\sqrt[n]{a}$ é um número inteiro positivo então os expoentes dos primos $p_1, p_2, \dots, p_r$ são todos da forma $n k_i$ pelas propriedades de potenciação, com $i = 1, 2, 3, \dots, r$ e k_i inteiro positivo. Dessa forma sendo $m_i = n k_i$ para $i = 1, 2, 3, \dots, r$. Assim teremos: $p_1^{n \cdot k_1}, p_2^{n \cdot k_2}, \dots, p_r^{n \cdot k_r}$. Concluindo assim a demonstração. ■

Agora apresentaremos alguns exemplos que ajudara na compreensão do Teorema (5.1) apresentado.

Exemplo 5.1. Qual o menor inteiro que devemos multiplicar para que o número $2^5 \cdot 5 \cdot 7^6$ seja um cubo perfeito?

Solução: Como o número já está em sua forma decomposta, pelo Teorema (5.1) devemos tornar cada expoente do número o menor múltiplo de 3 possível.

Assim devemos multiplicar o número por 2, pois é o menor inteiro que torna o expoente do primo 2 um múltiplo de 3; e multiplicar o número por 5^2 pois é o menor múltiplo de 5, que torna o expoente do primo 5 um múltiplo de 3; como o expoente do

primo 7 já é um múltiplo de 3 o mantemos. Assim o menor inteiro que devemos multiplicar ao número $2^5 \cdot 5 \cdot 7^6$ é $2 \cdot 5^2 = 50$.

Observação 5.1. Como podemos encontrar o menor número que devemos multiplicar o número dado para encontrar um cubo perfeito, poderia de forma análoga identificar qual o menor inteiro possível que se deve dividir um número dado para encontrar um cubo perfeito.

Exemplo 5.2. Qual o menor inteiro que devemos dividir o número $2^5 \cdot 5 \cdot 7^6$ para que tenhamos um cubo perfeito?

Solução: Como o número já está em sua forma decomposta, pelo teorema apresentado devemos tornar cada expoente do número o menor múltiplo de 3 possível. Assim devemos dividir o número por 2^2 , pois é o menor inteiro que torna o expoente do primo 2 um múltiplo de 3; e dividir o número por 5 pois é o menor múltiplo de 5, que torna o expoente do primo 5 um múltiplo de 3; como o expoente do primo 7 já é um múltiplo de 3 o mantemos. Assim o menor inteiro que devemos dividir o número $2^5 \cdot 5 \cdot 7^6$ é $2^2 \cdot 5 = 20$ para termos como resultado um número cúbico.

5.2 FATORES DO FATORIAL.

A próxima aplicação do TFA é usada para encontrar a maior potência de um primo p que está no fatorial do número n . O resultado é cobrado em exames nacionais de acesso (ENA) e em olimpíadas de matemática. O mesmo já se encontrava na proposição XVI em Legendre (1808).

Teorema 5.2. *Seja p um primo, então a maior potência de p que divide $n!$ é γ onde,*

$$\gamma = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Observação 5.2. Note que a soma acima é finita pois a partir de certo $i \in \mathbb{N}$, $p_i > n$ e a partir de p_i , todos os termos serão nulos.

Demonstração: No produto $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$, apenas os múltiplos de p contribuem com o fator p . dessa forma há $\left\lfloor \frac{n}{p} \right\rfloor$ múltiplos de p entre 1 e n . Desses os que contribuem com p^2 , contribuem com um fator extra p e há $\left\lfloor \frac{n}{p^2} \right\rfloor$ dentre esses últimos os que são múltiplos de p^3 contribuem com mais um fator p e há $\left\lfloor \frac{n}{p^3} \right\rfloor$. E assim segue encontrando a fórmula apresentada acima. Como queríamos demonstrar. ■

Exemplo 5.3. . Determine com quantos zeros termina $3500!$.

Solução: O problema é equivalente a determinar qual é a maior potência de 10 que divide $3500!$, e como há mais fatores 2 do que fatores 5 em $3500!$, o expoente dessa potência coincide com o da maior potência de 5 que divide $3500!$. Ou seja, sendo α o expoente da maior potência de 5 que aparece no número, temos que pelo Teorema (5.2) que α é:

$$\begin{aligned}
\alpha &= \left\lfloor \frac{3500}{5} \right\rfloor + \left\lfloor \frac{3500}{5^2} \right\rfloor + \left\lfloor \frac{3500}{5^3} \right\rfloor + \left\lfloor \frac{3500}{5^4} \right\rfloor + \left\lfloor \frac{3500}{5^5} \right\rfloor \\
&= 700 + 140 + 28 + 5 + 1 \\
&= 874.
\end{aligned}$$

Assim $3500!$ termina em 874 zeros.

Exemplo 5.4. Mostre que 2^{994} divide $1000!$, mas 2^{995} não divide $1000!$

Solução: A quantidade de vezes que o fator 2 aparece em $1000!$ fatorial é:

$$\begin{aligned}
\alpha &= \left\lfloor \frac{1000}{2} \right\rfloor + \left\lfloor \frac{1000}{2^2} \right\rfloor + \left\lfloor \frac{1000}{2^3} \right\rfloor + \dots + \left\lfloor \frac{1000}{2^8} \right\rfloor + \left\lfloor \frac{1000}{2^9} \right\rfloor \\
&= 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 \\
&= 994.
\end{aligned}$$

Como 2^{994} está na decomposição de $1000!$ temos 2^{994} divide $1000!$ e é a maior potência de 2 que divide $1000!$.

Assim 2^{995} não divide o fatorial de 1000.

