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

NIWLANDES DE FARIAS ARAÚJO

TESTES DE PRIMALIDADE: UM COMPLEMENTO PARA FORMAÇÃO DE PROFESSORES E UMA PROPOSTA DE ENSINO PARA A EDUCAÇÃO BÁSICA.

JUAZEIRO DO NORTE
2023

NIWLANDES DE FARIAS ARAÚJO

TESTES DE PRIMALIDADE: UM COMPLEMENTO PARA FORMAÇÃO DE PROFESSORES E UMA PROPOSTA DE ENSINO PARA A EDUCAÇÃO BÁSICA.

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Francisco Pereira Chaves

JUAZEIRO DO NORTE
2023

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Cariri
Sistema de Bibliotecas

A663t Araújo, Niwlandes de Farias.
Testes de primalidade: um complemento para formação de professores e uma proposta de ensino para a educação básica/ Niwlandes de Farias Araújo – 2023.
70 f. il. color.; 30 cm.
(Inclui bibliografia, p.52).

Dissertação (Mestrado) – Universidade Federal do Cariri, Centro de Ciências e Tecnologia, Programa de Pós-graduação em Matemática em Rede Nacional, Juazeiro do Norte, 2023.

Orientador: Prof. Dr. Francisco Pereira Chaves.

1. Aritmética. 2. Números primos. 3. Testes de primalidade. 4. Sequência didática. I. Chaves, Francisco Pereira (Orientador). II. Título.

CDD 513

Bibliotecário: João Bosco Dumont do Nascimento – CRB 3/1355

NIWLANDES DE FARIAS ARAÚJO

TESTES DE PRIMALIDADE: UM COMPLEMENTO PARA FORMAÇÃO DE PROFESSORES E UMA PROPOSTA DE ENSINO PARA A EDUCAÇÃO BÁSICA.

Dissertação de Mestrado apresentada ao Programa de Pós-graduação em Matemática em Rede Nacional do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Aprovada em: 24 de agosto de 2023.

BANCA EXAMINADORA

gov.br Documento assinado digitalmente
FRANCISCO PEREIRA CHAVES
Data: 19/10/2023 12:48:05-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Francisco Pereira Chaves
Orientador/UFCA

gov.br Documento assinado digitalmente
VALDIR FERREIRA DE PAULA JUNIOR
Data: 20/10/2023 13:36:41-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Valdir Ferreira de Paula Júnior
Membro Interno/UFCA

gov.br Documento assinado digitalmente
JANIELLY GONCALVES ARAUJO
Data: 20/10/2023 10:24:27-0300
Verifique em https://validar.iti.gov.br

Profa. Dra. Janielly Gonçalves Araújo
Membro Externo/IFCE

Dedico este trabalho a meu pai Nildo e à minha mãe Corrinha, pois só cheguei até aqui graças a vocês.

À minha segunda mãe Eliane, por sempre acreditar em mim.

Por fim, a minha amada esposa, Érica, que com sua enorme paciência, me acompanhou, motivou e aturou durante a licenciatura, especialização e agora mestrado. Saiba que esses títulos não são apenas meus, mas sim nossos.

Agradecimentos

Agradeço a todos os professores pelos seus preciosos ensinamentos ao longo do curso e, em especial, ao Prof. Dr. Francisco Pereira Chaves, ao qual sou grato por ter aceito me ajudar com o desenvolvimento desse trabalho.

Agradeço também a todos meus colegas que tanto me ajudaram e que tornaram possível a conclusão desse curso. À minha querida irmã Nilmara Farias de Araújo pela ajuda com o presente trabalho e, por fim, à minha esposa Érica Paiva Araújo, que me acompanha e apoia em todos os momentos.

RESUMO

A Matemática é uma ciência que desempenha um papel de extrema importância para o desenvolvimento tecnológico, dada sua vasta aplicação em áreas diversas. Diante das suas potenciais contribuições, vê-se a necessidade de exploração contínua, tendo em vista os mistérios e particularidades que perduram sem solução e que poderiam acarretar em novas descobertas. Os números primos, por exemplo, considerados por muitos matemáticos como os "átomos da aritmética", são ainda uma incógnita, no que diz respeito às curiosidades e mistérios que o envolvem e subsistem até os dias atuais. Assim, o presente trabalho, que trata de uma pesquisa de cunho bibliográfico, possui como objetivo principal, fornecer ao professor da educação básica o material necessário ao aprofundamento sobre números primos, com ênfase em critérios de primalidade. Além disso, o trabalho tem como objetivo apresentar uma proposta de ensino, para essa mesma etapa, por meio de uma sequência didática que atenda as especificidades da Base Nacional Comum Curricular (BNCC).

Palavras-chave: Aritmética. Números primos. Testes de primalidade. Sequência didática.

ABSTRACT

Mathematics is a science that plays an extremely important role in technological development, given its vast application in various areas. Given its potential contributions, there is a need for continuous exploration, considering the mysteries and peculiarities that persist without a solution and that could lead to new discoveries. Prime numbers, for example, considered by many mathematicians as the "atoms of arithmetic," are still an enigma, concerning the curiosities and mysteries that surround them and still persist to this day. Thus, the present work, which is a bibliographic research, aims to provide basic education teachers with the necessary material for a deeper understanding of prime numbers, with an emphasis on primality criteria. It also presents a teaching proposal for this same stage, through a didactic sequence that meets the specificities of the National Common Curricular Base (BNCC).

Keywords: Arithmetic. Prime numbers. Primality tests. Following teaching.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

A importância da Matemática é algo inquestionável, afinal de contas, toda tecnologia tem como base métodos matemáticos, mesmo que por tantas vezes não sejam sequer notados. Por outro lado, ao analisarmos cada um desses métodos, é fácil notar que a geometria, cálculo, probabilidade, entre outras áreas matemáticas empregadas na sua composição, se estruturam em um conceito mais simples, ainda que abstrato: os números.

Entre todas as características que podemos observar nos números naturais, um conjunto especial tem destaque, o conjunto dos números primos. Chamamos de primos os números naturais maiores que 1 e que possuem apenas dois divisores positivos: o 1 e ele mesmo. Os demais números naturais, maiores que 1, que não apresentam tal propriedade, são denominados compostos. Embora a definição seja simples, os números primos, como veremos no decorrer deste trabalho, são repletos de mistérios.

Os números primos são considerados por muitos matemáticos como os átomos da aritmética. Isso deve-se ao fato de que todos os números naturais maiores que um, ou são primos, ou podem ser escritos de modo único, a menos da ordem dos fatores, como a multiplicação entre primos, assim como os átomos compõem toda e qualquer matéria. Essa interessante propriedade ficou conhecida como o Teorema Fundamental da Aritmética (conferir Capítulo 2).

O registro mais antigo que apresenta relação com os números primos é o osso de Ishango, que possui cerca de 25 mil anos de idade. O achado apresenta três colunas de entalhes, onde, em uma delas, estão os primos entre 10 e 20, ou seja, os números: 11, 13, 17 e 19. Embora exista a possibilidade de ser apenas uma coincidência o fato de todos eles serem primos, esse pode ser o primeiro indício do interesse por tais números.

Apesar da relevante evidência, acredita-se que o conceito formal de número primo tenha surgido na Grécia Antiga, por volta de 300 a.C., onde Euclides de Alexandria apresentou em sua obra *Os Elementos*, mais especificamente no livro VII, uma de-

finição para números primos e compostos. Existe ainda a possibilidade do conceito de primalidade ter surgido através da Escola Pitagórica, por volta de 500 A.c., mas não existem evidências suficientes que confirmem tal hipótese.

Ainda em sua obra *Os Elementos*, mas agora no livro IX, Euclides de Alexandria demonstrou que o conjunto dos números primos é infinito. Ao longo do tempo, muitos outros matemáticos realizaram diferentes demonstrações para este teorema. Apresentamos algumas delas no Capítulo 3. Embora sejam louváveis e de grande importância, as demonstrações sobre a existência de infinitos primos não indicam caminhos para a determinação de números primos. Veja o que diz Ribenboim:

> [...] as diferentes demonstrações da existência de uma infinidade de números primos não são construtivas e não dão qualquer indicação sobre a determinação do enésimo número primo. Essas demonstrações não indicam tampouco quantos números primos existem inferiores a um dado número N. (RIBENBOIM, 2012, p. 149).

Alguns anos depois da definição apresentada por Euclides, o matemático Eratóstenes desenvolveu o primeiro método que se tem registro de determinar os números primos até um número n, método esse, que tornou-se popular como crivo de Eratóstenes (ver Capitulo 3). Na Tabela 1.1 estão apresentados os 90 primeiros números primos.

Tabela 1.1: Primeiros 90 números primos.

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

Fonte: Autor.

Ao observar a Tabela 1.1 percebemos que é extremamente difícil, senão impossível, estabelecer qualquer tipo de padrão ou regra de formação, o que nos leva a questionar: existe uma fórmula capaz de gerar o n-ésimo primo? A resposta é dada por Martinez et al. (2010, p. 324) "Existem fórmulas que geram números primos, mas que são tão complicadas que não ajudam muito nem a gerar números primos explicitamente nem a responder perguntas teóricas sobre a distribuição dos primos."Assim, mesmo com a sua existência, a aplicação de tais fórmulas tornam-se inviáveis em casos práticos na exploração desse conjunto.

Diante das fracassadas tentativas de encontrar uma fórmula prática para determinação do n-ésimo primo, surge o estudo da distribuição dos números primos.

> O grande avanço de Johann Carl Friedrich Gauss foi fazer uma pergunta diferente. Em vez de tentar prever a localização precisa do próximo primo, ele buscou ao menos descobrir quantos primos haveria entre os primeiros 100 números, os primeiros 1.000 e assim por diante. Se tomássemos o número N, haveria alguma maneira de estimar quantos primos encontraríamos entre os números 1 e N? (DU SAUTOY, 2007, p. 64).

Gauss iniciou, assim, a busca por funções capazes de estimar o número de primos inferiores a n. Para falarmos sobre elas, precisamos antes da definição a seguir.

Definição 1. *Seja $x > 0$ um número real. Designa-se por $\pi(x)$ o número de primos p, tais que $p \leq x$.*

Ao analisar uma tabela de primos na contracapa de um livro sobre logaritmos que havia ganhado, Gauss pôde perceber uma relação entre o número de primos até um número n e os logaritmos na base e. Assim, aos 15 anos de idade, Gauss conjecturou que $\pi(x) \cong \frac{x}{lnx}$, o que se mostrou verdadeiro, porém não tão preciso, ainda.

A palavra ainda, no fim do parágrafo anterior, deve-se ao fato de Gauss ter refinado sua estimativa com uma função integral logarítmica $Li(x)$, a qual satisfaz $Li(x) \cong \pi(x)$, produzindo resultados mais aproximados. Esta função é definida como

$$Li(x) = \int_2^x \frac{dt}{ln\, t}.$$

Mais uma vez, sua conjectura se provou verdadeira e deu origem ao chamado Teorema dos Números Primos.

Vale ressaltar que Adrien-Marie Legendre também desenvolveu, de forma independente, uma função capaz de estimar a quantidade de primos até um número n, porém não é tão precisa quanto a função $Li(x)$ de Gauss.

No ano de 1859, Georg Friedrich Bernhard Riemann foi ainda mais além, ao publicar um trabalho de 10 páginas sobre números primos, onde apresentou ao mundo uma fórmula para o número exato de primos até um número n. Tal fórmula não foi provada por ele e ficou conhecida como a hipótese de Riemann. Não apresentaremos aqui tal hipótese na sua linguagem matemática devido sua enorme complexidade.

Em 1900, a hipótese de Riemann passa a receber maior destaque, graças ao primeiro congresso internacional de matemáticos, ocorrido em Paris. Na ocasião, o professor David Hilbert apresentou 23 problemas que, segundo ele, ditariam os rumos dos matemáticos para as décadas seguintes. Até o fim do século XX um total

de 22 problemas foram solucionados, porém o oitavo da lista permanece sem solução até os dias atuais, trata-se da hipótese de Riemann.

Para que tenhamos noção da importância tamanha de tal hipótese, Du Sautoy afirma que

> Uma resposta para a hipótese de Riemann terá enormes implicações para muitos outros problemas matemáticos. Os números primos ocupam lugar tão fundamental na matemática que qualquer progresso na compreensão de sua natureza terá um impacto grandioso. A hipótese de Riemann parece ser um problema inevitável. Quando navegamos pelo terreno matemático, é como se todos os caminhos, em algum ponto, levassem necessariamente à mesma paisagem deslumbrante da hipótese de Riemann. (DU SAUTOY, 2007, p. 21).

As consequências decorrentes de tal demonstração não se restringiria apenas a matemática, mas afetaria diretamente o mundo do comércio. Isto dá-se pelo fato dos números primos serem a base de um sistema de criptografia chamado de RSA.

O RSA possui esse nome como forma de homenagem aos seus desenvolvedores, os cientistas Ron Rivest, Adi Shamir e Leonard Adleman, que em 1970, utilizando uma descoberta de Pierre de Fermat, encontraram uma maneira de proteger as transações com cartões de crédito, usando números primos. Atualmente, o sistema utiliza números com 100 algarismos.

A segurança desse sistema está intimamente ligada à falta de conhecimento sobre números primos, o que nos leva novamente aos impactos de uma possível demonstração da hipótese de Riemann. O conhecimento empregado em tal demonstração e o desenvolvido a partir dela, podem ser uma chave para quebrar os códigos utilizados pelo RSA, algo que poderia tornar o sistema inseguro.

Diante da espera por uma possível demonstração para a hipótese de Riemann, surge a natural questão: Atualmente existem métodos práticos e comprovados para verificar se um número é primo ou composto?

Perguntas como essa são naturais desde a educação básica, onde é introduzido o conceito de número primo, até os cursos de graduação e mestrado. Pensando nisso, o presente trabalho foi desenvolvido com o objetivo de fornecer ao professor da educação básica um material que proporcione o aprofundamento sobre números primos, com ênfase em critérios de primalidade, bem como apresentar uma proposta de ensino para a educação básica, que atenda as especificidades da Base Nacional Comum Curricular (BNCC). É importante observar que muitas vezes os critérios de primalidade não são abordados na graduação, o que reforça a importância do desenvolvimento deste trabalho.

Na educação básica, o estudo dos números primos deve iniciar no $6^{\underline{o}}$ ano do ensino fundamental, assim como defende a BNCC, e ao finalizá-lo, o aluno deve apresentar as seguintes habilidades:

> (EF06MA05) Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos “é múltiplo de”, “é divisor de”, “é fator de”, e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000.
> (EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor. (BRASIL, 2018, p. 301)

Desta forma, ao final do 6º ano, é ideal que o aluno não apenas compreenda o conceito de número primo mas também tenha familiaridade com algum critério de primalidade, uma vez que o mesmo deve ser capaz de classificar números naturais em primos e compostos. O discente deve, ainda, ser capaz de estabelecer critérios de divisibilidade por meio da observação de padrões e relações entre números.

No ano subsequente, a BNCC traz, como objeto de conhecimento, o estudo dos múltiplos e divisores de um número natural, que tem estreita relação com números primos e critérios de divisibilidade, e como habilidade a ser desenvolvida: "Resolver e elaborar problemas com números naturais, envolvendo as noções de divisor e de múltiplo, podendo incluir máximo divisor comum ou mínimo múltiplo comum, por meio de estratégias diversas, sem a aplicação de algoritmos."(BRASIL, 2018, p. 307). Ao fim dessa etapa de ensino, é ideal que o aluno seja capaz de decompor números naturais em fatores primos, pois, isso fornece um método mais prático e seguro na determinação dos múltiplos e divisores e consequentemente do mínimo múltiplo comum e máximo divisor comum, mesmo sem a aplicação de algoritmos.

Por fim, mas não menos importante, ao final de cada etapa o discente deve ser capaz de resolver e elaborar problemas envolvendo os conceitos abordados.

Para atingir os objetivos citados, iniciamos este trabalho dedicando o Capítulo 2 à apresentação de um resumo com conceitos e teorias fundamentais. Quanto ao Capítulo 3, o dividimos em três seções, sendo a primeira restrita a abordar apenas um teorema, apresentando diversas demonstrações interessantes que grandes matemáticos descobriram ao longo do tempo. Na segunda seção destacamos alguns testes de primalidade para números quaisquer, assim como também realizamos aplicações, e posteriormente comparações, entre os testes destacados. Para finalizar o Capitulo 3, abordamos características, curiosidades e testes de primalidade para alguns números primos de formas particulares. Por fim, o Capítulo 4 é dedicado a apresentar uma proposta de sequência didática, que venha a contribuir de forma significativa no processo de ensino e aprendizagem de números primos na educação básica.

Capítulo 2

Fundamentos

Para compreendermos algumas demonstrações que posteriormente serão realizadas, devemos, antes, enunciar e provar alguns resultados, o que faremos nesse capítulo. Para isso, tomaremos como base teórica [1], [2], [3], [4] e [5].

2.1 Princípio da Indução Matemática

Ao longo do trabalho utilizaremos muitas vezes o Princípio da Indução Matemática, também conhecido como Principio da Indução Finita (PIF), portanto faremos um breve resumo sobre o tema, partindo da ideia de que o leitor já está familiarizado com os axiomas de Peano e consequentemente com a equivalência entre os Axiomas 1, 2 e 3.

Axioma 1. *(Princípio da indução matemática) Seja $P(n)$ uma propriedade sobre o número natural n. Suponha que,*

i) $P(1)$ é válida;

ii) Para todo $n \in \mathbb{N}$ a validade de $P(n)$ implica a validade de $P(n+1)$;

Então $P(n)$ é válida para todo n natural.

Uma variação do PIF é o chamado Princípio da Indução Forte.

