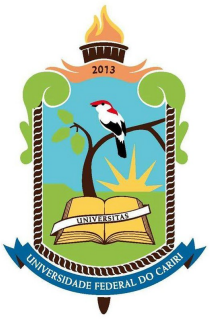


UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
EM REDE NACIONAL

WESLEY CASTRO TEIXEIRA

FERMAT E OS NÚMEROS PRIMOS

JUAZEIRO DO NORTE
2017

WESLEY CASTRO TEIXEIRA

FERMAT E OS NÚMEROS PRIMOS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional da Universidade Federal do Cariri, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Teoria dos Números.

Orientador:
Profª.Drª.Maria Silvana Alcântara Costa.
Co-Orientador:
Prof. Dr. Steve da Silva Vicentim

JUAZEIRO DO NORTE
2017

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Fermat e os Números Primos

Wesley Castro Teixeira

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional – PROFMAT do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Teoria de Números.

Aprovada em 20 de julho de 2017.

Banca Examinadora

Maria Silvana Alcantara Costa

Profa. Dra. Maria Silvana Alcântara Costa – UFCA

Orientadora

Prof. Dr. Steve da Silva Vicentim – UFCA
Co-Orientador

Valdinês Leite de Sousa Júnior

Prof. Dr. Valdinês Leite de Sousa Júnior – UFCA

A todos que me ajudaram, direta ou indiretamente, nessa jornada.

AGRADECIMENTOS

Aos meus pais, Elieusa de Castro Teixeira e Luciano Teixeira da Silva, por toda confiança, incentivo e apoio ao longo dessa jornada, principalmente por acreditarem no verdadeiro valor da educação.

A Maria Leidiane Lima Pereira, minha namorada, por todo carinho, amor, dedicação e, acima de tudo, por sempre acreditar no meu potencial.

A Maria Silvana Alcântara Costa, minha orientadora, por toda contribuição intelectual e pela disposição ao longo da realização dessa pesquisa.

A Steve da Silva Vicentim, meu co-orientador, que foi como um guia dentro desse vasto campo da álgebra e que através de nossas conversas mostrou uma nova maneira de enxergar a matemática.

A minha tia, Eliete de Castro e minha prima Priscyla de Castro, pela grande ajuda na produção desse trabalho.

Aos amigos, Leiliane Lima e Zé Maria Mota, por abrirem as portas de sua residência e assim permitirem um pouco de descanso para corpo e mente.

Aos companheiros de trabalho, Luzia, Aluizio e Ludmila, por tornarem as manhãs de trabalho mais divertidas.

À Sociedade Brasileira de Matemática (SBM) pela idealização do projeto.

A todos os professores do PROFMAT - UFCA por todas as horas dedicadas a melhoria da educação brasileira.

A todos os colegas de curso.

“ A Matemática é a rainha das ciências e a teoria dos números é a rainha das matemáticas.” (Gauss)

RESUMO

Ao longo da evolução da matemática, inúmeros estudiosos se dedicaram a expandir o conhecimento acerca dos números primos. Desde o princípio, com Euclides de Alexandria, o estudo dos números primos mostrou-se cercado de mais indagações do que respostas. Todavia, cada descoberta, mesmo as de menor relevância, sempre resultaram em grandes avanços na construção da Teoria dos Números. Ao longo da história, grandes matemáticos como Fermat, Euler, Gauss e Riemann desenvolveram pesquisas na Teoria dos Números, particularmente os números primos, e seus trabalhos foram essenciais para alavancar diversos campos da ciência, como a Matemática Computacional e a Criptografia. Por fim, o presente trabalho visa mostrar a importância de um desses matemáticos, Pierre de Fermat, para a evolução das ideias dos números primos, em especial o "grande", Pequeno Teorema de Fermat.

Palavras-chave: Teoria dos Números. Números Primos. Fermat.

ABSTRACT

Throughout the evolution of mathematics, countless scholars have devoted themselves to expanding knowledge about prime numbers. From the beginning, with Euclid of Alexandria, the study of prime numbers has been surrounded by more questions than answers. But, each discovery, even of less importance, has always resulted in great advances in the construction of Number Theory. At the same time, great mathematicians such as Fermat, Euler, Gauss, and Riemann have developed research into number theory, particularly prime numbers. Their work was essential to leverage various fields of science such as computational mathematics and cryptography. Finally, the present work aims to show the importance of one of these mathematicians, Pierre de Fermat, for the evolution of the ideas of the prime numbers, especially the "big", small theorem of Fermat.

Keywords: Number Theory. Prime numbers. Fermat.

SUMÁRIO

1 INTRODUÇÃO

Teoria dos números, ou como é comumente chamada Aritmética, é o ramo mais antigo da matemática, bem como o mais fascinante. O que talvez permita diferenciar a teoria dos números dos outros campos da referida área de conhecimento, seja o fato de que a maioria dos seus problemas esteja relacionado aos números inteiros. Dessa forma, dentre a infinitude dos inteiros, é possível encontrar certos números que, desde a sua descoberta, despertam o interesse de muitos matemáticos, os números primos.

A partir do surgimento dos números primos, perguntas surgiam sobre os mesmos: Quantos existem? Como é sua distribuição nos inteiros? Como identificá-los? Ao longo da evolução da Aritmética, alguns desses questionamento, foram resolvidos, entretanto, muitos outros se mantêm. Por exemplo, ainda não se sabe se existe uma função que gere somente primos. Também não se sabe, ao certo, como eles se distribuem ao longo do conjunto dos inteiros.

Diante dessa real importância dos números primos no entendimento da matemática, é necessário ao professor, um bom entendimento dos principais resultados sobre os mesmos. Assim, esse trabalho visa apresentar a esse profissional, mais uma fonte de pesquisa e aperfeiçoamento.

Além de apresentar os números primos, o trabalho visa destacar uma das contribuições mais relevantes do matemático, Pierre de Fermat (1601 - 1665), para o estudo da Aritmética. Seu teorema conhecido como, Pequeno Teorema de Fermat. A importância desse teorema é evidenciada pelas suas generalizações feitas por Euler, Gauss e Möbius. Generalizações essas, que se utilizam de recursos avançados tais como, a função de Möbius e a fórmula de inversão de Möbius [23].

O presente trabalho foi dividido em três partes. Inicialmente, no capítulo 2, apresentamos a construção do conjunto dos números naturais e definimos as operações de adição e multiplicação. Logo após, exibimos estruturas algébricas necessárias para o bom entendimento da caracterização do conjunto dos inteiros. E por fim, definimos a operação de congruência. Para a construção desse capítulo, os livros [4], [7], [8], [9], [11], [14], [24] foram de vital importância e podem ser consultados para maiores informações.

No capítulo 3, foi introduzido a noção de número primo. Concomitante a isso, exibimos e demonstramos resultados clássicos como, o Teorema Fundamental da Aritmética e o teorema que garante a infinitude dos números primos. Logo após, apresentamos

o teste de primalidade mais conhecido, o Crivo de Erastóstenes. E dando continuidade, mostramos alguns outros resultados a respeito do números primos. As obras [10], [18], [22], [20] foram as principais obras utilizadas nesse capítulo.

Por fim, no capítulo 4, é apresentado um breve relato sobre a vida de Fermat e de Euler, para em seguida, expor o Pequeno Teorema de Fermat. Por conseguinte, apresenta-se a sua principal generalização, creditada a Euler. Para isso foram definidos operações como ordem, função de Euler e raiz primitiva. Além do mais, ressaltamos a não veracidade da recíproca do Pequeno Teorema de Fermat, discorrendo sobre os pseudoprimos ou números de Carmichael. Os livros, [10], [21], [16] e [20] podem ser consultados caso haja a necessidade de uma melhor compreensão.

2 OS NÚMEROS INTEIROS

Desde o início da civilização, a humanidade sentiu a necessidade de contar e de registrar de maneira numérica o mundo a sua volta. Essa necessidade está intimamente ligada a existência dos números naturais ($\mathbb{N}$). Por exemplo, o homem criava situações interessantes na contagem de seus objetos, animais, etc. Ao levar seu rebanho para a pastagem o pastor podia relacionar uma pedra a cada animal. No momento em que ele recolhia os animais fazia a relação inversa. No caso de sobrar alguma pedra, poderia verificar a falta de algum animal. Essa necessidade de aprimorar os processos de contagem e seus registros tornou-se fundamental. Assim, foram criados os símbolos e regras originando diferentes sistemas de numeração.

O sistema de escrita numérica mais antigo registrado é o dos egípcios, que era formado por sete símbolos chaves, não posicional, ou seja, qualquer número era formado pela união desses, independente da ordem.

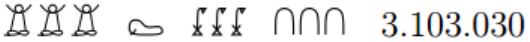
Figura 2.1: Numeração Egípcia

						
1.000.000	100.000	10.000	1.000	100	10	1

Fonte: Introdução a História da Matemática[16]

A seguir, exemplos de números grafados com o sistema egípcio.

Figura 2.2: Números na escrita egípcia

	21		3.103.030
	201		21.032
	475		38.500

Fonte: Introdução a História da Matemática[16]

Outro sistema bastante difundido e usado até hoje é o sistema de numeração Romano. É utilizado em representações de séculos, capítulos de livros, mostradores de relógios antigos, nomes de reis e papas e outros tipos de representações oficiais em documentos. Tal sistema não permite que sejam feitos cálculos, pois não se destinava a fazer operações aritméticas, mas apenas representar quantidades.

Figura 2.3: Numeração Romana

1	I	8	VIII
2	II	9	IX
3	III	10	X
4	IV	50	L
5	V	100	C
6	VI	500	D
7	VII	1000	M

Fonte: www.infopedia.pt[12]

Apenas séculos depois da criação dos números romanos é que surgiu um dos maiores avanços significativos da matemática, os algarismos arábicos, também chamados de indo-arábicos. Foram criados e desenvolvidos pela Civilização do Vale do Indo (atual Paquistão).

A chegada da numeração indo-arábica à Europa é atribuída ao matemático italiano Leonardo de Piza (1170 - 1250), apelidado de Fibonacci. Ele estudou em Bugia (Argélia) e o seu livro intitulado *Liber Abaci*, publicado em 1202, contribuiu para expandir o sistema arábico pela Europa.N o entanto, o uso generalizado deste sistema na Europa só se deu após a invenção da imprensa em 1450 [6].

O sistema de numeração árabe, que é decimal, é o mais usado atualmente e, para representar os números, são empregados apenas 10 símbolos diferentes: os denominados algarismos árabes.

Com o início do Renascimento surgiu a expansão comercial, aumentando a circulação de dinheiro e obrigando os comerciantes a trabalharem com situações envolvendo lucros e prejuízos. A maneira que eles encontraram de resolver tais situações problema consistia no uso dos símbolos "+" e "−". Por exemplo, suponha que um comerciante tenha três sacas de arroz de 10 kg cada em seu armazém. Se ele vendesse 5 Kg de arroz, escreveria o número 5 acompanhado do sinal −; se ele comprasse 7 Kg de arroz, escreveria o numeral 7 acompanhado do sinal + [19].

Utilizando essa nova simbologia, os matemáticos da época desenvolveram técnicas operacionais capazes de expressar qualquer situação envolvendo números positivos e negativos. Surgindo um novo conjunto numérico representado pela letra $\mathbb{Z}$, (de Zahlen, número em alemão), conhecido como conjuntos dos números inteiros, objeto de estudo desse capítulo.