Exemplo 5.5. Diga justificando, se o número $600!$ é divisível por 7^{99}

Solução: A quantidade de fatores 7 em $600!$ é:

$$\begin{aligned}
\alpha &= \left\lfloor \frac{600}{7} \right\rfloor + \left\lfloor \frac{600}{7^2} \right\rfloor + \left\lfloor \frac{600}{7^3} \right\rfloor \\
&= 85 + 12 + 1 \\
&= 98.
\end{aligned}$$

Dessa forma $600!$ não é divisível por 7^{99} , pois a quantidade de fatores 7 em $600!$ é 98. Para mais detalhes sobre os fatores do fatorial, consulte Hefez (2016) E Santos (2000).

Uma outra aplicação do Teorema Fundamental da Aritmética é relacionada a irracionalidade. O resultado aliado a prova por redução ao absurdo, se consegue demonstrar a irracionalidade de números da forma $\sqrt[n]{p}$ onde $p, n \in \mathbb{N}$ $n > 1$ e p primo, como demonstrado no Teorema (5.3) abaixo.

5.3 A IRRACIONALIDADE DE $\sqrt[n]{p}$ COM $p, n \in \mathbb{N}$, $n > 1$ E p PRIMO.

Sabemos que existem muitas demonstrações do caso mais simples dos números da forma $\sqrt[n]{p}$, que é $\sqrt{2}$, e por vários caminhos. Talvez a mais famosa seja por redução ao absurdo usando paridade. Aqui demonstraremos o caso geral por redução ao absurdo, usando o Teorema Fundamental da Aritmética.

Teorema 5.3. *Todo número da forma $\sqrt[n]{p}$, com p e $n \in \mathbb{N}$, $n > 1$ e p primo é irracional.*

Demonstração: Suponha que $\sqrt[n]{p}$ seja racional, logo existem naturais a e b com $b \neq 0$

tal que:

$$\sqrt[n]{p} = \frac{a}{b} \Rightarrow p = \frac{a^n}{b^n} \Rightarrow a^n = p \cdot b^n.$$

Dessa forma, teremos que,

$$a^n = p \cdot b^n. \quad (43)$$

Pelo Teorema Fundamental da Aritmética a e b possuem decomposição em fatores primos única. Fazendo as decomposições dos números a e b , o fator primo p pode aparecer ou não. Assim podemos dizer que,

$$a = p^i \cdot c$$

e

$$b = p^j \cdot d,$$

onde c e d representam o produto dos outros fatores primos diferentes de p . Substituindo as decomposições de a e b na equação (43) fica:

$$(p^i \cdot c)^n = p \cdot (p^j \cdot d)^n \Rightarrow p^{in} c^n = p^{jn+1} d^n.$$

Como temos duas decomposições elas devem ser a mesma pela unicidade, provada pelo Teorema Fundamental da Aritmética, mas isso não pode ocorrer pois os expoentes de p não podem ser iguais, contrariando assim o Teorema Fundamental da Aritmética. Como chegamos a uma contradição, a suposição inicial de que $\sqrt[n]{p}$ é racional é falsa, logo o contrário é verdade. Assim

$$\sqrt[n]{p}$$

é um número irracional, como queríamos demonstrar. ■

5.4 A IRRACIONALIDADE DE $\sqrt[n]{p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}}$ COM, $m_i < n$ PARA $i = \{1, 2, 3, \dots, r\}$

A próxima aplicação é para se mostrar a irracionalidade dos números da forma $\sqrt[n]{p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}}$ onde, $m_i < n$ para $i = \{1, 2, 3, \dots, r\}$ e a prova se dá pelo Teorema Fundamental da Aritmética e o processo por redução ao absurdo.

O resultado mostra a irracionalidade mais geral, mostra por exemplo que $\sqrt{3 \cdot 5}$, $\sqrt[3]{9}$ são irracionais. Ou seja, números da forma $\sqrt[n]{\alpha}$ com $\alpha, n \in \mathbb{N}$ e $n > 1$, onde:

$$\alpha = p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}$$

e $m_i < n$ para todo m_i , com $i = \{1, 2, 3, \dots, r\}$.

Demonstração: A demonstração vai ser por redução ao absurdo.

Suponhamos que $\sqrt[n]{\alpha}$, seja racional. Logo podemos escrever,

$$\sqrt[n]{\alpha} = \frac{a}{b},$$

com a e b números naturais e primos entre si, e $b \neq 0$. Assim,

$$\sqrt[n]{p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}} = \frac{a}{b} \Rightarrow a^n = b^n \cdot p_1^{m_1} \cdot \dots \cdot p_r^{m_r}.$$

Desse modo para algum $i = \{1, 2, 3, \dots, r\}$ existe um p_i , que tomaremos p_1 sem perda de generalidade, tal que

$$p_1^{m_1} | a^n \Rightarrow p_1 | a^n \Rightarrow p_1 | a.$$

Logo podemos escrever que $a = p_1 t$ com $t \in \mathbb{Z}$ positivo. Assim teremos:

$$\begin{aligned} a^n &= b^n \cdot p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r} \\ (p_1 t)^n &= b^n \cdot p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r} \\ p_1^n t^n &= b^n \cdot p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r} \\ p_1^j t^n &= b^n \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}, \end{aligned}$$

em que $j = n - m_1 \in \mathbb{N}$ pois $n - m_1 > 0$. Então,

$$\begin{aligned} p_1^j &| b^n \cdot p_2^{m_2} \dots p_r^{m_r} \Rightarrow \\ p_1 &| b^n \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}. \end{aligned}$$

Então segue que $p_1 \nmid p_2^{m_2} \cdot \dots \cdot p_r^{m_r}$ pois são primos distintos. Portanto

$$p_1 | b^n \Rightarrow p_1 | b,$$

que é um absurdo, pois chegamos a conclusão que $p_1 | a$ e $p_1 | b$ e supomos no início que $(a, b) = 1$. Logo os números da forma $\sqrt[n]{p_1^{m_1} \cdot p_2^{m_2} \cdot \dots \cdot p_r^{m_r}}$ onde, $m_i < n$ para $i = \{1, 2, 3, \dots, r\}$ são irracionais. ■

5.5 A IRRACIONALIDADE DO $\log 2$

Demonstração: Note inicialmente que $\log 2 > \log 1 = 0$. Suponha por absurdo que $\log 2$ é racional. Logo, $\log 2 = \frac{a}{b}$ onde $a, b \in \mathbb{Z}$ positivos e $(a, b) = 1$.

