UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Aritmética modular e aplicações: criptografia RSA e calendário perpétuo.

Ana Catarina Bruxelas

Dissertação de Mestrado do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT)

ICMC USP SÃO CARLOS

Ana Catarina Bruxelas

Aritmética modular e aplicações: criptografia RSA e calendário perpétuo.

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestra em Ciências – Mestrado Profissional em Matemática em Rede Nacional. *VERSÃO REVISADA*

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientador: Prof. Dr. Tiago Henrique Picon

USP – São Carlos
Janeiro de 2021

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

Bruxelas, Ana Catarina
B886a Aritmética modular e aplicações: criptografia RSA e calendário perpétuo. / Ana Catarina Bruxelas; orientador Tiago Henrique Picon. -- São Carlos, 2020.
167 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2020.

1. Divisibilidade. 2. Aritmética Modular. 3. Criptografia RSA. 4. Calendário Perpétuo. I. Picon, Tiago Henrique, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Ana Catarina Bruxelas

Modular arithmetic and applications: RSA cryptography and perpetual calendar

Dissertation submitted to the Instituto de Ciências Matemáticas e de Computação – ICMC-USP – in accordance with the requirements of the Professional Master's Program in Mathematics in National Network, for the degree of Master in Science. *FINAL VERSION*

Concentration Area: Professional Master Degree Program in Mathematics in National Network

Advisor: Prof. Dr. Tiago Henrique Picon

USP – São Carlos
January 2021

Dedico este trabalho a todas as pessoas que estiveram presentes em minha vida e instigaram-me a enfrentar novos desafios e buscar a aprendizagem.

AGRADECIMENTOS

Enfim é chegada a hora de pensar com o devido carinho, atenção e gratidão a todos que fizeram parte deste processo, de forma direta ou indireta.

À minha família pelo incentivo e participação ativa em todas as decisões da minha história. Ressalto especialmente o papel da minha mãe, que desde a primeira infância me guiou na orientação e no exemplo pelo gosto aos estudos, atendendo prontamente minha curiosidade e anseio em entender o mundo que me rodeia.

Aos meus amigos, minha família não biológica, por me fortalecerem sempre, mesmo nas minhas ausências. Ao meu companheiro de estudo Alan Cassaro, que dividiu comigo grande parte desta etapa da vida.

Como não mencionar meus alunos? Sim, eles sempre foram o combustível para meu aperfeiçoamento profissional. Suas dúvidas, interesses e dificuldades motivaram-me a questionar e refletir sobre aquilo que se estava determinado, levando-me a um olhar crítico e reflexivo sobre a educação e o ensino da Matemática. Cito aqui com extremo afeiçoamento a frase dita nos momentos de descobertas e soluções: “Viva a Matemática”!

Aos meus professores do PROFMAT, Alexandre Cassola, Sérgio Zani, Michela Tuchapesk, Erica Filletti e em especial aos professores Ires Dias e Hermano Ribeiro, declaro minha eterna gratidão e consideração por me guiarem com tamanha competência e dedicação na busca do saber.

Exalto os agradecimentos com grande estima e respeito ao meu orientador Prof. Tiago Henrique Picon, que mesmo antes da jornada do PROFMAT já me elucidava com ideias e diretrizes sobre o pensar e fazer Matemática. Durante toda a execução deste trabalho, me agraciou com uma exímia orientação, prontidão e paciência.

À vida que me foi dada e com ela todos os desafios a mim colocados.

“Não é o conhecimento, mas o ato de aprender, não a posse
mas o ato de chegar lá, que concede a maior satisfação.”
(Carl Friedrich Gauss)

RESUMO

BRUXELAS, A. C. **Aritmética modular e aplicações: criptografia RSA e calendário perpétuo.**. 2021. 167 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2021.

Tópicos em Aritmética Modular são raramente trabalhados no Ensino Básico e poucos professores possuem formação adequada sobre o assunto. Nessa dissertação buscou-se retratar premissas conceituais que colaborem com a formação do professor e sua prática, em alguns tópicos sobre Aritmética Modular. Propôs-se a tratar previamente conceitos iniciais em torno da ideia de divisibilidade e, sequencialmente, introduzir o conceito de congruência de maneira natural. Procurou-se proporcionar o aprofundamento no tema e clareza no entendimento teórico, fundamentando a apresentação dos resultados e teoremas relacionados, através de aplicações e realizações de exemplos diversos e não triviais. Dessa forma mostrou-se resultados relevantes do estudo das congruências como o Teorema de Fermat, Teorema de Euler e classes de equivalência. De modo a ilustrar algumas aplicações dos resultados tratados, apresenta-se o sistema de Criptografia RSA e o Calendário Perpétuo. Como conclusão, expôs-se uma proposta de sequência didática para os anos finais do Ensino Fundamental, evidenciando alguns conceitos e resultados da Aritmética Modular presentes no currículo de Matemática dessa etapa de ensino, segundo a Base Nacional Comum Curricular. Para embasar a sequência didática, utilizou-se da análise das grandezas e construções aritméticas e algébricas possíveis no calendário atual, adotando como norteador as conclusões realizadas acerca do Calendário Perpétuo e, consequentemente, sobre o Teorema de Zeller.

Palavras-chave: Divisibilidade, Aritmética Modular, Criptografia RSA, Calendário Perpétuo.

ABSTRACT

BRUXELAS, A. C. **Modular arithmetic and applications: RSA cryptography and perpetual calendar**. 2021. 167 p. Dissertação (Mestrado em Ciências – Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2021.

Topics in Modular Arithmetic are rarely worked in Basic Education and few teachers have proper training on the subject. In this dissertation, we sought to portray conceptual premises that collaborate with the teacher training and its practice in some topics on Modular Arithmetic. It was proposed to previously treat initial concepts around the idea of divisibility and, sequentially, to introduce the concept of congruence in a natural way. It sought to provide a deeper understanding of the theme and clarity in the theoretical understanding, supporting the presentation of the results and theorems related through applications and achievements of diverse and non-trivial examples. In this sense, relevant results from the study of congruences were shown, such as Fermat's Theorem, Euler's Theorem, and equivalence classes. The RSA Cryptography system and the Perpetual Calendar were presented to illustrate some applications of the treated results. In conclusion, a didactic sequence proposal was presented for the final years of Elementary School, showing some concepts and results of Modular Arithmetic present in the Mathematics curriculum of this teaching stage and according to the Common National Curricular Base. To support the didactic sequence, it was used the analysis of the arithmetic and algebraic quantities and constructions possible in the current calendar, adopting as a guideline the conclusions made about the Perpetual Calendar and, consequently, about the Zeller Theorem.

Keywords: Divisibility, Modular Arithmetic, RSA Cryptography, Perpetual Calendar.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

A discussão em torno das dificuldades identificadas pelo professor de Matemática no exercício da sua profissão são amplas e contemplam vários aspectos. Dentre elas, ocorre à necessidade de aprofundar-se em assuntos que, na sua formação específica e inicial, foram apresentados de forma tangencial ou com menor enfoque, limitando sua visão a um estado minimalista de conteúdos, propriedades e suas aplicações. O reconhecimento por parte do professor dessa problemática está em parte relacionada aos materiais didáticos que subsidiam sua prática, os desafios encontrados para alcançar os objetivos traçados para seu público e os métodos aplicados para essa finalidade.

Neste contexto foi que, enquanto professora de Matemática do Ensino Fundamental e Médio da rede pública e privada, despertou em mim os primeiros questionamentos sobre a forma como alguns temas eram abordados pelas obras e materiais utilizados diretamente pelos alunos e professores. Eram frequentes as situações nas quais me deparava com os alunos procurando algoritmos ou caminhos para resolver determinada situação problema, sem nenhuma atitude de investigação ou elaboração prévia. Muitas vezes ouvia dos alunos a predileção em realizar atividades do estilo “resolva” ou “calcule” a atividades que envolviam um contexto, conexão entre conteúdos anteriores ou com passos a serem formulados para alcançar uma solução.

A fim de trazer novas abordagens dos conteúdos para a sala de aula, buscando atividades que proporcionassem uma melhor maneira de tratamento e apresentação dos conteúdos propostos, de forma contextualizada e pensante, iniciei a utilização de problemas trazidos nos bancos de questões da OBMEP. Junto a essa decisão veio a certificação, não somente que os alunos precisavam de um outro olhar para a Matemática, mas todos envolvidos no processo. Essa certificação acentuou-se quando ingressei como professora nos programas OBMEP na Escola e PIC, ambos vinculados ao programa das Olimpíadas Brasileira de Matemática das Escolas Públicas - OBMEP, que somados às percepções anteriores provocaram-me a procurar uma formação complementar e uma nova abordagem em alguns tópicos da Matemática com os

alunos.

Durante os anos de 2016, 2018, 2019 e 2020 que atuei nos programas, chamou-me a atenção sobre o modo de tratamento feito nos materiais utilizados referente aos tópicos relacionados a Teoria dos Números, em especial a Aritmética Modular. A abordagem de tais temas era realizada de forma mais abrangente e com maior embasamento teórico, ainda assim os alunos mostravam excelentes resultados no seu entendimento, assimilação e aplicação dos conteúdos. Diante disso, dois pontos levantaram-se: o primeiro era em relação a comparar o tratamento dado aos temas de Aritmética, que eram comuns tanto nos programas quanto no currículo de Matemática do ensino regular; o segundo era como expandir a ideia dos números inteiros, suas propriedades e operações, por meio da Aritmética Modular, associando-a aos conteúdos trabalhados nos planejamentos curriculares dos anos nos quais ministrava as aulas.

Como forma de responder a esses anseios, ocorreu uma necessidade de pesquisar e correlacionar teoria e prática, utilizando os mais diversos materiais, de modo a ser inicialmente um estudo e formação profissional, e como consequência a isso, refletisse a uma nova proposta do ensino e aprendizagem de Matemática.

Nesse panorama, o presente trabalho foi constituído para abordar a teoria necessária, desde os fundamentos iniciais até os tópicos mais elaborados, de modo a proporcionar as ferramentas suficientes para o entendimento e aplicação que se propõe. Na perspectiva de aluna, senti a necessidade em reescrever e apresentar um rigor matemático nas demonstrações de alguns resultados de forma clara e sem omissão de passagens, assim como de fazer uso sistemático de aplicações e exemplos para os principais pontos da teoria, de forma mais abrangente daqueles apresentados em algumas bibliografias utilizadas no PROFMAT, por exemplo.

Nesta vertente os Capítulos 2 e 3 dedicaram-se a base teórica para a formulação dos resultados acerca do tema Aritmética Modular. No Capítulo 2 foram apresentados e explicitados alguns dos métodos de demonstração oriundos dos Axiomas de Peano, com enfoque para o Princípio da Indução Matemática. No Capítulo 3 discorreu-se sobre tópicos pertinentes a ideia de divisibilidade. Nessa perspectiva, associando resoluções de exemplos diversos, mostrou-se propriedades relacionadas à divisibilidade, apresentou-se o Teorema da Divisão Euclidiana, bem como resultados envolvendo o MDC entre dois números inteiros. Uma visão mais abrangente sobre tais temas foi provocada a partir da definição de números primos e, consequentemente, o Teorema Fundamental da Aritmética.

Com o intuito de aprofundar-se na visão sobre divisibilidade, aproveitando das características cíclicas do resto da divisão entre dois números inteiros, introduziu-se no Capítulo 4 os estudos acerca da Aritmética Modular a partir das congruências. Para esse desenvolvimento, além de conceitos e proposições relacionadas as Congruências, buscou-se levantar curiosidades e percepções que envolviam sua aplicação em assuntos presentes tanto no currículo de Matemática da Educação Básica quanto nos cursos oferecidos pelo PIC e OBMEP na Escola, como critérios de divisibilidade, problemas envolvendo divisão entre potências de números inteiros e equações

diofantinas lineares e não lineares.

Alguns teoremas significativos dos estudos de Congruências e suas aplicações foram apresentados no Capítulo 5. Para uma melhor compreensão dessa proposta, introduziu-se a definição de relações e classes de equivalência permitindo uma imersão das ideias apresentadas sobre a Aritmética Modular. Desse modo, apresentou-se o Teorema de Fermat e o Teorema de Euler como uma importante ferramenta na resolução de problemas que envolvam divisibilidade, mais especificamente, na linguagem das congruências. Procurou-se explorar o Teorema de Fermat como um caso particular do Teorema de Euler, utilizando aplicações que comparam a utilização de tais métodos, levando a discussão a uma análise qualitativa dos elementos que se possua inicialmente.

Como consequencia dos resultados apresentados sobre Aritmética Modular, algumas aplicações foram propostas. Nos Capítulos 6 e 7 sobre Criptografia, em especial o sistema de criptografia RSA e o calendário perpétuo. Em ambos foram realizadas contextualizações históricas e procedimentais nos quais fundamentam suas construções.

No capítulo destinado a Criptografia, mostrou-se a evolução deste método até os dias atuais, procurando fazer conexões sobre os assuntos relacionados a Aritmética Modular a cada passo demonstrado. De uma forma mais criteriosa e detalhada, explanou-se sobre o sistema de criptografia RSA e as etapas que o constituem, com a associação entre teoria e prática à partir da construção de exemplos numéricos.

Para alcançar o objetivo de contemplar um teorema que permita a determinação de uma data qualquer, segundo os padrões do calendário atual, detalhou-se a relação das grandezas ano, mês e dia quando averiguadas a contar de um ano de base e consideradas módulo 7. Essa argumentação, alicerçada nos resultados que culminaram no Teorema de Zeller, traz como metodologia a elaboração das generalizações baseado na inspeção do comportamento de sequências recursivas.

Como conclusão, propõe-se no Capítulo 8 uma sequência didática, que relaciona conteúdos presentes ao longo do currículo de Matemática dos anos finais do Ensino Fundamental, encontrados na Base Nacional Comum Curricular (BNCC), com a Aritmética Modular. Respaldada na elaboração de conceitos e generalizações com suporte em situações problemas diversos, a sequência didática fornece em seu contexto elementos nos quais permitam uma nova abordagem para assuntos já conhecidos pelos alunos e também incitem a construção de novos conceitos, como o tratamento do resto da divisão entre dois números pela sua perspectiva cíclica e a realização de operações conhecidas como “aritmética dos restos”. Ao longo do capítulo, procurou-se associar o vislumbramento curioso da Aritmética Modular à aplicação de habilidades aritméticas e algébricas essenciais para a construção de uma base matemática sólida, de forma a trazer como consequência melhores resultados no processo de aprendizagem.

CAPÍTULO

2

PRINCÍPIO DA INDUÇÃO MATEMÁTICA

Neste capítulo inicial apresentaremos ferramentas imprescindíveis para a demonstração de resultados matemáticos diversos. Faremos isso a partir de aplicações em torno de axiomas fundamentais do conjunto dos números naturais.

O matemático Giusepe Peano $(1858-1932)$ foi quem definiu com precisão o conjunto $\mathbb{N}$ dos números naturais, em 1889, na obra *"Arithmetices principia nova methodo exposita"*. A caracterização de seus elementos é baseado essencialmente na ideia de "sucessor de"; ele concluiu que toda teoria acerca do conjunto dos números naturais poderia ser realizada a partir de quatro axiomas, conhecidos como *Axiomas de Peano* que são:

(P_1) Existe uma função $s : \mathbb{N} \longrightarrow \mathbb{N}$ que associa a cada $n \in \mathbb{N}$ um elemento $s(n) \in \mathbb{N}$, chamado de sucessor de n.

(P_2) A função $s : \mathbb{N} \longrightarrow \mathbb{N}$ é injetiva.

(P_3) Existe um único elemento $n \in \mathbb{N}$, tal que $n \neq s(n)$ para qualquer $n \in \mathbb{N}$, esse elemento é o 1.

(P_4) Dado um subconjunto X tal que $X \subset \mathbb{N}$, se valem as propriedades

(i) $1 \in X$;

(ii) se $x \in X \Longrightarrow s(x) \in X$, então $X = \mathbb{N}$.

O quarto axioma, conhecido como *axioma da indução*, é a base para as contruções dos métodos de demonstrações que iremos discutir. A priori, ele nos diz que todo número natural n pode ser obtido a partir de 1 tomando seu sucessor $s(1)$, e o próximo natural fazendo $s(s(1))$, e assim por diante, desencadeando uma sequência de implicações. Assumindo a veracidade deste axioma, origina-se o método de demonstrações por indução, que anunciaremos a seguir.

Teorema 1 (Princípio da Indução Finita - PIF). Seja $P(n)$ uma propriedade do número natural $n \in \mathbb{N}$ tal que

(i) $P(1)$ é verdadeira;

(ii) se $P(n)$ é verdadeira para n, então $p(n+1)$ é verdadeira.
Então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Demonstração. Assumindo o axioma de Peano P_4 como hipótese, seja P uma propriedade que satisfaz (i) e (ii). Defina-se o conjunto

$$X = \{n \in \mathbb{N} : P(n) \text{ é verdadeira}\}.$$

Do fato que P satisfaz (i), segue que $P(1)$ é verdadeira, isto é, $1 \in X$. Do mesmo modo, P satisfaz (ii), então $P(n)$ ser verdadeira implica na validade de $P(n+1)$, ou seja, $n+1 \in X$. Assim $X = \mathbb{N}$, isto é, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$. □

Fazendo uma análise prática do PIF, observa-se que dado um certo conjunto $X \subset \mathbb{N}$, com $X \neq \emptyset$, contendo a propriedade $P(n)$, verifica-se inicialmente que 1 satisfaz $P(n)$, chamaremos esse passo de base indutiva. Em seguida, no que chamamos de passo indutivo, mostra-se como utilizar a validade de $P(n)$ para um dado $n \in \mathbb{N}$ - hipótese de indução, para verificar que $P(n+1)$ é válida, permitindo concluir que $P(n)$ é verdadeira para todo natural $n \geq 1$ tal que $n \in X$, ou seja, $P(n)$ é verdadeira para qualquer $n \in \mathbb{N}$.

O Princípio de Indução Finita tem inúmeras aplicações nos diversos campos de estudo da Matemática, a seguir daremos um exemplo que envolve algumas propriedades dos números naturais.

Exemplo 1. Para $n \in \mathbb{N}$, com n ímpar, vale a igualdade

$$1^2 + 3^2 + \ldots + n^2 = \binom{n+2}{3}$$

Do fato de n ser ímpar, então $n = 2k-1$ para $k \in \mathbb{N}$, reescrevemos a propriedade $P(n)$ a ser averiguada como

$$\sum_{i=1}^{k} (2i-1)^2 = \binom{2k+1}{3}.$$

(i) (*base de indução)* Para $k = 1$, temos

$$(2.1-1)^2 = 1 = \binom{3}{3} = \binom{2.1+1}{3},$$

logo, $P(1)$ é verdadeira.

(ii) (*passo indutivo*) Suponhamos que $P(n)$ é verdadeira para k, então mostraremos a veracidade de $P(n)$ para $k+1$. Temos

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

Pela hipótese de indução temos que $\sum_{i=1}^{k}(2i-1)^2 = \binom{2k+1}{3}$, logo

$$\begin{aligned}
\sum_{i=1}^{k+1}(2i-1)^2 &= \binom{2k+1}{3} + (2k+1)^2 \\
&= \frac{(2k+1)(2k)(2k-1)}{6} + (2k+1)^2 \\
&= \frac{(2k+1)(2k)(2k-1)}{6} + \frac{6(2k+1)^2}{6} \\
&= \frac{(2k+1)}{6}[2k(2k-1)+6(2k+1)] \\
&= \frac{(2k+1)}{6}(4k^2-2k+12k+6) \\
&= \frac{(2k+1)}{6}(4k^2+10k+6) \\
&= \frac{(2k+1)(2k+2)(2k+3)}{6} \\
&= \binom{2k+3}{3} \\
&= \binom{2(k+1)+1}{3}.
\end{aligned}$$

Assim, $P(n)$ é válida para $k+1$ e pelo Princípio da Indução Finita (PIF), $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Apresentaremos na sequência dois importantes teoremas diretamente consequentes do Princípio da Indução Finita.

Teorema 2 (**Princípio da Boa Ordenação - PBO**). Todo subconjunto não vazio $A \subset \mathbb{N}$ possui um menor elemento.

Demonstração. Seja $B \subset \mathbb{N}$ um conjunto não vazio e suponha por absurdo que B não contenha elemento mínimo. Defina-se o conjunto

$$A = \{n \in \mathbb{N} : n < m \,\forall\, m \in B\}.$$

Em particular $1 \notin B$, pois senão seria seu elemento mínimo, logo $1 \in A$. Pela definição de A, temos que se $n \in A$, então $n+1 \leqslant m$. Se $n+1 < m$, então $n+1 \in A$ e como $1 \in A$, pelo Teorema 1, $A = \mathbb{N}$ e $B = \emptyset$, uma contradição. Então $n+1 \in B$ e é seu elemento mínimo.

□

Exemplo 2. Apliquemos o Princípio da Boa Ordenação para mostrar que não existe um $m \in \mathbb{N}$ tal que $0 < m < 1$.

Suponha por absurdo que exista $m \in \mathbb{N}$, tal que $0 < m < 1$. Desse modo, definina o conjunto não vazio $B = \{m \in \mathbb{N} : 0 < m < 1\}$. Pelo Princípio da Boa Ordenação existe um natural $k \in B$ tal que $k \leqslant m$, para todo $m \in B$. Como $k \in B$ então $0 < k < 1$ e portanto, $0 < k^2 < k < 1$. Como $k^2 \in \mathbb{N}$, temos que $k^2 \in B$ e é seu elemento mínimo, uma contradição pois k é o elemento mínimo de B. Logo, $B = \emptyset$.

Teorema 3 (Princípio da Indução Completa - PIC). Sejam $X \subset \mathbb{N}$ e $m \in \mathbb{N}$, tal que $X = \{n \in \mathbb{N} : m \leqslant n\}$. Se $P(n)$ é uma propriedade sobre n, tal que

(i) $P(m)$ é verdadeira;

(ii) se $P(k)$ é verdadeira para todo natural $k \in \mathbb{N}$, tal que $m \leqslant k \leqslant n$, então $P(n+1)$ também é verdadeira.
Então, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$, ou seja, $\mathbb{N} = X$.

Demonstração. Seja $B \subset \mathbb{N}$ não vazio e que tenha a propriedade $P(n)$, para o qual $P(1)$ é verdadeira e $P(n)$ verdadeira implica que $P(n+1)$ seja verdadeira. Defina o conjunto não vazio

$$A = \{n \in \mathbb{N} : n < m \,\forall\, m \in B\}.$$

Pelo Teorema 2 A possui um menor elemento $a \neq 1$, pois $1 \in B$. Dessa forma, $a-1 \in B$ e por $P(n)$ que satisfaz B, temos que $P(a-1)$ implica em $P((a-1)+1) = P(a)$. Então $a \in B$, uma contradição. Logo, temos que $A = \emptyset$ e $P(n)$ é válida para qualquer $n \in \mathbb{N}$, ou seja, $B = \mathbb{N}$. □

Exemplo 3. A sequência de Fibonacci F_n é uma sequência definida recursivamente por

$$F_1 = 1, F_2 = 1 \quad \text{e} \quad F_n = F_{n-1} + F_{n-2}, \text{ para todo } n \geq 2.$$

Para todo $n, m \in \mathbb{N}$, com $n \geq 2$ temos

$$F_{n+m} = F_{n-1}F_m + F_nF_{m+1}.$$

Seja $P(n)$ a proriedade descrita acima, iremos utilizar o Princípio da Indução Completa sobre m para fazer a verificação pedida.

(i) (*base indutiva*) Para $m = 1$ temos que

$$F_{n+1} = F_n + F_{n-1} = F_nF_1 + F_{n-1}F_2,$$

logo $P(n)$ é verdadeira para $m = 1$.

(ii) (*passo indutivo)* Suponha que para todo $k \in \mathbb{N}$, com $1 \leq k \leq m$, $P(n)$ seja verdadeira, mostraremos que $m+1$ também é verdadeira. Assim,

$$F_{n+(m+1)} = F_{n+m} + F_{n+m-1}.$$

Assumindo a validade da hipótese de indução, ou seja, $F_{n+k} = F_{n-1}F_k + F_nF_{k+1}$ para todo $k = 1, 2 \ldots, m$ temos

$$\begin{aligned} F_{n+(m+1)} &= F_{n-1}F_m + F_nF_{m+1} + F_{n+m-1} \\ &= F_{n-1}F_m + F_nF_{m+1} + F_{n-1}F_{m-1} + F_nF_m \\ &= (F_{n-1}F_m + F_{n-1}F_{m-1}) + (F_nF_{m+1} + F_nF_m) \\ &= F_{n-1}(F_m + F_{m-1}) + F_n(F_{m+1} + F_m) \\ &= F_{n-1}F_{m+1} + F_nF_{m+2}. \end{aligned}$$

Portanto, $P(n)$ é verdadeira para $m+1$ e pelo Princípio da Indução Completa (PIC), segue que $P(n)$ aplica-se a todo $m \in \mathbb{N}$.

Neste exemplo observamos que foi necessário a verificação na base indutiva utilizando os dois primeiros termos da sequência de Fibonacci, assim como utilizamos os dois termos anteriores de $m+1$ no passo indutivo para a determinação da conclusão esperada.

CAPÍTULO

3

DIVISIBILIDADE

Neste capítulo introduziremos resultados, propriedades e definições importantes acerca do estudo de divisibilidade, que subsidiará teoricamente as discussões a serem realizadas nos próximos capítulos.

3.1 Divisibilidade

Ao realizarmos a divisão de um número inteiro por outro número inteiro, podemos obter ou não um quociente inteiro. A existência de uma relação de divisibilidade entre dois números inteiros é expressa na definição a seguir.

Definição 1. Dado os números inteiros a e b, dizemos que a divide b se existir um k inteiro, tal que $b = ak$. Chamamos a de divisor de b e b de múltiplo de a. Denotamos essa relação como $a \mid b$.

Para os casos que a não divide b, escrevemos que $a \nmid b$.

Exemplo 4. Temos em cada caso que

(i) $13 \mid 611$, pois existe um inteiro $k = 47$ tal que $611 = 13.47$;

(ii) $29 \nmid 971$, pois não existe $k \in \mathbb{Z}$ tal que $971 = 29k$.

Na sequência apresentaremos algumas propriedades da divisibilidade.

Proposição 1. Dados a, b, c e $n \in \mathbb{Z}$ temos:

(i) $1 \mid n$

(ii) $n \mid n$.

(iii) $n \mid 0$.

(iv) Se $n \mid a$, então $a = 0$ ou $|n| \leq |a|$.

(v) Se $a \mid b$ e $b \mid c$, então $a \mid c$.

(vi) Se $a \mid b$ e $a \mid c$, então $a \mid (bx+cy)$ para qualquer combinação linear $bx+cy$ de b e c, com coeficientes $x, y \in \mathbb{Z}$.

Demonstração. Sejam a, b, c e $n \in \mathbb{Z}$.

(i), (ii) e (iii) Temos que $n = 1n$ e $0 = 0n$ e pela definição de divisibilidade, segue que $1 \mid n$, $n \mid n$ e $n \mid 0$.

(iv) Suponha que $n \mid a$ e $a \neq 0$, então $a = n.k$ com $k \in \mathbb{Z}$ e $|k| \geq 1$, desse modo temos $|a| \geq |n||k| \geq |n|$.

(v) Como $a \mid b$, então existe um $m \in \mathbb{Z}$ tal que $b = am$. Do fato que $b \mid c$, então $c = b.k = amk$, para algum k inteiro, portanto $a \mid c$.

(vi) Como $a \mid b$ e $a \mid c$ então existem $m, n \in \mathbb{Z}$ tais que $b = am$ e $c = an$. Multiplicando as igualdades respectivamente pelos inteiros x e y temos

$$bx = amx \quad \text{e} \quad cy = any.$$

Somando ambas as igualdades obtemos

$$bx + cy = amx + any = a(mx + ny),$$

e portanto, $a \mid (bx+cy)$.

□

A Proposição acima nos fornece resultados de grande utilidade em muitos problemas aritméticos envolvendo divisibilidade. A seguir realizaremos dois exemplos nos quais se destaca principalmente a propriedade descrita no item (vi).

Exemplo 5. Se $19 \mid (3x+7y)$ então $19 \mid (43x+75y)$.

Da Proposição 1, temos do item (ii) que $19 \mid 19x$ e $19 \mid 19y$, então pelo item (vi) temos que $19 \mid (19x+19y)$. Se $19 \mid (3x+7y)$ então $19 \mid (8(3x+7y))$, ou seja, $19 \mid (24x+56y)$. Desse modo, novamente pelo item (vi) da Proposição 1, temos

$$19 \mid (19x+19y) + (24x+56y),$$

isto é, $19 \mid (43x+75y)$.

Exemplo 6. Para $a, b \in \mathbb{Z}$ temos que $a-b \mid a^n - b^n$, para $n \in \mathbb{N}$.

Seja a propriedade $P(n) : a-b \mid a^n - b^n$, para $n \in \mathbb{N}$. Procederemos por indução sobre n.

(i) Para $n = 1$ temos que $a-b \mid a^1 - b^1 = a-b$, logo $P(1)$ é verdadeira.

(ii) Supondo que $P(n)$ é verdadeira, verificaremos a validade para $P(n+1)$.

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

Pela hipótese de indução temos que $a-b \mid a^n - b^n$ e como $a-b \mid a-b$, da Proposição 1 segue que $a-b \mid a(a^n - b^n) + b^n(a-b)$. Assim, $P(n+1)$ é verdadeira e pelo Teorema 1 temos que $P(n)$ é válida para todo $n \in \mathbb{N}$.

3.1.1 Teorema da Divisão Euclidiana

A partir do teorema que apresentaremos na sequência, verifica-se que é sempre possível realizar a divisão entre dois números inteiros, ainda que um não seja múltiplo do outro. Sua fundamentação deve-se a Euclides que, em sua obra Elementos $(300\, a.C)$, apresenta a descrição do método para tal divisão somente para números naturais e comprimentos geométricos e é considerado um dos algoritmos mais antigos utilizados até os tempos atuais. Entretanto, a metodologia apresentada por Euclides baseava-se em subtrações sucessivas e não considerava a unicidade de alguns dos elementos envolvidos no processo. O algoritmo de Euclides foi generalizado ao longo da história por vários matemáticos, sendo aplicado em diversas áreas da Matemática.

Teorema 4 (Teorema da Divisão Euclidiana). Se a e b são inteiros e $b \neq 0$, então existem q e r inteiros, tais que

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

Os inteiros q e r são denominados quociente e resto da divisão euclidiana de a por b e, na condição dada, são únicos.

Demonstração. Sejam $a, b \in \mathbb{N}$.

Existência

Se $a < b$, então basta tomarmos $q = r = 0$.

Se $a > b$, então fixado o número b, suponhamos a existência de q e r tal que

$$a = bq + r \qquad \text{e} \qquad 0 \leq r < b. \tag{3.1}$$

Seja $P(n)$ a propriedade descrita em (3.1), procederemos por indução sobre a.

(i) Se $a = 1$ e como $b \in \mathbb{N}$, tal que $b \leq a$, temos $b = q = 1$ e $r = 0$. Logo $P(1)$ é verdadeira.

(ii) Suponha a validade de $P(a-1)$, verifiquemos que $P(n)$ satisfaz a. Assim, para $p, s \in \mathbb{Z}$ temos

$$a - 1 = bp + s, \qquad \text{e} \qquad 0 \leq s < b.$$

Logo

$$a = bp + (s+1).$$

Como $0 \leq s < b$ então $0 \leq s+1 < b+1$, ou seja, $0 \leq s+1 \leq b$. Se $s+1 < b$, então segue que $p = q$ e $r = s+1$. Se $s+1 = b$, então $a = bp + b = b(p+1)$. Assim, temos que $q = p+1$ e $r = 0$.

Portanto $P(a)$ é verdadeira e pelo Teorema 1, para todo $a \in \mathbb{N}$, existem q e r que satisfaça a condição descrita em (3.1).

Estenderemos agora o resultado para $a, b \in \mathbb{Z}$. Analisemos inicialmente o caso $a < 0$ e $b > 0$. Pelo resultado anterior temos

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

Logo

$$a = b(-q) + (-r). \tag{3.2}$$

Se $r = 0$ segue que $-q$ é o quociente da divisão euclidiana de a por b. Se $r > 0$, temos

$$\begin{aligned} a &= b(-q) + (-r) \\ &= b(-q) + b - b + (-r) \\ &= b(-q-1) + (b-r). \end{aligned}$$

Como $0 \leq r < b$, segue que $-b < -r < 0$ e somando b aos membros da desigualdade temos $0 < b - r < b$. Fazendo $q_1 = -q - 1$ e $r_1 = b - r$ e substituindo em (3.2), segue que $a = bq_1 + r_1$, onde $0 \leq r_1 < b$.

Para o caso $a < 0$ e $b < 0$ sigamos passos semelhantes, assim temos que

$$-a = -bq + r \qquad \text{e} \qquad 0 \leq r < -b. \tag{3.3}$$

Logo

$$\begin{aligned} a &= bq + (-r) \\ &= bq + b - b + (-r) \\ &= b(q+1) + (-b-r). \end{aligned}$$

Como $0 \leq r < -b$ e do fato que $b < 0$, temos $b < -r < 0$ e somando b aos membros dessa desigualdade segue que $0 < -b - r < -b$. Fazendo $q_2 = q + 1$ e $r_2 = -b - r$ e substituindo em (3.3) temos $a = bq_2 + r_2$, tal que $0 \leq r_2 < b$.

Unicidade

Suponha $r, r', q, q' \in \mathbb{Z}$, tais que

$$a = bq + r \text{ com } 0 \leq r < b \tag{3.4}$$

$$a = bq' + r' \text{ com } 0 \leq r' < b. \tag{3.5}$$

Como $r, r' \in \mathbb{Z}$, sem perda de generalidade, tomemos $r \geq r'$. Igualando o segundo membro das equações (3.4) e (3.5) encontramos

$$\begin{aligned} bq + r &= bq' + r' \\ r - r' &= bq' - bq \\ r - r' &= b(q' - q) \end{aligned} \tag{3.6}$$

Do fato que r e r' são menores que b, segue que $r - r' < b$ e por (3.6) $0 \leq b(q' - q) < b$. Mas como q e q' são inteiros, a desigualdade só é verdadeira para $q' - q = 0$, ou seja, $q' = q$. Consequentemente, $r' - r = 0$, isto é, $r' = r$ e portanto, q e r são únicos.

□

Exemplo 7. Façamos a divisão euclidiana entre os inteiros a e b dados.

(a) Se $a = 857$ e $b = 17$. Temos que $857 = 17.50 + 7$, logo $q = 50$ e $r = 7$.

(b) Se $a = 1323$ e $b = -29$. Temos que $1323 = (-29).46 + 11$, logo $q = 46$ e $r = 11$.

(c) Se $a = -2524$ e $b = 72$. Temos que $-2524 = 72.(-36) + 68$, logo $q = -36$ e $r = 68$.

O Teorema 4 nos permite conclusões ainda mais gerais e abrangentes. Por exemplo, fixando $m \geq 2$ pode-se escrever qualquer número natural n de forma única, como $n = mk + r$, com $k \in \mathbb{Z}$ e $0 \leq r < m$. Desse modo, para $m = 2$ temos que

$$n = 2k \quad \text{ou} \quad n = 2k + 1,$$

pois o resto r na divisão de um inteiro por 2 é 0 ou 1. Ainda, temos que $2k$ e $2k + 1$ são, respectivamente, a representação dos números pares e ímpares, ou seja, o conjunto dos números inteiros dividem-se em duas classes a partir da divisão euclidiana de seus elementos por 2.

O mesmo vale se tomarmos diferentes valores de m, para $m = 5$ por exemplo, temos que n poderá ser representado por uma das formas: $5k, 5k+1, 5k+2, 5k+3$ ou $5k+4$. Essa importante consequência do Teorema 4 será explorada ao longo deste trabalho sob várias perspectivas.

Utilizaremos a divisão euclidiana na verificação do teorema abaixo.

Teorema 5 (Representação dos números decimais). Para cada $n \in \mathbb{Z}$ e $n > 0$, existem únicos naturais $0 \leq a_0, a_1, \ldots, a_k < 10$, com $a_k \neq 0$ e $k \in \mathbb{Z}$, tais que

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_0 10^0.$$

Demonstração. Seja $P(n)$ a propriedade sobre n descrita, de modo que aplicaremos o Teorema 3 sobre n.

(i) Para $n = 1$ temos que $1 = a_0 10^0 = a_0$, logo $P(1)$ é verificada.

(ii) Suponhamos que para todo $x \in \mathbb{N}$, tal que $1 \leq x \leq n$ a propriedade $P(n)$ seja verdadeira, mostraremos sua validade para $n+1$. Pelo Teorema 4 temos

$$n+1 = bq + r, \qquad \text{com} \quad 0 \leq r < b.$$

Tomando $b = 10$ obtemos

$$n+1 = 10q + r, \qquad 0 \leq r < 10. \tag{3.7}$$

Do fato que $n, b \in \mathbb{N}$, segue que $q \geq 0$ e dessa forma temos dois casos a considerar:

- Se $q = 0$, então $n+1 = r = a_0$.
- Se $q > 0$, então $q < n$, pois para $q > n$ temos que $n+1 = 10q + r > 10n + r \geq 10n$, ou seja, $n+1 > 10n$ o que implica em $1 > 9n$, uma contradição.

Desse modo, para $1 \leq q \leq n$ e aplicando a hipótese de indução em (3.7) segue

$$\begin{aligned} n+1 &= 10(a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_0) + r \\ &= a_k 10^{k+1} + a_{k-1} 10^k + \ldots + a_0 10 + r \end{aligned}$$

Portanto, $P(n+1)$ é verdadeira e pelo Teorema 3, $P(n)$ é verdadeira para todo $n \in \mathbb{N}$. □

3.2 Máximo Divisor Comum (MDC)

Dados os inteiros a, b e x, todos diferentes de zero de forma que $x \mid a$ e $x \mid b$, pela propriedade (iv) da Proposição 1 temos que

$$|x| \leq |a| \iff -|a| \leq x \leq |a| \tag{3.8}$$

$$|x| \leq |b| \iff -|b| \leq x \leq |b|. \tag{3.9}$$

Desse modo, o conjunto de (3.8) dos divisores $D(a)$ de a é limitado superiormente por $|a|$ e finito. Do mesmo modo, temos em (3.9) o conjunto $D(b)$ dos divisores de b que é limitado superiormente por $|b|$. Analisando $D(a) \cap D(b)$, verifica-se que é não vazio, pois $1 \mid a$ e $1 \mid b$, portanto pelo Teorema 2 possuiu um elemento máximo $d \geq 1$, que chamamos de *máximo divisor comum* de a e b. Denotaremos o máximo divisor comum d de a e b como $\text{mdc}(a,b)$. Para $a, b = 0$ definimos $\text{mdc}(0,0) = 0$.

Definição 2. Sejam os inteiros a, b e d, com $d \geq 0$, diremos que o $\text{mdc}(a,b) = d$ quando as seguintes propriedades são satisfeitas:

(i) $d \mid a$ e $d \mid b$.

(ii) Para todo $c \in \mathbb{Z}$, se $c \mid a$ e $c \mid b$, então $c \mid d$.

Observação 1. A implicação (ii) na definição acima, nos permite verificar a unicidade de d. Seja d e $d^{'}$ $\text{mdc}(a,b)$. Pela propriedade (ii) temos que $d \mid d^{'}$ e $d^{'} \mid d$ e como $d \geq 0$, então $d = d^{'}$. Assim, o mdc $(a,b) = d$ é único.

Exemplo 8. Vamos determinar o $\text{mdc}(15,27)$.

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

$$D(27) = \{-27, -9, -3, -1, 1, 3, 9, 27\}.$$

Temos que $D(a) \cap D(b) = \{-3, -1, 1, 3\}$, portanto o $\text{mdc}(15,27) = 3$.

Proposição 2. Sejam $a, b \in \mathbb{Z}$.

(i) $\text{mdc}(0,a) = |a|$.

(ii) $\text{mdc}(1,a) = 1$.

(iii) $a \mid b$ se, e somente se, $\text{mdc}(a,b) = |a|$.

Demonstração. Sejam a, b e $c \in \mathbb{Z}$.

(i) Se $a = 0$, então $\text{mdc}(0,0) = 0 = |a|$. Se $a \neq 0$, então $|a| \mid 0$ e $|a| \mid a$. Tome $c \neq 0$ de modo que $c \mid a$ e $c \mid 0$, então por (iv) da Proposição 1 tem-se que $c \leq |a|$, o que implica em $c \mid |a|$.

(ii) Temos que $1 \mid a$ e $1 \mid 1$. Tome $c \neq 0$, de forma que $c \mid a$ e $c \mid 1$, então por (iv) da Proposição 1 tem-se que $|c| \leq 1$. Como 1 é seu maior divisor, segue que $c = 1$, portanto $c \mid d$, ou seja, $d = 1$.

(iii) Se $a \mid b$, então $|a| \mid a$ e $|a| \mid b$. Seja $c \neq 0$, se $c \mid a$ e $c \mid b$, então $c \mid |a|$, portanto $\text{mdc}(a,b) = |a|$. Reciprocamente, se $\text{mdc}(a,b) = |a|$, então $|a| \mid b$ e consequentemente, $a \mid b$.

□

O lema abaixo fundamenta um método para determinação do $\text{mdc}(a,b)$ para quaisquer $a, b \in \mathbb{Z}$.

Lema 1 (Euclides). Sejam $a, b, q \in \mathbb{Z}$ e r o resto da divisão euclidiana de a por b. Se $a = bq + r$, então $\text{mdc}(a,b) = \text{mdc}(b,r)$.

Demonstração. Queremos mostrar que $D(a) \cap D(b) = D(b) \cap D(r)$, implicando que ambos os conjuntos possuem o mesmo elemento máximo. De $a = bq + r$ segue que $r = a - bq$.

Seja $d \in D(a) \cap D(b)$, então $d \mid a$ e $d \mid b$ e por (vi) da Proposição 1, temos que $d \mid a - bq$ e como $a - bq = r$, então $d \mid r$ e, portanto, $d \in D(b) \cap D(r)$.

Do mesmo modo, se $d \in D(b) \cap D(r)$ então $d \mid b$ e $d \mid r$, logo $d \mid bq + r$ e como $bq + r = a$, então $d \mid a$ e, portanto, $d \in D(a) \cap D(b)$.

Assim, $D(a) \cap D(b) = D(b) \cap D(r)$ e $\text{mdc}(a,b) = \text{máx}\, D(a) \cap D(b) = \text{máx}\, D(b) \cap D(r) = \text{mdc}(b,r)$. □

Observação 2. Note que podemos escrever o Lema de Euclides como $\text{mdc}(a,b) = \text{mdc}(b, a - bq) = \text{mdc}(a, b - aq)$, no qual $a - bq$ é o resto da divisão euclidiana de a por b e $b - aq$, o resto da divisão euclidiana de b por a.

Exemplo 9. Dado o Lema 1, temos as identidades:

$$\text{mdc}(3,12) = \text{mdc}(3, 12 + 3.3) = \text{mdc}(3, 12 + 3.7) = \text{mdc}(3, 12 - 3.11).$$

Exemplo 10. Vamos calcular o $\text{mdc}(1095, 780)$.

Aplicando sucessivamente a divisão euclidiana temos as igualdades

$$\begin{aligned} 1095 &= 780.1 + 315 \\ 780 &= 315.2 + 150 \\ 315 &= 150.2 + 15 \\ 150 &= 15.10 + 0. \end{aligned}$$

Assim, pelo Lema 1 segue que $\text{mdc}(1095,780) = \text{mdc}(780,315) = \text{mdc}(315,150) = \text{mdc}(150,15) = \text{mdc}(15,0) = 15$.

Observa-se que, além de determinar um método para o cálculo do mdc entre dois números inteiros quaisquer, o Lema 1 nos permite escrever o mdc entre esses números a partir da soma de dois de seus múltiplos. No Exemplo 10 temos

$$\begin{aligned} 15 &= 315 - 150.2 \\ &= 315 - 2(780 - 315.2) \\ &= 1095 - 780 - 2.780 + 4(1095 - 780) \\ &= 1095(5) + 780(-7). \end{aligned}$$

Uma outra observação que se pode fazer no Exemplo 10, é que o último resto não nulo é exatamente o mdc procurado. Será uma mera coincidência? Verificaremos a seguir que não.

Lema 2. Seja $a, b \in \mathbb{Z}$ e $a \geq b$. Defina-se a sequência (r_k), com $k \in \mathbb{N}$, de modo que $r_1 = a$, $r_2 = b$ e para todo $k \geq 2$, se $r_k \neq 0$, r_{k+1} é o resto da divisão euclidiana de r_k por r_{k-1} e se $r_k = 0$, então a sequência termina.
Então a sequência (r_k) é finita e existe um k tal que $r_{k+1} = 0$.