2.1 O QUE É UM NÚMERO NATURAL ?

Com o avanço da ciência, novas descobertas na área da matemática surgiam e, com isso, antigos conceitos foram melhorados. Entretanto, a sua parte mais básica, os números naturais, acabou por certo tempo sendo ignorada. Até que, no final do século XIX, o matemático italiano, Giuseppe Peano (1858 - 1932) propôs uma lista de três axiomas que além de definir os naturais, sem depender dos inteiros, também permitiu definir as operações de adição e multiplicação. Tais axiomas são conhecidos como os axiomas de Peano [14].

Axioma 2.1 (Axiomas de Peano)

1. *Existe uma função injetiva s:* $\mathbb{N} \to \mathbb{N}$. *A imagem s(n) de cada número natural* $n \in \mathbb{N}$ *chama-se o sucessor de n.*

2. *Existe um único número natural* $1 \in \mathbb{N}$ *tal que* $1 \neq s(n)$ *para todo* $n \in \mathbb{N}$.

3. *Se um conjunto* $X \subset \mathbb{N}$ *é tal que* $1 \in X$ *e se s(X)*$\subset X$ *(isto é,* $n \in X \to s(n) \in X$*), então* $X = \mathbb{N}$.

Pelo segundo axioma de Peano, $\mathbb{N}$ é não vazio. Além disso $1 \notin Im(s)$ e $s(1) \in$ Im(s), concluímos que $1 \neq s(1)$ e portanto $\mathbb{N}$ possui pelo menos dois elementos. Da mesma forma podemos perceber que $s(s(1)) \neq s(1)$, pois s é injetiva e assim, se $s(1) \neq 1$, então $s(s(1)) \neq s(1)$. Portanto, $\mathbb{N}$ possui pelo menos três elementos. Tomando estes sucessores de forma repetida, vemos que cada elemento novo é diferente dos anteriores mencionados. Com isso, conseguimos varrer todos os elementos de $\mathbb{N}$. Em outras palavras, podemos obter qualquer número natural partindo do 1 e tomando seu sucessor e o sucessor do sucessor e assim por diante, até chegar ao número desejado. Sendo assim, os axiomas acima são suficientes para definir o conjunto dos naturais.

O terceiro axioma de Peano é conhecido como Princípio de Indução Finita. Ele é utilizado nas demonstrações das propriedades que dizem respeito aos números naturais. Veremos alguns exemplos no decorrer deste capítulo.

Agora que já conhecemos o conjunto dos naturais vamos definir duas operações neste conjunto, a adição, representada por $(+)$ e multiplicação, representada por $(\cdot)$.

Definição 2.1 *Sejam a e b são dois números naturais, definiremos:*

i) $a + 1 = s(a)$;

ii) $a + s(b) = s(a + b)$.

Isto é, fixado a, para $n = 1$ temos, $a + 1 = s(a)$. Se $n \neq 1$ então $n = s(b)$ para algum $b \in \mathbb{N}$. Logo, $a + n = a + s(b) = s(a + b)$.

Proposição 2.1 *A soma $a + b$ está definida para todo $a, b \in \mathbb{N}$.*

Demonstração: Considere $X = \{n \in \mathbb{N};\ a + n \text{ está definida}\}$, para todo $a \in \mathbb{N}$ tem-se $a + 1$ definido, portanto, $1 \in X$. Tomemos agora um $n \in X$, então $a + n$ está definido. Porém, pela definição 2.1, $a+s(n) = s(a+n)$ está definido, segue que $s(n) \in X$. Portanto, pelo terceiro axioma de Peano, $X = \mathbb{N}$. Assim a operação de adição está definida em $\mathbb{N}$. ■

Definição 2.2 *Se a e b são dois números naturais, definiremos.*

i) $a \cdot 1 = a$;

ii) $a \cdot (b + 1) = a \cdot b + a$.

Em outras palavras, fixado a, para $n = 1$ temos, $a \cdot 1 = a$. Se $n \neq 1$ então, $n = (b + 1)$ para algum $b \in \mathbb{N}$. Assim, $a \cdot n = a \cdot (b + 1) = a \cdot b + a$.

Proposição 2.2 *O produto $a.b$ está definida para todo $a, b \in \mathbb{N}$.*

Demonstração: Considere o conjunto $X = \{n \in \mathbb{N};\ a \cdot n \text{ está definida}\}$, para todo $a \in \mathbb{N}$ tem-se $a \cdot 1$ definido, portanto, $1 \in X$. Tomemos agora um $n \in X$, então $a \cdot n$ está definido. Porém, pela definição 2.2, $a \cdot s(n) = a \cdot n + a \cdot 1$ está definido. Assim, podemos afirmar que $s(n) \in X$. Logo pelo terceiro axioma de Peano, $X = \mathbb{N}$. Portanto, a operação de multiplicação fica definida em $\mathbb{N}$. ■

Definidas as operações básicas observamos que algumas propriedades são geradas. Estas propriedades têm por objetivo completar a apresentação do conjunto dos números naturais e são úteis no estudo das expressões algébricas. A demonstração da proposição imediatamente abaixo pode ser encontrada em [15].

Proposição 2.3 *Para todo $a, b, c \in \mathbb{N}$ são válidas as seguintes propriedades.*

i) $(a + b) + c = a + (b + c)$ *(Associatividade da Adição);*

ii) $a + b = b + a$ *(Comutatividade da Adição);*

iii) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(Associativa da Multiplicação);*

iv) $a \cdot b = b \cdot a$ *(Comutatividade da Multiplicação);*

v) $a \cdot 1 = a$ *(Elemento Neutro da Multiplicação);*

vi) $a \cdot (b + c) = a \cdot b + a \cdot c$ *(Distributividade).*

Teorema 2.1 (Princípio da Boa Ordenação) *Todo conjunto não-vazio* $A \subset \mathbb{N}$ *admite um elemento mínimo.*

Demonstração: Se $1 \in A$, então 1 é esse menor elemento de A, visto que, não há nenhum outro natural n com $n < 1$. Assim, suponha $1 \notin A$. Considere o conjunto $X = \{n \in \mathbb{N}; I_n \subset \mathbb{N} - A\}$, onde $I_n = \{1, 2, 3, ..., n\}$. Como $1 \notin A$, então $1 \in X$, e como A, por hipótese, é não-vazio, existe algum natural n que pertença a A e por consequência $n \notin X$. Com isso concluímos que $X \neq \mathbb{N}$. Assim, X não atende as hipóteses do terceiro axioma de Peano. Logo, deve existir algum n tal que $n \in X$ e $n + 1 \notin X$. Consequentemente $n + 1 \in A$. Portanto, $n + 1$ é o menor elemento de A. ∎

É importante salientar que o Princípio da Boa Ordenação e o Princípio da Indução Finita possuem uma relação bem próxima, no sentido de que, se assumimos o Princípio da Boa Ordenação como verdadeiro, então será possível demonstrar o Princípio da Indução Finita.

Teorema 2.2 (Princípio da Indução Finita) *Seja A um subconjunto dos números naturais. Se A possuir as duas propriedades:*

i) $1 \in A$*;*

ii) $n + 1 \in A$ *sempre que* $n \in A$*.*

Então $A = \mathbb{N}$*.*

Demonstração: Queremos mostrar que se A satisfaz (i) e (ii), então ele contém todos os naturais. Suponha que A não contenha todos os naturais. Logo, existe um conjunto B formado por todos os naturais que não estão contidos em A. Pelo Princípio da Boa Ordenação, B possui um menor elemento, digamos n_1, e este é maior que 1, pois por i), $1 \in A$. Então n_1 é sucessor de algum número natural, digamos n_0, além disso, $n_0 \in A$. Como A satisfaz (ii), $n_0 + 1 \in A$. Ou seja $n_1 \in A$. Gerando uma contradição. Assim, o conjunto B deve ser vazio e portanto A contém todos os naturais. ∎

O matemático e astrônomo italiano Francesco Maurolycus, em 1575, apresentou um resultado que exemplifica muito bem a utilização do Princípio da Indução Finita.

Exemplo 2.1 *Se* $n \in \mathbb{N}$*, então* $1 + 3 + ... + (2n - 1) = n^2$*.*

Demonstração: De fato sejam $P_n : 1 + 3 + ... + (2n - 1) = n^2$ e A o conjunto formando por todos os naturais n que possuem a propriedade P_n. Mostremos que $A = \mathbb{N}$.

i) Para $n = 1$ temos: $1 = 1^2$. Assim, $1 \in A$.

ii) Suponha que para algum $n \in \mathbb{N}$, com $n > 1$, P_n seja verdadeira. Mostremos que $n + 1 \in A$.

Por hipótese,

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

Adicionando $2n + 1$ em ambos os lados da igualdade acima, temos

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

Com isso, se $n \in A$ então $n + 1 \in A$. Portanto, pelo Princípio da Indução Finita, $A = \mathbb{N}$. ■

O exemplo acima foi a primeira aparição da utilização do Teorema 2.2. Porém, a prova por indução apenas se tornou uma ferramenta popular quando Blaise Pascal (1623 - 1662) a usou para as demonstrações das propriedades de seu "triângulo" (Triângulo de Pascal).

2.2 A CONSTRUÇÃO DOS INTEIROS

Nessa seção introduzimos a noção de número inteiro. Para construirmos os inteiros da forma desejada será necessário apresentar algumas *estruturas algébricas*. Ao final da construção será apresentado as principais propriedades das quais gozam os números inteiros. Iniciaremos pela definição de anel.

Definição 2.3 *Seja A um conjunto munido de duas operações $(+, \cdot)$. Dizemos que A é um anel se:*

$\boldsymbol{A}_1$) *Para todo $a, b, c \in A, (a + b) + c = a + (b + c)$;*

$\boldsymbol{A}_2$) *Para todo $a, b \in A, a + b = b + a$;*

$\boldsymbol{A}_3$) *Existe $0 \in A$, único, tal que $a + 0 = a$ para todo $a \in A$;*

$\boldsymbol{A}_4$) *Para todo $a \in A$ existe um único $\alpha \in A$ tal que $a + \alpha = 0$. O número α será representado por $-a$;*

$\boldsymbol{M}_1$) *Para todo $a, b, c \in A, (a \cdot b) \cdot c = a \cdot (b \cdot c)$;*

$\boldsymbol{M}_2$) *Para todo $a, b \in A, a \cdot b = b \cdot a$;*

$\boldsymbol{M}_3$) *Existe $1 \in A$, único, tal que $a \cdot 1 = a$ para todo $a \in A$;*

AM) *Para todo* $a, b, c \in A, a \cdot (b + c) = a \cdot b + a \cdot c$.

A seguir apresentamos alguns resultados sobre anéis, mas antes, se faz necessário apresentar o seguinte lema.

Lema 2.1 *Seja* a *um elemento de um anel. Se* $a + a = a$, *então* $a = 0$.

Demonstração: Como a é um elemento de uma anel, pelo item A_4 a possui inverso aditivo, assim $a + (-a) = 0$. Segue,

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

Por hipótese, $a + a = a$, logo,

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

Assim, $a = 0$. ■

As proposições a seguir são geradas a partir da definição de anel e, apesar de serem bastantes simples, garantem que certas "operações" possam ser realizadas nos inteiros. Apresentamos duas dessas propriedades. Mais detalhes sobre elas podem ser encontrados em [7].

Proposição 2.4 *Seja* A *um anel. Para todo* $a \in A$, *tem-se que* $a \cdot 0 = 0$.

Demonstração: Como $0 = 0 + 0$, então:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0,$$

assim, pelo Lema 2.1 concluímos que $a \cdot 0 = 0$. ■

A propriedade acima costuma ser citada da seguinte forma: Se um dos fatores de uma multiplicação é zero, então o seu produto é zero.

