UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Aplicações de congruência, possibilidades para o ensino de Matemática no Ensino Fudamental II

Carlos Elizandro Corrêa

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

ICMC USP
SÃO CARLOS

Carlos Elizandro Corrêa

Aplicações de congruência, possibilidades para o ensino de Matemática no Ensino Fudamental II

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

Área de Concentração: Mestrado Profissional em Matemática em Rede Nacional

Orientadora: Profa. Dra. Ires Dias

USP – São Carlos
Fevereiro de 2023

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

Corrêa, Carlos Elizandro
C824a Aplicações de congruência, possibilidades para o ensino de Matemática no Ensino Fudamental II / Carlos Elizandro Corrêa; orientadora Ires Dias. -- São Carlos, 2023.
61 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, 2023.

1. Divisibilidade. 2. Aritmética Modular. 3. Teoria dos Números. 4. Dígitos Verificadores. 5. Calendário. I. Dias, Ires, 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

Carlos Elizandro Corrêa

Applications of congruence, possibilities for teaching Mathematics in Elementary School II

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: Profa. Dra. Ires Dias

USP – São Carlos
February 2023

Dedico este trabalho à minha avó,
Maria Josefa Garcia dos Santos (in memoriam).

AGRADECIMENTOS

Agradeço primeiramente a Deus, pela vida, sabedoria e força para chegar até aqui.

Aos meus pais, Marlene e José Carlos, por todo esforço em minha educação, apoio e amor. Em especial, à minha noiva Thais, por todo apoio e que soube entender minha ausência durante esse período.

À minha orientadora, Dra. Ires Dias, por me aceitar como seu orientando, pela paciência, pelos ensinamentos ministrados não só durante esta dissertação, mas também durante as disciplinas do curso e exame de qualificação. E, principalmente, por ser uma pessoa amiga, que acolheu a mim e toda nossa turma do PROFMAT como uma mãe.

Aos professores do programa PROFMAT: Ladeira, Paulo, Zani, Erica e Michela, pelo conhecimento compartilhado conosco. Especialmente, ao Hermano e Ires (sim, de novo) por não pouparem esforços, nas sextas-feiras, sábado e até feriados. Eles sempre estiveram presentes para nos ajudar.

Aos amigos da turma do PROFMAT, em especial Adriana, Douglas e Meryelen, por todas as horas de estudo juntos, que deixaram nossas sextas-feiras mais leves. Pelas angústias e principalmente alegrias compartilhadas.

Aos meus amigos Valdécio e Camila, da graduação e do IFSP, pelas sugestões, correção ortográfica e incentivos para não desanimar.

A todos os professores que contribuíram com minha formação acadêmica, em especial ao Luciano e Antônio, queridos professores de Matemática, que me fizeram apaixonar por esta bela ciência, a Matemática.

Agradeço também todos que contribuíram, mesmo que indiretamente, para a realização deste sonho. MUITO OBRIGADO.

“Nossas dúvidas são traidoras e nos fazem perder o que,
com frequência, poderíamos ganhar,
por simples medo de arriscar.”
(William Shakespeare)

RESUMO

CORRÊA, C. E. **Aplicações de congruência, possibilidades para o ensino de Matemática no Ensino Fudamental II**. 2023. 61 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, 2023.

Apesar de o estudo de congruências estar voltado ao Ensino Superior, nosso objetivo neste trabalho é defender que é possível articular a Teoria dos Números com a prática de professores da Educação Básica, mais especificamente, nos anos finais do Ensino Fundamental II. O trabalho aborda a fundamentação teórica dos números, divisibilidade, congruências e apresentamos aplicações em sistemas de identificação com seus dígitos verificadores, código de barras, CPF, ISBN-13 e calendário. Por fim, são apresentadas possibilidades de atividades a serem aplicadas sobre os conceitos mencionados, com problemas relacionados ao cotidiano do aluno.

Palavras-chave: Divisibilidade, Aritmética Modular, Teoria dos Números, Dígitos Verificadores, Calendário.

ABSTRACT

CORRÊA, C. E. **Applications of congruence, possibilities for teaching Mathematics in Elementary School II**. 2023. 61 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, 2023.

Although the study of congruences is focused on Higher Education, our objective in this work is to defend that it is possible to articulate the Theory of Numbers with the practice of Basic Education teachers, more specifically, in the final years of Elementary School II. The work addresses the theoretical foundation of numbers, divisibility, congruences and we present applications in identification systems with their verification digits, bar code, CPF, ISBN-13 and calendar. Finally, possibilities of activities to be applied on the mentioned concepts are presented, with problems related to the student's daily life.

Keywords: Divisibility, Modular Arithmetic, Number Theory, Check Digits, Calendar.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

BNCC	Base Nacional Comum Curricular
CPF	Cadastro de Pessoa Física
EAN-13	European Article Number
ISBN	International Standard Book Number
ISO	Organização Internacional de Normalização
ISSN	International Standard Serial Number
PROFMAT	Programa de Mestrado Profissional em Matemática em Rede Nacional
UPC	Universal Product Code

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

A matemática, ciência historicamente produzida e transmitida pela humanidade, pode ser observada em diferentes situações, contextos e épocas, desde resolução de problemas cotidianos, até explicações complexas, demonstrando, assim, sua versatilidade. Atualmente, notamos grande progresso no campo da tecnologia e das ciências, sendo, a cada dia, anunciadas novas descobertas. Em muitos casos, os amantes da matemática têm buscado aprimorar os conhecimentos adquiridos, afim de consolidar a relevância de tal ciência para a humanidade. No âmbito da Educação Básica, cumpre elucidar a importância da prática pedagógica estar voltada para um ensino que desperte o interesse dos estudantes pela matemática, evidenciando sua vasta aplicabilidade em diferentes situações do dia a dia.

Dentre as teorias e conceitos matemáticos, tem-se a Teoria dos Números, em que se estuda as propriedades e as relações entre os números inteiros, sendo a aritmética modular uma das ferramentas mais importantes desta teoria que envolve o conceito de congruência. Entende-se por congruência a relação entre dois números inteiros que, divididos por um terceiro chamado módulo de congruência, deixam o mesmo resto. É um conceito muito importante e que está relacionado com divisibilidade e os restos de uma divisão de números inteiros.

Apesar dos conceitos de divisibilidade, serem poucos trabalhados na Educação Básica, nosso propósito, neste trabalho, é destacar que problemas relacionados à Teoria dos Números possuem um potencial motivador nos processos de ensino e de aprendizagem, bem como na formação do pensamento conceitual matemático. Se trabalhada de forma contextualizada a Teoria dos Números é ferramenta para o professor elaborar diferentes atividades, com vistas a desafiar os alunos e consolidar o aprendizado.

Dessa forma, o objetivo deste trabalho é estudar as principais aplicações da congruência modular. A congruência modular é frequentemente utilizada em situações cotidianas, muitas vezes desconhecidas pelas pessoas, como por exemplo para gerar diferentes códigos numéricos de identificação, como códigos de barras, números dos documentos de identidade, Cadastro

de Pessoa Física (CPF)[1], International Standard Book Number (ISBN), International Standard Serial Number (ISSN), criptografia, calendários e diversos fenômenos periódicos.

Diante do exposto, estruturamos o trabalho da seguinte forma: no segundo capítulo, apresentamos os conceitos iniciais relevantes ao tema, abordando as propriedades dos números inteiros, divisibilidade, divisão Euclidiana e por fim os critérios de congruência, com demonstrações e exemplos. No terceiro capítulo, versamos sobre as principais aplicações de congruências modulares em sistemas de identificação e validação dos dados, evidenciando a composição numérica dos códigos de barras e do CPF, bem como demonstração do uso de congruência modular na validação de códigos numéricos e aplicações com calendários.

Por fim, no quarto capítulo, apresentamos como utilizar o tema para o Ensino e a aprendizagem de matemática. Para tanto, propomos algumas atividades como possibilidades para nortear o trabalho do docente da Educação Básica. O propósito foi promover a discussão sobre a aplicação matemática dos restos, tendo como base, ou ponto de partida, temas relacionados ao cotidiano dos alunos e recomendados pela Base Nacional Comum Curricular (BNCC).

[1] https://www.gov.br/receitafederal/pt-br/assuntos/meu-cpf

CAPÍTULO

2

ALGUNS CONCEITOS FUNDAMENTAIS

Para compreendermos o uso de dígitos verificadores, calendários e aplicações precisamos conhecer algumas propriedades dos números inteiros, em especial, congruências. Neste capítulo apresentaremos alguns teoremas básicos que serão utilizados no decorrer deste trabalho juntamente com alguns resultados preliminares. Destacam-se os teoremas relacionados à divisibilidade, divisão euclidiana, dentre outras definições importantes.

2.1 Números Inteiros

Assim como as demais ciências, a Matemática é uma herança da humanidade desenvolvida desde a pré-história, quando os criadores de ovelha correlacionavam pedras a quantidade de ovelhas. Nos dias de hoje, observa-se a Matemática presente na tecnologia digital, na Medicina, na Engenharia, assim como em tantas outras profissões (NERIS *et al.*, 2021).

De acordo com Medeiros e Medeiros (1992), a origem dos números negativos é incerta. Segundo Anjos (2008), os chineses diferenciavam números positivos e negativos usando barras pretas representando os positivos e barras vermelhas representando os negativos. Possivelmente, eles trabalhavam dessa forma por causa de sua filosofia muito forte de opostos. Desta forma, os números negativos eram usados apenas como intermediários na execução de algum algoritmo ou interpretação de alguma situação problema. Já na matemática grega, não existia a ideia de número negativo, pois, para os gregos, a negatividade poderia ser propriedade da unidade e não do número.

Outras civilizações também tiveram suas contribuições quanto aos números inteiros, como a civilização hindu, por exemplo. A matemática hindu é reconhecida historicamente pelo trato sistemático dos números negativos, que aparecem de forma explicita na obra de Brahmagupta (628 d.C. aproximadamente), na qual são interpretados como dívidas (MILIES; COELHO, 2001). Na visão de Scalabrin, Lopes e Pozebon (2021) os árabes rejeitavam as

raízes negativas e grandezas negativas, porém, faziam uso de regras semelhantes ao que hoje conhecemos como regra de sinais e os gregos conheciam as grandezas negativas através dos seus teoremas geométricos.

Na Itália no século XIV, o surgimento de um sistema bancário propiciou a utilização de números negativos (MEDEIROS; MEDEIROS, 1992). Para Schubring (2007) foi Carnot (1753-1823) que empreendeu pela primeira vez uma análise sistemática das diversas provas da regra de sinais que, em 1867, possibilitou ao alemão Hermann Hankel (1839-1873) dar legitimidade aos números negativos, publicando "Teoria do Sistema dos números Complexos". Foi Dedekind (1831-1916), amigo de George Cantor (1845-1918), que fez referência da subtração como inversa da adição: $a-b=c-d$, logo $a+d=c+b$, demonstrando que esta relação é de equivalência, e o conjunto das classes de equivalência será o conjunto dos números Inteiros (TALAVERA, 2001).