Demonstração. Defina-se o conjunto $A = \{r_1, r_2, \ldots\} \subset \mathbb{N} \cup \{0\}$. Notavelmente, $A \neq \emptyset$ e pelo Teorema 2 ele possuiu um elemento mínimo que denotaremos por r_{k+1}. Pela definição da sequência (r_k) segue que $r_1 \geq r_2 > \ldots > r_k > r_{k+1}$ e se $r_{k+1} \neq 0$, então existe um elemento $r_{k+2} \in A$ tal que é o resto da divisão euclidiana de r_k por r_{k+1}. Logo $0 \leq r_{k+2} < r_{k+1}$, ou seja, r_{k+2} é elemento mínimo de A, uma contradição, pois r_{k+1} é seu elemento mínimo.

□

Teorema 6 (Algoritmo Euclidiano Estendido). Sejam $a, b \in \mathbb{Z}$ não nulos com $a \geq b$ e seja (r_k) a sequência definida no Lema 2, então

$$\text{mdc}(a,b) = r_k.$$

Demonstração. Pela definição de (r_k) temos que

$$r_1 \geq r_2 > \ldots > r_k > r_{k+1} = 0,$$

e para $k \geq 3$ temos que r_k é o resto da divisão euclidiana de r_{k-2} por r_{k-1}. Aplicando sucessiva-

mente o Lema 1 em cada uma das igualdades abaixo segue:

$$\begin{aligned} r_k &= \text{mdc}(r_k, r_{k+1}) = \text{mdc}(r_k, 0) \\ &= \text{mdc}(r_k, r_{k-1}) \\ &= \text{mdc}(r_{k-1}, r_{k-2}) \\ &= \quad \ldots \\ &= \text{mdc}(r_3, r_2) \\ &= \text{mdc}(r_2, r_1) \\ &= \text{mdc}(a, b). \end{aligned}$$

□

Dessa forma, temos pelo Lema 2 e pelo Teorema 6 que a sequência de divisões euclidianas realizadas no Exemplo 10 é uma caracterização geral, que se aplica a todo par de números inteiros que se busque determinar o mdc, isto é, teremos sempre um último resto nulo e o resto imediatamente anterior, será o mdc procurado.

Exemplo 11. Qual o maior valor possível para o $\text{mdc}(n+1, n^3+7)$?

Observe que $n^3+1 = (n+1)(n^2-n+1)$, então temos que

$$n^3+7 = n^3+1+6 = (n+1)(n^2-n+1)+6.$$

Pelo Lema 1 segue

$$\text{mdc}(n+1, n^3+7) = \text{mdc}(n+1, (n+1)(n^2-n+1)+6) = \text{mdc}(n+1, 6).$$

Assim, para o maior mdc possível basta tomar $n = 5$ portanto, o mdc procurado é 6.

Exemplo 12. Sejam m e n dois inteiros positivos e seja $a > 1$, se $d = \text{mdc}(m, n)$, tem-se que

$$\text{mdc}(a^m - 1, a^n - 1) = a^d - 1.$$

Suponha, sem perda de generalidade, que $m \geq n$. Fazendo a divisão euclidiana de m por n obtemos

$$m = nq + r, \qquad 0 \leq r < n.$$

Desse modo, reescrevemos

$$a^m - 1 = a^{nq+r} - 1 = a^{nq}a^r - 1 = a^{nq}a^r - a^r + a^r - 1 = a^r(a^{nq} - 1) + (a^r - 1). \tag{3.10}$$

Pelo Exemplo 6 temos que $a^n - 1 \mid a^{nq} - 1$, ou seja, $a^{nq} - 1$ é múltiplo de $a^n - 1$. Logo, pelo Lema 1 e por (3.10) temos

$$\text{mdc}(a^m - 1, a^n - 1) = \text{mdc}(a^n - 1, a^r(a^{nq} - 1) + (a^r - 1)) = \text{mdc}(a^n - 1, a^r - 1). \quad (3.11)$$

Como r é tal que $0 \leq r < n$, então seja $r_1 \geq r_2 > \ldots > r_k > r_{k+1}$ a sequência definida por r tal que $r_{k+1} = 0$. Dessa forma, temos pelo Teorema 6 que $r_k = \text{mdc}(m,n)$ e aplicando em (3.11) encontramos

$$\begin{aligned}
\text{mdc}(a^m - 1, a^n - 1) &= \text{mdc}(a^n - 1, a^{r_1} - 1) \\
&= \text{mdc}(a^{r_1} - 1, a^{r_2} - 1) \\
&= \quad \ldots \\
&= \text{mdc}(a^{r_k} - 1, a^{r_{k+1}} - 1) \\
&= \text{mdc}(a^{r_k} - 1, 0) \\
&= a^{r_k} - 1 \\
&= a^{\text{mdc}(m,n)} - 1 \\
&= a^d - 1.
\end{aligned}$$

O teorema a seguir nos fornece uma outra caracterização do máximo divisor comum entre dois números inteiros.

Teorema 7 (Bachet Bezout). Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, então

$$\text{mdc}(a,b) = \text{mín}\{x \in \mathbb{Z} : x = am + bn, \text{para } m,n \in \mathbb{Z}\}.$$

Demonstração. Seja $d = am + bn$ o menor elemento positivo do conjunto $X = \{x \in \mathbb{Z} : x = am + bn, \text{para } m,n \in \mathbb{Z}\}$. É possível verificar que $|a| + |b|$ gera uma combinação linear positiva e pelo Teorema 2 podemos afirmar a existência de d. Seguiremos as propriedades descritas na Definição 2 para verificar que $d = \text{mdc}(a,b)$.

Fazendo a divisão euclidiana de a por d temos que

$$a = dq + r, \qquad 0 \leq r < d,$$

logo

$$r = a - dq = a - (am + bn)q = a(1 - mq) + b(-nq),$$

portanto r é uma combinação linear de a e b. Como $0 \leq r < d$ teríamos que r seria o elemento mínimo de X, então $r = 0$ e $d \mid a$.

Analogamente, temos que

$$b = dq_1 + r_1, \qquad 0 \leq r_1 < d,$$

logo

$$r_1 = b - dq_1 = b - (am + bn)q_1 = b(1 - mq_1) + a(-nq_1),$$

portanto r_1 é uma combinação linear de a e b. Do fato de $0 \leq r_1 < d$, teríamos r_1 como elemento mínimo de X, então $r_1 = 0$ e $d \mid b$.

Seja c um divisor comum de a e b, então $c \mid a \iff a = ck$ e $c \mid b \iff b = ck_1$, para $k, k_1 \in \mathbb{Z}$. Logo

$$d = am + bn = ckm + ck_1 n = c(km + k_1 n),$$

portanto $c \mid d$. □

A consequência do Teorema 7 que mostraremos a seguir, nos garante que as combinações lineares possíveis para $ax + by$, com $x, y \in \mathbb{Z}$, são múltiplos de d.

Corolário 1. Sejam $a, b \in \mathbb{Z}$, ambos não nulos, e seja $d = \text{mdc}(a, b)$. Então

$$\{ax + by : x, y \in \mathbb{Z}\} = \{dz : z \in \mathbb{Z}\}.$$

Demonstração. Defina $A = \{ax + by : x, y \in \mathbb{Z}\}$ e $B = \{dz : z \in \mathbb{Z}\}$. Nosso intuito é mostrar que $A \subseteq B$ e $B \subseteq A$.

Pelo Teorema 7 existem x_0, y_0 tais que $d = ax_0 + by_0$, logo $d \in A$. Seja $r \in \mathbb{Z}$, temos que $dr = rax_0 + rby_0$ e portanto, $dr \in B$ e $B \subseteq A$. Como $d \mid ax + by$ para qualquer $ax + by \in A$, então $A \subseteq B$ e logo $A = B$. □

Exemplo 13. Quantos inteiros n, com $1 \leq n \leq 100$, podem ser escritos na forma

$$n = 462x + 966y?$$

Inicialmente, determinaremos o $\text{mdc}(462, 966)$ utilizando o Teorema 6:

$$966 = 462.2 + 42$$

$$462 = 42.11 + 0,$$

logo o $\text{mdc}(462, 966) = 42$. Pelo Teorema 7 segue que $n = 42 = 462x + 966y$ é o menor valor positivo para n e pelo Corolário 1 conclui-se que $n = 42z$, para $z \in \mathbb{Z}$. Assim, os múltiplos de 42 no intervalo dado são 42 e 84 e desse modo, existem 2 inteiros que satisfazem as condições dadas para n.

Definição 3. Dois números $a, b \in \mathbb{Z}$, ambos não nulos, são chamados de *primos entre si* se, e somente se, o $\text{mdc}(a, b) = 1$.

Exemplo 14. Os números 18 e 35 são primos entre si, pois o $\text{mdc}(18,35) = 1$.

Proposição 3. Dados $a, b \in \mathbb{Z}$, ambos não nulos, eles serão primos entre si se, e somente se, existirem $x, y \in \mathbb{Z}$ tais que

$$ax + by = 1.$$

Demonstração. Se $\text{mdc}(a,b) = d = 1$, então pelo Teorema 7 existem $r, s \in \mathbb{Z}$ tais que $ar + bs = 1$. Reciprocamente, se existem $r, s \in \mathbb{Z}$, tais que $ar + bs = 1$, temos pelo Corolário 1 que 1 é múltiplo de d, isto é, $d \mid 1$ e portanto $d = 1$. □

Proposição 4. Sejam a, b e $c \in \mathbb{Z}$ e $\text{mdc}(a,b) = 1$, se $a \mid bc$ então $a \mid c$.

Demonstração. Do fato que $a \mid bc$, então $bc = ak$, para $k \in \mathbb{Z}$. Como o $\text{mdc}(a,b) = 1$, segue pela Proposição 3 que existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Multiplicando a última igualdade por c temos

$$c = cax + cby = acx + aky = a(cx + ky),$$

portanto $a \mid c$. □

3.3 Números Primos e Teorema Fundamental da Aritmética

Definição 4 (Números Primos). Um número inteiro $p > 1$ é chamado de primo se tem como únicos divisores positivos p e 1. Denotamos por

$$\mathscr{P} = \{p \in \mathbb{N} : \text{p é primo}\}$$

o conjunto dos números primos.

Segue da definição que

$$p \in \mathscr{P} \iff p = ab, \text{ para } a, b \in \mathbb{N} \text{ tal que } a = 1 \text{ ou } b = 1.$$

Os números $n > 1$ não primos são chamados números compostos, sua caracterização é dada por

$$\mathscr{T} = \{n \in \mathbb{N} : n = x_0 x_1, \text{ com } x_0, x_1 > 1 \text{ e } x_0, x_1 \in \mathbb{N}\}.$$

Proposição 5. Sejam a, b e $p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

Demonstração. Temos que $p \mid a$ ou $p \nmid a$. Se $p \nmid a$, então $\text{mdc}(p,a) = 1$ e como $p \mid ab$, segue da Proposição 4 que $p \mid b$. □

Observação 3. A Proposição acima nos coloca a condição mínima para um dado primo p, tal que $p \mid ab$, pois p pode ser fator de ambos os números e assim, a divisibilidade é trivial.

Corolário 2. Dada a sequência de primos $p, p_1, p_2, \ldots, p_n$ e se $p \mid p_1 p_2 \ldots . p_n$, então $p = p_k$, para algum $k \in \{1, 2, \ldots, n\}$.

Demonstração. Seja a propriedade $P(n) : p \mid p_1 p_2 \ldots . p_n$, então $p = p_k$ para algum $k \in \{1, 2, \ldots, n\}$. Procederemos por indução sobre n que é a quantidade de primos p_k.

(i) Para $n = 1$ temos que se $p \mid p_1$ então $p = p_1$, pois p, p_1 são primos, logo $P(1)$ é verdadeira.

(ii) Suponha que $P(n)$ seja verdadeira para n, mostraremos a validade para $n+1$, ou seja, que

$$p \mid p_1 p_2 \ldots . p_n p_{n+1} \Longrightarrow p = p_k \text{ para algum } k \in \{1, 2, \ldots, n+1\}.$$

Pela Proposição 5 temos que $p \mid p_1 p_2 \ldots . p_n$ ou $p \mid p_{n+1}$. Pela hipótese de indução temos que se $p \mid p_1 p_2 \ldots . p_n$, então $p = p_k$ para algum $k \in \{1, 2, \ldots, n\}$, logo $p \nmid p_{n+1}$. Se $p \nmid p_1 p_2 \ldots . p_n$, então $p \mid p_{n+1}$ e portanto $p = p_{n+1}$.

Dessa forma $P(n+1)$ é verdadeira e pelo Teorema 1, $P(n)$ é válida para todo $n \in \mathbb{N}$. □

Teorema 8 (Teorema Fundamental da Aritmética). Todo número inteiro n, com $n > 1$, pode ser escrito de maneira única, a menos de ordem, como um produto de números primos.

Demonstração. Provaremos primeiramente a caracterização de n como fatoração de primos. Seja a propriedade $P(n) : n \in \mathbb{N}$, tal que para $n > 1$, n é um produto de primos. Faremos a indução completa sobre n.

(i) Para $n = 2$ temos que $P(2)$ é verdadeira, pois 2 é um número primo.

(ii) Se n é um número primo, então a verificação de $P(n)$ é imediata. Consideraremos então n composto, isto é, $n = x_1 x_2$, com $1 < x_1 < n$ e $1 < x_2 < n$, x_1, x_2 inteiros.

Suponha que para todo m tal que $2 \leq m \leq n$ onde $P(m)$ seja verdadeira, mostraremos a validade de $P(n+1)$.

Como $n+1$ é composto, então $n+1 = x_3 x_4$, tal que $1 < x_3 < n+1$ e $1 < x_4 < n+1$ e pela hipótese de indução existem primos $p_1, p_2, \ldots, p_r$ e $q_1, q_2, \ldots, q_s$ de forma que $x_3 = p_1 p_2 \ldots p_r$ e $x_4 = q_1 q_2 \ldots q_s$. Logo

$$n+1 = x_3 x_4 = (p_1 p_2 \ldots p_r)(q_1 q_2 \ldots q_s).$$

Logo $P(n+1)$ é verdadeira e pelo Teorema 3, temos que $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Provaremos a unicidade da fatoração de n em fatores primos. Dados os números primos p_i e q_j, com $i \in \{1, 2, \ldots, r\}$ e $j \in \{1, 2, \ldots, s\}$ e seja a propriedade $P(n) : n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$, para $n \in \mathbb{N}$ e $n > 1$, tal que $r = s$ e $p_i = q_j$. Procederemos por indução completa sobre n

(i) Para $n = 2$ temos que $2 = p_1 = q_1$, logo $P(2)$ é verdadeira.

(ii) Suponha que exista x tal que $2 \leq x < n$ de forma que $P(x)$ seja verdadeira. Mostraremos a validade de $P(n)$.

Se n é primo, então $n = p_r = q_s$ e a propriedade é verificada. Tomemos n composto, então

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s.$$

Temos que $p_1 \mid q_1 q_2 \dots q_s$ e pelo Corolário 2, tem-se que $p_1 = q_j$. Sem perda de generalidade, consideremos $p_1 = q_1$, portanto temos

$$n/p_1 = p_2 p_3 \dots p_r = q_2 q_3 \dots q_s.$$

Como $1 < n/p_1 < n$, temos pela hipótese de indução que as fatorações de n/p_1 são iguais, logo $r = s$ e p_i e p_j são iguais aos pares.

Assim, $P(n)$ é verdadeira e pelo Teorema 3, $P(n)$ é válida para todo $n \in \mathbb{N}$. □

A existência de infinitos números primos foi demonstrada primeiramente por Euclides, em sua obra *Os Elementos* (Livro IX, Proposição 20), é possível ter maiores detalhes em (JOYCE, 2013).

Teorema 9. Existem inifinitos números primos.

Demonstração. Seja $p_1, p_2, \dots, p_n$ uma sequência finita de primos. Seja a um número inteiro e $a > 1$, de forma que

$$a = p_1.p_2.\dots.p_n + 1.$$

Observe que para cada p_i da sequência definida, com $i \in \{1, 2, \dots, n\}$, temos que $p_i < a$. Se a é primo, então $a = p_j$ que não pertence a sequência de primos dada, comprovando a infinidade de primos.

Se a não é primo, então pelo Teorema 8 ele tem um fator primo q_k, tal que $q_k \neq p_i$. De fato, se $q_k = p_i$ teríamos que $q_k \mid p_1.p_2.\dots.p_n$ e $q_k \mid a$, e por (vi) da Proposição 1, segue que $q_k \mid p_1.p_2.\dots.p_n - a$. Dessa forma, $q_k \mid 1$, uma contradição já que q_k é primo.

Assim, existe um primo q que é fator de a e não pertence a sequência finita $p_1, p_2, \dots, p_n$ portanto, o conjunto de números primos é infinita. □

Teorema 10. Para todo $n \in \mathbb{Z}$, com $n > 1$, existem únicos primos distintos $p_1, p_2, \dots, p_r$, com $r > 1$, de modo que $p_1 < p_2 < \dots < p_r$ e únicos $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{N} \cup \{0\}$, tais que

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}.$$

Demonstração. Se n é primo não há nada a demonstrar. Para n composto temos pelo Teorema 8 que $n = p_1 p_2 \dots p_k$, para $k \in \{1, 2, \dots, r\}$, logo se p_i é único na fatoração, basta tomar $\alpha_i = 1$. Se existe $p_j = p_k$, então agrupando tais fatores primos comuns temos p_j^m, onde m é a quantidade de fatores $p_j = p_k$, assim basta tomar $\alpha_j = m$. Ainda pelo Teorema 8 temos a unicidade da representação. □

Exemplo 15. Seja $n = 2600$, então temos:

$$2600 = 2.2.2.5.5.13 = 2^3.5^2.13^1.$$

Vejamos a caracterização dos divisores de um número inteiro considerando sua decomposição em fatores primos.

Proposição 6. Seja $n \in \mathbb{Z}$, com $n > 1$, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, tal que $p_1 < p_2 < \dots < p_r$ são números primos e $\alpha_1, \alpha_2, \dots, \alpha_r \in \mathbb{N} \cup \{0\}$, então cada divisor positivo $a > 1$ de n é da forma

$$a = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}, \text{ com } 0 \leq \beta_i \leq \alpha_i,$$

para $i \in \{1, 2, \dots, r\}$.

Demonstração. Se $a = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$, com $0 \leq \beta_i \leq \alpha_i$, temos pelo Teorema 10 e do fato de $\alpha_i - \beta_i \geq 0$ que existe um inteiro k, tal que $k = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_r^{\alpha_r - \beta_r}$. Assim,

$$ak = (p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r})(p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \dots p_r^{\alpha_r - \beta_r}) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = n,$$

logo $a \mid n$.

Por outro lado, pela unicidade da fatoração de a e n, segue que todo divisor de n tem que ser dessa forma.

□

O resultado acima não só caracteriza todos os divisores naturais de um número inteiro, como fornece uma forma de determiná-los. Vejamos o exemplo.

Exemplo 16. Façamos a decomposição em fatores primos de 180:

$$180 = 2^2.3^2.5.$$

Note que os primos presentes na fatoração de 180 são $2, 3$ e 5, com expoentes $2, 2$ e 1, respectivamente. Desse modo, temos que os divisores positivos de 180 e diferentes de 1 são aqueles que contém ao menos um desses fatores, com expoentes menores ou iguais a 2 - para os números primos 2 e 3, igual a 1 - para o número primo 5. Utilizando-se do *Princípio Fundamental da*

Contagem sabemos que $3.3.2 = 18$ é o total de divisores positivos de 180. Assim, descrevendo os divisores de 180 temos:

1	3	$3^2 = 9$	5	$3.5 = 15$	$3^2.5 = 45$
2	$2.3 = 6$	$3^2.2 = 18$	$2.5 = 10$	$2.3.5 = 30$	$2.3^2.5 = 90$
$2^2 = 4$	$2^2.3 = 12$	$2^2.3^2 = 36$	$2^2.5 = 20$	$2^2.3.5 = 60$	$2^2.3^2.5 = 180$

A proposição abaixo nos fornece uma outra maneira de determinar o mdc entre dois números inteiros positivos.

Proposição 7 (Cálculo do mdc por fatoração). Sejam $a, b \in \mathbb{N}$, tais que $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$ e $p_1 < p_2 < \dots < p_r$ são números primos de forma que para todo $i \in \{1, 2, \dots, r\}$, temos $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}$. Então

$$\text{mdc}(a,b) = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r},$$

de modo que para cada i, $\gamma_i = \text{mín}\{\alpha_i, \beta_i\}$.

Demonstração. Seja o $\text{mdc}(a,b) = d$. Se $d = 1$, a comprovação é imediata, basta tomar $p_i^{\gamma_i}$ com $\gamma_i = 0$. Então seja $d \neq 1$, tal que $d = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_r^{\gamma_r}$ e $\gamma_i = \text{mín}\{\alpha_i, \beta_i\}$. Pela Proposição 6 temos que $d \mid a$ e $d \mid b$. Considere-se $c \in \mathbb{N}$ tal que $c \mid a$ e $c \mid b$, então pela Proposição 6 temos que $c = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \dots p_r^{\varepsilon_r}$, no qual para cada i que se tome, $0 \leq \varepsilon_i \leq \alpha_i, \beta_i$. Dessa forma $\varepsilon_i \leq \text{mín}\{\alpha_i, \beta_i\}$ e portanto $c \mid d$ e $d = \text{mdc}(a,b)$.

□

Exemplo 17. Calcularemos o $\text{mdc}(600, 1260)$ aplicando a decomposição em fatores primos. Fazendo a decomposição dos números dados em fatores primos temos:

$$600 = 2^3.3.5^2 = 2^3.3.5^2.7^0, \tag{3.12}$$

$$1260 = 2^2.3^2.5.7 = 2^2.3^2.5.7. \tag{3.13}$$

Comparando os primos existentes nas fatorações de ambos os números de (3.12) e (3.13) e aplicando a Proposição 7, segue que

$$\text{mdc}(600, 1260) = 2^2.3.5.7^0 = 60.$$

Observação 4. A fatoração de um número inteiro é uma ferramenta que nos possibilita uma variedade de aplicações e resultados. Contudo, é importante observar que, ao depararmos com números inteiros de ordens numéricas maiores, determinar se um número inteiro é primo ou composto não é uma tarefa simples.

Exemplo 18. A fatoração do número $2438297 = 757.3221$, note que para chegar a esses fatores, sem um recurso tecnológico, depara-se com a análise das possibilidades de divisibilidade pelos 133 números primos anteriores a 757. O mesmo pensamento aplica-se para o fator 3221, de modo que existem 321 números primos entre os dois fatores.

CAPÍTULO

4

ARITMÉTICA DOS RESTOS

São muitos os fenômenos do nosso cotidiano que estão relacionados à ideia de períodos ou ciclos: eventos que ocorrem uma vez na semana, sempre num mesmo dia, têm ciclos de 7 dias; a rotação da Terra em torno de seu eixo tem ciclo de 24 horas e sua translação em torno do Sol tem ciclo de 365 dias e 6 horas; os hodômetros dos carros têm ciclo de 100.000 km; os rerlógios de ponteiro têm um ciclo de 12 horas. Em tais situações notamos que, conhecendo o período de um dado fenômeno cíclico, prevemos exatamente suas repetições. Tais possibilidades relacionam-se a uma aritmética curiosa e peculiar: a aritmética dos restos.

Introduziremos neste capítulo o estudo dos restos da divisão euclidiana por um número inteiro positivo, pela luz dos estudos de Karl Friedrich Gauss, em seu livro *Disquisitiones Arithmeticae*.

4.1 Congruências

Definição 5. Seja $m \in \mathbb{N}$, diremos que dois números inteiros a e b *são congruentes módulo* m se os restos da divisão euclidiana de a e b por m são iguais. Sendo assim, escreve-se:

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

Vejamos alguns exemplos:

(i) $23 \equiv 10 \pmod{13}$, pois ambos deixam resto 10 na divisão por 13.

(ii) $49 \equiv 14 \pmod{5}$, pois ambos deixam resto 4 na divisão por 5.

(iii) $13 \equiv -1 \pmod{7}$, pois ambos deixam resto 6 na divisão por 7.

(iv) $16 \not\equiv 5 \pmod{3}$, pois o resto da divisão euclidiana de 16 e 5 por 3 são respectivamente 1 e 2.

Observação 5. Como a divisão de um número inteiro qualquer por 1 deixará sempre um resto nulo, nossos estudos utilizarão os valores para $m > 1$, no qual $m \in \mathbb{N}$.

Contudo, não seria prático precisarmos realizar a divisão euclidiana entre números a e b por um dado m para atestar sua congruência. A proposição a seguir será de grande valia neste quesito, servindo de instrumento para aplicações futuras e apoio para vários resultados na sequência.

Proposição 8. Sejam $a, b, m \in \mathbb{Z}$, tais que $m > 1$. Então $a \equiv b \pmod{m}$ se, e somente se, $m \mid b - a$.

Demonstração. Pelo Teorema 4 temos

$$a = mq_1 + r_1 \qquad \text{e} \qquad b = mq_2 + r_2,$$

no qual $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Supondo $a \equiv b \pmod{m}$ temos que $r_1 = r_2$ e desta forma

$$\begin{aligned} b - a &= mq_2 + r_2 - (mq_1 + r_1) \\ &= m(q_2 - q_1) + (r_2 - r_1) \\ &= m(q_2 - q_1). \end{aligned}$$

Portanto, pela Definição 1, $m \mid b - a$.

Agora considere, sem perda de generalidade, que $a < b$. Por hipótese sabemos que $m \mid (b - a)$, isto é, existe $q_3 \in \mathbb{Z}$, tal que $b - a = mq_3$. Assim,

$$\begin{aligned} mq_3 &= b - a \\ mq_3 &= (mq_2 + r_2) - (mq_1 + r_1) \\ mq_3 &= m(q_2 - q_1) + (r_2 - r_1) \\ (r_2 - r_1) &= mq_3 - m(q_2 - q_1) \\ (r_2 - r_1) &= m(q_3 - q_2 + q_1). \end{aligned}$$

Seja $k = q_3 - q_2 + q_1$. Considere os casos:

- $k > 0$. Então $r_2 = mk + r_1 \Rightarrow r_2 \geq mk \geq m$, um absurdo, pois $0 \leq r_2 < m$.
- $k < 0$. Então $r_1 = -mk + r_2 \Rightarrow r_1 \geq -mk \geq m$, um absurdo, pois $0 \leq r_1 < m$.

Dessa forma concluímos que $k = 0$, equivalentemente, $r_1 - r_2 = 0$. Logo, $r_1 = r_2$ e, portanto, $a \equiv b \pmod{m}$.

□

A operação de congruência define uma relação de equivalência, cuja a apresentação formal e com maiores detalhes será apresentada no Capítulo 5. A proposição a seguir descreve três propriedades das congruências.

Proposição 9. Sejam $a, b, c, m \in \mathbb{Z}$ tais que $m > 1$. Então:

(i) **Reflexiva**: $a \equiv a \pmod{m}$.

(ii) **Simétrica**: Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.

(iii) **Transitiva**: Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.

Demonstração. Para cada a, b e c inteiros segue:

(i) Como $m \mid a - a$, então segue da Proposição 8 que $a \equiv a \pmod{m}$.

(ii) Como $a \equiv b \pmod{m}$, então $m \mid b - a$. Dessa forma $m \mid -(b-a)$ e consequentemente $m \mid a - b$. Portanto, $b \equiv a \pmod{m}$.

(iii) Como $a \equiv b \pmod{m}$ temos que $m \mid b - a$, ou seja, $b - a = mk$, para algum $k \in \mathbb{Z}$. Logo, $b = mk + a$.

Analogamente como $b \equiv c \pmod{m}$ temos que $m \mid c - b$, ou seja, $c - b = mk'$, para algum $k' \in \mathbb{Z}$. Aplicando o valor de b determinado anteriormente, segue que $c - (mk + a) = mk'$. Assim, $c - a = mk' + mk = m(k' + k)$, o que implica $m \mid c - a$. Portanto, $a \equiv c \pmod{m}$.

□

A partir da definição e propriedades apresentadas até aqui, nota-se uma relação direta entre o resto da divisão de um dado número inteiro a por m e a congruência desse mesmo número a módulo m.

Podemos observar que calcular o resto da divisão euclidiana de um número a por m é o mesmo que determinar $r \in \{0, 1, 2, ..., m-1\}$ que é congruente a a módulo m.

A fim de sistematizar essas observações, enunciamos a proposição abaixo.

Proposição 10. Sejam a, r e m números inteiros tais que $m > 1$ e $0 \leq r < m$. Então r é o resto da divisão de a por m se, e somente se, $a \equiv r \pmod{m}$.

Demonstração. Sejam $a, r, m \in \mathbb{Z}$ tais que $m > 1$ e $0 \leq r < m$.

($\Rightarrow$) Supondo que r é o resto da divisão euclidiana de a por m, temos $a = mq + r$, para algum $q \in \mathbb{Z}$. Então $a - r = mq$, ou seja, $a \equiv r \pmod{m}$.

($\Leftarrow$) Como $a \equiv r \pmod{m}$, pelo Teorema 4 segue que $m \mid a - r \Leftarrow a - r = mq$, para algum q inteiro, ou seja, $a = mq + r$. Por hipótese $0 \leq r < m$ assim, pela unicidade do resto da divisão euclidiana, segue que r é o resto da divisão de a por m.

□

A Proposição anterior nos diz que todo número inteiro a é congruente módulo m a um, e somente um, dos números do conjunto $R \doteq \{0,1,2,...,m-1\}$. Denominamos o conjunto R por *sistema completo de resíduos módulo m*, o qual exploraremos detalhadamente mais a frente, ao tratarmos de classes residuais.

4.2 Congruências e operações

Nesta seção iremos apresentar algumas propriedade operatórias compatíveis com as congruências módulo m. Tais operações serão fundamentais em aplicações importantes de congruência, assim como aquelas propostas neste trabalho. Iremos conhecê-las e explorá-las a seguir.

4.2.1 Adição

Proposição 11. Dados $a,b,c,d,m \in \mathbb{Z}$, tais que $m > 1$, $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a+c \equiv b+d \pmod{m}$.

Demonstração. Suponhamos $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$. Aplicando a propriedade de simetria neste último temos que $d \equiv c \pmod{m}$. Dessa forma $m \mid b-a$ e $m \mid c-d$ e do item (vi) da Proposição 1, segue que $m \mid (b-a)-(c-d)$. Como $(b-a)-(c-d) = (b+d)-(a+c)$ temos que $m \mid (b+d)-(a+c)$ e portanto, $a+c \equiv b+d \pmod{m}$. □

Uma pergunta natural é questionarmos sobre a validade da "regra do cancelamento", ou seja, é possível simplificar uma dada congruência módulo m, onde temos um mesmo número inteiro somado em ambos os membros? No caso da adição, verificaremos na proposição a seguir que esta suposição é verdadeira.

Proposição 12. Se $a,b,c,m \in \mathbb{Z}$ e $m > 1$, então $a \equiv b \pmod{m}$ se, e somente se, $a+c \equiv b+c \pmod{m}$.

Demonstração. Para cada a,b,c e m inteiros segue:

($\Rightarrow$) Supondo que $a \equiv b \pmod{m}$ segue que $m \mid b-a$ e, consequentemente, $b-a = mk$, para algum $k \in \mathbb{Z}$. Adicionando c em ambos os termos da igualdade encontramos que $(b-a)+c = mk+c$, ou seja, $(b+c)-(a+c) = mk$ e portanto, $a+c \equiv b+c \pmod{m}$.

($\Leftarrow$) Supondo $a+c \equiv b+c \pmod{m}$ segue que $m \mid (b+c)-(a+c)$. Como $(b+c)-(a+c) = b-a$ temos que $m \mid b-a$ e portanto $a \equiv b \pmod{m}$.

□

Uma conclusão importante pode ser feita a partir das discussões realizadas até aqui em relação ao resto da divisão da soma de uma congruência qualquer.

Observe que dados $a,b,m \in \mathbb{Z}$ tais que r_1 e r_2 sejam os respectivos restos na divisão euclidiana de a e b por m, pela Proposição 10, segue que

$$a \equiv r_1 \pmod{m} \text{ e } b \equiv r_2 \pmod{m}.$$

Pela Proposição 11,

$$a+b \equiv r_1+r_2 \pmod{m}.$$

Denotando r como o resto da divisão euclidiana de r_1+r_2 por m, no qual $0 \leq r < m$ temos

$$a+b \equiv r_1+r_2 \equiv r \pmod{m},$$

ou seja, r é o resto da divisão euclidiana de $a+b$ por m.

Esse fato nos permite verificar que o resto da divisão por m da soma de dois números inteiros, é congruente módulo m à soma dos restos da divisão de cada um desses números por m.

Exemplo 19. Observe que

$$\begin{aligned} 27+51 &\not\equiv 73+38 \pmod{8} \\ 3+3 &\not\equiv 1+2 \pmod{8} \\ 6 &\not\equiv 3 \pmod{8}, \end{aligned}$$

pois $27 \not\equiv 73 \pmod{8}$ e $51 \not\equiv 38 \pmod{8}$.

4.2.2 Produto

Proposição 13. Dados $a,b,c,d,m \in \mathbb{Z}$, tais que $m > 1$, $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.

Demonstração. Do fato que $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$ e, aplicando a propriedade de simetria neste último, temos que $d \equiv c \pmod{m}$. Dessa forma $m \mid b-a$ e $m \mid c-d$ logo $m \mid (b-a)d$ e $m \mid (c-d)a$ implicando que $m \mid (b-a)d-(c-d)a$. Como $bd-ad+ad-ac = bd-ac$ segue que $m \mid bd-ac$ e portanto, $ac \equiv bd \pmod{m}$.

□

O resultado abaixo segue como consequência direta da Proposição 13.

Corolário 3. Para todos $n \in \mathbb{N}$ e $a,b,m \in \mathbb{Z}$, com $m > 1$, se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$.

Demonstração. Sejam a, b, m inteiros, no qual $m > 1$ e suponha que $m \mid (b-a)$. Consideremos o conjunto $X = \{n \in \mathbb{N} \text{ tal que } m \mid a^n - b^n\}$.

(i) $1 \in X$, pois por hipótese $m \mid b-a$.

(ii) Supondo que $n \in X$ verificaremos que de fato $n+1 \in X$.

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

Como $m \mid (b-a)$ e pela hipótese de indução $m \mid b^n - a^n$, segue do item (vi) da Proposição 1 que $m \mid b^n(b-a) + a(b^n - a^n)$. Logo, $m \mid b^{n+1} - a^{n+1}$.

Portanto, $n+1 \in X$ e pelo Teorema 1 segue que $X = \mathbb{N}$. Dessa forma, se $a \equiv b \pmod{m}$ então $a^n \equiv b^n \pmod{m}$, para todo $n \in \mathbb{N}$.

□

Contudo tendemos a concluir que na operação de multiplicação também vale a "lei do cancelamento". Veremos a seguir que é possível manter a congruência multiplicando um mesmo inteiro em ambos os seus membros, porém a lei do cancelamento não é verdadeira em geral.

Para elucidar tal comentário observe que $11.4 \equiv 7.4 \pmod{6}$, mas $11 \not\equiv 7 \pmod{6}$. Formalizaremos tais conclusões nas proposições abaixo.

Proposição 14. Se $a, b, c, m \in \mathbb{Z}$, $m > 1$ e $a \equiv b \pmod{m}$, então $ac \equiv bc \pmod{m}$.

Demonstração. Do fato que $a \equiv b \pmod{m}$, segue que $m \mid b-a$ e então $m \mid (b-a)c$. Como $c(b-a) = bc - ac$ temos portanto que $ac \equiv bc \pmod{m}$.

□

Conheceremos agora a condição necessária para que seja permitido a "regra do cancelamento" em uma multiplicação inserida numa congruência módulo m.

Proposição 15. Sejam $a, b, c, m \in \mathbb{Z}$, tais que $m > 1$. Se $ac \equiv bc \pmod{m}$ e $\text{mdc}(c, m) = 1$, então $a \equiv b \pmod{m}$.

Demonstração. Supondo que $ac \equiv bc \pmod{m}$ segue que $m \mid bc - ac$, ou seja, $m \mid (b-a)c$. Como $\text{mdc}(c, m) = 1$, pela Proposição 4 temos que $m \mid b-a$ e portanto $a \equiv b \pmod{m}$.

□

De fato, percebemos no exemplo dado anteriormente que $\text{mdc}(4, 6) \neq 1$ e de posse do argumento demonstrado, podemos apresentar outros exemplos no qual se aplica a "regra do cancelamento" associado a multiplicação em congruência:

(i) $15.3 \equiv 8.3 \pmod 7$, temos que $\text{mdc}(3,7) = 1$ e $15 \equiv 8 \pmod 7$.

(ii) $22.11 \equiv 4.11 \pmod 6$, temos que $\text{mdc}(11,6) = 1$ e $22 \equiv 4 \pmod 6$.

Estenderemos as relações entre o resto da divisão em uma congruência para a operação produto. Considerando $a, b \in \mathbb{Z}$ tais que r_1 e r_2 sejam seus respectivos restos na divisão euclidiana por m, pela Proposição 10 segue que

$$a \equiv r_1 \pmod m \text{ e } b \equiv r_2 \pmod m.$$

E pela Proposição 13,

$$ab \equiv r_1 r_2 \pmod m.$$

Denotando r como o resto da divisão euclidiana de $r_1 r_2$ por m, no qual $0 \leq r < m$ temos,

$$ab \equiv r_1 r_2 \equiv r \pmod m$$

ou seja, r também é o resto da divisão euclidiana de ab por m.

Podemos concluir então que o resto da divisão euclidiana por m do produto entre dois números inteiros é congruente módulo m ao produto dos restos da divisão de cada um desses números por m.

Para enterdermos melhor como tal conclusão pode nos ser útil na busca de alguns resultados, vejamos o exemplo a seguir.

Exemplo 20. Determinaremos o resto da divisão de 10^6 por 6.Note que

$$10 \equiv 4 \pmod 6$$

e

$$10^2 \equiv 4 \pmod 6.$$

Observe que

$$10^3 \equiv 10^2.10 \pmod 6.$$

Pelas conclusões e proposições vistas entre multiplicações e restos numa congruência dada, segue

$$10^3 \equiv 10^2.10 \equiv 4.4 \equiv 4 \pmod 6.$$

Dessa forma,

$$10^4 \equiv 10^3.10 \equiv 4.4 \equiv 4 \pmod 6$$

$$10^5 \equiv 10^4.10 \equiv 4.4 \equiv 4 \pmod 6$$

e

$$10^6 \equiv 10^4.10^2 \equiv 4.4 \equiv 4 \pmod 6.$$

Assim, 10^6 deixa resto 4 na divisão por 6.

4.3 Aplicações

Toda a teoria abordada anteriormente nos permite estudar a resolução de problemas interessantes envolvendo critérios de divisibilidade, determinação do resto de uma divisão por um inteiro em algoritmos envolvendo operações difíceis de serem calculadas trivialmente, determinação de soluções inteiras possíveis para uma equações com duas ou mais incógnitas, entre outros.

Nesta seção realizaremos alguns desses exemplos, que tem por intuito ir além de uma simples exemplificação, mas deixar subsídios que colaborem nas aplicações que serão apresentadas ao longo deste trabalho.

4.3.1 Critérios de divisibilidade

Como aplicação de congruência modular, estabeleceremos alguns critérios de divisibilidade por números naturais. Conforme Coutinho: "Se n for um inteiro positivo, então um critério de divisibilidade por n é uma regra que nos permite determinar se um dado inteiro é, ou não divisível por n, a um custo menor que o de efetuar a divisão."(COUTINHO, 2014, p. 61)

Contudo, ainda que o intuito de uma estratégia matemática seja realmente facilitar o trajeto até o resultado esperado, expressaremos aqui, em sua maioria, critérios que cumprem tal propóstio e outros que, ainda que não sejam viáveis de aplicação, nos exemplificam a possibilidade da formulação de um critério de divisibilidade para qualquer número inteiro n.

Antes de seguirmos para as formulações dos critérios desejados, relembramos que todo número natural n, pode ser escrito como $a_k a_{k-1}...a_1 a_0$, no qual a_0 é o algarismo da unidade, a_1 o algarismo da dezena e assim, sucessivamente. Observe que, com exceção de a_k, todos os demais algarismos podem assumir valores de 0 a 9. Desse modo, escrevendo o número inteiro n conforme o Teorema 5 temos:

$$n = a_k.10^k + a_{k-1}.10^{k-1} + ... + a_1.10 + a_0. \tag{4.1}$$

O número n em sua expansão decimal será utilizado repetidamente nos critérios que apresentaremos aqui.

Critério de divisibilidade por 3. Para elaborarmos um critério de divisibilidade por 3, inicialmente observamos que

$$10 \equiv 1 \pmod 3.$$

Pelo Corolário 3, segue que

$$10^r \equiv 1 \pmod 3, \text{ para } \forall\, r \in \mathbb{N}.$$

Retomando a identidade (4.1) temos

$$n = a_k.10^k + a_{k-1}.10^{k-1} ... + a_1.10 + a_0.$$

Pela reflexividade nas relações de congruência, podemos escrever

$$n \equiv a_k.10^k + a_{k-1}.10^{k-1} ... + a_1.10 + a_0 \pmod 3. \tag{4.2}$$

Mas como vimos que $10^r \equiv 1 \pmod 3$, então

$$a_k.10^k + a_{k-1}.10^{k-1} ... + a_1.10 + a_0 \equiv a_k + a_{k-1} + ... + a_1 + a_0 \pmod 3.$$

Logo, pela transitividade concluímos que

$$n \equiv a_k + a_{k-1} + ... + a_1 + a_0 \pmod 3.$$

Como buscamos $n \equiv 0 \pmod 3$, aplicando novamente a propriedade transitiva segue

$$a_k + a_{k-1} + ... + a_1 + a_0 \equiv 0 \pmod 3,$$

isto é, $3 \mid a_k + a_{k-1} + ... + a_1 + a_0$ se, e somente se, n é divisível por 3. Assim, um número inteiro n é divisível por 3 se, e somente se, a soma de seus algarismos seja divisível por 3.

O critério de divisibilidade por 9 é análogo ao encontrado para o número 3. Basta observar que todos os passos realizados são satisfeitos trocando módulo 3 pelo módulo 9

Critério de divisibilidade por 11. Utilizando de passos semelhantes ao realizado anteriormente, escreveremos um dos possíveis critérios de divisibilidade para o número 11.

Aplicando as propriedades da multiplicação conforme o Corolário 3 observamos que

$$10 \equiv -1 \pmod{11}$$

e

$$10^2 \equiv 1 \pmod{11}.$$

Logo

$$10^r \equiv (-1)^r \pmod{11}, \text{ para } \forall\, r \in \mathbb{N}.$$

Assim, a paridade de r determinará se a equivalência encontrada será 1 ou -1.

Seja o número n conforme (4.1), então podemos reescrever

$$a_k.10^k a_{k-1}.10^{k-1} ... + a_1.10 + a_0 \equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + ... + a_1(-1) + a_0 \pmod{11}$$

e por transitividade

$$n \equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + ... + a_1(-1) + a_0 \pmod{11}.$$

Dessa forma, para $n \equiv 0 \pmod{11}$, segue o critério procurado:

$$\begin{cases} a_0 - a_1 + \ldots - a_{k-1} + a_k \equiv 0 \pmod{11}, & k \text{ par}, \\ a_0 - a_1 + \ldots + a_{k-1} - a_k \equiv 0 \pmod{11}, & k \text{ ímpar}. \end{cases}$$

Um questionamento natural pode ser feito sobre a "real facilidade" em aplicar o critério anunciado. A opção em distinguir a paridade para k exerce uma função formalizadora, extinguindo-se de qualquer necessidade de memorização, considerando a naturalidade e familiariedade com que tratamos o sistema de numeração decimal. Vejamos o exemplo a seguir:

Exemplo 21. Verifique se os números 38.795.443 e 2.989.954 são divisíveis por 11.

Aplicando o critério encontrado para 38.795.443 temos:

$$3-4+4-5+9-7+8-3=5, \text{ então } 11 \nmid 38.795.443.$$

Ainda, pela Proposição 11, é possível afirmar que 5 é o resto da divisão do número dado por 11.

Aplicando o critério encontrado para 2.989.954 temos

$$4-5+9-9+8-9+2=0, \text{ então } 11 \mid 2.989.954.$$

Critério de divisibilidade por 2 e por 5. Não é difícil notar que fazendo a congruência de (4.1) nos módulos 2 e 5, estabelecemos um critério de divisibilidade para os mesmos. A verificação de que a condição de divisibilidade dependerá somente do algarismo a_0 é imediata, visto que $10^r \equiv 0 \pmod{2}$ e $10^r \equiv 0 \pmod{5}$ para qualquer $r \geq 1 \in \mathbb{N}$.