Proposição 2.5 *Seja* A *um anel. Para todo* $a, b \in A$

i) $(-1) \cdot a = -a$;

ii) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$;

iii) $(-a) \cdot (-b) = a \cdot b$.

Demonstração: Para i) basta mostrar que $(-1) \cdot a + a = 0$.
Por M_3 temos $a = 1 \cdot a$, assim,

$$(-1) \cdot a + a = (-1) \cdot a + 1 \cdot a = a \cdot (-1 + 1) = a \cdot 0 = 0.$$

Para ii) note que

$$(-a) \cdot b = ((-1) \cdot a) \cdot b = (-1) \cdot (a \cdot b) = -(a \cdot b).$$

Por outro lado temos $a \cdot (-b) = (-b) \cdot a$ Portanto,

$$a \cdot (-b) = -(b \cdot a) = -(a \cdot b).$$

Para iii) observemos que,

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b.$$

■

Chamamos um anel A de anel de integridade ou domínio de integridade se ele possuir a seguinte propriedade adicional:

$$\text{Para todo } a, b \in A, \text{ se } a \cdot b = 0, \text{ então } a = 0 \text{ ou } b = 0.$$

Além disso, em um domínio de integridade, os elementos possuem uma propriedade adicional, conhecida como lei do cancelamento. Isto é, podemos cancelar valores iguais em ambos os lados da igualdade.

Proposição 2.6 *Seja A um domínio de integridade. Para todo $a, b, c \in A$, se $a \neq 0$ e $ab = ac$, então $b = c$.*

Demonstração: Por hipótese temos:

$$ab = ac \Rightarrow ab + [(-a)c] = 0 \Rightarrow ab + [a(-c)] = 0 \Rightarrow a[b + (-c)] = 0.$$

Assim, $a = 0$ ou $b + (-c) = 0$. Como $a \neq 0$, então $b = c$. ■

Agora que já definimos o conjunto dos naturais e as estruturas algébricas necessárias, definiremos o conjunto dos números inteiros e algumas de suas propriedades. A definição abaixo foi extraída de [9], que pode ser consultado para maiores detalhes.

Definição 2.4 *O conjunto dos números inteiros, denotado por $\mathbb{Z}$, é um conjunto onde são definidas duas operações binárias;*

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (x, y) \mapsto x + y \qquad \cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (x, y) \mapsto x \cdot y,$$

as quais gozam dos seguintes propriedades:

Sejam $x, y, z \in \mathbb{Z}$,

i) ***Associatividade.*** $(x + y) + z = x + (y + z)$ *e* $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;

ii) ***Comutatividade.*** $x + y = y + x$ *e* $x \cdot y = y \cdot x$;

iii) ***Existência do elemento neutro;***
Existe $0 \in \mathbb{Z}$*, único, tal que* $x + 0 = x$ *para todo* $x \in \mathbb{Z}$.
Existe $1 \in \mathbb{Z}$*, único, tal que* $x \cdot 1 = x$ *para todo* $x \in \mathbb{Z}$.

iv) ***Existência do simétrico.*** *Para cada* $x \in \mathbb{Z}$*, existe* $-x \in \mathbb{Z}$*, único, tal que* $x + (-x) = 0$;

v) ***Distributividade.*** $x \cdot (y + z) = x \cdot y + x \cdot z$;

vi) $\mathbb{Z}$ ***não tem divisores de zero.*** *Se* $x \cdot y = 0$*, então* $x = 0$ *ou* $y = 0$.

Por possuir as propriedades acima dizemos que $\mathbb{Z}$ munido das operações de adição e multiplicação é um *domínio de integridade*. Concomitante a isso, em $\mathbb{Z}$ podemos definir uma relação de ordem, definida da seguinte maneira.

Definição 2.5 *Sejam* $x, y \in \mathbb{Z}$*. Dizemos que* x *é menor do que* y *e denotamos* $x < y$*, se existe um número natural* r *tal que* $y = x + r$.

Tal relação possui as seguintes propriedades.

i) **Tricotomia**: Uma, e somente uma, das relações a seguir é verdadeira. $x = y$, $x < y$ ou $y < x$

ii) **Transitividade**: Se $x < y$ e $y < z$,, então $x < z$.

iii) **Monotonicidade da adição**: Se $x < y$, então $x + z < y + z$.

iv) **Monotonicidade da multiplicação**: Se $x < y$, então $x \cdot z < y \cdot z$.

v) **Lei do corte**: Se $x + z < y + z$ ou $x \cdot z < y \cdot z$, então $x < y$.

A relação de ordem $x < y$ não é uma relação de ordem total, pois não possui a propriedade reflexiva. A fim de trabalharmos com uma relação de ordem total introduziremos a seguinte relação.

Definição 2.6 *Sejam* $x, y \in \mathbb{Z}$*. Dizemos que* x *é menor do que ou igual a* y *e denotamos* $x \leq y$*, se* $x < y$ *ou* $x = y$.

A relação $x \leq y$ goza das seguintes propriedades.

i) **Dicotomia**: $x \leq y$ ou $y \leq x$.

ii) **Reflexiva**: $x \leq x$.

iii) **Antissimétrica**: Se $x \leq y$ e $y \leq x$,, então $x = y$.

iv) **Transitividade**: Se $x \leq y$ e $y \leq z$,, então $x \leq z$.

v) **Monotonicidade da adição**: Se $x \leq y$, então $x + z \leq y + z$.

vi) **Monotonicidade da multiplicação**: Se $x \leq y$, então $x \cdot z \leq y \cdot z$.

Agora que definimos uma relação de ordem total em $\mathbb{Z}$, podemos expor um outro recurso importante dos inteiros: o módulo.

Definição 2.7 *Seja $a \in \mathbb{Z}$ definiremos módulo de a, representado por $|a|$ como:*

$$|a| = \begin{cases} -a, & se \quad a < 0, \\ a, & se \quad a \geq 0. \end{cases}$$

O módulo de um número atende as condições descritas logo a seguir.

Proposição 2.7 *Sejam $x, y \in \mathbb{Z}$, então:*

i) $|x| \geq 0$ *e* $|x| = 0$ *se, e somente se,* $x = 0$*;*

ii) $|xy| = |x| \cdot |y|$*;*

iii) $-|x| \leq x \leq |x|$*;*

iv) $|x| < y$ *se, e somente se,* $-y < x < y$*;*

v) Se $y \neq 0$*, então* $|x| \leq |x| \cdot |y|$.

Como consequência da proposição imediatamente acima, segue o resultado abaixo, conhecido como propriedade arquimediana

Proposição 2.8 (Propriedade Arquimediana) *Se $x, y \in \mathbb{Z}, y \neq 0$, então existe $n \in \mathbb{Z}$ tal que, $ny \geq x$.*

Demonstração: Pela Proposição 2.7, se $x, y \in \mathbb{Z}$ com $y > 0$ temos,

$$|xy| \geq |x| \text{ e } |y| \cdot |x| \geq |x|,$$

o que implica,

$$|y| \cdot |x| \geq x$$

pois $|x| \geq x$. Assim, se $y > 0$, basta tomar $n = |x|$ e se $y < 0$ tome $n = -|x|$. ∎

2.3 DIVISIBILIDADE NOS INTEIROS

Agora que já definimos o conjunto dos inteiros, utilizamos a operação de multiplicação para definir uma importante ferramenta no estudo dos números primos: a divisibilidade nos inteiros.

Definição 2.8 *Dados dois números inteiros a e b, dizemos que a divide b, representado por $a|b$, se existir $c \in \mathbb{Z}$, tal que $a \cdot c = b$.*

Quando a não divide b, representamos por $a \nmid b$. Se a divide b dizemos que a é um divisor de b ou, que b é um múltiplo de a ou ainda, que b é divisível por a.

Perceba que dentro dos inteiros nem sempre será possível obter uma divisão exata. Dessa forma, é necessário apresentar um importante recurso no que se refere a divisibilidade nos inteiros: a *Divisão Euclidiana*.

Teorema 2.3 (Divisão Euclidiana) *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$. Então existem dois inteiros únicos, q e r tais que*

$$b = aq + r$$

com $0 \leq r < |a|$.

Demonstração: Dividiremos a prova em dois casos.

Caso I. Suponha $a > 0$. Considere o conjunto

$$S = \{b - qa; q \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Pela Proposição 2.8, existe um $q \in \mathbb{Z}$ onde $q \cdot (-a) > -b$, assim, $b - qa > 0$ e portanto S é não vazio. Além disso, S é limitado inferiormente pelo 0. Logo, pelo princípio da boa ordenação S possui um menor elemento r. Logo $r = b - qa$ para algum q pertencente a $\mathbb{Z}$. Se $a|b$, então $r = 0$ e o resultado segue. Se $a \nmid b$ então $r \neq 0$, logo basta mostrar que $r < a$. Suponha por absurdo que $r > a$. Nesse caso, existe $0 < c < r$ tal que $r = c + a$. Logo $c + a = r = b - qa$. Segue então que $c = b - a(q + 1)$. Portanto $c \in S$ e é menor que r, gerando uma contradição. Assim, $r < a$ e a existência de q e r está provada.

Caso II. Suponha $a < 0$. Aplicamos o caso anterior com $b, |a|$. Assim, existem únicos $q, r \in \mathbb{Z}$ tais que $b = q|a| + r$. Se escrevermos $q_1 = -q$, então $b = q_1 a + r$, com $0 < r \leq |a|$.

Quanto à unicidade, suponha que existam dois elementos distintos, $r = b - qa$ e $r' = b - q'a$, onde $r < r' < a$. Temos que, $a|(r - r')$ o que implica $r - r' \geq a$. Assim, $r \geq a + r' > a$, gerando uma contradição. Logo, $r = r'$ e consequentemente, $q = q'$. ∎

Com isso temos uma noção básica de como funciona a divisão dos números inteiros. Além disso o fato de sempre ser possível realizar uma divisão, com ou sem resto,

gera inúmeras consequências. Apresentamos agora dois resultados que serão importantes ao longo do trabalho.

Proposição 2.9 *Sejam $a, b, c \in \mathbb{Z}$, tais que $a|(b \pm c)$. Então*

$$a|b \Longleftrightarrow a|c.$$

Demonstração: Suponha que $a|(b+c)$. Logo, existe $x \in \mathbb{Z}$ tal que $b + c = ax$. Se $a|b$, então existe $y \in \mathbb{Z}$ tal que $b = ay$. Dessas duas igualdades temos,

$$ay + c = ax.$$

Segue-se que, $c = a \cdot (x - y)$. Assim, $a|c$. A prova da implicação contrária é análoga. Simultaneamente, se $a|(b - c)$ e $a|b$, pelo caso anterior, temos que $a| - c$ e com isso $a|c$.

■

Proposição 2.10 *Sejam $a, b, c \in \mathbb{Z}$. Se $a|b$ e $a|c$, então para todo $x, y \in \mathbb{Z}$,*

$$a|(xb + yc).$$

Demonstração: Se $a|b$ e $a|c$, então existe m$f, g \in \mathbb{Z}$ tais que $b = fa$ e $cg = ga$. Portanto,

$$xb + yc = xfa + yga = a \cdot (xf + yg).$$

Ou seja, $a|(xb + yc)$. ■

2.3.1 CRITÉRIOS DE DIVISIBILIDADE

Existem casos onde os cálculos necessários para saber se um certo número divide outro podem ser reduzidos. Para isso, se utiliza dos critérios de divisibilidade.

Esses critérios são regras simples que permitem saber se o número inteiro a é ou não divisor de outro inteiro b, baseando-se em propriedades da sua representação decimal. Apresentamos os critérios para os primeiros cinco primos e assumimos todos os critérios como verdadeiros. Para maiores detalhes veja [[10], capítulo 9].