Iniciamos alguns conceitos fundamentais para o desenvolvimento de aplicações com congruências. Cumpre destacar que os dados deste capítulo baseiam-se nas definições dos livros: Aritmética de (HEFEZ, 2016), Álgebra Moderna de (DOMINGUES; IEZZI, 2003), Números: Uma introdução à Matemática de (MILIES; COELHO, 2001) e Elementos de Matemática - Notas de Aula de (DIAS; GODOY, 2012).

No conjunto dos **Números Inteiros**, denotado por $\mathbb{Z}$,

$$\mathbb{Z}=\{\ldots,\ -4,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \ldots\},$$

temos duas operações definidas, adição $(+)$ e multiplicação $(\cdot)$:

- $(+)$: $(a,b)\to a+b$
- $(\cdot)$: $(a,b)\to a\cdot b$

Em $\mathbb{Z}$ temos o subconjunto dos Números Naturais, denotado por $\mathbb{N}$,

$$\mathbb{N}=\{1,\ 2,\ 3,\ \ldots\}.$$

Escreveremos de forma axiomática algumas propriedades básicas do conjunto dos números inteiros, com essas duas operações.

Axioma 1. Associatividade da Adição

Para todos a,b,c inteiros temos que:

$$a+(b+c)=(a+b)+c.$$

Axioma 2. Comutatividade da Adição

Para todos a e b inteiros, temos que:

$$a+b=b+a.$$

Axioma 3. Elemento Neutro da Adição

Existe um único elemento, chamado de **zero**, indicado por 0, tal que, para todo inteiro a:

$$a+0=a.$$

Axioma 4. Elemento Oposto

Para cada a inteiro, existe um único elemento, chamado de **oposto** de a, indicado por $-a$, tal que:

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

Axioma 5. Associatividade da Multiplicação

Para todos a,b,c inteiros temos que:

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

Axioma 6. Comutatividade da Multiplicação

Para todos a e b inteiros, temos que:

$$a\cdot b=b\cdot a.$$

Axioma 7. Elemento Neutro da Multiplicação

Para todo a inteiro, existe um único **elemento neutro multiplicativo**, diferente de zero, indicado por 1, tal que:

$$1\cdot a=a.$$

Axioma 8. Lei do Cancelamento da Adição

Para todos a, b e c inteiros, temos que:

$$\text{Se } a+b=a+c, \text{ então, } b=c.$$

Axioma 9. Lei do Cancelamento da Multiplicação

Para todos a, b e c inteiros, com $a\neq 0$, temos que:

$$\text{Se } a\cdot b=a\cdot c, \text{ então, } b=c.$$

Axioma 10. Distributiva

Para todos a,b,c inteiros temos que:

$$a\cdot(b+c)=a\cdot b+a\cdot c.$$

2.2 Divisibilidade

Uma equação do tipo $a \cdot x = b$, com $a, b \in \mathbb{Z}$ e $a \neq 0$, pode ou não ter solução nos inteiros. Os casos em que tem solução em $\mathbb{Z}$ são estudados de maneira especial.

Definição 1. Sejam a e b inteiros. Dizemos que a **divide** b, se existir $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Também denotamos tal número inteiro c por $\frac{b}{a}$. Quando não existir um inteiro c tal que $b = a \cdot c$ dizemos que a **não divide** b.

Usamos a notação $a \mid b$ para indicar que a divide b e $a \nmid b$ quando a não divide b.

Exemplo 1.

- $4 \mid 24$, pois $4 \cdot 6 = 24$;
- $7 \mid 63$, pois $7 \cdot 9 = 63$;
- $3 \nmid 10$, pois não existe $c \in \mathbb{Z}$ tal que $3 \cdot c = 10$.

No próximo resultado apresentaremos as propriedades básicas da relação de divisibilidade, juntamente com suas demonstrações.

Teorema 1. Para quaisquer $a, b, c, d, m, n \in \mathbb{Z}$, temos:

i) Para $a \neq 0$, temos $a \mid a$, $1 \mid a$ e $a \mid 0$.

Demonstração. Note que as seguintes igualdades são verdadeiras:

$$\begin{aligned} a &= a \cdot 1; \\ a &= 1 \cdot a; \\ 0 &= 0 \cdot a. \end{aligned}$$

As igualdades acima mostram, respectivamente, que $a \mid a$, $1 \mid a$ e $a \mid 0$. ■

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

Demonstração. Se $a \mid b$ e $b \mid c$, então existem $x, y \in \mathbb{Z}$ tais que $b = a \cdot x$ e $c = b \cdot y$.

Substituindo b na segunda sentença, temos:

$$\begin{aligned} c = b \cdot y &\implies \\ c &= (a \cdot x) \cdot y \\ &= a \cdot (x \cdot y). \end{aligned}$$

Como $x \cdot y \in \mathbb{Z}$, obtemos $a \mid c$. ■

iii) Se $a \mid b$ e $c \mid d$, então $a \cdot c \mid b \cdot d$.

Demonstração. Se $a \mid b$ e $c \mid d$, então existem $x, y \in \mathbb{Z}$ tais que $b = a \cdot x$ e $d = c \cdot y$. Obtemos então:

$$\begin{aligned} b = a \cdot x \text{ e } d = c \cdot y &\implies \\ b \cdot d &= (a \cdot x) \cdot (c \cdot y) \\ &= (a \cdot c) \cdot (x \cdot y). \end{aligned}$$

Como $x \cdot y \in \mathbb{Z}$, temos $a \cdot c \mid b \cdot d$. ■

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

Demonstração. Se $a \mid b$ e $a \mid c$, então existem $x, y \in \mathbb{Z}$ tais que $b = a \cdot x$ e $c = a \cdot y$. Somando as duas sentenças temos:

$$b + c = a \cdot x + a \cdot y = a \cdot (x + y) .$$

Como $x + y \in \mathbb{Z}$, temos $a \mid (b + c)$. ■

v) Se $a \mid b$, então $a \mid m \cdot b$, para todo $m \in \mathbb{Z}$.

Demonstração. Se $a \mid b$, então existe $x \in \mathbb{Z}$ tal que $b = a \cdot x$. Para $m \in \mathbb{Z}$, temos:

$$\begin{aligned} b = a \cdot x &\implies \\ b \cdot m = (a \cdot x) \cdot m &= a \cdot (x \cdot m). \end{aligned}$$

Como $x \cdot m \in \mathbb{Z}$, obtemos $a \mid m \cdot b$, para todo $m \in \mathbb{Z}$. ■

vi) Se $a \mid b$ e $a \mid c$, então $a \mid (m \cdot b + n \cdot c)$, para todo m e $n \in \mathbb{Z}$.

Demonstração. Se $a \mid b$ e $a \mid c$, então existem $x, y \in \mathbb{Z}$ tais que $b = a \cdot x$ e $c = a \cdot y$. Para m e $n \in \mathbb{Z}$ temos:

$$\begin{aligned} b = a \cdot x &\implies b \cdot m = a \cdot x \cdot m \\ &\text{e} \\ c = a \cdot y &\implies c \cdot n = a \cdot y \cdot n . \end{aligned}$$

Somando obtemos:

$$b \cdot m + c \cdot n = a \cdot x \cdot m + a \cdot y \cdot n = a(x \cdot m + y \cdot n).$$

Como $x, y, m, n \in \mathbb{Z}$, temos $(x \cdot m + y \cdot n) \in \mathbb{Z}$, logo $a \mid (m \cdot b + n \cdot c)$. ■

2.2.1 Divisão Euclidiana

Dados dois números inteiros a e b, com $b \neq 0$, sempre podemos pensar na divisão de a por b, admitindo que pode sobrar um resto. Esse processo é o que chamamos de Divisão Euclidiana. Do próximo resultado mostraremos que sempre podemos fazer essa divisão de forma única.

Nesse resultado usaremos a relação de ordem definida nos inteiros.

Teorema 2 (**Algoritmo da Divisão**)**.** Para quaisquer inteiros a e b com $b \neq 0$, existem e são únicos os inteiros q e r tais que $a = q \cdot b + r$, onde $0 \leq r <\mid b \mid$.

Demonstração. Mostraremos primeiro a existência dos números q e r. Dados a e $b \in \mathbb{Z}$, com $b > 0$, consideremos o conjunto

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

Para $x = - \mid a \mid$, temos $a - b \cdot x = a - b(- \mid a \mid) = a + b \mid a \mid \geq 0$, pois $b > 0$ e $b \mid a \mid \geq a$.

Ou seja, $a - b \cdot x \in S$, logo $S \neq \emptyset$.

Pelo Princípio da Boa Ordenação[1] existe $min(S) = r$. Como $r \in S$, $r = a - b \cdot q \geq 0$, para algum $q \in \mathbb{Z}$.

Resta provar que $r < b$. Suponhamos por absurdo que $r \geq b$.

Para $x = q + 1$, temos que

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

Como $b > 0$, $r - b < r = min(S)$, o que contradiz a minimalidade de r. Portanto $r < b$.

Consideremos agora $b < 0$. Para todo $a \in \mathbb{Z}$, existem q' e $r' \in \mathbb{Z}$, tais que $a =\mid b \mid q' + r'$, com $0 \leq r' <\mid b \mid$. Ou seja, $a = (-b)q' + r' = b(-q') + r'$, então basta tomarmos $q = -q'$ e $r = r'$, e o resultado segue.

Mostraremos agora a unicidade dos números inteiros q e r. Suponhamos que existam q, q', r e r', tais que $a = q \cdot b + r$ com $0 \leq r <\mid b \mid$ e $a = q' \cdot b + r'$ com $0 \leq r' <\mid b \mid$. Então

$$\begin{aligned} b \cdot q' + r' = b \cdot q + r &\implies \\ r' - r = b \cdot q - b \cdot q' &\implies \\ r' - r = b(q - q') &\implies \\ \mid r' - r \mid =\mid b(q - q') \mid &\implies \\ \mid r' - r \mid =\mid b \mid\mid (q - q') \mid . & \end{aligned}$$

[1] Princípio da Boa Ordem: Todo conjunto não vazio de inteiros não negativos tem um menor elemento.

Por hipótese, $0 \leq r <\mid b \mid$, e $0 \leq r' <\mid b \mid$, logo

$$\begin{gathered} -\mid b \mid < -r' < 0 \text{ e } 0 < r <\mid b \mid \Longrightarrow \\ -\mid b \mid < r - r' <\mid b \mid \Longrightarrow \\ \mid r' - r \mid <\mid b \mid , \end{gathered}$$

consequentemente $\mid b \mid\mid (q - q') \mid <\mid b \mid$.

Se $q \neq q'$, então $\mid q - q' \mid \geq 1$, o que implica $b > b$, o que é um absurdo. Logo $q = q'$.

De $\mid r - r' \mid = b \mid (q - q') \mid$, temos $\mid r - r' \mid = 0$, o que implica que $r = r'$, como queríamos. ■

Definição 2. Os números q e r determinados no Teorema 2 são chamados, respectivamente, **quociente** e **resto** da divisão de a por b.