Axioma 2. *(Princípio da Indução Forte) Seja $P(n)$ uma propriedade sobre o número natural n. Suponha que,*

i) $P(n_0)$ é válida, para $n_0 \in \mathbb{N}$;

ii) Se $P(k)$ é válida para todo $n_0 \leq k \leq n$ então $P(n+1)$ é válida.

Então $P(n)$ é válida para todo $n \geq n_0$.

Uma outra variação de aparente simplicidade, mas de grande utilidade é o Princípio da Boa Ordem que apresentaremos em seguida.

Axioma 3. *(Princípio da Boa Ordem) Todo subconjunto não vazio $X \subset \mathbb{N}$ possui um menor elemento.*

Faremos um exemplo para melhor compreensão.

Exemplo 1. *Mostre que para todo n natural existe um inteiro q tal que,* $10^n - 1 = 3 \cdot q$.

Solução: Aplicaremos o PIF sobre n.

Se $n = 1$, então $10^1 - 1 = 9 = 3 \cdot 3$, portanto o resultado é válido para $n = 1$.

Suponha, por hipótese de indução, que o resultado seja válido para um certo n. Temos assim que, $10^n - 1 = 3 \cdot q$, para algum q inteiro. Veja agora que,

$$\begin{aligned} 10^n - 1 = 3 \cdot q &\Rightarrow 10 \cdot (10^n - 1) = 3 \cdot q \cdot 10 \\ &\Rightarrow 10^{n+1} - 10 = 30 \cdot q \\ &\Rightarrow 10^{n+1} - 1 = 30 \cdot q + 9 \\ &\Rightarrow 10^{n+1} - 1 = 3 \cdot (10 \cdot q + 3). \end{aligned}$$

Como $10 \cdot q + 3$ é inteiro, concluímos que o resultado também é válido para $n+1$ e consequentemente para todo n natural.

2.2 Divisibilidade e números primos

Definição 2. *Sejam $a, b \in \mathbb{Z}$, diremos que a divide b, se existir um $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Nesse caso, dizemos que a é divisor de b e b é múltiplo de a.*

Escreveremos $a \mid b$, como uma afirmação de que a divide b. No caso em que a não divide b, escreveremos simplesmente $a \nmid b$.

Proposição 1. *Se $a \mid b$ e $b \mid c$ então $a \mid c$.*

Demonstração: Considerando que $a \mid b$ e $b \mid c$ então existem $k, r \in \mathbb{Z}$ tais que, $b = a \cdot k$ e $c = b \cdot r$, daí segue que, $c = (a \cdot k) \cdot r = a \cdot (k \cdot r)$. Como $k \cdot r$ é inteiro, concluímos que $a \mid c$. ■

Proposição 2. *Se $a \mid b$ e $c \mid d$ então $a \cdot c \mid b \cdot d$.*

Demonstração: Se $a \mid b$ e $c \mid d$ então existem $k, r \in \mathbb{Z}$ tais que $b = a \cdot k$ e $d = c \cdot r$. Multiplicando as equações encontramos $b \cdot d = a \cdot c \cdot (k \cdot r)$. Observando que $k \cdot r$ é inteiro, concluímos que $a \cdot c \mid b \cdot d$. ■

Proposição 3. *Se $a \mid (b \pm c)$ então $a \mid b$, se e somente se, $a \mid c$.*

Demonstração: Suponha que $a \mid (b \pm c)$ e $a \mid b$, logo existem $k, r \in \mathbb{Z}$ tais que, $b \pm c = a \cdot k$ e $b = a \cdot r$. Assim, temos que $a \cdot r \pm c = a \cdot k$, portando $\pm c = a \cdot k - a \cdot r = a \cdot (k - r)$. Como $(k - r)$ é inteiro, concluímos que $a \mid c$. ■

Proposição 4. *Se* $a \mid b$ *então* $b = 0$ *ou* $\mid a \mid \leq \mid b \mid$.

Demonstração: Considere que $a \mid b$ e suponha que $b \neq 0$. Como $a \mid b$ existe $k \in \mathbb{Z}$ tal que $b = a \cdot k$ e sendo $b \neq 0$ temos que $k \neq 0$, logo $\mid k \mid \geq 1$, o que implica $\mid b \mid = \mid a \cdot k \mid = \mid a \mid \cdot \mid k \mid \geq \mid a \mid$. ■

Proposição 5. *Se* $a \mid b$ *e* $a \mid c$*, então* $a \mid (xb + yc)$*, para todo* $x, y \in \mathbb{Z}$.

Demonstração: Se $a \mid b$ e $a \mid c$ então existem $m, n \in \mathbb{Z}$ tais que $b = m \cdot a$ e $c = n \cdot a$, logo, para todo $x, y \in \mathbb{Z}$, temos $xb + yc = x(ma) + y(na) = a(xm + yn)$. Como $xm + yn \in \mathbb{Z}$ segue que $a \mid xb + yc$. ■

2.2.1 Divisão Euclidiana

Uma interessante propriedade, chamada propriedade Arquimediana de $\mathbb{Z}$, será de grande ajuda na demonstração do Teorema 1.

Proposição 6. *(Propriedade Arquimediana) Se* $a, b \in \mathbb{Z}$*, com* $b \neq 0$ *então existe* $n \in \mathbb{Z}$ *tal que,* $n \cdot b > a$.

Demonstração: Sendo $b \neq 0$ e inteiro, então $|b| \geq 1$, daí,

$$(|a| + 1) \cdot |b| \geq |a| + 1 > |a| \geq a.$$

Caso $b > 0$ então $|b| = b$ e, tomando $n = |a| + 1$, obtemos

$$n \cdot b = (|a| + 1) \cdot b = (|a| + 1) \cdot |b| > a.$$

Para o caso onde $b < 0$, temos que $|b| = -b$, logo, fazendo $n = -(|a| + 1)$, obtemos

$$n \cdot b = -(|a| + 1) \cdot b = (|a| + 1) \cdot (-b) = (|a| + 1) \cdot |b| > a.$$

Provando, deste modo, a existência de n. ■

Teorema 1. *Dados* $a, b \in \mathbb{Z}$*, com* $a \neq 0$*. Existem únicos inteiros* q *e* r *tais que:*

$$b = a \cdot q + r$$

com

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

Demonstração: Considere o conjunto $S = \{b - ya; y \in \mathbb{Z}\} \cap [\mathbb{N} \cup \{0\}]$.

Como $a \neq 0$ então $-a \neq 0$ e pela propriedade Arquimediana, existe um n inteiro tal que $n(-a) > (-b)$, ou ainda, $b - na > 0$, o que mostra que o conjunto S é

não vazio. Temos assim, pelo Princípio da Boa Ordem, que S possui um menor elemento que chamaremos de r. Como $r \in S$, então $r \geq 0$ e existe um q inteiro, tal que $r = b - aq$. Precisamos mostrar agora que $r < |a|$, o que faremos por redução ao absurdo.

Suponha, por absurdo, que $r \geq |a|$, logo, existe um $j \in \mathbb{N} \cup \{0\}$, tal que $r = |a| + j$, ou seja, $j = r - |a| = b - aq - |a|$. Sendo $|a| = a$ ou $|a| - a$, teríamos $j = b - (q \pm 1)a$, portanto, $j \in S$, o que é um absurdo pois, $j < r$, uma vez que $r = |a| + j$ e $|a| \geq 1$.

Concluímos assim que existem q e r inteiros, com $0 \leq r < |a|$, tais que

$$b = a \cdot q + r.$$

Resta provar que q e r são únicos. Para isto, suponha que existem $q, q', r, r' \in \mathbb{Z}$ tais que $b = a \cdot q + r = a \cdot q' + r'$, com $0 \leq r < |a|$ e $0 \leq r' < |a|$. Subtraindo membro a membro, $0 \leq r < |a|$ e $|a| > r' \geq 0$, obtemos

$$0 - |a| < r - r' < |a| - 0 \Rightarrow -|a| < r - r' < |a| \Rightarrow |r - r'| < |a|.$$

Por outro lado, $a \cdot q + r = a \cdot q' + r'$, somando e subtraindo aq' em ambos os lados da igualdade e tomando a em evidência, temos $a(q - q') = r' - r$, logo $|a| \cdot |q - q'| = |r - r'| < |a|$.

O que só ocorre, se $q = q'$ e $r = r'$. ■

Os números q e r chamam-se, respectivamente, de quociente e resto da divisão de b por a.

2.2.2 Máximo divisor comum e mínimo múltiplo comum

Definição 3. *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, se $d \in \mathbb{N}$ é tal que $d \mid a$ e $d \mid b$ diremos que d é um divisor comum de a e b. Além disso, caso d seja divisível por todo divisor comum de a e b diremos que d é o máximo divisor comum (MDC) de a e b e representaremos por (a, b).*

Exemplo 2. *Se $m = 8$ e $n = 12$ então $(m, n) = (8, 12) = 4$.*

É importante observar que sendo $d = (a, b)$, para todo c inteiro, temos que se $c \mid a$ e $c \mid b$ então, por definição, $c \mid d$, logo, $c \leqslant |c| \leqslant d$, ou seja, d é o maior dentre todos os divisores comuns de a e b, o que explica o motivo pelo qual d é chamado de máximo divisor comum.

Caso $(a, b) = 1$ diremos que a e b são primos entre si ou coprimos. É claro que isso significa que o único divisor comum positivo de a e b é 1.

Definição 4. *Sejam $a, b \in \mathbb{Z}$ e $d = (a, b)$. Define-se:*

i) $I(a,b) = \{ax + by; x, y \in \mathbb{Z}\}$;
ii) $d\mathbb{Z} = \{d \cdot m; m \in \mathbb{Z}\}$.

Note que, se $a \neq 0$ ou $b \neq 0$ então $I(a,b) \cap \mathbb{N}$ é não vazio, uma vez que tomando $x = a$ e $y = b$ temos $a \cdot a + b \cdot b = a^2 + b^2 \in I(a,b) \cap \mathbb{N}$. Assim, pelo Princípio da Boa Ordem, existe $d = min\{I(a,b) \cap \mathbb{N}\}$

Tal fato é importante para demonstração do teorema seguinte.

Teorema 2. *Sejam* $a, b \in \mathbb{Z}$, *com* $a \neq 0$ *ou* $b \neq 0$. *Se* $d = min\{I(a,b) \cap \mathbb{N}\}$, *então,*
i) d *é o MDC de* a *e* b;
ii) $I(a,b) = d\mathbb{Z}$.

Demonstração: i) Para mostrar que $d = (a,b)$, precisamos mostrar que d divide a e b e que para todo divisor comum c de a e b temos que $c \mid d$.

Suponha, por absurdo, que exista um $x \in I(a,b)$ tal que $d \nmid x$, então, pelo Teorema 1, existem q e r inteiros com $0 < r < d$ tais que

$$x = d \cdot q + r. \tag{2.1}$$

Por outro lado, como $d = min\{I(a,b) \cap \mathbb{N}\}$ e $x \in I(a,b)$ então existem $n, m, j, k \in \mathbb{Z}$ tais que

$$d = na + mb \tag{2.2}$$

e

$$x = ja + kb. \tag{2.3}$$

Substituindo (2.3) e (2.2) em (2.1) temos que,

$$ja + kb = (na + mb)q + r \Rightarrow r = (j - nq)a + (k - mq)b. \tag{2.4}$$

Logo $r \in I(a,b) \cap \mathbb{N}$ o que é um absurdo, uma vez que $r < d = min\{I(a,b) \cap \mathbb{N}\}$. Portanto d divide x para todo $x \in I(a,b)$. É fácil ver que $a, b \in I(a,b)$, concluímos assim que $d \mid a$ e $d \mid b$.

Considere agora um inteiro c tal que c é divisor comum de a e b. Temos assim, pela Proposição 5, que c divide todos os elementos de $I(a,b)$, logo $c \mid d$.

Fica provado, portanto, que $d = (a,b)$.

ii) Note que se $x \in I(a,b)$ então $d \mid x$, daí $x \in d\mathbb{Z}$, o que significa que $I(a,b) \subset d\mathbb{Z}$. Por outro lado, se $x \in d\mathbb{Z}$, então existe um inteiro y tal que $x = d \cdot y$. Como $d = (a,b)$ existem $n, m \in \mathbb{Z}$ tais que $d = na + mb$, desta forma podemos escrever $x = (na + mb) \cdot y = yna + myb$, logo $x \in I(a,b)$, ou seja, $d\mathbb{Z} \subset I(a,b)$.

Concluímos assim que $I(a,b) = d\mathbb{Z}$. ■

Proposição 7. *Para* $a, b \in \mathbb{Z}$, *temos que* $(a,b) = 1$ *se, e somente se, existem* $x, y \in \mathbb{Z}$ *tal que* $ax + by = 1$.

Demonstração: Seja $(a,b)=1$, pelo Teorema 2, temos que $1 \in I(a,b)$, logo existem $x,y \in \mathbb{Z}$ tal que $ax+by=1$. Reciprocamente, suponha que exista $x,y \in \mathbb{Z}$ tais que $ax+by=1$. Considere $d=(a,b)$, como $d \mid a$ e $d \mid b$, então $d \mid (ax+by)$, logo, $d \mid 1$, o que implica que $d=1$. ■

Teorema 3. *Sejam $a,b,c \in \mathbb{Z}$ com $(a,b)=1$. Se $a \mid bc$ então $a \mid c$.*

Demonstração: Se $a \mid bc$ e $(a,b)=1$ então existem $m,n,q \in \mathbb{Z}$ tais que,

$$bc = aq \tag{2.5}$$

e

$$ma + nb = 1. \tag{2.6}$$

Multiplicando a equação (2.6) por c e em seguida substituindo a equação (2.5) no resultado obtemos,

$$cma + ncb = c \Rightarrow cma + naq = c \Rightarrow a(cm+nq) = c.$$

Como $cm+nq$ é inteiro, segue que $a \mid c$. ■

Corolário 1. *Sejam $a,b,m \in \mathbb{Z}$ com $(a,m)=1$. Se $m \nmid b$ então $m \nmid a \cdot b$.*

Proposição 8. *Sejam $a,b,c \in \mathbb{Z}$ com $(a,b)=1$. Se $a \mid c$ e $b \mid c$ então $a \cdot b \mid c$.*

Demonstração: Como $(a,b)=1$ então, pela Proposição 7, existem x e y inteiros tais que,

$$ax + by = 1 \Rightarrow acx + bcy = c. \tag{2.7}$$

Segue, do fato de $a \mid c$ e $b \mid c$, que existem t e q inteiros tais que $c=at$ e $c=bq$. Substituindo esse resultado na equação (2.7), encontramos que:

$$acx + bcy = c \Rightarrow abqx + abty = c \Rightarrow ab(qx+ty) = c.$$

Como $(qx+ty) \in \mathbb{Z}$, concluímos que $ab \mid c$. ■

Definição 5. *Um número natural d será dito MDC de dados números inteiros $a_1,\ldots,a_n$, não todos nulos, se possuir as seguintes propriedades:*

i. d é um divisor comum de $a_1,\ldots,a_n$.

ii. Se c é um divisor comum de $a_1,\ldots,a_n$, então $c \mid d$.

O MDC, quando existe, é certamente único e será representado por $(a_1,\ldots,a_n)$.

Proposição 9. *Sejam $a_1, a_2, \ldots, a_n$ inteiros não todos nulos, então existe o MDC de $a_1, \ldots, a_{n-1}, a_n$ e vale a igualdade*

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

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

Se $n = 2$, o resultado é obviamente válido.

Suponha, por hipótese de indução, que para um certo n, o MDC de $a_1, \ldots, a_{n-1}, a_n$ existe e que $(a_1, \ldots, a_{n-1}, a_n) = (a_1, \ldots, (a_{n-1}, a_n))$. Devemos provar então que o resultado também é válido para $n + 1$.

Por hipótese, existe um d inteiro tal que $d = (a_1, \ldots, a_{n-1}, (a_n, a_{n+1}))$, uma vez que trata-se do MDC de n números. Note agora que, $d \mid a_1, \ldots, d \mid a_{n-1}$ e $d \mid (a_n, a_{n+1})$, consequentemente $d \mid a_1, \ldots, d \mid a_{n-1}, d \mid a_n$ e $d \mid a_{n+1}$.

Seja c um divisor comum de $a_1, a_2, \ldots, a_n, a_{n+1}$. Se $c \mid a_n$ e $c \mid a_{n+1}$ então $c \mid (a_n, a_{n+1})$, logo c é um divisor comum de $a_1, \ldots, a_{n-1}, (a_n, a_{n+1})$ e consequentemente $c \mid d$, ou seja, todo divisor comum de $a_1, a_2, \ldots, a_n, a_{n+1}$ divide d, o que prova que $d = (a_1, a_2, \ldots, a_n, a_{n+1})$. ■

Definição 6. *Dizemos que m é o mínimo múltiplo comum (MMC) de a e b se é o menor inteiro positivo que é divisível por a e b, nesse caso, escreveremos $m = [a, b]$.*

Exemplo 3. *Se $m = 8$ e $n = 12$ então $[m, n] = [8, 12] = 24$.*

Definição 7. *Diremos que um número natural m é o MMC dos inteiros não nulos $a_1, \ldots, a_n$, se possuir as seguintes propriedades:*

i. m é um múltiplo comum de $a_1, \ldots, a_n$.

ii. Se para todo múltiplo comum m' desses números, tem-se que $m \mid m'$.

É fácil ver que o MMC, se existe, é único, sendo denotado por $[a_1, \ldots, a_n]$.

Na seção seguinte apresentaremos uma forma de determinar o MDC e o MMC de dois ou mais números.

