# Ensino Aprendizagem de Matemática



Eliel Constantino da Silva
(Organizador)



Atena Editora
Ano 2019

**Eliel Constantino da Silva**
(Organizador)

# Ensino Aprendizagem de Matemática

Atena Editora
2019

Editora Executiva: Profª Drª Antonella Carvalho de Oliveira
Diagramação: Geraldo Alves
Edição de Arte: Lorena Prestes
Revisão: Os Autores

**Dados Internacionais de Catalogação na Publicação (CIP)**
**(eDOC BRASIL, Belo Horizonte/MG)**

E59 Ensino aprendizagem de matemática [recurso eletrônico] / Organizador Eliel Constantino da Silva. – Ponta Grossa (PR): Atena Editora, 2019.

Formato: PDF
Requisitos de sistema: Adobe Acrobat Reader
Modo de acesso: World Wide Web
Inclui bibliografia
ISBN 978-85-7247-545-7
DOI 10.22533/at.ed.457192008

1. Matemática – Estudo e ensino. 2. Prática de ensino. 3.Professores de matemática – Formação. I. Silva, Eliel Constantino da.

CDD 510.7

**Elaborado por Maurício Amormino Júnior – CRB6/2422**

Atena Editora
Ponta Grossa – Paraná - Brasil
www.atenaeditora.com.br
contato@atenaeditora.com.br

Atena Editora
Ano 2019

## APRESENTAÇÃO

Esta obra reúne importantes trabalhos que tem como foco a Matemática e seu processo de ensino e aprendizagem em salas de aula do Ensino Fundamental, Ensino Médio e Ensino Superior.

Os trabalhos abordam temas atuais e relevantes ao ensino e aprendizagem da Matemática, tais como: a relação da Matemática com a música no ensino de frações, livros didáticos e livros literários no ensino de Matemática, uso de instrumentos de desenho geométrico, jogos, animes e mangá como contribuições para o desenvolvimento da Matemática em sala de aula, análise dos problemas que envolvem o ensino de Trigonometria no Ensino Médio, a ausência do pensamento matemático e argumento dedutivo na Educação Matemática, investigação e modelagem matemática, tendências em Educação Matemática, formação inicial de professores de Matemática e apresentam um aprofundamento da Matemática através dos dígitos verificadores do cadastro de pessoas físicas (CPF), simetria molecular, análise numérica e o Teorema de Sinkhorn e Knopp.

A importância deste livro está na excelência e variedade de abordagens, recursos e discussões teóricas e metodológicas acerca do ensino e aprendizagem da Matemática em diversos níveis de ensino, decorrentes das experiências e vivências de seus autores no âmbito de pesquisas e práticas.

O livro inicia-se com seis capítulos que abordam o ensino e a aprendizagem da Matemática no Ensino Fundamental. Em seguida há 9 capítulos que abordam o ensino e a aprendizagem da Matemática no Ensino Médio, seguidos de 4 capítulos que abordam a temática do livro no Ensino Superior. E por fim, encontram-se 10 capítulos que trazem em seu cerne a Matemática enquanto área do conhecimento, sem a apresentação de uma discussão acerca do seu ensino e do processo de aprendizagem.

Desejo a todos os leitores, boas reflexões sobre os assuntos abordados, na expectativa de que essa coletânea contribua para suas pesquisas e práticas pedagógicas.

Eliel Constantino da Silva

## SUMÁRIO

# CAPÍTULO 19

## OS DÍGITOS VERIFICADORES DO CADASTRO DE PESSOAS FÍSICAS (CPF)

**Pedro Leonardo Pinto de Souza**
Universidade Federal de Ouro Preto
Ouro Preto – Minas Gerais

**Vinícius Vivaldino Pires de Almeida**
Universidade Federal de Ouro Preto
Ouro Preto – Minas Gerais

**Edney Augusto Jesus de Oliveira**
Universidade Federal de Ouro Preto
Ouro Preto – Minas Gerais

**RESUMO:** A presença dos dígitos verificadores tem se tornado cada vez mais recorrente no nosso cotidiano como uma das consequências da era da digitalização. Essa aplicação da teoria dos códigos surge para detectar erro de codificação (FINI, 2009). Há diversos padrões de códigos lineares cujo os dígitos verificadores são calculados de maneira análoga, variando apenas alguns parâmetros do seu sistema de codificação. Nosso objetivo nesse trabalho é definir uma maneira de calcular os dígitos verificadores de um código através das definições de produto interno sobre $\mathbb{R}$ e congruência modular módulo. Tendo em vista que os códigos dos quais definiremos o cálculo dos dígitos verificadores são lineares, é interessante escrevê-los como vetores de um espaço vetorial $\mathbb{R}^n$, em que cada coordenada é um elemento de $\mathbb{R}$, deste modo, podemos relacionar o produto interno e a congruência modular em uma equação, a qual o dígito verificador deverá satisfazer. Definiremos o sistema de codificação a ser utilizado no cálculo e exibiremos tal equação. O cálculo dos dígitos verificadores permite mensurar a segurança de um código controlado pelo dígito verificador. Assim, esse resultado torna-se essencial para entender melhor a construção de códigos mais complexos (FINI, 2009).

## THE CHECK DIGITS OF THE BRAZILIAN NATURAL REGISTER

**ABSTRACT:** The presence of check digits has become more recurrent in our everyday lives as one of the consequences of the digitalization era. This application of coding theory arises to detect coding error (FINI, 2009). There are several linear code patterns whose check digits are computed in an analogous way, varying only a few parameters of their coding system. Our objective in this work is to define a way to calculate the check digits of a code through the internal product definitions on $\mathbb{R}$ and modular congruence module. Since the codes from which we will define the calculation of the check digits are linear, it is interesting to write them as vectors of a vector space $\mathbb{R}^n$, where each coordinate is an element of $\mathbb{R}$, so we can relate the inner product and the modular congruence in an equation which the check digit must

satisfy. We will define the coding system to be used in the calculation and we will show the aforementioned equation. The check digits calculation allows you to measure the security of a code controlled by the check digit. Thus, this result becomes essential to a better understanding of the construction of more complex codes (FINI, 2009).

