Universidade Federal do Piauí

Centro de Ciências da Natureza

Pós-Graduação em Matemática

Mestrado Profissional em Matemática - PROFMAT

Introdução aos Métodos de Detecção de Erros em Sequências Numéricas

Sérgio Adriano Marques da Silva

Teresina - 2017

Sérgio Adriano Marques da Silva

Dissertação de Mestrado:

Introdução aos Métodos de Detecção de Erros em Sequências Numéricas

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Matemática, da Universidade Federal do Piauí, como requisito parcial para obtenção do grau de Mestre em Matemática, pelo programa PROFMAT - Mestrado Profissional em Matemática em Rede Nacional.

Orientador:
Prof. Dr. Gilvan Lima de Oliveira

Teresina - 2017

FICHA CATALOGRÁFICA
Serviço de Processamento Técnico da Universidade Federal do Piauí
Biblioteca Setorial do CCN

S586i Silva, Sérgio Adriano Marques da.
Introdução aos métodos de detecção de erros em sequências numéricas / Sérgio Adriano Marques da Silva. – Teresina, 2017.
55f. il.

Dissertação (Mestrado Profissional/PROFMAT) – Universidade Federal do Piauí, Centro de Ciências da Natureza, Pós-Graduação em Matemática, 2017.
Orientador: Prof. Dr.Gilvan Lima de Oliveira.

1. Matemática. 2. Sequência Numérica. 3. Dígito Verificador. I. Título

CDD 510

PROFMAT

UNIVERSIDADE FEDERAL DO PIAUÍ
CENTRO DE CIÊNCIAS DA NATUREZA
CENTRO DE EDUCAÇÃO ABERTA E À DISTÂNCIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

SBM

Dissertação de Mestrado submetida à coordenação Acadêmica Institucional, na Universidade Federal do Piauí, do Programa de Mestrado Profissional em Matemática em Rede Nacional para obtenção do grau de **Mestre em Matemática** intitulada: **Introdução aos Métodos de Detecção de Erros em Sequências Numéricas**, defendida **Sérgio Adriano Marques da Silva** em **14 / 08 / 2017** e aprovada pela Banca Examinadora constituída pelos professores:

Dr. Gilvan Lima de Oliveira (UFPI)
Presidente da Banca Examinadora

Dr. Jurandir de Oliveira Lopes (UFPI)
Examinador Interno

Me. Edson da Silva Lira (IFMA – Campus de Timon/MA)
Examinador Externo

À minha família e aos que torcem sinceramente por mim.

Agradecimentos

Agradeço a Deus por sua infinita misericórdia o por me permitir ter conquistas como este mestrado, em seu imenso amor.

Agradeço a minha família, minha grande riqueza, com quem sempre pude contar.

Agradeço aos professores do curso, que pacientemente e de maneira notável me transmitiram tanto conhecimento matemático como um pouco de sua experiência como profissionais. Trago aqui um profundo lamento pelo falecimento do professor João Benício de Melo Neto.

Agradeço meu orientador, que me indicou um tema, avaliou meu trabalho e me deu as orientações necessárias para que eu pudesse apresentar meus resultados.

Agradeço meus colegas de curso, com os quais socializei bastante, conhecendo realidades e opiniões diferentes da minha, e dos quais obtive muita ajuda no decorrer deste mestrado.

Agradeço finalmente a CAPES pelo apoio financeiro, que ajudou a custear transporte, alimentação e compra de livros, a SBM (Sociedade Brasileira de Matemática) por promover o PROFMAT, e à Universidade Federal do Piauí, por ser um polo de execução do programa.

"*Se te vendermos a nossa terra, ama-a como nós a amávamos. Proteje-a como nós a protegíamos. Nunca esqueças de como era esta terra quando dela tomaste posse: E com toda a tua força o teu poder e todo o teu coração - conserva-a para teus filhos e ama-a como Deus nos ama a todos. De uma coisa sabemos: o nosso Deus é o mesmo Deus, esta terra é por ele amada. Nem mesmo o homem branco pode evitar o nosso destino comum*".

Cacique Seattle, 1854

Resumo

Este trabalho apresenta os principais métodos de detecção de erros de transmissão de sequências numéricas pelo cálculo do dígito verificador, incluindo na discussão os seguintes tópicos: tipos de erros, os métodos de detecção pela Aritmética Modular e pelo grupo diedral D_5, a eficiência de cada um e algumas aplicações reais. Este trabalho também apresenta uma sugestão de abordagem desta temática no Ensino Médio.

Palavras-Chave: Erros de transmissão, Dígito Verificador, Eficiência de Métodos, Proposta para o Ensino.

Abstract

This paper presents the main methods of detecting numerical sequence transmission errors by calculating the check digit, including in the discussion the following topics: types of errors, methods of detection by Modular Arithmetic and the Dihedral Group D_5, the efficiency of each and some real applications. This paper also presents a suggestion to approach this theme in High School.

Keywords: Transcription Errors, Check Digit, Efficiency of Methods, Proposal for Teaching.

Lista de Figuras

Nota: Todas as figuras foram editadas pelo autor com o auxílio do software Photoscape.

Sumário

Capítulo 1

Introdução

A sociedade moderna, tida como a sociedade da informação, é altamente dependente de números e seus sistemas; não há nenhum setor econômico ou social que não faça uso de um sistema de numeração próprio. Em particular, é bastante grande a quantidade de sequências numéricas das quais depende qualquer cidadão atualmente: números de documentos, códigos de barra, numeração de veículos e cargas, números de celular, etc.

A codificação ou representação numérica de informações e elementos, apesar da extrema praticidade, está exposta a alguns riscos em seu uso, entre os quais as falhas humanas (erros de digitação ou de programação) e as falhas nas máquinas (interferências, ataques cibernéticos, etc.) durante a transmissão da informação. Estas falhas podem gerar grandes problemas. Um exemplo bastante comum são os códigos de barras, que serão detalhados no capítulo 3. Exemplo: em uma situação comum do cotidiano, quando um atendente de um caixa digita o código de um produto a máquina de registro (computador, por exemplo) acusa um erro, provavelmente o caixa digitou pelo menos um dos dígitos do código errado. O erro cometido, se foi identificado, certamente faz parte do conjunto de erros detectáveis pelo método do código de barras.

Para enfrentar estes riscos, foram desenvolvidos mecanismos matemáticos para detectar estes erros (operação com baixo custo computacional) e corrigi-los (com alto custo computacional) nas sequencias numéricas. Este trabalho dará uma introdução sobre os primeiros mecanismos, trazendo os principais modelos, suas características (como eficiência, limitações e aplicações), exemplos, alguns conceitos de matemática que os fundamentam, e duas propostas de abordagem para o tema no Ensino Médio.

1.1 Tipos de Erros de Transmissão

Cada método de detecção de erros tem um poder de detecção. Alguns mais eficientes (que detectam uma grande quantidade de tipos de erros), outros menos (capacidade de detecção limitada). Os erros, neste contexto, podem ser classificados em categorias. Faz-se necessária, assim, uma breve discussão sobre quais os erros mais comuns a serem cometidos na transmissão de uma sequência numérica.

Verhoeff em [11] elaborou uma tabela (1.1), baseada em trabalhos empíricos, que lista alguns tipos de erros de transmissão e sua frequência relativa.

Tipo de Erro	Configuração	Frequência percentual
Erros singulares	$\ldots a \ldots \mapsto \ldots b \ldots$	79,1
Transposição de algarismos adjacentes	$\ldots ab \ldots \mapsto \ldots ba \ldots$	10,2
Transposições intercaladas	$\ldots abc \ldots \mapsto \ldots cba \ldots$	0,8
Erros gêmeos	$\ldots aa \ldots \mapsto \ldots bb \ldots$	0,5
Erros fonéticos	-	0,5
Erros gêmeos intercalados	$\ldots aba \ldots \mapsto \ldots cbc \ldots$	0,3
Outros tipos	-	8,6

Tabela 1.1: Tipos de Erros.

Nos erros singulares, gêmeos e gêmeos intercalados, valores são arbitrariamente substituídos por outros; nos erros de algarismos adjacentes e intercalares, somente a ordem é alterada; os erros fonéticos decorrem de particularidades de um idioma. Um exemplo seria o fato de, em inglês, confundir-se foneticamente *eighteen* (18) com *eighty* (80). Em português, apesar de bem raros, podem ocorrer casos como, ao querer transmitir '107', o emissor leia *10 e 7*, e o receptor entenda *17*. O trabalho de Verhoeff também mostrou que dificilmente ocorrem dois erros simultâneos em uma operação.

1.2 Dígito Verificador

As técnicas mais difundidas de detecção de um erro na transmissão de uma sequência de números se baseiam no **dígito verificador**, um dígito que é acrescentado (na última posição, em todos os principais sistemas) a uma sequência inicial de dígitos e é determi-

nado a partir destes primeiros. A maneira pela qual este dígito verificador é calculado determina sua eficiência como ferramenta de detecção de erros (quanto mais tipos de erros detectados, maior a eficiência).

Quando é cometido um erro na transmissão de uma sequência numérica, gera-se uma **sequência-erro**. Se, ao calcularmos o dígito verificador desta sequência-erro por um método, o dígito resultante coincide com o dígito verificador da sequência correta, então considera-se que o método **não detecta** aquele erro. Caso contrário, se o cálculo do dígito verificador da sequência erro apontar um valor diferente do dígito da sequência correta, então o método usado **detecta** o erro cometido.

Este trabalho apresentará três métodos de obtenção do dígito verificador, dois baseados na Aritmética Modular, e um baseado em simetrias de polígonos (usando o grupo diedral D_5):

1. A aritmética modular, baseada na teoria das congruências, fornece as duas mais populares técnicas de obtenção de dígito verificador. Em ambas, o dígito verificador de uma sequência é a solução (única) de uma **equação de congruência**. A construção desta equação se faz por meio de um vetor de pesos (sequência fixa adotado para todos as sequências do sistema, pré-definida) ou uma permutação do conjunto de dígitos usáveis na sequência. Estes métodos são o tema do Capítulo 3.

2. O grupo diedral D_5, por sua vez, permite obter o dígito verificador como solução de uma equação construída sob uma permutação conveniente dos dígitos usados nas sequências de um sistema, não usando os conceitos de congruência. Seu modelo é mais eficiente que os primeiros, mas é computacionalmente mais exaustivo, o que em parte justifica sua popularidade limitada. O grupo D_5 e o método de Verhoeff são abordados no Capítulo 4.

Consideremos, por convenção própria, o conjunto dos algarismos indo-arábicos $\{0, 1, 2, ..., 9\}$ como Ω_{10}.

Capítulo 2

Fundamentação Matemática

Neste capítulo apresentaremos alguns resultados importantes sobre Teoria dos Números e Geometria Analítica necessários para os capítulos subsequentes.

2.1 Alguns resultados aritméticos

Teorema 1. *(Teorema da Divisão) Sejam a e b inteiros positivos. Existem números inteiros q e r tais que*

$$a = bq + r \quad e \quad 0 \leq r < b.$$

Além disso, q e r são únicos nas condições dadas acima.

Demonstração. Disponível na página 55 de Hefez [5]. ∎

Nos termos acima, os valores a, b, q e r são chamados de dividendo, divisor, quociente e resto, respectivamente.

Exemplo 1. *Tomando os números $a = 51$ e $b = 8$, temos que os únicos valores naturais $q > 0, 0 < r < 8$ que satisfazem à equação $51 = 8q + r$ são $q = 6$ e $r = 3$.* □

Lema 1. *(Lema de Gauss) Sejam a, b e c números inteiros. Se $a|bc$ e $mdc(a, b) = 1$, então $a|c$.*

Demonstração: Disponível na página 96 de Hefez [5]. ∎

Lema 2. *Se $0 < a < b < c < d$, então $c - b < d - a$.*

Demonstração: Segue diretamente do fato que $d - a = d + (-c + c) + (-b + b) - a = (d - c) + (c - b) + (b - a) > c - b$. ∎

Lema 3. *Em cada sequência de k números naturais consecutivos (crescente ou não), existe um, e somente um deles que é múltiplo de k.*

Demonstração:

Considere uma sequência crescente (o caso de uma sequência decrescente é análogo). Seja M o maior número da sequência. Consequentemente, $(M-k)+1$ é o menor deles. Note que $M \geq k$, pois o menor elemento da sequência é maior ou igual que 1, logo: $(M-k)+1 \geq 1 \Longrightarrow M-k \geq 1-1 \Longrightarrow M-k \geq 0 \Longrightarrow M \geq k$.

EXISTÊNCIA: Se for $M = k$, então ele é o múltiplo de k procurado. Se for $M > k$, então, pelo Teorema da divisão, existe $q > 0$ tal que $M = k \cdot q + r$, com $0 \leq r < k$. O valor procurado é $M - r$ (que faz parte da sequência de k dígitos proposta), pois temos $M - r = k \cdot q$.