2.2.3 Propriedades sobre os números primos

Lembremos que número primo é todo número inteiro maior que 1 que possui apenas dois divisores positivos: o 1 e e ele mesmo. Se um número inteiro maior que 1 não é primo, é chamado composto.

Proposição 10. *Sejam p e q números primos. Se $p \mid q$ então $p = q$.*

Demonstração: Se $p \mid q$ então $p = 1$ ou $p = q$, pois q é primo. Como p é primo então $p \neq 1$, logo, $p = q$. ■

Proposição 11. *Se $p \nmid a$, com p primo e $a \in \mathbb{Z}$, então $(p, a) = 1$.*

Demonstração: Seja $d = (p, a)$, como p é primo, segue que $d = 1$ ou $d = p$. Se p não divide a, então p é diferente de d, logo, $d = 1$. ■

Proposição 12. *Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$ então $p \mid a$ ou $p \mid b$.*

Demonstração: Sabendo que $p \mid ab$ temos duas possibilidades: $p \mid a$ ou $p \nmid a$. Se $p \mid a$ não há o que demonstrar. Se $p \nmid a$ então, pela Proposição 11, $(p, a) = 1$ o que implica, pelo Teorema 3, que $p \mid b$. É claro que, pelo mesmo raciocínio, se $p \nmid b$ então $p \mid a$. ■

Corolário 2. *Sejam $p, p_1, \ldots, p_n$ números primos. Se $p \mid p_1 \cdot \ldots \cdot p_n$, então $p = p_i$ para algum $i = 1, ..., n$.*

Demonstração: Demonstraremos por indução matemática sobre n.

Seja $n = 1$. Se $p \mid p_1$ então $p = p_1$, pois são ambos primos. Logo o resultado é válido para $n = 1$.

Suponha, por hipótese de indução, que para um certo n o resultado seja válido. Considere agora que $p \mid p_1 \cdot \ldots \cdot p_n \cdot p_{n+1}$, pela Proposição 12, $p \mid p_1 \cdot \ldots \cdot p_n$ ou $p \mid p_{n+1}$.

Se $p \mid p_{n+1}$ então $p = p_{n+1}$, caso $p \mid p_1 \cdot \ldots \cdot p_n$, segue, por hipótese de indução, que existe algum $i = 1, \ldots, n$, tal que $p = p_i$.

Portanto o resultado é válido para $n + 1$. Concluímos assim pelo PIF que a proposição é válida para todo $n \in \mathbb{N}$. ■

O teorema apresentado a seguir, conhecido como Teorema Fundamental da Aritmética, foi demonstrado por Gauss em 1796.

Teorema 4. *(Teorema Fundamental da Aritmética) Se $n \geq 2$ é um número natural então ou n é primo ou pode ser escrito de forma única, a menos da ordem dos fatores, como um produto de números primos.*

Demonstração: Provaremos através do Princípio da Indução Forte, para $n \geq 2$.

Como 2 é primo, se $n = 2$ o resultado é válido.

Considere, por hipótese de indução, que o resultado seja válido para todo número natural menor que n. Observe que temos duas possibilidades para n, ou n é primo ou n é composto.

Se n é primo, o resultado é obviamente válido.

Se n é composto, então existem n_1 e n_2 naturais com $1 < n_1 < n$ e $1 < n_2 < n$ tais que $n = n_1 \cdot n_2$. Como n_1 e n_2 são ambos menores que n segue, por hipótese, que existem $p_1, p_2, \ldots, p_r$ e $q_1, q_2, \ldots, q_s$ primos, tais que $n_1 = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ e

$n_2 = q_1 \cdot q_2 \cdot \ldots \cdot q_s$. Portando $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_s$, ou seja, o resultado é válido para n.

Mostraremos agora a unicidade da fatoração. Suponha que $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r = q_1 \cdot q_2 \cdot \ldots \cdot q_s$, onde p_i e q_j são primos, com $1 \leq i \leq r$ e $1 \leq j \leq r$. Veja que $p_1 \mid q_1 \cdot \ldots \cdot q_r$, logo, existe um j tal que $p_1 = q_j$, considere, sem perda de generalidade, que $p_1 = q_1$. Teríamos então que, $p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s$.

Seja $t = p_2 \cdot \ldots \cdot p_r$, como $t < n$ então, por hipótese, sua fatoração em primos é única. Portanto $r = s$ e p_i é igual a q_j aos pares.

Concluímos assim, pelo Princípio da Indução Forte, que o resultado é válido para todo $n \geq 2$ natural. ■

O Teorema Fundamental da Aritmética ainda pode ser apresentado da seguinte maneira.

Teorema 5. *Todo número natural $n > 1$ pode ser representado de forma única como,*

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_s^{\alpha_s}$$

onde $\alpha_1, \alpha_2, \ldots, \alpha_s \in \mathbb{N}$ e $p_1 < p_2 < \cdots < p_s$ são números primos.

A representação através do produto entre números primos, pode ser utilizada na determinação da quantidade de divisores de um número qualquer, bem como no cálculo da soma dos divisores, como também na determinação do MDC e MMC de dois ou mais números. Como pode ser verificado nos teoremas que seguem.

Teorema 6. *Seja $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, onde $p_1, \ldots, p_r$ são primos distintos e $\alpha_i \in \mathbb{N}$ para $i = 1, \ldots, r$. Se q divide n, então,*

$$q = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$$

onde, $0 \leq \beta_i \leq \alpha_i$, para $i = 1, \ldots, r$.

Demonstração: Seja q um divisor de n e p^β a potência de um primo na decomposição de q, como $q \mid n$ e $p^\beta \mid q$ então $p^\beta \mid n$. Sendo p um primo então p^β divide $p_i^{\alpha_i}$, para algum $i = 1, \ldots, r$, logo, $p = p_i$ e $\beta \leq \alpha_i$. ■

Partindo do Teorema 6 podemos determinar a quantidade de divisores de n apenas aplicando o Princípio Fundamental da Contagem.

Proposição 13. *Seja $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, onde $p_1, \ldots, p_r$ são primos distintos e $\alpha_i \in \mathbb{N}$ para $i = 1, \ldots, r$. Então o número de divisores de n é dado por $d_n = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_r + 1)$.*

Demonstração: Pelo Teorema 6, os divisores de n são da forma $p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$, com β_i inteiro e $0 \leq \beta_i \leq \alpha_i$, para $i = 1, \ldots, r$. Veja que existem assim $(\alpha_i + 1)$ escolhas possíveis para β_i. Como cada escolha distinta representa um divisor para n, concluímos, pelo Princípio Fundamental da Contagem, que o número de divisores de n é dado por $d_n = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_r + 1)$. ■

Dedicaremo-nos agora a apresentar uma forma para determinar (a, b) e $[a, b]$ utilizando a decomposição em fatores primos de a e b. Veja o teorema seguinte.

Teorema 7. *Sejam $a = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ e $b = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$, onde $p_1, \ldots, p_r$ são primos distintos, $0 \leq \alpha_i$ e $0 \leq \beta_j$, com $\alpha_i, \beta_i \in \mathbb{Z}$, para $i, j = 1, \ldots, r$. Temos que,*

$$(a, b) = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$$

e

$$[a, b] = p_1^{\delta_1} \cdot \ldots \cdot p_r^{\delta_r}$$

onde $\gamma_i = min\{\alpha_i, \beta_i\}$ e $\delta_i = max\{\alpha_i, \beta_i\}$.

Demonstração: É fácil ver que $p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$ divide a e b. Provaremos que para todo divisor comum c de a e b temos que $c \mid p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$.

Seja c um divisor comum de a e b, logo c é da forma $c = p_1^{\delta_1} \cdot \ldots \cdot p_r^{\delta_r}$, com $\delta_i \leq min\{\alpha_i, \beta_i\}$, o que implica que $c \mid p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$.

Concluímos assim que $(a, b) = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$.

Note que, sendo $m = [a, b]$, então m é o menor inteiro positivo que é divisível por a e b.

Para que m seja divisível por a e b devemos ter, pelo Teorema 6, $m = p_1^{\delta_1} \cdot \ldots \cdot p_r^{\delta_r}$, onde $\delta_i \geq \alpha_i$ e $\delta_i \geq \beta_i$ e para que m seja mínimo é óbvio que devemos tomar $\delta_i = max\{\alpha_i, \beta_i\}$. ■

O teorema que acabamos de demonstrar será utilizado na demonstração da seguinte proposição sobre MDC.

Proposição 14. *Sejam $a, b \in \mathbb{Z}$. Tem-se que:*

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

Demonstração: Pelo Teorema Fundamental da Aritmética podemos escrever $a = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ e $b = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$, onde p_i é primo, $0 \leq \alpha_i$ e $0 \leq \beta_j$, para $i, j = 1, \ldots, r$, e pelo Teorema 7, sabemos que $(a, b) = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$, onde $\gamma_i = min\{\alpha_i, \beta_i\}$. Note, com isso, que

$$\frac{a}{(a, b)} = p_1^{\alpha_1'} \cdot \ldots \cdot p_r^{\alpha_r'}$$

e

$$\frac{b}{(a,b)} = p_1^{\beta_1'} \cdot \ldots \cdot p_r^{\beta_r'}$$

onde $\alpha_i' = 0$ ou $\beta_i' = 0$, ou seja, $\frac{a}{(a,b)}$ e $\frac{b}{(a,b)}$ não possuem fatores em comum. Portanto, $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$. ■

Representaremos por $S(n)$ a soma dos divisores positivos de n.

Proposição 15. *Seja $n = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ onde $p_1, \ldots, p_r$ são primos distintos e $\alpha_i \in \mathbb{N}$, para $1 \leq i \leq r$. A soma dos divisores de n é dada por,*

$$S(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}.$$

Demonstração: Os divisores de n são dados, segundo o Teorema 6, por $q = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$, tomando todas as possíveis r-uplas $(\beta_1, \ldots, \beta_r)$, com $0 \leq \beta_i \leq \alpha_i$. Note que, com essa ideia, a soma dos divisores de n será dada então por

$$S(n) = (1 + p_1 + \ldots + p_1^{\alpha_1}) \cdot \ldots \cdot (1 + p_r + \ldots + p_r^{\alpha_r}).$$

Uma vez que todas as combinações são geradas na sua expansão. Como $1 + p_i + \ldots + p_i^{\alpha_i}$ trata-se da soma dos i primeiros termos de uma progressão geométrica de razão p_i, podemos facilmente calcular essa soma, de onde obtemos

$$S(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}.$$

■

Sendo n um número natural é óbvio que o mesmo é primo se, e somente se, $S(n) = n + 1$.

Corolário 3. *Sejam $n, m \in \mathbb{Z}$, com $(n, m) = 1$, tem-se que $S(n) \cdot S(m) = S(n \cdot m)$.*

Apresentaremos a seguir um outro teorema de grande relevância no estudo de números primos, conhecido como o Pequeno Teorema de Fermat. Todavia, antes de estudá-lo, precisamos de um resultado para auxiliar na sua demonstração. Trata-se do lema seguinte.

Lema 1. *Seja p um número primo. Temos que $p \mid \binom{p}{i}$, onde $\binom{p}{i} = \frac{p!}{i!(p-i)!}$, para $0 < i < p$, com $i \in \mathbb{N}$.*

Demonstração: Tomando $i = 1$ temos $\binom{p}{1} = p$. Como $p \mid p$ então o resultado é válido para $i = 1$. Podemos então considerar $1 < i < p$. Note que,

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p \cdot (p-1) \cdot \ldots \cdot (p-(i-1))}{i!}.$$

Veja agora que $p \nmid i!$, pois todos os fatores de $i!$ são menores que p, uma vez que $i < p$, logo, $(i!, p) = 1$.

Como $i! \mid p \cdot (p-1) \cdot \ldots \cdot (p-(i+1))$ e $(i!, p) = 1$, concluímos, pelo Teorema 3, que $i! \mid (p-1) \cdot \ldots \cdot (p-(i+1))$, ou seja, $\frac{(p-1)\cdot\ldots\cdot(p-(i+1))}{i!} \in \mathbb{Z}$ e consequentemente $p \mid \binom{p}{i}$. ■

Teorema 8. *(Pequeno Teorema de Fermat) Sendo p um número primo qualquer, temos que $p \mid a^p - a$, para todo $a \in \mathbb{Z}$.*

Demonstração: Se $p = 2$, veja que a^2 e a têm mesma paridade, logo, $a^2 - a$ é par e consequentemente divisível por 2, para todo $a \in \mathbb{Z}$. Provando assim a validade do teorema para $p = 2$.

Considere agora $p \geq 3$, o que significa que p é ímpar e com isso $(-a)^p - (-a) = -(a^p - a)$. Portanto, se $p \mid a^p - a$ então $p \mid (-a)^p - (-a)$. Podemos com isso considerar $a \geq 0$. Faremos a demonstração por indução matemática sobre a.

Se $a = 0$ então $0^p - 0 = 0$ e se $a = 1$ temos que $1^p - 1 = 0$, como $p \mid 0$ o resultado é válido para esses casos.

Suponha, por hipótese de indução, que o resultado seja válido para um certo a. Provaremos que vale para $a + 1$. Para isso, note que

$$\begin{aligned}(a+1)^p - (a+1) &= a^p + a^{p-1}\binom{p}{1} + a^{p-2}\binom{p}{2} + \ldots + a\binom{p}{p-1} + 1 - a - 1 \\ &= (a^p - a) + a^{p-1}\binom{p}{1} + a^{p-2}\binom{p}{2} + \ldots + a\binom{p}{p-1}.\end{aligned}$$

Por hipótese $p \mid a^p - a$ e, pelo Lema 1, segue que $p \mid a^{p-1}\binom{p}{1} + a^{p-2}\binom{p}{2} + \ldots + a\binom{p}{p-1}$, pois p divide cada parcela da soma. Portanto, $p \mid (a+1)^p - (a+1)$.

Concluímos assim, pelo PIF, que $p \mid a^p - a$, para todo $a \in \mathbb{Z}$. ■

Corolário 4. *Se $p \nmid a$, então $p \mid a^{p-1} - 1$.*

Demonstração: Veja que $a^p - a = a(a^{p-1} - 1)$, portanto, se $p \nmid a$ então, pela Proposição 12, $p \mid a^{p-1} - 1$. ■

Embora seja semelhante a um critério de primalidade, a recíproca do Pequeno Teorema de Fermat não é válida, ou seja, existem números inteiros n, compostos, tais que $n \mid a^{n-1} - 1$, com $(a, n) = 1$, para todo $a \in \mathbb{N}$. Apresentaremos um desses casos abaixo.

Exemplo 4. *Mostre que $561 \mid a^{560} - 1$, para todo a natural, tal que $(a, 561) = 1$.*

Solução: Seja $a \in \mathbb{N}$, tal que $(a, 561) = 1$. Como $561 = 3 \cdot 11 \cdot 17$ e $(a, 561) = 1$ então $(a, 3) = (a, 11) = (a, 17) = 1$, o que implica que $(a^{280}, 3) = (a^{56}, 11) = (a^{35}, 17) = 1$. Desta forma, pelo Pequeno Teorema de Fermat, temos que,

i) $3 \mid (a^{280})^2 - 1 \Rightarrow 3 \mid a^{560} - 1$;

ii) $11 \mid (a^{56})^{10} - 1 \Rightarrow 11 \mid a^{560} - 1$;

iii) $17 \mid (a^{35})^{16} - 1 \Rightarrow 17 \mid a^{560} - 1$.

Como $(3,\ 11) = (3,\ 17) = (11,\ 17) = 1$, concluímos, pela Proposição 8, que $561 \mid a^{560} - 1$, para todo $a \in \mathbb{N}$, com $(a, 561) = 1$.

Com base nesse exemplo, podemos definir um novo grupo de números, os denominados pseudoprimos.

Definição 8. *Seja n um número composto. Se $n \mid a^{n-1} - 1$, para $a > 1$ inteiro com $(a, n) = 1$, então n é chamado pseudoprimo na base a.*

Números como 561, que são pseudoprimos em todas as bases primas com ele, são chamado de números de Carmichael, em homenagem a Robert Daniel Carmichael que apresentou em 1912 alguns exemplos destes números, provando assim que a recíproca do Pequeno Teorema de Fermat não era verdadeira.

Os números de Carmichael são raros (apresentaremos os números menores que 30.000 na Tabela 2.1), por este motivo, o Pequeno Teorema de Fermat é muitas vezes apresentado como um teste de primalidade probabilístico.

Tabela 2.1: Números de Carmichael

$561 = 3 \cdot 11 \cdot 17$	$1105 = 5 \cdot 13 \cdot 17$	$1729 = 7 \cdot 13 \cdot 19$	$2465 = 5 \cdot 17 \cdot 29$	$2821 = 7 \cdot 13 \cdot 31$
$6601 = 7 \cdot 23 \cdot 41$	$8911 = 7 \cdot 19 \cdot 67$	$10585 = 5 \cdot 29 \cdot 73$	$15841 = 7 \cdot 31 \cdot 73$	$29341 = 13 \cdot 37 \cdot 61$

Fonte: Autor.

Embora o Pequeno Teorema de Fermat não seja de fato um teste de primalidade determinístico o mesmo é de grande utilidade nos testes que abordaremos ao longo deste trabalho, por esse motivo, apresentaremos um caso específico desse teorema, como um pré-teste de primalidade.