Da definição de logaritmos, temos que:

$$10^{\frac{a}{b}} = 2 \Rightarrow 10^a = 2^b \Rightarrow 2^a \cdot 5^a = 2^b.$$

Pelo Teorema Fundamental da Aritmética, as decomposições $2^a \cdot 5^a$ e 2^b devem ser iguais. para isso devemos ter $5^a = 1$, com isso a deve ser igual a 0, com isso

$$2^a \cdot 5^a = 1 = 2^b \Rightarrow b = 0.$$

Chegando assim a um absurdo, pois não está definido divisão por 0.

Portanto, $\log 2$ é um número irracional, como queríamos demonstrar. ■

5.6 CONDIÇÃO SOBRE OS TERMOS DO LOGARITMO PARA $\log_a b$ SER IRRACIONAL.

Proposição 5.1. *Sejam a e b positivos com $b \geq 2$ se as decomposições em fatores primos de a e b , apresentam pelo menos um fator que não é comum, então $\log_a b$ é um número irracional.*

Demonstração: Suponhamos por contra positiva que existem dois números inteiros m e n tal que $\log_a b = \frac{m}{n}$. Pela definição de logaritmos, temos que

$$a^{\frac{m}{n}} = b \iff b^n = a^m.$$

Da última igualdade com o auxílio do teorema, concluímos com o auxílio do Teorema Fundamental da Aritmética que os números a e b possuem exatamente os mesmos fatores primos. Com isso concluímos a demonstração por contra positiva. ■

Observação 5.3. Note que a recíproca da proposição não é verdadeira. veja que:

$$\log 20 = \log(2 \cdot 10) = \log 2 + \log 10 = \log 2 + 1.$$

Note que as decomposições de 10 e 20 em fatores primos são respectivamente $2 \cdot 5$ e $2^2 \cdot 5$, possuem os mesmos fatores primos em suas decomposições e mesmo assim temos como resulta um número irracional.

Portanto pela observação concluímos que a recíproca do teorema não é válida.

Outra aplicação do Teorema Fundamental da Aritmética está relacionada com os coeficientes inteiros de uma equação do 2º grau e com a determinação de possíveis raízes inteiras de polinômios especiais. Como apresentado a seguir.

5.7 RELAÇÃO ENTRE COEFICIENTES PRIMOS DISTINTOS DE UMA EQUAÇÃO DO 2º GRAU E RAÍZES DUPLAS.

Dada uma equação do 2º grau, de coeficientes inteiros e primos distintos, é possível que essa equação tenha uma raiz dupla?

Esse problema foi proposto pela revista do professor de matemática número 47. Vejamos como foi enunciado e vejamos sua demonstração usando o TFA.

Problema 5.1 (RPM Nº 47). *Uma equação do 2º grau, cujos coeficientes são todos números primos, pode apresentar duas raízes iguais (uma raiz dupla)?*

Demonstração: Para que a equação $ax^2 + bx + c = 0$ (com a , b e c primos) admita duas

raízes iguais, devemos ter

$$b^2 - 4ac = 0 \iff b^2 = 4ac,$$

o que implica b^2 par. Logo, b também é par pelas propriedades de paridade, como é primo, $b = 2$. Logo:

$$2^2 = 4ac \Rightarrow 2^2 = 2^2 ac.$$

Pelo Teorema Fundamental da Aritmética as fatorações devem ser iguais, daí teremos que $a \cdot c = 1$ o que é absurdo pois o produto de dois números primos é sempre maior que 1. Logo, se uma equação do 2^0 grau admite uma raiz dupla, então os coeficientes não podem ser todos primos. ■

5.8 APLICAÇÕES EM POLINÔMIOS ESPECIAIS

Exemplo 5.6. Determine se existem inteiros positivos x , y e z que satisfaçam a equação $2^x \cdot 3^4 \cdot 26^y = 39^z$

Solução: Note que a equação não está em sua forma fatorada. Fatorando cada termo teremos que:

$$2^x \cdot 3^4 \cdot 26^y = 39^z,$$

em sua forma fatorada fica:

$$\begin{aligned} 2^x \cdot 3^4 \cdot (2 \cdot 13)^y &= (3 \cdot 13)^z \implies \\ 2^{x+y} \cdot 3^4 \cdot 13^y &= 3^z \cdot 13^z. \end{aligned}$$

Pelo Teorema Fundamental da Aritmética as decomposições devem ser iguais. assim:

$$2^{x+y} = 2^0 \implies x + y = 0 \tag{44}$$

$$3^4 = 3^z \implies z = 4 \tag{45}$$

$$13^y = 13^z. \tag{46}$$

Com isso devemos ter $z = y = 4$ e $x = -4$ Logo a equação não possui inteiros que satisfaçam a equação, pois o expoente do primo 2 é um número negativo.

5.9 CRIPTOGRAFIA

Hoje o que mais se procura na matemática são aplicações práticas dos conteúdos e com o Teorema Fundamental da Aritmética não é diferente. Nesse trabalho apresentaremos o uso do TFA na criptografia, mais precisamente na criptografia RSA.

