Sistemas de Identificação Modular: Uma Aplicação no Ensino Fundamental

Modular Identification Systems: An Application in Elementary Education

Fernanda Rodrigues Alves Costa
Instituto Federal de Educação Ciências e Tecnologia de Minas Gerais - Belo Horizonte, MG
fernandaracosta@gmail.com

Marcelo Oliveira Veloso
Universidade Federal de São João del-Rei - UFSJ, Ouro Branco, MG
veloso@ufsj.edu.br

Resumo: Neste trabalho realizamos um breve estudo sobre os sistemas de identificação modular que detectam erros cometidos durante a transmissão, digitação ou leitura de dados. Listamos os erros mais frequentes cometidos por um operador ao digitar um número. Em particular, descrevemos três exemplos de sistemas de identificação modular, o CPF, o ISBN e o cartão de crédito, analisando-os em relação à capacidade de detectarem erros. Por fim, recomendamos uma aplicação direta em sala de aula utilizando o recurso dos blocos lógicos.

Palavras-chave: sistemas de identificação de erros; aritmética modular; blocos lógicos.

Abstract: In this paper we perform a brief study on modular identification systems that detects errors committed during transmission, typing or data reading. We list the most frequent mistakes made by an operator when entering a number. In particular, we describe three examples of modular identification systems, the CPF, the ISBN and the credit card, analyzing them for the ability to detect errors. Finally, we recommend a direct application in the classroom using the logic blocks.

Key words: error identification systems; modular arithmetic; logic blocks.

1 Introdução

"Os erros são quase sempre de uma natureza sagrada. Nunca tente corrigi-los. 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.

Recebido em 15/09/2017 - Aceito em 24/11/2017
RECEN 19(2) p.248-265 jul/dez 2017 DOI:10.5935/RECEN.2017.02.08

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.

Neste artigo apresentamos um breve estudo dos sistemas de identificação modular e exemplos que são avaliados quanto à capacidade de detectar erros. Além disso, propomos uma sequência didática para o desenvolvimento do tema com alunos do Ensino Fundamental.

O principal objetivo deste trabalho é servir como material de apoio para os professores de matemática, principalmente os que lecionam no Ensino Fundamental, em aulas sobre aritmética e suas aplicações. Proporcionado aos alunos uma oportunidade para refletirem, investigarem e construírem o próprio conhecimento. E exemplificar como ideias e conceitos abstratos levam ao desenvolvimento de tecnologias que estão presentes no nosso cotidiano e que visam o bem estar de toda a sociedade.

O texto foi organizado da seguinte maneira: na seção 2, apresentamos as conceitos básicos que fundamentam o trabalho. Na seção 3, discutimos sobre os tipos de erros cometidos ao digitar um número de identificação, definimos os sistemas de identificação modular e estabelecemos as condições para que os sistemas possam detectar determinados tipos de erros. Nas seções 4, 5 e 6 descrevemos, respectivamente, três exemplos concretos de sistema de identificação em utilização no Brasil: o CPF, o ISBN e o cartão de crédito. Para uma melhor compreensão da estrutura de cada um destes modelos analisamos situações concretas. Estes sistemas também são avaliados em relação a capacidade de detecção de erros. Na seção 7 apresentamos uma possibilidade de trabalho deste tema com alunos a partir do 6º ano 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. Por fim, na seção 8, apresentamos as considerações finais.

2 Conceitos iniciais

Nesta seção, apresentamos algumas definições e propriedades referentes à Teoria dos Números, mais especificamente à Aritmética Modular. Um estudo mais detalhado desse tema pode ser encontrado em [1, 2, 3].

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

Definição 2.1 *Sejam a e b números inteiros com $a \neq 0$. Dizemos que a divide b e denotamos 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 $6 = 2.3$, 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.*

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

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 igualdades por m e n, respectivamente, temos $ma = mck_1$ e $nb = nck_2$. Somando membro a membro, obtemos $ma + nb = c(mk_1 + nk_2)$. Assim, segue da Definição 2.1 que $c \mid (ma + nb)$. ■

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

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

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 $an - adc = 0$ e $a(n - dc) = 0$. Como $a \neq 0$, segue que $(n - dc) = 0$ e, portanto, $n = dc$.
4. Se $d \mid n$, temos que $n = dc$, $n \neq 0$ implica que $c \neq 0$. Portanto, $|c| \geq 1$ e $|n| = |dc| = |d||c| \geq |d|$.
5. Se $d \mid n$ e $n \mid d$, temos que $n = dk_1$ e $d = nk_2$, k_1, $k_2 \in \mathbb{Z}$. Então, $n = dk_1 = nk_2k_1$. Assim, $k_2k_1 = 1$, $k_1 = k_2 = \pm 1$ e, portanto, $|d| = |n|$.
6. Se $d \mid n$, então $n = dc$. Multiplicando ambos os lados desta igualdade por $m \in \mathbb{Z}$, temos $nm = dcm = d(cm)$. Assim, 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.