Corolário 5. *(Pré-teste de primalidade) Sejam a, p números inteiros, com $p > 2$ e $(p, a) = 1$. Se $p \nmid a^{p-1} - 1$ então p é composto.*

2.3 Congruências

Definição 9. *Sejam $a, b, c \in \mathbb{Z}$. Quando a e b deixam o mesmo resto na divisão por c, dizemos que a é congruente a b módulo c. Neste caso, escrevemos $a \equiv b \mod c$.*

Exemplo 5. *Veja que o resto de 8 e 5 na divisão por 3 é 2, logo, $8 \equiv 5 \mod 3$.*

Teorema 9. *Sejam a, b e m números inteiros com $m > 1$. Temos que $a \equiv b \mod m$ se, e somente se, $m \mid a - b$.*

Demonstração: Se $a \equiv b \mod m$, então pela Definição 9, a e b deixam o mesmo resto na divisão por m, logo, existem $k, j, r \in \mathbb{Z}$ tais que $a = km + r$ e $b = jm + r$, com $0 \leq r < m$. Daí, $a - b = km - jm = m(k - j)$, ou seja, $m \mid a - b$.

Reciprocamente, se $m \mid a - b$ existe $h \in \mathbb{Z}$ tal que $a - b = mh$, o que implica que $a = b + mh$.

Seja r o resto da divisão de a por m, temos que $a = km + r$, com k inteiro. Daí, $km + r = b + mh$, logo, $b = m(k - h) + r$.

Como $0 \leq r < m$, segue, pela unicidade do resto, que r é o resto da divisão de b por m o que significa que $a \equiv b \mod m$. ■

Proposição 16. *Dados $a, b, c, d, m \in \mathbb{Z}$, temos que:*

i) (Reflexiva) $a \equiv a \mod m$.

ii) (Simétrica) Se $a \equiv b \mod m$, então $b \equiv a \mod m$.

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

iv) (Compatibilidade com a soma e a diferença) Se $a \equiv b \mod m$ e $c \equiv d \mod m$ então $a \pm c \equiv b \pm d \mod m$.

v) (Compatibilidade com o produto) Se $a \equiv b \mod m$ e $c \equiv d \mod m$ então $a \cdot c \equiv b \cdot d \mod m$.

vi) (Cancelamento no produto) Seja $c \neq 0$ e $m > 1$. Temos que $ac \equiv bc \mod m$ se, e somente se, $a \equiv b \mod \frac{m}{(c,m)}$.

Demonstração. (i) Veja que $a - a = 0$, como $m \mid 0$, então $a \equiv a \mod m$.

(ii) Se $a \equiv b \mod m$, então existem $k, j, r \in \mathbb{Z}$ com $0 \leq r < m$ tal que $a = km + r$ e $b = jm + r$. Logo, $b - a = m(j - k)$, ou seja, $m \mid b - a$, o que significa que $b \equiv a \mod m$.

(iii) Se $a \equiv b \mod m$ e $b \equiv c \mod m$ então $m \mid a - b$ e $m \mid b - c$. Portanto, existem $k, j \in \mathbb{Z}$ tais que $a - b = km$ e $b - c = jm$, logo,

$$(a - b) + (b - c) = m(k + j),$$

ou seja,

$$a - c = m(k + j).$$

Daí, segue que $m \mid a - c$ e consequentemente, $a \equiv c \mod m$.

(iv) Como $a \equiv b \mod m$ e $c \equiv d \mod m$, então $m \mid a - b$ e $m \mid c - d$, logo, pela Proposição 5, $m \mid (a - b) \pm (c - d)$, ou seja, $m \mid (a + c) - (b + d)$ e $m \mid (a - c) - (b - d)$. Concluímos, assim, que $a + c \equiv b + d \mod m$ e $a - c \equiv b - d \mod m$.

(v) Como $a \equiv b \mod m$ e $c \equiv d \mod m$, então $m \mid a-b$ e $m \mid c-d$. Logo, $m \mid (a-b)c$ e $m \mid (c-d)b$, e pela Proposição 5, $m \mid (a-b)c+(c-d)b$. Portanto, $m \mid ac-bd$, que é equivalente a $ac \equiv bd \mod m$.

(vi) Suponha que $ac \equiv bc \mod m$, logo, $m \mid ac-bc$, ou ainda, $m \mid (a-b)c$. Desta forma, existe um inteiro k tal que $mk = (a-b)c$. Multiplicando ambos os lados da igualdade por $\frac{1}{(c,m)}$, temos

$$\frac{m}{(m,c)} \cdot k = \frac{c}{(m,c)} \cdot (a-b).$$

Como $\frac{m}{(m,c)}$ e $\frac{c}{(m,c)}$ são números inteiros, então $\frac{m}{(m,c)} \mid \frac{c}{(m,c)} \cdot (a-b)$.

Pela Proposição 14, temos que $\left(\frac{m}{(m,c)}, \frac{c}{(m,c)}\right) = 1$, e pelo Teorema 3, $\frac{m}{(m,c)} \mid (a-b)$, o que é equivalente a $a \equiv b \mod \frac{m}{(m,c)}$.

Reciprocamente, se $a \equiv b \mod \frac{m}{(m,c)}$ então $\frac{m}{(m,c)} \mid a-b$, logo existe um inteiro k, tal que $\frac{m}{(m,c)} \cdot k = (a-b)$. Multiplicando ambos os lados da igualdade por c, encontramos

$$m \cdot \frac{kc}{(m,c)} = (a-b)c = (ac-bc).$$

Como $\frac{kc}{(m,c)}$ é inteiro, concluímos que $m \mid (ac-bc)$, em outras palavras, $ac \equiv bc \mod m$. ■

Iremos definir agora dois tipos de sistemas de resíduos, completo e reduzido.

Definição 10. *Seja $m > 1$ inteiro. O conjunto de números inteiros $R' = \{r_1, r_2, \ldots, r_m\}$ é chamado de sistema completo de resíduos módulo m se:*

1. *$r_i \not\equiv r_j \mod m$, para todo $i \neq j$.*
2. *Dado um inteiro n qualquer, existe um r_i, tal que $n \equiv r_i \mod m$.*

Com $1 \leq i \leq m$ e $1 \leq j \leq m$.

Como já vimos, pelo algoritmo da divisão Euclidiana, para qualquer inteiro a o seu resto na divisão por m, deve pertencer ao conjunto $\{0, 1, \ldots, m-1\}$, isso significa que todo sistema completo de resíduos modulo m possui m elementos. Utilizando ainda o algoritmo da divisão Euclidiana podemos demonstrar a proposição seguinte, que garante por sua vez, que nenhum sistema reduzido de resíduos será vazio.

Proposição 17. *Sejam $n, m, r \in \mathbb{Z}$, com $m > 1$, tais que $n \equiv r \mod m$. Se $(n, m) = 1$, então $(r, m) = 1$.*

Demonstração: Sendo $n \equiv r \mod m$ então $m \mid n-r$, o que significa que existe um q inteiro tal que $n - r = mq$, ou ainda, $n = mq + r$.

Considere $(r, m) = d$. Temos assim que, $d \mid r$ e $d \mid m$, logo, $d \mid mq + r$, ou seja, $d \mid n$. Mas se $d \mid n$ e $d \mid m$ então $d \mid (n, m)$. Como $(n, m) = 1$, podemos concluir que $(r, m) = 1$. ■

Definição 11. *Seja $m > 1$ inteiro. O conjunto de números inteiros $R = \{r_1, r_2, \ldots, r_t\}$ é chamado de sistema reduzido de resíduos módulo m se:*

1. *$(r_i, m) = 1$, para todo $i = 1, 2 \ldots, t$.*
2. *$r_i \not\equiv r_j \mod m$ para todo $i \neq j$, com $1 \leq i \leq t$ e $1 \leq j \leq t$.*
3. *Para cada n inteiro, com $(n, m) = 1$ existem um r_i tal que $n \equiv r_i \mod m$.*

Proposição 18. *Considere $m \in \mathbb{Z}$, com $m > 1$. Dois sistemas reduzidos de resíduos modulo m possuem o mesmo número de elementos.*

Demonstração: Sejam os conjuntos $\{r_1, r_2, \ldots, r_t\}$ e $\{q_1, q_2, \ldots, q_s\}$ sistemas reduzidos de resíduos modulo m. Como $(r_1, m) = 1$ então $r_1 \equiv q_i \mod m$, para algum $1 \leq i \leq s$. Pelo mesmo raciocínio $r_2 \equiv q_j \mod m$, com $1 \leq j \leq s$ e $j \neq i$, uma vez que $r_1 \not\equiv r_2 \mod m$. Seguindo com este raciocínio, podemos concluir que cada elemento de $\{r_1, r_2, \ldots, r_t\}$ é congruente a um e apenas um elemento de $\{q_1, q_2, \ldots, q_s\}$, ou seja $t \leq s$.

De maneira análoga temos que cada elemento de $\{q_1, q_2, \ldots, q_s\}$ é congruente a um e apenas um elemento de $\{r_1, r_2, \ldots, r_t\}$, logo $s \leq t$.

Concluímos assim que $t = s$. ■

Partindo dessa demonstração podemos definir a função fi de Euler.

Definição 12. *Seja R um sistema reduzido de resíduos módulo m, com $m \in \mathbb{N}$. Define-se a função $\varphi : \mathbb{N} \to \mathbb{N}$, por $\varphi(1) = 1$ e $\varphi(m) = n(R)$ para todo $m > 1$, onde $n(R)$ representa o número de elementos do conjunto R.*

Lema 2. *Sejam a, b, c números inteiros. Se $(a, b) = (c, b) = 1$, então $(ac, b) = 1$.*

Demonstração: Considere $(ac, b) = d$. Suponha, por absurdo, que $d \neq 1$. Logo, pelo Teorema Fundamental da Aritmética, podemos escrever $d = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, onde $\alpha_i \in \mathbb{N}$ e p_i é primo, ambos os casos para $i = 1, 2, \ldots, s$.

Como $d \mid b$ e $p_1 \mid d$ então $p_1 \mid b$. De forma análoga, temos que $p_1 \mid ac$, pois $d \mid ac$, daí, pela Proposição 12, $p_1 \mid a$ ou $p_1 \mid c$. Veja agora que, se $p_1 \mid a$ então $p_1 \mid (a, b)$ e se $p_1 \mid c$ então $p_1 \mid (c, b)$. Em ambos os casos, temos que $p_1 \mid 1$, uma vez que $(a, b) = (c, b) = 1$, o que é um absurdo, pois p_1 é primo. Concluímos assim que $(ac, b) = 1$. ■

Teorema 10. *Sejam a e m números naturais, com $(a, m) = 1$. Se $\{r_1, \ldots, r_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo m, então $\{ar_1, \ldots, ar_{\varphi(m)}\}$ é um Sistema Reduzido de Resíduos módulo m.*

Demonstração: Sendo $(a, m) = 1$ e $(r_i, m) = 1$ então, pelo Lema 2, $(ar_i, m) = 1$, para $i = 1, 2, \ldots, \varphi(m)$. Provando, assim, que o item (1) da Definição 11 é satisfeito.

Para provar que o item (2) da Definição 11 é satisfeito, note que $r_i \not\equiv r_j \mod m$ para $i \neq j$, ou seja, $m \nmid r_i - r_j$. Como $(a, m) = 1$ segue, pelo Corolário 1 que $m \nmid a(r_i - r_j)$. Portanto, $ar_i \not\equiv ar_j \mod m$, para todo $i \neq j$.

Resta mostrar que o item (3) da Definição 11 é satisfeito. Para isso, veja que $(ar_1, m) = 1$, logo, existe um r_i tal que $ar_1 \equiv r_i \mod m$. De maneira análoga existe um r_j tal que $ar_2 \equiv r_j \mod m$, com $i \neq j$, uma vez que $ar_1 \not\equiv ar_2 \mod m$. Seguindo com esse raciocínio podemos concluir que cada elemento de $\{ar_1, \ldots, ar_{\varphi(m)}\}$ é congruente a um e apenas um elemento de $\{r_1, \ldots, r_{\varphi(m)}\}$. Como os dois conjuntos possuem o mesmo número de elementos segue que cada elemento de $\{r_1, \ldots, r_{\varphi(m)}\}$ é congruente a um e apenas um elemento de $\{ar_1, \ldots, ar_{\varphi(m)}\}$.

Logo, se para cada n inteiro, com $(n, m) = 1$ existe um r_i tal que $n \equiv r_i \mod m$, então existe ar_j tal que $n \equiv r_i \equiv ar_j \mod m$.

Portanto, $\{ar_1, \ldots, ar_{\varphi(m)}\}$ é um sistema reduzido de resíduos modulo m. ■

Teorema 11. *(Teorema de Euler) Sejam $a, m \in \mathbb{Z}$ com $m > 1$ e $(a, m) = 1$. Então*

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

Demonstração: Seja $r_1, r_2, \ldots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Pelo Teorema 10, segue que $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ é também um sistema reduzido de resíduos módulo m, uma vez que $(a, m) = 1$. Note agora que $ar_i \equiv r_j \mod m$ para algum i e j, com $1 \leq i, j \leq \varphi(m)$. Isso significa que

$$a^{\varphi(m)} \cdot r_1 \cdot r_2 \ldots \cdot r_{\varphi(m)} = a \cdot r_1 \cdot a \cdot r_2 \cdot \ldots \cdot a \cdot r_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \mod m.$$

Como $(r_1, m) = \ldots = (r_{\varphi(m)}, m) = 1$ então, pela Proposição 9, segue que $(r_1, r_2, \ldots, r_{\varphi(m)}, m) = 1$. Desta forma, temos que

$$\frac{a^{\varphi(m)} \cdot r_1 \cdot r_2 \ldots \cdot r_{\varphi(m)}}{r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)}} \equiv \frac{r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)}}{r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)}} \mod \frac{m}{(r_1, r_2, \ldots, r_{\varphi(m)}, m)}.$$

Concluímos, assim, que $a^{\varphi(m)} \equiv 1 \mod m$. ■

Um caso específico do Teorema de Euler merece destaque. Trata-se do caso onde m é primo, veja que isso implica que $\varphi(m) = m - 1$, uma vez que $(1, m) = (2, m) = \ldots = (m-1, m) = 1$, o que nos leva a concluir que $a^{m-1} \equiv 1 \mod m$, para m primo. É impossível não notar que o caso específico é equivalente ao Pequeno Teorema de Fermat (demonstrado anteriormente), desta forma, o Teorema de Euler trata-se de uma generalização do Pequeno Teorema de Fermat. Apresentaremos esse caso específico a seguir como um corolário.

Corolário 6. *Seja a um número inteiro e p um primo. Temos que $a^p \equiv a \mod p$. Além disso, caso $(a,p) = 1$, então $a^{p-1} \equiv 1 \mod p$.*

Note que, sendo $a, m \in \mathbb{Z}$ com $m > 1$ e $(a,m) = 1$, o Teorema de Euler garante a existência de um inteiro positivo h tal que $a^h \equiv 1 \mod m$. A definição seguinte, tem como base esse resultado.

Definição 13. *Sejam $a, m \in \mathbb{Z}$ com $m > 1$ e $(a,m) = 1$. Chama-se ordem de a módulo m, representado por $ord_m(a)$, o menor inteiro positivo, tal que, $a^{ord_m(a)} \equiv 1 \mod m$.*

Lema 3. *Sejam $a, m, n \in \mathbb{Z}$ com $m > 1$, $n > 0$ e $(a,m) = 1$. Segue que, $a^n \equiv 1 \mod m$ se, e somente se, $ord_m(a) \mid n$.*

Demonstração: Suponha que $a^n \equiv 1 \mod m$. Sabemos pela divisão Euclidiana que existem q e r inteiros, com $0 \leq r < ord_m(a)$ tal que $n = ord_m(a) \cdot q + r$.

Suponha por absurdo que $r \neq 0$. Veja agora que,

$$a^n = a^{ord_m(a)\cdot q + r} \equiv 1 \mod m.$$

Por outro lado, sabemos pela definição de $ord_m(a)$, que

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

Elevando ambos os lados a q, temos,

$$a^{ord_m(a)\cdot q} \equiv 1^q \mod m.$$

Multiplicando agora por a^r, segue que,

$$a^n = a^{ord_m(a)\cdot q + r} \equiv a^r \equiv 1 \mod m.$$

Portanto, $m \mid a^r - 1$, o que é um absurdo, pois $0 < r < ord_m(a)$ e $ord_m(a)$ é, por definição, o menor número positivo com tal propriedade.

Reciprocamente, suponha que $ord_m(a) \mid n$, logo existe um q inteiro tal que $n = ord_m(a) \cdot q$. Por definição temos que,

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

elevando ambos os lados a q obtemos,

$$a^n = a^{ord_m(a)\cdot q} \equiv 1^q \equiv 1 \mod m.$$

■

Capítulo 3

Números primos

O presente capitulo foi divido em três seções. Na primeira seção, exploraremos a infinidade dos números primos, na segunda, abordaremos alguns testes de primalidade e, por fim, na terceira, estudaremos a relação dos números de Mersenne e de Fermat com números primos.

3.1 Infinidade dos números primos

Nessa seção, apresentaremos algumas demonstrações interessantes para um dos teoremas mais importantes da aritmética: O Teorema da Infinitude dos Números Primos. Tais demonstrações podem ser encontradas em [2] e [6]. O Teorema citado possui o seguinte enunciado:

Teorema 12. *Existem infinitos números primos.*

3.1.1 Demonstração de Euclides

A demonstração seguinte é devida a Euclides e foi publicada originalmente na sua obra *Os Elementos*.

Demonstração: Suponha que exista uma quantidade finita de números primos. Neste caso, podemos supor que $p_1, \ldots, p_r$ sejam todos os números primos que existem. Veja que $n = p_1 \cdot \ldots \cdot p_r + 1$ é maior que todos os números primos listados, logo, n é composto e, consequentemente, divisível por algum p_i, com $i \in \{1, 2, \ldots, r\}$. Como $p_i \mid p_1 \cdot \ldots \cdot p_r$ e $p_i \mid n$ segue, pela Proposição 3, que $p_i \mid 1$, o que é um absurdo. Concluímos assim que existem infinitos números primos. ■

3.1.2 Demonstração de Goldbach

Em 1730 o matemático Christian Goldbach enviou a Euler uma carta contendo uma demonstração para o Teorema 12, onde eram utilizadas sequências de núme-

ros coprimos, porém antes de apresentá-la aqui, precisamos definir algumas ideias iniciais.