## 1 I INTRODUÇÃO

Neste trabalho iremos analisar os dígitos verificadores do cadastro de pessoas físicas (CPF) com um enfoque matemático, onde exibimos passo a passo o modo de obtê-los e para isso, nos baseamos no material citado em (FINI, 2009). Inicialmente mostraremos uma maneira de calcular os dígitos verificadores do CPF que nada mais é do que um código composto por  números. Para realizar o cálculo, encontramos o primeiro dígito verificador escrevendo os  primeiros números do CPF como um vetor $X \in \mathbb{R}^9$, de tal modo que o dígito verificador satisfaça uma equação que apresentaremos adiante. Em seguida, o segundo dígito verificador é calculado escrevendo os  primeiros números do CPF, seguido do primeiro digito verificador encontrado, como um vetor $Y \in \mathbb{R}$^10 de modo a satisfazer uma segunda equação que exibiremos adiante. O dígito verificador exerce um papel importante em um código, pois se no momento da digitação desse código ocorresse um erro (por exemplo, se digitássemos um número errado) o computador programado para executar o algoritmo detectaria o erro, uma vez que a equação que o dígito verificador deveria satisfazer não é verificada (FINI, 2009).

## 2 I CONCEITOS PRELIMINARES

Nesta seção iremos definir os conceitos matemáticos fundamentais no cálculo dos dígitos verificadores e estabeleceremos algumas notações que serão utilizadas ao longo do trabalho. Para uma maior compreensão do conteúdo aqui apresentado, exemplificaremos todas as definições de forma objetiva.

### 2.1 Divisão de Números Inteiros

**Definição 2.1.1.** Um número inteiro *a* é divisor de um número inteiro *b* (ou *b* é divisível por *a*), quando existe um número $c \in \mathbb{Z}$, tal que *b* = *ac*. Nesse caso, dizemos que b é múltiplo de a, e para denotar que *a* divide *b*, utilizamos *a* I *b*.

Quando *a* I *b* e *a* ≠ 0, dizemos que o número inteiro *c*, tal que *b* = *a* · *c*, com *c* $\in \mathbb{Z}$, é o quociente de *b* por *a*.

**Exemplo 2.1.1.** O número 0 divide ele próprio. De fato, para todo *c* $\in \mathbb{Z}$, temos que 0 = 0 · *c*.

**Exemplo 2.1.2.** De acordo com a definição acima – 3 I 18, pois tomando *c* = – 6 $\in \mathbb{Z}$ temos que $18 = (-3) \cdot (-6)$.

Note que 20 não é divisível por –3, pois não existe nenhum número inteiro *c* com a propriedade 20 = (–3) · *c*. Nesse caso escrevemos $-3 \nmid 20$.

Em geral, se *b* for um número inteiro que não é divisível por *a*, então escrevemos $a \nmid b$. Vale destacar que existem infinitos pares (*a*,*b*) de números inteiros, tais que nenhum dos dois é divisor do outro, como por exemplo, tome *a* = 2 e *b* um número ímpar maior do que 1, que sempre teremos $a \nmid b$ e $b \nmid a$. Isso nos leva a concluir que a "operação" de divisão em $\mathbb{Z}$ não é assegurada. Porém, se observarmos na reta o conjunto dos números inteiros e dentro dela destacarmos os múltiplos de $a \in \mathbb{Z}$, veremos que todo número inteiro está "próximo" de um múltiplo de $a$. A formalização do conceito de próximo será dada de forma rigorosa no Teorema Divisão Euclidiana.

**Teorema 2.1.1** (Teorema da Divisão Euclidiana)**.** *Se* $a$ e $b$ *são inteiros e* $a > 0$, *então existem números* $q$ e $r$ *inteiros, tais que* $b = aq + r$ *com* $0 \leq r < b$.

*Demonstração.* Vamos primeiro garantir que dados $a > 0$ e $b$ inteiros, existem inteiros $q$ e $r$ com $0 \leq r < b$. Considere os conjuntos

$$A = \{n \in N \mid b < na\} \quad \text{e} \quad B = \{n \in N \mid b \geq na\}.$$

A propriedade arquimediana é citada por Hefez (2011) dos inteiros garante que $A \neq \emptyset$.

Se $A = \mathbb{N}$, então $b < a$, e nesse caso, tome $q = 0$ e $r = b$.

Se $A \neq \mathbb{N}$, então $A$ possui um menor elemento (Princípio da Boa Ordem de $\mathbb{Z}$) citado em Hefez (2011), digamos $q + 1$. Assim, $q + 1$ é o menor inteiro tal que

$$b < (q + 1)a \quad \text{e} \quad b \geq qa.$$

Daí,

$$0 \leq b - aq < a.$$

Tomando $r = b - aq$, temos a existência de *q* e *r* como desejado. Agora provemos a sua unicidade. Suponha que existam $q_1$ e $r_1 \in \mathbb{Z}$ tais que, $b = aq_1 + r_1$ $0 \leq r_1 < a$, temos que $aq + r = b = aq_1 + r_1$, e assim, $a(q - q_1) = r + 1 - r$. Agora, suponha $r \neq r_1$ e $r > r_1$. Daí, $r_1 - r < 0$ e, como $a > 0$, segue que $q - q_1 < 0$. Assim $q_1 - q > 0$, isto é, $q_1 - q \geq 1$. Como $a(q - q_1) = r_1 - r$, segue que $r = r_1 + a(q_1 - q)$. Logo, $q_1 - q \geq 1$. Portanto, $r \geq a$, o que é um absurdo.

