Carla Rejane Fick Pinz

Dígitos Verificadores e Detecção de Erros

Rio Grande - Rio Grande do Sul - Brasil
agosto, 2013

Carla Rejane Fick Pinz

Dígitos Verificadores e Detecção de Erros

Dissertação submetida por Carla Rejane Fick Pinz como requisito parcial para obtenção do grau de Mestre, pelo Curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) junto ao Instituto de Matemática, Estatística e Física da Universidade Federal do Rio Grande.

Universidade Federal do Rio Grande – FURG

Instituto de Matemática, Estatística e Física – IMEF

Mestrado Profissional em Matemática em Rede Nacional – PROFMAT

Orientador: Edite Taufer

Rio Grande - Rio Grande do Sul - Brasil

agosto, 2013

P661d Pinz, Carla Rejane Fick.
Dígitos Verificadores e Detecção de Erros / Carla Rejane Fick Pinz. – 2013.

53 f.

Dissertação (Mestrado) – Universidade Federal do Rio Grande – Mestrado Profissional em Matemática.

Orientadora: Ma. Edite Taufer.

1. Matemática. 2. Aritmética. 3. Álgebra 4. Dígitos Verificadores. I. Taufer, Edite. II. Título.

CDU 51

Catalogação na fonte: Bibliotecário Cléríston Ribeiro Ramos CRB10/1889

Carla Rejane Fick Pinz

Dígitos Verificadores e Detecção de Erros

Dissertação submetida por Carla Rejane Fick Pinz como requisito parcial para obtenção do grau de Mestre, pelo Curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) junto ao Instituto de Matemática, Estatística e Física da Universidade Federal do Rio Grande.

Trabalho aprovado. Rio Grande - Rio Grande do Sul - Brasil, 10 de agosto de 2013:

Ma. Edite Taufer

Dr. Alessandro de Lima Bicho

Dr. Antonio Paques

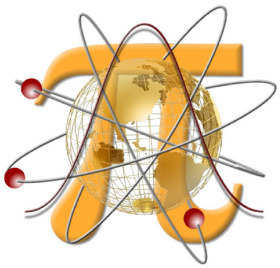
Rio Grande - Rio Grande do Sul - Brasil
agosto, 2013

Este trabalho é dedicado ao professor da escola pública brasileira.

Colaboradores

UNIVERSIDADE FEDERAL DO RIO GRANDE

http://www.furg.br/



INSTITUTO DE MATEMÁTICA FÍSICA E ESTATÍSTICA

http://www.imef.furg.br/

MESTRADO PROFISSIONAL EM REDE NACIONAL

http://www.profmat-sbm.org.br/

SOCIEDADE BRASILEIRA DE MATEMÁTICA

http://www.sbm.org.br/

Agradecimentos

A Deus pela infinidade de bênçãos recebidas em minha vida.

Aos meus pais, Remi (com saudades) e Hilda, ao meu esposo, Ismar, aos meus filhos, Leonardo e Isabela, por todo incentivo, compreeensão e apoio - sem vocês nada teria sentido.

A todos os professores que me acompanharam durante o mestrado, em especial à professora Edite pela orientação neste trabalho.

Aos meus colegas pelo convívio desses dois anos e em especial pela ajuda na superação dos momentos críticos.

Aos idealizadores do PROFMAT pela oportunidade de formação, a nivel de mestrado, concedida aos professores de escolas públicas.

A todos que de forma direta ou indireta, auxiliaram na elaboração deste trabalho.

"O assunto mais importante do mundo pode ser simplificado até ao ponto em que todos possam apreciá-lo e compreendê-lo. Isso é - ou deveria ser - a mais elevada forma de arte."Charles Chaplin

Resumo

Este trabalho propõe um estudo sobre códigos numéricos e detecção de erros de transmissão. Os códigos são de uso rotineiro, sua estrutura é simples e motiva alguns aspectos da teoria de divisibilidade, de uma forma diferenciada. A pesquisa trata da estrutura de alguns códigos e, com cálculos simples, detecta-se a presença de um erro de transmissão. Por fim, fazemos uma proposta pedagógica, a qual almeja fomentar hábitos de pesquisa no aprendiz e, especialmente, colocar a Matemática como uma ciência do seu cotidiano.

Palavras-chave: Aritmética. Álgebra. Dígitos Verificadores.

Abstract

This work proposes the study of numerical codes and the detection of transmission errors. The codes are commonly used, their structure is simple and they motivate the study of some aspects of the theory of divisibility using a different approach. The research focuses on the structures of some of these codes and by performing simple calculations we try to detect the presence of transmission errors. We also propose a pedagogical approach wich aims to teach the student research skills and tries to showcase mathematics as an everyday science.

Keywords: Arithmetics, Algebra, Check Digits

Lista de ilustrações

Sumário

Introdução

A educação tem como princípio a transferência cultural e como resultado a evolução da sociedade. Almejando a eficácia desse processo, estão acontecendo investimentos importantes tanto nos aspectos físicos de algumas escolas, como na formação continuada dos professores e gestores. Um exemplo disso é o PROFMAT, que também visa ações pedagógicas transformadoras.

Na Matemática existem vários estudos interessantes que abordam o uso das tecnologias, da Resolução de Problemas, Modelagem Matemática, Etnomatemática, utilização de jogos, etc. Este trabalho juntar-se-á a vários outros no intuito de contribuir para o ensino-aprendizagem de Matemática no Brasil.

Acreditamos que a contextualização é um recurso didático capaz de auxiliar a aprendizagem significativa e por isso elaboramos esta proposta de trabalho. Entretanto, na ampliação dos PCN's para o Ensino Médio [9], encontramos a advertência:

> É preciso, no entanto, cuidar para que essa generalização não induza à banalização, com o risco de perder o essencial da aprendizagem escolar que é seu caráter sistemático, consciente e deliberado. Em outras palavras: contextualizar os conteúdos escolares não é liberá-los do plano abstrato da transposição didática para aprisioná-los no espontaneísmo e na cotidianidade.

Levando em consideração esta advertência, nos propomos ao estudo dos conceitos matemáticos que embasam os sitemas verificadores de dígitos e também ao estudo formal de tais sistemas, fornecendo ao professor tanto conhecimento aprofundado quanto a visão da possibilidade de levar as ideias básicas de tais conhecimentos aos estudantes.

Desejamos mostrar a Matemática como ciência em construção, focada na atualidade, por isso construímos esse trabalho. Abordaremos o aspecto em que os códigos numéricos asseguram uma transmissão correta de informações.

A comunicação ampliou-se devido à tecnologia. Assim, cada pessoa, cada empresa, cada produto precisa ser identificado de forma única. Essa identificação, em muitos casos, é feita através de sequências numéricas que carregam consigo informações das mais variadas. Para que estas informações sejam comunicadas, ou transmitidas de maneira eficiente, utilizam-se conceitos Sistemas de Verificação de Dígitos.

No Capítulo 1, lembramos subsídios teóricos necessários ao leitor para o estudo sobre *Códigos Numéricos e Detecção de Erros de Transmissão*, utilizando como referências

principalmente as obras [3], [6] e [5].

No Capítulo 2, destacamos a importância dos Dígitos Verificadores na transmissão correta de informações. Utilizamos alguns aspectos da teoria de divisibilidade e mostramos exemplos. Com isso, buscamos chamar atenção para a real possibilidade desse estudo no *Ensino Básico*. Este capítulo é referenciado por [1], [10], [7] e [4].

No Capítulo 3, a partir de exemplos formalizamos os conceitos abordados no Capítulo 2. Destacamos justificativas algébricas dos algoritmos utilizados na detecção de erros e também ressaltamos os tipos de erros mais comuns, tendo como referências [10] e [2].

No Capítulo 4, apresentamos uma proposta de atividade educacional, onde sugerimos uma sequência de ações que podem ser adaptadas a diferentes etapas e anos do Ensino Básico, orientando-nos com os Parâmetros Curriculares Nacionais do Ensino Fundamental e Médio.

1 Conceitos Preliminares

Este capítulo é dedicado a apresentação de alguns conceitos, definições e resultados algébricos que embasam a teoria de códigos verificadores de erros.

1.1 Divisão de Inteiros

Definição 1.1.1. (Divisibilidade nos Inteiros) Sejam a e $b \in \mathbb{Z}$, diz-se que a *é divisor de* b, se e somente se existe $c \in \mathbb{Z}$ tal que $b = a.c$. Utiliza-se a seguite notação $a|b$ e lê-se a divide b.

Se não existe $c \in \mathbb{Z}$ tal que $b = a.c$, temos que $a \nmid b$ e lê-se a não divide b.

Definição 1.1.2. Sejam a e b dois números inteiros, onde $a \neq 0$ ou $b \neq 0$, chama-se *máximo divisor comum (mdc) de* a *e* b o inteiro d $(d > 0)$, que satisfaz as seguintes condições:

i) $d|a$ e $d|b$;

ii) Se d' é um inteiro tal que $d'|a$ e $d'|b$, então $d'|d$, ou seja, todo divisor comum de a e b é também divisor de d.

Usaremos como notação para esta relação $mdc(a, b) = d$.

Teorema 1.1.1. (Agoritmo da Divisão de Euclides) Dados os inteiros positivos a e b, existe um único par de inteiros q e r (denominados respectivamente quociente e resto) tal que $b = q \cdot a + r$, com $0 \leq r < a$.

Definição 1.1.3. Um número $p \in \mathbb{Z}$ é dito *primo* se satisfaz as seguintes condições:

i) $p \neq 0$;

ii) $p \neq 1$ e $p \neq -1$;

iii) Os únicos divisores de p são 1, -1, p e $-p$.