Para esta demonstração considere a sequência de números $F_n = 2^{2^n} + 1$, para $n \geq 0$ inteiro. Tal sequência é conhecida como os números de Fermat, dedicaremos a Seção 3.3 para dissertar sobre esses números.

É possível demonstrar, faremos na Seção 3.3, que $F_n - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1}$, utilizaremos esse fato como verdade na demonstração que segue.

Demonstração: Considere $m < n$, logo, $F_m \mid F_0 \cdot F_1 \cdot \ldots \cdot F_m \cdot \ldots \cdot F_{n-1}$, ou seja, $F_m \mid F_n - 2$. Suponha, por absurdo, que exista um número primo p que divida F_m e F_n. Se $p \mid F_m$ então $p \mid F_n - 2$, o que implica que $p \mid 2$, uma vez que $p \mid F_n$. Sendo p primo, temos que $p = 2$, o que é um absurdo, pois p divide F_m e F_n que são ímpares.

Concluímos, assim, que não existe número primo p tal que $p \mid F_n$ e $p \mid F_m$, com m diferente de n, ou seja, $(F_m, F_n) = 1$.

Sendo $F_0, F_1, F_2, \ldots, F_n, \ldots$ uma sequência infinita de números primos entre si, dois a dois, se p é fator primo de F_0, p_1 é fator de $F_1, ..., p_n$ é fator de $F_n, \ldots$, então $p, p_1, p_2, \ldots, p_n, \ldots$ são todos distintos, o que prova que existem infinitos números primos. ■

É importante observar que para tal demonstração não é necessária a utilização dos números de Fermat, mas apenas de uma sequência infinita de números naturais, tal que seus termos sejam primos entre si, dois a dois.

3.1.3 Demonstração de Euler

Para a demonstração que se segue, partiremos da ideia de que o leitor já possui familiaridade com séries.

Demonstração: Suponha, por absurdo, que a quantidade de números primos é finita e que $p_1, \ldots, p_r$ sejam todos eles. Veja agora que $1/p_i < 1$, para $i = 1, 2, \ldots, r$, logo, a soma dos termos da progressão geométrica infinita de razão $1/p_i$ é dada por,

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1 - \frac{1}{p_i}}.$$

Ao multiplicarmos, membro a membro, todas as igualdades para $i = 1, 2, \ldots, r$, obtém-se que,

$$\prod_{i=1}^{r} \left(\sum_{k=0}^{\infty} \frac{1}{p_i^k} \right) = \prod_{i=1}^{r} \left(\frac{1}{1 - \frac{1}{p_i}} \right).$$

Efetuando-se as operações do primeiro membro da igualdade, teremos, de acordo com o Teorema Fundamental da Aritmética, a soma dos inversos de todos os números

naturais, cada um contado um única vez. Desta forma,

$$\prod_{i=1}^{r}\left(\sum_{k=0}^{\infty}\frac{1}{p_i^k}\right)=\sum_{n=1}^{\infty}\frac{1}{n}.$$

E consequentemente,

$$\sum_{n=1}^{\infty}\frac{1}{n}=\prod_{i=1}^{r}\left(\frac{1}{1-\frac{1}{p_i}}\right).$$

É sabido que o primeiro membro da igualdade trata-se de um série divergente, onda a soma é infinita, porém o segundo membro trata-se de um produto com r fatores e cujo resultado é obviamente finito. Tal igualdade é um absurdo.

Concluímos, assim, que existem uma infinidade de números primos. ■

3.1.4 Demonstração de Métrod

A demonstração de Métrod, de 1917, têm muita semelhança com a dada por Euclides, como podemos ver a seguir.

Demonstração: Suponha que existam apenas r números primos, e sejam eles, $p_1 < p_2 < \ldots < p_r$. Considere,

$$S_i=\frac{p_1\cdot p_2\cdot\ldots\cdot p_r}{p_i},\ i=1,2,\ldots r$$

e

$$S=\sum_{i=1}^{r}S_i.$$

Veja que se S é composto então $p_i \mid S$ para algum $i=1,2,\ldots r$. Se S é primo então $S=p_i$ para algum i, o que também significa que $p_i \mid S$.

Note que $p_i \mid S_j$ sempre que $i \neq j$, mas $p_i \nmid S_i$. Logo não existe p_i tal que $p_i \mid S$, pois $p_i \mid S_1+\ldots+S_{i-1}+S_{i+1}+\ldots+S_r$, mas $p_i \nmid S_i$.

Concluímos assim que o número de primos não podem ser finito. ■

3.2 Testes de Primalidade

Diante da infinidade dos números primos e da ausência de fórmulas para encontrá-los surge a necessidade de testes capazes de terminar se um determinado número é primo ou composto. Para atender tal ponto dedicaremos esta sessão ao estudo de alguns testes de primalidade para números quaisquer, tendo como fonte de pesquisa os livros [2], [7], [8] e [6].

3.2.1 Crivo de Eratóstenes

Por volta de 230 a.C, Eratóstenes desenvolveu o primeiro método sistemático de verificação sobre a primalidade de um número natural qualquer, método esse que ficou conhecido como crivo de Eratóstenes, sendo considerado um dos principais resultados obtidos na antiguidade sobre números primos, assim como afirma Eves (2011, p. 623) "Os principais resultados obtidos na Antiguidade foram a prova da infinidade dos primos e o crivo de Eratóstenes para determinar os primos inferiores a um inteiro dado n".

Para entendermos como funciona o crivo de Eratóstenes iremos, agora, por meio do seu uso, determinar todos os números primos até 100.

Começamos escrevendo todos os números em sua ordem natural de 2 até o 100. Como mostra a tabela abaixo.

Tabela 3.1: Números naturais de 2 a 100.

	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

Fonte: Autor.

Devemos agora riscar todos os múltiplos de 2, maiores que 2.

Tabela 3.2: Múltiplos de 2, maiores que ele, riscados.

	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~~

Fonte: Autor.

Repetimos o processo com o próximo número não riscado, no caso o 3. Após isso, o número seguinte não riscado será o 5 e mais uma vez repetimos o processo. Seguindo com este raciocínio para todos os números não riscados após o 5. Ao finalizar obtemos a Tabela 3.3, onde restam apenas números primos.

Tabela 3.3: Números primos até 100.

	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~~

Fonte: Autor.

Veja que esse teste não apenas responde se o número 100 é primo, mas também apresenta todos os primos de 1 a 100. Porém, é importante observar que se a intenção é apenas determinar se 100 é primo ou composto, o Lema 4, que apresentaremos a seguir, se mostra mais prático.

Ao utilizarmos o crivo para encontrar os primos até o 100, pode-se perceber que após riscarmos os múltiplos de 7, os números que sobram são todos números primos. Logo é natural o questionamento: É necessário continuar o processo até qual número?

A resposta pode ser obtida a partir do lema abaixo, o mesmo é devido a Eratóstenes.

Lema 4. *Seja $n \in \mathbb{N}$, com $n > 1$. Se n não é divisível por nenhum número primo p, que satisfaça a condição $p^2 \leq n$, então n é primo.*

Demonstração: Suponha, por absurdo, que n seja composto, isto é, não seja primo e não seja divisível por nenhum número primo p, tal que $p^2 \leq n$.

Sendo n um número composto, existe ao menos um número primo que divide n, chamemos de q o menor destes primos. Como $q \mid n$, então existe um $r \in \mathbb{N}$ tal que $n = q.r$, o que significa que $r \mid n$. Note que $q \leq r$, pois q é o menor número primo que divide n, logo, $q^2 \leq q \cdot r = n$. O que é um absurdo, pois, por hipótese, n não é divisível por nenhum primo com tal propriedade. ■

O Lema 4 nos fornece um método para verificar se um número qualquer é primo ou composto. Por exemplo, para determinar se 97 é primo precisamos apenas verificar se 97 é divisível por $2, 3, 5$ ou 7, uma vez que o número primo seguinte a 7 é 11 e $11^2 = 121 > 97$. Como $2, 3, 5$ e 7 não dividem 97, podemos concluir que 97 é primo. Uma observação importante é que o lema em questão pode se tornar mais prático quando aplicado em conjunto com critérios de divisibilidade.

Por sua simplicidade, esse teste é muito interessante para alunos da educação básica, porém o mesmo pode se tornar extremamente trabalhoso se tentarmos verificar a primalidade de grandes números. Quando tentamos verificar a primalidade de 135457, por exemplo, começamos a entender suas limitações, pois precisamos conhecer os números primos p tais que $p^2 \leq 135457$, ou seja, os primos até $368 \leq \sqrt{135457}$ e verificar se 135457 é divisível por algum deles, o que está longe de ser prático.

3.2.2 Teorema de Wilson

Antes de enunciar o Teorema de Wilson, precisamos estudar algumas proposições sobre congruências.

Proposição 19. *Sejam $a, m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1 \mod m$, possui solução se, e só se, $(a, m) = 1$. Além disso, suponha que x_0 é solução de $aX \equiv 1 \mod m$, então temos que x é solução de $aX \equiv 1 \mod m$ se, e somente se, $x_0 \equiv x \mod m$.*

Demonstração: Veja que x_0 é solução de $aX \equiv 1 \mod m$ se, e só se, $m \mid ax_0 - 1$, ou seja se, e só se, existe um y inteiro, tal que $ax - 1 = my$, ou ainda, $ax - my = 1$. Pela Proposição 7, existe y tal que $ax - my = 1$ se, e somente se, $(a, m) = 1$. Portanto, $aX \equiv 1 \mod m$, possui solução se, e só se, $(a, m) = 1$. Provando assim a primeira parte da proposição.

Para a segunda parte, note que se x_0 e x são soluções de $aX \equiv 1 \mod m$, então $ax_0 \equiv ax \mod m$, daí sendo $(a, m) = 1$ então $x_0 \equiv x \mod m$.

Suponha agora que x_0 é uma solução de $aX \equiv 1 \mod m$ e $x_0 \equiv x \mod m$. Teríamos, assim, que $ax_0 \equiv ax \equiv 1 \mod m$. Logo x é também solução. Terminando assim a prova da proposição. ■

Como as soluções de $aX \equiv 1 \mod m$ são todas congruentes módulo m, teremos uma solução única no conjunto $\{1, \ldots, m-1\}$, uma vez que os elementos deste conjunto são dois a dois incongruentes modulo m.

Definição 14. *As soluções de $aX \equiv 1 \mod m$, com $(a, m) = 1$ são chamadas de inversos de a.*

Proposição 20. *Sejam $a, p \in \mathbb{Z}$ com p primo. Temos que a é o seu próprio inverso módulo p se, e só se, $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$.*

Demonstração: Se a é seu próprio inverso, então $a^2 \equiv 1 \mod p$, logo, $p \mid a^2 - 1$. Veja que $a^2 - 1 = (a-1)(a+1)$, daí, como p é primo, temos que $p \mid a-1$ ou $p \mid a+1$, o que implica que $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$.

Considere agora que $a \equiv 1 \mod p$ ou $a \equiv -1 \mod p$, isso significa que, $p \mid a-1$ ou $p \mid a+1$. Logo, $p \mid (a-1)(a+1)$, o que por sua vez, implica que $a^2 \equiv 1 \mod p$. ■

Teorema 13. *(Teorema de Wilson) Seja p um número inteiro com $p \geq 2$. Tem-se que p é primo se, e somente se, $(p-1)! \equiv -1 \mod p$.*

Demonstração: Se $p = 2$ o resultado é obviamente válido. Iremos considerar então $p > 2$. Sabemos, pela Proposição 19, que para todo $a \in \{1, 2, 3, \ldots, p-1\}$ a congruência $aX \equiv 1 \mod p$ possui solução, uma vez que $(a, p) = 1$. Temos ainda que, para $X \in \{1, 2, 3, \ldots, p-1\}$ a solução é única.

Note agora que os únicos elementos do conjunto $\{1, 2, 3, \ldots, p-1\}$ que satisfazem a Proposição 20 são 1 e $p-1$, logo, apenas eles são seus próprios inversos. Podemos então agrupar os $p-3$ elementos do conjunto $\{2, 3, \ldots, p-2\}$ em $\frac{p-3}{2}$ pares, de modo que sejam um inverso do outro, ou seja, que seu produto seja congruente a 1 módulo p. Desta forma, ao multiplicarmos, membro a membro, as congruências obtidas, teremos

$$2 \cdot 3 \cdot \ldots \cdot p - 2 \equiv 1^{\frac{p-3}{2}} \mod p. \tag{3.1}$$

Multiplicando ambos os lados por $p-1$, concluímos que $(p-1)! \equiv (p-1) \equiv -1 \mod p$.

Reciprocamente, suponha que $(p-1)! \equiv -1 \mod p$, mas p não é primo. Como, por hipótese, p é composto, então existem $r, s \in \mathbb{Z}$, com $1 < r < p$ e $1 < s < p$, tais que $p = r \cdot s$. Note que, $(p-1)! \equiv -1 \mod p$ equivale dizer que $p \mid (p-1)! + 1$, daí, como $r \mid p$, então $r \mid (p-1)! + 1$.

Sendo $r < p$ então existe um t natural tal que $p - t = r$. Logo, $r \mid (p-1)!$, uma vez que $(p-1)! = (p-1) \ldots (p-t) \ldots 2$.

Mas se $r \mid (p-1)! + 1$ e $r \mid (p-1)!$ então $r \mid 1$, o que é um absurdo, pois $r > 1$. Portanto, p é primo. ■

Através do Teorema de Wilson é possível determinar se um dado número é primo ou não. Vejamos alguns exemplos:

Exemplo 6. *Verifique se são primos os seguintes números:*

a) 7

b) 13

Solução:

a) Note que,

$$(7-1)! = 6! = 720 \equiv -1 \mod 7.$$

Logo, pelo Teorema de Wilson, 7 é primo.

b) Veja que,

$$\begin{aligned} 12 &\equiv -1 \mod 13, \\ 12 = 2 \cdot 6 &\equiv -1 \mod 13, \\ 12 = 3 \cdot 4 &\equiv -1 \mod 13, \\ 5 \cdot 8 &\equiv 1 \mod 13, \\ 7 \cdot 11 &\equiv -1 \mod 13, \end{aligned}$$

e

$$9 \cdot 10 \equiv -1 \mod 13.$$

Multiplicando todas a congruências, temos que

$$12! \equiv -1 \mod 13.$$

Concluímos, assim, que 13 é um número primo.

Assim como no crivo de Eratóstenes o Teorema de Wilson pode tornar-se muito trabalhoso para números com muitas casas decimais.

3.2.3 Testes de Lucas

O pré-teste de primalidade que definimos no Capítulo 2 (Corolário 5), será de grande utilidade nos próximos testes, por este motivo, o reescreveremos utilizando agora noções de congruência.

Proposição 21. *(Pré-teste de primalidade) Sejam a, p números inteiros, com $p > 2$ e $(p, a) = 1$. Se $a^{p-1} \not\equiv 1 \mod p$ então p é composto.*

Nos testes 1, 2 e 3, apresentados a seguir, supõe-se a existência de um inteiro $a > 1$ tal que $a^{n-1} \equiv 1 \mod n$, para $n > 1$ natural. Sabemos, pela Proposição 19, que $a \cdot X \equiv 1 \mod n$, com X inteiro, possui solução, se, e só se, $(a, n) = 1$. Desta forma $a \cdot a^{n-2} \equiv 1 \mod n$ só é possível se, $(a, n) = 1$, pois a^{n-2} é, nesse caso, uma solução de $a \cdot X \equiv 1 \mod n$. Logo, devemos sempre tomar $(a, n) = 1$, e caso $a^{n-1} \not\equiv 1 \mod n$, poderemos concluir, pela Proposição 21, que n é composto. Para uma melhor compreensão veja o exemplo abaixo.

Exemplo 7. *Verifique se 253 é primo:*

Solução: Observe que,

$$\begin{aligned} 2^8 \equiv 3 \mod 253 \;&\Rightarrow\; 2^{40} = (2^8)^5 \equiv 3^5 \equiv -10 \mod 253 \\ &\Rightarrow\; 2^{120} = (2^{40})^3 \equiv (-10)^3 \equiv 12 \mod 253 \\ &\Rightarrow\; 2^{240} = (2^{120})^2 \equiv 144 \mod 253. \end{aligned} \tag{3.2}$$

Veja também que,

$$2^{10} \equiv 12 \mod 253 \Rightarrow 2^{12} \equiv 48 \mod 253. \tag{3.3}$$

Multiplicando as congruências (3.2) e (3.3) obtemos

$$2^{252} \equiv 81 \mod 253.$$

Como $(2, 253) = 1$ e $2^{252} \not\equiv 1 \mod 253$ concluímos, pelo pré-teste de primalidade, que 253 é composto.

Pelo pré-teste de primalidade, sabemos que uma condição necessária para p ser primo é $(p, a) = 1$ e $a^{p-1} \equiv 1 \mod p$, contudo, essa condição não é suficiente, ou seja, um número p pode satisfazer essas duas hipóteses e não ser primo, pois pode

se tratar de um pseudoprimo na base a. Por mais que o pré-teste não garanta que p seja primo, alguns dados nos mostram que esse pode ser um forte indicativo de que p é primo. Até 10000, por exemplo, existem 1251 números p tais que, $(p, 2) = 1$ e $2^{p-1} \equiv 1 \mod p$, destes apenas 22 não são primos, logo, a probabilidade de p ser primo nesse caso é de $\frac{1229}{1251} \cong 98,24\%$. Se além disso tivermos também $(p, 3) = 1$ e $3^{p-1} \equiv 1 \mod p$ a probabilidade sobe para $\frac{1229}{1236} \cong 99,43\%$, tendo em vista que apenas 7 números que satisfazem as duas condições não são primos.