Demonstrado em Teorema 1.2 de [3].

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

Exemplo 2.2 *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 $a = q_1 m + r_1$ e $b = q_2 m + r_2$. Logo, $a - b = m(q_1 - q_2) + (r_1 - r_2)$ e $(a - b) - m(q_1 - q_2) = (r_1 - r_2)$.

Se $a \equiv b \pmod{m}$, temos que $m \mid (a - b)$ e $m \mid m(q_1 - q_2)$. 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, $a - b = m(q_1 - q_2)$. Como $m \mid m(q_1 - q_2)$, segue que $m \mid (a - b)$ e, pela Definição 2.4, que $a \equiv b \pmod{m}$. ■

Exemplo 2.3 *Como $21 = 2.10 + 1$ e $13 = 2.6 + 1$, 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 a Proposição 2.3).

Proposição 2.3 *Sejam a, b, c e m números inteiros com $m > 0$. 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 que $m \mid a - b$. 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 $a \equiv c \pmod{m}$.

■

O teorema a seguir estabelece que a relação de equivalência é compatível com as operações de adição e multiplicação no conjunto dos números 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. $a \equiv b \pmod{m}$ e $r \equiv s \pmod{m} \Rightarrow m \mid a - b$ 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. $a \equiv b \pmod{m}$ e $r \equiv s \pmod{m} \Rightarrow m \mid a - b$ 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 $mdc(a, b)$, é o inteiro positivo d que satisfaz:*

1. *$d \mid a$ e $d \mid b$;*
2. *Se existe um inteiro c tal que $c \mid a$ e $c \mid b$, então $c \leq d$.*

Exemplo 2.4 *Observe que $mdc(4, 14) = 2$ 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 não nulos. Se $c \mid ab$ e $mdc(b, c) = 1$ então $c \mid a$.*

Demonstração: Sejam $m, n \in \mathbb{Z}$ tais que $mb + nc = 1$. Multiplicando ambos os membros dessa igualdade por a, obtemos $(ab)m + c(an) = a$. Como $c \mid (ab)$, segue da Proposição 2.1 que $c \mid a$. ■

3 Sistemas de identificação modular

Frequentemente utilizamos 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 utiliza alguma informação redundante transmitida em simultâneo com o código que se pretende comunicar. Esta 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 ultimo 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 o operador sobre a ocorrência do mesmo. E, consequentemente, da necessidade de reescrever o número.

Os erros cometidos ao digitar um número foram sistematicamente investigados por autores como Beckley e Verhoeff, citados em [4, 5, 6]. Estas pesquisas revelam que cerca de 79% dos erros ocorrem com a digitação equivocada de um único dígito, como, por exemplo, digitar 1.573, quando o correto seria 1.673. Este tipo de erro recebe o nome de erro singular. Os chamados erros de transposição, cerca de 11% dos erros de digitação, são divididos em dois casos: os erros de transposição adjacente e os erros de transposição intercalada. O primeiro tipo corresponde à troca de posição de dois dígitos diferentes situados lado a lado, enquanto o segundo corresponde à troca de posição de dois dígitos diferentes intercalada por um terceiro dígito. Por exemplo, escrever 3.876, quando o correto seria 3.786 configura um erro de transposição adjacente, enquanto escrever o número 3.687 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 observamos na Tabela 1, que citamos abreviando tabela publicada em [4, 5, 6].

Tabela 1. *Tipos de erros*

Tipo de erro		**Frequêcia relativa**
erro singular	$\cdots a \cdots \to \cdots b \cdots$	79,1%
erro de transposição adjacente	$\cdots ab \cdots \to \cdots ba \cdots$	10,2%
erro de transposição intercalada	$\cdots acb \cdots \to \cdots bca \cdots$	0,8%
outros erros	–	9,9%
Total		100%

É necessário esclarecermos que existem especificidades em cada sistema de códigos ou até mesmo em cada idioma que podem mudar significativamente a distribuição de probabilidades da Tabela 1.