Teorema 1.1.2. (Teorema Fundamenal da Aritmética) Todo número inteiro $a > 1$ é um número primo ou pode ser escrito de maneira única como produto de números primos (desconsiderando a ordem), ou seja, $a = p_1 \cdot p_2 \cdot ... \cdot p_r$, com $p_1, p_2, ..., p_r$ números primos positivos.

Definição 1.1.4. Dados dois inteiros a e b se $mdc(a, b) = 1$, diz-se que a e b são *primos entre si*.

1.2 Congruências

Definição 1.2.1. Sejam a e b números inteiros quaisquer e m inteiro diferente de zero, diz-se que a *é côngruo a* b *módulo* m se $m|(a - b)$, em outros termos, se $a - b = m \cdot q$, para um conveniente inteiro q.

Utilizaremos a notação de Gauss:

$$a \equiv b \ (mod\ m)$$

Simbolicamente:

$$a \equiv b \ (mod\ m) \Leftrightarrow m|(a - b).$$

Ressaltamos que $a \equiv b \ (mod\ m)$ se e somente se $a \equiv b \ (mod\ -m)$, pois se $a - b = m \cdot q$, para um inteiro q conveniente, decorre que $a - b = (-m) \cdot (-q)$. Então nos restringiremos as congruências com módulos inteiros positivos.

Ainda, como $a \equiv b \ (mod\ 1)$ para todo e qualquer a e b pertencentes aos inteiros, então considera-se somente $m > 1$.

Em geral, se $a \equiv b \ (mod\ m)$ e $0 \leq r \leq m - 1$, dizemos que r é o *resíduo de* a.

Chamamos a atenção que o termo *resíduo* se aplica a qualquer número inteiro, positivo ou negativo, mas erroneamente é compreendido como o resto da divisão de um número inteior positivo.

A congruência módulo m é uma relação de equivalência em $\mathbb{Z}$.

Se $x \in \mathbb{Z}$, $\overline{x} = \{a \in \mathbb{Z} : \ a \ \equiv \ x \ (mod\ m)\}$, e $a \in \overline{x} \Leftrightarrow \ a \ \equiv \ x \ (mod\ m)$.

Assim, $\overline{x} = \{x + km : k \in \mathbb{Z}\}$.

Definição 1.2.2. Chamamos de conjunto quociente de $\mathbb{Z}$, pela relação de equivalência $\equiv \ (mod\ m)$, e denotamos por $\mathbb{Z}/_{\equiv (mod\ m)}$, ao conjunto das classes de equivalência relativamente a relação $\equiv \ (mod\ m)$.

Assim,

$$\mathbb{Z}/_{\equiv (mod\ m)} = \{\overline{x} : x \in \mathbb{Z}\} = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}.$$

Que é representado por $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m-1}\}$.

Ainda,

i) $\overline{a} = \overline{b} \Leftrightarrow a \equiv b \ (mod\ m)$;

ii) Se $\overline{a} \cap \overline{b} \neq \varnothing \Rightarrow \overline{a} = \overline{b}$;

iii) $\bigcup_{a \in \mathbb{Z}} \overline{a} = \mathbb{Z}$.

1.3 Grupos

Definição 1.3.1. Seja um conjunto G não vazio onde está definida uma operação $*$ entre os pares de G, denotada por,

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

$$(x, y) \rightsquigarrow x * y.$$

Dizemos que o par $(G, *)$ é um *grupo* se são válidas as seguintes propriedades, respectivamente, *associatividade*, *elemento neutro* e*o inverso em relação a operação* $*$:

i) $(a * b) * c = a * (b * c) \ \ \forall a, b$ e $c \in G$;

ii) $\exists\ e \in G$ tal que $a * e = e * a = a$, $\forall a \in G$;

iii) $\forall a \in G$, $\exists a' \in G$ tal que $a * a' = a' * a = e$.

Se, além disso cumprir a propriedade da *comutatividade*, ou seja, se $a * b = b * a$, para quaisquer a e $b \in G$, o grupo é chamado de *grupo abeliano*.

Definição 1.3.2. Um grupo $(G, *)$ em que o conjunto G é finito é chamado de *grupo finito*. Neste caso o número de elementos de G é chamado *ordem do grupo*, denotado por $o(G)$.

São alguns exemplos de grupos:

Grupos de Permutações:

Permutação é o termo usado na teoria de grupos para designar uma bijeção de um conjunto nele mesmo. Se E indica um conjunto finito não vazio, denotaremos $S(E)$ o conjunto das permutações dos elementos de E.

Um caso particular dos *Grupos de Permutações*, é aquele em que $E = \{1, 2, ..., n\}$, quando $n \geq 1$, chamado então de *Grupo Simétrico de grau* n, denotado por S_n.

Usaremos a notação usual para o estudo de Grupos Simétricos:

Se $\sigma \in S_n$ e $\sigma(1) = i_1$, $\sigma(2) = i_2$, ... , $\sigma(n) = i_n$, com $i_j \in E$, $1 \leq j \leq n$, então:

$$\sigma = \begin{pmatrix} 1 & 2 & ... & n \\ i_1 & i_2 & ... & i_n \end{pmatrix}$$

Grupos de Simetrias (Grupos Dihedrais):

Um tipo de grupo de permutações muito particular são os grupos das simetrias do polígono regular.

Chama-se *simetria* de um polígono regular P qualquer aplicação bijetora $\sigma : P \to P$ que *preserva as distâncias*. *Preservar distâncias* significa que se a e b são pontos quaisquer do polígono, então a distância de $\sigma(a)$ a $\sigma(b)$ é igual a distância de a a b. O número de simetrias de um polígono regular de n lados é o dobro do seu número de lados, ou seja, $2n$.

Em particular, considerando o pentágono regular, as simetrias que se aplicam neste pentágono são as rotações, as reflexões.

Geometricamente, seguem as rotações e as possíveis reflexões do pentágono regular:

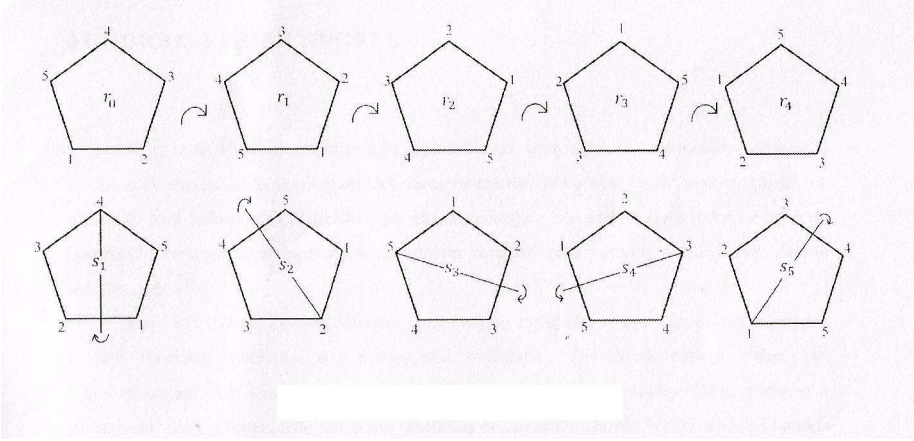


Figura 1 – Simetrias do Pentágono Regular.

Que são descritas por:

$$r_0 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} \qquad r_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}$$

$$r_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \qquad r_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \end{pmatrix}$$

$$r_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} \qquad s_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$$

$$s_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \qquad s_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

$$s_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} \qquad s_5 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$$

A partir do grupo Dihedral de ordem 10, denotado por D_5, construímos uma tabela para a operação composição ($\circ$). Usaremos $0, 1, 2, 3, 4$ para as rotações e $5, 6, 7, 8, 9$ para as reflexões:

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

Tabela 1 – Composição em D_5

A incompreensão deste capítulo não impede que o leitor prossiga, pois no capítulo seguinte, a partir de operações elementares com os Núneros Inteiros, abordamos os Dígitos Verificadores nos Códigos Numéricos.

2 Dígitos Verificadores no Cotidiano

Existe a necessidade de que todo tipo de comunicação seja eficiente. Para que as pessoas se comuniquem, através da tecnologia, de forma satisfatória é importante que cada produto, cada documento seja identificado de forma única. Inicialmente essa identificação era feita com nomes, com o tempo passou-se a usar *Códigos Numéricos*. A partir de então, verificou-se dois principais problemas: as falhas ocorridas nas transmissões dos dados e a segurança destas transmissões.

Quanto à segurança, temos a Criptografia, que estuda métodos para modificar as informações, com o objetivo de torná-las acessíveis apenas ao destinatário real.

Quanto às falhas de transmissão, ocorridas por erros humanos, temos os *Dígitos Verificadores*. Sua estrutura é simples e capaz de detectar a maioria dos erros cometidos.

No que segue, vamos dar exemplos cotidianos onde há o uso de Códigos Numéricos e fazer a análise do Dígito Verificador. Para facilitar o entendimento, usaremos a notação de *vetor* e *produto escalar*:

Definição 2.0.3. Diz-se que x é um *vetor* do $\mathbb{R}^n$ se $x = (x_1, x_2, ..., x_n)$ com $x_i \in \mathbb{R}$ onde $1 \leq i \leq n$.