UNICIDADE: Suponha que existam dois valores a, b na sequência que sejam múltiplos de k. Admita $b > a$, $b = kb_0$ e $a = ka_0$. Como a diferença entre dois elementos da sequência nunca é maior que a diferença entre o maior e menor elemento dela (conforme Lema 2), temos $0 < b - a = k(b_0 - a_0) < M - (M - (k-1)) = k - 1 \Longrightarrow k(b_0 - a_0) < k - 1 < k \Longrightarrow k(b_0 - a_0) < k \Longrightarrow b_0 - a_0 < 1$, uma contradição com fato de a_0 e b_0 serem ambos naturais. ∎

Exemplo 2. *A sequência 12, 13, 14, 15, 16, 17, 18 de 7 números naturais consecutivos tem apenas um único múltiplo de 7, a saber o 14.* □

2.2 Relações de Equivalência

Considere um conjunto X não vazio e uma relação $\sim$ entre seus elementos. Esta relação é chamada **relação de equivalência** se satisfaz a três propriedades, para $x, y, z \in X$:

(a) **propriedade reflexiva**: $x \sim x$.

(b) **propriedade simétrica**: se $x \sim y$, então $y \sim x$.

(c) **propriedade transitiva**: se $x \sim y$, e $y \sim z$, então $x \sim z$.

Exemplo 3. *A relação de igualdade em qualquer conjunto não vazio é uma relação de equivalência.* □

2.3 Congruência

Definição. Sejam a, b números inteiros e $m > 1$ um número natural. Dizemos que a é **congruente** a b módulo m, representando por $a \equiv b(mod\, m)$, se os restos das divisões tanto de a como de b por m, pela divisão euclidiana, forem iguais.

Exemplo 4. *Como os restos das divisões de 55 e 87 por 8 são ambos iguais a 7, então* $87 \equiv 55\ (mod\ 8)$. □

Quando dois valores a, b não forem congruentes entre si, dizemos que a é **incongruente** a b módulo m e representamos por $a \not\equiv b(mod\, m)$. Alguns resultados importantes obtidos diretamente da definição de congruência são apresentados a seguir.

Proposição 1. *Suponha que* $a, b, m \in \mathbb{Z}$. *Tem que* $a \equiv b(mod\, m)$ *se e somente se* $m|b-a$. *Em particular, se* $a \equiv 0(mod\, m)$, *então* $m|a$.

Demonstração: ($\Longrightarrow$) Se $a \equiv b(mod\, m)$, então existem q_a, q_b e r inteiros $(0 < r < m)$ tais que $a = mq_a + r$ e $b = mq_b + r$. Então temos $b - a = mq_b + r - (mq_a + r) = m(q_b - q_a)$, o que equivale a afirmar que $m|b - a$.

($\Longleftarrow$) Seja $a = mq' + r'$ e $b = mq'' + r''$, com $r' < m$ e $r'' < m$, conforme o Teorema da divisão. Se $m|b - a$, então $m|(mq' + r') - (mq'' + r'') \Longrightarrow m|m(q' - q'') + (r' - r'') \Longrightarrow m|(r' - r'')$. Mas $m|(r' - r'') \Longrightarrow r' = r''$. Logo $a \equiv b(mod\, m)$. ■

Proposição 2. *A relação de congruência é uma relação de equivalência.*

Demonstração: Devemos mostrar que a relação de congruência respeita as três propriedades da seção 1.2. Sejam então $a, b, c, d \in \mathbb{Z}$ e $m > 1$.

(a) $a \equiv a(mod\, m)$.

Uma vez que $m|0$, então $m|a - a$, resultando consequentemente em $a \equiv a(mod\, m)$.

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

Se $m|n$, então $m| - n$, para qualquer $n \in \mathbb{Z}$. Consequentemente, se $m|a - b$, então $m|b - a$.

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

Se $m|(a - b)$ e $m|(b - c)$, então $m|[(a - b) + (b - c)]$, logo $m|(a - c)$. ■

Proposição 3. *Sejam $a, b, c, d \in \mathbb{Z}$, com $m > 1$. Então são válidas as seguintes propriedades:*

1. Se $a \equiv b(mod\, m)$ e $c \equiv d(mod\, m)$, então $a + c \equiv b + d(mod\, m)$.

   Demonstração. Como $m|[(b-a)+(d-c)]$, então $m|[(b+d)-(a+c)]$, daí $a + c \equiv b + d(mod\, m)$.

2. Se $a \equiv b(mod\, m)$ e $c \equiv d(mod\, m)$, então $a - c \equiv b - d(mod\, m)$.

   Demonstração. Análoga à demonstração do item anterior.

3. Se $a \equiv b(mod\, m)$ e $c \equiv d(mod\, m)$, então $ac \equiv bd(mod\, m)$.

   Demonstração. Pela identidade $bd - ac = d(b-a) + a(d-c)$, e pelo fato de $m|b-a$ e $m|d-c$, temos que $m|bd-ac$. ∎

Outros 4 resultados importantes, no contexto de congruência, são apresentados nas proposições a seguir.

Proposição 4. *A equação de congruência $R + x \equiv c(mod\, m)$ tem solução única em $X = \{0, 1, 2, .., m-1\}$, para $R \geq 0$ fixo, $c \geq 0$ e $m > 1$.*

Demonstração: Observe que $R + x - c$, com $x \in X$, representa uma coleção de m valores consecutivos $\{R-c, R-c+1, ..., R-c+m-2, R-c+m-1\}$. Pelo Lema 3 apenas um destes valores é divisível por m. ∎

Os elementos do conjunto de números $R + x - c$ descrito acima têm por restos de sua divisão por m os valores $0, 1, 2, 3, ..., m-1$ (não necessariamente nesta ordem, mas preservando sua ordem circular); todo conjunto com esta característica é chamado *sistema completo de resíduos* módulo m. Quaisquer dois elementos deste conjunto são incongruentes módulo m entre si.

Proposição 5. *Se $a+b \equiv 0(mod\, m)$ e $a \equiv 0(mod\, m)$, então $b \equiv 0(mod\, m)$, para $m, b > 0$.*

Demonstração: Se $b = 0$ não há o que fazer. Considere então $b \neq 0$. Se $a+b \equiv 0(mod\, m)$, $\exists\, d_1 \in \mathbb{Z}$ tal que $a + b = m \cdot d_1$. Analogamente, se $a \equiv 0(mod\, m)$, $\exists\, d_2 \in \mathbb{Z}$ tal que $a = m \cdot d_2$. Daí:

$$b = (a + b) - a = m \cdot d_1 - m \cdot d_2 = m(d_1 - d_2).$$

o que garante que $b \equiv 0(mod\, m)$, pois $d_1 - d_2 \neq 0$. ∎

Proposição 6. *Se* $a + b \not\equiv 0(mod\, m)$ *e* $a \equiv 0(mod\, m)$*, então* $b \not\equiv 0(mod\, m)$*.*

Demonstração: Se tivéssemos $a \equiv 0(mod\, m)$ e $b \equiv 0(mod\, m)$, pelo item 1 na Proposição 3, teríamos $a + b \equiv 0(mod\, m)$, uma contradição. ∎

Proposição 7. *Sejam* m *e* p *números inteiros, e* $s \in \{1, 2, ..., m-1\}$*. Então* $ps \not\equiv 0(mod\, m)$ *se, e somente se,* $mdc(p, m) = 1$*.*

Demonstração:
($\Longrightarrow$) Suponha por absurdo que $mdc(p, m) = q > 1$. Sejam $k_m = \dfrac{m}{q}$ e $k_p = \dfrac{p}{q}$. Então $p \cdot k_m = \dfrac{p \cdot m}{q} = \dfrac{p}{q} \cdot m = k_p \cdot m \Longrightarrow m | p \cdot k_m \Longrightarrow p \cdot k_m \equiv 0(mod\, m)$, uma contradição.
($\Longleftarrow$) Se $mdc(m, p) = 1$, então $m \nmid p$. Suponha que $ps \equiv 0(mod\, m)$, então $m|ps$, mas como $m \nmid p$, temos que $m \mid s$, pelo Lema de Gauss. Mas isto é uma contradição, pois $s < m$. ∎

2.4 Produto Interno

Considere dois vetores $\vec{v} = (v_1, v_2, ..., v_n)$ e $\vec{w} = (w_1, w_2, ..., w_n)$. Define-se como produto interno de $\vec{v}$ e $\vec{w}$, denotado por $\vec{v} \cdot \vec{w}$, o número real obtido pelo somatório:

$$\sum_{i=1}^{n} v_i \cdot w_i = v_1 \cdot w_1 + v_2 \cdot w_2 + ... + v_n \cdot w_n.$$

Este conceito pode ser aplicado a qualquer par de sequências que possam ser aritmeticamente interpretadas como vetores. Uma importante propriedade de produto interno é a comutatividade: $\vec{v} \cdot \vec{w} = \vec{w} \cdot \vec{v}$.

Exemplo 5. *O produto interno dos vetores* $\vec{a} = (2, 2, 3, 4)$ *e* $\vec{b} = (0, 3, 2, 9)$ *é* $\vec{a} \cdot \vec{b} = 2 \cdot 0 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 9 = 0 + 6 + 6 + 36 = 48$. □

2.5 Permutações

Definição 1. *Seja* X *um conjunto finito de números naturais. Uma permutação* ϕ *do conjunto* X *é uma bijeção da forma* $\phi : X \longrightarrow X$*.*

Exemplo 6. *A expressão abaixo representa uma permutação* σ *da forma* $\sigma : X \to X$*, para* $X = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

$$\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 5 & 8 & 2 & 6 & 9 & 3 & 7 & 4 & 1 \end{pmatrix}$$

Nesta permutação temos $\sigma(0) = 0$, $\sigma(1) = 5$, $\sigma(2) = 8$, ..., $\sigma(9) = 1$. □

Permutação é uma operação que poder ser composta. Referindo-se ao exemplo anterior, podemos ter, por exemplo, $\sigma(\sigma(1)) = \sigma(5) = 9$. Podemos escrever $\sigma(\sigma(1))$ como $\sigma^2(1)$. Outro exemplo: $\sigma(\sigma(\sigma(\sigma(3)))) = 6$ pode ser escrito como $\sigma^4(3) = 6$. Esta será a notação usada no decorrer deste trabalho. Para um estudo mais detalhado, temos Gonçalves [4].

2.6 Grupos

Definição. Um grupo é um conjunto $G \neq \emptyset$ no qual está definida uma operação $*$, da forma

$$* : G \times G \to G.$$

$$(a, b) \to a * b.$$

que satisfaz às seguintes propriedades:

(a) **Associatividade**: dados a, b, $c \in$ G, temos que:

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

(b) **Elemento neutro**: existe um elemento $e \in$ G tal que para todo $a \in G$ temos:

$$a * e = e * a = a.$$

(c) **Elemento inverso**: dado um elemento a $\in$ G qualquer, existe um elemento $a' \in G$ (o inverso de a) tal que:

$$a * a' = a' * a = e.$$

Um grupo G no qual a operação $*$ é comutativa (isto é, para quaisquer $a, b \in G$, $a * b = b * a$) é chamado ***abeliano***. O número de elementos de um grupo é chamado de ***ordem de um grupo***. Como referência mais detalhada, temos Coutinho [1].

Exemplo 7. *Os inteiros, racionais, reais e complexos são grupos para a soma. Já para a multiplicação são grupos os racionais não nulos, os reais mão nulos e os complexos não nulos.* □

Capítulo 3

Dígito Verificador e Aritmética Modular

Neste capítulo será discutido inicialmente o método de obtenção de dígitos verificadores por vetor de pesos, e na sequência o método que usa permutação.

3.1 Dígito Verificador por Vetor de Pesos

A maioria dos sistemas é composto por sequências numéricas com o mesmo número de dígitos, sendo que na maioria estes dígitos são os algarismos indo-arábicos (elementos de Ω_{10}). Considere então uma sequência $d_1d_2d_3...d_{n-1}$ de $n-1$ dígitos, pertencente a um sistema de códigos numéricos. A ela podemos associar um vetor v, da forma

$$v = (d_1, d_2, d_3, ..., d_{n-1}),$$

e ao sistema um outro vetor, da forma

$$\lambda = (\lambda_1, \lambda_2, \lambda_3, ..., \lambda_{n-1}).$$

Ao primeiro vetor, daremos a denominação de ***vetor de identificação*** ou ***vetor característico*** da sequência. Ao segundo vetor, daremos o nome de ***vetor de pesos*** do sistema.

Definição. Considere um vetor de pesos $\lambda = (\lambda_1, \lambda_2, \lambda_3, ..., \lambda_{n-1})$ de um sistema e um vetor $v = (d_1, d_2, d_3, ..., d_{n-1})$ característico de uma sequência qualquer, ambos com $n-1$ coordenadas (todas naturais), e os números naturais c, λ_n e m, com $m > d_i$ para todo i.

Define-se por ***dígito verificador***, *número de verificação* ou *número de controle* qualquer elemento $x \in \mathbb{N}$, $x < m$, que seja solução da equação de congruência

$$(\lambda_n x + \sum_{i=1}^{n-1} \lambda_i d_i) \equiv c(mod\ \ m). \tag{3.1}$$

A expressão $\sum_{i=1}^{n-1} \lambda_i d_i$ tem por resultado um número natural, e pode ser reescrita usando a notação de produto interno (ver seção 2.5):

$$\sum_{i=1}^{n-1} \lambda_i d_i = \lambda \cdot v.$$

Desta forma, podemos reescrever o somatório do primeiro membro da expressão (3.1) e representá-lo da forma

$$\lambda_n x + \lambda \cdot v \equiv c(mod\ \ m).$$

Unicidade do dígito verificador

A maioria das aplicações do conceito da dígito verificador (inclusive as que serão abordadas neste trabalho) toma como coordenadas de v e de λ os algarismos indo-arábicos (Ω_{10}), $c = 0$ e $\lambda_n = 1$.