- **Critério para o 2:** Para determinar se um número é múltiplo de 2 basta verificar se o mesmo é par. Ou seja, todo número par é múltiplo de 2.
- **Critério para o 3:** Para saber se um número é múltiplo de 3 basta verificar se a soma dos seus algarismos resulta em um múltiplo de 3.
- **Critério para o 5:** Sempre que um número terminar em 5 ou 0 ele será um múltiplo de 5.

- **Critério para o 7:** Multiplique por 2 o último algarismo do número. Subtraia este valor do número inicial sem o último algarismo. Se caso o resultado for um múltiplo de 7, então o número inicial também o é.
- **Critério para o 11:** Um número é divisível por 11 quando a diferença entre as somas dos valores absolutos dos algarismos de ordem ímpar e a dos de ordem par é divisível por 11.

Tomemos como exemplo os números 1595 e 714. Observamos que 714 é par logo, 2|714. Além disso, perceba que

$$7 + 1 + 4 = 12$$

que é um múltiplo de 3 e assim, 3|714. Perceba também que o último algarismo é o 4, logo

$$2 \cdot 4 = 8; \;\; 71 - 8 = 63,$$

que é um múltiplo de 7, portanto 7|714. No que se refere ao número 1595, perceba que o mesmo termina em 5, portanto 5|1595. Além disso a soma das ordens ímpares

$$S_i = 5 + 5 = 10,$$

e soma das ordens pares

$$S_p = 9 + 1 = 10,$$

E pelo critério de divisibilidade,

$$S_i - S_p = 10 - 10 = 0.$$

Concluímos que, 11|1595 pois, 0 é divisível por 11.

2.4 MÍNIMO MÚLTIPLO COMUM E MÁXIMO DIVISOR COMUM

Os cálculos de MMC e MDC se referem aos múltiplos e aos divisores de um número. As noções de MMC e MDC são apresentadas durante o ensino fundamental e são ampliadas à medida que o aluno vai seguindo seus estudos.

Nesse trabalho, apresentamos as definições e proposições ligadas ao estudo do MMC e do MDC da maneira que é apresentada nos cursos de graduação.

Definição 2.9 *Dizemos que m é o mínimo múltiplo comum entre dois números u e $v \in \mathbb{Z}$, e escrevemos $m = mmc(u, v)$, se:*

i) $m > 0$;

ii) m é múltiplo comum de u e v;

iii) m é o menor dos múltiplos comuns, no sentido de que se m' é um múltiplo comum de u e v e $m' > 0$, então $m|m'$.

Definição 2.10 *Dados dois inteiros u e $v \in \mathbb{Z}$, dizemos que um natural d é o máximo divisor comum entre dois números u e v, e escrevemos $d = mdc(u, v)$, se:*

i) d é um divisor comum de u e v, isto é, d é divisor tanto de u quanto de v;

ii) d é o maior dos divisores comuns , no sentido de que se d' é um divisor comum de u e v, então $d'|d$.

Tendo em vista as definições acima apresentadas, passamos a apresentar propriedades referentes ao uso do mmc e mdc no conjuntos dos números inteiros. O próximo teorema nos dá uma segunda e importante caracterização do máximo divisor comum.

Teorema 2.4 *Sejam $a, b \in \mathbb{Z}$ com $a, b > 0$. Então:*

$$mdc(a, b) = min\ \{x \in \mathbb{Z} | x > 0\ e\ x = ma + nb;\ com\ m, n \in \mathbb{Z}\}.$$

Demonstração: Inicialmente perceba que o conjunto

$$A = \{x \in \mathbb{Z} | x > 0 \text{ e } x = ma + nb; \text{ com } m, n \in \mathbb{Z}\}$$

é não-vazio, pois, $a = a \cdot 1 + b \cdot 0$.
Além disso, A é limitado inferiormente pelo zero, portanto pelo Princípio da Boa Ordenação possui um menor elemento.
Seja $d = am + bn$ o menor inteiro positivo que é combinação linear de a e b. Mostremos que, $d|a$ e $d|b$. Pela divisão euclidiana podemos escrever $a = dq + r$ com $0 \leq r < d$. Assim,

$$r = a - dq = a - q \cdot (ma + nb) = (1 - qm) \cdot a - (qn) \cdot b,$$

e portanto, r é uma combinação linear de a e b. Como $0 \leq r < d$ e d é o menor inteiro positivo que é combinação linear, com coeficientes inteiros de a e b, podemos afirmar que, $r = 0$ e portanto, $d|a$. O caso é análogo para $d|b$.

Para mostrar que d é o mdc devemos mostrar que para qualquer outro $c \in \mathbb{Z}$ divisor comum, então $d \geq c$. Como

$$d = ma + nb,$$

se $c|a$ e $c|b$, tem-se pela Proposição 2.9 que, $c|(ma + nb)$ ou seja, $c|d$ e portanto,

$$d \geq c.$$

■

A seguir, apresentamos mais resultados sobre máximo divisor comum.

Teorema 2.5 *Para todo $a, b \in \mathbb{Z}$, com $a, b > 0$ e $n \in \mathbb{N}$, tem-se que*

$$mdc(na, nb) = n \cdot mdc(a, b).$$

Demonstração: Pelo Teorema 2.4,

$$mdc(na, nb) = min\{d \in \mathbb{Z} | d > 0; d = xna + ynb; \text{ com } x, y \in \mathbb{Z}\}.$$

Assim,

$$mdc(na, nb) = xna + ynb = n \cdot (xa + yb) = n \cdot mdc(a, b).$$

E segue o resultado. ■

Corolário 2.1 *Dados $a, b \in \mathbb{Z}$ não nulos e d =$mdc(a, b)$, então*

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

Demonstração: Pelo Teorema 2.5, temos:

$$d \cdot mdc\left(\frac{a}{d}, \frac{b}{d}\right) = mdc\left(d \cdot \frac{a}{d}, d \cdot \frac{b}{d}\right) = mdc(a, b) = d.$$

Como $d \neq 0$ tem-se que $mdc(a/d, b/d) = 1$. ■

O próximo teorema assegura uma importante relação entre mmc e mdc. Conhecendo o *mdc(a,b)* é possível determinar o *mmc(a,b)*.

Teorema 2.6 *Sejam $a, b \in \mathbb{Z}$. Então*

$$mmc(a, b) \cdot mdc(a, b) = |ab|.$$

Demonstração: Se a e b são nulos não há o que fazer, além disso, note que a afirmação é válida para a e b se, e somente se, também é válida para $\pm a$ e $\pm b$. Logo, sem perda de generalidade suponhamos a e b positivos.

Façamos *m=mmc(a,b)* e *d=mdc(a,b)*, e seja $m' = ab/d$. Note que, m' é múltiplo de a e b pois,

$$m' = a \cdot \frac{b}{d}$$

e,

$$m' = b \cdot \frac{a}{d}.$$

Assim, falta apenas mostrar que m' é o menor dos múltiplos. Para isso, tomemos c, um outro múltiplo comum de a e b. Assim, existem $x, y \in \mathbb{Z}$ tal que $c = xa$ e $c = yb$.

Por outro lado, como $d = mdc(a, b)$ logo existem $k, q \in \mathbb{Z}$ tal que $d = ak + bq$. Assim:

$$\begin{aligned} dc &= ack + bcq \\ &= aybk + bxaq \\ &= ab \cdot (yk + xq). \end{aligned}$$

Concluindo que,

$$c = (yk + xq) \cdot \frac{ab}{d},$$

ou seja, c é múltiplo de m' e portanto, $m' \leq c$. O que garante que $m' = mmc(a, b) = m$. ■

Proposição 2.11 *Sejam $p, n \in \mathbb{Z}$. O $mdc(p, n) = 1$ se, e somente se, existem $r, s \in \mathbb{Z}$ tais que $rp + sn = 1$.*

Demonstração: Suponha $mdc(p, n) = 1$. Assim, pelo Teorema 2.4 existem $r, s \in \mathbb{Z}$ tais que, $rp + sn = mdc(p, n) = 1$.

Por outro lado, suponha que existam $r, s \in \mathbb{Z}$ tais que, $rp + sn = 1$. Seja $d = mdc(p, n)$, então $d|(rp + sn)$, logo $d|1$ e portanto, $d = 1$. ■

Teorema 2.7 (Lema de Gauss) *Sejam $a, b, p \in \mathbb{Z}$. Se $p|a.b$ e $mdc(a, p) = 1$, então $p|b$.*

Demonstração: Se $p|a.b$, então existe $c \in \mathbb{Z}$ tal que $a.b = p.c$. Por hipótese, $mdc(a, p) = 1$, assim, pela Proposição 2.11 existem $r, s \in \mathbb{Z}$ tais que:

$$rp + sa = 1.$$

Multiplicando ambos os lados por b,

$$rpb + sab = b,$$

substituindo ab por pc,

$$rpb + spc = b \Rightarrow p(rb + sc) = b,$$

portanto, $p|b$. ■

2.5 CONGRUÊNCIA

Afim de facilitar futuras demonstrações apresentamos aqui uma noção rápida sobre congruência e algumas consequências que nos será de grande importância.

Definição 2.11 *Sejam a e b inteiros, dizemos que a é congruente a b módulo $m(m > 0)$ se $m|(a - b)$. Denotaremos por $a \equiv b \ mod \ m$.*

Decorre, diretamente da definição as seguintes afirmações:

Proposição 2.12 *Sejam a e b dois números inteiros. Então:*

i) $a \equiv a \ mod \ m$;

ii) *Se* $a \equiv b \ mod \ m$, *então* $b \equiv a \ mod \ m$;

iii) *Se* $a \equiv b \ mod \ m$ *e* $b \equiv c \ mod \ m$, *então* $a \equiv c \ mod \ m$.

O próximo teorema assegura que a congruência é compatível com as operações de adição e multiplicação nos inteiros.

Proposição 2.13 *Sejam a, b, c, d e m números inteiros, com $m > 1$:*

i) *Se* $a \equiv b \ mod \ m$ *e* $c \equiv d \ mod \ m$, *então* $a + c \equiv b + d \ mod \ m$;

ii) *Se* $a \equiv b \ mod \ m$ *e* $c \equiv d \ mod \ m$, *então* $ac \equiv bd \ mod \ m$.

Demonstração: Para i), perceba que $m|(b - a) + (c - d)$ e assim $m|(b + d) - (a + c)$. Para ii) note que, $bd - ac = d(b - a) + a(d - c)$ e como por hipótese $m|b - a$ e $m|d - c$ podemos concluir que, $m|bd - ac$. ■

Concomitante a isso, é importante ressaltar que o cancelamento aditivo e multiplicativo também são válidos na congruência, que será apresentado a seguir.