Definição 2.0.4. Sejam $x = (x_1, x_2, ..., x_n)$ e $y = (y_1, y_2, ..., y_n)$ vetores do $\mathbb{R}^n$. O *produto escalar* entre x e y é definido por:

$$x \cdot y = x_1 \cdot y_1 + x_2 \cdot y_2 + ... + x_n \cdot y_n.$$

2.1 Código de Barras

O código de barras é uma forma de identificar produtos mundialmente utilizada, é representado por uma sequência numérica, que passou por alterações no decorrer do tempo. Atualmente, o Sistema "European Article Numbering"com 13 dígitos (EAN - 13) é o mais utilizado. Mas existem variações, como por exemplo o Universal Product Code (UPC), muito utilizado nos EUA e no Canadá.

O EAN-13: da esquerda para a direita, os três primeiros dígitos identificam o país de origem do produto, os quatro seguintes identificam a empresa fabricante filiada, os

próximos cinco indicam um produto específico e o último é o dígito verificador. Para ilustrar, segue a Figura 2[1]:

Figura 2 – Distribuição dos dígitos do Códigos de Barras.

Agora, definiremos o algoritmo para determinar o Dígito Verificador no sistema EAN-13.

Suponhamos que um determinado produto está identificado, no sistema EAN-13, pela sequência de dígitos $a_1a_2...a_{12}a_{13}$, onde os doze primeiros são determinados através de um método padrão em cada país, por um órgão com tal responsabilidade. Qual é o décimo terceiro dígito? Este é o chamado *Dígito Verificador*, aqui denotado por x e calculado da seguinte forma:

Primeiramente, escrevemos a sequência como um vetor α

$$\alpha = (a_1, a_2, ..., a_{11}, a_{12}, x).$$

O Sistema EAN-13 utiliza o vetor fixo chamado de *vetor peso*

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

Então, calcula-se o produto escalar

$$\alpha \cdot \omega = (a_1, ..., a_{12}, x) \cdot (1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$$
$$= a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + x.$$

Agora, o Dígito Verificador x é escolhido de forma que a soma acima seja um múltiplo de 10, isto é:

$$\alpha \cdot \omega \equiv 0 \ (mod\ 10).$$

[1] Disponível em: <http://www.proteste.org.br/familia/nc/noticia/entenda-o-codigo-de-barras>. Acesso em: 29/05/2013.

A título de exemplo, utilizamos o código da Figura 2 para verificar o algoritmo:

$$\alpha \cdot \omega = (7,8,9,8,3,5,7,4,1,0,0,1,x) \cdot (1,3,1,3,1,3,1,3,1,3,1,3,1)$$

$$= 7 \cdot 1 + 8 \cdot 3 + 9 \cdot 1 + 8 \cdot 3 + 3 \cdot 1 + 5 \cdot 3 + 7 \cdot 1 + 4 \cdot 3 + 1 \cdot 1 + 0 \cdot 3 + 0 \cdot 1 + 1 \cdot 3 + x$$

$$= 105 + x \equiv \ 0 \ (mod\ 10).$$

Então, o Dígito Verificador é 5, confirmando o código da Figura 2.

2.2 ISBN

Outro sistema universalmente adotado é o que se usa na identificação de livros, o "International Standard Book Number"(ISBN). Ele também sofreu alterações com o passar dos anos, de 1969 até o final de 2006 ele era composto por 10 dígitos. Os dois primeiros dígitos identificam um determinado grupo, os quatro seguintes, o editor, os próximos três identificam o título do livro e o último é o dígito de verificação, denotado aqui por y.

Como feito anteriormente, vamos escrever essa sequência através de um vetor α

$$\alpha = (a_1, a_2, ..., a_9, y).$$

O Sistema ISBN utiliza o vetor peso ω

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

E, então calcula-se o produto escalar entre α e ω :

$$\alpha \cdot \omega = (a_1, ..., a_9, y) \cdot (10,9,8,7,6,5,4,3,2,1)$$

$$= 10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + y.$$

O dígito verificador y é escolhido para que a soma anterior seja um múltiplo de 11, ou seja:

$$\alpha \cdot \omega = 0 \ (mod\ 11).$$

Este método possui um inconveniente. É necessário acrescentar mais um símbolo para representar a situação onde $y = 10$. A convenção usual é utilizar o símbolo X (número 10, em romanos).

Como ilustração temos a Figura 3[2]:

[2] Disponível em:<http://www.abebooks.com/books/search-number-code-10-13-digit/ISBN.shtml>. Acesso em: 29/05/2013.

Figura 3 – ISBN.

Aplicando o algoritmo a esse exemplo, temos:

$$\alpha \cdot \omega = (0, 7, 6, 4, 5, 2, 6, 4, 1, y) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$$

$$= 10 \cdot 0 + 9 \cdot 7 + 8 \cdot 6 + 7 \cdot 4 + 6 \cdot 5 + 5 \cdot 2 + 4 \cdot 6 + 3 \cdot 4 + 2 \cdot 1 + y$$

$$= 217 + y \equiv 0 \ (mod\ 11).$$

Logo, $y = 3$ confirmando o código de nosso exemplo.

A partir de janeiro de 2007, o novo ISBN é composto de 13 dígitos, ficando idêntico ao código de barras do sistema EAN-13.

2.3 CPF

O Cadastro de Pessoas Físicas (CPF), do Brasil, da Receita Federal [3] é um banco de dados que armazena informações dos cidadãos que se inscrevem voluntariamente no cadastro. Este cadastro possui 11 dígitos: os 8 primeiros identificam este contribuinte, o nono indica o estado brasileiro onde ele é registrado e os dois últimos são os dígitos verificadores.

Diferente do Registro Geral (RG), o CPF é padrão em todo o Brasil e é único para cada cidadão.

O CPF possui dois dígitos verificadores, calculados separadamente. A seguir temos o algoritmo para determinação destes dois dígitos.

Suponhamos que um determinado cidadão tem por número de CPF a sequência de dígitos $a_1a_2...a_{10}a_{11}$. Os dígitos verificadores aqui serão denotados por x e y, respectivamente.

Vamos escrever esta sequência através de um vetor α

$$\alpha = (a_1, a_2, ..., a_9, x, y).$$

[3] http://www.receita.fazenda.gov.br/pessoafisica/cpf/InscricaoCPF.htm

Calcula-se inicialmente o dígito x, ou seja, considera-se o vetor α_1 com os 10 primeiros dígitos de α. Utilizando o vetor fixo ω_1

$$\omega_1 = (10, 9, 8, 7, 6, 5, 4, 3, 2, 1).$$

Então, calcula-se o produto escalar

$$\alpha_1 \cdot \omega_1 = (a_1, ..., a_9, x).(10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$$
$$= 10a_1 + 9a_2 + 8a_3 + 7a_4 + 6a_5 + 5a_6 + 4a_7 + 3a_8 + 2a_9 + x.$$

Agora, o dígito verificador x é escolhido de forma que a soma acima seja um múltiplo de 11,

$$\alpha_1 \cdot \omega_1 = 0 \ (mod\ 11).$$

Se o dígito verificador for 10, ele será substituído por zero.

Definindo o dígito por x_0, é substituido em α e calculamos y utilizando o vetor fixo ω_2

$$\omega_2 = (11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1).$$

Por fim, calcula-se o produto escalar destes vetores:

$$\alpha \cdot \omega_2 = (a_1, ..., a_9, x_0, y) \cdot (11, 10, 9, 8, 7, 6, 5, 4, 3, 2, 1) =$$

$$= 11a_1 + 10a_2 + 9a_3 + 8a_4 + 7a_5 + 6a_6 + 5a_7 + 4a_8 + 3a_9 + 2x_0 + y.$$

Agora, o segundo dígito verificador y é escolhido de forma que a soma acima também seja um múltiplo de 11, isto é:

$$\alpha \cdot \omega_2 = 0 \ (mod\ 11).$$

Se o dígito verificador for 10, ele será substituído por zero.

Como exemplo, vamos considerar o CPF da Figura 4, destacando a sua sequência numérica e escrevendo-a em forma vetorial.

Calcularemos, conforme o algoritmo, o dígito x. Temos $\alpha_1 = (4, 6, 7, 5, 3, 9, 1, 5, 0, x)$. Assim,

$$\alpha_1 \cdot \omega_1 = (4, 6, 7, 5, 3, 9, 1, 5, 0, x) \cdot (10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$$

Figura 4 – CPF

$$= 10 \cdot 4 + 9 \cdot 6 + 8 \cdot 7 + 7 \cdot 5 + 6 \cdot 3 + 5 \cdot 9 + 4 \cdot 1 + 3 \cdot 5 + 2 \cdot 0 + x$$
$$= 267 + x \equiv 0 \ (mod\ 11).$$

Portanto, $x = 8$, o que confirma o primeiro dígito verificador.

Incluímos tal dígito ao vetor $\alpha = (4, 6, 7, 5, 3, 9, 1, 5, 0, 8, y)$, e calculamos y utilizando o vetor fixo ω_2. Segue o produto escalar,

$$\alpha \cdot \omega_2 = 11 \cdot 4 + 10 \cdot 6 + 9 \cdot 7 + 8 \cdot 5 + 7 \cdot 3 + 6 \cdot 9 + 5 \cdot 1 + 4 \cdot 5 + 3 \cdot 5 + 2x + y$$
$$= 323 + y \equiv 0 \ (mod\ 11).$$

O que nos confirma $y = 7$, como o segundo dígito verificador deste CPF, e garante sua validade.

2.4 Título Eleitoral

O Título de Eleitor é o documento necessário para que o brasileiro vote e participe da vida política do País. É exigido a quitação eleitoral do servidor público na hora da contratação, para tirar ou renovar o Passaporte ou fazer o Cadastro de Pessoa Física (CPF). Como ilustração temos a Figura 5:

O número do título eleitoral é composto por 12 dígitos. Os 8 primeiros são sequenciais e identificam o eleitor, os 2 seguintes são referentes a Unidade da Federação de origem da inscrição e os dois últimos constituem os dígitos verificadores, determinados com base no módulo 11, sendo o primeiro calculado sobre o número sequencial e o segundo sobre o código da Unidade da Federação seguido do primeiro dígito verificador.