Definição 3. Sejam a e b inteiros e $b \neq 0$, dizemos que $\left[\frac{a}{b}\right]$ é a **parte inteira** do razão $\frac{a}{b}$.

Proposição 1. Sejam a e b inteiros e $b > 0$, $\left[\frac{a}{b}\right] = q$ é o quociente da divisão euclidiana de a por b.

Demonstração. Seja a divisão euclidiana de a por b:

$$a = b \cdot q + r, \text{ com } 0 \leq r < b. \tag{2.1}$$

Dividindo (2.1) por b, obtemos:

$$\frac{a}{b} = q + \frac{r}{b}, \text{ com } 0 \leq \frac{r}{b} < 1.$$

Pelo Teorema 2 $q \in \mathbb{Z}$ e único, temos que a parte inteira é q. ■

Exemplo 2. $\left[\frac{5}{3}\right] = 1$, pois $5 = 3 \cdot 1 + 2$.

Observação 1. De modo geral, se $a \neq 0$ e $a < b$, o número de múltiplos não nulos de a menores ou iguais a b é igual ao quociente da divisão de b por a, ou seja, é igual a parte inteira $\left[\frac{b}{a}\right]$ do racional $\frac{b}{a}$.

Proposição 2. Dados a, b e c tais que $0 < a < b < c$, então o número de múltiplos de a entre b e c é dado por:

a) $\left[\frac{c}{a}\right] - \left[\frac{b}{a}\right]$, se excluir b na contagem.

Demonstração. O resultado segue diretamente da Proposição 1, calculamos os múltiplos não nulos de a menores ou iguais a c e subtraímos os múltiplos de a não nulos menores ou iguais a b, respectivamente $\left[\frac{c}{a}\right]$ e $\left[\frac{b}{a}\right]$. ■

b) $\left[\frac{c}{a}\right] - \left[\frac{b-1}{a}\right]$, se incluir b na contagem.

Demonstração. Como $\left[\frac{c}{a}\right]$ é o número de múltiplos de a entre 1 e c, devemos subtrair os múltiplos de a anteriores a b, ou seja, $\left[\frac{b-1}{a}\right]$. ■

2.3 Congruência

A aritmética modular foi introduzida pela primeira vez no livro *Disquisitiones Aritmeticae* escrito por Carl Friedrich Gauss e publicado em 1801. Utilizada até os dias de hoje, **congruência** é uma linguagem que visa simplificar a divisibilidade de números inteiros. É um conceito muito importante relacionado a divisibilidade e os restos da divisão euclidiana.

Definição 4. Seja $m \neq 0$ um número inteiro fixo e a, b inteiros. Dizemos a é **côngruo** a b **módulo** m se os restos de sua divisão euclidiana por m são iguais.

Usamos a notação $a \equiv b \bmod m$.

Exemplo 3. $7 \equiv 33 \bmod 2$, pois os restos da divisão de 7 e 33 por 2 são iguais a 1.

Um modo mais eficaz de verificarmos a congruência modulo m entre dois números, ao invés de ficarmos comparando os restos da divisão euclidiana por m, é utilizando o resultado a seguir.

Teorema 3. Sejam a e $b \in \mathbb{Z}$ e $m \in \mathbb{N}$, dizemos que $a \equiv b \bmod m$ se, e somente se, $a-b$ é divisível por m.

Demonstração. ($\Rightarrow$) Considere a divisão euclidiana de a e b, respectivamente, por m: $a = m \cdot q + r$, com $0 \leq r < m$ e $b = m \cdot q' + r'$, com $0 \leq r' < m$. Como $a \equiv b \bmod m$, pela Definição 4, temos que os restos r e r' são iguais, calculando então $a-b$

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

Logo $m \mid a-b$.

($\Leftarrow$) Note que o fato de $a-b$ ser divisível por m temos:

$$\begin{aligned} a - b &= (m \cdot q + r) - (m \cdot q' + r') \\ &= m(q - q') + r - r'. \end{aligned} \tag{2.2}$$

Como $a-b$ é divisível por m e $m(q-q')$ também, temos que $m \mid r-r'$. Como $-m < r-r' < m$ e neste intervalo o único valor divisível por m é 0, temos $r-r'=0$, o que implica que $r=r'$.

Portanto a e b deixam os mesmos restos quando divididos por m. ■

Exemplo 4. $5 \equiv 12 \bmod 7$, pois $7 \mid (5-12)$.

Observação 2. Na divisão de um inteiro a por m, obtêm-se $k \in \mathbb{Z}$ e $0 \leq r < m$, tal que $a = m \cdot k + r$, logo $a - r = m \cdot k$, o que implica que $a \equiv r \bmod m$, ou seja, todo inteiro é congruente módulo m ao resto de sua divisão por m.

Exemplo 5. $12 \equiv 2 \bmod 5$, pois o resto da divisão de 12 por 5 é 2.

Da definição de congruência módulo m, as proposições abaixo nos mostram que esta é uma relação de equivalência em $\mathbb{Z}$.

Proposição 3. Seja $m > 0$ um inteiro fixo. Para todos $a,\ b,\ c \in \mathbb{Z}$, tem-se que:

i) **Reflexiva:** $a \equiv a \bmod m$.

Demonstração. Pelo Teorema 1, note que $m \mid 0 = a - a$, então $a \equiv a \bmod m$. ■

ii) **Simétrica:** $a \equiv b \bmod m$, então $b \equiv a \bmod m$.

Demonstração. Pelo Teorema 3, temos que $m \mid a-b$, logo $a-b = m \cdot k$, $k \in \mathbb{Z}$. Multiplicando ambos os membros por (-1) obtemos $-(a-b) = -(m \cdot k)$, ou seja, $b-a = m \cdot (-k)$. Portanto $m \mid b-a$, equivalentemente $b \equiv a \bmod m$. ■

iii) **Transitiva:** $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$.

Demonstração. Pelo Teorema 3 temos que

$$m \mid a-b \ \Rightarrow\ a-b = m \cdot k,\ k \in \mathbb{Z}, \tag{2.3}$$

$$m \mid b-c \ \Rightarrow\ b-c = m \cdot k',\ k' \in \mathbb{Z}. \tag{2.4}$$

Efetuando a adição de (2.3) e (2.4), então

$$a - c = (a-b) + (b-c) = m \cdot k - m \cdot k' = m(k-k').$$

Portanto $m \mid a-c$, equivalentemente $a \equiv c \bmod m$. ■

Veremos adiante mais propriedades interessantes da relação de congruência.

Proposição 4. Seja $m > 0$ um inteiro fixo. Para todos $a,\ b,\ c \in \mathbb{Z}$, temos as seguintes propriedades:

i) Se $a \equiv b \bmod m$, então $a \pm c \equiv b \pm c \bmod m$.

Demonstração. Se $a \equiv b \bmod m$, então $m \mid a-b$. Note que $a-b = (a \pm c) - (b \pm c)$, o que implica que $m \mid (a \pm c) - (b \pm c)$, equivalentemente $a \pm c \equiv b \pm c \bmod m$. ■

ii) Se $a \equiv b \bmod m$, então $a \cdot c \equiv b \cdot c \bmod m$.

Demonstração. Se $a \equiv b \bmod m$, então $m \mid a-b$, logo temos que existe $k \in \mathbb{Z}$ tal que $a-b = m \cdot k$, multiplicando a sentença por c, temos $a \cdot c - b \cdot c = (a-b)c = m \cdot k \cdot c = m(k \cdot c)$, ou seja $m \mid a \cdot c - b \cdot c$, equivalentemente $a \cdot c \equiv b \cdot c \bmod m$. ■

iii) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a \pm c \equiv b \pm d \bmod m$.

Demonstração. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então do Item i) temos $a \pm c \equiv b \pm c \bmod m$ e $b \pm c \equiv b \pm d \bmod m$. Da transitividade, Proposição 3, temos então $a \pm c \equiv b \pm d \bmod m$. ■

iv) Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a \cdot c \equiv b \cdot d \bmod m$.

Demonstração. Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então do Item ii) temos $a \cdot c \equiv b \cdot c \bmod m$ e $b \cdot c \equiv b \cdot d \bmod m$. Da transitividade, temos então $a \cdot c \equiv b \cdot d \bmod m$. ■

v) Se $a \equiv b \bmod m$ e $r \geq 1 \in \mathbb{Z}$, então $a^r \equiv b^r \bmod m$.

Demonstração. Sejam a, b, m e r números inteiros com $m \geq 0$ e $r \geq 1$ tais que $a \equiv b \bmod m$, ou seja, $m \mid b-a$.

Vamos mostrar por indução sobre r que $a^r \equiv b^r \bmod m$.

(I) Se $r = 1$, então $a^1 \equiv b^1 \bmod m$, pois $m \mid b-a$.

(II) Se $a^r \equiv b^r \bmod m$, então

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

Como $m \mid b-a$ e por hipótese de indução $m \mid b^r - a^r$, temos que $m \mid b^r(b-a) + a(b^r - a^r) = b^{r+1} - a^{r+1}$. Logo $a^{r+1} \equiv b^{r+1} \bmod m$.

Assim, pelo princípio da indução, $a^r \equiv b^r \bmod m$, para todo $r \geq 1$. ■

Proposição 5. O resto da divisão de $a+b$ por $m>1$ depende apenas dos restos da divisão de a e de b por m.

Demonstração. Sejam a e $b \in \mathbb{Z}$ cujos restos da divisão por m sejam respectivamente r_1 e r_2, então $a \equiv r_1 \mod m$ e $b \equiv r_2 \mod m$, logo pelo Item iii), $a+b \equiv r_1+r_2 \mod m$. Seja $0 \leq r < m$ o resto da divisão de r_1+r_2 por m, então $a+b \equiv r_1+r_2 \equiv r \mod m$. ■

Proposição 6. O resto da divisão de $a \cdot b$ por $m>1$ depende apenas dos restos da divisão de a e de b por m.

Demonstração. Sejam a e $b \in \mathbb{Z}$ cujos restos da divisão por m sejam respectivamente r_1 e r_2, então $a \equiv r_1 \mod m$ e $b \equiv r_2 \mod m$, logo pelo Item iv), $a \cdot b \equiv r_1 \cdot r_2 \mod m$. Seja $0 \leq r < m$ o resto da divisão de $r_1 \cdot r_2$ por m, então $a \cdot b \equiv r_1 \cdot r_2 \equiv r \mod m$. ■

CAPÍTULO

3

ALGUMAS APLICAÇÕES DE CONGRUÊNCIA

3.1 Dígitos Verificadores

Desde as civilizações antigas havia a necessidade de que os objetos fossem identificados de forma única e segura. Hoje, com a disseminação tecnológica crescente a cada dia, a troca de informações na Internet[1] deve ser feita de forma fidedigna aos dados reais. Para a segurança dessas informações é utilizado a Criptografia[2] e para identificação de pessoas, produtos, documentos etc são utilizados códigos numéricos identificados de forma única. Para a validação desses códigos, por conseguinte, são utilizados os Dígitos verificadores, os DV-S.