Como os números divisíveis por 2 por definição são os pares, enunciamos o seguinte critério de divisibilidade:

Um número inteiro n é divisível por 2 *se, e somente se,* a_0 *for da forma* $2k$*, para qualquer* $k \in \mathbb{Z}$.

Os números divisíveis por 5 são 0 e o próprio 5, então o critério de divisibilidade por 5 é enunciado por:

Um número inteiro n é divisível por 5 *se, e somente se, seu algarismo da unidade for* 0 *ou* 5.

Critério de divisibilidade por 7. No intuito de determinarmos um critério de divisibilidade por 7, precisaremos optar por quais caminhos seguir, ou melhor, o mais conveniente neste caso. Um deles seria analisar as congruências módulo 7 das potências de base 10, dessa forma

encontraríamos o seguinte resultado:

$$\begin{aligned}
10 &\equiv 3 && \pmod 7,\\
10^2 &\equiv 2 && \pmod 7,\\
10^3 &\equiv 10^2.10 \equiv 6 && \pmod 7,\\
10^4 &\equiv 10^3.10 \equiv (-1).3 \equiv 4 && \pmod 7,\\
10^5 &\equiv 10^4.10 \equiv 4.3 \equiv 5 && \pmod 7,\\
10^6 &\equiv 10^5.10 \equiv 5.3 \equiv 1 && \pmod 7,\\
10^7 &\equiv 10^6.10 \equiv 1.3 \equiv 3 && \pmod 7,\\
10^8 &\equiv 10^7.10 \equiv 3.3 \equiv 2 && \pmod 7.
\end{aligned}$$

De fato, se continuarmos a verificação, é possível notar que os resultados se repetem num ciclo a cada seis expoentes da base 10. Note que a diversidade de resultados encontrados nos permitiria escrever um critério de divisibilidade por 7 de complexa utilidade, já que teríamos seis coeficientes distintos a cada seis ordens decimais.

Assim, procuraremos encontrar uma relação mais simplificada e que cumpra ao propósito de fornecer-nos um critério de divisibilidade mais fácil de ser aplicado.

Voltemos ao número n visto em (4.1) e vamos reescrevê-lo da seguinte forma:

$$n = 10(a_k.10^{k-1} + a_{k-1}.10^{k-2} + ... + a_1) + a_0.$$

Denote $N = (a_k.10^{k-1} + a_{k-1}.10^{k-2} + ... + a_1)$, então

$$n = 10N + a_0. \tag{4.3}$$

Para ajudar no entendimento do que foi feito em (4.3), tomemos o número 724.388.124. Note que isolando o algarismo da unidade $a_0 = 4$ temos

$$724.388.124 = (72.438.812)10 + 4,$$

de modo que neste caso temos $N = 72.438.812$.

Voltando a discussão anterior, multiplicando (4.3) por 2 temos

$$2n = 20N + 2a_0.$$

Pela propriedade reflexiva das congruências segue

$$2n \equiv 20N + 2a_0 \pmod 7.$$

Como $20 \equiv -1 \pmod 7$, temos

$$2n \equiv -N + 2a_0 \pmod 7.$$

Multiplicando ambos os membros da congruência por (-1) encontramos

$$-2n \equiv N - 2a_0 \pmod 7.$$

Observe que se $n \equiv 0 \pmod 7$, claramente $-2n \equiv 0 \pmod 7$ e assim $N - 2a_0 \equiv 0 \pmod 7$. Portanto, *um número inteiro n é divisível por* 7 *se, e somente se,* $N - 2a_0$ *for divisível por* 7*, no qual* $N = (a_k.10^{k-1} + a_{k-1}.10^{k-2} + ... + a_1)$.

Exemplo 22. Verifiquemos se o número 896 é divisível por 7.

Temos que $N = 89$ e $89 - 2 \times 6 = 77$. Como 77 é divisível por 7, segue pelo critério encontrado que 896 também é divisível por 7.

Exemplo 23. Tomemos o número 12.845 para averiguarmos sua possível divisibilidade por 7.

Temos que

$$N = 1284 \quad \text{e} \quad 1284 - 2 \times 5 = 1274.$$

Mas note que 1274 é um número que não nos permite a conclusão procurada sem realizar a divisão euclidiana habitual. Então, aplicando o critério novamente, temos que

$$N' = 127 \quad \text{e} \quad 127 - 2 \times 4 = 119$$

e seguindo de forma análoga para 119 encontramos

$$N'' = 11 \quad \text{e} \quad 11 - 2 \times 9 = -7.$$

Como -7 é divisível por 7, segue sequencialmente que 7 divide $119, 1274$ e, como queríamos saber, 12.845.

Portanto, o critério de divisibilidade por 7 encontrado é uma regra recursiva, podendo ser aplicado quantas vezes se fizer necessário.

Já ficou evidente que podemos manipular as propriedades das congruências e criar critérios de divisibilidade para qualquer inteiro n. Porém, para determinados números, esse é mais um fato de deslumbramento do que um ferramenta prática. Isso não nos impedirá de contemplar a flexibilidade que nos permite as operaçãoes e propriedade da aritmética modular e, levados por esta curiosidade matemática, criemos um critério de divisibilidade para o número 29.

Retornemos ao número n dado em (4.1). Reescrevendo n como observado em (4.3) temos

$$n \equiv 10N + a_0 \pmod{29}.$$

Pela Proposição 14, multipliquemos ambos os membros da conguêcia acima por 3, obtemos

$$3n \equiv 30N + 3a_0 \pmod{29}.$$

Observe que $30 \equiv 1 \pmod{29}$ e pela Proposição 11 temos

$$3n \equiv N + 3a_0 \pmod{29}.$$

Dessa forma, para $n \equiv 0 \pmod{29}$ segue que $N + 3a_0 \equiv 0 \pmod{29}$. Portanto, para verificar a divisibilidade de um dado número inteiro por 29 podemos optar por averiguar tal condição para $N + 3a_0$.

Já mostramos que tal estratégia é recursiva, ou seja, pode ser aplicada consecutivamente até uma simplificação pertinente. Claro que o objetivo para o critério formulado não é acrescentar "mais uma regra a ser recordada" e sim enfatizar as possibilidades ofertadas pelas aplicações das congruências.

Exemplo 24. Vamos testar a ferramenta construída para o critério de divisibilidade por 29 no número 22.678.

Pela definição apresentada $N = 2267$, então

$$2267 + 3 \times 8 = 2291.$$

Aplicando sequencialmente a condição temos $N' = 229$, logo

$$229 + 3 \times 1 = 232.$$

Continuamente temos $N'' = 23$, portanto

$$23 + 3 \times 2 = 29.$$

Logo, 22.678 é divisível por 29.

Pois bem, quem no cerne da sua educação básica pode imaginar uma possibilidade real em escolher um número inteiro aleatório e construir uma regra que indique as condições de divisibilidade para ele? Talvez não seja imaginação que falte aos alunos. Infelizmente, tópicos relevantes e interessantes da Teoria dos Números não são explorados como instrumentos construtores dos pensamento algébrico e aritmético nos currículos escolares públicos, mas pretendemos ao longo de várias das construções feitas neste trabalho deixar levantamentos para esta reflexão.

Até o momento optamos por apresentar critérios de divisibilidade por alguns números primos e, para finalizarmos as discussões sobre essa vertente, faremos uma análise em torno de números compostos, no intuito de encontrarmos uma generalidade comum entre eles que possa servir de estratégia no estudo e resolução de situações problemas variados.

É facilmente encontrado em livros e materiais didáticos o seguinte enunciado: *um número inteiro é divisível por* 6 *se ele for divisível por* 2 *e por* 3*, simultaneamente*. Analisemos as implicações contidas nesta afirmação:

(i) Pelo Teorema 8 temos que $6 = 3 \times 2$.

(ii) Dessa forma, um número para ser divisível por 6 deve conter em sua fatoração única ao menos um fator 2 e um fator 3.

(iii) mdc $(2,3) = 1$.

Observe que (i), (ii) e (iii) já seriam suficientes para nos convencer da veracidade da afirmação, mas queremos a partir desse exemplo verificar a possibilidade dessas condições valerem para outros números inteiros compostos. A seguir mostraremos a veracidade da afirmação anterior.

Proposição 16. Sejam $a,n,m \in \mathbb{Z}$ no qual $a \equiv 0 \pmod{m}$ e $a \equiv 0 \pmod{n}$, tal que $\text{mdc}(m,n) = 1$, então $a \equiv 0 \pmod{mn}$.

Demonstração. De $a \equiv 0 \pmod{m}$ temos que $a = mk$, para algum $k \in \mathbb{Z}$, e como $a \equiv 0 \pmod{n}$ segue que $m.k \equiv 0 \pmod{n}$, ou seja, $n \mid mk$. Mas $\text{mdc}(m,n) = 1$ e pela Proposição 4 então $n \mid k$ implicando que $k = nk'$ para algum $k' \in \mathbb{Z}$. Logo, $a = mnk'$, ou seja, $mn \mid a$ e portanto $a \equiv 0 \pmod{mn}$. □

Com esse resultado, não só mostramos formalmente o critério de divisibilidade por 6 enunciado mas comprovamos um caminho para determinar uma série de possíveis divisibilidades para números compostos. Por exemplo, tomemos o número $12 = 2^2.3$, pela proposição anterior temos que como $\text{mdc}(4,3) = 1$, então um número para ser divisível por 12 tem que ser simultaneamente divisível por 3 e 4. O mesmo podemos verificar para o número $45 = 3^2.5$, como $\text{mdc}(9,5) = 1$ segue que um número para ser divisível por 45 tem que ser divisível por 9 e 5.

Vejamos como tal comprovação pode nos ajudar na resolução de problemas mais elaborados.

Exemplo 25. Verificaremos que $2222^{5555} + 5555^{2222}$ é divisível por 231.

Note que $231 = 3.7.11$ e como $\text{mdc}(3,7,11) = 1$ temos pela Proposição 16 que para determinar se o número dado é divisível por 231, basta mostrarmos que ele é divisível po $3,7$ e 11. Faremos então a verificação para os três casos:

(i) Observe que $2222 \equiv 2 \pmod{3}$ e pelo Corolário 3 temos $2222^2 \equiv 2^2 \equiv 1 \pmod{3}$, então

$$2222^{5555} \equiv 2222.(2222^2)^{2777} \equiv 2.1^{2777} \equiv 2 \pmod{3}.$$

Do mesmo modo temos que $5555 \equiv 2 \pmod{3}$ e $5555^2 \equiv 2^2 \equiv 4 \equiv 1 \pmod{3}$, então

$$5555^{2222} \equiv (5555^2)^{1111} \equiv 1^{1111} \equiv 1 \pmod{3}.$$

Da Proposição 11 segue

$$2222^{5555} + 5555^{2222} \equiv 2 + 1 \equiv 3 \equiv 0 \pmod{3}.$$

(ii) Observe que $2222 \equiv 3 \pmod 7$ e $2222^2 \equiv 3^2 \equiv 2 \pmod 7$. Façamos então uma análise sobre os restos da divisão de uma potência de base 2 por 7.

Como $2^3 \equiv 1 \pmod 7$ temos pelo Teorema 4 que

$$2^{3q+r} \equiv (2^3)^q.2^r \equiv 1^q.2^r \equiv 2^r \pmod 7.$$

Aplicando essa ideia ao nosso problema encontramos

$$2222^{5555} \equiv 2222.(2222^2)^{2777} \equiv 3.2^{3.925+2} \equiv 3.(2^3)^{925}.2^2 \equiv 3.1.4 \equiv 12 \equiv 5 \pmod 7.$$

Temos que $5555 \equiv 4 \pmod 7$ e $5555^2 \equiv 4^2 \equiv 2 \pmod 7$. Dessa forma, caímos numa situação igual ao da primeira parcela, então

$$5555^{2222} \equiv (5555^2)^{1111} \equiv 2^{1111} \equiv (2^3)^{370}.2 \equiv 1.2 \equiv 2 \pmod 7,$$

e da Proposição 11 segue

$$2222^{5555} + 5555^{2222} \equiv 5 + 2 \equiv 7 \equiv 0 \pmod 7.$$

(iii) Fazendo uso do critério de divisibilidade por 11 construído anteriormente, temos

$$2222 \equiv 2-2+2-2 \equiv 0 \pmod{11} \text{ e } 5555 \equiv 5-5+5-5 \equiv 0 \pmod{11}.$$

Portanto, por (i),(ii) e (iii), segue que $2222^{5555} + 5555^{5555}$ é divisível por 231.

4.3.2 Potências

Uma aplicação importante sobre congruências é o cálculo de restos da divisão de uma potência por um número inteiro qualquer. Utilizaremos das propriedades já relacionadas, manipulando-as convenientemente para determinar a solução de um dado problema. Tal abordagem será feita através da resolução de uma série de exemplos aqui propostos.

Exemplo 26. Suponha que queiramos calcular o resto da divisão de 3^{1567} por 11. Fazendo o estudo das potências de base 3 módulo 11 temos que

$$\begin{aligned}
3 &\equiv 3 && \pmod{11},\\
3^2 &\equiv 9 && \pmod{11},\\
3^3 &\equiv 5 && \pmod{11},\\
3^4 &\equiv 3.5 \equiv 15 \equiv 4 && \pmod{11},\\
3^5 &\equiv 3.4 \equiv 12 \equiv 1 && \pmod{11}.
\end{aligned}$$

O Corolário 3 nos permite generalizar que números da forma 3^{5k} são congruentes a 1 módulo 11. Isso implica que na resolução, o módulo 5 funcionará como um "módulo auxiliar" a

ser utilizado no expoente, de modo que possamos reescrevê-lo pelo Teorema 4 da forma $5k+r$. Assim, como $1567 = 5.313+2$ segue

$$3^{1567} \equiv 3^{5.313+2} \equiv (3^5)^{313}.3^2 \equiv (1)^{313}.9 \equiv 9 \pmod{11}.$$

Logo o resto procurado é 9.

Exemplo 27. Vamos reelaborar o problema acima utilizando o número $3^{1567^{1570}}$. Agindo de forma similar já sabemos que 5 é o "módulo auxiliar" no expoente na base 3 módulo 11. Dessa forma, vejamos qual é a divisão do expoente 1567^{1570} módulo 5:

$$\begin{aligned} 1567 &\equiv 2 && \pmod 5, \\ 1567^2 &\equiv 4 && \pmod 5, \\ 1567^4 &\equiv 4^4 \equiv 16 \equiv 1 && \pmod 5. \end{aligned}$$

Com isso, percebemos que o expoente é oportuno quando escrito na forma $4k'+r$. Observe ainda que na verdade, tanto neste exemplo quanto no anterior, não há necessidade alguma de determinarmos o valor de k e k', então

$$1567^{1570} \equiv 1567^{4k'+2} \equiv (1567^4)^{k'}.1567^2 \equiv 1.4 \equiv 4 \pmod{5}.$$

Logo, 1567^{1570} deixa resto 4 na divisão por 5 e portanto é da forma $5k+4$. Retornando ao nosso problema incial segue

$$3^{1567^{1570}} \equiv 3^{5k+4} \equiv 3^{5k}.3^4 \equiv 1.4 \equiv 4 \pmod{11}.$$

Dessa forma 4 é o resto procurado. Apesar de semelhantes, note que neste último problema utilizamos um "segundo módulo auxiliar" quando encontramos a generalidade de $1567^{4k'} \equiv 1 \pmod 5$, submetendo assim, proveitosamente, o expoente 1570 módulo 4. Na verdade esta é uma estratégia muito valiosa na resolução de problemas deste tipo, nos permitindo simplificar números e operações que envolvem muitos dígitos. Sigamos com outros exemplos.

Exemplo 28. (FOMIN; GENKIN; ITENBERG, 2012, p. 105) Encontre o resto da divisão do número $10^{10}+10^{100}+10^{1000}+...+10^{10.000.000.000}$ por 7.

Sabemos que $10 \equiv 3 \pmod 7$ e que $10^3 \equiv -1 \pmod 7$, mediante a isso, reescreveremos a soma a fim de usarmos esses resultados:

$$\begin{aligned} 10^{10}+10^{100}+\ldots+10^{10.000.000.000} &= 10[10^9+10^{99}+\ldots+10^{9.999.999.999}] \\ &= 10[(10^3)^3+(10^3)^{33}+\ldots+(10^3)^{3.333.333.333}]. \end{aligned}$$

Denote $n = 10[(10^3)^3 + (10^3)^{33} + \ldots + (10^3)^{3.333.333.333}]$ e assim temos

$$\begin{aligned} n &\equiv 3[(-1^3)^3 + (-1^3)^{33} + \ldots + (-1^3)^{3.333.333.333}] \pmod 7 \\ &\equiv 3.[\underbrace{(-1) + (-1) + \cdots + (-1)}_{\text{10 vezes}}] \pmod 7 \\ &\equiv 3.(-10) \equiv 3.4 \equiv 12 \equiv 5 \pmod 7. \end{aligned}$$

Dessa forma o resto pedido é 5. Talvez tenha sido observado logo nas primeiras premissas que, a partir de $10^3 \equiv -1 \pmod 7$ e aplicando o Corolário 3, poderíamos facilmente encontrar $10^6 \equiv 1 \pmod 7$, nos apresentando o resultado que fielmente buscamos nos exemplos anteriores. A opção de trabalhar com expoente o 3 foi mediante a simplicidade de sua decomposição nos números dados.

O comentário anterior permite-nos uma abertura para o seguinte questionamento : "Será sempre possível encontrar uma congruência equivalente a 1 para qualquer potência analisada no módulo m?" A resposta é não! Contudo, veremos em capítulos posteriores propriedades que nos permitem identificar quais situações isso se aplica. Diante disso, no problema a seguir utilizaremos uma outra abordagem para determinar o resto pedido.

Exemplo 29. Determine o resto da divisão de 6^{1939} por 22.

Observe todas as congruências abaixo:

$$\begin{aligned} 6 &\equiv 6 \pmod{22}, \\ 6^2 &\equiv 14 \pmod{22}, \\ 6^3 &\equiv 4 \pmod{22}, \\ 6^4 &\equiv 2 \pmod{22}, \\ 6^5 &\equiv 12 \pmod{22}, \\ 6^6 &\equiv 6 \pmod{22}, \\ 6^7 &\equiv 14 \pmod{22}. \end{aligned}$$

Apesar de não termos encontrado nenhuma potência com resto 1 podemos notar que as potências da forma 6^n, para algum $n \in N$, satisfazem uma regularidade periódica módulo 22, isto é: $\{6, 14, 4, 2, 12, ...\}$, no qual 5 é o período de repetição desse padrão, ou seja, será nosso "módulo auxiliar" aplicado ao expoente n.

Para convencer-nos da veracidade da observação, suponha que o padrão repita-se k vezes, assim temos que $6^{5k-4} \equiv 6$, $6^{5k-3} \equiv 14$, $6^{5k-2} \equiv 4$, $6^{5k-1} \equiv 2$ e $6^{5k} \equiv 12 \pmod{22}$. Mostremos

que o ciclo repete-se por $(k+1)$ vezes:

$$\begin{aligned}
& 6^{5k+1} \equiv 6^{5k}.6 \equiv 12.6 \equiv 72 \equiv 6 && (\text{mod } 22),\\
\Rightarrow\ & 6^{5k+2} \equiv 6^{5k+1}.6 \equiv 6.6 \equiv 36 \equiv 14 && (\text{mod } 22),\\
\Rightarrow\ & 6^{5k+3} \equiv 6^{5k+2}.6 \equiv 14.6 \equiv 84 \equiv 4 && (\text{mod } 22),\\
\Rightarrow\ & 6^{5k+4} \equiv 6^{5k+3}.6 \equiv 4.6 \equiv 24 \equiv 2 && (\text{mod } 22),\\
\Rightarrow\ & 6^{5k+5} \equiv 6^{5k+4}.6 \equiv 2.6 \equiv 12 && (\text{mod } 22).
\end{aligned}$$

Portanto, por indução finita, concluímos que para qualquer $k \in N$ a regularidade se manterá.

Assim, para resolver nosso problema notamos que $1939 \equiv 4 \pmod 5$, indicando que 6^{1939} refere-se ao quarto resto na sequência do padrão detectado, portanto

$$6^{1939} \equiv 6^4 \equiv 2 \pmod{22}.$$

A ideia aqui apresentada é uma versão formal, a partir do uso das congruências, de uma das técnicas trabalhadas em exercícios sobre divisão euclidiana e fenômenos periódicos com alunos da Educação Básica participantes de programas como PIC e OBMEP na Escola.

Finalizaremos com um problema diferente dos expostos até agora e curioso. Ele faz uma alusão de quão amplo pode ser o uso da aritmética modular em situações diversas e que, aparentemente por uma leitura inicial, não indicam recair sobre ela.

Exemplo 30. (FOMIN; GENKIN; ITENBERG, 2012, p. 107) Foi calculada a soma dos algarismos do número 2^{100}, depois foi calculada a soma dos algarismos do número resultante, e assim por diante, até sobrar um único algarismo. Qual é este algarismo?

Talvez a primeira motivação que nos venha a cabeça seja ir "abrindo" esta soma em suas primeiras parcelas e tentar encontrar alguma regularidade que nos indique um caminho a seguir. Se feito isto, verifica-se que este tão sonhado padrão não existe. Vamos então analisar os algarismos deste resultado de outra forma já aplicada por nós neste capítulo.

Sejam $a_k a_{k-1}...a_1 a_0$ os algarismos de 2^{100} escritos em sua expansão decimal, tal que

$$2^{100} = a_k.10^k + a_{k-1}.10^{k-1} + ... + a_1.10 + a_0.$$

Note que para nossa satisfação $10^n \equiv 1 \pmod 9$ para qualquer $n \in N$, então temos

$$a_k.10^k + a_{k-1}.10^{k-1} + ... + a_1.10 + a_0 \equiv a_k + a_{k-1} + ... + a_1 + a_0 \pmod 9.$$

Logo, por transitividade, segue

$$2^{100} \equiv a_k + a_{k-1} + ... + a_1 + a_0 \pmod 9.$$

Com isso, nosso desafio está resumido em determinarmos o resto da divisão da potência 2^{100} por 9. Isso recai sobre o uso de estratégias já realizadas nos exemplos anteriores. Observe que $2^6 \equiv 1 \pmod 9$ e pelo Teorema 4 temos que $100 = 6q+4$, portanto

$$a_k + a_{k-1} + ... + a_1 + a_0 \equiv 2^{100} \equiv (2^6)^q.2^4 \equiv 1.16 \equiv 7 \pmod 9.$$

Assim, o algarismo pedido é igual a 7.

4.3.3 Equações Diofantinas

Seguiremos no intuito de apresentar aplicações distintas ao uso da aritmética modular através das congruências. Nesta sessão, associaremos as propriedades de congruência a equações diofantinas de maneira geral. Consideremos a definição para essas equações como "[...] são equações polinomiais, em várias incógnitas, com coeficientes inteiros (ou racionais), das quais se buscam soluções restritas ao conjunto dos números inteiros" (SAMPAIO; CAETANO, 2014, p. 83).

Exemplo 31. Nas equações diofantinas abaixo, os inteiros x, y, z são desconhecidos e as demais incógnitas são constantes dadas.

(i) $ax + by = k$.

(ii) $x^n + y^n = z^n$.

(iii) $x^2 - ay^2 = 1$.

(iv) $\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}$.

O nome faz menção ao matemático grego Diofanto de Alexandria, do século II, que dedicou-se a resolver problemas cujas as soluções eram números inteiros ou racionais. Suas contribuições foram de grande significado no desenvolvimento da Álgebra e que, posteriormente, influenciou os estudos relativos à Teoria dos Números. Em seu livro *Arithmetica* apresentou 130 problemas variados que envolviam equações polinomiais do primeiro e segundo grau.

Ainda não se conhece um método geral que permita decidir se uma equação diofantina arbitrária possuiu ou não soluções inteiras, ou até mesmo um método que estabeleça quantas soluções ela admite. Nesta expectativa, veremos como o uso das congruências podem contribuir na determinação das raízes ou na ausência delas, em algumas equações diofantinas aqui apresentadas.

Para equações diofantinas lineares onde $ax + by = c$, tais que $a, b, c \in Z$, já se conhece métodos que indiquem a existência de raízes inteiras e sua determinação sem necessariamente fazer uso de congruências, como é possível verificar em (SAMPAIO; CAETANO, 2014) e (HEFEZ, 2014). O problema a seguir foi tirado de (ENQ-2018.2, 2018), através dele apresentaremos uma solução alternativa para essas equações utilizando as propriedades de congruência.

Exemplo 32. Considere a equação diofantina linear $5x+3y=2018$. Escreva a solução geral em $\mathbb{Z}$.

Suponha que existam $x_0, y_0 \in \mathbb{Z}$ tais que

$$5x_0 + 3y_0 = 2018. \tag{4.4}$$

Logo, por se tratar de uma relação entre números inteiros, podemos observar que

$$\begin{aligned} 5x_0 + 3y_0 &\equiv 2018 \pmod 5 \iff \\ 3y_0 &\equiv 3 \pmod 5, \end{aligned}$$

ou seja, para que a equação dada possua soluções inteiras basta mostrarmos que existe um y_0 que satisfaça a equivalência encontrada. Aplicando o resultado da Proposição 14 temos

$$3y_0 \equiv 3 \pmod 5 \Longrightarrow y_0 \equiv 2.3y_0 \equiv 2.3 \equiv 6 \equiv 1 \pmod 5.$$

Assim, comprovamos a existência procurada e que os possíveis valores de y_0 são dados por $y_0 = 5k+1$ para algum $k \in \mathbb{Z}$. Substituindo em (4.4) segue

$$\begin{aligned} 5x_0 + 3(5k+1) &= 2018 \\ 5x_0 &= 2015 - 15k \\ x_0 &= -3k + 403. \end{aligned}$$

Dessa forma, os valores de x_0 são dados por $x_0 = -3k+403$ e portanto, todas as soluções inteiras para a equação são

$$\begin{cases} x = -3k + 403, \\ y = 5k + 1, \qquad \forall, k \in \mathbb{Z}. \end{cases}$$

Diante de equações diofantinas não lineares, ou seja, que envolvam várias variáveis em graus superiores a 1, encontrar um possível conjunto de raízes pode não ser tão simples. Contudo, uma estratégia que pode ser útil ao tratarmos dessas equações é a certificação da existência de soluções para a mesma. Nessa perspectiva, vejamos o exemplo a seguir:

Exemplo 33. Considere a equação diofantina $x^2 + y^2 + z^2 = 8w + 7$, no qual $x, y, z, w \in \mathbb{Z}$. Analisemos as possibilidades dela possuir soluções inteiras.

Vamos admitir que existam $x_0, y_0, z_0, w_0 \in \mathbb{Z}$ de forma que $x_0^2 + y_0^2 + z_0^2 = 8w_0 + 7$. Como trata-se de uma relação entre números inteiros, por conveniência, façamos:

$$\begin{aligned} x_0^2 + y_0^2 + z_0^2 &\equiv 8w_0 + 7 \pmod 8, \\ x_0^2 + y_0^2 + z_0^2 &\equiv 7 \pmod 8. \end{aligned} \tag{4.5}$$

Porém pelo Teorema 4, como $0, 1, 2, 3, 4, 5, 6, 7$ são os possíveis restos de um inteiro n na divisão por 8, segue que n^2 será congruente no módulo 8 a :

$n \pmod 8$	0	1	2	3	4	5	6	7
$n^2 \pmod 8$	0	1	4	1	0	1	4	1.

Logo, realizando a combinação das possibilidades para a soma $x_0^2+y_0^2+z_0^2$, temos como possíveis restos na divisão por 8 os números $\{0,1,2,3,4,5,6\}$, uma contradição já que por (4.5) temos que $x_0^2+y_0^2+z_0^2 \equiv 7 \pmod 8$.

Com isso, pudemos a partir de aplicações simples das propriedades das congruências determinar e inexistência de soluções para a equação $x^2+y^2+z^2 = 8w+7$, sem mesmo antes tentar solucioná-la. Essas mesmas ideias podem ser aplicadas também em equações diofantinas exponenciais, ou seja, quando pelo menos um de seus expoentes é uma variável. Tais equações estão presentes em muitos problemas importantes estudado em Teroria dos Números, que envolvem em sua resolução teoremas e conceitos diversos desta área. Encerremos então nossa reflexão com o exemplo a seguir, no qual buscaremos soluções para uma equação diofantina exponencial, com base nas observações feitas até aqui.

Exemplo 34. Determine x e $y \in \mathbb{Z}$ tais que

$$x^2+15 = 2^y.$$

Analisando a equação módulo 3 temos

$$x^2 \equiv x^2+15 \equiv 2^y \pmod 3.$$

Façamos agora o estudo de cada termo desta congruência no módulo 3. Encontramos então como possibilidades de congruência para x^2:

$x \pmod 3$	0	1	2
$x^2 \pmod 3$	0	1	1 .

Logo, x^2 só será congruente a 0 ou 1 no módulo 3.

Vejamos como se comportam as potências de base 2 neste módulo. Note que $2 \equiv 2 \pmod 3$ e $2^2 \equiv 1 \pmod 3$, logo $2^{2k+1} \equiv 2 \pmod 3$ e $2^{2k} \equiv 1 \pmod 3$ para qualquer $k \in \mathbb{N}$, implicando que o y procurado é da forma $2k$.

Retornando a equação dada temos

$$x^2+15 = 2^{2k} \iff 2^{2k}-x^2 = 15 \iff (2^k-x)(2^k+x) = 15.$$

Se $x > 0$, é claro que $(2^k-x) < (2^k+x)$ e daí segue os possíveis resultados para o produto são:

$$\text{(I)} \quad \begin{cases} 2^k + x = 15 \\ 2^k - x = 1 \end{cases} \iff x = 7 \ \ e \ \ k = 3,$$

$$\text{(II)} \quad \begin{cases} 2^k + x = 5 \\ 2^k - x = 3 \end{cases} \iff x = 1 \ \ e \ \ k = 2,$$

obtendo assim, respectivamente, que $y_1 = 6$ e $y_2 = 4$ e portanto, os possíveis pares (x, y) que satisfazem as condições dadas como solução da equação são $(7,6)$ e $(1,4)$.

CAPÍTULO

5

O PEQUENO TEOREMA DE FERMAT E TEOREMA DE EULER

Foi de posse do texto *Arithmetica de Diofanto* que o francês Pierre de Fermat (1601 – 1665) começou a interessar-se pela Teoria dos Números e anotar, às margens de suas obras, resultados importantes que influenciariam estudiosos póstumos, nos quais transformariam essa área da Matemática.

O primeiro sucessor que deu continuidade as ideias de Fermat, provando e estendendo grande parte de seus resultados, foi o matemático suiço Leonhard Euler (1707 – 1783) que difundiu a Teoria dos Números como até então não havia ocorrido. É possível encontrar maiores detalhes em (COUTINHO, 2014).

Neste capítulo apresentaremos uma das importantes consequências geradas entre o encontro das ideias desses dois matemáticos. Pretendemos a partir do Pequeno Teorema de Fermat, construir sua generalização - o Teorema Euler-Fermat, no qual é um resultado fundamental para as aplicações sugeridas neste trabalho.

5.1 O Pequeno Teorema de Fermat

Segundo (HEFEZ, 2014) já se era conhecida desde a antiguidade a divisibilidade por um número p primo de alguns casos como $2^p - 2$. Contudo, foi Fermat que apresentou a generalização deste resultado que ficou conhecido como o *Pequeno Teorema de Fermat*. Acompanhando os avanços conquistados na Teoria dos Números, expressaremos tal teorema a partir do uso das congruências. Antes de enunciarmos a demonstração de tal resultado a seguinte ferramenta preliminar é apresentada.

Lema 3. Seja p um número primo. Os números $\binom{p}{i}$, no qual $0 < i < p$, são todos divisíveis por p.

Antes da demonstração desse resultado, relembramos que um número binomial é a relação entre dois números naturais p e i, com $p \geq i$, dada por

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

Demonstração. Para $i = 1$ o resultado é imediato, tomemos então $1 < i < p$. Como $\binom{p}{i} \in \mathbb{N}$ segue

$$i! \mid p(p-1)...(p-i+1).$$

Mas como $i < p$ tem-se que $(i!, p) = 1$ e portanto, pela Proposição 4,

$$i! \mid (p-1)...(p-i+1).$$

Logo $p \mid \binom{p}{i}$ para qualquer p primo.

□

Teorema 11 (Pequeno Teorema de Fermat). Sejam p um número primo e a um número inteiro, então

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

Demonstração. Façamos a indução finita a a natural. Seja $X = \{a \in N \cup \{0\} : a^p \equiv a \pmod{p}$, no qual p é um número primo $\}$.

(i) $0 \in X$, pois $p \mid 0^p - 0$.

(ii) Suponhamos que $a \in X$ e verificaremos que $(a+1) \in X$. Observe que pelo Binômio de Newton

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

Segue pela hipótese de indução que $p \mid a^p - a$ e pelo Lema 3 temos que $p \mid \binom{p}{i}$, então $p \mid (a+1)^p - (a+1)$, ou seja, $(a+1)^p \equiv (a+1) \mod p$.

Portanto, $(a+1) \in X$ e pelo Teorema 1, $a^p \equiv a \pmod{p}$ para qualquer $a \in \mathbb{N} \cup \{0\}$.

De posse desse resultado, estenderemos a validade do teorema para todo inteiro tomando $a < 0$. Por essa afirmação temos que $-a > 0$, logo

$$(-a)^p \equiv -a \pmod{p}. \tag{5.1}$$

Se $p \neq 2$, então $(-a)^p = -a^p$ e substituindo esse resultado em (5.1) segue que

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

Multiplicando ambos os membros dessa congruência por (-1) verificamos que $a^p \equiv a \pmod{p}$.

Se $p = 2$ o resultado segue imediatamente pois $(-a)^p = a^p$ e aplicando em (5.1) temos que $a^p - (-a) = a^p - a$ e portanto, $a^p \equiv a \pmod{p}$.

□

O resultado desse teorema ultrapassa a beleza e curiosidade matemática que o permeia e é uma ferramenta importante na resolução de vários problemas aritméticos. No Capítulo 4 mostramos algumas aplicações do uso das congruências sem a utilização desse resultado. A cada situação, buscavamos estratégias para encontrar uma simplificação conveniente que nos ajudasse em sua resolução. Nos exemplos abaixo veremos como essa busca pode ser otimizada com a aplicação do Pequeno Teorema de Fermat.

Exemplo 35. Vejamos que $17 \mid a^{28} - a^{12}$, para qualquer $a \in \mathbb{Z}$.

Note que

$$a^{28} - a^{12} = a^{11}(a^{17} - a), \tag{5.2}$$

e pelo Pequeno Teorema de Fermat temos que

$$a^{17} - a \equiv 0 \pmod{17}. \tag{5.3}$$

Logo, por (5.2) e (5.3), segue

$$a^{28} - a^{12} \equiv a^{11}(a^{17} - a) \equiv a^{11}0 \equiv 0 \pmod{17}.$$

Portanto, $17 \mid a^{28} - a^{12}$ para qualquer número a inteiro.

Exemplo 36. Determinaremos o resto da divisão de 2^{56} por 17.

Pelo Pequeno Teorema de Fermat sabemos que

$$2^{17} \equiv 2 \pmod{17}.$$

Reescrevendo 56 pela sua divisão euclidiana por 17 temos $56 = 17.3 + 5$ e dessa forma

$$2^{56} \equiv (2^{17})^3.2^5 \equiv 2^3.2^5 \equiv 2^8 \equiv 9 \pmod{17}.$$

Logo, o resto da divisão de 2^{56} por 17 é 9.

Uma outra situação abordada no Capítulo 4 foi o estudo em torno de equações diofantinas. Como dito anteriormente, tais equações quando não lineares, possuem um grau de dificuldade maior no que se diz respeito a determinação de suas soluções inteiras, e portanto, torna-se eficaz

conhecer uma possível existência de tais soluções. Apresentamos no exemplo a seguir uma aplicação do Pequeno Teorema de Fermat para a situação descrita, ele é um exercício proposto em (COUTINHO, 2014, p. 101).

Exemplo 37. Mostre que a equação $x^{13} + 12x + 13y^6 = 1$ não admite soluções inteiras.

Observe que por tratar-se de uma relação entre números inteiros podemos fazer

$$x^{13} + 12x \equiv x^{13} + 12x + 13y^6 \equiv 1 \pmod{13}. \tag{5.4}$$

Pelo Teorema 11 temos que

$$x^{13} \equiv 13 \pmod{13}, \tag{5.5}$$

então por (5.4) e (5.5) segue que

$$x^{13} + 12x \equiv x + 12x \equiv 13x \equiv 0 \pmod{13}.$$

Logo não existe x inteiro tal que $x^{13} + 12x \equiv 1 \pmod{13}$ e, portanto, $x^{13} + 12x + 13y^6 = 1$ não possui soluções inteiras.

O Pequeno Teorema de Fermat foi assumido para $a \in \mathbb{Z}$. Ao restringirmos tal número a de forma que $\text{mdc}(a, p) = 1$, temos uma outra versão para esse teorema. Vale citar que ambos são conhecidos como Pequeno Teorema de Fermat nas diversas referências utilizadas neste trabalho.

Corolário 4. Sejam a, p números inteiros, no qual p é um número primo e $\text{mdc}(a, p) = 1$, então

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

Demonstração. Pelo Teorema 11 sabemos que $a^p \equiv a \pmod{p}$ e então $p \mid a^p - a$ implicando que $p \mid a(a^{p-1} - 1)$. Como $\text{mdc}(a, p) = 1$, segue pela Proposição 4 que $p \mid a^{p-1} - 1$, logo $a^{p-1} \equiv 1 \pmod{p}$.

□

Exemplo 38. Vemos que o Corolário 4 não se verifica na congruência

$$11^3 \equiv 3 \pmod{4},$$

no qual 4 não é um número primo. Contudo, se analisarmos a congruência

$$11^4 \equiv 1 \pmod{5},$$

para 5 que é um número primo, temos a verificação do resultado dado.

O Corolário 4 mostra-se como um caminho para facilitar os resultados, na busca da tão estimada "congruência a 1" em resoluções de problemas diversos, sem precisar necessariamente

resolver várias sequências de potenciações ao módulo dado. Essa busca tornar-se-à cada vez mais acertiva ao longo desse capítulo. Vejamos alguns exemplos.

Exemplo 39. Determinaremos o resto da divisão de 19^{39^4} por 191.

Note que 191 é primo e então $\text{mdc}(19,191) = 1$. Logo, pelo Corolário 4, temos

$$19^{190} \equiv 1 \pmod{191}. \tag{5.6}$$

Reescreveremos o expoente 39^4 a partir do módulo auxiliar 190. Temos que $39^2 = 1521$ e pela a divisão euclidiana de 1521 por 190 segue que $1521 = 190q + 1$, para algum $q \in \mathbb{Z}$. Assim, $39^4 = (190q+1)^2 = 190k + 190k' + 1$, no qual $k, k' \in \mathbb{Z}$. Aplicando os resultados em (5.6) segue

$$19^{39^4} \equiv 19^{190k+190k'+1} \equiv (19)^{190^k}(19)^{190^{k'}}19 \equiv 1.1.19 \equiv 19 \pmod{191}.$$

Assim, o resto da divisão dada é 19.

O próximo exemplo é um problema sugerido em (FOMIN; GENKIN; ITENBERG, 2012, p. 114).

Exemplo 40. Prove que o número $30^{239} + 239^{30}$ não é primo.

A ideia principal aqui é buscar um módulo conveniente que permita a redução de ambos os termos pelas propriedades de congruência. Analisando o segundo termo da adição nota-se que 239 é primo e então $\text{mdc}(239,31) = 1$. Assim, pelo Corolário 4 temos

$$239^{30} \equiv 1 \pmod{31}. \tag{5.7}$$

Aplicando o mesmo módulo para o primeiro termo, tem-se que $30^2 \equiv 1 \pmod{31}$ e dessa forma

$$30^{239} \equiv (30^2)^{119}.30 \equiv 30 \pmod{31}. \tag{5.8}$$

Logo, por (5.7) e (5.8) segue

$$30^{239} + 239^{30} \equiv 1 + 30 \equiv 31 \equiv 0 \pmod{31}.$$

Portanto, o número $30^{239} + 239^{30}$ é múltiplo de 31 e, consequentemente, não primo.

Os Exemplos de 1 a 5 trouxeram situações nos quais aplicamos, separadamente, ambos os resultados apresentados pelo Pequeno Teorema de Fermat. Finalizamos esta seção propondo um problema no qual utilizaremos as duas versões do Teorema.

Exemplo 41. Mostraremos que não existe inteiro x, tal que $103 \mid x^3 - 2$.

Observemos que nosso problema resume-se em determinar a existência de solução para a congruência $x^3 \equiv 2 \pmod{103}$. Como 103 é um número primo, verifiquemos os casos abaixo:

(i) Se $\text{mdc}(x,103)=1$ então pelo Corolário 4 temos que $x^{102}\equiv 1 \pmod{103}$ e de $102=3.34$ segue

$$(x^3)^{34}\equiv x^{102}\equiv 2^{34} \pmod{103},$$

um absurdo, pois $x^{102}\equiv 1 \pmod{103}$

(ii) Se $\text{mdc}(x,103)\neq 1$ então pelo Teorema 11 temos que $x^{103}\equiv x \pmod{103}$ e dessa forma

$$x^{103}\equiv x^3.x^{100}\equiv 2.x^{100} \pmod{103},$$

um absurdo, pois sabemos que $x^{103}\equiv x \pmod{103}$.

Portanto por (i) e (ii) não existe $x\in\mathbb{Z}$ de modo que $x^3\equiv 2 \pmod{103}$, ou seja, $103\nmid x^3-2$.

5.2 Classes residuais

Pretendemos embasar as operações realizadas nas congruências sob a perspectiva das relações de equivalência e, consequentemente, compará-las e utilizá-las no entendimento das propriedades pertinentes às classes residuais. Trataremos também da operação de divisão no módulo m, assim como sua condição de existência e aplicações.

5.2.1 Relações de equivalência

No Capítulo 4 verificamos a semelhança entre as relações de congruência e igualdade em $\mathbb{Z}$, enfatizando que isso não seriam meros eventos aleatórios e interessantes, pois ambas tratavam-se de relações de equivalência. De uma maneira simples e geral, todas essas relações são aplicadas a fim de comparar dois elementos de um conjunto dado. A partir das caracterizações das relações de equivalência, veremos sua compatibilidade com as demais relações mencionadas.

Definição 6. Uma relação $\mathscr{R}$ entre dois conjuntos X e Y, não necessariamente distintos, é um subconjunto do produto cartesiano $\text{X}\times\text{Y}$, isto é, $\mathscr{R}\subseteq \text{X}\times\text{Y}$. Se $(x,y)\in\mathscr{R}$ dizemos que x ***está relacionado com*** y pela relação $\mathscr{R}$, denotada por $x\mathscr{R}y$.

Uma relação $\mathscr{R}$ sobre um conjunto X é denominada uma relação de equivalência sobre X se, e somente se, as propriedades a seguir são satisfeitas:

- ***(reflexiva)*** Para todo $x\in\text{X}, (x,x)\in\mathscr{R}$, ou seja, $x\mathscr{R}x$.
- ***(simétria)*** Para todo $x,y\in\text{X}$ se $(x,y)\in\mathscr{R}$, então $(y,x)\in\mathscr{R}$, ou seja, $y\mathscr{R}x$.
- ***(transitiva)*** Para todo $x,y,z\in\text{X}$ se $(x,y)\in\mathscr{R}$ e $(y,z)\in\mathscr{R}$, então $(x,z)\in\mathscr{R}$, ou seja, $x\mathscr{R}z$.

Exemplo 42. Dado o produto caretesiano $\mathbb{Z} \times \mathbb{Z} = \{(x,y); (x,y) \in \mathbb{Z}\}$ definimos a relação de equivalência

$$\mathscr{R}(m) = \{(x,y); x \equiv y \pmod{m}\}.$$

Para $m = 7$ temos que $\mathscr{R}(7) = \{(x,y) : x \equiv y \pmod{7}\}$. Note que $(3,17) \in \mathscr{R}(7)$ pois $3 \equiv 17 \pmod{7}$ e $(5,15) \notin \mathscr{R}$ já que $5 \not\equiv 15 \pmod{7}$.

As relações de equivalência são usadas para classificar elementos de um conjunto em subconjuntos com propriedades semelhantes. Dessa forma, apresentar uma relação de equivalência a um dado conjunto X é o mesmo que determinar uma "partição" de X, ou seja, uma família de subconjuntos, dois a dois disjuntos, cuja a união é o próprio X.