Para a verificação da validade do código referente ao Título Eleitoral, procede-se de forma semelhante ao CPF. Vetorialmente, escrevemos a sequência referente a um determinado eleitor, como:

$$\alpha = (a_1, a_2, ..., a_7, a_8, a_9, a_{10}, x, y).$$

Figura 5 – Título de Eleitor

Calcula-se inicialmente o dígito x, considerando α_1 com os 8 primeiros dígitos de α. Utilizando o vetor fixo ω_1

$$\omega_1 = (9, 8, 7, 6, 5, 4, 3, 2, 1).$$

Calcula-se o produto escalar

$$\alpha_1 \cdot \omega_1 = (a_1, ..., a_8, x) \cdot (9, 8, 7, 6, 5, 4, 3, 2, 1)$$
$$= 9a_1 + 8a_2 + 7a_3 + 6a_4 + 5a_5 + 4a_6 + 3a_7 + 2a_8 + x.$$

E determina-se o primeiro dígito verificador de tal forma que:

$$\alpha_1 \cdot \omega_1 = 0 \ (mod\ 11).$$

Determinado o valor x_0 do primeiro dígito verificador, calcula-se o segundo, y, utilizando a sequência (a_9, a_{10}, x_0, y) e o vetor fixo $\omega_2 = (4, 3, 2, 1)$. Assim,

$$(a_9, a_{10}, x_0, y) \cdot \omega_2 = (a_9, a_{10}, x_0, y) \cdot (4, 3, 2, 1)$$
$$= 4a_9 + +3a_{10} + 2x_0 + y$$

Agora, o segundo dígito verificador y é escolhido de forma que a soma acima seja um múltiplo de 11, isto é,

$$(a_9, a_{10}, x, y) \cdot \omega_2 \equiv 0 \ (mod\ 11).$$

Verificaremos a validade de um Titulo Eleitoral cujo número é $666952404 - 42$.

Temos $\alpha = (0, 6, 6, 6, 9, 5, 2, 4, 0, 4, x, y)$.

Calcula-se o produto escalar $\alpha_1 \cdot \omega_1$:

$$\alpha_1 \cdot \omega_1 = (0,6,6,6,9,5,2,4,0,4,x) \cdot (9,8,7,6,5,4,3,2,1)$$

$$= 9 \cdot 0 + 8 \cdot 6 + 7 \cdot 6 + 6 \cdot 6 + 5 \cdot 9 + 4 \cdot 5 + 3 \cdot 2 + 2 \cdot 4 + x$$

$$= 205 + x \equiv 0 \ (mod\ 11).$$

Portanto $x = 4$. Agora calcularemos y,

$$(a_9, a_{10}, x, y) \cdot \omega_2 = (4,3,2,1) = (0,4,4,y) \cdot (4,3,2,1)$$

$$= 0 + 12 + 8 + y = 20 + y \equiv 0 \ (mod\ 11).$$

De onde temos $y = 2$, o que nos garante que a sequência refere-se a um Título Eleitoral válido.

2.5 Cartão de Crédito

O número de um cartão de crédito é formado pos 16 dígitos. Eles estão organizados da seguinte forma: os quatro primeiros dígitos são o número de identificação da entidade que proporciona o cartão, o dígito seguinte indica o tipo de cartão e a identificação da entidade financeira (American Express, VISA, etc), os dez seguintes determinam a quem pertence o cartão e, o dígito final é o dígito de verificação.

Como ilustração, temos a Figura 6:

Figura 6 – Cartão de Crédito

Para determinação do dígito verificador usa-se o Algoritmo de Luhn, criado por Hans Peter Luhn, em 1954.

Consideremos o vetor, referente a sequência numérica do cartão de crédito:

$$\alpha = (a_1, a_2, ..., a_{12}, a_{13}, a_{14}, a_{15}, x).$$

O algoritmo consiste em:

i) Multiplicar por 2 os dígitos que aparecem nas posições ímpares $a_1, a_3, ..., a_{15}$ e tomar o resto da divisão por 9 de cada um destes resultados;

ii) Somar todos estes restos e denotar tal soma por A;

iii) Somar todos os dígitos que aparecem nas posições pares $a_2, a_4, ..., a_{14}, x$, denotar por B;

iv) Finalmente, calcular $A + B \equiv 0 \ (mod\ 10)$.

Ou seja, são aplicadas as seguintes permutações a cada dígito do código numérico:

$$\gamma = (\sigma, I, \sigma, I, ..., \sigma, I),$$

onde I é a permutação identidade e $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}$.

Aplicando ao exemplo da ilustração, temos:

$A = 2+6+1+5+2+6+1+5 = 28$ e $B = 2+4+6+8+2+4+6+x = 32+x$.

Concluindo a utilização do algoritmo,

$$A + B = 28 + 32 + x = 60 + x \equiv 0 \ (mod\ 10).$$

Logo o dígito verificador deveria ser $x = 0$, o que nos garante que o cartão de crédito da Figura 6 é falso.

2.6 Marco Alemão

Outro exemplo interessante, embora não cotidiano, é a numeração utilizada pelo Deusche Bundesbank, órgão emissor de dinheiro da Alemanha, utilizado antes do Euro [4]. As cédulas do Marco Alemão são identificadas com 11 dígitos. Além dos dez algarismos utiliza as letras A, D, G, K, L, N, S, U, V e Z. Para verificar a validade da nota, as letras são trocadas por números, conforme a tabela:

O código usado pelo banco, para a verificação da validade da cédula, utiliza a tabela de operação do grupo D_5, ao invés de utilizar uma permutação e suas potências, utiliza dez permutações diferentes.

Estas dez permutações são dadas na Tabela 3

[4] Mesmo depois de mais de 10 anos de sua substituição, ainda aceito. Disponível em:<http://viagem.uol.com.br/ultnot/deutsche-welle/2012/01/07/marco-alemao-a-forca-de-uma-moeda-morta-viva.jhtm.> Acesso em 02/05/2013.

A	D	G	K	L	N	S	U	V	Z
0	1	2	3	4	5	6	7	8	9

Tabela 2 – Letras e seus respectivos algarismos

	0	1	2	3	4	5	6	7	8	9
σ_1	1	5	7	6	2	8	3	0	9	4
σ_2	5	8	0	3	7	9	6	1	4	2
σ_3	8	9	1	6	0	4	3	5	2	7
σ_4	9	4	5	3	1	2	6	8	7	0
σ_5	4	2	8	6	5	7	3	9	0	1
σ_6	2	7	9	3	8	0	6	4	1	5
σ_7	7	0	4	6	9	1	3	2	5	8
σ_8	0	1	2	3	4	5	6	7	8	9
σ_9	1	5	7	6	2	8	3	0	9	4
σ_{10}	5	8	0	3	7	9	6	1	4	2

Tabela 3 – Permutações

A Figura 7, é uma cédula de Marco Alemão. Vamos verificar a sua validade, referente ao código numérico.

Figura 7 – Cédula de Marco Alemão

O número de série da cédula da Figura 7 é $AA3457494N2$. Utilizando a Tabela 2, o reescrevemos somente com algarismos 00345749452.

Aplicamos ordenadamente as permutações dadas na Tabela 3:

Por σ_1 temos $0 \longrightarrow 1$, $\sigma_2 : 0 \longrightarrow 5$, $\sigma_3 : \ 3 \longrightarrow 6$, $\sigma_4 : \ 4 \longrightarrow 1$, $\sigma_5 : \ 5 \longrightarrow 7$, $\sigma_6 : \ 7 \longrightarrow 4$, $\sigma_7 : \ 4 \longrightarrow 9$, $\sigma_8 : \ 9 \longrightarrow 9$, $\sigma_9 : \ 4 \longrightarrow 2$, $\sigma_{10} : \ 5 \longrightarrow 9$ e a última é fixa, $2 \longrightarrow 2$.

Agora operaremos com os resultados das permutações. Para isso, utilizamos a tabela da operação composição ($\circ$) do Grupo Dihedral 5, na Tabela 1 (página 19):

$$1 \cdot 5 = 6 \cdot 6 = 0 \cdot 1 = 1 \cdot 7 = 8 \cdot 4 = 9 \cdot 9 = 0 \cdot 9 = 9 \cdot 2 = 7 \cdot 9 = 3 \cdot 2 = 0.$$

De onde podemos concluir que a cédula em questão é verdadeira.

Abordando estes exemplos, mostramos algoritmos para determinação do *Dígito verificador* de alguns sistemas de verificação de dígitos. No próximo capítulo, destacamos justificativas algébricas destes algoritmos e também ressaltamos os tipos de erros mais comuns.

3 Sistemas de Verificação de Dígitos

Perguntamos, por que tais algoritmos geram Dígitos de Verificação capazes de detectar erros na transmissão dos dados? Todos os tipos de erros são detectados? Vamos analisar estas questões, observando inicialmente que podemos ter muitos tipos de erros.

Por exemplo, no Sistema EAN-13 antes mencionado, temos 10^{13} possíveis códigos compostos por 13 dígitos e somente 10 possíveis Dígitos Verificadores. Assim, considerando que cada dígito verificador tenha o mesmo número de códigos ligados a ele, existem 10^{12} códigos para cada dígito verificador. São muitas as possibilidades de códigos parecidos e por isso muitas possibilidades de erros não detectados.