Nestas condições ($\lambda_n = 1$ e $c = 0$), pela Proposição 4. (página 07), a solução da equação (3.1), sempre existe e é única, pois a expressão (3.1) pode ser reescrita da forma

$$x + \lambda \cdot v \equiv 0(mod\ \ m),$$

tomando $R = \lambda \cdot v$.

Cálculo do dígito verificador.

Na prática, os sistemas que usam dígito verificador por vetor de pesos incorporam o valor λ_n como a última coordenada de seu vetor de pesos, e o dígito verificador x como a última coordenada do vetor característico, pondo $x = d_n$. Assim, o vetor de pesos de um sistema que usa sequências de n dígitos tem um vetor de pesos com n coordenadas. Nestes termos, temos que $x = d_n$ é um dígito verificador se

$$\lambda \cdot v = \sum_{i=1}^{n} \lambda_i d_i \equiv c(mod\ \ m).$$

Exemplo 8. *Calcule o dígito verificador k da sequencia 54638376k, com módulo 11, vetor de pesos* $\lambda = (3, 2, 1, 3, 2, 1, 3, 2, 1)$ *e* $c = 5$.

Solução: Tomando o somatório $\sum_{i=1}^{n} \lambda_i d_i$ como produto interno de λ com o vetor característico da sequência $v = (5, 4, 6, 3, 8, 3, 7, 6, k)$, (com $k = d_n$) temos:

$$\begin{aligned} \lambda \cdot v &= (3, 2, 1, 3, 2, 1, 3, 2, 1) \cdot (5, 4, 6, 3, 8, 3, 7, 6, k) \\ &= 3 \cdot 5 + 2 \cdot 4 + 1 \cdot 6 + 3 \cdot 3 + 2 \cdot 8 + 1 \cdot 3 + 3 \cdot 7 + 2 \cdot 6 + 1 \cdot k \\ &= 15 + 8 + 6 + 9 + 16 + 3 + 21 + 12 + k \\ &= 90 + k. \end{aligned}$$

A única solução positiva da equação $90 + k \equiv 5 (mod\ 11)$ em Ω_{10} é 3. Logo, a sequência completa é $q = 546383763$. □

Como um dígito verificador detecta um erro?

Quando se comete um erro de transmissão de uma sequência numérica de um sistema, geramos uma sequência-erro. Chamemos de v o vetor característico da sequência original e v_E o vetor característico da sequência-erro.

Para a sequência original (correta) temos naturalmente que $\lambda \cdot v \equiv c (mod\ m)$. A sequência-erro, por sua vez, tem por produto interno $\lambda \cdot v_E$, para o qual temos duas possibilidades:

1. Se tivermos $\lambda \cdot v_E \equiv c (mod\ m)$, então o dígito verificador obtido como solução desta equação é o mesmo obtido a partir da sequência original, e neste caso afirmamos que o erro cometido **não foi detectado**.

2. Se tivermos $\lambda \cdot v_E \not\equiv c (mod\ m)$, então o dígito verificador obtido como solução desta equação **não** é o mesmo obtido a partir da sequência original, e neste caso afirmamos que o erro cometido **foi detectado**.

Exemplo 9. *Considere um sistema de sequências numéricas que possuam 7 dígitos, sendo 6 próprios do sistema e o último sendo um dígito verificador. Suponha que ele use vetor de pesos* $\lambda = (1, 4, 4, 5, 5, 7, 1)$, $m = 9$ *e* $c = 3$.

1. *A sequência 2409728 pode ser usada no sistema, pois tomando v = (2, 4, 0, 9, 7, 2, 8) e o* λ *fornecido, temos que, de fato,* $\lambda \cdot v = 120$, *e* $120 \equiv 3 (mod\ 9)$.

2. *Suponha que tenha ocorrido o erro singular* $7 \longrightarrow 0$*, na* 5^a *posição da sequência do item anterior. Temos assim o vetor-erro* $v_E = (2, 4, 0, 9, 0, 2, 8)$*, para o qual* $\lambda \cdot v_E = 85$*. Como* $85 \not\equiv 3(mod\ 9)$*, este erro* ***é detectado*** *pelo método do sistema em questão.*

3. *Suponha que tenha ocorrido a transposição adjacente dos dois últimos dígitos da sequência em questão, gerando assim a sequência-erro 2409782 e consequentemente o vetor erro* $v_E = (2, 4, 0, 9, 7, 8, 2)$*, para o qual temos que* $\lambda \cdot v_E = 156$*. Como* $156 \equiv 3(mod\ 9)$*, este erro* ***não é detectado****.* □

Proposição 8. *Considere uma sequência* $(d_1, d_2, d_3, ..., d_{n-1}, d_n)$ *qualquer de n coordenadas (todos elementos de* Ω_{10}*), da qual* d_n *seja o dígito verificador, e um método de detecção de erros com vetor de pesos* $\lambda = (1, 1, 1, ..., 1, 1)$*, com n coordenadas, e* $m = 10$*. Este método detecta corretamente todos os erros singulares (a), mas nenhum erro de transposição (b).*

Demonstração: (a) Suponha que tenha ocorrido o erro singular $d_i \longrightarrow d_E$ (troca do dígito d_i da *i-ésima* coordenada por um dígito diferente d_E) na sequência, gerando uma sequência-erro com vetor erro v_E, e que o método **não o tenha detectado**. Temos então que:

$$\lambda \cdot v = d_1 + d_2 + ... + d_i + ... + d_n \equiv 0(mod\ 10) \tag{3.2}$$

e

$$\lambda \cdot v_E = d_1 + d_2 + ... + d_E + ... + d_n \equiv 0(mod\ 10). \tag{3.3}$$

Somando (3.2) com a expressão oposta de (3.3), temos, pelo item 2 da proposição 3 (página 07), que:

$$\lambda \cdot v - \lambda \cdot v_E = d_i - d_E \equiv 0(mod\ 10).$$

Como $0 < d_i, d_E < 10$, então $d_i - d_E \equiv 0(mod\ 10) \Longleftrightarrow d_i = d_E$, uma contradição.

(b) Como todas as coordenadas do vetor de pesos são iguais a 1, temos $\sum_{i=1}^{n} \lambda_i d_i = \sum_{i=1}^{n} d_i$. Qualquer erro de transposição (mais que isso, qualquer reordenação que se faça das coordenadas do vetor característico) gera uma vetor v_E para o qual $\lambda \cdot v_E = \lambda \cdot v$, logo

$\lambda \cdot v_E \equiv 0(mod\ 10)$ (pela comutatividade da adição), não alterando a validade da equação de congruência e, consequentemente, não possibilitando a detecção do erro. ■

Nas seções seguintes, serão apresentados alguns sistemas que usam sequências numéricas e têm o dígito verificador como ferramenta de detecção de erros.

3.1.1 Códigos de Barra no sistema EAN-13

Os códigos de barras são uma categoria de códigos de catalogação de mercadorias e serviços (ex.: boletos bancários, cartões de acesso, etc.), todos baseados inicialmente no modelo UPC (Universal Product Code), proposto em 1973 por George J. Laurer e colaboradores (funcionários da IBM, International Business Machines, grande empresa de informática), e inicialmente usado nos EUA e Canadá. Nas décadas seguintes surgiram algumas variantes, como o EAN-13 (European Article Numbering System) e o JAN (Japanese Article Numbering System). O UPC e o EAN-13 são os mais usados comercialmente.

O sistema EAN-13 utiliza 13 dígitos, sendo 2 ou 3 para identificar o país de origem de um produto, os 4 ou 5 seguintes para identificar o fabricante do produto, os 5 dígitos seguintes identificam o produto em particular, e o último número é o dígito verificador. Produtos brasileiros, por exemplo, sempre se iniciam pela sequência 789. A figura 3.1 ilustra o código de barras de um produto brasileiro.

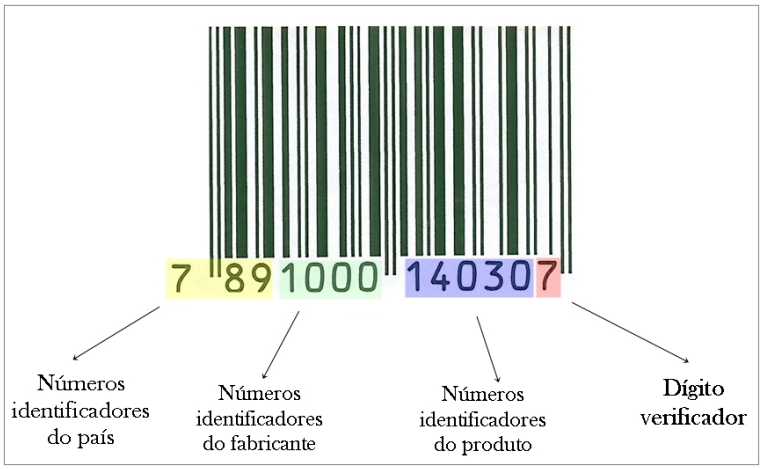

Figura 3.1: Código de barras do modelo EAN-13.

Para cálculo do dígito verificador, o sistema EAN-13 utiliza o vetor de pesos λ = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1), $c = 0$ e $m = 10$.

Exemplo 10. *Verifique que o dígito verificador do código de barras acima é realmente 7.*

Solução: Tomando $v = (7, 8, 9, 1, 0, 0, 0, 1, 4, 0, 3, 0, x)$ e $\lambda = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$, mostremos que $x = 7$. Com efeito, temos que:

$$\lambda \cdot v = (1,3,1,3,1,3,1,3,1,3,1,3,1) \cdot (7,8,9,1,0,0,0,1,4,0,3,0,x) =$$

$$1 \cdot 7 + 3 \cdot 8 + 1 \cdot 9 + 3 \cdot 1 + 1 \cdot 0 + 3 \cdot 0 + 1 \cdot 0 + 3 \cdot 1 + 1 \cdot 4 + 3 \cdot 0 + 1 \cdot 3 + 3 \cdot 0 + 1 \cdot x =$$

$$7 + 24 + 9 + 3 + 0 + 0 + 0 + 3 + 4 + 0 + 3 + 0 + x =$$

$$= 53 + x \equiv 0(mod\ 10).$$

A única solução em Ω_{10} da equação $53 + x \equiv 0(mod\ 10)$ é $x = 7$, confirmando a validade do dígito. □

Dois resultados bastante interessantes sobre a detecção de erros do sistema EAN-13 são apresentados a seguir. Para eles, considere $\lambda = (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$ e um vetor característico $v = (d_1, d_2, ..., d_{13})$ de uma sequência em EAN-13, considerando d_{13} como sendo o dígito verificador.

Proposição 9. *Toda transposição adjacente é detectada pela verificação do EAN-13 se, e somente se,* $|d_i - d_{i+1}| \neq 5$.

Demonstração: Suponhamos que a transposição tenha ocorrido com o vetor original com d_i na posição par e d_{i+1} na posição ímpar (o caso contrário é análogo), gerando um vetor-erro da forma v_E. Temos então:

$$\lambda \cdot v = 1 \cdot d_1 + 3 \cdot d_2 + \ldots + 3 \cdot d_i + 1 \cdot d_{i+1} + .. + 1 \cdot d_{13}. \tag{3.4}$$

$$\lambda \cdot v_E = 1 \cdot d_1 + 3 \cdot d_2 + \ldots + 3 \cdot d_{i+1} + 1 \cdot d_i + .. + 1 \cdot d_{13}. \tag{3.5}$$

Somando (3.5) à oposta de (3.4), temos

$$\lambda \cdot v_E - \lambda \cdot v = 3d_{i+1} + d_i - (3d_i + d_{i+1}) \Longrightarrow \lambda \cdot v_E - \lambda \cdot v = 2(d_{i+1} - d_i). \tag{3.6}$$

($\Longrightarrow$) Provemos que, se $|d_{i+1} - d_i| = 5$, então o erro não é detectado. Com efeito, se $|d_{i+1} - d_i| = 5$, então $d_{i+1} - d_i = \pm 5$, logo $2(d_{i+1} - d_i) = \pm 10$ e então, por (3.6)

$$\lambda \cdot v_E - \lambda \cdot v = \pm 10.$$

Logo temos que:

$$\lambda \cdot v_E - \lambda \cdot v \equiv 10(mod\ 10) \equiv 0(mod\ 10).$$

Mas $\lambda \cdot v_E - \lambda \cdot v \equiv 0(mod\ 10) \Longrightarrow \lambda \cdot v_E \equiv 0(mod\ 10)$, pela Proposição 5 (página 07). Por sua vez, $\lambda \cdot v_E \equiv 0(mod\ 10)$ implica que o erro não é detectado.

