

## Sistemas de Identificação Modular: uma aplicação no ensino fundamental

Fernanda Rodrigues Alves Costa<sup>1</sup>  
Marcelo Oliveira Veloso<sup>2</sup>

**Resumo:** O trabalho descreve três exemplos de sistemas de identificação modular analisando-os em relação a capacidade de detecção de erros. Também propõe uma aplicação direta em sala de aula, utilizando o recurso dos blocos lógicos.

**Palavras-chave:** Aritmética Modular, Sistemas de Identificação de Erros, Blocos Lógicos.

### 1 Introdução

*“Os erros são quase sempre de uma natureza sagrada. Nunca tente os corrigir. Pelo contrário: Racionalize-os, compreenda-os a fundo. Depois disso, lhe será possível sublimá-los.”*  
(Salvador Dalí)

Imagine se em uma transferência bancária o operador cometesse um erro ao digitar o número da conta e o valor fosse depositado para um desconhecido. Seria uma situação realmente desagradável, mas as chances desta falha ocorrer são raras.

O número que identifica uma conta bancária é gerado por um sistema capaz de detectar a maioria dos erros cometidos durante a sua leitura, digitação e transmissão. Estes sistemas utilizam um ou mais algarismos acrescentados ao número original que permitem alertar o operador da ocorrência de um erro. Este dígito adicional é conhecido como dígito verificador.

O dígito verificador é determinado por algoritmos que utilizam conceitos simples da Teoria dos Números, mais especificamente Aritmética Modular. Por isto, estes sistemas são conhecidos como *Sistemas de Identificação Modular*.

Os Sistemas de Identificação Modular têm grande importância no comércio, na identificação civil, na arrecadação de tributos e em muitas outras áreas. Eles são amplamente utilizados em códigos de barra, documentos de identificação, passaportes, notas fiscais, boletos de cobrança bancária etc.

Este artigo estuda os Sistemas de Identificação Modular e apresenta alguns exemplos que são avaliados quanto a capacidade de detectar erros. Além disso, propõe uma aula para alunos do ensino fundamental sobre o tema. Para isso, a seção 2, apresenta as noções básicas

---

<sup>1</sup>Aluna do Mestrado Profissional em Matemática, Turma 2012  
Instituição: Universidade Federal de São João del-Rei - UFSJ  
E-mail: fernandaracosta@gmail.com

<sup>2</sup>Orientador do Trabalho de Conclusão de Curso  
Departamento de Física e Matemática - Defim, CAP-UFSJ  
E-mail: veloso@ufs.edu.br

da Teoria dos Números, que fundamentam o texto. A seção 3, discute sobre os tipos de erros cometidos ao digitar um número de identificação, define os Sistemas de Identificação Modular e estabelece as condições para que os sistemas possam detectar determinados tipos de erros.

As seções que seguem descrevem três exemplos concretos de sistema de identificação em utilização no país: o CPF, o ISBN e o cartão de crédito. Para uma melhor compreensão da estrutura de cada um destes modelos são analisadas situações concretas. Estes sistemas também são avaliados em relação a capacidade de detecção de erros.

Finalmente, a seção 7 apresenta uma possibilidade de trabalho deste tema com alunos do 6º e 7º anos do ensino fundamental. Uma sequência didática baseada na metodologia de Resolução de Problemas e Investigação Matemática é cuidadosamente descrita para orientar o trabalho do professor. A proposta utiliza o recurso dos blocos lógicos para oportunizar a vivência de experiências de codificação e transmissão de dados.

Deseja-se que a realização da prática possibilite aos estudantes refletir, investigar e construir conhecimento. Também, espera-se que esse trabalho seja útil a professores e alunos, mostrando como ideias e conceitos abstratos levam ao desenvolvimento de tecnologias que visam ao bem estar da nossa sociedade. Almeja-se ainda, que a leitura deste artigo motive um estudo mais aprofundado sobre a Teoria dos Números e os Sistemas de Identificação Modular.

## 2 Conceitos Iniciais

Esta seção, apresenta algumas definições e propriedades referentes à Teoria dos Números, mais especificamente à Aritmética Modular. Um estudo mais detalhado desse tema pode ser encontrado em Hefez [1], Neto [6] e Santos [10].

Neste texto,  $\mathbb{Z}$  representa o conjunto dos números inteiros com suas operações usuais de adição (+) e multiplicação ( $\cdot$ ) e suas relações de ordem ( $\leq$ ).

**Definição 2.1** *Sejam  $a$  e  $b$  números inteiros com  $a \neq 0$  dizemos que  $a$  divide  $b$  e vamos denotar por  $a \mid b$ , se existir um inteiro  $c$  tal que  $b = ac$ . Se  $a$  não divide  $b$ , escrevemos  $a \nmid b$ .*

É usual dizer que  $a$  é um **divisor** de  $b$ , ou  $b$  é **divisível** por  $a$ , ou ainda  $b$  é um **múltiplo** de  $a$  quando  $a \mid b$ .

**Exemplo 2.1** *Como  $6 = 2 \cdot 3$ , então 2 divide 6 e denotamos por  $2 \mid 6$ . Segue que 2 é um **divisor** de 6, ou 6 é **divisível** por 2, ou ainda 6 é um **múltiplo** de 2.  $\diamond$*

**Definição 2.2** *Um número inteiro  $n$  é **primo** se  $n > 1$  e se possui apenas dois divisores positivos  $n$  e 1. Se  $n > 1$  não é primo dizemos que  $n$  é **composto**.*

**Exemplo 2.2** *Os inteiros 2, 3, 5, 7, 11, 13, 17, 23, 127 e 239 são números primos. Já os inteiros 8 ( $8 = 2 \cdot 4$ ) e 33 ( $33 = 3 \cdot 11$ ) não são primos, ou seja, são números compostos.  $\diamond$*

**Proposição 2.1** *Se  $a, b, c, m$  e  $n$  são inteiros,  $c \mid a$  e  $c \mid b$ , então  $c \mid (ma + nb)$ .*

**Demonstração.** Se  $c \mid a$  e  $c \mid b$  então existem inteiros  $k_1$  e  $k_2$  com  $a = ck_1$  e  $b = ck_2$ . Multiplicando essas duas equações por  $m$  e  $n$ , respectivamente, teremos  $ma = mck_1$  e  $nb = nck_2$ . Somando membro a membro, obtemos  $ma + nb = c(mk_1 + nk_2)$ , segue da Definição 2.1 que  $c \mid (ma + nb)$ .  $\square$

**Definição 2.3** Para cada inteiro  $x$ , define-se o inteiro módulo ou valor absoluto de  $x$ , denotado por  $|x|$ , pela igualdade:

$$|x| = \begin{cases} x & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}$$

Segue da definição que  $|x| \geq 0$ , para todo  $x$  e que  $|x| = 0$  se, e somente se,  $x = 0$ .

**Teorema 2.1** *Sejam  $a, d$  e  $n$  números inteiros. Então:*

1.  $1 \mid n, n \mid n$  e  $n \mid 0$
2.  $d \mid n \Rightarrow ad \mid an$
3.  $ad \mid an$  e  $a \neq 0 \Rightarrow d \mid n$
4.  $d \mid n$  e  $n \neq 0 \Rightarrow |d| \leq |n|$
5.  $d \mid n$  e  $n \mid d \Rightarrow |d| = |n|$
6.  $d \mid n$  e  $m \in \mathbb{Z} \Rightarrow d \mid nm$

**Demonstração.** As afirmações são verificadas individualmente.

1. Observe que  $n = 1.n$ ,  $n = n.1$  e  $0 = n.0$ .
2. Se  $d \mid n$  então existe  $c \in \mathbb{Z}$  tal que  $n = dc$ . Logo  $an = (ad)c$ , isto é,  $ad \mid an$ .
3. Se  $ad \mid an$  então  $an = adc$ , para algum inteiro  $c$ . Logo  $an - adc = 0$ , colocando  $a$  em evidência escrevemos  $a(n - dc) = 0$ , como  $a \neq 0$ , segue que  $(n - dc) = 0$  e portanto  $n = dc$ .
4. Se  $d \mid n$ , temos que  $n = dc$  e  $n \neq 0$  implica que  $c \neq 0$ . Logo  $|c| \geq 1$ . Portanto,  $|n| = |dc| = |d||c| \geq |d|$ .
5. Se  $d \mid n$  e  $n \mid d$ , temos que  $n = dk_1$  e  $d = nk_2$  então  $n = nk_1k_2$ . Assim,  $k_1k_2 = 1$ , logo,  $k_1 = k_2 = \pm 1$  e portanto,  $|d| = |n|$ .
6. Se  $d \mid n$  então  $n = dc$ , multiplicando ambos os lados desta igualdade por  $m \in \mathbb{Z}$  temos  $nm = dcm = d(cm)$  e segue pela Definição 2.1 que  $d \mid nm$ .