Dígito(s) verificador(es) ou número de controle é um sistema de autenticação usado para a validação da autenticidade de valor numérico ou alfanumérico a fim de evitar/detectar fraudes, erros de transmissão, digitação, entre outros. O dígito verificador é gerado por um algoritmo específico, a partir dos dígitos anteriores. Para cada padrão de código tem-se o seu algoritmo.

Os principais erros são cometidos pelos humanos na digitação. Esses erros foram categorizados por Verhoeff (1969) na Tabela 1, juntamente com suas frequências.

A seguir trabalharemos com alguns exemplos mais corriqueiros, nos quais são empregados os Dígitos Verificadores. Para facilitar nossa notação, as sequências de códigos numéricos aqui trabalhadas serão representadas por uma n-upla[3].

Seja $a_1a_2a_3\ldots a_n$ uma sequência, então esta será denotada pela n-upla $\alpha = (a_1, a_2, a_3, \ldots, a_n)$. Os dígitos verificadores são obtidos a partir de cálculos por um algoritmo e um vetor fixo, também chamado de vetor de verificação, $\beta = (b_1, b_2, b_3, \ldots, b_n)$. No algoritmo

[1] Sistema estruturado em escala mundial para uso público e irrestrito, constituído por uma coleção de "redes" definidas como Sistemas Autônomos que se relacionam por meio da arquitetura de protocolos TCP/IP (CGI, 2018).

[2] A palavra Criptografia é originária do grego e é formada por duas partes: kryptós, que significa "segredo" e logia, "estudo" (SILVA, 2019).

[3] Uma n-upla, (1, 2, 3, ..., n), é uma sequencia ordenada de n elementos.

Tabela 1 – Tipos de erros e suas frequências

Tipo de Erro	Formato	Frequência (%)
Únicos	$\ldots a \ldots \longmapsto \ldots b \ldots$	79.00
Transposição adjacente	$\ldots ab \ldots \longmapsto \ldots ba \ldots$	10.20
Transposição alternada	$\ldots abc \ldots \longmapsto \ldots cba \ldots$	0.80
Gêmeos	$\ldots aa \ldots \longmapsto \ldots bb \ldots$	0.60
Gêmeos alternado	$\ldots aba \ldots \longmapsto \ldots cbc \ldots$	0.30
Outros		9.10

α e β são multiplicados termo a termo de mesmo índice e posteriormente somados, resultando em um inteiro.

$$\begin{aligned} \alpha \cdot \beta &= (a_1, a_2, a_3, \ldots, a_n) \cdot (b_1, b_2, b_3, \ldots, b_n) \\ &= a_1 \cdot b_1 + a_2 \cdot b_2 + a_3 \cdot b_3 + \ldots + a_n \cdot b_n \\ &= k; k \in \mathbb{Z}. \end{aligned}$$

3.2 Código de Barras

A aplicação de congruências trouxe grande contribuição para o mundo moderno, como a verificação do código de barras capaz de identificar produtos mundialmente utilizados e tentar evitar erros. O código é composto por uma sequência numérica, que foi evoluindo conforme a necessidade humana.

Um dos códigos de barras mais usado no mundo é a Numeração Européia de Artigos, do inglês European Article Number (EAN-13), sucessor do antigo Código de Produto Universal, do inglês Universal Product Code (UPC), constituído de treze dígitos $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}$, conforme Figura 1:

Figura 1 – Código de barras - Chocolate Lacta

Fonte: Elaborada pelo autor.

Os doze primeiros são determinados a cargo da unidade responsável de cada país, sendo que o último é o dígito de controle, ou seja, é determinado com base nos dígitos iniciais.

Os dígitos do código de barras EAN-13 são alternadamente multiplicados por um e três e pelo algoritmo para realizar a verificação da sequência: este é o vetor verificador.

$$(1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1).$$

Posteriormente essas multiplicações são somadas e deverá ser um múltiplo de dez, ou seja, congruente a zero módulo dez, caso contrário houve um erro na leitura ou digitação do código.

Sendo α a n-upla correspondente ao código de barras e o β o vetor de verificação, temos:

$$\alpha = (a_1,\ a_2,\ a_3,\ \ldots,\ a_{11},\ a_{12},\ a_{13}) \text{ e}$$
$$\beta = (1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1,\ 3,\ 1).$$

Calculamos o produto membro a membro de α com β e somando-os:

$$\begin{aligned}\alpha\cdot\beta &= (a_1,a_2,\ldots,a_{12},a_{13})\cdot(1,3,1,3,1,3,1,3,1,3,1,3,1)\\ &= a_1+3\cdot a_2+a_3+3\cdot a_4+a_5+3\cdot a_6+a_7+3\cdot a_8+a_9+3\cdot a_{10}+a_{11}+3\cdot a_{12}+a_{13}.\end{aligned}$$

Então a_{13} é determinado de tal modo que a soma seja um múltiplo de dez, ou seja:

$$\alpha\cdot\beta \equiv 0 \bmod 10.$$

Exemplo 6. Considere o código de barras do chocolate na Figura 1, 7622300991500, e chamemos o dígito verificador, no caso 0, de a_{13}.

Sendo a_{13} o dígito verificador, temos a n-upla $\alpha = (7,6,2,2,3,0,0,9,9,1,5,0,a_{13})$ representando o código de barras e calculando o produto pelo vetor de verificação β, temos:

$$\begin{aligned}\alpha\cdot\beta &= (7,6,2,2,3,0,0,9,9,1,5,0,a_{13})\cdot(1,3,1,3,1,3,1,3,1,3,1,3,1)\\ &= 7+(6\cdot3)+2+(2\cdot3)+3+(0\cdot3)+0+(9\cdot3)+9+(1\cdot3)+5+(0\cdot3)+a_{13}\\ &= 7+18+2+6+3+27+9+3+5+a_{13}\\ &= 80+a_{13},\end{aligned}$$

então

$$\begin{aligned}80+a_{13} &\equiv 0 \bmod 10 \implies\\ a_{13} &\equiv 0 \bmod 10.\end{aligned}$$

Como a_{13} é um dígito, $a_{13} \in \{0,1,2,...,8,9\}$, logo $a_{13} = 0$. O que confere com o dígito da Figura 1.

3.3 CPF - Cadastro de Pessoas Físicas

O CPF é um documento brasileiro feito pela Receita Federal que armazena informações cadastrais de contribuintes e tem a finalidade de identificar os cidadãos. Composto por uma numeração com onze dígitos, conforme a Figura 2, o CPF é único e exclusivo para cada pessoa e só pode ser modificado mediante decisão judicial. Não há idade mínima para a inscrição e é permitida a brasileiros ou estrangeiros, residentes no Brasil ou exterior.

Figura 2 – Comprovante de inscrição no CPF

Fonte: https://auniao.pb.gov.br/

Dos onze dígitos do CPF, os dois últimos são dígitos verificadores, os quais são determinados a partir dos números anteriores e calculados um de cada vez. O décimo dígito, a_{10}, é o primeiro verificador e é o resultado de uma congruência módulo 11 com os nove dígitos anteriores. O décimo primeiro dígito, a_{11}, é o segundo verificador, determinado a partir dos anteriores através de outra congruência módulo 11, já incluindo o décimo dígito encontrado. Para cada verificação, é utilizado um vetor verificador específico, que veremos adiante.

Seja $a_1a_2a_3\ldots a_9a_{10}a_{11}$ os dígitos de um CPF, então:

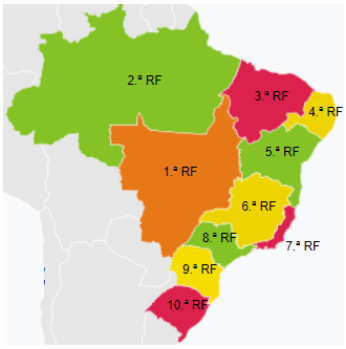
- $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8$ são os números base;
- a_9 representa a região fiscal onde a pessoa fez o registro;
- a_{10} e a_{11} são dígitos verificadores.

A Região Fiscal onde é emitido o CPF tem a identificação segundo a Tabela 2 e o mapa da Figura 3.

Tabela 2 – Código da região fiscal do CPF

1 - DF, GO, MS, MT e TO	5 - BA e SE	9 - PR e SC
2 - AC, AM, AP, PA, RO e RR	6 - MG	0 - RS
3 - CE, MA e PI	7 - ES e RJ	
4 - AL, PB, PE, RN	8 - SP	

Figura 3 – Região fiscal do CPF no mapa



Fonte: http://clubes.obmep.org.br/blog/a-matematica-nos-documentos-cpf/

Podem existir casos específicos em que esse nono dígito não esteja de acordo com os determinados acima.

O primeiro vetor de verificação do CPF é

$$\beta_1 = (10,9,8,7,6,5,4,3,2,1),$$

e após encontrarmos o décimo dígito, aplicamos o vetor de verificação

$$\beta_2 = (11,10,9,8,7,6,5,4,3,2,1).$$

Seja $\alpha = (a_1,a_2,a_3,...,a_9,a_{10},a_{11})$ nossa n-upla correspondente ao CPF, β_1 e β_2 os vetores de verificações. Calculamos o dígito a_{10} utilizando o vetor de verificação β_1 e posteriormente o dígito a_{11} com o vetor β_2.

Sendo α' a n-upla correspondente ao CPF suprimido do dígito a_{11}, calculamos o produto escalar:

$$\begin{aligned}\alpha' \cdot \beta_1 &= (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10}) \cdot (10,9,8,7,6,5,4,3,2,1) \\ &= 10 \cdot a_1 + 9 \cdot a_2 + 8 \cdot a_3 + 7 \cdot a_4 + 6 \cdot a_5 + 5 \cdot a_6 + 4 \cdot a_7 + 3 \cdot a_8 + 2 \cdot a_9 + a_{10}.\end{aligned}$$

Então a_{10} é determinado de tal modo que a soma acima seja um múltiplo de 11, ou seja:

$$\alpha' \cdot \beta_1 \equiv 0 \bmod 11.$$

Como temos uma congruência módulo 11, quando o resto for dez, por regra, é considerado zero. E quando o resto for zero, também utilizamos zero.

Analogamente ao algoritmo anterior, calculamos o último dígito utilizando o vetor de verificação β_2. Temos α a n-upla do CPF, agora com a_{10} já definido anteriormente, calculamos o produto com o vetor β_2:

$$\begin{aligned}\alpha \cdot \beta_2 &= (a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8,a_9,a_{10},a_{11}) \cdot (11,10,9,8,7,6,5,4,3,2,1) \\ &= 11 \cdot a_1 + 10 \cdot a_2 + 9 \cdot a_3 + 8 \cdot a_4 + 7 \cdot a_5 + 6 \cdot a_6 + 5 \cdot a_7 + 4 \cdot a_8 + 3 \cdot a_9 + 2 \cdot a_{10} + a_{11}.\end{aligned}$$

Então a_{11} é determinado de tal modo que a soma acima seja um múltiplo de 11, ou seja:

$$\alpha \cdot \beta_2 \equiv 0 \bmod 11.$$

Em ambas as congruências acima buscamos o menor número inteiro que seja solução. Para este caso em especial, como no primeiro passo, se o resultado da congruência for o valor dez, devemos substitui-lo por zero.