A teoria de códigos verificadores não quer somente analisar os possíveis erros, mas sim detectar e, talvez até corrigir, os mais comuns. Por exemplo, o número do CPF conforme definido no capítulo anterior; imaginemos que seja criado um sistema para detectar o erro de permutar os dígitos a_3 e a_8. A construção matemática de tal sistema pode vir a ser interessante, mas a chance de tal erro ser cometido é bastante baixa, conforme Jacobus Koos Verhoeff.

O matemático holandês, nascido em 1927, Jacobus Koos Verhoeff investigou de forma sistemática os tipos de erros cometidos por operadores humanos e apresentou a seguinte tabela com as frequências relativas dos erros mais comuns.

Tipo de erro	Frequência relativa
erro único $...a... \mapsto ...b...$	79%
transposição adjacente $...ab... \mapsto ...ba...$	$10,2\%$
transposição alterna $...abc... \mapsto ...cba...$	$0,8\%$
erro gêmeo $...aa... \mapsto ...bb...$	$0,6\%$
erro gêmeo alternado $...aba... \mapsto ...cbc...$	$0,3\%$
outros	$9,1\%$

Tabela 4 – Tipos de erros e suas frequências segundo Verhoeff

No que segue, abordaremos os casos de maior frequência.

3.1 Erro Único e Erros de Transposição

De acordo com a tabela de Verhoeff, o erro único é o mais comum. Se nos remetermos ao primeiro exemplo visto no Capítulo 2 referente ao EAN-13, percebemos a

presença do vetor de identificação (α) e um vetor peso (ω). Vimos que o último dígito do vetor de identificação é o dígito verificador. Para determiná-lo, procede-se do seguinte modo:

$$\alpha \cdot \omega = 0(mod\ 10).$$

Neste sistema, suponhamos que um determinado produto tenha recebido o código de barras

$$789120000\mathbf{9}183.$$

Quando essa informação foi transmitida, cometeu-se um *Erro Único*. A sequência numérica digitada foi $789120000\mathbf{8}183$.

O computador, ao verificar a leitura, calcula:

$$\alpha \cdot \omega = (7,8,9,1,2,0,0,0,0,8,1,8,3) \cdot (1,3,1,3,1,3,1,3,1,3,1,3,1)$$

$$= 7+24+9+3+2+0+0+0+0+24+1+24+3 = 97.$$

Como o resultado obtido não é múltiplo de 10, o computador emitirá um sinal indicando que aconteceu um erro, possibilitando sua correção. Mas, o erro também seria detectado se não houvesse o vetor peso, pois a soma dos dígitos seria diferente. Contudo, ele é fundamental para a detecção dos erros onde existe uma mudança de ordem de dois dígitos consecutivos, a chamada *Transposição Adjacente*.

No exemplo da Figura 2 do Capítulo anterior, se acontecer uma *Transposição Adjacente* entre os dígitos a_7 e a_8, a verificação acontece da seguinte forma:

$$\alpha \cdot \omega = (7,8,9,8,3,5,\mathbf{4},\mathbf{7},1,0,0,1,5) \cdot (1,3,1,3,1,3,1,3,1,3,1,3,1)$$

$$= 7\cdot 1+8\cdot 3+9\cdot 1+8\cdot 3+3\cdot 1+5\cdot 3+4\cdot 1+7\cdot 3+1\cdot 1+0\cdot 3+0\cdot 1+1\cdot 3+5\cdot 1 = 116$$

Como 116 não é equivalente a zero módulo 10, o erro seria detectado.

Mas, existem transposições onde isso não acontece, nesse mesmo exemplo, se a transposição fosse nos dígitos a_4 e a_5, teríamos:

$$\alpha \cdot \omega = (7,8,9,\mathbf{3},\mathbf{8},5,7,4,1,0,0,1,x).(1,3,1,3,1,3,1,3,1,3,1,3,1)$$

$$= 7\cdot 1+8\cdot 3+9\cdot 1+3\cdot 3+8\cdot 1+5\cdot 3+7\cdot 1+4\cdot 3+1\cdot 1+0\cdot 3+0\cdot 1+1\cdot 3+5\cdot 1$$

$$= 100 \equiv\ 0(mod\ 10).$$

Onde o erro não seria detectado e assim, podemos afirmar que este sistema *não* detecta toda Transposição Adjacente.

Teorema 3.1.1. Uma Transposição Adjacente é detectada pelo EAN-13, se e somente se, $|a_i - a_{i+1}| \neq 5$.

Demonstração:

($\Rightarrow$) Seja $a_1, a_2, ..., a_i, a_{i+1}, ..., a_{12}, a_{13}$, a sequência de dígitos de um determinado produto no sistema EAN-13, que utiliza dígitos de 0 a 9. Pelo algoritmo verificador:

$$a_1 + 3a_2 + ... + 3a_i + a_{i+1} + ... + 3a_{12} + a_{13} \equiv 0 \ (mod\ 10). \quad (1)$$

Suponhamos que essa sequência tenha sido erroneamente digitada, com a seguinte transposição adjacente:

$$a_1, a_2, ..., a_{i+1}, a_i, ..., a_{12}, a_{13}.$$

Faremos o cálculo para verificar o algoritmo de detecção de erro:

$$a_1 + 3a_2 + ... + 3a_{i+1} + a_i + ... + 3a_{12} + a_{13} \equiv 0 \ (mod\ 10). \quad (2)$$

De $(2) - (1)$, temos:

$$2a_i - 2a_{i+1} \equiv 0 \ (\ mod 10) \Leftrightarrow 2(a_i - a_{i+1}) \equiv 0 \ (mod\ 10).$$

Daí,

$$2 \cdot (a_i - a_{i+1}) \equiv 0 \ (mod\ 10) \Leftrightarrow |a_i - a_{i+1}| = 5.$$

Pois, se $a_i - a_{i+1} = 0$ teríamos $a_i = a_{i+1}$, e não teria problema de tal erro de digitação.

($\Leftarrow$) A demonstração é análoga.

Portanto, conclui-se que o erro por transposição adjacente será detectado se, e somente se, $|a_i - a_{i+1}| \neq 5$.

□

Para darmos continuidade a análise dos erros mais comuns, vamos utilizar o que segue.

Definição 3.1.1. Consideremos A como o conjunto de dígitos usados na codificação. Sejam $\alpha = (a_1, a_2, ..., a_n)$, $a_i \in A$, $1 \leq i \leq n$, para um certo inteiro n positivo, o vetor

de identificação, $\omega = (w_1, w_2, ..., w_n)$, com $w_i \in A$, $1 \leq i \leq n$, um vetor peso e $c \in A$ um número inteiro fixado.

Para m, um inteiro positivo fixo (o número de elementos do conjunto A), define-se o número de identificação a_n como o único elemento de A que verifica a equação:

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

Um *Sistema de Verificação de Dígitos* assim definido será denotado por:

$$C = (A, m, n, c, w).$$

Note que $A = \{0, 1, 2, ..., m-1\}$. Nesse caso, tomando as classes residuais módulo m, temos que o dígito verificador a_n é o único elemento de A tal que:

$$\overline{a_n} = \overline{w_n}^{-1}(\overline{c} - \sum_{i=1}^{n-1} \overline{a_i} \cdot \overline{w_i}),$$

quando $w_i \in A$ possuir elemento inverso em A.

Para dar continuidade ao nosso estudo:

Teorema 3.1.2. Suponhamos um sistema $C = (A, m, n, c, w)$, onde $\omega = (w_1, w_2, ..., w_n)$, $w_i \in A$, $1 \leq i \leq n$ e $\alpha = (a_1, a_2, ..., a_n)$, $a_i \in A$, $1 \leq i \leq n$. De modo que

$$\alpha \cdot \omega = a_1 \cdot w_1 + a_2 \cdot w_2 + ... + \alpha_n \cdot w_n \equiv c \ (mod\ m).$$

Então,

i) Todo erro consistente numa única alteração na posição i-ésima será detectado se e somente se $mdc(w_i, m) = 1$;

ii) Todo erro de transposição da forma

$$...a_i....a_j... \mapsto ...a_j....a_i...$$

será detectado se e somente se $mdc(w_i - w_j, m) = 1$.

Demonstração:

Seja $C = (A, m, n, c, w)$ com $\alpha = (a_1, a_2, ..., a_n)$, $a_i \in A$, $1 \leq i \leq n$ a sequência de dígitos do código nas condições do teorema e $\omega = (w_1, w_2, ..., w_n)$, $w_i \in A$, $1 \leq i \leq n$ o vetor peso.

i) ($\Rightarrow$) Suponhamos que a sequência de dígitos tenha sido digitada com o erro único, ou seja, o dígito a_i $(1 \leq i \leq n)$ fora substituído por um b_i e $a_i \neq b_i$. Ao vetor resultante, chamamos de $\beta = (a_1, a_2, ..., b_i, ..., a_n)$.

Segue que, $\alpha \cdot \omega - \beta \cdot \omega = (a_i - b_i)w_i$, e o erro não será detectado se e somente se

$$(a_i - b_i)w_i \equiv 0 \ (mod\ m) \Longleftrightarrow m \mid (a_i - b_i)w_i.$$

Seja $\overline{x}$ a classe residual de um inteiro x em $\mathbb{Z}_m$, pode-se reescrever tal afirmação como:

$$\alpha \cdot \omega - \beta \cdot \omega \equiv 0 \ (mod\ m) \Leftrightarrow (\overline{a_i} - \overline{b_i})\overline{w_i} = \overline{0} \ \ em \quad \mathbb{Z}_m.$$

Se $mdc(w_i, m) = 1$, $\overline{w_i}$ é invertível em $\mathbb{Z}_m$. Como $a_i \neq b_i$ temos $\overline{a_i} \neq \overline{b_i}$, e o erro será detectado.

