Eduardo Gomes da Silva

Explorando vertentes matemáticas nos códigos de barras

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Instituto de Biociência, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto.

Orientador: Prof. Dr. Jéfferson Luiz Rocha Bastos

São José do Rio Preto

2013

Eduardo Gomes da Silva

Explorando vertentes matemáticas nos códigos de barras

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Instituto de Biociência, Letras e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Campus de São José do Rio Preto.

Banca Examinadora

Prof. Dr. Jéfferson Luiz Rocha Bastos
UNESP - São José do Rio Preto/SP
Orientador

Prof. Dr. Clotilzio Moreira dos Santos
UNESP - São José do Rio Preto/SP

Prof^a. Dr^a. Ires Dias
USP - São Carlos/SP

São José do Rio Preto
2013

Agradecimentos

Agradeço primeiramente a Deus por me iluminar e guiar em todos os momentos e proporcionar diversas oportunidades ao longo da minha vida.

Agradeço a todos os colegas e professores do PROFMAT que me apoiaram nos momentos mais difíceis, dividiram momentos de incertezas e colaboraram de forma mútua para a superação de vários obstáculos. Ao Professor Dr. Jéfferson Luiz Rocha Bastos que me orientou neste trabalho.

Agradeço também a todos colegas de profissão e diversos colaboradores, em especial a todos o professores e funcionários da Escola Estadual Expedicionário Diogo Garcia Martins da cidade de Alto Alegre-SP.

Agradeço meus pais, meus irmãos e toda minha família que sempre acreditaram em meu potencial e contribuiram com muito incentivo, reconhecimento, colaboração, entre outros fatores.

Agradeço em especial a Silvilene, que nesse período de PROFMAT foi namorada, noiva e agora esposa que deu suporte, compreendeu e compartilhou os bons e maus momentos, em nenhuma ocasião deixou de acreditar, hoje tenho a certeza de que está tão feliz quanto eu.

À CAPES, pelo apoio financeiro.

Resumo

O código de barras é uma das tecnologias de identificação automática mais usada em todo o mundo e a sua presença pode ser encontrada nas mais diversas áreas. Quem de nós nunca observou nos supermercados os produtos passando facilmente pelas máquinas registradoras? Apesar de presentes na vida cotidiana, a estrutura e compreensão dos códigos de barras são pouco exploradas nas instituições de ensino básico em nosso país, mas podem se tornar uma fonte de motivação do estudo de alguns temas matemáticos e apresentar questões instigantes que muitas vezes passam despercebidas. A compreensão dos códigos de barras pode possibilitar a extração e interpretação de informações, promovendo uma leitura diferenciada, pois os números transpõem a barreira dos idiomas, sendo utilizado em todo o mundo. O estudo pode ser estendido a outros códigos identificadores como números de contas bancárias, cartões de crédito, RG, CPF dentre muitos outros presentes em nosso dia a dia. É de fundamental importância frisar os objetivos de utilização e toda estrutura matemática dos códigos identificadores em geral com a finalidade de viabilizar registros, facilitar situações que envolva os diversos produtos, fabricantes, países de origem e detectar possíveis erros nos processamentos de dados. A tradução de números para barras de espessura variável, a facilidade de executar registros, assim como a leitura realizada por meios tecnológicos e humanos também serão abordados. Vamos estudar a história dos códigos de barras seu funcionamento básico, análise de eventuais erros e apresentar códigos mais sofisticados, a fim de despertar a curiosidade de nossos alunos. Será desenvolvida uma atividade que utiliza a aritmética das classes residuais que é um tema presente na Matemática nos códigos de barras.

Palavras-chave: Código de Barras. Detecção de Erros. Classes Residuais.

Abstract

The Bar Code is one of the most used technologies of automatic identification in the whole world and its presence can be found on most diverse areas. Who of us never look at the supermarkets on the products easily going through the register? Even though of being present in our lives, the structures and comprehension of bar codes are underexplored in our basic teaching institutions, but could become one important source of motivation in some mathematics studies and show tempting questions that very often go unnoticed. The comprehension of the bar codes could make possible the expression and interpretation of information, promoting a different view, because the numbers transpose the language barriers. The study could be extended to other identification codes as account numbers, credit cards, IDs, CPF among others presents in our daily life. Is fundamental importance to emphasize the utilization objectives and the whole mathematical structures of the identification codes in general with the purpose of making possible records, making easy situations that involve diverse products, manufacturers, country of origin and, mainly to detect possible errors in data processing. The translation from numbers to bars of variable thickness, the easy to run records, thus the reading through technological means and humans also will be addressed. We're going to study the story of bar codes, its basic operations, analysis of possible errors and show more sophisticated codes, in order to arouse the curiosity of the students. Will be developed an activity that uses the arithmetic mean of residual groups that is one of the subjects in mathematics of bar codes.

Keywords: *Bar codes. Error detection. Residual classes.*

Sumário

Capítulo 1

Um pouco da história dos códigos de barras

A primeira patente de um código de barras ocorreu em 1952, sendo atribuída a Joseph Woodland e Bernard Silver, que consistia numa classificação identificada através de padrões envolvendo circunferências concêntricas.

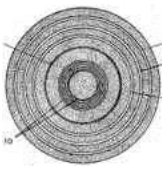

Figura 1.1: Primeiro código patenteado

Mas para esse acontecimento se concretizar, houve uma grande evolução ao longo dos anos envolvendo cálculo com utilização de máquinas, que vem desde o século XVII, com contribuições de matemáticos notáveis como Blaise Pascal, Wilhelm Leibniz, B. Bouchon, Joseph-Marie Jacquard, Sir Charles Wheatstone, Charles P. Babbage, Hermann Hollerith entre outros. Todos esses estudos trouxeram como contribuição, após muitas evoluções, aparelhos utilizados atualmente, como calculadoras, computadores, scanners entre outros que hoje fazem parte da vida moderna. Com todas essas tecnologias e a necessidade de facilitação no armazenamento de dados em diversas áreas surgem os códigos de barras. Na década de 1970 foi definido um formato numérico para identificar produtos e empresas

de assessoria como a Uniform Grocery Product Code Council, solicitaram a diversas companhias que elaborassem um código adequado, onde a IBM apresentou a proposta vencedora. O criador do código foi George J. Laurer. O código passou a ser conhecido como Universal Product Code (UPC) que foi aceito formalmente em 1973 e adotado nos Estados Unidos e Canadá.

Figura 1.2: Código UPC

O código UPC consiste em uma sequência de 12 dígitos expressos de forma binária e traduzidos para a forma de barras. Mais tarde Laurer solicitou uma ampliação do código UPC para permitir uma maior difusão do sistema e abranger também a identificação do país de origem de cada produto, surgindo assim um novo código de 13 dígitos, adotado em 1976 com o nome Europen Article Numbering system (EAN), sendo utilizado em outros países com outras nomenclaturas como, por exemplo, no Japão Japanese Article Numbering system (JAN).

Figura 1.3: Código EAN

A criação desses códigos facilitou o armazenamento de informações, o controle de estoques de mercadorias, as transações bancárias, entre outras atividades rotineiras atuais. O equipamento necessário e responsável em ler os dados de alguns códigos de barras é o scanner que consiste em um módulo ótico, um decodificador e um cabo que faz a

interligação entre o decodificador e o computador. A função do módulo ótico é realizar a leitura do símbolo do código de barras fornecendo uma saída elétrica ao computador que corresponde às barras e espaços inseridos no código. O decodificador reconhece a simbologia faz uma análise do conteúdo e transmite estes dados ao computador com um formato numérico tradicional.

Figura 1.4: Scanner

Capítulo 2

Os códigos de barras

Neste capítulo daremos ênfase ao estudo da estrutura e do funcionamento dos Códigos de Barras e de outros códigos numéricos identificadores. Basearemos nossos estudos principalmente no artigo *A Matemática dos Códigos de Barras* de POLCINO MILIES [9].

2.1 Estrutura do código UPC

O código de barras atuais são formados por listras brancas e pretas de espessura variável, distribuídas alternadamente. Essas listras ou barras são classificadas de quatro maneiras: finas, médias, grossas e muito grossas.

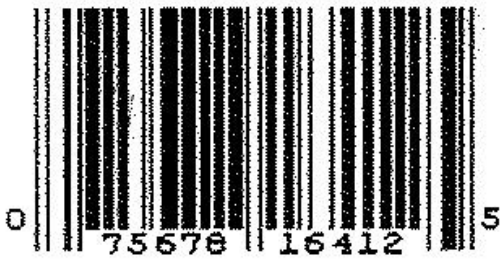

Figura 2.1: Código UPC

Traduzindo o formato das possíveis barra para um formato binário, temos que o símbolo "zero"representa as barras brancas e o símbolo "um", as barras pretas. Assim, 0 representa uma barra branca fina, 00 uma barra branca média, 000 uma barra branca

grossa e 0000 uma barra branca muito grossa. De maneira análoga procede as possíveis sequências envolvendo o símbolo 1, formando os quatro tipos de barras pretas. Além disso, as barras mais compridas verticalmente apresentadas nas extremidades e no centro da figura são consideradas as barras limites e não fazem parte da codificação. Já sabemos que o código UPC é formado por uma sequência de 12 números. Cada um desses números são formados por uma sequência de sete símbolos iguais a 0 ou 1, determinando assim uma combinação dos diversos tipos de barras já apresentadas. Por exemplo, o símbolo 7 da figura é a sequência 0111011, que é traduzido em uma barra branca fina, uma barra preta grossa, outra barra branca fina e uma barra preta média. Em qualquer situação um dígito é formado por quatro barras alternadas de acordo com a cor e de espessura variável. Outro fato curioso é que o operador dos caixas de supermercados, por exemplo, não escolhem um lado específico do código para registrar o produto. Ora passa o código de barras na sequência da esquerda para direita, ora da direita para esquerda e, o scanner distingue o produto da mesma maneira. Entenda como isso é possível. As barras mais compridas do centro da figura dividem o código de barras em duas partes. Vamos distingui-los como lado esquerdo e lado direito do código. Os dígitos são codificados diferentemente em cada lado e isto é feito conforme a *Tabela* 2.1, onde a codificação de um determinado número do lado direito é obtido da sua codificação do lado esquerdo, trocando cada 0 por 1 e cada 1 por 0.