Exemplo 7. Vejamos se o CPF da Figura 2, $250.991.832-04$, é um número válido. É importante salientar que não necessariamente é um CPF oficial do banco de dados da Receita Federal, apenas é um número que pode ou não cumprir os requisitos de validação.

Vamos primeiramente determinar a_{10}, o primeiro dígito verificador. Da n-upla tem-se que:

$$\alpha' = (2,5,0,9,9,1,8,3,2,a_{10}),$$

e calculando o algoritmo com o vetor de verificação β_1:

$$\begin{aligned}\alpha' \cdot \beta_1 &= (2,5,0,9,9,1,8,3,2,a_{10}) \cdot (10,9,8,7,6,5,4,3,2,1) \\ &= 2\cdot 10+5\cdot 9+0\cdot 8+9\cdot 7+9\cdot 6+1\cdot 5+8\cdot 4+3\cdot 3+2\cdot 2+a_{10} \\ &= 20+45+0+63+54+5+32+9+4+a_{10} \\ &= 232+a_{10},\end{aligned}$$

então temos a congruência

$$\begin{aligned}232+a_{10} &\equiv 0 \bmod 11 \implies \\ 1+a_{10} &\equiv 0 \bmod 11.\end{aligned}$$

Logo $a_{10} = 10$, mas como regra mencionada acima, a_{10} será substituído por zero.

Incluímos o zero como o primeiro verificador do CPF, $\alpha = (2,5,0,9,9,1,8,3,2,0,a_{11})$ e calculamos o produto escalar com o vetor de verificação β_2 para determinar a_{11}:

$$\begin{aligned}\alpha \cdot \beta_2 &= (2,5,0,9,9,1,8,3,2,0,a_{11}) \cdot (11,10,9,8,7,6,5,4,3,2,1) \\ &= 2\cdot 11+5\cdot 10+0\cdot 9+9\cdot 8+9\cdot 7+1\cdot 6+8\cdot 5+3\cdot 4+2\cdot 3+0\cdot 2+a_{11} \\ &= 22+50+0+72+63+6+40+12+6+0+a_{11} \\ &= 271+a_{11},\end{aligned}$$

então temos a congruência

$$\begin{aligned}271+a_{11} &\equiv 0 \bmod 11 \implies \\ 7+a_{11} &\equiv 0 \bmod 11.\end{aligned}$$

Logo $a_{11} = 4$, o segundo dígito verificador é quatro. Portanto o CPF da Figura 2 é validado pelo algoritmo.

3.4 ISBN-13: International Standard Book Number

O ISBN é um sistema internacional padronizado que identifica numericamente os livros segundo o título, o autor, o país, a editora, individualizando-os inclusive por edição. Utilizado também para identificar software, seu sistema numérico é convertido em código de barras, o que elimina barreiras linguísticas e facilita a circulação e comercialização das obras.

Em 1966, em Berlim, na Alemanha, durante a Terceira Conferência Internacional de Pesquisa de Mercado de Livros e Racionalização no Comércio de Livros, levantou-se uma discussão sobre a necessidade e a viabilidade da criação de um sistema internacional de numeração para livros, para facilitar o controle de estoque e venda, visto que, até então, tal controle era feito de maneira analógica. Com o avanço da tecnologia e dos computadores, os distribuidores e livreiros europeus daquela época começaram a discutir sobre mecanismos para facilitar esse processo. Percebeu-se, então, que o pré-requisito para ter um sistema automatizado eficiente seria através de um número de identificação único e simples para cada publicação. Contudo, somente em 1967, no Reino Unido, foi introduzido por J. Whitaker Sons, o sistema de numeração de livros, conhecido por International Standard Book.

No ano de 1968, o Comitê de Documentação Técnica 46 da Organização Internacional de Normalização (ISO) levantou o questionamento sobre a possibilidade de adaptar o sistema inglês para uso internacional. Assim, entre os anos de 1968 e 1969, o Comitê elaborou um relatório, que circulou para todos os países que pertencem à ISO, chegando, então, nos Estados Unidos. Como resultado dos encontros do Comitê, o ISBN é aprovado como norma ISO 2108, que resultou na criação, em 1971, das primeiras agências internacionais do ISBN e na implantação do padrão em países fora da Europa e dos Estados Unidos. Neste mesmo ano, o centro Regional para o Fomento do Livro na América Latina e no Caribe (Cerlalc), iniciou uma série de esforços para estimular os países da região a adotarem a padronização e, em 1978, o Brasil implantou a primeira Agência Brasileira do ISBN.

Entre os anos de 1978 e 1992, o padrão original precisou passar por revisões para se adequar às necessidades de metadados e, em 2005 com o aparecimento de novas mídias, o sistema foi expandido para cobrir mais de 160 países. Dessa forma, o código, que até então era composto por dez dígitos, expandiu para treze números, em 2007, recebendo mais especificações, e ficou conhecido como ISBN-13.

Atualmente, com essa combinação, é possível individualizar e catalogar as informações particulares e específicas de cada uma das diversas publicações produzidas ao redor do mundo. Essa combinação é reconhecida em mais de 200 países e possibilita o compartilhamento de metadados, representando um marco no mercado editorial.

Funcionando como um número de CPF para os livros, cada sequência é criada por meio de uma combinação dos treze dígitos, conforme a Figura 4.

Vamos ver o significado de cada grupo ou código.

Figura 4 – Estrtura ISBN-13

Fonte: https://www.cblservicos.org.br/isbn/estrutura/

Os três primeiros dígitos, Código GTIN, são determinados pelo GS1, antigo EAN International, que gerencia dados de códigos de barras de produtos. Hoje, o prefixo 978 é utilizado pelo mercado editorial podendo ser criados outros padrões conforme a necessidade. Já o grupo registrante é responsável pela identificação do país, região geográfica ou a área de idioma. No Brasil o número mais utilizado é o 85, porém desde 2018, devido à demanda o número 65 passou a ser utilizado.

O elemento Registrante, pode conter até sete dígitos, isto é, varia de acordo com o número esperado de edições do editor. Ele identifica um editor ou uma marca particular em um grupo de registro. Podendo conter até seis dígitos, a Publicação identifica a edição especial de uma obra por um editor específico, e o Dígito de Controle ou Dígito Verificador, garante que o ISBN-13 seja único e exclusivo, determinado por meio de um cálculo utilizando um algoritmo de módulo onze.

Neste sistema de codificação o dígito verificador é obtido multiplicando e somando a n-upla pelo vetor de verificação $(1,3,1,3,1,3,1,3,1,3,1,3,1)$.

Por exemplo, o ISBN-13 do livro do autor Hefez (2016) tem o número 978-85-8337-105-2. Conferiremos o seu dígito verificador, sendo α a n-upla correspondente ao número ISBN-13 e $\beta = (1,3,1,3,1,3,1,3,1,3,1,3,1)$ o vetor verificação:

$$\begin{aligned}\alpha \cdot \beta &= (9,7,8,8,5,8,3,3,7,1,0,5,a_{13}) \cdot (1,3,1,3,1,3,1,3,1,3,1,3,1) \\ &= 9+7\cdot 3+8+8\cdot 3+5+8\cdot 3+31+3\cdot 3+7+1\cdot 3+0+5\cdot 3+a_{13} \\ &= 9+21+8+24+5+24+3+9+7+3+0+15+a_{13} \\ &= 128+a_{13},\end{aligned}$$

então temos a congruência

$$\begin{aligned}128+a_{13} &\equiv 0 \bmod 10 \implies \\ 8+a_{13} &\equiv 0 \bmod 10.\end{aligned}$$

Logo $a_{13} = 2$.

Observação 3. O sistema ISBN anteriormente adotado, ou ISBN-10, é constituído de dez dígitos, o vetor peso de verificação é $(10,9,8,7,6,5,4,3,2,1)$ e sua verificação é feita módulo 11. Neste sistema de codificação, caso o dígito verificador resulte em dez, devemos utilizar um símbolo para representar este número. A convenção usual é utilizar o símbolo X.

O livro *Applied Abstract Algebra* do autor Lidl e Pilz tem o ISBN-10 $038796035X$. Já o ISBN-13, deste mesmo livro, é o código anterior acrescido de 978 no início e recalculado o dígito verificador obtendo então $978-0387960357$.

Em cada um dos casos acima é necessário utilizar o vetor pesos correspondente ao tipo de código.

O digito verificador do livro $038796035X$ codificado no sistema ISBN-10 é determinado pelo algoritmo

$$\begin{aligned}&(0,3,8,7,9,6,0,3,5,a_{10})\cdot(10,9,8,7,6,5,4,3,2,1)=\\&=0\cdot 10+3\cdot 9+8\cdot 8+7\cdot 7+9\cdot 6+6\cdot 5+0\cdot 4+3\cdot 3+5\cdot 2+a_{10}\cdot 1\\&=0+27+64+49+54+30+0+9+10+a_{10}\\&=243+a_{10},\end{aligned}$$

então

$$\begin{aligned}243+a_{10}\equiv 0 \bmod 11 \implies\\ 1+a_{10}\equiv 0 \bmod 11.\end{aligned}$$

Logo $a_{10}=10$, então devemos substitui-lo por X, confirmando o ISBN-10 do livro mencionado.

3.5 Detecção de Erro

Foi adotada a verificação com um vetor de pesos pois, caso ocorra uma transposição adjacente ($\ldots ab\ldots \longmapsto \ldots ba\ldots$) conseguimos detecta-la. Se não houvesse o vetor peso e acontecesse uma troca de qualquer dígito com outro da sequencia a congruência modulo m ainda seria válida:

$$a_1+a_2+a_3+\ldots+a_{12}+a_{13}=a_2+a_1+a_3+\ldots+a_{12}+a_{13}\equiv 0 \bmod m.$$

Teorema 4. Uma transposição adjacente ($\ldots a_i a_{i+1}\ldots \mapsto \ldots a_{i+1}a_i\ldots$) é detectada pelo sistema EAN-13 se, e somente se, $|a_i-a_{i+1}|\neq 5$.

Demonstração. Seja $a_1a_2\ldots a_ia_{i+1}\ldots a_{13}$, $0\leq a_k\leq 9$, um código de barras do sistema EAN-13 e $\omega=(1,3,1,3,1,3,1,3,1,3,1,3,1)$ o vetor peso de verificação.