□

O próximo resultado é conhecido como Algoritmo da Divisão ou Algoritmo de Euclides.

**Teorema 2.2** *Sejam  $a$  e  $b$  dois números inteiros com  $a > 0$ . Então existem inteiros  $q$  e  $r$  tais que*

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

*Os inteiros  $q$  e  $r$  são únicos e são designados, respectivamente, por quociente e resto da divisão de  $b$  por  $a$ .*

**Demonstração.** Veja Teorema 1.2 no livro [10].

□

**Definição 2.4** Se  $a$  e  $b$  são inteiros dizemos que  $a$  é congruente a  $b$  módulo  $m$  ( $m > 0$ ) se  $m \mid (a - b)$ , notação  $a \equiv b \pmod{m}$ . O caso em que  $a$  não é congruente a  $b$  módulo  $m$  denotamos por  $a \not\equiv b \pmod{m}$ .

**Exemplo 2.3** Temos que  $11 \equiv 3 \pmod{2}$  pois  $2 \mid (11 - 3)$ . ◇

**Proposição 2.2** Sejam  $a$  e  $b$  inteiros. Então  $a \equiv b \pmod{m}$  se, e somente se,  $a$  e  $b$  possuem o mesmo resto na divisão por  $m$ .

**Demonstração.** Pelo Algoritmo da Divisão, Teorema 2.2, existem  $q_1, q_2, r_1, r_2$ , inteiros com  $0 \leq r_1, r_2 < m$ , tais que  $a = q_1m + r_1$  e  $b = q_2m + r_2$ . Logo,  $a - b = m(q_1 - q_2) + (r_1 - r_2)$ , segue que  $(a - b) - m(q_1 - q_2) = (r_1 - r_2)$ .

Como  $a \equiv b \pmod{m}$ , temos que  $m \mid (a - b)$ , temos ainda que  $m \mid m(q_1 - q_2)$ . Portanto, pela Proposição 2.1,  $m \mid (a - b) - m(q_1 - q_2)$ , ou seja,  $m \mid (r_1 - r_2)$ . Agora note que  $|r_1 - r_2| < m$ . Contudo isso só é possível se  $r_1 = r_2$ .

Reciprocamente, se  $a$  e  $b$  possuem o mesmo resto na divisão por  $m$ , pelo Teorema 2.2, existem inteiros  $r, q_1, q_2$  tais que  $a = mq_1 + r$  e  $b = mq_2 + r$ . Logo,  $a - b = m(q_1 - q_2)$ . Assim,  $m \mid m(q_1 - q_2)$  e, portanto,  $m \mid (a - b)$ , segue pela Definição 2.4 que  $a \equiv b \pmod{m}$ . □

**Exemplo 2.4** Como  $21 = 2 \cdot 10 + 1$  e  $13 = 2 \cdot 6 + 1$  temos que  $21 \equiv 13 \pmod{2}$  pois o resto da divisão de 21 e de 13 por 2 são iguais a 1. ◇

A relação  $\pmod{m}$  é uma relação de equivalência, ou seja, é reflexiva, simétrica e transitiva (veja 2.3).

**Proposição 2.3** Seja  $a, b, c$  e  $m$  números inteiros e  $m > 0$ . Então

1.  $a \equiv a \pmod{m}$
2. Se  $a \equiv b \pmod{m}$ , então  $b \equiv a \pmod{m}$
3. Se  $a \equiv b \pmod{m}$  e  $b \equiv c \pmod{m}$ , então  $a \equiv c \pmod{m}$

**Demonstração.**

1. Como  $m \mid 0$ , então  $m \mid (a - a)$ , o que implica  $a \equiv a \pmod{m}$ .
2. Como  $a \equiv b \pmod{m}$ , pela definição 2.4 temos  $m \mid a - b$ , segue pelo Teorema 2.1 que  $m \mid -(a - b) = b - a$ . Logo  $m \mid b - a$  e portanto,  $b \equiv a \pmod{m}$ .
3. Como  $a \equiv b \pmod{m}$  e  $b \equiv c \pmod{m}$ , então  $m \mid a - b$  e  $m \mid b - c$ . Segue da Proposição 2.1 que  $m \mid [(a - b) + (b - c)]$ , logo  $m \mid a - c$ , o que implica  $a \equiv c \pmod{m}$ . □

No teorema a seguir percebe-se que a relação de equivalência é compatível com as operações de adição e multiplicação nos inteiros.

**Teorema 2.3** Se  $a, b, c, r, s$  e  $m$  são inteiros tais que  $a \equiv b \pmod{m}$  e  $r \equiv s \pmod{m}$ , então

1.  $a + c \equiv b + c \pmod{m}$
2.  $a - c \equiv b - c \pmod{m}$

$$3. ac \equiv bc \pmod{m}$$

$$4. a + r \equiv b + s \pmod{m}$$

$$5. ar \equiv bs \pmod{m}$$

**Demonstração.** Aplicando o Teorema 2.1 e a Definição 2.4, obtemos:

$$1. a \equiv b \pmod{m} \Rightarrow m \mid a - b \Rightarrow m \mid a - c + c - b \Rightarrow m \mid (a + c) - (b + c) \Rightarrow a + c \equiv b + c \pmod{m}.$$

$$2. a \equiv b \pmod{m} \Rightarrow m \mid a - b \Rightarrow m \mid (a - c) - (b - c) \Rightarrow a - c \equiv b - c \pmod{m}.$$

$$3. a \equiv b \pmod{m} \Rightarrow m \mid a - b \Rightarrow m \mid (a - b)c \Rightarrow m \mid ac - bc \Rightarrow ac \equiv bc \pmod{m}.$$

$$4. a \equiv b \pmod{m} \text{ e } r \equiv s \pmod{m} \Rightarrow m \mid a - b \text{ e } m \mid r - s \Rightarrow m \mid (a - b) + (r - s) \Rightarrow m \mid (a + r) - (b + s) \Rightarrow a + r \equiv b + s \pmod{m}.$$

$$5. a \equiv b \pmod{m} \text{ e } r \equiv s \pmod{m} \Rightarrow m \mid a - b \text{ e } m \mid r - s \Rightarrow m \mid r(a - b) + b(r - s) \Rightarrow m \mid ar - bs \Rightarrow ar \equiv bs \pmod{m}.$$

□

**Definição 2.5** *Sejam  $a$  e  $b$  inteiros, com  $a \neq 0$  ou  $b \neq 0$ . O máximo divisor comum de  $a$  e  $b$ , denotado por  $\text{mdc}(a, b)$ , é o inteiro positivo  $d$  que satisfaz:*

$$1. d \mid a \text{ e } d \mid b.$$

$$2. \text{Se existe um inteiro } c \text{ tal que } c \mid a \text{ e } c \mid b \text{ então } c \leq d.$$

**Exemplo 2.5** *Observe que  $\text{mdc}(4, 14) = 2$  pois os divisores de 4 são  $\{\pm 1, \pm 2, \pm 4\}$  e 4 não divide 14. ◇*

**Proposição 2.4** *Sejam  $a, b$  e  $c$  números inteiros. Se  $a \mid bc$  e  $\text{mdc}(a, b) = 1$  então  $a \mid c$ .*

**Demonstração.** Veja Proposição 1.21 em Neto [6]. □

**Teorema 2.4** *Sejam  $p$  e  $k$  números inteiros. Então  $pb \not\equiv 0 \pmod{k}$ , para todo  $b \in \{1, \dots, k - 1\}$  se, e somente se,  $\text{mdc}(p, k) = 1$ .*

**Demonstração.** Suponha que  $\text{mdc}(p, k) = d > 1$ . Então  $d \mid p$  e  $d \mid k$ , e assim  $p = dd_1$  e  $k = dd_2$  com  $d_2 \in \{1, \dots, k - 1\}$ . Fazendo  $b = d_2$  temos que

$$pb = pd_2 = dd_1d_2 = d_1dd_2 = d_1k \equiv 0 \pmod{k}.$$

Como  $pb \not\equiv 0 \pmod{k}$  temos um absurdo. Portanto  $d = 1$ , ou seja,  $\text{mdc}(p, k) = 1$ .

Reciprocamente, como  $\text{mdc}(p, k) = 1$  temos que  $k \nmid p$ . Seja  $b \in \{1, \dots, k - 1\}$  tal que  $pb \equiv 0 \pmod{k}$ . Logo  $k \mid pb$  e  $\text{mdc}(p, k) = 1$ . Segue da Proposição 2.4 que  $k \mid b$ . Um absurdo, pois  $0 < b \leq k - 1$ . Portanto,  $pb \not\equiv 0 \pmod{k}$ . □

### 3 Sistemas de Identificação Modular

Frequentemente utilizam-se um número para identificar rapidamente um artigo, uma propriedade, um livro ou uma pessoa. Estes números de identificação podem armazenar uma grande quantidade de dados e informações. Sua utilização é observada no Registro de Identidade (RG), no Cadastro de Pessoa Física (CPF), no Código de Endereçamento Postal (CEP), na identificação de livros (ISBN), no código de barras, na conta bancária e em várias outras situações. Estes números de identificação são, em geral, formados de algarismos (códigos numéricos) ou de letras e algarismos (códigos alfanuméricos).