Dessa forma, as codificações do lado esquerdo apresentam uma quantidade ímpar de símbolos 1 e as codificações do lado direito apresentam uma quantidade par de símbolos 1. Através da verificação da paridade, o scanner identifica imediatamente o sentido em que a leitura do código de barras está sendo realizada, consequentemente identifica o produto de ambas as maneiras.

2.2 Estrutura do código EAN

Como já vimos o código EAN possui um dígito a mais que o código UPC. Esse dígito tem a finalidade de identificar o país de origem do produto. A estrutura do código EAN é semelhante do código UPC. A diferença está na quantidade de dígitos, que são 13.

Dígito	do lado esquerdo	do lado direito
0	0001101	1110010
1	0011001	1100110
2	0010011	1101100
3	0111101	1000010
4	0100011	1011100
5	0110001	1001110
6	0101111	1010000
7	0111011	1000100
8	0110111	1001000
9	0001011	1110100

Tabela 2.1: Codificação UPC.

Mas como utilizar esse novo código sem alterar todo o sistema das máquinas leitoras já existentes? Não seria viável a existência de máquinas distintas para ambos os códigos nem mesmo a substituição das máquinas existentes, pois a intenção era a utilização simultânea dos códigos UPC e EAN. Assim os EUA e o Canadá, que utilizam os códigos UPC, adotaram um zero antes da codificação utilizada anteriormente.

Figura 2.2

A figura mostra o mesmo código expresso nas duas formas. É fácil verificar que os

códigos representados pelas barras são idênticos e a sequência numérica apresentada ao leitor humano no código EAN-13 é apenas precedida do dígito zero em relação à sequência do código UPC-A. A partir daí, os demais países passaram a ser identificados pelos dois ou três primeiros dígitos dos códigos de barras. Os produtos produzidos no Brasil, por exemplo, têm os códigos iniciados com a sequência 789. Uma tabela completa, com os números de identificação de cada país, pode ser encontrada na página da internet *http://www.barcodeisland.com/ean13.phtml*[2].

O objetivo era manter o padrão de tamanho dos códigos de barras e não ter que modificar o sistema dos scanners já existentes. A ideia adotada foi de que o número a ser acrescentado estivesse implícito na forma de codificação utilizada anteriormente. Como o dígito acrescentado situa-se no início da sequência, não foi preciso alterar a estrutura de funcionamento do lado direito dos códigos, o que ainda permite que as leitoras identifiquem o lado correspondente do mesmo. Só que a codificação do lado esquerdo passou a ter uma variação, que depende exclusivamente do dígito inicial. A sequência que representa um dígito do lado esquerdo pode apresentar uma quantidade par ou ímpar de símbolos 1, obedecendo a *Tabela* 2.2.

Dígito	do lado esquerdo ímpar	do lado esquerdo par	do lado direito
0	0001101	0100111	1110010
1	0011001	011001	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Tabela 2.2: Codificação EAN.

Portanto, a alternância dos dígitos do lado esquerdo do código se diferencia na quantidade par ou ímpar de dígitos 1, sempre levando em consideração o dígito inicial de cada código de barras e obedecendo a *Tabela* 2.3.

Dígito inicial	1^o	2^o	3^o	4^o	5^o	6^o
0	ímpar	ímpar	ímpar	ímpar	ímpar	ímpar
1	ímpar	ímpar	par	ímpar	par	par
2	ímpar	ímpar	par	par	ímpar	par
3	ímpar	ímpar	par	par	par	ímpar
4	ímpar	par	ímpar	ímpar	par	par
5	ímpar	par	par	ímpar	ímpar	par
6	ímpar	par	par	par	ímpar	ímpar
7	ímpar	par	ímpar	par	ímpar	par
8	ímpar	par	ímpar	par	par	ímpar
9	ímpar	par	par	ímpar	par	ímpar

Tabela 2.3: Alternância em função do dígito inicial

Observando a situação em que o dígito inicial é zero, verificamos que os seis dígitos restante apresentarão uma quantidade ímpar de símbolos 1, o que volta a estrutura dos códigos UPC, já apresentados, resolvendo assim o problema gerado pela inclusão de um novo dígito e promovendo a continuidade da utilização das máquinas leitoras já existentes. Para entender melhor o EAN-13, analisemos o exemplo, correspondente a um produto fabricado no Brasil. Veja a figura:

Figura 2.3: Código EAN-13

O dígito inicial é o 7. Assim a sequência dos seis dígitos seguintes, segundo a tabela será: ímpar, par, ímpar, par, ímpar e par. Os demais dígitos apresentados no lado esquerdo são 8, 9, 5, 0, 0 e 0. De acordo com a tabela de codificação de EAN-13, o código de barras da figura é obtido através da seguinte situação:

- $8 \mapsto 0110111$(ímpar);
- $9 \mapsto 0010111$ (par);
- $5 \mapsto 0110001$(ímpar);
- $0 \mapsto 0100111$ (par);
- $0 \mapsto 0001101$ (ímpar);
- $0 \mapsto 0100111$ (par).

Não nos preocupamos com a paridade dos seis dígitos apresentado no lado direito do código, pois são apresentados na tabela e todos apresentam uma quantidade par de dígitos 1. Geralmente os dois ou três dígitos iniciais de um código de barras identificam o país de origem do produto. O restante apresentado no lado esquerdo do código (quatro ou cinco dígitos) serve para identificar o fabricante. Os cinco primeiros dígitos do lado direito identificam o produto específico e o último dígito é o dígito verificador obtido segundo critérios matemáticos que veremos nas próximas seções. Analisado o código citado anteriormente, temos:

País de origem	**Fabricante**	**Produto**	**Dígito de Verificação**
789	5000	26624	1

Tabela 2.4: Análise do código de barras

2.3 Aritmética das Classes Residuais

Nesta seção nossos estudos estão baseados principalmente nas definições encontradas nos livros *Elementos de Aritmética* de Hefez, Abramo[7] e *Números: Uma Introdução*

à Matemática, de Francisco César P. Milies e Sonia Pitta Coelho[8].

Veremos como, a partir da divisão euclidiana, Gauss desenvolveu uma aritmética dos restos da divisão dos números naturais por um número fixado m e aplicá-la no desenvolvimento da teoria dos números, o que é muito utilizado na matemática dos códigos de barras, principalmente na detecção de possíveis erros. Não convém considerar o número fixado $m = 1$, pois o resto da divisão de qualquer inteiro por 1 é sempre nulo.

Definição 2.3.1. *Seja $m \neq 0$ um inteiro fixo. Dois inteiros a e b dizem-se congruentes módulos m se m divide a diferença $a - b$ e escrevemos $a \equiv b \ (mod\ m)$.*

Assim, $a \equiv b \ (mod\ m)$ se, e somente se, $m \mid (a - b)$, ou seja, se existir um inteiro q tal que $a = b + mq$.

Proposição 2.3.2. *Dados dois inteiros a e b, temos $a \equiv b \ (mod\ m)$ se, e somente se, a e b possuem o mesmo resto quando divididos por m.*

Demonstração

Sejam

$$a = mq_1 + r_1, \ com\ 0 \leq r_1 < m,$$

$$b = mq_2 + r_2, \ com\ 0 \leq r_2 < m.$$

Então,

$$a - b = m(q_1 - q_2) + (r_1 - r_2),$$

logo,

$$m \mid (a - b) \ se\ e\ somente\ se\ m \mid (r_1 - r_2).$$

Mas como $0 \leq \mid r_1 - r_2 \mid < m$, temos que $m \mid (r_1 - r_2)$ se e somente se $r_1 - r_2 = 0$.

Consequentemente, $a \equiv b \ (mod\ m)$ se e somente se $r_1 = r_2$. ∎

Verificaremos agora as propriedades da congruência.

Proposição 2.3.3. *Sejam $m > 0$ um inteiro fixo, e a, b, c, d inteiros arbitrários. Então, valem as seguintes propriedades:*

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

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

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

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

(v) *Se* $a \equiv b \ (mod\ m)$, *então* $a + c \equiv b + c \ (mod\ m)$.

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

(vii) *Se* $a \equiv b \ (mod\ m)$, *então* $a^n \equiv b^n \ (mod\ m)$, *para todo inteiro positivo* n.

(viii) *Se* $a + c \equiv b + c \ (mod\ m)$, *então* $a \equiv b \ (mod\ m)$.

Demonstração

As propriedades (i) e (ii) são imediatas.

Para provar (iii), observamos que, se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, temos que $m \mid (a - c)$ e $m \mid (b - c)$. Consequentemente, $m \mid (a - b) + (b - c)$, isto é, $m \mid (a - c)$, logo $a \equiv c \ (mod\ m)$.

A demonstração de (iv) é análoga à anterior e (v) segue de (iv), observando por (i) que $c \equiv c \ (mod\ m)$.

Para provar (vi), temos que, se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, existem inteiros q_1 e q_2 tais que $a = b + q_1 m$ e $c = d + q_2 m$. Logo $ac = bd + (bq_2 + dq_1 + q_1 q_2 m)m$, isto é, $m \mid (ac - bd)$. Portanto $ac \equiv bd \ (mod\ m)$.

A demonstração de (vii) segue de (vi), tomando-se $a = c$, $b = d$ e usando indução em n.

Para demonstrar $(viii)$, observemos que, se $a + c \equiv b + c \ (mod\ m)$, temos que $m \mid (a + c) - (b + c)$, logo $m \mid (a - b)$, isto é, $a \equiv b \ (mod\ m)$. ∎

Proposição 2.3.4. *Seja* m *um inteiro fixo e sejam* a, b *e* c *inteiros arbitrários. Se* $mdc(c, m) = 1$, *então* $ac \equiv bc \ (mod\ m)$ *implica* $a \equiv b \ (mod\ m)$.