Por isso, o pré-teste em questão é apresentado em muitos trabalhos como um teste de primalidade probabilístico, porém, como ele não é um teste conclusivo, os testes seguintes se fazem necessários para garantir de forma precisa se um número p é primo.

O Teste 1, apresentado a seguir, é considerado como uma recíproca do Pequeno Teorema de Fermat (veja Teorema 8) e foi descoberto pelo matemático François Édouard Anatole Lucas em 1876.

Teste 1. *Seja $n > 1$ um número inteiro. Supõe-se que exista um inteiro $a > 1$ tal que:*

i) $a^{n-1} \equiv 1 \mod n$;

ii) $a^m \not\equiv 1 \mod n$, *para* $m = 1, 2, \ldots, n-2$.

Então n é primo.

Demonstração: Suponha que exista um $a > 1$ inteiro que satisfaz i) e ii). Temos assim que $ord_n(a) = n - 1$. Note agora que, $n \mid a^{n-1} - 1$, logo, existe um inteiro q tal que $a^{n-1} - 1 = n \cdot q$, o que implica que, $a \cdot (a^{n-2}) - nq = 1$ e, pela Proposição 7, $(a, n) = 1$.

Sendo $(a, n) = 1$ segue, pelo Teorema de Euler, que $a^{\varphi(n)} \equiv 1 \mod n$ e pelo Lema 3, $n - 1 \mid \varphi(n)$ uma vez que $ord_n(a) = n - 1$.

Por fim, como $0 < \varphi(n) \leq n - 1$ então $n - 1 = \varphi(n)$. Concluímos assim que n é primo. ■

Observe que a aplicação do Teste 1 não é prática nem mesmo para números inferiores a 100, como mostraremos no exemplo a seguir. Sua falta de praticidade, em relação aos testes seguintes, deve-se a necessidade de determinar r tal que $a^m \equiv r \mod n$, para $m = 1, 2, \ldots, n-2$.

Exemplo 8. *Verifique se 17 é primo:*

Solução: Tomaremos $a = 2$, pois $2 > 1$ e $(2, 17) = 1$. Veja que,

$$2^4 \equiv -1 \mod 17.$$

Elevando ambos os lados a 4, obtemos,

$$2^{16} = 2^{17-1} \equiv (-1)^4 \equiv 1 \mod 17.$$

Logo, 17 satisfaz o item *i)* do Teste 1.

Para o item *ii)*, precisamos determinar r tal que $2^m \equiv r \mod 17$. Para isso, iremos analisar cada caso, tomando $m = 1, 2, \ldots, 15$. Veja:

$$\begin{aligned}
2^1 = 2 &\equiv 2 \mod 17,\\
2^2 = 4 &\equiv 4 \mod 17,\\
2^3 = 8 &\equiv 8 \mod 17,\\
2^4 = 16 &\equiv 16 \mod 17,\\
2^5 = 32 &\equiv 15 \mod 17,\\
2^6 = 64 &\equiv 13 \mod 17,\\
2^7 = 128 &\equiv 9 \mod 17,
\end{aligned}$$

e

$$2^8 = 256 \equiv 1 \mod 17.$$

Como $2^8 = 256 \equiv 1 \mod 17$, o teste se mostra inconclusivo. Verificaremos agora o teste para $a = 3$. Para isso, temos:

$$3^5 = 243 \equiv 5 \mod 17 \Rightarrow 3^{15} \equiv 5^3 \equiv 6 \mod 17 \Rightarrow 3^{16} \equiv 6 \cdot 3 \equiv 1 \mod 17.$$

Portanto o item *i)* é satisfeito. Para verificar o item *ii)*, precisamos determinar r tal que $3^m \equiv r \mod 17$, para $m = 1, 2, \ldots, 15$. Observe:

$$\begin{aligned}
3^1 &\equiv 3 \mod 17,\\
3^2 &\equiv 9 \mod 17,\\
3^3 &\equiv 10 \mod 17,\\
3^4 &\equiv 13 \mod 17,\\
3^5 &\equiv 5 \mod 17,\\
3^5 \equiv 5 \mod 17 &\Rightarrow 3^6 \equiv 5 \cdot 3 \equiv 15 \mod 17,\\
3^5 \equiv 5 \mod 17 &\Rightarrow 3^7 \equiv 5 \cdot 3^2 \equiv 11 \mod 17,\\
3^5 \cdot 3^4 \equiv 5 \cdot 10 \mod 17 &\Rightarrow 3^8 \equiv 16 \mod 17,\\
3^3 \equiv 10 \mod 17 &\Rightarrow 3^9 \equiv 10^3 \equiv 14 \mod 17,\\
3^5 \equiv 5 \mod 17 &\Rightarrow 3^{10} \equiv 5^2 \equiv 8 \mod 17,\\
3^{10} \equiv 8 \mod 17 &\Rightarrow 3^{11} \equiv 8 \cdot 3 \equiv 7 \mod 17,\\
3^{11} \equiv 7 \mod 17 &\Rightarrow 3^{12} \equiv 7 \cdot 3 \equiv 4 \mod 17,\\
3^{12} \equiv 4 \mod 17 &\Rightarrow 3^{13} \equiv 4 \cdot 3 \equiv 12 \mod 17,\\
3^{13} \equiv 12 \mod 17 &\Rightarrow 3^{14} \equiv 12 \cdot 3 \equiv 2 \mod 17,
\end{aligned}$$

e

$$3^{14} \equiv 2 \mod 17 \Rightarrow 3^{15} \equiv 2 \cdot 3 \equiv 6 \mod 17.$$

Como em nenhum caso $r = 1$ então o item *ii)* do Teste 1 é satisfeito. Concluímos assim, pelo Teste 1, que 17 é primo.

Em 1891 Lucas reformulou o Teste 1. O resultado obtido é apresentado no Teste 2.

Teste 2. *Seja $n > 1$ inteiro. Supõe-se que exista um inteiro $a > 1$, tal que:*

i) $a^{n-1} \equiv 1 \mod n$;

ii) $a^m \not\equiv 1 \mod n$, *para m natural, onde $m < n-1$ e $m \mid n-1$.*

Então n é primo.

Demonstração: Suponha que exista um $a > 1$ inteiro que satisfaz *i)* e *ii)*.

Como $a^{n-1} \equiv 1 \mod n$ então $n \mid a^{n-1} - 1$, ou seja, existe um inteiro q tal que $a^{n-1} - 1 = n \cdot q$, logo, $a \cdot (a^{n-2}) - n \cdot q = 1$ e, consequentemente, $(a, n) = 1$.

Pelo fato de $(a, n) = 1$, segue, pelo Lema 3, que $ord_n(a) \mid n-1$. Veja que $ord_n(a)$ não pode ser menor que $n-1$, pois, pelo item *ii)*, para todo $m < n-1$ com m divisor de $n-1$ temos que $a^m \not\equiv 1 \, mod, n$. Portanto, $ord_n(a) = n-1$.

Ainda pelo de fato de $(a, n) = 1$ segue, pelo Teorema de Euler, que $a^{\varphi(n)} \equiv 1 \mod n$. Temos assim que $ord_n(a) \mid \varphi(n)$, onde $0 < \varphi(n) \leq n - 1$. Sendo $ord_n(a) = n - 1$, concluímos que $\varphi(n) = n - 1$, o que significa que n é primo. ■

O Teste 2 apresenta uma evolução em comparação ao Teste 1, pois agora precisamos determinar r tal que $a^m \equiv r \mod n$, para $0 < m < n - 1$ e tal que $m \mid n - 1$ ao invés de tomar $m = 1, 2, \ldots, n - 2$, o que significa uma redução no número de congruências que precisaremos trabalhar. Porém não podemos deixar de ressaltar que, em contrapartida, surge a necessidade de determinar os divisores de $n - 1$.

Veja os dois exemplos seguintes.

Exemplo 9. *Verifique se* 17 *é primo.*

Solução: Pelo Exemplo 8, sabemos que o item *i)* do Teste 2 é satisfeito para $a = 3$.

Precisamos agora determinar os divisores m com, $0 < m < 16$, de $17 - 1 = 16$. Para isto, veja que $16 = 2^4$, logo, os divisores procurados são $2^0 = 1$, $2^1 = 2$, $2^2 = 4$ e $2^3 = 8$. Pelo Exemplo 8, sabemos que

$$\begin{aligned} 3^1 &\equiv 3 \mod 17, \\ 3^2 &\equiv 9 \mod 17, \\ 3^4 &\equiv 13 \mod 17, \end{aligned}$$

e

$$3^8 \equiv 16 \mod 17.$$

Portanto, pelo Teste 2, 17 é primo.

Exemplo 10. *Verifique se 109 é primo ou composto.*

Solução: Tomaremos $a = 6$. Veja que,

$$\begin{aligned} 6^3 &\equiv -2 \mod 109, \\ 6^{18} = 6^{3 \cdot 6} &\equiv (-2)^6 \equiv 64 \mod 109, \\ 6^{36} = 6^{18 \cdot 2} &\equiv 64^2 \equiv 63 \mod 109, \end{aligned}$$

e

$$6^{108} = 6^{36 \cdot 3} \equiv 63^3 \equiv 1 \mod 109.$$

Logo, o item *i)* do Teste 2 é satisfeito.

Precisamos agora determinar m tal que $m \mid 108$ e $0 < m < 108$. Sendo $108 = 2^2 \cdot 3^3$, seus divisores que satisfazem as condições de m, são dados por $2^t \cdot 3^s$, com $t = 0, 1, 2$ e $s = 0, 1, 2, 3$, donde obtemos os seguintes resultados:

$$\begin{aligned}
2^0 \cdot 3^0 &= 1, \\
2^1 \cdot 3^0 &= 2, \\
2^2 \cdot 3^0 &= 4, \\
2^0 \cdot 3^1 &= 3, \\
2^1 \cdot 3^1 &= 6, \\
2^2 \cdot 3^1 &= 12, \\
2^0 \cdot 3^2 &= 9, \\
2^1 \cdot 3^2 &= 18, \\
2^2 \cdot 3^2 &= 36, \\
2^0 \cdot 3^3 &= 27,
\end{aligned}$$

e

$$2^1 \cdot 3^3 = 54.$$

Iremos agora determinar r tal que $6^m \equiv r \mod 109$, para $m = 1, 2, 3, 4, 6, 9, 12, 18, 27, 36, 54$. Para isto, utilizaremos o fato de que $6^3 \equiv -2 \mod 109$. Observe:

$$\begin{aligned}
6^1 &\equiv 6 \mod 109, \\
6^2 &\equiv 36 \mod 109, \\
6^3 = 216 &\equiv 107 \mod 109, \\
6^4 = 1296 &\equiv 97 \mod 109, \\
6^5 = 7776 &\equiv 37 \mod 109, \\
6^3 \equiv (-2) \mod 109 &\Rightarrow 6^6 \equiv (-2)^2 \equiv 4 \mod 109, \\
6^3 \equiv (-2) \mod 109 &\Rightarrow 6^9 \equiv (-2)^3 \equiv 101 \mod 109, \\
6^3 \equiv (-2) \mod 109 &\Rightarrow 6^{12} \equiv (-2)^4 \equiv 16 \mod 109, \\
6^3 \equiv (-2) \mod 109 &\Rightarrow 6^{18} \equiv (-2)^6 \equiv 64 \mod 109, \\
6^3 \equiv (-2) \mod 109 &\Rightarrow 6^{27} \equiv (-2)^9 \equiv 33 \mod 109, \\
6^3 \equiv (-2) \mod 109 &\Rightarrow 6^{36} \equiv (-2)^{12} \equiv 63 \mod 109,
\end{aligned}$$

e

$$6^3 \equiv (-2) \mod 109 \Rightarrow 6^{54} \equiv (-2)^{18} \equiv 108 \mod 109.$$

Percebemos assim que 109 satisfaz o item *ii)* do Teste 2. Portanto, pelo Teste 2, 109 é primo.

O leitor pode perceber, que mesmo com uma redução no número de congruências, em comparação ao Teste 1, o Teste 2 é ainda muito trabalhoso.

Em 1967 os matemáticos John Brillhart e John L. Selfridge, modificaram os testes de Lucas tornando-os mais práticos. Veja o teste seguinte.

Teste 3. *Seja $n > 1$ um número inteiro. Supõe-se que, para todo fator primo p de $n-1$, exista um inteiro $a > 1$, tal que:*

i) $a^{n-1} \equiv 1 \mod n$

ii) $a^{\frac{n-1}{p}} \not\equiv 1 \mod n$

Então n é primo.

Demonstração: Suponha, por absurdo, que n satisfaz *i)* e *ii)*, mas não é primo.

Como n é composto, então $\varphi(n) \neq n-1$. Daí, $\varphi(n) < n-1$ o que implica que $n-1 \nmid \varphi(n)$, o que significa por sua vez que existe um primo p tal que $p^r \mid n-1$ e $p^r \nmid \varphi(n)$, para algum $r \in \mathbb{N}$. Veja agora que, $a^{n-1} \equiv 1 \mod n$, ou seja, $n \mid a^{n-1}-1$, logo existe um inteiro t tal que $a^{n-1}-1 = nt$ que é equivalente a $a(a^{n-2}) - nt = 1$, temos assim, pela Proposição 7, que $(a,n) = 1$, o que nos leva a concluir, pelo Lema 3, que $ord_n(a) \mid n-1$ e $ord_n(a) \nmid \dfrac{n-1}{p}$, uma vez que n satisfaz *i)* e *ii)*.

Note que, $ord_n(a) \mid n-1$ garante a existência de um inteiro q tal que $n-1 = ord_n(a) \cdot q$, dessa forma,

$$p^r \mid n-1 \Rightarrow p^r \mid ord_n(a) \cdot q \Rightarrow p^{r-1} \mid \frac{ord_n(a) \cdot q}{p}.$$

Por outro lado,

$$ord_n(a) \nmid \frac{n-1}{p} \Rightarrow ord_n(a) \nmid \frac{ord_n(a) \cdot q}{p} \Rightarrow ord_n(a) \nmid \frac{q}{p} \cdot ord_n(a).$$

O que significa que $\dfrac{q}{p}$ não é inteiro, logo, $p \nmid q$ com isso $(p,q) = 1 = (p^r, q)$. Pelo fato de $p^r \mid ord_n(a) \cdot q$ e $(p^r, q) = 1$ segue, pelo Teorema 3, que $p^r \mid ord_n(a)$.

Sendo $(a,n) = 1$ temos, pelo Teorema de Euler, que $a^{\varphi(n)} \equiv 1 \mod n$ e, pelo Lema 3, $ord_n(a) \mid \varphi(n)$, implicando assim que $p^r \mid \varphi(n)$, o que é um absurdo.

Concluímos assim que n não pode ser composto, portanto, n é primo. ■

Podemos perceber que o Teste 3 apresenta uma grande vantagem em relação ao Teste 2, pois o número de fatores primos na decomposição de $n-1$ sempre será menor ou igual ao número de divisores positivos de $n-1$, desconsiderando o próprio

$n-1$, o que representa, na prática, uma diminuição no número de congruências a se trabalhar. Veja os exemplos seguintes, para uma melhor comparação com os testes 1 e 2.

Exemplo 11. *Verifique se 17 é primo.*

Solução: Tomaremos $a = 3$. Pelo exemplo 8, sabemos que $3^{16} \equiv 1 \mod 17$. Logo, o item *i)* do Teste 3 é satisfeito.

Note agora que, $17 - 1 = 16 = 2^4$, logo, 16 apresenta um único fator primo, no caso o número 2. Basta então determinar r, tal que $3^{\frac{17-1}{2}} = 3^8 \equiv r \mod 17$. Pelo exemplo 8, temos que $3^8 \equiv 16 \mod 17$. Portanto, o item *ii)* é satisfeito, o que implica que 17 é primo.

Exemplo 12. *Determine se 109 é primo ou composto.*

Solução: Tomaremos $a = 6$. Pelo exemplo 10, sabemos que $6^{108} \equiv 1 \mod 109$, ou seja, o item *i)* é satisfeito.

Note que, $108 = 2^2 \cdot 3^3$, logo seus fatores primos são 2 e 3, precisamos assim determinar r_1 e r_2 tal que,

$$6^{\frac{109-1}{2}} = 6^{54} \equiv r_1 \mod 109$$

e

$$6^{\frac{109-1}{3}} = 6^{36} \equiv r_2 \mod 109.$$

Pelo exemplo 10, sabemos que $6^{36} \equiv 63 \mod 109$ e $6^{54} \equiv 108 \mod 109$. Portanto o item *ii)* é satisfeito e com isso concluímos que 109 é primo.

É importante ressaltar que o resultado inconclusivo obtido no Exemplo 8 não é algo restrito ao Teste 1, podendo acontecer também nos testes 2 e 3. Esse fato só evidencia a deficiência que existe atualmente em testes eficazes para determinação da primalidade de números quaisquer.

3.3 Números primos especiais

Apresentaremos nesta sessão alguns números de formas específicas e suas curiosas relações com os números primos. Tomaremos como embasamento teórico as obras [2] e [6].

3.3.1 Números de Fermat

Chamamos de números de Fermat os números que podem ser escritos sob a forma $F_n = 2^{2^n} + 1$, para $n \geq 0$ inteiro.

Fermat acreditava, como foi descrito em uma carta enviada a Mersenne em 1640, que esses números eram todos primos. Sua hipótese pode ter considerado o fato de $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ serem todos primos, porém não se sabe ao certo se haviam outros motivos para tal hipótese.