Analogamente, prova-se que a desigualdade $r_1 < r$ também é um caso impossível. Assim, $r = r_1$ e consequentemente $q = q_1$.

**Exemplo 2.1.3.** Determine o quociente e o resto da divisão $b = aq + r$ quando $b = 156$ e $a = 11$.

**Solução:** Pelo Teorema da Divisão Euclidiana, temos que $156 = 11 \cdot q +$

$r = 11 \cdot 14 + r \Rightarrow r = 2$. Logo $q = 11$ e $r = 2$.

**Números Primos**

**Definição 2.1.2.** *Um número inteiro p é chamado número primo, quando as seguintes condições se verificam:*

(i) $p \neq 0$;

(ii) $p \neq \pm 1$;

(iii) *Os* únicos *divisores de são* $\pm 1, \pm p$.

**Teorema 2.1.2** (Teorema Fundamental da Aritmética)**.** Sejam $n \in \mathbb{N}$ e $n > 1$, temos que ou *n* é primo ou então existem $p_i$ primos com $1 \leq i \leq k$ tais que

$$n = p_1^{\alpha 1} \cdot p_2{}^{\alpha 2} \cdot \ldots \cdot p_k{}^{\alpha k}$$

com $p_1 < p_2 < \ldots < p_k$ e $\alpha\_i \in \mathbb{N}$ (Dummit and Foote Abstract Algebra, 2003).

A seguir apresentaremos um importante resultado referente ao conjunto dos números primos, cuja prova que apresentaremos é uma elegante demonstração publicada no livro "Os Elementos", devida ao matemático Euclides (300 a.C.).

**Teorema 2.1.3** (Teorema de Euclides)**.** Existem infinitos números primos.

*Demonstração.* Suponha, por contradição, que exista uma quantidade finita de números primos e seja $X = \{p_1, p_2, \ldots, p_m\}$ o conjunto de todos os números primos.

Agora, considere o número natural *n* dado por

$$n = (p_1 \cdot p_2 \cdot \ldots \cdot p_m) + 1.$$

Como $n = (p_1 \cdot p_2 \cdot \ldots \cdot p_m) + 1 > 1$, então pelo Teorema Fundamental da Aritmética, ou *n* é primo ou pode ser escrito como um produto de números primos.

Uma vez que não existe tal que $p_i \in X$ tal que $p_i \mid n$, segue que *n* não pode ser escrito como produto de números primos. Logo *n* é primo.

Por outro lado, $n > p_i$ para todo $p_i \in X$, donde concluímos que $n \notin X$, o que é uma contradição, pois *n* é primo. Essa contradição surge quando supomos que o conjunto *X* dos números primos é finito. Portanto existem infinitos números primos.

## 2.2 Congruências

**Definição 2.2.1.** Sejam $a, b$, inteiros quaisquer e tal que $m \in \mathbb{Z}$ *tal que* $m \neq 0$. Dizemos que $a$ e $b$ são congruentes módulo $m$, quando $m \mid (a - b)$, isto é, se $a - b = mq$ para algum $q \in \mathbb{Z}$. Para denotar que $a$ é côngruo a $b$ módulo $m$, utilizamos $a \equiv b \ (mod\ m)$.

**Proposição 2.2.1.** Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 0$ fixado. Então

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

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

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

*Demonstração.* (i) Temos que $m \mid 0$ para todo $m \in \mathbb{Z}$. Em particular, 0 = $a - a$, assim, como $m \mid 0$, segue que $m \mid (a - a)$. Logo $a \equiv a\ (mod\ m)$.

(ii) Se $a \equiv b\ (mod\ m)$, então $m \mid (a - b)$, isto é, $a - b = mq, q \in \mathbb{Z}$ daí, $-(a - b) = -mq$ Deste modo $b - a = mq\ , q \in \mathbb{Z}$. Portanto $b \equiv a\ (mod\ m)$.

(iii) Dado que $a \equiv b\ (mod\ m)$, segue que $m \mid (a - b)$, assim, $a - b = mq,\ q \in,\ \mathbb{Z}$ e $b \equiv c\ (mod\ m)$. Deste modo $m \mid (b - c)$, ou seja, $b - c = mq\ ,\ q \in \mathbb{Z}$. Daí, como $b = mq + c$, temos que $a - b = mq$, isto é $a - (mq + c) = mq$. Logo $a - c = m(q - q)$ e, portanto, $a \equiv c\ (mod\ m)$.

Uma relação que satisfaz os itens (i), (ii), e (iii) é chamada de relação de equivalência. Deste modo a relação de congruência modulo *m* é uma relação de equivalência sobre $\mathbb{Z}$, ou seja, o conjunto $\mathbb{Z}$ pode ser particionado em subconjuntos de modo que quaisquer dois elementos em um mesmo subconjunto são congruentes módulo *m*.

**Definição 2.2.3.** Sejam $a, b, d$ inteiros, tal que $d \geq 0$. Dizemos que $d$ é o máximo divisor comum (mdc) de $a$ e $b$ quando são válidas as seguintes propriedades:

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

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

**Definição 2.2.4.** Sejam $a, b$ inteiros. Dizemos que $a$ e $b$ são primos entre si quando $mdc(a, b) = 1$, isto é, $a$ e $b$ não possuem nenhum divisor primo em comum.

**Proposição 2.2.1.** Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 0$ fixado. Então

(i) Se $a \equiv b\ (mod\ m)$ se, e somente se, $a$ e $b$ possuem o mesmo resto na divisão euclidiana por $m$.

(ii) Se $mdc\ (c, m) = 1$ e $ac \equiv bc\ (mod\ m)$, então $a \equiv b\ (mod\ m)$.