Transformando a sequência EAN-13 em uma n-upla, consideremos que a_i ocupa uma posição de ordem par, $\alpha = (a_1, a_2, \ldots, a_i, a_{i+1}, \ldots, a_{13})$ e aplicando o algoritmo verificador temos:

$$\alpha \cdot \omega = a_1 + 3 \cdot a_2 + \ldots + 3 \cdot a_i + a_{i+1} + \ldots + 3 \cdot a_{12} + a_{13} \equiv 0 \bmod 10. \tag{3.1}$$

Suponhamos uma transposição adjacente do código EAN13 $a_1 a_2 \ldots a_{i+1} a_i \ldots a_{13}$ e aplicando o algoritmo verificador temos:

$$\alpha' \cdot \omega = a_1 + 3 \cdot a_1 + \ldots + 3 \cdot a_{i+1} + a_i + \ldots + 3 \cdot a_{12} + a_{13} \equiv 0 \bmod 10. \tag{3.2}$$

Se $a_{i+1} = a_i$, os dígitos são iguais, ou seja, não há transposição. Logo é necessário que $a_{i+1} \neq a_i$.

De (3.2) - (3.1) temos:

$$\begin{aligned} 3 \cdot a_{i+1} + a_i - (3 \cdot a_i + a_{i+1}) \equiv 0 \bmod 10 &\Leftrightarrow \\ 2 \cdot a_{i+1} - 2 \cdot a_i \equiv 0 \bmod 10 &\Leftrightarrow \\ 2(a_{i+1} - a_i) \equiv 0 \bmod 10 &\Leftrightarrow |a_{i+1} - a_i| = 5. \end{aligned}$$

Portanto uma transposição adjacente é detectada se, e somente se, $|a_i - a_{i+1}| \neq 5$. ■

3.6 Calendário

A contagem do tempo vem desde a pré-história, com indícios de pinturas das cavernas. Com a sucessão de dias e noites e as fases da Lua, este fenômeno foi dando a intuição de dias e meses. Somente com o desenvolvimento da agricultura que os povos primitivos se aperceberam do ciclo das estações do ano.

O primeiro calendário que se tenha registro, segundo Leopold (2015), foi criado no ano de 2700 a.C pelos Sumérios, na Mesopotâmia, região localizada hoje entre o Iraque, Irã e Jordânia, no Oriente Médio, e melhorado pelos Caldeus, território localizado na região do Iraque, Síria e Turquia. Este calendário era constituído de 12 meses lunares, com 29 ou 30 dias. Cada mês se iniciava na lua nova, o que totalizava 354 dias no ano, e o tornava mais curto do que o calendário solar, criado pelos egípcios por volta de 2500 a.C. Os Caldeus o corrigiam, acrescentando um mês a cada três anos.

Existiram diversos calendários ao decorrer da história, cada um criado conforme a crença ou conhecimentos dos povos de cada época ou região. Atualmente, na maioria dos países é usado o calendário Gregoriano, instituído pelo Papa Gregório XIII, em 1582, e sua composição é resultado de uma reformulação do Calendário Juliano, implantado pelos romanos. Este calendário é baseado no movimento da Terra em torno do Sol, que tem a duração de $365 + \frac{97}{400}$ dias (365,2425 dias), que equivale a 365 dias, 5 horas, 49 minutos e 12 segundos. Em

24 de fevereiro, através da bula publicada pelo Papa Gregório XIII, ficou instituído um novo calendário:

I) O dia seguinte a 4 de outubro (quinta-feira) seria o dia 15 de outubro (sexta-feira).

II) Os anos múltiplos de 4 são bissextos[4], com exceção dos anos centenários (múltiplos de 100) que só seriam bissextos se forem múltiplos de 400.

III) O inicio do ano é primeiro de janeiro, os meses alteram-se com 31 e 30 dias, começando em janeiro com 31 dias, exceto fevereiro que teria 28 dias ou 29 dias nos anos bissextos. O mês de agosto têm 31 dias.

Note que a diferença da contagem dos nos bissextos no Item II) da bula se justifica pois $0,2425 = \frac{1}{4} - \frac{1}{100} + \frac{1}{400}$.

O algoritmo a seguir foi escrito de acordo com o livro de Hefez (2016).

3.6.1 Algoritmo de Zeller

A fórmula que estabeleceremos é conhecido como Algoritmo de Zeller, em homenagem a Julius Christian Johannes Zeller $(1822-1899)$, terá validade a partir do ano 1601 e devido à irregularidade de fevereiro, o colocaremos como último mês, ou seja, mês 1 será março, mês 2 abril, etc, até os meses 11 e 12, que serão janeiro e fevereiro (do ano seguinte). Assim, janeiro e fevereiro de um determinado ano serão considerados como meses 11 e 12 do ano anterior.

Definição 5. Uma data (d,m,A) será constituída por três números, onde:

i) d representa o dia.

ii) m representa o mês, conforme a Tabela 3.

iii) A um ano posterior a 1600.

Por exemplo, 23 de janeiro de 2022 será denotado por $(23,11,2021)$ e 2 de fevereiro de 2021 por $(2,12,2020)$.

[4] Ano bissexto é quando tem um dia extra em fevereiro, isto é, possui 366 dias

Tabela 3 – Meses do ano no Algoritmo de Zeller

Meses	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

Vamos ainda determinar os dias da semana conforme a Tabela 4:

Tabela 4 – Dias da semana no Algoritmo de Zeller

domingo	1
segunda-feira	2
terça-feira	3
quarta-feira	4
quinta-feira	5
sexta-feira	6
sábado	0

Para determinar o dia da semana $s(d,m,A)$ da data (d,m,A) procederemos por partes. Determinaremos inicialmente uma fórmula para o dia da semana do primeiro dia do mês 1 (março) do ano A, $s(1,1,A)$. Posteriormente, acharemos uma fórmula para o dia da semana do primeiro dia do mês m do ano A, $s(1,m,A)$. E, finalmente, a fórmula para $s(d,m,A)$. A proposição a seguir auxiliar-nos-á nessa tarefa.

Proposição 7. Seja $A > 1600$. Então, no intervalo $(1600,A]$,

i) o número de anos múltiplos de 4 é

$$\left[\frac{A}{4}\right] - \left[\frac{1600}{4}\right] = \left[\frac{A}{4}\right] - 400.$$

Demonstração. Decorre diretamente da Proposição 2, tomando o intervalo $(1600,A]$. ■

ii) o número de anos centenários que não são bissextos é

$$\left[\frac{A}{100}\right] - \left[\frac{A}{400}\right] - 12.$$

Demonstração. Basta realizarmos a subtração dos anos centenários e os anos centenários bissextos no respectivo intervalo, utilizando-se da propriedade anterior, que são dados por:

$$\left[\frac{A}{100}\right] - \left[\frac{1600}{100}\right] - \left\{\left[\frac{A}{400}\right] - \left[\frac{1600}{400}\right]\right\} = \left[\frac{A}{100}\right] - \left[\frac{A}{400}\right] - 12.$$

■

iii) o número de anos bissextos é

$$b = \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] - 388.$$

Demonstração. Decorre diretamente de i) − ii):

$$\left[\frac{A}{4}\right] - 400 - \left\{\left[\frac{A}{100}\right] - \left[\frac{A}{400}\right] - 12\right\} = \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] - 388.$$

■

Denotaremos provisoriamente por s o dia da semana de primeiro de março de 1601, que iremos determinar posteriormente.

Como 1602 não é bissexto, o dia primeiro de março de 1602 ocorrerá após 365 dias. Sendo $365 \equiv 1 \bmod 7$, segue-se que o dia 1 de março de 1602 ocorrerá em um dia da semana posterior a s, ou seja, cairá no dia $s+1 \bmod 7$, onde a notação ($a \bmod 7$) significa o resto da divisão de a por 7.

Analogamente $s(1,1,1603) = s+2 \bmod 7$. Para calcular $s(1,1,1604)$, uma precaução deve ser tomada, pois o mês de fevereiro de 1604, contado como mês 12 do ano anterior, tem 29 dias, logo, a passagem de primeiro de março de 1603 para primeiro de março de 1604 ocorrerá após 366 dias e, como $366 \equiv 2 \bmod 7$, temos que $s(1,1,1604) = s+2+2 \bmod 7$. Vemos então que cada ano bissexto que passa devemos somar 1 (módulo 7) ao dia da semana do ano anterior e cada ano bissexto devemos somar 2.

Assim, como a nossa contagem inicia-se no ano de 1601, e sendo b o número de anos bissextos no intervalo $(1600, A]$, temos que

$$s(1,1,A) = s + A - 1600 + b \bmod 7. \tag{3.3}$$

Consultando o calendário do ano corrente, 2022, verificamos que o primeiro dia de março deste ano foi uma terça-feira, logo $s(1,1,2022) = 3$. Calculando b pela proposição Item iii), e substituindo na equação (3.3) obtemos

$$\begin{aligned} b &= \left[\frac{2022}{4}\right] - \left[\frac{2022}{100}\right] + \left[\frac{2022}{400}\right] - 388 \\ &= 505 - 20 + 5 - 388 = 102 \end{aligned}$$

então

$$\begin{aligned} 3 = s(1,1,A) \equiv s + 2022 - 1600 + 102 \bmod 7 &\implies \\ 3 \equiv s + 6 \bmod 7 &\implies \\ -3 \equiv s \bmod 7 &\implies \\ 4 \equiv s \bmod 7. & \end{aligned}$$

Temos $s \equiv 4 \bmod 7$, logo s representa uma quarta-feira.

As considerações acima, juntamente com a proposição Item iii) e o fato que

$$1600 + 388 \equiv 0 \bmod 7,$$

provam o resultado a seguir.

Proposição 8. Tem-se que

$$s(1,1,A) = 4 + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \bmod 7. \tag{3.4}$$

Agora, para passarmos de primeiro de março para primeiro de abril, devemos somar 31 dias, e como $31 \equiv 3 \bmod 7$, temos que

$$s(1,2,A) \equiv s(1,1,A) + 3 \bmod 7,$$

logo, a constante de $s(1,2,A)$ é 7. Como $30 \equiv 2 \bmod 7$, temos que

$$s(1,3,A) \equiv s(1,2,A) + 2 \equiv s(1,1,A) + 5 \bmod 7,$$

logo, a constante de $s(1,3,A)$ é 9, e assim sucessivamente somando os números 2 ou 3 ao primeiro dia da semana do mês anterior para obter o primeiro dia da semana de um determinado mês, até chegarmos ao mês 12 (fevereiro). Assim, os termos constantes que devemos somar à expressão

$$A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \bmod 7,$$

para obter o dia da semana de um determinado mês m de um ano A são:

$$4, 7, 9, 12, 14, 17, 20, 22, 25, 27, 30, 33,$$

ou seja,

$$4, 0, 2, 5, 0, 3, 6, 1, 4, 6, 2, 5 \bmod 7.$$

Escrevendo os dados na Tabela 5 temos:

Tabela 5 – Acréscimo de dias entre os meses

m	meses	acréscimo	$s(1,m,A)$	*mod* 7
1	Março	0	$s(1,1,A)=4$	4
2	Abril	3	$s(1,2,A)=7$	0
3	Maio	2	$s(1,3,A)=9$	2
4	Junho	3	$s(1,4,A)=12$	5
5	Julho	2	$s(1,5,A)=14$	0
6	Agosto	3	$s(1,6,A)=17$	3
7	Setembro	3	$s(1,7,A)=20$	6
8	Outubro	2	$s(1,8,A)=22$	1
9	Novembro	3	$s(1,9,A)=25$	4
10	Dezembro	2	$s(1,10,A)=27$	6
11	Janeiro	3	$s(1,11,A)=30$	2
12	Fevereiro	3	$s(1,12,A)=33$	5

Existe uma fórmula empírica em função de $m = 1,2,\ldots,11,12$ que fornece esses valores mod 7:

$$2+\left[\frac{13\cdot m-1}{5}\right].$$

Provamos assim o resultado a seguir:

Proposição 9.

$$s(1,m,A)=2+\left[\frac{13\cdot m-1}{5}\right]+A+\left[\frac{A}{4}\right]-\left[\frac{A}{100}\right]+\left[\frac{A}{400}\right] \bmod 7. \tag{3.5}$$

Como a cada dia do mês que passa devemos somar 1 módulo 7 ao dia da semana do dia anterior, obtemos imediatamente o **Algoritmo de Zeller**.