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

$$x_1x_2x_3\ldots x_nC,$$

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

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

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

Os sistemas deste tipo são chamados de *sistema módulo* k e a soma $p_1x_1 + p_2x_2 + \cdots + p_nx_n + C$, por soma controle ou soma teste, que iremos designar 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 $k \mid S$, ou seja, a soma teste é um múltiplo de k.

Analisemos 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 a solução da 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 a seguinte congruência:

$$\begin{aligned} 3 \cdot 8 + 1 \cdot 5 + 3 \cdot 4 + C &\equiv 0 \pmod{10}; \\ 24 + 5 + 12 + C &\equiv 0 \pmod{10}; \\ 41 + C &\equiv 0 \pmod{10}. \end{aligned}$$

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 $3 \cdot 7 + 1 \cdot 6 + 3 \cdot 3 + 2 = 38$ e $38 \not\equiv 0 \pmod{10}$.

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 $\{p_1, p_2, \ldots, p_n\}$, detecta todo erro singular $a_i \to a_i'$, na $i-$ésima posição, se, e somente se, $mdc\,(p_i, k) = 1$.*

Demonstração: Considere um número $a_1a_2a_3\cdots a_n$ 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 $a_i \to a_i'$ na $i-$ésima posição. Neste caso, $a_i \neq a_i'$. Apesar do erro cometido é possível termos $S' \equiv 0 \pmod{k}$ e assim não podemos detectar o erro. Caso contrário, $S' \not\equiv 0 \pmod{k}$, podemos detectar o erro.

Contudo se considerarmos a diferença

$$\begin{aligned} S' - S &= (p_1a_1 + p_2a_2 + \cdots + p_ia_i' + \cdots + p_na_n) - (p_1a_1 + p_2a_2 + \cdots + p_ia_i + \cdots + p_na_n) \\ &= p_ia_i' - p_ia_i \\ &= p_i(a_i' - a_i), \end{aligned}$$

observamos que um erro singular $a_i \to a_i'$, na $i-$ésima posição, é detectável se, e somente se, $p_i(a_i' - a_i) \not\equiv 0 \pmod{k}$. É fácil ver que $p_i(a_i' - a_i) \not\equiv 0 \pmod{k}$ se, e somente se, $mdc\,(p_i, k) = 1$. De fato, suponha que $p_i(a_i' - a_i) \not\equiv 0 \pmod{k}$ e $mdc\,(p_i, k) = d > 1$. Então $p_i = dd_1$ e $k = dd_2$, com $d_2 \in \{0, 1, 2, \cdots, k-1\}$. Agora observe que para $a_i' = d_2$ e $a_i = 0$ obtemos

$$p_i a_i' = pd_2 = dd_1 d_2 = d_1 dd_2 = d_1 k \equiv 0 \pmod{k}$$

e assim $p(a_i' - a_i) \equiv 0 \pmod{k}$. Absurdo! Portanto, $d = 1$. Por outro lado, suponha que $mdc\,(p_i, k) = 1$ e $p(a_i' - a_i) \equiv 0 \pmod{k}$. Então $k \mid p_i(a_i' - a_i)$ e segue da Proposição 2.4 que $k \mid (a_i' - a_i)$. Temos novamente um absurdo, pois $(a_i' - a_i) \in \{0, 1, 2, \cdots, k-1\}$. Verificando nossa afirmação. Portanto, um erro singular $a_i \to a_i'$, na $i-$ésima posição, é detectável se, e somente se, $mdc\,(p_i, k) = 1$. ■

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

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

$$\begin{aligned} S' - S &= (p_1a_1 + \cdots + p_ia_j + \cdots + p_ja_i + \cdots + p_na_n) - (p_1a_1 + \cdots + p_ia_i + \cdots + p_ja_j + \cdots + p_na_n) \\ &= p_ia_j + p_ja_i - p_ia_i - p_ja_j \\ &= p_i(a_j - a_i) + p_j(a_j - a_i) \\ &= (p_i - p_j)(a_j - a_i). \end{aligned}$$

Portanto, o sistema detecta todas as transposições de algarismos nas posições i e j se para quaisquer $a_i, a_j \in \{0, 1, 2, ..., k-1\}$ com $a_i \neq a_j$, temos $(p_i - p_j)(a_j - a_i) \not\equiv 0 \pmod{k}$. De modo análogo à demonstração do teorema anterior, esta condição é equivalente a $mdc\,(p_i - p_j, k) = 1$. ■

Estes resultados justificam uma maior utilização de sistemas módulo 11, pela facilidade de encontrar pesos primos com 11, usando apenas um carácter para o 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, utilizamos o 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 algarismo 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.