($\Longleftarrow$) Suponha $|d_{i+1} - d_i| \neq 5$. Se os dígitos d_i e d_{i+1} forem iguais, não há erro cometido; se são diferentes, então $2|d_{i+1} - d_i| \neq 10$, ou seja $2|d_{i+1} - d_i| \in \{2, 4, 6, 8, 12, 14, 16, 18\}$ e, portanto, $2(d_{i+1} - d_i) \not\equiv 0\ (mod\ 10)$.

Mas isto (pela expressão 3.6) equivale a afirmar que $\lambda \cdot v_E - \lambda \cdot v \not\equiv 0\ (mod\ 10)$, o que, também pela Proposição 5 (página 07), força $\lambda \cdot v_E \not\equiv 0(mod\ 10)$, resultando assim na detecção do erro. ∎

Proposição 10. *A verificação do EAN-13 não detecta transposição não adjacente d_i e d_j se a diferença $i - j$ for par.*

Demonstração: Observe inicialmente que

$$\lambda \cdot v = 1d_1 + 3d_2 + 1d_3 + ... + 3d_{12} + 1d_{13} =$$
$$3 \cdot (d_2 + d_4 + \ldots + d_{12}) + 1 \cdot (d_1 + d_3 + \ldots + d_{13}) =$$
$$3(\sum_{k=1}^{6} d_{2k}) + (\sum_{k=1}^{7} d_{2k-1}). \tag{3.7}$$

Se a diferença $i - j$ é par, então ou são os índices i, j ambos pares, ou ambos ímpares. Suponha então que houve uma transposição entre dois dígitos de posição par (o caso para ímpares é análogo), gerando um vetor-erro v_E. Nesta circunstância, nenhum dos somatórios da expressão (3.7) acima tem valor alterado, pela comutatividade da adição. Logo

$$\lambda \cdot v_E = \lambda \cdot v \equiv 0(mod\ 10),$$

e o erro não é, portanto, detectado. ∎

De maneira mais geral, qualquer reordenação dos dígitos de posição par (de modo que, após a reordenação, ainda permaneçam todos em posições pares) de uma sequência em EAN-13 não é detectada pelo método deste sistema; o mesmo ocorre (maneira análoga) com os dígitos de ordem ímpar. Mais que isso, ainda que os dígitos de ordem par e ímpar reordenem-se entre si simultaneamente (preservando, contudo, a paridade de suas posições), estes erros não são detectados pelo método usado no sistema do EAN-13.

Exemplo 11. *Considere a sequência fictícia 2250432810359 do EAN-13. Para ela temos v = (2, 2, 5, 0, 4, 3, 2, 8, 1, 0, 3, 5, 9) e $\lambda \cdot v = 80$.*

1. *Suponha ter havido uma transposição adjacente entre o 3º e o 4º dígitos (observe que $|5 - 0| = 5$), gerando a sequência-erro 2205432810359 e consequentemente o vetor erro v_E = (2, 2, 0, 5, 4, 3, 2, 8, 1, 0, 3, 5, 9). Temos que $\lambda \cdot v_E = 90$. Como $90 \equiv 0 \pmod{10}$, o erro cometido* ***não*** *foi detectado.*

2. *Suponha agora ter havido uma transposição entre o 5º e o 9º dígitos (note que ambos de posição ímpar, e diferença de índices evidentemente par). Este erro gera uma sequência-erro 2205132840359, com respectivo vetor v_E = (2, 2, 0, 5, 1, 3, 2, 8, 4, 0, 3, 5, 9). Para este vetor temos que $\lambda \cdot v_E = 80$, e consequentemente este erro também* ***não*** *é detectado.* □

3.1.2 CPF, CNPJ no Brasil

O **CPF** (Cadastro Nacional de Pessoa Física) é o mais importante documento pessoal dos cidadãos brasileiros. Ele tem 11 dígitos, sendo 9 atribuídos pelo sistema, e 2 dígitos verificadores. O primeiro dígito verificador é calculado sobre os nove primeiros usando o vetor de pesos λ_1 = (10, 9, 8, 7, 6, 5, 4, 3, 2, 1), e o segundo dígito é calculado usando os dez primeiros (inclusive o primeiro dígito verificador) e seu vetor de pesos λ_2 = (11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1), ambos usando $m = 11$. No entanto, esse método tem uma limitação: a solução da equação de congruência gerada pode ser 10. Nesse caso, põe-se o 0 como dígito verificador, sem a necessidade de um símbolo adicional para representar a solução 10 obtida.

O **CNPJ** (Cadastro Nacional de Pessoa Jurídica), documento fiscal brasileiro, é semelhante ao CPF, e usa uma sequência numérica com 14 dígitos, sendo os 12 primeiros atribuídos pelo sistema, o 13º é o primeiro dígito verificador (com $m = 11$) dos 12 primeiros, e o 14º é segundo o dígito verificador, (também com $m = 11$) dos 13 anteriores, com vetores de peso λ_1 = (5, 4, 3, 2, 9, 8, 7, 6, 5, 4, 3, 2, 1) e λ_2 = (6, 5, 4, 3, 2, 9, 8, 7, 6, 5, 4, 3, 2, 1), respectivamente.

Como no caso do CPF, se a solução da equação de congruência for 10, põe-se 0 como dígito verificador.

Exemplo 12. *Calcule os dois dígitos verificadores x_1, x_2 de um CPF fictício cujos 9 primeiros dígitos sejam 123103107*

Solução: Pondo $v_1 = (1,\ 2,\ 3,\ 1,\ 0,\ 3,\ 1,\ 0,\ 7,\ x_1)$, para o cálculo do primeiro dígito temos:

$$\begin{aligned}\lambda_1 \cdot v_1 &= (10,9,8,7,6,5,4,3,2,1)\cdot(1,2,3,1,0,3,1,0,7,x_1)\\ &= 10\cdot 1+9\cdot 2+8\cdot 3+7\cdot 1+6\cdot 0+5\cdot 3+4\cdot 1+3\cdot 0+2\cdot 7+1\cdot x_1\\ &= 10+18+24+7+0+15+4+0+14+x_1\\ &= 92+x_1.\end{aligned}$$

Como a única solução da equação $92 + x_1 \equiv 0(mod\ 11)$ é $x_1 = 7$, o CPF em questão é, até o momento, $1231031037x_2$. Para o cálculo do segundo dígito, pondo $v_2 = (1,\ 2,\ 3,\ 1,\ 0,\ 3,\ 1,\ 0,\ 7,\ 7,\ x_2)$ temos:

$$\begin{aligned}\lambda_2 \cdot v_2 &= (11,10,9,8,7,6,5,4,3,2,1)\cdot(1,2,3,1,0,3,1,0,7,7,x_2)\\ &= 11\cdot 1+10\cdot 2+9\cdot 3+8\cdot 1+7\cdot 0+6\cdot 3+5\cdot 1+4\cdot 0+3\cdot 7+2\cdot 7+1\cdot x_2\\ &= 11+20+27+8+0+18+5+0+21+14+x_2\\ &= 124+x_2.\end{aligned}$$

Como a única solução da equação $124 + x_2 \equiv 0(mod\ 11)$ em Ω_{10} é $x_2 = 8$, o CPF em questão, completo, é 12310310778. □

3.1.3 ISBN

ISBN é a sigla de 'Internacional Standart Book Number', um sistema que usa sequências de 11 dígitos (10 atribuídos pelo sistema e o último sendo o dígito verificador), um vetor de pesos $\lambda = (10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$, $c = 0$ e $m = 11$ para catalogar obras bibliográficas em âmbito mundial.

Exemplo 13. *Calcule o dígito de verificação w de um livro fictício com número ISBN 7-5463-1132-w.*

Solução: Tomando $v = (7, 5, 4, 6, 3, 1, 1, 3, 2, w)$, temos

$$\begin{aligned}\lambda \cdot v &= 10\cdot 7+9\cdot 5+8\cdot 4+7\cdot 6+6\cdot 3+5\cdot 1+4\cdot 1+3\cdot 3+2\cdot 2+1\cdot w\\ &= 70+45+32+42+18+5+4+9+4+w\\ &= 229+w.\end{aligned}$$

A única solução w para a equação $229 + w \equiv 0(mod\ 11)$ em Ω_{10} é $w = 2$. Logo, o número ISBN completo do referido livro é *7-5463-1132-2*. □

O ISBN possui uma limitação de dígitos. Por exemplo, se fossemos calcular o dígito verificador z da sequência *4-40043379-z*, teríamos que z precisa ser a solução de $166 + z \equiv 0(mod 11)$, ou seja, $z = 10$. Mas como $10 \notin \Omega_{10}$, usa-se, para representá-lo, a letra X. O ISBN em questão seria *4-40043379-X*. Este problema também ocorre com o os sistemas do CPF e do CNPJ. Nestes, no entanto, se adota o 0 como dígito verificador, em vez da adoção de um símbolo adicional.

3.1.4 Poder de Detecção de Erros com Vetor de Pesos

O dígito verificador, como ferramenta de detecção de erros em um sistema, tem sua eficiência avaliada diretamente pelos tipos de erros que consegue detectar. Para o método que usa vetor de pesos, a escolha, aleatória ou não, do valor m e do vetor de pesos λ influencia na capacidade de detecção do método. O teorema seguir mostra como se dá esta influência.

Teorema 2. *Sejam $m > 1$ um número natural e $\lambda = (\lambda_1, \lambda_2, ...\lambda_n)$ um vetor de pesos. Considere um vetor característico $v = (d_1, d_2, ...d_n)$, com $d_i < m$ quando $i \in \{1, 2, \ldots n\}$, para os quais*

$$\lambda \cdot v = \lambda_1 d_1 + \lambda_2 d_2 + ... + \lambda_n d_n \equiv 0(mod\ m).$$

Então

(a) Todo erro singular em v só será detectado se mdc(λ_i, m) = 1, para $i \in \{1, 2, \ldots n\}$

(b) Todo erro de transposição da forma

$$\ldots v_i \ldots v_j \ldots \mapsto \ldots v_j \ldots v_i \ldots$$

será detectado se e somente se mdc(λ_i - λ_j, m) = 1.

Demonstração. (a) Suponha ter havido um erro singular no qual o dígito errado tenha sido na posição j, com a troca $d_j \longrightarrow d_E$, gerando um vetor erro da forma v_E, e que o erro **foi detectado**; logo:

$$\lambda \cdot v = \lambda_1 \cdot d_1 + \lambda_2 \cdot d_2 + \ldots + \lambda_j \cdot d_i + \ldots + \lambda_n \cdot d_n. \tag{3.8}$$

$$\lambda \cdot v_E = \lambda_1 \cdot d_1 + \lambda_2 \cdot d_2 + \ldots + \lambda_j \cdot d_E + \ldots + \lambda_n \cdot d_n. \tag{3.9}$$

Consequentemente:

$$\lambda \cdot v \equiv 0(mod\ m). \tag{3.10}$$

$$\lambda \cdot v_E \not\equiv 0(mod\ m). \tag{3.11}$$

Subtraindo (3.9) de (3.8):

$$\lambda \cdot v - \lambda \cdot v_E = \lambda_j d_j - \lambda_j d_E = \lambda_j (d_j - d_E).$$

Pela Proposição 6 (página 8), aplicada aos resultados (3.10) de (3.11), temos:

$$\lambda \cdot v - \lambda \cdot v_E \not\equiv 0(mod\ m).$$

Logo, temos que

$$\lambda_j (d_j - d_E) \not\equiv 0(mod\ m).$$

Como $d_i - d_j < m$, pelas hipóteses da Proposição 7., página 08., a equação $\lambda_j(d_j - d_E) \not\equiv 0(mod\ m)$ só é verdadeira se, e somente se, $mdc(\lambda_j, m) = 1$ (tome $s = d_i - d_j$ e $p = \lambda_j$). Como o erro singular pode ocorrer em qualquer posição da sequência, tem-se a plena validade do resultado apresentado.

(b) Suponha que tenha ocorrido a permutação entre os dígitos d_i e d_j, gerando uma sequência-erro de vetor v_E. Temos assim:

$$\lambda \cdot v = \lambda_1 \cdot d_1 + \ldots + \lambda_i d_i + \ldots + \lambda_j d_j + \ldots + \lambda_n \cdot d_n. \tag{3.12}$$

$$\lambda \cdot v_E = \lambda_1 \cdot d_1 + \ldots + \lambda_i d_j + \ldots + \lambda_j d_i + \ldots + \lambda_n \cdot d_n. \tag{3.13}$$

Subtraindo (3.13) de (3.13), temos:

$$\begin{aligned}
\lambda \cdot v - \lambda \cdot v_E = & \\
(\lambda_i d_i - \lambda_i d_j) + (\lambda_j d_j - \lambda_j d_i) = & \\
\lambda_i (d_i - d_j) - \lambda_j (d_i - d_j) = & \\
(\lambda_i - \lambda_j)(d_i - d_j) = & \qquad (3.14) \\
(\lambda_j - \lambda_i)(d_j - d_i). & \qquad (3.15)
\end{aligned}$$

Observação. Considere como oficial, nos cálculos a seguir, a expressão (3.14) se $\lambda_i - \lambda_j > 0$, ou a expressão (3.14), se $\lambda_j - \lambda_i > 0$. Se $\lambda_j = \lambda_i$, então $\lambda \cdot v = \lambda \cdot v_E$, e nenhum erro será detectado. Se $d_j = d_i$, então não houve erro cometido.