Para isso no entanto apresentaremos um breve histórico da origem da criptografia, sua evolução e de sua importância na sociedade atual.

A palavra criptografia tem origem grega e o radical *kriptos* significa oculto, portanto a palavra criptografia significa escrita oculta, assim a criptografia estuda os métodos para codificar(ocultar) uma mensagem de modo que só o verdadeiro destinatário consiga decodificar. Ao longo da história vários processos criptográficos foram criados, um dos mais famosos foi a cifra de César (utilizado na Roma antiga por Júlio Cesar), utilizada pelo líder romano para propósitos militares (era a forma secreta de comunicação com seus oficiais que estavam nos campos de batalha).

O sistema consistia em substituir uma letra do alfabeto original por uma outra letra, seguindo um determinado padrão (no caso cada letra era substituída pela que ficava três posições acima).

Só que, como os outros sistemas criptográficos, foram encontradas formas de descobrir os padrões, fazendo com que esses sistemas tenham entrado em desuso, ou sido aperfeiçoados para que não fossem descobertos os seus padrões por intrusos. A partir daí, a cada quebra de padrões, outros modelos criptográficos foram sendo criados, cada vez mais complexos para que não fosse possível que seus padrões fossem descobertos por terceiros(intrusos).

Um dos sistemas criptográficos que foi criado e que até os dias de hoje ainda se utiliza e que foi criado usando conhecimentos de teoria dos números, foi o sistema RSA. O sistema de criptografia RSA é um dos métodos de criptografia de chave pública bastante conhecido. Ele foi criado em 1978 por pesquisadores que trabalhavam no Massachusetts Institute of Technology (M.I.T.).

As letras da sigla R.S.A. correspondem às iniciais dos seus três criadores : Ron L. Rivest, Adi Shamir e Leonard Adleman. Segundo Coutinho (2005), "há vários outros códigos de chave pública, mas o RSA é o mais utilizado atualmente em transações comerciais". Para um maior aprofundamento consulte Coutinho (2005).

Para que o método RSA possa ser implementado precisamos de dois parâmetros básicos: dois números primos distintos de grande magnitude que chamaremos de p e q .

Mas a primeira fase do processo de codificação de uma mensagem inicia-se com a pré-codificação. Como o sistema foi criado utilizando conhecimentos de teoria dos números, mensagens silábicas devem ser convertidas em números segundo uma tabela que pode se iniciar por exemplo com o número 10 correspondendo à letra A e terminar no número 35 correspondendo a letra Z. Convenciona-se que o espaço entre as palavras será substituído pelo número 99.

Após a conversão numérica, a mensagem pode ser quebrada em blocos obedecendo os seguintes critérios:

- Cada bloco não deve ser iniciado com zero.
- Cada bloco deve ser menor que o produto dos primos escolhidos.

Após o processo de codificação, devemos iniciar o processo de criptografia, precisamos conhecer uma chave denominada pública ou de codificação que é formada por dois números n e e . Onde:

- n é produto dos primos p e q mencionados acima e;
- e deve ser um inteiro positivo invertível módulo $\varphi(n)$, ou seja, $(e, \varphi(n)) = 1$.

Esse número e , quando se conhecem p e q é fácil calcular $\varphi(n)$, uma vez que $\varphi(n) = (p-1)(q-1)$. O par (n, e) é chamado de chave de codificação do sistema RSA.

Cada bloco b criado obedecendo os critérios acima, será codificado obtendo-se a forma reduzida de b^e módulo n , isto é, $C(b) = \text{resto da divisão de } b^e \text{ por } n$. Ou seja, utilizamos conhecimentos da aritmética modular, isto é, de congruências: $C(b) \equiv b^e \pmod{n}$.

Para o processo de decodificação, é necessária a chave de decodificação, conhecida apenas pela pessoa que irá decodificar a mensagem. A chave de decodificação também é denominada como chave privada e é formada pelo par (n, d) . Onde:

- O número d é o inverso de e módulo $\varphi(n)$.

Se chamarmos de a um bloco da mensagem codificada, então $D(a)$ será o resultado do processo de decodificação que é obtido da seguinte forma: $D(a) = \text{resto da divisão de } a^d \text{ por } n$. Em termos de aritmética modular, $D(a)$ é a forma reduzida de $a^d \pmod{n}$.

Para decodificar a mensagem deve-se encontrar a forma reduzida de todos os blocos codificados, utilizando-se a chave (n, d) , e separá-los de dois em dois algarismos. Finalmente, faz-se a correspondência desses blocos de dois algarismos com as letras da tabela, obtendo-se assim a mensagem enviada. Calcular d é fácil, desde que $\varphi(n)$ e e sejam conhecidos, pois basta aplicar o algoritmo de Euclides estendido, ou seja, determinar a solução da congruência

$$e \cdot d \equiv 1 \pmod{\varphi(n)}.$$

No entanto, para calcularmos $\varphi(n)$ é necessário conhecermos os dois fatores primos de n ou seja p e q . Torna-se difícil descobrir os números p e q , pois são números primos da ordem de 100 ou mais algarismos.

Para fixar o entendimento do sistema RSA, vamos imaginar a seguinte situação: suponha que João queira se comunicar em segredo com sua amiga Maria, para testar o processo de criptografia RSA, para isso João escolhe dois números $p = 7$ e $q = 11$ primos e faz o seu produto encontrando $n = p \cdot q = 77$; em seguida calcula $\varphi(n) = (7-1) \cdot (11-1) = 60$. Agora João escolhe o número e tal que $(e, \varphi(n)) = 1$. Assim seja $e = 7$ a sua escolha, com o par $(n, e) = (77, 7)$ João está com a chave de codificação e a envia para Maria. Ela deseja enviar a palavra PROFMAT para ele de forma secreta.