(iii) $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então $ac \equiv bd\ (mod\ m)$. Essa propriedade pode ser generalizada, por indução, para *n* congruências.

*Demonstração.* (i) (⇒): Pelo Teorema da Divisão Euclidiana, temos que existem

$q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tais que

$$a = mq_1 + r_1, \quad b = mq_2 + r_2, \quad 0 \leq r_1 < m \text{ e } 0 \leq r_2 < m.$$

Por hipótese, temos que $a \equiv b\ (mod\ m)$, assim, $m \mid a - b$, isto é, $m \mid (mq_1 + r_1) - (mq_2 + r_2) = m(q_1 - q_2) + (r_1 - r_2)$. daí $m \mid r_1 - r_2$. Logo $r_1 = r_2$

($\Leftarrow$): Se $a = mq + r$ e $b = mq + r$, então $a - b = mq - mq + 0 = m(q - q)$. Portanto $a \equiv b\ (mod\ m)$.

(ii) Se $ac \equiv bc\ (mod\ m)$, então $(ac - bc) = mq$, ou seja, $c(a - b) = mq$ para algum $q \in \mathbb{Z}$.

Deste modo, temos que $m \mid c$ ou $m \mid (a - b)$.

Como $mdc\ (c, m) = 1$, segue que $m \nmid c$. Logo $m \mid (a - b)$ e, portanto, $a \equiv b$ $(mod\ m)$.

(iii) Se $a_1 \equiv b_1 (mod\ m), a_2 \equiv b_2 (mod\ m), \ldots, a_n \equiv b_n (mod\ m)$, então $a_1 \cdot a_2 \cdot \ldots \cdot a_n = b_1 \cdot b_2 \cdot \ldots \cdot b_n (mod\ m)$.

Em particular, se $a_1 = a_2 = \ldots = a_n$ e $b_1 = b_2 = \ldots = b_n$, temos que $a_n \equiv b_n (mod\ m)$.

**Exemplo 2.2.1.** Para ilustrar essa última propriedade, mostre que $10^{200} - 1$ é divisível por 11.

**Solução:** Como $10^{200} \equiv -1\ (mod\ 11)$, então, pela propriedade 2.2.1 item (iii), $10^{200} \equiv (-1)^{200} (mod\ 11)$, o que implica em $10^{200} \equiv 1\ (mod\ 11)$. Daí, pela definição de congruência, $10^{200} - 1$ é divisível por 11.

## 2.3 Produto Interno Sobre $\mathbb{R}$

Para calcular os dígitos verificadores, além dos conceitos já definidos, utilizaremos também o produto interno definido no conjunto dos números reais entre dois vetores.

**Definição 2.3.1.** *Seja V um espaço vetorial sobre* $\mathbb{R}$. *Um produto interno em V sobre* $\mathbb{R}$, *é uma aplicação*

$$\Psi(\cdot\,,\cdot): V \times V \to \mathbb{R}$$
$$(u, v) \mapsto \Psi(u, v)$$

*que satisfaz todas as propriedades.*

(*i*) $\Psi(u + v, w) = \Psi(u, w) + \Psi(v, w)$ para todos $u, v, w \in V$ .

(*ii*) $\Psi(\alpha u, v) = \alpha\Psi(u, v)$ para todos $u, v \in V$ e $\alpha \in \mathbb{R}$.

(*iii*) $\Psi(u, v) = \Psi(v, u)$ para todos $u, v \in V$ .

(*iv*) $\Psi(u, u) > 0$ se $u \neq 0$ e $\Psi(u, u) = 0$ se, e somente se, $u = 0$.

**Exemplo 2.3.1.** Sejam $X = (x_1, \ldots, x_n)$, $Y = (y_1, \ldots, y_n) \in \mathbb{R}^n$ e defina a aplicação dada por

$$\Psi(X,Y) = \Psi\big((x_1, \ldots, x_n), (y_1, \ldots, y_n)\big) = \sum_{i=1}^{n} x_i y_i.$$

A aplicação definida é um produto interno em $\mathbb{R}^n$. A prova deste exemplo pode ser encontrada em (Ulhoa; 2003).

**Exemplo 2.3.2.** Sejam $u = (1, -1, 1)$ e $v = (0, 2, 4)$. Determine o produto interno $u, v$.

**Solução:** Para calcular o produto interno entre os vetores $u$ e $v$, basta aplicar a definição dada no exemplo 2.3.1, em que $X = u = (1, -1, 1)$ e $Y = v =$ (0,2,4). Deste modo, temos que

$$\langle u, v\rangle = \langle (1, -1, 1), (0, 2, 4)\rangle = 1\ 0 + (-1) \cdot 2 + 1 \cdot 4 = 2.$$

Logo $u, v = 2$.

**Exemplo 2.3.3.** Verifique se a aplicação dada por

$$\begin{array}{lccc} \Psi(u, \mathrm{v}): & \mathbb{R}^2 \mathrm{x}\, \mathbb{R}^2 & \rightarrow & \mathbb{R} \\ & \big((a,b),(x,y)\big) & \mapsto & \Psi\big((a,b),(x,y)\big) = ab + xy \end{array}$$

é um produto interno de $\mathbb{R}^2$.

**Solução:** Vamos mostrar que a aplicação dada não é um produto interno e, para tanto, considere $u = (1, 2), v = (\pi, -3)$ e $w = (4, 7)$

(i) $\Psi(u + v, w) = \Psi\big((1, 2) + (\pi, -3), (4, 7)\big) = 27 - \pi.$

Por outro lado,

$$\Psi(u, w) + \Psi(v, w) = \Psi\big((1, 2), (4, 7)\big) + \Psi\big((\pi, -3), (4, 7)\big) = 58 - 3\pi.$$

Logo, $\Psi(u + v, w) \neq \Psi(u, w) + \Psi(v, w)$. Assim, a aplicação definida não é produto interno em $\mathbb{R}^2$, pois o item (i) da definição 2.3.1 não é satisfeito.