É necessário destacarmos a importância dos Teoremas 3.1 e 3.2 como mecanismos para a construção de novos sistemas modulares.

4 Número do CPF

O Cadastro de Pessoas Físicas, mais conhecido como CPF, é o registro de um cidadão na Receita Federal brasileira. Neste registro 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 [7], permite calcular os dígitos de controle.

$$x_{10} = \left(\sum_{i=1}^{9} i x_i \pmod{11} \right) \pmod{10};$$
$$x_{11} = \left(\sum_{i=2}^{10} (i-1) x_i \pmod{11} \right) \pmod{10}.$$

Com a finalidade de ilustrar a aplicação do 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 obtemos a seguinte expressão para x_{10}:

$x_{10} = ((1.\mathbf{0} + 2.\mathbf{4} + 3.\mathbf{3} + 4.\mathbf{6} + 5.\mathbf{5} + 6.\mathbf{8} + 7.\mathbf{3} + 8.\mathbf{0} + 9.\mathbf{6}) \pmod{11}) \pmod{10};$
$x_{10} = ((0 + 8 + 9 + 24 + 25 + 48 + 21 + 0 + 54) \pmod{11}) \pmod{10};$
$x_{10} = ((189 \pmod{11})) \pmod{10};$
$x_{10} = 2 \pmod{10};$
$x_{10} = 2.$

O resultado confirma o valor do primeiro dígito verificador. Calculemos agora o segundo dígito, x_{11}:

$x_{11} = ((1.\mathbf{4} + 2.\mathbf{3} + 3.\mathbf{6} + 4.\mathbf{5} + 5.\mathbf{8} + 6.\mathbf{3} + 7.\mathbf{0} + 8.\mathbf{6} + 9.\mathbf{2}) \pmod{11}) \pmod{10};$
$x_{11} = ((4 + 6 + 18 + 20 + 40 + 18 + 0 + 48 + 18) \pmod{11}) \pmod{10};$
$x_{11} = ((172 \pmod{11})) \pmod{10};$
$x_{11} = 7 \pmod{10};$

$x_{11} = 7$.

Os cálculos confirmam o valor do segundo dígito de controle. Assim, concluímos 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.

O 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 fosse feita de forma mais criteriosa. Mesmo assim, a falha na detecção de erros é de apenas 0,22% nos casos de erro singular e de 0,17% nos erros de transposição. A demonstração destes resultados pode ser encontrada em [7], 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 $\{9, 8, 7, 6, 5, 4, 3, 2, 9, 8\}$.

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 [6], 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)[1]. 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 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 número 85 o identificador do Brasil. 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 ao 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, determinaremos o dígito verificador deste sistema resolvendo a equação abaixo, adaptada de [8]:

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

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 de verificação é 6 porque

$$S=\mathbf{9}+3.\mathbf{7}+\mathbf{8}+3.\mathbf{8}+\mathbf{5}+3.\mathbf{0}+\mathbf{1}+3.\mathbf{0}+\mathbf{6}+3.\mathbf{1}+\mathbf{9}+3.\mathbf{6}+\mathbf{6},$$
$$S=9+21+8+24+5+0+1+0+6+3+9+18+6=110\equiv 0 \pmod{10}.$$

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

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

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 do Teorema 3.2, uma vez que $mdc(2,10)=2>1$. ■

Exemplo 5.1 *Se $a_9=6$ e $a_8=1$ forem trocados teríamos $S'-S=2(a_9-a_8)=2.5=10$ e o erro não seria detectado.*

[1]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.

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

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

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

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

Logo, o sitema 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; o último dígito, na extremidade direita, representa o dígito verificador.

Esse dígito é utilizado para decidir se um cartão de crédito é válido e pode ser calculado por uma fórmula chamada *Algoritmo de Luhn*. Segundo [9], 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 o número dos cartões de crédito e de débito.