Demonstração

Se $ac \equiv bc \ (mod\ m)$, temos que $m \mid (a - b)c$. Como $mdc(c, m) = 1$, por hipótese, vem do teorema de Euclides que $m \mid (a - b)$. Logo $a \equiv b \ (mod\ m)$. ∎

Verificamos que, se $mdc(c, m) = d \neq 1$, existem inteiros a e b tais que a e b não são congruentes módulo m, mas $ac \equiv bc \ (mod\ m)$.

Exemplo 2.3.1. *Sejam os inteiros a e b, respectivamente 2 e 3, que não são congruentes módulo 7. Considerando $c = 14$ temos que $mdc(14, 7) = 7 \neq 1$. Então:*

$$2.14 \equiv 3.14 \ (mod\ 7)$$

$$28 \equiv 42 \equiv 0 \ (mod\ 7).$$

A partir das congruências, veremos as classes residuais dos *Inteiros módulo m.*

Definição 2.3.5. *O conjunto $[a] = \{x \in \mathbb{Z};\ x \equiv a \ (mod\ m)\}$ é chamado de classe residual módulo m do elemento $a \in \mathbb{Z}$. Assim, o conjunto de todas as classes residuais módulo m será denotado por $\mathbb{Z}_m$.*

Exemplo 2.3.2. *Seja $m = 2$, então:*

$$[0] = \{x \in \mathbb{Z};\ x \equiv 0 \ (mod\ 2)\},$$

$$[1] = \{x \in \mathbb{Z};\ x \equiv 1 \ (mod\ 2)\}.$$

Temos também que $[a] = [0]$, se a é par e $[a] = [1]$, se a é ímpar.

Exemplo 2.3.3. *Seja $m = 3$, então:*

$$[0] = \{3\lambda;\ \lambda \in \mathbb{Z}\},$$

$$[1] = \{3\lambda + 1;\ \lambda \in \mathbb{Z}\},$$

$$[2] = \{3\lambda + 2;\ \lambda \in \mathbb{Z}\}.$$

Temos que $[a] = [0]$, se a é múltiplo de 3; $[a] = [1]$, se a tem resto 1 quando dividido por 3; $[a] = [2]$, se a tem resto 2 quando dividido por 3.

Proposição 2.3.6. *As classes residuais módulo m possuem as seguintes propriedades:*

i) $[a] = [b]$ *se, e somente se,* $a \equiv b \ (mod\ m)$*;*

ii) Se $[a] \cap [b] \neq \emptyset$*, então* $[a] = [b]$*;*

Demonstração

i) Suponhamos que $a \equiv b \ (mod\ m)$; queremos provar que $[a] = [b]$, isto é, uma igualdade entre conjuntos. Dado $x \in [a]$, por definição temos $x \equiv a \ (mod\ m)$. Da Proposição 2.3.3 (iii) e por hipótese segue imediatamente que $x \in [b]$. Logo $[a] \subset [b]$. Reciprocamente, se $[a] = [b]$, temos que $a \in [b]$, assim $a \equiv b \ (mod\ m)$.

ii) Se $[a] \cap [b] \neq \emptyset$, consideremos um inteiro c que pertença a ambas as classes. Como $c \in [a]$, temos que $c \equiv a \ (mod\ m)$ e de forma análoga, $c \equiv b \ (mod\ m)$. Assim, $a \equiv b \ (mod\ m)$ e de i), $[a] = [b]$.

∎

Seja dado $x \in \mathbb{Z}_m$. Um número a tal que $x = [a]$ será denominado de representante de x. Observe que x é determinado por a, mas há infinitos números naturais b tais que $x = [b]$, ou seja, qualquer inteiro $b \in [a]$ é tal que $[b] = [a]$.

Exemplo 2.3.4. *Se $m = 2$, qualquer natural par é representante da classe residual* $[0]$ *e qualquer natural ímpar é representante da classe residual* $[1]$.

Exemplo 2.3.5. *Se $m = 3$, qualquer múltiplo de 3 é representante da classe residual* $[0]$. *Temos que 1, 4, 7, 10, etc, são representantes da classe residual* $[1]$, *enquanto 2, 5, 8, 11. etc, são representantes da classe residual* $[2]$.

Proposição 2.3.7. *Para cada $a \in \mathbb{Z}$ existe um, e somente um $r \in \mathbb{N}$,* com $r < m$, tal que $[a] = [r]$.

Demonstração Seja $a \in \mathbb{N}$. Pela divisão euclidiana, existem dois únicos naturais q e r, com $r < m$, tais que $a = m.q + r$. Logo, é único o natural r tal que $0 \leq r < m$ e $a \equiv r \ (mod\ m)$. Consequentemente, é único o natural r tal que $0 \leq r < m$ e $[a] = [r]$. ∎

Corolário 2.3.8. *Existem exatamente m classes residuais módulo m distintas, a saber:* $[0], [1], ..., [m-1]$.

Assim, reparte-se o conjunto $\mathbb{Z}$ dos números inteiros em subconjuntos, onde cada um deles é formado por todos os números inteiros que possuem o mesmo resto quando

divididos por m. Isto nos dá a seguinte partição de $\mathbb{Z}$:

$$[0] = \{x \in \mathbb{Z};\ x \equiv 0\ (mod\ m)\},$$

$$[1] = \{x \in \mathbb{Z};\ x \equiv 1\ (mod\ m)\},$$

$$\vdots$$

$$[m-1] = \{x \in \mathbb{Z};\ x \equiv\ m-1\ (mod\ m)\}.$$

Paramos em $[m-1]$, pois tem-se que $[m] = [0]$, $[m+1] = [1]$, etc. Assim,

$$\mathbb{Z}_m = \{[0], [1], ..., [m-1]\}.$$

Em $\mathbb{Z}_m$ definimos as seguintes operações:

Adição:

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \mapsto \mathbb{Z}_m$$

$$([a], [b]) \mapsto [a+b]$$

Multiplicação:

$$. : \mathbb{Z}_m \times \mathbb{Z}_m \mapsto \mathbb{Z}_m$$

$$([a], [b]) \mapsto [a.b]$$

Definidas estas operações usando os representantes a e b para as classes residuais $[a]$ e $[b]$, respectivamente, é fácil verificar que ao mudarmos os representantes das classes $[a]$ e $[b]$, não mudam os valores de $[a+b]$ e de $[a.b]$.

Lema 2.3.9. *Sejam* $a \equiv a^{'}\ (mod\ m)$ *e* $b \equiv b^{'}\ (mod\ m)$, *então* $[a+b] = [a^{'} + b^{'}]$ *e* $[a.b] = [a^{'}.b^{'}]$.

Demonstração

A demonstração é consequência imediata da Proposição 2.3.3 (iv) e (vi) e da Proposição 2.3.6 (i). ∎

As operações definidas acima, gozam das seguintes propriedades:

Propriedades da Adição

Para todos $[a], [b], [c] \in \mathbb{Z}_m$, temos:

A_1) **Associatividade:** $([a] + [b]) + [c] = [a] + ([b] + [c])$;

A_2) **Comutatividade:** $[a] + [b] = [b] + [a]$;

A_3) **Existência de zero:** $[a] + [0] = [a]$ para todo $[a] \in \mathbb{Z}_m$;

A_4) **Existência de simétrico:** Para todo $a < m$, tem-se que

$$[a] + [m - a] = [0].$$

Note que apesar da existência de simétrico não valer em $\mathbb{N}$, temos que ela vale em $\mathbb{Z}_m$.

Demonstração

As demonstrações são realizadas com base nos axiomas referentes as operações com números inteiros. Provaremos A_1) e A_4).

A_1) $[a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)]$.

Da propriedade associativa dos números inteiros temos:

$[a + (b + c)] = [(a + b) + c] = ([a] + [b]) + [c]$

A_4) Dado $[a] \in \mathbb{Z}_m$ vamos considerar a classe de $-a$ que é oposto de $[a]$, ou seja, $-[a] = [-a]$ cujo menor representante positivo é obtido: $[-a] = [0] - [a] = [m] - [a] = [m - a]$. Assim,

$$[a] + [m - a] = [a + (m - a)] = [m] = [0].$$

Para provar a unicidade, suponhamos que $[b] \in \mathbb{Z}_m$ também verifica $[a] + [b] = 0$ ou $[b] + [a] = 0$. Temos,

$$[b] = [b] + [0] = [b] + ([a] + [-a]) = ([b] + [a]) + [-a] = [0] + [-a] = [-a],$$

concluindo a demonstração. ∎

Propriedades da Multiplicação

Para todos $[a], b], [c] \in \mathbb{Z}_m$, temos:

M_1) **Associatividade:** $([a].[b]).[c] = [a].([b].[c])$;

M_2) **Comutatividade:** $[a].[b] = [b].[a]$;

M_3) **Existência de unidade:** $[a].[1] = [a]$.

AM) **Distributividade:** $[a].([b] + [c]) = [a].[b] + [a].[c]$.

Demonstração

Todas estas propriedades são fáceis de ser demonstradas. Vamos demonstrar na sequência, como exemplo, a propriedade AM:

$$[a].([b]+[c]) = [a].[b+c] = [a.(b+c)] = [a.b + a.c]$$

$$= [a.b] + [a.c] = [a].[b] + [a].[c]$$

∎

Um conjunto munido de uma operação de adição e de uma operação de multiplicação, com as propriedades acima, será chamado de anel. Por isso, $\mathbb{Z}_m$, com as operações acima, é um anel, chamado *anel das classes residuais módulo m.*

Definição 2.3.10. *Um elemento $[a] \in \mathbb{Z}_m$ será dito invertível, quando existir $[b] \in \mathbb{Z}_m$ tal que $[a].[b] = 1$ e diremos que $[b]$ é o inverso de $[a]$.*

Exemplo 2.3.6. *As tabelas da adição e da multiplicação em $\mathbb{Z}_2 = \{[0], [1]\}$ são:*

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$.$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Exemplo 2.3.7. *As tabelas da adição e da multiplicação em $\mathbb{Z}_3 = \{[0], [1], [2]]\}$ são:*

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$.$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Exemplo 2.3.8. *As tabelas da adição e da multiplicação em $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ são:*

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$.$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

É interessante notar que em $\mathbb{Z}_4$ existem dois elementos não nulos cujo produto é nulo: $[2] \neq [0]$ e, no entanto, $[2].[2] = [0]$.