Teorema 5 (Algoritmo de Zeller)**.** Para um calendário Gregoriano a partir de 1601, o dia s é dado por:

$$s(d,m,A)=d+1+\left[\frac{13\cdot m-1}{5}\right]+A+\left[\frac{A}{4}\right]-\left[\frac{A}{100}\right]+\left[\frac{A}{400}\right] \bmod 7.$$

Exemplo 8. Determinar o dia da semana em que foi o dia 15 de maio de 1991.

Pelo Algoritmo de Zeller temos que $d = 15$, maio é o mês 3 e $A = 1991$, obtemos

$$\begin{aligned} s(15,3,1991) &= 15+1+\left[\frac{13\cdot 3-1}{5}\right]+1991+\left[\frac{1991}{4}\right]-\left[\frac{1991}{100}\right]+\left[\frac{1991}{400}\right] \bmod 7 \\ &= 2007+7+497-19+4=2496\equiv 4 \bmod 7, \end{aligned}$$

Temos então que o referido dia foi uma quarta-feira.

Exemplo 9. Determinar o dia da semana em que foi o dia 19 de junho de 1959.

Pelo Algoritmo de Zeller temos que $d = 19$, junho é o mês 4 e $A = 1959$, obtemos

$$\begin{aligned} s(19,4,1959) &= 19+1+\left[\frac{13\cdot 4-1}{5}\right]+1959+\left[\frac{1959}{4}\right]-\left[\frac{1959}{100}\right]+\left[\frac{1959}{400}\right] \bmod 7 \\ &= 1979+10+489-19+4 = 2463 \equiv 6 \bmod 7, \end{aligned}$$

Temos então que o dia 19 de junho de 1959 foi uma sexta-feira.

CAPÍTULO

4

SUGESTÕES DE ATIVIDADES EM SALA DE AULA

Diante dos conceitos apresentados neste trabalho, apresentaremos neste capítulo propostas para o professor de matemática utilizar em sala de aula. No contexto do cenário educacional brasileiro atual, defendemos que o ensino da matemática deve se dar de forma contextualizada, de modo que os alunos percebam a importância a aplicabilidade da matemática nas diversas situações cotidianas e que os processos de ensino e aprendizado tenham sentido e significado.

Nesse sentido, procuramos articular nosso tema com atividades atreladas aos conhecimentos, competências e habilidades previstas na Base Nacional Comum Curricular (BNCC), buscando evidenciar que é factível trabalhar com noções de congruência e divisibilidade na Educação Básica. A BNCC é um documento normativo de referência obrigatória para elaboração dos currículos escolares e propostas pedagógicas no âmbito da Educação Básica brasileira. Ao encontro disso, as atividades aqui sugeridas estão relacionadas com os eixos de Números e Álgebra e são trabalhadas no pensamento matemático, multiplicação, divisão, múltiplo, quociente e resto da divisão. Além disso, conectam-se com as seguintes habilidades do Ensino Fundamental II: EF06MA06 (Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor.), EF07MA05 (Resolver um mesmo problema utilizando diferentes algoritmos.), EF07MA11 (Compreender e utilizar a multiplicação e a divisão de números racionais, a relação entre elas e suas propriedades operatórias.) (BRASIL, 2018). No que tange aos anos iniciais do Ensino Fundamental, nossa proposta revisita as seguintes habilidades do ciclo: EF04MA12 (Reconhecer, por meio de investigações, que há grupos de números naturais para os quais as divisões por um determinado número resultam em restos iguais, identificando regularidades.), EF01MA01 (Utilizar números naturais como indicador de quantidade ou de ordem em diferentes situações cotidianas e reconhecer situações em que os números não indicam contagem nem ordem, mas sim código de identificação) (BRASIL, 2018).

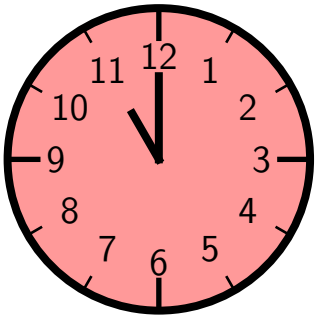
Com o objetivo de contribuir com o ensino de matemática e suas tecnologias, neste

capítulo apresentamos propostas que podem nortear a prática docente. As atividades apresentadas abordam o conhecimento matemático sobre restos, ou seja, congruência modular. Como já citado na Seção 2.3, Gauss observou que usava com frequência a frase "*a* da o mesmo resto que *b* quando divididos por *m*", então Gauss criou uma notação para isso. Congruência, então, nada mais é do que uma linguagem. Iniciaremos as atividades trabalhando os restos da divisão para introduzir a notação de congruência.

As sugestões de atividades propostas são melhores aproveitadas nos últimos anos do Ensino Fundamental II, devido a uma melhor consolidação dos conhecimentos pelos alunos. Entretanto, podem ser adaptadas pelo professor para serem aplicadas nos demais anos. Reforçamos que os exercícios são possibilidades e que o docente pode adequar da forma que achar melhor para desenvolver com suas turmas, considerando, ainda, os conhecimentos e habilidades que se espera que os estudantes desenvolvam.

4.1 Atividade: A Aritmética do Relógio

Uma proposta de atividade inicial para familiarização e introdução do tema congruência é a periodicidade de alguns eventos. Observa-se que os conceitos matemáticos que descrevem esses eventos do cotidiano do aluno são ligados à divisibilidade, como é o caso do relógio, por exemplo.



Atividade 1. Cada dia tem 24 horas. Nos relógios analógicos temos um ciclo de 12 horas e nos digitais temos opções com 12 e 24 horas. Temos, então, uma congruência módulo 12 num período de 24 horas do dia. Veja que:

- 13 horas e 1 hora deixam o mesmo resto e sem mencionar a notação de congruência, $13 \equiv 1 \bmod 12$, podemos exemplificar para o aluno

$$\begin{array}{r|l} 13 & 12 \\ \hline 1 & 1 \end{array} \quad \text{e} \quad \begin{array}{r|l} 1 & 12 \\ \hline 1 & 0 \end{array}.$$

- 17 horas e 5 horas são equivalentes matematicamente, ou seja, 17 é congruente a 5 módulo 12, pois ambos deixam o mesmo resto ao serem divididos por 12, $17 \equiv 5 \bmod 12$;
- Pode-se utilizar mais exemplos com os alunos, introduzindo a notação de congruência.

4.2 Atividade: Descobrindo os Dígitos Verificadores do CPF

Na concepção da importância de apresentar a matemática de maneira contextualizada com a realidade dos alunos, pensamos nesta atividade referente aos dígitos do CPF.

Como proposta de atividade, os alunos terão de calcular o dígito verificador do CPF. Para tanto, faz-se necessário conhecer os fundamentos e a razão dos dígitos presentes no documento. Sugerimos que o professor peça que os alunos se dividam em duplas. Em seguida, o docente pode elaborar um CPF com os nove primeiros dígitos e solicitar a turma que calculem os dígitos verificadores. Outra possibilidade é solicitar previamente que cada aluno traga seu CPF e troquem entre a dupla, para que cada um calcule os dígitos verificadores do CPF do colega.

Atividade 2. Sendo um CPF de números iniciais 801.046.050, calcule os dígitos verificadores d_1, d_2 e informe a qual estado este CPF pertence (número gerado aleatoriamente pelo autor).

Sendo d_1 o primeiro dígito verificador, usaremos o algoritmo visto na Seção 3.3 e montaremos uma tabela para facilitar os cálculos CPF, o vetor pesos e realizando a multiplicação temos:

8	0	1	0	4	6	0	5	0	d_1
x	x	x	x	x	x	x	x	x	x
10	9	8	7	6	5	4	3	2	1

$$80+0+8+0+24+30+0+15+0+d_1 = 157+d_1.$$

Então $157+d_1$ deve ser múltiplo de 11, ou seja $157+d_1 = 11\cdot k$, com k inteiro. Efetuando a divisão Euclidiana de 157 por 11 (neste momento o aluno pode-se utilizar o método da chave) obtemos $q = 14$ e $r = 3$. Assim necessitamos que $3+d_1 = 11 \implies d_1 = 11-3 = 8$.

$$\begin{array}{r|l} 157 & 11 \\ \cline{2-2} 47 & 14 \\ 3 & \end{array}$$

Para obtermos d_2,

8	0	1	0	4	6	0	5	0	8	d_2
x	x	x	x	x	x	x	x	x	x	x
11	10	9	8	7	6	5	4	3	2	1

$$88+0+9+0+28+36+0+20+0+16+d_2 = 197+d_2.$$

Então $197+d_2$ deve ser múltiplo de 11, ou seja $197+d_2 = 11\cdot k'$, com k' inteiro. Efetuando a divisão, obtemos $q' = 17$ e $r' = 10$. Assim necessitamos que $10+d_2 = 11 \implies d_2 = 11-10 = 1$.

O CPF informado tem dígitos 801.046.050-81 e tem como região fiscal o estado do Rio Grande o Sul.

Observação 4. No cálculo de d_1 o professor pode explicar que: "O resto da divisão de uma soma por um número é o mesmo que o da divisão da soma dos restos das parcelas por esse mesmo número" (Proposição 5).

Exemplo 10. Qual o resto da soma $6+17+31$ por 4? É o mesmo que a soma dos restos das parcelas $2+1+3=6$ e 6 deixa resto 2 na divisão por 4. Portanto, o resto da soma $6+17+31$ divido por 4 é 2. Ou ainda, na solução de d_1 da atividade: Qual o resto da soma divido por 11, $80+8+24+30+15 \implies 3+8+2+8+4=25$ e 25 deixa resto 3 na divisão por 11.