**Exemplo 2.3.4.** Sejam $A = (a_{ij}), B = (b_{ij}) \in \mathbb{M}_2(\mathbb{R})$. Defina a aplicação

$$\Psi(A, B) = \sum_{i=1}^{2} (a_{ii} + b_{ii}).$$

Verifique se a aplicação acima é um produto interno.

**Solução:** Seja $A = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.

Note que

$$\Psi(A, A) = \Psi\left(\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\right) = 0 \cdot 0 + 0 \cdot 0 = 0;$$

mas  não é a matriz nula. Portanto, a aplicação definida não é um produto interno em $\mathbb{M}_2(\mathbb{R}$.

**Proposição 2.3.1.** Seja $V$ um espaço vetorial sobre $\mathbb{R}$ com um produto interno $\langle \cdot\, , \cdot \rangle$.

(i) $\langle 0, u\rangle = 0$, para todo $u \in V$.

(ii) $\langle u, v + \alpha w\rangle = \langle u, v\rangle + \alpha\langle u, w\rangle$, para todos $u, v, w \in V$ e $\alpha \in \mathbb{R}$.

*Demonstração.* (i) Temos que $\langle 0, u\rangle = \langle 0 + 0, u\rangle = \langle 0, u\rangle + \langle 0, u\rangle$. Logo, $\langle 0, u\rangle = 0$, para todo $u \in V$.

(ii) De fato, pois

$$\langle u, v + \alpha w\rangle = \langle u, v\rangle + \langle u, \alpha w\rangle = \langle u, v\rangle + \langle \alpha u, w\rangle = \langle u, v\rangle + \alpha\langle u, w\rangle.$$

Na próxima seção faremos um apanhado histórico sobre o que são os códigos e o Cadastro de Pessoas Físicas - CPF, além de mostrar como o CPF é construído e qual a sua importância. Ao final desta seção, munidos de todo o conhecimento aqui exposto, vamos apresentar um método utilizado no cálculo dos dígitos verificadores do CPF e faremos alguns exemplos práticos deste cálculo.

## 3 I CÓDIGOS

Os códigos fazem parte da vida cotidiana: temos um Registro de Identidade (RG) numerado, e, para pagarmos impostos sobre a nossa renda, temos um número de Cadastro de Pessoas Físicas (CPF). Moramos em um endereço com Código de Endereçamento Postal (CEP), nosso carro tem um registro de chassi e carrega uma chapa com números e letras que dizem onde ele está cadastrado. Quando trabalhamos, temos, em geral, a Carteira Profissional, votamos com um Título de Eleitor identificado, os países e as cidades têm códigos de discagem de telefones; no supermercado, na farmácia, nas bancas de revistas, nas livrarias, os produtos são acompanhados de etiquetas com seu código e outros (FINI; 2003).

A finalidade dos códigos é viabilizar o registro, o acompanhamento e às vezes toda a execução de uma operação humana. Nesse sentido, há códigos que concentram grande quantidade de dados e informações. E há bons exemplos de como eles podem agilizar as tarefas do nosso cotidiano, como é o caso dos códigos de barras óticos (FINI; 2003).

Mas afinal, o que é um código? Segundo o dicionário Aurélio; “um código é um sistema convencional, rigorosamente estruturado, de símbolos ou de sinais e de regras combinatórias integrado no processo da comunicação". Os códigos de identificação de pessoas, objetos, situações e outros. São, em geral, formados de algarismos ou de letras e algarismos que podem ou devem ser controlados, para tornar possível detectar erros de codificação. Para "avisar" que há erro de codificação, foi criado um grupo de algarismos, chamados "dígito de verificação" que são justapostos ao código de identificação, geralmente no final. Nosso objetivo nesse trabalho é identificar e compreender como esses dígitos de verificação são determinados em alguns casos

(FINI; 2003).

Existem vários tipos de códigos, dentre eles, alguns códigos de barras que seguem o modelo EAN/UPC (European Article Number / Universal Product Code). Um exemplo de código de barras EAN, é o código de barras que utiliza a estrutura EAN-13, que nada mais é, do que o número identificador de um produto. O primeiro produto a utilizar a tecnologia do código de barras no Brasil foi a Castanha de Caju Cauê, em 1985.

O sistema de identificação usado para o cadastramento de pessoas físicas e jurídicas no Brasil, que fornece o número de CPF e CNPJ, emitido pela Receita Federal e o cadastramento de livros, que fornece o código ISBN (International Standard Book Number) é o EAN - 11, que é um dos tópicos deste trabalho.

## 4 I SISTEMA DE IDENTIFICAÇÃO UTILIZADO NO CADASTRAMENTO DE PESSOAS FÍSICAS

O Cadastro de Pessoas Físicas (CPF) (Figura 4) foi criado em 1968 e instituído no mesmo ano, substituindo o até então Registro de Pessoas Físicas, que era o registro das pessoas físicas obrigadas a apresentar a declaração de rendimentos e bens. Foi batizado de Cartão de Identificação do Contribuinte (CIC) (Figura 4), tornando obrigatório a sua menção, a partir do ano de 1970, em vários documentos, como por exemplo, no controle de locação de bens móveis e imóveis, e nas escrituras apresentadas aos registros dos imóveis. O sucessor do CIC foi o cartão do CPF que ainda é muito utilizado atualmente (Receita Federal; 2016).

A partir disso, a lista de exigências de menção do CPF só aumentou, ultrapassando os limites do imposto de renda e tornando-se um documento de suma importância no cotidiano do brasileiro (Receita Federal; 2016).