Para se detectar e evitar fraudes e possíveis erros de transmissão, digitação ou leitura, a maioria dos sistemas de identificação utilizam alguma informação redundante transmitida em simultâneo com o código que se pretende comunicar. Essa informação adicional ou redundância é chamada de dígito verificador, algarismo de controle ou ainda algarismo de teste. Na maioria dos sistemas de identificação o dígito verificador é o último dígito da sequência e seu valor é calculado utilizando Aritmética Modular. Por esse motivo, estes sistemas são conhecidos como *Sistemas de Identificação Modular*.

A utilização de dígitos verificadores não permite a correção automática do erro. Contudo permite que o sistema alerte ao operador sobre a ocorrência do mesmo. E, conseqüentemente, da necessidade de reescrever o número.

Os erros cometidos ao digitar um número foram sistematicamente investigados por autores como Beckley e Verhoeff citados por Milies [4] e [5] e também por Picado [7]. Estas pesquisas revelam que cerca de 79% dos erros ocorrem com a digitação equivocada de um único dígito, como, por exemplo, digitar 1573, quando o correto seria 1673. Este tipo de erro recebe o nome de erro singular. Outros 11% dos erros, chamados de erros de transposição, dividem-se em dois casos: os erros de transposição adjacente e os erros de transposição intercalada. O primeiro tipo refere-se à troca de posição de dois dígitos diferentes situados lado a lado e o segundo, refere-se à troca de posição de dois dígitos diferentes intercalado por um terceiro dígito. Por exemplo, escrever 3876, quando o correto seria 3786 configura um erro de transposição adjacente, enquanto escrever o número 3687 representa um erro de transposição intercalada. Os demais 9,9% dos erros estão distribuídos em diversas categorias, nenhuma delas representando mais de 1% do total. Estes estudos também nos dizem que a incidência de mais de um erro ao digitar um número é muito pouco provável.

Assim, os erros que serão considerados neste texto, singular e de transposição, cobrem mais de 90% dos erros possivelmente cometidos pelo homem. Como vemos na Tabela 1, que citamos abreviando tabela publicada em Milies [5] e Picado [7].

| Tipo de erro                     |   | Frequência relativa |
|----------------------------------|---|---------------------|
| erro singular                    | $\dots a \dots \rightarrow \dots b \dots$     | 79,1%               |
| erro de transposição adjacente   | $\dots ab \dots \rightarrow \dots ba \dots$   | 10,2%               |
| erro de transposição intercalada | $\dots acb \dots \rightarrow \dots bca \dots$ | 0,8%                |
| outros erros                     | —   | 9,9%                |
| Total                            |   | 100%                |

Tabela 1: Tipos de erros mais comuns.

É necessário esclarecer que existem especificidades em cada sistema de códigos ou até mesmo em cada idioma que podem mudar significativamente essa distribuição de probabilidades.

Nos sistemas que utilizam a aritmética modular um número de identificação é da forma

$$x_1x_2x_3 \dots x_nC,$$

onde  $C$  é o algarismo de controle ou dígito verificador. O valor de  $C$  é determinado pela congruência

$$p_1x_1 + p_2x_2 + \dots + p_nx_n + C \equiv 0 \pmod{k}$$

onde os elementos  $\{p_1, p_2, \dots, p_n\}$  são previamente escolhidos e denominados pesos.

Os sistemas deste tipo são chamados de *Sistema módulo  $k$*  e a soma,  $p_1x_1 + p_2x_2 + \dots + p_nx_n + C$ , por soma controle ou soma teste, sendo designada por  $S$ .

Usualmente é utilizado o zero nesta congruência embora qualquer outro valor inteiro entre 0 e  $k - 1$  possa ser empregado. Essa escolha se deve à vantagem de que, se  $S \equiv 0 \pmod{k}$  temos que  $k \mid S$  e portanto a soma teste é um múltiplo de  $k$ .

Outra forma para determinar o dígito verificador é utilizar a congruência

$$p_1x_1 + p_2x_2 + \dots + p_nx_n \pmod{k} = C$$

Veja a situação a seguir para melhor compreensão da estrutura de um sistema modular.

**Exemplo 3.1** *Uma empresa utiliza três dígitos,  $x_1x_2x_3$ , para identificar cada produto que vende. Para ter certeza de que estes números serão corretamente transmitidos, ela acrescenta um quarto dígito (o algarismo de controle) em cada número, criando o código de identificação  $x_1x_2x_3C$ . O dígito de controle,  $C$ , é determinado resolvendo a equação,  $3x_1 + x_2 + 3x_3 + C \equiv 0 \pmod{10}$ , ou seja, a empresa utiliza um sistema módulo 10 com pesos  $\{3, 1, 3\}$ .*

*Assim, para o produto identificado pelo número 854,  $C = 9$ , pois  $C$  é escolhido para satisfazer à seguinte congruência,*

$$3 \cdot 8 + 5 + 3 \cdot 4 + C \equiv 0 \pmod{10}$$

$$24 + 5 + 12 + C \equiv 0 \pmod{10}$$

$$41 + C \equiv 0 \pmod{10}$$

*O dígito 9 foi escolhido como dígito de controle porque  $41 + 9 = 50$  e  $50 \equiv 0 \pmod{10}$ . Portanto, o código de identificação desse produto é 8549. Já o número 7632 é um código inválido, uma vez que  $3 \cdot 7 + 6 + 3 \cdot 3 + 2 = 38$  e  $38 \not\equiv 0 \pmod{10}$ .  $\diamond$*

Os teoremas a seguir estabelecem as condições para que Sistemas de Identificação Modular detectem os erros singulares e de transposição.

**Teorema 3.1** *Um sistema de identificação módulo  $k$ , com pesos  $\{p_1, p_2, \dots, p_n\}$ , detecta todo erro singular,  $a_i \rightarrow a'_i$ , na  $i$ -ésima posição se, e somente se,  $\text{mdc}(p_i, k) = 1$ .*

**Demonstração.** Considere um número  $a_1a_2a_3 \dots a_n$  de um sistema de identificação módulo  $k$ , cujo dígito de verificação é  $a_n$  e a soma teste é  $S$ . Sabe-se que  $S \equiv 0 \pmod{k}$ . Designaremos por  $S'$  a soma teste com a troca  $a_i \rightarrow a'_i$  na  $i$ -ésima posição. Apesar de se tratar de uma soma incorreta podemos ter  $S' \equiv 0 \pmod{k}$  ou  $S' \not\equiv 0 \pmod{k}$ , casos em que o erro é ou não é detectado, respectivamente.

Calculando a diferença,  $S' - S$ , temos:

$$\begin{aligned} S' - S &= (p_1a_1 + p_2a_2 + \dots + p_ia'_i + \dots + p_na_n) - (p_1a_1 + p_2a_2 + \dots + p_ia_i + \dots + p_na_n) \\ &= p_1a_1 + p_2a_2 + \dots + p_ia'_i + \dots + p_na_n - p_1a_1 - p_2a_2 - \dots - p_ia_i - \dots - p_na_n \end{aligned}$$

$$\begin{aligned}
&= p_i a'_i - p_i a_i \\
&= p_i (a'_i - a_i)
\end{aligned}$$

Dessa forma, um erro  $a_i \rightarrow a'_i$  na  $i$ -ésima posição é detectável se, e somente se,  $p_i(a'_i - a_i) \not\equiv 0 \pmod{k}$ , para  $a_i, a'_i \in \{0, 1, 2, \dots, k-1\}$  e  $a_i \neq a'_i$ .