4.3 Atividade: Calendário

Para iniciarmos o tema, faremos uma introdução para familiarização e relembrar algumas definições sobre calendários. Devemos relembrar com a turma a quantidade de dias em cada mês do ano e o que é um ano bissexto. Janeiro têm 31 dias, fevereiro têm 28 ou 29 dias, $\cdots$, dezembro tem 31 dias. Os anos bissextos tem 1 dia a mais em fevereiro, 29 dias ao todo. O ano é bissexto quando for múltiplo de 4, exceto os anos seculares (múltiplos de 100), mas voltam a ser se forem múltiplo de 400.

Na Atividade 3, é fornecido o dia da semana que caiu o primeiro dia de um determinado ano. Posteriormente, fornecemos uma outra data aos alunos e pedimos que descubram em qual dia da semana tal data caiu. Nesta atividade é evidenciado a periodicidade 7. A atividade foi feita baseada no ano corrente desta dissertação e pode ser adaptada para o ano de aplicação com os alunos.

Atividade 3. Em 2022 o dia primeiro de janeiro foi num sábado. Que dia da semana foi 24 de agosto deste mesmo ano?

Primeiramente devemos notar que os dias da semana são cíclicos e que quando dividimos os dias presentes numa mesma coluna por 7, eles deixam um mesmo resto. Começaremos montando a Tabela 6 para as primeiras semanas do ano:

Tabela 6 – Primeiras semanas de janeiro/2022

Sáb	Dom	Seg	Ter	Qua	Qui	Sex
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21

Observamos que temos uma relação em cada coluna, no sábado $1 \equiv 8 \equiv 15 \bmod 7$, no domingo $2 \equiv 9 \equiv 16 \bmod 7$ e assim por diante. Relacionaremos os dias da semana aos seus restos quando divididos por 7 e recordando que o resto está entre 0 e 6, temos:

Sáb $\leftrightarrow$ 1, Dom $\leftrightarrow$ 2, Seg $\leftrightarrow$ 3, Ter $\leftrightarrow$ 4, Qua $\leftrightarrow$ 5, Qui $\leftrightarrow$ 6, Sex $\leftrightarrow$ 0.

Vamos listar os meses com sua respectiva quantidade de dias passados até a data procurada na Tabela 7. Devemos lembrar se o ano em questão é ou não bissexto. Exemplo $2022 = 4 \cdot 505 + 2$, logo este ano não é bissexto.

Tabela 7 – Dias decorridos

Mês	Dias
Janeiro	31
Fevereiro	28
Março	31
Abril	30
Maio	31
Junho	30
Julho	31
Agosto	24
Total	236

Então devemos somar todos os dias que se passaram e resolve-lo módulo 7, ou seja, analisarmos o resto por 7, $236 \equiv 5 \mod 7$, pois $236 = 33 \cdot 7 + 5$. Concluímos, assim, que o dia procurado foi uma quarta-feira.

Para reforçar os conceitos de calendário, pode-se propor atividades como:

Atividade 4. "Se o primeiro de janeiro de 2023 será um domingo, qual o dia da semana terminá o ano $(31/12/2022)$?", ou "Um determinado ano bissexto começa em uma sexta-feira. Em que dia da semana termina este ano?", ou "Se o dia 13 caiu em sexta-feira, em que dia da semana se iniciou este mês"

Nas próximas atividades trabalharemos o Algoritmo de Zeller para determinarmos dias específicos sem necessidade de uma data conhecida ou o dia da semana que se iniciou o ano. Nesta atividade devemos iniciar reforçando a Definição 3, parte inteira de um número racional. Adiante faremos o cálculo de "Datas Matemáticas", que consistem em dias de essência histórico-matemática.

O algoritmo de Zeller é dado por

$$s(d,m,A) = d + 1 + \left[\frac{13 \cdot m - 1}{5}\right] + A + \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right] \mod 7,$$

e utilizamos os meses e dias como abaixo:

Meses	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

domingo	1
segunda-feira	2
terça-feira	3
quarta-feira	4
quinta-feira	5
sexta-feira	6
sábado	0

Atividade 5. Comemorado em 6 de maio, o Dia da Matemática, é uma homenagem a Júlio César de Mello e Souza, professor de matemática e escritor brasileiro. Júlio nasceu no Rio de Janeiro em 6 de maio de 1885 e escrevia com o pseudônimo do autor árabe Malba Tahan. Dentre suas obras, "O Homem que Calculava" é a de maior sucesso conhecida mundialmente e traduzida em doze idiomas. Utilizando o Algoritmo de Zeller, determine em que dia da semana nasceu o Júlio.

Pelo Algoritmo de Zeller, $d = 6$, maio corresponde a $m = 3$, $A = 1885$, calculando:

$$\begin{aligned} s(6,3,1885) &= 6+1+\left[\frac{13\cdot 3-1}{5}\right]+1885+\left[\frac{1885}{4}\right]-\left[\frac{1885}{100}\right]+\left[\frac{1885}{400}\right] \bmod 7 \\ &= 1892+7+471-18+4 = 2356 \equiv 4 \bmod 7. \end{aligned}$$

Então Júlio nasceu em uma quarta-feira.

Atividade 6. O Dia do Pi é comemorado anualmente em 14 de março. Devido a aproximação de Pi, $\pi \approx 3,14$ e o modo como os americanos registram as datas, Mês/Dia, 14 de março é reconhecido mundialmente pelo dia do Pi. Utilize o Algoritmo de Zeller e calcule o dia da semana que ocorreu o dia do Pi deste ano.

Utilizando o Algoritmo de Zeller temos $d = 14$, $m = 1$, $A = 2022$:

$$\begin{aligned} s(14,1,2022) &= 14+1+\left[\frac{13\cdot 1-1}{5}\right]+2022+\left[\frac{2022}{4}\right]-\left[\frac{2022}{100}\right]+\left[\frac{2022}{400}\right] \bmod 7 \\ &= 2037+2+505-20+5 = 2529 \equiv 2 \bmod 7. \end{aligned}$$

Concluímos que o dia do Pi deste ano caiu numa segunda-feira.

Atividade 7. Como atividade final do tema, pode-se propor aos alunos calcularem o dia da semana de seu nascimento, ou o dia da semana do nascimento do professor, ou alguma data de comemoração histórica.

Conforme já elucidamos, as atividades aqui apresentadas foram apenas alguns exemplos, dentro das diversas possibilidades de aplicação dos conceitos de congruência e divisibilidade.

A presente pesquisa não se esgota aqui , tendo em vista a complexidade e vastidão do tema apresentado. Contudo, nosso propósito foi defender que é possível articular a Teoria dos Números com a prática do docente da Educação Básica. Esperamos que o trabalho contribua com a prática pedagógica dos professores de matemática, corroborando com processos de ensino e aprendizagem carregados de sentido e significado. Por fim, esperamos que a Matemática seja cada vez mais difundida como ciência ricamente produzida e elaborada ao longo da história da humanidade. Que nossos estudantes sejam capazes de visualizar o mundo por meio da matemática, constatando sua presença nas diversas situações e contextos da vida.

4.4 Considerações Finais

Durante o curso PROFMAT, adquiri um aprendizado único, graças às disciplinas que aparentam ser "elementares", mas na verdade não são. Além disso, a convivência com colegas-professores e os docentes do ICMC-USP foi enriquecedora. O trabalho desenvolvido foi uma grande oportunidade de aprofundamento em matemática e história da matemática.

Esperamos que este trabalho possa auxiliar o professor na introdução do tema de Congruências e destacar a importância dos restos em divisões, buscando atividades presentes no dia-a-dia que ajudem a resolver problemas de forma mais clara e objetiva. Embora esta proposta não esteja claramente presente na BNCC, o conteúdo abordado, teoria da divisibilidade, é estudado a partir do 6º ano do Ensino Fundamental, conforme previsto na BNCC.

A teoria das congruências modulares oferece muitos benefícios, seja no contexto escolar ou no cotidiano do aluno, pois possibilita a aquisição de competências e habilidades necessárias que auxiliam no cálculo, reflexão e comparação, fatores fundamentais para a tomada de decisão. Vemos que é possível justificar alguns resultados que não são apresentados diretamente no dia a dia, como o cálculo de dígitos verificadores, códigos de barras e CPF.

REFERÊNCIAS

ANJOS, M. F. dos. **A difícil aceitação dos números negativos: um estudo da teoria dos números de Peter Barlow (1776-1862)**. Dissertação, 2008. Citado na página 25.

BRASIL. **Base Nacional Comum Curricular**. [S.l.], 2018. Disponível em: <http://basenacionalcomum.mec.gov.br>. Acesso em: 29-08-2022. Citado na página 53.

CGI. **Diretrizes, recomendações e especificações técnicas para a aplicação da lei sobre Internet no Brasil**. [S.l.], 2018. Disponível em: <https://www.cgi.br/media/docs/publicacoes/4/GT%20Marco%20Civil%20e%20as%20responsabilidades%20do%20CGI.br.pdf>. Acesso em: 25-09-2021. Citado na página 37.

DIAS, I.; GODOY, S. M. S. de. **SMA0341 e SLC0603 - Elementos de Matemática**. [S.l.: s.n.], 2012. Citado na página 26.

DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. 4. ed. São Paulo: Atual, 2003. Citado na página 26.

HEFEZ, A. **Aritmética - Coleção PROFMAT**. 2. ed. Rio de Janeiro: SBM, 2016. ISBN 978-85-8337-105-2. Citado nas páginas 26, 44 e 47.

LEOPOLD, G. L. **Congruência e Aplicações**. Dissertação, 2015. Citado na página 46.

MEDEIROS, A.; MEDEIROS, C. Números negativos: uma história de incertezas. v. 7, n. 8, p. 49–59, 1992. Citado nas páginas 25 e 26.

MILIES, C. P.; COELHO, S. P. **Números: Uma introdução à Matemática**. 3. ed. São Paulo: Edusp, 2001. 240 p. Citado nas páginas 25 e 26.

NERIS, H. E. B.; DREFS, A. D.; SOUSA, D. B. de; LINS, A. F. História dos números inteiros como regência para o 7º ano do ensino fundamental ii. 2021. Citado na página 25.

SCALABRIN, T. B.; LOPES, A. R. L. V.; POZEBON, S. Constituição dos números inteiros: um movimento histórico. 2021. Citado na página 25.

SCHUBRING, G. Um outro caso de obstáculos epistemológicos: o princípio de permanência. v. 20, n. 28, p. 1–20, 2007. Citado na página 26.

SILVA, E. G. d. **Criptografia RSA: da teoria à aplicação em sala de aula**. Dissertação, 2019. Citado na página 37.

TALAVERA, L. M. B. **Uma Abordagem Histórica dos Números Negativos**. 2001. Disponível em: <http://www.mat.ufrgs.br/~vclotilde/disciplinas/html/reais_relativos-web/reais_relativos_texto_historia_negativos.htm>. Acesso em: 14-04-2022. Citado na página 26.

VERHOEFF, J. **Error detecting decimal codes**. Amsterdam: MC Tracts, 1969. Mathematical Centre tracts, 29. Citado na página 37.


ICMC
USP
SÃO CARLOS