Se tivermos ou $(\lambda_i - \lambda_j) \equiv 0(mod\ m)$ ou $(d_i - d_j) \equiv 0(mod\ m)$, então

$$\lambda \cdot v - \lambda \cdot v_E = (\lambda_i - \lambda_j)(d_i - d_j) \equiv 0(mod\ m).$$

Mas se $\lambda \cdot v - \lambda \cdot v_E \equiv 0(mod\ m)$, então, pela Proposição 5. (página 07), temos que $\lambda \cdot v_E \equiv 0(mod\ m)$, o que implica na não detecção do erro.

Logo, para detectar o erro, precisamos ter simultaneamente $(\lambda_j - \lambda_i) \not\equiv 0(mod\ m)$ e $(d_i - d_j) \not\equiv 0(mod\ m)$.

A primeira incongruência só ocorre se, e somente se, $mdc(\lambda_j - \lambda_i, m) = 1$, como consequência direta da Proposição 7 (página 08), tomando $s = 1$ e $p = \lambda_j - \lambda_i$ ou $p = \lambda_i - \lambda_j$ (conforme a observação acima); a segunda é sempre verdadeira, como consequência do Lema 2 (página 04). ∎

À luz deste teorema fica claro que, para que ocorra a detecção destes dois tipos de erros (erros que juntos, pela tabela 1.1, somam mais de 90% dos erros básicos cometidos), é preciso que o valor de m escolhido seja primo com todas as coordenadas do vetor de pesos λ e com todas as diferenças possíveis entre estas mesmas. Isso justifica o fato que no método da maioria dos sistemas, o valor m é primo.

O três sistemas que usam dígitos verificadores calculados com vetor de pesos fixo expostos neste trabalho usam m primo, o 11. No entanto, todos têm a desvantagem de ocorrer uma solução da equação de congruência o valor 10, que não pertence a Ω_{10}. A saída encontrada pelo ISBN é acrescentar um dígito alfabético extra; já os sistemas CPF/CNPJ usam 0 caso a solução da equação de congruência não seja menor que 10.

3.2 Dígito Verificador por Permutação

Nesta seção será exposto o método de cálculo de dígito verificador onde não existe a figura do vetor de pesos λ fixo. A ferramenta usada é, agora, uma permutação, que, assim como o vetor de pesos, permite obter um membro de uma equação de congruência.

3.2.1 Método

Definição. Seja $v = (d_1, d_2, ..., d_{n-1})$ um vetor característico de uma sequência numérica de $n-1$ dígitos (todos elementos de Ω_{10}), $\sigma : \Omega_{10} \longrightarrow \Omega_{10}$ uma permutação, e um número

primo m, para o qual $d_i < m$ para todo $i < n$. O dígito de verificação desta sequência, pelo método das permutações, é dado pela solução x da equação:

$$\sigma(d_1) + \sigma(d_2) + ... + \sigma(d_{n-1}) + \sigma(x) \equiv c(mod\ m). \tag{3.16}$$

Esta definição, contudo, é pouco utilizada na prática; o procedimento mais comum, ao se usar permutações e congruência no cálculo do dígito verificador, é compor o primeiro membro de (3.16) ainda como soma de parcelas, mas aplicando a permutação σ apenas em alguns dígitos. O exemplo abaixo ilustra esta situação.

Exemplo 14. *Considere uma sequência $d : d_1d_2...d_{n-1}x$ de n dígitos (com n par), e duas permutações $\sigma_p : \Omega_{10} \longrightarrow \Omega_{10}$ e $\sigma_i : \Omega_{10} \longrightarrow \Omega_{10}$, que usadas alternadamente, são restrições de uma função σ a ser aplicada sob os dígitos da sequência d, tal que:*

1. *$\sigma(d_j) = \sigma_p(d_j)$, se j for par.*

2. *$\sigma(d_j) = \sigma_i(d_j)$, se j for ímpar.*

Nestes termos, o dígito verificador da sequência seria a solução x da equação

$$\sigma_i(d_1) + \sigma_p(d_2) + ... + \sigma_i(d_{n-1}) + \sigma_p(x) \equiv c(mod\ m).$$

Se $m > 10$ a solução da equação é única, conforme a Proposição 4 (página 07), tomando $R = \sigma_i(d_1) + \sigma_p(d_2) + ... + \sigma_i(d_{n-1})$. □

Devido ao grande número de possibilidades de aplicações deste método (pois podem ser definidas várias permutações e várias formas de se aplicar cada uma delas), a análise do seu poder de detecção de erros leva em conta muitos casos. Neste trabalho avaliaremos este ponto apenas no sistema de numeração de cartões de créditos.

Tipos mais avançados da aplicação deste método encontram-se citados em Picado [8], tais como os métodos IBM Generalizado, PTT (do banco alemão) e Colenbrander.

3.2.2 Sistema IBM e Cartões de Crédito

Numeração de Cartões

Um exemplo de elaboração do dígito verificador por permutação é o método da IBM usado na numeração dos cartões de crédito de uso internacional. Esta numeração é regida

pela normativa ISO/IEC 7812, elaborada pela International Organization for Standardization (ISO) em 1989 (disponível em [6]). As sequências desta numeração têm 16 dígitos, sendo os 6 primeiros referentes à instituição que emitiu o cartão (IIN em inglês, cujo controle da numeração são de responsabilidade da Associação Americana de Bancos), os 9 seguintes são referentes ao cliente dono do cartão, o 16º é ao dígito verificador.

O cálculo do dígito verificador dos cartões usa $c = 0$, $m = 10$ e, na obtenção do primeiro membro da equação (3.16), usa a permutação ζ abaixo, que é aplicada somente nos dígitos de índice ímpar; os dígitos de índice par mantêm-se inalterados.

$$\zeta = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}$$

Esta permutação é parte do Algoritmo de Luhn, um método aritmético criado em 1957 por Hans Peter Luhn (1896-1964), engenheiro da IBM (mais detalhes em [3]).

Considere uma sequência $d_1 d_2 ... d_{15} x$. O dígito verificador, pelo método da IBM, para cartões de crédito, é o valor x para o qual temos:

$$\zeta(d_1) + d_2 + \zeta(d_3) + d_4 + \ldots + \zeta(d_{13}) + d_{14} + \zeta(d_{15}) + x \equiv 0 (mod\ 10). \tag{3.17}$$

O valor de x, nas condições acima, é único.

Exemplo 15. *Determine o dígito verificador x da numeração fictícia de um cartão de crédito 004455-242477111-x, pelo método da IBM.*

Solução: Aplicando ζ à sequência proposta, temos

$$\zeta(0) + 0 + \zeta(4) + 4 + \zeta(5) + 5 + \zeta(2) + 4 + \zeta(2) + 4 + \zeta(7) + 7 + \zeta(1) + 1 + \zeta(1) + x =$$
$$0 + 0 + 8 + 4 + 1 + 5 + 4 + 8 + 4 + 8 + 5 + 7 + 2 + 1 + 2 + x =$$
$$59 + x.$$

Como $x = 1$ é a única solução de $59 + x \equiv 0 (mod\ 10)$ em Ω_{10}, o número do cartão, completo, é *004455-242477111-1.* □

Para simplificar a notação, definamos por $\phi(s)$ o primeiro membro da equação (3.17) acima, tomando $s = d_1 d_2 ... d_{15} x$ e pondo $x = d_{16}$:

$$\phi(s) = \zeta(d_1) + d_2 + \zeta(d_3) + d_4 + \ldots + \zeta(d_{13}) + d_{14} + \zeta(d_{15}) + d_{16}.$$

Se durante a transmissão de número de cartão de créditos de vetor característico v ocorrer um erro, gerando assim uma sequência-erro s_E, temos que:

1. se $\phi(s_E) \equiv 0(mod\ 10)$, então o erro cometido não foi detectado pelo método.

2. se $\phi(s_E) \not\equiv 0(mod\ 10)$, então o método detectou o erro.

Dois resultados interessantes envolvendo o método IBM, para uma sequência de 16 dígitos de um cartão de crédito, são apresentados a seguir. Antes, contudo, demonstraremos um lema.

Lema 4. *A igualdade* $\zeta(m) + n - (m + \zeta(n)) = 0$ *(com* $n \neq m$*) só ocorre se tivermos* $m = 0$ *e* $n = 9$*, ou* $m = 9$ *e* $n = 0$*.*

Demonstração: Observemos que:

$$\begin{aligned}\zeta(m) + n - (m + \zeta(n)) = \\ \zeta(m) - m + n - \zeta(n) = \\ (\zeta(m) - m) - (\zeta(n) - n).\end{aligned}$$

Definindo a função auxiliar $h : \Omega_{10} \longrightarrow \Omega_{10}$ tal que $h(x) = \zeta(x) - x$, temos $h(0) = 0$, $h(1) = 1$, $h(2) = 2$, $h(3) = 3$, $h(4) = 4$, $h(5) = -4$, $h(6) = -3$, $h(7) = -2$, $h(8) = -1$ e $h(9) = 0$.

Dessa forma, temos que $\zeta(m) + n - (m + \zeta(n)) = 0$ somente se $h(m) - h(n) = 0$ o que equivale a $h(m) = h(n)$, o que só ocorre se $m = 0$ e $n = 9$, ou $m = 9$ e $n = 0$, uma vez que 0 e 9 são os único valores que tem mesma imagem pela função auxiliar $h(x)$. ∎

Note, que, para quaisquer $a, b \in \Omega_{10}$, $|h(a) - h(b)| \leq 8$.

Proposição 11. *O método da IBM não detecta transposições de coordenadas de índices de mesma paridade.*

Demonstração: Podemos representar $\phi(v)$ como:

$$\phi(v) = \sum_{k=1}^{8} \zeta(d_{2k-1}) + \sum_{k=1}^{8} d_{2k},$$

com o primeiro somatório fazendo o referência aos dígitos de posição ímpar, e o segundo somatório fazendo referência aos dígitos de posição par. Suponha que ocorra uma transposição entre quaisquer dois dígitos de posição de mesma paridade. Essa transposição gera uma sequência-erro s_E, para o qual ainda vale $\phi(v_E) \equiv 0(mod\ 10)$, pois a transposição cometida envolve dois termos do mesmo somatório, e isto não altera a soma neste somatório, de modo que se tem

$$\phi(s_E) = \sum_{k=1}^{8} \zeta(d_{2k-1}) + \sum_{k=1}^{8} d_{2k} = \phi(v),$$

e, consequentemente, o erro não é detectado. ∎

Proposição 12. *O método da IBM descrito acima detecta todo erro singular (a) e toda transposição adjacente exceto se formada por -09- ou -90- (b).*

Demonstração: (a) Considere uma sequência numérica $d_1d_2d_3 \ldots d_{15}d_{16}$. Suponha que houve, na transmissão do vetor característico v da sequência acima, um erro singular $d_j \to d_E$, com j ímpar (o caso se j é par é análogo), gerando um vetor-erro $v_E = (d_1, ..., d_{j-1}, d_E, d_{j+1}, ..., d_{16})$. Então, fazendo uso da mesma função auxiliar do Lema 4, temos:

$$\begin{aligned} \phi(v) - \phi(v_E) = \\ (\zeta(d_1) + \ldots + \zeta(d_j) + \ldots + d_{16}) - (\zeta(d_1) + \ldots + \zeta(d_E) + \ldots + d_{16}) = \\ \zeta(d_j) - \zeta(d_E). \end{aligned}$$

Como $\zeta(d_j) \neq \zeta(d_E)$ e $0 \leq \zeta(d_j), \zeta(d_E) < 10$, então $0 < \zeta(d_j) - \zeta(d_E) < 10$, portanto $\zeta(d_j) - \zeta(d_E) \not\equiv 0(mod\ 10)$ e, consequentemente, $\phi(v) - \phi(v_E) \not\equiv 0(mod\ 10)$.

Ora, como $\phi(v) \equiv 0(mod\ 10)$, então $\phi(v_E) \not\equiv 0(mod\ 10)$ (pela Proposição 6, página 08), o que significa que o erro é detectado.

(b) Suponha que ocorra uma transposição adjacente entre os termos d_j e d_{j+1} de v (ambos evidentemente diferentes), com j ímpar (se j for par, trata-se de maneira análoga), gerando um vetor-erro $v_E = (d_1, ..., d_{j+1}, d_j, ..., d_{16})$. Então, fazendo uso da mesma função

auxiliar $h(x)$ do Lema 4, temos:

$$\begin{aligned}
&\phi(v) - \phi(v_E) = \\
&(\zeta(d_1) + \ldots + \zeta(d_j) + d_{j+1} + \ldots + d_{16}) - (\zeta(d_1) + \ldots + \zeta(d_{j+1}) + d_j + \ldots + d_{16}) = \\
&(\zeta(d_j) + d_{j+1}) - (\zeta(d_{j+1}) + d_j) = \\
&(\zeta(d_j) - d_j) - (\zeta(d_{j+1}) - d_{j+1}) = \\
&h(d_j) - h(d_{j+1}).
\end{aligned}$$

Temos então duas possibilidades:

1. se $\phi(v) - \phi(v_E) = h(d_j) - h(d_{j+1}) \neq 0$, então $\phi(v) - \phi(v_E) \in \{-8, -7, -6, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6, 7, 8\}$. Em todo caso, $\phi(v) - \phi(v_E) \not\equiv 0(mod\ 10)$, e pela Proposição 06 (página 08), $\phi(v_E) \not\equiv 0(mod\ 10)$, o que implicaria na detecção do erro.