Proposição 2.14 *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$ e $d = mdc(c, m)$. Temos,*

$$ac \equiv bc \ mod \ m \Leftrightarrow a \equiv b \ mod \ \tfrac{m}{d}.$$

Demonstração: Como o $mdc(^m/_d, ^c/_d) = 1$, então,

$$ac \equiv bc \ mod \ m \Leftrightarrow m|(b - a)c.$$

E assim,

$$\frac{m}{d}|(b - a)\frac{c}{d} \Leftrightarrow \frac{m}{d}|b - a.$$

E portanto,

$$a \equiv b \ mod \ \tfrac{m}{d}.$$

■

Corolário 2.2 *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$ e $mdc(c, m) = 1$. Temos*

$$ac \equiv bc \ mod \ m \Leftrightarrow a \equiv b \ mod \ m.$$

Proposição 2.15 *Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$. Temos,*

$$a + c \equiv b + c \ mod \ m \Longrightarrow a \equiv b \ mod \ m.$$

Demonstração: Se $a \equiv b \ mod \ m$, então $a + c \equiv b + c \ mod \ m$, pois $c \equiv c \ mod \ m$. Por outro lado se

$$a + c \equiv b + c \ mod \ m,$$

então

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

que por sua vez implica, $m|b - a$, ou seja,

$$a \equiv b \ mod \ m.$$

■

3 OS NÚMEROS PRIMOS

Dentre todas as civilizações que contribuem ou contribuíram para o engrandecimento da matemática, nenhuma apresentou uma importância mais significativa do que a civilização grega. Foi na Grécia que o conhecimento matemático passou a ser essencialmente abstrato, as demonstrações se tornaram a ferramenta que garantia a veracidade de todas as afirmações. Porém, a matemática, como a conhecemos, teve seu pontapé inicial dado por Ptolomeu Sóter (323-283 a.C), general macedônio de Alexandre, o Grande; pois, sob suas ordens foi construído o "Templo das Musas", um lugar de inspiração artística e literária.

Dentro desse museu se encontrava a maior joia científica da época, a biblioteca de Alexandria, e foi nesse ambiente que o grande matemático da época, Euclides de Alexandria, apresentou seu magnífico trabalho de sistematização de conhecimentos, Os Elementos.

Pouco se sabe sobre a vida de Euclides, pois existem poucos relatos sobre ele, tendo sido escritos séculos após sua morte, por Proclo (412 - 485) e Pappus de Alexandria (290 - 350). Acredita-se que nasceu provavelmente no século III a.C, e a causa da sua morte é completamente desconhecida. Além disso, nenhuma imagem ou descrição da aparência física de Euclides foram feitas durante sua vida. Assim, as representações de Euclides em obras de arte é o produto da imaginação artística.

Euclides foi professor da escola real de Alexandria e é conhecido como o "Pai da Geometria". Além de sua principal obra, Os Elementos, ele também escreveu sobre perspectivas, seções cônicas, geometria esférica e teoria dos números.

Porém, não foi apenas Euclides que se utilizou da grande biblioteca de Alexandria para marcar seu nome na história da matemática. Outro grego também a utilizou como palco para o seu grande feito de, em 245 a.C, calcular a circunferência da Terra, com uma precisão assombrosa para a época. Tal grego foi Eratóstenes de Cirene, que era matemático, astrônomo, filósofo, geógrafo e bibliotecário dessa tão grandiosa biblioteca.

Eratóstenes nasceu em Cirene no ano de 276 a.C., tendo durante a sua juventude estudado em Atenas. Posteriormente, o faraó Ptolomeu III (284 - 222 a.C) convidou-o a ser bibliotecário na biblioteca de Alexandria, cargo que Eratóstenes assumiria no ano de 245 a.C.

Além de conseguir determinar a circunferência da Terra, Eratóstenes também foi

o criador do conhecido *Crivo de Eratóstenes*: o primeiro teste de primalidade conhecido, que é ainda uma importante ferramenta na teoria dos números. O crivo é citado na obra Introdução à Aritmética de Nicomedes (280 - 210 a.C).

Apesar de seu sucesso como estudioso e escritor, a parte final da vida de Eratóstenes foi trágica, pois ficou cego e, aos 80 anos de idade, induziu sua própria morte parando de comer.

A contribuição desses dois grandes nomes para o estudo sobre números primos é o que apresentamos nesse capítulo.

Definição 3.1 *Um número natural, maior que 1, que possua apenas dois divisores positivos, 1 e ele mesmo, será chamado de número primo.*

Se n não é primo, então será chamado de composto. Observamos abaixo os números primos que estão entre 1 e 1000.

Tabela 3.1: Primos entre 1 e 1000

2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
59	61	67	71	73	79	83	89	97	101	103	107	109	113	127	131
137	139	149	151	157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281	283	293	307	311
313	317	331	337	347	349	353	359	367	373	379	383	389	397	401	409
419	421	431	433	439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593	599	601	607	613
617	619	631	641	643	647	653	659	661	673	677	683	691	701	709	719
727	733	739	743	751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911	919	929	937	941
947	953	967	971	977	983	991	997								

Não é possível destacar uma sequência lógica na tabela dos números primos. Alguns matemáticos já dedicaram uma parte da sua vida na tentativa de encontrar um padrão nos números primos, dentre eles, Euclides, Fibonacci (1170 - 1250), Gauss (1777 - 1855), Euler (1707 - 1783), Goldbach (1690 - 1764), Riemann (1826 - 1866), Fourier (1772 - 1837), Jacobi (1804 - 1851), Legendre (1752 - 1833), Cauchy (1789 - 1857), Hilbert (1862 - 1943), Hardy (1877 - 1947), Littlewood (1855 - 1977), Ramanujan (1887 - 1920) entre outros, e apesar de todos esses esforços ainda procura-se entender a tabela dos números primos.

Alguns primos da lista estão a uma distância de dois números um do outro, ou seja, existem inteiros p e $p + 2$ primos. Tais primos são chamados de primos gêmeos. Podemos exemplificar com (3 e 5), (5 e 7), (347 e 349) entre outros.

Ainda não se sabe se existem infinitos números primos gêmeos. Porém, um resultado importante devido a Viggo Brun (1885 - 1978), matemático norueguês, mostra

que mesmo que existam infinitos primos gêmeos. Eles se tornam muito escassos quando olhamos para números muito grandes, o que torna a conjectura mais difícil de ser provada.

3.1 TEOREMA FUNDAMENTAL DA ARITIMÉTICA

A química possui a *tabela periódica dos elementos*, proposta por Dimitri Mendeleev (1834 -1907), e todas as moléculas conhecidas do planeta são decompostas em elementos dessa tabela. Aqui, nesse trabalho, esses elementos são os números primos.

Antes de apresentarmos o Teorema Fundamental da Aritmética faz-se necessário conhecer a seguinte proposição.

Proposição 3.1 *Todo número primo que divide um produto divide pelo menos um dos fatores.*

Demonstração: Suponha que $p|ab$ e que $p \nmid a$ vamos provar que $p|b$. Se $p \nmid a$ implica que $mdc(p, a) = 1$ e pelo Teorema 2.7, $p|b$ ■

Teorema 3.1 (Teorema Fundamental da Aritmética) *Todo número natural maior que 1 ou é primo ou pode ser representado de maneira única (exceto pela ordem) como produto de fatores primos.*

Demonstração: Provaremos por indução para $n \geq 2$.

Para $n = 2$ o teorema é verdadeiro pois 2 é primo. Suponhamos por hipótese que para todo número natural k com $2 \leq k < n$ o teorema é verdadeiro. Mostremos que vale para n.

Se n é primo não há nada o que fazer. Portanto, suponhamos n composto. Assim existem inteiros n_1 e n_2 com $1 \leq n_1 < n$ e $1 \leq n_2 < n$ tal que $n = n_1 \cdot n_2$. Por hipótese existem primos tais que,

$$n_1 = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_r,$$

e,

$$n_2 = q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot q_s.$$

Portanto,

$$n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_r \cdot q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot q_s.$$

Agora mostramos que tal decomposição é única. Suponhamos

$$n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_r = q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot q_s,$$

onde os p_i e q_j são todos primos, como

$$p_1 | q_1 \cdot q_2 \cdot q_3 \cdot ... \cdot q_s,$$

$p_1 = q_j$ para algum j, onde $1 \leq j \leq s$. Sem perda de generalidade podemos supor que $p_1 = q_1$. Portanto

$$p_2 \cdot ... \cdot p_r = q_2 \cdot ... \cdot q_s$$

Como $p_2 \cdot ... \cdot p_r < n$, a hipótese acarreta $r = s$ e p_i e q_j são iguais aos pares. ■

3.2 INFINITUDE DOS PRIMOS

Outro tópico bastante discutido sobre números primos durante o desenvolvimento da teoria dos números, "os números primos são ou não infinitos?". Existem várias demonstrações que comprovam a infinitude dos números primos como a demonstração de Euler e a de Furstenberg. Porém, usaremos a demonstração mais conhecida, que foi apresentada no livro IX de Os Elementos.

Teorema 3.2 *Existem infinitos números primos.*

Demonstração: Suponha que existam finitos números primos $p_1, p_2, ..., p_k$. Agora considere o número natural n como sendo,

$$n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k + 1.$$

O número n não pode ser primo pois estamos supondo que os únicos primos existentes são $p_1, p_2..p_k$ e $n \neq p_i$, para todo $1 \leq i \leq k$.

Pelo Teorema Fundamental da Aritmética n possui um fator primo p que deve ser um dos $p_1, p_2, ...p_k$ e, consequentemente, divide o produto $p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k$. Como $p|n$, pela Proposição 2.9, $p|1$, gerando uma contradição. ■

3.3 O CRIVO DE ERATÓSTENES

O Crivo de Eratóstenes é um método simples para encontrar números primos até um certo valor limite.

Lema 3.1 *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: Suponha que n não seja divisível por nenhum número primo p onde $p^2 \leq n$ e que não seja primo. Seja q o menor número primo que divide n; então

$$n = qn_1,$$

com $q \leq n_1$. Segue daí que

$$q^2 \leq qn_1 = n.$$

Logo, n é divisível por um número primo q tal que $q^2 \leq n$, gerando uma contradição.

■

O exemplo a seguir ilustra a utilização desse lema.

Exemplo 3.1 *Mostremos que 131 é primo.*

Demonstração: Calculando a raiz quadrada de 131 temos, $\sqrt{131} \approx 11$. Assim, pelo Lema 3.1 basta verificar os números primos entre 2 e 11 que são: 2,3,5,7 e 11. Como 131 é ímpar eliminamos divisão por 2. Com isso nossa lista de fatores a serem testados se resume aos números 3,5,7 e 11. Utilizando os critérios de divisibilidade apresentados no capítulo anterior, verificamos que nenhum dos números 3,5,7 e 11 divide 131 de forma inteira. Logo concluímos que 131 é primo. ■

A palavra crivo refere-se a um utensílio utilizado para separar componentes de uma mistura. E é justamente esse o objetivo do crivo de Eratóstenes: separar os componentes (números primos) da mistura (números naturais).

Utilizamos o crivo de Eratóstenes para encontrar os primos entre 1 e 1000. Utilizamos o Lema 3.1 e os critérios de divisibilidade apresentados no capítulo anterior. Descreveremos o processo a seguir.

Tabela 3.2: Naturais entre 1 e 100

1	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

Inicialmente, determina-se o maior número a ser checado. Ele corresponde à raiz quadrada do valor limite, maior inteiro menor que a raiz. No caso, a raiz de 100 que é 10.

Iniciamos com o primeiro número primo, no caso o 2, e retiramos todos os seus múltiplos. Como todo número par é um múltiplo de 2, nossa tabela agora possui apenas os números impares, com exceção do 2.

Agora passamos para o próximo número primo, o número 3, e retiramos todos os seus múltiplos. Perceba que aqui pode ser utilizado os critérios de divisibilidade, o que facilitará os cálculos. Continue a fazer isso até o primo mais próximo do nosso valor limite, ou seja até o 7.

Ao final retiramos o número 1, pois ele não é primo, e com isso terá sobrado apenas os números primos.

Tabela 3.3: Resultado Final

~~1~~	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~~

Podemos utilizar o crivo para construir a tabela 3.1. Porém, apesar de simples o crivo de Eratóstenes se torna bastante inviável quando desejamos encontrar números primos em intervalos muito grandes.