Exemplo 2.3.9. *As tabelas da adição e da multiplicação em* $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ *são:*

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$.$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

Um anel onde todo elemento não nulo possui um inverso multiplicativo é chamado de ***corpo***. Note que $\mathbb{Z}_2$, $\mathbb{Z}_3$ e $\mathbb{Z}_5$, com as operações acima definidas, são corpos. Note que em um corpo tem-se que se $x \neq 0$ e $y \neq 0$, então $x.y \neq 0$.

Caracterizaremos os elementos invertíveis de $\mathbb{Z}_m$.

Proposição 2.3.11. $[a] \in \mathbb{Z}_m$ *é invertível se, e somente se,* $mdc(a, m) = 1$.

Demonstração Se $[a]$ é invertível, então existe $[b] \in \mathbb{Z}_m$ tal que $[1] = [a].[b] = [a.b]$. Logo, $a.b \equiv 1 \ (mod \ m)$, isto é, existe um natural t tal que $a.b - t.m = 1$ e, consequentemente, $mdc(a, m) = 1$.

Reciprocamente, se $mdc(a, m) = 1$, existem naturais b e t tais que $a.b - m.t = 1$ e, consequentemente, $[1 + m.t] = [a.b]$. Logo,

$$[1] = [1] + [m.t] = [1 + m.t] = [a.b] = [a].[b].$$

Portanto, $[a]$ é invertível. ∎

Corolário 2.3.12. $\mathbb{Z}_m$ *é um corpo se, e somente se,* m *é primo.*

Demonstração Suponha por absurdo que $\mathbb{Z}_m$ é um corpo e m não é primo, então $m = m_1.m_2$ com $1 < m_1 < m$ e $1 < m_2 < m$. Logo, $[0] = [m] = [m_1].[m_2]$ com $[m_1] \neq 0$ e $[m_2] \neq 0$, contradição.

Reciprocamente, suponha m primo. Como $mdc(i, m) = 1$ para $i = 1, ..., m-1$, segue-se da Proposição 2.3.11 que $[1], [2], ..., [m-1]$ são invertíveis. Logo, $\mathbb{Z}_m$ é um corpo. ∎

2.4 Identificação de erros nos códigos EAN-13 e UPC

Já presenciamos situações onde o operador de caixa tenta passar o código de barras várias vezes e, por algum motivo como por exemplo, a embalagem estar molhada ou o código estar enrugado, a máquina não registra o produto. Nesta situação o operador olha a sequência de dígitos do código de barras e a digita manualmente. Quando o operador comete um equívoco, geralmente de forma imediata, a máquina leitora detecta o erro cometido, pois se não fosse assim pagaríamos um valor diferente, do valor da mercadoria que estamos levando.

Sabemos que os dígitos dos códigos de barras identificam, nessa ordem, o país de origem, o fabricante, o produto e, por fim o dígito de verificação que tem a finalidade de detectar possíveis erros de digitação. Deste modo, os doze primeiros dígitos surgem naturalmente e o 13º dígito é calculado segundo critérios e padrões bem definidos.

Entendamos como é calculado o dígito verificador do código EAN-13 que denotaremos por x. Sendo assim o código $a_1a_2...a_{12}x$, representa o código de barras de um determinado produto, onde escreveremos esta sequência como um vetor α, tal que:

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

O sistema EAN-13 utiliza um vetor fixo que chamaremos de vetor pesos, que é:

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

Voltando ao código EAN-13, calculamos o produto escalar dos dois vetores:

$$\alpha.\omega = (a_1, a_2, ..., a_{11}, a_{12}, x).(1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1)$$

$$= a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + x$$

$$= 3(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}) + (a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + x)$$

Logo, o dígito verificador x é definido de tal forma que a soma acima seja múltiplo de 10, ou seja,

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

Exemplo 2.4.1. *Vamos descobrir, através do método citado sobre o código EAN-13, o dígito verificador de um produto cujo doze primeiros dígitos são 789432181175.*

Seja x o dígito de verificação e $\alpha = (7, 8, 9, 4, 3, 2, 1, 8, 1, 1, 7, 5, x)$, façamos o produto escalar $\alpha.\omega$. Assim,

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

$$= 7.1 + 8.3 + 9.1 + 4.3 + 3.1 + 2.3 + 1.1 + 8.3 + 1.1 + 1.3 + 7.1 + 5.3 + x.1$$

$$= 7 + 24 + 9 + 12 + 3 + 6 + 1 + 24 + 1 + 3 + 7 + 15 + x$$

$$= 112 + x$$

Como $112 + x \equiv 0 \ (mod\ 10)$, temos que $x = 8$. Portanto o dígito de verificação é 8 e o código completo é 7894321811758.

Exemplo 2.4.2. *Em um supermercado, o código de barras de um produto estava danificado, impossibilitando a leitura através do scanner. O operador decidiu digitar o código manualmente, só que encontrou a seguinte situação:*

Figura 2.4: Código de barras

Como proceder quando o dígito que não está legível? É lógico que em uma situação de supermercado seria viável realizar a troca do produto, mas utilizando as estratégias matemáticas acima citadas, conseguiríamos descobrir o dígito danificado.

Iniciaremos chamando de y o dígito danificado. Calculando o produto vetorial, temos

$$7 + 9 + 9 + 1 + 0 + 0 + 3 + 3(8 + 6 + 0 + y + 0 + 1) = 29 + 3(15 + y)$$

$$= 29 + 45 + 3y = 74 + 3y$$

Como $74 + 3y$ é múltiplo de 10, temos que o único possível valor para o dígito y é 2. Portanto o código de barras danificado é 7896901200013.

A verificação de erros nos códigos UPC ocorre da mesma maneira. Por apresentar apenas 12 dígitos, o formato do vetor de pesos é:

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

Quando a máquina não registra a leitura automaticamente, cabe ao operador de caixa realizá-la manualmente, o que poderá ocasionar diversos erros. Analisemos a situação onde ocorre apenas um erro de digitação, que é o erro mais comum como veremos mais adiante.

Exemplo 2.4.3. *Voltando ao código do Exemplo 2.4.1, imagine que a leitura automática não foi possível e o operador digitou erroneamente o código de barras da seguinte forma:*

7894321817758

É fácil verificar que o 10º dígito foi digitado errado. Será que a máquina leitora consegue identificar esse erro?

Fazendo o produto escalar $\alpha.\omega$, temos:

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

$$= 7.1 + 8.3 + 9.1 + 4.3 + 3.1 + 2.3 + 1.1 + 8.3 + 1.1 + 7.3 + 7.1 + 5.3 + 8.1$$

$$= 7 + 24 + 9 + 12 + 3 + 6 + 1 + 24 + 1 + 21 + 7 + 15 + 8 = 138$$

Como 138, não é múltiplo de 10, o erro de digitação seria verificado.

Vejamos uma situação onde são ocorridos dois erros de digitação que não serão identificados, pois eles se compensam mutuamente e, a soma do produto escalar $\alpha.\omega$ continua sendo um múltiplo de 10.

Exemplo 2.4.4. *Um determinado produto possui o código de barras* 7896256050295 *como identificador. Em uma situação onde o registro foi realizado manualmente foram ocorridos dois erros de digitação, porque o operador de caixas registrou* 7896$\underline{7}$56055$\underline{2}$95*. Através do produto escalar* $\alpha.\omega$*, veremos que os erros não serão detectados.*

$$\alpha.\omega = (7,8,9,6,7,5,6,0,5,3,2,9,5).(1,3,1,3,1,3,1,3,1,3,1,3,1)$$

$$= 7.1 + 8.3 + 9.1 + 6.3 + 7.1 + 5.3 + 6.1 + 0.3 + 5.1 + 5.3 + 2.1 + 9.3 + 5.1$$

$$= 7 + 24 + 9 + 18 + 7 + 15 + 6 + 0 + 5 + 15 + 2 + 27 + 5 = 140$$

Como 140 é múltiplo de 10, o erro não seria detectado. Assim, o sistema de códigos EAN-13 não consegue identificar todos os erros de dois dígitos, ocorridos na digitação.

Outro erro muito comum é a transposição de dois dígitos consecutivos. Veremos adiante que nem todo erro deste tipo pode ser identificado nos códigos EAN-13.

Exemplo 2.4.5. *Um determinado produto possui o seguinte código de barras:* 7891000014936*. Feito o registro de forma manual, houve uma transposição adjacente, sendo digitados os dígitos na forma* 7891000041936*. Fazendo o produto escalar, temos:*

$$7.1 + 8.3 + 9.1 + 1.3 + 0.1 + 0.3 + 0.1 + 0.3 + 4.1 + 1.3 + 9.1 + 3.3 + 6.1$$

$$= 7 + 24 + 9 + 3 + 4 + 3 + 9 + 9 + 6 = 74$$

Como 74 não é múltiplo de 10, o erro seria detectado.

Exemplo 2.4.6. *Analisando o mesmo código de barras, consideremos outro erro de transposição adjacente. O registro realizado agora foi* 7891000019436*.*

Procedendo como o exemplo anterior, temos:

$$7.1 + 8.3 + 9.1 + 1.3 + 0.1 + 0.3 + 0.1 + 0.3 + 1.1 + 9.3 + 4.1 + 3.3 + 6.1$$

$$= 7 + 24 + 9 + 3 + 1 + 27 + 4 + 9 + 6 = 90$$

Sabendo que existe um erro, mas como 90 é múltiplo de 10, esse erro não pode ser identificado.