Então Maria deve proceder da seguinte forma: Deve fazer a pré-codificação da mensagem, ou seja, associar cada letra da palavra PROFMAT a um número com dois

dígitos, conforme Tabela (4) para a pré-codificação e usará o símbolo 99 para indicar o espaço entre palavras.

Tabela 4 – Tabela de pré-codificação

A	B	C	B	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: Elaborada pelo autor.

Assim após a pré-codificação a mensagem fica:

25272415221029.

Em seguida quebra a mensagem em blocos b de forma que o número de cada bloco é menor que n . Os blocos escolhidos foram com forme Tabela (5).

Tabela 5 – Blocos escolhidos

25	27	24	15	22	10	29
b_1	b_2	b_3	b_4	b_5	b_6	b_7

Fonte: Elaborada pelo autor.

Agora deve-se calcular os restos das congruências

$$r_n \equiv b_n^e \pmod{n},$$

para $n = \{1, 2, \dots, 6, 7\}$.

Para $n = 1$,

$$r_1 \equiv b_1^e \pmod{n} \Rightarrow r_1 \equiv 25^7 \pmod{77}.$$

Como

$$25 \equiv 25 \pmod{77} \tag{47}$$

$$25^2 = 625 \equiv 9 \pmod{77} \tag{48}$$

$$(25^2)^3 \equiv 9^3 \pmod{77} \Rightarrow 25^6 \equiv 4 \cdot 9 = 36 \pmod{77}. \tag{49}$$

multiplicando (47) e (49) teremos:

$$25^7 \equiv 25 \cdot 36 = 900 \equiv 53 \pmod{77}.$$

Logo $r_1 = 53$.

Para $n = 2$ teremos:

$$r_2 \equiv 27^7 \pmod{77}.$$

Como

$$27 \equiv 27 \pmod{77} \quad (50)$$

$$27^2 = 729 \equiv 36 \pmod{77} \quad (51)$$

$$(27^2)^3 \equiv 36^3 = 36 \cdot 36^2 = 36 \cdot 1296 \equiv 36 \cdot 64 = 2304 \equiv 71 \pmod{77}. \quad (52)$$

multiplicando (50) e (52) teremos:

$$27^7 \equiv 27 \cdot 71 = 1917 \equiv 69 \pmod{77}.$$

Logo $r_2 = 69$.

Para $n = 3$ teremos:

$$r_3 \equiv 24^5 \pmod{77}.$$

Como

$$24 \equiv 24 \pmod{77} \quad (53)$$

$$24^2 = 576 \equiv 37 \pmod{77} \quad (54)$$

$$(24^2)^3 \equiv 37^3 \equiv 64 \pmod{77}. \quad (55)$$

Multiplicando as equações (53) e (55) teremos que:

$$24^7 \equiv 24 \cdot 64 = 1536 \equiv 73 \pmod{77}.$$

Logo $r_3 = 73$.

Para $n = 4$, teremos:

$$r_4 \equiv 15^7 \pmod{77}.$$

Como

$$15 \equiv 15 \pmod{77} \quad (56)$$

$$15^2 = 225 \equiv 71 \equiv (-6) \pmod{77} \quad (57)$$

$$(15^2)^3 \equiv (-6)^3 = -216 \equiv 15 \pmod{77}. \quad (58)$$

Logo, multiplicando termo a termo as equações (56) e (58) teremos:

$$15^7 \equiv 15 \cdot 15 = 225 \equiv 71 \pmod{77}.$$

Logo $r_4 = 71$.

Para $n = 5$, teremos:

$$r_5 \equiv 22^7 \pmod{77}.$$

Como

$$22 \equiv 22 \pmod{77} \tag{59}$$

$$(22^2) = 484 \equiv 22 \pmod{77} \tag{60}$$

$$(22^2)^3 \equiv 22^3 = 10626 \equiv 22 \pmod{77}. \tag{61}$$

Logo multiplicando termo a termo (59) e (61) teremos:

$$22^7 \equiv 22 \cdot 22 = 484 \equiv 22 \pmod{77}.$$

Portanto, $r_5 = 22$.

Para $n = 6$, teremos:

$$r_6 \equiv 10^7 \pmod{77}.$$

Como

$$10 \equiv 10 \pmod{77} \tag{62}$$

$$10^3 = 1000 \equiv 76 \equiv (-1) \pmod{77} \tag{63}$$

$$(10^3)^2 \equiv (-1)^2 = 1 \equiv 1 \pmod{77}. \tag{64}$$

Logo multiplicando as congruências (62) e (64) termo a termo, teremos:

$$10^7 \equiv 10 \cdot 1 = 10 \pmod{77}.$$

Portanto, $r_6 = 10$.

Para $n = 7$, teremos:

$$r_7 \equiv 29^7 \pmod{77}.$$

Como

$$29 \equiv 29 \pmod{77} \quad (65)$$

$$29^2 = 841 \equiv 71 \pmod{77} \quad (66)$$

$$(29^2)^3 \equiv 71^3 = 71 \cdot 5041 \equiv 71 \cdot 36 = 2556 \equiv 15 \pmod{77}. \quad (67)$$

Logo multiplicando as congruências (65) e (67) termo a termo, teremos:

$$29^7 \equiv 29 \cdot 15 = 435 \equiv 50 \pmod{77}.$$

Portanto, $r_7 = 50$.