E esta condição é equivalente a  $\text{mdc}(p_i, k) = 1$ , pelo Teorema 2.4.  $\square$

**Teorema 3.2** *Um sistema de identificação módulo  $k$ , com pesos  $\{p_1, p_2, \dots, p_n\}$ , detecta todos os erros de transposição dos algarismos  $a_i$  e  $a_j$  nas posições  $i$  e  $j$  se, e somente se,  $\text{mdc}(p_i - p_j, k) = 1$ .*

**Demonstração.** Neste caso, a diferença entre a soma teste do número errado e a soma teste correta é

$$\begin{aligned}
S' - S &= (p_1 a_1 + \dots + p_i a_j + \dots + p_j a_i + \dots + p_n a_n) - (p_1 a_1 + \dots + p_i a_i + \dots + p_j a_j + \dots + p_n a_n) \\
&= p_1 a_1 + \dots + p_i a_j + \dots + p_j a_i + \dots + p_n a_n - p_1 a_1 - \dots - p_i a_i - \dots - p_j a_j - \dots - p_n a_n \\
&= p_i a_j + p_j a_i - p_i a_i - p_j a_j \\
&= p_i a_j - p_i a_i + p_j a_i - p_j a_j \\
&= p_i (a_j - a_i) + p_j (a_i - a_j) \\
&= (p_i - p_j)(a_j - a_i)
\end{aligned}$$

Portanto, o sistema detecta todas as transposições de algarismos nas posições  $i$  e  $j$  se, e somente se, para quaisquer  $a_i, a_j \in \{0, 1, 2, \dots, k-1\}$  com  $a_i \neq a_j$ , se tem  $(p_i - p_j)(a_j - a_i) \not\equiv 0 \pmod{k}$  que é equivalente a  $\text{mdc}(p_i - p_j, k) = 1$ , pelo Teorema 2.4.  $\square$

Estes resultados justificam uma maior utilização de sistemas módulo 11, pela facilidade de encontrar pesos primos com 11, usando apenas um carácter para algarismo de controle. Este método, porém, tem uma pequena desvantagem, no conjunto dos dígitos de 0 a 9, não há nenhum que represente o número 10, sendo necessário incluir mais um símbolo para representar este número. Em geral utiliza-se sua representação em algarismo romano, “X”, sendo este método denominado módulo 11 completo. Outra possibilidade é o esquema módulo 11 restrito, que utiliza o dígito 0 para representar o 10.

No caso  $k = 10$  as condições dos Teoremas 3.1 e 3.2 são incompatíveis: é impossível satisfazer o segundo se o primeiro for verificado pois, nesse caso, os pesos são necessariamente ímpares e temos que a diferença entre dois números ímpares é um número par. Portanto, qualquer sistema módulo 10 que tenha 100% de eficiência na detecção dos erros singulares não detectará todos os erros de transposição.

Faz-se necessário destacar a importância dos Teoremas 3.1 e 3.2 como mecanismo para a construção de novos sistemas modulares.

## 4 Número do CPF

O Cadastro de Pessoas Física, mais conhecido como CPF é o registro de um cidadão na Receita Federal brasileira no qual devem estar todos os contribuintes (pessoas físicas brasileiras ou estrangeiras com negócios no Brasil). O CPF armazena informações fornecidas pelo próprio contribuinte e por outros sistemas da Receita Federal. Sua posse não é obrigatória, mas é necessária em várias situações, como abertura de contas em bancos e emissão de passaporte, por exemplo.

O número de um CPF tem nove dígitos de identificação e mais dois dígitos verificadores que são indicados por último. Portanto, um CPF tem onze algarismos.

O dígito anterior aos dígitos verificadores (isto é, o terceiro dígito da direita para a esquerda) identifica a unidade federativa em que a pessoa registrou-se pela primeira vez. Por exemplo, a origem do CPF 043.658.306-27 é Minas Gerais, cujo código é “6”. Segue a lista com o número que identifica cada um dos estados brasileiros:

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

Seja  $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}x_{11}$  um número de CPF, onde  $x_i$  representa um dígito de identificação para  $1 \leq i \leq 9$  e  $x_{10}$  e  $x_{11}$  são os dígitos de controle. O algoritmo abaixo, adaptado de Souza [13], permite calcular estes dígitos de controle.

$$x_{10} = \left( \sum_{i=1}^9 ix_i \pmod{11} \right) \pmod{10}$$

$$x_{11} = \left( \sum_{i=2}^{10} (i-1)x_i \pmod{11} \right) \pmod{10}$$

Com a finalidade de ilustrar a aplicação deste algoritmo, vamos verificar a autenticidade do CPF 043.658.306 – 27 calculando os dígitos de controle,  $x_{10}$  e  $x_{11}$ .

Fazendo as devidas substituições obtém-se a seguinte expressão para  $x_{10}$ :

$$x_{10} = ((1.0 + 2.4 + 3.3 + 4.6 + 5.5 + 6.8 + 7.3 + 8.0 + 9.6) \pmod{11}) \pmod{10}$$

$$x_{10} = ((0 + 8 + 9 + 24 + 25 + 48 + 21 + 0 + 54) \pmod{11}) \pmod{10}$$

$$x_{10} = ((189 \pmod{11}) \pmod{10})$$

$$x_{10} = 2 \pmod{10}$$

$$x_{10} = 2$$

Esse resultado confirma o valor do primeiro dígito verificador, agora calcula-se o segundo dígito,  $x_{11}$ :

$$x_{11} = ((1.4 + 2.3 + 3.6 + 4.5 + 5.8 + 6.3 + 7.0 + 8.6 + 9.2) \pmod{11}) \pmod{10}$$

$$x_{11} = ((4 + 6 + 18 + 20 + 40 + 18 + 0 + 48 + 18) \pmod{11}) \pmod{10}$$

$$x_{11} = ((172 \pmod{11}) \pmod{10})$$

$$x_{11} = 7 \pmod{10}$$

$$x_{11} = 7$$

Os cálculos confirmam o valor do segundo dígito de controle. Assim, conclui-se que o CPF 043.658.306 – 27 é autêntico.

É importante ressaltar que o fato de um número de CPF ser autenticado pelos seus dígitos verificadores não o torna um CPF válido. Para isso, é necessário que ele esteja cadastrado

no banco de dados da Receita Federal. Assim, um número correto de CPF nem sempre será um documento já emitido. É o que acontece, por exemplo, com números de CPF que têm todos os dígitos iguais, apesar de serem autenticados pelos seus dígitos verificadores, eles não são válidos.

Esse sistema, que utiliza dois dígitos verificadores, melhora o método módulo 11 restrito. Porém, poderia ter uma maior capacidade de detecção de erros, caso a escolha dos pesos tivesse sido feita de forma mais criteriosa. Mesmo assim, a falha na detecção de erros é de apenas 0,22% dos casos de erro singular e 0,17% dos erros de transposição. A demonstração destes resultados pode ser encontrada em Souza [13], ANEXO A.

Um fato interessante é a implementação no Brasil do Registro de Identidade Civil (RIC). Ele será um cartão com chip que conterá os números de RG, CPF, Título de Eleitor, PIS (Programa de Integração Social), PASEP (Programa de Formação do Patrimônio do Servidor Público), Carteira de Trabalho e Carteira Nacional de Habilitação. Nele constará, ainda, um campo com informações como o tipo sanguíneo e se a pessoa é ou não doadora de órgãos.

O identificador será um número de onze dígitos, sendo o último um dígito verificador, que é calculado empregando o sistema módulo 11 restrito e os seguintes pesos  $\{9, 8, 7, 6, 5, 4, 3, 2, 9, 8\}$ .

Com o RIC, haverá uma padronização nacional do sistema para emissão de RG, colocando um fim à emissão de identidade por estado. O governo pretende substituir todos os documentos em até 10 anos.

## 5 Código ISBN

O ISBN - International Standard Book Number - é um dos sistemas de identificação mais antigos, criado em 1967 e oficializado como norma internacional em 1972. Ele identifica numericamente os livros segundo o título, o autor, o país e a editora, individualizando inclusive edições diferentes.

O sistema é controlado pela Agência Internacional do ISBN, que orienta e delega poderes às agências nacionais. No Brasil, a Fundação Biblioteca Nacional representa a Agência Brasileira desde 1978, com a função de atribuir o número de identificação aos livros editados no país.

Inicialmente o ISBN era composto por dez dígitos,  $x_1x_2x_3x_4x_5x_6x_7x_8x_9C$ , onde os nove primeiros identificavam o livro e o décimo era o dígito verificador. Segundo Picado [7], este sistema que indicaremos por ISBN-10, utiliza os pesos  $\{10, 9, 8, 7, 6, 5, 4, 3, 2, 1\}$  e uma congruência módulo 11.

Assim, o cálculo do dígito verificador do ISBN-10 era efetuado da seguinte forma:

$$10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + C \equiv 0 \pmod{11}$$

Se o valor  $C$  necessário para satisfazer esta condição fosse 10, este seria substituído por um "X". Como no último romance de Eça de Queirós, *A Cidade e As Serras*, cujo ISBN-10 é o número 85-87328-14-X.

A partir de 1º de janeiro de 2007, o ISBN passou de dez para treze dígitos, sendo conhecido por ISBN-13, o que tornou possível o uso do código de barras denominado EAN (European Article Number)<sup>3</sup>. O objetivo foi aumentar a capacidade do sistema, devido ao crescente número de publicações. A nova numeração foi precedida pelo número 978, que identifica o

---

<sup>3</sup>O sistema EAN (European Article Number) adotado na Europa em 1976 é análogo ao sistema UPC (Universal Product Code), o primeiro código de barras, criado nos E.U.A. em 1973. Esse código de 13 dígitos é atualmente utilizado no mundo inteiro principalmente para a identificação de itens do varejo.

produto livro e o número de controle foi recalculado. Quando o “prefixo 978” se esgotar, será adotado o “prefixo 979”.