Denominaremos por *classes de equivalência* as subdivisões de um conjunto produzidas por uma relação de equivalência. Formalmente, se X é um conjunto e $\sim$ uma relação de equivalência definida em X, então a classe de equivalência $\bar{x}$ de x é constituída de todos os elementos relacionados a x por $\sim$. Assim,

$$\bar{x} = \{y \in \mathrm{X}; y \sim x\}.$$

Note que se $\bar{x} \cap \bar{y} = \varnothing$, então $x \nsim y$ e, por outro lado, se $\bar{x} = \bar{y}$ então $x \sim y$. Com isso temos as seguintes propriedade das classes de equivalência:

1. *Tomando um elemento qualquer de uma classe de equivalência é possível determinar todos os outros dessa mesma classe*.

2. *Como cada elemento pertence a sua própria classe de equivalência, a união de todas as classes de equivalência é o conjunto* X.

Assim, as várias classes de equivalência representam um partição do conjunto X. O conjunto de todas as classes de equivalência de $\sim$ em X é conhecido como *conjunto quociente* de X por $\sim$. Note que os elementos do conjunto quociente de X são subconjuntos, ou seja, as classes de equivalência. Portanto, o conjunto quociente não é um subconjunto de X e sim um conjunto das partes de X.

5.2.2 Anel dos inteiros módulo m

Nosso intuito é aplicar as construções gerais das relações de equivalência nos inteiros a partir das relações de congruência. O conjunto quociente de $\mathbb{Z}$, definido pela relação de congruência módulo m é chamado de *anel dos inteiros módulo m* e pode ser denotado como $\mathbb{Z}_m$.

Por definição, os elementos de $\mathbb{Z}_m$ são subconjuntos de $\mathbb{Z}$, isto é, classes de equivalência, cada uma delas formada pelos números inteiros que possuem o mesmo resto na divisão por m.

Desse modo, para $a,x,m \in \mathbb{Z}$ e $m > 1$, temos que os elementos da classe de $\bar{a}$ são todos $x \in \mathbb{Z}$ tais que $a - x = km$, para algum $k \in \mathbb{Z}$. Assim,

$$\bar{a} = \{x \in \mathbb{Z}; x \equiv a \pmod{m}\}.$$

O conjunto $\bar{a}$ é chamado de *classe residual módulo m* do elemento a de $\mathbb{Z}$.

Exemplo 43. Para ilustrarmos os conceitos estabelecidos, tomemos $m = 4$. Então as classes residuais de $\mathbb{Z}_4$ são :

$\bar{0} = \{x \in \mathbb{Z}; x \equiv 0 \pmod{4}\}$,

$\bar{1} = \{x \in \mathbb{Z}; x \equiv 1 \pmod{4}\}$,

$\bar{2} = \{x \in \mathbb{Z}; x \equiv 2 \pmod{4}\}$,

$\bar{3} = \{x \in \mathbb{Z}; x \equiv 3 \pmod{4}\}$.

Proposição 17. As classes residuais possuem as seguintes propriedades:

(i) $\bar{a} = \bar{b} \Leftrightarrow a \equiv b \pmod{m}$.

(ii) Se $\bar{a} \cap \bar{b} \neq \varnothing \Rightarrow \bar{a} = \bar{b}$.

(iii) $\bigcup_{a \in \mathbb{N}} \bar{a} = \mathbb{Z}$.

Demonstração. Sejam $a,b,m \in \mathbb{Z}$, com $m > 1$.

(i) Do fato que $\bar{a} = \bar{b}$ segue que $a \in \bar{b}$, logo $a \equiv b \pmod{m}$. Reciprocamente, se $a \equiv b \pmod{m}$ temos que $a \equiv x \pmod{m}$ e $b \equiv x \pmod{m}$, então $x \in \bar{a}$ e $x \in \bar{b}$ e pela unicidade do resto da divisão euclidiana $\bar{a} = \bar{b}$.

(ii) Se $\bar{a} \cap \bar{b} \neq \varnothing$, então existe $x \in \bar{a}$ e $x \in \bar{b}$, isto é, $x \equiv a \pmod{m}$ e $x \equiv b \pmod{m}$, o que implica que $a \equiv b \pmod{m}$, e por (i) temos que $\bar{a} = \bar{b}$.

(iii) Seja $x \in \bigcup_{a \in \mathbb{N}} \bar{a}$, então $x \in \bar{x}$. Assim, temos pela reflexidade das relações de congruência que $x \equiv x \pmod{m}$ e portanto $x \in \mathbb{Z}$. Por outro lado, tomemos $x \in \mathbb{Z}$. Fazendo a divisão euclidiana de x por m temos $x = mq + r$, nos quais q, r são únicos e $0 \leq r < m$, segundo o Teorema 4. Logo $x \equiv r \pmod{m}$ e pela definição de classes residuais $x \in \bar{r}$. Como $\bar{r} \in \bigcup_{a \in \mathbb{N}} \bar{a}$, segue que $x \in \bigcup_{a \in \mathbb{N}} \bar{a}$.

□

A Proposição 17 nos leva a conclusão que um elemento de uma classe residual é representante de toda a classe, observe:

Exemplo 44. Se $m = 5$, temos que $\{3, 8, 13, 18, ...\}$ são representantes de $\bar{3}$. Da mesma forma, $\{0, 5, 10, ...\}$ são os representantes de $\bar{0}$.

Se $m > 0$ a Proposição 10 nos garante que todo inteiro a é congruo a um único x módulo m, no qual $0 \leq x < m$. Transpondo tal fato para a linguagem apresentada nessa seção, representaremos $\mathbb{Z}_m$ pela partição

$$\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{m-1}\}.$$

Uma característica de $\mathbb{Z}_m$ são as definições das operações de soma, diferença e produto. Pelas Proposições 11 e 13 vimos que tais operações são compatíveis as relações de congruência, ou seja, aplicam-se ao quociente. Nessa perspectiva, definiremos tais operações entre classes residuais como

$$\begin{aligned} \bar{a} + \bar{b} &\doteq \overline{a+b} \\ \bar{a} - \bar{b} &\doteq \overline{a-b} \\ \bar{a}.\bar{b} &\doteq \overline{a.b} \end{aligned}$$

Ao analisar as definições, precisamos garantir a boa definição, isto é, "se mudarmos os representantes de $\bar{a}$ e $\bar{b}$ a igualdade manteria-se?" Considere $\bar{a}$ e $\bar{b}$ como duas classes de $\mathbb{Z}_m$ no qual $\bar{a}' = \bar{a}$ e $\bar{b}' = \bar{b}$. Dessa forma, temos que

$$a \equiv a' \pmod{m} \text{ e } b \equiv b' \pmod{m},$$

e pelas Proposições 11 e 13 segue que

$$a \pm b \equiv a' \pm b' \pmod{m} \text{ e } a.b \equiv a'.b' \pmod{m}.$$

Portanto,

$$\overline{a+b} \doteq \overline{a'+b'} \text{ e } \overline{a.b} \doteq \overline{a'.b'},$$

de modo a certificar que as operações acima estão bem definidas.

Exemplo 45. Observemos as tabelas de soma e produto em $\mathbb{Z}_6$.

Até o presente momento não tratamos sobre a divisão de um dado número inteiro a módulo m. As implicações que envolvem tal operação mostrarão resultados valiosos nas aplicações de teoremas e formulações que serão realizadas. Recorreremos aqui a ideia da divisão como a multiplicação de um número real pelo seu inverso, mais precisamente, sendo a um número real não nulo existe $b \in \mathbb{R}^*$ tal que $a.b = 1$ e $b \doteq \frac{1}{a}$ é conhecido como o inverso de a. Analogamente, transportanto essa ideia para aritmética modular, dizemos que

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$

Tabela 1 – Soma

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{0}$	$\bar{2}$	$\bar{4}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{0}$	$\bar{3}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{4}$	$\bar{2}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Tabela 2 – Produto

Definição 7. Se $\bar{a}, \bar{x} \in \mathbb{Z}_m$ então $\bar{x}$ é o inverso de $\bar{a}$ se a equação $\bar{a}.\bar{x} = \bar{1}$ é verificada em $\mathbb{Z}_m$.

Com isso avançamos ao próximo ponto: conhecermos as condições de existência de tal inverso. A proposição abaixo cumpre tal finalidade.

Proposição 18. Sejam $a, x, m \in \mathbb{Z}$ e $m > 1$, então $ax \equiv 1 \pmod{m}$ se, e somente se, $\text{mdc}(a,m) = 1$.

Demonstração. Sejam $a, x, m \in \mathbb{Z}$ tais que $m > 1$, temos:

($\Rightarrow$) Admitindo que $ax \equiv 1 \pmod{m}$, então existe $y \in \mathbb{Z}$ tal que $ax - 1 = my$. Reescrevendo a equação temos $ax - my = 1$, e pela Proposição 3 segue que $\text{mdc}(a,m) = 1$.

($\Leftarrow$) Se $\text{mdc}(a,m) = 1$ então pelo Proposição 3 a equação $ax - my = 1$ com $x, y \in \mathbb{Z}$ possui solução. Portanto $ax = 1 + my$ o que implica em $ax \equiv 1 \pmod{m}$.

□

Por exemplo, na tabela do produto de $\mathbb{Z}_6$ contruída no Exemplo 45 temos que $\bar{5}.\bar{5} = \bar{1}$, logo $\bar{5}$ é seu próprio inverso em $\mathbb{Z}_6$.

Dizemos então que a é invertível módulo m quando $\text{mdc}(a,m) = 1$ e x é o inverso multiplicativo de a módulo m. Essa afirmação responde a um levantamento feito no Capítulo 4 sobre em quais situações seriam possíveis encontrar a congruência de um número a 1, no módulo dado. Uma característica importante a ser acrescentada é que o inverso multiplicativo de um número inteiro, quando existe, é único módulo m. De fato, se $ax \equiv ax_1 \equiv 1 \pmod{m}$ segue que

$$x \equiv x.1 \equiv x.ax_1 \equiv a.x.x_1 \equiv 1.x_1 \equiv x_1 \pmod{m}.$$

Se observarmos criteriosamente, notamos que além de determinarmos as condições para executarmos divisões em $\mathbb{Z}_m$, é possível determinar o inverso multiplicativo, caso exista, de um dado inteiro a partir do Teorema 6.

Exemplo 46. Qual o inverso multiplicativo de $\bar{7}$ em $\mathbb{Z}_{24}$?

Pela Proposição 18 sabemos que o inverso multiplicativo procurado existe, pois $\text{mdc}(7,24) = 1$. Determiná-lo é o mesmo que encontrarmos $x_0, y_0 \in \mathbb{Z}$ que satisfaçam a equação diofantina

$$7x - 24y = 1. \tag{5.9}$$

Aplicando o Teorema 6 encontramos $x_0 = 7$ e $y_0 = 2$ e substituindo em (5.9) segue

$$7.7 - 24.2 = 1,$$

que é equivalente a

$$7.7 \equiv 1 \pmod{24}.$$

Portanto, $\bar{7}$ é seu próprio inverso em $\mathbb{Z}_{24}$.

Mais do que uma metodologia para determinar o inverso multipliativo em $\mathbb{Z}_m$, sua apresentação cumpre ao propósito de relacionarmos as diversas construções e definições que vem sendo explicitadas neste trabalho, podendo ainda ser visto como objeto de contextualização de assuntos abordados em capítulos antecessores.

O conjunto dos elementos invertíveis de $\mathbb{Z}_m$ é de importante aplicabilidade no teorema que mostraremos na próxima seção e será denotado por $\mathbb{Z}_m^*$. De modo geral,

$$\mathbb{Z}_m^* = \{\bar{a} \in \mathbb{Z}; \text{mdc}(a,m) = 1\}.$$

Uma propriedade de $\mathbb{Z}_m^*$ é que ele é multiplicativamente fechado, ou seja, o produto de dois elementos de $\mathbb{Z}_m^*$ é um elemento de $\mathbb{Z}_m^*$. Para verificar essa afirmação tomemos $\bar{a}$ e $\bar{b}$ com os seus respectivos inversos $\bar{x}$ e $\bar{x}_1$ em $\mathbb{Z}_m$, então

$$(\bar{a}.\bar{b})(\bar{x}.\bar{x}_1) = (\bar{a}.\bar{x})(\bar{b}.\bar{x}_1) = \bar{1}.\bar{1} = \bar{1}.$$

Exemplo 47. Verifiquemos a tabela de produtos de $\mathbb{Z}_8$.

.	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Observe que em $\mathbb{Z}_8$ os elementos invertíveis são $\bar{1},\bar{3},\bar{5}$ e $\bar{7}$, e, portanto, constituem $\mathbb{Z}_8^*$. Ainda podemos verificar que $\mathbb{Z}_8^*$ é multiplicativamente fechado, notando que os inversos multiplicativos de $\bar{1},\bar{3},\bar{5}$ e $\bar{7}$ pertencem a $\mathbb{Z}_8^*$.

Dado $\mathbb{Z}_m = \{\bar{a}_1,\bar{a}_2,...,\bar{a}_{(m-1)}\}$, dizemos que o conjunto $\{a_1,a_2,...,a_{(m-1)}\}$ é um sistema completo de resíduos módulo m pois seus elementos representam todas as classes residuais de $\mathbb{Z}_m$. Isso equivale a dizer que $a_i \not\equiv a_j \pmod{m}$ para $i \neq j$ e, para todo $n \in \mathbb{Z}$, existe um a_i, tal que $n \equiv a_i \pmod{m}$. O conjunto $\{0,1,2,...,m-1\}$ é um exemplo de sistema completo de resíduos do módulo m.

De forma análoga, o conjunto $\{b_1,b_2,...,b_k\}$, é chamado de sistema reduzido de resíduos módulo m se, e somente se, $\mathbb{Z}_m^* = \{\bar{b}_1,\bar{b}_2,...,\bar{b}_k\}$, ou seja, seus elementos representam todas as classes invertíveis de $\mathbb{Z}_m$. Logo, é implícito verificar que $\text{mdc}(b_i,m) = 1$ para qualquer $i = \{1,2,...,k\}$ e $b_i \not\equiv b_j \pmod{m}$ para $i \neq j$, são as propriedades que caracterizam um sistema de resíduos módulo m.

No Exemplo 47, temos que $\{0,1,2,3,4,5,6,7\}$ formam um sistema completo de resíduos no módulo 8, pois representam todos os possíveis restos na divisão por 8. Já o conjunto $\{1,3,5,7\}$ constituem um sistema reduzido de resíduos no módulo 8, pois $\mathbb{Z}_8^* = \{\bar{1},\bar{3},\bar{5},\bar{7}\}$.

5.3 O Teorema Euler-Fermat

De posse dos resultado anteriores, definiremos uma função denotada por $\varphi(m)$ chamada de função de Euler e mostraremos algumas de suas características fundamentais. Na sequência, apresentaremos uma generalização do Pequeno Teorema de Fermat através da óptica das contribuições de Euler. De fato, o Pequeno Teorema de Fermat não pode ser estendido a um número inteiro qualquer, por exemplo, $6 \nmid 6^{6-1}-1$ pois $6^{6-1}-1 \equiv 5 \not\equiv 1 \pmod{6}$. Nessa motivação, enunciaremos o Teorema Euler-Fermat de modo a abranger todo inteiro positivo.

5.3.1 A função $\varphi(m)$

Definição 8. A função $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ com $m \longrightarrow \varphi(m)$, onde

$$\varphi(m) = \#\mathbb{Z}_m^*$$

é chamada de *função φ de Euler* e # é a cardinalidade do conjunto $\mathbb{Z}_m^*$. Note que a função está bem definida, pois como vimos na seção anterior, $\mathbb{Z}_m^*$ é um conjunto finito.

A cardinalidade, por exemplo, para $m = 1$ e $m = 2$ é $\varphi(1) = \varphi(2) = 1$. No Exemplo 47, temos que $\#\mathbb{Z}_8 = \varphi(8) = 4$.

Dado $\mathbb{Z}^*{}_m = \{\bar{b}_1,\bar{b}_2,...,\bar{b}_{\varphi(m)}\}$, sabemos pela definição apresentada no final da seção anterior que o conjunto $\{b_1,b_2,...,b_{\varphi(m)}\}$, com $\varphi(m)$ elementos é um sistema reduzido de resíduos.

Para um dado p primo temos que

$$\varphi(p) = p - 1,$$

uma vez que todos os elementos das classes residuais de p, exceto $\bar{0}$, são primos com ele. Por exemplo, $\varphi(5) = 5 - 1 = 4$, $\varphi(11) = 11 - 1 = 10$.

Será fundamental para o que se seguirá calcular o valor de $\varphi(m)$ para um m natural qualquer. Para isso, mostraremos uma sequência de resultados a fim de promover os elementos necessários para sua determinação numérica.

Proposição 19. Se p é um número primo e $r \in \mathbb{N}$, então temos que

$$\varphi(p^r) = p^r - p^{r-1}.$$

Demonstração. Pela definião de $\varphi(m)$ temos que $\varphi(p^r)$ é um número natural menor que p^r e indica o total de números primos com p^r em $[1, p^r) \cap \mathbb{N}$. Por outro lado, os números naturais menores e não primos com p^r são aqueles divisíveis por p, expressos na sequência

$$p, 2p, 3p, ..., p^{r-1}.$$

Dessa forma, de 1 a p^r temos extamente p^{r-1} números não primos com p, e portanto, $\varphi(p^r) = p^r - p^{r-1}$. □

Exemplo 48.

(i) $\varphi(16) = \varphi(2^4) = 2^4 - 2^3 = 8$.

(ii) $\varphi(27) = \varphi(3^3) = 3^3 - 3^2 = 18$.

Para tratarmos os casos em que se tenha um m qualquer, mostraremos a seguir que $\varphi(m)$ é uma função multiplicativa.

Proposição 20. Sejam $m, n \in \mathbb{N}$ tais que $\text{mdc}(m, n) = 1$, então

$$\varphi(mn) = \varphi(m)\varphi(n).$$

Demonstração. Organizaremos os números de 1 a $m.n$ conforme a tabela abaixo:

Inicialmente, note que cada coluna representa um sistema completo de resíduos módulo m.

Seja $r \in \{1, 2, ..., m-1\}$, denotemos uma linha r da tabela acima por

$$r, m + r, ..., (n-1)m + r.$$

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m & 2m & 3m & \cdots & n.m \end{array}$$

Pelo Teorema 6 sabemos que $\text{mdc}(r,m) = \text{mdc}(km+r,m)$ para $\forall\, k \in \mathbb{Z}$ no qual $0 \leq k \leq n-1$. Se $\text{mdc}(r,m) = d$ para $d > 1$, então d é divisor comum de todos os elementos da linha r e portanto nenhum de seus elementos é primo com $m.n$. Assim, as linhas da tabela onde seus elementos sejam todos primos com m, ou seja, $\text{mdc}(m,r) = 1$ são em quantidade $\varphi(m)$.

A partir dessa observação resta-nos procurar os elementos destas $\varphi(m)$ linhas que são também primos com n, isto é, $\text{mdc}(km+r,n) = \text{mdc}(n,r) = 1$. Para isso, mostraremos inicialmente que os elementos de cada uma das $\varphi(m)$ linhas formam um sistema completo de resíduos módulo n.

Sejam $km+r$ e $k'm+r$ elementos da linha r no qual $0 \leq k,k' \leq n-1$, tal que $km+r \equiv k'm+r \pmod{n}$. Pela Proposição 12 segue

$$km \equiv k'm \pmod{n}.$$

Do fato que $\text{mdc}(m,n) = 1$ segue pela Proposição 14

$$k \equiv k' \pmod{n}.$$

Mas, como $0 \leq k,k' \leq n-1$, pela unicidade do resto no Teorema 4 temos que $k = k'$. Logo, o conjunto $\{r, m+r, 2m+r, \ldots (n-1)m+r\}$ formam um sistema completo de resíduos no módulo n. Dessa forma, temos que cada uma das $\varphi(m)$ linhas possuem $\varphi(n)$ elementos primos com n e logo primos com nm. Portanto, tomando as $\varphi(m)$ linhas determinadas, onde cada uma delas tem $\varphi(n)$ elementos primos com n e m conclui-se que os total de elementos simultaneamente primos com m e n é $\varphi(m)\varphi(n)$.

□

Exemplo 49. Determinar $\varphi(24)$.

Note que $24 = 3.8$ e como $\text{mdc}(3,8) = 1$, então pela Proposição 20 segue

$$\varphi(24) = \varphi(3)\varphi(8).$$

Pela Proposição 19 temos

$$\varphi(3) = 3^1 - 3^0 = 3 - 1 = 2,$$
$$\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4.$$

Logo,

$$\varphi(3).\varphi(8) = 2.4 = 8.$$

Considerando os resultados demonstrados até o presente momento, podemos apresentar o teorema para determinação de $\varphi(m)$ para qualquer $m \in \mathbb{N}$.

Teorema 12. Seja $m > 1$ no qual $m = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$ é a fatoração única de m em primos distintos. Então

$$\varphi(m) = m\prod_{i=1}^{k}(1 - \frac{1}{p_i}).$$

Demonstração. Dado $m = p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$, para cada $p_i^{\alpha_i}$ no qual $i \in \{1,2,...,k\}$, segue da Porposição 19 que

$$\varphi(p^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}.$$

Logo, pela Proposição 20 temos

$$\varphi(m) = \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = m\prod_{i=1}^{k}(1 - \frac{1}{p_i}).$$

□

Exemplo 50. Vamos calcular o $\varphi(60)$.

Observe que $60 = 2^2.3.5$ e pela Proposição 20, temos

$$\varphi(60) = \varphi(2^2)\varphi(3)\varphi(5).$$

Logo

$$\varphi(60) = (2^2 - 2)(3 - 1)(5 - 1) = 2.2.4 = 16.$$

5.3.2 O Teorema de Euler-Fermat

Vimos em algumas aplicações apresentadas no Capítulo 4 como é conveniente encontrar a congruência de uma dada potência a 1 módulo m. O Pequeno Teorema de Fermat mostrou-se como grande aliado em tais situações quando as mesmas estavam submetidas a um módulo p, sendo p um número primo.

Mas ainda nos deparamos com uma lacuna: como proceder diante de problemas em um módulo $m \in \mathbb{Z}$ e não primo? A resposta é o tema central desta seção. O Teorema Euler-Fermat nos permitirá tratar de forma geral o resultado apresentado pelo Pequeno Teorema de Fermat, estendendo sua aplicação a qualquer número inteiro. A proposição a seguir trás um resultado que nos subsidiará na demostração do referido teorema.

Proposição 21. Sejam $a, m \in \mathbb{Z}$ e $m > 1$, tais que $\text{mdc}(a,m) = 1$. Se $\{x_1, x_2, ..., x_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo m, então $\{ax_1, ax_2, ..., ax_{\varphi(m)}\}$ também é um sistema reduzido de resíduos módulo m.

Demonstração. Mostraremos que $\{ax_1, ax_2, ..., ax_{\varphi(m)}\}$ possuem as propriedades de um sistema reduzido de resíduos.

Como $\text{mdc}(a,m) = 1$ e $\text{mdc}(x_i, m) = 1$ para quaisquer $i \in \{1, 2, ..., \varphi(m)\}$ segue que $\text{mdc}(ax_i, m) = 1$. De fato, pelo Teorema 7, sabemos que existem $x, x', y, y' \in \mathbb{Z}$ tais que $ax + my = 1$ e $x_i x' + my' = 1$. Multiplicando a primeira equação por x_i temos

$$axx_i + myx_i = x_i. \tag{5.10}$$

Substituindo (5.10) na segunda identidade segue

$$(axx_i + myx_i)x' + my' = ax_i(xx') + my' = 1,$$

e portanto, $\text{mdc}(ax_i, m) = 1$.

Por outro lado, como $\text{mdc}(a,m) = 1$ temos que se $ax_i \equiv ax_j \pmod{m}$, pela Proposição 14, então $x_i \equiv x_j \pmod{m}$. Como x_i e x_j são elementos de um mesmo sistema reduzido de resíduos, segue que $i = j$. Logo,$\{ax_1, ax_2, ..., ax_{\varphi(m)}\}$ é um sistema reduzido de resíduos no módulo m.

□

O exemplo a seguir mostrará a validade dessa proposição em um caso particular e introduzirá a ideia a ser utilizada na demostração do teorema que se pretende enunciar.

Exemplo 51. Seja $m = 10$ e $a = 3$, então $\{1, 3, 7, 9\}$ é um sistema reduzido de resíduos módulo 10. Pela Proposição 21, o conjunto $\{3 \times 1, 3 \times 3, 3 \times 7, 3 \times 9\}$ também é um sistema reduzido de resíduos módulo 10, ou seja, cada membro desse conjunto é congruente a exatamente um dos elementos de $\{1, 3, 7, 9\}$. Do fato:

$$\begin{aligned} 3.1 &\equiv 3 \pmod{10}, \\ 3.3 &\equiv 9 \pmod{10}, \\ 3.7 &\equiv 1 \pmod{10}, \\ 3.9 &\equiv 7 \pmod{10}. \end{aligned}$$

Multiplicando os membros dessa congruência obtemos

$$3^4(1.3.7.9) \equiv (1.3.7.9) \pmod{10}.$$

Como $\text{mdc}(1.3.7.9, 10) = 1$, aplicando a Proposição 14 obtemos

$$3^4 \equiv 1 \pmod{10}.$$

Obseve que $\varphi(10) = 4$, ou seja, $3^{\varphi(10)} \equiv 1 \pmod{10}$.

Teorema 13 (Teorema Euler-Fermat). Sejam $a, m \in \mathbb{Z}$ com $m > 1$ e $\text{mdc}(a,m) = 1$, então

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{5.11}$$

Demonstração. Como $\text{mdc}(a,m) = 1$ temos pela Proposição 21 que se $\{x_1, x_2, ..., x_{\varphi(m)}\}$ é um sistema reduzido de resíduos módulo m, então $\{ax_1, ax_2, ..., ax_{\varphi(m)}\}$ também é um sistema reduzido de resíduos módulo m. Dessa forma, para cada $i \in \{1, 2, ..., \varphi(m)\}$ existe um único $j \in \{1, 2, ..., \varphi(m)\}$, tal que

$$ax_i \equiv x_j \pmod{m}.$$

Multiplicando os membros gerados por essa congruência temos

$$\prod_{i=1}^{\varphi(m)} ax_i \equiv \prod_{j=1}^{\varphi(m)} x_j \pmod{m},$$

implicando em

$$a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} x_i \equiv \prod_{j=1}^{\varphi(m)} x_j \pmod{m}.$$

Mas, como para cada x_i e x_j temos que $\text{mdc}(x_i, m) = (x_j, m) = 1$, segundo a Proposição 14, podemos simplificar os fatores $\prod_{i=1}^{\varphi(m)} x_i$ e $\prod_{j=1}^{\varphi(m)} x_j$, obtendo $a^{\varphi(m)} \equiv 1 \pmod{m}$.

□

Na sequência, mostraremos alguns exemplos nos quais o Teorema 5.11 é utilizado como estratégia na resolução de problemas variados.

Exemplo 52. Determinaremos o dígito das dezenas do número 3^{84}.

Perceba que determinando o resultado da divisão do número dado por 100, o dígito das dezenas é simultaneamente encontrado. Como $\text{mdc}(3, 100) = 1$, pelo Teorema 5.11 sabemos que

$$3^{\varphi(100)} \equiv 1 \pmod{100}. \tag{5.12}$$

Determinando $\varphi(100)$ segundo o Teorema 12, encontramos

$$\varphi(100) = \varphi(2^2)\varphi(5^2) = (2^2 - 2)(5^2 - 5) = 40 \tag{5.13}$$

Logo, aplicando o resultado determinado em (5.13) na congruência (5.12) temos

$$3^{\varphi(100)} \equiv 3^{40} \equiv 1 \pmod{100}. \tag{5.14}$$

Pelo Teorema 4 temos que $84 = 40.2 + 4$ e portanto, considerando as equivalências obtidas em (5.14) temos

$$3^{84} \equiv (3^{40})^2 3^4 \equiv 1.3^4 \equiv 81 \pmod{100}.$$

Então, o resto da divisão de 3^{84} por 100 é 81, e portanto o dígito das dezenas é 8.

Exemplo 53. Para qualquer $n \in \mathbb{N}$, temos que $15 \mid 77^{16n} - 1$.

Traduzindo o problema para a linguagem que estamos utilizando, queremos mostrar que

$$77^{16n} - 1 \equiv 0 \pmod{15} \iff 77^{16n} \equiv 1 \pmod{15}. \tag{5.15}$$

Supondo que $77^{16n} \equiv 1 \pmod{15}$, como $\text{mdc}(15,77) = 1$, pelo Teorema 5.11 sabemos que

$$77^{\varphi(15)} \equiv 1 \pmod{15}. \tag{5.16}$$

Pelo Teorema 12, temos

$$\varphi(15) = \varphi(3)\varphi(5) = (3-1)(5-1) = 8. \tag{5.17}$$

Aplicando o resultado da identidade (5.17) na congruência (5.16) segue

$$77^{\varphi(15)} \equiv 77^8 \equiv 1 \pmod{15}. \tag{5.18}$$

Utilizando a equivalência determinada em (5.18) na congruência (5.15) verificamos

$$77^{16n} \equiv (17^8)^{2n} \equiv 1^{2n} \equiv 1 \pmod{15}.$$

Logo, para todo $n \in \mathbb{N}$ temos $77^{16n} \equiv 1 \pmod{15}$, ou seja, $15 \mid 77^{16n} - 1$.

O exemplo abaixo foi retirado do banco de questões de (OBM-1991, 1991).

Exemplo 54. Demonstre que existem infinitos múltiplos de 1991 que são da forma 19999...99991.
De fato, vamos reescrever o número 19999...99991 de forma a utilizar a decomposição na base decimal:

$$19999...99991 = 2.10^n - 9.$$

Note que o problema resume-se a mostrar que $2.10^n - 9 \equiv 0 \pmod{1991}$ para $\forall\, n \in \mathbb{N}$. Isso é o mesmo que

$$2.10^n - 9 \equiv 1991 \pmod{1991}. \tag{5.19}$$

Utilizando-se da Proposição 11 na equivalência (5.19), obtemos

$$2.10^n \equiv 2000 \pmod{1991}. \tag{5.20}$$

Note que $\text{mdc}(1991, 2000) = 1$ e pela Proposição 18, 2000 é invertível módulo 1991, o que nos permite a seguinte simplificação da equivalência (5.20)

$$2.10^n \equiv 2000.10^{n-3} \equiv 10^{n-3} \equiv 1 \pmod{1991}.$$

Pelo Teorema 5.11 sabemos que $10^{\varphi(1991)} \equiv 1 \pmod{1991}$ e então, segue que $10^{\varphi(1991)^k} \equiv 1 \pmod{1991}$ para $\forall\, k \in \mathbb{N}$. Dessa forma, basta tomar $n = \varphi(1991)k - 3$ para determinar os infinitos múltiplos pedidos.

Construímos uma série de argumentos até aqui a fim de cumprir o propósito de definir caminhos que permitam simplificações e estratégias eficientes à problemas tratados pela perspectiva da aritmética modular. Muitas das situações apresentadas recaíram de forma análoga em, por exemplo, determinar $s \in \mathbb{N}$ tal que $4^s \equiv 1 \pmod{15}$. Façamos uma análise mais detalhada a partir dessa situação.

Sabemos pelo Teorema 5.11 que como $\text{mdc}(4,15) = 1$, o número s não só existe como pode ser determinado pela função $\varphi(15)$. De fato, $s = \varphi(15) = \varphi(3)\varphi(5) = (3-1)(5-1) = 8$ e tem-se que $4^8 \equiv 1 \pmod{8}$.

O exemplo a primeira vista pode parecer redundante e óbvio diante do Teorema de Euler-Fermat, mas as perguntas que podem ser feitas a partir dele são instigantes: será que este resultado é único? Ou ainda, será que $\varphi(m)$ é o menor expoente que satisfaça a congruência dada?

As respostas podem ser retiradas claramamente, basta tomar $s = 2$. Verifica-se que $4^2 \equiv 16 \equiv 1 \pmod{15}$, portanto $\varphi(15)$ não é o único e nem o menor valor para s.

Essas observações abre-nos espaço para expandirmos a compreensão e o trato das definições, teoremas e aplicações acerca das congruências, de modo a analisá-las com maiores possibilidades. Motivados pelos argumentos levantados acima, apresentamos a definição abaixo.

Definição 9. Dado $a, m \in \mathbb{Z}$ com $m > 1$ e $\text{mdc}(a,m) = 1$, denotamos de ordem de a módulo m o número natural dado por

$$\text{ord}_m(a) = min\{i \in \mathbb{N}; a^i \equiv 1 \pmod{m}\}.$$

Pelo exemplo anterior vimos que $s = 2$ é o menor expoente tal que $4^s \equiv 1 \pmod{m}$, então $\text{ord}_{15}(4) = 2$.

Temos pelo Teorema 5.11 que $\text{ord}_m(a) \leq \varphi(m)$. Para os casos onde $\text{ord}_m(a) = \varphi(m)$, dizemos que a é raiz primitiva módulo m. Por exemplo, 3 é raiz primitiva módulo 5, pois $\varphi(5) = 5-1 = 4$ e verificando que $3 \equiv 3 \pmod{5}$, $3^2 \equiv 4 \pmod{5}$, $3^3 \equiv 2 \pmod{5}$, $3^4 \equiv 1 \pmod{5}$ então $\text{ord}_5(3) = 4$.

Proposição 22. Sejam $a, m \in \mathbb{Z}$ e $m > 1$ com $\text{mdc}(a,m) = 1$. Temos que $a^t \equiv 1 \pmod{m}$, para algum $t \in \mathbb{N}$ se, e somente se, $\text{ord}_m(a) \mid t$.

Demonstração.

($\Rightarrow$) Por hipótese tem-se que $a^t \equiv 1 \pmod{m}$ e como $\text{mdc}(a,m) = 1$, pela Definição 9, temos que $a^{ord_m(a)} \equiv 1 \pmod{m}$ e $t \geq \text{ord}_m(a)$. Para $t = \text{ord}_m(a)$ o resultado é trivial. Tomemos $t > \text{ord}_m(a)$, fazendo a divisão euclidiana de t por $\text{ord}_m(a)$ temos $t = \text{ord}_m(a)q + r$, no qual $0 \leq r < \text{ord}_m(a)$. Logo

$$a^t \equiv a^{ord_m(a)q+r} \equiv (a^{ord_m(a)})^q a^r \equiv a^r \equiv 1 \pmod{m},$$

uma contradição, pois $0 \leq r <$ ord$_m(a)$ e ord$_m(a)$ é o menor expoente natural i tal que $a^i \equiv 1 \pmod{m}$. Portanto, $r = 0$ e $t =$ ord$_m(a)q$, o que implica que ord$_m(a) \mid t$.

($\Leftarrow$) Se ord$_m(a) \mid t$, então $t =$ ord$_m(a).k$ para algum $k \in \mathbb{Z}$. Do fato que mdc$(a,m) = 1$ e pela Definição 9, segue que $a^{ord_m(a)} \equiv 1 \pmod{m}$, logo

$$1 \equiv a^{ord_m(a)} \equiv (a^{ord_m(a)})^k \equiv a^t \pmod{m}.$$

□

O Corolário a seguir enriquece as apurações feitas acerca do assunto abordado nessa seção e será útil no desenvolvimento das aplicações a serem apresentadas ao final desta seção.

Corolário 5. Sejam $a, m \in \mathbb{Z}$ e $m > 1$ com mdc$(a,m) = 1$. Temos que ord$_m(a) \mid \varphi(m)$.

Demonstração. Como mdc$(a,m) = 1$ segue do Teorema 5.11 que $a^{\varphi(m)} \equiv 1 \pmod{m}$, e portanto, pela Proposição 22, ord$_m(a) \mid \varphi(m)$.

□

Observação 6. O Teorema de Euler-Fermat acrescido do Corolário 5, nos permite reduzir de forma significativa os possíveis candidatos a ordem de um número módulo m. Vejamos o exemplo a seguir.

Exemplo 55. Qual o menor valor de x de modo que $2^x \equiv 1 \pmod{97}$?

Como mdc$(2,97) = 1$, temos pelo Teorema 5.11 que

$$2^{\varphi(97)} \equiv 1 \pmod{97}. \tag{5.21}$$

Do fato de 97 ser um número primo segue que $\varphi(97) = 97 - 1 = 96$ e por (5.21) segue

$$2^{96} \equiv 1 \pmod{97}. \tag{5.22}$$

Como buscamos o menor valor para x então queremos determinar a ord$_{97}(2)$, e pelo Corolário 5 temos a seguinte relação

$$\text{ord}_{97}(2) \mid \varphi(97) \Longrightarrow \text{ord}_{97}(2) \mid 96.$$

Dessa forma, reduzimos nossa procura pela ord$_{97}(2)$ no conjunto dos divisores de 96, isto é, ord$_{97}(2) \in \{1,2,3,4,6,8,12,16,32,24,48,96\}$. Averiguando a partir dos elementos do conjunto

de divisores de 96 temos

$$\begin{aligned}
2^1 &\equiv 2 && \pmod{97},\\
2^2 &\equiv 4 && \pmod{97},\\
2^3 &\equiv 8 && \pmod{97},\\
2^4 &\equiv 16 && \pmod{97},\\
2^6 &\equiv 64 && \pmod{97},\\
2^8 &\equiv 62 && \pmod{97},\\
2^{12} &\equiv (2^6)^2 \equiv 64^2 \equiv 22 && \pmod{97},\\
2^{16} &\equiv (2^8)^2 \equiv 62^2 \equiv 61 && \pmod{97},\\
2^{24} &\equiv (2^{12})^2 \equiv 22^2 \equiv 96 && \pmod{97},\\
2^{32} &\equiv (2^{16})^2 \equiv 61^2 \equiv 35 && \pmod{97},\\
2^{48} &\equiv (2^{24})^2 \equiv 96^2 \equiv 1 && \pmod{97}.
\end{aligned}$$

Note que pela equivalência (5.22) já sabemos o resultado para o expoente 96, logo

$$x = \text{ord}_{97}(2) = 48.$$

Encerramos esta seção com uma última aplicação dos resultados envolvendo a ordem de um número módulo m na resolução de problemas de divisibilidade.

Exemplo 56. Encontre o menor n tal que $2^{2005} \mid 17n-1$.

Buscamos pelo menor n tal que

$$17^n \equiv 1 \pmod{2^{2005}}.$$

Segundo a Definição 9 temos que $n = \text{ord}_{2^{2005}}(17)$ e pelo Corolário 5 segue que

$$\text{ord}_{2^{2005}}(17) \mid \varphi(2^{2005}).$$

Como $\varphi(2^{2005}) = (2^{2005} - 2^{2004}) = 2^{2004}$, temos que $\text{ord}_{2^{2005}}(17) = 2^k$, no qual $k \in \{0,1,2,...,2004\}$, dessa forma

$$17^{2^k} \equiv 1 \pmod{2^{2005}} \Longrightarrow 17^{2^k} - 1 \equiv 0 \pmod{2^{2005}}.$$

Assim temos

$$17^{2^k} - 1 = (17-1)(17+1)(17^2+1)...(17^{2^{k-1}}+1) = 2^{2005}q, \text{ onde } q \in \mathbb{Z}.$$

Note que o único fator de $17^{2^k} - 1$ múltiplo de 4 é o (17 -1), os demais fatores são da forma $(17^{2^r}+1)$ e somente múltiplos de 2. Logo, para que se tenhamos 2005 fatores 2, o número k que satisfaz essas condições é 2001, portanto

$$\text{ord}_{2^{2005}}(17) = n = 2001.$$

CAPÍTULO

6

CRITPTOGRAFIA RSA

A história da humanidade é marcada pela sua extensa necessidade de comunicação nos contextos mais diversos. A troca de informações de forma sigilosa e segura vem participando de construções sociais, políticas, econômicas, entre outras ao longo dos tempos; induzindo a criação de métodos para cifrar e decifrar mensagens. Da troca de segredos militares a transmissão de dados numa transação bancária, a criptografia permeia práticas do cotidiano e sua evolução trouxe consigo aplicações matemáticas inovadoras, algumas embasadas nas principais definições apresentadas nos capítulos anteriores deste trabalho.

Com a expansão computacional em meados do século XX, a Teoria dos Números contribuiu diretamente para a criação de novos métodos criptográficos, passando a não ser vista como somente uma área pura e abstrata da Matemática, mas também de aplicações práticas. Faremos nessa seção uma ligação entre alguns resultados em torno da aritmética modular mostrados até aqui com alguns sistemas criptográficos, e em especial e de forma mais detalhada, o RSA.

6.1 Introdução a ideia de Criptografia

A criptografia tem como finalidade transmitir de forma segura uma mensagem oculta de um transmissor a um receptor. A evolução hitórica dessa prática está no fato da criação de estratégias nas quais mensagens emitidas, ainda que interceptadas por terceiros, só pudessem ter significação para os devidos destinatários das mesmas. Neste contexto surgem a criação de *chaves* e algoritmos de cifragem, isto é, uma regra para transformar um texto original no cifrado. Discutiremos sobre alguns procedimentos utilizados para ocultar e recuperar informações transmitidas por uma mensagem.

Ao longo de vários séculos foram desenvolvidos vários métodos de cifragem, em consonância com as ferramentas acessíveis a cada período. Um dos métodos criptográficos mais

famosos da antiguidade foi o utilizado por Júlio César, em Roma, em sua comunicação com Cícero. O sistema era muito simples, considerando o alfabeto cíclico, para cada letra que se quisesse escrever considerava-se a terceira letra a sua direita. Nesse sentido, seja $\mathscr{A}$ o alfabeto com 26 letras L utilizadas por César, temos a seguinte descrição das cifras

$\mathscr{A}$	A	B	C	D	E	F	G	H	I	J	K	L	M
Cifras	D	E	F	G	H	I	J	K	L	M	N	O	P

$\mathscr{A}$	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifras	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Tabela 3 – Alfabeto segundo a cifra de César.

Exemplo 57. Neste sistema criptográfico proposto por César, se quiséssemos enviar a seguinte mensagem: *DEMOCRACIA ACIMA DE TUDO*, obteríamos a cifra:

DEMOCRACIA ACIMA DE TUDO
GHPRFUDFLD DFLPD GH WXGR

Numa perspectiva matemática, e mais especificamente da aritmética modular, podemos transpor o método criptográfico de César para uma linguagem já abordada neste trabalho.

Uma nova associação dos códigos.

Considerando o alfabeto cíclico, e isso é de extrema relevância para as aplicações que realizaremos, atribuímos a cada *i-ésima* letra L do alfabeto $\mathscr{A}$ o *i-ésimo* número em $[0,25]$. Como $[0,25]$ é exatamente os restos na divisão por 26, estamos na verdade associando cada letra L_i do alfabeto $\mathscr{A}$ a uma classe residual de $\mathbb{Z}_{26}$. Assim, a codificação $C(L_i)$ estipulada pelo método de César pode ser ecrita de forma geral como

$$C(L_i) \equiv L_i + 3 \pmod{26}, \tag{6.1}$$

no qual L_i pode ser substituída pelo respectivo representante da classe residual de cada letra do alfabeto $\mathscr{A}$, para encontramos a codifiação desejada. Mediante ao exposto, reconstruímos a representação de $\mathscr{A}$ feita na Tabela 3 como:

$\mathscr{A}$	A	B	C	D	E	F	G	H	I	J	K	L	M
Cifras	0	1	2	3	4	5	6	7	8	9	10	11	12

$\mathscr{A}$	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifras	13	14	15	16	17	18	19	20	21	22	23	24	25

Tabela 4 – Alfabeto $\mathscr{A}$ em $\mathbb{Z}_{26}$.

Exemplo 58. Para encriptar a palavra *FELIZ*, segundo as observações realizadas acima, faríamos

$$\begin{aligned}
C(F) &\equiv 5+3 \equiv 8 && (\text{mod } 26) \Longrightarrow C(F) = I \\
C(E) &\equiv 4+3 \equiv 7 && (\text{mod } 26) \Longrightarrow C(E) = H \\
C(L) &\equiv 11+3 \equiv 14 && (\text{mod } 26) \Longrightarrow C(L) = O \\
C(I) &\equiv 8+3 \equiv 11 && (\text{mod } 26) \Longrightarrow C(I) = L \\
C(Z) &\equiv 25+3 \equiv 28 \equiv 2 && (\text{mod } 26) \Longrightarrow C(Z) = C.
\end{aligned}$$

Assim, a palavra *FELIZ* fica cifrada como IHOLC.