Feito a codificação dos blocos, Maria ficou com o novo bloco a ser enviado para João.

$$53 - 69 - 73 - 71 - 22 - 10 - 15.$$

De posse desse código João agora deve decodificar essa mensagem, mas para isso ele precisa criar sua chave particular (secreta), (n, d) onde d é o inverso multiplicativo de $e \pmod{\varphi(n)}$.

Para calcular a sua chave privada, ele deve resolver a congruência:

$$e \cdot d \equiv 1 \pmod{\varphi(n)}.$$

Como $\varphi(n) = (7-1) \cdot (11-1) = 6 \cdot 10 = 60$, para determinar o valor de d , João precisa encontrar a solução da congruência:

$$7 \cdot d \equiv 1 \pmod{60}.$$

Usando o algoritmo estendido de Euclides temos que:

$$60 = 7 \cdot 8 + 4 \Rightarrow 60 - 7 \cdot 8 = 4 \quad (68)$$

$$7 = 4 \cdot 1 + 3 \Rightarrow 7 - 4 \cdot 1 = 3 \quad (69)$$

$$4 = 3 \cdot 1 + 1 \Rightarrow 4 - 3 = 1 \quad (70)$$

$$3 = 3 \cdot 1. \quad (71)$$

Como o último resto obtido antes do resto nulo foi 1 então $(60, 7)=1$.

Agora substituindo (69) em (70) teremos

$$4 - (7 - 4 \cdot 1) = 1 \Rightarrow 2 \cdot 4 - 7 = 1. \quad (72)$$

Agora substituindo (68) em (72) fica:

$$2 \cdot (60 - 7 \cdot 8) - 7 = 1 \Rightarrow 2 \cdot 60 - 17 \cdot 7 = 1. \quad (73)$$

Aplicando congruência $\pmod{60}$ em (73) teremos:

$$\begin{aligned} 2 \cdot 60 - 17 \cdot 7 &\equiv 1 \pmod{60} \\ -17 \cdot 7 &\equiv 1 \pmod{60} \\ (-17 \cdot 7)^2 &\equiv 1 \pmod{60} \\ 17^2 \cdot 7 \cdot 7 &\equiv 1 \pmod{60} \\ 2023 \cdot 7 &\equiv 1 \pmod{60} \\ 43 \cdot 7 &\equiv 1 \pmod{60}. \end{aligned}$$

Logo o número d , inverso multiplicativo de $7 \pmod{60}$ é 43. Agora que João tem a sua chave privada de decodificação ($d = 43, n = 77$) esta pronto para decodificar o código enviado por Maria.

Para decodificar ele tem que encontrar os restos das congruências

$$R_n \equiv r_n^d \pmod{77},$$

com $n = \{1, 2, 3, 4, 5, 6, 7\}$, onde r_n representa os blocos a serem decodificados enviado por Maria.

Fazendo os cálculos para a decodificação.

para $n=1$, teremos:

$$R_1 \equiv 53^{43} \pmod{77}.$$

Como

$$53^3 \equiv 36 \pmod{77} \quad (74)$$

$$(53)^5 \equiv 23 \pmod{77} \quad (75)$$

$$23^3 \equiv 1 \pmod{77} \quad (76)$$

$$53^{40} = (53^5)^8 \equiv 23^8 = (23^3)^2 \cdot 23^2 \equiv 67 \pmod{77}. \quad (77)$$

Logo multiplicando termo a termo as congruências (74) e (77) teremos que:

$$53^{43} \equiv 36 \cdot 67 = 2412 \equiv 25 \pmod{77}.$$

Logo $R_1 = 25$.

Para $n = 2$, teremos:

$$R_2 \equiv 69^{43} \pmod{77}.$$

Como

$$69^3 \equiv (-8)^3 = -512 \equiv 27 \pmod{77} \quad (78)$$

$$15^5 \equiv 1 \pmod{77} \quad (79)$$

$$69^4 \equiv 15 \pmod{77} \quad (80)$$

$$69^{40} = (69^4)^{10} \equiv 15^{10} = (15^5)^2 \equiv 1 \pmod{77}. \quad (81)$$

Logo multiplicando termo a termo as congruências (78) e (81) teremos que:

$$69^{43} \equiv 27 \cdot 1 = 27 \pmod{77}.$$

Logo $R_2 = 27$.

Para $n = 3$, teremos:

$$R_3 \equiv 73^{43} \pmod{77}.$$

Como

$$73^3 \equiv (-4)^3 \equiv 13 \pmod{77} \quad (82)$$

$$73^4 \equiv (-4)^4 \equiv 25 \pmod{77} \quad (83)$$

$$25^2 \equiv 9 \pmod{77} \quad (84)$$

$$73^{40} = (73^4)^{10} \equiv 25^{10} = (25^2)^5 \equiv 9^5 \equiv 67. \quad (85)$$

Logo multiplicando termo a termo as congruências (82) e (85) teremos que:

$$73^{43} \equiv 13 \cdot 67 = 871 \equiv 24 \pmod{77}.$$

Logo $R_3 = 24$.

Para $n = 4$, teremos:

$$R_4 \equiv 71^{43} \pmod{77}.$$

Como

$$71^3 \equiv (-6)^3 \equiv 15 \pmod{77} \quad (86)$$

$$71^5 \equiv (-6)^5 \equiv 1 \pmod{77} \quad (87)$$

$$71^{40} = (71^5)^8 \equiv 1^8 = 1 \pmod{77}. \quad (88)$$

Logo multiplicando termo a termo as congruências (86) e (88) teremos que:

$$71^{43} \equiv 15 \cdot 1 = 15 \pmod{77}.$$

Logo $R_4 = 15$.