3.4 OUTROS RESULTADOS

Uma vez definidos os números primos e apresentados importantes teoremas, exibimos outros resultados relevantes ao estudo dos números primos.

Definição 3.2 *Sendo $n \geq k$, com n e k pertencentes ao conjunto do números naturais, o número binomial $\binom{n}{k}$ é dado por:*

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} = \frac{n!}{k! \cdot (n-k)!}.$$

Lema 3.2 *Seja p um número primo. Os números $\binom{p}{k}$, onde $0 < k < p$, são todos divisíveis por p.*

Demonstração: O resultado vale para $k = 1$. Então podemos supor $1 < k < p$. Nesse caso, $k!|p(p-1)\cdots(p-k+1)$. Como $mdc(k!, p) = 1$, decorre que $k!|(p-1)\cdots(p-k+1)$, e o resultado se segue, pois

$$\binom{p}{k} = p\frac{(p-1)\cdots(p-k+1)}{k!}.$$

■

Encerramos esse capítulo com um dos problemas mais interessantes da teoria dos números e que se refere aos números primos, a conhecida conjectura de Goldbach.

Christian Goldbach (1690 - 1764) nasceu na cidade de Königsberg, na Prússia (atualmente, Kalingrado, na Rússia) onde viveu até 1764. Goldbach fez parte da Academia Imperial de São Petersburgo, onde atuou como professor não apenas de matemática,

mas também de história. Assumiu ainda o cargo de Ministro do Exterior na Rússia, em 1742.

Na matemática, trabalhou com teoria dos números, teoria de curvas, séries infinitas e integração de equações diferenciais. Mas, sua contribuição mais famosa está relacionada com os números primos. Esta conjectura foi proposta em uma carta que escreveu a outro famoso matemático, Leonhard Euler. A famosa Conjectura de Goldbach diz que,

"Todo número par maior que 3 é igual à soma de dois números primos."

Exemplo 3.2

$$\begin{array}{rclrcl} 4 & = & 2+2 & 20 & = & 7+23 \\ 8 & = & 3+5 & 130 & = & 3+127 \\ 36 & = & 5+31 & 198 & = & 97+101 \end{array}$$

É fato que ainda não há demonstração, porém, já existem resultados significativos. Em 1930 o matemático russo Lev Genrikhovich (1905 - 1938) conseguiu provar que todo número natural pode ser expresso como sendo a soma de até 20 números primos. Em 1937 o matemático Ivan Matveyevich Vinogradov (1891 - 1983) conseguiu provar que todo número ímpar suficientemente grande pode ser representado como sendo soma de até 3 números primos. Em 1973 o matemático chinês Chen Jing Run (1933 - 1996) provou que todo número par suficientemente grande é soma de um número primo com outro número que é obtido com produto de no máximo dois primos [25].

4 A ARITMÉTICA DE FERMAT

Nascido no dia 17 de agosto de 1601, em Beaumont-de-Lomages, França, e tendo morrido no dia 12 de janeiro de 1665, em Castres, França, Pierre de Fermat foi um político e advogado francês, residente da cidade de Toulouse. Considerado o "Príncipe dos Amadores", ele nunca teve formalmente a matemática como a principal atividade de sua vida. Jurista e magistrado por profissão, dedicava à Matemática apenas as suas horas de lazer e, mesmo assim, foi considerado por Blaise Pascal o maior matemático de seu tempo.

Contudo, este grande gênio matemático perpassou várias gerações, fazendo com que várias mentes se debruçassem com respeito sob o seu legado, composto por contribuições nos mais diversos ramos das matemática, estre eles: o Cálculo Geométrico e Infinitesimal, a Teoria dos Números e Teoria da Probabilidade.

Fermat produziu um tratado intitulado *Método para Encontrar Máximos e Mínimos*, estudou curvas do tipo $y = x^n$, onde $n \in \mathbb{Z}$, o que hoje é conhecida como "parábolas" ou "hipérboles de Fermat". Apesar de Fermat e Descartes (1596 - 1650) terem inventado a geometria analítica, independentemente um do outro, Fermat foi muito mais longe ao introduzir os eixos perpendiculares e ao formular equações para retas, circunferências, parábolas e hipérboles. Foi a partir destes conhecimentos que foi capaz de resolver problemas geométricos sobre lugares geométricos no plano e no espaço.

Porém, o principal campo de estudo de Fermat era o da Teoria dos Números, no qual se consagrou. Fermat deu considerável impulso à aritmética superior moderna e exerceu, assim, grande influência sobre o desenvolvimento da álgebra. Deve-se a ele alguns teoremas originais, notáveis pela concepção. Sem embargo, o mais famoso dos teoremas de Fermat é o que passou a história da matemática com a designação de "Último Teorema de Fermat" que diz:

$$\text{Sejam } a, b, c, n \in \mathbb{N}. \text{ Então } a^n + b^n \neq c^n, \text{ para todo } n > 2.$$

Em 1934, Louis Trenchard More (1870 - 1944) descobriu uma nota de Isaac Newton (1643 - 1727) dizendo que o seu cálculo, antes considerado como invenção, fora baseado no método de Fermat para estabelecer tangentes. Foi a primeira pessoa a enunciar o Pequeno Teorema de Fermat, embora a primeira pessoa a publicar a prova do teorema tenha sido Euler, em 1736, no artigo "Theorematum quorundam ad numeros primos spectantium

demonstratio".

Pierre de Fermat casou-se com a prima de sua mãe, Louise de Long, em 1 de junho de 1631. O casal teve cinco filhos: dois filhos e três filhas. Seu filho mais velho, Clément-Samuel, também se tornou um advogado e herdou seu escritório após a sua morte; mais tarde também publicou documentos matemáticos do pai.

O resultado de Fermat sobre números primos veio a se chamar de pequeno teorema para que houvesse uma distinção do tão aclamado "Último Teorema de Fermat". Demonstrado por Euler, esse é dos principais recursos para determinar se um número não é primo.

Além de demonstrar o teorema, Euler também foi o autor da sua mais conhecida generalização. Além disso foi o responsável por verificar que a "fórmula" para números primos descoberta por Fermat estava errada. Assim, é impossível falar sobre Fermat sem mencionar das contribuições de Euler.

Leonhard Euler, nascido em 15 de abril de 1707, na Basileia, Suíça, considerado por muitos a maior mente do século XVIII e um dos maiores matemáticos da história. Ele estudou na Universidade de Basel, onde seu mentor, Jean Bernoulli (1667 - 1748), percebendo desde cedo seu talento e investiu na sua formação.

Euler é considerado o matemático mais prolífico da história. Publicou em média 800 livros e artigos. Até mesmo após a cegueira seu ritmo de produção não diminuiu. Suas contribuições percorrem os campos da matemática e da física.

Além disso, Euler foi o responsável pela introdução de diversos símbolos matemáticos. A letra "e" para o número cujo o logaritmo neperiano, $\ln e$, vale 1, o símbolo π para denotar a razão entre a circunferência e o diâmetro do círculo, o símbolo i para expressar $\sqrt{-1}$ além das notações $\sin(x), \cos(x), \tan(x), \sec(x), \cot(x)$. Na geometria convencionou usar letras minúsculas para os lados do triângulo e as letras maiúsculas para os ângulos.

Ele foi enterrado no cemitério luterano de Smolensk na Ilha de Vassiliev. Em 1785, a Academia de Ciências da Rússia pôs um busto de mármore de Leonhard Euler em um pedestal próxima à reitoria e, em 1837, esculpiram uma lápide para ele. Para comemorar os duzentos e cinquenta anos do nascimento dele, a lápide foi transferida em 1956, junto com seus restos mortais, para a necrópole do século XVIII, no monastério Alexander Nevsky, o cemitério Tikhvin.

No que se refere ao Pequeno Teorema de Fermat, não podemos esquecer de citar que o teorema, como teste de primalidade, não é perfeito. Em 1910, o matemático Robert Carmichael (1879 - 1967) encontrou números compostos que passavam pelo teste do teorema, os pseudoprimos absolutos, ou números de Carmichael, cuja definição será apresentado logo a frente.

A esperança era que tais números fossem finitos. Contudo, em 1956, Paul Erdõs (1913 - 1996) esquematizou uma técnica, que determinava pseudoprimos muito grandes, mas apenas em 1992, Carl Pomerance (Joplin, Missouri, 1944) e dois colegas da Univer-

sidade da Geórgia. Finalmente, após muito tempo, transformaram a técnica de Erdôs numa sólida demonstração.

4.1 O PEQUENO TEOREMA DE FERMAT

Nesse capítulo apresentamos e demonstramos os resultados mais relevantes da pesquisa, O Pequeno Teorema de Fermat e o Teorema de Euler. Além disso, fazemos um breve estudo sobre os pseudoprimos.

Teorema 4.1 (Pequeno Teorema de Fermat) *Sejam p e $a \in \mathbb{Z}$. Se p é um número primo, então $a^p \equiv a \ mod\ p$, para todo $a \in \mathbb{Z}$.*

Demonstração: Inicialmente perceba que para $p = 2$ a afirmação

$$a^2 \equiv a \ mod\ 2$$

é verdadeira pois, $a^2 - a = a(a-1)$ é par. Em razão de ser o produto de dois inteiros consecutivos.

Para p, primo ímpar, demonstraremos usando indução sobre a. Antes, perceba que será suficiente mostrar que é válido para $a \geq 0$ pois, $-a < 0$ teremos:

$$(-a)^p - (-a) = -a^p + a = -(a^p - a).$$

Assim,

i) Para $a = 0$ o teorema é válido pois $p|0$.

ii) Supondo verdadeiro para algum $a > 0$ mostremos que é válido para $a + 1$.

Pelo Binômio de Newton temos:

$$(a+1)^p - (a+1) = a^p - a + \tbinom{p}{1}a^{p-1} + ... + \tbinom{p}{p-1}a.$$

Por hipótese $p|a^p - a$ e pelo Lema 3.2, $p|\binom{p}{i}$, portanto

$$p|(a+1)^p - (a+1).$$

E o teorema está demonstrado. ∎

O Pequeno Teorema de Fermat também pode ser reescrito da seguinte forma.

Teorema 4.2 (Pequeno Teorema de Fermat - Segunda Versão) *Sejam p e $a \in \mathbb{Z}$, com p primo. Se $mdc(a,p) = 1$, então $a^{p-1} \equiv 1 \ mod\ p$.*

Demonstração: Pelo Teorema 4.1 temos $a^p \equiv a \ mod \ p$. Assim existe um $k \in \mathbb{Z}$ tal que:

$$a^p - a = kp \Leftrightarrow a(a^{p-1} - 1) = kp.$$

Como $mdc(a, p) = 1$, então $p \nmid a$, logo $p|(a^{p-1} - 1)$. Portanto,

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

■

Vejamos algumas consequências desse Teorema.

Proposição 4.1 *Seja $q = 2n + 1$ um número primo. Então ou $q|2^n - 1$ ou $q|2^n + 1$.*

Demonstração: Inicialmente perceba que q não pode dividir ambos pois do contrário $q|2^n + 1 - (2^n - 1) = 2$ o que é impossível.

Além disso, como o $mdc(q, 2) = 1$, pelo Pequeno Teorema de Fermat temos, $2^{q-1} \equiv 1 \ mod \ q$. Por outro lado, $q - 1 = 2n + 1 - 1 = 2n$. Assim, $2^{q-1} - 1 = 2^{2n} - 1 \equiv 0 \ mod \ q$. Portanto $q|2^{2n} - 1 = (2^n + 1) \cdot (2^n - 1)$. Como q não pode dividir ambos, então ou $q|2^n + 1$ ou $q|2^n - 1$. ■

Antes de apresentarmos a generalização do Pequeno Teorema de Fermat, é necessário definir algumas importantes ferramentas matemáticas.