Apenas em 1732 provou-se que a hipótese de que todos os números de Fermat eram primos, é falsa. Euler apresentou, nesse mesmo ano, uma decomposição para $F_5 = 4.294.967.297 = 641 \cdot 6700417$, provando assim que trata-se de um número composto.

A demora para comprovar que F_5 é composto, não se deve a dificuldade de calcular $2^{2^5} + 1$, mas sim da falta de critérios de primalidade eficientes para testar sua natureza.

Em 1877 o matemático Jean François Théophile Pépin, formulou, utilizando o Teste 1 de Lucas, um critério de primalidade específico para os números de Fermat, que ficou conhecido como teste de Pepin.

Teste de Pepin: *Seja* $F_n = 2^{2^n}+1$, *com* $n > 0$ *inteiro. Se* $3^{\frac{F_n-1}{2}} \equiv -1 \mod F_n$ *então* F_n *é primo.*

Demonstração: Note que $F_n - 1 = 2^{2^n}$, logo $F_n - 1$ possui apenas o número 2 como fator primo. Veja agora que,

$$\begin{aligned} 3^{\frac{F_n-1}{2}} \equiv -1 \mod F_n \quad &\Rightarrow \quad \left(3^{\frac{F_n-1}{2}}\right)^2 \equiv (-1)^2 \mod F_n \\ &\Rightarrow \quad 3^{F_n-1} \equiv 1 \mod F_n. \end{aligned}$$

Obviamente se $3^{\frac{F_n-1}{2}} \equiv -1 \mod F_n$ então $3^{\frac{F_n-1}{2}} \not\equiv 1 \mod F_n$. Temos assim que F_n satisfaz os itens *i)* e *ii)* do teste 3, portanto F_n é primo. ■

Exemplo 13. *Utilize o teste de Pepin para mostrar que* F_3 *é primo.*

Solução: Sabemos que $F_3 = 257$, logo, precisamos determinar r tal que $3^{\frac{257-1}{2}} = 3^{128} \equiv r \mod 257$.

Observe que,

$$\begin{aligned} 3^5 \equiv -14 \mod 257 \quad &\Rightarrow \quad 3^{15} \equiv (-14)^3 \equiv -174 \mod 257 \\ &\Rightarrow \quad 3^{16} = 3^{15} \cdot 3 \equiv -174 \cdot 3 \equiv -8 \mod 257 \\ &\Rightarrow \quad 3^{48} = \left(3^{16}\right)^3 \equiv (-8)^3 \equiv 2 \mod 257 \\ &\Rightarrow \quad 3^{64} = 3^{48} \cdot 3^{16} \equiv -8 \cdot 2 \equiv -16 \mod 257 \\ &\Rightarrow \quad 3^{128} = \left(3^{64}\right)^2 \equiv (-16)^2 \equiv -1 \mod 257. \end{aligned}$$

O que prova que F_3 é primo.

Outra interessante propriedade sobre os números de Fermat é a possibilidade de escrever sua sequência através de recorrência. Como pode ser observado na proposição seguinte.

Proposição 22. *Seja F_n um número de Fermat, para $n \geq 1$, temos que $F_n - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1}$.*

Demonstração: A demonstração será realizada por indução sobre n.

Seja $P(n) : F_n - 2 = F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1}$.

Para $n = 1$ sabemos que $F_1 = 2^2 + 1$ e $F_0 = 3$. Note agora que,

$$F_1 - 2 = 2^2 + 1 - 2 = 3.$$

Portanto $P(1)$ é válida.

Suponha, por hipótese de indução, que $P(n)$ seja válido para um certo n. Provaremos que $P(n+1)$ é também válido. Observe que

$$F_0 \cdot F_1 \cdot \ldots \cdot F_n = (F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1})\, F_n.$$

Por hipótese, segue que

$$\begin{aligned} F_0 \cdot F_1 \cdot \ldots \cdot F_n &= (F_n - 2)\, F_n \\ &= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) \\ &= \left(2^{2^n}\right)^2 - 1 \\ &= 2^{2^{n+1}} - 1 \\ &= 2^{2^{n+1}} - 1 + (1 - 1) \\ &= 2^{2^{n+1}} + 1 - 2 \\ &= F_{n+1} - 2. \end{aligned}$$

Portanto $P(n+1)$ é válida. Concluímos assim pelo PIF que $P(n)$ é válido para todo n natural. ■

Há ainda questionamentos que permanecem sem resposta sobre os números de Fermat, como por exemplo: Existem infinitos números de Fermat primos?

A falta de resposta para tal questionamento torna ainda mais intrigante o estudo acerca desses números, a medida que ressalta também a falta de conhecimento sobre o assunto.

3.3.2 Números de Mersenne

Números que podem ser escritos sob a forma $2^p - 1$, com p primo, são chamados de números de Mersenne e representados por M_p. Caso M_p seja primo, dizemos que o mesmo é um primo de Mersennne.

Os números de Mersenne, assim como os Fermat, não são todos primos, ou seja, na sua sequência temos números primos e compostos.

Por exemplo, $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ e $M_7 = 127$ são todos primos, mas $M_{11} = 2047$ é composto, tendo como fatores primos 23 e 89.

Ao analisarmos a definição de números de Mersenne podemos questionar: se p fosse composto, poderia $2^p - 1$ ser primo? A resposta pode ser obtida na proposição abaixo.

Proposição 23. *Se $2^n - 1$ é primo então n é primo.*

Demonstração: Seja $2^n - 1$ um número primo. Suponha, por absurdo, que n é composto, logo, existem $a, b \geq 2$ inteiros, tais que $n = a \cdot b$. Note que

$$2^a \equiv 1 \mod 2^a - 1 \Rightarrow (2^a)^b \equiv 1^b \mod 2^a - 1 \Rightarrow 2^n \equiv 1 \mod 2^a - 1.$$

Portanto $2^a - 1 \mid 2^n - 1$, o que é um absurdo pois $2^n - 1$ é primo e $1 < 2^a - 1 < 2^n - 1$. ■

Existem ainda testes de primalidade para os números de Mersenne possuindo como base as sucessões de Lucas, entretanto, no presente trabalho, não abordamos tais sucessões, o que torna inviável a apresentação de tais testes.

Os números de Mersenne têm uma forte relação com números perfeitos, que serão definidos a seguir.

Definição 15. *Dizemos que $n \in \mathbb{N}$ é um número perfeito se a soma dos seus divisores positivos é igual a $2n$, ou seja, se $S(n) = 2n$.*

Veja, por exemplo, que os divisores positivos de 6 são 1, 2, 3 e 6. Como $1 + 2 + 3 + 6 = 12 = 2 \cdot 6$, dizemos que 6 é um número perfeito.

Acredita-se que os números perfeitos foram assim denominados por questões religiosas, uma vez que algumas religiões pregam que o mundo foi criado em 6 dias, como 6 é o menor número que satisfaz a Definição 15, e provavelmente o primeiro a ser descoberto, a relação foi estabelecida.

E quanto a relação dos números perfeitos e o números de Mersenne? Essa pergunta pode ser respondida pela Proposição 24 e pelo Teorema 14, sendo suas demonstrações devidas a Euclides e Euler, respectivamente.

Proposição 24. *Seja p um número primo. Se $M_p = 2^p - 1$ é primo então $n = 2^{p-1}(2^p - 1)$ é um número perfeito.*

Demonstração: Seja $n = 2^{p-1}(2^p - 1)$, com p e $(2^p - 1)$ primos. Sendo $2^p - 1$ primo, então os divisores de n são 2^i e $2^i(2^p - 1)$, para $i = 0, 1, \ldots, (p-1)$. Logo, a soma dos divisores é dada por

$$\sum_{i=0}^{p-1} 2^i + \sum_{i=0}^{p-1} 2^i(2^p - 1).$$

Veja que os dois somatórios nada mais são, que a soma dos p primeiros termos de uma progressão geométrica de razão 2. Desta forma, temos que:

$$\begin{aligned}
\sum_{i=0}^{p-1} 2^i + \sum_{i=0}^{p-1} 2^i(2^p - 1) &= \frac{2^p - 1}{2 - 1} + \frac{(2^p - 1)(2^p - 1)}{2 - 1} \\
&= (2^p - 1) + (2^p - 1)(2^p - 1) \\
&= (2^p - 1)(1 + 2^p - 1) \\
&= 2^p(2^p - 1) = 2 \cdot n.
\end{aligned}$$

Portanto, n é um número perfeito. ■

Observe que a utilização da função $S(n)$, definida na Proposição 15, poderia reduzir os cálculos para tal demonstração, porém optamos por não utilizá-la, por se tratar de um caso simples.

Teorema 14. *Se n é um número perfeito par então podemos escrever $n = 2^{p-1}M_p$, onde, $M_p = 2^p - 1$ é primo.*

Demonstração: Seja n um número perfeito par, logo podemos escrever $n = 2^{p-1} \cdot q$, com $p \geq 2$ inteiro e q ímpar. Temos assim que $(2^{p-1}, q) = 1$, daí, pelo Corolário 3, segue que,

$$S(n) = 2n \Rightarrow S(2^{p-1}) \cdot S(q) = 2^p \cdot q \Rightarrow (2^p - 1) \cdot S(q) = 2^p \cdot q.$$

Veja, agora, que $(2^p - 1) \mid 2^p \cdot q$, porém como $(2^p - 1, 2^p) = 1$, temos, de forma mais específica, que $(2^p - 1) \mid q$, o que significa que existe um c inteiro, obviamente diferente de q, tal que $q = (2^p - 1) \cdot c$. Daí,

$$(2^p - 1) \cdot S(q) = 2^p \cdot q \Rightarrow (2^p - 1) \cdot S(q) = 2^p \cdot (2^p - 1) \cdot c \Rightarrow S(q) = 2^p \cdot c.$$

Por outro lado, $q = (2^p - 1) \cdot c$ implica que $q + c = 2^p \cdot c$.

Temos assim que $c = 1$ é a única possibilidade. Suponha que $c \neq 1$, como q e c são divisores de q, segue que $2^p \cdot c = S(q) \geq 1 + c + q > c + q = 2^p \cdot c$, o que é um absurdo.

Concluímos, assim, que $S(q) = q + 1 = 2^p$, ou seja, $q = 2^p - 1$ é primo e, consequentemente, p é primo e $n = 2^{p-1}(2^p - 1)$. ■

O Teorema 14 nos fornece um método de encontrar números de Mersenne que são primos, partindo de números perfeitos. Veja que se n é perfeito e par, bastaria fatorar n escrevendo $n = 2^m q$, com q ímpar, para obtermos assim um número primo q. Porém, atualmente só conhecemos 51 números perfeitos, o que nos leva a pensar que encontrar números perfeitos talvez seja uma tarefa tão difícil quanto encontrar primos, tornando assim, pelo menos por hora, o método inutilizável nesse sentido.

Capítulo 4

Sequência didática

No exercício do planejamento acadêmico é comum que o docente opte pela adoção de estratégias que facilitem o processo de ensino e aprendizagem, visando sempre a sua efetividade e significância. Dentre tais estratégias, pode-se citar as denominadas sequências didáticas, que podem ser aplicadas em diferentes níveis de ensino e associadas a demais métodos educacionais, a depender das necessidades identificadas.

As sequências didáticas, de acordo com Zabala (1998), são um conjunto de atividades, que como o próprio nome expressa, possuem uma ordem ou sequência, organizadas e articuladas entre si, com o intuito de atingir objetivos educacionais por meio de etapas. Cada uma dessas etapas, assim como a própria sequência didática, deve possuir início, meio e fim bem definidos e com objetivos claros. Dessa forma, é indispensável que o responsável saiba como e de onde partir, para que todas contribuam e promovam a construção de um conhecimento significativo e eficaz ao atingir o objetivo final, ponto de chegada.

Segundo Dolz e Schneuwly (2004 apud MONTEIRO; CASTILHO; SOUZA, 2019) as sequências didáticas podem ser vistas como instrumentos capazes de auxiliar o professor no processo de planejamento, onde o autor acredita que o conhecimento que os alunos já possuem, devem ser levados em consideração ao definir um ponto de partida e que em cada etapa, o nível de dificuldade possa ser ampliado, implicando em uma construção do conhecimento de forma gradual. Para que isso ocorra, há a importância de que durante o seu desenvolvimento, o professor esteja sempre atento à evolução e às dificuldades dos alunos, visto que nem sempre todos estarão no mesmo nível, o que pode exigir uma adaptação ou flexibilização em algumas atividades e etapas propostas, de modo que contribua para a continuidade da sequência planejada, atingindo o objetivo definido dentro no tempo estimado. Por esse motivo, torna-se fundamental a relação de comunicação e confiança entre os alunos e o professor, para que, por esse meio, o aluno sinta-se sempre confortável em expor suas

dúvidas, evitando que lacunas possam ser formadas ou etapas possam ser concluídas sem que o objetivo seja alcançado.

Para que todos os alunos estejam sempre envolvidos nas atividades propostas, além do que já foi levantado anteriormente, é valiosa a reafirmação por parte do professor, durante todo o processo, sobre a importância que possui o conteúdo abordado e sobre suas possíveis contribuições no que diz respeito ao desenvolvimento acadêmico e pessoal do discente, podendo, este, ser o fator motivador capaz de promover também a consciência de que a construção do conhecimento deve ser efetivada de forma autônoma, onde nessas circunstâncias, o professor assume então o papel de mediador, responsável por guiar o aluno para que ele consiga atingir esse feito não com o único intuito de conseguir um bom desempenho nas avaliações, mas pela vontade e interesse próprio de se obter conhecimento.

Por fim, reconsiderando a ideia inicial, vale ressaltar que, apesar da evidente vantagem de poder ser aplicada em diversas fases do ensino, o que independe da faixa etária predominante da turma, é importante frisar que não existe uma sequência única capaz de atender todos os objetivos que possam ser estabelecidos, em qualquer disciplina, com qualquer conteúdo abordado. Posto isto, vê-se então a necessidade do planejamento adequado diante dos pontos que se pretende partir e chegar, no contexto e área em que se pretende aplicar e do conhecimento prévio que os alunos já detêm, para que assim seja possível se estabelecer uma sequência didática apropriada que favoreça, de fato, uma aprendizagem significativa.

Diante de tantas vantagens, desenvolvemos a presente sequência didática, como um sugestão, para atingir as habilidades listadas pela BNCC quanto ao estudo dos números primos. A mesma é constituída por quatro partes e foi elaborada considerando como público alvo turmas do 6^{o} ano do ensino fundamental. O leitor mais atento deve perceber que a Parte 3 pode facilmente ser empregada em turmas do 7^{o} ano, todavia, defendemos ainda sua aplicação no 6^{o} ano, dado que aborda uma importante aplicação para números primos o que consequentemente traz mais significado para tal conteúdo e ressalta sua importância.

4.1 Números Primos

4.1.1 Parte 1: Múltiplos, Divisores e Números Primos

Objetivos:

- Compreender as definições de múltiplo e divisor, estabelecendo relação biunívoca entre divisor e fator de um número dado;
- Classificar números em primos ou compostos.

Tempo estimado: 90 min.

Desenvolvimento:

Sugerimos que o professor inicie a aula com as definições de múltiplo e divisor, resolvendo, de modo conjunto com os discentes, alguns exemplos que estrategicamente envolvam esses conceitos. É interessante que ao determinar os divisores, o docente destaque o fato de que o dividendo é igual ao produto do divisor pelo quociente, logo, se um número é divisor também será fator, estabelecendo assim uma relação biunívoca e uma forma de realizar fatoração.

Uma vez compreendidas as noções de múltiplo e divisor, propomos que o professor apresente aos alunos uma lista com os oito ou dez primeiros números naturais e peça para que determinem os seus divisores. Em seguida, o docente pode questionar quais semelhanças os números 2, 3, 5 e 7 apresentam, guiando os alunos de modo que percebam que estes apresentam apenas dois divisores: o 1 e ele mesmo. O docente pode então, utilizando tal característica, apresentar as definições de número primo e composto. Podem surgir nesse momento algumas perguntas do tipo: Existem outros números primos? Os números primos são infinitos ou finitos? Como encontrar números primos? Para tais questionamentos pode-se explicar que de fato existem infinitos números primos e que atualmente há métodos que facilitam a classificação desses números, como o crivo de Eratóstenes, que será apresentado na aula seguinte, mas ainda não existem fórmulas simples que gerem uma infinidade de primos. Nesse ponto, é interessante explicar a grande importância destes números para os sistemas de criptografia e, consequentemente, para o mercado financeiro, o que justifica o interesse por métodos para encontrá-los.

Por fim, para consolidar os conceitos vistos e avaliar a eficácia na aprendizagem, sugerimos que os alunos resolvam, de forma individual, uma atividade que vise determinar múltiplos e divisores de alguns números, bem como encontrar outros números primos.

4.1.2 Parte 2: Crivo de Eratóstenes e critérios de divisibilidade

Objetivo:

- Desenvolver métodos mais práticos para a classificação de números em primos ou compostos;
- Estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000.

Tempo estimado: 90 min.

Desenvolvimento:

Com a sugestão de atividade apresentada ao fim da aula 1, os alunos devem ter percebido que encontrar números primos não é uma tarefa tão simples. Aproveitando tal percepção sugerimos que o professor apresente o crivo de Eratóstenes como um método para ajudar nesse processo, realizando, em conjunto com os alunos, a construção de alguns crivos, até que os mesmos percebam que a partir de um certo valor sobrarão apenas números primos e, utilizando tal descoberta, aborde o Lema 4, dando assim mais significado ao mesmo.