Para $n = 5$, teremos:

$$R_5 \equiv 22^{43} \pmod{77}.$$

Como

$$22^3 = 35937 \equiv 22 \pmod{77} \quad (89)$$

$$22^2 = 484 \equiv 22 \pmod{77} \quad (90)$$

$$22^5 = 22^3 \cdot 22^2 \equiv 22^2 \equiv 22 \pmod{77} \quad (91)$$

$$22^{40} = (22^5)^8 \equiv 22^8 \equiv 22 \pmod{77}. \quad (92)$$

Logo multiplicando termo a termo as congruências (89) e (92) teremos que:

$$22^{43} \equiv 22 \cdot 22 = 484 \equiv 22 \pmod{77}.$$

Logo $R_5 = 22$.

Para $n = 6$, teremos:

$$R_6 \equiv 10^{43} \pmod{77}.$$

Como

$$10^3 \equiv 76 \equiv (-1) \pmod{77} \quad (93)$$

$$10^{10} \equiv (-10) \pmod{77} \quad (94)$$

$$10^{40} = (10^{10})^4 \equiv (-10)^4 \equiv (-10) \pmod{77}. \quad (95)$$

Logo multiplicando termo a termo as congruências (93) e (95) teremos que:

$$10^{43} \equiv (-1) \cdot (-10) = 10 \pmod{77}.$$

Logo $R_6 = 10$.

Para $n = 7$, teremos:

$$R_7 \equiv 50^{43} \pmod{77}.$$

Como

$$50^3 \equiv (-27)^3 \equiv 29 \pmod{77} \quad (96)$$

$$50^8 \equiv 15 \pmod{77} \quad (97)$$

$$50^{40} = (50^8)^5 \equiv 15^5 \equiv 1 \pmod{77}. \quad (98)$$

Logo multiplicando termo a termo as congruências (96) e (98) teremos que:

$$50^{43} \equiv 29 \cdot 1 = 29 \pmod{77}.$$

Logo $R_7 = 29$.

Portanto, como era de se esperar após decodificada a mensagem formada pelos blocos $R_1 = (25)$, $R_2 = (27)$, $R_3 = (24)$, $R_4 = (15)$, $R_5 = (22)$, $R_6 = (10)$, $R_7 = (29)$ representa a mensagem pré-codificada por Maria, o que mostra que o sistema funciona.

Porque o RSA funciona?

O método apresentado só será útil, se após a decodificação de um bloco codificado, tivermos de volta o bloco correspondente da mensagem original. Digamos que temos um sistema RSA de parâmetros p e q , onde $n = p \cdot q$. Então os dados de codificação é (n, e) a chave pública a qual todos tem acesso e os dados da decodificação é (n, d) que é a chave privada. Queremos mostrar que:

$$DC(b) \equiv b \pmod{n}.$$

Por definição de codificação(C) e decodificação(DC), temos que:

$$DC(b) = (b^e)^d \equiv b^{d \cdot e} \pmod{n}.$$

Como d é o inverso de $e \pmod{\varphi(n)}$, temos que $e \cdot d = 1 + k\varphi(n)$.

$$\begin{aligned} DC(b) = (b^e)^d &\equiv b^{d \cdot e} \pmod{n} \\ &\equiv b^{1+k(n-1)(p-1)} \pmod{n}. \end{aligned}$$

como $n = p \cdot q$ e $(p, q) = 1$, calculemos as congruências.

$$DC(b) \equiv (b^e)^d \equiv b^{1+k(n-1)(p-1)} \pmod{p} \quad (99)$$

e

$$DC(b) \equiv (b^e)^d \equiv b^{1+k(n-1)(p-1)} \pmod{q}. \quad (100)$$

Resolvendo (99), temos que considerar 2 casos:

1. Se $p \nmid b$ temos pelo Teorema de Fermat que $b^{p-1} \equiv 1 \pmod{p}$, logo:

$$\begin{aligned} DC(b) \equiv (b^e)^d &\equiv b^{1+k(n-1)(p-1)} \pmod{p} \\ &\equiv b \cdot (b^{p-1})^{k(q-1)} \pmod{p} \\ &\equiv b \cdot 1 = b \pmod{p}. \end{aligned}$$

2. Se $p|b$ temos que $b \equiv 0 \pmod{p}$, logo $b^{1+k(n-1)(p-1)} \equiv 0^{1+k(n-1)(p-1)} \equiv 0 \pmod{p}$.

Portanto a congruência é válida para todo b .

De forma análoga $b^{e \cdot d} \equiv b \pmod{q}$. Portanto pelas propriedades de congruência.

$$\begin{aligned} DC(b) \equiv (b^e)^d &\equiv b \pmod{[p, q]} \\ &\equiv b \pmod{p \cdot q} \\ &\equiv b \pmod{n}. \end{aligned}$$

Isso encerra a demonstração de que o método funciona.

O que torna seguro o RSA?

O RSA só é seguro se for difícil calcular d , conhecendo apenas a chave pública (n, e) . Como d é dado em função de $\varphi(n)$ e e , mas só sabemos calcular $\varphi(n)$ se soubermos a fatoração única de n para determinar os seus fatores únicos p e q . Mas se n for grande essa é uma tarefa difícil, já que não se conhece ainda um algoritmo de fatoração rápido.

Para mais detalhes consulte Coutinho (2005), Lemos (2001) E Silva (2021).

6 CONCLUSÃO

Na matemática os teoremas que são apresentados como fundamentais são, como sua própria determinação, essenciais para o desenvolvimento de uma cadeia de conhecimentos matemáticos. Isso pode ser visto nos teoremas fundamentais da álgebra, do cálculo, da semelhança, da proporcionalidade, da aritmética entre outros. O Teorema Fundamental da Aritmética está presente na construção de vários outros tópicos da matemática, nesse trabalho foi mostrado apenas um pequeno percentual das aplicações visíveis desse importante teorema, que está presente desde o tempo de Euclides de Alexandria.