O Exemplo 2.4.6 mostra que o sistema de detecção de erros dos códigos EAN-13, não consegue detectar todo erro de transposição cometido.

Teorema 2.4.1. *Um erro de transposição adjacente, do tipo*

$$...a_i a_{i+1}... \mapsto ...a_{i+1}a_i...$$

não é detectado pelo sistema EAN-13 se, e somente se,$\mid a_i - a_{i+1} \mid = 5$.

Demonstração Sendo o código EAN-13 $a_1a_2a_3...a_{13}$. Considerados os dígitos consecutivos a_i e a_{i+1}, sendo $i = \{1, 2, ..., 12\}$, temos duas possibilidades:

1) Se i for par, multiplica-se a_i por 1,e

2) Se i for ímpar, multiplica-se a_i por 3.

Havendo um erro de digitação (transposição adjacente), teremos dois vetores V_1 e V_2, tal que

$$V_1 = (a_1, ..., a_i, a_{i+1}, ..., a_{13}),$$

e

$$V_2 = (a_1, ..., a_{i+1}, a_i, ..., a_{13}),\ com\ a_i \neq a_{i+1}.$$

Supondo, sem perda de generalidade, i par, $c \in \mathbb{N}$ e que o erro não foi detectado, temos:

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

e,

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

Assim,

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

$$3a_i + a_{i+1} \equiv 3a_{i+1} + a_i\ (mod\ 10)$$

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

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

Logo, $10 \mid 2(a_i - a_{i+1})$, o que implica que $5 \mid (a_i - a_{i+1})$.

Como a_i,$a_{i+1} \in \{1, ..., 9\}$ e, por hipótese, $a_i \neq a_{i+1}$, temos que $\mid a_i - a_{i+1} \mid = 5$.

Portanto, se o erro não foi detectado temos $\mid a_i - a_{i+1} \mid = 5$.

Para o caso de i ímpar a demonstração é análoga.

Reciprocamente, se $\mid a_i - a_{i+1} \mid = 5$ e, supondo, sem perda de generalidade, i ímpar e, $a_i > a_{i+1}$.

Sendo $V_1 = (a_1, ..., a_i, a_{i+1}, ..., a_{13})$ e

$$a_1 + 3a_2 + ... + a_i + 3a_{i+1} + ... + a_{13} \equiv c \ (mod\ 10),$$

vamos mostrar que

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

Assim,

$$a_i - a_{i+1} = 5 \Rightarrow 2(a_i - a_{i+1}) = 10$$

Logo, $10 \mid 2(a_i - a_{i+1}) = 2a_i - 2a_{i+1} = 3a_i + a_{i+1} - a_i - 3a_{i+1}$

$$\Rightarrow 10 \mid (3a_i + a_{i+1}) - (3a_{i+1} + a_i).$$

Então,

$$(3a_i + a_{i+1}) - (3a_{i+1} + a_i) \equiv 0 \ (mod\ 10)$$

$$3a_i + a_{i+1} \equiv 3a_{i+1} + a_i$$

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

Por hipótese

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

Portanto, se $\mid a_i - a_{i+1} \mid = 5$, o erro de transposição adjacente não é detectado.

A demonstração para os casos i par e $a_i < a_{i+1}$ é análoga. ∎

Existem vários erros que podem ser cometidos, quando o registro do código identificador é feito manualmente. Os erros num único dígito e as transposições são os erros mais frequentes. Segundo J. Verhoeff, uma síntese da frequência dos erros mais cometidos é traduzida pela tabela a seguir:

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

Tabela 2.5: Tipos de erros e suas frequências segundo Verhoeff.

2.5 Identificação de erros nos códigos identificadores

Agora que temos algumas ferramentas da Aritmética, vamos definir uma linguagem geral, com o objetivo de descrever diversos métodos de codificação existente. Denotaremos por $\mathcal{A}$ o conjunto de valores que podem assumir os dígitos utilizados na codificação. No caso do código UPC, esse conjunto é

$$\mathcal{A} = \{x \in \mathbb{Z} \mid \ 0 \leq \ x \leq \ m-1\}.$$

O vetor com os dados $\alpha' = (a_1, ..., a_{n-1})$ será chamado de **vetor de informação** e o vetor com o dígito de verificação será chamado de **número** ou **vetor de identificação**.

Definição 2.5.1. *Sejam $\omega = (w_1, ..., w_n)$, com $w_i \in \mathcal{A}$, $1 \leq i \leq \ n$ um vetor de pesos e $c \in \mathcal{A}$ um inteiro fixado. Dados dois inteiros positivos m e n e um conjunto de números $a_1, ..., a_{n-1}$ tais que $a_i \in \mathcal{A}$, $1 \leq \ i \leq n-1$, define-se o número de verificação a_n como o único elemento de $\mathcal{A}$ que verifica a equação:*

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

Um sistema de codificação assim definido será denotado por $\mathcal{C} = (\mathcal{A}, m, n, c, w)$.

Tomadas as classes módulo m, temos que a_n é o único elemento de $\mathcal{A}$ que verifica

$$[a_n] = [w_n]^{-1} \left([c] - \sum_{i=1}^{n-1} [a_i][w_i] \right)$$

pois, frequentemente $\mathcal{A} = \{0, 1, ..., m-1\}$.

Exemplo 2.5.1. *Em um sistema usado por alguns bancos, o número da conta de cada cliente é composto com 9 dígitos, sendo o último o dígito de verificação. Utilizada a notação definida, o sistema pode ser descrito como* $\mathcal{C} = (\mathcal{A}, 10, 2, 0, w)$*, onde* $\mathcal{A} = \{0, 1, ..., 9\}$ *e* $w = (7, 3, 9, 7, 3, 9, 7, 3, 9)$*. Verifica-se o número da conta* $95 - 005541 - 9$*, que utiliza este sistema, temos que:*

$$(9, 5, 0, 0, 5, 5, 4, 1, 9).(7, 3, 9, 7, 3, 9, 7, 3, 9) =$$

$$63 + 15 + 15 + 45 + 28 + 3 + 81 = 250 \equiv 0 \ (mod\ 10)$$

Exemplo 2.5.2. *Consideremos o Exemplo 2.5.1, suponhamos que foi cometido um erro em uma digitação (transposição adjacente), sendo a mesma conta considerada e, com número digitado* $95 - 005514 - 9$*. Verificaremos que, neste caso, o erro seria detectado, pois:*

$$(9, 5, 0, 0, 5, 5, 1, 4, 9).(7, 3, 9, 7, 3, 9, 7, 3, 9) =$$

$$63 + 15 + 15 + 45 + 7 + 12 + 81 = 238$$

Como 238 não é múltiplo de 10, o erro seria detectado.

Nem todo erro de transposição pode ser identificado por este sistema. Considerando ainda as informações dos exemplos anteriores, veremos uma situação onde ocorreu um erro de transposição, que não será identificado.

Exemplo 2.5.3. *Agora, vamos supor que o registro manual foi realizado da seguinte forma:* $95 - 500541 - 9$*. Vejamos:*

$$(9, 5, 5, 0, 0, 5, 4, 1, 9).(7, 3, 9, 7, 3, 9, 7, 3, 9) =$$

$$63 + 15 + 45 + 45 + 28 + 3 + 81 = 280 \equiv 0 \ (mod\ 10)$$

Portanto, houve um erro de transposição que não foi identificado.

Em todos exemplos que envolveram os códigos identificadores até o momento vimos situações em que possíveis erros foram identificados e, outras situações em que ocorreram erros, mas não foram detectados. Na criação de códigos identificadores a intenção sempre é minimizar ou eliminar qualquer possibilidade de erro. O teorema a seguir descreve a capacidade de detectar erros que tem um sistema assim definido.

Teorema 2.5.2. *Sejam m um inteiro positivo e $\omega = (w_1, ..., w_n)$ um vetor de pesos. Suponhamos que um vetor de identificação $\alpha = (a_1, ..., a_n)$, onde assumimos que $0 \leq a_i \leq n$ para todo índice i, $1 \leq i \leq n$, satisfaz a condição*

$$\alpha.\omega = a_1w_1 + ... + a_nw_n \equiv \ c \ (mod \ m)$$

Então:

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

2. *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

1. Vamos supor que o digito a_i tenha sido trocado por outro digito b_i. Sejam $\alpha = (a_1, a_2, ..., a_i, ..., a_n)$ e $\beta = (a_1, a_2, ..., b_i, ..., a_n)$ os vetores resultantes da troca. Neste caso o erro não será detectado se, e somente se $\alpha.w \equiv \beta.w \ (mod \ m)$, isto é, se e somente se $m|(a_i - b_i)w_i$.

($\Longleftarrow$) Vamos supor que $mdc(w_i, m) = 1$ e que o erro não foi detectado. Então segue que $m|(a_i - b_i)w_i$. Como, por hipótese, w_i e m são primos, chegamos que $m|a_i - b_i$. Mas $0 \leq a_i, b_i < m$ e assim $a_i - b_i = 0$, ou seja, $a_i = b_i$, que é um absurdo pois, por hipótese, $a_i \neq b_i$.

($\Longrightarrow$) Vamos supor que todo erro é detectado e que $mdc(w_i, m) = d \neq 1$. Sejam $x_i = a_i + \frac{m}{d}$ e $y_i = a_i - \frac{m}{d}$.

Afirmação: $0 \leq x_i < m$ ou $0 \leq y_i < m$.

De fato, se $m \leq x_i$ e $y_i < 0$ então $m \leq a_i + \frac{m}{d}, a_i - \frac{m}{d} < 0$ e assim $m - \frac{m}{d} < \frac{m}{d}$. Portanto $md < 2m$ e então $d < 2$, o que é um absurdo.

Seja $b_i = x_i$ ou y_i satisfazendo $0 \leq b_i < m$. Então $(a_i - b_i)w_i = (\pm\frac{m}{d})w_i = m(\pm\frac{w_i}{d})$ isto é, o erro que substitui a_i por b_i não é detectado, que é um absurdo.