2. se $h(d_j) - h(d_{j+1}) = 0$, então ou temos $d_j = 0$ e $d_{j+1} = 9$ (sequência -09-), ou $d_j = 9$ e $d_{j+1} = 0$ (sequência -90-), conforme Lema 4 (pondo $m = d_i$ e $n = d_{i+1}$). Neste caso, $\phi(v) - \phi(v_E) \equiv 0(mod\ 10) \implies \phi(v_E) \equiv 0(mod\ 10)$, o que implica na não detecção do erro de transposição. ∎

Exemplo 16. *Considere uma numeração fictícia de um cartão de créditos s = 8756-5390-7866-7686. Temos que* $\phi(s) = 80$ *e, naturalmente,* $80 \equiv 0(mod\ 10)$. *Simulemos ter cometido três erros.*

1. *Suponha ter ocorrido erro singular 7 → 3 no nono dígito da sequência. Este erro gera uma sequência erro* s_E *= 8756-5390-3866-7686 para a qual temos:*

$$\begin{aligned}
\phi(s_E) &= 7 + 7 + 1 + 6 + 1 + 3 + 9 + 0 + 6 + 8 + 3 + 6 + 5 + 6 + 7 + 6 \\
&= 81.
\end{aligned}$$

   Como $81 \not\equiv 0(mod\ 10)$, *o erro é detectado.*

2. *Suponha ter ocorrido uma transposição adjacente entre o 2º e o 3º dígito. A sequência-erro* s_E *=8576-5390-7866-7686 gerada é tal que:*

$$\begin{aligned}
\phi(s_E) &= 7 + 5 + 5 + 6 + 1 + 3 + 9 + 0 + 5 + 8 + 3 + 6 + 5 + 6 + 7 + 6 \\
&= 82.
\end{aligned}$$

   Como $82 \not\equiv 0(mod\ 10)$, *a transposição cometida também é detectada.*

3. *Suponha ter ocorrido uma transposição adjacente entre o 7º e o 8º dígito (um erro na sequência -09-). Este erro gera uma sequência-erro s_E =8576-5309-7866-7686 para a qual temos:*

$$\begin{aligned}\phi(s_E) &= 7+7+1+6+1+3+0+9+5+8+3+6+5+6+7+6 \\ &= 80.\end{aligned}$$

O erro, portanto, não pode ser detectado. □

Vale ressaltar que os bancos, de maneira independente da normativa ISO/IEC 7812, podem complementar seus sistemas de segurança de numeração com outros métodos, gerando sequências adicionais que são (eventualmente) impressas nos cartões, mas não podem alterar o padrão da sequência principal e de seus 16 dígitos.

Capítulo 4

Dígito Verificador e o Grupo D_5

Jacobus (Koos) Verhoeff (1927 -) é um matemático, cientista computacional e artista holandês aposentado. Seu método de elaboração de dígito verificadores foi publicado em 1969 (ver [11]) em sua tese de doutorado. Este modelo se baseia não em Aritmética Modular, mas no grupo diedral D_5, um grupo composto pelas 10 permutações de um pentágono e a operação de composição entre elas. Sua vantagem sobre os métodos modulares é que este método detecta todos os erros singulares, todos os erros de tranposição adjacente e usa apenas os elementos de Ω_{10}.

4.1 Simetrias do Pentágono Regular

Sobre cada polígono regular de n lados podem ser determinadas tanto rotações em torno do centro da circunferência inscrita ao polígono quanto eixos de simetria, que ligam ou vértices opostos, ou um vértice ao ponto médio do lado oposto (dependendo da paridade do número de lados do polígono). As rotações são em número de n, todas com ângulos $i \cdot \frac{2\pi}{n}$, com $i = 0, ..., n-1$, em um dos dois sentidos (horário ou anti-horário). As reflexões também são em número de n, tanto se n for ímpar (um eixo de simetria para cada vértice), como se n for par (mas neste caso, existem $n/2$ simetrias entre vértices opostos e $n/2$ simetrias entre pontos médios de lados opostos).

Permutações de um pentágono regular

Considere um pentágono regular com vértices numerados de A até E, no sentido anti-horário. Este pentágono possui 5 eixos de simetria, cada um ligando um dos vértice ao ponto médio do lado oposto. Cada eixo destes determina uma reflexão diferente.

Este pentágono possui, no sentido horário (assim como no anti-horário), 5 rotações entre seus vértices. Estas rotações têm ângulos de $0rad$, $\frac{2\pi}{5}rad$, $\frac{4\pi}{5}rad$, $\frac{6\pi}{5}rad$ e $\frac{8\pi}{5}rad$. Observe que rotações em sentidos diferentes podem ter mesmo resultado. Por exemplo, a rotação de $\frac{6\pi}{5}rad$ no sentido horário coincide com a rotação de $\frac{4\pi}{5}rad$ no sentido anti-horário.

Denotemos cada rotação por R_i, com $i = 0, 1, 2, 3, 4$, e cada reflexão por S_j, com $j = 5, 6, 7, 8, 9$, conforme as figuras 4.1 e 4.2.

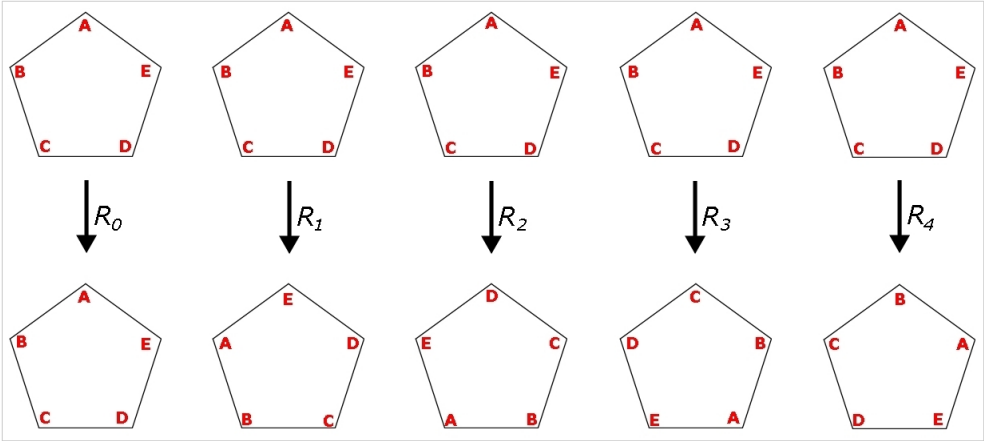

Figura 4.1: Rotações R_i do pentágono regular.

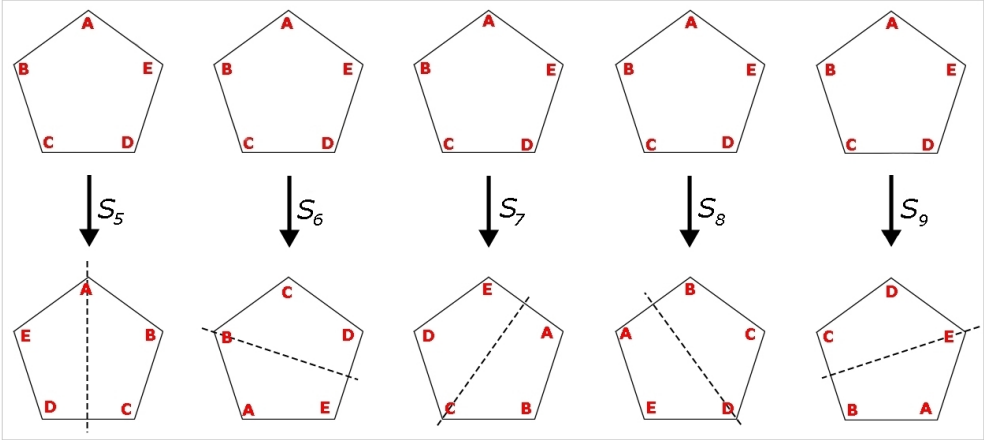

Figura 4.2: Reflexões S_i do pentágono regular.

Definição. Define-se por *permutação do pentágono regular* cada uma das 5 reflexões S_5, S_6, S_7, S_8 e S_9 e cada uma das 5 rotações R_0, R_1, R_2, R_3 e R_4 definidas sobre o polígono.

Definição. Define-se por D_5 o conjunto formado pelas 10 permutações definidas sobre o pentágono regular.

4.2 O Grupo D_5

4.2.1 Composição de Permutações

As permutações de um pentágono regular podem ser compostas entre si, efetuadas sequenciadamente. Sejam então $A, B \in D_5$. Denotemos por $A \circ B$ a composição das permutações A e B, efetuadas nesta ordem, formalmente definida como:

$$\circ : G \times G \longrightarrow G$$

$$\circ(A, B) \longrightarrow A \circ B$$

Esta operação de composição sempre resulta em outra permutação do pentágono, ou seja, $A \circ B \in D_5$. Por exemplo, a rotação R_2 composta com R_3 equivale à rotação R_0. Simbolicamente: $R_2 \circ R_3 = R_4$. A Figura 4.3 exemplifica a composição $S_6 \circ R_3$.

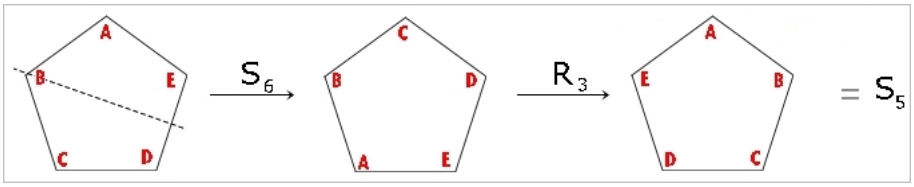

Figura 4.3: Composição $S_6 \circ R_3 = S_5$.

A tabela 4.1 no fim desta subseção traz todas as composições possíveis entre os elementos de D_5. Nela, os valores $X_i \circ Y_j$ são tomados com X_i da primeira coluna e Y_j da primeira linha.

Três resultados podem ser obtidos da análise direta da tabela (4.1) sobre a operação composição:

1. Resultado 1: para quaisquer $X, Y, Z \in D_5$ temos $(X \circ Y) \circ Z = X \circ (Y \circ Z)$.

2. Resultado 2: R_0 é elemento neutro (o único), pois $X \circ R_0 = R_0 \circ X = X$, para todo $X \in D_5$.

3. Resultado 3: para qualquer elemento $X \in D_5$, existe um elemento $Y \in D_5$, único, tal que $X \circ Y = Y \circ X = R_0$.

Estes resultados permitem concluir que o conjunto D_5 forma em grupo sobre a operação composição ($\circ$) apresentada acima, uma vez que esta operação satisfaz às três condições

requisitadas pela definição de grupo: o Resultado 1 mostra que a composição satisfaz à Associatividade; o Resultado 2 mostra que existem um único elemento neutro; e o Resultado 3 mostra que cada elemento de D_5 tem um elemento inverso. Destas três condições, a associatividade tem uma grande importância nas demonstrações que atestam a eficiência do método de Verhoeff para alguns tipos de erro.

$\circ$	R_0	R_1	R_2	R_3	R_4	S_5	S_6	S_7	S_8	S_9
R_0	R_0	R_1	R_2	R_3	R_4	S_5	S_6	S_7	S_8	S_9
R_1	R_1	R_2	R_3	R_4	R_0	S_7	S_8	S_9	S_5	S_6
R_2	R_2	R_3	R_4	R_0	R_1	S_9	S_5	S_6	S_7	S_8
R_3	R_3	R_4	R_0	R_1	R_2	S_6	S_7	S_8	S_9	S_5
R_4	R_4	R_0	R_1	R_2	R_3	S_8	S_9	S_5	S_6	S_7
S_5	S_5	S_8	S_6	S_9	S_7	R_0	R_2	R_4	R_1	R_3
S_6	S_6	S_9	S_7	S_5	S_8	R_3	R_0	R_2	R_4	R_1
S_7	S_7	S_5	S_8	S_6	S_9	R_1	R_3	R_0	R_2	R_4
S_8	S_8	S_6	S_9	S_7	S_5	R_4	R_1	R_3	R_0	R_2
S_9	S_9	S_7	S_5	S_8	S_6	R_2	R_4	R_1	R_3	R_0

Tabela 4.1: Composições em D_5.

4.3 Dígito Verificador pelo Grupo D_5

Pelo método de Verhoeff, o dígito verificador é a solução de uma equação cujo primeiro membro é uma composição de permutações aplicadas sobre os dígitos da sequência.