Nessa vertente seria possível constuir vários métodos de cifragens diferente, mudando a regra de permutação das letras, ou até mesmo, considerando um alfabeto $\mathscr{A}'$ com vários outros símbolos.

Chamamos a atenção ao fato de que, de posse da congruência (6.1), é possível não somente cifrar uma mensagem mas também decifra-la. De fato, determinar a congruência de decodificação é uma tarefa simples, tal que

$$L_i \equiv C(L_i) - 3 \pmod{26}. \tag{6.2}$$

Métodos criptogáficos como o descrito acima são conhecidos como *métodos de substituição simples*. A vulnerabilidade de tais métodos encontram-se na possibilidade da análise da frequência das letras numa mensagem cifrada. Efetivamente um interceptador tendo conhecimento da língua e estrutura ortográfica na qual a mensagem foi expedida, é possível confabular sobre possíveis combinações entre as letras num geral.

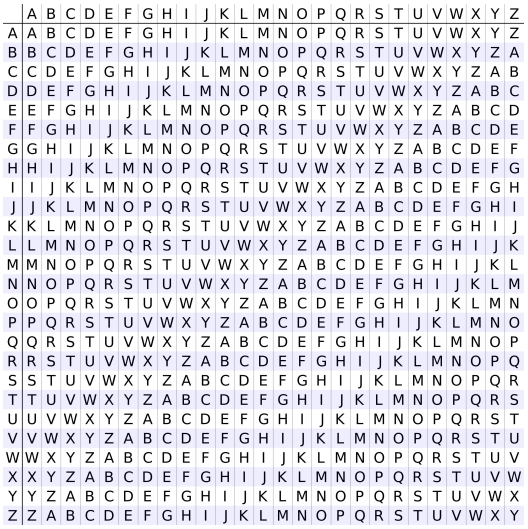
Uma forma encontrada para contornar a possibilidade da contagem de frequência das letras, a fim de quebrar um sistema criptográfico, foi a criação de sistemas de *cifras de substituição polialfabéticas*, ou seja, utiliza-se de vários alfabetos e permutações para a substituição das letras, assim uma mesma letra pode ser representada por vários símbolos distintos numa mesma mensagem.

Citaremos o método de Vigenère como um exemplo de sistema criptográfico polialfabético devido a sua ampla repercursão e facilidade de aplicação. Nele utiliza-se uma série de diferentes "Cifras de César", baseadas numa *chave* que é aplicada tanto na cifragem quanto na decifragem. Na prática, refere-se a uma tabela constituída pelo mesmo número de linhas e colunas no qual o alfabeto é escrito repetidamente, de forma que a cada linha, cada letra desloca-se ciclicamente uma posição em relação a anterior.

Escolhida uma *chave*, que pode ser uma palavra, uma sequência de letras ou uma frase, a cifração ocorria do seguinte modo: "Se sobre uma dada letra do texto encontra-se uma determinada letra da palavra chave, então se substitui essa por aquela que lhe corresponde na sua coluna e na linha que começa com a letra da palavra chave" (HEFEZ, 2014, p. 314).

Exemplo 59. Abaixo temos a *Tabula Recta* que é a tabela utilizada no método de encriptação de Vigenère.

Figura 1 – Tabula Recta de Vigenère.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Fonte: Fields (2011).

Vamos codificar a frase “Liberdade a todos”, a partir da palavra chave CENTRO. Seguindo a metodologia descrita, escreveremos :

L I B E R D A D E A T O D O S
C E N T R O C E N T R O C E N.

Observe que para encriptar a primeira letra da mensagem, no caso o L, olharemos na coluna que lhe representa, na terceira linha, ou seja, na linha correspondente a letra C, obtendo N. Seguindo este mesmo raciocínio, temos a mensagem encriptada:

NMOXIRCHRTKCFSF.

Perceba que letras iguais da mensagem original, foram encriptadas com cifras diferentes, ilustrando essa forte característica de segurança proposta pelo método de Vigenère.

Podemos também expressar o sistema criptográfico de Vigenère utilizando conceitos da aritmética modular. Consideremos o alfabeto $\mathscr{A}$ com as respectivas associações entre suas letras ao intervalo $(0,25)$ e seja $L_1, L_2, ..., L_{n-1}$ uma sequência de letras a ser cifrada por uma palavra chave constituída pela sequência de letras $P_1, P_2, ..., P_{m-1}$, tal que $m < n$. Calculamos a sequência cifrada $C_1, C_2, ..., C_{n-1}$ da seguinte forma

$$C_i \equiv L_i + P_i \pmod{26}. \tag{6.3}$$

Note que para as m primeiras letras, a *i-ésima* letra da mensagem é somada a *i-ésima* letra da chave, depois as letras da chave repetem-se a cada ciclo de m letras até que toda a mensagem seja encriptada. Comparando o resultado encontrado com a congruência (6.1) percebe-se que

para cada letra codificada da mensagem, usa-se uma Cifra de César diferente, dependendo da letra da chave na qual tal letra está associada.

Exemplo 60. Fazendo uso da congruência (6.3), encriptemos a palavra Matemática usando a chave FERMAT.

Chamemos de $C_1, C_2, ..., C_{10}$ a sequência das cifras de cada letra da palavra Matemática. Utilizando a Tabela 4 que associa cada letra do alfabeto $\mathscr{A}$ a um representante dos elementos de $\mathbb{Z}_{26}$, temos:

$$\begin{aligned}
C_1 &\equiv 12+5 \equiv 17 && \pmod{26} \Longrightarrow C_1 = R \\
C_2 &\equiv 0+4 \equiv 4 && \pmod{26} \Longrightarrow C_2 = E \\
C_3 &\equiv 19+17 \equiv 36 \equiv 10 && \pmod{26} \Longrightarrow C_3 = K \\
C_4 &\equiv 4+12 \equiv 16 && \pmod{26} \Longrightarrow C_4 = Q \\
C_5 &\equiv 12+0 \equiv 12 && \pmod{26} \Longrightarrow C_5 = M \\
C_6 &\equiv 0+19 \equiv 19 && \pmod{26} \Longrightarrow C_6 = T \\
C_7 &\equiv 19+5 \equiv 24 && \pmod{26} \Longrightarrow C_7 = Y \\
C_8 &\equiv 8+4 \equiv 12 && \pmod{26} \Longrightarrow C_8 = M \\
C_9 &\equiv 2+17 \equiv 19 && \pmod{26} \Longrightarrow C_9 = T \\
C_{10} &\equiv 0+12 \equiv 12 && \pmod{26} \Longrightarrow C_5 = M.
\end{aligned}$$

Logo, a palavra Matemática é cifrada como REKQMTYMT.

Assim como no método de César, a decifração da mensagem pode ser feita usando o mesmo algorítmo da cifração com simples manipulações algébricas, de forma que

$$L_i \equiv C_i - P_i \pmod{26}. \tag{6.4}$$

O que torna o método de Vigenère mais robusto em relação ao método de César é a possibilidade de utilizar-se de múltiplas letras do texto cifrado, para uma mesma letra do texto original, ocultando assim informações sobre a fequência de uma dada letra.

Os métodos polialfabéticos ganharam uma nova perspectiva com a criação das máquinas cifradoras. No contexto da Segunda Guerra Mundial duas dessas máquinas desempenharam participação fundamental no desfecho da guerra: a alemã Enigma e a japonesa Purple. A Enigma era uma máquina que poderia ser configurada numa quantidade gigantesca de maneiras diferentes, como segue

$$\frac{3!26^3}{10!} = \binom{26}{2}\binom{24}{2}\binom{22}{2}\binom{20}{2}\binom{18}{2}\binom{16}{2}\binom{14}{2}\binom{12}{2}\binom{10}{2}\binom{8}{2}.$$

Ao final de cada dia as instruções de configurações eram trocadas para o dia seguinte. Não descreveremos detalhadamente o funcionamento dessas máquinas, nos ateremos a dizer que,

de uma forma geral, elas permutavam as letras da mensagem original através de um circuito que era ajustado por uma nova chave diariamente. O sistema de cifragem alemã foi quebrado pelos britânicos com a ajuda de Alan Turing, que participou do desenvolvimento de um sistema eletrônico capaz de rapidamente considerar as várias configurações da Enigma, até determinar aquela que estava sendo usada.

Figura 2 – Máquina Enigma.

Fonte: Buccoliero (2020).

O bom funcionamento dos métodos de criptografia depende não somente do destinatário receber de forma segura uma mensagem, mas que também consiga decifrá-la. Dessa forma, um sistema complexo de cifragem não é suficiente se não houver uma maneira segura e eficiente de realizar a troca das "chaves de decodificação" e diante disso, pairava um problema a ser aperfeiçoado nos sistemas criptográficos.

Até meados do século XX os sistemas criptográficos adotavam *chaves simétricas*, ou seja, a mesma chave era utilizada para cifrar e decifrar uma mensagem. Com o grande advento dos computadores, por volta de 1970, surgiu espaço para uma nova proposta: a de métodos criptográficos com *chaves assimétricas*, isto é, a utilização de chaves distintas para cifragem e decifragem de mensagens. É nesta nova perspectiva que a Teoria dos Números exerce papel fundamental, proporcionando o embasamento necessário para esta nova proposta, principalmente através do uso dos resultados em torno de congruências.

O primeiro passo para esta nova vertente criptográfica foi realizada pelos norte-americanos Whitfield Driffe, Martin Helman e Ralph Merkle, através do método criados por eles denominado de DHM. Sua inovação estava na utilização de *chaves públicas*, isto é, as chaves de cifragem eram de conhecimento com livre acesso, e na não necessidade de um intermediário para troca das senhas para decodificação. No seu funcionamento utilizavam-se de resultados da aritmética modular. A promoção da segurança deste método, baseava-se na ideia geral que dados $a, m, x, y \in \mathbb{N}$, de modo que

$$a^x \equiv y \pmod{m},$$

é fácil determinar y conhecendo a, m e x, contudo o caminho inverso, ou seja, determinar x conhecendo a, y e m é totalmente inviável de ser calculado, mesmo com uso de computadores. O ponto frágil do sistema DHM estava na limitação entre a troca das senhas para decifragem, elas ocorreriam entre as partes interessadas uma de cada vez, não atendendo a demanda de um mercado crescente e globalizado. Porém, foi do próprio Driffe a publicação que sugeria a utilização de chaves assimétricas, sendo uma chave pública para cifração e uma chave oculta para decifração, de modo a ser impossível determinar o processo inverso sem estar de posse da chave oculta.

6.2 O sistema RSA

Finalmente, em 1978, norteados no método DHM e pelas considerações de Driffe, Ronald Rivest, Adi Shamir e Leonard Adleman criaram o primeiro sistema criptográfico com a utilização de chaves assimétricas, que ficou comenhecido como RSA. A base do sistema é dado pela facilidade em determinar números primos de ordens numéricas elevadas, e de contrapartida, na dificuldade em fatorar o produto desses números. Acrescenta-se ainda que a matemática necessária para a execução do método são propriedades e teoremas parcialmente elementares da Teoria dos Números.

As cifras geradas pelo RSA não só ofereceram uma opção segura na troca de informações entre usuários localizados a qualquer distância do globo quanto criaram, como uma consequência direta, um método de assinaturas digitais muito comum hoje em dia.

Mostraremos a seguir, de forma mais detalhada e exemplificada, os passos que constituem o funcionamento do sistema RSA assim como sua eficiência, aplicando para tal os resultados em torno dos estudos de congruências realizadas nos capítulos anteriores.

6.2.1 Transformando uma mensagem em blocos

Antes de começarmos o desbravamento do método RSA, façamos algumas denotações. Estabeleceremos o alfabeto $\mathscr{A}$ como nossa base de códigos para construir uma mensagem a ser codificada. Todavia, os sistemas criptogáficos atuais utilizam-se de todos os códigos estabelecidos pelo ASCII [1], não sendo necessário inclusive o uso da base decimal. Definiremos ainda como L_i, com $i \in \{0, 1, 2, ..., 25\}$, as letras do alfabeto $\mathscr{A}$ e 99 a representação dos espaços entre as palavras. Note que a eficácia da utilização do 99 está no fato dos números 9 e 99 não representarem nenhuma letra no intervalo proposto para $\mathscr{A}$. Desse modo, para o caso que

[1] O nome ASCII vem do inglês *American Standard Code for Information Interchange* ou *"Código Padrão Americano para o Intercâmbio de Informação"*. Ele é baseado no alfabeto romano e sua função é padronizar a forma como os computadores representam letras, números, acentos, sinais diversos e alguns códigos de controle.

estamos tratando, os números $88, 77, 66, 55$ e 44 também poderiam ser tomados na determinação dos espaços entre as palavras, pela mesma justificativa aplicada a 99.

Para utilização do sistema RSA é necessário transpor a mensagem escrita em uma sequência numérica, dessa forma associaremos para cada *i-ésimo* L_i da mensagem a ser codicada, o *i-ésimo* número em $[10, 35]$. Provavelmente paira um questionamento sobre a escolha do intervalo, a resposta é rápida: a utilização de números com um algarismo pode causar uma "confusão" no momento da decodificação. Por exemplo, a cifra 14 pode representar B e E, ou somente M, baseando-se na associação para cada L_i de $\mathscr{A}$ em $[0, 25]$. Desse modo, a escolha da representação com dois algarismos para cada código de linguagem não é condição única, mas minimal.

Segue a transposição de $\mathscr{A}$ no intervalo proposto:

L_i	A	B	C	D	E	F	G	H	I	J	K	L	M
Cifras	10	11	12	13	14	15	16	17	18	19	20	21	22

L_i	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cifras	23	24	25	26	27	28	29	30	31	32	33	34	35

Tabela 5 – Alfabeto $\mathscr{A}$ no intervalo definido para análise do RSA.

Exemplo 61. Codificaremos, segundo os parâmetros estabelecidos, a mensagem: "PENSO LOGO EXISTO ". Encontramos a sequência

$$25142328249921241624991433182829 24.$$

Nos métodos criptográficos citados na seção anterior vimos que uma das fragilidades enfrentadas na história da criptografia é driblar a possibilidade da quebra do código de cifração, a partir da análise da frequência dos símbolos. Um olhar mais apurado para o Exemplo 61 pode-se perceber algumas possíveis brechas para confabulações acerca da codificação que foi aplicada. Neste ponto da nossa discussão entra uma estratégia crucial aplicada no método RSA: a conversão da nossa sequência numérica em blocos.

Para a concretização desse passo, façamos primeiramente a determinação dos subsídios numéricos que serão a base para a elaboração das chaves aplicadas e, consequentemente, dos processos de codificação e decodificação. Para isso, escolhe-se dois números primos distintos, p e q, e determina-se um $m \in \mathbb{N}$, tal que $m = pq$.

A decomposição da sequência numérica em blocos não é feita de maneira única e não se prende a nenhuma estrutura linguística. Cada bloco b_k é um número natural, tal que $b_k < m$ e que não comece pelo algarismo 0. Respeitando essas condições, um bloco b_k pode ter comprimentos arbitrários e variados conforme se deseje.

Exemplo 62. Façamos a divisão da sequência encontrada para nossa mensagem em blocos. Definiremos os algarismos $p = 17$ e $p = 19$ e, portanto, $m = 17.19 = 323$. Com isso, cada bloco b_k será construído de forma que $b_k < 323$. Temos então que

$$25 - 142 - 32 - 82 - 49 - 92 - 124 - 162 - 49 - 91 - 43 - 318 - 282 - 92 - 4,$$

é a sequência dos blocos $b_1, b_2, \ldots, b_{15}$ para nosso exemplo.

Exemplo 63. Assumindo os mesmo valores de p e q e, consequentemente, para m, uma outra maneira de determinar uma sequência de blocos b_k para a mensagem proposta é a apresentada a seguir:

$$251 - 42 - 32 - 8 - 249 - 9 - 212 - 41 - 62 - 49 - 9 - 143 - 31 - 82 - 82 - 9 - 24,$$

de modo que a sequência $b_1, b_2, \ldots, b_{17}$ representa também uma configuração pertinente para a divisão da nossa mensagem codificada em blocos.

6.2.2 O processso de codificação

Dada a separação dos blocos b_k, realizaremos a partir deles a codificação, um a um, segundo alguns parâmetros, conforme estabelecidos a seguir.

Elegeremos um $e \in \mathbb{N}$ de forma que $\text{mdc}(e, \varphi(m)) = 1$, ou seja, segundo a Proposição 18 o natural e é invertível no módulo $\varphi(m)$. Como $m = pq$, temos pela Proposição 12 que

$$\varphi(m) = (p-1)(q-1).$$

O par (e, m) é chamado de chave de codificação, e no RSA é de conhecimento público, podendo ser acessada por qualquer pessoa. Entretanto, os números p e q são ocultos e sua não divulgação é um dos princípios da segurança deste método como compreenderemos melhor ao longo desta seção.

Exemplo 64. Se tomarmos $p = 7$ e $q = 11$ para elaborar uma chave de codificação como a definida acima, temos que $m = 7.11 = 77$ e

$$\varphi(m) = (7-1)(11-1) = 60.$$

Assim, teríamos que determinar o natural e de modo que $\text{mdc}(e, 60) = 1$. Como $60 = 2^2.3.5$, pela Proposição 6 sabemos que e pode ser qualquer número natural que não contenha em sua fatoração os primos $2, 3$ e 5 ou que seja um número primo diferente de $2, 3$ e 5. Escolhendo $e = 91$, temos que a chave de codificação divulgada para criptografar uma dada mensagem no sistema RSA é $(91, 77)$.

No caso em que estamos tratando, expresso no Exemplo 62, como p e q são conhecidos, o cálculo de $\varphi(m)$ e e são triviais. Vale ressaltar que e pode ser qualquer representante de uma das classes de $\mathbb{Z}^*_{\varphi(m)}$.

Chamaremos de $C(b_k)$ o resulado da codificação dos blocos b_k estipulados previamente, dado por

$$C(b_k) \equiv b_k^e \pmod{m}. \tag{6.5}$$

Após a determinação da sequência $C(b_1), C(b_2), ..., C(b_k)$ é importante que os números encontrados não sejam reunidos de modo a formar um único número; isso comprometeria a decodificação da mensagem.

Exemplo 65. Vejamos como ficará a codificação dos blocos encontradados no Exemplo 62, seguindo o algoritmo estipulado em (6.5).

Como $p = 17$ e $q = 19$, segue que

$$\varphi(m) = \varphi(323) = (17-1)(19-1) = 288.$$

Agora vamos escolher e que deve pertencer a $\mathbb{Z}^*_{288}$. Utilizaremos $e = 5$, por ser o menor número primo com 288. Aplicando a regra para codificação e algumas das propriedades das congruências vistas no Capítulo 3, temos

$$\begin{aligned}
C(b_1) &\equiv 25^5 \equiv 25^3.25^2 \equiv 121.302 \equiv 43 && \pmod{323},\\
C(b_2) &\equiv 142^5 \equiv (142^2)^2.142 \equiv 138^2.142 \equiv 92 && \pmod{323},\\
C(b_3) &\equiv 32^5 \equiv (32^2)^2.32 \equiv 55^2.32 \equiv 118.32 \equiv 223 && \pmod{323},\\
C(b_4) &\equiv 82^5 \equiv (82^2)^2.82 \equiv 264^2.82 \equiv 233 && \pmod{323},\\
C(b_5) &\equiv 49^5 \equiv (49^2)^2.49 \equiv 140^2.49 \equiv 121 && \pmod{323},\\
C(b_6) &\equiv 92^5 \equiv (92^2)^2.92 \equiv 66^2.92 \equiv 232 && \pmod{323},\\
C(b_7) &\equiv 124^5 \equiv 124^3.124^2 \equiv 278.195 \equiv 269 && \pmod{323},\\
C(b_8) &\equiv 162^5 \equiv (162^2)^2.162 \equiv 81^2.162 \equiv 101.162 \equiv 212 && \pmod{323},\\
C(b_9) &\equiv C(b_5) \equiv 121 && \pmod{323},\\
C(b_{10}) &\equiv 91^5 \equiv (91^2)^2.91 \equiv 206^2.91 \equiv 123.91 \equiv 211 && \pmod{323},\\
C(b_{11}) &\equiv 43^5 \equiv 43^3.43^2 \equiv 49.234 \equiv 161 && \pmod{323},\\
C(b_{12}) &\equiv 318^5 \equiv (-5)^5 \equiv (-5)^3.(-5)^2 \equiv -125.25 \equiv 105 && \pmod{323},\\
C(b_{13}) &\equiv 282^5 \equiv (-41)^5 \equiv (-41)^3.(-41)^2 \equiv 201.66 \equiv 23 && \pmod{323},\\
C(b_{14}) &\equiv C(b_6) \equiv 232 && \pmod{323},\\
C(b_{15}) &\equiv 4^5 \equiv 1024 \equiv 55 && \pmod{323}.
\end{aligned}$$

Observe que seria completamente inviáveis realizar tais operações sem a utilização das propriedades de congruência de modo a simplificar os números encontrados.

Portanto, nossa sequência de blocos codificados $C(b_1), C(b_2)..., C(b_{15})$ é

$$43 - 92 - 223 - 233 - 121 - 232 - 269 - 212 - 121 - 211 - 161 - 105 - 23 - 232 - 55.$$

Note que a separação dos blocos implica diretamente no resultado encontrado no processo de codificação, dessa forma a sequência de codificação seria diferente se utilizassemos os blocos definidos no Exemplo 63.

Observação 7. Na determinação dos blocos b_k definiu-se a condição de que os mesmos não se iniciassem por 0 e neste ponto da discussão é possível verificar a clareza dessa ação. Analisando a equivalência de codificação (6.5) percebe-se, por exemplo, que a codificação de um bloco 025 é numericamente equivalente a codificação de um bloco 25, mas essa equivalência não se aplica a conversão correta das letras da mensagem criptografada.

6.2.3 O processo de decodificação

O procedimento de decodificação dos blocos $C(b_k)$ é realizada a partir de uma chave de decodificação (m,d), oculta e de posse somente do receptor da mensagem, no qual $d \in \mathbb{N}$ tal que

$$de \equiv 1 \pmod{\varphi(m)}, \tag{6.6}$$

ou seja, d é o inverso multiplicativo de e módulo $\varphi(m)$. Como o conhecimento de e e m são informações acessíveis, encontramos o valor de d resolvendo a equação diofantina

$$de - \varphi(m)t = 1, \qquad t \in \mathbb{Z}. \tag{6.7}$$

Exemplo 66. Vamos calcular d para $e = 5$ e $m = 323$ do Exemplo 65. Como $\varphi(m) = 288$ e $\text{mdc}(e, \varphi(m)) = \text{mdc}(d, \varphi(m)) = 1$, temos a seguinte congruência linear

$$5d \equiv 1 \pmod{288}. \tag{6.8}$$

De posse do conceito sobre sistemas reduzidos de resíduos apresentado no Capítulo 5, sabemos que como 5 e d são invertíveis, ambos pertencem a $\mathbb{Z}^*_{288}$. Com isso, poderíamos determinar os elementos desse conjunto e encontrar o valor de d, resolvendo a congruência. Contudo, não acreditamos ser o modo mais simplificado e optaremos por outra abordagem.

Reescrevendo a congruência (6.8) como

$$5d = 1 + 288t \Longrightarrow 5d - 288t = 1, \quad t \in \mathbb{Z} \tag{6.9}$$

e aplicando o Teorema 6, temos que $d = -115$. Mas como $d \in \mathbb{N}$ fazemos $d = 288 - 115 = 173$, de modo que 173 é o menor inteiro positivo tal que $-115 \equiv x \pmod{288}$.

Chamaremos de $D(C(b_k))$ o resultado do processo de decodificação, que é determinado por

$$D(C(b_k)) \equiv (C(b_k))^d \pmod{m}. \tag{6.10}$$

Da mesma maneira que no processo de codificação, o procedimento de decodificação é aplicado individualmente a cada bloco encontrado $C(b_k)$.

Um sistema criptográfico só é eficiente se, após aplicar a decifragem num código recebido, obtém-se a mensagem original na íntegra. Assim, o sistema RSA como estamos apresentando, só seria útil se

$$D(C(b_k)) = b_k. \tag{6.11}$$

Mas, note que a equação acima é o mesmo que verificar a congruência

$$D(C(b_k)) \equiv (C(b_k))^d \equiv (b_k^e)^d \equiv (b_k)^{ed} \equiv b_k \pmod{m}. \tag{6.12}$$

Observe que a possibilidade de resumirmos nossa resposta acerca da funcionabilidade do RSA na verificação da congruência $D(C(b_k)) \equiv b_k \pmod{m}$ é mediante ao cuidado ao longo do processo em manter $1 < b_k, D(C(b_k)) \leq m-1$, e em não misturar os blocos codificados.

A verificação de (6.12) não é imediata, então a faremos detalhadamente a seguir. Como $m = pq$, no qual p e q são primos distintos e, portanto, $\text{mdc}(p,q) = 1$, segue da Proposição 16 que se $b_k^{ed} \equiv b_k \pmod{m}$, então

$$b_k^{ed} \equiv b_k \pmod{p} \tag{6.13}$$

e

$$b_k^{ed} \equiv b_k \pmod{q}. \tag{6.14}$$

Façamos a verificação para p. Substituindo a equação encontrada em (6.7) na equação (6.13) temos

$$b_k^{ed} \equiv b_k^{1+\varphi(m)t} \equiv b_k.b_k^{[(p-1)(q-1)]t} \pmod{p}. \tag{6.15}$$

Analisando a congruência (6.15) observa-se os possíveis casos:

(i) Se $p \nmid b_k$, então pelo Corolário 4 temos que

$$b_k^{p-1} \equiv 1 \pmod{p},$$

e aplicando o resultado em 6.15 segue

$$b_k^{ed} \equiv b_k(b_k^{(p-1)})^{(q-1)t} \equiv b_k.1^{(q-1)t} \equiv b_k \pmod{p}.$$

(ii) Se $p \mid b$, então $b_k \equiv 0 \pmod{p}$ e logo $b_k^{ed} \equiv 0 \pmod{p}$, e por transitividade

$$b_k^{ed} \equiv b_k \pmod{p}.$$

Assim, por (i) e (ii) temos que $b_k^{ed} \equiv b_k \pmod{p}$ para $\forall b_k \in \mathbb{Z}$. De forma análoga verifica-se que $b_k^{ed} \equiv b_k \pmod{q}$ e portanto

$$b_k^{ed} \equiv b_k \pmod{pq} \Longrightarrow b_k^{ed} \equiv b_k \pmod{m}.$$

Dessa forma fica comprovado a validade da congruência (6.12) e, consequentemente, a funcionabilidade e eficiência da aplicação do método RSA. Com isso, sabemos que ao aplicarmos a regra apresentada em (6.10) obteremos os blocos designados primordialmente da mensagem original.

Motivados pelas discussões acima, aplicaremos o algoritmo de decodificação no exemplo numérico que estamos desenvolvendo ao longo dessa seção. No Exemplo 66 encontramos $d = 173$, e como já se pode imaginar, trabalhar com um expoente dessa grandeza, acrescido aos números encontrados para $C(b_k)$ com $k \in \{1,2,...,15\}$, não é uma tarefa rápida usando recursos restritos. Na prática tais cálculos são feitos por programas computacionais específicos. Faremos a decodificação de alguns blocos determinados no Exemplo 65.

Exemplo 67. Tomando o bloco codificado $C(b_1) = 43$, determinaremos $D(C(b_1))$. Note que

$$D(C(b_1)) \equiv 43^d \equiv 43^{173} \pmod{323}.$$

Para possibilitar o cálculo usando recursos tangíveis a nós, reescreveremos o expoente em parcelas de números menores e aplicaremos uma sequência de proposições e estratégias acerca das congruências, mostradas no Capítulo 4. Escrevendo $d = 173 = 2^7 + 2^5 + 2^3 + 5$, podemos obter as congruências

$$\begin{aligned}
&43^2 \equiv 234 && \pmod{323},\\
&43^{2^2} \equiv (43^2)^2 \equiv 169 && \pmod{323},\\
&43^{2^3} \equiv (43^{2^2})^2 \equiv 169^2 \equiv 137 && \pmod{323},\\
&43^{2^4} \equiv (43^{2^3})^2 \equiv 137^2 \equiv 35 && \pmod{323},\\
&43^{2^5} \equiv (43^{2^4})^2 \equiv 35^2 \equiv 256 && \pmod{323},\\
&43^{2^6} \equiv (43^{2^5})^2 \equiv 256^2 \equiv 290 && \pmod{323},\\
&43^{2^7} \equiv (43^{2^6})^2 \equiv 290^2 \equiv 120 && \pmod{323},\\
&43^5 \equiv (43^{2^2}).43 \equiv 169.43 \equiv 161 && \pmod{323}.
\end{aligned}$$

Dessa forma, fazendo as substituições adequadas, temos

$$\begin{aligned}
D(C(b_1)) &\equiv 43^{173} \equiv 43^{2^7+2^5+2^3+5} \equiv 43^{2^7}.43^{2^5}.43^{2^3}.43^5\\
&\equiv 120.256.137.161 \equiv 35.93 \equiv 25 \pmod{323}.
\end{aligned}$$

Portanto, $D(C(b_1)) \equiv b_1 \equiv 25 \pmod{323}$, como se esperava segundo a equação (6.12).

Uma outra maneira de decodificar os blocos encontrados no Exemplo 65 é a partir do uso das equações diofantinas lineares, mais especificamente, através dos métodos de resolução explicitados no Capítulo 4. Vejamos como tal ideia pode ser aplicada.

Exemplo 68. Façamos a decodificação do bloco $C(b_{13})$, determinado no Exemplo 65.

Sabemos que $C(b_{13}) \equiv 23 \pmod{323}$ e aplicando a congruência (6.10), buscamos

$$D(C(b_{13})) \equiv (C(b_{13}))^d \pmod{323}. \tag{6.16}$$

Pela Proposição 16 temos que

$$\begin{cases} D(C(b_{13})) \equiv (C(b_{13}))^d \pmod{17}, \\ D(C(b_{13})) \equiv (C(b_{13}))^d \pmod{19}, \end{cases} \Longrightarrow D(C(b_{13})) \equiv (C(b_{13}))^d \pmod{323}. \tag{6.17}$$

Temos

$$D(C(b_{13})) \equiv 23^{173} \equiv 4^{173} \pmod{17}, \tag{6.18}$$
$$D(C(b_{13})) \equiv 23^{173} \equiv 6^{173} \pmod{19}. \tag{6.19}$$

Pelo Corolário 4 sabemos que $6^{16} \equiv 1 \pmod{17}$ e $4^{18} \equiv 1 \pmod{19}$. Fazendo a divisão euclidiana de 173 por 16 e 18, escrevemos $173 = 16.10 + 13$ e $173 = 18.9 + 11$. Substituindo em (6.18) e (6.19) temos

$$D(C(b_{13})) \equiv 6^{16.10+13} \equiv (6^{16})^{10}.6^{13} \equiv 6^{13} \equiv (6^2)^6.6 \equiv 2^6.6 \equiv 10 \pmod{17}$$

e

$$D(C(b_{13})) \equiv 4^{18.9+11} \equiv (4^1 18)^9.4^{11} \equiv 4^{11} \equiv (4^3)^3.4^2 \equiv 7^3.(-3) \equiv -3 \equiv 16 \pmod{19}.$$

Logo

$$D(C(b_{13})) \equiv 10 \pmod{17}, \tag{6.20}$$
$$D(C(b_{13})) \equiv 16 \pmod{19}. \tag{6.21}$$

A simplificação encontrada acima pode ser escrita da forma

$$D(C(b_{13})) = 10 + 17p, \quad p \in \mathbb{Z}, \tag{6.22}$$
$$D(C(b_{13})) = 16 + 19t, \quad t \in \mathbb{Z}. \tag{6.23}$$

Assim, igualando (6.22) a (6.23) obtemos a equação diofantina

$$\begin{aligned} 19t + 16 &= 10 + 17p \\ 19t - 17p &= -6 \\ 17p - 19t &= 6. \end{aligned} \tag{6.24}$$

Como $D(C(b_{13})) > 0$, nosso problema recai em determinar a solução minimal, pertencentes aos $\mathbb{N}$, da equação diofantina (6.24). Procederemos conforme mostrado no Exemplo 32.

Buscaremos inicialmente a solução geral para a equação (6.24) nos $\mathbb{Z}$, desse modo suponha que existam $p_0, t_0 \in \mathbb{Z}$ tais que

$$17p_0 - 19t_0 = 6. \tag{6.25}$$

Como se trata de uma relação entre números inteiros, sem perda de generalidade, observamos que

$$\begin{aligned} 17p_0 - 19t_0 &\equiv 6 \pmod{17} \\ -2t_0 &\equiv 6 \pmod{17}. \end{aligned} \tag{6.26}$$

Com isso, para que (6.25) possua soluções inteiras basta mostrarmos que existe o inteiro t_0 que satisfaça a equivalência (6.26). Aplicando o resultado expresso na Proposição 14 temos

$$-2t_0 \equiv -9(-2t_0) \equiv 18t_0 \equiv t_0 \equiv -54 \equiv 14 \pmod{17}. \tag{6.27}$$

Assim comprova-se a existência do inteiro t_0 de forma que seus possíveis valores são dados por

$$t_0 = 17k + 14,\ k \in \mathbb{Z}. \tag{6.28}$$

Substituindo o resultado de (6.28) na equação (6.25) temos

$$\begin{aligned} 17p_0 - 19(17k+14) &= 6, \\ 17p_0 - 19.17k - 266 &= 6, \\ 17p_0 &= 19.17k + 272, \\ p_0 &= 19k + 16. \end{aligned} \tag{6.29}$$

Portanto, as soluções inteiras para a equação (6.25) são dadas por

$$\begin{cases} p = 19k + 16, \\ t = 17k + 14, \quad \forall, k \in \mathbb{Z}. \end{cases}$$

Como buscamos a menor solução positiva para p e t, ou seja, $19k + 16 \geq 0$ e $17k + 14 \geq 0$ note que para todo $k \geq 0$ encontramos uma solução positiva para a equação (6.25), logo a solução minimal procurada é dada por $k = 0$, assim

$$\begin{cases} p = 19.0 + 16 = 16, \\ t = 17.0 + 14 = 14. \end{cases}$$

Aplicando o valor minimal encontrado para p na igualdade (6.22) segue que

$$D(C(b_{13})) = 10 + 17.16 = 282,$$

logo $D(C(b_{13})) = b_{13} = 282$, comprovando a eficiência e funcionabilidade do RSA.

Não realizaremos a decodificação dos demais blocos encontrados no Exemplo 65, pois a metodologia e fundamentação teórica é a mesma utilizada nos dois últimos exemplos. É importante salientar que os métodos de decodificação apresentados nesta seção não são únicos, existem outros resultados e teoremas aritméticos que podem ser utilizados para esta finalidade.

Para ilustrar todos os passos aplicados no sistema RSA realizaremos um exemplo geral - da encriptação a decifração. É importante salientar que na prática onde esse sistema é utilizado, as etapas são realizadas de uma forma mais concisa e rápida, devido ao uso de ferramentas e programas computacionais. Desse modo, o exemplo que trabalharemos pode servir também como norteador para o professor, que após tomar conhecimento do embasamento teórico apresentado ao logo da seção, queira elaborar uma atividade de aplicação para incrementar seu planejamento curricular.

Exemplo 69. Vamos enviar a mensagem CONGRUO, criptografada segundo o sistema RSA, para o destinatário Y.

Inicalmente selecionaremos dois primos distintos r e s, para determinação das chaves de codificação (e,m), de conhecimento público, e de decodificação (m,d), que será enviada de forma oculta a Y. Determinaremos $r = 11$ e $s = 29$.

Chave de codificação. Temos que $m = rs = 319$ e $e \in \mathbb{N}$, tal que $\text{mdc}(e, \varphi(m)) = 1$. Pela Proposição 12 segue que

$$\varphi(m) = (r-1)(s-1) = 28.10 = 280.$$

Pelo Teorema 8 escrevemos $280 = 2^3.5$, logo escolheremos e de forma a não conter nenhum desses fatores primos em sua decomposição, a fim de garantir a condição definida. Tomaremos $e = 3$, assim temos que a chave pública de codificação é $(3, 319)$.

Chave de decodificação. Determinaremos $d \in \mathbb{N}$, tal que $de \equiv 1 \pmod{\varphi(m)}$ resolvendo a equação diofantina

$$3d - 280t = 1, \qquad \text{com } t \in \mathbb{Z}. \tag{6.30}$$

Aplicando o Teorema 6 a equação (6.30) temos que $d = -93$, mas como $d \in \mathbb{N}$ segue que $d = 280 - 93 = 187$ é o menor inteiro positivo, tal que $-93 \equiv x \pmod{280}$. Dessa forma a chave de decodificação a ser enviada ocultamente para Y é $(319, 187)$.

Preparação para codificação.Iremos agora fazer a transposição da nossa mensagem segundo os códigos dados na Tabela 5. Assim, encontramos

$$122422316273024.$$

Fazendo uma separação em blocos (b_k) de forma que $b_k < m$ temos

$$122-42-316-27-302-4, \tag{6.31}$$

criando assim a sequência de blocos para codificação $b_1,\ldots,b_6$.

Processo de codificação. Aplicando a chave de codificação na equivalência (6.5), temos a codificação dos bolcos da sequência (6.31):

$$\begin{aligned}
C(b_1) &\equiv 122^3 \equiv 122^2.122 \equiv 210.122 \equiv 100 && (\text{mod } 319),\\
C(b_2) &\equiv 42^3 \equiv 42^2.422 \equiv 169.42 \equiv 80 && (\text{mod } 319),\\
C(b_3) &\equiv 316^3 \equiv (-3)^3 \equiv -27 \equiv 292 && (\text{mod } 319),\\
C(b_4) &\equiv 27^3 \equiv 27^2.27 \equiv 91.27 \equiv 224 && (\text{mod } 319),\\
C(b_5) &\equiv 302^3 \equiv (-17)^3 \equiv 191 && (\text{mod } 319),\\
C(b_6) &\equiv 4^3 \equiv 64 && (\text{mod } 319).
\end{aligned}$$

Logo a sequência codificada $C(b_1),\ldots,C(b_6)$ que será enviada a Y é

$$100-80-292-224-191-64. \tag{6.32}$$

Processo de decodificação. Uma vez recebido por Y a sequência (6.32), ele fará a decodificação a partir da chave $(319,280)$. Suponha que Y realize a decodificação dos blocos cifrados que recebeu segundo a metodologia utilizada no Exemplo 67. Primeiramente, Y reescreve d como $d = 187 = 4^3+3^4+6^2+6$ e aplica a equivalência (6.10) a cada $C(b_k)$ recebido, conforme mostrado a seguir.

- $C(b_1)$

  Como $C(b_1) = 100$ obtém-se as congruências

$$\begin{aligned}
100^4 &\equiv (100^2)^2 \equiv 111.111 \equiv 199 && (\text{mod } 319),\\
100^{4^2} &\equiv (100^4)^4 \equiv 199^4 \equiv (199^2)^2 \equiv 45^2 \equiv 111 && (\text{mod } 319),\\
100^{4^3} &\equiv (100^{4^2})^4 \equiv 111^4 \equiv (111^2)^2 \equiv 199^2 \equiv 45 && (\text{mod } 319),\\
100^3 &\equiv 254 && (\text{mod } 319),\\
100^{3^2} &\equiv (100^3)^3 \equiv 254^3 \equiv 34 && (\text{mod } 319),\\
100^{3^3} &\equiv (100^{3^2})^3 \equiv 34^3 \equiv 67 && (\text{mod } 319),\\
100^{3^4} &\equiv (100^{3^3})^3 \equiv 67^3 \equiv 265 && (\text{mod } 319),\\
100^6 &\equiv (100^3)^2 \equiv 254^2 \equiv 78 && (\text{mod } 319),\\
100^{6^2} &\equiv (100^6)^6 \equiv 78^6 \equiv (78^3)^2 \equiv 199^2 \equiv 45 && (\text{mod } 319).
\end{aligned}$$

Aplicando a equivalência (6.10) temos

$$\begin{aligned} D(C(b_1)) &\equiv C(b_1) && (\text{mod } 319),\\ &\equiv 100^{187} && (\text{mod } 319),\\ &\equiv 100^{4^3+3^4+6^2+6} && (\text{mod } 319),\\ &\equiv 100^{4^3}.100^{3^4}.100^{6^2}.100^6 && (\text{mod } 319),\\ &\equiv 45.265.45.78 && (\text{mod } 319),\\ &\equiv 111.265.78 && (\text{mod } 319),\\ &\equiv 122 && (\text{mod } 319), \end{aligned}$$

de forma que $D(C(b_1)) \equiv b_1 \equiv 122 \pmod{319}$.

- $C(b_2)$

  Como $C(b_2) = 80$ obtém-se as congruências

$$\begin{aligned} &80^4 \equiv (80^2)^2 \equiv 20^2 \equiv 81 && (\text{mod } 319),\\ &80^{4^2} \equiv (80^4)^4 \equiv 81^4 \equiv (81^2)^2 \equiv 181^2 \equiv 223 && (\text{mod } 319),\\ &80^{4^3} \equiv (80^{4^2})^4 \equiv 223^4 \equiv (223^2)^2 \equiv 284^2 \equiv 268 && (\text{mod } 319),\\ &80^3 \equiv 5 && (\text{mod } 319),\\ &80^{3^2} \equiv (80^3)^3 \equiv 5^3 \equiv 125 && (\text{mod } 319),\\ &80^{3^3} \equiv (80^{3^2})^3 \equiv 125^3 \equiv 207 && (\text{mod } 319),\\ &80^{3^4} \equiv (80^{3^3})^3 \equiv 207^3 \equiv 267 && (\text{mod } 319),\\ &80^6 \equiv (80^3)^2 \equiv 5^2 \equiv 25 && (\text{mod } 319),\\ &80^{6^2} \equiv (80^6)^6 \equiv 25^6 \equiv (25^3)^2 \equiv 313^2 \equiv 36 && (\text{mod } 319). \end{aligned}$$

Aplicando a equivalência (6.10) temos

$$\begin{aligned} D(C(b_2)) &\equiv C(b_2) && (\text{mod } 319),\\ &\equiv 80^{187} && (\text{mod } 319),\\ &\equiv 80^{4^3+3^4+6^2+6} && (\text{mod } 319),\\ &\equiv 80^{4^3}.80^{3^4}.80^{6^2}.80^6 && (\text{mod } 319),\\ &\equiv 268.267.25.36 && (\text{mod } 319),\\ &\equiv 42 && (\text{mod } 319), \end{aligned}$$

de forma que $D(C(b_2)) \equiv b_2 \equiv 42 \pmod{319}$.

- $C(b_3)$

Como $C(b_3) = 292$ obtém-se as congruências

$$\begin{aligned}
&292^4 \equiv (292^2)^2 \equiv 91^2 \equiv 306 && (\text{mod } 319),\\
&292^{4^2} \equiv (292^4)^4 \equiv 306^4 \equiv (306^2)^2 \equiv 169^2 \equiv 170 && (\text{mod } 319),\\
&292^{4^3} \equiv (292^{4^2})^4 \equiv 170^4 \equiv (170^2)^2 \equiv 190^2 \equiv 53 && (\text{mod } 319),\\
&292^3 \equiv 292^2.292 \equiv 91.292 \equiv 95 && (\text{mod } 319),\\
&292^{3^2} \equiv (292^3)^3 \equiv 95^3 \equiv 222 && (\text{mod } 319),\\
&292^{3^3} \equiv (292^{3^2})^3 \equiv 222^3 \equiv 305 && (\text{mod } 319),\\
&292^{3^4} \equiv (292^{3^3})^3 \equiv 305^3 \equiv (-14)^3 \equiv 127 && (\text{mod } 319),\\
&292^6 \equiv (292^3)^2 \equiv 95^2 \equiv 93 && (\text{mod } 319),\\
&292^{6^2} \equiv (292^6)^6 \equiv 93^6 \equiv (93^3)^2 \equiv 158^2 \equiv 82 && (\text{mod } 319).
\end{aligned}$$

Aplicando a equivalência (6.10) temos

$$\begin{aligned}
D(C(b_3)) &\equiv C(b_3) && (\text{mod } 319),\\
&\equiv 292^{187} && (\text{mod } 319),\\
&\equiv 292^{4^3+3^4+6^2+6} && (\text{mod } 319),\\
&\equiv 292^{4^3}.292^{3^4}.292^{6^2}.292^6 && (\text{mod } 319),\\
&\equiv 53.127.93.82 && (\text{mod } 319),\\
&\equiv 316 && (\text{mod } 319),
\end{aligned}$$

de forma que $D(C(b_3)) \equiv b_3 \equiv 316 \pmod{319}$.