2. Vamos supor que os dígitos a_i, a_j tenham sido trocados.

Sejam $\alpha = (a_1, a_2, ..., a_i, ..., a_j, ..., a_n)$ e $\beta = (a_1, a_2, ..., a_j, ..., a_i, ..., a_n)$ os vetores resultantes da troca. Neste caso o erro não será detectado se, e somente se $\alpha.w \equiv \beta.w \ (mod\, m)$, isto é, se e somente se $m|(a_i - a_j)(w_i - w_j)$.

($\Longleftarrow$) Vamos supor que $mdc(w_i - w_j, m) = 1$ e que o erro não foi detectado. Então segue que $m|(a_i - a_j)(w_i - w_j)$. Como, por hipótese, $w_i - w_j$ e m são primos, chegamos que $m|a_i - a_j$. Mas $0 \leq a_i, a_j < m$ e assim $a_i - a_j = 0$, ou seja, $a_i = a_j$, que é um absurdo pois $a_i \neq a_j$, por hipótese.

($\Longrightarrow$) Vamos supor que todo erro é detectado e que $mdc(w_i - w_j, m) = d \neq 1$. Usando as ideias anteriores, temos que se $a_j = a_i + \frac{m}{d}$ ou $a_j = a_i - \frac{m}{d}$ então o erro de transposição cometido trocando-se a_i por a_j não é detectado, chegando assim a um absurdo. ∎

A melhor forma de ter certeza que o sistema de codificação será capaz de detectar todos os erros únicos e todos os erros de transposição é considerar, para o valor do módulo m, um número primo. De fato, existem vários sistemas em uso que procedem desta forma.

Exemplo 2.5.4. *O ISBN (International Standart Book Number) é um sistema universal adotado para registros de livros que trabalha com congruência módulo 11, onde utiliza o conjunto* $\mathcal{A} = \{0, 1, ..., 9\}$ *e o vetor de identificação* $\omega = (10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$. *Assim, um certo livro possui o número ISBN 85-08-07666-5, onde o dígito de verificação é 5 pois:*

$$(8, 5, 0, 8, 0, 7, 6, 6, 6, 5).(10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$$

$$= 80 + 45 + 56 + 35 + 24 + 18 + 12 + 5)$$

$$= 275 \equiv 0 \ (mod\ 11).$$

Este método é bastante eficaz na detectação de possíveis erros, porém apresenta um pequeno inconveniente. Para entender melhor a situação, analisemos o exemplo a seguir.

Exemplo 2.5.5. *Vamos encontrar o dígito de verificação y, utilizando os métodos do ISBN, de um livro cujo código nesse sistema é 0-387-96035-y. Temos que:*

$$(0, 3, 8, 7, 9, 6, 0, 3, 5, y).(10, 9, 8, 7, 6, 5, 4, 3, 2, 1)$$

$$= 27 + 64 + 49 + 54 + 30 + 9 + 10 + y)$$

$$= 243 + y \equiv 0 \ (mod\ 11)$$

$$y \equiv -243 \ (mod\ 11)$$

$$y \equiv -1 \ (mod\ 11)$$

$$y \equiv 10 \ (mod\ 11)$$

Assim, o dígito verificador y é igual a 10, mas no conjunto $\mathcal{A} = \{0, 1, ..., 9\}$*, não temos nenhum dígito que represente o* 10*. Portanto, a convenção usual é utilizar o símbolo* $\boldsymbol{X}$ *para representar essa situação, sendo o código do livro citado 0-387-96035-X.*

Finalizando, vamos compreender o funcionamento e os métodos de detecção de erros de alguns códigos identificadores como o CNPJ, o CPF e o RG-SP, presentes no nosso dia a dia.

Exemplo 2.5.6. *Analisemos como se calcula o Número-Controle do CNPJ do Ministério da Fazenda. O CNPJ, tem configuração com 14 dígitos, onde os primeiros oito dígitos são o número-base, os quatro seguintes o número de ordem das filiais da empresas, o penúltimo o dígito de verificação (DV) em relação aos doze anteriores e o último é o DV referente aos treze anteriores, que são calculados através de congruência, como veremos a seguir. Outra particularidade é que o oitavo dígito era DV módulo 10 dos sete anteriores, isso para os CNPJ emitidos anteriormente a 1993, mas a partir daí, a regra foi abandonada e o oitavo dígito foi incorporado ao número identificador, para ampliar a capacidade de 10 milhões para 100 milhões de cadastros.*

Logo, no CNPJ, o penúltimo dígito (DV) corresponde ao resto da divisão por 11 do produto escalar entre o vetor α *da base do código constituído de 12 dígitos (número-base e ordem das filiais), pelo vetor* $\omega = (6, 7, 8, 9, 2, 3, 4, 5, 6, 7, 8, 9)$*. O resto 10 é considerado 0, mas algumas instituições, como o Banco do Brasil, por exemplo, tratam o 10, em seus números de contas, como "X". O último dígito (DV) corresponde ao resto da divisão por 11 do produto escalar* $\omega' = (5, 6, 7, 8, 9, 2, 3, 4, 5, 6, 7, 8, 9)$ *pelos vetor composto pelos 13 dígitos iniciais que compõem o CNPJ. Por exemplo, o cálculo do DV do CNPJ nº 18781203/0001 é:*

i) Cálculo do 13^o *dígito*

$$(1,8,7,8,1,2,0,3,0,0,0,1)(6,7,8,9,2,3,4,5,6,7,8,9)$$

$$= 6+56+56+72+2+6+15+9$$

$$= 222 \equiv 2 \ (mod\ 11)$$

Assim o 13^o *dígito é* 2.

ii) Cálculo do 14^o *dígito*

$$(1,8,7,8,1,2,0,3,0,0,0,1,2)(5,6,7,8,9,2,3,4,5,6,7,8,9)$$

$$= 5+48+49+64+9+4+12+8+18$$

$$= 217 \equiv 8 \ (mod\ 11)$$

Assim o 14^o *dígito é* 8.

Portanto o número comlpeto do CNPJ em questão é 18781203/0001-28

Exemplo 2.5.7. *O CPF, também número-controle do Ministério da Fazenda, tem configuração apresentando 11 dígitos, onde os primeiros oito são o número-base, o nono define a Região Fiscal, o penúltimo o dígito de verificação (DV) referente aos nove dígitos anteriores e o último o dígito de verificação em relação aos dez dígitos anteriores, o que é bem semelhante ao cálculo dos DV do CNPJ. O primeiro DV é o resto da divisão por 11 do produto escalar* $\alpha.\omega$*, onde* α *é obtido pelos 9 primeiros dígitos do código e o vetor* $\omega = (1,2,3,4,5,6,7,8,9)$ *e o outro DV é o resto da divisão por 11 do produto escalar* $\alpha.\omega'$*, onde* α *é obtido pelos 10 primeiros dígitos do código e o vetor* $\omega' = (0,1,2,3,4,5,6,7,8,9)$*. Veja o exemplo do CPF cujo número sem o DV é 282.646.438:*

i) Cálculo do 10^o *dígito*

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

$$= 2+16+6+24+20+36+28+24+72$$

$$= 228 \equiv 8 \ (mod\ 11)$$

Assim o penúltimo dígito é 8.

ii) Cálculo do 11^o *dígito*

$$(2, 8, 2, 6, 4, 6, 4, 3, 8, 8).(0, 1, 2, 3, 4, 5, 6, 7, 8, 9)$$

$$8 + 4 + 18 + 16 + 30 + 24 + 21 + 64 + 72$$

$$= 257 \equiv \ 4 \ (mod\ 11)$$

Assim o último dígito é 4.

Portanto o número do CPF completo é 282.646.438-84.

Exemplo 2.5.8. *O Dígito Verificador (DV) do número da Carteira de Identidade SSP-SP (RG) é calculado utilizando a congruência módulo 11 do produto escalar* $\alpha.\omega$*, onde* α *é o vetor formado pelos números da identidade (geralmente 8 dígitos) e* $\omega = (9, 8, 7, 6, 5, 4, 3, 2)$*. Então o DV do RG/SSP-SP cujo número é 28839471 é*

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

$$= 18 + 64 + 56 + 18 + 45 + 16 + 21 + 2 = 240, onde$$

$$240 \equiv \ 9 \ (mod\ 11)$$

Portanto o DV é 9, sendo o RG completo 28.839.471-9.

Caso o resto seja 10, o DV será a letra X*.*

Capítulo 3

Diversos códigos de barras atuais

Citaremos, neste capítulo, apenas a existência de outros códigos de barras e aparelhos leitores utilizados atualmente.

1. Os códigos de barras alfanuméricos são capazes de representar maiores informações sobre o produto.

Figura 3.1: Código alfanuméricos

2. O **Código 39** foi desenvolvido por algumas indústrias que necessitavam codificar o alfabeto, assim como os números, em códigos de barras. É utilizado na identificação em estoques e em processos nos segmentos industriais, mas este sistema produz códigos de barras relativamente longos e não podem ser adequados a largura da etiqueta.

3. O **Código 128** provém da necessidade de uma seleção mais ampla de caracteres do

que o Código 39. A largura da etiqueta é compacta e resulta um símbolo denso. Sua utilização é frequente na industria de transporte.

4. O código **Intercalado 2 de 5** também é compacto e utilizado frequentemente nas caixas de papelão e por operadores logísticos.

5. O Código de barras bidimensional ou **PDF417** é uma simbologia não linear de alta densidade. É considerado um arquivo portátil e não apenas um número identificador. Possivelmente em um futuro próximo, esse tipo de identificação poderá aparecer nas carteiras de motoristas em alguns estados. Caso isso ocorra, o código armazenará informações como nome, foto, o resumo de seus registros de motorista e outras informações pertinentes. Seu tamanho pode ser como o de um selo postal. O código de barras bidimensional pode aparecer também na versão colorida, onde seus criadores afirmam que sua capacidade é tão grande quanto a nossa imaginação.