A matemática é uma disciplina obrigatória em nossa formação, dada a sua importância na formação do raciocínio lógico dedutivo de nossos alunos. Isso se confirma em Brasil (1999) , que diz: "A Matemática ajuda a estruturar o pensamento e o raciocínio dedutivo, além de ser uma ferramenta para tarefas específicas em quase todas as atividades humanas".

Nas competências e habilidades a serem desenvolvidas nos PCN's do ensino médio diz que:

- Desenvolver a capacidade de utilizar a Matemática na interpretação e intervenção no real.
- Aplicar conhecimentos e métodos matemáticos em situações reais, em especial em outras áreas do conhecimento.

Hoje se busca no ensino de matemática, principalmente na educação básica, aplicações práticas dos conteúdos ensinados em sala de aula, essa cobrança esta nos documentos básicos que regem a educação, A bncc diz:

espera-se que eles desenvolvam a capacidade de identificar oportunidade de utilização da matemática, para resolver problemas, aplicando conceitos e procedimentos e resultado para obter soluções e interpreta-las segundo os contextos de utilização.(BRASIL, 2018)

Nesse trabalho o Teorema Fundamental da Aritmética, aliado a outros resultados básicos estão sendo aplicados, para a determinação de outros resultados práticos, que podem ajudar os alunos na oportunidade de resolver problemas do cotidiano. O TFA aliado a aritmética modular desenvolvida por Gauss, tem como uma de suas aplicações mais úteis na prática, na criptografia RSA. Esse sistema é tão fundamental aliado a rede mundial de computadores, que sem ele muitas das atividades de nosso dia a dia que envolve a segurança de nossas informações confidenciais, como, compras com cartões de crédito, transações bancárias, conversas por mensagem de textos, seriam impraticáveis.

Por fim creio que o trabalho traz consigo um extenso material sobre o Teorema Fundamental da Aritmética e suas aplicações, possibilitando ao público leitor uma visão de integração entre os ramos da matemática e a sua aplicabilidade a situações da realidade. Atendendo dessa forma ao que se pede nos documentos que norteiam a nossa educação. Para que dessa forma os nossos alunos possam obter êxito no processo de ensino

aprendizagem dessa disciplina que é tão fundamental nas diversas áreas do conhecimento. E que sirva de fonte de pesquisa e estudo para alunos que queiram participar de olimpíadas matemáticas e que queiram ingressar em um PROFMAT , através do exame nacional de acesso (ENA).

REFERÊNCIAS

- ALENCAR FILHO, Edgard de. **Teoria elementar dos Números**. Nobel, SP, 1981.
- BERTONE, Ana Maria Amarillo. **Introdução à Teoria dos Números**. UFU, 2014.
- BICUDO, Irineu. **Os elementos**. Unesp, 2009.
- BOYER, Carl B; MERZBACH, Uta C. **História da matemática**. Editora Blucher, 2019.
- BRASIL. **Parâmetros curriculares nacionais: ensino médio**. *Brasília: MEC*, 1999.
- BRASIL. **Base Nacional Comum Curricular**. *Brasília: MEC*, 2018.
- CARVALHO, Paulo Cezar Pinto; MORGADO, Augusto César. **Matemática discreta**. Coleção PROFMAT. Rio de Janeiro: SBM, 2015.
- COUTINHO, Severino Colier. **Números inteiros e criptografia RSA**. IMPA, 2005.
- EULER, Leonhard. **Elements of algebra**. Springer Science & Business Media, 2012.
- EULER, Leonhard Paul. **Nota Histórica**. *Revista Elementos*. 4^a edição ano, p. 86–90, 2004.
- EVES, Howard Whitley; *et al.* **Introdução à história da matemática**. Unicamp Campinas, 2004.
- GAUSS, C. F. **Disquisitiones arithmeticae**. New Haven, 1995.
- HEFEZ, Abramo. **Aritmética**. Coleção PROFMAT. Sociedade Brasileira de Matemática, 2016.
- LEGENDRE, Adrien Marie. **Essai sur la theorie des nombres; par AM Legendre, membre de l’Institut et de la Legion d’Honneur..** chez Courcier, imprimeur-libraire pour les mathematiques, quai des Augustins, 1808.
- LEMOES, Manoel. **Criptografia, números primos e algoritmos**. IMPA, 2001.
- NASCIMENTO, Mauri Cunha do; ARAUJO Feitosa, Hércules de. **Elementos da Teoria dos Números**. Unesp, 2013.
- SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. Rio de Janeiro: IMPA, 2000.

SILVA, Wirlan Chagas da. **A criptografia e seu desenvolvimento matemático**. 2021. 109 f. Dissertação (Mestrado Profissional em Matemática em rede Nacional) – Universidade da Integração Internacional da Lusofonia Afro-Brasileira, Redenção, 2021. Disponível em: <http://repositorio.unilab.edu.br:8080/jspui/handle/123456789/2440>. Acesso em: 13 jul. 2023.

VICENTIN, Giovani Heinzen; AGUIAR, Marcos Gabriel Souza. Clubes de Matemática da OBMEP: Disseminando o estudo de matemática. **b_Euclides**. [S.l.], 2020. Disponível em: http://clubes.obmep.org.br/blog/b_euclides/. Acesso em: 13 jul. 2023.

WITTMANN, Axel D. Carl Friedrich Gauss and the Gauss Society: a brief overview. **History of Geo-and Space Sciences**, v. 11, n. 2, p. 199–205, 2020. Disponível em: <https://hgss.copernicus.org/articles/11/199/2020/>. Acesso em: 13 jul. 2023.