- $C(b_4)$

  Como $C(b_4) = 224$ obtém-se as congruências

$$\begin{aligned}
&224^4 \equiv (224^2)^2 \equiv 93^2 \equiv 36 && (\text{mod } 319),\\
&224^{4^2} \equiv (224^4)^4 \equiv 36^4 \equiv (36^2)^2 \equiv 20^2 \equiv 81 && (\text{mod } 319),\\
&224^{4^3} \equiv (224^{4^2})^4 \equiv 81^4 \equiv (81^2)^2 \equiv 181^2 \equiv 223 && (\text{mod } 319),\\
&224^3 \equiv 97 && (\text{mod } 319),\\
&224^{3^2} \equiv (224^3)^3 \equiv 97^3 \equiv 14 && (\text{mod } 319),\\
&224^{3^3} \equiv (224^{3^2})^3 \equiv 14^3 \equiv 192 && (\text{mod } 319),\\
&224^{3^4} \equiv (224^{3^3})^3 \equiv 192^3 \equiv 235 && (\text{mod } 319),\\
&224^6 \equiv (224^3)^2 \equiv 97^2 \equiv 158 && (\text{mod } 319),\\
&224^{6^2} \equiv (224^6)^6 \equiv 158^6 \equiv (158^3)^2 \equiv 196^2 \equiv 136 && (\text{mod } 319).
\end{aligned}$$

Aplicando a equivalência (6.10) temos

$$\begin{aligned} D(C(b_4)) &\equiv C(b_4) && (\text{mod } 319),\\ &\equiv 224^{187} && (\text{mod } 319),\\ &\equiv 224^{4^3+3^4+6^2+6} && (\text{mod } 319),\\ &\equiv 224^{4^3}.224^{3^4}.224^{6^2}.224^6 && (\text{mod } 319),\\ &\equiv 223.235.158.136 && (\text{mod } 319),\\ &\equiv 89.115 && (\text{mod } 319),\\ &\equiv 27 && (\text{mod } 319), \end{aligned}$$

de forma que $D(C(b_4)) \equiv b_4 \equiv 27 \pmod{319}$.

- $C(b_5)$

  Como $C(b_5) = 191$ obtém-se as congruências

$$\begin{aligned} &191^4 \equiv (224^2)^2 \equiv 93^2 \equiv 36 && (\text{mod } 319),\\ &191^{4^2} \equiv (191^4)^4 \equiv 146^4 \equiv (146^2)^2 \equiv 262^2 \equiv 59 && (\text{mod } 319),\\ &191^{4^3} \equiv (191^{4^2})^4 \equiv 59^4 \equiv (59^2)^2 \equiv 291^2 \equiv 146 && (\text{mod } 319),\\ &191^3 \equiv 273 && (\text{mod } 319),\\ &191^{3^2} \equiv (191^3)^3 \equiv 273^3 \equiv 273^2.273 \equiv 202.273 \equiv 278 && (\text{mod } 319),\\ &191^{3^3} \equiv (191^{3^2})^3 \equiv 278^3 \equiv 278^2.278 \equiv 86.278 \equiv 302 && (\text{mod } 319),\\ &191^{3^4} \equiv (191^{3^3})^3 \equiv 302^3 \equiv (-17)^3 \equiv -128 \equiv 191 && (\text{mod } 319),\\ &191^6 \equiv (191^3)^2 \equiv 273^2 \equiv 202 && (\text{mod } 319),\\ &191^{6^2} \equiv (191^6)^6 \equiv 206^6 \equiv (206^3)^2 \equiv 86^2 \equiv 59 && (\text{mod } 319). \end{aligned}$$

Aplicando a equivalência (6.10) temos

$$\begin{aligned} D(C(b_5)) &\equiv C(b_5) && (\text{mod } 319),\\ &\equiv 191^{187} && (\text{mod } 319),\\ &\equiv 191^{4^3+3^4+6^2+6} && (\text{mod } 319),\\ &\equiv 191^{4^3}.191^{3^4}.191^{6^2}.191^6 && (\text{mod } 319),\\ &\equiv 146.191.202.59 && (\text{mod } 319),\\ &\equiv 133.115 && (\text{mod } 319),\\ &\equiv 302 && (\text{mod } 319), \end{aligned}$$

de forma que $D(C(b_5)) \equiv b_5 \equiv 302 \pmod{319}$.

- $C(b_6)$

Como $C(b_6) = 64$ obtém-se as congruências

$$\begin{aligned}
64^4 &\equiv (64^2)^2 \equiv 268^2 \equiv 49 && (\text{mod } 319),\\
64^{4^2} &\equiv (64^4)^4 \equiv 49^4 \equiv (49^2)^2 \equiv 168^2 \equiv 152 && (\text{mod } 319),\\
64^{4^3} &\equiv (64^{4^2})^4 \equiv 152^4 \equiv (152^2)^2 \equiv 136^2 \equiv 313 && (\text{mod } 319),\\
64^3 &\equiv 245 && (\text{mod } 319),\\
64^{3^2} &\equiv (64^3)^3 \equiv 245^3 \equiv 245^2.245 \equiv 53.245 \equiv 225 && (\text{mod } 319),\\
64^{3^3} &\equiv (64^{3^2})^3 \equiv 225^3 \equiv 225^2.225 \equiv 223.225 \equiv 92 && (\text{mod } 319),\\
64^{3^4} &\equiv (64^{3^3})^3 \equiv 92^3 \equiv 9 && (\text{mod } 319),\\
64^6 &\equiv (64^3)^2 \equiv 245^2 \equiv 53 && (\text{mod } 319),\\
64^{6^2} &\equiv (64^6)^6 \equiv 53^6 \equiv (53^3)^2 \equiv 223^2 \equiv 284 && (\text{mod } 319).
\end{aligned}$$

Aplicando a equivalência (6.10) temos

$$\begin{aligned}
D(C(b_6)) &\equiv C(b_6) && (\text{mod } 319),\\
&\equiv 64^{187} && (\text{mod } 319),\\
&\equiv 64^{4^3+3^4+6^2+6} && (\text{mod } 319),\\
&\equiv 64^{4^3}.64^{3^4}.64^{6^2}.64^6 && (\text{mod } 319),\\
&\equiv 313.9.53.284 && (\text{mod } 319),\\
&\equiv 265.59 && (\text{mod } 319),\\
&\equiv 4 && (\text{mod } 319),
\end{aligned}$$

de forma que $D(C(b_6)) \equiv b_6 \equiv 4 \pmod{319}$.

Portanto, o destinatário Y encontra a sequência decifrada

$$122 - 42 - 316 - 27 - 302 - 4,$$

que é igual a sequência (6.31) e desse modo, resta apenas realizar a conversão dos códigos conforme mostrado na Tabela 5, comprovando assim que recebeu a mensagem na íntegra.

Em resumo, o RSA é um sistema criptográfico de chave pública, que permite a comunicação por meios inseguros de forma que, somente o receptor de uma dada mensagem, consiga decifrá-la por meio de uma chave. A partir de dois números primos distintos p e q, determinam-se:

- a chave de codificação (e,m), de acesso público, no qual e é um número invertível em $\mathbb{Z}_{\varphi(m)}$ e m é o produto de p e q;
- a chave oculta de decodificação (d,m), no qual d é o inverso multiplicativo de e em $\mathbb{Z}_{\varphi(m)}$.

Os números p,q e $\varphi(m)$ não são de conhecimento público e, após a criação das chaves, devem ser esquecidos por medida de segurança.

Realmente é fascinante a grandeza do resultado que apresenta diante da baixa complexidade téorica que o embasa. A utilização da aritmética modular não se trata apenas de um "facilitador das contas", mas sem a simplificação numérica que ela proporciona seria impossível determinar resíduos de potências com tantos dígitos, em qualquer sistema tecnológico existente. Na prática, sua aplicação está ligado ao uso de computadores, tanto para resolução dos algoritmos quanto para a escolha adequada dos primos p e q.

A eficiência e segurança do RSA alicersam-se na facilidade em determinar primos de ordens numéricas grandes - estima-se que os primos utilizados nas encriptações tem em torno de 100 algarismos, e em contra partida, na dificuldade em fatorar números de tais grandezas ou maiores. Existem teoremas que permitem não só o teste de primalidade quanto garantem a existência de infinitos números primos, porém não se conhece a existência de algorítmos que realizem, em tempo polinomial, a fatoração de um número (MARTINEZ *et al.*, 2013). Além do mais, não é suficiente que p e q escolhidos sejam somente "grandes", existe uma forma eficiente de fazê-los, de modo a assegurar a não fatoração rápida de m. Para maiores informações e detalhes sugere-se a referência (COUTINHO, 2014).

CAPÍTULO

7

ARITMÉTICA MODULAR APLICADA AO CALENDÁRIO

7.1 Contrução da ideia organizativa do tempo - os calendários

Desde a pré-história o homem adotou como prática de sustentação e sobrevivência o conhecimento da natureza, expressa em suas mais diversas manifestações naturais. A partir da observação constante do mundo ao seu redor foi possível perceber e entender alguns fenômenos e seus padrões, que passaram a guiar atividades importantes como migração e agricultura. É neste contexto que a ideia de conhecimento e organização do tempo inserem-se como fundamentais na existência humana.

As medidas de tempo utilizadas tinham por base a repetitividade dos fenômenos naturais e dentre esses fenômenos, destacamos a movimentação dos corpos celestes. Foi olhando para o céu que o homem criou divisões para os intervalos de tempo ligados as estações do ano, meses, dias e anos; buscando determinar padrões pertinentes e eficientes para direcionar condutas importantes de sua época. A identificação dos movimentos de rotação e revolução relacionados ao Sol e a Lua foram as bases para as configurações dessa organização temporal, na qual deu origem aos calendários. Vamos entender melhor a implicação desses movimentos na determinação dessas unidades de tempo.

Tomando um eixo simétrico e imaginário que passa pelos polos norte e sul geográficos da Terra, a rotação define-se como o movimento giratório da Terra em torno desse eixo. Tal movimento acontece no sentido ocidente-oriente e considerando o Sol como a estrela de referência, esse ciclo completa-se entre 23 horas 59 minutos 39 segundos e 24 horas e 30 segundos, a depender da variação da ascenção reta do Sol. Chama-se de dia solar a conclusão ou duração desse ciclo observado por um mesmo meridiano e que, convencionalmente, foi aproximado para

24 h.

A Terra descreve sua órbita elíptica quase circular, pois a elipcidade da órbita terrestre é muito pequena, girando em torno do Sol através do movimento conhecido como revolução. Sua duração é de aproximadamente 365 d 06 h 09 m 09 s, tal período é o que chamamos de ano sideral. Analisando a revolução da Terra em torno do Sol, considerando como referência a passagem do Sol médio pelo ponto vernal [1], temos que o tempo de duas passagens consecutivas é de aproximadamente 365 d 05 h 48 m 45 s, intervalo esse que denomina-se ano trópico. É o ano trópico que regula o retorno das estações e que baseiam-se os calendários solares. Ao longo desse movimento, a distância que nos separa do Sol sofre uma variação, o que implica também numa mudança em sua velocidade, fatos esses responsáveis pelas estações do ano. Para maiores detalhes, imagens e outras aferições acerca dos movimentos de rotação e revolução da Terra sugere-se (DARROZ, 2010).

Os movimentos de rotação e revolução também são realizados pela Lua - em torno da Terra neste caso, e ambos possuem o mesmo período. O movimento de revolução da Lua em torno da Terra permite-nos que a vejamos de formas diferentes ao longo desse persurso, onde essas mudanças visíveis em seu aspecto é o que chamamos de fase. O período que se interpõe de uma fase a outra, igual e consecutiva, é denominado de lunação. A lunação é um intervalo temporal compreendido entre duas conjunções consecutivas entre a Lua e o Sol, não apresenta um valor constante, variando entre 29 dias e 6 horas e 29 dias e 20 horas. Seu valor médio é de 29 dias, 12 horas e 44 minutos.

O movimento que a Lua realiza em torno da Terra é contínuo, o que na realidade imprime a cada instante de observação uma nova fase lunar. Com isso, a Lua possui infinitas fases, mas somente quatro delas possuem nomes proprios – Lua nova, Lua quarto crescente, Lua cheia e Lua quarto minguante. A passagem de tempo entre uma dessas fases para outra acontece em um período de aproximadamente sete dias, é possível verificar detalhadamente as fases da Lua e seu movimento orbital em torno da Terra em (FILHO; SARAIVA, 2018). Apesar de inutitivo, não se tem uma afirmação única para a origem da contagem da semana como o conjunto de sete dias. A movimentação da Lua é uma das hipóteses, existem várias outras menções a ideia do conjunto de sete dias que provém da observação de outros astros como também da cultura religiosa de povos variados.

Dessa forma, os movimentos astronômicos de rotação e revolução da Terra nos conferem as medidas de tempo do dia e do ano e a lunação, nos confere a medida de tempo do mês. Em resumo, um calendário é o instrumento que exprime de forma simplificada teorias astronômicas associadas a realizar a mensuração cronológica do tempo, a partir da percepção dos ciclos que lhe são conferidos. Como se pôde notar, as diversas ciclicidades apresentadas não são números exatos, que apresentam múltiplos e submúltiplos, o que gera dificuldades na criação de um

[1] O ponto de intersecção entre o equador celeste e a eclíptica por onde passa o Sol no seu movimento anual aparente ao transitar do hemisfério Sul para o hemisfério Norte.

calendário, pois em determinados intervalos de tempo essas diferenças precisam ser corrigidas.

Grande parte dos calendários primitivos eram baseados na Lua, para os povos de Atenas, Jerusalém ou Babilônia a passagem da Lua nova para a Lua crescente marcavam o início de um novo mês.

O primeiro calendário a basear-se no Sol foi o egípicio que utilizava um ano com 12 meses de 30 dias, acrescidos de 5 dias adicionais em correspondência aos aniversários dos deuses Osíris, Horus, Isis, Neftis e Set, totalizando 365 dias. Quando Roma conquistou o Egito, seus conhecimentos serviram como base para a elaboração de um novo calendário romano, insituído por Júlio César.

Assistido pelo astrônomo grego Sosísgenes, no ano de 45 a.C, César modifica o calendário romano tornando-o um calendário solar. As principais características apresentadas pelo chamado *calendário juliano* era a organização dos anos em 365 dias, o acréscimo do ano bissexto com 366 dias a cada ciclo de quatro anos e a fixação de 12 meses em um ano.

Anos depois de sua implementação, o calendário juliano passou por algumas reformas, dentre elas vale ressaltar a estipulação da configuração organizativa dos meses do ano como ainda se utiliza.

Mês	**Nome**	**Dias**
1	JANUARIUS	31
2	FEBRUARIUS	29/30
3	MARTIUS	31
4	APRILIS	30
5	MAIUS	31
6	JUNIUS	30
7	QUINTILIS	31
8	SEXTILIS	30
9	SEPTEMBER	31
10	OCTOBER	30
11	NOVEMBER	31
12	DECEMBER	30

Tabela 6 – Calendário juliano antes da reforma

Mês	**Nome**	**Dias**
1	JANEIRO	31
2	FEVEREIRO	28/29
3	MARÇO	31
4	ABRIL	30
5	MAIO	31
6	JUNHO	30
7	JULHO	31
8	AGOSTO	31
9	SETEMBRO	30
10	OUTUBRO	31
11	NOVEMBRO	30
12	DEZEMBRO	31

Tabela 7 – Calendário juliano após a reforma

Ainda que utilizasse medições mais apuradas, e que tenha sido aprimorado ao longo do tempo por sucessores romanos, o calendário juliano apresentava uma diferença de 1 dia a cada 128 anos e aproximadamente três dias em 400 anos.

7.2 O calendário gregoriano

Com o acúmulo de tal diferença do calendário juliano, após um período de quase quatro séculos, houve um deslocamento na data do equinócio [2] da primavera gerando conflitos religiosos em relação a comemoração da Páscoa. Após algumas tentativas sem sucesso de propor a realização de uma reforma no calendário juliano, foi somente em meados de 1576, pelo comando do papa Gregório XIII, que uma comissão foi formada por astrônomos e matemáticos célebres da época, a fim de estudar e construir um projeto de modificação do calendário juliano.

O *calendário gregoriano* – assim chamado em homenagem ao papa Gregório, foi oficializado em 24 de fevereiro de 1582 através da emissão da bula Inter Gravíssimas, que trazia especificamente os pontos primordiais do novo calendário. Dentre elas

- estipulava que o dia imediatamente posterior ao dia 04 de outubro de 1582, do calendário juliano, seria o dia 15 de outubro no novo calendário, fazendo assim a correção da diferença de 10 dias no equinócio da primavera.
- Determinou-se ainda que a cada intervalo de quatro anos – para os anos múltiplos de quatro e com exceção dos anos múltiplos de 100, teria-se um ano bissexto.
- Passou-se a considerar o início de um novo ano a partir do primeiro dia de janeiro.

A adoção pelo novo calendário não aconteceu de forma imediata em todos os lugares e sua aceitação em alguns países demoraram séculos. O principal motivo à resistência na adoção do novo calendário provinha de questões religiosas - a aceitação em países católicos foi quase imediata, enquanto em países prostestantes e ortodoxos sua adoção ocorreu de forma gradativa, influenciada por questões políticas e sociais de cada época, é possível verificar alguns exemplos na Tabela 8 para alguns exemplos. Conforme (JUNIOR, 2012) " A maior resistência à reforma gregoriana ocorreu em países ligados à Igreja Ortodoxa, como Sérvia, Iugoslávia, Bulgária, Romênia e Grécia, dentre outros, os quais somente durante ou após a Primeira Guerra Mundial resolveram adotar o novo calendário". Atualmente, mesmo povos e países que por motivos religiosos ou culturais fazem uso de outros calendários, utilizam-se do calendário gregoriano em suas relações internacionais - pode-se dizer que ele é considerado praticamente universal.

A duração do ano gregoriano é em média de 365 d 05 h 49 m 12 s, isto é, tem atualmente 27 s a mais do que o ano trópico. A acumulação desta diferença ao longo do tempo representará um dia a cada 3000 anos. É evidente que não valia a pena os astrônomos de

[2] Na astronomia, o equinócio é definido como o instante em que o Sol, em sua órbita aparente -como vista da Terra, cruza o equador celeste - a linha do equador terrestre projetada na esfera celeste. Esse evento ocorre duas vezes por ano, na primavera e outono. Durante dois dias do ano, as noites e os dias terão quase a mesma duração, 12 horas aproximadamente. O evento ocorre em consequência da inclinação no eixo da Terra que resulta na incidência da luz solar diretamente sobre a faixa intertropical durante alguns períodos do ano.

Ano	Localidade
1582	Portugal e Espanha
1583	Grande parte países da Europa Ocidental
1584	Brasil
1700	Alemanha e países protestantes
1752	Grã-Bretanha
1873	Japão
1912	China
1918	União Soviética
1924	Grécia e Igrejas Ortodoxas

Tabela 8 – Adoção do calendário greogoriano.

Gregório XIII atender a tão pequena e longínqua diferença, nem na atualidade ela tem ainda qualquer importância. Talvez lá para o ano 5000 da nossa era, se ainda continuarmos com o mesmo calendário, seja necessário ter isso em consideração. Para maiores detalhes acerca da história e evolução do calendário sugere-se a referência (MARQUES, s.d).

7.3 O Teorema de Zeller

Nosso intuito nessa seção é construir uma fórmula pela qual, a partir das variáveis numéricas como ano, mês e dia do mês, encontre-se o dia da semana dessa referida data. Faremos uma análise ponto a ponto dos passos utilizados na inserção de cada elemento da fórmula. Para isso, trataremos de aspectos conceituais que embasarão nosso argumento, criando subsídios práticos e teóricos para que se possa refletir e construir abordagens que permitam sua aplicação nos anos finais do Ensino Fundamental.

A ideia por trás da fórmula que desejamos é do matemático e reverendo Julius Christian Johannes Zeller $(1822 - 1899)$ que segundo (STOCKTON, 2010) publicou quatro documentos a cerca do calendário gregoriano e juliano, onde apresentou os cálculos do dia da semana a partir de uma data qualquer - já considerando as variáveis numéricas ano, mês e dia do mês. Tal fórmula ficou conhecida como *"Congruência de Zeller"*, para obter mais informações sobre sua estruturação original sugere-se (WIKIPÉDIA, 2020).

Foi do próprio Zeller as nomenclaturas que utilizaremos para o trato dos dias da semana e do mês. Para os dias da semana, enumeraremos a iniciar-se no domingo, de forma a representarmos como abaixo

domingo	*segunda-feira*	*terça-feira*	*quarta -feira*	*quinta-feira*	*sexta-feira*	*sábado*
1	2	3	4	5	6	7

Tabela 9 – Representação numérica dos dias da semana.

Pensando na variação de dias ocorridos nos anos bissextos, mais especificamente no

mês de fevereiro, Zeller propôs que os meses de janeiro e fevereiro sejam contados no final, iniciando a ordenação dos meses em março. Na prática, isso implica em uma reorganização da enumeração e ciclo dos meses do ano diferente da que utilizamos. Por exemplo, para o dia 31 de janeiro de 2020, na notação proposta, consideraríamos que estaria no ano de 2019. Dessa forma, adotaremos a organização

Meses	***Numeração*** (m)
Março	1
Abril	2
Maio	3
Junho	4
Julho	5
Agosto	6
Setembro	7
Outubro	8
Novembro	9
Dezembro	10
Janeiro	11
Fevereiro	12

Tabela 10 – Representação numérica dos meses do ano - Congruência de Zeller.

Denotaremos uma data como (d,m,A), no qual d é o dia do mês m no ano A. A fórmula que se pretende mostrar determinará, a partir dessas variáveis, o dia da semana que representaremos por $s(d,m,A)$. Por exemplo, $s(09,02,2020)$ é o dia da semana referente ao nono dia do mês de abril, do ano de 2020. Como tal data foi uma quinta-feira, temos que $s(09,02,2020) = 5$.

Para realizar a contagem do total de dias em um intervalo de anos, conforme são organizados no calendário atual, necessita-se levar em consideração o acréscimo de um dia a cada ano bissexto presente nesse intervalo. Com isso, um primeiro passo para estabelecer essa contagem é a quantificação de anos bissextos dentro do período analisado. Para cumprir tal propósito, apresentaremos uma sequência de definição e resultados.

Definição 10. Dados $a,b \in \mathbb{Z}$, com $b \neq 0$, denotamos por $\left\lfloor \frac{a}{b} \right\rfloor$ a parte inteira do número racional $\frac{a}{b}$.

Proposição 23. Dados $a,b \in \mathbb{Z}$ e $b \neq 0$, temos que $\left\lfloor \frac{a}{b} \right\rfloor = q$, tal que q é o quociente da divisão euclidiana de a por b.

Demonstração. Pelo Teorema 4 escrevemos

$$a = bq + r, \text{onde } 0 \leqslant r < b. \tag{7.1}$$

Fazendo a divisão de (7.1) por b, temos

$$\frac{a}{b} = q + \frac{r}{b}, \text{onde } 0 \leqslant \frac{r}{b} < 1.$$

Como pelo Teorema 4, $q \in \mathbb{Z}$ e é único, logo segue o resultado. □

Exemplo 70. Dados os números racionais abaixo temos que suas respectivas partes inteiras são:

(a) $\left\lfloor \frac{7}{5} \right\rfloor = 1$, pois $7 = 5.1 + 2$.

(b) $\left\lfloor \frac{29}{4} \right\rfloor = 7$, pois $29 = 4.7 + 1$.

(c) $\left\lfloor \frac{1783}{100} \right\rfloor = 17$, pois $1783 = 100.17 + 83$.

Em consequência da Proposição 23, podemos observar que se $a > b$, então bq é o maior múltiplo de b, menor ou igual a a. Em outras palavras, q não é somente a parte inteira de $\frac{a}{b}$, como também a quantidade de múltiplos de b entre 1 e a.

Corolário 6. Dados $a, b, c \in \mathbb{Z}$ e $0 < b < a < c$. O número de múltiplos de b em $[a, c]$ é dado por

(i) $\left\lfloor \frac{c}{b} \right\rfloor - \left\lfloor \frac{a}{b} \right\rfloor$, se a não é múltiplo de b

(ii) $\left\lfloor \frac{c}{b} \right\rfloor - \left\lfloor \frac{a-1}{b} \right\rfloor$, se a é múltiplo de b

Demonstração.

(i) Segue direto da Proposição 23.

(ii) Como $a < c$, então os múltiplos de b entre 1 e c, incluem também na contagem os múltiplos de b entre 1 e a. Dessa forma, para que a pertença a contagem total, subtraímos de $\left\lfloor \frac{c}{b} \right\rfloor$ o número de múltiplos de b anteriores a a, ou seja, $\left\lfloor \frac{a-1}{b} \right\rfloor$.

□

Exemplo 71. Vamos determinar a quantidade de múltiplos de 7 entre

(a) $[372, 1224]$

$$\left\lfloor \frac{1224}{7} \right\rfloor - \left\lfloor \frac{372}{7} \right\rfloor = 174 - 52 = 122.$$

(b) $[546, 2373]$

$$\left\lfloor \frac{2373}{7} \right\rfloor - \left\lfloor \frac{546-1}{7} \right\rfloor = 339 - 77 = 262.$$

Observe que no item b consideramos também o 546 na contagem dos múltiplos. Outro ponto a salientar é que só faz sentido considerar o item (ii) do Corolário 6 quando a em questão é múltiplo de b.

Para as deduções que se seguem adotaremos o ano base de 1600, que como visto na seção anterior, foi o primeiro ano bissexto após a implementação do calendário gregoriano. Observa-se o ano de 1600 é um ano conveniente para início das contagens já que ele é múltiplo de 4 e 400, desse modo consideraremos o intervalo aberto nesse ano.

Agora temos os precedentes necessários para identificar os anos bissextos em um dado intervalo.

Proposição 24. Seja $A > 1600$, então no intervalo $(1600, A]$ a quantidade de anos bissextos b é dado por

$$b = \left\lfloor \frac{A}{4} \right\rfloor - \left\lfloor \frac{A}{100} \right\rfloor + \left\lfloor \frac{A}{400} \right\rfloor - 388.$$

Demonstração. Temos que $b \in \mathbb{N}$, é tal que b é múltiplo de 4 e 400 e não múltiplo de 100. Dessa forma, aplicaremos o Corolário 6 nas etapas a seguir.

(i) Determinaremos todos os múltiplos de 4 em $(1600, A]$:

$$\left\lfloor \frac{A}{4} \right\rfloor - \left\lfloor \frac{1600}{4} \right\rfloor = \left\lfloor \frac{A}{4} \right\rfloor - 400. \tag{7.2}$$

(ii) Determinaremos todos os múltiplos de 100 e não múltiplos de 400 em $(1600, A]$:

$$\begin{aligned} & \left\lfloor \frac{A}{100} \right\rfloor - \left\lfloor \frac{1600}{100} \right\rfloor - \left\{ \left\lfloor \frac{A}{400} \right\rfloor - \left\lfloor \frac{1600}{400} \right\rfloor \right\} \\ = & \left\lfloor \frac{A}{100} \right\rfloor - 16 - \left\{ \left\lfloor \frac{A}{400} \right\rfloor - 4 \right\} \\ = & \left\lfloor \frac{A}{100} \right\rfloor - \left\lfloor \frac{A}{400} \right\rfloor - 12. \end{aligned} \tag{7.3}$$

(iii) Fazendo a subtração de (7.2) e (7.3), temos:

$$\begin{aligned} & \left\lfloor \frac{A}{4} \right\rfloor - 400 - \left\{ \left\lfloor \frac{A}{100} \right\rfloor - \left\lfloor \frac{A}{400} \right\rfloor - 12 \right\} \\ = \quad & \left\lfloor \frac{A}{4} \right\rfloor - \left\lfloor \frac{A}{100} \right\rfloor + \left\lfloor \frac{A}{400} \right\rfloor - 388, \end{aligned}$$

como pretendiamos demonstrar.

□

Denotaremos por s o primeiro dia do mês de março do ano base de nossa contagem, na construção que faremos temos o ano incial $A_i = 1600$. Partindo de s faremos uma sequência de observações de modo a analisar o comportamento do dia da semana, conforme avançamos os anos a partir de A_i.

Para encontrarmos $s(1,1,1601)$, como 1601 não é um ano bissexto, consideramos que passaram-se 365 dias a partir de s. Como a contagem dos dias é organizada em semanas com 7 dias, temos uma ciclicidade de período 7, ou seja, podemos fazer a análise desse total de dias como $365 \equiv 1 \pmod 7$. Assim,

$$s(1,1,1601) \equiv s(1,1,1600) + 365 \equiv s + 1 \pmod 7.$$

Seguindo essa mesma ideia, para avançarmos para $s(1,1,1602)$, também acrescentaremos 365 dias pois 1602 não é bissexto, então

$$s(1,1,1602) \equiv s(1,1,1600) + 1 + 365 \equiv s + 1 + 1 \pmod 7.$$

Como o ano de 1603 também não é bissexto, segue que

$$s(1,1,1603) \equiv s(1,1,1600) + 1 + 1 + 365 \equiv s + 1 + 1 + 1 \pmod 7.$$

Para avançarmos para o ano de 1604 temos a variante que ele é um ano bissexto, com isso, teremos um acréscimo de 366 dias. Como $366 \equiv 2 \pmod 7$, temos que

$$s(1,1,1604) \equiv s(1,1,1600) + 1 + 1 + 1 + 366 \equiv s + 1 + 1 + 1 + 2 \pmod 7.$$

Analisando o progresso de $s(1,1,1600)$ para $s(1,1,1604)$ verificamos que, a partir de s, acrescentou-se 1 no dia da semana para cada ano comum do intervalo $(1600, 1604]$ e acrescentou-se 1, para cada ano bissexto deste mesmo intervalo. Com isso, podemos escrever esse resultado de forma generalizada por meio da equivalência

$$s(1,1,A) \equiv s + (A - 1600) + b \pmod 7. \tag{7.4}$$

Usaremos a própria equivalência (7.4) para determinar o valor de s. Sabemos que $s(1,1,2020)$ foi um domingo, dessa forma

$$1 \equiv s + (A - 1600) + b \pmod 7. \tag{7.5}$$

Calculando b pela Proposição 24 temos

$$\begin{aligned} b &= \left\lfloor \frac{2020}{4} \right\rfloor - \left\lfloor \frac{2020}{100} \right\rfloor + \left\lfloor \frac{2020}{400} \right\rfloor - 388 \\ &= 505 - 20 + 5 - 388 \\ &= 102. \end{aligned}$$

Aplicando o resultado acima em (7.5) encontramos

$$s \equiv 1 - (2020 - 1600) - 102 \equiv 1 - 0 - 4 \equiv -3 \equiv 4 \pmod 7. \tag{7.6}$$

Assim, $s(1,1,1600)$ foi uma quarta-feira e aplicando na equação (7.4) escrevemos:

Proposição 25. Seja $A > 1600$ e $A, b \in \mathbb{N}$, tal que b é a quantidade de anos bissextos em $(1600, A]$, a relação que determina o dia da semana, do primeiro dia de março no ano A, é dada por

$$s(1,1,A) \equiv 4 + (A - 1600) + b \pmod 7.$$

Exemplo 72. Vamos determinar o dia da semana do primeiro dia de março, do ano de 2020.

Pela Proposição 25, temos que

$$s(1,1,2120) \equiv 4 + (2120 - 1600) + b \pmod 7. \tag{7.7}$$

Calculando b pela Proposição 24, encontramos

$$\begin{aligned} b &= \left\lfloor \frac{2120}{4} \right\rfloor - \left\lfloor \frac{2120}{100} \right\rfloor + \left\lfloor \frac{2120}{400} \right\rfloor - 388 \\ &= 530 - 21 + 5 - 388 \\ &= 126. \end{aligned}$$

Retornando para a equivalência (7.7), segue

$$s(1,1,2120) \equiv 4 + 520 + 126 \equiv 4 + 2 + 0 \equiv 6 \pmod 7.$$

Logo o primeiro dia do mês de março do ano de 2120 será uma sexta-feira.

Conforme observado, a passagem dos anos para a formulação do resultado expresso na Proposição 25 foi feita a partir de um dia e ano base, considerando os acréscimos pertinentes a cada período. Usaremos essa mesma ideia recursiva para inserir na nossa fórmula a variável

m, ou seja, analisaremos os acréscimos mês a mês, a partir da data base $s(1,1,A)$, a fim de buscarmos uma generalização que nos permita levar em consideração a mudança dos meses.

Partindo do primeiro dia do mês de março, temos que até o primeiro dia do mês de abril passaram-se 31 dias, então

$$s(1,2,A) = s(1,1,A) + 31. \tag{7.8}$$

Note que $s(1,2,A)$ é constituído da data base e um acréscimo que representa quantos dias "a frente" ele está. Nessa mesma perspectiva, vejamos abaixo a caracterização na variação de cada mês m do ano, a partir de março:

Meses	***Caracterização da variação mês a mês***	***Acréscimos***
Março	$s(1,1,A) = s(1,1,A) + 0$	0
Abril	$s(1,2,A) = s(1,1,A) + 31$	31
Maio	$s(1,3,A) = s(1,1,A) + 31 + 30$	61
Junho	$s(1,4,A) = s(1,1,A) + 61 + 31$	92
Julho	$s(1,5,A) = s(1,1,A) + 92 + 30$	122
Agosto	$s(1,6,A) = s(1,1,A) + 122 + 31$	153
Setembro	$s(1,7,A) = s(1,1,A) + 153 + 31$	184
Outubro	$s(1,8,A) = s(1,1,A) + 184 + 30$	214
Novembro	$s(1,9,A) = s(1,1,A) + 214 + 31$	245
Dezembro	$s(1,10,A) = s(1,1,A) + 245 + 30$	275
Janeiro	$s(1,11,A) = s(1,1,A) + 275 + 31$	306
Fevereiro	$s(1,12,A) = s(1,1,A) + 306 + 31$	337
Março	$s(1,1,A+1) = s(1,1,A) + 337 + 28$ ou $s(1,1,A+1) = s(1,1,A) + 337 + 29$	365 ou 366

Tabela 11 – Acréscimos dos dias para a variação dos meses a partir de $s(1,1,A)$.

Observamos que a variação entre os meses, ou seja, os acréscimos aplicados, será o mesmo nos meses de 1 a 12 independente do ano em questão. Com isso é possível caracterizar o dia da semana, do primeiro dia de cada mês, a partir das constantes respresentadas pelos acréscimos.

Exemplo 73. Por exemplo, sabemos que $s(1,1,2020)$ foi um domingo e então $s(1,8,2020)$ estará a 214 dias "a frente". Aqui recaímos na necessidade em considerar a construção cíclica da semana, analisando que $214 \equiv 4 \pmod 7$ obtemos que

$$s(1,8,2020) \equiv s(1,1,2020) + 4 \equiv 1 + 4 \equiv 5 \pmod 7,$$

ou seja, o primeiro dia do mês de outubro é uma quinta-feira.

Com isso, para atender a finalidade na qual nos propusemos, percebe-se a necessidade em considerar os acréscimos no módulo 7. A tabela abaixo organiza os acréscimos de dias aplicados em cada mês a partir de $s(1,1,A)$, sob a visão das duas perspectivas.

(m)	***Mês***	***Acréscimos***	***Módulo 7***
1	*Março*	0	0
2	*Abril*	31	3
3	*Maio*	61	5
4	*Junho*	92	1
5	*Julho*	122	3
6	*Agosto*	153	6
7	*Setembro*	184	2
8	*Outubro*	214	4
9	*Novembro*	245	0
10	*Dezembro*	275	2
11	*Janeiro*	306	5
12	*Fevereiro*	337	1

Tabela 12 – Acréscimos dos dias para a variação dos meses a partir de $s(1,1,A)$, módulo 7.

A sequência formada pela última coluna da Tabela 12 representa então a caracterização de cada um dos meses m no módulo 7, permitindo simplificar a determinação de respostas como a pedida no Exemplo 73.

Contudo, nosso intuito não é escrever uma equivalência para cada valor de m, situação que já se cumpriria a partir das Tabelas 11 e 12. Queremos determinar uma relação única e para isso, recaímos na necessidade de representar a caracterização dos meses de forma geral.

Verifiquemos que a variação do acréscimo de dias, de um mês para o outro, acontece de forma não regular

Mudança dos meses	***Acréscimos em dias***	***Módulo 7***
Março - Abril	31	3
Abril - Maio	30	2
Maio - Junho	31	3
Junho - Julho	30	2
Julho - Agosto	31	3
Agosto - Setembro	31	3
Setembro - Outrubro	30	2
Outubro - Novembro	31	3
Novembro - Dezembro	30	2
Dezembro - Janeiro	31	3
Janeiro - Fevereiro	31	3

Tabela 13 – Acréscimos mês a mês considerados módulo 7

Note que a variação mês a mês será de 3 ou 2 no módulo 7, a depender do mês, sendo que a cada cinco meses repete-se a variação de 3, que corresponde respectivamente aos meses de julho e agosto, dezembro e janeiro.

No intuito de compensar tal irregularidade e poder tratar da variação dos meses de forma

unificada, Zeller propôs uma função piso que permite gerar as constantes características de cada mês, demonstradas na Tabela 12. A função de Zeller é dada por

$$Z(m) \equiv \left\lfloor \frac{13m-1}{5} \right\rfloor - 2 \pmod 7, \tag{7.9}$$

no qual $\frac{13}{5} = 2,6$ é a variação entre os meses no período de cinco meses consecutivos e m é o mês segundo a numeração estipulada na Tabela 10.

Exemplo 74. Aplicando a função de Zeller conforme (7.9) para o mês de agosto, temos

$$Z(6) \equiv \left\lfloor \frac{13.6-1}{5} \right\rfloor - 2 \equiv 15-2 \equiv 1-2 \equiv 1+5 \equiv 6 \pmod 7,$$

que é equivalente ao resultado encontrado na Tabela (12) para o mês proposto.

Agora, unindo a função de Zeller as contruções anteriores, podemos concluir o propósito de escrever uma equivalência geral inserindo a variante m ao estudo que estamos realizando.

Proposição 26. Sejam $A > 1600$ e $b, m \in \mathbb{N}$, tais que b é a quantidade de anos bissextos em $(1600, A]$ e $m \in \{1,2,3,...,12\}$, a relação que determina o dia da semana, do primeiro dia de um mês m no ano A, é dada por

$$s(1,m,A) \equiv s(1,1,A) + \left\lfloor \frac{13m-1}{5} \right\rfloor - 2 \pmod 7.$$

Exemplo 75. Usaremos a Proposição 26 para determinar o dia da semana, do primeiro dia do mês de novembro do ano de 1832. Sabemos que

$$s(1,9,1832) \equiv s(1,1,1832) + \left\lfloor \frac{13.9-1}{5} \right\rfloor - 2 \pmod 7. \tag{7.10}$$

Calculando $s(1,1,1832)$ pela Proposição 25, temos

$$s(1,1,1832) \equiv 4 + (1832-1600) + b \pmod 7. \tag{7.11}$$

Determinando b pela Proposição 24, encontramos

$$\begin{aligned} b &= \left\lfloor \frac{1832}{4} \right\rfloor - \left\lfloor \frac{1832}{100} \right\rfloor + \left\lfloor \frac{1832}{400} \right\rfloor - 388 \\ &= 458 - 18 + 4 - 388 \\ &= 56. \end{aligned}$$

Aplicando o resultado encontrado para b na equivalência (7.11), segue

$$s(1,1,1832) \equiv 4 + (1832-1600) + 56 \equiv 4 + 232 + 56 \equiv 4 + 1 \equiv 5 \pmod 7. \tag{7.12}$$

Encontrando a caracterização do mês de novembro, pela função de Zeller, temos

$$Z(9) \equiv \left\lfloor \frac{13.9-1}{5} \right\rfloor - 2 \equiv \left\lfloor \frac{116}{5} \right\rfloor - 2 \equiv 23 - 2 \equiv 2 - 2 \equiv 0 \pmod 7. \tag{7.13}$$

Substituindo os resultados encontrados em (7.12) e (7.13) em (7.11) temos

$$s(1,9,1832) \equiv 5+0 \equiv 5 \pmod 7.$$

Logo, o dia da semana do primeiro dia de novembro do ano de 1832 foi uma quinta-feira.

Para finalizar nosso objetivo, passemos para inserção da variante restante para compor nossa relação: os dias do mês d. Neste intuito, verifiquemos a situação: qual é o dia da semana do quinto dia de um mês m?

Realizemos a análise dia a dia, partindo de $s(1,m,A)$ que, convenientemente, já sabemos como determinar:

Dia do mês (d)	***Dia da semana de*** (d)
1	$s(1,m,A) \pmod 7$
2	$s(2,m,A) \equiv s(1,m,A)+1 \pmod 7$
3	$s(3,m,A) \equiv s(1,m,A)+2 \pmod 7$
4	$s(4,m,A) \equiv s(1,m,A)+3 \pmod 7$
5	$s(5,m,A) \equiv s(1,m,A)+4 \pmod 7$

Tabela 14 – Determinação do dia da semana de d a partir de $s(1,m,A)$.

É claro notar que, para cada dia do mês que se passa, acrescenta-se 1 no dia da semana do dia anterior. Logo, para determinar um dia d acrescenta-se $(d-1)$ a $s(1,m,A)$, o que nos permite generalizar

$$s(d,m,A) \equiv s(1,m,A)+(d-1) \pmod 7. \tag{7.14}$$

Desse modo, tendo em mãos uma relação com todas as variantes estipuladas inicialmente, façamos as substituições e simplificações pertinentes. Substituindo a Proposição 26 na equação (7.14), segue

$$s(d,m,A) \equiv s(1,1,A)+\left\lfloor \frac{13m-1}{5} \right\rfloor -2+(d-1) \pmod 7. \tag{7.15}$$

Aplicando as Proposições 25 e 24 na equivalência 7.15, temos

$$s(d,m,A) \equiv 4+(A-1600)+\left\lfloor \frac{A}{4} \right\rfloor -\left\lfloor \frac{A}{100} \right\rfloor +\left\lfloor \frac{A}{400} \right\rfloor -388+\left\lfloor \frac{13m-1}{5} \right\rfloor -2+(d-1) \pmod 7. \tag{7.16}$$

Realizando as simplificações adequadas em (7.16), encontramos o *Teorema de Zeller*:

Teorema 14 (*Zeller*). Sejam $A > 1600$ e $b,m,d \in \mathbb{N}$, tal que b é a quantidade de anos bissextos em $(1600,A]$ e $m \in \{1,2,3,...,12\}$, a relação que determina o dia da semana do dia d de um mês m no ano A é dada por

$$s(d,m,A) \equiv 1+d+\left\lfloor \frac{13m-1}{5} \right\rfloor +A+\left\lfloor \frac{A}{4} \right\rfloor -\left\lfloor \frac{A}{100} \right\rfloor +\left\lfloor \frac{A}{400} \right\rfloor \pmod 7.$$

Exemplo 76. Qual foi o dia da semana de 29 de fevereiro de 1864?

Note que tratamos o mês de fevereiro como pertencente ao ano anterior, ou seja, o útimo mês do ano de 1863. Desse modo, aplicando o Teorema 14, temos:

$$\begin{aligned} s(29,12,1863) &\equiv 1+29+\left\lfloor\frac{13.12-1}{5}\right\rfloor+1863+\left\lfloor\frac{1863}{4}\right\rfloor-\left\lfloor\frac{1863}{100}\right\rfloor+\left\lfloor\frac{1863}{400}\right\rfloor \pmod 7 \\ &\equiv 30+31+1+3-4+4 \pmod 7 \\ &\equiv 65 \pmod 7 \\ &\equiv 2 \pmod 7. \end{aligned}$$

Assim, o dia da semana de 29 de fevereiro do ano de 1864 foi uma segunda-feira.

Apresentados o conceito e construções acerca do calendário gregoriano, a partir das observações de Zeller, seguiremos com alguns levantamentos que buscam nortear uma aplicação de tais ideias em uma sala regular de ensino. Deixaremos para a próxima seção discussões metodológicas e curriculares acerca do assunto, buscando aqui proporcionar reflexões teóricas e práticas para o professor e sua formação, de modo a subsidiar uma melhor aplicabilidade e entendimento sobre o tema. Levantaremos a seguir alguns pontos a serem reconstruídos, pensando na utilização de algumas informações de modo geral e levando em consideração a organização numérica dos meses conforme a conhecemos no calendário atual. Utilizaremos de conceitos, já demostrados neste trabalho, da aritmética modular como forma de modelagem das situações propostas.

Utilizamos nas construções o ano inicial $A_i = 1600$, ou seja, fizemos nosso cálculo sempre tendo base o intervalo $(1600, A]$. Todavia, pesando na prática dentro da sala de aula, tomarmos um ano tão remoto seria a melhor opção? Ou ainda, para um professor que deseje aplicar tais ideias, seria essa uma informação necessária e obrigatória para a realização de uma sequência didática?