Figura 3.2: Código barras bidimensional

Figura 3.3: Código bidimensional colorido

6. A Leitora tipo Caneta Esferográfica funciona a partir de uma fonte de luz de frequência pré definida e de um fotodiodo, desenvolvido para ler essa frequência,

que estão na ponta da caneta, que se arrasta sobre a superfície do código, onde as barras escuras absorvem a luz e as barras brancas a refletem, determinando assim a espessura e o espaçamento das barras. Esse sistema é similar ao código Morse.

Figura 3.4: Leitora tipo caneta esferográfica

7. A Leitora a Laser funcionam de modo parecido ao das leitoras esferográfica, contudo utiliza o raio laser como fonte de energia e um espelho para redimensionar todo o raio pela superfície do código.

Figura 3.5: Leitora a laser

8. A Leitora CCD *(Charge Coupled Device)* utiliza uma matriz com centenas de micro sensores de luz alinhados que fazem uma leitura de forma panorâmica. Os outros leitores emitem luz para dimensionar o código, enquanto o CCD utiliza apenas a luz do ambiente.

Figura 3.6 Leitora CCD

9. Os Leitores com Câmeras são os mais modernos, pois operam através da leitura de centenas de linhas dispostas em qualquer posição, diferentemente dos outros citados que leem apenas uma linha. Esse tipo de leitor pode estar presente em diversos tipos de aparelhos que possuem câmeras e produzem imagens, como por exemplo, o celular.

Figura 3.7: Leitoras com câmeras

Capítulo 4

Aplicação da Matemática dos códigos de barras no ensino básico

4.1 Introdução

Vimos que a matemática está presente nos códigos de barras. Observamos também que seu funcionamento prático na vida moderna depende da Aritmética Modular. Situações que envolvem esses conhecimentos muitas vezes não são abordadas em sala de aula no ensino básico. A atividade a ser desenvolvida e aplicada consiste na resolução de sistemas lineares, considerando o conjunto das classes residuais $\mathbb{Z}_m$ utilizando assim conceitos relacionados a Aritmética Modular, ramo da Matemática relacionado diretamente a toda estrutura dos códigos de barras e demais códigos identificadores. Muitos jogos de computadores utilizam essa lógica em seu funcionamento. Problemas como esses são chamados jogos lineares finitos. O público alvo para essa atividade é a 2^{a} série do ensino médio, entretanto podemos extender sua aplicação para as outras séries do ensino médio e, dependendo do contexto até mesmo nas séries finais do ensino fundamental. O principal objetivo da atividade é mostrar aos alunos a utilização e aplicação de sistemas lineares de forma diferenciada, além de trabalhar de forma direta ou indireta a aritmética das classes residuais.

4.2 Descrição, metodologia e aplicação

Iniciamos a atividade avaliando os conhecimentos prévios dos alunos sobre o assunto, através de discussão e da resolução de sistemas lineares mais simples e abrangendo todo o conjunto dos números reais. Pode-se aplicar também uma atividade envolvendo números binários, preparando-os para lidar com situações em $\mathbb{Z}_2$.

Após a análise dos resultados e, se necessário, a retomada dos conteúdos em questão, iniciamos a preparação para a atividade principal com uma atividade preliminar, com o objetivo de que o público alvo possa conhecer, praticar e familiarizar-se com números e vetores binários.

Atividade Inicial: Dados os vetores binários u e v, em cada caso determine $u + v$:

a) $u = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ e $v = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$

b) $u = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$ e $v = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}$

c) $u = [1, 0, 1, 1]$ e $v = [1, 1, 1, 1]$

d) $u = [1, 1, 0, 1, 0]$ e $v = [0, 1, 1, 1, 0]$

Resolução

a) $u + v = \begin{bmatrix} 0+1 \\ 1+1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$

b) $u + v = \begin{bmatrix} 1+1 \\ 1+1 \\ 0+1 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$

c) $u + v = [1+1, 0+1, 1+1, 1+1] = [0, 1, 0, 0]$

d) $u + v = [1+0, 1+1, 0+1, 1+1, 0+0] = [1, 0, 1, 0, 0]$

Após a realização das atividades e situações citadas, da análise e avaliação positiva dos resultados, iniciaremos a aplicação da atividade principal deste trabalho, que consiste em uma situação contendo uma fileira com cinco lâmpadas A, B, C, D e E que é controlada por cinco interruptores 1, 2, 3, 4 e 5. Cada interruptor muda o estado da lâmpada diretamente sobre ele e os estados das lâmpadas imediatamente adjacentes à esquerda e a direita. Mudar o estado significa acender a lâmpada caso esteja apagada ou, apagá-la caso esteja acesa. Por exemplo, ao apertar o interruptor 3, as lâmpadas B, C e D terão o estado alterado ou, ao apertar o interruptor 5, as lâmpadas D e E terão o estado alterado.

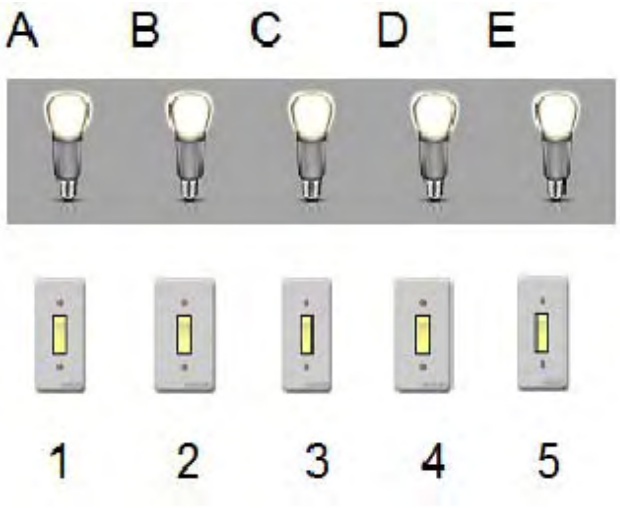

Figura 4.1: Atividade principal

O ideal seria a iniciação da atividade com um dispositivo real com as lâmpadas e interruptores ou um programa de computador que simule a situação descrita acima. Assim os alunos participariam de situações pré-definidas ou criadas no decorrer da atividade, executando a resolução das situações por tentativa e erro. Com uma situação melhor elaborada como, por exemplo, a **Atividade Principal**, que veremos adiante, entrará em cena a resolução dos sistemas lineares evolvendo vetores binários, utilizando como estratégias procedimentos matemáticos presentes na estrutura dos códigos de barras.

A notação binária será muito útil na solução de problemas envolvendo situações liga/desliga. Vamos trabalhar em $\mathbb{Z}_2$, sendo assim 0 representando desligado e 1 liga-

do. Para representar os estados das cinco lâmpadas utilizaremos um vetor em $\mathbb{Z}_2^5$. Por exemplo, o vetor

$$\begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix},$$

corresponde a situação onde as lâmpadas A, B e E estão acesas e, as lâmpadas C e D estão apagadas.

A ação de cada interruptor, também será representada por vetores em $\mathbb{Z}_2^5$, onde a mudança de estado de uma lâmpada será representado por 1. Caso contrário, a representação será 0. Logo, a ação de cada interruptor é dada por

$$x_1 = \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \; x_2 = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \; x_3 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}, \; x_4 = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}, \; x_5 = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

Considerando como exemplo, o estado inicial v, como ligadas apenas as lâmpadas A e D, onde

$$v = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 0 \end{bmatrix},$$

ao apertar o interruptor 2, temos a soma

$$v + x_2 = \begin{bmatrix} 1+1 \\ 0+1 \\ 0+1 \\ 1+0 \\ 0+0 \end{bmatrix},$$

que em $\mathbb{Z}_2^5$ é

$$v + x_2 = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

Com isso, ficarão ligadas apenas as lâmpadas B, C e D.

Sendo qualquer o estado inicial u das lâmpadas, ao apertar os interruptores na ordem 4, 2, 1, 2, 3 e 4, temos que

$$u + x_4 + x_2 + x_1 + x_2 + x_3 + x_4 = u + x_1 + 2x_2 + x_3 + 2x_4 = u + x_1 + x_3,$$

pois a adição é comutativa em $\mathbb{Z}_2$, onde $2 = 0$. Chegaríamos ao mesmo resultado apertando apenas o interruptor 1 e 3 independentemente da ordem. Concluímos então que em qualquer situação, não é preciso apertar nenhum interruptor mais de uma vez.

Para chegar a uma situação estipulada s, quando possível, a partir de uma situação inicial u, precisamos determinar, caso existam, os escalares a, b, c, d e e, tais que

$$u + x_1a + x_2b + x_3c + x_4d + x_5e = s,$$

o que equivale a resolver o seguinte sistema linear em $\mathbb{Z}_2$:

$$x_1a + x_2b + x_3c + x_4d + x_5e = s - u,$$

ou

$$x_1a + x_2b + x_3c + x_4d + x_5e = s + u.$$

Com base nesta estratégia, buscaremos a solução da **Atividade Principal** a seguir.

Atividade Principal: Considerando o esquema de lâmpadas e interruptores citado acima. Suponha inicialmente que todas as luzes estejam apagadas.

a) Podemos pressionar os interruptores em alguma ordem de modo que as lâmpadas A, C e E fiquem acesas?

b) Podemos pressionar os interruptores em alguma ordem de modo que só a primeira lâmpada fique acessa?

Resolução

(a) Como todas as lâmpadas estão desligadas, temos que $u = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$ e nosso objetivo a ser alcançado é $s = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$.

O sistema linear $x_1a + x_2b + x_3c + x_4d + x_5e = s - u = s + u$ que representa esta situação é

$$\begin{cases} a + b = 1 \\ a + b + c = 0 \\ b + c + d = 1 \\ c + d + e = 0 \\ d + e = 1 \end{cases}$$

que em $\mathbb{Z}_2$ se reduz para

$$\begin{cases} a + e = 0 \\ b + e = 1 \\ c = 1 \\ d + e = 1 \end{cases}$$

Sendo e uma variável livre, temos exatamente duas soluções em $\mathbb{Z}_2$ correspondentes a $e = 0$ e $e = 1$.