Em 2012, a Receita Federal do Brasil implementou o serviço gratuito de inscrição no Cadastro de Pessoas Físicas pela internet. Ao final da solicitação de inscrição efetivada com sucesso, era gerado automaticamente, o número de inscrição no CPF e o "Comprovante de Inscrição no CPF". Todavia, continuaram os canais tradicionais de atendimento CPF (Receita Federal; 2016).

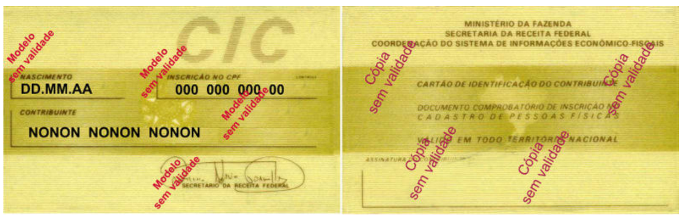


Figura 3: Modelo do Cartão de Identificação do Contribuinte, o primeiro cartão utilizado como sendo um tipo de cadastro de pessoas físicas.

Retirado em https://pt.wikipedia.org/wiki/Ficheiro:CIC_frente_e_verso.jpg.

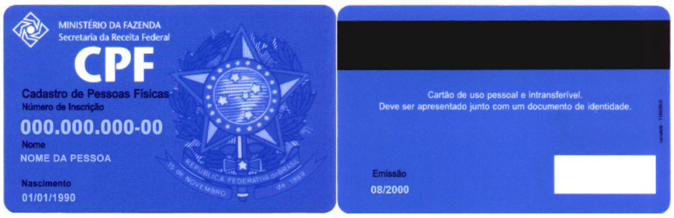


Figura 4: Cartão do CPF. Sucessor do CIC e bastante comum até os dias de hoje.

Retirada de https://iltomvargas.blogspot.com/2017/01/contribuinte-pode-atualizar-cpf-pela.html.

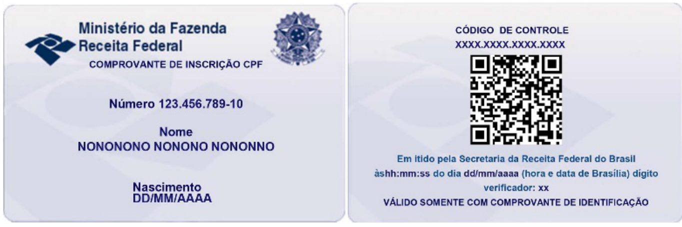


Figura 5: CPF Digital. Criado em 2012 pela Receita Federal para facilitar a inscrição, sendo o sucessor do cartão usual do CPF.

Retirada de https://www.creditooudebito.com.br/como-tirar-segunda-via-cpf-pela-internet/.

O CPF surgiu substituindo o Registro de Pessoas Físicas com o objetivo de reunir informações detalhadas sobre as pessoas físicas, para que a Administração Tributária pudesse coletar essas informações das pessoas que eram obrigadas a apresentar a declaração de rendimentos e bens (Receita Federal; 2016). Mas como era formado os números do CPF? Veremos a seguir, como eram e como são compostos agora, esses números que conhecemos como CPF.

## 4.1. Composição do número do CPF

O Registro de Pessoas Físicas era composto por seis dígitos. Com a criação do CPF, foram introduzidos o sétimo e o oitavo dígito, sendo o oitavo obtido através de um cálculo. Posteriormente, foi introduzido o nono dígito, que até hoje baseia-se na subdivisão do país em dez regiões, chamadas de regiões fiscais (Figura 6). Pouco tempo depois, foram introduzidos dois dígitos no número de inscrição, que eram calculados e chamados de números de controle. Em 1972, a 8ª Região Fiscal (Estado de São Paulo) esgotou o estoque de números e o oitavo dígito que antes era calculado, passou a integrar uma sequência aleatória de oito dígitos (Receita Federal; 2016).

Atualmente o CPF ainda é composto por uma sequência de oito dígitos aleatórios por região fiscal, o nono sendo o código correspondente a determinada região (Figura 7) e os dois últimos chamados de dígitos verificadores. Neste trabalho, apresentaremos um método utilizado no processo de cálculo do 10º e 11º dígitos (Receita Federal; 2016).

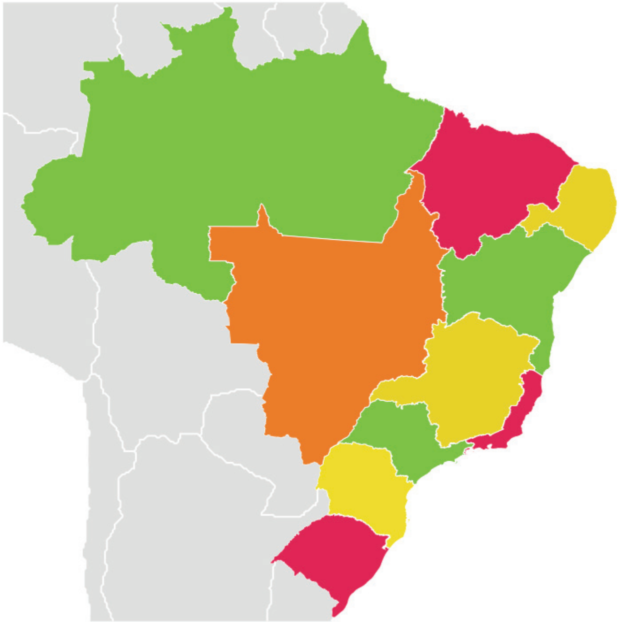

Figura 6: Mapa da subdivisão das dez regiões fiscais do Brasil

Retirada em https://pt.wikipedia.org/wiki/Regi%C3%A3o_fiscal#/media/File:Brazil_Fiscal_regions_Labelled_Map.svg.