Para responder a essas perguntas retomaremos alguns pontos desencadeadores do resultado dado pelo Teorema 14. A escolha feita de $A_i = 1600$ segue utilizada na referência (HEFEZ, 2014), já pensando na simplificação dos cálculos estabelecidos e exclusão da contagem desse ano como bissexto, pois dentro das relações encontradas o ano tem início no primeiro dia de março. Dessa forma, pensando numa generalização, tomando A_i, A quaisquer anos maiores que 1583, podemos ter as seguintes situações:

- A_i e A são ambos bissextos;
- A_i é bissexto e A não é bissexto;
- A_i não é bissextos e A é bissexto;
- A_i e A são ambos não bissextos.

Dentro dessas quatro possibilidades, verifica-se pelo Corolário 6 e pela utilização da ordenação dos meses a iniciar-se em março, que o cálculo dos anos bissextos dentro de um intervalo geral $(A_i, A]$ pode ser descrito como

Proposição 27. Sejam $A_i, A > 1583$ e $A_i, A, b \in \mathbb{N}$, tal que b é a quantidade de anos bissextos em $(A_i, A]$, então

$$b = \left\lfloor \frac{A}{4} \right\rfloor - \left\lfloor \frac{A}{100} \right\rfloor + \left\lfloor \frac{A}{400} \right\rfloor - \left\lfloor \frac{A_i}{4} \right\rfloor + \left\lfloor \frac{A_i}{100} \right\rfloor - \left\lfloor \frac{A_i}{400} \right\rfloor,$$

Demonstração. A demonstração segue diretamente do Corolário 6 e da Proposição 24. □

O passo consequente da construção do Teorema 14, e que fundamenta todos os demais passos, é a conclusão expressa na Proposição 25. Como todas as observações posteriores foram sequências recursivas a partir dela, é importante que a tratemos com atenção. Seguindo nessa perspectiva de tratarmos de forma geral os anos A_i e A, reeescrevemos a proposição

Proposição 28. Sejam $A_i, A > 1583$ e $b, s, A_i, A \in \mathbb{N}$, tais que b é a quantidade de anos bissextos em $(A_i, A]$, a relação que determina o dia da semana do primeiro dia de março no ano A é dada por

$$s(1,1,A) \equiv s + (A - A_i) + b \pmod 7,$$

no qual s é o dia da semana referente ao primeiro dia de março do mês A_i.

Observa-se nas Proposições 27 e 28, que a escolha de A_i pode ser feita de forma conveniente a situação que se deseja apresentar.

Para finalizarmos essa reflexão teórica acerca do resultado mostrado no Teorema 14, analisemos o que ele nos propõe: utilizar uma contagem para os meses do ano, através de uma organização sequencial que não é a que vivenciamos em nossa prática. E ainda, considerarmos os meses de janeiro e fevereiro como pertencentes ao ano anterior a A.

Vejamos como podemos adaptar nossos resultados de modo a proporcionar uma relação que se aplique as condições reais da organização do calendário atual. Denotando como m' a organização dos meses no calendário regular gregoriano e m, a organização proposta por Zeller, temos

	jan	***fev***	***mar***	***abr***	***mai***	***jun***	***jul***	***ago***	***set***	***out***	***nov***	***dez***
m	11	12	1	2	3	4	5	6	7	8	9	10
m'	1	2	3	4	5	6	7	8	9	10	11	12

Tabela 15 – Discriminação numérica de m e m'.

Comparando os valores estipulados entre as linhas, percebemos que recaímos sobre o problema da "Cifra de César", mostrado detalhadamente no Exemplo 57, do Capítulo 6. Neste

caso estamos tratando os meses em $\mathbb{Z}_{12}$ e desta forma, percebemos que a permutação entre m e $m^{'}$ pode ser escrita como

$$m \equiv \begin{cases} m^{'}-2 \pmod{12} & \text{para} \quad m^{'} \in \{1,2,...,10\}, \\ m^{'}-10 \pmod{12} & \text{para} \quad m^{'} \in \{11,12\}. \end{cases} \tag{7.17}$$

Um leitor mais cético pode estar se perguntando: mas a função de Zeller (7.9) constrói a sequência característica de cada mês m em $\mathbb{Z}_7$, isso não mudaria a relação entre m e $m^{'}$ expressa em (7.17)? Para responder a esse questionamento, vamos organizar os meses do ano, segundo m e $m^{'}$ módulo 7.

(mod 7)	1	2	3	4	5	6	7	1	2	3	4	5
m	mar	abr	mai	jun	jul	ago	set	out	nov	dez	jan	fev
$m^{'}$	jan	fev	mar	abr	mai	jun	jul	ago	set	out	nov	dez

Tabela 16 – Organização de m e $m^{'}$ módulo 7.

Comprova-se assim que a relação se mantém, ou seja, a variação de m para $m^{'}$ continua sendo da mesma quando analisadas no módulo 7. Dessa forma, aplicando (7.17) em (7.9), encontramos

(i) para $m \in \{1,2,...,10\}$

$$\begin{aligned} Z(m) &\equiv \left\lfloor \frac{13m-1}{5} \right\rfloor - 2 \pmod{7} \\ &\equiv \left\lfloor \frac{13(m^{'}-2)-1}{5} \right\rfloor - 2 \pmod{7} \\ &\equiv \left\lfloor \frac{13m^{'}-2}{5} \right\rfloor \pmod{7}. \end{aligned}$$

(ii) para $m \in \{11,12\}$

$$\begin{aligned} Z(m) &\equiv \left\lfloor \frac{13m-1}{5} \right\rfloor - 2 \pmod{7} \\ &\equiv \left\lfloor \frac{13(m^{'}+10)-1}{5} \right\rfloor - 2 \pmod{7} \\ &\equiv \left\lfloor \frac{13m^{'}+130-1}{5} \right\rfloor - 2 \pmod{7} \\ &\equiv \left\lfloor \frac{13m^{'}+4}{5} \right\rfloor + 25 - 2 \pmod{7} \\ &\equiv \left\lfloor \frac{13m^{'}+4}{5} \right\rfloor + 2 \pmod{7}. \end{aligned}$$

Assim, escrevemos $Z(m)$ em função de $m^{'}$ como

$$Z(m^{'}) \equiv \begin{cases} \left\lfloor \dfrac{13m^{'}-2}{5} \right\rfloor & (\text{mod } 7) \quad \text{para} \quad m^{'} \in \{1,2,...,10\} \\ \left\lfloor \dfrac{13m^{'}+4}{5} \right\rfloor + 2 & (\text{mod } 7) \quad \text{para} \quad m^{'} \in \{11,12\}. \end{cases} \tag{7.18}$$

A função (7.18) permite determinar a variação característica de cada mês considerando a organização convencional do calendário. Contudo, retomando as construções feitas até a determinação do Teorema 14 e as Tabelas 15 e 16, verificamos que os ajustes feitos na determinação da função (7.18) sempre inicia-se no mês de março. A implicação disso é que os meses de janeiro e fevereiro, pensando na sequência cíclica que estão inseridas, continuam a pertencer ao ano anterior. Para que esta diferença de uma unidade no ano não apareça nas aplicações e relações que consideram a organização usual do calendário, faremos seu "ajuste" na função (7.18), de tal modo que obteremos

$$Z(m^{'}) \equiv \begin{cases} \left\lfloor \dfrac{13m^{'}-2}{5} \right\rfloor & (\text{mod } 7) \quad \text{para} \quad m^{'} \in \{1,2,...,10\} \\ \left\lfloor \dfrac{13m^{'}+4}{5} \right\rfloor + 1 & (\text{mod } 7) \quad \text{para} \quad m^{'} \in \{11,12\}. \end{cases} \tag{7.19}$$

Reescrevendo a Proposição 26 em função de (7.19), temos:

Proposição 29. Sejam $A_i, A > 1583$ e $b, m^{'}, A_i, A \in \mathbb{N}$, tais que b é a quantidade de anos bissextos em $(A_i, A]$ e $m^{'} \in \{1,2,3,...,12\}$, a relação que determina o dia da semana do primeiro dia de um mês $m^{'}$ no ano A é dada por

$$s(1,m^{'},A) \equiv s(1,1,A) + Z(m^{'}) \pmod 7. \tag{7.20}$$

Exemplo 77. Qual será o dia da semana do primeiro dia de fevereiro do ano de 2123?

Aplicando a Proposição 29 na situação, procuramos

$$s(1,2^{'},2123) \equiv s(1,1,2123) + Z(m^{'}) \pmod 7. \tag{7.21}$$

Por simplicidade, denotamos $A_i = 2020$ e, consequentemente, $s = 1$. Substituindo a Proposição 28 e a função (7.19) em (7.21), obtemos

$$s(1,2^{'},2123) \equiv 1 + (2023 - 2020) + b + \left\lfloor \frac{13m^{'}+4}{5} \right\rfloor + 1 \pmod 7. \tag{7.22}$$

Determinando b pela Proposição 27, encontramos

$$b = \left\lfloor \frac{2123}{4} \right\rfloor - \left\lfloor \frac{2123}{100} \right\rfloor + \left\lfloor \frac{2123}{400} \right\rfloor - \left\lfloor \frac{2020}{4} \right\rfloor + \left\lfloor \frac{2020}{100} \right\rfloor - \left\lfloor \frac{2020}{400} \right\rfloor \tag{7.23}$$

$$= 530 - 21 - 5 - 505 + 20 - 5 \tag{7.24}$$

$$= 24, \tag{7.25}$$

e substituindo os resultados em (7.21), segue

$$s(1,2^{'},2123) \equiv 1 + 2123 - 2020 + 24 + \left\lfloor \frac{13.2+4}{5} \right\rfloor + 1 \equiv 1 + 5 + 3 + 6 + 1 \equiv 2 \pmod 7.$$

Dessa forma, o dia da semana do primeiro dia de fevereiro do ano de 2123 será uma segunda-feira.

Dentro dessa perspectiva que estamos desenvolvendo, para a inserção da variante d dia, nota-se que a ideia é a mesma apresentada na Tabela 14, e desse modo, podemos reescrever a equivalência (7.14) em função de $m^{'}$ como

$$s(d,m^{'},A) \equiv s(1,m^{'},A) + (d-1) \pmod 7. \tag{7.26}$$

Com isso, é possível cumprir aos propósitos estabelecidos, de forma a escrever uma relação entre ano, mês e dia do mês que determine o respectivo dia da semana para esta data, utilizando a denotação numérica usual do calendário, a partir de qualquer data de base A_i. Aplicando na equivalência (7.26) os resultados de Proposição 29, temos

$$s(d,m^{'},A) \equiv s(1,1,A) + Z(m^{'}) + (d-1) \pmod 7. \tag{7.27}$$

Substituindo os resultados da Proposição 28 encontramos

$$s(d,m^{'},A) \equiv s + (A - A_i) + b + Z(m^{'}) + (d-1) \pmod 7. \tag{7.28}$$

Teorema 15 (*Zeller II*). Sejam $A_i, A > 1583$ e $b, m^{'}, d, A, A_i \in \mathbb{N}$,tais que b é a quantidade de anos bissextos em $(A_i, A]$ e $m^{'} \in \{1,2,3,...,12\}$, a relação que determina o dia da semana do dia d de um mês $m^{'}$ no ano A é dada por

$$s(d,m^{'},A) \equiv s + (d-1) + (A - A_i) + Z(m^{'}) + b \pmod 7.$$

Exemplo 78. A cidade de São Paulo comemora seu aniversário no dia 25 de janeiro e ela completou 300 anos em 1854. Qual foi o dia da semana dessa comemoração?

Aplicando o Teorema 15 a situação proposta, temos

$$s(25,1,1854) \equiv s + (25-1) + (1854 - A_i) + Z(m^{'}) + b \pmod 7. \tag{7.29}$$

Denotando $A_i = 1600$, temos pelo resultado de (7.6) que $s = 4$ e aplicando a função (7.19) em (7.29) temos

$$s(25,1,1854) \equiv 4 + (25-1) + (1854-1600) + \left\lfloor \frac{13.1+4}{5} \right\rfloor + 1 + b \pmod 7. \tag{7.30}$$

Calculando b pela Proposição 27 temos

$$\begin{aligned} b &= \left\lfloor \frac{1854}{4} \right\rfloor - \left\lfloor \frac{1854}{100} \right\rfloor + \left\lfloor \frac{1854}{400} \right\rfloor - \left\lfloor \frac{1600}{4} \right\rfloor + \left\lfloor \frac{1600}{100} \right\rfloor - \left\lfloor \frac{1600}{400} \right\rfloor \\ &= 463 - 18 + 4 - 400 + 16 - 4 \\ &= 61. \end{aligned}$$

Aplicando o valor de b determinado acima na equivalência (7.30), obtemos

$$\begin{aligned} s(25,1,1854) &\equiv 4 + (25-1) + (1854-1600) + \left\lfloor \frac{13.1+4}{5} \right\rfloor + 1 + 61 \pmod 7 \\ &\equiv 4 + 24 + 254 + 4 + 61 \pmod 7 \\ &\equiv 4 \pmod 7. \end{aligned}$$

Assim, o aniversário de 300 anos da cidade de São Paulo foi uma quarta-feira.

Exemplo 79. Este exercício foi retirado de (HEFEZ, 2014). Descubra em qual dia do mês de maio cairá o Dia das Mães de 2085.

O primeiro ponto a observar é que os dias do mês pertencentes ao mesmo dia da semana deixam sempre o mesmo resto na divisão por 7. Outro ponto importante é que fazemos o tratamento das informações encontradas sempre utilizando o primeiro elemento da classe residual respectiva de $\mathbb{Z}_7$. Logo, se determinarmos qual é o dia d referente ao primeiro domingo do mês de maio, saberemos que o dia das mães é o elemento seguinte na classe residual na qual pertencem.

Tomaremos $A_i = 2020$ e, portanto, temos que $s = 1$. Pelo Teorema 15 escrevemos nosso problema como

$$1 \equiv 1 + (d-1) + (2085-2020) + \left\lfloor \frac{13.5-2}{5} \right\rfloor + b \pmod 7. \tag{7.31}$$

Encontrando b pela Proposição 27, temos

$$\begin{aligned} b &= \left\lfloor \frac{2085}{4} \right\rfloor - \left\lfloor \frac{2085}{100} \right\rfloor + \left\lfloor \frac{2085}{400} \right\rfloor - \left\lfloor \frac{2020}{4} \right\rfloor + \left\lfloor \frac{2020}{100} \right\rfloor - \left\lfloor \frac{2020}{400} \right\rfloor \\ &= 521 - 20 + 5 - 505 + 20 - 5 \\ &= 16. \end{aligned}$$

Aplicando o resultado em (7.31) segue

$$d \equiv 1 - (2085 - 2020) - \left\lfloor \frac{13.5 - 2}{5} \right\rfloor - 16 \equiv 1 - 65 - 12 - 16 \equiv -1 \equiv 6 \pmod 7.$$

Então, os dias do mês d referentes aos domingos de maio de 2085 deixam resto 6 na divisão por 7. Assim, o segundo domingo do mês de maio é $6 + 7 = 13$ e portanto, o Dia das Mães de 2085 será no dia 13 de maio.

CAPÍTULO

8

APLICAÇÕES PARA OS ANOS FINAIS DO ENSINO FUNDAMENTAL DE TÓPICOS DA ARITMÉTICA MODULAR - DESVENDANDO PADRÕES NO CALENDÁRIO.

8.1 Por que a Aritmética Modular?

Ao se propor a uma breve reflexão sobre a metodologia e forma de apresentação de elementos da Teoria dos Números presentes na área da Aritmética no currículo do Ensino Fundamental, percebe-se que seus diversos tópicos são inseridos e tratados de forma desassociativa, tanto em relação a suas proprias propriedades quanto à associação com outros eixos matemáticos. Tal ponto é também elencado pelos Parâmetros Curriculares Nacionais (BRASIL, 1998):

> "Embora o estudo dos números e das operações seja um tema importante no currículo do ensino fundamental, constata-se, com frequência, que muitos alunos chegam ao final dessa fase de formação, com um conhecimento insuficiente sobre como eles são utilizados e sem ter desenvolvido uma ampla compreensão dos diferentes significados das operações."(BRASIL, 1998, p.95)

Na Base Nacional do Currículo Comum (BNCC), a construção da ideia de números, suas propriedades e operações são abordadas no eixo de Números desde o primeiro ano do Ensino Fundamental, perpassando de forma evolutiva para todos os demais anos dessa modalidade de ensino. A BNCC contempla uma visão de progressão vertical em torno dos objetos de conhecimento e habilidades apresentadas ao longo dos eixos, de forma que as construções e procedimentos acerca dos conceitos sejam conectadas e amplificadas ao longo de todo o

processo. Dessa forma, para o eixo de números, descreve que ao concluir os anos finais do ensino fundamental

> "a expectativa é a de que os alunos resolvam problemas com números naturais, inteiros e racionais, envolvendo as operações fundamentais, com seus diferentes significados, e utilizando estratégias diversas, com compreensão dos processos neles envolvidos." (BRASIL, 2017, p.269)

Contudo, o que se percebe no contexto escolar na abordagem em torno dos assuntos organizados no eixo de Números, é uma prática voltada principalmente para a resolução de algorítmos, com pouca ênfase para um olhar qualitativo, investigativo e associativo em torno das propriedades que os envolvem. Logo no início da segunda etapa do Ensino Fundamental – mais especificamente no 6º ano, propõe-se o trabalho com assuntos importantes da Aritmética como múltiplos, divisores, divisão euclidiana e critérios de divisibilidade. O tratamento que vem se aplicando a tais temas estão voltados a apresentação de um conjunto de regras e cálculos desconectados de situações práticas, não proporcionando ao aluno percepções de implicações gerais que seus conceitos e ideias podem fornecer.

Algumas relações significativas no conjunto dos números inteiros, em torno das operações e validação de propriedades numéricas, são praticamente inexploradas no contexto regular da sala de aula. Na operação da divisão euclidiana, por exemplo, não se explora sobre condições de existência e unicidade do quociente e do resto em caráter associativo a outras ideias aritméticas, como o papel do quociente numa sequência de múltiplos e divisores de um número inteiro ou o comportamento cíclico do resto. Outro exemplo é a abordagem do sistema de numeração na base decimal, que se atém ao reconhecimento de ordens e classes numéricas e o valor posicional de um algarismo, sem qualquer exploração de seu uso para utilização e entendimento de relações de igualdade, equivalência e propriedades relacionadas as operações básicas.

Aprofundando neste olhar sobre os aspectos aritméticos, pode-se refletir como o tratamento de alguns desses asssuntos em sala de aula, a partir de uma metodologia com natureza investigativa e analítica, pode contribuir e propocionar a elaboração de hipóteses, comparações e formulações mais abrangentes na utilização dos números e suas construções. Tais implicações vem ao encontro com uma preocupação concreta no ensino da matemática, no que diz respeito ao tratamento fragmentado e independente que se dá aos tópicos e eixos presentes em seu currículo. Essa abordagem vem causando uma série de paradigmas e insucessos relacionados ao interesse e aprendizagem da matemática.

Por outro lado, a abstração do raciocínio hipotético, a transposição para a linguagem simbólica propria da matemática, as transformações de padrões percebidos em generalizações, a comparação entre grandezas, são bases para o tratamento e aprendizado algébrico. Assim, para que se possa sair de casos particulares e conseguir observar e estabelecer relações de igualdades ou equivalências, de modo a manipular operações e propriedades numéricas a fim de formular

uma ideia geral e pertinente, é preciso que se conheça, domine, entenda e aplique com segurança conceitos já estabelecidos, ou seja, necessita-se que a relação entre a base aritmética flua de forma associativa e contínua para a construção da base algébrica.

Segundo (BRASIL, 2017), o eixo Álgebra presente no currículo de matemática, tem como finalidade a construção do pensamento algébrico e ressalta o caráter contribuitivo e relacional do eixo de Números nessa construção. Como afirma (LINS; GIMENEZ, 1997, p. 159) "devemos buscar é a coexistência da educação algébrica com a aritmética, de modo que uma esteja implicada na outra".

Nessa perspectiva, entende-se que a abordagem aplicacada a alguns tópicos da Teoria dos Números, presentes no currículo de Matemática, pode ser encarado como uma ferramenta a contribuir no processo de transição sem rupturas, entre a Aritmética e a Álgebra. Com isso, também interfere-se diretamente em questões como o resultado no processo de ensino aprendizado, pois segundo (GIL, 2008.118 f) a relação entre a Aritmética e a Álgebra pode também justificar as dificuldades apresentadas pelos alunos no aprendizado da matemática. Ela acrescenta ainda que, em observação e reflexão sobre a introdução e tratamento aplicado ao ensino da Álgebra, percebe-se que alguns dos procedimentos algébricos escolhidos são contraditórios ou diferentes aos aritméticos dos quais os alunos estavam acostumados, esse quadro acentua-se no fato dos alunos muitas vezes carregarem para as situações de aprendizado atual, dificuldades herdadas em contextos aritméticos anteriores.

Dessa maneira, percebemos que ao propormos um olhar diferenciado e reflexivo sobre determinados conteúdos e processos aritméticos, através da abordagem de tópicos da Teoria dos Números, estamos atendendo a uma demanda significativa do ensino da matemática, promovendo tanto uma melhor percepção e domínio das bases aritméticas, quanto a construção de uma linha direta e associativa ao uso algébrico, consequentemente, ampliando os subsídios para o alcance das competências elencadas no currículo de Matemática para o Ensino Fundamental nos anos finais, especificados na BNCC.

8.2 Relações matemáticas presentes no calendário - uma proposta de sequência didática

Nosso intuito é abordar características da Aritmética Modular através de uma série de intervenções, a partir de situações problemas em torno do calendário atual, que possibilitem um olhar diferenciado para a divisão euclidiana, ao tratamento e aplicação dos seus elementos como o quociente e em especial o resto.

Em relação ao quociente, desejamos relacioná-lo a uma sequência de múltiplos de um número natural num dado intervalo, ampliando assim sua compreensão para além da ideia que ganha nos modelos partitivos e quotativos – modelos enfaticamente e restritivamente utilizados

no tratamento da operação de divisão no Ensino Fundamental em grande parte dos materiais didáticos utilizados.

No que se trata do resto, espera-se explorar seu aspecto cíclico, a partir da percepção da sequência dos valores que pode assumir, projetando esse comportamento para situações diversas e gerais. Concomitantemente, pretende-se inferir alguns aspectos da Aritmética dos restos relacionando-a a ideia de equivalência e igualdade de algumas propriedades das operações com números naturais.

Ao longo do processo espera-se introduzir gradativamente a linguagem algébrica na representação das generalizações e na relação entre grandezas, formuladas com base na observação de comportamentos recursivos das sequências construídas.

Como finalização desse processo, espera-se ter como resultado final um conjunto de resultados que permitam definir uma relação, a partir das grandezas dias, meses e ano, que possibilite a determinação do dia da semana de uma data escolhida. Para tanto, teremos como referência os resultados demonstrados no Capítulo 7.

Para esta proposta, adotaremos uma definição para sequência didática apresentada por (ZABALA, 1998, p. 18), como sendo "um conjunto de atividades ordenadas, estruturadas e articuladas para a realização de certos objetivos educacionais, que têm um princípio e um fim conhecidos tanto pelos professores como pelos alunos."

Nas articulações estruturais e concretização da sequência didática, é importante a criação de um ambiente investigativo, reflexivo e analítico em torno dos conceitos e ideias matemáticas que iremos abordar, de modo que "[...] os alunos partilhem ideias, raciocínios, processos, estabeleçam conexões, comparações e analogias, construam conjecturas e negociem significados e desenvolvam capacidades de comunicar e argumentar." (KFOURI; D'AMBRÓSIO, 2006, p. 2).

Para isso destaca-se o papel do professor como fundamental, pois é através de sua mediação que será possível o desenvolvimento de um diálogo que cause intrigação e desejo de participação nos alunos e que ao mesmo tempo, conduza pelos cenários descritos, a fim que se alcance os resultados esperados.

Procurou-se que a sequência elaborada, contemplasse aspectos e objetos de conhecimento presentes ao longo dos eixos de Números e Álgebra, no currículo de matemática do Ensino Fundamental nos anos finais, apresentado na BNCC. Contudo, acredita-se que para a melhor compreensão e assimilação dos processos que serão utilizados, conclui-se que ela pode ser aplicada nos 8º e 9º anos do Ensino Fundamental.

Dividiremos as ações da aplicação da sequência didática em oito etapas, cada uma delas ocorrerá com base em "situações desafiadoras" que serão os instrumentos utilizados para subsidiar as discussões e conclusões em torno dos objetivos almejados para cada etapa. As sete primeiras situações desafiadoras tem o intuito de proporcionarem as ferramentas procedimentais para o alcance da proposta final, e a última tem caráter avaliativo. Aqui entendemos a avaliação

como uma ferramenta que permita o aluno e professor averiguarem e refletirem sobre o uso das construções matemáticas realizadas, levantar possíveis dificuldades e traçar intervenções pontuais. Denominaremos como SD_n as situações desafiadoras, tal que n representa sua ordem no contexto geral, e O_n os objetivos pretendidos com a SD_n respectiva.

Como introdução ao assunto, propõe-se a apresentação da abordagem histórica da elaboração do calendário, até a chegada da presente versão. Os tópicos primordiais estão sintetizados na primeira seção do Capítulo 7. A contextualização histórica de um objeto de estudo traz para dentro do campo de análise uma visão que extrapola os limites de uma área de conhecimento específico, inserindo uma percepção globalizada das implicações que tal objeto infere na sociedade. Neste sentido, de acordo com (FESTAS, 2015)

> "Considera-se que o pensamento e o conhecimento decorrem das relações entre pessoas envolvidas numa atividade que está sempre inserida num contexto social, cultural e histórico. Desse modo, a aprendizagem é situada em uma prática do mundo em que vivemos e resulta da atividade e da participação do indivíduo nessa prática." (FESTAS, 2015, p. 717)

Ao que se trata dos aspectos referentes aos fenômenos astronômicos relacionados à constituíção do calendário, pode-se considerar a realização de um trabalho interdisciplinar, apoiado por professores de outras áreas do conhecimento. Por exemplo, em observação a BNCC, dentro do componente de Ciências da Natureza, um dos eixos norteadores para o desenvolvimento das competências estipuladas para essa área é o de Terra e Universo. Neste eixo, para os anos do ensino fundamental que se sugeriu esta aplicação, é possível encontrar conteúdos que se destinam a desenvolver habilidades correlatas ao assunto, como:

> " Justificar, por meio da construção de modelos e da observação da Lua no céu, a ocorrência das fases da Lua e dos eclipses, com base nas posições relativas entre Sol, Terra e Lua.
>
> Relacionar diferentes leituras do céu e explicações sobre a origem da Terra, do Sol ou do Sistema Solar às necessidades de distintas culturas (agricultura, caça, mito, orientação espacial e temporal etc.)" (BRASIL, 2017, p. 351)

A associação entre as áreas de conhecimento na abordagem sobre o contexto histórico do calendário atende também o perfil de trabalho integrador sugerido na BNCC, ao organizar as competências específicas das diversas áreas do conhecimento de forma a possibilitar uma articulação horizontal entre elas. Contudo, a sugestão do trabalho compartilhado e em parceria com as demais áreas do conhecimento não será expresso por nós de forma detalhada na sequência didática que estamos apresentando.

SD_1: "Quem inventou o calendário?"

O_1: Associar o conhecimento e entendimento de fenômenos naturais a atividades básicas da sociedade. Reconhecer nos fenômenos atronômicos padrões percepítiveis e mensuráveis. Relacionar a importância da projeção dos padrões de tempo no contexto social.

Para o desenvolvimento das discussões a partir de SD_1 , é interessante dividir a turma em grupos, onde cada um desses grupos receba uma das fichas abaixo:

De onde surgiu a necessidade de organizar o tempo?	**Na sua opinião, o que contribuiu para as primeiras civilizações elaborarem suas rotinas de vida e sobrevivência?**
Existem outras maneiras de se organizar um calendário, diferente da que conhecemos?	**O que são anos bissextos?**
Num contexto imaginário, o grupo conheceu um jovem de uma aldeia de nativos de outro continente. Lá, eles organizam o tempo completamente diferente nós. Curioso, ele quer saber sobre como fazemos isso aqui. Descreva para ele nossso calendário, com as características que julga importante para o entendimento dele.	

Tabela 17 – Fichas para realização de SD_1.

Cada grupo tem um tempo para discutir sobre o conteúdo da ficha que recebeu e depois disso, o professor proporciona o espaço para que os alunos contem sobre as discussões feitas, na ordem pertinente. Assim, o professor parte da contribuição dos alunos e acrescenta os pontos relevantes e importantes para a construção coerente do contexto. Um ponto importante dessa etapa é a introdução da ideia de ciclicidade, utilizando dos proprios padrões percebidos nos fenômenos astronômicos levantados e das grandezas consequentes deles. É interessante descrever seus ciclos e chamar a atenção para as formas de repetição destes ciclos.

Ao final dessa atividade, as estruturas do calendário atual já terão sido elencadas e definidas como base, como a enumeração dos meses e seus respectivos dias, as condições para determinação de um ano bissexto, a disposição dos dias da semana. Concomitante a isso, define-se a nomenclatura que será aplicada para tais grandezas, como por exemplo: A (ano), m (meses), d (dia do mês), D (dias da semana). Para os dias da semana é interessante neste momento estipular uma sequência numérica que os represente, como mostrado na Tabela 9, e também sua representação com relação as demais grandezas, como $D(d,m,A)$ sendo o dia da semana de uma referida data. Para todas essas representações, sugere-se que fiquem expostas na sala de forma permanente, como suporte visual para as demais etapas.

Os momentos de situações desafiadoras que se seguirão abordarão os conceitos matemáticas pertinentes à contrução final pretendida. Na próxima *SD*, utilizaremos do contexto que estará

sendo debatido, para indicar o objetivo final que se deseja alcançar e fomentar a curiosidade dos alunos em relação a ele.

SD_2: No dia 8 de março de 2020 foi inaugurada na escola municipal Prof. Paulo Freire a biblioteca "Maria Firmina dos Reis", nome que faz referência e homenagem a primeira romancista negra brasileira. Sabendo que o dia da inauguração foi um domingo e que o funcionamento da biblioteca acontece em escalas a cada três dias, não importanto o dia da semana, responda:

(a) Em que dia da semana foi o 100º dia de funcionamento da biblioteca?

(b) Para que a biblioteca complete 20 domingos abertos, quantos dias de funcionamento precisarão?

(c) Qual será o dia da semana do aniversário de 5 anos de inauguração da biblioteca?

O_2: Ampliar a aplicabilidade do Teorema da Divisão Euclidiana, através da enfatização do resto, como estratégia em resoluções de problemas que envolvem fenômenos periódicos. Reconhecer padrões e formular generalizações, inclusive com uso da simbologia matemática propria, a partir do conjunto dos possíveis restos na divisão euclidiana entre dois números naturais. Aferir o conhecimento prévio dos alunos acerca das grandezas presentes no calendário e sua organização, assim como a compreensão e utilização de operações e propriedades referentes ao números naturais na resolução de uma situação problema.

Durante o processo de elaboração da solução por parte do aluno, o professor pode exercer a mediação e intervenção a partir de questionamentos como: "O que você está contabilizando nesta operação?", "Percebe alguma regularidade entre os números que aparecem num mesmo dia da semana?","Como você está organizando a contagem do tempo: em blocos de anos, meses ou dias?"

Após o tempo estipulado para cada atividade, é importante que os alunos tenham um espaço para apresentarem suas estratégias, de modo a discutir também quais foram as dificuldades encontradas por eles. Neste momento, conduzidos pelo professor, é possível que com base nas diversas formas de resolução do desafio, os alunos comparem seus métodos e concluam sobre erros, ou percepções mais gerais sobre a situação. Dessa forma, sugere-se que essa prática se repita ao longo das propostas para as próximas situações desafiadoras.

Em SD_2, a ideia é utilizar as discussões acerca do item "a" para abordar sobre o *Teorema da Divisão Euclidiana* e as características do conjunto do resto. Para isso, a situação discutida dará desencadeamento a outras observações, mais gerais, que servirão de base para o professor formalizar alguns conceitos importantes. É oportuna a organização dos dias de funcionamento da biblioteca, conforme a tabela abaixo

domingo	**segunda**	**terça**	**quarta**	**quinta**	**sexta**	**sábado**
1º	6º	4º	2º	7º	5º	3º
8º	13º	18º	16º	14º	19º	17º
15º	20º					

Tabela 18 – Funcionamento da biblioteca até o 20º dia.

A partir dela, é possível explorar relações e características pertinentes ao conceito que se espera, podendo ter como subsídio para isso questionamentos como:

- É possível que 38º dia de funcionamento da biblioteca seja numa segunda-feira? Use a tabela para justificar sua resposta.
- Existe uma "regra" para um número aparecer em uma determinada coluna desta tabela?

Dessa forma, após as conclusões acima, pode-se expressar a resolução do problema a partir do *Teorema da Divisão Euclidiana* de 100 por 7

$$100 = 7.14 + 2,$$

ou seja, o dia da semana que a biblioteca terá seu 100º dia de funcionamento é aquele que deixa resto 2 na divisão por 7, assim será uma quarta-feira.

Mediante ao resultado apresentado, é oportuno e importante apresentar o Teorema 4 na sua forma geral.

Veremos as discussões e resoluções do item "b" como uma maneira de abordar o tratamento generalizado de um número natural a, a partir do resto r deixado entre a divisão euclidiana desse número a por outro número natural. Para isso retomaremos a Tabela 18 e, utilizando o Teorema 4, propõe-se que os alunos indiquem uma representação generalizada para os termos presentes em cada coluna da tabela. Dessa forma, as conclusões recaem em algo como:

domingo	**segunda**	**terça**	**quarta**	**quinta**	**sexta**	**sábado**
1º	6º	4º	2º	7º	5º	3º
8º	13º	18º	16º	14º	19º	17º
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$7q+1$	$7q+6$	$7q+4$	$7q+2$	$7q+7$	$7q+5$	$7q+3$

Tabela 19 – Generalização dos dias de funcionamento da biblioteca.

Desse modo, espera-se que os alunos concluam que os dias de funcionamento aos domingos são representados por um número que deixa resto 1 na divisão euclidiana por 7, então

ele é da forma $7q+1$ e q representa quantos ciclos semanais completam-se desde o início da contagem. Uma forma de ilucidar tais resultados é apresentado a seguir:

Ordenação dos domingos de funcionamento q	**Total de dias de funcionamento**
1º	$7.0+1=1$
2º	$7.1+1=8$
3º	$7.2+1=15$
$\vdots$	$\vdots$
q	$7(q-1)+1$

Tabela 20 – Generalização do total de dias de funcionamento da biblioteca para abertura aos domingos.

Assim, como procura-se $q=20$, segue que

$$7(20-1)+1=134,$$

ou seja, após 134 dias de funcionamento, a biblioteca completará o 20º domingo de abertura.

Como não se havia discutido sobre o Teorema 4 antes da realização da SD_2 pelos alunos, nas explanações e discussões sobre a resolução do item "c", espera-se que apareçam estratégias variadas, algumas que incluam contagens distintas, envolvendo as grandezas de tempo presente no calendário. Mediante a isso, os questionamentos abaixo podem contribuir nas percepções e formalizações que se espera construir ao longo dessa sequência:

- Quais as diferentes grandezas relacionadas a contagem do tempo puderam ser percebidas nesta situação e que também estão no calendário?
- Foi possível perceber regularidades nos períodos de todas essas grandezas averiguadas e utilizadas para resolução pedida? Descreva as possíveis dificuldades e diferenças percebidas.

Dadas as respostas, acredita-se ser possível o apontamento de algumas irregularidades como a quantidade de dias do ano – bissextos e não bissextos, ou quantidade de dias em cada mês. Mediante a isso, pode-se lançar o objetivo final da sequência didática através do questionamento:

"É possivel estabelecer uma relação matemática que permita determinar o dia da semana em uma data qualquer que se queira?"

É considerável que devido as irregularidades observadas, os alunos associem a resposta para tal pergunta como negativa. Assim, estabelecer o compromisso com o grupo onde uma série de considerações e percepções culminarão num resultado afirmativo para esse desafio, é uma

estratégia para o envolvimento e aguçamento da curiosidade de todos a favor do trabalho a ser realizado. Uma sugestão para o professor aplicador é deixar a pergunta acima exposta no quadro, durante todo o desenvolvimento da sequência didática.

A realização da solução do item "c" através do uso do Teorema 4, deve ser apresentada também como alternativa. Dessa forma, chamando a atenção para a existência de um ano bissexto b no intervalo averiguado, ou seja, o ano de 2024, verificamos que o total de dias existentes nos 5 anos após a abertura da biblioteca é

$$\text{Total de dias} = 365.5 + b = 365.5 + 1 = 1826.$$

Como esses dias estão organizados em ciclos de sete dias, temos

$$1826 = 7.260 + 6,$$

isto é, temos 260 ciclos semanais completos e mais seis dias. Como a abertura da biblioteca no dia 08 de março de 2020 foi um domingo, então seis dias a frente será um sábado.

A questão abaixo foi adaptada de "Problema de Gincana: Olimpíadas da Era Moderna", encontrado em (Clube da Matemática da OBMEP, 2012). Sua elaboração foi pensada para ser resolvida gradativamente, ou seja, a partir do primeiro item, cada questão é apresentada ao grupo após as resoluções e conclusões do item anterior terem sido concluídas.

SD_3 : Leia com atenção as informações abaixo.

A primeira Olimpíada da Era Moderna aconteceu em Atenas em 1896.
A última ocorreu em 2016, no Rio de Janeiro.
Por causa das duas grandes guerras mundiais, houve interrupção dos jogos nos períodos de 1914 a 1918 e de 1939 a 1945.
Houve uma edição comemorativa das Olimpíadas em 1906, na cidade de Atenas.
Os jogos olímpicos ocorrem de quatro em quatro anos.

Tabela 21 – Oimpíadas da Era Moderna - SD_3

Agora, vamos responder as questões:

(a) Com base nas informações dadas, qual o número total de Olimpíadas efetivamente realizadas desde a primeira edição?

(b) Dada as conclusões feitas no item a, descreva uma relação entre a quantidade de múltiplos de quatro, num intervalo numérico 1 a a, e o quociente da divisão euclidiana de a por quatro. Para contribuir nas reflexões, determine quantos múltiplos de 4 temos de 1 a 118.

(c) Note que uma grande parte das olímpiadas coincide com anos bissextos. A partir da relação estabelecida no item anterior, determine quantos anos bissextos teremos até o ano de 2099.

(d) Supondo que a tradição olímpica mantenha-se por muitos séculos, sem interrupções e nas mesmas condições de período, quantos eventos olímpicos teríamos concluído do ano atual até o ano 2520?

(e) Encontre a quantidade de anos bissextos para o mesmo período dado no item d.

(f) Escreva um relação geral que permita determinar a quantidade de anos bissextos num intervalo $[A_i, A_f]$ e $(A_i, A_f]$, onde A_i e A_f representam anos em nosso calendário atual.

O_3 : Elaborar estratégias para quantificar os múltiplos de um número natural dentro de um intervalo numérico, estabelecendo relações entre a quantidade procurada e o quociente da divisão euclidiana entre dois números naturais. Definir uma relação geral para determinação da quantidade de anos bissextos em um intervalo de anos.

Para a realização de SD_3 , sugere-se a criação de um ambiente que proporcione o debate de ideias e colaboração mútua entre os pares e o professor. A perspectiva é que o professor atue como participante ativo e instigativo na realização da atividade, a fim de que as hipóteses e levantamentos feitos, possam a cada passo gerar as percepções esperadas e sejam traspostas para uma linguagem matemática mais formal e generalizada. Dessa forma, o professor poderá organizar as informações dadas pelos alunos no quadro, fazendo os questionamentos e apontamentos pertinentes às contruções. É importante que, para cada questão, os alunos tenham um tempo para suas proprias elaborações.

Faremos a seguir uma sequência de observações, a título de norteamento do trabalho do professor. É possível que muitos dos pontos mencionados possam vir da contribuição dos alunos, assim como outros levantamentos relevantes que não serão especificados por nós.

No primeiro item de SD_3, espera-se retomar o conceito de múltiplos e reforçar sua representação a partir de uma igualdade, como por exemplo

$$\begin{aligned} 1896 &= 4.474 && (8.1)\\ 1900 &= 4.475 && (8.2)\\ 1904 &= 4.476 && (8.3)\\ \vdots &= \vdots \\ 2016 &= 4.504. && (8.4) \end{aligned}$$

Dessa forma, contribuir para a associação entre o fator multiplicado por 4 e seu sentido de ordenação no conjunto dos múltiplos de 4, como por exemplo

$$M_4 = \{4,8,12,16,\ldots\} = \{4.1,4.2,4.3,4.4,\ldots\}.$$

Aplicando a observação acima na situação pedida, verifica-se a necessidade em determinar a quantidade de elementos do conjunto $\{474,475,\ldots,504\}$, que é dado por

$$504-474+1=31.$$

Essa relação utilizada para contagem de elementos em um conjunto será aprofundada nos itens posteriores, contudo é importante chamar a atenção ao fato de adicionarmos 1 a nossa situação para contabilizar também o elemento 474. Assim, como tivemos uma edição extraordinária em 1906 e nos anos de 1916, 1940 e 1944 não ocorreram os jogos olímpicos, chega-se a um total de $31+1-3=29$ olímpiadas realizadas até o momento estipulado.

A dedução que se espera para o segundo item de SD_3 é fundamental para construir a ideia por trás da função piso e inserir sua representação matemática. Note que nosso intuito é qualificar o elemento encontrado na função piso, relacionando ao quociente q da divisão euclidiana entre dois números naturais, sem o interesse de formalizações acerca dela, conforme os resultados apresentados no Corolário 6.

Espera-se que os alunos relacionem as igualdades (8.2), (8.3), (8.4) e (8.4), a divisão euclidiana dos números dados quando divididos por quatro, deixando resto zero. Contudo, para contribuir nesse processo de relação e abstração, sugere-se começar as discussões pelo exemplo pedido. Fazendo a divisão euclidiana sugerida temos

$$118 = 4.29+2. \tag{8.5}$$

Descrevendo o conjunto dos múltiplos de 4 entre 1 e 118, obtemos a igualdade

$$\{4,8,12,\ldots 116\} = \{4.1,4.2,4.3,\ldots,4.29\},$$

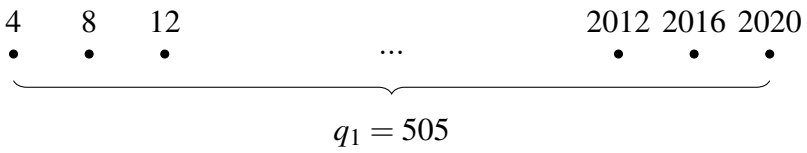
propiciando subsídios de comparação entre o quociente da divisão euclidiana realizada em (8.5) e o número total de múltiplos de quatro, discriminados no conjunto acima. Assim, após tais conclusões, o professor pode "combinar" com os alunos a escrita que será usada para representar a quantidade de múltiplos de 4, no intervalo $[1,a]$, com $a \in \mathbb{N}$, como

$$\left\lfloor \frac{a}{4} \right\rfloor.$$

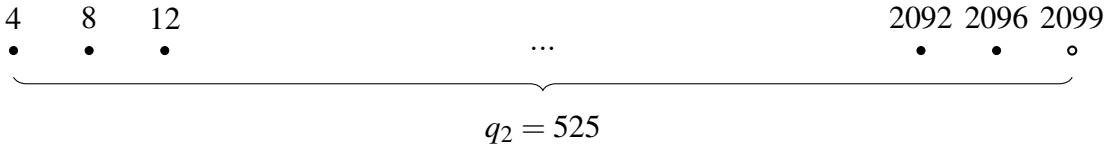
Para o terceito item de SD_3, pretende-se agrupar as percepções dos dois itens anteriores, de modo a ampliar sua aplicação para a contagem de elementos em conjunto de múltiplos por 4 entre intervalos diversos. Outro ponto que se introduzirá a partir desse item, é o estabelecimento do intervalo para contagem de anos bissextos presentes nele. Denotaremos que os intervalos

relacionados à contagem dos anos bissextos será de $(01,01,A)$ a $(01,01,A+1)$. O problema nos pede a quantidade de anos bissextos até 2099 e considerando o ano de início para contagem como o ano deste trabalho, buscamos a quantidade de múltiplos de 4 em $[2020,2099)$. Assim, uma forma de ilustrar a situação é:

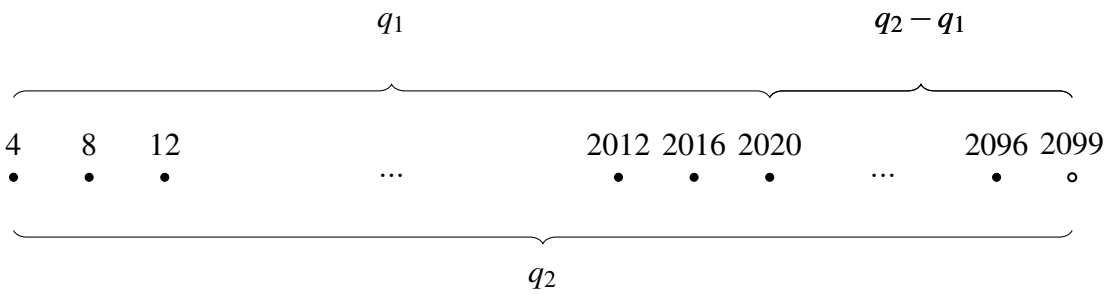
- Temos que $\left\lfloor \frac{2020}{4} \right\rfloor = q_1$ é a quantidade de múltiplos de 4 entre 1 e 2020, conforme a representação abaixo:



- Temos que $\left\lfloor \frac{2099}{4} \right\rfloor = q_2$ é a quantidade de múltiplos de 4 entre 1 e 2099, conforme a representação abaixo:



- Pelas observações acima, temos portanto que $q_2 - q_1$ é a quantidade de múltiplos de 4 entre 2020 e 2099, conforme a representação:



Mas, note pelas representações que como 2020 é múltiplo de 4 e então está presente tanto no primeiro quanto no segundo intervalo mensurado, ao fazermos $q_2 - q_1$ estamos excluíndo-o da contagem. Por isso, para contabilizá-lo fazemos o acréscimo de 1 a $q_2 - q_1$, análogo a situação encotrada no item "a". Uma ideia similiar pode ser levantada a respeito do ano de 2099, ele faz parte do intervalo, mas não foi contabilizado por não ser múltiplo de 4. Dessa forma, o problema pode ser expresso por

$$\left\lfloor \frac{2099}{4} \right\rfloor - \left\lfloor \frac{2020}{4} \right\rfloor + 1 = 525 - 505 + 1 = 21,$$

que é a quantidade de anos bissextos pedido.