Se $e = 0$, temos $\begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{bmatrix}$, ou seja, nesta situação apertando os interruptores 2, 3 e 4, em qualquer ordem, apenas as lâmpadas A, C e E ficarão acesas.

Agora, se $e = 1$, temos $\begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \end{bmatrix}$, ou seja, nesta situação apertando os interruptores 1, 3 e 5, em qualquer ordem, apenas as lâmpadas A, C e E ficarão acesas.

É fácil verificar que as duas soluções funcionam.

(b) Analogamente, temos $s = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$, que se reduz ao sistema

$$\begin{cases} a + b = 1 \\ a + b + c = 0 \\ b + c + d = 0 \\ c + d + e = 0 \\ d + e = 0 \end{cases}$$

que em $\mathbb{Z}_2$ que é equivalente

$$\begin{cases} a + e = 0 \\ b + e = 1 \\ c = 1 \\ d + e = 1 \\ 0 = 1 \end{cases}$$

que é um absurdo, mostrando que o sistema não tem solução. Portanto é impossível começar com todas as lâmpadas apagadas e acender apenas a primeira.

Os dois questionamentos são apenas exemplos de como a atividade pode ser explorada. Podemos iniciar com uma situação mais simples como, por exemplo, deixar todas as lâmpadas acesas onde o aluno pode facilmente chegar a uma conclusão através de tentativas e observações. Outros questionamentos poderão surgir no decorrer da aplicação e devemos explorá-los de forma conveniente. Devem-se explorar também situações onde há uma única solução, mais que uma solução, como o item (a) e também situações onde não há solução como o item (b) e observar o comportamento dos alunos ao lidar com esse tipo de sistemas lineares em $\mathbb{Z}_2$.

4.3 Avalição dos resultados

Após a realização das etapas descritas, é indispensável uma reflexão dos resultados obtidos em $\mathbb{Z}_2$, realizando uma comparação com o sistema de numeração decimal e, também uma análise sobre a possibilidade dos jogos lineares e a resolução de sistemas lineares em $\mathbb{Z}_m$, para qualquer m natural diferente de 1.

A avaliação final da atividade poderá ser a elaboração, em grupo, de um jogo linear envolvendo sistemas lineares com diversas variáveis e equações, para a obtenção das devidas soluções, além da utilização de vetores pertencentes a $\mathbb{Z}_m$ para qualquer m natural, tal que $m > 2$.

Como atividade complementar, poderá ser aplicada a seguinte situação:

Atividade complementar: Considere uma fileira com apenas três lâmpadas, que podem estar apagadas, acesas com luz azul clara ou acesas com luz azul escura. Sob as lâmpadas estão três interruptores, A, B e C; cada um deles muda o estado das lâmpadas para o próximo estado, ou seja: desligada, azul clara, azul escura, desligada, ... O interruptor A muda o estado das duas primeiras lâmpadas, o interruptor B muda todas as três lâmpadas e o interruptor C muda as últimas duas. Se todas as três lâmpadas estiverem inicialmente desligadas, é possível pressionar de um jeito que as lâmpadas fiquem nesta ordem: desligada, azul clara e azul escura?

Resolução

Nesta atividade vamos utilizar sistemas lineares em $\mathbb{Z}_3$. As ações dos interruptores correspondem aos vetores

$$a = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}, \; b = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \; c = \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix},$$

em $\mathbb{Z}_3^3$ e a situação final pretendida é $s = \begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$, onde 0 é desligado, 1 é azul claro e 2 é azul escuro. A solução consiste em encontrar escalares x_1, x_2 e x_3 em $\mathbb{Z}_3$ tais que

$$x_1 a + x_2 b + x_3 c = s,$$

que se reduz ao sistema

$$\begin{cases} x_1 + x_2 = 0 \\ x_1 + x_2 + x_3 = 1 \\ x_2 + x_3 = 2 \end{cases}$$

que em $\mathbb{Z}_3$ que é equivalente

$$\begin{cases} x_1 = 2 \\ x_2 = 1 \\ x_3 = 1 \end{cases}$$

o que significa, que devemos pressionar duas vezes o interruptor A, uma vez o interruptor B e uma vez o interruptor C, que também é fácil de se verificar.

4.4 Conclusão e considerações finais

Pode ser explorada em qualquer situação, a criatividade dos alunos e a dos professores que vierem a utilizar dessas atividades. A curiosidade também é um elemento que pode contribuir para o sucesso das atividades. O interessante, como já foi citado, é a utilização de um material concreto, que simule a situação descrita na atividade principal, assim a curiosidade e o interesse do público alvo despertaria de forma diferenciada. Mas isto

pode não ser viável devido ao custo e, até mesmo a dificuldade de encontrar profissionais capacitados para construí-la. Neste trabalho houve diversos colaboradores, contudo não obtiveram sucesso na construção do material concreto utilizando materiais de baixo custo. Mesmo com este obstáculo, a atividade pode facilmente ser aplicada no ensino básico público, utilizando-se de diversos materiais como cartazes, ilustrações, lousa, giz e outras ideias que poderão surgir.

Capítulo 5

Conclusão

A Matemática presente nos códigos de barras, vai além do armazenamento de dados e informações. Em sua estrutura estão presentes conhecimentos da Aritmética, da Álgebra e alguns requisitos do Cálculo, como *produto vetorial (escalar)*. Através desta vertente matemática pode-se explorar diversas situações em sala de aula, como a atividade principal deste trabalho que utilizou conceitos da Aritmética Modular para explorar situações que envolvam jogos lineares finitos e utilizem como estratégia de solução, a resolução de sistemas lineares não apenas no conjunto dos números reais, mas também em $\mathbb{Z}_m$, que é algo pouco explorado na Educação Básica.

Em relação aos códigos de barras, é de fundamental importância que se explore atividades básicas sobre sua história, funcionamento e toda estrutura matemática. Até a elaboração deste trabalho, considerava que o armazenamento de informações dos produtos industrializados era feito de forma singular e que cada estabelecimento comercial, tinha suas próprias regras e estratégias de armazenamento. Por exemplo, acreditava que uma mesma mercadoria X era armazenada de forma distinta em diversos estabelecimentos.

Também é de fundamental importância que a Matemática de outros códigos identificadores como CPF, RG, contas bancárias, cartões de credito, boletos bancários entre outras situações, sejam abordadas em sala de aula no decorrer da jornada de estudo no Ensino Básico sendo o site Dígitos Verificadores[4] um bom instrumento para esta prática.

Não devemos omitir a importância da estrutura dos códigos identificadores que utiliza procedimentos matemáticos para minimizar ou evitar erros que poderiam gerar proble-

mas no armazenamento de dados e informações nas inúmeras situações cotidianas que se utilizam destes registros de forma manual ou automática.

Discussão e estudos subsequentes

Nos trabalhos e estudos posteriores é importante ressaltar e mostrar o funcionamento e a qualidade dos novos modelos de códigos de barra e de outros códigos identificadores, juntamente com as novas tecnologias aliadas a Matemática, para que seja possível consolidar ferramentas de reconhecimento e de segurança, viabilizando registros e armazenamento de dados, aumentando a capacidade de detecção de erros e a quantidade de informações num código identificador e, minimizando o tempo gasto nos processamentos.

Também, pode-se estudar a atualização do código ISBN, citado neste trabalho, que desde 1º de janeiro de 2007, passou de 10 para 13 dígitos, com a adoção do prefixo 978. Com isso o dígito verificador sofrerá alterações. O objetivo da atualização foi aumentar a capacidade do sistema, devido ao crescente número de publicações, com suas edições e formatos.

Referências Bibliográficas

[1] AGÊNCIA BRASILEIRA DO ISBN. Disponível em: <http://www.isbn.bn.br/>. Acesso em 20/03/2013.

[2] BARCODE ISLAND. Disponível em: <http://www.barcodeisland.com/ean13.phtml./>. Acesso em 22/03/2013.

[3] EBAH (A rede social para o compartilhamento acadêmico). A evolução do código de barras e o surgimento da realidade aumentada e sua ulilização na administração moderna. Disponível em: <http://www.ebah.com.br/content/ABAAABjgsAJ/a-evolucao-codigo-barras-surgimento-realidade-aumentada-sua-utilização-na-administracao-moderna/>. Acesso em 30/01/2013.

[4] GHIORZI, Telmo. Dígitos verificadores. Disponível em: <http://ghiorzi.org/cgcancpf.htm./>. Acesso em 04/02/2013.

[5] GRECO, Alessandro(As aventuras na História - Códigos de barras). Guia do estudante.Disponível em: <http://www.guia do estudante.abril.com.br/aventuras-historia/codigo-barras-434117.shtml/>. Acesso em 01/03/2013.

[6] GS1 BRASIL (Associação Brasileira de Automação). Disponível em: <http://www.gs1br.org/>. Acesso em 26/02/2013.

[7] HEFEZ, Abramo.Elementos de aritmética. 2.ed. Rio de Janeiro: SBM, 2011. (Coleção do Professor de Matemática)

[8] MILIES, Francisco César Polcino e COELHO, Sonia Pitta. Números: Uma introdução à Matemática. 3. ed. 2. reimpr. - São Paulo: Editora da Universidade de São Paulo, 2006. (Acadêmia; 20).

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

[10] POOLE, David. Álgebra linear. São Paulo: Pioneira Thomson Lcarninz, 2004.

[11] PORTAL DO PROFESSOR. Disponível em: <http://portaldoprof=18763essor.mec.gov.br/fichaTecnicaAula.html?aula/>. Acesso em 20/03/2013.

[12] WIKIPÉDIA (A enciclopédia livre). Disponível em: <http://pt.wikipedia.org/>. Acesso em 14/02/2013.