Mesmo com a utilização do Lema 4 determinar se um número é primo ou composto, segue sendo, em alguns casos, uma tarefa trabalhosa, pois pode ser necessário realizar muitas divisões. Para tornar tal método mais prático é interessante o uso de critérios de divisibilidade, critérios esses que devem ser "descobertos"pelos próprios alunos. Para estabelecer um critério de divisibilidade por 2, sugerimos que o professor apresente uma lista com alguns múltiplos de 2, por exemplo, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20 e 22 e em seguida pergunte aos alunos se conseguem perceber algum padrão. A ideia é que percebam que todos terminam em 0, 2, 4, 6, ou 8, o que indicaria um possível motivo para estabelecer assim um critério de divisibilidade. Por se tratar de um caso simples, o professor pode apresentar uma demonstração e esclarecer que apenas a observação não é garantia de algo verdadeiro, e para isto, existem as demonstrações. De maneira semelhante, podemos determinar os critérios de divisibilidade por 3, 4, 5, 8, 9, 10, 100 e 1000.

Para guiar os alunos a descobrirem um critério de divisibilidade por 6, sugerimos que o professor comece observando o fato de que, se 6 é divisor de um número n, também será fator do mesmo, ou seja, podemos escrever $n = 6 \cdot k$ para algum k natural. Sendo $6 = 2 \cdot 3$, segue que $n = 2 \cdot 3 \cdot k$, portanto 2 e 3 também são fatores de n. Com isso, os alunos devem perceber que para que um número seja divisível por 6, o mesmo dever ser por 2 e 3, e para estes, temos critérios já estabelecidos.

Como atividade de fixação, sugerimos a realização de uma competição em sala de aula, para assim trabalhar os conteúdos de forma lúdica. Para tal, o docente deve inicialmente selecionar alguns números entre primos e compostos, em seguida dividir a turma em grupos e então sortear algum número dos já selecionados. Cada equipe deverá decidir se o mesmo é primo ou não. Se o grupo acertar, ele ganha um ponto. Se errar perde um ponto, caso tenha. Ao final da aula o grupo com mais pontos será o vencedor.

4.1.3 Parte 3: Aplicações dos números primos

Objetivo:

- Determinar múltiplos e divisores, por meio da decomposição em fatores primos;
- Entender a importância dos números primos na Matemática e em outras áreas.

Tempo estimado: 90 min.

Desenvolvimento:

Nesse ponto os alunos já devem compreender o conceito de múltiplos e divisores, serem capazes de realizar fatorações e reconhecer números primos, utilizando para tal o Lema 4 em conjunto com critérios de divisibilidade. Partindo de tal ponto, o professor pode realizar algumas fatorações, sempre conduzindo até sobrarem apenas fatores primos. Por exemplo, o número 30 pode ser dividido por 2, sendo $30 = 2 \cdot 15$. O número 15 por sua vez pode ser divido por 3, sendo $15 = 3 \cdot 5$. Daí, $30 = 2 \cdot 3 \cdot 5$. Em tal momento, pode-se questionar a turma se é possível dividir novamente algum desses fatores de modo a obter uma nova decomposição. A ideia com isto é que os alunos percebam que a decomposição em fatores primos é única, a menos da ordem dos fatores e que todos os números naturais maiores que 1 ou são primos ou podem ser expressos como um produto único entre números primos. O docente pode então explicar que tais afirmações compõem o Teorema Fundamental da Aritmética, que é essencial no estudo da matemática e que tem aplicações em várias áreas da ciência e tecnologia, como a criptografia.

Mas por que decompor um número em fatores primos? Existe alguma vantagem? Questionamentos desse tipo são comuns e devem sempre ser utilizados como impulsionadores na apresentação de novos conceitos, logo é interessante que o professor explique que essa decomposição pode ser utilizada para determinar os divisores do número decomposto e que, para isso, basta considerar todas as combinações possíveis dos seus fatores.

A decomposição em fatores primos é ainda muito útil na determinação do máximo divisor comum (MDC). Para que os discentes percebam tal importância, sugerimos que o professor desafie a turma a determinar o maior divisor comum de dois números, de preferência compostos. É provável que os alunos escrevam os divisores de cada número e em seguida por meio de observação concluam qual é o maior divisor comum aos dois. Tal raciocínio deve ser elogiado para desenvolvimento de autoconfiança e motivação, porém deve-se questionar novamente: Haveria uma maneira mais prática? Os alunos devem ser guiados a concluírem, de forma autônoma, que basta apenas decompor em fatores primos e tomar os fatores comuns. De maneira semelhante pode-se determinar o mínimo múltiplo comum, sugerimos que o faça, pois reforça a importância da decomposição e consequentemente dos números primos.

4.1.4 Parte 4: Resolução de problemas

Objetivo:

- Resolver problemas que envolvam os conceitos de múltiplo, divisor e número primo.

Tempo estimado: 90 min.

Desenvolvimento:

Sugerimos que esta aula seja dividida em duas etapas. Para a primeira etapa propomos que sejam formadas equipes de três alunos, que devem então serem desafiadas a resolverem os problemas do anexo A.1.

Para a segunda etapa, nossa sugestão é que seja realizado um pequeno debate entre as equipes, para compartilhar ideias e discutir as soluções encontradas, onde, nesse ponto, o professor pode apresentar também suas próprias considerações.

Capítulo 5

Conclusão

No decorrer deste trabalho, pudemos compreender um pouco mais sobre a história dos números primos, desde as primeiras evidências do seu estudo até os dias atuais, onde se tornaram uma ferramenta indispensável para o sistema financeiro. Acompanhada por tal importância, percebemos o quão limitado é o nosso conhecimento sobre esses números tão fascinantes, o que a princípio pode ser considerado como algo negativo, entretanto, é também o que torna esse um dos campos mais estimulantes da Matemática, afinal de contas ainda temos muito a explorar e descobrir.

Diante de certas barreiras sobre os números primos, como por exemplo, a falta de fórmulas para encontrá-los, abordamos diferentes testes de primalidade, que demonstraram ser um importante instrumento para determinar se um número é primo ou composto. O estudo de tais testes se apresenta ainda como um complemento para a formação de professores, pois tais testes muitas vezes não são abordados dentro da graduação em licenciatura.

Por fim, apresentamos uma proposta de sequência didática sobre números primos, desenvolvida para uma turma do $6^{\underline{o}}$ ano do ensino fundamental, mas que pode facilmente ser estendida para outras turmas que necessitem rever tais conceitos. Esperamos que tal sequência contribua de forma significativa no ensino dos números primos, despertando a curiosidade e estimulando o interesse dos alunos não apenas por este tema, mas pela Matemática em geral.

Perante os pontos levantados ao longo deste trabalho, percebemos a importância não apenas de trabalhar tal conteúdo em sala, mas também de incentivar seu estudo. Não é possível saber onde, nem quando surgirá alguém capaz de desvendar os mistérios que ainda pairam sobre tais números e que possibilite, com isso, mudar a forma como os vemos.

Referências Bibliográficas

1 MORGADO, A. C.; CARVALHO, P. C. P. *Matemática discreta*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2015.

2 HEFEZ, A. *Aritmética*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2013.

3 MARTINEZ, F. B. et al. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. 5. ed. Rio de Janeiro: IMPA, 2010.

4 SANTOS, J. P. d. O. *Introdução à teoria dos números*. Rio de Janeiro: IMPA, 2000. v. 3.

5 BEZERRA, M. d. N. *Teoria dos números: um curso introdutório*. Belém: EditAedi, 2018.

6 RIBENBOIM, P. *Números primos: velhos mistérios e novos recordes*. Rio de Janeiro: IMPA, 2012.

7 EVES, H. *Introdução à história da matemática*. 5. ed. Campinas: Unicamp, 2011.

8 GUNDLACH, B. H. *Números e numerais*. São Paulo: Atual, 1993.

9 BRASIL. *Base Nacional Comum Curricular*. Brasília: MEC, 2018.

10 ZABALA, A. *A prática educativa: como ensinar*. Vitória: ArtMed, 1998.

11 MONTEIRO, J. C.; CASTILHO, W. S.; SOUZA, W. A. de. Sequência didática como intrumento de promoção da aprendizagem significativa. *Revista Debates em Educação Científica e Tecnológica*, Porto Alegre, v. 9, n. 01, p. 292–305, 2019.

12 SAUTOY, M. D. *A música dos números primos: a história de um problema não resolvido na matemática*. São Paulo: Editora Schwarcz-Companhia das Letras, 2007.

Apêndice A

Sugestões de Atividades

A.1 Questões da OBMEP

As questão a seguir são retiradas de provas da Olimpíada Brasileira de Matemática das Escolas Publicas (OBMEP) de nivel 1, 2 e 3 e podem ser resolvidas através dos conceitos e ideias apresentados na sequência didática.

1. **(Questão 6 - nivel 1 - 2015)** Qual é o algarismo das unidades do número,

$$1 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11 \cdot 13 \cdot 15 \cdot 17 \cdot 19 - 2015?$$

a) 0

b) 1

c) 5

d) 6

e) 8

Solução: Alternativa a)

Considere $n = 1 \cdot 3 \cdot 5 \cdot 7 \cdot 9 \cdot 11 \cdot 13 \cdot 15 \cdot 17 \cdot 19$. Temos que n é divisivel por 5, uma vez que 5 é um de seus fatores primos. Logo, seu algarismo da unidade deve ser 0 ou 5. Como n não possui fatores 2 o mesmo não é divisivel por 2 e portanto seu algarismo da unidade não pode ser 0.

Concluímos assim que n termina em 5 e consequentemente $n-2015$ termina em 0.

2. **(Questão 8 - nivel 1 - 2014)** Ana Maria apertou as teclas $19 \times 106 =$ de sua calculadora e o resultado 2014 apareceu no visor. Em seguida, ela limpou o visor e

fez aparecer novamente 2014 com uma multiplicação de dois números naturais, mas, desta vez, apertando seis teclas em vez de sete. Nesta segunda multiplicação, qual foi o maior algarismo cuja tecla ela apertou?

a) 5

b) 6

c) 7

d) 8

e) 9

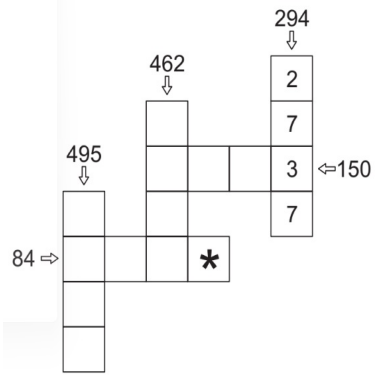
Solução: Alternativa c)

Perceba que as teclas $\times$ e $=$ serão apertadas em ambos os casos, devemos então reduzir, em uma, a quantidade de teclas numéricas a serem apertadas. Para isto, precisamos decompor 106 em fatores primos. Veja:

$$\begin{array}{r|l} 106 & 2 \\ 53 & 53 \\ 1 & \end{array}$$

Logo $106 = 2 \cdot 53$. Podemos escrever então $2014 = 1 \cdot 2014 = 19 \cdot 106 = 2 \cdot 19 \cdot 53 = 38 \cdot 53 = 2 \cdot 1007$. É fácil ver agora que para aparecer 2014 no visor da calculadora apertando seis teclas devemos apertar, não necessariamente nessa ordem, $38 \times 53 =$, o que significa que o maior algarismo apertado é 8.

3. **(Questão 3 - nivel 2 - 2019)** As casas da figura abaixo devem ser preenchidas com números primos. Em cada linha ou coluna, o produto dos números deve ser igual ao número indicado pela seta. A coluna indicada por 294 já está preenchida. Qual é o número que deve ser escrito na casa marcada com $*$?



a) 2

b) 3

c) 5

d) 7

e) 11

Solução: Alternativa a)

Inicialmente iremos decompor todos os números apresentados em fatores primos. Veja:

150	2	84	2	462	2	495	3
75	3	42	2	231	3	165	3
25	5	21	3	77	7	55	5
5	5	7	7	11	11	11	11
1		1		1		1	

Ressaltamos que no processo de decomposição é interessante a utilização dos critérios de primalidade.

Temos assim que,

$$\begin{aligned} 150 &= 2 \cdot 3 \cdot 5 \cdot 5 \\ 84 &= 2 \cdot 2 \cdot 3 \cdot 7 \\ 462 &= 2 \cdot 3 \cdot 7 \cdot 11 \\ 495 &= 3 \cdot 3 \cdot 5 \cdot 11 \end{aligned}$$

Devemos começar a preencher a tabela com os fatores comuns. Observe que 84 e 465 tem apenas o 3 como fator comum, logo o mesmo deve ocupar a posição de interseção destes números. Já 462 e 150 tem em comum 2 e 3, como o 3 já foi inserido, devemos ter o número 2 na interseção dos mesmos. Por fim os números 84 e 462 tem 2, 3 e 7 como fatores primos comuns, sendo que 2 e 3 já foram inseridos, portando para sua interseção devemos ter o 7. Observe a figura abaixo.

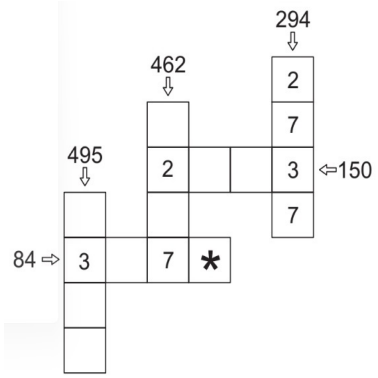


Figura A.1: OBMEP

Como $84 = 2 \cdot 2 \cdot 3 \cdot 7$, concluímos que $* = 2$.

4. **(Questão 9 - nivel 2 - 2019)** Um número inteiro positivo é chamado de tetrapar quando é divisível quatro vezes consecutivas por 2 e o resultado da última divisão é um número ímpar. Por exemplo, o número 80 é tetrapar, pois $80 \div 2 = 40$, $40 \div 2 = 20$, $20 \div 2 = 10$ e $10 \div 2 = 5$. Quantos são os números tetrapares de três algarismos?

a) 26

b) 28

c) 30

d) 56

e) 62

Solução: Alternativa b)

Um número n será tetrapar se $n = 2^4 \cdot q$, onde q é um número natural ímpar. Note que, $16 \cdot 5 = 80$ e $16 \cdot 7 = 112$, logo 112 é o primeiro número com três algarismos que é tetrapar. Veja agora que $2^4 \cdot 61 = 976$ e $2^4 \cdot 63 = 1008$, logo 976 é o ultimo tetrapar com 3 algarismos. Determinar a quantidade de tetrapares com três algarismos é equivalente a determinar quantos números ímpares a sequencia abaixo apresenta.

$$7, 8, 9, 10, \ldots, 59, 60, 61$$

A sequencia contem $61 - 6 = 55$ números, como ela começa e termina com números ímpares a quantidade de ímpares excede a quantidade de pares em um. Logo, sendo $x - 1$ a quantidade de número pares a quantidade de ímpares será x. Daí, $x - 1 + x = 55$, portanto $x = 28$.

5. **(Questão 11 - nivel 3 - 2018)** Qual é o maior valor possível para o máximo divisor comum de dois números naturais cujo produto é 6000?

a) 10

b) 20

c) 30

d) 40

e) 60

Solução: Alternativa b)

Inicialmente iremos decompor 6000 em fatores primos.

6000	2
3000	2
1500	2
750	2
375	3
125	5
25	5
5	5
1	

Temos assim que $6000 = 2^4 \cdot 3 \cdot 5^3$.

Considere agora $a, b \in \mathbb{N}$ tais que $a \cdot b = 6000$. Para que o MDC de a e b seja máximo, a e b devem ter a maior quantidade possível de fatores primos em comum. Logo as possibilidades são: $a = 2^2 \cdot 3 \cdot 5^2$ e $b = 2^2 \cdot 5$, $a = 2^2 \cdot 5^2$ e $b = 2^2 \cdot 3 \cdot 5$, $a = 2^2 \cdot 3 \cdot 5$ e $b = 2^2 \cdot 5^2$ ou $a = 2^2 \cdot 5$ e $b = 2^2 \cdot 3 \cdot 5^2$. Em qualquer uma das escolhas teríamos que $MDC(a, b) = 2^2 \cdot 3^0 \cdot 5^1 = 20$, sendo este o maior valor possível.

6. **(Questão 17 - nível 3 - 2016)** Quantos são os números naturais n tais que $\frac{5n-12}{n-8}$ é também um número natural?

a) 4

b) 5

c) 6

d) 7

e) 8

Solução: Alternativa d)

Note que,

$$\frac{5n-12}{n-8} = \frac{5n-40+40-12}{n-8} = \frac{5(n-8)+28}{n-8} = \frac{5(n-8)}{n-8} + \frac{28}{n-8} = 5 + \frac{28}{n-8}.$$

Perceba que, $\frac{5n-12}{n-8}$ é natural se $\frac{28}{n-8} \geqslant -5$, foi inteiro.
Sendo $28 = 2^2 \cdot 7$ seus divisores inteiros são:

$$\begin{aligned}
\pm 2^0 \cdot 7^0 &= \pm 1 \\
\pm 2^0 \cdot 7^1 &= \pm 7 \\
\pm 2^1 \cdot 7^0 &= \pm 2 \\
\pm 2^1 \cdot 7^1 &= \pm 14 \\
\pm 2^2 \cdot 7^0 &= \pm 4 \\
\pm 2^2 \cdot 7^1 &= \pm 28
\end{aligned}$$

Como $\frac{28}{n-8} \geqslant -5$ iremos considerar apenas $1, 2, 4, \pm 7, \pm 14, \pm 28$.

Precisamos agora determinar n tal que $n - 8 = i$, para $i = 1, 2, 4, \pm 7, \pm 14, \pm 28$. Veja que $n - 8 = -14$ e $n - 8 = -28$ não possuem soluções naturais, portanto os possíveis valores para n são: 9, 10, 12, 15, 1, 22, 36.