4.3.1 Notação com algarismos

A aplicação do grupo D_5 no cálculo de dígitos verificadores de sequências precisa ser alterada, para usarmos não as simetrias, mas algarismos. Para tanto, adotemos as equivalências $R_0 = 0$, $R_1 = 1$, $R_2 = 2$, $R_3 = 3$, $R_4 = 4$, $S_5 = 5$, $S_6 = 6$, $S_7 = 7$, $S_8 = 8$ e $S_9 = 9$. Nesta nova notação, representaremos a operação *composição* (representada por '$\circ$') agora por '$\bullet$', onde.

$$\bullet : \Omega_{10} \times \Omega_{10} \longrightarrow \Omega_{10}$$

$$\bullet(A, B) \longrightarrow A \bullet B.$$

Cada composição exposta na tabela 4.1 será reescrita sob nesta nova notação. Por exemplo, a composição $R_2 \circ S_8 = S_9$ será escrita agora como $2 \bullet 8 = 9$. A mudança de notação aplicada em toda a tabela 4.1 resulta na tabela 4.2 a seguir.

$\bullet$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	7	8	9	5	6
2	2	3	4	0	1	9	5	6	7	8
3	3	4	0	1	2	6	7	8	9	5
4	4	0	1	2	3	8	9	5	6	7
5	5	8	6	9	7	0	2	4	1	3
6	6	9	7	5	8	3	0	2	4	1
7	7	5	8	6	9	1	3	0	2	4
8	8	6	9	7	5	4	1	3	0	2
9	9	7	5	8	6	2	4	1	3	0

Tabela 4.2: Composição em D_5 sob a nova notação.

Um resultado simples mas importante e verificável por rápida inspeção da tabela é exposto no lema abaixo.

Lema 5. *Para $a, b, c \in D_5$, se $a \neq b$, então $c \bullet a \neq c \bullet b$ e $a \bullet c \neq b \bullet c$.*

4.3.2 Definição e Exemplo

Definição. Considere um vetor característico $v = (a_1, a_2, ..., a_{n-1})$, a operação '$\bullet$' sobre o grupo diedral D_5 e uma permutação ϕ de D_5 tal que, para todo $a,\ b \in D_5$, tenhamos:

$$a \bullet \phi(b) \neq b \bullet \phi(a) \tag{4.1}$$

O dígito verificador, pelo método de Verhoeff, é a solução x ($x \in D_5$) da equação

$$\phi(a_1) \bullet \phi^2(a_2) \bullet \phi^3(a_3) \bullet ... \bullet \phi^{n-1}(a_{n-1}) \bullet x = 0. \tag{4.2}$$

A solução de (4.2) é única, pois pondo $s = \phi(a_1) \bullet \phi^2(a_2) \bullet \phi^3(a_3) \bullet ... \bullet \phi^{n-1}(a_{n-1})$, temos que $s \in D_5$, logo é constante, e pelo Lema 05, $s \bullet x = 0$ tem solução única.

É imprescindível, para a o cálculo do dígito verificador por este método, que a permutação ϕ satisfaça o resultado (4.1). Quando uma aplicação em um grupo G tem esta característica, ela é chamada de ***aplicação antissimétrica***. Dois exemplos clássicos de permutações anti-simetricas de D_{10} é a permutação $\theta = (1,4)(2,3)(5,8,6,9,7)$, citada em Picado [8], e a permutação $\tau = (0,1,5,8,9,4,2,7)(3,6)$, citada em Polcino Millies [9].

Exemplo 17. *Considere o seguinte código fictício* $03328791664x$*, e determinemos qual seria seu dígito de verificação* x *pelo método de Verhoeff, usando a permutaçãoτ* $= (0,1,5,8,9,4,2,7)(3,6)$.

Solução. Devemos obter x como solução da equação

$$\tau(0) \bullet \tau^2(3) \bullet \tau^3(3) \bullet \tau^4(2) \bullet \tau^5(8) \bullet \tau^6(7) \bullet \tau^7(9) \bullet \tau^8(1) \bullet \tau^9(6) \bullet \tau^{10}(6) \bullet \tau^{11}(4) \bullet x = 0.$$

A permutação τ é da forma

$$\tau = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \end{pmatrix}$$

A tabela (4.3) abaixo traz todas as permutações τ^n até a $n = 11$, permitindo assim o cálculo direto do dígito verificador.

τ^0	0	1	2	3	4	5	6	7	8	9
τ^1	1	5	7	6	2	8	3	0	9	4
τ^2	5	8	0	3	7	9	6	1	4	2
τ^3	8	9	1	6	0	4	3	5	2	7
τ^4	9	4	5	3	1	2	6	8	7	0
τ^5	4	2	8	6	5	7	3	9	0	1
τ^6	2	7	9	3	8	0	6	4	1	5
τ^7	7	0	4	6	9	1	3	2	5	8
τ^8	0	1	2	3	4	5	6	7	8	9
τ^9	1	5	7	6	2	8	3	0	9	4
τ^{10}	5	8	0	3	7	9	6	1	4	2
τ^{11}	8	9	1	6	0	4	3	5	2	7

Tabela 4.3: Iterações de τ até a 11ª ordem.

Efetuando os devidos cálculos, usando a propriedade associativa da operação $\bullet$, temos:

$$\tau(0) \bullet \tau^2(3) \bullet \tau^3(3) \bullet \tau^4(2) \bullet \tau^5(8) \bullet \tau^6(7) \bullet \tau^7(9) \bullet \tau^8(1) \bullet \tau^9(6) \bullet \tau^{10}(6) \bullet \tau^{11}(4) \bullet x = 0$$
$$1 \bullet 3 \bullet 6 \bullet 5 \bullet 0 \bullet 4 \bullet 8 \bullet 1 \bullet 3 \bullet 6 \bullet 0 \bullet x = 0$$
$$(1 \bullet 3) \bullet (6 \bullet 5) \bullet (0 \bullet 4) \bullet (8 \bullet 1) \bullet (3 \bullet 6) \bullet 0 \bullet x = 0$$
$$4 \bullet 3 \bullet 4 \bullet 6 \bullet 7 \bullet 0 \bullet x = 0$$
$$(4 \bullet 3) \bullet (4 \bullet 6) \bullet (7 \bullet 0) \bullet x = 0$$
$$2 \bullet 9 \bullet 7 \bullet x = 0$$
$$8 \bullet 7 \bullet x = 0$$
$$3 \bullet x = 0.$$

Em consulta a tabela (4.2), a única solução de $3 \bullet x = 0$ é $x = 2$. Assim, o código completo é *033287916642*. □

4.3.3 Poder de detecção do método de Verhoeff

A proposição a seguir mostra o poder de detecção de erros do método de Verhoeff e a importância de uma aplicação anti-simétrica de D_5 na obtenção do dígito verificador.

Proposição 13. *Considere uma sequência de dígitos $d_1d_2...d_{n-1}$ (com $d_i \in D_5$ para todo $i \leq n$) e uma permutação σ de D_5 tal que*

$$m \bullet \sigma(n) \neq n \bullet \sigma(m), \tag{4.3}$$

para todo $m, n \in D_5$. O método de Verhoeff detecta todos os erros singulares (a) e todos os erros de transposição adjacente (b) cometidos na sequência.

Demonstração:

(a) Considere que na transmissão da sequência original $d_1d_2...d_i...d_{n-1}$ tenha ocorrido um único erro singular $d_i \longrightarrow d_E$, gerando a sequência erro $d_1d_2...d_E...d_{n-1}$. Sejam x' e x'' os dígitos verificadores das sequência original e errada, respectivamente. Provemos que $x' \neq x''$, implicando assim na detecção do erro.

Nestas condições, temos que:

$$\sigma(d_1) \bullet ... \bullet \sigma^{i-1}(d_{i-1}) \bullet \sigma^i(d_i) \bullet \sigma^{i+1}(d_{i+1}) \bullet ... \bullet \sigma^{n-1}(d_{n-1}) \bullet x' = 0$$

e

$$\sigma(d_1) \bullet ... \bullet \sigma^{i-1}(d_{i-1}) \bullet \sigma^i(d_E) \bullet \sigma^{i+1}(d_{i+1}) \bullet ... \bullet \sigma^{n-1}(d_{n-1}) \bullet x'' = 0.$$

Pondo $a = \sigma(d_1) \bullet ... \bullet \sigma^{i-1}(d_{i-1})$ e $b = \sigma^{i+1}(d_{i+1}) \bullet ... \bullet \sigma^{n-1}(d_{n-1})$ para simplificar a notação, temos:

$$a \bullet \sigma^i(d_i) \bullet b \bullet x' = a \bullet \sigma^i(d_E) \bullet b \bullet x'' = 0. \tag{4.4}$$

Como σ^i também é uma permutação de D_5 (logo é injetiva), temos $\sigma^i(d_i) \neq \sigma^i(d_E)$, e pelo Lema 5:

$$\begin{aligned} \sigma^i(d_i) &\neq \sigma^i(d_E) \\ a \bullet \sigma^i(d_i) &\neq a \bullet \sigma^i(d_E) \\ a \bullet \sigma^i(d_i) \bullet b &\neq a \bullet \sigma^i(d_E) \bullet b. \end{aligned}$$

Se tivéssemos $x' = x''$, ainda pelo Lema 5, teríamos:

$$a \bullet \sigma^i(d_i) \bullet b \bullet x' \neq a \bullet \sigma^i(d_E) \bullet b \bullet x'',$$

uma contradição da igualdade exposta na expressão (4.4).

(b) Considere que na transmissão da sequência original $d_1d_2...d_i...d_{n-1}$ tenha ocorrido transposição adjacente $...d_id_{i+1}... \longrightarrow ...d_{i+1}d_i....$ Sejam x' e x'' os dígitos verificadores das sequência original e errada, respectivamente. Provemos também que $x' \neq x''$, implicando assim na detecção do erro.

Nestas condições, temos que:

$$\sigma(d_1) \bullet ... \bullet \sigma^i(d_i) \bullet \sigma^{i+1}(d_{i+1}) \bullet ... \bullet \sigma^{n-1}(d_{n-1}) \bullet x' = 0.$$

e

$$\sigma(d_1) \bullet ... \bullet \sigma^i(d_{i+1}) \bullet \sigma^{i+1}(d_i) \bullet ... \bullet \sigma^{n-1}(d_{n-1}) \bullet x'' = 0.$$

Pondo $a = \sigma(d_1) \bullet ... \bullet \sigma^{i-1}(d_{i-1})$ e $b = \sigma^{i+2}(d_{i+2}) \bullet ... \bullet \sigma^{n-1}(d_{n-1})$, para simplificar a notação, temos:

$$a \bullet \sigma^i(d_i) \bullet \sigma^{i+1}(d_{i+1}) \bullet b \bullet x' = a \bullet \sigma^i(d_{i+1}) \bullet \sigma^{i+1}(d_i) \bullet b \bullet x'' = 0. \tag{4.5}$$

Se tomarmos $m = \sigma^i(d_i)$ e $n = \sigma^i(d_{i+1})$ expressão (4.3), que é uma das hipóteses da proposição, temos:

$$\begin{aligned} m \bullet \sigma(n) &\neq n \bullet \sigma(m) \\ \sigma^i(d_i) \bullet \sigma(\sigma^i(d_{i+1})) &\neq \sigma^i(d_{i+1}) \bullet \sigma(\sigma^i(d_i)) \\ \sigma^i(d_i) \bullet \sigma^{i+1}(d_{i+1}) &\neq \sigma^i(d_{i+1}) \bullet \sigma^{i+1}(d_i). \end{aligned}$$

Consequentemente, pelo Lema 5:

$$\begin{aligned} a \bullet \sigma^{i}(d_i) \bullet \sigma^{i+1}(d_{i+1}) &\neq a \bullet \sigma^{i}(d_{i+1}) \bullet \sigma^{i+1}(d_i) \\ a \bullet \sigma^{i}(d_i) \bullet \sigma^{i+1}(d_{i+1}) \bullet b &\neq a \bullet \sigma^{i}(d_{i+1}) \bullet \sigma^{i+1}(d_i) \bullet b. \end{aligned}$$

Se tivéssemos $x' = x''$, ainda pelo Lema 5, teríamos:

$$a \bullet \sigma^{i}(d_i) \bullet \sigma^{i+1}(d_{i+1}) \bullet b \bullet x' \neq a \bullet \sigma^{i}(d_{i+1}) \bullet \sigma^{i+1}(d_i) \bullet b \bullet x''.$$

uma contradição da igualdade exposta na expressão (4.5). ∎

O método de Verhoeff consegue detectar tanto erros singulares como erros de transposição adjacentes, qualidades também presentes no método da ISBN; no entanto, o método de Verhoeff usa apenas os elementos de Ω_{10}, algo que sob o método da ISBN não é possível por conta da necessidade de um dígito extra.

4.3.4 Aplicação

Segundo N. R. Wagner [7], além da eficiência plena para erros singulares e erros de transposição, o método de Verhoeff detecta 95.555% dos erros gêmeos e 94.222% das transposições intercaladas e erros gêmeos intercalados. Apesar da eficiência perante todos os outros métodos citados neste trabalho, é raramente usado, sendo muito poucas as referências a ele na literatura matemática. O mais clássico exemplo de seu uso (mais precisamente, de uma variante sua) era a antiga produção do marco alemão, a moeda que circulou na Alemanha até de 1949 a 2002, antes do advento do Euro. A Universidade de Coimbra (Portugal), referência em trabalhos sobre códigos numéricos e similares, utiliza um algoritmo semelhante ao método de Verhoeff para gerar matrículas de alunos e códigos de componentes curriculares.