Tabela dos códigos correspondentes às regiões fiscais do Brasil, que são utilizados no cálculo dos dígitos verificadores do CPF pelo sistema EAN-11.

| CÓDIGO EAN-11 PARA AS UNIDADES DA FEDERAÇÃO | |
|---|---|
| BRASIL | |
| 0 | Rio Grande do Sul |
| 1 | Distrito Federal, Goiás, Mato Grosso, Mato Grosso do Sul e Tocantins |
| 2 | Acre, Amapá, Amazonas, Pará, Rondônia e Roraima |
| 3 | Ceará, Maranhão e Piauí |
| 4 | Alagoas, Paraíba, Pernambuco e Rio Grande do Norte |
| 5 | Bahia e Sergipe |
| 6 | Minas Gerais |
| 7 | Espírito Santo e Rio de Janeiro |
| 8 | São Paulo |
| 9 | Paraná e Santa Catarina |

## 4.2. Os Dígitos Verificadores do CPF

Vamos agora, mostrar uma maneira de encontrar os dígitos verificadores do CPF, para isso, estabeleceremos algumas definições.

**Definição 4.2.1.** *Um determinado vetor fixo utilizado em um sistema de codificação é chamado vetor de pesos.*

Denotaremos por $I_{10} = \{a \in \mathbb{Z}\,; 0 \leq a \leq 10\}$ como sendo o conjunto de todos os valores que os dígitos verificadores podem assumir.

Sejam e $m, n \in \mathbb{N}$ e $a_{10}^*, a_{11}^*$, respectivamente o 10º e o 11º dígitos do CPF, ou seja, os dígitos verificadores e $X = (x_1, x_2, \dots, x_8, b)$; $Y = (x_1, x_2, \dots, x_8, b, a_{10}^*)$, onde $x_i \in I_9$, onde *b* é o número da Região Fiscal e $a_{10}^*$ é o primeiro dígito verificador. O vetor *X* será chamado de **vetor de informação** e o vetor *Y* **vetor de identificação**.

**Definição 4.2.2.** Sejam $w = (w_1, w_2, \dots, w_n)$; $w_i \in B = \{a \in Z; 0 \leq a \leq m - 1\}$, um vetor de pesos e $c \in I_{10}$ um número fixado. Dados $m, n$ e um conjunto de números $a_1, a_2, \dots, a_{n-1}$; $a_i \in B$, $1 \leq i \leq n - 1$. Define-se o **número de verificação** $a_n$ como sendo o único elemento de $I_9$ que satisfaz a seguinte equação:

$$\sum_{i=1}^{n} a_i w_i \equiv c \ (mod\ m). \quad (1)$$

Um sistema de codificação assim definido, será denotado por:

$$C = (I_9, m, n, c, w). \quad (2)$$

Como o CPF utiliza o sistema EAN-11, os vetores previamente escolhidos e denominados vetores de pesos para serem utilizados neste sistema são $w_1^* = (1,2,3,4,5,6,7,8,9), w_2^* = (0,1,2,3,4,5,6,7,8,9)$ para determinação do 10º e o 11º dígitos, respectivamente.

No nosso caso, para determinarmos $a_{10}^*$ e $a_{11}^*$, o 1º e o 2º dígito verificador, utilizaremos *m* = 11 e *n* = 9 para o primeiro sistema de codificação $C_1 = (I_{10}, 11, 9, a_{10}^*, w^*)$ e $m = 11, n = 10$ para o segundo sistema de codificação $C_2 = (I_{10}, 11, 10, a_{11}^*, w^*)$, respectivamente. Sendo assim, os dígitos verificadores $a_{10}^*, a_{11}^* \in I_{10}$ são os números de $I_{10}$ que verificam as equações:

$$[\langle X, w_1^* - a_{10}^* \rangle] \equiv 0 \ (mod\ 11). \quad (3)$$

$$[\langle Y, w_2^* - a_{11}^* \rangle] \equiv 0 \ (mod\ 11). \quad (4)$$

em que $\langle \cdot, \cdot \rangle$ é o produto escalar definido no Exemplo 2.3.1, *X* o vetor de informação e *Y* o vetor de identificação.

Caso $a_{10}^* = a_{11}^* = 10$ em (3) ou (4) (o que é possível, já que estamos trabalhando na congruência módulo 11), tomamos este dígito sendo 0 por convenção.

**Exemplo 4.2.3.** Dado que os oito primeiros dígitos de um CPF gerado no estado de Minas Gerais são 124.135.41, vamos calcular os seus dígitos verificadores.

Sendo este CPF gerado no estado de Minas Gerais, o seu código de região fiscal é 6. Daí, segue que os 9 primeiros dígitos deste CPF são 124.135.416. Utilizando a equação (3) para encontrarmos o primeiro dígito verificador, temos:

$$[\langle X, w_1^* \rangle - a_{10}^*] \equiv 0 \pmod{11}$$

$$\Leftrightarrow [\langle (1,2,4,1,3,5,4,1,6), (1,2,3,4,5,6,7,8,9) \rangle - a_{10}^*] \equiv 0 \pmod{11}$$

$$\Leftrightarrow [156 - a_{10}^*] \equiv 0 \pmod{11}$$

$$\Leftrightarrow 156 = 11 \cdot 14 + a_{10}^* \Leftrightarrow a_{10}* = 2.$$

Logo, o único $a_{10}^* \in I_{10}$ que satisfaz esta equação é $a_{10}^* = 2$, pois $[156 - 2] \equiv 0 \pmod{11}$. A unicidade de $a_{10}^*$ é garantida pelo fato de $a_{10}^*$ ser o resto da divisão de 154 por 11. Agora que sabemos o valor de $a_{10}^*$, vamos calcular o segundo dígito verificador utilizando a equação ( 4 ). Desse modo, temos que:

$$[\langle Y, w_2^* \rangle - a_{11}^*] \equiv 0 \pmod{11}$$

$$\Leftrightarrow [\langle (1,2,4,1,3,5,4,1,6,2), (0,1,2,3,4,5,6,7,8,9) \rangle - a_{11}^*] \equiv 0 \pmod{11}$$

$$\Leftrightarrow [147 - a_{11}^*] \equiv 0 \pmod{11}$$

$$\Leftrightarrow 147 = 11 \cdot 13 + a_{11}^* \Leftrightarrow a_{11}^* = 4.$$

Deste modo, temos que o único $a_{11}^* \in I_{10}$ que satisfaz esta equação é $a_{11}^* = 4$, pois $[147 - 4] \equiv 0 \pmod{11}$ e, portanto, os códigos verificadores encontrados configuram o CPF: 124.135.416-24.

## 5 I RESULTADOS E DISCUSSÕES

Os resultados obtidos neste trabalho evidenciam a estreita relação entre a matemática e os códigos tal como conhecemos no nosso cotidiano. É importante ressaltar que os códigos facilitam o armazenamento de informações e a comunicação, além da eficiência da aplicação dos dígitos verificadores ao gerar segurança nas mais variadas formas de comunicação e, principalmente, entender como a Álgebra Linear pode ser utilizada em diversas aplicações práticas ao enxergar por exemplo, os dígitos que compõem o CPF como um vetor de um espaço vetorial.

## REFERÊNCIAS


DOMINGUES, Hygino H.; IEZZI, Gelson. Álgebra **Moderna**. 4 ed. São Paulo: Atual 2003.

DUMMIT, D. S.; FOOTE, Richard M. **Abstract algebra**. Hoboken: Wiley, 2004.

FINI, Maria Inês. **Controle dos Códigos de Identificação**. Revista do Professor – Atualidades, SEESP, Edição nº2, p. 70 – 75, 2009.

GS1 BRASIL (Associação Brasileira de Automação). Disponível em: <http://www.gs1br.org/>. Acesso em 15 jan. 2018.

GS1 BRASIL (Associação Brasileira de Automação). **Código de Barras EAN/UPC**. Disponível em: <https://www.gs1br.org/>. Acesso em 10 jul. 2017.

HEFEZ, Abramo. **Elementos de Aritmética.** 2. ed. Rio de Janeiro: SBM, 2011. (Coleção do Professor de Matemática)

ISBN. **ISBN - International Standard Book Number**. Disponível em: <http://www.isbn.bn.br/website/>. Acesso em 10 jul. 2017.

POLCINO MILIES, C. **A matemática dos códigos de barras.** Programa de Iniciação Científica da OBMEP. Rio de Janeiro: OBMEP, 2009, v., p. 131-179

RECEITA FEDERAL. Subsecretaria de Arrecadação e Atendimento. **1968 A 1981 - Começa a Era da Secretaria da Receita Federal**. Disponível em: <https://idg.receita.fazenda.gov.br/sobre/institucional/memoria/imposto-de- renda/historia/1968-a-1981-comeca-a-era-da-secretaria-da-receita-federal>. Acesso em 9 jul. 2017.

RECEITA FEDERAL. Subsecretaria de Arrecadação e Atendimento. **Informações Gerais sobre o CNPJ.** Disponível em: <http://idg.receita.fazenda.gov.br/orientacao/tributaria/cadastros/cadastronacional- de-pessoas-juridicas-cnpj/informacoes-gerais-sobre-o-cnpj>. Acesso em 6 dez. 2017.

RECEITA FEDERAL. **Cadastro Sincronizado Nacional.** Histórico. Disponível em: <https://www16.receita.fazenda.gov.br/cadsinc/sobre-o-projeto/historico/>. Acesso em 6 dez. 2017.

TIM HARFORD E BEN CRIGHTON. **Como o código de barras, nascido na praia, mudou a economia global.** Disponível em: <http://www.bbc.com/portuguese/geral-38553635>. Acesso em 26 jan. 2018.

U. COELHO, M.L. LOURENÇO. **Um Curso de Álgebra Linear.** 2 ed. São Paulo: EDUSP 2011.

U.S. ISBN AGENCY. **FAQs: General Questions.** Disponível em: <http://www.isbn.org/faqs general questions#isbn faq2>. Acesso em 8 dez. 2017.

## SOBRE O ORGANIZADOR

**Eliel Constantino da Silva -** Licenciado e Bacharel em Matemática pela Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP), Brasil, e Universidade do Minho, Portugal, respectivamente. Mestre em Educação Matemática pela Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP). Membro do Grupo de Pesquisa em Informática, outras Mídias e Educação Matemática (GPIMEM) e membro do Grupo de Pesquisa Ensino e Aprendizagem como Objeto da Formação de Professores (GPEA). Atuou como professor bolsista do Departamento de Educação Matemática do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP). Tem interesse e desenvolve pesquisas nos seguintes temas: Educação Matemática, Pensamento Computacional, Robótica, Programação Computacional, Tecnologias Digitais na Educação, Ensino e Aprendizagem, Teoria Histórico-Cultural e Formação de Professores. Atualmente é doutorando em Educação Matemática pela Universidade Estadual Paulista "Júlio de Mesquita Filho" (UNESP), editor de conteúdo da Geekie, colunista do InfoGeekie, membro do Comitê Técnico Científico da Atena Editora, professor do Colégio Internacional Radial e desenvolve ações de formação de professores relacionadas ao uso de tecnologias e Pensamento Computacional na Educação.

## ÍNDICE REMISSIVO

Agência Brasileira do ISBN
ISBN 978-85-7247-545-7
9 788572 475457