Definição 4.1 *Seja $n \in \mathbb{Z}$, com $n > 0$. A função Euler, denotada por $\varphi(n)$, é definida como a quantidade de elementos do conjunto:*

$$\{x \in \mathbb{N}; x \leq n \ e \ mdc(x, n) = 1\}.$$

Se n for primo, então $\varphi(n) = n - 1$.

Exemplo 4.1 $\varphi(1) = 1 = \varphi(2)$, $\varphi(3) = 2 = \varphi(4)$, $\varphi(8) = 4 = \varphi(12)$ *etc...*

Definição 4.2 *Seja $m \in \mathbb{N}$. O conjunto $\{r_0, r_1, ...r_n\}$ será dito um sistema completo de resíduos módulo m se:*

i) $r_i \not\equiv r_j \ mod \ m$, para todo $i \neq j$;

ii) Para todo $a \in \mathbb{Z}$ existe um $r_i \in \{r_0, r_1, ...r_n\}$ tal que $a \equiv r_i \ mod \ m$.

A partir de um sistema de resíduos, podemos obter um sistema reduzido de resíduo módulo m. Para isso basta retirar os $r_i \in \{r_0, r_1, ...r_n\}$ onde $mdc(r_i, m) \neq 1$. A seguir apresentamos um resultado que utilizamos na demonstração do Teorema de Euler. A demonstração da proposição pode ser encontrada em [[10], capítulo 10].

Proposição 4.2 *Sejam $r_1, r_2, r_3, ..., r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m e $a \in \mathbb{Z}$ tal que $mdc(a, m) = 1$. Então $ar_1, ..., ar_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m.*

Generalizamos o Pequeno Teorema de Fermat com o Teorema de Euler, o qual evidencia a importância da função φ.

Teorema 4.3 (Teorema de Euler) *Sejam a e $m \in \mathbb{Z}$, com $m > 0$ e $mdc(a, m) = 1$. Então*

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

Demonstração: Seja $r_1, ..., r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Logo, pela Proposição 4.2, $ar_1, ..., ar_{\varphi(m)}$ formam um sistema reduzido de resíduos módulo m. Portanto,

$$a^{\varphi(m)} r_1 \cdot r_2 \cdots r_{\varphi(m)} = ar_1 \cdot ar_2 \cdots ar_{\varphi(m)1} \cdot r_2 \cdots r_{\varphi(m)} \ mod \ m.$$

Como $r_1 \cdot r_2 \cdots r_{\varphi(m)}$ é um sistema reduzido de resíduos, então podemos concluir que,

$$mdc(r_1 \cdot r_2 \cdots r_{\varphi(m)}, m) = 1.$$

Segue do Corolário 2.2 que,

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

■

Apesar de o Pequeno Teorema de Fermat não funcionar perfeitamente como um teste de primalidade, ele é uma ferramenta bastante útil para determinar a não primalidade dos números. Em outras palavras, dados $m, a \in \mathbb{Z}$ com $mdc(a, m) = 1$ de tal maneira que $m \nmid a^{m-1} - 1$, então m não pode ser primo.

Um importante resultado, que utiliza como base o Pequeno Teorema de Fermat, foi publicada em 1878 por Édouard Lucas (1842 - 1891). O seu teorema, além de ser um teste de primalidade, também constitui uma recíproca parcial do Pequeno Teorema de Fermat.

Antes de apresentar o Teorema de Lucas, se faz necessário definir o que é a ordem de um número.

Definição 4.3 *Dados $a, b \in \mathbb{Z}$ com $a > 0$ e $mdc(a, b) = 1$, definimos a ordem de b módulo a, denotada por $\mathrm{ord}_a\, b$, como sendo o menor inteiro positivo t tal que $b^t \equiv 1 \ mod \ a$.*

Exemplo 4.2 *Seja $a = 10$ e $b = 9$. Como $9^1 \equiv 9 \ mod \ 10$ e $9^2 \equiv 1 \ mod \ 10$. Temos que $\mathrm{ord}_{10}\, 9 = 2$.*

Teorema 4.4 *Seja $n \in \mathbb{N}$ e $m, a \in \mathbb{Z}$. Se $mdc(a,m) = 1$ e $a^n \equiv 1 \ mod\ m$, então* $\mathrm{ord}_m\, a \mid n$.

Demonstração: Denotemos por $b = \mathrm{ord}_n\, a$. Assim, $a^b \equiv 1 \ mod\ m$. Aplicando a divisão euclidiana segue que $n = qb + r$ com $0 \leq r < b$. Logo

$$a^n = a^{bq+r} = a^{bq} \cdot a^r.$$

Como $b = \mathrm{ord}_n\, a$, então $r = 0$ e portanto $n = qb$. ■

Proposição 4.3 *Sejam p e q números primos ímpares distintos. Se $q|2^p - 1$, então $q = 2kp + 1$. Onde $k \in \mathbb{N}$.*

Demonstração: Suponha que $q|2^p - 1$. Isto significa que $2^p \equiv 1 \ mod\ q$. Seja $\mathrm{ord}_q\, 2 = k_0$ temos $k_0|p$. Como $2 \not\equiv 1 \ mod\ q$, temos $k_0 > 1$ logo $k_0 = p$. Como $mdc(2,q) = 1$, pelo pequeno Teorema de Fermat, $2^{q-1} \equiv 1 \ mod\ q$, novamente temos $p = k_0|q-1$. Logo, existe $r \in \mathbb{Z}$ tal que $pr = q - 1$. Seja $q = 2l + 1$, como p e ímpar, concluímos que $r = 2k$. Assim, $q = 2kp + 1$.

■

Corolário 4.1 *Sejam $a, m \in \mathbb{Z}$, com $m > 1$ e $mdc(a,m) = 1$. Então* $\mathrm{ord}_m\, a|\varphi(m)$.

Demonstração: Pelo Teorema de Euler $a^{\varphi(m)} \equiv 1 \ mod\ m$ então pelo Teorema 4.4 $\mathrm{ord}_m\, a|\varphi(m)$. ■

Teorema 4.5 (Teorema de Lucas) *Sejam $a, m \in \mathbb{N}$ com $m > 1$ e $mdc(a,m) = 1$. Se,*

$$a^{m-1} \equiv 1 \ mod\ m,$$

onde,

$$a^k \not\equiv 1 \ mod\ m, \ para\ todo\ k < m - 1,$$

então m é primo.

Demonstração: Por hipótese $a^{m-1} \equiv 1 \ mod\ m$ com isso,

$$\mathrm{ord}_m\, a = m - 1.$$

Assim, pelo Corolário 4.1,

$$\mathrm{ord}_m\, a = m - 1|\varphi(m).$$

Logo, $m-1 \leq \varphi(m)$. Por outro lado $\varphi(m) \leq m-1$. Portanto $\varphi(m) = m-1$ e m é primo.

■

Definição 4.4 *Sejam $a, n \in \mathbb{Z}$. Um inteiro composto n, é chamado pseudoprimo de base a se:*

$$a^{n-1} \equiv 1 \ mod \ n.$$

Se n é pseudoprimo para todo inteiro a onde $mdc(a, n) = 1$, então chamaremos n de número de Carmichael.

Um importante teorema referente aos números de Carmichael é o critério de Korselt, em homenagem a seu criador Alwin Reinhold Korselt (1864 - 1947). O critério, além de fornecer uma segunda caracterização dos pseudoprimos também apresenta uma forma de identificá-los sem a necessidade de se utilizar o Teorema 4.1.

Antes de enuciarmos o Teorema de Korselt será necessário definirmos alguns recursos que serão necessários em sua demonstração.

Definição 4.5 *Sejam $n, a \in \mathbb{Z}$ com $n > 0$ e $mdc(a, n) = 1$. Dizemos que a é uma raiz primitiva módulo n se* $\text{ord}_n a = \varphi(n)$.

Definição 4.6 *Um inteiro n será dito livre de quadrados se a sua decomposição em fatores primos é da forma $\pm p_1, \cdots p_r$, onde $p_1, ..., p_r$ são primos distintos.*

Apresentamos agora o teorema cuja demonstração pode ser vista com mais detalhes em [21].

Teorema 4.6 (Critério de Korselt) *Seja n um número composto. Então n é número de Carmichael se, e somente se, n é livre de quadrados e $p - 1$ divide $n - 1$ para todo p primo que divide n.*

Demonstração: ($\Rightarrow$) Suponha que exista um primo p tal que $p^2 \mid n$. Por hipótese n é um número de Carmichael logo, $a^n \equiv a \ mod \ n$ para todo a inteiro, e assim

$$a^n \equiv a \ mod \ p^2.$$

Tomando $a = p$ temos, $p^n \equiv p \ mod \ p^2$, ou seja

$$p^2 \mid p^n - p$$

segue então que $p \mid p^{n-1} - 1$. Como $p|p^{n-1}$ então $p|1$, o que é um absurdo. Assim n é livre de quadrados. Seja p divisor primo de n e g uma raiz primitiva módulo p. Como n é um número de Carmichael

$$g^n \equiv g \ mod \ n,$$

e por $p|n$ temos $g^n \equiv g \ mod \ p$ ou seja,

$$p \mid g \cdot (g^{n-1} - 1).$$

Mas, $mdc(p, g) = 1$ logo, $p|g^{n-1} - 1$, em outras palavras,

$$g^{n-1} \equiv 1 \ mod \ p.$$

Como g é uma raiz primitiva módulo p temos,

$$\mathrm{ord}_p \, g = p - 1.$$

Portanto pelo Teorema 4.4, $p - 1 \mid n - 1$.
($\Leftarrow$) Seja p um divisor primo de n e seja $1 \leq b < n$ um inteiro tal que $mdc(b, n) = 1$, como $p|n$ temos, $mdc(b, p) = 1$. Pelo Teorema 4.1,

$$b^{p-1} \equiv 1 \ mod \ p.$$

Por hipótese, existe $k \in \mathbb{Z}$ tal que $n - 1 = (p - 1)k$, logo

$$b^{n-1} = b^{(n-1)k} = \left(b^{(p-1)}\right)^k \equiv 1 \ mod \ p.$$

Como n fatora-se

$$n = p_1 \cdot p_2 \cdots p_r$$

com todos os p_i distintos, pois n é livre de quadrados, para todo $1 \leq i \leq r$ temos que

$$p_i \mid (b^{n-1} - 1).$$

Logo,

$$n \mid (b^{n-1} - 1),$$

ou seja, $b^{n-1} \equiv 1 \ mod \ n$. ∎

Tabela 4.4: Os 16 números de Carmichael menores do que 100000.

$561 = 3{\cdot}11 \cdot 17$	$15841 = 7{\cdot}31 \cdot 73$
$1105 = 5{\cdot}13 \cdot 17$	$29341 = 13{\cdot}37 \cdot 61$
$1729 = 7{\cdot}13 \cdot 19$	$41041 = 7{\cdot}11 \cdot 13 \cdot 41$
$2465 = 5{\cdot}17 \cdot 29$	$46657 = 13{\cdot}37 \cdot 97$
$2821 = 7{\cdot}13 \cdot 31$	$52633 = 7{\cdot}73 \cdot 103$
$6601 = 7{\cdot}23 \cdot 41$	$62745 = 3{\cdot}5 \cdot 47 \cdot 89$
$8911 = 7{\cdot}19 \cdot 67$	$63973 = 7{\cdot}13 \cdot 19 \cdot 37$
$10585 = 5{\cdot}29 \cdot 73$	$75361 = 11{\cdot}13 \cdot 17 \cdot 31$

4.2 NÚMEROS DE FERMAT

Em uma carta a Marin Mersenne (1588 - 1648), Fermat afirmou que teria encontrado uma fórmula capaz de detectar números primos, apesar de não ter conseguido demonstrar. Acreditava que sua conjectura estava certa. Apenas após 100 anos, Euler conseguiu mostrar que a "descoberta" de Fermat não era correta. Para $n = 5$ a equação acima não nos fornece um número primo, 4294967297 = 641 x 6700417, logo, a equação não nos fornece apenas números primos. Hoje atribui-se aos números primos que satisfazem a fórmula elaborada por Fermat como Primos de Fermat. Na verdade não se sabe se a equação fornece outros números primos além dos cinco primeiros.