Capítulo 5

Aplicação no Ensino

Neste capítulo será apresentada uma sugestão de aplicação do conteúdo deste trabalho no Ensino Médio (incluindo a modalidade Técnica-Profissional). Para tanto, primeiramente apontaremos motivos para esta abordagem; em seguida, uma breve discussão sobre propostas de conteúdos não curriculares na escola. E finalmente, uma sugestão de aplicação.

5.1 Motivação

Vários fatores (educacionais, sociais, científicos) podem ser usados para justificar uma abordagem sobre erros e dígitos verificadores no Ensino Médio, dentre os quais destacam-se três:

1. **Legislação e Cidadania**. A legislação educacional orienta sobre o uso da matemática como ferramenta de cidadania. Os Parâmetros Curriculares Nacionais [10] trazem em seu texto, como finalidades do ensino de Matemática no nível médio levar o aluno a (entre outros pontos):

   > (a) aplicar seus conhecimentos matemáticos a situações diversas, utilizando-os na interpretação da ciência, na atividade tecnológica e nas atividades cotidianas.
   >
   > (b) analisar e valorizar informações provenientes de diferentes fontes, utilizando ferramentas matemáticas para formar uma opinião própria que lhe permita expressar-se criticamente sobre problemas da Matemática, das outras áreas do conhecimento e da atualidade.

A maior parte da população brasileira desconhece a existência dos sistemas de segurança de informações mantidos pelos governos, repartições e empresas, desconhecendo também o significado da maioria dos números sequenciais que o cercam, e a sua necessidade. Os métodos de dígitos verificadores de sequências numéricas, por serem bastante acessíveis (estão presentes em documentos, codificação de produtos, etc.), fornecem boa ferramenta de introdução destas ideias no público geral.

2. **A matemática precisa ser significativa**. Existe muitas indagações dos estudante pelo o 'por que' de muitos conteúdos de matemática serem parte do Currículo do Ensino Médio. Muitas vezes o professor argumenta a importância daquele tópico, mas não consegue convencer seu público. Neste sentido, toda atividade que esclareça a aplicabilidade de um conteúdo é importante.

3. **Revelação de Talentos**. Nas duas últimas décadas uma grande quantidade de estudantes com grande potencial matemático vêm sendo revelados no Brasil nas escolas de educação básica e nas Universidades, a maioria pelos seus resultados em atividades e projetos (como competições científicas locais, OBMEP (Olímpiada Brasileira de Matemática das Escolas Públicas) e OBM) que rompem com um modelo arcaico e tradicional de se trabalhar Matemática, gerando um ambiente favorável a que alunos com excepcional talento possam demonstrá-lo. Atividades contextualizadas e aplicadas, exatamente por se mostrarem como uma proposta mais interessante de exposição de conteúdos, podem quebrar preconceitos e paradigmas pessoais.

5.2 Abordagens

5.2.1 Métodos pela Aritmética Modular

A Teoria das Congruências é de extrema importância para a análise do poder de detecção dos métodos expostos (capítulos 3 e 4), principalmente por permitir que provemos que alguns tipos de erros são detectados em cada método, além de dar as garantias tanto da existência de um dígito verificador quanto da unicidade deste dígito. No entanto, no contexto de Ensino Médio, uma abordagem do tema pela Aritmética Modular teria como limitação o fato de que a Teoria de Congruências, de maneira formal, não faz parte do currículo do Ensino Médio (ver BRASIL [2]).

Por outro lado, existe uma grande quantidade de páginas na internet que versam o tema 'dígito verificador'. A grande maioria não adota a teoria de congruência usada neste trabalho, optando por usar uma espécie de 'busca manual' do dígito verificador, auxiliados por ferramentas como tabelas, mapas, calculadoras, etc. No exemplo a seguir ilustra-se um caso destes, onde calcula-se o dígito verificador de uma sequência pelo EAN-13 sem uso de congruências.

Exemplo 18. *Considere a sequência incompleta de 12 dígitos 785890025126 e calculemos seu dígito verificador sem usar congruência, pelo método do EAN-13. Para tanto, dividiremos este cálculo em etapas:*

1. *Adicione todos os dígitos das posições pares, e multiplique o resultado obtido por 3.*

$$8 + 8 + 0 + 2 + 1 + 6 = 25$$

$$3 \cdot 25 = 75.$$

2. *Some todos os dígitos das posições ímpares.*

$$7 + 5 + 9 + 0 + 5 + 2 = 28.$$

3. *Some os resultados das etapas 1 e 2.*

$$75 + 28 = 103.$$

4. *Determine que valor menor que 10, somado ao resultado da etapa 3, gera um múltiplo de 10. Esse valor é o dígito verificador.*

   O menor múltiplo de 10 maior que 103 é 110, logo o dígito verificador da sequência é 110-103 = 7, e a sequência completa é 7858900251267.

As etapas 1, 2 e 3 do cálculo do exemplo anterior equivalem, do ponto de vista prático, à montagem e cálculo de um produto interno, notando que o vetor de pesos do EAN-13 tem todas as suas coordenadas de posição par iguais a 3, e as coordenadas de posição ímpar iguais a 1. A etapa 4 equivale, por sua vez, a resolver a equação de congruência (com $m = 10$, daí a colocação 'múltiplo de 10') que se obtêm quando o cálculo do dígito verificador é feito usando a Aritmética Modular. As duas maneiras de obter o dígito verificador levam naturalmente à mesma resposta. □

Diante destas duas maneiras (*teoria das congruências* × *método de 'busca'*) possíveis para abordar o tema 'Dígito Verificador pela Aritmética Modular' no Ensino Médio, o professor teria duas opções:

1. Usar Teoria das Congruência. Por ser baseado em conceitos matemáticos ausentes no Currículo do Ensino Médio, uma abordagem neste sentido exigiria do professor, além do domínio do método, o bom senso sobre se seu alunado tem fundamentação matemática suficiente para compreendê-lo durante a atividade na sala de aula, e se o tempo previsto para esta abordagem seria suficiente para sua completa execução.

2. Usar o método da 'busca manual'. O professor, adotando esta opção, teria a vantagem de ter grande referencial disponível na internet, de fácil acesso e compreensão. A sugestão apresentada na próxima seção foi elaborada conforme esta opção.

5.2.2 Método de Verhoeff

O método de Verhoeff precisa, para sua compreensão básica, de conceitos como permutações do pentágono, permutação anti-simétrica, grupo, etc., sendo assim bastante avançado para ser abordado no Ensino Médio.

5.3 Sugestão de Abordagem

Sugerimos aqui uma atividade sobre o dígito verificador calculado com Vetor de Pesos, usando a técnica da 'busca manual do dígito verificador'. Para tal, não se exige do aluno nenhum conhecimento matemático especial. A atividade é dividida em 7 etapas.

Etapa 1. Apresentação da atividade. O professor apresentaria o tema 'Dígito Verificador', destacando que é este um conceito presente na nossa vida cotidiana (citando superficialmente vários exemplos), e qual a sua principal função nas sequência numéricas: a detecção de erros de transmissão.

Etapa 2. O professor apresentaria, rigorosamente, os sistemas que usará em sala, destacando um pouco de seu uso, contexto histórico e regras de construção (o que significa cada dígito ou grupo de dígitos da sequência, e qual seu vetor de pesos). Ele dividiria em seguida sua turma em grupos e daria a cada um sistema diferente.

Etapa 3. Mostra. O professor calcularia (usando o procedimento da 'busca do dígito', tal como no Exemplo 18), com o acompanhamento da turma, o dígito verificador de um exemplo de sequência numérica pertencente a um dos sistemas escolhidos (pode-se até fazer mais de um exemplo de mais de um sistema), como meio de garantir aos alunos que o procedimento executado ali é o válido.

Etapa 4. Os alunos fariam a verificação do dígito verificador de um exemplo real. Se, por exemplo, um grupo tiver ficado com o EAN-13, bastaria o grupo escolher um produto de uso cotidiano (caderno, caixinha de achocolatado, etc.) e fazer a verificação. Um grupo que tenha ficado com CPF poderia fazer a verificação com o documento de um de seus integrantes.

Etapa 5. O professor introduziria, nesta etapa, a discussão sobre erros, focando sua exposição nos dois tipos de erros mais frequentes conforme a tabela 1.1 (página 02), os erros singulares e os erros de transposição adjacente. Em seguida o professor determinaria que cada grupo cometesse os dois erros na sequência que avaliou, em dois casos diferentes, gerando duas sequências-erro.

Etapa 6. Os alunos fariam a reverificação do dígito verificador em suas sequências-erro, tal como foi feito na etapa 4. Neste ponto, o professor definiria "detecção": se o dígito verificador da sequência-erro coincidir com o dígito original, o erro **não** foi detectado; analogamente, se o dígito não coincidir, o erro **foi** detectado.

Etapa 7. Conclusão da atividade. O professor concluiria a atividade destacando que o método de detecção de erros analisado tem um 'poder', e esse poder é avaliado pelos tipos de erros que consegue detectar.

AUTONOMIA E AVALIAÇÃO

O professor, dentro de sua autonomia de trabalho em sala de aula, de particularidades pessoais e profissionais, e das condições de seu público, pode alterar livremente as etapas apresentadas, unindo duas ou mais, ou criando outras etapas de execução. A avaliação da participação dos alunos na atividade também fica a cargo do professor e dos critérios que ele estabelecer para ela.

Conclusão

A sociedade humana é cada vez mais dependente de seus sistemas, dos mais simples e primordiais, como os sistemas de escrita e numeração, aos mais avançados e modernos, como os sistemas de informação que conectam todas as partes do mundo. Este trabalho visou discutir com um pouco mais de detalhe os métodos mais elementares de detecção de erros na transmissão de sequências numéricas, trazendo exemplos do cotidiano e discutindo a eficiência matemática de cada um (pela quantidade de tipos de erros detectáveis e sua frequência total), assim como algumas de suas aplicações e limitações.

Inicialmente foram expostos alguns resultados matemáticos de álgebra e aritmética que fundamentam o funcionamento dos métodos de detecção de erros e a análise de sua eficiência. Em seguida, estes foram expostos de maneira objetiva, ressaltando suas vantagens e limitações e sua aplicação com exemplos do cotidiano. Finalmente, foram propostas duas abordagens do tema para o Ensino Médio, citando motivos para adotá-las e maneiras de executá-las.

Os três métodos expostos neste trabalho têm limitações e vantagens. O método de Verhoeff é bastante eficiente, apesar do rigor computacional. O método por vetor de pesos (da Aritmética Modular) têm a desvantagem de (para uma maior eficiência) precisar estar usando o valor m igual a 11 ou maior, e uma vez que as equações de congruência podem ter solução fora de Ω_{10}, exige-se ou a adoção de símbolos adicionais, ou a atribuição de valores de Ω_{10} como dígito verificador, sendo que estas atribuições podem reduzir a própria eficiência do método perante alguns tipos de erros. Os métodos de permutação (ainda pela Aritmética Modular), por sua grande variabilidade, tem de ser analisados caso a caso.

Referências Bibliográficas

[1] Coutinho, S. C. *Números Inteiros e Criptografia RSA*. Coleção Matemática e Aplicações, IMPA, Rio de Janeiro, 2014.

[2] BRASIL. Secretaria de Educação Básica. Ministério da Educação e Cultura. *Orientações Curriculares para o Ensino Médio*. Brasília, 2006. Disponível em: portal.mec.gov.br/seb/arquivos/pdf/book_volume_01_internet.pdf. Acessado em: 25/08/2017.

[3] Data Genetics. *Credit Cards*. Acessado em: 24/08/2017, e disponível em: http://www.datagenetics.com/blog/july42013/index.html.

[4] Gonçalves, Adilson. *Introdução à Álgebra*. Ed. 3. 194 pp. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1995

[5] Hefez, Abramo.- *Aritmética*. Coleção Profmat, Rio de Janeiro, 2014.

[6] International Organization for Standardization. *ISO/IEC 7812-1:2015*. Disponível em: https://www.iso.org/standard/66011.html. Acesso em: 07 de abril de 2017.

[7] N. R. Wagner. *The Laws of Cryptography With Java Code. [Online]*. Disponível em: http://www.cs.utsa.edu/ wagner/lawsbookcolor/laws.pdf. Acesso em: 07/04/2017

[8] Picado, Jorge. *A álgebra dos sistemas de identificação: da aritmética modular aos grupos diedrais*. Boeltim da Sociedade Portuguesa de Matemática, 2011.

[9] Polcino Milies, C. F. *A matemática dos códigos de barras*. Programa de Iniciação Científica da OBMEP. Rio de Janeiro, pgs. 133-183.

[10] Secretaria de Educação. *Parâmetros Curriculares Nacionais: Matemática*. MEC, Brasília, 1998.

[11] Verhoeff, J. *Error Detecting Decimal Codes*. Mathematical Centre, Amsterdam, 1969.