Constatamos a autenticidade de um cartão resolvendo a equação que segue, adaptada de [7, 9]: $\overline{2x_1}+x_2+\overline{2x_3}+x_4+\overline{2x_5}+x_6+\overline{2x_7}+x_8+\overline{2x_9}+x_{10}+\overline{2x_{11}}+x_{12}+\overline{2x_{13}}+x_{14}+\overline{2x_{15}}+C \equiv 0 \pmod{10}$, onde x_i é o algarismos do número do cartão na posição i e C o algarismo de controle. Temos ainda que:

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

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 infor-

mação faz as seguintes operações:

$$\begin{aligned} S &= 2.\mathbf{4} + \mathbf{0} + 2.\mathbf{7} + \mathbf{2} + 2.\mathbf{0} + \mathbf{3} + 2.\mathbf{8} + \mathbf{8} + 2.\mathbf{7} + \mathbf{0} + 2.\mathbf{4} + \mathbf{8} + 2.\mathbf{0} + \mathbf{9} + 2.\mathbf{7} + \mathbf{1} \\ &= 8 + 0 + 14 + 2 + 0 + 3 + 16 + 8 + 14 + 0 + 8 + 8 + 0 + 9 + 14 + 1 \\ &= 8 + 0 + (14 - 9) + 2 + 0 + 3 + (16 - 9) + 8 + (14 - 9) + 0 + 8 + 8 + 0 + 9 + (14 - 9) + 1 \\ &= 8 + 0 + 5 + 2 + 0 + 3 + 7 + 8 + 5 + 0 + 8 + 8 + 0 + 9 + 5 + 1 \\ &= 69. \end{aligned}$$

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 em um algarismo com índice par ou o erro ocorre em um algarismo de índice ímpar.

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

No caso de erro em um 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 transformações a seguir.

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

Se S' fosse múltiplo de 10, teríamos que $10 \mid (S' - S)$. Logo, 10 dividiria $(\overline{2a_i'} - \overline{2a_i})$, o que é um absurdo, pois $(\overline{2a_i'} - \overline{2a_i})$ é um número inteiro não nulo entre -9 e 9. ■

Portanto, 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 [7].

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 Proposta didática

Nesta seção, propomos uma sequência didática para trabalhar com os estudantes do Ensino Fundamental o tema identificadores de erros, utilizando os blocos lógicos como recurso didático. Esperamos com o desenvolvimento desta proposta que os alunos, realizando apenas operações aritméticas, compreendam a tecnologia dos códigos identificadores de erros.

Os blocos lógicos foram criados na década de 50 pelo matemático húngaro Zoltan Paul Dienes. Segundo [10], o modelo mais utilizado nas escolas brasileiras tem 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.

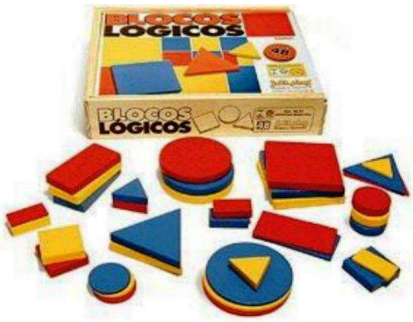

Figura 1. Blocos Lógicos

Assim, cada peça possui quatro atributos. Por exemplo, podemos ter um círculo, vermelho, grande e fino. O objetivo da sequência é propor atividades que estimulem os estudantes a determinar um código que identifique cada peça e a transmitir uma lista de peças utilizando o código construído por eles. Esta atividade permitirá que os alunos percebam como identificar um artigo por uma sequência numérica agiliza a transmissão de informações e a importância do dígito verificador para identificação de possíveis erros durante a transmissão, digitação ou leitura de dados.

Para o desenvolvimento dessa proposta, sugerimos a organização da turma em grupos de trabalho heterogêneos, compostos de 4 a 5 alunos em diferentes níveis de aprendizagem. Orientamos iniciar a discussão com uma conversa informal sobre códigos e números de identificação. É interessante preparar uma pequena exposição de embalagens com códigos de barras, documentos pessoais, cartões bancários, folhas de cheque, livros, entre outros objetos que possuam número de identificação.

Após esse primeiro momento, os grupos deverão iniciar a exploração livre dos blocos lógicos. É importante que o professor faça perguntas que oportunize aos alunos discutir sobre as características das peças e agrupar as peças considerando diferentes critérios. Nesta etapa, não se espera que os estudantes demonstrem dificuldades, embora seja interessante que o professor represente no quadro alguns dos esquemas, tabelas ou desenhos utilizados pelos grupos como forma de registro.