Definição 4.7 *Todos os números na forma* $F_n = 2^{2^n} + 1$ *são chamados números de Fermat.*

Exemplo 4.3 *Para* $n = 0$, $F_0 = 2^{2^0} + 1 = 2 + 1 = 3$.
Para $n = 1, F_1 = 2^{2^1} + 1 = 4 + 1 = 5$.
Para $n = 2, F_2 = 2^{2^2} + 1 = 16 + 1 = 17$.
Para $n = 3, F_3 = 2^{2^3} + 1 = 256 + 1 = 257$.
Para $n = 4, F_4 = 2^{2^4} + 1 = 65536 + 1 = 65537$.
Para $n = 5, F_5 = 2^{2^5} + 1 = 4294967296 + 1 = 4294967297$.

Para encerrar, apresentamos alguns resultados bastantes conhecidos sob os números de Fermat.

Lema 4.1 *Um número de Fermat é igual ao produto de todos os anteriores mais 2.*

Demonstração: Usamos indução sobre n para demonstrá-lo.

Para $n = 1$ a afirmação é verdadeira pois,

$$F_1 = 2^{2^1} + 1 = 4 + 1 = 2 + 1 + 2 = (2^{2^0} + 1) + 2 = F_0 + 2.$$

Suponha agora que,

$$F_n = (\prod_{i=0}^{n-1} F_i) + 2$$

e mostremos que,

$$F_{n+1} = (\prod_{i=0}^{n} F_i) + 2.$$

Por hipótese,

$$F_0 \cdot F_1 \cdots F_{n-1} + 2 = F_n$$

assim,

$$F_0 \cdot F_1 \cdots F_{n-1} = F_n - 2.$$

Multiplicando ambos os lados por F_n e logo após somando 2 temos:

$$F_0 \cdot F_1 \cdots F_{n-1} \cdot F_n + 2 = (F_n - 2) \cdot F_n + 2$$

o que implica em,

$$F_0 \cdot F_1 \cdots F_{n-1} \cdot F_n + 2 = (2^{2^n} + 1 - 2) \cdot (2^{2^n} + 1) - 2$$

e assim,

$$(\prod_{i=0}^{n} F_i) + 2 = (2^{2^n} - 1) \cdot (2^{2^n} + 1) - 2$$

com isso,

$$(\prod_{i=0}^{n} F_i) + 2 = (2^{2^n})^2 - 1 + 2.$$

Portanto,

$$(\prod_{i=0}^{n} F_i) + 2 = 2^{2^{n+1}} + 1 = F_{n+1}.$$

■

Corolário 4.2 *Dados F_m e F_n, dois números de Fermat. Se $m \neq n$, então $mdc(F_n, F_m) = 1$.*

Demonstração: Suponha que p é um divisor de F_n e F_m. Pelo Lema 4.1 acima $F_m = F_0 \cdot F_1 \cdot F_2 \cdots F_n \cdots F_{m-1} + 2$. Como p divide F_n e F_m, então p divide 2. Logo, $p = 2$ ou $p = 1$. Como os primos de Fermat são todos ímpares, $p \neq 2$. Portanto, $mdc(F_n, F_m) = 1$.

■

Proposição 4.4 *Todo número de Fermat maior que 3 é da forma $6n - 1$.*

Demonstração: É suficiente mostrar que 6 divide $F_n + 1$.

$$F_n + 1 = F_0 \cdot F_1 \cdots F_{n-1} + 3 = 3 \cdot F_1 \cdots F_{n-1} + 3 = 3 \cdot (F_1 \cdots F_{n-1} + 1).$$

Como $(F_1 \cdots F_{n-1} + 1)$ é par, temos que $6 \mid F_n + 1$. ■

Proposição 4.5 *O algarismo das unidades do número de Fermat é 7 para todo $n \geq 2$.*

Demonstração: Inicialmente provamos por indução que $2^{2^n} \equiv 6 \ mod\ 10$, para todo $n \geq 2$. Para $n = 2$ temos,

$$2^{2^2} = 16 \text{ e } 10|16 - 6,$$

ou seja

$$2^{2^2} \equiv 6 \ mod \ 10.$$

Suponha que $2^{2^n} \equiv 6 \ mod \ 10$ para $n \geq 2$, mostramos que vale para $n+1$. Por hipótese,

$$2^{2^n} \equiv 6 \ mod \ 10,$$

assim, $(2^{2^n})^2 \equiv (6)^2 \ mod \ 10$ o que resulta,

$$2^{2^{n+1}} \equiv 36 \ mod \ 10.$$

Porém, $36 \equiv 6 \ mod \ 10$ e assim,

$$2^{2^{n+1}} \equiv 6 \ mod \ 10.$$

Como $2^{2^{n+1}} \equiv 6 \ mod \ 10$ e $1 \equiv 1 \ mod \ 10$, temos que,

$$2^{2^n} + 1 \equiv 7 \ mod \ 10.$$

O que prova o resultado. ■

5 CONSIDERAÇÕES FINAIS

Nesse trabalho foi apresentado um estudo sobre os números primos, em especial o Pequeno Teorema de Fermat. Concomitante a isso, procurou-se apresentar consequências relevantes do teorema para o estudo da aritmética, como o Teorema de Euler, o Teorema de Korselt e o Teorema de Lucas.

É inegável o impacto das conjecturas de Fermat para o desenvolvimento da matemática. No instante em que foi firmada a escolha desse tema, não se vislumbrou a gama de conhecimentos necessário para o seu entendimento e demonstração, o que para o bom entendimento do trabalho, acabou ocorrendo.

A ideia de explorar o universo dos números primos se mostra bastante construtiva e de grande valia para o mundo acadêmico, em especial para os educadores. O estudo dos números primos vai muito além da própria aritmética, por exemplo, a álgebra e a criptografia. Um ponto interessante encontrado foi a facilidade para se compreender os teoremas que envolvem os números primos e ao mesmo tempo a dificuldade que existe para demonstrá-los.

Espera-se que esse trabalho possa servir de apoio aos professores de matemática da educação básica e aos alunos universitários dos cursos de exatas. Muitos dos assuntos aqui tratados, podem ser adaptados e apresentados aos alunos do ensino médio e/ou alunos em nível olímpicos. Por fim, há a expectativa que o presente trabalho possa auxiliar no crescimento dos educadores e assim um melhoramento na educação nacional.

REFERÊNCIAS

[1] ABIERTO, Alexandre; MATHEUS,Carlos; MOREIRA, Gustavo Carlos. **Aspectos Ergódicos da Teoria dos Números**. Impa. Rio de Janeiro. 2007. (26 Colóquio Brasileiro de Matemática)

[2] APOSTOL, Tom M. **Introduction to Analytic Number Theory**. Springer-Verlag. New York. 1976.

[3] BARBOSA, Gabriela. **Números Primos e o Teorema Fundamental da Aritmética no Sexto ano do Ensino Fundamental**. Rio de Janeiro: IMPA, 2015. (Dissertação de Mestrado).

[4] CYDARA, C. Ripoll; JAIME, B. Ripoll; ALVERI, A. Sant'Ana. **O mímino múltiplo comum e o máximo divisor comum generalizados**. Revista Matemática Universitária. nº 40. junho/2006. Pág 59-74.

[5] DIAS,Cristina Helena Bovo Batista. **Números Primos e Divisibilidade: Estudo de Propriedades**. Rio Claro: Universidade Estadual Paulista, 2013. (Dissertação de Mestrado).

[6] EstudoKids. Disponivel em: <www.estudokids.com.br/algarismos-arabicos-historia-e-sistema-de-numeracao-arabe/>. Acesso em 20 de Abril de 2017.

[7] EVARISTO,Jaime; PERDIGÃO, Eduardo. **Introdução à Álgebra Abstrata**. Maceió. 2013. (Formato Digital/Versão 01.2013a).

[8] FREITAS,Natanael Charles Brito. **Princípio da indução matemática: Fundamentos Teórico e Aplicações na Educação Básica**. Fortaleza: UECE, 2013. (Dissertação de Mestrado).

[9] GONÇALVES, Adilson. **Introdução à Algebra**. Impa. Rio de Janeiro. 2008 (Projeto Euclides)

[10] HEFEZ, Abramo. **Aritmética**. Rio de Janeiro: SBM, 2014. (Coleção PROFMAT).

[11] HEFEZ, Abramo. **Curso de Algebra. Volume 1**. Rio de Janeiro: SBM, 2002. (Coleção Matemática Universitária)

[12] Infopedia. Disponível em: <http://https://www.infopedia.pt/numeracao-romana>. Acesso em 20 de Abril de 2017

[13] JURKIEWICZ, Samuel. **Divibilidade e Números Inteiros: Introdução a Aritmética Modular**. Brasil. 2006. (Coleção OBMEP)

[14] LIMA, Elon Lages. **Análise real Volume 1. Função de uma variável**. Rio de Janeiro: IMPA, 2006. (Coleção Matemática Universitária).

[15] MACHADO, Gabriela Maria. **A construção dos números**. São Carlos: UFSCAR, 2014. (Monografia).

[16] MOL, Rogério Santos. **Introdução à história da matemática**. Belo Horizonte. CAED-UFMG, 2013. (Coleção EAD - Matemática)

[17] MONTEIRO, Luiz Henrique Jacy. **Elementos de Álgebra**. Rio de Janeiro. IMPA, 1969. (Ao livro técnico S.A)

[18] MOREIRA, Carlos Gustavo T. de A.; SALDANHA, Nicolau C. **Testes de primalidade: Probabilísticos e Determinísticos**. Impa. Rio de Janeiro. 2011 (Projeto Klein)

[19] Mundo Educação. <mundoeducacao.bol.uol.com.br/matematica/o-surgimento-dos-numeros-inteiros.htm> Acessado em 20 de Abril de 2017

[20] NETO, Antonio Caminha Munoz. **Tópicos de Matemática Elementar: Volume 5**. Rio de Janeiro: SBM, 2014. (Coleção do Professor de Matemática).

[21] RIBAS, Sávio. **Infinitos Números de Carmichael**. UFMG. 2013. (Dissertação de Mestrado).

[22] SANTOS, José Plínio de Oliveira. **Introdução a Teoria dos Números**. Rio de Janeiro: IMPA, 1998. (Coleção Matemática Universitária).

[23] SERPA, Cristina. **Do Pequeno Teorema de Fermat às Famílias Gerais de Congruências**. Lisboa: SPM, p.16-23, 2012.

[24] SILVA,Viviane Ribeiro Tomaz da; VIEIRA, Ana Cristina. **Números Inteiros: Divisibilidade, Primos, MDC e MMC**. UFMG. 2006. (Coleção Matemática Universitária).

[25] Universidade Federal Fluminense. <www.uff.br/sintoniamatematica/grandestemaseproblemas/grandestemaseproblemas-html/audio-goldbach-br.html> Acessado em 20 de Abril de 2017.