($\Leftarrow$) Se $mdc(w_i, m) = d \neq 1$, d inteirto positivo. egue que $b_i = a_i + m/d$ ou $b_i = a_i - m/d$ verifica a condição $0 \leq b_i \leq m - 1$ e o erro de substituir a_i por esse b_i não seria detectado.

Então, todo erro que consiste numa única alteração na posição i-ésima será detectado se e somente se $mdc(w_i, m) = 1$.

ii) ($\Rightarrow$) Suponhamos que o erro cometido seja do tipo

$$\alpha = ...a_i....a_j... \quad \longrightarrow \quad \alpha^{'} = ...a_j....a_i....$$

Nesse caso podemos calcular a diferença

$$\alpha \cdot \omega - \alpha^{'} \cdot \omega = (a_i w_i + a_j w_j) - (a_j w_i + a_i w_j) = (a_i - a_j)(w_i - w_j).$$

Assim, este erro não seria detectado se e somente se

$$(a_i - a_j)(w_i - w_j) \equiv 0 \ (mod\ m).$$

Ou seja,

$$(a_i - a_j)(w_i - w_j) \equiv 0 \ (mod\ m) \Longleftrightarrow m \mid (a_i - a_j)(w_i - w_j).$$

Denotando por $\overline{x}$ a classe residual de um inteiro x em $\mathbb{Z}_m$ pode-se reescrever tal afirmação como:

$$\alpha \cdot \omega - \alpha^{'} \cdot \omega \equiv 0 \ (mod\ m) \Leftrightarrow (\overline{a_i} - \overline{a_j})(\overline{w_i} - \overline{w_j}) = \overline{0} \ \ em \quad \mathbb{Z}_m.$$

A demonstração é análoga a de *i)*.

Portanto, todo erro de transposição da forma

$$...a_i....a_j... \longrightarrow ...a_j....a_i....$$

será detectado se e somente se $mdc(w_i - w_j, m) = 1$.

□

A partir desse teorema concluímos que para detectar todos os erros únicos e todos erros de transposição, um sistema de verificação de dígitos deve ter um número primo como número de elementos de A, ou seja, m deve ser primo.

Dando continuidade, observamos que se tomarmos o número m primo e o conjunto A formado por todos os inteiros positivos menores que m, m é primo com cada componente do vetor peso. Isso sugere escolher o vetor peso da seguinte forma:

Definição 3.1.2. Dado um vetor de informação $\alpha = (a_1, a_2, ..., a_{n-1}, a_n)$ podemos escolher n permutações $\sigma_1, \sigma_2, ..., \sigma_n$ do conjunto A. Considerando o vetor peso $\sigma = (\sigma_1, \sigma_2, ..., \sigma_n)$, fixado $c \in A$, o dígito a_n deve verificar a equação:

$$\sigma(\alpha) = \sigma_1(a_1) + ... + \sigma_n(a_n) \equiv c \ (mod\ m).$$

Neste caso o *dígito verificador* pode ser determinado por:

$$a_n = \sigma_n^{-1}(c - \sum_{i=1}^{n-1} \sigma_i(a_i)).$$

Esse tipo de codificação é utilizado nos cartões de crédito (página 27).

De maneira geral:

Se o código numérico que identifica o objeto possuir um número *par* de dígitos é considerada a seguinte permutação:

$$\gamma = (\sigma, I, \sigma, I, ..., \sigma, I).$$

Mas, se o código numérico que identifica o objeto possuir um número *ímpar* de dígitos é considerada a seguinte permutação:

$$\gamma = (I, \sigma, I, ..., \sigma, I).$$

Onde I é a permutação identidade e $\sigma = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}$.

Note que esta codificação permite detectar todo erro único de digitação e toda transposição adjacente exceto nos casos onde a_i e a_j assumem os valores 0 e 9 ou 9 e 0, pois estes dígitos são fixos por σ.

O código que utiliza m primo detecta todo erro único e todo erro de transposição. Será que existe um código com essa capacidade de detecção com módulo par? Como resposta a essa pergunta:

Teorema 3.1.3. Se um sistema numérico de detecção de erros, com módulo par, detecta todo erro único de digitação, então para todo par de índices i, j existe um erro de transposição entre as posições i e j que não é detectado pelo sistema.

Demonstração: Pelo sistema de verificação de dígito $C = (A, m, n, c, w)$ considerado. Tome m par, e vamos trabalhar com os números entre 0 a $2m - 1$, inclusive. Usando a congruência módulo $2m$, e os dígitos como elementos de $\mathbb{Z}_{2m}$.

Suponha que o sistema transforma o vetor $\alpha = (a_1, a_2, ..., a_n)$ em um outro vetor, cuja notação será $\alpha' = (\sigma_1(a_1), \sigma_2(a_2), ..., \sigma_n(a_n))$. Como, por hipótese, o sistema é capaz de detectar todo erro único de digitação, temos que a aplicação na posição $i-ésima$ deve ser uma permutação de $\mathbb{Z}_{2m}$.

Para que o sistema detecte todo erro de transposição entre as posições i e j é necessário que

$$\sigma_i(a) + \sigma_j(b) \neq \sigma_j(a) + \sigma_i(b),$$

para todo par de elementos diferentes $a, b \in \mathbb{Z}_{2m}$, ou seja, esta aplicação $\sigma = \sigma_i - \sigma_j$ é uma permutação em $\mathbb{Z}_{2m}$.

Mas como m varia entre 0 e $2m - 1$, inclusive, temos

$$0 + 1 + 2 + ... + 2m = \frac{(2m-1) \cdot 2m}{2} = 2m \cdot m - m \equiv m \ (mod\ 2m).$$

Ou seja,

$$\overline{0} + \overline{1} + \overline{2} + ... + \overline{2m-1} = \overline{m} em \mathbb{Z}_{2m}.$$

Logo,

$$\overline{m} = \sum_{x \in \mathbb{Z}_{2m}} \overline{x} = \sum_{x \in \mathbb{Z}_{2m}} \overline{\sigma(x)} = \sum_{x \in \mathbb{Z}_{2m}} (\overline{\sigma_i(x)} - \overline{\sigma_j(x)}) = \sum_{x \in \mathbb{Z}_{2m}} \overline{\sigma_i(x)} - \sum_{x \in \mathbb{Z}_{2m}} \overline{\sigma_j(x)} = \overline{m} - \overline{m} = \overline{0}$$

em $\mathbb{Z}_{2m}$ e isto é uma contradição.

Portanto, existe um erro de transposição que não é detectado por este sistema de verificação de dígitos.

□

Assim, o código que considera m com módulo par é falho!

Em nosso estudo vimos vários sistemas para detecção de erros usando dígitos de verificação, e dentre eles o único capaz de detectar todos os erros únicos e todos os erros de transposição é o caso $\mathbb{Z}_{11}$, mas com o inconveniente de precisar o dígito extra.

Em 1969, Verhoeff desenvolveu, em sua tese, um método simples, com os componentes do grupo dihedral D_5 que também detecta todos os erros únicos e todas as transposições adjacentes, sem a necessidade de símbolos extras. A ideia de Verhoeff consiste em escolher o dígito verificador de forma que

$$\sigma(a_1) \cdot \sigma^2(a_2) \cdot ... \cdot \sigma^{n-1}(a_{n-1}) = 0 \ \ em \quad D_5.$$

Note que σ é uma permutação de D_5. Por isso, ela foi escolhida para desenvolver esse sistema pois, por verificação direta:

$$a \cdot \sigma(b) \neq b \cdot \sigma(a)$$

para todo a, $b \in D_5$.

Como σ^i é também uma permutação de D_5, para todo inteiro positivo i temos que o sistema detecta todo erro único.

As transposições adjacentes são detectadas se e somente se

$$\sigma^i(a_i) \cdot \sigma^{i+1}(a_{i+1}) \neq \sigma^i(a_{i+1}) \cdot \sigma^{i+1}(a_i).$$

Mas sabemos que $a \cdot \sigma(b) \neq b \cdot \sigma(a)$ para todo $a,\ b \in D_5$, se aplicarmos a permutação σ^i, obtemos

$$\sigma^i(a) \cdot \sigma^{i+1}(b) \neq \sigma^i(b) \cdot \sigma^{i+1}(a) \ \ a, b \in D_5.$$

Uma variante desse método é o nosso último exemplo, visto no Capítulo 2 (página 28). Embora não seja do nosso cotidiano, é um sistema capaz de detectar todos os erros únicos e todas as transposições (com o incoveniente de não distinguir entre a letra e o número que lhe é atribuído), e por isso, interessante ser mencionado.

Tendo destacado algumas justificativas algébricas dos Sistemas Verificadores de Erros e ressaltado os tipos de erros mais comuns, vamos apresentar uma Proposta Pedagógica que almeja levar estes conhecimentos ao Ensino Básico.

4 Proposta Pedagógica

Os Parâmetros Curriculares Nacionais (PCN's), elaborados pelo Ministério da Educação e do Desporto, nos comunicam uma referência para o trabalho dos professores do Ensino Fundamental e Médio. Tendo-os por base e destacando alguns dos objetivos neles propostos (Anexo A) elaboramos uma sequência de ações pedagógicas buscando levar o tema "Dígitos Verificadores e Detecção de Erros" para a Educação Básica.