No quarto e quinto itens seguiremos um desencadeamento de ideias que apliquem as percepções feitas nos itens anteriores e proporcione situações que colaborem na interpretação dos intervalos construídos, para contagem dos múltiplos de quatro. No item "d" é importante ressaltar com o grupo de alunos que no intervalo respectivo a situação dada estamos contabilizando 2020 e 2520, ambos múltiplos de quatro. Dessa forma, encontra-se

$$\left\lfloor \frac{2520}{4} \right\rfloor - \left\lfloor \frac{2020}{4} \right\rfloor + 1 = 630 - 505 + 1 = 126 \tag{8.6}$$

eventos olímpicos no período pedido.

Logo no início das discussões sobre o item "e" é fundamental que os alunos notem as particularidades da contagem pedida, isto é, o intervalo mensurado é de $(01/01/2020)$ a $(01/01/2520)$, conforme os padrões estabelecidos anteriormente para a contagem dos anos bissextos. Sequencialmente, surge a necessidade de considerar que nem todos os anos olímpicos encontrados no item "d" são bissextos. Segue daí a pergunta geradora:"quem devemos tirar da contagem?" Das respostas elencadas pelos alunos neste momento, é importante levá-los a distinguir que todo múltiplo de 400 é também mútiplo de 100, mas o contrário não se aplica. Por isso, pode-se propor uma contagem em três etapas:

(i) Determinaremos todos os múltiplos de 100 no intervalo $[2020, 2520]$.

$$\left\lfloor \frac{2520}{100} \right\rfloor - \left\lfloor \frac{2020}{100} \right\rfloor = 25 - 20 = 5.$$

(ii) Determinaremos todos os múltiplos de 400 no intervalo $[2020, 2520]$.

$$\left\lfloor \frac{2520}{400} \right\rfloor - \left\lfloor \frac{2020}{400} \right\rfloor = 6 - 5 = 1.$$

(iii) Subtraímos (ii) de (i) para obtermos somente os números que não são múltiplos de 400, logo $5 - 1 = 4$.

Temos por (8.6) os múltiplos de 4 de $[2020, 2520]$. Logo, como 2520 é múltiplo de 4, precisamos retirá-lo do resultado encontado, devido ao intervalo considerado na contagem dos anos bissextos. Assim, subtraindo também de (8.6) o determinado em (iii) temos

$$126 - 1 - 4 = 121$$

anos bissextos no intervalo de $[2020, 2520)$.

No item "f", espera-se que os alunos consigam reunir todas as reflexões, padrões e conclusões feitas ao longo dos cinco itens anteriores, de forma a usar uma linguagem matemática adequada para formulação da generalização esperada. Considerando a fragilidade que os alunos demonstram em trabalhar com a conexão entre vários conceitos, ideias e abstrações, é importante

optar por um recurso adequado. Uma sugestão é a organização das discussões em pontos principais. A seguir descreveremos um exemplo.

Vamos inicialmente elencar as grandezas presentes nesta contagem e definir suas representações algébricas:

- A_i e A_f são respectivamente ano inicial e ano final do intervalo analisado;
- b é a quantidade de anos bissextos no intervalo $[A_i, A_f)$;
- M_4 é a quantidade de múltiplos de 4 no intervalo $[A_i, A_f)$;
- M_{100} é a quantidade de múltiplos de 100 no intervalo $[A_i, A_f)$;
- M_{400} é a quantidade de múltiplos de 400 no intervalo $[A_i, A_f)$.

Consequente a isso, outro ponto a ser tratado com o grupo é a reflexão sobre o cálculo de M_4, considerando as diversas situações de A_i e A_f. Dessa forma, retomando as observações realizadas nos itens de "a" a "e", pode-se fomentar a discussão entre a relação de A_i e A_f serem múltiplos de quatro e o acréscimo ou retirada de 1, a depender da situação. Aqui pretende-se incentivar a discussão e analogia sobre a utilização das ferramentas apresentadas nesta *SD*, na finalidade de realizar a contagem de elementos em um conjunto. Neste contexo, é importante delinear as possíveis situações que podem ser encontradas:

- A_i e A_f não são múltiplos de 4.
- A_i e A_f são múltiplos de 4.
- A_i é múltiplo de 4 e A_f não é múltiplo de 4.
- A_i não é múltiplo de 4 e A_f é múltiplo de 4.

Descrevemos os casos acima subsidiados pelos exemplos que trataram, em sua maioria, dos múltiplos de 4. Contudo, para o contagem de anos bissextos, será necessário que tais conclusões de estendam também para os múltiplos de 100 e 400. Por isso, é interessante chamar a atenção que os itens elencados acima aplicam-se também a eles.

A partir da notação proposta, transcrevendo o resultado encontrado no item "d", temos que b é dado como

$$b = M_4 - (M_{100} - M_{400}), \tag{8.7}$$

tal que pelas conclusões feitas, temos

$$M_4 = \begin{cases} \left\lfloor \frac{A_f}{4} \right\rfloor - \left\lfloor \frac{A_i}{4} \right\rfloor, & \text{se } A_i, A_f \text{ forem ambos múltiplos ou não múltiplos de } 4. \\ \left\lfloor \frac{A_f}{4} \right\rfloor - \left\lfloor \frac{A_i}{4} \right\rfloor + 1, & \text{se somente } A_i \text{ for múltiplos múltiplo de } 4. \\ \left\lfloor \frac{A_f}{4} \right\rfloor - \left\lfloor \frac{A_i}{4} \right\rfloor - 1, & \text{se somente } A_f \text{ for múltiplos múltiplo de } 4. \end{cases}$$

$$M_{100} = \begin{cases} \left\lfloor \frac{A_f}{100} \right\rfloor - \left\lfloor \frac{A_i}{100} \right\rfloor, & \text{se } A_i, A_f \text{ forem ambos múltiplos ou não múltiplos de } 100. \\ \left\lfloor \frac{A_f}{100} \right\rfloor - \left\lfloor \frac{A_i}{100} \right\rfloor + 1, & \text{se somente } A_i \text{ for múltiplos múltiplo de } 100. \\ \left\lfloor \frac{A_f}{100} \right\rfloor - \left\lfloor \frac{A_i}{100} \right\rfloor - 1, & \text{se somente } A_f \text{ for múltiplos múltiplo de } 100. \end{cases}$$

$$M_{400} = \begin{cases} \left\lfloor \frac{A_f}{400} \right\rfloor - \left\lfloor \frac{A_i}{400} \right\rfloor, & \text{se } A_i, A_f \text{ forem ambos múltiplos ou não múltiplos de } 400. \\ \left\lfloor \frac{A_f}{400} \right\rfloor - \left\lfloor \frac{A_i}{400} \right\rfloor + 1, & \text{se somente } A_i \text{ for múltiplos múltiplo de } 400. \\ \left\lfloor \frac{A_f}{400} \right\rfloor - \left\lfloor \frac{A_i}{400} \right\rfloor - 1, & \text{se somente } A_f \text{ for múltiplos múltiplo de } 400. \end{cases}$$

SD$_4$: Joaquim decidiu que iria montar uma rotina diária de leitura para ler os livros que há tempos está querendo apreciar. Para isso, ele contou o número total de páginas dos livros que seriam lidos e organizou uma sequência, sem interrupções, de quatro períodos, conforme descrito abaixo:

Períodos	**Total de dias no período**	**Número de páginas a serem lidas por dia**
1º	12	10
2º	18	15
3º	23	20
4º	28	25

Tabela 22 – Organização dos períodos de leitura de Joaquim - SD_4

Joaquim deu início a sua maratona de leituras numa quarta-feira.

(a) Qual foi o dia da semana em que Joaquim concluiu suas leituras?

(b) Usando o *Teorema da Divisão Euclidiana*, encontre a soma dos restos de cada um dos números apresentados na coluna "período em dias" na divisão por 7. Qual o resto da divisão euclidiana do resultado desta soma por 7?

(c) Comparando os resultados encontrados em 1 e 2 é possível perceber alguma correspondência? Dado as observações, descreva uma solução alternativa para o primeiro item.

O_4 : Reconhecer a relação de equivalência entre o resto da divisão euclidiana entre uma soma inicial e um número natural dado com o resto da divisão euclidiana da soma dos restos, de cada uma das parcelas da soma inicial, pelo mesmo número natural.

Devido as abordagens anteriores que ressaltaram a relação da organização de uma quantidade de dias em semanas através de ciclos de 7 dias, espera-se que os alunos associem as definições e aplicações do *Teorema da Divisão Euclidiana* para a resolução do primeiro item. Com isso, chegaremos a ideias convergentes a

$$12+18+23+28=81,$$

dias totais de leitura. Como esses 81 dias estão organizados em semanas de sete dias, temos

$$81=11.7+4, \tag{8.8}$$

ou seja, passaram-se 11 semanas inteiras mais quatro dias. Na situação, a contagem do ciclo semanal começou numa quarta-feira, então é interessante ilustrar a sequência dos dias da semana aplicada ao caso:

Dias da semana (**S**)	quarta	quinta	sexta	sábado	domingo	segunda	terça
Ordenação do dia da semana	1º	2º	3º	4º	5º	6º	7º

Tabela 23 – Organização do ciclo semanal - SD_4.

Assim, fica evidente a verificação de que o ciclo de sete dias encerra-se na terça-feira, e portanto, quatro dias a frente será um sábado.

Nos itens "b" e "c" pretende-se que os alunos verifiquem a relação de equivalência entre o resto da divisão euclidiana de uma soma por sete e o resto da divisão euclidiana da soma dos restos de cada parcela por sete. Não se deseja tratar com formalidade a aritmética das classes residuais, mas sim sua ideia a partir de resultados perceptíveis em exemplos numéricos, no intuito de se tornar uma ferramenta de simplificação para cálculos futuros.

Durante as discussões sobre as conclusões encontradas nesses itens, uma abordagem que pode contribuir para elaboração da visão geral de que SD_4 propõe, é a realizada a partir da estrutura a seguir:

$$\begin{array}{rrcl} & 12 & = & 1.7+5 \\ & 18 & = & 2.7+4 \\ + & 23 & = & 3.7+2 \\ & 28 & = & 4.7+0 \\ \hline & 81 & = & 7(1+2+3+4)+(5+4+2+0). \end{array}$$

Substituindo o primeiro membro da última igualdade, pelo resultado dado em (8.8), temos

$$\begin{array}{rrcl} & 12 & = & 1.7+5 \\ & 18 & = & 2.7+4 \\ + & 23 & = & 3.7+2 \\ & 28 & = & 4.7+0 \\ \hline & 7.11+4 & = & 7(1+2+3+4)+(5+4+2+0). \end{array}$$

Note que com apoio da igualdade, podemos tornar visual e claro a relação entre os termos de cada membro obtidos nessa soma. No esquema acima, a última igualdade traz as duas primeiras parcelas de cada membro já convenientemente escritas como múltiplos de sete. No segundo membro é importante chamar a atenção ao fato de que a adição dos termos múltiplos de 7 geraram uma soma também múltiplos de 7, ou seja, uma quantidade definida de ciclos completos. Dessa forma, nosso olhar volta-se para a soma dos restos encontrada no segundo membro. Observe que na soma destes restos encontramos

$$5+4+2+0=11,$$

mas a quantidade 11 permite mais um ciclo de 7, então

$$11=7.1+4,$$

obtendo o resto final do segundo membro igual a 4, equivalentemente ao resto encontado no primeiro membro da mesma igualdade.

Assim, pudemos através dessa reflexão construir com eles uma justificativa para a relação percebida nos itens “b” e “c”, levando em considerações outros conceitos, princípios e propriedades do conjunto dos números naturais. Tal construção nos fornece referência para mostrarmos sua validade para quaisquer outros números naturais.

Retomando com os alunos a generalização do *Teorema da Divisão Euclidiana*, dados os números $\{a_1, a_2, a_3, ..., a_n\} \in \mathbb{N}$ quando divididos por um número natural b, temos a soma

$$\begin{array}{rrcl} & a_1 & = & q_1.b + r_1 \\ & a_2 & = & q_2.b + r_2 \\ & a_3 & = & q_3.b + r_3 \\ + & \vdots & = & \vdots \\ & a_n & = & q_n.b + r_n \\ \hline bq_k + r_k & & = & b(q_1 + q_2 + q_3 + ... + q_n) + (r_1 + r_2 + r_3 + ... + r_n), \end{array}$$

permitindo a mesma argumentação feita no exemplo numérico descrita anteriormente.

Como pretendemos utilizar da aritmética dos restos como ferramenta nos cálculos que estão sendo realizados em torno da nossa sequência didática, após os levantamentos feitos em SD_4, é interessante estipular com o grupo de alunos a forma de representação para aplicação dessas conclusões. Nas atividades apresentadas até o presente momento, frisou-se os ciclos de 7 dias e o papel do resto nesta contagem. Devido a tal importância que exerce, propõe-se ao grupo que, ao tratar dos restos da divisão euclidiana entre dois números, representaremos esse resto por $\bar{r}$. Por exemplo, uma forma de escrevermos uma solução alternativa para o primeiro item de SD_4, por essa nova linguagem, seria

$$S = \bar{5} + \bar{4} + \bar{2} + \bar{0} = \bar{4},$$

no qual cada $\bar{r}$ acima representa os respectivos restos na divisão euclidiana por 7 dos períodos dados.

O texto que subsidiará a próxima *SD* foi retirado de (MATEMÁTICA, 1998-2020).

SD$_5$:

Quando começa um século?
Um século começa em um ano 01 e termina em um ano 00.
Por exemplo, o século XX começou em 1901 e terminou em 2000 e o século XXI começou em 2001 e terminará em 2100. No entanto, para alguns, que reconhecem as alterações feitas ao calendário Gregoriano em 1582, um século começa em um ano 00 e acaba em um ano 99. Os séculos na História são numerados com algarismos romanos e nomeados com ordinais do I até o IX (primeiro, segundo, terceiro...) e com cardinais do X em diante (dez, onze, doze, treze...).

Tabela 24 – Quando começa um século - SD_5.

(a) Com base no texto acima, segundo o calendário Gregoriano, qual será o dia da semana que iniciaremos o próximo século? (Dica: o primeiro dia do ano de 2020 foi uma quarta-feira).

(b) Dadas as observações do item anterior, é possível descrever uma relação geral que permita determinar o primeiro dia de um ano qualquer?

(c) Aplique a relação encontrada no item b e encontre o dia da semana do primeiro dia do ano de 2003.

O_5 : Aplicar corretamete conclusões realizadas anteriormente acerca do cálculo dos anos bissextos e da aritmética dos restos referentes a operação de adição. Formular a partir das observações feitas em uma sequência recursiva, uma generalização para determinar o dia da semana do primeiro dia do ano, em um ano qualquer.

Nesta etapa da nossa sequência didática, recorreremos as definições e metodologias realizadas na seção sobre o Teorema de Zeller, com as devidas adptações necessárias.

Para a discussão sobre o resultado pedido no item "a", sugere-se a construção de uma sequência na mesma ideia da apresentada para a determinação da Proposição 25. É importante retomar com o grupo de alunos a nomenclatura adotada para cada grandeza utilizada, assim como a prática de simplificar os números encontrados utilizando o resto na divisão euclidiana por sete - reforçando as conclusões aferidas em SD_4. Neste sentido, pode-se introduzir essas observações comparando os dias da semana D e suas respectivas representações numéricas, ao resto da divisão euclidiana destes números por sete. Um ponto a se levantar com o grupo é a representação do sábado como o 7º dia da semana, que pelo olhar dos restos na divisão por 7, temos que ele é dado por $\bar{0}$.

Nesta perspectiva, como quarta-feira foi definida como o quarto dia da semana, introduzimos a análise da situação proposta de modo a chamar a atenção inicialmente para um primeiro período, entre $01/01/2020$ a $01/01/2021$. Temos que como 2020 é bissexto, o primeiro dia do ano de 2021 é após 366 dias do início de 2020, de forma que

$$D_{(1/1/2021)} = 4 + 366 = 4 + 7.52 + 2 = 7.52 + 6,$$

ou seja, uma sexta-feira. Com isso, podemos levantar com o grupo pontos como: "se o ano de partida não for bissexto o período será de 365 dias, que deixa resto 1 na divisão por sete". "Podemos utilizar somente o resto da divisão por sete em nossa análise?" A partir desses levantamentos, sugere-se a organização da sequência:

Período	Acréscimo aplicado	Dia da semana (D)
$2021-2022$	$\bar{6}+\bar{1}$	$7=\bar{0}$
$2022-2023$	$\bar{0}+\bar{1}$	$\bar{1}$
$2023-2024$	$\bar{1}+\bar{1}$	$\bar{2}$
$2024-2025$	$\bar{2}+\bar{2}$	$\bar{4}$
$\vdots$	$\vdots$	$\vdots$

Tabela 25 – Sequência dos acréscimos de dias ano a ano - item a de SD_5.

O intuito é que se conclua sobre um processo para determinar D na última linha da sequência acima, isto é, para o ano de 2100. É importante salientar que D é dado pelo resto da divisão euclidiana do número total de dias encontrado por 7. Durante o processo, as discussões devem levar a duas observações importantes: é preciso quantificar o total de anos e o total de anos bissextos no período; acrescentaremos $\bar{1}$ para cada um deles em nossa contagem.

Na quantificação dos anos bissextos, vale ressaltar nas discussões que o intervalo buscado é [2020,2100) e que tanto 2020 quanto 2100 são múltiplos de 4. Outro ponto a considerar é que nesse período mensurado temos que 2100 é múltiplo de 100 e que não temos múltiplos de 400, então $M_{400}=0$. Dessa forma, utilizando o resultado dado em (8.7), temos

$$\begin{aligned} b &= M_4 - M_{100} \\ &= \left\lfloor \frac{2100}{4} \right\rfloor - \left\lfloor \frac{2020}{4} \right\rfloor - \left(\left\lfloor \frac{2100}{100} \right\rfloor - \left\lfloor \frac{2020}{100} \right\rfloor - 1 \right) \\ &= 525 - 505 \\ &= 20. \end{aligned}$$

Para quantificar o total de anos do período, basta fazer $2100-2020=80$. Assim, D na última linha da sequência pode ser dado por

$$D_{(01/01/2100)} = 4+80+20 = \bar{4}+\bar{3}+\bar{6} = \bar{6}.$$

Logo, o primeiro dia do ano de 2100 será uma sexta-feira.

Para item "b", espera-se que reconheçam no processo descrito no item anterior um caminho que possa ser generalizado para outras situações que se queira. Com isso, partindo do primeiro dia s de um ano A_i que se tome por base, pode-se determinar o dia da semana D, do primeiro dia de um ano A_f qualquer, como

$$D_{(1/1/A_f)} = s + (A_f - A_i) + b. \tag{8.9}$$

Para o item "c" procurou-se proporcionar um cenário que levasse a utilização da generalização (8.9) e, simultaneamente, estender sua aplicação em casos onde $A_i > A_f$. Tal percepção

estará implícita a partir do resultado encontrado no item "c", por isso é propício que o professor aplicador faça observações cuidadosas das devolutivas dos alunos, a fim de realizar intervenções e apontamentos necessários para dar clareza a dedução. Neste cenário, uma estratégia é traduzir a situação como: "Utilizando os mesmos passos do primeiro item, ou seja, se começamos a contagem em 2003 e chegarmos a 2020, sabemos que o resultado será 4, uma quarta-feira. De qual dia da semana partimos?" Aplicando essas informações em (8.9), escrevemos

$$4 = s + (2020 - 2003) + b. \tag{8.10}$$

Uma análise que julgamos interessante em relação a contagem dos anos bissextos é procurar sempre fazer a leitura da situação em termos qualitativos. Por exemplo, neste caso o intervalo dos anos claramente não tem múltiplos de 100 e nem de 400, portanto o problema se resume na contagem dos múltiplos de 4. Dessa forma, temos pelo resultado de (8.7)

$$\begin{aligned} b &= M_4 - (M_{100} - M_{400}) \\ &= \left\lfloor \frac{2020}{4} \right\rfloor - \left\lfloor \frac{2003}{4} \right\rfloor - 1 - (0-0) \\ &= 505 - 500 - 1 \\ &= 4, \end{aligned}$$

e, portanto, retornando para (8.10) segue

$$\begin{aligned} 4 &= +s + 17 + 4 \\ 4 &= s + 21 \\ s &= 4 - 21 \\ s &= 4 - 7.3. \end{aligned} \tag{8.11}$$

Observe que s é um dia da semana e estamos tratando essa grandeza com base no seu respectivo resto na divisão por 7. Na igualdade (8.11) deixamos convenientemente explícito a parcela múltiplo de 7, desse modo temos que $4 - 7.3$ deixará resto 4 na divisão euclidiana por 7 e logo, o primeiro dia do ano de 2003 foi uma quarta-feira.

O fragmento a seguir foi adaptado de (DIANA, 2012-2020) e subsidiará a próxima *SD*.

SD$_6$: Você sabia?

Os Sertões, de Euclides da Cunha

"Os Sertões" é uma das obras mais emblemáticas do escritor pré-modernista Euclides da Cunha $(1866-1909)$, publicada em 01 de dezembro de 1902. A obra regionalista narra os acontecimentos da sangrenta Guerra de Canudos, liderada por Antônio Conselheiro $(1830-1897)$, que ocorreu no Interior da Bahia, durante 1896 e 1897. Trata-se de um relato histórico mesclado à literatura, posto que Euclides foi convidado pelo Jornal Estado de São Paulo para cobrir a guerra no Arraial de Canudos e nesse momento, surgiu sua obra.
Por esse motivo, "Os Sertões" representa um marco da literatura e na história do Brasil, sendo, portanto, analisada por outras áreas do conhecimento, tal qual: Antropologia, Sociologia, Geografia e História.
A obra possui um caráter crítico e realista nunca antes abordado por um literato do Brasil, donde Euclides por meio de uma linguagem cientificista recrimina o nacionalismo e ufanismo exacerbado da sociedade brasileira da época, mostrando a face cotidiana e realista do país e das pessoas que o compõem.
De tal modo, trata-se de uma prosa científica e artística, acabando com essa visão idealista do índio herói e do negro trabalhador, abordado com entusiasmo pelos escritores do romantismo.

Tabela 26 – Adaptação de Os Sertões - SD_6

(a) Em $01/12/2052$ comemora-se 150 anos de publicação desta importante obra literária brasileira. Determine qual será o dia da semana desse evento.

(b) Estabeleça uma relação geral que permita determinar o dia da semana D do primeiro dia de um mês m no ano A_f.

O_6 : Reconhecer o padrão presente em uma sequência recursiva acerca da quantidade de dias que cada mês acrescenta, ao realizar-se uma contagem a partir do primeiro dia do ano. Utilizar de generalizações definidas anterioremente para formular uma relação que permita determinar o dia da semana do primeiro dia de um mês, num ano qualquer.

No item "a" algumas estratégias de resoluções podem ser levantadas pelos alunos tomando como início das contagens referências diversas. É importante explorar as contribuições e levá-los a reflexões em torno delas, de modo a favorecer a tomada de decisões que simplifiquem o processo de contagem e que se apliquem também a outras situações.

Um ponto relevante neste item é a aplicação da relação (8.9) para determinar o primeiro dia do ano de 2052 e, dessa forma, "o que precisamos descobrir é como contar o total de dias até o primeiro dia do mês de dezembro." Neste intuito, deixando a escolha do momento adequado para o professor aplicador, sugere-se a construção de uma tabela como a realizada na Tabela 11, mas que inicie-se no mês de janeiro e considere a contagem dos dias para anos comuns e bissextos. Segue abaixo um exemplo.

Meses	***Acréscimo dos dias nos meses***	***Total de dias desde*** $D_{(1/1/A)}$
Janeiro	$D_{(1/1/A)} = D_{(1/1/A)} + 0$	0
Fevereiro	$D_{(1/2/A)} = D_{(1/1/A)} + 31$	31
Março	$D_{(1/3/A)} = D_{(1/1/A)} + 31 + 28$	59
	$D_{(1/3/A)} = D_{(1/1/A)} + 31 + 29$	60
Abril	$D_{(1/4/A)} = D_{(1/1/A)} + 59 + 31$	90
	$D_{(1/4/A)} = D_{(1/1/A)} + 60 + 31$	91
Maio	$D_{(1/5/A)} = D_{(1/1/A)} + 90 + 30$	120
	$D_{(1/5/A)} = D_{(1/1/A)} + 91 + 30$	121
Junho	$D_{(1/6/A)} = D_{(1/1/A)} + 120 + 31$	151
	$D_{(1/6/A)} = D_{(1/1/A)} + 121 + 31$	152
Julho	$D_{(1/7/A)} = D_{(1/1/A)} + 151 + 30$	181
	$D_{(1/7/A)} = D_{(1/1/A)} + 152 + 30$	182
Agosto	$D_{(1/8/A)} = D_{(1/1/A)} + 181 + 31$	212
	$D_{(1/8/A)} = D_{(1/1/A)} + 182 + 31$	213
Setembro	$D_{(1/9/A)} = D_{(1/1/A)} + 212 + 31$	243
	$D_{(1/9/A)} = D_{(1/1/A)} + 213 + 31$	244
Outubro	$D_{(1/10/A)} = D_{(1/1/A)} + 243 + 30$	273
	$D_{(1/10/A)} = D_{(1/1/A)} + 244 + 30$	274
Novembro	$D_{(1/11/A)} = D_{(1/1/A)} + 273 + 31$	304
	$D_{(1/11/A)} = D_{(1/1/A)} + 274 + 31$	305
Dezembro	$D_{(1/12/A)} = D_{(1/1/A)} + 304 + 30$	334
	$D_{(1/12/A)} = D_{(1/1/A)} + 305 + 30$	335
Janeiro	$D_{(1/1/A+1)} = D_{(1/1/A)} + 334 + 31$	365
	$D_{(1/1/A+1)} = D_{(1/1/A)} + 335 + 31$	366

Tabela 27 – Acréscimos dos dias mês a mês a partir de $D_{(1/1/A)}$

Mediante as observações da tabela, como o ano de 2052 é um ano bissexto, de $01/01/2052$ até $01/12/2052$ passaram-se 335 dias. Desse modo, aplicando (8.9) a situação, temos

$$\begin{aligned} D_{(1/12/2052)} &= D_{(1/1/2052)} + 335 \\ &= s + (2052 - A_i) + b + 335. \end{aligned} \tag{8.12}$$

Escolhendo $A_i = 2020$, temos $s = 4$ e aplicando em (8.12) encontramos

$$D_{(1/12/2052)} = 4 + (2052 - 2020) + b + 335. \tag{8.13}$$

Fazendo a análise qualitativa para o cálculo de b, notamos que, no intervalo de anos analisado, não temos múltiplos de 100 e nem de 400, de modo que $M_{100} = 0$ e $M_{400} = 0$. Em relação aos

múltiplos de 4, verifica-se que 2020 e 2052 o são, desse modo, temos por (8.7) que

$$\begin{aligned} b &= M_4 - (M_{100} - M_{400}) \\ &= \left\lfloor \frac{2052}{4} \right\rfloor - \left\lfloor \frac{2020}{4} \right\rfloor - (0-0) \\ &= 513 - 505 \\ &= 8. \end{aligned}$$

Retornando para (8.13) temos

$$\begin{aligned} D_{(1/12/2052)} &= 4+32+8+335 \\ &= \bar{4}+\bar{4}+\bar{1}+\bar{6} \\ &= \overline{15} \\ &= \bar{1} \end{aligned}$$

e, portanto, o aniversário de 150 anos da publicação da obra "Os Sertões" será num domingo.

No item "b", espera-se que os passos realizados em "a" sejam generalizados e possam ser representados pela simbologia matemática adequada. Assim, o dia da semana $D_{(1/m/A)}$, do primeiro dia do mês m, tal que m é o acréscimo de dias a partir do primeiro dia do ano A_f, é dado por

$$D_{(1/m/A_f)} = D_{(1/1/A_f)} + m.$$

Utilizando o resultado encontrado em (8.9), tem-se que

$$D_{(1/m/A_f)} = s + (A_f - A_i) + b + m, \tag{8.14}$$

tal que $D_{(1/m/A_f)}$ é o menor resto na divisão por 7.

O fragmento a seguir, foi retirado da matéria encontrada em (SANSON, 2015).

SD$_7$: Leia o fragmento abaixo.

Você conhece os chamados "Feriados Matemáticos"?

(...)Uma das coisas que poucos sabem é que existem os chamados "feriados matemáticos". Calma, não são datas de folga a mais no seu calendário, mas sim dias adotados por matemáticos e cientistas para representar, e em alguns casos até "comemorar", alguns cálculos e números específicos. Aqui no Brasil, pouco se sabe sobre essas datas, mas essas celebrações possuem uma tradição considerável nos Estados Unidos, pois elas se originaram por lá.(...)

Dia da Raiz Quadrada

A raiz quadrada não possui uma data específica de comemoração anual, mas tem dias determinados por anos que representam raízes exatas. O conceito foi criado pelo professor americano Ron Gordon, de Redwood City, na Califórnia, quando anunciou a data de 9 de setembro de 1981$(9,9,81)$ como Dia da Raiz Quadrada.

Desde então, todos os dias com números iguais ao do mês em questão, e que, multiplicados, resultem na dezena final do ano são considerados Dia da Raiz Quadrada. Dessa forma, os últimos dias dessa comemoração ocorridos foram $(2,2,04)$ e $(3,3,09)$. Já o próximo que vai ocorrer é logo em abril do ano que vem, em $(4,4,16)$.

O Dia da Raiz Quadrada possui um site próprio e uma página no Facebook para que as pessoas interessadas possam se reunir e trocar ideias nos períodos que antecedem as datas.

Tabela 28 – Feriados Matemáticos - SD_7

(a) Qual será o dia da semana do próximo "feriado matemático" referente ao dia da raiz quadrada?

(b) Utilize as observações feitas no item anterior e descreva uma relação entre um dia do mês m, e os dias da semana decorrentes do primeiro dia do mês m.

(c) Seja $D_{(d/m/A_f)}$, tal que $D_{(d/m/A_f)}$ é o menor resto na divisão por sete, o dia da semana de um dia d no mês m, em um ano A_f. Reunindo as observações e conclusões feitas, generalize uma relação matemática que permita determinar $D_{(d/m/A_f)}$ para qualquer data que se queira.

O_7 : Deduzir a partir de uma sequência recursiva a relação entre um dia do mês e o dia da semana anterior a ele. Aplicar tal percepção a generalizações já realizadas anteriormente, de forma a inserir a grandeza referente ao dia do mês, proporcionando a construção de uma relação ainda mais geral na determinação do dia da semana, em uma data qualquer do calendário atual.

É importante que o aluno reconheça em todo o processo que vem sendo descrito, a partir das resoluções e discussões das situações desafiadoras, a abordagem espiralada dos conceitos e aplicações. Desse modo, ele tem como ponto de partida uma conclusão assimilada anteriormente e é motivado a fazer novas formulações, que expandam as percepções já realizadas.

Não distinto a essa ideia, o item "a" da SD_7 tem como objetivo que os alunos recorram a relação (8.14) para subsidiar as contagens para o dia que se pede. A partir do entendimento do texto de referência, traça-se que procuramos o dia da semana de $05/05/2025$. Uma estratégia para a explicitação da relação entre o dia procurado, com (8.14) é a mostrada na sequência abaixo:

$$\begin{aligned} D_{(01/05/2025)} &= D_{(01/05/2025)} \\ D_{(02/05/2025)} &= D_{(01/05/2025)} + 1 \\ D_{(03/05/2025)} &= D_{(01/05/2025)} + 2 \\ D_{(04/05/2025)} &= D_{(01/05/2025)} + 3 \\ D_{(05/05/2025)} &= D_{(01/05/2025)} + 4. \end{aligned}$$

Note que os acréscimos aplicados a $D_{(01/05/2025)}$ mostram o quanto caminha-se nos dias da semana a partir dele, assim, temos que

$$\begin{aligned} D_{(05/05/2025)} &= D_{(01/05/2025)} + 4 \\ &= s + (2025 - A_i) + b + m + 4. \end{aligned} \tag{8.15}$$

Por conveniência, toma-se $A_i = 2020$ e logo $s = 4$. Dessa forma, temos que b são os múltiplos de 4 no intervalo $[2020, 2025)$ e, portanto, $b = 2$. Pela Tabela 27, temos que $m = 120$ e aplicando tais observações em (8.15), encontramos

$$\begin{aligned} D_{(05/05/2025)} &= 4 + 5 + 2 + 120 + 4 \\ &= \bar{4} + \bar{5} + \bar{2} + \bar{1} + \bar{4} \\ &= \bar{2}. \end{aligned}$$

Logo, o dia da raiz quadrada de $D_{(05/05/2025)}$ será uma segunda-feira.

Com a base de reflexão apresentada no item "a", é explícito observar que dado um dia d do mês, o dia da semana que o representa difere de 1, em relação ao dia da semana do dia anterior, o que responde o solicitado no item "b". Assim, a generalização pedida no terceiro item é imediata, de forma a obtermos:

$$D_{(d/m/A_f)} = D_{(1/m/A_f)} + d - 1. \tag{8.16}$$

Aplicando as conclusões de (8.14) em (8.16), temos

$$D_{(d/m/A_f)} = s + (A_f - A_i) + b + m + d - 1, \tag{8.17}$$

tal que $D_{(d/m/A_f)}$ é o menor resto na divisão por 7, determinando assim a generalização pedida.

Finalizado SD_7 é interessante retomar com os alunos o objetivo geral apresentado no início das discussões, ainda em SD_1, e propor uma comparação com os resultados finais encontrados, para fidelizar o cumprimento de tal objetivo. Nesta perspectiva, apresentamos uma situação

desafiadora final que tem como objetivo a aplicação da referida relação e, concomitantemente, avalie o uso dos recursos numéricos e algébricos apresentados ao longo dos procedimentos realizados anterioremente.

SD_8 : Agora é o momento da verdade: em que dia da semana será seu aniversário de 50 anos ?

O_8: Avaliar o emprego das relações algébricas e aritméticas construídas acerca da grandeza dia da semana a partir das referências dia, mês e ano.

Note que ao propormos um desafio que é particular a realidade de cada aluno, estamos proporcionando também uma ferramenta que permita a averiguação da compreensão individual acerca do tema desenvolvido na sequência didática. Como a resolução de SD_8 perpassa a utilização de todas as conclusões e conceitos estabelecidos nas *SD* anteriores, permite um ollhar para possíveis dificuldades específicas dos alunos, contribuindo assim para uma intervenção pontual do professor nesses casos.

Para colaborar com o professor na correção dessa atividade, sugere-se o uso do site: *http://www.supercalendario.com.br/.*

Em toda a sequência didática apresentada, através da resolução das SD_n, foi possível observar que os problemas não estavam resumidos na resolução de uma equação ou algorítmo, mas na fomentação do pensamento algébrico. Para (PONTES; BRANCO, 2009), a construção do pensamento algébrico está diretamente relacionado às situações de aprendizagem que apresentamos aos alunos. Segundo o mesmo autor, tais situações devem

> "(...) dar-se ênfase aos significados que podem ser representados por símbolos levando os alunos a "pensar genericamente", percebendo regularidades e explicitando essas regularidades através de estruturas ou expressões matemáticas e a "pensar funcionalmente", estabelecendo relações entre variáveis." (PONTES; BRANCO, 2009, p. 14)

Dessa forma, ao selecionar tópicos da aritmética modular implícitos nos eixos do currículo do Ensino Fundamental dos anos finais, pode-se proporcionar o uso de propriedades do conjunto dos números naturais e inteiros de forma mais abrangente e qualitativa, diferindo do trato que recebem comumente nas práticas de ensino. Acrescenta-se ainda a contribuição na transição para o uso da linguagem específica e aprimoramento do pensamento algébrico, a partir do uso e exploração de sequências e regularidades.

REFERÊNCIAS

BRASIL. **Parâmetros Curriculares Nacionais: Matemática.** Brasília: MEC/SEF, 1998. P. 90-148. Citado na página 137.

____. **Base Nacional Comum Curricular**. Brasília:MEC, 2017. Disponível em: <Disponívelem:http://basenacionalcomum.mec.gov.br/images/BNCC_20dez_site.pdf>. Acesso em: 22/03/2020. Citado nas páginas 138, 139 e 141.

BUCCOLIERO, V. 2020. Disponível em: <https://casahacker.org/hackblog/2020/8/20/criptografia-uma-breve-histria>. Acesso em: 05/09/2020. Citado na página 98.

Clube da Matemática da OBMEP. **Probelmas de Gincana - Olimpíadas da Era Moderna**. 2012. Disponível em: <http://clubes.obmep.org.br/blog/problema-de-gincana-olimpiadas-da-era-moderna/#:~:text=Problema%20de%20Gincana%3A%20Olimp%C3%ADadas%20da%20Era%20Moderna,-Problema&text=A%20primeira%20Olimp%C3%ADada%20da%20Era,e%20de%201939%20a%201945.> Acesso em: 10/07/2020. Citado na página 146.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. 2. ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada-IMPA, 2014. 226 p. Citado nas páginas 56, 71, 74 e 114.

DARROZ, L. M. **O Planeta Terra**. [S.l.], 2010. Disponível em: <https://lief.if.ufrgs.br/pub/cref/n20_Darroz/texto_terra.html>. Acesso em: 22/07/2020. Citado na página 116.

DIANA, D. **Os Sertões, de Euclides da Cunha**. 2012–2020. Disponível em: <https://www.todamateria.com.br/os-sertoes-de-euclides-da-cunha/>. Acesso em: 17/07/2020. Citado na página 158.

ENQ-2018.2. **Exame Nacional de Qualificação-ENQ-2018.2**. 2018. Disponível em: <https://www.profmat-sbm.org.br/wp-content/uploads/sites/23/2018/07/ENQ-20182-gabarito.pdf>. Acesso em: 15/06/2019. Citado na página 67.

FESTAS, M. I. F. A aprendizagem contextualizada: análise dos seus fundamentos e práticas pedagógica. **Educ. Pesqui.São Paulo**, n. 3, p. 713–728, Jul./Set.2015, 2015. Disponível em: <https://doi.org/10.1590/S1517-9702201507128518>. Citado na página 141.

FIELDS, B. T. 2011. Disponível em: <https://en.wikipedia.org/wiki/Tabula_recta#/media/File:Vigen%C3%A8re_square_shading.svg>. Acesso em: 15/08/2020. Citado na página 96.

FILHO, K. de S. O.; SARAIVA, M. de F. O. **Fases da Lua**. [S.l.], 2018. Disponível em: <http://www.astro.ufrgs.br/lua/lua.htm>. Acesso em: 18/08/2020. Citado na página 116.

FOMIN, D.; GENKIN, S.; ITENBERG, I. **Círculos Matemáticos. A experiência Russa**. 1. ed. Rio de Janeiro: IMPA, 2012. 292 p. Citado nas páginas 64, 66 e 75.

GIL, K. H. **Reflexões sobre as dificuldades dos alunos na aprendizagem de álgebra.** Dissertação (Mestrado) — Originalmente apresentada como dissertação de Mestrado, Pontifícia Católica do Rio Grande do Sul – Faculdade de Física, Porto Alegre, 2008.118 f. Disponível em: <Disponívelem:http://repositorio.pucrs.br/dspace/bitstream/10923/2962/1/000401324-Texto%2BCompleto-0.pdf.> Citado na página 139.

HEFEZ, A. **Aritmética**. 1. ed. Rio de Janeiro: Coleção PROFMAT-SBM, 2014. 338 p. Citado nas páginas 67, 71, 95, 129 e 134.

JOYCE, D. E. **Proposition 20**. 2013. Disponível em: <https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html>. Acesso em: 27/08/2020. Citado na página 45.

JUNIOR, M. A. R. **Os Calendários e a sua contribuição para o Ensino da Astronomia**. Dissertação (Mestrado) — Faculdade de Ciências da Universidade de Porto - Departamento de Física e Astronomia, Porto, 2012. Citado na página 118.

KFOURI, W.; D'AMBRÓSIO, U. Explorar e investigar para aprender matemática através da modelagem matemática. In: ENCONTRO BRASILEIRO DE ESTUDANTES EM PÓS - GRADUAÇÃO EM MATEMÁTICA, 10. Belo Horizonte: Anais Belo Horizonte, 2006. Disponível em: <http://www.fae.ufmg.br/ebrapem/completos/09.> Acesso em: 19/06/2020. Citado na página 140.

LINS, R. C.; GIMENEZ, J. **Perspectivas em Aritmética e Álgebra para o século XXI**. 6. ed. Campinas,SP: Papirus, 1997. Citado na página 139.

MARQUES, M. N. **Origem e Evolução do Nosso Calendário**. s.d. Disponível em: <http://www.mat.uc.pt/~helios/Mestre/H01orige.htm>. Acesso em: 11/02/2020. Citado na página 119.

MARTINEZ, F.; MOREIRA, C. G.; SALDANHA, N.; TENGAN, E. **Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro**. 3. ed. Rio de Janeiro: IMPA, 2013. Citado na página 114.

MATEMÁTICA, S. **Quando começa um século**. 1998–2020. Disponível em: <https://www.somatematica.com.br/curiosidades/c53.php>. Acesso em: 11/07/2020. Citado na página 155.

OBM-1991. **Olimpíada Brasileira de Matemática**. 1991. Disponível em: <https://www.obm.org.br/content/uploads/2019/01/GUGU_Problemas_Teoria_Numeros.pdf>. Acesso em: 22/08/2019. Citado na página 88.

PONTES, J. P.; BRANCO, N. **Álgebra no ensino básico: Material de Apoio do Ensino Básico**. Lisboa, 2009. Citado na página 164.

SAMPAIO, J. C.; CAETANO, P. A. S. **Introdução a Teoria dos Números:um curso breve**. 1. ed. São Carlos: EduFSCAR, 2014. 109 p. Citado na página 67.

SANSON, R. **Você conhece os feriados matemáticos?** 2015. Disponível em: <https://www.megacurioso.com.br/datas-comemorativas/85745-voce-conhece-os-chamados-feriados-matematicos.htm>. Acesso em: 15/07/2020. Citado na página 161.

STOCKTON, D. J. R. **The Calendrical Works of Rektor Chr. Zeller: The Day-of-Week and Easter Formulae.** 2010. Disponível em: <http://ss64.net/merlyn/zeller-c.htm#Zbio>. Acesso em: 10/02/2020. Citado na página 119.

WIKIPÉDIA. **Zeller's Congruence**. 2020. Disponível em: <https://en.wikipedia.org/wiki/Zeller%27s_congruence>. Citado na página 119.

ZABALA, A. **A prática educativa: como ensinar.** 1. ed. Porto Alegre: ArtMed, 1998. Citado na página 140.


ICMC
USP
SÃO CARLOS