O dígito de verificação de um ISBN-13 é de 1 dígito com valores entre 0 e 9, mostrado como um caractere final no término da sequência. Veja o exemplo de ISBN-13: 978 – 85 – 85818 – 25 – 8, referente ao livro *Elementos de Aritmética* de Abramo Hefez. O primeiro elemento, 978, é especificado pela Agência Internacional do ISBN, em conformidade com o sistema global de numeração de produtos e indica a indústria, neste caso, publicação de livros. O segundo elemento identifica os grupos nacionais geográficos, sendo o identificador do Brasil o 85. O terceiro elemento refere-se ao editor, nesse caso a Sociedade Brasileira de Matemática (SBM). O quarto elemento é um elemento de publicação, destinado para o editor da publicação, que etiquetou o livro com o número 25. Por fim, o quinto elemento corresponde o dígito verificador.

Os diferentes componentes do ISBN-13 (indústria, país, editor e título) possuem quantidade variada de dígitos. Esta variação permite que os idiomas mais utilizados e que as grandes editoras tenham um número de identificação menor, possibilitando catalogar um maior número de livros.

O ISBN-13 utiliza os pesos  $\{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1\}$  e  $k = 10$ . Logo, determina-se o dígito verificador deste sistema resolvendo a equação abaixo, adaptada de Lourenço [3]:

$$x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12} + C \equiv 0 \pmod{10}$$

onde  $x_i$  são os algarismos do código ISBN-13 na posição  $i$  e  $C$  o dígito de controle.

Por exemplo, o livro *O homem que calculava*, de Malba Tahan, tem como ISBN-13 o número 978-85-0106-196-6. O dígito final, de verificação é 6 porque

$$\begin{aligned} S &= \mathbf{9} + \mathbf{3.7} + \mathbf{8} + \mathbf{3.8} + \mathbf{5} + \mathbf{3.0} + \mathbf{1} + \mathbf{3.0} + \mathbf{6} + \mathbf{3.1} + \mathbf{9} + \mathbf{3.6} + \mathbf{6} = \\ &= 9 + 21 + 8 + 24 + 5 + 0 + 1 + 0 + 6 + 3 + 9 + 18 + 6 = 110 \equiv 0 \pmod{10} \end{aligned}$$

**Teorema 5.1** *O sistema ISBN-13 detecta todo erro singular.*

**Demonstração.** Como os pesos do sistema ISBN-13 são  $\{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1\}$ ,  $\text{mdc}(1, 10) = 1$  e  $\text{mdc}(3, 10) = 1$ , segue direto pelo Teorema 3.1 que esse sistema detecta todo erro singular.  $\square$

Portanto, este sistema tem uma eficiência de 100% na detecção de erros singulares.

**Teorema 5.2** *O sistema ISBN-13 não detecta todos os erros de transposição adjacente.*

**Demonstração.** Segue direto do Teorema 3.2, uma vez que  $\text{mdc}(2, 10) = 2 > 1$ .  $\square$

**Exemplo 5.1** *Se  $a_9 = 6$  e  $a_8 = 1$  forem trocados teríamos  $S' - S = 2(a_9 - a_8) = 2(6 - 1) = 10$  e o erro não seria detectado.*  $\diamond$

Verifica-se que as trocas de algarismos adjacentes  $\dots a_i a_{i+1} \dots \rightarrow \dots a_{i+1} a_i \dots$  que este sistema não detecta são aquelas em que  $|a_{i+1} - a_i| = 5$ . Com efeito, supondo  $i$  par, temos que a diferença entre a soma teste do número errado e a soma teste correta é dada por:

$$S' - S = (a_1 + \dots + 3a_{i+1} + a_i + \dots + C) - (a_1 + \dots + 3a_i + a_{i+1} + \dots + C) = 2(a_{i+1} - a_i)$$

No caso em que  $i$  é ímpar, tem-se a diferença com o sinal trocado,  $2(-a_{i+1} + a_i)$ . Segue que,

$$10 \mid S' \Leftrightarrow 10 \mid (S' - S) \Leftrightarrow 10 \mid 2(a_{i+1} - a_i) \Leftrightarrow |a_{i+1} - a_i| = 5$$

Logo, o sistema ISBN-13 não detecta os seguintes casos de transposição adjacente “05”, “50”, “16”, “61”, “27”, “72”, “38”, “83”, “49” e “94” o que corresponde a 10 dos 90 casos possíveis. Este sistema tem assim uma eficiência de 88,9% na detecção deste tipo de erro. Mas esse é um problema sem relevância prática, uma vez que leitores ópticos são muito precisos e, quando muito, cometem erros singulares.

## 6 Número do Cartão de Crédito

Os principais números de cartões de crédito no Brasil possuem uma sequência de 16 dígitos, os 6 primeiros dígitos definem a instituição emissora, sendo que o primeiro desses seis dígitos caracteriza a bandeira do cartão, por exemplo, 4 - Visa e 5 - Mastercard. Os nove dígitos que seguem identificam o cliente e o último dígito, na extremidade direita, representa o dígito verificador.

Esse dígito final do número do cartão, dígito de verificação, é utilizado para decidir se um cartão de crédito é válido e pode ser calculado por uma fórmula chamada *Algoritmo de Luhn*. Segundo Kirtland [2] esta fórmula foi assim nomeada em homenagem ao cientista Hans Peter Luhn (1896-1964), um engenheiro da IBM (International Business Machines), que recebeu em 1960 a patente dos Estados Unidos por inventar a técnica. Atualmente, o algoritmo é de domínio público, conhecido como Módulo 10 IBM, sendo largamente utilizado por bancos e demais entidades financeiras para validar cartões de crédito e débito.

Verifica-se a autenticidade de um cartão resolvendo a equação que segue, adaptada de Kirtland [2] e Souza [13]:

$\overline{2x_1} + x_2 + \overline{2x_3} + x_4 + \overline{2x_5} + x_6 + \overline{2x_7} + x_8 + \overline{2x_9} + x_{10} + \overline{2x_{11}} + x_{12} + \overline{2x_{13}} + x_{14} + \overline{2x_{15}} + C \equiv 0 \pmod{10}$ , onde  $x_i$  é o algarismo do número do cartão na posição  $i$  e  $C$  o algarismo de controle. Temos ainda que:

$$\overline{2x_i} = \begin{cases} 2x_i, & \text{se } 2x_i < 10 \\ 2x_i - 9, & \text{se } 2x_i \geq 10 \end{cases}$$

Portanto, após os algarismos do identificador serem multiplicados pelos pesos 2 e 1 alternadamente, em cada produto, subtrai-se 9 quando este é maior ou igual a 10 e escolhe-se o algarismo de controle  $C$  de forma a que a soma teste seja um múltiplo de 10.

Esse sistema, com um único dígito de verificação, detecta erros típicos que as pessoas cometem quando transcrevem números de cartão, por exemplo, em compras via internet. Para ilustrar esta situação, suponha que ao digitar o número 4073038870480971 de um cartão de crédito, tenha se cometido um erro, e que o número de fato digitado fosse 4072038870480971. Ao fazer a verificação de leitura, o computador que recebeu a informação faz as seguintes operações:

$$\begin{aligned} S &= 2.4 + 0 + 2.7 + 2 + 2.0 + 3 + 2.8 + 8 + 2.7 + 0 + 2.4 + 8 + 2.0 + 9 + 2.7 + 1 = \\ &= 8 + 0 + 14 + 2 + 0 + 3 + 16 + 8 + 14 + 0 + 8 + 8 + 0 + 9 + 14 + 1 = \\ &= 8 + 0 + (14 - 9) + 2 + 0 + 3 + (16 - 9) + 8 + (14 - 9) + 0 + 8 + 8 + 0 + 9 + (14 - 9) + 1 = \\ &= 8 + 0 + 5 + 2 + 0 + 3 + 7 + 8 + 5 + 0 + 8 + 8 + 0 + 9 + 5 + 1 = 69 \end{aligned}$$

Como o resultado obtido não é um múltiplo de 10, o computador avisa que foi cometido algum erro e o número deve ser novamente digitado.

**Teorema 6.1** *O Algoritmo de Luhn ou Módulo 10 IBM detecta todo erro singular.*

**Demonstração.** Considere separadamente dois casos: o erro ocorre num algarismo com índice par ou o erro ocorre num algarismo de índice ímpar.

Nas posições de índice par o peso é 1 e sendo  $\text{mdc}(1, 10) = 1$ , pelo Teorema 3.1, todos os erros singulares são detectados.