Logo após a exploração do material, o professor deverá apresentar a proposta de atividade para a turma. A tarefa será estabelecer um código que identificará cada uma das peças e transmitir para outro grupo uma mensagem contendo uma lista com o código de pelo menos 10 peças. Esperamos que o professor incentive a turma a discutir sobre as diferentes possibilidades de solucionar a situação proposta e a perceber a importância de estabelecer um código padrão.

A seguir, apresentamos na Figura 2 uma possibilidade de associação entre um algarismo e uma característica das peças.

Ressaltamos que diferentes códigos podem ser elaborados pelo professor, ou pelos alunos, para identificação dos blocos lógicos nessa proposta de trabalho. Sugerimos uma sequência

FORMA	ALGARISMO
Círculo	1
Quadrado	2
Triângulo	3
Retângulo	4

COR	ALGARISMO
Amarelo	1
Azul	2
Vermelho	3

TAMANHO	ALGARISMO
Grande	1
Pequeno	2

ESPESSURA	ALGARISMO
Fino	1
Grosso	2

Figura 2. Sugestão de algarismo por característica da peça

de 5 algarismos, onde o 1º algarismo identifica a forma, o 2º a cor, o 3º o tamanho, o 4º a espessura e o 5º é o dígito verificador calculado a partir dos anteriores. 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 $x_1 + 2x_2 + 3x_3 + 4x_4$. Este é um sistema módulo 5 com pesos $\{1, 2, 3, 4\}$. Assim, por exemplo, um círculo, vermelho, grande e fino será identificado pelo código $1311 - 4$. Oserve que $mdc\,(p_i, 5) = 1$ para $i = \{1, 2, 3, 4\}$, verificando a condição do Teorema 3.1 para detecção de erro singular. Como $mdc\,(p_i - p_j, 5) = 1$ para $i, j \in \{1, 2, 3, 4\}$, a condição do Teorema 3.2 para detecção de erros de transposição é verificada. Portanto, a escolha por este modelo não é aleatória uma vez que ele detecta todos os casos de erro singular e de transposição.

Retomando a atividade, é possível que mesmo o professor apresentando a relação estabelecida na Figura 2, os grupos respondam a questão com diferentes códigos, pois podem estabelecer ordens distintas 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. É importante que os alunos percebam a necessidade de se estabelecer um padrão e elaborem um código único para identificação das peças. Por exemplo:

$$1^o\ algarismo \rightarrow forma;$$
$$2^o\ algarismo \rightarrow cor;$$
$$3^o\ algarismo \rightarrow tamanho;$$
$$4^o\ algarismo \rightarrow espessura.$$

Antes dos alunos iniciarem o processo de etiquetar as peças dos blocos lógicos, o professor verificará se todos os grupos compreenderam o padrão estabelecido pela turma. Neste momento é interessante fixar um cartaz ou anotar no quadro o código definido pela turma e que deverá ser utilizado por todos os grupos. Esperamos que os alunos percebam que identificar numericamente as peças simplifica e agiliza a transmissão de informações.

Após cada grupo etiquetar, transmitir e receber uma lista com pelo menos dez códigos, iniciasse a etapa de decodificar e conferir os dados recebidos com os emissores. O professor deverá motivar o debate sobre segurança na transmissão de informações e erros na leitura, escrita e transmissão de dados, sendo propício novas questões para discussão, tais como: Quais foram os erros cometidos na transmissão das listas? Há erros comuns aos grupos? Há formas de evitar ou minimizar essas falhas?

É importante ressaltar que os alunos, individualmente ou em grupo, devem ser orientados a sistematizar e registrar as observações, os questionamentos e as conclusões que forem surgindo durante o trabalho.

Após a discussão sobre os erros cometidos na transmissão e recepção de dados, o professor apresentará a teoria dos dígitos verificadores. Conceitos como erro singular e de transposição devem ser formalizados. Em sua exposição, o professor ressaltará a simplicidade dessa teoria, suas inúmeras aplicações no dia a dia e a 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 elaborado pela turma, chegamos ao momento em que surge o grande desafio da proposta: elaborar uma fórmula para determinar o dígito verificador do código criado para identificação dos blocos lógicos. O professor deve levantar algumas questões: A fórmula elaborada pela turma estabelece uma relação com os primeiros algarismos? É eficiente na detecção de erros? Quais as limitações do sistema elaborado pelo seu grupo?