Queremos proporcionar, aos estudantes, a oportunidade de vivenciar a sequência de atividades que buscam levá-lo a:

- saber informar-se, comunicar-se, argumentar, compreender informações, aguçar sua criatividade e seu espírito investigativo;
- utilizar os recursos disponíveis para pesquisa;
- analisar e valorizar informações;
- participar socialmente, de forma prática e solidária;
- utilizar algoritmos para determinar dígitos verificadores;
- elaborar conjecturas sobre os possíveis erros;
- perceber a Matemática como ciência voltada a solução de problemas da atualidade.

Essa proposta pedagógica tem como público alvo os estudantes da Educação Básica, podendo ser adaptada as suas diferentes etapas e anos. Mas, de uma forma especial pode ser utilizada no componente curricular Seminário Integrado, fazendo parte da nova modalidade do Ensino Médio da Rede Estadual de Educação do Rio Grande do Sul - o Ensino Politécnico - implantado em 2012, que busca desenvolver projetos diversificados.

Nossa proposta, infere que os alunos saibam operar com números naturais e inteiros, em especial dominem o algoritmo da divisão de inteiros.

Durante o processo, propomos a nomeação de objetos que sejam identificados com códigos numéricos, exemplificando a presença dos dígitos verificadores. Como por exemplo: embalagens de produtos, cartões de crédito, livros, documentos, instigando a criatividade do estudante. Fazemos questão de utilizar recursos tecnológicos pois acreditamos que eles podem ser ferramentas para o ensino, atuando com várias finalidades, [8]:

> • como fonte de informação, poderoso recurso para alimentar o processo de ensino e aprendizagem;
>
> • como auxiliar no processo de construção de conhecimento;
>
> • como ferramenta para realizar determinadas atividades – uso de planilhas eletrônicas, processadores de texto, banco de dados, etc.

Neste sentido, utilizar a internet como uma fonte de pesquisa, e o projetor multimídia que favorece a apresentação, para o grande grupo, dos assuntos estudados.

No que segue vamos detalhar a sequência de ações que compõem nossa proposta pedagógica:

4.1 Descrição Geral

Pretende-se desenvolver este trabalho em uma turma de 35 alunos em 4 etapas, na escola, com duração de aproximadamente 90 minutos.

4.1.1 Primeira etapa:

Esta será dividida em duas partes:

4.1.1.1 Parte 1

Inicia-se a aula com uma conversa informal, abordando o assunto comunicação. Instigando a participação dos estudantes.

Queremos destacar que a comunicação é fundamental nas relações e que existem muitos aspectos que podem ser considerados quando falamos sobre o assunto como, por exemplo, as artes, as tecnologias, as subjetividades da comunicação não verbal, entre outros. Através desse diálogo, levar a turma a se restringir na comunicação escrita, e a considerar a Matemática como uma ciência envolvida neste processo. Ressaltar a importância das sequências numéricas que identificam uma pessoa, um produto, uma situação. Perguntar: utilizando as sequências numéricas, elas podem contribuir para que a transmissão de dados seja feita sem equívocos, quais os possíveis erros cometidos?

Proporcionaremos condições para que o aluno tenha a possibilidade de perceber que, quando nos comunicamos através de palavras, fica relativamente fácil identificar um erro de digitação. Muitas vezes, esta palavra se torna um agrupamento de letras que não comunicam no nosso idioma. Isso não acontece com a comunicação através de números, pois qualquer sequência numérica pode ser vista como uma "palavra" válida. Destacar que a Matemática busca resolver tais problemas através da teoria dos *Dígitos Verificadores*. E, informaremos que estes são dígitos acrescentados à sequência numérica, no intuito de detectar e até corrigir erros.

A seguir pode ser proposto, como exercício, a questão do ANEXO B[1].

Após resolver a questão, comentar sobre situações onde a troca de um dígito pode gerar problemas indesejáveis.

4.1.1.2 Parte 2

Com a ajuda dos aprendizes listar exemplos, onde sequências numéricas são utilizadas na comunicação de informações e, devido a isso precisam ser feitas sem erros. Orientar para que surjam os números de documentos (CPF e Título de Eleitor), de ISBN, dos cartões de crédito e dos códigos de barras (Capítulo 2 deste trabalho).

Como continuidade, dar início a organização em grupos de no máximo 5 estudantes. Após a divisão, cada grupo será responsabilizado da pesquisa sobre um dos assuntos antes listados. Neste momento serão dirigidos ao laboratório de informática onde darão início a pesquisa, buscando as informações iniciais na internet. Tal pesquisa deverá ser concluída em ambiente extra-escola, utilizando, de preferência, outras fontes.

Com as informações obtidas os grupos deverão elaborar uma apresentação de 8 a 12 minutos para socialização das informações com os demais, sendo assuntos do próximo encontro.

4.1.2 Segunda etapa:

Cada grupo fará sua apresentação, no tempo de 8 a 12 minutos.

Após o término das apresentações, solicitar que cada aluno traga no próximo encontro um documento, ou um livro, ou um cartão de crédito, para aplicação dos algoritmos a exemplos reais.

4.1.3 Terceira etapa:

Esta será dividida em 3 partes.

4.1.3.1 Parte 1

A concatenação das informações da segunda etapa, e explanação pela professora sobre a Teoria dos Códigos de Verificação de Dígitos destacando a sua importância para a transmissão de dados eficaz.

4.1.3.2 Parte 2

Aplicação de algoritmos para cálculo dos Dígitos Verificadores e análise de alguns erros comuns.

[1] Disponivel em:<http://www.questoesdeconcursos.com.br/home/public>. Acesso em: 30/05/2013.

4.1.3.3 Parte 3

Propor a leitura de algum material que trate do assunto, a critério do professor (vide referências deste trabalho).

4.1.4 Quarta etapa:

Esta também será desenvolvida em duas partes.

4.1.4.1 Parte 1

Propor a resolução dos exercícios do ENEM e de concurso público que abordem o assunto.(sugestão no ANEXO C [2]).

4.1.4.2 Parte 2

Avaliação das atividades desenvolvidas, a critério do professor ministrante.

[2] Disponíveis em: <http://www.questoesdeconcursos.com.br/home/public> e <http://inep.gov.br/web/enem/edicoes-anteriores/provas-e-gabaritos>. Acesso em:30/05/2013.

5 Conclusão

Esse trabalho reflete nosso intuito, como professores, em buscar a Matemática desenvolvida no Educação Básica como ciência do cotidiano, focada em auxiliar na resolução de diversos problemas.

Ele motivou reflexões amplas sobre o currículo do Ensino Fundamental e Médio, sua necessidade e importância. Mas também fortaleceu a convicção de que se pode e deve trabalhar com "temas novos", que estão ou não diretamente relacionados com os conteúdos programáticos. Pois estes tem a capacidade de entusiasmar estudantes, despertá-los, ampliar seus conhecimentos.

Neste sentido, ao abordar o tema *Dígitos Verificadores e a Detecção de Erros*, reiteramos conceitos matemáticos de forma diferenciada, os aplicamos aos Sistemas Verificadores de Dígitos. E através de alguns exemplos, fixamos a teoria de divisibilidade. Por fim, elaboramos uma sequência de ações pedagógicas com o objetivo de tornar acessível, esses conhecimentos, aos estudantes.

Pretendemos, como continuidade natural para este trabalho o estudo da Criptografia, que trabalha com métodos para codificar informações, com o objetivo de torná-las acessíveis apenas ao destinatário. O que é útil também na questão da transmissão de dados.

Portanto, desejamos que este trabalho possa ser um incentivo aos professores da Educação Básica, seja em relação ao contínuo estudo ou em consequente domínio de assuntos aqui abordados. Frisamos, a ousadia e a coragem andam juntas na busca de ações que possam vir a ser motivadoras e promotoras de uma aprendizagem ativa dos estudantes.

Anexos

ANEXO A – Os Parâmetros Curriculares Nacionais na Proposta Pedagógica

Os Parâmetros Curriculares Nacionais (PCN's), elaborados pelo Ministério da Educação e do Desporto, nos comunicam uma referência para o trabalho dos professores do Ensino Fundamental e Médio. Eles têm por objetivo garantir às crianças e jovens brasileiros os conhecimentos necessários para o exercício da cidadania. Embora não sejam uma diretriz obrigatória, orientam as reflexões dos envolvidos no processo educativo, em especial ao professor norteando as ações do cotidiano escolar. Citamos alguns dos objetivos gerais propostos pelos PCNs para o Ensino Fundamental[8], que almejam levar os alunos a:

- compreender a cidadania como participação social e política, assim como exercício de direitos e deveres políticos, civis e sociais, adotando, no dia a dia, atitudes de solidariedade, cooperação e repúdio às injustiças, respeitando o outro e exigindo para si o mesmo respeito;

- posicionar-se de maneira crítica, responsável e construtiva nas diferentes situações sociais, utilizando o diálogo como forma de mediar conflitos e de tomar decisões coletivas;

- conhecer características fundamentais do Brasil nas dimensões sociais, materiais e culturais como meio para construir progressivamente a noção de identidade nacional e pessoal e o sentimento de pertinência ao país;

- conhecer e valorizar a pluralidade do patrimônio sociocultural brasileiro, bem como aspectos socioculturais de outros povos e nações, posicionando-se contra qualquer discriminação baseada em diferenças culturais, de classe social, de crenças, de sexo, de etnia ou outras características individuais e sociais;

- desenvolver o conhecimento ajustado de si mesmo e o sentimento de confiança em suas capacidades afetiva, física, cognitiva, ética, estética, de inter-relação pessoal e de inserção social, para agir com perseverança na busca de conhecimento e no exercício da cidadania;

- utilizar as diferentes linguagens - verbal, matemática, gráfica, plástica e corporal - como meio para produzir, expressar e comunicar suas ideias, interpretar e usufruir

das produções culturais, em contextos públicos e privados, atendendo a diferentes intenções e situações de comunicação;

- saber utilizar diferentes fontes de informação e recursos tecnológicos para adquirir e construir conhecimentos;
- questionar a realidade formulando problemas e tratando de resolvê-los, utilizando para isso o pensamento lógico, a criatividade, a intuição, a capacidade de análise crítica, selecionando procedimentos e verificando sua adequação.