No caso de erro num algarismo de índice ímpar, temos que  $S' - S = \overline{2a'_i} - \overline{2a_i}$ , onde  $S'$  é a soma teste de um número com um erro singular e  $S$  é a soma teste de um número correto. Mas observe que  $\overline{2a'_i}$  e  $\overline{2a_i}$  são o resultado de uma das seguintes transformações:

|                   |                                  |
|-------------------|----------------------------------|
| $0 \rightarrow 0$ | $5 \rightarrow 10 \rightarrow 1$ |
| $1 \rightarrow 2$ | $6 \rightarrow 12 \rightarrow 3$ |
| $2 \rightarrow 4$ | $7 \rightarrow 14 \rightarrow 5$ |
| $3 \rightarrow 6$ | $8 \rightarrow 16 \rightarrow 7$ |
| $4 \rightarrow 8$ | $9 \rightarrow 18 \rightarrow 9$ |

Segue, que se  $S'$  fosse múltiplo de 10, teríamos que  $10 \mid (S' - S)$ . Logo, 10 dividiria  $(\overline{2a'_i} - \overline{2a_i})$ , o que é absurdo, pois  $(\overline{2a'_i} - \overline{2a_i})$  é um número inteiro não nulo entre  $-9$  e  $9$ . Portanto, todos os erros singulares também são detectados quando ocorre num algarismo de índice ímpar.  $\square$

Assim, o Algoritmo de Luhn detecta todo erro singular. Ele também detecta todas as transposições de algarismos adjacentes, com exceção dos casos “09” e “90”, ou seja, detecta 88 casos em 90. Dessa forma, o Algoritmo de Luhn possui uma taxa de detecção de transposições adjacentes de 97,8%, melhor do que os 88,9% observado no sistema ISBN. Uma exposição mais detalhada sobre os erros de transposição pode ser encontrada em Souza [13].

Mas o dígito verificador não é o bastante para garantir a segurança no uso de cartões de crédito, por isso ainda há um código de três dígitos que fica atrás do cartão. Esse código é gerado pela própria instituição e calculado ao criptografar o número do cartão e sua data de validade. Cada empresa decide qual algoritmo usar nessa criptografia e a chave de decodificação não é pública.

## 7 Uma aplicação em sala de aula: Blocos Lógicos

Os blocos lógicos foram criados pelo matemático húngaro Zoltan Paul Dienes, por volta da década de 50. Segundo, Simons [12], o modelo mais frequente nas escolas apresenta-se em caixas contendo 48 peças geométricas, divididas em:

1. Quatro formas: círculos, quadrados, triângulos e retângulos;
2. Três cores: amarelo, azul e vermelho;
3. Dois tamanhos: grande e pequeno;
4. Duas espessuras: fino e grosso;

Assim, cada peça possui 4 atributos. Por exemplo, pode-se ter um círculo, vermelho, grande e fino. O objetivo desta proposta é trabalhar com este material estimulando os estudantes a representar cada bloco por uma sequência numérica, um código.

Espera-se que o trabalho com esse material favoreça o desenvolvimento cognitivo dos estudantes nas noções abstratas de classificação, seriação, ordem e sistematização de padrões, bem como possibilite vivenciar as ideias iniciais de transmissão de dados, percebendo a importância dos dígitos verificadores e conhecendo a teoria dos códigos identificadores de erros.

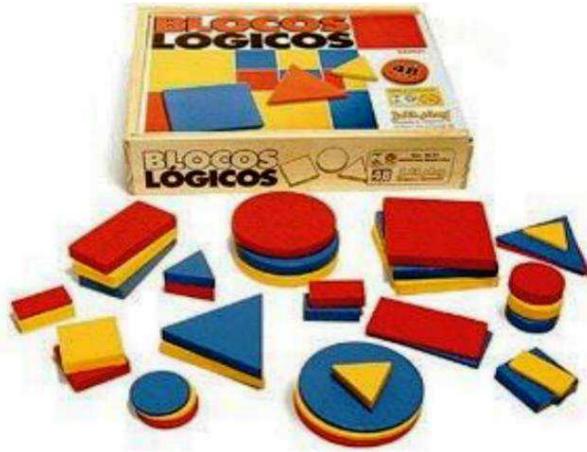


Figura 1: Blocos Lógicos

## 7.1 Proposta de trabalho

Propõe-se uma sequência didática para o trabalho com estudantes do Ensino Fundamental, para desenvolver o tema, códigos identificadores de erros, utilizando os blocos lógicos.

O objetivo é estimular os alunos a compreender a tecnologia dos códigos identificadores, estabelecendo uma relação entre as características de cada peça e um código que a identifique. Uma sugestão é uma sequência de 5 algarismos onde o 1º algarismo identifica a forma, o 2º a cor, o 3º o tamanho, o 4º a espessura e por último o 5º algarismo é o dígito verificador calculado a partir dos anteriores. As tabelas, a seguir, associam um algarismo a cada característica.

| FORMA     | ALGARISMO | COR      | ALGARISMO |
|-----------|-----------|----------|-----------|
| Círculo   | 1         | Amarelo  | 1         |
| Quadrado  | 2         | Azul     | 2         |
| Triângulo | 3         | Vermelho | 3         |
| Retângulo | 4         |          |           |

| TAMANHO | ALGARISMO | ESPESSURA | ALGARISMO |
|---------|-----------|-----------|-----------|
| Grande  | 1         | Fino      | 1         |
| Pequeno | 2         | Grosso    | 2         |

Figura 2: Tabelas

Para determinar o algarismo de controle,  $C$ , do código  $x_1x_2x_3x_4 - C$  basta calcular o resto da divisão por 5 da soma:  $x_1 + 2x_2 + 3x_3 + 4x_4$ . Esse é um sistema módulo 5 com pesos  $\{1, 2, 3, 4\}$ .

Assim, por exemplo, um círculo, vermelho, grande e fino será identificado pelo código  $1311 - 4$ . Uma tabela com essa sugestão de código, referente às 48 peças dos blocos lógicos, pode ser encontrada no Anexo 1.

Observe que  $\text{mdc}(p_i, 5) = 1$  para  $i = \{1, 2, 3, 4\}$ , verificando a condição do Teorema 3.1 para detecção de erro singular. Agora, perceba que  $\text{mdc}(p_i - p_j, 5) = 1$  para  $i, j \in \{1, 2, 3, 4\}$ , verificando a condição do Teorema 3.2 para detecção de erros de transposição. Portanto, a

escolha por este modelo não é aleatória uma vez que ele detecta todos os casos de erro singular e de transposição.

Vale ressaltar que outros códigos podem ser elaborados pelo professor (ou pelos alunos) para identificação dos blocos lógicos nessa sequência de trabalho.

## 7.2 Metodologia

A proposta baseia-se na metodologia de Resolução de Problemas e Investigação Matemática discutidos por Polya [9] e Ponte [10] e está em consonância com as orientações apresentadas nos Parâmetros Curriculares Nacionais (PCN). Nesta concepção o aluno tanto aprende matemática resolvendo problemas, como aprende matemática para resolvê-los. Assim, guardada as devidas proporções, diante de um problema, o aluno se vê em uma situação análoga àquela em que muitas vezes o matemático está ao exercer sua atividade. Isto é, o aluno deve ser capaz de realizar tentativas, estabelecer hipóteses, testar essas hipóteses e validar seus resultados, provando que são verdadeiros ou, em caso contrário, mostrando algum contra-exemplo.

Essa opção de trabalho traz implícita a convicção de que o conhecimento matemático ganha significado quando os alunos têm situações desafiadoras para resolver, e trabalham coletivamente para desenvolver estratégias de resolução. Neste sentido, é fundamental que o professor estabeleça condições adequadas para a interação dos estudantes, criando um clima favorável à convivência em grupo de maneira produtiva e cooperativa.

A organização dos alunos em grupos de trabalho influencia o processo de ensino e aprendizagem, e pode ser otimizada quando o professor interfere nessa organização. Agrupamentos adequados, que levem em conta a diversidade dos alunos, tornam-se eficazes na individualização do ensino e atendimento à diversidade de aprendizagem. A esse respeito, os PCN trazem:

Como um incentivador da aprendizagem, o professor estimula a cooperação entre os alunos, tão importante quanto a própria interação professor-aluno. O confronto entre o que o aluno pensa e o que pensam seus colegas, seu professor e as demais pessoas com quem convive é uma forma de aprendizagem significativa, principalmente por pressupor a necessidade de formulação de argumentos (dizendo, descrevendo, expressando) e de validá-los (questionando, verificando, convencendo). (PCN, 1998, p. 38).

Assim, para o desenvolvimento dessa proposta, sugere-se a organização da turma em grupos de trabalho heterogêneos, compostos de 4 a 5 alunos em diferentes níveis de aprendizagem.

O trabalho nessa perspectiva exige do professor uma conduta diferente da aula tradicional. Neste papel, o professor é responsável por relatar os procedimentos empregados e as diferenças encontradas, promover o debate sobre resultados e métodos, orientar as reformulações e valorizar as soluções mais adequadas apresentadas por cada grupo. Ele também decide se é necessário prosseguir o trabalho ou se é o momento de elaborar uma síntese.