Neste ponto, pressupomos que os alunos se apropriaram do sentido do problema, estejam motivados a buscar uma solução para essas questões e a fazer novas perguntas. Assim, várias estratégias e ideias informais podem surgir durante a discussão e precisam ser valorizadas pelo professor. A realização de simulações para verificar a eficiência do dígito verificador construído pelos grupos deve ser reconhecida e estimulada.

Recomendamos 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, os estudantes devem perceber 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 no início desta seção.

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 5^{o} algarismo, o professor pode 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, indicamos a produção de um relatório descrevendo a prática, as conclusões e os conceitos matemáticos envolvidos. 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 a serem mencionados nos relatos.

8 Considerações finais

Neste trabalho abordamos as noções básicas de Teoria dos Números e sua aplicação no cálculo do dígito verificador de sistemas de identificação modular. Discutimos sobre a utilização dos números de identificação no cotidiano e os erros cometidos na leitura, escrita e transmissão destes números. Recorremos à Aritmética Modular para generalizar os siste-

mas de identificação estudados e destacamos a importância dos Teoremas 3.1 e 3.2 para a construção de novos sistemas modulares. Apresentamos 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 descrita para o trabalho com estudantes do Ensino Fundamental. A sequência didática recorreu à exploração dos blocos lógicos para criar um ambiente motivador e estimulador à aprendizagem.

Problemas relativos a correção de erros não foram discutidos neste texto. Acreditamos 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.

Professores de matemática, que atuam principalmente no Ensino Fundamental, poderão utilizar este trabalho como um instrumento para o desenvolvimento de aulas de aritmética. Para tanto, buscamos utilizar uma linguagem simples e objetiva, apresentando ao longo do texto exemplos e situações concretas que auxiliam o professor no planejamento de aulas.

Além disso, esperamos que a realização da prática em sala de aula contribua para o desenvolvimento dos alunos e fomente o interesse por projetos e atividades de investigação e exploração. Desejamos, também, 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, acreditamos 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 oportunidade ímpar de aprendizagem, possibilitando momentos de reflexão, investigação e construção de conhecimento que, em geral, não observamos no dia-a-dia da sala de aula. Confiamos também, que, motivados por este, outros trabalhos possam ser elaborados apresentando aplicações da matemática afim de serem desenvolvidos na Educação Básica.

9 Agradecimentos

Agradecemos à Coordenação de Aperfeiçoamento Pessoal de Nível Superior (CAPES) pela concessão de bolsa de estudo durante todo o período de realização do curso, Mestrado Profissional em Matemática (PROFMAT), e pela histórica contribuição no desenvolvimento da educação e da ciência brasileira.

Referências

[1] HEFEZ, A. Elementos de Aritmética. 2. ed., SBM, Rio de Janeiro, 2011.

[2] NETO, A. C. M. Tópicos de Matemática Elementar: Teoria dos Números. Coleção do Professor de Matemática, v. 5, SBM, Rio de Janeiro, 2012.

[3] SANTOS, J. P. O. Introdução à Teoria dos Números. IMPA, Rio de Janeiro, 2012.

[4] MILIES, F. C. P. A matemática dos códigos de barras. *Revista do Professor de Matemática*, v. 65, p. 46-53, 2008.

[5] MILIES, F. C. P. A matemática dos códigos de barras: detectando erros. *Revista do Professor de Matemática*, v. 68, p. 38-42, 2009.

[6] PICADO, J. A álgebra dos sistemas de identificação: da artmética modular aos grupos diedrais. *Boletim da Sociedade Portuguesa de Matemática*, nº 44, 2011.

[7] SOUZA, N. P. Uma análise dos esquemas de dígitos verificadores usados no Brasil. Dissertação (Mestrado), UERJ, 2013.

[8] LOURENÇO, P. J. P. Aritmética Modular: aplicações nos sistemas de identificação. Faculdade de Ciências e Tecnologia da Universidade de Coimbra, Coimbra, 2011.

[9] KIRTLAND, J. Indefication Numbers and Check Digit Schemes. USA: The Mathematical Association of America, 2001.

[10] SIMONS, U. M. Blocos Lógicos. Vozes, Petrópolis, 2007.