ANEXO B – EXERCÍCIO

PRIMEIRO ENCONTRO

Exercício B.0.1. (TRT-MS) Nicanor deveria efetuar a divisão de um número inteiro e positivo N, de três algarismos, por 63; entretanto, ao copiar N, ele enganou-se, invertendo as posições dos dígitos extremos e mantendo o seu dígito central. Assim, ao efetuar a divisão do número obtido por 63, obteve quociente 14 e resto 24. Nessas condições, se q e r são, respectivamente, o quociente e o resto da divisão de N por 63, então:

a) q + r = 50.

b) r < 40.

c) q < 9.

d) r é múltiplo de 4.

e) q é um quadrado perfeito.

Resolução: Seja $N^{'}$ o número inteiro escrito por engano, então:

$$N^{'} = 63 \cdot 14 + 24$$

$$N^{'} = 906$$

Portanto, N é obtido invertendo os dígitos extremos e mantendo o central, logo:

$$N = 609 = 63 \cdot 9 + 42$$

Então $q = 9$ e $r = 42$.

A alternativa "e" é a correta.

ANEXO C – EXERCÍCIOS

QUARTO ENCONTRO

Exercício C.0.2. ENEM(2005) Os números de identificação utilizados no cotidiano (de contas bancárias, de CPF, de Carteira de Identidade, etc) usualmente possuem um dígito de verificação, normalmente representado após o hífen, como em $17326 - 9$. Esse dígito adicional tem a finalidade de evitar erros no preenchimento ou digitação de documentos. Um dos métodos usados para gerar esse dígito utiliza os seguintes passos:

- multiplica-se o último algarismo por 1, o penúltimo por 2, o antepenúltimo por 1 e assim por diante, sempre alternando multiplicações por 1 e por 2;
- soma-se 1 a cada um dos resultados dessas multiplicações que for maior do que ou igual a 10;
- somam-se os resultados obtidos;
- calcula-se o resto da divisão dessa soma por 10, obtendo-se assim o dígito verificador.

O dígito de verificação fornecido pelo processo acima para o número 24685 é:

a) 1

b) 2

c) 4

d) 6

e) 8

Exercício C.0.3. ENEM (2009) Para cada indivíduo, a sua inscrição no Cadastro de Pessoas Físicas (CPF) é composto por um número de 9 algarismos e outro número de 2 algarismos, na forma d_1d_2, em que os dígitos d_1 e d_2 são denominados dígitos verificadores. Os dígitos verificadores são calculados, a partir da esquerda, da seguinte maneira: os 9 primeiros algarismos são multiplicados pela sequência $10, 9, 8, 7, 6, 5, 4, 3, 2$ (o primeiro por 10, o segundo por 9, e assim sucessivamente); em seguida, calcula-se o resto r da divisão da soma dos resultados das multiplicações por 11, e se esse resto r for 0 ou 1, d_1 é zero,

caso contrário $d_1 = (11 - r)$. O dígito d_2 é calculado pela mesma regra, na qual os números a serem multiplicados pela sequência dada são contados a partir do segundo algarismo, sendo d_1 o último algarismo, isto é, d_2 é zero se o resto s da divisão por 11 das somas das multiplicações for 0 ou 1, caso contrário, $d_2 = (11 - s)$.

Suponha que João tenha perdido seus documentos, inclusive o cartão de CPF e, ao dar queixa da perda na delegacia, não conseguisse lembrar quais eram os dígitos verificadores, recordando-se apenas que os nove primeiros algarismos eram 123.456.789. Neste caso, os dígitos verificadores d_1 e d_2 esquecidos são, respectivamente,

a) 0 e 9

b) 1 e 4

c) 1 e 7

d) 9 e 1

e) 0 e 1

Exercício C.0.4. CESPE(2010) Uma rede bancária, denominada Banco X, é formada por inúmeras agências. As contas-correntes de seus clientes são identificadas pelos números da agência e conta. O número da agência é composto de quatro dígitos, que são algarismos escolhidos entre 0 e 9, seguidos por um dígito verificador; o número da conta é composto de seis dígitos, também escolhidos entre os algarismos de 0 a 9, mais um dígito verificador. Em ambos os casos, o dígito verificador é computado a partir dos demais dígitos. Contas-correntes em agências distintas, mesmo com igual número de conta, são contas-correntes diferentes.

O dígito verificador do número da agência é determinado da seguinte forma: multiplica-se cada um dos dígitos desse número, da esquerda para a direita, por 5, 4, 3 e 2, respectivamente; somam-se esses produtos; divide-se essa soma por 11 e separa-se o resto r dessa divisão. O dígito verificador é obtido subtraindo-se de 11 esse resto, da seguinte forma: se esse valor for maior que 10, considera-se Y como sendo o dígito verificador; se for 10, o dígito verificador será igual a 0; em qualquer outro caso, o dígito verificador será igual a $11 - r$. Por exemplo, $1234 - 3$ poderia ser o número de uma agência do Banco X.

Com base no texto acima, julgue o item seguinte: Se $4321 - t$ é o número de uma agência do Banco X, em que t é o dígito identificador, então t = 4.

( )CERTO ( )ERRADO

Resoluções:

Exercício C.0.2: Utilizando os passos do enunciado da questão para gerar o dígito verificador:

$$5 \cdot 1 = 5$$

$$8 \cdot 2 = 16$$

$$6 \cdot 1 = 6$$

$$4 \cdot 2 = 8$$

A seguir, temos:

$$5 + 17 + 6 + 8 + 2 = 38 = 3 \cdot 10 + 8.$$

Portanto o dígito verificador é 8 e alternativa correta é a "e".

Exercício C.0.3: Calculando o primeiro dígito verificador:

$$1 \cdot 10 + 2 \cdot 9 + 3 \cdot 8 + 4 \cdot 7 + 5 \cdot 6 + 6 \cdot 5 + 7 \cdot 4 + 8 \cdot 3 + 9 \cdot 2$$

$$= 10 + 18 + 24 + 28 + 30 + 30 + 28 + 24 + 18$$

$$= 28 + 52 + 60 + 52 + 18 = 80 + 112 + 18 = 210.$$

Como $210 = 11 \cdot 19 + 1$, temos $d_1 = 0$.

Cálculando o segundo dígito veridicador:

$$2 \cdot 10 + 3 \cdot 9 + 4 \cdot 8 + 5 \cdot 7 + 6 \cdot 6 + 7 \cdot 5 + 8 \cdot 4 + 9 \cdot 3 + 0 \cdot 2$$

$$= 20 + 27 + 32 + 35 + 36 + 35 + 32 + 27$$

$$= 47 + 67 + 71 + 59 = 114 + 130 = 244.$$

Como

$$244 = 11 \cdot 22 + 2$$

temos

$$d_2 = 11 - 2 = 9.$$

A alternativa "a" é a correta.

Exercício C.0.4: Utilizando os passos do enunciado da questão para gerar o dígito verificador:

$$5 \cdot 4 = 20$$

$$4 \cdot 3 = 12$$

$$3 \cdot 2 = 6$$

$$2 \cdot 1 = 2$$

A seguir, temos:

$$20 + 12 + 6 + 2 = 40 = 3 \cdot 11 + 7.$$

Portanto o digito verificador é $d = 11 - 7 = 4$ e o item está "correto".

Referências

[1] Waldemar de Maio, *Estruturas algébricas e matemática discreta*, LTC, São Paulo, SP, Brasil, 2009. Citado na página 14.

[2] Carlos Correia de Sá e Jorge Rocha, *Treze viagens pelo mundo da matemática*, U.Portoeditorial, São Paulo, SP, Brasil, 2012. Citado na página 14.

[3] Hygino Domingues e Gelson Iezzi, *Álgebra moderna*, Atual Editora, São paulo, SP, Brasil, 2003. Citado na página 14.

[4] Daniel Argenta e Rafael Amorim, *Estudo e implementação de dígitos verificadores*, Disponível em: <http://magnum.ime.uerj.br>, Acesso em: 12 de maio de 2013. Citado na página 14.

[5] Arnaldo Garcia e Yves Lequain, *Elementos de Álgebra*, IMPA, Rio de Janeiro , RJ, Brasil, 2002. Citado na página 14.

[6] Adilson Gonçalves, *Introdução a Álgebra*, IMPA, CNpq, Rio de Janeiro, RJ , Brasil, 2005. Citado na página 14.

[7] JURISPRO, *Que significam os números do nosso cartão de crédito?*, Disponível em: <http://jurispro.net>, Acesso em: 20 de maio de 2013. Citado na página 14.

[8] MEC, *Parâmetros curriculares nacionais - terceiro e quarto ciclos*, 1998. Citado 2 vezes nas páginas 40 e 46.

[9] MEC, *Parâmetros curriculares nacionais - ensino médio*, 1999. Citado na página 13.

[10] Francisco Cesar Polcino Milies, *A matemática dos códigos de barras*, Mini-curso apresentado na Bienal da Sociedade Brasileira de Matemática. UFG (2006). Citado na página 14.