A sequência proposta é indicada para o trabalho com estudantes do 6º e 7º anos do Ensino Fundamental, sendo previsto, aproximadamente, quatro aulas de 50 minutos. Um maior tempo pode ser exigido em função dos diferentes níveis de aprendizagem da turma, conhecimento prévio sobre o tema e envolvimento com a dinâmica.

No que tange aos recursos didáticos, serão necessários: blocos lógicos, etiquetas adesivas, dicionário, folha de almaço, caneta, lápis, lápis de cor e borracha.

### 7.3 Objetivos

Os objetivos dessa sequência de trabalho são:

- Etiquetar as peças dos blocos lógicos.
- Vivenciar as ideias iniciais de transmissão de dados.
- Perceber a importância do dígito verificador.
- Conhecer a teoria dos códigos identificadores de erros.
- Calcular o dígito verificador de algumas peças.
- Reconhecer o uso dos códigos identificadores em situações do cotidiano.

### 7.4 Expectativas de aprendizagem

As expectativas de aprendizagem desenvolvidas nessa proposta serão:

- Reconhecer as figuras planas que têm a forma do quadrado, retângulo, triângulo e círculo.
- Classificar, ordenar e estabelecer padrões.
- Efetuar cálculos com números naturais envolvendo as operações de adição, subtração, multiplicação e divisão.
- Utilizar os conceitos de número primo, múltiplos e divisores de números naturais.

### 7.5 Sequência didática

A primeira etapa dessa sequência é a motivação para o trabalho com o tema. Oriente-se uma conversa informal sobre códigos e números de identificação. Também é interessante organizar uma pequena exposição de embalagens com códigos de barras, documentos pessoais, cartões de crédito, folha de cheque, livros, entre outros objetos que possuam números de identificação.

Para criar um ambiente estimulador, sugere-se ao professor fazer perguntas que despertem o interesse sobre o tema e permitir que os alunos façam o relato de alguma experiência pessoal. No final desse primeiro momento, caso nenhum aluno faça a sugestão, o professor deverá orientar a consulta ao dicionário e registro do significado da palavra *código*.<sup>4</sup> Pode-se aqui, manusear o dicionário observando o contexto semântico da palavra e selecionar a acepção mais adequada no verbete do dicionário.

Após esse primeiro momento, as caixas com os blocos lógicos serão entregues aos grupos e os alunos irão explorar o material livremente. Oriente-se ao professor fazer perguntas que

---

<sup>4</sup>Verbete no dicionário Aurélio: s.m. Coleção de leis: Código Penal. / Coleção de regras e preceitos. / Sistema de símbolos que permite a representação de uma informação: código Morse. / Conjunto de regras que permite a transposição de sistemas de símbolos sem alterar o significado da informação transmitida. / Linguística Conjunto de todos os elementos lingüísticos vigentes numa comunidade e postos à disposição dos indivíduos para servir-lhes de meios de comunicação; língua. // Código de barras, código que utiliza barras verticais, impresso na embalagem de um artigo e que, submetido a um leitor óptico, permite a identificação do artigo, seu preço e dados sobre seu estoque.

oportunizem aos grupos pensar sobre os atributos das peças. Em seguida, o professor solicitará aos alunos que formem conjuntos considerando características comuns das peças, isto é, a forma, a cor, o tamanho e a espessura. Nesta etapa, não se espera que os estudantes demonstrem dificuldades, embora seja interessante que o professor represente no quadro algum dos esquemas, tabelas ou desenhos utilizados pelos grupos como forma de registro.

Logo em seguida a exploração do material, o professor fixará, em local adequado para que todos possam visualizar, um cartaz com a relação que associa um algarismo a cada característica das peças, Figura 2 - Tabelas. O professor fará a leitura das tabelas esclarecendo possíveis dúvidas e apresentará a atividade a ser realizada:

- Etiquete cada peça com um código relacionando suas características aos dados das tabelas apresentados no cartaz.

É possível responder a questão com diferentes códigos, pois cada grupo pode estabelecer uma ordem distinta para os atributos das peças. Por exemplo, um grupo pode estabelecer que o 1º algarismo identifique a forma, o 2º a cor, o 3º o tamanho, o 4º a espessura e um outro grupo pode identificar as peças segundo o critério, espessura, cor, forma e tamanho.

O professor deverá explorar essa situação, pedindo aos grupos que digam alguns códigos e que os outros grupos tentem descobrir qual é a peça associada a esse código. O objetivo é que os alunos percebam a necessidade de se estabelecer um padrão e elaborem um código único para identificação das peças. Por exemplo:

1º algarismo → forma  
2º algarismo → cor  
3º algarismo → tamanho  
4º algarismo → espessura

Uma preocupação do professor neste momento deve ser que todos compreendam a situação problema proposta e participem das discussões.

Dando continuidade ao trabalho, o professor orientará que todos os grupos etiquetem os blocos lógicos. Aqui, o professor deve ficar atento para que todos os grupos utilizem a ordem estabelecida pela turma e os dados do cartaz, Figura 2 - Tabelas. Quando todos concluírem, o professor irá propor a transmissão de dados entre os grupos:

- Selecione 10 peças e anote a descrição em seu caderno.
- Escreva uma lista com o código que identifica cada uma das peças escolhidas.
- Envie a lista com os códigos a um outro grupo.

Nesta atividade, os alunos poderão perceber que identificar numericamente as peças simplifica e agiliza a transmissão de informações.

Após cada grupo transmitir e receber uma lista com os dez códigos o professor indicará a próxima atividade:

- Decodifique a lista que você recebeu.
- Identifique as peças escolhidas pelo outro grupo.
- Confira as informações com o outro grupo.

As atividades anteriores, estabelecer um código padrão e enviar mensagens entre os grupos, podem motivar o debate sobre segurança na transmissão de informações e erros na leitura, escrita e transmissão de dados. Sendo propício novas questões:

- Quais foram os erros cometidos na transmissão das listas?
- Há erros comuns aos grupos?
- Como evitar ou minimizar essas falhas?

É importante ressaltar que os grupos devem ser orientados a sistematizar e registrar as observações e as conclusões que forem surgindo durante o trabalho. Conceitos como erro singular e de transposição devem ser formalizados pelo professor.

Após discussão sobre os erros cometidos na transmissão e recepção de dados, o professor irá apresentar a teoria dos dígitos verificadores. Em sua exposição, o professor deve ressaltar a simplicidade dessa teoria, suas inúmeras aplicações no dia a dia e eficiência na detecção de erros. A situação proposta no Exemplo 3.1 ou o Código de Barras (Sistema EAN-13) pode ser utilizado para ilustrar o uso do dígito verificador e seu cálculo.

Retomando o trabalho com os blocos lógicos e o código de identificação criado, chegamos ao momento em que surge o grande desafio da proposta:

- Elabore uma fórmula para determinar o dígito verificador do código criado para identificação dos blocos lógicos.
- A fórmula elaborada estabelece uma relação com os primeiros algarismos?
- Essa fórmula é eficiente na detecção de erros?
- Quais as limitações do sistema elaborado pelo seu grupo?

Acredita-se que os alunos já se apropriaram do sentido do problema e espera-se que estejam motivados a buscar uma solução para essas questões e fazer novas perguntas. Nesse sentido, várias estratégias e ideias informais podem surgir e devem ser discutidas pela turma e valorizadas pelo professor.

É importante que o professor solicite o registro dos processos gerais utilizados na elaboração da fórmula para o cálculo do dígito verificador. E também, estimule as justificativas, pedindo aos alunos que mostrem se os códigos criados são adequados, do ponto de vista da detecção de erros. Neste ponto, esperamos que os estudantes percebam que a utilização de números primos torna o sistema mais eficiente.

Em seguida o professor pode apresentar (ou construir coletivamente) uma fórmula única para o cálculo do dígito verificador para a turma. Uma sugestão de sistema módulo 5 com pesos  $\{1, 2, 3, 4\}$  foi apresentada na Seção 5.1 e uma tabela com os códigos para as 48 peças dos blocos lógicos segundo esse sistema encontra-se no Anexo 1.

Neste momento é importante que o professor faça uma síntese dos conceitos trabalhados: algoritmo da divisão, resto da divisão, números primos, divisores e múltiplos de números naturais.

Para verificar se os estudantes compreenderam o algoritmo elaborado para o cálculo do 5º algarismo, o professor poderá escolher algumas peças e pedir que os alunos calculem o dígito verificador. Outra estratégia é escrever alguns códigos inválidos, ou faltando um dos dígitos e solicitar que os alunos tentem encontrar o erro e em seguida corrigi-lo.

Para finalizar, os grupos irão produzir um relatório, descrevendo a prática, as conclusões e os conceitos matemáticos envolvidos, incluindo uma autoavaliação e a avaliação da atividade.

## 7.6 Avaliação e encerramento

Esta sequência de trabalho deve fazer parte do processo de ensino e aprendizagem e como tal precisa ser avaliada. Avaliar permite ao professor e ao estudante monitorar o desempenho e verificar quais aspectos precisam ser melhor trabalhados. Assim, os grupos irão produzir um relatório, descrevendo a prática, as conclusões e os conceitos matemáticos envolvidos, bem como deverão ser incentivados a realizar uma autoavaliação e a avaliação da atividade.

Durante os trabalhos, o professor deverá avaliar os estudantes, observando a postura, as estratégias que desenvolvem, a capacidade de argumentar e utilizar a linguagem e simbologia própria da matemática. Desenhos, esquemas e tabelas também devem ser valorizados como forma de registro.

Pode ocorrer que os relatórios produzidos pelos estudantes sejam inicialmente pouco desenvolvidos, com respostas curtas e justificativas insuficientes ou não fundamentadas. Uma alternativa, para sanar essa dificuldade, é fornecer roteiros e indicar, durante a discussão nos grupos, pontos importantes de serem mencionados nos relatos.

Outra possibilidade de avaliação é uma apresentação oral para a classe, onde cada grupo explicará a proposta elaborada para o cálculo do dígito verificador e a matemática envolvida em suas investigações.

## 8 Considerações Finais

Neste trabalho abordou-se as noções básicas de Teoria dos Números e sua aplicação no cálculo do dígito verificador de Sistemas de Identificação Modular.

Versou-se sobre a utilização dos números de identificação no cotidiano e os erros cometidos na leitura, escrita e transmissão destes números. Recorreu-se a Aritmética Modular para generalizar os sistemas de identificação estudados e percebeu-se a importância dos Teoremas 3.1 e 3.2 para a construção de novos sistemas modulares.

Foram apresentados três exemplos concretos de sistema de identificação em utilização no país: o CPF, o ISBN e o cartão de crédito. Situações concretas foram utilizadas para ilustrar a aplicação destes modelos e para uma melhor compreensão da estrutura de cada sistema.

Uma proposta de aplicação da teoria dos códigos foi didaticamente descrita para o trabalho com estudantes do ensino fundamental. A sequência didática recorreu a exploração dos blocos lógicos para criar um ambiente motivador e estimulador da aprendizagem.

Problemas relativos a correção de erros não foram discutidos neste texto. Acredita-se ser necessário a realização de estudos posteriores para melhor compreensão de métodos que possam além de detectar os erros, fazer sua correção automática. Os chamados Sistemas Corretores de Erros.

Espera-se que a realização da prática em sala de aula contribua para o desenvolvimento dos alunos e fomenta o interesse por projetos e atividades de investigação e exploração.

Em relação aos professores, deseja-se ter cumprido o objetivo de motivar um estudo mais aprofundado sobre Aritmética Modular, mostrando como ideias e conceitos matemáticos levam ao desenvolvimento de tecnologias que visam o avanço e o bem estar social.

Enfim, acredita-se que este trabalho possa contribuir para que alunos e professores construam uma visão mais completa da verdadeira natureza da atividade matemática. E percebam que o estudo de temas aparentemente abstratos como *Sistemas de Identificação Modular* é uma fantástica oportunidade de aprendizagem, possibilitando momentos de reflexão, investigação e construção de conhecimento que, em geral, não observamos no dia-a-dia da sala de aula.

# ANEXO 1

| PEÇA | VETOR PESO |   |   |   | DV* |
|------|------------|---|---|---|-----|
|      | 1          | 2 | 3 | 4 |     |
| 1    | 1          | 1 | 1 | 1 | 0   |
| 2    | 1          | 1 | 1 | 2 | 4   |
| 3    | 1          | 1 | 2 | 1 | 3   |
| 4    | 1          | 1 | 2 | 2 | 2   |
| 5    | 1          | 2 | 1 | 1 | 2   |
| 6    | 1          | 2 | 1 | 2 | 1   |
| 7    | 1          | 2 | 2 | 1 | 0   |
| 8    | 1          | 2 | 2 | 2 | 4   |
| 9    | 1          | 3 | 1 | 1 | 4   |
| 10   | 1          | 3 | 1 | 2 | 3   |
| 11   | 1          | 3 | 2 | 1 | 2   |
| 12   | 1          | 3 | 2 | 2 | 1   |
| 13   | 2          | 1 | 1 | 1 | 1   |
| 14   | 2          | 1 | 1 | 2 | 0   |
| 15   | 2          | 1 | 2 | 1 | 4   |
| 16   | 2          | 1 | 2 | 2 | 3   |
| 17   | 2          | 2 | 1 | 1 | 3   |
| 18   | 2          | 2 | 1 | 2 | 2   |
| 19   | 2          | 2 | 2 | 1 | 1   |
| 20   | 2          | 2 | 2 | 2 | 0   |
| 21   | 2          | 3 | 1 | 1 | 0   |
| 22   | 2          | 3 | 1 | 2 | 4   |
| 23   | 2          | 3 | 2 | 1 | 3   |
| 24   | 2          | 3 | 2 | 2 | 2   |
| 25   | 3          | 1 | 1 | 1 | 2   |
| 26   | 3          | 1 | 1 | 2 | 1   |
| 27   | 3          | 1 | 2 | 1 | 0   |
| 28   | 3          | 1 | 2 | 2 | 4   |
| 29   | 3          | 2 | 1 | 1 | 4   |
| 30   | 3          | 2 | 1 | 2 | 3   |
| 31   | 3          | 2 | 2 | 1 | 2   |
| 32   | 3          | 2 | 2 | 2 | 1   |
| 33   | 3          | 3 | 1 | 1 | 1   |
| 34   | 3          | 3 | 1 | 2 | 0   |
| 35   | 3          | 3 | 2 | 1 | 4   |
| 36   | 3          | 3 | 2 | 2 | 3   |
| 37   | 4          | 1 | 1 | 1 | 3   |
| 38   | 4          | 1 | 1 | 2 | 2   |
| 39   | 4          | 1 | 2 | 1 | 1   |
| 40   | 4          | 1 | 2 | 2 | 0   |
| 41   | 4          | 2 | 1 | 1 | 0   |
| 42   | 4          | 2 | 1 | 2 | 4   |
| 43   | 4          | 2 | 2 | 1 | 3   |
| 44   | 4          | 2 | 2 | 2 | 2   |
| 45   | 4          | 3 | 1 | 1 | 2   |
| 46   | 4          | 3 | 1 | 2 | 1   |
| 47   | 4          | 3 | 2 | 1 | 0   |
| 48   | 4          | 3 | 2 | 2 | 4   |

\* Dígito Verificador (Resto da divisão por 5)

Figura 3: Etiquetas para as peças dos blocos lógicos

## Referências

- [1] Hefez, Abramo. *Elementos de aritmética*. SBM, 2<sup>a</sup> ed., Rio de Janeiro, 2011.
- [2] Kirtland, Joseph. *Indefication Numbers and Check Digit Schemes*. USA: The Mathematical Association of America, 2001.

- [3] Lourenço, Paulo Jorge Pais. *Aritmética Modular: aplicações nos sistemas de identificação*. Faculdade de Ciências e Tecnologia da Universidade de Coimbra, Coimbra, 2011.
- [4] Milies, Francisco César Polcino. *A matemática dos Códigos de Barras*. Revista do Professor de Matemática, v. 65, p. 46-53, 2008.
- [5] Milies, Francisco César Polcino. *A matemática dos códigos de barras: detectando erros*. Revista do Professor de Matemática, v. 68, p. 38-42, 2009.
- [6] Neto, Antonio Caminha Muniz. *Tópicos de Matemática Elementar, Teoria dos Números*. SBM, Coleção do Professor de Matemática, Vol.5, Rio de Janeiro, 2012.
- [7] Picado, Jorge. *A álgebra dos sistemas de identificação: da aritmética modular aos grupos diedrais*. Boletim da Sociedade Portuguesa de Matemática, nº 44, 2011.
- [8] Polya, George. *A arte de resolver problemas*. Rio de Janeiro: Editora Interciência, 2006.
- [9] Ponte, João Pedro da. *Investigações Matemáticas na Sala de Aula*. Belo Horizonte: Autêntica Editora, 2009.
- [10] Santos, José Plínio de Oliveira. *Introdução à Teoria dos Números*. IMPA, Rio de Janeiro, 2012.
- [11] Secretaria de Educação Fundamental. *Parâmetros Curriculares Nacionais: Matemática*. Brasília: MEC/SEF, 1998.
- [12] Simons, Ursula Marianne. *Blocos Lógicos*. Petrópolis, Rio de Janeiro. Editora Vozes, 2007.
- [13] Souza, Natália Pedroza de. *Uma análise dos esquemas de dígitos verificadores usados no Brasil*. Dissertação de Mestrado em Ciências Computacionais, Universidade do Estado do Rio de Janeiro, 2013.
- [14] [www.isbn.bn.br](http://www.isbn.bn.br). *Agência Brasileira do ISBN, Fundação Biblioteca Nacional*. Acesso em 08/02/2014.